# Modelo ng Data ng Mga Na-verify na Kredensyal v1.1

[Rekomendasyon ng W3C](https://www.w3.org/standards/types#REC) 03 Marso 2022

Higit pang mga detalye tungkol sa dokumentong ito

**Ang bersyon na ito:**

<https://www.w3.org/TR/2022/REC-vc-data-model-20220303/>

**Pinakabagong nai-publish na bersyon:**

<https://www.w3.org/TR/vc-data-model/>

**Pinakabagong draft ng editor:**

<https://w3c.github.io/vc-data-model/>

**Kasaysayan:**

<https://www.w3.org/standards/history/vc-data-model>

[Gumawa ng kasaysayan](https://github.com/w3c/vc-data-model/commits/)

**Ulat sa pagpapatupad:**

<https://w3c.github.io/vc-test-suite/implementations/>

**Mga editor:**

[Manu Sporny](https://www.linkedin.com/in/manusporny/) ( [Digital Bazaar](https://digitalbazaar.com/) ) (v1.0, v1.1)

[Grant Noble](https://www.linkedin.com/in/grant-noble-8253994a/) ( [ConsenSys](https://consensys.net/) ) (v1.0)

[Dave Longley](https://github.com/dlongley) ( [Digital Bazaar](https://digitalbazaar.com/) ) (v1.0)

[Daniel C. Burnett](https://www.linkedin.com/in/daburnett/) ( [ConsenSys](https://consensys.net/) ) (v1.0)

[Brent Zundel](https://www.linkedin.com/in/bzundel/) ( [Evernym](https://www.evernym.com/) ) (v1.0)

[Kyle Den Hartog](https://www.linkedin.com/in/kyledenhartog/) ( [MATTR](https://mattr.global/) ) (v1.1)

**Mga may-akda:**

[Manu Sporny](https://digitalbazaar.com/) ( [Digital Bazaar](https://digitalbazaar.com/) )

[Dave Longley](https://digitalbazaar.com/) ( [Digital Bazaar](https://digitalbazaar.com/) )

[David Chadwick](https://www.linkedin.com/in/david-chadwick-36816395/) ( [Unibersidad ng Kent](https://www.kent.ac.uk/) )

**Feedback:**

[GitHub w3c/vc-data-model](https://github.com/w3c/vc-data-model/) ( [mga pull request](https://github.com/w3c/vc-data-model/pulls/) , [bagong isyu](https://github.com/w3c/vc-data-model/issues/new/choose) , [bukas na isyu](https://github.com/w3c/vc-data-model/issues/) )

**Errata:**

[Umiiral ang Errata](https://w3c.github.io/vc-data-model/errata.html) .

Tingnan din [**ang mga pagsasalin**](https://www.w3.org/Translations/?technology=vc-data-model) .

[Copyright](https://www.w3.org/Consortium/Legal/ipr-notice#Copyright) © 2022 [W3C](https://www.w3.org/)® ( [MIT](https://www.csail.mit.edu/) , [ERCIM](https://www.ercim.eu/) , [Keio](https://www.keio.ac.jp/) , [Beihang](https://ev.buaa.edu.cn/) ). [Nalalapat ang pananagutan](https://www.w3.org/Consortium/Legal/ipr-notice#Legal_Disclaimer) ng W3C , [trademark](https://www.w3.org/Consortium/Legal/ipr-notice#W3C_Trademarks) at pinahihintulutang mga panuntunan sa [lisensya ng dokumento .](https://www.w3.org/Consortium/Legal/2015/copyright-software-and-document" \o "Paunawa at Lisensya ng W3C Software at Dokumento)

Abstract

[Ang mga kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-credential) ay bahagi ng ating pang-araw-araw na buhay; Ang mga lisensya sa pagmamaneho ay ginagamit upang igiit na tayo ay may kakayahang magpatakbo ng isang sasakyang de-motor, ang mga degree sa unibersidad ay maaaring gamitin upang igiit ang ating antas ng edukasyon, at ang mga pasaporte na ibinigay ng pamahalaan ay nagbibigay-daan sa amin upang makapaglakbay sa pagitan ng mga bansa. Ang pagtutukoy na ito ay nagbibigay ng mekanismo upang ipahayag ang mga ganitong uri ng mga [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) sa Web sa paraang cryptographically secure, paggalang sa privacy, at machine-verify.

Katayuan ng Dokumentong Ito

*Inilalarawan ng seksyong ito ang katayuan ng dokumentong ito sa oras ng paglalathala nito. Ang isang listahan ng kasalukuyang mga publikasyong W3C at ang pinakabagong rebisyon ng teknikal na ulat na ito ay makikita sa*[*W3C technical reports index*](https://www.w3.org/TR/)*sa https://www.w3.org/TR/.*

Ang mga komento tungkol sa detalyeng ito ay malugod na tinatanggap anumang oras, ngunit dapat malaman ng mga mambabasa na ang panahon ng komento tungkol sa partikular na bersyon ng dokumentong ito ay natapos na at ang Working Group ay hindi gagawa ng mga makabuluhang pagbabago sa bersyong ito ng detalye sa yugtong ito. Mangyaring maghain ng mga isyu nang direkta sa [GitHub](https://github.com/w3c/vc-data-model/issues/) , o ipadala ang mga ito sa [public-vc-comments@w3.org](mailto:public-vc-comments@w3.org) ( mag [-subscribe](mailto:public-vc-comments-request@w3.org?subject=subscribe) , [archives](https://lists.w3.org/Archives/Public/public-vc-comments/) ).

Nakatanggap ang Working Group ng feedback sa pagpapatupad na nagpapakita na mayroong hindi bababa sa dalawang pagpapatupad para sa bawat normative feature sa detalye. Ang grupo ay nakakuha ng mga ulat mula sa labing-apat (14) na pagpapatupad. Para sa mga detalye, tingnan ang [test suite](https://github.com/w3c/vc-test-suite/) at [ulat ng pagpapatupad](https://w3c.github.io/vc-test-suite/implementations/) .

Ang dokumentong ito ay nai-publish ng [Verifiable Credentials Working Group](https://www.w3.org/groups/wg/vc) bilang isang Rekomendasyon gamit ang [Recommendation track](https://www.w3.org/2021/Process-20211102/#recs-and-notes) .

Inirerekomenda ng W3C ang malawak na pag-deploy ng detalyeng ito bilang pamantayan para sa Web.

Ang Rekomendasyon ng W3C ay isang detalye na, pagkatapos ng malawakang pagbuo ng pinagkasunduan, ay ineendorso ng W3C at ng mga Miyembro nito, at may mga pangako mula sa mga miyembro ng Working Group sa [walang royalty na paglilisensya](https://www.w3.org/Consortium/Patent-Policy/" \l "sec-Requirements) para sa mga pagpapatupad.

Ang dokumentong ito ay ginawa ng isang pangkat na tumatakbo sa ilalim ng [W3C Patent Policy](https://www.w3.org/Consortium/Patent-Policy/) . Ang W3C ay nagpapanatili ng isang [pampublikong listahan ng anumang mga pagsisiwalat ng patent na](https://www.w3.org/groups/wg/vc/ipr) ginawa kaugnay ng mga naihatid ng grupo; Kasama rin sa page na iyon ang mga tagubilin para sa pagsisiwalat ng patent. Ang isang indibidwal na may aktwal na kaalaman sa isang patent na pinaniniwalaan ng indibidwal na naglalaman ng [(mga) Mahahalagang Claim](https://www.w3.org/Consortium/Patent-Policy/#def-essential) ay dapat ibunyag ang impormasyon alinsunod sa [seksyon 6 ng Patakaran sa Patent ng W3C](https://www.w3.org/Consortium/Patent-Policy/" \l "sec-Disclosure) .

Ang dokumentong ito ay pinamamahalaan ng [2 Nobyembre 2021 W3C Process Document](https://www.w3.org/2021/Process-20211102/) .

## 1.Panimula

Ang seksyong ito ay hindi normatibo.

[Ang mga kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-credential) ay bahagi ng ating pang-araw-araw na buhay; Ang mga lisensya sa pagmamaneho ay ginagamit upang igiit na tayo ay may kakayahang magpatakbo ng isang sasakyang de-motor, ang mga degree sa unibersidad ay maaaring gamitin upang igiit ang ating antas ng edukasyon, at ang mga pasaporte na ibinigay ng pamahalaan ay nagbibigay-daan sa amin upang makapaglakbay sa pagitan ng mga bansa. Ang mga [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) na ito ay nagbibigay ng mga benepisyo sa amin kapag ginamit sa pisikal na mundo, ngunit ang kanilang paggamit sa Web ay patuloy na mahirap makuha.

Sa kasalukuyan, mahirap ipahayag ang mga kwalipikasyon sa edukasyon, data ng pangangalagang pangkalusugan, mga detalye ng account sa pananalapi, at iba pang uri ng personal na impormasyong nababasa ng machine-readable ng third-party sa Web [.](https://www.w3.org/TR/vc-data-model/#dfn-verify)Dahil sa kahirapan sa pagpapahayag ng mga digital na [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) sa Web, nagiging mahirap na makatanggap ng parehong mga benepisyo sa pamamagitan ng Web na ibinibigay sa atin ng mga pisikal na [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) sa pisikal na mundo.

Ang pagtutukoy na ito ay nagbibigay ng karaniwang paraan upang ipahayag ang mga [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) sa Web sa paraang cryptographically secure, paggalang sa privacy, at machine-verify.

Para sa mga hindi pamilyar sa mga konseptong nauugnay sa mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) , ang mga sumusunod na seksyon ay nagbibigay ng pangkalahatang-ideya ng:

* Ang mga bahagi na bumubuo ng isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials)
* Ang mga bahagi na bumubuo ng isang [nabe-verify na presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations)
* Isang ecosystem kung saan inaasahang magiging kapaki-pakinabang ang mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) at na-verify na mga [presentasyon](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-presentations)
* Ang mga kaso ng paggamit at mga kinakailangan na nagbigay-alam sa detalyeng ito.

### **1.1Ano ang isang Napapatunayang Kredensyal?**

Ang seksyong ito ay hindi normatibo.

Sa pisikal na mundo, ang isang [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) ay maaaring binubuo ng:

* Impormasyong nauugnay sa pagtukoy sa [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) ng [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) (halimbawa, isang larawan, pangalan, o numero ng pagkakakilanlan)
* Impormasyong nauugnay sa awtoridad na nagbibigay (halimbawa, isang pamahalaang lungsod, pambansang ahensya, o katawan ng sertipikasyon)
* Impormasyong nauugnay sa uri ng [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) na ito (halimbawa, isang Dutch passport, isang American driving license, o isang health insurance card)
* Impormasyong nauugnay sa mga partikular na katangian o pag-aari na iginiit ng awtoridad na nagbigay tungkol sa [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) (halimbawa, nasyonalidad, mga klase ng sasakyang may karapatang magmaneho, o petsa ng kapanganakan)
* Katibayan na nauugnay sa kung paano nakuha ang [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential)
* Impormasyong nauugnay sa mga hadlang sa kredensyal (halimbawa, petsa ng pag-expire, o mga tuntunin ng paggamit).

Ang isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ay maaaring kumatawan sa lahat ng parehong impormasyon na kinakatawan ng isang pisikal na [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) . Ang pagdaragdag ng mga teknolohiya, tulad ng mga digital na lagda, ay ginagawang mas nakikita at mas mapagkakatiwalaan ang mga [nabe-verify na kredensyal kaysa sa kanilang mga pisikal na katapat.](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials)

[Ang mga may hawak](https://www.w3.org/TR/vc-data-model/#dfn-holders) ng [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ay maaaring bumuo ng mga [nabe-verify na presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) at pagkatapos ay ibahagi ang mga [nabe-verify na presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) na ito sa mga [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) upang patunayan na mayroon silang mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) na may ilang partikular na katangian.

Ang parehong [mga nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-credentials) at na-verify na mga [presentasyon](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-presentations) ay maaaring maipadala nang mabilis, na ginagawa itong mas maginhawa kaysa sa kanilang mga pisikal na katapat kapag sinusubukang magtatag ng tiwala sa malayo.

Bagama't sinusubukan ng pagtutukoy na ito na pahusayin ang kadalian ng pagpapahayag ng mga digital na [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) , sinusubukan din nitong balansehin ang layuning ito sa ilang layuning nagpapanatili ng privacy. Ang pagtitiyaga ng digital na impormasyon, at ang kadalian kung saan maaaring makolekta at maiugnay ang magkakaibang mga mapagkukunan ng digital na data, ay binubuo ng isang alalahanin sa privacy na ang paggamit ng mga [kredensyal na](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential)[nabe](https://www.w3.org/TR/vc-data-model/#dfn-verify) -verify at madaling mabasa ng machine ay nagbabanta na lumala. Binabalangkas at sinusubukan ng dokumentong ito na tugunan ang ilan sa mga isyung ito sa Seksyon [7.Mga Pagsasaalang- alang sa Privacy](https://www.w3.org/TR/vc-data-model/#privacy-considerations) . Ang mga halimbawa ng kung paano gamitin ang data model na ito gamit ang mga teknolohiyang nagpapahusay sa privacy, tulad ng mga zero-knowledge proof, ay ibinibigay din sa buong dokumentong ito.

Ang salitang "nabe-verify" sa mga terminong [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) at na-verify na [presentasyon](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-presentations) ay tumutukoy sa katangian ng isang [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) o [pagtatanghal](https://www.w3.org/TR/vc-data-model/" \l "dfn-presentations) bilang maaaring ma- [verify](https://www.w3.org/TR/vc-data-model/#dfn-verify) ng isang [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) , gaya ng tinukoy sa dokumentong ito. Ang pagpapatunay ng isang kredensyal ay hindi nagpapahiwatig na ang katotohanan ng mga [claim](https://www.w3.org/TR/vc-data-model/#dfn-claims) na naka-encode doon ay maaaring masuri; gayunpaman, maaaring isama ng issuer ang mga halaga sa property ng [ebidensya](https://www.w3.org/TR/vc-data-model/" \l "dfn-evidence) upang matulungan ang verifier na ilapat ang kanilang lohika sa negosyo upang matukoy kung ang mga claim ay may sapat na katotohanan para sa kanilang mga pangangailangan.

### **1.2Pangkalahatang-ideya ng Ecosystem**

Ang seksyong ito ay hindi normatibo.

Inilalarawan ng seksyong ito ang mga tungkulin ng mga pangunahing aktor at ang mga ugnayan sa pagitan nila sa isang ecosystem kung saan inaasahang magiging kapaki-pakinabang ang mga [nabe-verify na kredensyal .](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials)Ang isang tungkulin ay isang abstraction na maaaring ipatupad sa maraming iba't ibang paraan. Ang paghihiwalay ng mga tungkulin ay nagmumungkahi ng malamang na mga interface at protocol para sa standardisasyon. Ang mga sumusunod na tungkulin ay ipinakilala sa detalyeng ito:

[**may hawak**](https://www.w3.org/TR/vc-data-model/#dfn-holders)

Ang isang tungkulin na maaaring gampanan ng isang [entity](https://www.w3.org/TR/vc-data-model/#dfn-entities) sa pamamagitan ng pagkakaroon ng isa o higit pang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) at pagbuo ng [mga nabe-verify na presentasyon](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-presentations) mula sa kanila. Kasama sa mga halimbawang may hawak ang mga mag-aaral, empleyado, at mga customer.

[**tagabigay**](https://www.w3.org/TR/vc-data-model/#dfn-issuers)

Isang tungkuling ginagampanan ng isang [entity](https://www.w3.org/TR/vc-data-model/#dfn-entities) sa pamamagitan ng paggigiit ng mga [claim](https://www.w3.org/TR/vc-data-model/#dfn-claims) tungkol sa isa o higit pang mga [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) , paglikha ng isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) mula sa mga [paghahabol](https://www.w3.org/TR/vc-data-model/" \l "dfn-claims) na ito , at pagpapadala ng [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) sa isang may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) . Kabilang sa mga halimbawang issuer ang mga korporasyon, non-profit na organisasyon, asosasyon ng kalakalan, pamahalaan, at indibidwal.

[**paksa**](https://www.w3.org/TR/vc-data-model/#dfn-subjects)

Isang [entity](https://www.w3.org/TR/vc-data-model/#dfn-entities) kung aling mga [claim](https://www.w3.org/TR/vc-data-model/#dfn-claims) ang ginawa. Kabilang sa mga halimbawang paksa ang tao, hayop, at bagay. Sa maraming mga kaso, ang may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) ng isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ay ang paksa, ngunit sa ilang mga kaso ay hindi. Halimbawa, maaaring hawak ng isang magulang (ang may- [ari](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) ) ang [nabe-verify na mga kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ng isang bata (ang [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) ), o ang isang may-ari ng alagang hayop (ang may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) ) ay maaaring may hawak ng [nabe-verify na mga kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ng kanilang alagang hayop (ang [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) ). Para sa higit pang impormasyon tungkol sa mga espesyal na kaso na ito, tingnan ang Appendix[C.Relasyon ng May-hawak ng Paksa](https://www.w3.org/TR/vc-data-model/#subject-holder-relationships) .

[**taga-verify**](https://www.w3.org/TR/vc-data-model/#dfn-verifier)

Isang tungkuling ginagampanan ng isang [entity](https://www.w3.org/TR/vc-data-model/#dfn-entities) sa pamamagitan ng pagtanggap ng isa o higit pang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) , opsyonal sa loob ng isang [nabe-verify na presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) , para sa pagproseso. Kasama sa mga halimbawang verifier ang mga employer, security personnel, at mga website.

[**na-verify na pagpapatala ng data**](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-data-registries)

Isang tungkulin na maaaring gampanan ng isang system sa pamamagitan ng pag-mediate sa paggawa at pag- [verify](https://www.w3.org/TR/vc-data-model/#dfn-verify) ng mga identifier, key, at iba pang nauugnay na data, gaya ng mga [nabe](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) -verify na schema ng kredensyal, mga pagpaparehistro ng pagbawi, mga pampublikong key ng nagbigay, at iba pa, na maaaring kailanganin upang gumamit ng mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) . Ang ilang mga pagsasaayos ay maaaring mangailangan ng mga magkakaugnay na pagkakakilanlan para sa [mga paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) . Kasama sa mga halimbawang na-verify na registry ng data ang mga pinagkakatiwalaang database, mga desentralisadong database, mga database ng government ID, at mga distributed ledger. Kadalasan mayroong higit sa isang uri ng nabe-verify na registry ng data na ginagamit sa isang ecosystem.

Diagram, timeline

Description automatically generated

(img src: <https://www.w3.org/TR/vc-data-model/diagrams/ecosystem.svg>)

*Pigura*1*Ang mga tungkulin at daloy ng impormasyon ay bumubuo ng batayan para sa pagtutukoy na ito.*

TANDAAN

[Pigura1](https://www.w3.org/TR/vc-data-model/#roles)sa itaas ay nagbibigay ng isang halimbawa ng ecosystem kung saan ibababa ang iba pang mga konsepto sa detalyeng ito. Umiiral ang iba pang ecosystem, gaya ng mga protektadong kapaligiran o proprietary system, kung saan nagbibigay din ng benepisyo ang mga [nabe-verify na kredensyal .](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials)

### **1.3Use Cases and Requirements**

Ang seksyong ito ay hindi normatibo.

Ang dokumentong Verifiable Credentials Use Cases [ [VC-USE-CASES](https://www.w3.org/TR/vc-data-model/#bib-vc-use-cases) ] ay nagbabalangkas ng ilang mahahalagang paksa na maaaring maging kapaki-pakinabang sa mga mambabasa, kabilang ang:

* Isang mas masusing pagpapaliwanag sa mga [tungkuling](https://www.w3.org/TR/vc-use-cases/" \l "user-roles) ipinakilala sa itaas
* Ang mga [pangangailangang](https://www.w3.org/TR/vc-use-cases/" \l "user-needs) natukoy sa mga vertical ng merkado, gaya ng edukasyon, pananalapi, pangangalagang pangkalusugan, retail, propesyonal na paglilisensya, at pamahalaan
* Mga karaniwang [gawain](https://www.w3.org/TR/vc-use-cases/" \l "user-tasks) na ginagampanan ng mga tungkulin sa ecosystem, pati na rin ang mga nauugnay na kinakailangan ng mga ito
* Mga karaniwang [pagkakasunud-sunod at daloy](https://www.w3.org/TR/vc-use-cases/" \l "user-sequences) na tinukoy ng Working Group.

Bilang resulta ng pagdodokumento at pagsusuri sa dokumento ng mga kaso ng paggamit, ang mga sumusunod na kanais-nais na katangian ng ecosystem ay natukoy para sa detalyeng ito:

* [Ang mga kredensyal ay](https://www.w3.org/TR/vc-data-model/#dfn-credential) kumakatawan sa mga pahayag na ginawa ng isang [nagbigay](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) .
* [Ang mga nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ay kumakatawan sa mga pahayag na ginawa ng isang [tagabigay](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) sa paraang maliwanag at may kinalaman sa privacy.
* [Ang mga may hawak](https://www.w3.org/TR/vc-data-model/#dfn-holders) ay nagsasama-sama ng mga koleksyon ng mga [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) at/o [nabe-verify na mga kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) mula sa iba't ibang [tagabigay](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) sa isang artifact, isang [presentasyon](https://www.w3.org/TR/vc-data-model/" \l "dfn-presentations) .
* Binabago ng mga may hawak ang mga [presentasyon](https://www.w3.org/TR/vc-data-model/" \l "dfn-presentations) sa [mga nabe](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-presentations) -verify na presentasyon para maging maliwanag ang mga ito.
* [Ang mga nag](https://www.w3.org/TR/vc-data-model/#dfn-issuers) -isyu ay maaaring magbigay ng mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) tungkol sa anumang [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) .
* Ang pagkilos bilang [issuer](https://www.w3.org/TR/vc-data-model/#dfn-issuers) , [holder](https://www.w3.org/TR/vc-data-model/#dfn-holders) , o [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) ay hindi nangangailangan ng pagpaparehistro o pag-apruba ng anumang awtoridad, dahil ang tiwala na kasangkot ay bilateral sa pagitan ng mga partido.
* Binibigyang -daan ng mga nabe-verify na [presentasyon ang sinumang taga-](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-presentations)[verify](https://www.w3.org/TR/vc-data-model/#dfn-verifier) na i- [verify](https://www.w3.org/TR/vc-data-model/#dfn-verify) ang pagiging tunay ng mga na- verify na [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-credentials) mula sa sinumang [nagbigay](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) .
* Maaaring makatanggap ang mga may [hawak ng](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders)[mga nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) mula sa sinuman.
* [Maaaring makipag-ugnayan ang mga may hawak](https://www.w3.org/TR/vc-data-model/#dfn-holders) sa sinumang [tagabigay](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) at anumang [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) sa pamamagitan ng anumang ahente ng gumagamit.
* [Ang mga may hawak](https://www.w3.org/TR/vc-data-model/#dfn-holders) ay maaaring magbahagi ng mga [nabe-verify na presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) , na maaaring ma- [verify](https://www.w3.org/TR/vc-data-model/#dfn-verify) nang hindi inilalantad ang pagkakakilanlan ng [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) sa [nagbigay](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) .
* [Ang mga may hawak](https://www.w3.org/TR/vc-data-model/#dfn-holders) ay maaaring mag-imbak ng mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) sa anumang lokasyon, nang hindi naaapektuhan ang kanilang pag- [verify](https://www.w3.org/TR/vc-data-model/#dfn-verify) at nang hindi nalalaman ng [nagbigay](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) ang anumang bagay tungkol sa kung saan sila naka-imbak o kapag sila ay na-access.
* [Ang mga may hawak](https://www.w3.org/TR/vc-data-model/#dfn-holders) ay maaaring magpakita ng mga [nabe-verify na presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) sa anumang [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) nang hindi naaapektuhan ang pagiging tunay ng mga claim at hindi inilalantad ang aksyon na iyon sa [nagbigay](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) .
* Maaaring i-verify ng isang [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) ang mga nabe- [verify na](https://www.w3.org/TR/vc-data-model/#dfn-verify)[presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) mula sa sinumang may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) , na naglalaman ng mga patunay ng mga [claim](https://www.w3.org/TR/vc-data-model/#dfn-claims) mula sa sinumang [nagbigay](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) .
* Hindi dapat nakadepende ang pag- [verify sa mga direktang pakikipag-ugnayan sa pagitan](https://www.w3.org/TR/vc-data-model/#dfn-verify)[ng mga issuer](https://www.w3.org/TR/vc-data-model/#dfn-issuers) at [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) .
* [Hindi dapat ibunyag ng pag- verify](https://www.w3.org/TR/vc-data-model/#dfn-verify) ang pagkakakilanlan ng [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) sa sinumang [nagbigay](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) .
* Ang detalye ay dapat magbigay ng paraan para makapagbigay ang [mga issuer](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) ng mga nabe- verify na [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-credentials) na sumusuporta sa pumipiling pagsisiwalat, nang hindi nangangailangan ng lahat ng conformant software na suportahan ang feature na iyon.
* [Ang mga nag](https://www.w3.org/TR/vc-data-model/#dfn-issuers) -isyu ay maaaring magbigay ng [mga nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-credentials) na sumusuporta sa pumipiling pagsisiwalat.
* Kung sinusuportahan ng isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ang pumipiling pagsisiwalat, maaaring magpakita ang mga may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) ng mga patunay ng mga [claim](https://www.w3.org/TR/vc-data-model/#dfn-claims) nang hindi inilalantad ang buong [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) .
* Maaaring ibunyag ng mga nabe-verify na [presentasyon ang mga katangian ng isang](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-presentations)[nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) , o matugunan ang mga [hinango na predicate](https://www.w3.org/TR/vc-data-model/" \l "dfn-predicates) na hinihiling ng [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) . [Ang mga nagmula na predicate](https://www.w3.org/TR/vc-data-model/#dfn-predicates) ay mga kundisyon ng Boolean, tulad ng mas malaki kaysa, mas mababa sa, katumbas ng, ay nasa set, at iba pa.
* [Ang mga nag](https://www.w3.org/TR/vc-data-model/#dfn-issuers) -isyu ay maaaring mag-isyu ng mga maaaring bawiin na [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) .
* Ang mga proseso ng cryptographically na nagpoprotekta sa mga [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) at [presentasyon](https://www.w3.org/TR/vc-data-model/" \l "dfn-presentations) , at pag-verify ng mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) at na-verify na mga [presentasyon](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-presentations) , ay dapat na deterministiko, bi-directional, at walang pagkawala. Ang anumang pag-verify ng isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) o na-verify na [presentasyon](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-presentations) ay dapat na nababago sa generic na modelo ng data na tinukoy sa dokumentong ito sa isang deterministikong proseso, upang ang resultang [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) o [presentasyon](https://www.w3.org/TR/vc-data-model/" \l "dfn-presentations) ay semantically at syntactically na katumbas ng orihinal na konstruksyon, upang ito ay maproseso. sa isang interoperable na paraan.
* [Ang mga nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) at na-verify na mga [presentasyon](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-presentations) ay dapat na serializable sa isa o higit pang nababasa ng machine na mga format ng data. Ang proseso ng serialization at/o de-serialization ay kailangang deterministic, bi-directional, at lossless. Ang anumang serialization ng isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) o na-verify na [pagtatanghal](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-presentations) ay kailangang ma-transform sa generic na modelo ng data na tinukoy sa dokumentong ito sa isang deterministikong proseso upang ang resultang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ay maaaring maproseso sa isang interoperable na paraan. Kailangan ding mabuo ang serialized na form mula sa modelo ng data nang walang pagkawala ng data o nilalaman.
* Ang data model at serialization ay dapat na extendable na may kaunting koordinasyon.
* Ang pagpapawalang-bisa ng [nagbigay](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) ay hindi dapat magbunyag ng anumang nakakapagpakilalang impormasyon tungkol sa [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) , sa may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) , sa partikular na [kredensyal na nabe](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-credentials) -verify , o sa [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) .
* [Maaaring ibunyag](https://www.w3.org/TR/vc-data-model/#dfn-issuers) ng mga nag-isyu ang dahilan ng pagbawi.
* [Ang mga nagbigay ng pagpapawalang](https://www.w3.org/TR/vc-data-model/#dfn-issuers) - bisa ng mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ay dapat makilala sa pagitan ng pagbawi para sa cryptographic na integridad (halimbawa, ang signing key ay nakompromiso) kumpara sa pagbawi para sa pagbabago ng status (halimbawa, ang lisensya sa pagmamaneho ay sinuspinde).
* [Ang mga nag- isyu](https://www.w3.org/TR/vc-data-model/#dfn-issuers) ay maaaring magbigay ng serbisyo para sa pag-refresh ng isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) .

### **1.4Pagsunod**

Pati na rin ang mga seksyong minarkahan bilang non-normative, lahat ng mga alituntunin sa pag-akda, diagram, halimbawa, at mga tala sa detalyeng ito ay hindi normatibo. Ang lahat ng iba pa sa detalyeng ito ay normatibo.

Ang mga pangunahing salita ay MAY , MUST , MUST NOT , RECOMMENDED , at DAPAT sa dokumentong ito ay dapat bigyang-kahulugan tulad ng inilarawan sa [BCP 14](https://datatracker.ietf.org/doc/html/bcp14) [ [RFC2119](https://www.w3.org/TR/vc-data-model/#bib-rfc2119) ] [ [RFC8174](https://www.w3.org/TR/vc-data-model/#bib-rfc8174) ] kapag, at kapag lamang, lumilitaw ang mga ito sa lahat ng capitals, tulad ng ipinapakita dito.

Ang isang **sumusunod na dokumento** ay anumang konkretong pagpapahayag ng modelo ng data na sumusunod sa mga normatibong pahayag sa detalyeng ito. Sa partikular, lahat ng nauugnay na normatibong pahayag sa Mga Seksyon [4.Pangunahing Konsepto](https://www.w3.org/TR/vc-data-model/#basic-concepts) ,[5.Mga Advanced na Konsepto](https://www.w3.org/TR/vc-data-model/#advanced-concepts) , at [6.](https://www.w3.org/TR/vc-data-model/#syntaxes)DAPAT ipatupad ang mga [syntax](https://www.w3.org/TR/vc-data-model/#syntaxes) ng dokumentong ito . DAPAT na deterministic, bi-directional, at lossless ang format ng serialization para sa sumusunod na dokumento gaya ng inilalarawan sa Seksyon[6.Mga Syntax](https://www.w3.org/TR/vc-data-model/#syntaxes) . Ang [naaayon na dokumento ay](https://www.w3.org/TR/vc-data-model/" \l "dfn-conforming-document)MAAARING ipadala o itago sa anumang format ng serialization.

Ang isang **sumusunod na processor** ay anumang algorithm na natanto bilang software at/o hardware na bumubuo o gumagamit ng isang [sumusunod na dokumento](https://www.w3.org/TR/vc-data-model/" \l "dfn-conforming-document) . DAPAT gumawa ng mga error ang mga sumusunod na processor kapag ang mga hindi sumusunod na dokumento ay natupok.

Ang detalyeng ito ay hindi gumagawa ng mga normatibong pahayag patungkol sa pagsang-ayon ng mga tungkulin sa ecosystem, gaya ng mga nag- [isyu](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) , may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) , o mga taga- [verify](https://www.w3.org/TR/vc-data-model/#dfn-verifier) , dahil ang pagsang-ayon ng mga tungkulin sa ecosystem ay lubos na ginagamit, kaso ng paggamit, at partikular sa market vertical.

Ang mga mekanismo ng digital proof, na isang subset ay mga digital signature, ay kinakailangan upang matiyak ang proteksyon ng isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) . Ang pagkakaroon at pagpapatunay ng mga patunay, na maaaring nakadepende sa syntax ng patunay (halimbawa, gamit ang JSON Web Signature ng isang JSON Web Token para sa pagpapatunay ng key holder), ay isang mahalagang bahagi ng pagproseso ng isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) . Sa oras ng paglalathala, ang mga miyembro ng Working Group ay nagpatupad ng mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) gamit ang hindi bababa sa tatlong patunay na mekanismo:

* Na-secure ang JSON Web Token [ [RFC7519](https://www.w3.org/TR/vc-data-model/#bib-rfc7519) ] gamit ang JSON Web Signatures [ [RFC7515](https://www.w3.org/TR/vc-data-model/#bib-rfc7515) ]
* Mga Katibayan ng Integridad ng Data [ [DATA-INTEGRITY](https://www.w3.org/TR/vc-data-model/#bib-data-integrity) ]
* Camenisch-Lysyanskaya Zero-Knowledge Proofs [ [CL-SIGNATURES](https://www.w3.org/TR/vc-data-model/#bib-cl-signatures) ].

Pinapayuhan ang mga tagapagpatupad na tandaan na hindi lahat ng mekanismo ng patunay ay na-standardize sa petsa ng paglalathala ng detalyeng ito. Inaasahan ng grupo na ang ilan sa mga mekanismong ito, gayundin ang mga bago, ay mag-iisa na mag-mature at maging standardized sa oras. Dahil mayroong maraming wastong mekanismo ng patunay, ang pagtutukoy na ito ay hindi nag-standardize sa alinmang mekanismo ng digital na lagda. Ang isa sa mga layunin ng pagtutukoy na ito ay magbigay ng modelo ng data na maaaring protektahan ng iba't ibang mga mekanismo ng digital proof sa kasalukuyan at hinaharap. Ang pagsunod sa detalyeng ito ay hindi nakadepende sa mga detalye ng isang partikular na mekanismo ng patunay; nangangailangan ito ng malinaw na pagtukoy sa mekanismo na ginagamit ng isang [napapatunayang kredensyal .](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-credentials)

Ang dokumentong ito ay naglalaman din ng mga halimbawa na naglalaman ng JSON at JSON-LD na nilalaman. Ang ilan sa mga halimbawang ito ay naglalaman ng mga character na di-wastong JSON, tulad ng mga inline na komento ( //) at ang paggamit ng ellipsis ( ...) upang tukuyin ang impormasyon na nagdaragdag ng maliit na halaga sa halimbawa. Ang mga nagpapatupad ay binabalaan na alisin ang nilalamang ito kung nais nilang gamitin ang impormasyon bilang wastong JSON o JSON-LD.

## 2.Terminolohiya

Ang seksyong ito ay hindi normatibo.

Ang mga sumusunod na termino ay ginagamit upang ilarawan ang mga konsepto sa detalyeng ito.

**paghahabol**

Isang paninindigan na ginawa tungkol sa isang [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) .

**kredensyal**

Isang set ng isa o higit pang mga [claim](https://www.w3.org/TR/vc-data-model/#dfn-claims) na ginawa ng isang [issuer](https://www.w3.org/TR/vc-data-model/#dfn-issuers) . Ang **nabe-verify na kredensyal** ay isang tamper-evident na kredensyal na may akda na maaaring ma-verify sa pamamagitan ng cryptographic. Maaaring gamitin ang mga nabe-verify na kredensyal upang bumuo [ng mga nabe-verify na presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) , na maaari ding ma-verify sa pamamagitan ng cryptographic. Ang mga [claim](https://www.w3.org/TR/vc-data-model/#dfn-claims) sa isang kredensyal ay maaaring tungkol sa iba't ibang [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) .

**pagliit ng data**

Ang pagkilos ng paglilimita sa dami ng nakabahaging data nang mahigpit sa pinakamababang kinakailangan upang matagumpay na maisakatuparan ang isang gawain o layunin.

**desentralisadong identifier**

Isang portable na URL-based na identifier, na kilala rin bilang isang **DID** , na nauugnay sa isang [entity](https://www.w3.org/TR/vc-data-model/#dfn-entities) . Ang mga identifier na ito ay kadalasang ginagamit sa isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) at nauugnay sa mga [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) kung kaya't ang isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) mismo ay madaling ma-port mula sa isang [repositoryo](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential-repository) patungo sa isa pa nang hindi na kailangang ibigay muli ang [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) . Ang isang halimbawa ng isang DID ay did:example:123456abcdef.

**desentralisadong dokumento ng pagkakakilanlan**

Tinutukoy din bilang isang **DID na dokumento** , ito ay isang dokumentong naa-access gamit ang isang [nabe-verify na registry ng data](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-data-registries) at naglalaman ng impormasyong nauugnay sa isang partikular na [desentralisadong identifier](https://www.w3.org/TR/vc-data-model/" \l "dfn-decentralized-identifiers) , tulad ng nauugnay na [repositoryo](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential-repository) at pampublikong key na impormasyon.

**hango na panaguri**

Isang nabe-verify, boolean na assertion tungkol sa halaga ng isa pang katangian sa isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) . Ang mga ito ay kapaki-pakinabang sa zero-knowledge-proof-style na [nabe-verify na mga presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) dahil maaari nilang limitahan ang pagsisiwalat ng impormasyon. Halimbawa, kung ang isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ay naglalaman ng isang katangian para sa pagpapahayag ng isang partikular na taas sa sentimetro, ang isang hinangong predicate ay maaaring sumangguni sa katangian ng taas sa na- verify na [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-credentials) na nagpapakita na ang nag- [isyu](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) ay nagpapatunay sa isang halaga ng taas na nakakatugon sa minimum na kinakailangan sa taas, nang hindi aktwal na ibinubunyag ang partikular na halaga ng taas. Halimbawa, ang [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) ay mas mataas sa 150 sentimetro.

**nilalang**

Isang bagay na may kakaiba at independiyenteng pag-iral, gaya ng isang tao, organisasyon, o device na gumaganap ng isa o higit pang mga tungkulin sa ecosystem.

**graph**

Isang network ng impormasyon na binubuo ng mga [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) at ang kanilang kaugnayan sa iba pang mga [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) o data.

**may hawak**

Ang isang tungkuling maaaring gampanan ng isang [entity](https://www.w3.org/TR/vc-data-model/#dfn-entities) sa pamamagitan ng pagkakaroon ng isa o higit pang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) at pagbuo ng [mga presentasyon](https://www.w3.org/TR/vc-data-model/" \l "dfn-presentations) mula sa kanila. Ang isang may hawak ay karaniwang, ngunit hindi palaging, isang [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) ng [nabe-verify na mga kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) na hawak nila. Iniimbak ng mga may hawak ang kanilang mga [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) sa mga [imbakan ng kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential-repository) .

**tagapagbigay ng pagkakakilanlan**

Ang isang tagapagbigay ng pagkakakilanlan, kung minsan ay dinadaglat bilang IdP , ay isang sistema para sa paglikha, pagpapanatili, at pamamahala ng impormasyon ng pagkakakilanlan para sa mga may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) , habang nagbibigay ng mga serbisyo sa pagpapatotoo sa [mga umaasa](https://www.w3.org/TR/vc-data-model/" \l "dfn-relying-parties) na aplikasyon ng partido sa loob ng isang federation o distributed network. Sa kasong ito ang may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) ay palaging ang [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) . Kahit na ang mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ay mga [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) ng may hawak , ipinapalagay na ang mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ay nananatili sa [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects), at kung hindi, ninakaw sila ng isang umaatake. Ang pagtutukoy na ito ay hindi gumagamit ng terminong ito maliban kung paghahambing o pagmamapa ng mga konsepto sa dokumentong ito sa iba pang mga detalye. Hinahati ng detalyeng ito ang konsepto ng [tagapagbigay ng pagkakakilanlan](https://www.w3.org/TR/vc-data-model/" \l "dfn-identity-providers) sa dalawang magkaibang konsepto: ang [nagbigay](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) at ang may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) .

**tagabigay**

Ang isang tungkulin na maaaring gampanan ng isang [entity](https://www.w3.org/TR/vc-data-model/#dfn-entities) sa pamamagitan ng paggigiit ng mga [claim](https://www.w3.org/TR/vc-data-model/#dfn-claims) tungkol sa isa o higit pang mga [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) , paglikha ng [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) mula sa mga [paghahabol](https://www.w3.org/TR/vc-data-model/" \l "dfn-claims) na ito , at pagpapadala ng [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) sa isang may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) .

**pagtatanghal**

Ang data na nakuha mula sa isa o higit pang [nabe-verify na mga kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) , na ibinigay ng isa o higit pang [mga issuer](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) , na ibinabahagi sa isang partikular na [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) . Ang **nabe-verify na presentasyon** ay isang tamper-evident na presentasyon na naka-encode sa paraang mapagkakatiwalaan ang pagiging may-akda ng data pagkatapos ng proseso ng cryptographic na pag-verify. Ang ilang partikular na uri ng mga nabe-verify na presentasyon ay maaaring maglaman ng data na na-synthesize mula sa, ngunit hindi naglalaman ng, orihinal na mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) (halimbawa, mga zero-knowledge proof).

**imbakan**

Isang programa, gaya ng storage vault o personal na [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) na wallet, na nag-iimbak at nagpoprotekta sa access sa mga [nabe-verify na kredensyal ng mga may](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials)[hawak](https://www.w3.org/TR/vc-data-model/#dfn-holders) .

**piling pagsisiwalat**

Ang kakayahan ng isang may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) na gumawa ng mga desisyon tungkol sa kung anong impormasyon ang ibabahagi.

**paksa**

Isang bagay tungkol sa kung saan ang mga [paghahabol](https://www.w3.org/TR/vc-data-model/" \l "dfn-claims) ay ginawa.

**pagpapatunay**

Ang katiyakan na ang isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) o isang na-verify na [presentasyon](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-presentations) ay nakakatugon sa mga pangangailangan ng isang [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) at iba pang umaasa na mga stakeholder. Ang detalyeng ito ay napipilitan sa pag- [verify ng mga](https://www.w3.org/TR/vc-data-model/#dfn-verify)[nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) at na-verify na mga [presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) anuman ang kanilang paggamit. Ang pagpapatunay ng mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) o na-verify na mga [presentasyon](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-presentations) ay wala sa saklaw ng detalyeng ito.

**na-verify na pagpapatala ng data**

Isang tungkulin na maaaring gampanan ng isang system sa pamamagitan ng pag-mediate sa paggawa at pag- [verify](https://www.w3.org/TR/vc-data-model/#dfn-verify) ng mga identifier, key, at iba pang nauugnay na data, gaya ng mga [nabe](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) -verify na schema ng kredensyal, mga pagpaparehistro ng pagbawi, mga pampublikong key ng nagbigay, at iba pa, na maaaring kailanganin upang gumamit ng mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) . Ang ilang mga pagsasaayos ay maaaring mangailangan ng mga magkakaugnay na pagkakakilanlan para sa [mga paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) . Ang ilang mga registry, tulad ng para sa mga UUID at pampublikong key, ay maaaring kumilos lamang bilang mga namespace para sa mga identifier.

**pagpapatunay**

Ang pagsusuri kung ang isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) o na-verify na [presentasyon](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-presentations) ay isang tunay at napapanahong pahayag ng nagbigay o nagtatanghal, ayon sa pagkakabanggit. Kabilang dito ang pagsuri na: ang kredensyal (o presentasyon) ay sumusunod sa detalye; ang paraan ng patunay ay nasiyahan; at, kung naroroon, magtagumpay ang pagsusuri sa katayuan. Ang pag-verify ng isang kredensyal ay hindi nagpapahiwatig ng pagsusuri sa katotohanan ng mga [claim](https://www.w3.org/TR/vc-data-model/#dfn-claims) na naka-encode sa kredensyal.

**taga-verify**

Isang tungkuling ginagampanan ng isang [entity](https://www.w3.org/TR/vc-data-model/#dfn-entities) sa pamamagitan ng pagtanggap ng isa o higit pang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) , opsyonal sa loob ng isang [nabe-verify na presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) para sa pagproseso. Ang ibang mga detalye ay maaaring sumangguni sa konseptong ito bilang isang **umaasa na partido** .

**URI**

Isang Uniform Resource Identifier, gaya ng tinukoy ng [ [RFC3986](https://www.w3.org/TR/vc-data-model/#bib-rfc3986) ].

### **4.4Paksa ng kredensyal**

Ang isang [nabe-verify na kredensyal ay](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) naglalaman ng mga [claim](https://www.w3.org/TR/vc-data-model/#dfn-claims) tungkol sa isa o higit pang mga [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) . Tinutukoy ng detalyeng ito ang isang credentialSubject [katangian](https://www.w3.org/TR/vc-data-model/" \l "dfn-property) para sa pagpapahayag ng mga [paghahabol](https://www.w3.org/TR/vc-data-model/" \l "dfn-claims) tungkol sa isa o higit pang mga [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) .

DAPAT may ari- [arian](https://www.w3.org/TR/vc-data-model/" \l "dfn-property) ang isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) . credentialSubject

**kredensyalPaksa**

Ang halaga ng ari- credentialSubject [arian](https://www.w3.org/TR/vc-data-model/" \l "dfn-property) ay tinukoy bilang isang hanay ng mga bagay na naglalaman ng isa o higit pang mga katangian na bawat isa ay nauugnay sa isang [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) ng [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) . Ang bawat bagay ay MAAARING maglaman idng , gaya ng inilarawan sa Seksyon[4.2Mga Identifier](https://www.w3.org/TR/vc-data-model/#identifiers) .

Credential

{

"@context": [

"https://www.w3.org/2018/credentials/v1",

"https://www.w3.org/2018/credentials/examples/v1"

],

"id": "http://example.edu/credentials/3732",

"type": ["VerifiableCredential", "UniversityDegreeCredential"],

"issuer": "https://example.edu/issuers/565049",

"issuanceDate": "2010-01-01T00:00:00Z",

**"credentialSubject"** : {

"id": "did:example:ebfeb1f712ebc6f1c276e12ec21",

"degree": {

"type": "BachelorDegree",

"pangalan": "Bachelor ng Agham at Sining"

}

}

}

Verifiable Credential (may patunay)

{   
 "@context": [   
 "https://www.w3.org/2018/credentials/v1",   
 "https://www.w3.org/2018/credentials/examples/v1",   
 "https:// w3id.org/security/suites/ed25519-2020/v1"   
 ],   
 "id": "http://example.edu/credentials/3732",   
 "type": [   
 "VerifiableCredential",   
 "UniversityDegreeCredential"   
 ],   
 "issuer ": "https://example.edu/issuers/565049",   
 "issuanceDate": "2010-01-01T00:00:00Z",   
 "credentialSubject": {   
 "id": "did:example:ebfeb1f712ebc6f1c276",   
 " ce12ec degree": {   
 "uri":"BachelorDegree",   
 "name": "Bachelor of Science and Arts"   
 }   
 },   
 "proof": {  
 "type": "Ed25519Signature2020",   
 "created": "2022-02-25T14:58:43Z",   
 "verificationMethod": "https://example.edu/issuers/565049#key-1",   
 "proofPurpose": "assertionMethod",   
 "proofValue": "zeEdUoM7m9cY8ZyTpey83yBKeBcmcvbyrEQzJ19rD2UXArU2U1jPGoEt   
rRvGYppdiK37GU4NBeoPakxpWhAvsVSt"   
 }   
}

Verifiable Credential (bilang JWT)

---------------- JWT header ---------------   
{   
 "alg": "ES256",   
 "typ": "JWT"   
​​}   
--------------- JWT payload ---------------   
// TANDAAN: Ang halimbawa sa ibaba ay gumagamit ng wastong VC-JWT serialization   
// na duplicate ang iss, nbf, jti, at mga sub na field sa   
// Na-verify na Kredensyal (vc) na field.   
{   
 "vc": {   
 "@context": [   
 "https://www.w3.org/2018/credentials/v1",   
 "https://www.w3.org/2018/credentials/examples/v1"   
 ] ,   
 "id": "http://example.edu/credentials/3732",   
 "type": [   
 "VerifiableCredential",   
 "  
  
 "issuer": "https://example.edu/issuers/565049",   
 "issuanceDate": "2010-01-01T00:00:00Z",   
 "credentialSubject": {   
 "id": "did:example:ebfeb1f712ebc6f1c271"ebfeb1f712ebc6f1c276e ,   
 "degree": {   
 "type": "BachelorDegree",   
 "name": "Bachelor of Science and Arts"   
 }   
 }   
 },   
 "iss": "https://example.edu/issuers/565049",   
 "nbf" : 1262304000,   
 "jti": "http://example.edu/credentials/3732",   
 "sub": "did:example:ebfeb1f712ebc6f1c276e12ec21"  
}   
--------------- JWT ---------------   
eyJhbGciOiJFUzI1NiIsInR5cCI6IkpXVCJ9.eyJ2YyI6eyJAY29udGV4dCI6WyJodHRwczovL3  
d3dy53My5vcmcvMjAxOC9jcmVkZW50aWFscy92MSIsImh0dHBzOi8vd3d3LnczLm9yZy8yMDE4L   
2NyZWRlbnRpYWxzL2V4YW1wbGVzL3YxIl0sImlkIjoiaHR0cDovL2V4YW1wbGUuZWR1L2NyZWRl   
bnRpYWxzLzM3MzIiLCJ0eXBlIjpbIlZlcmlmaWFibGVDcmVkZW50aWFsIiwiVW5pdmVyc2l0eUR   
lZ3JlZUNyZWRlbnRpYWwiXSwiaXNzdWVyIjoiaHR0cHM6Ly9leGFtcGxlLmVkdS9pc3N1ZXJzLz   
U2NTA0OSIsImlzc3VhbmNlRGF0ZSI6IjIwMTAtMDEtMDFUMDA6MDA6MDBaIiwiY3JlZGVudGlhb   
FN1YmplY3QiOnsiaWQiOiJkaWQ6ZXhhbXBsZTplYmZlYjFmNzEyZWJjNmYxYzI3NmUxMmVjMjEi   
LCJkZWdyZWUiOnsidHlwZSI6IkJhY2hlbG9yRGVncmVlIiwibmFtZSI6IkJhY2hlbG9yIG9mIFN   
jaWVuY2UgYW5kIEFydHMifX19LCJpc3MiOiJodHRwczovL2V4YW1wbGUuZWR1L2lzc3VlcnMvNT   
Y1MDQ5IiwibmJmIjoxMjYyMzA0MDAwLCJqdGkiOiJodHRwOi8vZXhhbXBsZS5lZHUvY3JlZGVud  
GlhbHMvMzczMiIsInN1YiI6ImRpZDpleGFtcGxlOmViZmViMWY3MTJlYmM2ZjFjMjc2ZTEyZWMy   
MSJ9.z5vgMTK1nfizNCg5N-niCOL3WUIAL7nXy-nGhfDEZYO8kJfxDZYO8kJfxDZWJ8kJfJfJnXy-nGhDEZYO89   
.

Posibleng ipahayag ang impormasyong nauugnay sa maraming [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) sa isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) . Ang halimbawa sa ibaba ay tumutukoy sa dalawang [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) na mag-asawa. Tandaan ang paggamit ng array notation upang iugnay ang maraming [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) sa credentialSubjectproperty.

[HALIMBAWA7](https://www.w3.org/TR/vc-data-model/#example-specifying-multiple-subjects-in-a-verifiable-credential): Pagtukoy ng maraming paksa sa isang nabe-verify na kredensyal

{

"@context": [

"https://www.w3.org/2018/credentials/v1",

"https://www.w3.org/2018/credentials/examples/v1"

],

"id": "http://example.edu/credentials/3732",

"type": ["VerifiableCredential", "RelationshipCredential"],

"issuer": "https://example.com/issuer/123",

"issuanceDate": "2010-01-01T00:00:00Z",

"credentialSubject": **[{**

**"id": "did:example:ebfeb1f712ebc6f1c276e12ec21",**

**"name": "Jayden Doe",**

**"asawa": "ginawa:halimbawa:c276e12ec21ebfeb1f712ebc6f1"**

**}, {**

**"id": "did:example:c276e12ec21ebfeb1f712ebc6f1",**

**"name": "Morgan Doe",**

**"asawa": "ginawa:example:ebfeb1f712ebc6f1c276e12ec21"**

**}]**

}

### **4.5Tagapagbigay**

Tinutukoy ng detalyeng ito ang isang property para sa pagpapahayag ng [nagbigay](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) ng isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) .

DAPAT may ari- [arian](https://www.w3.org/TR/vc-data-model/" \l "dfn-property) ang isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) . issuer

**tagabigay**

Ang halaga ng issuer [property ay](https://www.w3.org/TR/vc-data-model/#dfn-property)DAPAT na alinman sa isang [URI](https://www.w3.org/TR/vc-data-model/#dfn-uri) o isang bagay na naglalaman ng isang id [property](https://www.w3.org/TR/vc-data-model/#dfn-property) . Inirerekomenda na ang [URI](https://www.w3.org/TR/vc-data-model/#dfn-uri) sa issuero nito iday isa kung saan, kung hindi sanggunian, ay magreresulta sa isang dokumentong naglalaman ng impormasyong nababasa ng makina tungkol sa [nagbigay](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) na maaaring magamit upang i- [verify](https://www.w3.org/TR/vc-data-model/#dfn-verify) ang impormasyong ipinahayag sa [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) .’

[HALIMBAWA8](https://www.w3.org/TR/vc-data-model/#example-usage-of-issuer-property): Paggamit ng ari-arian ng nagbigay

Credential {

"@context": [

"https://www.w3.org/2018/credentials/v1",

"https://www.w3.org/2018/credentials/examples/v1"

],

"id": "http://example.edu/credentials/3732",

"type": ["VerifiableCredential", "UniversityDegreeCredential"],

**"issuer": "https://example.edu/issuers/14"** ,

"issuanceDate": "2010-01-01T19:23:24Z",

"credentialSubject": {

"id": "did:example:ebfeb1f712ebc6f1c276e12ec21",

"degree": {

"type": "BachelorDegree",

"pangalan": "Bachelor ng Agham at Sining"

}

}

}

Verifiable Credential (may patunay)

{   
 "@context": [   
 "https://www.w3.org/2018/credentials/v1",   
 "https://www.w3.org/2018/credentials/examples/v1",   
 "https:// w3id.org/security/suites/ed25519-2020/v1"   
 ],   
 "id": "http://example.edu/credentials/3732",   
 "type": [   
 "VerifiableCredential",   
 "UniversityDegreeCredential"   
 ],   
 "issuer ": "https://example.edu/issuers/14",   
 "issuanceDate": "2010-01-01T19:23:24Z",   
 "credentialSubject": {   
 "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",   
 " degree": {   
 "type": "BachelorDegree",   
 "name": "Bachelor of Science and Arts"   
 }   
 },   
 "proof": {  
 "type": "Ed25519Signature2020",   
 "created": "2022-02-25T14:58:43Z",   
 "verificationMethod": "https://example.edu/issuers/14#key-1",   
 "proofPurpose": "assertionMethod",   
 "proofValue": "z4kWncP1KLByEaSU3oaijUNk8GPGCCgntz8q4Gk55QuMwQe1dsWgSmf7   
RsRNYgfJUChdSV22khsfpBsX7ub14aYbe"   
 }   
}

Verifiable Credential (bilang JWT)  
---------------- JWT header ---------------   
{   
 "alg": "ES256",   
 "typ": "JWT"   
​​}   
--------------- JWT payload ---------------   
// TANDAAN: Ang halimbawa sa ibaba ay gumagamit ng wastong VC-JWT serialization   
// na duplicate ang iss, nbf, jti, at mga sub na field sa   
// Na-verify na Kredensyal (vc) na field.   
{   
 "vc": {   
 "@context": [   
 "https://www.w3.org/2018/credentials/v1",   
 "https://www.w3.org/2018/credentials/examples/v1"   
 ] ,   
 "id": "http://example.edu/credentials/3732",   
 "type": [   
 "VerifiableCredential",   
 "  
  
 "issuer": "https://example.edu/issuers/14",   
 "issuanceDate": "2010-01-01T19:23:24Z",   
 "credentialSubject": {   
 "id": "did:example:ebfeb1f712ebc6f1c276"e12ec276e12ec ,   
 "degree": {   
 "type": "BachelorDegree",   
 "name": "Bachelor of Science and Arts"   
 }   
 }   
 },   
 "iss": "https://example.edu/issuers/14",   
 "nbf" : 1262373804,   
 "jti": "http://example.edu/credentials/3732",   
 "sub": "did:example:ebfeb1f712ebc6f1c276e12ec21"  
}   
--------------- JWT ---------------   
eyJhbGciOiJFUzI1NiIsInR5cCI6IkpXVCJ9.eyJ2YyI6eyJAY29udGV4dCI6WyJodHRwczovL3  
d3dy53My5vcmcvMjAxOC9jcmVkZW50aWFscy92MSIsImh0dHBzOi8vd3d3LnczLm9yZy8yMDE4L   
2NyZWRlbnRpYWxzL2V4YW1wbGVzL3YxIl0sImlkIjoiaHR0cDovL2V4YW1wbGUuZWR1L2NyZWRl   
bnRpYWxzLzM3MzIiLCJ0eXBlIjpbIlZlcmlmaWFibGVDcmVkZW50aWFsIiwiVW5pdmVyc2l0eUR   
lZ3JlZUNyZWRlbnRpYWwiXSwiaXNzdWVyIjoiaHR0cHM6Ly9leGFtcGxlLmVkdS9pc3N1ZXJzLz   
E0IiwiaXNzdWFuY2VEYXRlIjoiMjAxMC0wMS0wMVQxOToyMzoyNFoiLCJjcmVkZW50aWFsU3Via   
mVjdCI6eyJpZCI6ImRpZDpleGFtcGxlOmViZmViMWY3MTJlYmM2ZjFjMjc2ZTEyZWMyMSIsImRl   
Z3JlZSI6eyJ0eXBlIjoiQmFjaGVsb3JEZWdyZWUiLCJuYW1lIjoiQmFjaGVsb3Igb2YgU2NpZW5   
jZSBhbmQgQXJ0cyJ9fX0sImlzcyI6Imh0dHBzOi8vZXhhbXBsZS5lZHUvaXNzdWVycy8xNCIsIm   
5iZiI6MTI2MjM3MzgwNCwianRpIjoiaHR0cDovL2V4YW1wbGUuZWR1L2NyZWRlbnRpYWxzLzM3M  
zIiLCJzdWIiOiJkaWQ6ZXhhbXBsZTplYmZlYjFmNzEyZWJjNmYxYzI3NmUxMmVjMjEifQ.oOoii   
TBKC6zbJ8rx916SSHEKk4Fhc5-gFD8sQh5-   
gFD8sQh6AA

Posible ring magpahayag ng karagdagang impormasyon tungkol sa nagbigay sa pamamagitan ng pag-uugnay ng isang bagay sa ari-arian ng nagbigay:

[HALIMBAWA9](https://www.w3.org/TR/vc-data-model/#example-usage-of-issuer-expanded-property): Paggamit ng issuer expanded property

Credential

{

"@context": [

"https://www.w3.org/2018/credentials/v1",

"https://www.w3.org/2018/credentials/examples/v1"

],

"id": "http://example.edu/credentials/3732",

"type": ["VerifiableCredential", "UniversityDegreeCredential"],

**"tagapagbigay": {**

**"id": "did:example:76e12ec712ebc6f1c221ebfeb1f",**

**"pangalan": "Halimbawang Unibersidad"**

**}** ,

"issuanceDate": "2010-01-01T19:23:24Z",

"credentialSubject": {

"id": "did:example:ebfeb1f712ebc6f1c276e12ec21",

"degree": {

"type": "BachelorDegree",

"pangalan": "Bachelor ng Agham at Sining"

}

}

}

Verifiable Credential (may patunay)

{   
 "@context": [   
 "https://www.w3.org/2018/credentials/v1",   
 "https://www.w3.org/2018/credentials/examples/v1",   
 "https:// w3id.org/security/suites/ed25519-2020/v1"   
 ],   
 "id": "http://example.edu/credentials/3732",   
 "type": [   
 "VerifiableCredential",   
 "UniversityDegreeCredential"   
 ],   
 "issuer ": {   
 "id": "did:example:76e12ec712ebc6f1c221ebfeb1f",   
 "name": "Example University"   
 },   
 "issuanceDate": "2010-01-01T19:23:24Z",   
 "credentialSubject": {   
 "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",   
 "degree": {   
 "type": "BachelorDegree",  
 "name": "Bachelor of Science and Arts"   
 }   
 },   
 "proof": {   
 "type": "Ed25519Signature2020",   
 "created": "2022-02-25T14:58:43Z",   
 "verificationMethod": "ginawa: halimbawa:76e12ec712ebc6f1c221ebfeb1f#key-1", " proofPurpose   
 ": "assertionMethod",   
 "proofValue": " z2Xdmp6YDYz5RPKeRFDcPYorAmnERyr7aRNzv176oLMxwcQUK7GgKxTHj8k   
"

Verifiable Credential (bilang JWT)

---------------- JWT header ---------------   
{   
 "alg": "ES256",   
 "typ": "JWT"   
​​}   
--------------- JWT payload ---------------   
// TANDAAN: Ang halimbawa sa ibaba ay gumagamit ng wastong VC-JWT serialization   
// na duplicate ang iss, nbf, jti, at mga sub na field sa   
// Na-verify na Kredensyal (vc) na field.   
{   
 "vc": {   
 "@context": [   
 "https://www.w3.org/2018/credentials/v1",   
 "https://www.w3.org/2018/credentials/examples/v1"   
 ] ,   
 "id": "http://example.edu/credentials/3732",   
 "type": [   
 "VerifiableCredential",   
 "  
  
  
 "id": "did:example:76e12ec712ebc6f1c221ebfeb1f",   
 "name": "Example University"   
 },   
 "issuanceDate": "2010-01-01T19:23:24Z",   
 "credentialSubject": {   
 "id": "did: halimbawa:ebfeb1f712ebc6f1c276e12ec21",   
 "degree": {   
 "type": "BachelorDegree",   
 "name": "Bachelor of Science and Arts"   
 }   
 }   
 },   
 "iss": {   
 "id": "did:example:76e12ec712ebc1f",6f1b   
 "name": "Example University"   
 },   
 "nbf": 1262373804,   
 "jti": "http://example.edu/credentials/3732",   
 "sub": "did:example:ebfeb1f712ebc6f1c276e12ec21"   
}   
--------------- JWT ----- ----------  
eyJhbGciOiJFUzI1NiIsInR5cCI6IkpXVCJ9.eyJ2YyI6eyJAY29udGV4dCI6WyJodHRwczovL3   
d3dy53My5vcmcvMjAxOC9jcmVkZW50aWFscy92MSIsImh0dHBzOi8vd3d3LnczLm9yZy8yMDE4L   
2NyZWRlbnRpYWxzL2V4YW1wbGVzL3YxIl0sImlkIjoiaHR0cDovL2V4YW1wbGUuZWR1L2NyZWRl   
bnRpYWxzLzM3MzIiLCJ0eXBlIjpbIlZlcmlmaWFibGVDcmVkZW50aWFsIiwiVW5pdmVyc2l0eUR   
lZ3JlZUNyZWRlbnRpYWwiXSwiaXNzdWVyIjp7ImlkIjoiZGlkOmV4YW1wbGU6NzZlMTJlYzcxMm   
ViYzZmMWMyMjFlYmZlYjFmIiwibmFtZSI6IkV4YW1wbGUgVW5pdmVyc2l0eSJ9LCJpc3N1YW5jZ   
URhdGUiOiIyMDEwLTAxLTAxVDE5OjIzOjI0WiIsImNyZWRlbnRpYWxTdWJqZWN0Ijp7ImlkIjoi   
ZGlkOmV4YW1wbGU6ZWJmZWIxZjcxMmViYzZmMWMyNzZlMTJlYzIxIiwiZGVncmVlIjp7InR5cGU   
iOiJCYWNoZWxvckRlZ3JlZSIsIm5hbWUiOiJCYWNoZWxvciBvZiBTY2llbmNlIGFuZCBBcnRzIn  
19fSwiaXNzIjp7ImlkIjoiZGlkOmV4YW1wbGU6NzZlMTJlYzcxMmViYzZmMWMyMjFlYmZlYjFmI   
iwibmFtZSI6IkV4YW1wbGUgVW5pdmVyc2l0eSJ9LCJuYmYiOjEyNjIzNzM4MDQsImp0aSI6Imh0   
dHA6Ly9leGFtcGxlLmVkdS9jcmVkZW50aWFscy8zNzMyIiwic3ViIjoiZGlkOmV4YW1wbGU6ZWJ   
mZWIxZjcxMmViYzZmMWMyNzZlMTJlYzIxIn0.ev4-5Dx9nRy\_RUwWMLvnCJ1i-bizgom5VcyYE0   
TpGsJ7-bPr6NFUh426Yzx5kc5cEh-a0JPPYBqM6jyrgmyvzA

TANDAAN

Ang halaga ng issuer [property](https://www.w3.org/TR/vc-data-model/#dfn-property) ay maaari ding JWK (halimbawa, "https://example.com/keys/foo.jwk") o [DID](https://www.w3.org/TR/vc-data-model/#dfn-decentralized-identifiers) (halimbawa, "did:example:abfe13f712120431c276e12ecab").

Credential

{

"@context": [

"https://www.w3.org/2018/credentials/v1",

"https://www.w3.org/2018/credentials/examples/v1"

],

"id": "http://example.edu/credentials/3732",

"type": ["VerifiableCredential", "UniversityDegreeCredential"],

"issuer": "https://example.edu/issuers/14",

**"issuanceDate": "2010-01-01T19:23:24Z"** ,

"credentialSubject": {

"id": "did:example:ebfeb1f712ebc6f1c276e12ec21",

"degree": {

"type": "BachelorDegree",

"pangalan": "Bachelor ng Agham at Sining"

}

}

}

Verifiable Credential (may patunay)

{   
 "@context": [   
 "https://www.w3.org/2018/credentials/v1",   
 "https://www.w3.org/2018/credentials/examples/v1",   
 "https:// w3id.org/security/suites/ed25519-2020/v1"   
 ],   
 "id": "http://example.edu/credentials/3732",   
 "type": [   
 "VerifiableCredential",   
 "UniversityDegreeCredential"   
 ],   
 "issuer ": "https://example.edu/issuers/14",   
 "issuanceDate": "2010-01-01T19:23:24Z",   
 "credentialSubject": {   
 "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",   
 " degree": {   
 "type": "BachelorDegree",   
 "name": "Bachelor of Science and Arts"   
 }   
 },   
 "proof": {  
 "type": "Ed25519Signature2020",   
 "created": "2022-02-25T14:58:43Z",   
 "verificationMethod": "https://example.edu/issuers/14#key-1",   
 "proofPurpose": "assertionMethod",   
 "proofValue": "z4kWncP1KLByEaSU3oaijUNk8GPGCCgntz8q4Gk55QuMwQe1dsWgSmf7   
RsRNYgfJUChdSV22khsfpBsX7ub14aYbe"   
 }   
}

Verifiable Credential (bilang JWT)

---------------- JWT header ---------------   
{   
 "alg": "ES256",   
 "typ": "JWT"   
​​}   
--------------- JWT payload ---------------   
// TANDAAN: Ang halimbawa sa ibaba ay gumagamit ng wastong VC-JWT serialization   
// na duplicate ang iss, nbf, jti, at mga sub na field sa   
// Na-verify na Kredensyal (vc) na field.   
{   
 "vc": {   
 "@context": [   
 "https://www.w3.org/2018/credentials/v1",   
 "https://www.w3.org/2018/credentials/examples/v1"   
 ] ,   
 "id": "http://example.edu/credentials/3732",   
 "type": [   
 "VerifiableCredential",   
 "  
  
 "issuer": "https://example.edu/issuers/14",   
 "issuanceDate": "2010-01-01T19:23:24Z",   
 "credentialSubject": {   
 "id": "did:example:ebfeb1f712ebc6f1c276"e12ec276e12ec ,   
 "degree": {   
 "type": "BachelorDegree",   
 "name": "Bachelor of Science and Arts"   
 }   
 }   
 },   
 "iss": "https://example.edu/issuers/14",   
 "nbf" : 1262373804,   
 "jti": "http://example.edu/credentials/3732",   
 "sub": "did:example:ebfeb1f712ebc6f1c276e12ec21"  
}   
--------------- JWT ---------------   
eyJhbGciOiJFUzI1NiIsInR5cCI6IkpXVCJ9.eyJ2YyI6eyJAY29udGV4dCI6WyJodHRwczovL3  
d3dy53My5vcmcvMjAxOC9jcmVkZW50aWFscy92MSIsImh0dHBzOi8vd3d3LnczLm9yZy8yMDE4L   
2NyZWRlbnRpYWxzL2V4YW1wbGVzL3YxIl0sImlkIjoiaHR0cDovL2V4YW1wbGUuZWR1L2NyZWRl   
bnRpYWxzLzM3MzIiLCJ0eXBlIjpbIlZlcmlmaWFibGVDcmVkZW50aWFsIiwiVW5pdmVyc2l0eUR   
lZ3JlZUNyZWRlbnRpYWwiXSwiaXNzdWVyIjoiaHR0cHM6Ly9leGFtcGxlLmVkdS9pc3N1ZXJzLz   
E0IiwiaXNzdWFuY2VEYXRlIjoiMjAxMC0wMS0wMVQxOToyMzoyNFoiLCJjcmVkZW50aWFsU3Via   
mVjdCI6eyJpZCI6ImRpZDpleGFtcGxlOmViZmViMWY3MTJlYmM2ZjFjMjc2ZTEyZWMyMSIsImRl   
Z3JlZSI6eyJ0eXBlIjoiQmFjaGVsb3JEZWdyZWUiLCJuYW1lIjoiQmFjaGVsb3Igb2YgU2NpZW5   
jZSBhbmQgQXJ0cyJ9fX0sImlzcyI6Imh0dHBzOi8vZXhhbXBsZS5lZHUvaXNzdWVycy8xNCIsIm   
5iZiI6MTI2MjM3MzgwNCwianRpIjoiaHR0cDovL2V4YW1wbGUuZWR1L2NyZWRlbnRpYWxzLzM3M  
zIiLCJzdWIiOiJkaWQ6ZXhhbXBsZTplYmZlYjFmNzEyZWJjNmYxYzI3NmUxMmVjMjEifQ.6MNXY   
zdnWzepi1\_-OurjRj0yv0aokF1MgWqNmYxYzI3NmUxMmVjMjEifQ.6MNXY zdnWzepi1\_-OurjRj0yv0aokF1MgWqngde-QZKNSUrb-

TANDAAN

Inaasahan na ang susunod na bersyon ng detalyeng ito ay magdaragdag ng ari- validFrom [arian](https://www.w3.org/TR/vc-data-model/" \l "dfn-property) at hindi na gagamitin ang ari- issuanceDate [arian](https://www.w3.org/TR/vc-data-model/" \l "dfn-property) pabor sa isang bagong ari- issued [arian](https://www.w3.org/TR/vc-data-model/" \l "dfn-property) . Ang hanay ng mga halaga para sa parehong mga katangian ay inaasahang mananatili bilang [ [XMLSCHEMA11-2](https://www.w3.org/TR/xmlschema11-2/#dateTime) ] pinagsamang mga date-timestring. Ang mga nagpapatupad ay pinapayuhan na ang validFromat mga ari- issued [arian](https://www.w3.org/TR/vc-data-model/" \l "dfn-property) ay nakalaan at ginagamit para sa anumang iba pang layunin ay hindi hinihikayat.

### **4.7Mga Katibayan (Mga Lagda)**

Hindi bababa sa isang mekanismo ng patunay, at ang mga detalyeng kinakailangan upang suriin ang patunay na iyon, DAPAT ipahayag para sa isang [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) o [pagtatanghal](https://www.w3.org/TR/vc-data-model/" \l "dfn-presentations) upang maging isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) o na-verify na [pagtatanghal](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-presentations) ; ibig sabihin, upang ma- [verify](https://www.w3.org/TR/vc-data-model/#dfn-verify) .

Tinutukoy ng detalyeng ito ang dalawang klase ng mga mekanismo ng patunay: mga panlabas na patunay at mga naka-embed na patunay. Ang isang **panlabas na patunay** ay isa na bumabalot sa isang expression ng modelong ito ng data, tulad ng isang JSON Web Token, na idinetalye sa Seksyon[6.3.1JSON Web Token](https://www.w3.org/TR/vc-data-model/#json-web-token) . Ang isang naka-embed na **patunay** ay isang mekanismo kung saan ang patunay ay kasama sa data, tulad ng isang Linked Data Signature, na idinetalye sa Seksyon[6.3.2Mga Katibayan ng Integridad ng Data](https://www.w3.org/TR/vc-data-model/#data-integrity-proofs) .

Kapag nag-embed ng patunay, DAPAT gamitin ang proof [property .](https://www.w3.org/TR/vc-data-model/#dfn-property)

**patunay**

Isa o higit pang mga cryptographic na patunay na maaaring magamit upang makita ang pakikialam at i-verify ang pagiging may-akda ng isang [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) o [presentasyon](https://www.w3.org/TR/vc-data-model/" \l "dfn-presentations) . Ang partikular na paraan na ginamit para sa isang [naka-embed na patunay ay](https://www.w3.org/TR/vc-data-model/" \l "dfn-embedded-proof)DAPAT isama gamit ang type [property](https://www.w3.org/TR/vc-data-model/#dfn-property) .

Dahil ang paraan na ginagamit para sa isang mathematical proof ay nag-iiba ayon sa representasyong wika at sa teknolohiyang ginamit, ang hanay ng mga pares ng pangalan-halaga na inaasahan bilang ang halaga ng proof [property](https://www.w3.org/TR/vc-data-model/#dfn-property) ay mag-iiba nang naaayon. Halimbawa, kung ang mga digital na lagda ay ginagamit para sa mekanismo ng patunay, ang proof [property](https://www.w3.org/TR/vc-data-model/#dfn-property) ay inaasahang magkakaroon ng mga pares ng pangalan-halaga na may kasamang lagda, isang reference sa nilagdaan na entity, at isang representasyon ng petsa ng pagpirma. Ang halimbawa sa ibaba ay gumagamit ng RSA digital signatures.

[HALIMBAWA11](https://www.w3.org/TR/vc-data-model/#example-usage-of-the-proof-property-on-a-verifiable-credential): Paggamit ng proof property sa isang nabe-verify na kredensyal

{

"@context": [

"https://www.w3.org/2018/credentials/v1",

"https://www.w3.org/2018/credentials/examples/v1"

],

"id": "http://example.gov/credentials/3732",

"type": ["VerifiableCredential", "UniversityDegreeCredential"],

"issuer": "https://example.edu",

"issuanceDate": "2010-01-01T19:23:24Z",

"credentialSubject": {

"id": "did:example:ebfeb1f712ebc6f1c276e12ec21",

"degree": {

"type": "BachelorDegree",

"pangalan": "Bachelor ng Agham at Sining"

}

},

**"patunay": {**

**"type": "Ed25519Signature2020",**

**"nilikha": "2021-11-13T18:19:39Z",**

**"verificationMethod": "https://example.edu/issuers/14#key-1",**

**"proofPurpose": "assertionMethod",**

**"proofValue": "z58DAdFfa9SkqZMVPxAQpic7ndSayn1PzZs6ZjWp1CktyGesjuTSwRdo**

**WhAfGFCF5bppETSTojQCrfFPP2oumHKtz"**

**}**

}

TANDAAN

Gaya ng tinalakay sa Seksyon[1.4Pagsunod](https://www.w3.org/TR/vc-data-model/#conformance) , mayroong maraming mabubuhay na mekanismo ng patunay, at ang detalyeng ito ay hindi nagsa-standardize o nagrerekomenda ng anumang solong patunay na mekanismo para sa paggamit sa mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) . Para sa higit pang impormasyon tungkol sa proofmekanismo, tingnan ang mga sumusunod na detalye: Data Integrity [ [DATA-INTEGRITY](https://www.w3.org/TR/vc-data-model/#bib-data-integrity) ], Linked Data Cryptographic Suites Registries [ [LDP-REGISTRY](https://www.w3.org/TR/vc-data-model/#bib-ldp-registry) ], at JSON Web Signature (JWS) Unencoded Payload Option [ [RFC7797](https://www.w3.org/TR/vc-data-model/#bib-rfc7797) ]. Ang isang listahan ng mga patunay na mekanismo ay makukuha sa Verifiable Credentials Extension Registry [ [VC-EXTENSION-REGISTRY](https://www.w3.org/TR/vc-data-model/#bib-vc-extension-registry) ].

### **4.8Expiration**

Tinutukoy ng detalyeng ito ang expirationDate [property](https://www.w3.org/TR/vc-data-model/#dfn-property) para sa pagpapahayag ng impormasyon sa pag-expire ng [kredensyal .](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential)

**Petsa ng pagkawalang bisa**

Kung naroroon, ang value ng expirationDate [property ay](https://www.w3.org/TR/vc-data-model/#dfn-property)DAPAT na isang string value ng isang [ [XMLSCHEMA11-2](https://www.w3.org/TR/xmlschema11-2/#dateTime) ] na date-timekumakatawan sa petsa at oras na ang [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) ay tumigil na maging wasto.

[HALIMBAWA12](https://www.w3.org/TR/vc-data-model/#example-usage-of-the-expirationdate-property): Paggamit ng expirationDate property

Credential

{

"@context": [

"https://www.w3.org/2018/credentials/v1",

"https://www.w3.org/2018/credentials/examples/v1"

],

"id": "http://example.edu/credentials/3732",

"type": ["VerifiableCredential", "UniversityDegreeCredential"],

"issuer": "https://example.edu/issuers/14",

"issuanceDate": "2010-01-01T19:23:24Z",

**"ExpirationDate": "2020-01-01T19:23:24Z"** ,

"credentialSubject": {

"id": "did:example:ebfeb1f712ebc6f1c276e12ec21",

"degree": {

"type": "BachelorDegree",

"pangalan": "Bachelor ng Agham at Sining"

}

}

}

Verifiable Credential (may patunay)

{   
 "@context": [   
 "https://www.w3.org/2018/credentials/v1",   
 "https://www.w3.org/2018/credentials/examples/v1",   
 "https:// w3id.org/security/suites/ed25519-2020/v1"   
 ],   
 "id": "http://example.edu/credentials/3732",   
 "type": [   
 "VerifiableCredential",   
 "UniversityDegreeCredential"   
 ],   
 "issuer ": "https://example.edu/issuers/14",   
 "issuanceDate": "2010-01-01T19:23:24Z",   
 "expirationDate": "2020-01-01T19:23:24Z",   
 "credentialSubject ": {   
 "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",  
 "degree": {   
 "type": "BachelorDegree",   
 "name": "Bachelor of Science and Arts"   
 }  
 },   
 "proof": {   
 "type": "Ed25519Signature2020",   
 "created": "2022-02-25T14:58:43Z",   
 "verificationMethod": "https://example.edu/issuers/14#key- 1", " proofPurpose   
 ": "assertionMethod",   
 "proofValue": "z3zwi434j3HdZv3C3TJxBnwmmiBgrtzRjM2oeDtZyAEkDeNDBeB9Metc vyB4ZZUvQswKqPdgk5cFSAny   
"

Verifiable Credential (bilang JWT)

---------------- JWT header ---------------   
{   
 "alg": "ES256",   
 "typ": "JWT"   
​​}   
--------------- JWT payload ---------------   
// TANDAAN: Ang halimbawa sa ibaba ay gumagamit ng wastong VC-JWT serialization   
// na duplicate ang iss, nbf, jti, at mga sub na field sa   
// Na-verify na Kredensyal (vc) na field.   
{   
 "vc": {   
 "@context": [   
 "https://www.w3.org/2018/credentials/v1",   
 "https://www.w3.org/2018/credentials/examples/v1"   
 ] ,   
 "id": "http://example.edu/credentials/3732",   
 "type": [   
 "VerifiableCredential",   
 "  
  
 "issuer": "https://example.edu/issuers/14",   
 "issuanceDate": "2010-01-01T19:23:24Z",   
 "expirationDate": "2020-01-01T19:23:24Z",   
 "credentialSubject": {   
 "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",   
 "degree": {   
 "type": "BachelorDegree",   
 "name": "Bachelor of Science and Arts"   
 }   
 }   
 },   
 "exp": 157479066 ,   
 "iss": "https://example.edu/issuers/14",   
 "nbf": 1262373804,   
 "jti": "http://example.edu/credentials/3732",   
 "sub": "did:example:ebfeb1f712ebc6f1c276e12ec21"   
}   
--------------- JWT ---------------  
eyJhbGciOiJFUzI1NiIsInR5cCI6IkpXVCJ9.eyJ2YyI6eyJAY29udGV4dCI6WyJodHRwczovL3   
d3dy53My5vcmcvMjAxOC9jcmVkZW50aWFscy92MSIsImh0dHBzOi8vd3d3LnczLm9yZy8yMDE4L   
2NyZWRlbnRpYWxzL2V4YW1wbGVzL3YxIl0sImlkIjoiaHR0cDovL2V4YW1wbGUuZWR1L2NyZWRl   
bnRpYWxzLzM3MzIiLCJ0eXBlIjpbIlZlcmlmaWFibGVDcmVkZW50aWFsIiwiVW5pdmVyc2l0eUR   
lZ3JlZUNyZWRlbnRpYWwiXSwiaXNzdWVyIjoiaHR0cHM6Ly9leGFtcGxlLmVkdS9pc3N1ZXJzLz   
E0IiwiaXNzdWFuY2VEYXRlIjoiMjAxMC0wMS0wMVQxOToyMzoyNFoiLCJleHBpcmF0aW9uRGF0Z   
SI6IjIwMjAtMDEtMDFUMTk6MjM6MjRaIiwiY3JlZGVudGlhbFN1YmplY3QiOnsiaWQiOiJkaWQ6   
ZXhhbXBsZTplYmZlYjFmNzEyZWJjNmYxYzI3NmUxMmVjMjEiLCJkZWdyZWUiOnsidHlwZSI6IkJ   
hY2hlbG9yRGVncmVlIiwibmFtZSI6IkJhY2hlbG9yIG9mIFNjaWVuY2UgYW5kIEFydHMifX19LC  
JleHAiOjE1Nzc5MDY2MDQsImlzcyI6Imh0dHBzOi8vZXhhbXBsZS5lZHUvaXNzdWVycy8xNCIsI   
m5iZiI6MTI2MjM3MzgwNCwianRpIjoiaHR0cDovL2V4YW1wbGUuZWR1L2NyZWRlbnRpYWxzLzM3   
MzIiLCJzdWIiOiJkaWQ6ZXhhbXBsZTplYmZlYjFmNzEyZWJjNmYxYzI3NmUxMmVjMjEifQ.M4eB   
gls2xrn00dp5JX7UBzEPauEOTWhtMjR-omIIhVHBBI4-ksHH5F6nFHuKo6pDu7W8c-i\_knDTlRr   
1zRp3IA

TANDAAN

Inaasahan na idaragdag ng susunod na bersyon ng detalyeng ito ang validUntil [property](https://www.w3.org/TR/vc-data-model/#dfn-property) sa paraang hindi na ginagamit, ngunit pinapanatili ang pabalik na compatibility sa expirationDate [property](https://www.w3.org/TR/vc-data-model/#dfn-property) . Ang mga nagpapatupad ay pinapayuhan na ang ari- validUntil [arian](https://www.w3.org/TR/vc-data-model/" \l "dfn-property) ay nakalaan at ang paggamit nito para sa anumang iba pang layunin ay hindi hinihikayat.

Credential

{

"@context": [

"https://www.w3.org/2018/credentials/v1",

"https://www.w3.org/2018/credentials/examples/v1"

],

"id": "http://example.edu/credentials/3732",

"type": ["VerifiableCredential", "UniversityDegreeCredential"],

"issuer": "https://example.edu/issuers/14",

"issuanceDate": "2010-01-01T19:23:24Z",

"credentialSubject": {

"id": "did:example:ebfeb1f712ebc6f1c276e12ec21",

"degree": {

"type": "BachelorDegree",

"pangalan": "Bachelor ng Agham at Sining"

}

},

**"CredentialStatus": {**

**"id": "https://example.edu/status/24",**

**"type": "CredentialStatusList2017"**

**}**

}

Verifiable Credential (may patunay)

{   
 "@context": [   
 "https://www.w3.org/2018/credentials/v1",   
 "https://www.w3.org/2018/credentials/examples/v1",   
 "https:// w3id.org/security/suites/ed25519-2020/v1"   
 ],   
 "id": "http://example.edu/credentials/3732",   
 "type": [   
 "VerifiableCredential",   
 "UniversityDegreeCredential"   
 ],   
 "issuer ": "https://example.edu/issuers/14",   
 "issuanceDate": "2010-01-01T19:23:24Z",   
 "credentialSubject": {   
 "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",   
 " degree": {   
 "type": "BachelorDegree",   
 "name": "Bachelor of Science and Arts"   
 }   
 },   
 "credentialStatus": {  
 "id": "https://example.edu/status/24",   
 "type": "CredentialStatusList2017"   
 },   
 "proof": {   
 "type": "Ed25519Signature2020",   
 "created": "2022-02-25T14 :58:43Z",   
 "verificationMethod": "https://example.edu/issuers/14#key-1", " proofPurpose   
 ": "assertionMethod",   
 "proofValue": " z3BXsFfx1qJ5NsTkKqREjQ3AGh6RAmCwvgu1HcDSAHzK3800000   
"

Verifiable Credential (bilang JWT)

---------------- JWT header ---------------   
{   
 "alg": "ES256",   
 "typ": "JWT"   
​​}   
--------------- JWT payload ---------------   
// TANDAAN: Ang halimbawa sa ibaba ay gumagamit ng wastong VC-JWT serialization   
// na duplicate ang iss, nbf, jti, at mga sub na field sa   
// Na-verify na Kredensyal (vc) na field.   
{   
 "vc": {   
 "@context": [   
 "https://www.w3.org/2018/credentials/v1",   
 "https://www.w3.org/2018/credentials/examples/v1"   
 ] ,   
 "id": "http://example.edu/credentials/3732",   
 "type": [   
 "VerifiableCredential",   
 "  
  
 "issuer": "https://example.edu/issuers/14",   
 "issuanceDate": "2010-01-01T19:23:24Z",   
 "credentialSubject": {   
 "id": "did:example:ebfeb1f712ebc6f1c276"e12ec276e12ec ,   
 "degree": {   
 "type": "BachelorDegree",   
 "name": "Bachelor of Science and Arts"   
 }   
 },   
 "credentialStatus": {   
 "id": "https://example.edu/status/24" ,   
 "type": "CredentialStatusList2017"   
 }   
 },   
 "iss": "https://example.edu/issuers/14",   
 "nbf": 1262373804,   
 "jti": "http://example.edu/credentials/3732",   
 "sub": "did:example:ebfeb1f712ebc6f1c276e12ec21"   
}   
--------------- JWT ----- ----------  
eyJhbGciOiJFUzI1NiIsInR5cCI6IkpXVCJ9.eyJ2YyI6eyJAY29udGV4dCI6WyJodHRwczovL3   
d3dy53My5vcmcvMjAxOC9jcmVkZW50aWFscy92MSIsImh0dHBzOi8vd3d3LnczLm9yZy8yMDE4L   
2NyZWRlbnRpYWxzL2V4YW1wbGVzL3YxIl0sImlkIjoiaHR0cDovL2V4YW1wbGUuZWR1L2NyZWRl   
bnRpYWxzLzM3MzIiLCJ0eXBlIjpbIlZlcmlmaWFibGVDcmVkZW50aWFsIiwiVW5pdmVyc2l0eUR   
lZ3JlZUNyZWRlbnRpYWwiXSwiaXNzdWVyIjoiaHR0cHM6Ly9leGFtcGxlLmVkdS9pc3N1ZXJzLz   
E0IiwiaXNzdWFuY2VEYXRlIjoiMjAxMC0wMS0wMVQxOToyMzoyNFoiLCJjcmVkZW50aWFsU3Via   
mVjdCI6eyJpZCI6ImRpZDpleGFtcGxlOmViZmViMWY3MTJlYmM2ZjFjMjc2ZTEyZWMyMSIsImRl   
Z3JlZSI6eyJ0eXBlIjoiQmFjaGVsb3JEZWdyZWUiLCJuYW1lIjoiQmFjaGVsb3Igb2YgU2NpZW5   
jZSBhbmQgQXJ0cyJ9fSwiY3JlZGVudGlhbFN0YXR1cyI6eyJpZCI6Imh0dHBzOi8vZXhhbXBsZS  
5lZHUvc3RhdHVzLzI0IiwidHlwZSI6IkNyZWRlbnRpYWxTdGF0dXNMaXN0MjAxNyJ9fSwiaXNzI   
joiaHR0cHM6Ly9leGFtcGxlLmVkdS9pc3N1ZXJzLzE0IiwibmJmIjoxMjYyMzczODA0LCJqdGki   
OiJodHRwOi8vZXhhbXBsZS5lZHUvY3JlZGVudGlhbHMvMzczMiIsInN1YiI6ImRpZDpleGFtcGx   
lOmViZmViMWY3MTJlYmM2ZjFjMjc2ZTEyZWMyMSJ9.YQKQUu\_zreDs69AZ8YqpMGHLl9V\_tWH4N   
S9P9l67J1wWHf0QCyt5hyuA8ckM4seV-1TRbeiHwdJ3VRkDMcwFcg

Ang pagtukoy sa modelo ng data, mga format, at mga protocol para sa mga scheme ng status ay wala sa saklaw para sa detalyeng ito. May Nabe-verify na Registry ng Extension ng Kredensyal [ [VC-EXTENSION-REGISTRY](https://www.w3.org/TR/vc-data-model/#bib-vc-extension-registry) ] na naglalaman ng mga available na status scheme para sa mga implementer na gustong magpatupad ng [nabe](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) -verify na pagsuri sa katayuan ng kredensyal.

### **4.10Mga pagtatanghal**

MAAARING gamitin ang mga [pagtatanghal](https://www.w3.org/TR/vc-data-model/" \l "dfn-presentations) upang pagsamahin at ipakita ang [mga kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) . Maaari silang i-package sa paraang [mapapatunayan](https://www.w3.org/TR/vc-data-model/" \l "dfn-verify) ang pagiging may-akda ng data . Ang data sa isang [presentasyon](https://www.w3.org/TR/vc-data-model/" \l "dfn-presentations) ay kadalasang tungkol sa parehong [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) , ngunit walang limitasyon sa bilang ng mga [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) o [nagbigay](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) sa data. Ang pagsasama-sama ng impormasyon mula sa maraming [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ay isang karaniwang paggamit ng mga [nabe-verify na presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) .

Ang isang [nabe-verify na pagtatanghal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) ay karaniwang binubuo ng mga sumusunod na katangian:

**id**

Opsyonal ang id [property at](https://www.w3.org/TR/vc-data-model/#dfn-property)MAAARING gamitin para magbigay ng natatanging identifier para sa [presentation](https://www.w3.org/TR/vc-data-model/#dfn-presentations) . Para sa mga detalyeng nauugnay sa paggamit ng property na ito, tingnan ang Seksyon[4.2Mga Identifier](https://www.w3.org/TR/vc-data-model/#identifiers) .

**uri**

Ang ari- type [arian](https://www.w3.org/TR/vc-data-model/" \l "dfn-property) ay kinakailangan at nagpapahayag ng uri ng [pagtatanghal](https://www.w3.org/TR/vc-data-model/" \l "dfn-presentations) , tulad ng VerifiablePresentation. Para sa mga detalyeng nauugnay sa paggamit ng property na ito, tingnan ang Seksyon[4.3Mga uri](https://www.w3.org/TR/vc-data-model/#types) .

**mapapatunayang kredensyal**

Kung naroroon, ang halaga ng verifiableCredential [property ay](https://www.w3.org/TR/vc-data-model/#dfn-property)DAPAT mabuo mula sa isa o higit pang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) , o ng data na nakuha mula sa mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) sa isang cryptographically [verifiable](https://www.w3.org/TR/vc-data-model/#dfn-verify) na format.

**may hawak**

Kung mayroon, ang halaga ng holder [property](https://www.w3.org/TR/vc-data-model/#dfn-property) ay inaasahang maging isang [URI](https://www.w3.org/TR/vc-data-model/#dfn-uri) para sa entity na bumubuo ng [presentation](https://www.w3.org/TR/vc-data-model/#dfn-presentations) .

**patunay**

Kung naroroon, tinitiyak ng halaga ng proof [property na mabe-](https://www.w3.org/TR/vc-data-model/#dfn-property)[verify](https://www.w3.org/TR/vc-data-model/#dfn-verify) ang [presentasyon](https://www.w3.org/TR/vc-data-model/" \l "dfn-presentations) . Para sa mga detalyeng nauugnay sa paggamit ng property na ito, tingnan ang Seksyon[4.7Mga Katibayan (Mga Lagda)](https://www.w3.org/TR/vc-data-model/#proofs-signatures) .

Ang halimbawa sa ibaba ay nagpapakita ng isang [nabe-verify na presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) na nag-embed ng mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) .

[HALIMBAWA14](https://www.w3.org/TR/vc-data-model/#example-basic-structure-of-a-presentation): Pangunahing istruktura ng isang pagtatanghal

{

"@context": [

"https://www.w3.org/2018/credentials/v1",

"https://www.w3.org/2018/credentials/examples/v1"

],

"id": "urn:uuid:3978344f-8596-4c3a-a978-8fcaba3903c5",

"type": ["VerifiablePresentation", "CredentialManagerPresentation"],

**"verifiableCredential": [{ ... }],**

**"patunay": [{ ... }]**

}

Ang mga nilalaman ng verifiableCredential [property](https://www.w3.org/TR/vc-data-model/#dfn-property) na ipinapakita sa itaas ay mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) , gaya ng inilalarawan ng detalyeng ito. Ang mga nilalaman ng proof [property](https://www.w3.org/TR/vc-data-model/#dfn-property) ay mga patunay, gaya ng inilarawan ng Data Integrity [ [DATA-INTEGRITY](https://www.w3.org/TR/vc-data-model/#bib-data-integrity) ] na detalye. Ang isang halimbawa ng isang [nabe-verify na presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) gamit ang JWT proof na mekanismo ay ibinigay sa seksyon [6.3.1JSON Web Token](https://www.w3.org/TR/vc-data-model/#json-web-token) .

**4.10.1Mga Pagtatanghal Gamit ang Mga Hinangong Kredensyal**

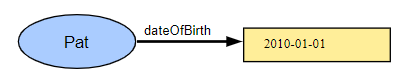
Maaaring bigyang-daan ng ilang zero-knowledge cryptography scheme ang mga may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) na hindi direktang patunayan na hawak nila ang mga [claim](https://www.w3.org/TR/vc-data-model/#dfn-claims) mula sa isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) nang hindi inilalantad ang mismong [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) . Sa mga scheme na ito, ang isang [claim](https://www.w3.org/TR/vc-data-model/#dfn-claims) mula sa isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ay maaaring gamitin upang makakuha ng isang ipinakitang halaga, na kung saan ay cryptographically iginiit upang mapagkakatiwalaan ng isang [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) ang halaga kung pinagkakatiwalaan nila ang [nagbigay](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) .

Halimbawa, maaaring gamitin ang isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) na naglalaman ng [claim](https://www.w3.org/TR/vc-data-model/#dfn-claims) date of birth upang makuha ang ipinakitang halaga over the age of 15sa paraang [nabe](https://www.w3.org/TR/vc-data-model/#dfn-verify) -verify sa cryptographically . Ibig sabihin, mapagkakatiwalaan pa rin ng isang [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) ang nakuhang halaga kung pinagkakatiwalaan nila ang [nagbigay](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) .

TANDAAN

Para sa isang halimbawa ng isang ZKP-style na [nabe-verify na presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) na naglalaman ng nakuhang data sa halip na mga direktang naka-embed na na-verify na mga [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-credentials) , tingnan ang Seksyon[5.8Zero-Knowledge Proofs](https://www.w3.org/TR/vc-data-model/#zero-knowledge-proofs) .

Ang mga selective disclosure scheme na gumagamit ng zero-knowledge proofs ay maaaring gumamit ng mga [claim](https://www.w3.org/TR/vc-data-model/#dfn-claims) na ipinahayag sa modelong ito upang patunayan ang mga karagdagang pahayag tungkol sa mga [claim](https://www.w3.org/TR/vc-data-model/#dfn-claims) na iyon . Halimbawa, ang isang [claim](https://www.w3.org/TR/vc-data-model/#dfn-claims) na tumutukoy [sa petsa ng kapanganakan ng isang paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) ay maaaring gamitin bilang isang predicate upang patunayan na ang edad ng [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) ay nasa loob ng isang partikular na hanay, at samakatuwid ay patunayan na ang [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) ay kwalipikado para sa mga diskwento na may kaugnayan sa edad, nang hindi aktwal na isiniwalat ang petsa ng kapanganakan ng [paksa .](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects)Ang may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) ay may kakayahang umangkop na gamitin ang [claim](https://www.w3.org/TR/vc-data-model/#dfn-claims) sa anumang paraan na naaangkop sa nais na [mabe-verify na presentasyon](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-presentations) .



(img src: <https://www.w3.org/TR/vc-data-model/diagrams/claim-example-2.svg>)

*Pigura*9*Isang pangunahing pahayag na nagsasaad na ang petsa ng kapanganakan ni Pat ay Enero 1, 2010. Ang pag-encode ng petsa ay matutukoy ng schema.*

## .Mga Advanced na Konsepto

Pagbuo sa mga konseptong ipinakilala sa Seksyon[4.Mga Pangunahing Konsepto](https://www.w3.org/TR/vc-data-model/#basic-concepts) , ang seksyong ito ay nagsasaliksik ng mas kumplikadong mga paksa tungkol sa mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) .

### **5.1Mga Detalye ng Lifecycle**

Ang seksyong ito ay hindi normatibo.

Seksyon[1.2Ang Pangkalahatang-ideya ng Ecosystem ay](https://www.w3.org/TR/vc-data-model/#ecosystem-overview) nagbigay ng pangkalahatang-ideya ng [nabe-verify na credential](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ecosystem. Ang seksyong ito ay nagbibigay ng higit pang detalye tungkol sa kung paano ang ecosystem ay inaasahang gumana.

Diagram

Description automatically generated

(img src: <https://www.w3.org/TR/vc-data-model/diagrams/ecosystemdetail.svg>)

*Pigura*10*Ang mga tungkulin at impormasyon ay dumadaloy para sa detalyeng ito.*

Ang mga tungkulin at daloy ng impormasyon sa [napapatunayang credential](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-credentials) ecosystem ay ang mga sumusunod:

* Ang isang [issuer](https://www.w3.org/TR/vc-data-model/#dfn-issuers) ay nagbibigay ng isang **nabe -verify na**[kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-credentials) sa isang may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) . Palaging nangyayari ang pagpapalabas bago ang anumang iba pang mga aksyon na kinasasangkutan ng isang [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) .
* Maaaring **ilipat** ng isang may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) ang isa o higit pa sa mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) nito sa isa pang may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) .
* Ang isang may [hawak ay](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders)**nagpapakita** ng isa o higit pa sa mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) nito sa isang [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) , opsyonal sa loob ng isang [nabe-verify na presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) .
* Bine - [verify ng](https://www.w3.org/TR/vc-data-model/#dfn-verify)[verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) ang pagiging tunay ng ipinakitang [nabe-verify na presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) at na-verify na mga [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-credentials) . Dapat kasama dito ang pagsuri sa [katayuan ng kredensyal](https://www.w3.org/TR/vc-data-model/" \l "status) para sa pagbawi ng mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) .
* Maaaring **bawiin ng isang**[issuer](https://www.w3.org/TR/vc-data-model/#dfn-issuers) ang isang nabe - [verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) .
* Maaaring **tanggalin** ng may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) ang isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) .

TANDAAN

Ang pagkakasunud-sunod ng mga aksyon sa itaas ay hindi naayos, at ang ilang mga aksyon ay maaaring gawin nang higit sa isang beses. Ang ganitong pagkilos-pag-ulit ay maaaring agaran o sa anumang susunod na punto.

Ang pinakakaraniwang pagkakasunud-sunod ng mga aksyon ay naisip na:

1. Ang isang [issuer ay nag-](https://www.w3.org/TR/vc-data-model/#dfn-issuers)[isyu](https://www.w3.org/TR/vc-data-model/#lifecycle-details) sa isang may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) .
2. Ang may [hawak ay](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders)[nagpapakita](https://www.w3.org/TR/vc-data-model/#lifecycle-details) sa isang [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) .
3. Bine - [verify](https://www.w3.org/TR/vc-data-model/#lifecycle-details)[ng verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) ang .

Ang pagtutukoy na ito ay hindi tumutukoy sa anumang protocol para sa paglilipat ng mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) o na-verify na mga [presentasyon](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-presentations) , ngunit kung ipagpalagay na ang ibang mga detalye ay tumutukoy kung paano sila inililipat sa pagitan ng mga entity, kung gayon ang Verifiable Credential Data Model na ito ay direktang naaangkop.

Hindi rin tinukoy ng detalyeng ito ang isang balangkas ng awtorisasyon o ang mga desisyon na maaaring gawin ng isang taga- [verify](https://www.w3.org/TR/vc-data-model/#dfn-verifier) pagkatapos ma- [verify](https://www.w3.org/TR/vc-data-model/#dfn-verify) ang isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) o na-verify na [pagtatanghal](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-presentations) , na isinasaalang-alang ang may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) , ang mga [nagbigay](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) ng mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) , ang mga nilalaman ng na- verify na mga [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-credentials) , at ang sarili nitong mga patakaran .

Sa partikular, Mga Seksyon[5.6Mga Tuntunin ng Paggamit](https://www.w3.org/TR/vc-data-model/#terms-of-use) at [C.Tinutukoy ng Mga Relasyon ng May-hawak ng Paksa](https://www.w3.org/TR/vc-data-model/" \l "subject-holder-relationships) kung paano matutukoy ng isang [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) ang:

* Kung ang may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) ay isang [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) ng isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) .
* Ang relasyon sa pagitan ng [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) at ng may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) .
* Kung ang orihinal na may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) ay nagpasa ng isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) sa isang kasunod na may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) .
* Anumang mga paghihigpit gamit ang mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ng may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) o [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) .

### **5.2Trust Model**

Ang seksyong ito ay hindi normatibo.

Ang [nabe](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) -verify na modelo ng tiwala ng mga kredensyal ay ang sumusunod:

* Pinagkakatiwalaan ng [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) ang [nagbigay](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) ng [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) na natanggap nito. Upang maitatag ang tiwala na ito, ang isang [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) ay inaasahang:
  + Magsama ng [patunay](https://www.w3.org/TR/vc-data-model/" \l "proofs-signatures) na nagpapatunay na ang [nagbigay](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) ng kredensyal ay nakabuo ng [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) (iyon ay, ito ay isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ), o
  + Nailipat sa paraang malinaw na nagpapatunay na ang nag- [isyu](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) ay nakabuo ng [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) at na ang na- verify na [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-credentials) ay hindi pinakialaman sa transit o storage. Maaaring humina ang tiwala na ito depende sa pagtatasa ng panganib ng [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) .
* Pinagkakatiwalaan ng lahat ng [entity ang](https://www.w3.org/TR/vc-data-model/#dfn-entities)[nabe-verify na registry ng data](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-data-registries) upang maging maliwanag at maging isang tamang talaan kung aling data ang kinokontrol ng kung aling mga [entity](https://www.w3.org/TR/vc-data-model/#dfn-entities) .
* Pinagkakatiwalaan ng may-ari at taga-verify ang nagbigay [ng](https://www.w3.org/TR/vc-data-model/#dfn-holders) totoo [(](https://www.w3.org/TR/vc-data-model/#dfn-verifier)[iyon](https://www.w3.org/TR/vc-data-model/#dfn-issuers) ay, hindi mali) na mga [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) tungkol sa [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) , at mabilis na bawiin ang mga ito kapag naaangkop.
* Ang may- [ari](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) ay nagtitiwala sa [repositoryo](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential-repository) na mag-imbak ng mga [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) nang ligtas, upang hindi ibigay ang mga ito sa sinuman maliban sa may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) , at hindi masira o mawala ang mga ito habang sila ay nasa pangangalaga nito.

Naiiba ng trust model na ito ang sarili nito sa ibang mga trust model sa pamamagitan ng pagtiyak na:

* [Ang nag- isyu](https://www.w3.org/TR/vc-data-model/#dfn-issuers) at ang [verifier ay](https://www.w3.org/TR/vc-data-model/#dfn-verifier) hindi kailangang magtiwala sa [repositoryo](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential-repository)
* [Hindi kailangang malaman o pagkatiwalaan ng nag- isyu](https://www.w3.org/TR/vc-data-model/#dfn-issuers) ang [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) .

Sa pamamagitan ng pag-decoupling ng tiwala sa pagitan ng [tagapagbigay ng pagkakakilanlan](https://www.w3.org/TR/vc-data-model/" \l "dfn-identity-providers) at ng [umaasa na partido](https://www.w3.org/TR/vc-data-model/" \l "dfn-relying-parties) , ang isang mas nababaluktot at dynamic na modelo ng tiwala ay nilikha upang ang kumpetisyon sa merkado at pagpili ng customer ay tumaas.

Para sa higit pang impormasyon tungkol sa kung paano nakikipag-ugnayan ang trust model na ito sa iba't ibang modelo ng pagbabanta na pinag-aralan ng Working Group, tingnan ang dokumento ng Mga Verifiable Credentials Use Cases [ [VC-USE-CASES](https://www.w3.org/TR/vc-data-model/#bib-vc-use-cases) ].

TANDAAN

Ang modelo ng data na nakadetalye sa detalyeng ito ay hindi nagpapahiwatig ng isang transitive na modelo ng tiwala, tulad ng ibinigay ng mas tradisyonal na mga modelo ng tiwala ng Certificate Authority. Sa Verifiable Credentials Data Model, ang isang [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) ay direktang nagtitiwala o hindi nagtitiwala sa isang [issuer](https://www.w3.org/TR/vc-data-model/#dfn-issuers) . Bagama't posibleng bumuo ng mga transitive trust model gamit ang Verifiable Credentials Data Model, hinihikayat ang mga tagapagpatupad na [alamin ang tungkol sa mga kahinaan sa seguridad na](https://datatracker.ietf.org/doc/draft-iab-web-pki-problems/) ipinakilala sa pamamagitan ng [malawakang pagtatalaga ng tiwala](https://www.usenix.org/conference/imc-05/perils-transitive-trust-domain-name-system) sa paraang pinagtibay ng mga system ng Certificate Authority.

### **5.3Extensibility**

Isa sa mga layunin ng Verifiable Credentials Data Model ay ang paganahin ang walang pahintulot na pagbabago. Upang makamit ito, kailangang mapalawak ang modelo ng data sa iba't ibang paraan. Ang modelo ng data ay kinakailangan upang:

* Magmodelo ng mga kumplikadong ugnayang multi-entity sa pamamagitan ng paggamit ng modelo ng data na nakabatay sa [graph .](https://www.w3.org/TR/vc-data-model/#dfn-graphs)
* Palawakin ang mga bokabularyo na nababasa ng makina na ginagamit upang ilarawan ang impormasyon sa modelo ng data, nang hindi gumagamit ng sentralisadong sistema para sa paggawa nito, sa pamamagitan ng paggamit ng [ [LINKED-DATA](https://www.w3.org/TR/vc-data-model/#bib-linked-data) ].
* Suportahan ang maraming uri ng cryptographic proof na format sa pamamagitan ng paggamit ng Data Integrity Proofs [ [DATA-INTEGRITY](https://www.w3.org/TR/vc-data-model/#bib-data-integrity) ] at iba't ibang signature suite na nakalista sa Linked Data Cryptographic Suites Registry [ [LDP-REGISTRY](https://www.w3.org/TR/vc-data-model/#bib-ldp-registry) ]
* Ibigay ang lahat ng mekanismo ng pagpapalawak na nakabalangkas sa itaas sa isang format ng data na sikat sa mga developer ng software at mga may-akda ng web page, at pinagana sa pamamagitan ng paggamit ng [ [JSON-LD](https://www.w3.org/TR/vc-data-model/#bib-json-ld) ].

Ang diskarteng ito sa pagmomodelo ng data ay madalas na tinatawag na open world assumption , ibig sabihin, ang anumang entity ay maaaring magsabi ng anuman tungkol sa anumang ibang entity. Bagama't ang diskarteng ito ay tila sumasalungat sa pagbuo ng simple at predictable na mga software system, ang pagbabalanse ng extensibility sa katumpakan ng program ay palaging mas mahirap sa isang open world assumption kaysa sa mga closed software system.

Ang natitirang bahagi ng seksyong ito ay naglalarawan, sa pamamagitan ng isang serye ng mga halimbawa, kung paano nakakamit ang parehong pagpapalawak at kawastuhan ng programa.

Ipagpalagay natin na magsisimula tayo sa [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) na ipinapakita sa ibaba.

[HALIMBAWA15](https://www.w3.org/TR/vc-data-model/#example-a-simple-credential): Isang simpleng kredensyal

Credential

{

"@context": [

"https://www.w3.org/2018/credentials/v1",

"https://www.w3.org/2018/credentials/examples/v1"

],

"id": "http://example.com/credentials/4643",

"type": ["VerifiableCredential"],

"issuer": "https://example.com/issuers/14",

"issuanceDate": "2018-02-24T05:28:04Z",

"credentialSubject": {

"id": "did:example:abcdef1234567",

"pangalan": "Jane Doe"

}

}

Verifiable Credential (may patunay)

{   
 "@context": [   
 "https://www.w3.org/2018/credentials/v1",   
 "https://www.w3.org/2018/credentials/examples/v1",   
 "https:// w3id.org/security/suites/ed25519-2020/v1"   
 ],   
 "id": "http://example.com/credentials/4643",   
 "type": [   
 "VerifiableCredential"   
 ],   
 "issuer": "https ://example.com/issuers/14",   
 "issuanceDate": "2018-02-24T05:28:04Z",   
 "credentialSubject": {   
 "id": "did:example:abcdef1234567",   
 "name": " Jane Doe"   
 },   
 "patunay": {   
 "type": "Ed25519Signature2020",   
 "created": "2022-02-25T14:58:43Z",   
 "verificationMethod": "https://example.edu/issuers/14#keys-1",  
 "proofPurpose": "assertionMethod",   
 "proofValue": "zyrpmzxPy2fDzqv9Pgr4XBzX2rys1FDuLNkYRVmhXuyype8fB44qNX8m   
NnXf99i7x1eSpLdYKNhEKkn   
 }   
} 4Jwmd"

Verifiable Credential (bilang JWT)

---------------- JWT header ---------------   
{   
 "alg": "ES256",   
 "typ": "JWT"   
​​}   
--------------- JWT payload ---------------   
// TANDAAN: Ang halimbawa sa ibaba ay gumagamit ng wastong VC-JWT serialization   
// na duplicate ang iss, nbf, jti, at mga sub na field sa   
// Na-verify na Kredensyal (vc) na field.   
{   
 "vc": {   
 "@context": [   
 "https://www.w3.org/2018/credentials/v1",   
 "https://www.w3.org/2018/credentials/examples/v1"   
 ] ,   
 "id": "http://example.com/credentials/4643",   
 "type": [   
 "VerifiableCredential"   
 ],  
  
 "issuanceDate": "2018-02-24T05:28:04Z",   
 "credentialSubject": {   
 "id": "did:example:abcdef1234567",   
 "name": "Jane Doe"   
 }   
 },   
 "iss": "https ://example.com/issuers/14",   
 "nbf": 1519450084,   
 "jti": "http://example.com/credentials/4643",   
 "sub": "did:example:abcdef1234567"   
}   
-- ------------- JWT ---------------   
eyJhbGciOiJFUzI1NiIsInR5cCI6IkpXVCJ9.eyJ2YyI6eyJAY29udGV4dCI6WyJodHRwczovL3   
d3dy53My5vcmcvMjAxOC9jcmVkZW50aWFscy92MSIsImh0dHBzOi8vd3d3LnczLm9yZy8yMDE4L   
2NyZWRlbnRpYWxzL2V4YW1wbGVzL3YxIl0sImlkIjoiaHR0cDovL2V4YW1wbGUuY29tL2NyZWRl   
bnRpYWxzLzQ2NDMiLCJ0eXBlIjpbIlZlcmlmaWFibGVDcmVkZW50aWFsIl0sImlzc3VlciI6Imh  
0dHBzOi8vZXhhbXBsZS5jb20vaXNzdWVycy8xNCIsImlzc3VhbmNlRGF0ZSI6IjIwMTgtMDItMj   
RUMDU6Mjg6MDRaIiwiY3JlZGVudGlhbFN1YmplY3QiOnsiaWQiOiJkaWQ6ZXhhbXBsZTphYmNkZ   
WYxMjM0NTY3IiwibmFtZSI6IkphbmUgRG9lIn19LCJpc3MiOiJodHRwczovL2V4YW1wbGUuY29t   
L2lzc3VlcnMvMTQiLCJuYmYiOjE1MTk0NTAwODQsImp0aSI6Imh0dHA6Ly9leGFtcGxlLmNvbS9   
jcmVkZW50aWFscy80NjQzIiwic3ViIjoiZGlkOmV4YW1wbGU6YWJjZGVmMTIzNDU2NyJ9.oIDq\_   
JtiKwm1AVikEjMuurZcfZdTtNAvus63k2kbD1HF2l\_5V36ekulxPPY7rKYEeiH3e6bTq1urNoML   
K3UipA

Itong [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ay nagsasaad na ang [entity](https://www.w3.org/TR/vc-data-model/#dfn-entities) na nauugnay sa did:example:abcdef1234567ay namemay halagang Jane Doe.

Ngayon, ipagpalagay natin na gustong palawigin ng developer ang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) para mag-imbak ng dalawang karagdagang impormasyon: isang internal na corporate reference number, at ang paboritong pagkain ni Jane.

Ang unang bagay na dapat gawin ay lumikha ng JSON-LD na konteksto na naglalaman ng dalawang bagong termino, tulad ng ipinapakita sa ibaba.

[HALIMBAWA16](https://www.w3.org/TR/vc-data-model/#example-a-json-ld-context): Isang kontekstong JSON-LD

{

"@context": {

"referenceNumber": "https://example.com/vocab#referenceNumber",

"favoriteFood": "https://example.com/vocab#favoriteFood"

}

}

Matapos magawa ang kontekstong JSON-LD na ito, ini-publish ito ng developer sa isang lugar upang ma-access ito ng mga [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) na magpoproseso ng [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) . Ipagpalagay na ang konteksto ng JSON-LD sa itaas ay nai-publish sa https://example.com/contexts/mycontext.jsonld, maaari naming palawigin ang halimbawang ito sa pamamagitan ng pagsasama ng konteksto at pagdaragdag ng mga bagong [katangian](https://www.w3.org/TR/vc-data-model/" \l "dfn-property) at [uri ng](https://www.w3.org/TR/vc-data-model/" \l "dfn-type)[kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-credential) sa [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) .

[HALIMBAWA17](https://www.w3.org/TR/vc-data-model/#example-a-verifiable-credential-with-a-custom-extension): Isang nabe-verify na kredensyal na may custom na extension

{

"@context": [

"https://www.w3.org/2018/credentials/v1",

**"https://example.com/contexts/mycontext.jsonld"**

],

"id": "http://example.com/credentials/4643",

"type": ["VerifiableCredential", "CustomExt12"],

"issuer": "https://example.com/issuers/14",

"issuanceDate": "2018-02-24T05:28:04Z",

**"referenceNumber": 83294847,**

"credentialSubject": {

"id": "did:example:abcdef1234567",

"name": "Jane Doe",

**"favoriteFood": "Papaya"**

}

}

Ang halimbawang ito ay nagpapakita ng pagpapalawak ng Verifiable Credentials Data Model sa isang walang pahintulot at desentralisadong paraan. Tinitiyak din ng mekanismong ipinapakita na ang [mga nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-credentials) na ginawa sa paraang ito ay nagbibigay ng mekanismo upang maiwasan ang mga salungatan sa namespace at kalabuan ng semantiko.

Ang isang dynamic na modelo ng extensibility tulad nito ay nagpapataas ng pasanin sa pagpapatupad. Ang software na isinulat para sa naturang sistema ay kailangang matukoy kung ang mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) na may mga extension ay katanggap-tanggap batay sa profile ng panganib ng application. Ang ilang mga application ay maaaring tumanggap lamang ng ilang mga extension habang ang mga lubos na secure na kapaligiran ay maaaring hindi tumanggap ng anumang mga extension. Ang mga pagpapasyang ito ay nakasalalay sa mga developer ng mga application na ito at partikular na hindi ang domain ng detalyeng ito.

Hinihimok ang mga developer na tiyaking available ang mga konteksto ng extension na JSON-LD. Magdudulot ng error ang mga pagpapatupad na hindi makakuha ng konteksto. Kasama sa mga diskarte sa pagtiyak na palaging available ang mga konteksto ng extension na JSON-LD ang paggamit ng mga URL na naka-address sa content para sa mga konteksto, pag-bundle ng mga dokumento ng konteksto sa mga pagpapatupad, o pagpapagana ng agresibong pag-cache ng mga konteksto.

Pinapayuhan ang mga tagapagpatupad na bigyang-pansin ang mga extension point sa detalyeng ito, tulad ng sa Mga Seksyon[4.7Mga Katibayan (Mga Lagda)](https://www.w3.org/TR/vc-data-model/#proofs-signatures) , [4.9katayuan](https://www.w3.org/TR/vc-data-model/#status) ,[5.4Mga Schema ng Data](https://www.w3.org/TR/vc-data-model/#data-schemas) ,[5.5Nagre- refresh](https://www.w3.org/TR/vc-data-model/#refreshing) , [5.6Mga Tuntunin ng Paggamit](https://www.w3.org/TR/vc-data-model/#terms-of-use) , at[5.7Katibayan](https://www.w3.org/TR/vc-data-model/#evidence) . Bagama't hindi tinukoy ng detalyeng ito ang mga konkretong pagpapatupad para sa mga extension point na iyon, ang Verifiable Credentials Extension Registry [ [VC-EXTENSION-REGISTRY](https://www.w3.org/TR/vc-data-model/#bib-vc-extension-registry) ] ay nagbibigay ng hindi opisyal, na-curate na listahan ng mga extension na magagamit ng mga developer mula sa mga extension point na ito.

#### 5.3.1Semantic Interoperability

Tinitiyak ng detalyeng ito na ang mga "plain" na JSON at JSON-LD syntax ay semantically compatible nang hindi nangangailangan ng mga pagpapatupad ng JSON na gumamit ng JSON-LD processor. Upang makamit ito, ipinapataw ng detalye ang mga sumusunod na karagdagang kinakailangan sa parehong mga syntax:

* DAPAT iproseso ng mga processor na nakabatay sa JSON ang @contextsusi, na tinitiyak na umiiral ang mga inaasahang halaga sa inaasahang pagkakasunud-sunod para sa uri ng [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) na pinoproseso. Ang pagkakasunud-sunod ay mahalaga dahil ang mga susi na ginamit sa isang [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) , na tinukoy gamit ang mga halagang nauugnay sa @context, ay tinukoy gamit ang mekanismong "mga unang tinukoy na panalo" at ang pagbabago ng pagkakasunud-sunod ay maaaring magresulta sa ibang pangunahing kahulugang "panalo".
* DAPAT gumawa ng error ang mga processor na nakabatay sa JSON-LD kapag muling tinukoy ng konteksto ng JSON-LD ang anumang termino sa [aktibong konteksto](https://www.w3.org/TR/json-ld/" \l "dfn-active-context) . Ang tanging paraan upang baguhin ang kahulugan ng mga umiiral na termino ay ang pagpapakilala ng bagong termino na naglilinaw sa aktibong konteksto sa loob ng saklaw ng bagong terminong iyon. Dapat basahin ng mga may-akda na interesado sa feature na ito ang tungkol sa @protectedfeature sa detalye ng JSON-LD 1.1.

Ang isang dokumentong nababasa ng tao na naglalarawan sa inaasahang pagkakasunud-sunod ng mga halaga para sa ari- @context [arian](https://www.w3.org/TR/vc-data-model/" \l "dfn-property) ay inaasahang mai-publish ng sinumang tagapagpatupad na naghahanap ng interoperability. Ang isang paglalarawang nababasa ng makina (iyon ay, isang normal na dokumento ng Konteksto ng JSON-LD) ay inaasahang ma-publish sa URL na tinukoy sa @context [property](https://www.w3.org/TR/vc-data-model/#dfn-property) ng mga tagapagpatupad ng JSON-LD na naghahanap ng interoperability.

Ginagarantiyahan ng mga kinakailangan sa itaas ang semantic interoperability sa pagitan ng JSON at JSON-LD para sa mga terminong tinukoy ng @contextmekanismo. Bagama't gagamitin ng mga JSON-LD processor ang partikular na mekanismong ibinigay at mabe-verify na tama ang lahat ng termino, tahasang tinatanggap ng mga JSON-based na processor ang parehong hanay ng mga termino nang hindi sinusuri kung tama ang mga ito. Sa madaling salita, ang konteksto kung saan nangyayari ang pagpapalitan ng data ay tahasang nakasaad para sa parehong JSON at JSON-LD sa pamamagitan ng paggamit ng parehong mekanismo. Kaugnay ng mga processor na nakabatay sa JSON, nakakamit ito sa magaan na paraan, nang hindi kinakailangang gumamit ng mga library sa pagpoproseso ng JSON-LD.

### **5.4Mga Schema ng Data**

Ang mga schema ng data ay kapaki-pakinabang kapag nagpapatupad ng isang partikular na istraktura sa isang ibinigay na koleksyon ng data. Mayroong hindi bababa sa dalawang uri ng mga schema ng data na isinasaalang-alang ng detalyeng ito:

* Mga schema ng pag-verify ng data, na ginagamit upang i- [verify](https://www.w3.org/TR/vc-data-model/#dfn-verify) na ang istraktura at mga nilalaman ng isang [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) o [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ay sumusunod sa isang naka-publish na schema.
* Mga schema ng pag-encode ng data, na ginagamit upang imapa ang mga nilalaman ng isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) sa isang alternatibong format ng representasyon, tulad ng isang binary na format na ginamit sa isang zero-knowledge proof.

Mahalagang maunawaan na ang mga schema ng data ay nagsisilbing ibang layunin mula sa @contextproperty, na hindi nagpapatupad ng istraktura ng data o data syntax, o nagbibigay-daan sa kahulugan ng mga arbitrary na pag-encode sa mga alternatibong format ng representasyon.

Tinutukoy ng detalyeng ito ang sumusunod na [property](https://www.w3.org/TR/vc-data-model/#dfn-property) para sa pagpapahayag ng schema ng data, na maaaring isama ng isang [issuer](https://www.w3.org/TR/vc-data-model/#dfn-issuers) sa mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) na ibinibigay nito:

**credentialSchema**

Ang value ng credentialSchema [property ay](https://www.w3.org/TR/vc-data-model/#dfn-property)DAPAT isa o higit pang data schema na nagbibigay sa mga [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) ng sapat na impormasyon para matukoy kung ang ibinigay na data ay sumusunod sa ibinigay na schema. credentialSchema DAPAT tukuyin ng bawat isa ang nito type(halimbawa, JsonSchemaValidator2018), at isang id [property](https://www.w3.org/TR/vc-data-model/#dfn-property) na DAPAT ay isang [URI](https://www.w3.org/TR/vc-data-model/#dfn-uri) na nagpapakilala sa schema file. Ang mga tiyak na nilalaman ng bawat schema ng data ay tinutukoy ng partikular na kahulugan ng uri.

TANDAAN

Nagbibigay ang credentialSchema [property](https://www.w3.org/TR/vc-data-model/#dfn-property) ng pagkakataong i-annotate ang mga kahulugan ng uri o i-lock ang mga ito sa mga partikular na bersyon ng bokabularyo. Ang mga may-akda ng mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ay maaaring magsama ng isang static na bersyon ng kanilang bokabularyo na ginagamit credentialSchemana naka-lock sa ilang mekanismo ng proteksyon ng integridad ng nilalaman. Ginagawa ring posible ng credentialSchema [property na magsagawa ng syntactic checking sa](https://www.w3.org/TR/vc-data-model/#dfn-property)[kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-credential) at gumamit ng mga mekanismo ng pag- [verify](https://www.w3.org/TR/vc-data-model/#dfn-verify) gaya ng JSON Schema [ [JSON-SCHEMA-2018](https://www.w3.org/TR/vc-data-model/#bib-json-schema-2018) ] validation.

[HALIMBAWA18](https://www.w3.org/TR/vc-data-model/#example-usage-of-the-credentialschema-property-to-perform-json-schema-validation): Paggamit ng credentialSchema property para magsagawa ng JSON schema validation

Credential

{

"@context": [

"https://www.w3.org/2018/credentials/v1",

"https://www.w3.org/2018/credentials/examples/v1"

],

"id": "http://example.edu/credentials/3732",

"type": ["VerifiableCredential", "UniversityDegreeCredential"],

"issuer": "https://example.edu/issuers/14",

"issuanceDate": "2010-01-01T19:23:24Z",

"credentialSubject": {

"id": "did:example:ebfeb1f712ebc6f1c276e12ec21",

"degree": {

"type": "BachelorDegree",

"pangalan": "Bachelor ng Agham at Sining"

}

},

**"credentialSchema": {**

**"id": "https://example.org/examples/degree.json",**

**"type": "JsonSchemaValidator2018"**

**}**

}

Verifiable Credential (may patunay)

{   
 "@context": [   
 "https://www.w3.org/2018/credentials/v1",   
 "https://www.w3.org/2018/credentials/examples/v1",   
 "https:// w3id.org/security/suites/ed25519-2020/v1"   
 ],   
 "id": "http://example.edu/credentials/3732",   
 "type": [   
 "VerifiableCredential",   
 "UniversityDegreeCredential"   
 ],   
 "issuer ": "https://example.edu/issuers/14",   
 "issuanceDate": "2010-01-01T19:23:24Z",   
 "credentialSubject": {   
 "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",   
 " degree": {   
 "type": "BachelorDegree",   
 "name": "Bachelor of Science and Arts"   
 }   
 },   
 "credentialSchema": {  
 "id": "https://example.org/examples/degree.json",   
 "type": "JsonSchemaValidator2018"   
 },   
 "proof": {   
 "type": "Ed25519Signature2020",   
 "created": "2022-02 -25T14:58:43Z", "   
 verificationMethod": "https://example.edu/issuers/14#keys-1", " proofPurpose   
 ": "assertionMethod",   
 "proofValue": "   
z5JKxik9jw25W2s9Q3N3RMovCVLSt8Ksy2b1BTZRt8Ksy6bBTZFCt8Ksy3bJWFCt1h6bBTZFCt8Ksy6b1WQTyb

Verifiable Credential (bilang JWT)

---------------- JWT header ---------------   
{   
 "alg": "ES256",   
 "typ": "JWT"   
​​}   
--------------- JWT payload ---------------   
// TANDAAN: Ang halimbawa sa ibaba ay gumagamit ng wastong VC-JWT serialization   
// na duplicate ang iss, nbf, jti, at mga sub na field sa   
// Na-verify na Kredensyal (vc) na field.   
{   
 "vc": {   
 "@context": [   
 "https://www.w3.org/2018/credentials/v1",   
 "https://www.w3.org/2018/credentials/examples/v1"   
 ] ,   
 "id": "http://example.edu/credentials/3732",   
 "type": [   
 "VerifiableCredential",   
 "  
  
 "issuer": "https://example.edu/issuers/14",   
 "issuanceDate": "2010-01-01T19:23:24Z",   
 "credentialSubject": {   
 "id": "did:example:ebfeb1f712ebc6f1c276"e12ec276e12ec ,   
 "degree": {   
 "type": "BachelorDegree",   
 "name": "Bachelor of Science and Arts"   
 }   
 },   
 "credentialSchema": {   
 "id": "https://example.org/examples/degree. json",   
 "type": "JsonSchemaValidator2018"   
 }   
 },   
 "iss": "https://example.edu/issuers/14",   
 "nbf": 1262373804,  
 "jti": "http://example.edu/credentials/3732",   
 "sub": "did:example:ebfeb1f712ebc6f1c276e12ec21"   
}  
--------------- JWT ---------------   
eyJhbGciOiJFUzI1NiIsInR5cCI6IkpXVCJ9.eyJ2YyI6eyJAY29udGV4dCI6WyJodHRwczovL3   
d3dy53My5vcmcvMjAxOC9jcmVkZW50aWFscy92MSIsImh0dHBzOi8vd3d3LnczLm9yZy8yMDE4L   
2NyZWRlbnRpYWxzL2V4YW1wbGVzL3YxIl0sImlkIjoiaHR0cDovL2V4YW1wbGUuZWR1L2NyZWRl   
bnRpYWxzLzM3MzIiLCJ0eXBlIjpbIlZlcmlmaWFibGVDcmVkZW50aWFsIiwiVW5pdmVyc2l0eUR   
lZ3JlZUNyZWRlbnRpYWwiXSwiaXNzdWVyIjoiaHR0cHM6Ly9leGFtcGxlLmVkdS9pc3N1ZXJzLz   
E0IiwiaXNzdWFuY2VEYXRlIjoiMjAxMC0wMS0wMVQxOToyMzoyNFoiLCJjcmVkZW50aWFsU3Via   
mVjdCI6eyJpZCI6ImRpZDpleGFtcGxlOmViZmViMWY3MTJlYmM2ZjFjMjc2ZTEyZWMyMSIsImRl   
Z3JlZSI6eyJ0eXBlIjoiQmFjaGVsb3JEZWdyZWUiLCJuYW1lIjoiQmFjaGVsb3Igb2YgU2NpZW5   
jZSBhbmQgQXJ0cyJ9fSwiY3JlZGVudGlhbFNjaGVtYSI6eyJpZCI6Imh0dHBzOi8vZXhhbXBsZS  
5vcmcvZXhhbXBsZXMvZGVncmVlLmpzb24iLCJ0eXBlIjoiSnNvblNjaGVtYVZhbGlkYXRvcjIwM   
TgifX0sImlzcyI6Imh0dHBzOi8vZXhhbXBsZS5lZHUvaXNzdWVycy8xNCIsIm5iZiI6MTI2MjM3   
MzgwNCwianRpIjoiaHR0cDovL2V4YW1wbGUuZWR1L2NyZWRlbnRpYWxzLzM3MzIiLCJzdWIiOiJ   
kaWQ6ZXhhbXBsZTplYmZlYjFmNzEyZWJjNmYxYzI3NmUxMmVjMjEifQ.GRJHwxvQfgEOP8TaaBn   
p2ZCPjFlA\_KodpdBupHsRroql10gaE--8oAXR1e-wOuxjFoK-T814h9LKnv71IMI38Q

Sa halimbawa sa itaas, tinutukoy ng [issuer](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers)credentialSchema ang isang , na tumuturo sa isang [ [JSON-SCHEMA-2018](https://www.w3.org/TR/vc-data-model/#bib-json-schema-2018) ] file na maaaring gamitin ng isang [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) upang matukoy kung maayos na nabuo ang [nabe-verify na kredensyal .](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials)

TANDAAN

Para sa impormasyon tungkol sa mga link sa JSON Schema [ [JSON-SCHEMA-2018](https://www.w3.org/TR/vc-data-model/#bib-json-schema-2018) ] o iba pang opsyonal na mekanismo ng pag- [verify](https://www.w3.org/TR/vc-data-model/#dfn-verify) , tingnan ang dokumentong Mga Alituntunin sa Pagpapatupad ng Mga Na-verify na Kredensyal [ [VC-IMP-GUIDE](https://www.w3.org/TR/vc-data-model/#bib-vc-imp-guide) ].

Ang mga schema ng data ay maaari ding gamitin upang tukuyin ang mga pagmamapa sa iba pang mga binary na format, gaya ng mga ginamit upang magsagawa ng mga patunay na walang kaalaman. Para sa higit pang impormasyon sa paggamit ng credentialSchema [property](https://www.w3.org/TR/vc-data-model/#dfn-property) na may zero-knowledge proofs, tingnan ang Seksyon[5.8Zero-Knowledge Proofs](https://www.w3.org/TR/vc-data-model/#zero-knowledge-proofs) .

[HALIMBAWA19](https://www.w3.org/TR/vc-data-model/#example-usage-of-the-credentialschema-property-to-perform-zero-knowledge-validation): Paggamit ng credentialSchema property para magsagawa ng zero-knowledge validation

{

"@context": [

"https://www.w3.org/2018/credentials/v1",

"https://www.w3.org/2018/credentials/examples/v1"

],

"id": "http://example.edu/credentials/3732",

"type": ["VerifiableCredential", "UniversityDegreeCredential"],

"issuer": "https://example.edu/issuers/14",

"issuanceDate": "2010-01-01T19:23:24Z",

"credentialSubject": {

"id": "did:example:ebfeb1f712ebc6f1c276e12ec21",

"degree": {

"type": "BachelorDegree",

"pangalan": "Bachelor ng Agham at Sining"

}

},

**"credentialSchema": {**

**"id": "https://example.org/examples/degree.zkp",**

**"type": "ZkpExampleSchema2018"**

**}** ,

"patunay": { **...** }

}

Sa halimbawa sa itaas, tinutukoy ng [issuer](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers)credentialSchema ang isang pagturo sa isang zero-knowledge packed binary data format na may kakayahang baguhin ang input data sa isang format, na pagkatapos ay magagamit ng isang [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) upang matukoy kung ang patunay na ibinigay kasama ng [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ay pwede.

### **5.5Nagre-refresh**

Kapaki-pakinabang para sa mga system na paganahin ang manu-mano o awtomatikong pag-refresh ng isang nag-expire na [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) . Para sa higit pang impormasyon tungkol sa mga nag-expire [na nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-credentials) , tingnan ang Seksyon[4.8Expiration](https://www.w3.org/TR/vc-data-model/#expiration) . Tinutukoy ng detalyeng ito ang isang refreshService [property](https://www.w3.org/TR/vc-data-model/#dfn-property) , na nagbibigay-daan sa isang [issuer](https://www.w3.org/TR/vc-data-model/#dfn-issuers) na magsama ng link sa isang serbisyo sa pag-refresh.

Maaaring isama ng [issuer](https://www.w3.org/TR/vc-data-model/#dfn-issuers) ang serbisyo sa pag-refresh bilang isang elemento sa loob ng [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) kung ito ay para sa [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) o sa may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) (o pareho), o sa loob ng [nabe-verify na presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) kung ito ay para lang sa may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) . Sa huling kaso, binibigyang-daan nito ang may- [ari](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) na i-refresh ang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) bago gumawa ng [nabe-verify na presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) na ibabahagi sa isang [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) . Sa dating kaso, kasama ang serbisyo sa pag-refresh sa loob ng [nabe-verify na kredensyal ay](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) nagbibigay-daan sa may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) o sa [verifier](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifier)upang magsagawa ng mga pag-update sa hinaharap ng [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) .

Ang serbisyo sa pag-refresh ay inaasahan lamang na gagamitin kapag ang [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) ay nag-expire na o ang [nagbigay ng](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers)[impormasyon](https://www.w3.org/TR/vc-data-model/#dfn-credential) sa katayuan ng kredensyal . [Pinapayuhan](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) ang mga nag-isyu na huwag ilagay ang ari- refreshService [arian](https://www.w3.org/TR/vc-data-model/" \l "dfn-property) sa isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) na hindi naglalaman ng pampublikong impormasyon o kung saan ang serbisyo ng pag-refresh ay hindi protektado sa anumang paraan.

TANDAAN

Ang paglalagay ng ari- refreshService [arian](https://www.w3.org/TR/vc-data-model/" \l "dfn-property) sa isang [nabe](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) -verify na kredensyal upang ito ay maging available sa mga [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) ay maaaring mag-alis ng kontrol at pahintulot mula sa may- [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) at payagan ang na-verify na [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-credentials) na direktang maibigay sa [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) , at sa gayon ay maiiwasan ang may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) .

**refreshService**

Ang halaga ng refreshService [property ay](https://www.w3.org/TR/vc-data-model/#dfn-property)DAPAT na isa o higit pang mga serbisyo sa pag-refresh na nagbibigay ng sapat na impormasyon sa software ng tatanggap upang ma-refresh ng tatanggap ang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) . DAPAT tukuyin ng bawat refreshServicevalue ang nito (halimbawa, ) at ang , na siyang [URI](https://www.w3.org/TR/vc-data-model/#dfn-uri) ng serbisyo. May inaasahan na ang impormasyong nababasa ng machine ay kailangang makuha mula sa URI. Ang tumpak na nilalaman ng bawat serbisyo sa pag-refresh ay tinutukoy ng partikular na kahulugan ng [uri .](https://www.w3.org/TR/vc-data-model/" \l "dfn-type)typeManualRefreshService2018idrefreshService

[HALIMBAWA20](https://www.w3.org/TR/vc-data-model/#example-usage-of-the-refreshservice-property-by-an-issuer): Paggamit ng refreshService property ng isang issuer

{

"@context": [

"https://www.w3.org/2018/credentials/v1",

"https://www.w3.org/2018/credentials/examples/v1"

],

"id": "http://example.edu/credentials/3732",

"type": ["VerifiableCredential", "UniversityDegreeCredential"],

"issuer": "https://example.edu/issuers/14",

"issuanceDate": "2010-01-01T19:23:24Z",

"credentialSubject": {

"id": "did:example:ebfeb1f712ebc6f1c276e12ec21",

"degree": {

"type": "BachelorDegree",

"pangalan": "Bachelor ng Agham at Sining"

}

},

**"refreshService": {**

**"id": "https://example.edu/refresh/3732",**

**"type": "ManualRefreshService2018"**

**}**

}

Sa halimbawa sa itaas, tinukoy ng [issuer](https://www.w3.org/TR/vc-data-model/#dfn-issuers)refreshService ang isang manual na maaaring gamitin sa pamamagitan ng pagdidirekta sa may [hawak](https://www.w3.org/TR/vc-data-model/#dfn-holders) o sa [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) sa https://example.edu/refresh/3732.

### **5.6Mga Tuntunin ng Paggamit**

Ang mga tuntunin ng paggamit ay maaaring gamitin ng isang [issuer](https://www.w3.org/TR/vc-data-model/#dfn-issuers) o isang may- [ari](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) upang ipaalam ang mga tuntunin kung saan inilabas ang isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) o na-verify na [presentasyon](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-presentations) . [Inilalagay ng tagabigay](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) ang kanilang mga tuntunin sa paggamit sa loob ng [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) . [Inilalagay ng may hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) ang kanilang mga tuntunin sa paggamit sa loob ng isang [nabe-verify na presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) . Tinutukoy ng detalyeng ito ang isang termsOfUse [katangian](https://www.w3.org/TR/vc-data-model/" \l "dfn-property) para sa pagpapahayag ng impormasyon ng mga tuntunin ng paggamit.

Ang halaga ng termsOfUse [property](https://www.w3.org/TR/vc-data-model/#dfn-property) ay nagsasabi sa [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) kung anong mga aksyon ang kinakailangan nitong gawin (isang obligasyon ), hindi pinapayagang gawin (isang pagbabawal ), o pinapayagang gawin (isang pahintulot ) kung ito ay upang tanggapin ang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) o [nabe-verify na presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) .

TANDAAN

Ang karagdagang pag-aaral ay kinakailangan upang matukoy kung paano inilalagay ng isang [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) na hindi isang may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) ang mga tuntunin ng paggamit sa kanilang [nabe-verify na mga kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) . Ang isang paraan ay maaaring para sa [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) na humiling sa nag- [isyu](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) na ilagay ang mga tuntunin ng paggamit sa loob ng ibinigay na mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) . Ang isa pang paraan ay maaaring para sa [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) na magtalaga ng isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) sa isang may- [ari](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) at maglagay ng mga tuntunin ng mga paghihigpit sa paggamit sa ipinagkaloob na [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) .

**mga Tuntunin ng Paggamit**

DAPAT tumukoy ang halaga ng termsOfUse [ari](https://www.w3.org/TR/vc-data-model/" \l "dfn-property) -arian ng isa o higit pang mga patakaran sa mga tuntunin ng paggamit kung saan ibinigay ng creator ang [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) o [presentasyon](https://www.w3.org/TR/vc-data-model/" \l "dfn-presentations) . Kung ang tatanggap (isang may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) o [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) ) ay hindi handang sumunod sa mga tinukoy na tuntunin ng paggamit, gagawin nila ito sa kanilang sariling pananagutan at maaaring magkaroon ng legal na pananagutan kung lalabag sila sa nakasaad na mga tuntunin ng paggamit. DAPAT tukuyin ng bawat value ang [uri](https://www.w3.org/TR/vc-data-model/" \l "dfn-type) nito , halimbawa, , at MAY tukuyin ang instance nito . Ang mga tiyak na nilalaman ng bawat termino ng paggamit ay tinutukoy ng partikular na kahulugan ng [uri .](https://www.w3.org/TR/vc-data-model/" \l "dfn-type)termsOfUseIssuerPolicyidtermsOfUse

[HALIMBAWA21](https://www.w3.org/TR/vc-data-model/#example-usage-of-the-termsofuse-property-by-an-issuer): Paggamit ng termsOfUse property ng isang issuer

Credential

{

"@context": [

"https://www.w3.org/2018/credentials/v1",

"https://www.w3.org/2018/credentials/examples/v1"

],

"id": "http://example.edu/credentials/3732",

"type": ["VerifiableCredential", "UniversityDegreeCredential"],

"issuer": "https://example.edu/issuers/14",

"issuanceDate": "2010-01-01T19:23:24Z",

"credentialSubject": {

"id": "did:example:ebfeb1f712ebc6f1c276e12ec21",

"degree": {

"type": "BachelorDegree",

"pangalan": "Bachelor ng Agham at Sining"

}

},

**"mga Tuntunin ng Paggamit": [{**

**"type": "IssuerPolicy",**

**"id": "http://example.com/policies/credential/4",**

**"profile": "http://example.com/profiles/credential",**

**"pagbabawal": [{**

**"assigner": "https://example.edu/issuers/14",**

**"assignee": "AllVerifiers",**

**"target": "http://example.edu/credentials/3732",**

**"action": ["Archival"]**

**}]**

**}]**

}

Verifiable Credential (may patunay)

{   
 "@context": [   
 "https://www.w3.org/2018/credentials/v1",   
 "https://www.w3.org/2018/credentials/examples/v1",   
 "https:// w3id.org/security/suites/ed25519-2020/v1"   
 ],   
 "id": "http://example.edu/credentials/3732",   
 "type": [   
 "VerifiableCredential",   
 "UniversityDegreeCredential"   
 ],   
 "issuer ": "https://example.edu/issuers/14",   
 "issuanceDate": "2010-01-01T19:23:24Z",   
 "credentialSubject": {   
 "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",   
 " degree": {   
 "type": "BachelorDegree",   
 "name": "Bachelor of Science and Arts"   
 }   
 },   
 "termsOfUse": [  
 {   
 "type": "IssuerPolicy",   
 "id": "http://example.com/policies/credential/4",   
 "profile": "http://example.com/profiles/credential",   
 "prohibition" : [   
 {   
 "assigner": "https://example.edu/issuers/14",   
 "assignee": "AllVerifiers",   
 "target": "http://example.edu/credentials/3732",   
 "action" : [   
 "Archival"   
 ]   
 }   
 ]   
 }   
 ],   
 "proof": {   
 "type": "Ed25519Signature2020",   
 "nilikha": "2022-02-25T14:58:43Z",   
 "verificationMethod": "https://example.edu/issuers/14#keys-1",  
 "proofPurpose": "assertionMethod",   
 "proofValue": "z2ty8BNvrKCvAXGqJVXF8aZ1jK5o5uXFvhXJksUXhn61uSwJJmWdcntf   
qvZTLbWmQHpieyhdcrG43em37R"Jo8   
 } bsw   
}

Verifiable Credential (bilang JWT)

---------------- JWT header ---------------   
{   
 "alg": "ES256",   
 "typ": "JWT"   
​​}   
--------------- JWT payload ---------------   
// TANDAAN: Ang halimbawa sa ibaba ay gumagamit ng wastong VC-JWT serialization   
// na duplicate ang iss, nbf, jti, at mga sub na field sa   
// Na-verify na Kredensyal (vc) na field.   
{   
 "vc": {   
 "@context": [   
 "https://www.w3.org/2018/credentials/v1",   
 "https://www.w3.org/2018/credentials/examples/v1"   
 ] ,   
 "id": "http://example.edu/credentials/3732",   
 "type": [   
 "VerifiableCredential",   
 "  
  
 "issuer": "https://example.edu/issuers/14",   
 "issuanceDate": "2010-01-01T19:23:24Z",   
 "credentialSubject": {   
 "id": "did:example:ebfeb1f712ebc6f1c276"e12ec276e12ec ,   
 "degree": {   
 "type": "BachelorDegree",   
 "name": "Bachelor of Science and Arts"   
 }   
 },   
 "termsOfUse": [   
 {   
 "type": "IssuerPolicy",   
 "id": "http:/ /example.com/policies/credential/4",   
 "profile": "http://example.com/profiles/credential",   
 "pagbabawal":[   
 {   
 "assigner": "https://example.edu/issuers/14",   
 "assignee": "AllVerifiers",  
 "target": "http://example.edu/credentials/3732",   
 "action": [   
 "Archival"   
 ]   
 }   
 ]   
 }   
 ]   
 },   
 "iss": "https://example.edu/issuers/14" ,   
 "nbf": 1262373804,   
 "jti": "http://example.edu/credentials/3732",   
 "sub": "did:example:ebfeb1f712ebc6f1c276e12ec21"   
}   
------------- -- JWT ---------------   
eyJhbGciOiJFUzI1NiIsInR5cCI6IkpXVCJ9.eyJ2YyI6eyJAY29udGV4dCI6WyJodHRwczovL3   
d3dy53My5vcmcvMjAxOC9jcmVkZW50aWFscy92MSIsImh0dHBzOi8vd3d3LnczLm9yZy8yMDE4L   
2NyZWRlbnRpYWxzL2V4YW1wbGVzL3YxIl0sImlkIjoiaHR0cDovL2V4YW1wbGUuZWR1L2NyZWRl  
bnRpYWxzLzM3MzIiLCJ0eXBlIjpbIlZlcmlmaWFibGVDcmVkZW50aWFsIiwiVW5pdmVyc2l0eUR   
lZ3JlZUNyZWRlbnRpYWwiXSwiaXNzdWVyIjoiaHR0cHM6Ly9leGFtcGxlLmVkdS9pc3N1ZXJzLz   
E0IiwiaXNzdWFuY2VEYXRlIjoiMjAxMC0wMS0wMVQxOToyMzoyNFoiLCJjcmVkZW50aWFsU3Via   
mVjdCI6eyJpZCI6ImRpZDpleGFtcGxlOmViZmViMWY3MTJlYmM2ZjFjMjc2ZTEyZWMyMSIsImRl   
Z3JlZSI6eyJ0eXBlIjoiQmFjaGVsb3JEZWdyZWUiLCJuYW1lIjoiQmFjaGVsb3Igb2YgU2NpZW5   
jZSBhbmQgQXJ0cyJ9fSwidGVybXNPZlVzZSI6W3sidHlwZSI6Iklzc3VlclBvbGljeSIsImlkIj   
oiaHR0cDovL2V4YW1wbGUuY29tL3BvbGljaWVzL2NyZWRlbnRpYWwvNCIsInByb2ZpbGUiOiJod   
HRwOi8vZXhhbXBsZS5jb20vcHJvZmlsZXMvY3JlZGVudGlhbCIsInByb2hpYml0aW9uIjpbeyJh   
c3NpZ25lciI6Imh0dHBzOi8vZXhhbXBsZS5lZHUvaXNzdWVycy8xNCIsImFzc2lnbmVlIjoiQWx  
sVmVyaWZpZXJzIiwidGFyZ2V0IjoiaHR0cDovL2V4YW1wbGUuZWR1L2NyZWRlbnRpYWxzLzM3Mz   
IiLCJhY3Rpb24iOlsiQXJjaGl2YWwiXX1dfV19LCJpc3MiOiJodHRwczovL2V4YW1wbGUuZWR1L   
2lzc3VlcnMvMTQiLCJuYmYiOjEyNjIzNzM4MDQsImp0aSI6Imh0dHA6Ly9leGFtcGxlLmVkdS9j   
cmVkZW50aWFscy8zNzMyIiwic3ViIjoiZGlkOmV4YW1wbGU6ZWJmZWIxZjcxMmViYzZmMWMyNzZ   
lMTJlYzIxIn0.YMeGs\_5KDNzta-h\_ehAY9RS6jyyJ8kB36QOXQL6GR1WCkWUz7S2ZUUsBblvipk   
cgnA4fCfdjI5c\_aZI3Ce8byw

Sa halimbawa sa itaas, ipinagbabawal ng [issuer](https://www.w3.org/TR/vc-data-model/#dfn-issuers) (ang ) ang mga [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) (ang ) na iimbak ang data sa isang archive. assignerassignee

[HALIMBAWA22](https://www.w3.org/TR/vc-data-model/#example-usage-of-the-termsofuse-property-by-a-holder): Paggamit ng termsOfUse property ng isang may-ari

{

"@context": [

"https://www.w3.org/2018/credentials/v1",

"https://www.w3.org/2018/credentials/examples/v1",

{

"@protected": totoo,

"VerifiablePresentationTermsOfUseExtension": {

"@id": "https://www.w3.org/2018/credentials/examples#VerifiablePresentationExtension",

"@context": {

"@protected": totoo,

"mga Tuntunin ng Paggamit": {

"@id": "https://www.w3.org/2018/credentials#termsOfUse",

"@type": "@id"

}

}

}

}

],

"id": "did:example:ebfeb1f712ebc6f1c276e12ec21",

"type": ["VerifiablePresentation", "VerifiablePresentationTermsOfUseExtension"],

"verifiableCredential": [{

"@context": [

"https://www.w3.org/2018/credentials/v1",

"https://www.w3.org/2018/credentials/examples/v1"

],

"id": "http://example.edu/credentials/3732",

"type": ["VerifiableCredential", "UniversityDegreeCredential"],

"issuer": "https://example.edu/issuers/14",

"issuanceDate": "2010-01-01T19:23:24Z",

"credentialSubject": {

"id": "did:example:ebfeb1f712ebc6f1c276e12ec21",

"degree": {

"type": "BachelorDegree",

"pangalan": "Bachelor ng Agham at Sining"

}

},

"patunay": { **...** }

}],

**"mga Tuntunin ng Paggamit": [{**

**"type": "HolderPolicy",**

**"id": "http://example.com/policies/credential/6",**

**"profile": "http://example.com/profiles/credential",**

**"pagbabawal": [{**

**"assigner": "did:example:ebfeb1f712ebc6f1c276e12ec21",**

**"assignee": "https://wineonline.example.org/",**

**"target": "http://example.edu/credentials/3732",**

**"action": ["3rdPartyCorrelation"]**

**}]**

**}]** ,

"patunay": [ ... ]

}

TANDAAN

Babala: Ang termsOfUseproperty ay hindi wastong tinukoy sa loob ng saklaw na VerifiablePresentationkonteksto. Isa itong bug na may kontekstong bersyon 1 at aayusin sa konteksto ng bersyon 2. Pansamantala, ang mga tagapagpatupad na gustong gumamit ng feature na ito ay kakailanganing palawigin ang konteksto ng kanilang [nabe-verify na presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) na may karagdagang termino na tumutukoy sa termsOfUseproperty, na pagkatapos ay magagamit sa tabi ng [nabe](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) -verify na uri ng presentasyon na property, upang ang termino ay maging semantically na kinikilala sa isang JSON-LD processor.

Sa halimbawa sa itaas, ang may- [ari](https://www.w3.org/TR/vc-data-model/#dfn-holders) (ang assigner), na siya ring [paksa](https://www.w3.org/TR/vc-data-model/#dfn-subjects) , ay nagpahayag ng termino ng paggamit na nagbabawal sa [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) (ang assignee, https://wineonline.example.org) mula sa paggamit ng impormasyong ibinigay upang iugnay ang may- [ari](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) o [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) gamit ang isang third-party na serbisyo. Kung gagamit ang [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) ng isang third-party na serbisyo para sa ugnayan, lalabagin nila ang mga tuntunin kung saan ginawa ng may- [ari](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) ang [presentasyon](https://www.w3.org/TR/vc-data-model/" \l "dfn-presentations) .

Inaasahang gagamitin din ang feature na ito ng mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) na ibinigay ng pamahalaan upang turuan ang mga digital na wallet na limitahan ang kanilang paggamit sa mga katulad na organisasyon ng pamahalaan sa pagtatangkang protektahan ang mga mamamayan mula sa hindi inaasahang paggamit ng sensitibong data. Katulad nito, ang ilang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) na ibinigay ng pribadong industriya ay inaasahang maglilimita sa paggamit sa loob ng mga departamento sa loob ng organisasyon, o sa mga oras ng negosyo. Hinihimok ang mga tagapagpatupad na magbasa nang higit pa tungkol sa mabilis na umuusbong na tampok na ito sa naaangkop na seksyon ng Mga Alituntunin sa Pagpapatupad ng Mga Napapatunayang Kredensyal [ [VC-IMP-GUIDE](https://www.w3.org/TR/vc-data-model/#bib-vc-imp-guide) ] na dokumento.

### **5.7Ebidensya**

Ang ebidensiya ay maaaring isama ng isang [tagabigay](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) upang mabigyan ang [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) ng karagdagang impormasyong sumusuporta sa isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) . Ito ay maaaring gamitin ng [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) upang itatag ang kumpiyansa kung saan ito umaasa sa mga claim sa [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) .

Halimbawa, maaaring suriin ng isang [tagabigay](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) ang pisikal na dokumentasyong ibinigay ng [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) o magsagawa ng isang hanay ng mga pagsusuri sa background bago ibigay ang [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) . Sa ilang partikular na sitwasyon, ang impormasyong ito ay kapaki-pakinabang sa [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) kapag tinutukoy ang panganib na nauugnay sa pag-asa sa isang partikular na [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) .

Tinutukoy ng detalyeng ito ang pag- evidence [aari](https://www.w3.org/TR/vc-data-model/" \l "dfn-property) para sa pagpapahayag ng impormasyon ng ebidensya.

**ebidensya**

Ang halaga ng ari- evidence [arian ay](https://www.w3.org/TR/vc-data-model/" \l "dfn-property)DAPAT na isa o higit pang mga scheme ng ebidensya na nagbibigay ng sapat na impormasyon para sa isang [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) upang matukoy kung ang ebidensyang nakalap ng nag- [isyu](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) ay nakakatugon sa mga kinakailangan sa kumpiyansa nito para sa pag-asa sa [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) . Ang bawat scheme ng ebidensya ay kinikilala ayon sa [uri](https://www.w3.org/TR/vc-data-model/" \l "dfn-type) nito . Opsyonal ang id [property , ngunit kung mayroon,](https://www.w3.org/TR/vc-data-model/#dfn-property)DAPAT maglaman ng URL na tumuturo kung saan mahahanap ang higit pang impormasyon tungkol sa halimbawang ito ng ebidensya. Ang tumpak na nilalaman ng bawat scheme ng ebidensya ay tinutukoy ng partikular na kahulugan ng evidence [uri .](https://www.w3.org/TR/vc-data-model/" \l "dfn-type)

TANDAAN

Para sa impormasyon tungkol sa kung paano maaaring suportahan ng detalye ang mga attachment at reference sa mga [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) at hindi kredensyal na data, tingnan ang dokumentong Mga Alituntunin sa Pagpapatupad ng Mga Na-verify na Kredensyal [ [VC-IMP-GUIDE](https://www.w3.org/TR/vc-data-model/#bib-vc-imp-guide) ].

[HALIMBAWA23](https://www.w3.org/TR/vc-data-model/#example-usage-of-the-evidence-property): Paggamit ng ari-arian ng ebidensya

{

"@context": [

"https://www.w3.org/2018/credentials/v1",

"https://www.w3.org/2018/credentials/examples/v1"

],

"id": "http://example.edu/credentials/3732",

"type": ["VerifiableCredential", "UniversityDegreeCredential"],

"issuer": "https://example.edu/issuers/14",

"issuanceDate": "2010-01-01T19:23:24Z",

"credentialSubject": {

"id": "did:example:ebfeb1f712ebc6f1c276e12ec21",

"degree": {

"type": "BachelorDegree",

"pangalan": "Bachelor ng Agham at Sining"

}

},

**"ebidensya": [{**

**"id": "https://example.edu/evidence/f2aeec97-fc0d-42bf-8ca7-0548192d4231",**

**"type": ["DocumentVerification"],**

**"verifier": "https://example.edu/issuers/14",**

**"evidenceDocument": "DriversLicense",**

**"subjectPresence": "Pisikal",**

**"documentPresence": "Pisikal",**

**"licenseNumber": "123AB4567"**

**}]** ,

"patunay": { **...** }

}

TANDAAN

Sa evidencehalimbawang ito, iginiit ng [nagbigay](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) na pisikal nilang itinugma ang [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) ng [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) sa isang pisikal na kopya ng lisensya sa pagmamaneho na may nakasaad na numero ng lisensya. Ang lisensya sa pagmamaneho na ito ay ginamit sa proseso ng pagbibigay upang i-verify na na-verify ng "Example University" ang paksa bago ang pag-isyu ng kredensyal at kung paano nila ito ginawa (pisikal na pag-verify).

TANDAAN

Ang ari- evidence [arian](https://www.w3.org/TR/vc-data-model/" \l "dfn-property) ay nagbibigay ng iba't ibang at komplementaryong impormasyon sa ari- proof [arian](https://www.w3.org/TR/vc-data-model/" \l "dfn-property) . Ginagamit ang ari- evidence [arian](https://www.w3.org/TR/vc-data-model/" \l "dfn-property) upang ipahayag ang sumusuportang impormasyon, gaya ng dokumentaryong ebidensya, na nauugnay sa integridad ng [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) . Sa kabaligtaran, ginagamit ang proof [property](https://www.w3.org/TR/vc-data-model/#dfn-property) upang ipahayag ang mga mathematical proof na nabe-verify ng machine na nauugnay sa pagiging tunay ng [nagbigay](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) at integridad ng [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) . Para sa karagdagang impormasyon tungkol sa proof [property](https://www.w3.org/TR/vc-data-model/#dfn-property) , tingnan ang Seksyon [4.7Mga Katibayan (Mga Lagda)](https://www.w3.org/TR/vc-data-model/#proofs-signatures) .

### **5.8Zero-Knowledge Proofs**

Ang zero-knowledge proof ay isang cryptographic na paraan kung saan mapapatunayan ng isang entity sa isa pang entity na alam nila ang isang partikular na halaga nang hindi inilalantad ang aktwal na halaga. Ang isang tunay na halimbawa sa mundo ay nagpapatunay na ang isang kinikilalang unibersidad ay nagbigay ng degree sa iyo nang hindi inilalantad ang iyong pagkakakilanlan o anumang iba pang personal na nakakapagpakilalang impormasyon na nasa degree.

Ang mga pangunahing kakayahan na ipinakilala ng mga mekanismong walang kaalaman sa patunay ay ang kakayahan ng isang may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) na:

* Pagsamahin ang maramihang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) mula sa maraming [tagabigay](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) sa isang [nabe-verify na presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) nang hindi naghahayag ng mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) o mga pagkakakilanlan ng [paksa sa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects)[verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) . Ginagawa nitong mas mahirap para sa [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) na makipagsabwatan sa alinman sa mga issuer tungkol sa mga ibinigay na [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) .
* Piliing ibunyag ang mga [claim](https://www.w3.org/TR/vc-data-model/#dfn-claims) sa isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) sa isang [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) nang hindi nangangailangan ng pagpapalabas ng maraming atomic na [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) . Nagbibigay-daan ito sa isang may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) na magbigay ng isang [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) na may eksaktong impormasyong kailangan nila at wala nang iba pa.
* Gumawa ng nakuhang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) na naka-format ayon sa schema ng data ng [verifier sa](https://www.w3.org/TR/vc-data-model/#dfn-verifier) halip na sa nag- [isyu](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) , nang hindi kinakailangang isangkot ang [nagbigay](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) pagkatapos ng ma-verify na pagpapalabas ng [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-credentials) . Nagbibigay ito ng malaking kakayahang umangkop para sa mga may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) na gamitin ang kanilang ibinigay na mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) .

Inilalarawan ng detalyeng ito ang isang modelo ng data na sumusuporta sa pumipili na pagbubunyag sa paggamit ng mga mekanismong walang kaalaman sa patunay. Itinatampok ng mga halimbawa sa ibaba kung paano magagamit ang modelo ng data upang mag-isyu, magpakita, at mag- verify ng mga [kredensyal na nabe](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-credentials) -verify na walang kaalaman .

Para sa isang may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) na gumamit ng zero-knowledge [verifiable presentation](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) , kailangan nila ng [issuer](https://www.w3.org/TR/vc-data-model/#dfn-issuers) na nag-isyu ng isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) sa paraang nagbibigay-daan sa may- [ari](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) na makakuha ng isang patunay mula sa orihinal na ibinigay na [verifiable na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) , para maipakita ng may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) ang impormasyon sa isang [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) sa paraang nagpapahusay sa privacy. Ito ay nagpapahiwatig na ang may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) ay maaaring patunayan ang bisa ng [nagbigay](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers)lagda nang hindi inilalantad ang mga halagang nilagdaan, o kapag inilalantad lamang ang ilang napiling halaga. Ang karaniwang kasanayan ay gawin ito sa pamamagitan ng pagpapatunay ng kaalaman sa pirma, nang hindi inilalantad ang mismong lagda. Mayroong dalawang kinakailangan para sa mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) kapag gagamitin ang mga ito sa mga zero-knowledge proof system.

* Ang [nabe-verify na kredensyal ay](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials)DAPAT maglaman ng Katibayan, gamit ang ari- proof [arian](https://www.w3.org/TR/vc-data-model/" \l "dfn-property) , upang ang may- [ari](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) ay makakuha ng isang [nabe-verify na pagtatanghal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) na naghahayag lamang ng impormasyon kaysa sa nilalayon na ihayag ng may- [ari .](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders)
* Kung ginagamit ang isang kahulugan ng [kredensyal ,](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential)DAPAT tukuyin ang kahulugan ng kredensyal sa [property](https://www.w3.org/TR/vc-data-model/#dfn-credential)[,](https://www.w3.org/TR/vc-data-model/#dfn-property) upang magamit ito ng lahat ng partido upang magsagawa ng iba't ibang mga cryptographic na operasyon sa zero-knowledge. credentialSchema

Ang sumusunod na halimbawa ay nagpapakita ng isang paraan ng paggamit ng mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) sa zero-knowledge. Gumagamit ito ng Camenisch-Lysyanskaya Signature [ [CL-SIGNATURES](https://www.w3.org/TR/vc-data-model/#bib-cl-signatures) ], na nagbibigay-daan sa pagtatanghal ng [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) sa paraang sumusuporta sa privacy ng may- [ari](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) at [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) sa pamamagitan ng paggamit ng pumipiling pagsisiwalat ng mga [nabe](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) -verify na halaga ng kredensyal. Ang ilang iba pang cryptographic system na umaasa sa zero-knowledge proofs upang piliing ibunyag ang mga attribute ay makikita rin sa [ [LDP-REGISTRY](https://www.w3.org/TR/vc-data-model/#bib-ldp-registry) ].

[HALIMBAWA24](https://www.w3.org/TR/vc-data-model/#example-a-verifiable-credential-that-supports-cl-signatures): Isang nabe-verify na kredensyal na sumusuporta sa CL Signatures

{

"@context": [

"https://www.w3.org/2018/credentials/v1",

"https://www.w3.org/2018/credentials/examples/v1"

],

"type": ["VerifiableCredential", "UniversityDegreeCredential"],

**"credentialSchema": {**

**"id": "did:example:cdf:35LB7w9ueWbagPL94T9bMLtyXDj9pX5o",**

**"type": "did:example:schema:22KpkXgecryx9k7N6XN1QoN3gXwBkSU8SfyyYQG"**

**}** ,

"issuer": "did:example:Wz4eUg7SetGfaUVCn8U9d62oDYrUJLuUtcy619",

"credentialSubject": {

"givenName": "Jane",

"familyName": "Doe",

"degree": {

"type": "BachelorDegree",

"name": "Bachelor of Science and Arts",

"college": "College of Engineering"

}

},

**"patunay": {**

**"type": "CLSignature2019",**

**"issuerData": "5NQ4TgzNfSQxoLzf2d5AV3JNiCdMaTgm...BXiX5UggB381QU7ZCgqWivUmy4D",**

**"attributes": "pPYmqDvwwWBDPNykXVrBtKdsJDeZUGFA...tTERiLqsZ5oxCoCSodPQaggkDJy",**

**"pirma": "8eGWSiTiWtEA8WnBwX4T259STpxpRKuk...kpFnikqqSP3GMW7mVxC4chxFhVs",**

**"signatureCorrectnessProof": "SNQbW3u1QV5q89qhxA1xyVqFa6jCrKwv...dsRypyuGGK3RhhBUvH1tPEL8orH"**

**}**

}

Ang halimbawa sa itaas ay nagbibigay ng [nabe](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) -verify na kahulugan ng kredensyal sa pamamagitan ng paggamit ng ari- credentialSchema [arian](https://www.w3.org/TR/vc-data-model/" \l "dfn-property) at isang partikular na patunay na magagamit sa Camenisch-Lysyanskaya Zero-Knowledge Proof system.

Ginagamit ng susunod na halimbawa ang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) sa itaas upang makabuo ng bagong nakuhang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) na may patunay na nagpapanatili ng privacy. Ang nakuhang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ay inilalagay sa isang [nabe-verify na presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) , upang ang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ay maghahayag lamang ng mga [claim](https://www.w3.org/TR/vc-data-model/#dfn-claims) at karagdagang metadata ng kredensyal na nilayon ng may- [ari .](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders)Para magawa ito, inaasahang matutugunan ang lahat ng sumusunod na kinakailangan:

* Ang bawat nakuhang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) sa loob ng isang [nabe-verify na pagtatanghal ay](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations)DAPAT maglaman ng lahat ng impormasyong kinakailangan upang ma-verify ang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) , alinman sa pamamagitan ng direktang pagsasama nito sa loob ng kredensyal, o sa pamamagitan ng pagtukoy sa kinakailangang impormasyon.
* Ang isang [nabe-verify na presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations)ay HINDI DAPAT mag-leak ng impormasyon na magbibigay-daan sa [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) na iugnay ang may- [ari](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) sa maraming [nabe-verify na mga presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) .
* DAPAT maglaman ng [property](https://www.w3.org/TR/vc-data-model/#dfn-property) ang [verifiable presentation](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) para ma-enable ang [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) na masuri na ang lahat ng nakuhang [verifiable na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) sa [verifiable presentation](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) ay ibinigay sa parehong may- [ari](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) nang hindi naglalabas ng personal na pagkakakilanlan na impormasyon na hindi nilalayong ibahagi ng may- [ari .](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders)proof

[HALIMBAWA25](https://www.w3.org/TR/vc-data-model/#example-a-verifiable-presentation-that-supports-cl-signatures): Isang nabe-verify na presentasyon na sumusuporta sa CL Signatures

{

"@context": [

"https://www.w3.org/2018/credentials/v1",

"https://www.w3.org/2018/credentials/examples/v1"

],

"type": "VerifiablePresentation",

"napapatunayang kredensyal": [

{

"@context": [

"https://www.w3.org/2018/credentials/v1",

"https://www.w3.org/2018/credentials/examples/v1"

],

"type": ["VerifiableCredential", "UniversityDegreeCredential"],

**"credentialSchema": {**

**"id": "did:example:cdf:35LB7w9ueWbagPL94T9bMLtyXDj9pX5o",**

**"type": "did:example:schema:22KpkXgecryx9k7N6XN1QoN3gXwBkSU8SfyyYQG"**

**}** ,

"issuer": "did:example:Wz4eUg7SetGfaUVCn8U9d62oDYrUJLuUtcy619",

"credentialSubject": {

"degreeType": "BachelorDegree",

"degreeSchool": "Kolehiyo ng Engineering"

},

**"patunay": {**

**"type": "AnonCredDerivedCredentialv1",**

**"primaryProof": "cg7wLNSi48K5qNyAVMwdYqVHSMv1Ur8i...Fg2ZvWF6zGvcSAsym2sgSk737",**

**"nonRevocationProof": "mu6fg24MfJPU1HvSXsf3ybzKARib4WxG...RSce53M6UwQCxYshCuS3d2h"**

**}**

}],

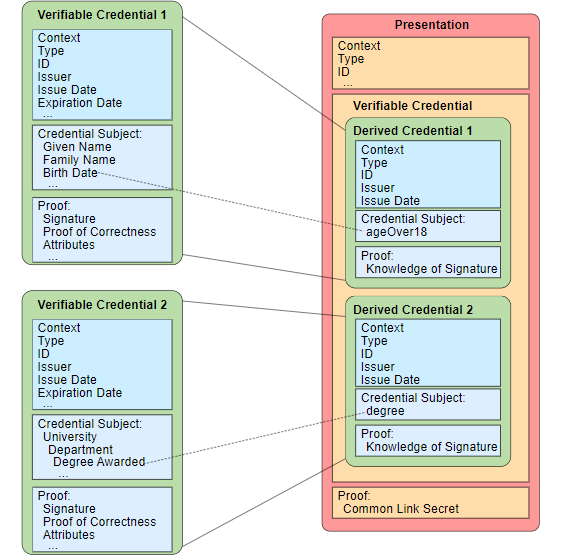
**"patunay": {**

**"type": "AnonCredPresentationProofv1",**

**"proofValue": "DgYdYMUYHURJLD7xdnWRinqWCEY5u5fK...j915Lt3hMzLHoPiPQ9sSVfRrs1D"**

**}**

}



(img src: <https://www.w3.org/TR/vc-data-model/diagrams/zkp-cred-pres.svg>)

*Pigura*11*Isang visual na halimbawa ng ugnayan sa pagitan ng mga kredensyal at mga hinangong kredensyal sa isang [pagtatanghal](https://www.w3.org/TR/vc-data-model/" \l "dfn-presentations) ng ZKP .*

TANDAAN

Ang mga mahahalagang detalye tungkol sa format para sa kahulugan ng [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) at ng mga patunay ay sinasadyang tinanggal dahil ang mga ito ay nasa labas ng saklaw ng dokumentong ito. Ang layunin ng seksyong ito ay gabayan ang mga tagapagpatupad na gustong palawigin ang mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) at na-verify na mga [presentasyon](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-presentations) upang suportahan ang mga zero-knowledge proof system.

### **5.9Mga pagtatalo**

Mayroong hindi bababa sa dalawang magkaibang kaso na isasaalang-alang para sa isang [entity](https://www.w3.org/TR/vc-data-model/#dfn-entities) na gustong i-dispute ang isang [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) na ibinigay ng isang [nagbigay](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) :

* Dini-dispute ng isang [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) ang isang paghahabol na ginawa ng [nagbigay](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) . Halimbawa, ang ari- address [arian](https://www.w3.org/TR/vc-data-model/" \l "dfn-property) ay hindi tama o luma na.
* Dini - dispute ng isang [entity](https://www.w3.org/TR/vc-data-model/#dfn-entities) ang isang posibleng maling claim na ginawa ng [nagbigay](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) tungkol sa ibang [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) . Halimbawa, inaangkin ng isang impostor ang numero ng social security para sa isang [entity](https://www.w3.org/TR/vc-data-model/#dfn-entities) .

Ang mekanismo para sa pagbibigay ng a DisputeCredentialay kapareho ng para sa isang regular na [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) maliban na ang credentialSubject identifier sa DisputeCredential [property](https://www.w3.org/TR/vc-data-model/#dfn-property) ay ang identifier ng pinagtatalunang [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) .

Halimbawa, kung ang isang [kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-credential) na may pagkakakilanlan ng https://example.org/credentials/245ay pinagtatalunan, maaaring ibigay ng [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) ang [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) na ipinapakita sa ibaba at ipakita ito sa [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) kasama ng pinagtatalunang [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) .

[HALIMBAWA26](https://www.w3.org/TR/vc-data-model/#example-a-subject-disputes-a-credential): Pinagtatalunan ng isang paksa ang isang kredensyal

{

"@context": [

"https://www.w3.org/2018/credentials/v1",

"https://www.w3.org/2018/credentials/examples/v1"

],

"id": "http://example.com/credentials/123",

"type": ["VerifiableCredential", "DisputeCredential"],

**"credentialSubject": {**

**"id": "http://example.com/credentials/245",**

**"currentStatus": "Pinagtatalunan",**

**"statusReason": {**

**"value": "Hindi napapanahon ang address.",**

**"lang": "en"**

**},**

**}** ,

"issuer": "https://example.com/people#me",

"issuanceDate": "2017-12-05T14:27:42Z",

"patunay": { **...** }

}

[Sa nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) sa itaas , sinasabi ng [tagabigay](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) na mali ang address sa pinagtatalunang [kredensyal na nabe -verify.](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-credentials)

TANDAAN

Kung walang identifier ang isang [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) , maaaring gamitin ang isang identifier na naka-address sa content para tukuyin ang pinagtatalunang [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) . Katulad nito, maaaring gamitin ang mga identifier na naka-address sa content para natatanging tukuyin ang mga indibidwal na claim.

TANDAAN

Ang lugar ng pag-aaral na ito ay mabilis na umuunlad at ang mga developer na interesado sa pag-publish ng mga [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) na tumututol sa katotohanan ng iba pang mga [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) ay hinihimok na basahin ang seksyong nauugnay sa mga hindi pagkakaunawaan sa dokumentong Mga Alituntunin sa Pagpapatupad ng Mga Napapatunayang Kredensyal [ [VC-IMP-GUIDE](https://www.w3.org/TR/vc-data-model/#bib-vc-imp-guide) ].

### **5.10Awtorisasyon**

Ang seksyong ito ay hindi normatibo.

[Ang mga nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ay inilaan bilang isang paraan ng mapagkakatiwalaang pagtukoy ng mga [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) . Bagama't kinikilala na ang Role Based Access Controls (RBACs) at Attribute Based Access Controls (ABACs) ay umaasa sa pagkakakilanlan na ito bilang isang paraan ng pagpapahintulot sa mga [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) na mag-access ng mga mapagkukunan, ang detalyeng ito ay hindi nagbibigay ng kumpletong solusyon para sa RBAC o ABAC. Ang pahintulot ay hindi angkop na paggamit para sa detalyeng ito nang walang kasamang balangkas ng awtorisasyon.

Isinaalang-alang ng Working Group ang mga kaso ng paggamit ng pahintulot sa panahon ng paggawa ng detalyeng ito at ginagawa ang gawaing iyon bilang isang layer ng arkitektura na binuo sa ibabaw ng detalyeng ito.

## 6.Mga syntax

Ang modelo ng data tulad ng inilarawan sa Mga Seksyon [3.Core Data Model](https://www.w3.org/TR/vc-data-model/#core-data-model) ,[4.Pangunahing Konsepto](https://www.w3.org/TR/vc-data-model/#basic-concepts) , at [5.Ang Advanced na Konsepto](https://www.w3.org/TR/vc-data-model/#advanced-concepts) ay ang canonical structural representation ng isang [verifiable credential](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) o [verifiable presentation](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) . Ang lahat ng mga serialization ay mga representasyon ng modelo ng data na iyon sa isang partikular na format. Tinutukoy ng seksyong ito kung paano naisasakatuparan ang modelo ng data sa JSON-LD at plain JSON. Bagama't ang mga syntactic mapping ay ibinibigay para lamang sa dalawang syntax na ito, maaaring gumamit ang mga application at serbisyo ng anumang iba pang syntax ng representasyon ng data (gaya ng XML, YAML, o CBOR) na may kakayahang ipahayag ang modelo ng data. Dahil ang mga kinakailangan sa pag- [verify](https://www.w3.org/TR/vc-data-model/#dfn-verify) at [pagpapatunay](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential-validation) ay tinukoy sa mga tuntunin ng modelo ng data, ang lahat ng mga serialization syntax ay kailangang isalin nang deterministiko sa modelo ng data para sa pagproseso, [pagpapatunay .](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential-validation), o paghahambing. Ang detalyeng ito ay hindi gumagawa ng mga kinakailangan para sa suporta ng anumang partikular na format ng serialization.

Ang inaasahang arity ng mga value ng property sa detalyeng ito, at ang resultang datatype na nagtataglay ng mga value na iyon, ay maaaring mag-iba depende sa property. Kung mayroon, ang mga sumusunod na katangian ay kinakatawan bilang isang halaga:

* id [ari-arian](https://www.w3.org/TR/vc-data-model/" \l "dfn-property)
* issuer [ari-arian](https://www.w3.org/TR/vc-data-model/" \l "dfn-property)
* issuanceDate [ari-arian](https://www.w3.org/TR/vc-data-model/" \l "dfn-property)
* expirationDate [ari- arian](https://www.w3.org/TR/vc-data-model/" \l "dfn-property) .

Ang lahat ng iba pang mga katangian, kung mayroon, ay kinakatawan bilang isang solong halaga o isang hanay ng mga halaga.

### **6.1JSON**

Ang modelo ng data, tulad ng inilarawan sa Seksyon[3.Core Data Model](https://www.w3.org/TR/vc-data-model/#core-data-model) , maaaring i-encode sa JavaScript Object Notation (JSON) [ [RFC8259](https://www.w3.org/TR/vc-data-model/#bib-rfc8259) ] sa pamamagitan ng pagmamapa ng mga value ng property sa mga uri ng JSON tulad ng sumusunod:

* Ang mga numerong halaga na kinakatawan bilang IEEE754 ay DAPAT na kinakatawan bilang isang uri ng Numero.
* DAPAT kinakatawan ang mga halaga ng Boolean bilang isang uri ng Boolean.
* DAPAT kinakatawan ang halaga ng sequence bilang isang uri ng Array.
* DAPAT kinakatawan ang mga hindi nakaayos na hanay ng mga halaga bilang isang uri ng Array.
* Ang mga hanay ng mga [katangian ay](https://www.w3.org/TR/vc-data-model/" \l "dfn-property)DAPAT na kinakatawan bilang isang uri ng Bagay.
* DAPAT kinakatawan ang mga walang laman na halaga bilang isang null na halaga.
* DAPAT kinakatawan ang ibang mga value bilang isang String type.

TANDAAN

Dahil ang mga pagbabagong nakalista dito ay may potensyal na hindi magkatugma na mga interpretasyon, ang karagdagang pag-profile ng JSON format ay kinakailangan upang magbigay ng isang tiyak na pagbabago sa modelo ng data.

### **6.2JSON-LD**

Ang [ [JSON-LD](https://www.w3.org/TR/vc-data-model/#bib-json-ld) ] ay isang format na nakabatay sa JSON na ginagamit para i-serialize ang [Linked Data](http://www.w3.org/TR/ld-glossary/#linked-data) . Ang syntax ay idinisenyo upang madaling maisama sa mga naka-deploy na system na gumagamit na ng JSON, at nagbibigay ng maayos na landas ng pag-upgrade mula sa JSON patungo sa [ [JSON-LD](https://www.w3.org/TR/vc-data-model/#bib-json-ld) ]. Pangunahing nilayon itong maging isang paraan upang magamit ang Naka-link na Data sa mga kapaligiran ng programming na nakabatay sa Web, upang bumuo ng mga interoperable na serbisyo sa Web, at mag-imbak ng Naka-link na Data sa mga storage engine na nakabatay sa JSON.

Ang [ [JSON-LD](https://www.w3.org/TR/vc-data-model/#bib-json-ld) ] ay kapaki-pakinabang kapag pinalawak ang modelo ng data na inilalarawan sa detalyeng ito. Ang mga instance ng modelo ng data ay naka-encode sa [ [JSON-LD](https://www.w3.org/TR/vc-data-model/#bib-json-ld) ] sa parehong paraan na naka-encode ang mga ito sa JSON (Seksyon[6.1JSON](https://www.w3.org/TR/vc-data-model/#json) ), kasama ang pagdaragdag ng @context [property](https://www.w3.org/TR/vc-data-model/#dfn-property) . Ang [konteksto ng JSON-LD](https://www.w3.org/TR/json-ld/" \l "the-context) ay inilarawan nang detalyado sa detalye ng [ [JSON-LD](https://www.w3.org/TR/vc-data-model/#bib-json-ld) ] at ang paggamit nito ay idinetalye sa Seksyon[5.3Extensibility](https://www.w3.org/TR/vc-data-model/#extensibility) .

MAAARING gumamit o pagsamahin ang maraming konteksto upang ipahayag ang anumang arbitraryong impormasyon tungkol sa mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) sa idiomatic na JSON. Ang [konteksto ng JSON-LD](https://www.w3.org/TR/json-ld/#the-context) , na makukuha sa https://www.w3.org/2018/credentials/v1, ay isang static na dokumento na hindi naa-update at samakatuwid ay maaaring i-download at i-cache ang panig ng kliyente. Ang nauugnay na dokumento ng bokabularyo para sa Verifiable Credentials Data Model ay available sa https://www.w3.org/2018/credentials.

#### 6.2.1Syntactic Sugar

Sa pangkalahatan, ang modelo ng data at mga syntax na inilarawan sa dokumentong ito ay idinisenyo upang ang mga developer ay maaaring kumopya at mag-paste ng mga halimbawa upang isama ang mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) sa kanilang mga software system. Ang layunin ng disenyo ng diskarteng ito ay magbigay ng mababang hadlang sa pagpasok habang tinitiyak pa rin ang pandaigdigang interoperability sa pagitan ng magkakaibang hanay ng mga software system. Inilalarawan ng seksyong ito ang ilan sa mga pamamaraang ito, na malamang na hindi mapapansin ng karamihan sa mga developer, ngunit kung saan ang mga detalye ay magiging interesado sa mga nagpapatupad. Ang pinakakapansin-pansing syntactic sugar na ibinigay ng [ [JSON-LD](https://www.w3.org/TR/vc-data-model/#bib-json-ld) ] ay:

* Ang @idat @typemga keyword ay naka-alyas sa idat ayon sa typepagkakabanggit, na nagbibigay-daan sa mga developer na gamitin ang detalyeng ito bilang idiomatic na JSON.
* Ang mga uri ng data, gaya ng mga integer, petsa, unit ng sukat, at URL, ay awtomatikong tina-type upang magbigay ng mas malakas na garantiya ng uri para sa mga sitwasyon ng paggamit na nangangailangan ng mga ito.
* Ang verifiableCredentialat mga proof [katangian](https://www.w3.org/TR/vc-data-model/" \l "dfn-property) ay itinuturing bilang mga lalagyan ng graph . Ibig sabihin, mga mekanismong ginagamit upang ihiwalay ang mga set ng data na iginiit ng iba't ibang entity. Tinitiyak nito, halimbawa, ang wastong cryptographic separation sa pagitan ng data graph na ibinigay ng bawat [issuer](https://www.w3.org/TR/vc-data-model/#dfn-issuers) at ang ibinigay ng may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) na nagpapakita ng [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) upang matiyak na ang pinagmulan ng impormasyon para sa bawat graph ay napanatili.
* Ang @protectedfeature na katangian ng [ [JSON-LD](https://www.w3.org/TR/vc-data-model/#bib-json-ld) ] 1.1 ay ginagamit upang matiyak na ang mga terminong tinukoy ng detalyeng ito ay hindi ma-override. Nangangahulugan ito na hangga't ang parehong @contextdeklarasyon ay ginawa sa itaas ng isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) o na-verify na [presentasyon](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-presentations) , ginagarantiyahan ang interoperability para sa lahat ng terminong nauunawaan ng mga user ng modelo ng data, gumagamit man sila ng isang [ [JSON-LD](https://www.w3.org/TR/vc-data-model/#bib-json-ld) ] processor o hindi.

### **6.3Mga Format ng Patunay**

Ang modelo ng data na inilarawan sa detalyeng ito ay idinisenyo upang maging proof na format na agnostic. Ang pagtutukoy na ito ay hindi karaniwang nangangailangan ng anumang partikular na digital proof o format ng lagda. Habang ang data model ay ang canonical representation ng isang [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) o [presentasyon](https://www.w3.org/TR/vc-data-model/" \l "dfn-presentations), ang mga mekanismo ng pagpapatunay para sa mga ito ay madalas na nakatali sa syntax na ginagamit sa pagpapadala ng dokumento sa pagitan ng mga partido. Dahil dito, kailangang tukuyin ng bawat mekanismo ng pagpapatunay kung ang pagpapatunay ng patunay ay kinakalkula laban sa estado ng dokumento bilang ipinadala, laban sa posibleng binagong modelo ng data, o laban sa ibang anyo. Sa oras ng paglalathala, hindi bababa sa dalawang format ng patunay ang aktibong ginagamit ng mga nagpapatupad at nadama ng Working Group na ang pagdodokumento kung ano ang mga format na patunay na ito at kung paano ginagamit ang mga ito ay magiging kapaki-pakinabang sa mga nagpapatupad. Ang mga seksyong nagdedetalye sa kasalukuyang mga format ng patunay na aktibong ginagamit upang magbigay ng mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ay:

* Seksyon[6.3.1JSON Web Token](https://www.w3.org/TR/vc-data-model/#json-web-token) , at
* Seksyon[6.3.2Mga Katibayan ng Integridad ng Data](https://www.w3.org/TR/vc-data-model/#data-integrity-proofs) .

#### 6.3.1JSON Web Token

Ang JSON Web Token (JWT) [ [RFC7519](https://www.w3.org/TR/vc-data-model/#bib-rfc7519) ] ay isa pa ring malawakang ginagamit na paraan upang ipahayag ang mga [claim](https://www.w3.org/TR/vc-data-model/#dfn-claims) na ililipat sa pagitan ng dalawang partido. Ang pagbibigay ng representasyon ng Verifiable Credentials Data Model para sa JWT ay nagbibigay-daan sa mga kasalukuyang system at library na lumahok sa ecosystem na inilalarawan sa Seksyon [1.2Pangkalahatang- ideya ng Ecosystem](https://www.w3.org/TR/vc-data-model/#ecosystem-overview) . Ang isang JWT ay nag-e-encode ng isang hanay ng mga [claim](https://www.w3.org/TR/vc-data-model/#dfn-claims) bilang JSON object na nakapaloob sa isang JSON Web Signature (JWS) [ [RFC7515](https://www.w3.org/TR/vc-data-model/#bib-rfc7515) ] o JWE [ [RFC7516](https://www.w3.org/TR/vc-data-model/#bib-rfc7516) ]. Para sa detalyeng ito, ang paggamit ng JWE ay wala sa saklaw.

##### *Kaugnayan sa Nabe-verify na Modelo ng Data ng Mga Kredensyal*

Tinutukoy ng detalyeng ito ang mga panuntunan sa pag-encode ng Verifiable Credential Data Model sa JWT at JWS. Tinutukoy pa nito ang mga panuntunan sa pagpoproseso kung paano at kailan dapat gamitin ang mga partikular na pangalan ng [claim](https://www.w3.org/TR/vc-data-model/#dfn-claims) na nakarehistro sa JWT at mga pangalan ng parameter ng header na nakarehistro sa JWS na nakarehistro upang payagan ang mga system batay sa JWT na sumunod sa detalyeng ito. Kung ang mga partikular na pangalan ng [claim at mga parameter ng header na ito ay naroroon,](https://www.w3.org/TR/vc-data-model/#dfn-claims)MAAARING tanggalin ang kani-kanilang katapat sa karaniwang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) at [nabe-verify na presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) upang maiwasan ang pagdoble.

##### *Mga Extension ng JSON Web Token*

Ang detalyeng ito ay nagpapakilala ng dalawang bagong nakarehistrong pangalan ng [claim](https://www.w3.org/TR/vc-data-model/#dfn-claims) , na naglalaman ng mga bahaging iyon ng karaniwang [nabe-verify na mga kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) at [nabe-verify na mga presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) kung saan walang malinaw na mga panuntunan sa pag-encode para sa JWT. Ang mga bagay na ito ay nakapaloob sa JWT payload gaya ng sumusunod:

* vc: JSON object, na DAPAT naroroon sa isang JWT na [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) . Ang bagay ay naglalaman ng [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) ayon sa detalyeng ito.
* vp: JSON object, na DAPAT naroroon sa isang JWT [verifiable presentation](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) . Ang bagay ay naglalaman ng [pagtatanghal](https://www.w3.org/TR/vc-data-model/" \l "dfn-presentations) ayon sa detalyeng ito.

##### *Mga Pagsasaalang-alang ng JWT at JWS*

###### Pag-encode ng JWT

Upang mag-encode ng isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) bilang isang JWT, ang mga partikular na [katangian](https://www.w3.org/TR/vc-data-model/" \l "dfn-property) na ipinakilala ng detalyeng ito ay DAPAT na alinman sa:

* Naka-encode bilang karaniwang mga parameter ng header ng JOSE, o
* [Naka-encode bilang mga nakarehistrong pangalan ng claim](https://www.w3.org/TR/vc-data-model/#dfn-claims) ng JWT , o
* Nakapaloob sa bahagi ng lagda ng JWS.

Kung walang tinukoy na tahasang panuntunan, ang mga [property](https://www.w3.org/TR/vc-data-model/#dfn-property) ay naka-encode sa parehong paraan tulad ng sa isang karaniwang [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) , at idinaragdag sa vc [claim](https://www.w3.org/TR/vc-data-model/#dfn-claims) ng JWT. Tulad ng lahat ng JWT, ang JWS-based na lagda ng isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) na kinakatawan sa JWT syntax ay kinakalkula laban sa literal na halaga ng string ng JWT na ipinakita sa kabuuan ng wire, bago ilapat ang anumang mga panuntunan sa pag-decode o pagbabago. Inilalarawan ng mga sumusunod na talata ang mga panuntunang ito sa pag-encode.

Kung naroroon ang isang JWS, ang digital signature ay tumutukoy sa alinman sa [nagbigay](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) ng [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) , o sa kaso ng isang [nabe-verify na presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) , sa may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) ng na- verify na [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-credentials) . Pinatutunayan ng JWS na issnilagdaan ng JWT ang nilalamang JWT payload at samakatuwid, maaaring tanggalin ang proof [ari](https://www.w3.org/TR/vc-data-model/" \l "dfn-property) -arian.

Kung walang JWS, DAPAT magbigay ng proof [property](https://www.w3.org/TR/vc-data-model/#dfn-property) . Maaaring gamitin ang [ari](https://www.w3.org/TR/vc-data-model/" \l "dfn-property) -arian upang kumatawan sa isang mas kumplikadong patunay, gaya ng maaaring kailanganin kung iba ang gumawa sa [nagbigay](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) , o isang patunay na hindi batay sa mga digital na lagda, gaya ng Proof of Work. MAAARING may kasamang JWS at [property](https://www.w3.org/TR/vc-data-model/#dfn-property) ang [nagbigay](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) . Para sa mga dahilan ng backward compatibility, DAPAT gamitin ng issuer ang JWS para kumatawan ng mga patunay batay sa isang digital signature. proof proof

Nalalapat ang mga sumusunod na panuntunan sa mga header ng JOSE sa konteksto ng detalyeng ito:

* alg DAPAT itakda para sa mga digital na lagda. Kung kailangan lang ang proof [property](https://www.w3.org/TR/vc-data-model/#dfn-property) para sa napiling paraan ng lagda (iyon ay, kung walang pagpipilian ng algorithm sa loob ng paraang iyon), DAPAT itakda ang algheader sa . none
* kid MAAARING gamitin kung maraming key ang nauugnay sa [nagbigay](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) ng JWT. Ang pangunahing pagtuklas ay wala sa saklaw ng pagtutukoy na ito. Halimbawa, ang kidmaaaring sumangguni sa isang susi sa isang [DID na dokumento](https://www.w3.org/TR/vc-data-model/#dfn-decentralized-identifier-documents) , o maaaring maging identifier ng isang susi sa loob ng isang JWKS.
* typ, kung naroroon, DAPAT itakda sa JWT.

Para sa backward compatibility sa mga JWT processor, DAPAT gamitin ang mga sumusunod na rehistradong pangalan ng claim ng JWT, sa halip na o bilang karagdagan sa, kani-kanilang karaniwang [nabe](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) -verify na mga katapat na kredensyal:

* exp DAPAT kumatawan sa expirationDate [property](https://www.w3.org/TR/vc-data-model/#dfn-property) , na naka-encode bilang UNIX timestamp ( NumericDate).
* iss DAPAT kumatawan sa pag- issuer [aari](https://www.w3.org/TR/vc-data-model/" \l "dfn-property) ng isang nabe-verify na kredensyal o sa pag- holder [aari](https://www.w3.org/TR/vc-data-model/" \l "dfn-property) ng isang na-verify na pagtatanghal.
* nbf DAPAT kumakatawan issuanceDatesa , naka-encode bilang isang timestamp ng UNIX ( NumericDate).
* jti DAPAT kumatawan sa pag- id [aari](https://www.w3.org/TR/vc-data-model/" \l "dfn-property) ng [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) o na-verify na [pagtatanghal](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-presentations) .
* sub DAPAT kumatawan sa ari- id [arian](https://www.w3.org/TR/vc-data-model/" \l "dfn-property) na nakapaloob sa credentialSubject.

TANDAAN

Sa bearer credentialsat presentations, subay hindi naroroon.

* aud DAPAT kumatawan (ibig sabihin, tukuyin) ang nilalayong madla ng [nabe-verify na presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) (ibig sabihin, ang [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) na nilayon ng nagtatanghal na may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) na tumanggap at i-verify ang [nabe-verify na presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) ).

Maaaring gamitin ang iba pang mga parameter ng header ng JOSE at mga pangalan ng claim ng JWT na hindi tinukoy dito kung hindi tahasan ang paggamit ng mga ito. DAPAT idagdag ang mga karagdagang [nabe -verify na](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials)[claim](https://www.w3.org/TR/vc-data-model/#dfn-claims) sa kredensyal sa ari- arian ng JWT. credentialSubject

TANDAAN

Para sa higit pang impormasyon tungkol sa paggamit ng mga parameter ng header ng JOSE at/o mga pangalan ng claim ng JWT na hindi tinukoy dito, tingnan ang dokumentong Mga Alituntunin sa Pagpapatupad ng Mga Na-verify na Kredensyal [ [VC-IMP-GUIDE](https://www.w3.org/TR/vc-data-model/#bib-vc-imp-guide) ].

Ang bersyon na ito ng detalye ay hindi tumutukoy sa mga panuntunan sa pag-encode na tukoy sa JWT para sa mga konseptong nakabalangkas sa Mga [Advanced na Konsepto](https://www.w3.org/TR/vc-data-model/#advanced-concepts) ng Seksyon (halimbawa, refreshService, termsOfUse, at evidence). Ang mga konseptong ito ay maaaring i-encode nang walang anumang pagbabago, at maaaring idagdag sa vcJWT [claim](https://www.w3.org/TR/vc-data-model/#dfn-claims) .

TANDAAN

Binabalaan ang mga tagapagpatupad na ang mga JWT ay walang kakayahang mag-encode ng maraming [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) at sa gayon ay hindi kayang mag-encode ng isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) na may higit sa isang [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) . Maaaring suportahan ng mga JWT ang maraming paksa sa hinaharap at pinapayuhan ang mga tagapagpatupad na sumangguni sa [Registry](https://www.iana.org/assignments/jwt/) ng Claim ng JSON Web Token para sa mga pangalan ng claim ng JWT na maraming paksa o ang detalye ng [Nested JSON Web Token](https://datatracker.ietf.org/doc/draft-yusef-oauth-nested-jwt/) .

###### JWT Decoding

Upang i-decode ang isang JWT sa isang karaniwang [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) o [presentasyon ,](https://www.w3.org/TR/vc-data-model/" \l "dfn-presentations)DAPAT isagawa ang sumusunod na pagbabagong-anyo :

1. Gumawa ng JSON object.
2. Idagdag ang content mula sa vco vp [claim](https://www.w3.org/TR/vc-data-model/#dfn-claims) sa bagong JSON object.
3. Ibahin ang anyo ng natitirang mga partikular na header at [claim](https://www.w3.org/TR/vc-data-model/#dfn-claims) sa JWT , at idagdag ang mga resulta sa bagong [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) o [presentation](https://www.w3.org/TR/vc-data-model/#dfn-presentations) na JSON object.

Upang baguhin ang mga partikular na header at [claim ng JWT ,](https://www.w3.org/TR/vc-data-model/#dfn-claims)DAPAT gawin ang sumusunod :

* Kung naroroon, DAPAT ma-convert expang UNIX timestamp sa isang [ [XMLSCHEMA11-2](https://www.w3.org/TR/xmlschema11-2/#dateTime) ] , at DAPAT gamitin upang itakda ang halaga ng [property](https://www.w3.org/TR/vc-data-model/#dfn-property) ng bagong JSON object. date-timeexpirationDate credentialSubject
* Kung issnaroroon, DAPAT gamitin ang value para itakda ang issuer [property](https://www.w3.org/TR/vc-data-model/#dfn-property) ng bagong [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) na JSON object o ang holder [property](https://www.w3.org/TR/vc-data-model/#dfn-property) ng bagong [presentation](https://www.w3.org/TR/vc-data-model/#dfn-presentations) na JSON object.
* Kung naroroon, DAPAT ma-convert nbfang UNIX timestamp sa isang [ [XMLSCHEMA11-2](https://www.w3.org/TR/xmlschema11-2/#dateTime) ] , at DAPAT gamitin upang itakda ang halaga ng [property](https://www.w3.org/TR/vc-data-model/#dfn-property) ng bagong JSON object. date-timeissuanceDate
* Kung subnaroroon, DAPAT gamitin ang value para itakda ang value ng id [property](https://www.w3.org/TR/vc-data-model/#dfn-property) ng credentialSubjectbagong [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) na JSON object.
* Kung jtinaroroon, DAPAT gamitin ang value para itakda ang value ng id [property](https://www.w3.org/TR/vc-data-model/#dfn-property) ng bagong object ng JSON.

[HALIMBAWA27](https://www.w3.org/TR/vc-data-model/#example-jwt-header-of-a-jwt-based-verifiable-credential-using-jws-as-a-proof-non-normative): JWT header ng isang JWT-based na nabe-verify na kredensyal gamit ang JWS bilang isang patunay (non-normative)

{

"alg": "RS256",

"typ": "JWT",

"bata": "did:example:abfe13f712120431c276e12ecab#keys-1"

}

Sa halimbawa sa itaas, ang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ay gumagamit ng isang proofbatay sa JWSmga digital na lagda, at ang kaukulang [verification](https://www.w3.org/TR/vc-data-model/#dfn-verify) key ay maaaring makuha gamit ang kid header parameter.

[HALIMBAWA28](https://www.w3.org/TR/vc-data-model/#example-jwt-payload-of-a-jwt-based-verifiable-credential-using-jws-as-a-proof-non-normative): JWT payload ng JWT-based verifiable credential gamit ang JWS bilang patunay (non-normative)

{

"sub": "did:example:ebfeb1f712ebc6f1c276e12ec21",

"jti": "http://example.edu/credentials/3732",

"iss": "https://example.com/keys/foo.jwk",

"nbf": 1541493724,

"iat": 1541493724,

"exp": 1573029723,

"nonce": "660!6345FSer",

"vc": {

"@context": [

"https://www.w3.org/2018/credentials/v1",

"https://www.w3.org/2018/credentials/examples/v1"

],

"type": ["VerifiableCredential", "UniversityDegreeCredential"],

"credentialSubject": {

"degree": {

"type": "BachelorDegree",

"pangalan": "Bachelor ng Agham at Sining"

}

}

}

}

Sa halimbawa sa itaas, vchindi naglalaman ng id [property](https://www.w3.org/TR/vc-data-model/#dfn-property) dahil ginagamit ng JWT encoding ang jti attribute para kumatawan sa isang natatanging identifier. Ine - subencode ng attribute ang impormasyong kinakatawan ng id [property](https://www.w3.org/TR/vc-data-model/#dfn-property) ng credentialSubject. Ang nonceay idinagdag upang ihinto ang isang replay na pag-atake.

[HALIMBAWA29](https://www.w3.org/TR/vc-data-model/#example-verifiable-credential-using-jwt-compact-serialization-non-normative): Nabe-verify na kredensyal gamit ang JWT compact serialization (non-normative)

eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6ImRpZDpleGFtcGxlOmFiZmUxM2Y3MTIxMjA0

MzFjMjc2ZTEyZWNhYiNrZXlzLTEifQ. **eyJzdWIiOiJkaWQ6ZXhhbXBsZTplYmZlYjFmNzEyZWJjNmYxY**

**zI3NmUxMmVjMjEiLCJqdGkiOiJodHRwOi8vZXhhbXBsZS5lZHUvY3JlZGVudGlhbHMvMzczMiIsImlzc**

**yI6Imh0dHBzOi8vZXhhbXBsZS5jb20va2V5cy9mb28uandrIiwibmJmIjoxNTQxNDkzNzI0LCJpYXQiO**

**jE1NDE0OTM3MjQsImV4cCI6MTU3MzAyOTcyMywibm9uY2UiOiI2NjAhNjM0NUZTZXIiLCJ2YyI6eyJAY**

**29udGV4dCI6WyJodHRwczovL3d3dy53My5vcmcvMjAxOC9jcmVkZW50aWFscy92MSIsImh0dHBzOi8vd**

**3d3LnczLm9yZy8yMDE4L2NyZWRlbnRpYWxzL2V4YW1wbGVzL3YxIl0sInR5cGUiOlsiVmVyaWZpYWJsZ**

**UNyZWRlbnRpYWwiLCJVbml2ZXJzaXR5RGVncmVlQ3JlZGVudGlhbCJdLCJjcmVkZW50aWFsU3ViamVjd**

**CI6eyJkZWdyZWUiOnsidHlwZSI6IkJhY2hlbG9yRGVncmVlIiwibmFtZSI6IjxzcGFuIGxhbmc9J2ZyL**

**UNBJz5CYWNjYWxhdXLDqWF0IGVuIG11c2lxdWVzIG51bcOpcmlxdWVzPC9zcGFuPiJ9fX19** .KLJo5GAy

BND3LDTn9H7FQokEsUEi8jKwXhGvoN3JtRa51xrNDgXDb0cq1UTYB-rK4Ft9YVmR1NI\_ZOF8oGc\_7wAp

8PHbF2HaWodQIoOBxxT-4WNqAxft7ET6lkH-4S6Ux3rSGAmczMohEEf8eCeN-jC8WekdPl6zKZQj0YPB

1rx6X0-xlFBs7cl6Wt8rfBP\_tZ9YgVWrQmUWypSioc0MUyiphmyEbLZagTyPlUyflGlEdqrZAv6eSe6R

txJy6M1-lD7a5HTzanYTWBPAUHDZGyGKXdJw-W\_x0IWChBzI8t3kpG253fg6V3tPgHeKXE94fz\_QpYfg

--7kLsyBAfQGbg

[HALIMBAWA30](https://www.w3.org/TR/vc-data-model/#example-jwt-header-of-a-jwt-based-verifiable-presentation-non-normative): JWT header ng isang JWT based verifiable presentation (non-normative)

{

"alg": "RS256",

"typ": "JWT",

"bata": "did:example:ebfeb1f712ebc6f1c276e12ec21#keys-1"

}

Sa halimbawa sa itaas, ang [nabe-verify na presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) ay gumagamit ng isang proofbatay sa JWSmga digital na lagda, at ang kaukulang [verification](https://www.w3.org/TR/vc-data-model/#dfn-verify) key ay maaaring makuha gamit ang kid header na parameter.

[HALIMBAWA31](https://www.w3.org/TR/vc-data-model/#example-jwt-payload-of-a-jwt-based-verifiable-presentation-non-normative): JWT payload ng isang JWT based verifiable presentation (non-normative)

{

"iss": "did:example:ebfeb1f712ebc6f1c276e12ec21",

"jti": "urn:uuid:3978344f-8596-4c3a-a978-8fcaba3903c5",

"aud": "did:example:4a57546973436f6f6c4a4a57573",

"nbf": 1541493724,

"iat": 1541493724,

"exp": 1573029723,

"nonce": "343s$FSFDa-",

"vp": {

"@context": [

"https://www.w3.org/2018/credentials/v1",

"https://www.w3.org/2018/credentials/examples/v1"

],

"type": ["VerifiablePresentation"],

**// base64url-encoded JWT bilang string na**

"verifiableCredential": [" **...** "]

}

}

Sa halimbawa sa itaas, vphindi naglalaman ng id [property](https://www.w3.org/TR/vc-data-model/#dfn-property) dahil ginagamit ng JWT encoding ang jti attribute para kumatawan sa isang natatanging identifier. verifiableCredential naglalaman ng string array ng mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) gamit ang JWTcompact serialization. Ang nonceay idinagdag upang ihinto ang isang replay na pag-atake.

[HALIMBAWA32](https://www.w3.org/TR/vc-data-model/#example-verifiable-presentation-using-jwt-compact-serialization-non-normative): Na-verify na presentasyon gamit ang JWT compact serialization (non-normative)

eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6ImRpZDpleGFtcGxlOjB4YWJjI2tleTEifQ. **e**

**yJpc3MiOiJkaWQ6ZXhhbXBsZTplYmZlYjFmNzEyZWJjNmYxYzI3NmUxMmVjMjEiLCJqdGkiOiJ1cm46d**

**XVpZDozOTc4MzQ0Zi04NTk2LTRjM2EtYTk3OC04ZmNhYmEzOTAzYzUiLCJhdWQiOiJkaWQ6ZXhhbXBsZ**

**To0YTU3NTQ2OTczNDM2ZjZmNmM0YTRhNTc1NzMiLCJuYmYiOjE1NDE0OTM3MjQsImlhdCI6MTU0MTQ5M**

**zcyNCwiZXhwIjoxNTczMDI5NzIzLCJub25jZSI6IjM0M3MkRlNGRGEtIiwidnAiOnsiQGNvbnRleHQiO**

**lsiaHR0cHM6Ly93d3cudzMub3JnLzIwMTgvY3JlZGVudGlhbHMvdjEiLCJodHRwczovL3d3dy53My5vc**

**mcvMjAxOC9jcmVkZW50aWFscy9leGFtcGxlcy92MSJdLCJ0eXBlIjpbIlZlcmlmaWFibGVQcmVzZW50Y**

**XRpb24iLCJDcmVkZW50aWFsTWFuYWdlclByZXNlbnRhdGlvbiJdLCJ2ZXJpZmlhYmxlQ3JlZGVudGlhb**

**CI6WyJleUpoYkdjaU9pSlNVekkxTmlJc0luUjVjQ0k2SWtwWFZDSXNJbXRwWkNJNkltUnBaRHBsZUdGd**

**GNHeGxPbUZpWm1VeE0yWTNNVEl4TWpBME16RmpNamMyWlRFeVpXTmhZaU5yWlhsekxURWlmUS5leUp6Z**

**FdJaU9pSmthV1E2WlhoaGJYQnNaVHBsWW1abFlqRm1OekV5WldKak5tWXhZekkzTm1VeE1tVmpNakVpT**

**ENKcWRHa2lPaUpvZEhSd09pOHZaWGhoYlhCc1pTNWxaSFV2WTNKbFpHVnVkR2xoYkhNdk16Y3pNaUlzS**

**W1semN5STZJbWgwZEhCek9pOHZaWGhoYlhCc1pTNWpiMjB2YTJWNWN5OW1iMjh1YW5kcklpd2libUptS**

**WpveE5UUXhORGt6TnpJMExDSnBZWFFpT2pFMU5ERTBPVE0zTWpRc0ltVjRjQ0k2TVRVM016QXlPVGN5T**

**Xl3aWJtOXVZMlVpT2lJMk5qQWhOak0wTlVaVFpYSWlMQ0oyWXlJNmV5SkFZMjl1ZEdWNGRDSTZXeUpvZ**

**EhSd2N6b3ZMM2QzZHk1M015NXZjbWN2TWpBeE9DOWpjbVZrWlc1MGFXRnNjeTkyTVNJc0ltaDBkSEJ6T**

**2k4dmQzZDNMbmN6TG05eVp5OHlNREU0TDJOeVpXUmxiblJwWVd4ekwyVjRZVzF3YkdWekwzWXhJbDBzS**

**W5SNWNHVWlPbHNpVm1WeWFXWnBZV0pzWlVOeVpXUmxiblJwWVd3aUxDSlZibWwyWlhKemFYUjVSR1ZuY**

**21WbFEzSmxaR1Z1ZEdsaGJDSmRMQ0pqY21Wa1pXNTBhV0ZzVTNWaWFtVmpkQ0k2ZXlKa1pXZHlaV1VpT**

**25zaWRIbHdaU0k2SWtKaFkyaGxiRzl5UkdWbmNtVmxJaXdpYm1GdFpTSTZJanh6Y0dGdUlHeGhibWM5S**

**jJaeUxVTkJKejVDWVdOallXeGhkWExEcVdGMElHVnVJRzExYzJseGRXVnpJRzUxYmNPcGNtbHhkV1Z6U**

**EM5emNHRnVQaUo5ZlgxOS5LTEpvNUdBeUJORDNMRFRuOUg3RlFva0VzVUVpOGpLd1hoR3ZvTjNKdFJhN**

**TF4ck5EZ1hEYjBjcTFVVFlCLXJLNEZ0OVlWbVIxTklfWk9GOG9HY183d0FwOFBIYkYySGFXb2RRSW9PQ**

**nh4VC00V05xQXhmdDdFVDZsa0gtNFM2VXgzclNHQW1jek1vaEVFZjhlQ2VOLWpDOFdla2RQbDZ6S1pRa**

**jBZUEIxcng2WDAteGxGQnM3Y2w2V3Q4cmZCUF90WjlZZ1ZXclFtVVd5cFNpb2MwTVV5aXBobXlFYkxaY**

**WdUeVBsVXlmbEdsRWRxclpBdjZlU2U2UnR4Snk2TTEtbEQ3YTVIVHphbllUV0JQQVVIRFpHeUdLWGRKd**

**y1XX3gwSVdDaEJ6STh0M2twRzI1M2ZnNlYzdFBnSGVLWEU5NGZ6X1FwWWZnLS03a0xzeUJBZlFHYmciX**

**X19** .ft\_Eq4IniBrr7gtzRfrYj8Vy1aPXuFZU-6\_ai0wvaKcsrzI4JkQEKTvbJwdvIeuGuTqy7ipO-EYi

7V4TvonPuTRdpB7ZHOlYlbZ4wA9WJ6mSVSqDACvYRiFvrOFmie8rgm6GacWatgO4m4NqiFKFko3r58Lu

eFfGw47NK9RcfOkVQeHCq4btaDqksDKeoTrNysF4YS89INa-prWomrLRahnwLOo1Etp3E4ESAxg73CR2

kA5AoMbf5KtFueWnMcSbQkMRdWcGC1VssC0tB0JffVjq7ZV6OTyV4kl1-UVgiPLXUTpupFfLRhf9QpqM

BjYgP62KvhIvW8BbkGUelYMetA

#### 6.3.2Mga Katibayan ng Integridad ng Data

Ginagamit ng detalyeng ito ang Linked Data upang mag-publish ng impormasyon sa Web gamit ang mga pamantayan, gaya ng mga URL at JSON-LD, upang matukoy ang mga [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) at ang mga nauugnay na katangian ng mga ito. Kapag ang impormasyon ay ipinakita sa ganitong paraan, ang iba pang nauugnay na impormasyon ay madaling matuklasan at ang mga bagong impormasyon ay madaling pagsamahin sa umiiral na graph ng kaalaman. Ang Linked Data ay napapalawak sa isang desentralisadong paraan, na lubos na nagpapababa ng mga hadlang sa malawakang pagsasama. Ang modelo ng data sa detalyeng ito ay gumagana nang maayos sa [Data Integrity](https://w3c-ccg.github.io/data-integrity-spec/) at sa nauugnay na [Linked Data Cryptographic Suite](https://w3c-ccg.github.io/ld-cryptosuite-registry/) na idinisenyo upang protektahan ang data model gaya ng inilalarawan ng detalyeng ito.

Hindi tulad ng paggamit ng JSON Web Token, walang karagdagang pre- o post-processing ang kailangan. Ang format ng Data Integrity Proofs ay idinisenyo upang simple at madaling protektahan ang [mga nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-credentials) at na-verify na [mga presentasyon](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-presentations) . Ang pagprotekta sa isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) o na-verify na [presentasyon](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-presentations) ay kasing simple ng pagpasa ng isang wastong halimbawa sa detalyeng ito sa isang pagpapatupad ng Linked Data Signatures at pagbuo ng isang digital na lagda.

TANDAAN

Para sa higit pang impormasyon tungkol sa iba't ibang katangian ng iba't ibang format ng syntax (halimbawa, JSON+JWT, JSON-LD+JWT, o JSON-LD+LD-Proofs), tingnan ang dokumentong Mga Alituntunin sa Pagpapatupad ng Mga Na-verify na Kredensyal [ [VC-IMP-GUIDE](https://www.w3.org/TR/vc-data-model/#bib-vc-imp-guide) ] .

## 7.Mga Pagsasaalang-alang sa Privacy

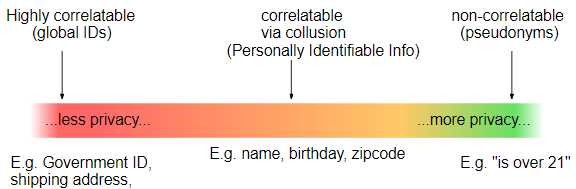
Ang seksyong ito ay hindi normatibo.

Idinedetalye ng seksyong ito ang mga pangkalahatang pagsasaalang-alang sa privacy at partikular na implikasyon sa privacy ng pag-deploy ng Verifiable Credentials Data Model sa mga production environment.

### **7.1Spectrum ng Privacy**

Ang seksyong ito ay hindi normatibo.

Mahalagang kilalanin na mayroong isang spectrum ng privacy mula sa pseudonymous hanggang sa matinding natukoy. Depende sa kaso ng paggamit, ang mga tao ay may iba't ibang antas ng kaginhawaan tungkol sa kung anong impormasyon ang nais nilang ibigay at kung anong impormasyon ang maaaring makuha mula sa kung ano ang ibinigay.



(img src: <https://www.w3.org/TR/vc-data-model/diagrams/privacy-spectrum.svg>)

*Pigura*12*Ang spectrum ng privacy mula sa pseudonymous hanggang sa ganap na natukoy.*

Halimbawa, karamihan sa mga tao ay malamang na gustong manatiling hindi nagpapakilala kapag bumibili ng alak dahil ang kinakailangang pagsusuri sa regulasyon ay batay lamang sa kung ang isang tao ay higit sa isang partikular na edad. Bilang kahalili, para sa mga medikal na reseta na isinulat ng isang doktor para sa isang pasyente, ang botika na tumutupad sa reseta ay kinakailangan upang mas matibay na kilalanin ang medikal na propesyonal at ang pasyente. Samakatuwid walang isang diskarte sa privacy na gumagana para sa lahat ng mga kaso ng paggamit. Ang mga solusyon sa privacy ay partikular sa kaso ng paggamit.

TANDAAN

Kahit na para sa mga gustong manatiling anonymous kapag bumibili ng alak, maaaring kailanganin pa rin ang photo identification para magbigay ng naaangkop na katiyakan sa merchant. Maaaring hindi kailangang malaman ng merchant ang iyong pangalan o iba pang mga detalye (maliban sa lampas ka na sa isang partikular na edad), ngunit sa maraming pagkakataon ay maaaring hindi pa rin sapat ang patunay lamang ng edad upang matugunan ang mga regulasyon.

Ang Verifiable Credentials Data Model ay nagsusumikap na suportahan ang buong privacy spectrum at hindi kumukuha ng mga pilosopikal na posisyon sa tamang antas ng anonymity para sa anumang partikular na transaksyon. Ang mga sumusunod na seksyon ay nagbibigay ng patnubay para sa mga nagpapatupad na gustong umiwas sa mga partikular na senaryo na salungat sa privacy.

### **7.2Personal na Makikilalang Impormasyon**

Ang seksyong ito ay hindi normatibo.

Ang data na nauugnay sa mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) na nakaimbak sa credential.credentialSubjectfield ay madaling kapitan ng mga paglabag sa privacy kapag ibinahagi sa mga [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) . Ang personal na pagtukoy ng data, gaya ng identifier na ibinigay ng pamahalaan, address sa pagpapadala, at buong pangalan, ay madaling magamit upang matukoy, masubaybayan, at maiugnay ang isang [entity](https://www.w3.org/TR/vc-data-model/#dfn-entities) . Kahit na ang impormasyong mukhang hindi personal na makikilala, tulad ng kumbinasyon ng petsa ng kapanganakan at isang postal code, ay may napakalakas na ugnayan at mga kakayahan sa pag-de-anonymize.

Lubos na pinapayuhan ang mga tagapagpatupad na bigyan ng babala ang mga may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) kapag nagbabahagi sila ng data sa mga ganitong uri ng katangian. [Ang mga nag- isyu](https://www.w3.org/TR/vc-data-model/#dfn-issuers) ay mahigpit na pinapayuhan na magbigay ng mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) na nagpoprotekta sa privacy kapag posible. Halimbawa, ang pagbibigay ng mga ageOver [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) sa halip na petsa ng kapanganakan ng mga na- verify na [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-credentials) kapag ang isang [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) ay gustong tukuyin kung ang isang [entity](https://www.w3.org/TR/vc-data-model/#dfn-entities) ay lampas sa edad na 18.

Dahil ang isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ay kadalasang naglalaman ng personally identifiable information (PII), ang mga nagpapatupad ay mahigpit na pinapayuhan na gumamit ng mga mekanismo habang iniimbak at dinadala ang mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) na nagpoprotekta sa data mula sa mga hindi dapat mag-access dito. Kasama sa mga mekanismo na maaaring isaalang-alang ang Transport Layer Security (TLS) o iba pang paraan ng pag-encrypt ng data habang nasa transit, pati na rin ang pag-encrypt o mga mekanismo ng kontrol sa pag-access ng data upang maprotektahan ang data sa isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) habang nakapahinga.

### **7.3Identifier-Based Correlation**

Ang seksyong ito ay hindi normatibo.

[Tinutukoy ang mga paksa](https://www.w3.org/TR/vc-data-model/#dfn-subjects) ng mga [nabe](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) -verify na kredensyal gamit ang credential.credentialSubject.idfield. Ang mga identifier na ginamit upang tukuyin ang isang [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) ay lumilikha ng mas malaking panganib ng ugnayan kapag ang mga identifier ay matagal nang nabubuhay o ginagamit sa higit sa isang web domain.

Katulad nito, ang pagsisiwalat ng [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) na pagkakakilanlan ( credential.id) ay humahantong sa mga sitwasyon kung saan maraming [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) , o isang [issuer](https://www.w3.org/TR/vc-data-model/#dfn-issuers) at isang [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) , ay maaaring magsabwatan upang iugnay ang may- [ari](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) . Kung gusto ng mga may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) na bawasan ang ugnayan, dapat silang gumamit ng mga [nabe-verify na scheme ng kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) na nagbibigay-daan sa pagtatago ng identifier sa panahon ng [nabe-verify na presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) . Inaasahan ng mga ganitong scheme na bubuo ng may- [ari](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) ang identifier at maaaring pahintulutan pa ang pagtatago ng identifier mula sa [issuer](https://www.w3.org/TR/vc-data-model/#dfn-issuers) , habang pinapanatili pa rin ang identifier na naka-embed at naka-sign sa [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) .

Kung ang mga malakas na katangian ng anti-correlation ay isang kinakailangan sa isang [nabe](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) -verify na sistema ng mga kredensyal, lubos na ipinapayo na ang mga identifier ay alinman sa:

* Nakatali sa iisang pinanggalingan
* pang-isahang gamit
* Hindi man nagamit, ngunit sa halip ay pinalitan ng panandaliang, single-use bearer token.

### **7.4Pagkakaugnay na Batay sa Lagda**

Ang seksyong ito ay hindi normatibo.

Ang mga nilalaman ng mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ay sinigurado gamit ang credential.prooffield. Ang mga [katangian](https://www.w3.org/TR/vc-data-model/" \l "dfn-property) sa field na ito ay lumilikha ng mas malaking panganib ng ugnayan kapag ang parehong mga halaga ay ginagamit sa higit sa isang session o domain at ang halaga ay hindi nagbabago. Kasama sa mga halimbawa ang verificationMethod, created, proofPurpose, at mga jwsfield.

Kung kinakailangan ang matibay na mga katangian ng anti-correlation, pinapayuhan na ang mga signature value at metadata ay muling bubuo sa bawat oras na gumagamit ng mga teknolohiya tulad ng mga third-party na pairwise signature, zero-knowledge proof, o group signature.

TANDAAN

Kahit na gumagamit ng mga anti-correlation na lagda, ang impormasyon ay maaaring nasa isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) na tinatalo ang mga anti-correlation na katangian ng cryptography na ginamit.

### **7.5Long-Lived Identifier-Based Correlation**

Ang seksyong ito ay hindi normatibo.

[Ang mga nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ay maaaring maglaman ng mga pangmatagalang identifier na maaaring magamit upang iugnay ang mga indibidwal. Kasama sa mga uri ng identifier na ito ang mga [subject](https://www.w3.org/TR/vc-data-model/#dfn-subjects) identifier, email address, government-issued identifier, organization-issue identifier, address, healthcare vitals, [nabe-verify na credential](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) -specific na JSON-LD na konteksto, at marami pang ibang uri ng pangmatagalang identifier.

Ang mga organisasyong nagbibigay ng software sa mga may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) ay dapat magsikap na tukuyin ang mga field sa [mga nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-credentials) na naglalaman ng impormasyon na maaaring magamit upang maiugnay ang mga indibidwal at bigyan ng babala ang mga may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) kapag ang impormasyong ito ay ibinahagi.

### **7.6Fingerprinting ng Device**

Ang seksyong ito ay hindi normatibo.

May mga mekanismong panlabas sa mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) na ginagamit upang subaybayan at iugnay ang mga indibidwal sa Internet at sa Web. Ang ilan sa mga mekanismong ito ay kinabibilangan ng Internet protocol (IP) address tracking, web browser fingerprinting, evercookies, advertising network tracker, mobile network position information, at in-application Global Positioning System (GPS) API. Ang paggamit ng mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ay hindi makakapigil sa paggamit ng iba pang mga teknolohiyang ito sa pagsubaybay. Gayundin, kapag ginamit ang mga teknolohiyang ito kasabay ng mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) , maaaring matuklasan ang bagong nauugnay na impormasyon. Halimbawa, ang isang kaarawan na isinama sa isang posisyon ng GPS ay maaaring gamitin upang lubos na maiugnay ang isang indibidwal sa maraming website.

Inirerekomenda na pigilan ng mga system na may paggalang sa privacy ang paggamit ng iba pang mga teknolohiya sa pagsubaybay kapag ginagamit ang mga [nabe](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) -verify na kredensyal. Sa ilang mga kaso, maaaring kailanganing i-disable ang mga teknolohiya sa pagsubaybay sa mga device na nagpapadala ng mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) sa ngalan ng isang may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) .

### **7.7Pabor sa Abstract na Claim**

Ang seksyong ito ay hindi normatibo.

Upang bigyang-daan ang mga tatanggap ng [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) na gamitin ang mga ito sa iba't ibang sitwasyon nang hindi naghahayag ng higit pang PII kaysa sa kinakailangan para sa mga transaksyon, dapat isaalang-alang ng mga [issuer](https://www.w3.org/TR/vc-data-model/#dfn-issuers) ang paglilimita sa impormasyong nai-publish sa isang [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) sa isang minimal na hanay na kinakailangan para sa mga inaasahang layunin. Ang isang paraan upang maiwasan ang paglalagay ng PII sa isang [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) ay ang paggamit ng abstract na [property](https://www.w3.org/TR/vc-data-model/#dfn-property) na nakakatugon sa mga pangangailangan ng mga [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) nang hindi nagbibigay ng partikular na impormasyon tungkol sa isang [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) .

Halimbawa, ginagamit ng dokumentong ito ang ageOver [property](https://www.w3.org/TR/vc-data-model/#dfn-property) sa halip na isang partikular na petsa ng kapanganakan, na bumubuo ng mas malakas na PII. Kung ang mga retailer sa isang partikular na market ay karaniwang nangangailangan ng mga mamimili na mas matanda sa isang partikular na edad, maaaring piliin ng isang [issuer](https://www.w3.org/TR/vc-data-model/#dfn-issuers) na pinagkakatiwalaan sa market na iyon na mag-alok ng isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) na nagsasabing natugunan ng mga [paksa ang kinakailangang iyon sa halip na mag-alok ng mga](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects)[nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) na naglalaman ng mga [claim](https://www.w3.org/TR/vc-data-model/#dfn-claims) tungkol sa mga partikular na petsa ng kapanganakan. Nagbibigay-daan ito sa mga indibidwal na customer na bumili nang hindi nagpapakita ng partikular na PII.

### **7.8Ang Prinsipyo ng Pag-minimize ng Data**

Ang seksyong ito ay hindi normatibo.

Nagaganap ang mga paglabag sa privacy kapag ang impormasyong ibinunyag sa isang konteksto ay tumagas sa isa pa. Ang tinatanggap na pinakamahusay na kasanayan para sa pagpigil sa mga naturang paglabag ay upang limitahan ang impormasyon na hinihiling, at natanggap, sa ganap na minimum na kinakailangan. Ang pamamaraang ito sa pagliit ng data ay kinakailangan ng regulasyon sa maraming hurisdiksyon, kabilang ang Health Insurance Portability and Accountability Act (HIPAA) sa United States at ang General Data Protection Regulation (GDPR) sa European Union.

Sa mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) , ang pag-minimize ng data para sa mga [issuer](https://www.w3.org/TR/vc-data-model/#dfn-issuers) ay nangangahulugan ng paglilimita sa nilalaman ng isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) sa minimum na kinakailangan ng mga potensyal na [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) para sa inaasahang paggamit. Para sa mga [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) , ang pag-minimize ng data ay nangangahulugan ng paglilimita sa saklaw ng impormasyong hinihiling o kinakailangan para sa pag-access ng mga serbisyo.

Halimbawa, ang lisensya sa pagmamaneho na naglalaman ng numero ng driver's ID, taas, timbang, kaarawan, at address ng tahanan ay isang [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) na naglalaman ng higit pang impormasyon kaysa kinakailangan upang matukoy na ang tao ay higit sa isang tiyak na edad.

Itinuturing na pinakamahusay na kasanayan para sa mga [issuer](https://www.w3.org/TR/vc-data-model/#dfn-issuers) na i-atomize ang impormasyon o gumamit ng signature scheme na nagbibigay-daan para sa [selective disclosure](https://www.w3.org/TR/vc-data-model/#dfn-selective-disclosure) . Halimbawa, ang isang [nagbigay](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) ng mga lisensya sa pagmamaneho ay maaaring mag-isyu ng isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) na naglalaman ng bawat katangian na lumalabas sa isang lisensya sa pagmamaneho, pati na rin isang hanay ng mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) kung saan ang bawat na-verify na [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-credentials) ay naglalaman lamang ng isang katangian, gaya ng kaarawan ng isang tao. Maaari rin itong mag-isyu ng mas abstract na [mga nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-credentials) (halimbawa, isang na-verify na [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-credentials) na naglalaman lamang ng isang ageOverkatangian). Ang isang posibleng adaptasyon ay para sa [mga issuer](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers)upang magbigay ng mga secure na HTTP endpoint para sa pagkuha ng mga single-use [bearer na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-bearer-credentials) na nagpo-promote ng pseudonymous na paggamit ng mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) . Dapat isaalang-alang ng mga tagapagpatupad na ito ay hindi praktikal o hindi ligtas, ang paggamit ng [mga piling pamamaraan ng pagsisiwalat](https://www.w3.org/TR/vc-data-model/" \l "dfn-selective-disclosure) na nag-aalis ng pag-asa sa mga nag- [isyu](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) sa oras ng pagpapatunay at binabawasan ang panganib sa temporal na ugnayan mula sa [mga nagbigay](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) .

[Ang mga verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) ay hinihimok na humiling lamang ng impormasyon na talagang kinakailangan para sa isang partikular na transaksyon na mangyari. Ito ay mahalaga para sa hindi bababa sa dalawang dahilan. ito:

* Binabawasan ang pananagutan sa [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) para sa paghawak ng napakasensitibong impormasyon na hindi nito kailangan.
* Pinapahusay ang privacy ng indibidwal sa pamamagitan lamang ng pagtatanong ng impormasyong kinakailangan para sa isang partikular na transaksyon.

TANDAAN

Bagama't posibleng isagawa ang prinsipyo ng minimum na pagsisiwalat, maaaring imposibleng maiwasan ang malakas na pagkakakilanlan ng isang indibidwal para sa mga partikular na kaso ng paggamit sa isang session o sa maraming session. Hindi maaaring bigyang-diin ng mga may-akda ng dokumentong ito kung gaano kahirap matugunan ang prinsipyong ito sa mga totoong sitwasyon.

### **7.9Mga Kredensyal ng Tagapagdala**

Ang seksyong ito ay hindi normatibo.

Ang **kredensyal ng tagadala** ay isang piraso ng impormasyong nagpapahusay sa privacy, gaya ng tiket sa konsiyerto, na nagbibigay ng karapatan sa may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) ng kredensyal ng may hawak sa isang partikular na mapagkukunan nang hindi nagbubunyag ng sensitibong impormasyon tungkol sa may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) . Ang mga kredensyal ng maydala ay kadalasang ginagamit sa mga kaso ng paggamit na mababa ang panganib kung saan ang pagbabahagi ng kredensyal ng maydala ay hindi nababahala o hindi magreresulta sa malaking pagkalugi sa ekonomiya o reputasyon.

[Ang mga nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) na mga [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-bearer-credentials) ng may hawak ay ginagawang posible sa pamamagitan ng hindi pagtukoy sa [subject](https://www.w3.org/TR/vc-data-model/#dfn-subjects) identifier, na ipinahayag gamit ang id [property](https://www.w3.org/TR/vc-data-model/#dfn-property) , na naka-nest sa credentialSubject [property](https://www.w3.org/TR/vc-data-model/#dfn-property) . Halimbawa, ang sumusunod na [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ay isang may [hawak na kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-bearer-credentials) :

[HALIMBAWA33](https://www.w3.org/TR/vc-data-model/#example-usage-of-issuer-properties): Paggamit ng mga ari-arian ng issuer

Credential

{

"@context": [

"https://www.w3.org/2018/credentials/v1",

"https://www.w3.org/2018/credentials/examples/v1"

],

"id": "http://example.edu/credentials/temporary/28934792387492384",

"type": ["VerifiableCredential", "UniversityDegreeCredential"],

"issuer": "https://example.edu/issuers/14",

"issuanceDate": "2017-10-22T12:23:48Z",

"credentialSubject": {

**// tandaan na ang 'id' property ay hindi tinukoy para sa mga kredensyal ng maydala**

"degree": {

"type": "BachelorDegree",

"pangalan": "Bachelor ng Agham at Sining"

}

}

}

Verifiable Credential (may patunay)

{   
 "@context": [   
 "https://www.w3.org/2018/credentials/v1",   
 "https://www.w3.org/2018/credentials/examples/v1",   
 "https:// w3id.org/security/suites/ed25519-2020/v1"   
 ],   
 "id": "http://example.edu/credentials/temporary/28934792387492384",   
 "type": [   
 "VerifiableCredential", "   
 UniversityDegreeCredential" "issuer": "https://example.edu/issuers/14", "issuanceDate": "2017-10-22T12:23:48Z", "credentialSubject": { "degree": { "type": "BachelorDegree ", "pangalan":"Bachelor of Science and Arts" } }, "proof": { "type": "Ed25519Signature2020",  
 "created": "2022-02-25T14:58:43Z",   
 "verificationMethod": "https://example.edu/issuers/14#keys-1",   
 "proofPurpose": "assertionMethod",   
 "proofValue": "z49oZrBSGbo4ASwCLCms2YGkGbgHtFyAv8J5849XF4qwhNqRvs92FZtH   
ZdHFMcA1uwDWNKhxvikAvRfmUjKFJUUWT"   
 }   
}

Bagama't ang mga [kredensyal ng maydala](https://www.w3.org/TR/vc-data-model/" \l "dfn-bearer-credentials) ay maaaring mapahusay ang pagkapribado, dapat itong maingat na gawin upang hindi aksidenteng magbunyag ng higit pang impormasyon kaysa sa inaasahan ng may- [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) ng [kredensyal ng maydala](https://www.w3.org/TR/vc-data-model/" \l "dfn-bearer-credentials) . Halimbawa, ang paulit-ulit na paggamit ng parehong [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-bearer-credentials) ng may hawak sa maraming site ay nagbibigay-daan sa mga site na ito na potensyal na magsabwatan upang labis na subaybayan o iugnay ang may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) . Gayundin, ang impormasyong maaaring mukhang hindi nagpapakilala, gaya ng petsa ng kapanganakan at postal code, ay maaaring gamitin para sa istatistikal na pagkilala sa isang indibidwal kapag ginamit nang magkasama sa parehong [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-bearer-credentials) o session ng maydala.

Dapat tiyakin ng mga nag-isyu ng mga kredensyal ng maydala na ang mga [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) ng [maydala](https://www.w3.org/TR/vc-data-model/" \l "dfn-bearer-credentials)[ay](https://www.w3.org/TR/vc-data-model/#dfn-bearer-credentials) nagbibigay ng mga benepisyong nagpapahusay sa privacy na:

* Ay pang-isahang gamit, kung posible.
* Huwag maglaman ng personal na pagkakakilanlan ng impormasyon.
* Hindi masyadong nakakaugnay.

Dapat bigyan ng babala ang mga may [hawak ng kanilang software kung ang mga](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders)[kredensyal ng maydala](https://www.w3.org/TR/vc-data-model/#dfn-bearer-credentials) na naglalaman ng sensitibong impormasyon ay inisyu o hiniling, o kung may panganib sa pagkakaugnay kapag pinagsasama ang dalawa o higit pang mga [kredensyal ng maydala](https://www.w3.org/TR/vc-data-model/" \l "dfn-bearer-credentials) sa isa o higit pang mga sesyon. Bagama't maaaring imposibleng matukoy ang lahat ng mga panganib sa ugnayan, ang ilan ay maaaring tiyak na matukoy.

[Ang mga verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) ay hindi dapat humiling ng mga [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-bearer-credentials) ng may hawak na maaaring gamitin upang labis na maiugnay ang may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) .

### **7.10Mga Pagsusuri sa Bisa**

Ang seksyong ito ay hindi normatibo.

Kapag nagpoproseso ng mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) , ang mga [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) ay inaasahang magsasagawa ng marami sa mga pagsusuring nakalista sa Appendix[A.Pagpapatunay](https://www.w3.org/TR/vc-data-model/#validation) pati na rin ang iba't ibang partikular na pagsusuri sa proseso ng negosyo. Maaaring kasama sa mga pagsusuri sa bisa ang pagsusuri:

* Ang katayuan ng propesyonal na lisensya ng may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) .
* Isang petsa ng pag-renew o pagbawi ng lisensya.
* Ang mga sub-kwalipikasyon ng isang indibidwal.
* Kung mayroong relasyon sa pagitan ng may- [ari](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) at ng [entidad](https://www.w3.org/TR/vc-data-model/" \l "dfn-entities) kung saan sinusubukang makipag-ugnayan ng may- [ari .](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders)
* Ang impormasyon ng geolocation na nauugnay sa may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) .

Ang proseso ng pagsasagawa ng mga pagsusuring ito ay maaaring magresulta sa pagtagas ng impormasyon na humahantong sa isang paglabag sa privacy ng may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) . Halimbawa, ang isang simpleng operasyon gaya ng pagsuri sa isang listahan ng pagbawi ay maaaring mag-abiso sa [nagbigay](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) na ang isang partikular na negosyo ay malamang na nakikipag-ugnayan sa may- [ari](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) . Maaari nitong bigyang-daan ang mga [issuer](https://www.w3.org/TR/vc-data-model/#dfn-issuers) na makipagsabwatan at iugnay ang mga indibidwal nang hindi nila nalalaman.

[Hinihimok ang mga issuer](https://www.w3.org/TR/vc-data-model/#dfn-issuers) na huwag gumamit ng mga mekanismo, gaya ng mga listahan ng pagbawi ng [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) na natatangi bawat [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) , sa panahon ng proseso ng pag- [verify](https://www.w3.org/TR/vc-data-model/#dfn-verify) na maaaring humantong sa mga paglabag sa privacy. Ang mga organisasyong nagbibigay ng software sa mga may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) ay dapat na magbabala kapag may kasamang impormasyon ang mga [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) na maaaring humantong sa mga paglabag sa privacy sa panahon ng proseso ng pag-verify. [Dapat isaalang-alang ng mga verifier](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifier) ang pagtanggi sa mga [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) na nagdudulot ng mga paglabag sa privacy o nagbibigay-daan sa masasamang kasanayan sa privacy.

### **7.11Mga Tagabigay ng Imbakan at Pagmimina ng Data**

Ang seksyong ito ay hindi normatibo.

Kapag nakatanggap ang isang may [hawak ng isang](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders)[nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) mula sa isang nag- [isyu](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) , ang na- verify na [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-credentials) ay kailangang itago sa isang lugar (halimbawa, sa isang imbakan ng [kredensyal ).](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential)[Binabalaan ang mga may hawak](https://www.w3.org/TR/vc-data-model/#dfn-holders) na ang impormasyon sa isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ay sensitibo sa likas na katangian at napaka-indibidwal, na ginagawa itong isang mataas na halaga na target para sa pagmimina ng data. Ang mga serbisyong nag-a-advertise ng libreng storage ng mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ay maaaring sa katunayan ay nagmimina ng personal na data at nagbebenta nito sa mga organisasyong gustong bumuo ng mga indibidwal na profile sa mga tao at organisasyon.

Kailangang malaman ng mga may [hawak ang mga tuntunin ng serbisyo para sa kanilang imbakan ng](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders)[kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-credential) , partikular ang ugnayan at mga proteksyon sa pagmimina ng data para sa mga nag-iimbak ng kanilang mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) sa service provider.

Kasama sa ilang epektibong pagpapagaan para sa data mining at profiling ang paggamit ng:

* Mga service provider na hindi nagbebenta ng iyong impormasyon sa mga third party.
* Software na nag-e-encrypt ng mga [nabe](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) -verify na kredensyal upang hindi matingnan ng isang service provider ang mga nilalaman ng [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) .
* Software na lokal na nag-iimbak ng [mga nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-credentials) sa isang device na kinokontrol mo at hindi nag-a-upload o nagsusuri ng iyong impormasyon nang higit sa iyong inaasahan.

### **7.12Pagsasama-sama ng mga Kredensyal**

Ang seksyong ito ay hindi normatibo.

Ang paghawak ng dalawang piraso ng impormasyon tungkol sa parehong [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) ay halos palaging nagpapakita ng higit pa tungkol sa [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) kaysa sa kabuuan ng dalawang piraso, kahit na ang impormasyon ay inihatid sa pamamagitan ng magkaibang mga channel. Ang pagsasama-sama ng mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ay isang panganib sa privacy at ang lahat ng kalahok sa ecosystem ay kailangang magkaroon ng kamalayan sa mga panganib ng pagsasama-sama ng data.

Halimbawa, kung ang dalawang [kredensyal ng maydala](https://www.w3.org/TR/vc-data-model/" \l "dfn-bearer-credentials) , isa para sa isang email address at pagkatapos ay isa na nagsasaad na ang may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) ay lampas sa edad na 21, ay ibinigay sa maraming session, ang [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) ng impormasyon ay mayroon na ngayong natatanging identifier pati na rin ang impormasyong nauugnay sa edad para sa ang indibidwal na iyon. Madali na ngayong lumikha at bumuo ng isang profile para sa may- [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) na parami nang paraming impormasyon ang na-leak sa paglipas ng panahon. Ang pagsasama-sama ng mga [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) ay maaari ding isagawa sa maraming site sa pagsasabwatan sa isa't isa, na humahantong sa mga paglabag sa privacy.

Mula sa isang teknolohikal na pananaw, ang pagpigil sa pagsasama-sama ng impormasyon ay isang napakahirap na problema sa privacy na tugunan. Habang ang mga bagong cryptographic technique, gaya ng zero-knowledge proofs, ay iminumungkahi bilang mga solusyon sa problema ng aggregation at correlation, ang pagkakaroon ng mga pangmatagalang identifier at browser tracking techniques ay tinatalo kahit ang pinakamodernong cryptographic techniques.

Ang solusyon sa mga implikasyon sa privacy ng ugnayan o pagsasama-sama ay malamang na hindi teknolohikal sa kalikasan, ngunit sa halip ay hinihimok ng patakaran. Samakatuwid, kung ayaw ng isang may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) na pagsama-samahin ang impormasyon tungkol sa kanila, dapat nilang ipahayag ito sa mga [nabe-verify na presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) na kanilang ipinadala.

### **7.13Mga Pattern ng Paggamit**

Ang seksyong ito ay hindi normatibo.

Sa kabila ng pinakamahusay na pagsisikap na tiyakin ang privacy, ang aktwal na paggamit ng mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ay maaaring potensyal na humantong sa de-anonymization at pagkawala ng privacy. Maaaring mangyari ang ugnayang ito kapag:

* Ang parehong [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ay ipinakita sa parehong [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) nang higit sa isang beses. Maaaring ipahiwatig ng [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) na ang may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) ay iisang indibidwal.
* Ang parehong [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ay ipinakita sa iba't ibang mga [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) , at alinman sa mga [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) na iyon ay nakikipagsabwatan o ang isang third party ay may access sa mga talaan ng transaksyon mula sa parehong mga [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) . Ang isang mapagmasid na partido ay maaaring magpahiwatig na ang indibidwal na nagpapakita ng [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ay ang parehong tao sa parehong mga serbisyo. Ibig sabihin, ang mga account ay kinokontrol ng parehong tao.
* Ang isang [subject](https://www.w3.org/TR/vc-data-model/#dfn-subjects) identifier ng isang [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) ay tumutukoy sa parehong [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) sa maraming [presentasyon](https://www.w3.org/TR/vc-data-model/" \l "dfn-presentations) o [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) . Kahit na may iba't ibang [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) na ipinakita, kung ang tagatukoy ng [paksa ay pareho, ang mga](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects)[verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) (at ang mga may access sa mga log ng [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) ) ​​ay maaaring magpahiwatig na ang may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) ng [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) ay iisang tao.
* Ang pinagbabatayan na impormasyon sa isang [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) ay maaaring gamitin upang matukoy ang isang indibidwal sa mga serbisyo. Sa kasong ito, gamit ang impormasyon mula sa iba pang mapagkukunan (kabilang ang impormasyong direktang ibinigay ng may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) ), maaaring gumamit ang mga [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) ng impormasyon sa loob ng [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) upang iugnay ang indibidwal sa isang umiiral nang profile. Halimbawa, kung ang isang may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) ay nagpapakita ng mga [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) na may kasamang postal code, edad, at kasarian, maaaring iugnay ng isang [verifier ang](https://www.w3.org/TR/vc-data-model/#dfn-verifier)[paksa](https://www.w3.org/TR/vc-data-model/#dfn-subjects) ng [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) na iyon sa isang naitatag na profile. Para sa higit pang impormasyon, tingnan ang [ [DEMOGRAPHICS](https://www.w3.org/TR/vc-data-model/#bib-demographics) ].
* Pagpasa ng identifier ng isang [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) sa isang sentralisadong server ng pagbawi. Maaaring iugnay ng sentralisadong server ang paggamit ng [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) sa mga pakikipag-ugnayan. Halimbawa, kung ang isang [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) ay ginagamit para sa patunay ng edad sa ganitong paraan, maaaring malaman ng sentralisadong serbisyo sa lahat ng dako na ipinakita ang [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) (lahat ng mga tindahan ng alak, mga bar, mga tindahan ng nasa hustong gulang, mga pagbili ng lottery, at iba pa).

Sa bahagi, posibleng pagaanin ang de-anonymization na ito at pagkawala ng privacy sa pamamagitan ng:

* Paggamit ng isang globally-natatanging identifier bilang [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) para sa anumang partikular na [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) at hindi kailanman muling gamitin ang [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) na iyon .
* Kung sinusuportahan ng [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) ang pagbawi, gamit ang isang serbisyong ipinamamahagi sa buong mundo para sa pagbawi.
* Pagdidisenyo ng mga revocation API na hindi nakadepende sa pagsusumite ng ID ng [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) . Halimbawa, gumamit ng listahan ng pagbawi sa halip na isang query.
* Pag-iwas sa pag-uugnay ng impormasyong nagbibigay ng personal na pagkakakilanlan sa anumang partikular na pangmatagalang pagkakakilanlan ng [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) .

Nauunawaan na ang mga diskarte sa pagpapagaan na ito ay hindi palaging praktikal o kahit na tugma sa kinakailangang paggamit. Minsan kinakailangan ang ugnayan.

Halimbawa, sa ilang programa sa pagsubaybay sa inireresetang gamot, kinakailangan ang pagsubaybay sa paggamit. Kailangang makumpirma ng mga entity ng pagpapatupad na hindi dinadaya ng mga indibidwal ang system para makakuha ng maraming reseta para sa mga kinokontrol na substance. Itong ayon sa batas o regulasyong pangangailangang iugnay ang paggamit ay sumasalungat sa mga indibidwal na alalahanin sa privacy.

[Gagamitin din ang mga nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) upang sadyang maiugnay ang mga indibidwal sa mga serbisyo, halimbawa, kapag gumagamit ng isang karaniwang katauhan upang mag-log in sa maraming serbisyo, kaya ang lahat ng aktibidad sa bawat isa sa mga serbisyong iyon ay sadyang naka-link sa parehong indibidwal. Hindi ito isang isyu sa privacy hangga't ginagamit ng bawat isa sa mga serbisyong iyon ang ugnayan sa inaasahang paraan.

Ang mga panganib sa privacy ng paggamit ng [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) ay nangyayari kapag ang hindi sinasadya o hindi inaasahang ugnayan ay lumitaw mula sa pagtatanghal ng mga [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) .

### **7.14Pagbabahagi ng Impormasyon sa Maling Partido**

Ang seksyong ito ay hindi normatibo.

Kapag pinili ng isang may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) na magbahagi ng impormasyon sa isang [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) , maaaring mangyari na ang [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) ay kumikilos nang hindi maganda at humiling ng impormasyon na maaaring magamit upang saktan ang may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) . Halimbawa, maaaring humingi ng bank account number ang isang [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) , na maaaring gamitin kasama ng iba pang impormasyon upang dayain ang may- [ari](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) o ang bangko.

[Dapat magsikap ang mga issuer](https://www.w3.org/TR/vc-data-model/#dfn-issuers) na i-tokenize ang pinakamaraming impormasyon hangga't maaari upang kung ang isang may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) ay hindi sinasadyang magpadala ng mga [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) sa maling [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) , ang sitwasyon ay hindi sakuna.

Halimbawa, sa halip na magsama ng bank account number para sa layunin ng pagsuri sa balanse sa bangko ng isang indibidwal, magbigay ng token na nagbibigay-daan sa [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) na suriin kung ang balanse ay mas mataas sa isang partikular na halaga. Sa kasong ito, maaaring mag-isyu ang bangko ng isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) na naglalaman ng token sa pagsuri ng balanse sa isang may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) . Pagkatapos ay isasama ng may-ari ang nabe [- verify na](https://www.w3.org/TR/vc-data-model/#dfn-holders)[kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) sa isang [nabe-verify na presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) at ibibigkis ang token sa isang ahensya sa pagsuri ng kredito gamit ang isang digital na lagda. Maaaring ibalot ng [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) ang [nabe-verify na presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations)sa kanilang digital signature, at ibalik ito sa nagbigay para dynamic na suriin ang balanse ng account.

Gamit ang diskarteng ito, kahit na ibinahagi ng isang may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) ang token ng balanse ng account sa maling partido, hindi matutuklasan ng isang attacker ang bank account number, o ang eksaktong halaga sa account. At dahil sa validity period para sa counter-signature, hindi nakakakuha ng access sa token nang higit sa ilang minuto.

### **7.15Dalas ng Pag-isyu ng Claim**

Ang seksyong ito ay hindi normatibo.

Gaya ng nakadetalye sa Seksyon[7.13Mga Pattern ng Paggamit](https://www.w3.org/TR/vc-data-model/#usage-patterns) , ang mga pattern ng paggamit ay maaaring maiugnay sa ilang uri ng pag-uugali. Ang bahagi ng ugnayang ito ay nababawasan kapag ang isang may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) ay gumagamit ng isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) nang hindi nalalaman ng [nagbigay](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) . [Maaaring talunin ng mga issuer](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) ang proteksyong ito gayunpaman, sa pamamagitan ng paggawa ng maikli at awtomatikong pag-renew ng kanilang mga [nabe-verify na kredensyal .](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials)

Halimbawa, ang isang ageOver [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ay kapaki-pakinabang para sa pagkakaroon ng access sa isang bar. Kung ang isang [issuer](https://www.w3.org/TR/vc-data-model/#dfn-issuers) ay nag- isyu ng tulad ng isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) na may napakaikling petsa ng pag-expire at isang mekanismo ng awtomatikong pag-renew, kung gayon ang [issuer](https://www.w3.org/TR/vc-data-model/#dfn-issuers) ay posibleng iugnay ang pag-uugali ng may- [ari](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) sa paraang negatibong nakakaapekto sa may- [ari](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) .

Dapat silang bigyan ng babala ng mga organisasyong nagbibigay ng software sa mga may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) kung paulit-ulit silang gumagamit [ng mga kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-credential) na may maikling habang-buhay, na maaaring magresulta sa ugnayan ng pag-uugali. Dapat iwasan ng mga nag-isyu ang pagbibigay [ng mga](https://www.w3.org/TR/vc-data-model/#dfn-issuers)[kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-credential) sa paraang nagbibigay-daan sa kanila na maiugnay ang mga pattern ng paggamit.

### **7.16Mas gusto ang Mga Kredensyal na Pang-isahang Gamit**

Ang seksyong ito ay hindi normatibo.

Ang isang perpektong sistemang may kinalaman sa privacy ay mangangailangan lamang ng impormasyong kinakailangan para sa pakikipag-ugnayan sa [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) na ibunyag ng may- [ari](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) . Pagkatapos, ire - record ng [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) na natugunan ang kinakailangan sa pagsisiwalat at makakalimutan ang anumang sensitibong impormasyong ibinunyag. Sa maraming kaso, ang mga nakikipagkumpitensyang priyoridad, tulad ng pasanin sa regulasyon, ay pumipigil sa perpektong sistemang ito na gamitin. Sa ibang mga kaso, pinipigilan ng mga pangmatagalang identifier ang solong paggamit. Ang disenyo ng anumang [nabe](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) -verify na ecosystem ng mga kredensyal, gayunpaman, ay dapat magsumikap na maging kasing-pribado hangga't maaari sa pamamagitan ng pagpipili sa mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) sa isahang gamit hangga't maaari.

Ang paggamit ng single-use na [nabe-verify na mga kredensyal ay](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) nagbibigay ng ilang mga benepisyo. Ang unang benepisyo ay sa mga [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) na makatitiyak na sariwa ang data sa isang [nabe-verify na kredensyal .](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials)Ang pangalawang benepisyo ay para sa mga may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) , na nakakaalam na kung walang pangmatagalang pagkakakilanlan sa [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) , ang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) mismo ay hindi magagamit upang subaybayan o iugnay ang mga ito online. Sa wakas, walang dapat magnakaw ang mga umaatake, na ginagawang mas ligtas na gumana sa loob ang buong ecosystem.

### **7.17Pribadong Pagba-browse**

Ang seksyong ito ay hindi normatibo.

Sa isang mainam na senaryo ng pribadong pagba-browse, walang PII na ipapakita. Dahil maraming [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) ang may kasamang PII, dapat silang bigyan ng babala ng mga organisasyong nagbibigay ng software sa mga may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) tungkol sa posibilidad na ibunyag ang impormasyong ito kung gusto nilang gumamit ng mga [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) at [presentasyon](https://www.w3.org/TR/vc-data-model/" \l "dfn-presentations) habang nasa private browsing mode. Dahil iba ang pinangangasiwaan ng bawat vendor ng browser sa pribadong pagba-browse, at maaaring walang ganitong feature ang ilang browser, mahalagang malaman ng mga tagapagpatupad ang mga pagkakaibang ito at magpatupad ng mga solusyon nang naaayon.

### **7.18Mga Epekto sa Pakikipagtulungan ng Nag-isyu sa Pagkapribado**

Ang seksyong ito ay hindi normatibo.

Hindi masasabi na ang mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ay umaasa sa mataas na antas ng tiwala sa mga [nagbigay](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) . Ang antas kung saan maaaring samantalahin ng isang may [hawak ang mga posibleng proteksyon sa privacy ay kadalasang nakadepende nang husto sa suportang ibinibigay ng isang](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders)[issuer](https://www.w3.org/TR/vc-data-model/#dfn-issuers) para sa mga naturang feature. Sa maraming kaso, ang mga proteksyon sa privacy na gumagamit ng mga zero-knowledge proofs, mga diskarte sa pag-minimize ng data, mga kredensyal ng maydala, abstract claim, at mga proteksyon laban sa signature-based correlation, ay nangangailangan ng [issuer](https://www.w3.org/TR/vc-data-model/#dfn-issuers) na aktibong suportahan ang mga ganoong kakayahan at isama ang mga ito sa mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) na kanilang ibibigay. .

Dapat ding tandaan na, bilang karagdagan sa isang pag-asa sa paglahok ng [issuer upang magbigay ng](https://www.w3.org/TR/vc-data-model/#dfn-issuers)[mga nabe](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) -verify na kakayahan ng kredensyal na makakatulong na mapanatili ang privacy ng may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) at [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) , umaasa ang mga may hawak sa [mga](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders)[issuer](https://www.w3.org/TR/vc-data-model/#dfn-issuers) upang hindi sadyang ibagsak ang mga proteksyon sa privacy. Halimbawa, maaaring lagdaan ng isang [issuer ang](https://www.w3.org/TR/vc-data-model/#dfn-issuers)[mga nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) gamit ang isang signature scheme na nagpoprotekta laban sa signature-based na ugnayan. Mapoprotektahan nito ang may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) mula sa pagkakaugnay ng halaga ng lagda dahil ito ay ibinabahagi sa mga [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) . Gayunpaman, kung ang [nagbigay](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) ay lumikha ng isang natatanging susi para sa bawat ibinigay[kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-credential) , posibleng masubaybayan ng [nagbigay ang mga](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers)[presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-presentations) ng [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) , anuman ang kawalan ng kakayahan ng isang [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) na gawin ito.

## 8.Mga Pagsasaalang-alang sa Seguridad

Ang seksyong ito ay hindi normatibo.

Mayroong ilang mga pagsasaalang-alang sa seguridad na dapat malaman ng mga [issuer](https://www.w3.org/TR/vc-data-model/#dfn-issuers) , [holders](https://www.w3.org/TR/vc-data-model/#dfn-holders) , at [verifiers](https://www.w3.org/TR/vc-data-model/#dfn-verifier) kapag nagpoproseso ng data na inilarawan ng detalyeng ito. Ang pagbalewala o hindi pag-unawa sa mga implikasyon ng seksyong ito ay maaaring magresulta sa mga kahinaan sa seguridad.

Habang sinusubukan ng seksyong ito na i-highlight ang isang malawak na hanay ng mga pagsasaalang-alang sa seguridad, hindi ito kumpletong listahan. Hinihimok ang mga tagapagpatupad na humingi ng payo sa mga propesyonal sa seguridad at cryptography kapag nagpapatupad ng mga mission critical system gamit ang teknolohiyang nakabalangkas sa detalyeng ito.

### **8.1Mga Suite at Aklatan ng Cryptography**

Ang seksyong ito ay hindi normatibo.

Ang ilang aspeto ng modelo ng data na inilarawan sa detalyeng ito ay maaaring maprotektahan sa pamamagitan ng paggamit ng cryptography. Mahalaga para sa mga nagpapatupad na maunawaan ang mga cryptography suite at mga aklatan na ginagamit upang lumikha at magproseso ng mga [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) at [presentasyon](https://www.w3.org/TR/vc-data-model/" \l "dfn-presentations) . Ang pagpapatupad at pag-audit ng mga cryptography system ay karaniwang nangangailangan ng malaking karanasan. Makakatulong din ang epektibong [red teaming](https://en.wikipedia.org/wiki/Red_team) na alisin ang bias sa mga pagsusuri sa seguridad.

Ang mga cryptography suite at library ay may shelf life at kalaunan ay nahuhulog sa mga bagong pag-atake at pag-unlad ng teknolohiya. Kailangang isaalang-alang ito ng mga sistema ng kalidad ng produksyon at tiyaking umiiral ang mga mekanismo upang madali at aktibong i-upgrade ang mga nag-expire o sirang cryptography suite at library, at para mapawalang-bisa at mapalitan ang mga kasalukuyang [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) . Ang regular na pagsubaybay ay mahalaga upang matiyak ang pangmatagalang posibilidad ng mga sistema sa pagpoproseso ng mga [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) .

### **8.2Proteksyon sa Integridad ng Nilalaman**

Ang seksyong ito ay hindi normatibo.

[Ang mga nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ay kadalasang naglalaman ng mga URL sa data na nasa labas ng [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) mismo. Ang naka-link na content na umiiral sa labas ng isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) , tulad ng mga larawan, JSON-LD Contexts, at iba pang data na nababasa ng machine, ay kadalasang hindi pinoprotektahan laban sa pakikialam dahil ang data ay nasa labas ng proteksyon ng [patunay](https://www.w3.org/TR/vc-data-model/" \l "proofs-signatures) sa [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) . Halimbawa, ang mga sumusunod na naka-highlight na link ay hindi protektado ng integridad ng nilalaman ngunit malamang na dapat ay:

[HALIMBAWA34](https://www.w3.org/TR/vc-data-model/#example-non-content-integrity-protected-links): Mga link na hindi protektado ng integridad ng nilalaman

{

"@context": [

**"https://www.w3.org/2018/credentials/v1"** ,

**"https://www.w3.org/2018/credentials/examples/v1"**

],

"id": "http://example.edu/credentials/58473",

"type": ["VerifiableCredential", "AlumniCredential"],

"credentialSubject": {

"id": "did:example:ebfeb1f712ebc6f1c276e12ec21",

"image": **"https://example.edu/images/58473"** ,

"alumniOf": {

"id": "did:example:c276e12ec21ebfeb1f712ebc6f1",

"pangalan": [{

"value": "Halimbawang Unibersidad",

"lang": "en"

}, {

"value": "Exemple d'Université",

"lang": "fr"

}]

}

},

"patunay": { **...** }

}

Bagama't hindi nagrerekomenda ang detalyeng ito ng anumang partikular na proteksyon sa integridad ng nilalaman, pinapayuhan ang mga may-akda ng dokumento na gustong matiyak na protektado ng integridad ang mga link sa nilalaman na gumamit ng mga scheme ng URL na nagpapatupad ng integridad ng nilalaman. Dalawang ganoong scheme ay ang [ [HASHLINK](https://www.w3.org/TR/vc-data-model/#bib-hashlink) ] na detalye at ang [ [IPFS](https://www.w3.org/TR/vc-data-model/#bib-ipfs) ]. Binabago ng halimbawa sa ibaba ang nakaraang halimbawa at nagdaragdag ng proteksyon sa integridad ng nilalaman sa JSON-LD Contexts gamit ang detalye ng [ [HASHLINK](https://www.w3.org/TR/vc-data-model/#bib-hashlink) ], at proteksyon sa integridad ng nilalaman sa larawan sa pamamagitan ng paggamit ng link na [ [IPFS](https://www.w3.org/TR/vc-data-model/#bib-ipfs) ].

[HALIMBAWA35](https://www.w3.org/TR/vc-data-model/#example-content-integrity-protection-for-links-to-external-data): Proteksyon sa integridad ng nilalaman para sa mga link sa panlabas na data

{

"@context": [

"https://www.w3.org/2018/credentials/v1 **?hl=z3aq31uzgnZBuWNzUB** ",

"https://www.w3.org/2018/credentials/examples/v1 **?hl=z8guWNzUBnZBu3aq31** "

],

"id": "http://example.edu/credentials/58473",

"type": ["VerifiableCredential", "AlumniCredential"],

"credentialSubject": {

"id": "did:example:ebfeb1f712ebc6f1c276e12ec21",

"image": **"ipfs:/ipfs/QmXfrS3pHerg44zzK6QKQj6JDk8H6cMtQS7pdXbohwNQfK/image"** ,

"alumniOf": {

"id": "did:example:c276e12ec21ebfeb1f712ebc6f1",

"pangalan": [{

"value": "Halimbawang Unibersidad",

"lang": "en"

}, {

"value": "Exemple d'Université",

"lang": "fr"

}]

}

},

"patunay": { **...** }

}

TANDAAN

Pinagtatalunan kung ang JSON-LD Contexts sa itaas ay nangangailangan ng proteksyon dahil ang mga pagpapatupad ng produksyon ay inaasahang magpapadala ng mga static na kopya ng mahahalagang JSON-LD Contexts.

Bagama't ang halimbawa sa itaas ay isang paraan upang makamit ang proteksyon sa integridad ng nilalaman, may iba pang mga solusyon na maaaring mas angkop para sa ilang partikular na application. Hinihimok ang mga nagpapatupad na maunawaan kung paano maaaring magresulta ang mga link sa external na content na nababasa ng makina na hindi pinoprotektahan ang integridad ng nilalaman sa matagumpay na pag-atake laban sa kanilang mga application.

### **8.3Mga Hindi Nilagdaan na Claim**

Ang seksyong ito ay hindi normatibo.

Ang pagtutukoy na ito ay nagbibigay-daan sa paggawa ng mga [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) na hindi naglalaman ng mga lagda o patunay ng anumang uri. Ang mga uri ng [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) na ito ay kadalasang kapaki-pakinabang para sa intermediate storage, o self-asserted na impormasyon, na kahalintulad sa pagsagot sa isang form sa isang web page. Dapat malaman ng mga tagapagpatupad na ang mga uri ng [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) na ito ay hindi [mabe](https://www.w3.org/TR/vc-data-model/" \l "dfn-verify) -verify dahil ang pagiging may-akda ay hindi kilala o hindi mapagkakatiwalaan.

### **8.4Pagbubuklod ng Token**

Ang seksyong ito ay hindi normatibo.

Maaaring kailanganin ng isang [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) na tiyakin na ito ang nilalayong tatanggap ng isang [nabe-verify na presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) at hindi ang target ng isang [man-in-the-middle na pag-atake](https://en.wikipedia.org/wiki/Man-in-the-middle_attack) . Ang mga diskarte tulad ng token binding [ [RFC8471](https://www.w3.org/TR/vc-data-model/#bib-rfc8471) ], na nag-uugnay sa kahilingan para sa isang [nabe-verify na presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) sa tugon, ay maaaring ma-secure ang protocol. Ang anumang hindi secure na protocol ay madaling kapitan ng man-in-the-middle attacks.

### **8.5Bundling Dependent Claim**

Ang seksyong ito ay hindi normatibo.

Itinuturing na pinakamahusay na kasanayan para sa mga [issuer](https://www.w3.org/TR/vc-data-model/#dfn-issuers) na i-atomize ang impormasyon sa isang [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) , o gumamit ng signature scheme na nagbibigay-daan para sa selective disclosure. Sa kaso ng atomization, kung hindi ito gagawin nang secure ng nag- [isyu](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) , maaaring magsama-sama ang may [hawak ng iba't ibang](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders)[kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-credential) sa paraang hindi nilayon ng [nagbigay](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) .

Halimbawa, maaaring mag-isyu ang isang unibersidad ng dalawang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) sa isang tao, bawat isa ay naglalaman ng dalawang [pag-aari](https://www.w3.org/TR/vc-data-model/" \l "dfn-property) , na dapat pagsama-samahin upang italaga ang "gampanan" ng taong iyon sa isang partikular na "kagawaran", gaya ng "Miyembro ng Staff" sa " Department of Computing", o "Post Graduate Student" sa "Department of Economics". Kung ang mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) na ito ay atomized upang ilagay lamang ang isa sa mga [katangiang](https://www.w3.org/TR/vc-data-model/" \l "dfn-property) ito sa bawat [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) , ang unibersidad ay maglalabas ng apat na [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) sa tao, bawat isa ay naglalaman ng isa sa mga sumusunod na pagtatalaga: "Staff Member", "Post Graduate Student", "Department of Pag-compute", at " [maaaring ilipat ang nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-credentials) ng "Staff Member" at "Department of Economics" sa isang [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) , na magkakasamang bubuo ng maling [claim](https://www.w3.org/TR/vc-data-model/#dfn-claims) .

### **8.6Highly Dynamic na Impormasyon**

Ang seksyong ito ay hindi normatibo.

Kapag naibigay ang mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) para sa napaka-dynamic na impormasyon, dapat tiyakin ng mga tagapagpatupad na ang mga oras ng pag-expire ay naitakda nang naaangkop. Ang mga panahon ng pag-expire na mas mahaba kaysa sa timeframe kung saan valid ang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ay maaaring lumikha ng mga mapagsamantalang kahinaan sa seguridad. Ang mga panahon ng pag-expire na mas maikli kaysa sa timeframe kung saan ang impormasyong ipinahayag ng [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ay wasto ay lumilikha ng isang pasanin sa mga may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) at [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) . Samakatuwid, mahalagang magtakda ng mga panahon ng validity para sa mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) na naaangkop sa kaso ng paggamit at ang inaasahang panghabambuhay para sa impormasyong nakapaloob sa [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) .

### **8.7Pagnanakaw at Pagpapanggap ng Device**

Ang seksyong ito ay hindi normatibo.

Kapag naka-store ang mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) sa isang device at nawala o nanakaw ang device na iyon, posibleng magkaroon ng access ang isang attacker sa mga system gamit ang mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ng biktima . Kasama sa mga paraan upang mabawasan ang ganitong uri ng pag-atake:

* Pinapagana ang proteksyon ng password, pin, pattern, o biometric na pag-unlock ng screen sa device.
* Pag-enable ng password, biometric, o multi-factor na pagpapatotoo para sa [credential](https://www.w3.org/TR/vc-data-model/#dfn-credential)[repository](https://www.w3.org/TR/vc-data-model/#dfn-credential-repository) .
* Pinapagana ang password, biometric, o multi-factor na pagpapatotoo kapag nag-a-access ng mga cryptographic key.
* Paggamit ng hiwalay na hardware-based na signature device.
* Lahat o anumang kumbinasyon ng nasa itaas.

## 9.Mga Pagsasaalang-alang sa Accessibility

Ang seksyong ito ay hindi normatibo.

Mayroong ilang mga pagsasaalang-alang sa pagiging naa-access na dapat malaman ng mga nagpapatupad kapag nagpoproseso ng data na inilarawan sa detalyeng ito. Tulad ng pagpapatupad ng anumang pamantayan sa web o protocol, ang pagbalewala sa mga isyu sa pagiging naa-access ay ginagawang hindi magagamit ng malaking subset ng populasyon ang impormasyong ito. Mahalagang sundin ang mga alituntunin at pamantayan ng accessibility, gaya ng [ [WCAG21](https://www.w3.org/TR/vc-data-model/#bib-wcag21) ], upang matiyak na ang lahat ng tao, anuman ang kakayahan, ay maaaring gamitin ang data na ito. Ito ay lalong mahalaga kapag nagtatatag ng mga system na gumagamit ng cryptography, na dati nang lumikha ng mga problema para sa mga pantulong na teknolohiya.

Idinidetalye ng seksyong ito ang pangkalahatang pagsasaalang-alang sa pagiging naa-access na dapat isaalang-alang kapag ginagamit ang modelong ito ng data.

### **9.1Data First Approach**

Ang seksyong ito ay hindi normatibo.

Maraming mga pisikal na [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) na ginagamit ngayon, tulad ng mga kard ng pagkakakilanlan ng pamahalaan, ay may mahinang mga katangian ng accessibility, kabilang ang, ngunit hindi limitado sa, maliit na print, pag-asa sa maliliit at mataas na resolution na mga larawan, at walang mga affordance para sa mga taong may kapansanan sa paningin.

Kapag ginagamit ang data model na ito para gumawa ng [mga nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-credentials) , iminumungkahi na gumamit ang mga taga-disenyo ng data model ng data first approach. Halimbawa, dahil sa pagpili ng paggamit ng data o isang graphical na larawan upang ilarawan ang isang [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) , dapat ipahayag ng mga taga-disenyo ang bawat elemento ng larawan, gaya ng pangalan ng isang institusyon o ang propesyonal na [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) , sa paraang nababasa ng makina sa halip na umasa sa isang interpretasyon ng manonood sa larawan upang maihatid ang impormasyong ito. Mas gusto ang paggamit ng data first approach dahil nagbibigay ito ng mga pangunahing elemento ng pagbuo ng iba't ibang interface para sa mga taong may iba't ibang kakayahan.

## 10.Mga Pagsasaalang-alang sa Internasyonalisasyon

Ang seksyong ito ay hindi normatibo.

Pinapayuhan ang mga tagapagpatupad na magkaroon ng kamalayan sa ilang pagsasaalang-alang sa internationalization kapag nag-publish ng data na inilarawan sa detalyeng ito. Tulad ng anumang mga pamantayan sa web o pagpapatupad ng mga protocol, ang pagwawalang-bahala sa internationalization ay nagpapahirap para sa data na gawin at gamitin sa magkakaibang hanay ng mga wika at lipunan, na naglilimita sa applicability ng detalye at makabuluhang binabawasan ang halaga nito bilang isang pamantayan.

Lubos na pinapayuhan ang mga tagapagpatupad na basahin ang mga Strings sa Web: Language and Direction Metadata na dokumento [ [STRING-META](https://www.w3.org/TR/vc-data-model/#bib-string-meta) ], na inilathala ng W3C Internationalization Activity, na nagpapaliwanag sa pangangailangang magbigay ng maaasahang metadata tungkol sa teksto upang suportahan ang internasyonalisasyon. Para sa pinakabagong impormasyon sa mga pagsasaalang-alang sa internasyonalisasyon, hinihimok din ang mga tagapagpatupad na basahin ang dokumentong Mga Alituntunin sa Pagpapatupad ng Mga Napapatunayang Kredensyal [ [VC-IMP-GUIDE](https://www.w3.org/TR/vc-data-model/#bib-vc-imp-guide) ].

Binabalangkas ng seksyong ito ang mga pangkalahatang pagsasaalang-alang sa internasyonalisasyon na dapat isaalang-alang kapag ginagamit ang modelong ito ng data at nilayon na i-highlight ang mga partikular na bahagi ng Strings sa Web: dokumento ng Metadata ng Wika at Direksyon [ [STRING-META](https://www.w3.org/TR/vc-data-model/#bib-string-meta) ] na maaaring interesadong basahin ng mga nagpapatupad.

### **10.1Wika at Batayang Direksyon**

Ang seksyong ito ay hindi normatibo.

Lubos na hinihikayat ang mga publisher ng data na basahin ang seksyon sa Cross-Syntax Expression sa Strings sa Web: Language and Direction Metadata document [ [STRING-META](https://www.w3.org/TR/vc-data-model/#bib-string-meta) ] upang matiyak na ang pagpapahayag ng wika at base na impormasyon ng direksyon ay posible sa maraming expression syntax, tulad ng bilang [ [JSON-LD](https://www.w3.org/TR/vc-data-model/#bib-json-ld) ], [ [JSON](https://www.w3.org/TR/vc-data-model/#bib-json) ], at CBOR [ [RFC7049](https://www.w3.org/TR/vc-data-model/#bib-rfc7049) ].

Ang pangkalahatang pattern ng disenyo ay ang paggamit ng sumusunod na template ng markup kapag nagpapahayag ng isang text string na naka-tag ng isang wika at, opsyonal, isang partikular na baseng direksyon.

[HALIMBAWA36](https://www.w3.org/TR/vc-data-model/#example-design-pattern-for-natural-language-strings): Pattern ng disenyo para sa mga natural na string ng wika

" ari- [arian](https://www.w3.org/TR/vc-data-model/#dfn-property) ": {

"value": " **Ang halaga ng string** ",

"lang": " LANGUAGE"

"dir": " DIRECTION"

}

Gamit ang pattern ng disenyo sa itaas, ang sumusunod na halimbawa ay nagpapahayag ng pamagat ng isang libro sa wikang Ingles nang hindi tinukoy ang direksyon ng teksto.

[HALIMBAWA37](https://www.w3.org/TR/vc-data-model/#example-expressing-natural-language-text-as-english): Pagpapahayag ng natural na teksto ng wika bilang Ingles

"pamagat": {

"value": " **HTML at CSS: Pagdidisenyo at Paglikha ng mga Website** ",

"lang": " en"

}

Ang susunod na halimbawa ay gumagamit ng katulad na pamagat na ipinahayag sa wikang Arabic na may baseng direksyon ng kanan-papuntang-kaliwa.

[HALIMBAWA38](https://www.w3.org/TR/vc-data-model/#example-arabic-text-with-a-base-direction-of-right-to-left): Arabic na teksto na may baseng direksyon ng kanan-papuntang-kaliwa

"pamagat": {

"value": " **HTML at CSS: تصميم و إنشاء مواقع الويب** ",

"lang": " ar"

"dir": " rtl"

}

TANDAAN

Ang teksto sa itaas ay malamang na ma-render nang mali bilang kaliwa-pakanan nang walang tahasang pagpapahayag ng wika at direksyon dahil maraming mga system ang gumagamit ng unang character ng isang string ng teksto upang matukoy ang direksyon ng teksto.

Ang mga nagpapatupad na gumagamit ng JSON-LD ay mahigpit na hinihimok na [palawigin](https://www.w3.org/TR/vc-data-model/" \l "extensibility) ang JSON-LD Context na tumutukoy sa internationalized na [property](https://www.w3.org/TR/vc-data-model/#dfn-property) at gamitin ang Scoped Context feature ng JSON-LD para i-alias ang @value, @language, at mga @directionkeyword sa value, lang, at dir, ayon sa pagkakabanggit. Ang isang halimbawa ng JSON-LD Context snippet na gumagawa nito ay ipinapakita sa ibaba.

[HALIMBAWA39](https://www.w3.org/TR/vc-data-model/#example-specifying-scoped-aliasing-for-language-information): Pagtukoy sa saklaw na aliasing para sa impormasyon ng wika

"title": {

**"@context": {"value": "@value", "lang": "@language", "dir": "@direction"}** ,

"@id": "https://www.w3.org/2018/credentials/examples#title"

}

### **10.2Masalimuot na Markup ng Wika**

Ang seksyong ito ay hindi normatibo.

Kapag maraming wika, base na direksyon, at anotasyon ang ginagamit sa isang natural na string ng wika, karaniwang kinakailangan ang mga mas kumplikadong mekanismo. Posibleng gumamit ng mga markup language, gaya ng HTML, upang mag-encode ng text na may maraming wika at base na direksyon. Posible ring gamitin ang rdf:HTMLdatatype para i-encode nang tumpak ang mga naturang value sa JSON-LD.

Sa kabila ng kakayahang mag-encode ng impormasyon bilang HTML, ang mga nagpapatupad ay lubos na hindi hinihikayat na gawin ito dahil ito ay:

* Nangangailangan ng ilang bersyon ng isang HTML processor, na nagpapataas ng pasanin sa pagpoproseso ng wika at impormasyon ng base na direksyon.
* Pinapataas ang pag-atake sa seguridad kapag ginagamit ang modelong ito ng data dahil ang bulag na pagpoproseso ng HTML ay maaaring magresulta sa pagsasagawa ng scripttag na na-inject ng isang attacker sa isang punto sa panahon ng proseso ng paggawa ng data.

Kung nararamdaman ng mga nagpapatupad na dapat silang gumamit ng HTML, o iba pang mga markup na wika na may kakayahang maglaman ng mga executable na script, upang tugunan ang isang partikular na kaso ng paggamit, pinapayuhan silang suriin kung paano gagamitin ng isang attacker ang markup upang i-mount ang mga pag-atake ng injection laban sa isang consumer ng markup at pagkatapos ay i-deploy pagpapagaan laban sa mga natukoy na pag-atake.

## A.Pagpapatunay

Ang seksyong ito ay hindi normatibo.

Bagama't ang detalyeng ito ay hindi nagbibigay ng pamantayan sa pagsang-ayon para sa proseso ng [pagpapatunay](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential-validation) ng mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) o na-verify na mga [presentasyon](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-presentations) , ang mga mambabasa ay maaaring malaman kung paano ang impormasyon sa modelong ito ng data ay inaasahang gagamitin ng mga [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) sa panahon ng proseso ng [pagpapatunay](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential-validation) . Kinukuha ng seksyong ito ang isang seleksyon ng mga pag-uusap na hawak ng Working Group na may kaugnayan sa inaasahang paggamit ng mga field ng data sa detalyeng ito ng mga [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) .

### **A.1Paksa ng kredensyal**

Ang seksyong ito ay hindi normatibo.

Sa mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) na ipinakita ng isang may- [ari](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) , ang halagang nauugnay sa ari- id [arian](https://www.w3.org/TR/vc-data-model/" \l "dfn-property) para sa bawat credentialSubjectisa ay inaasahang matukoy ang isang [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) sa [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) . Kung ang may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) din ang [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) , maaaring patotohanan ng [verifier ang may](https://www.w3.org/TR/vc-data-model/#dfn-verifier)[hawak](https://www.w3.org/TR/vc-data-model/#dfn-holders) kung mayroon silang pampublikong key metadata na nauugnay sa may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) . Pagkatapos ay maaaring patotohanan ng [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) ang may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) gamit ang isang lagda na nabuo ng may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) na nakapaloob sa [nabe-verify na presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) . Ang ari- id [arian](https://www.w3.org/TR/vc-data-model/" \l "dfn-property)ay opsyonal. [Maaaring gumamit ang mga verifier](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifier) ng iba pang mga [katangian](https://www.w3.org/TR/vc-data-model/" \l "dfn-property) sa isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) upang natatanging tukuyin ang isang [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) .

TANDAAN

Para sa impormasyon sa kung paano maaaring gumana ang pagpapatotoo at WebAuthn sa mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) , tingnan ang dokumentong Mga Alituntunin sa Pagpapatupad ng Mga Na-verify na Kredensyal [ [VC-IMP-GUIDE](https://www.w3.org/TR/vc-data-model/#bib-vc-imp-guide) ].

### **A.2Tagapagbigay**

Ang seksyong ito ay hindi normatibo.

Ang halagang nauugnay sa ari- issuer [arian](https://www.w3.org/TR/vc-data-model/" \l "dfn-property) ay inaasahang matukoy ang isang [tagabigay](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) na kilala at pinagkakatiwalaan ng [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) .

Ang nauugnay na metadata tungkol sa issuer [property](https://www.w3.org/TR/vc-data-model/#dfn-property) ay inaasahang magiging available sa [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) . Halimbawa, maaaring mag-publish ang isang [issuer](https://www.w3.org/TR/vc-data-model/#dfn-issuers) ng impormasyong naglalaman ng mga pampublikong key na ginagamit nito upang digital na lagdaan ang mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) na ibinigay nito. May kaugnayan ang metadata na ito kapag sinusuri ang mga patunay sa mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) .

### **A.3Petsa ng pagpapalabas**

Ang seksyong ito ay hindi normatibo.

Ang issuanceDateay inaasahang nasa loob ng isang inaasahang hanay para sa [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) . Halimbawa, maaaring suriin ng isang [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) na ang petsa ng pag-isyu ng isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ay wala sa hinaharap.

### **A.4Mga Katibayan (Mga Lagda)**

Ang seksyong ito ay hindi normatibo.

Ang mekanismo ng cryptographic na ginamit upang patunayan na ang impormasyon sa isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) o na-verify na [pagtatanghal](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-presentations) ay hindi pinakialaman ay tinatawag na isang patunay . Maraming uri ng cryptographic na patunay kabilang ang, ngunit hindi limitado sa, mga digital na lagda, zero-knowledge proofs, Proofs of Work, at Proofs of Stake. Sa pangkalahatan, kapag nagbe-verify ng mga patunay, ang mga pagpapatupad ay inaasahang matiyak na:

* Available ang patunay sa anyo ng isang kilalang suite ng patunay.
* Ang lahat ng kinakailangang proof suite [property](https://www.w3.org/TR/vc-data-model/#dfn-property) ay naroroon.
* [Ang algorithm sa pag- verify](https://www.w3.org/TR/vc-data-model/#dfn-verify) ng suite ng patunay , kapag inilapat sa data, ay nagreresulta sa isang katanggap-tanggap na patunay.

Ang ilang mga patunay ay mga digital na lagda. Sa pangkalahatan, kapag nagbe-verify ng mga digital na lagda, ang mga pagpapatupad ay inaasahang matiyak na:

* Ang tinatanggap na kamakailang metadata tungkol sa pampublikong susi na nauugnay sa lagda ay magagamit. Halimbawa, maaaring kabilang sa metadata ang mga [property](https://www.w3.org/TR/vc-data-model/#dfn-property) na nauugnay sa expiration, may-ari ng key, o pangunahing layunin.
* Ang susi ay hindi sinuspinde, binawi, o nag-expire.
* Inaasahang mabe-verify ang cryptographic signature.
* Kung inaasahan ng cryptographic suite ang isang proofPurpose [property](https://www.w3.org/TR/vc-data-model/#dfn-property) , inaasahang umiiral ito at magiging valid na value, gaya ng assertionMethod.

TANDAAN

Ang digital signature ay nagbibigay ng ilang mga proteksyon, maliban sa tamper resistance, na hindi kaagad halata. Halimbawa, ang isang Linked Data Signature created [property](https://www.w3.org/TR/vc-data-model/#dfn-property) ay nagtatatag ng petsa at oras bago ang [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) ay hindi dapat ituring na na- [verify](https://www.w3.org/TR/vc-data-model/#dfn-verify) . verificationMethod [Tinukoy ng property](https://www.w3.org/TR/vc-data-model/" \l "dfn-property) , halimbawa, ang pampublikong key na magagamit para i-verify ang digital signature . Ang pag-derefer sa isang pampublikong URL ng key ay nagpapakita ng impormasyon tungkol sa controller ng key, na maaaring suriin laban sa nagbigay ng [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) . Malinaw na ipinapahayag ng ari - proofPurpose [arian ang layunin para sa patunay at tinitiyak na ang impormasyong ito ay protektado ng lagda.](https://www.w3.org/TR/vc-data-model/" \l "dfn-property)Ang isang patunay ay karaniwang nakakabit sa a[nabe-verify na presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) para sa mga layunin ng pagpapatunay at sa isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) bilang isang paraan ng paggigiit.

### **A.5Expiration**

Ang seksyong ito ay hindi normatibo.

Ang expirationDateay inaasahang nasa loob ng isang inaasahang hanay para sa [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) . Halimbawa, maaaring suriin ng isang [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) na ang petsa ng pag-expire ng isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ay wala sa nakaraan.

### **A.6Katayuan**

Ang seksyong ito ay hindi normatibo.

Kung credentialStatusavailable ang property, inaasahang susuriin ng [verifier ang status ng isang](https://www.w3.org/TR/vc-data-model/#dfn-verifier)[nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ayon sa kahulugan ng [uri para sa](https://www.w3.org/TR/vc-data-model/" \l "dfn-type)[nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) at ang sariling pamantayan sa pagsusuri ng katayuan ng [verifier .](https://www.w3.org/TR/vc-data-model/#dfn-verifier)Halimbawa, masisiguro ng isang [verifier na ang status ng](https://www.w3.org/TR/vc-data-model/#dfn-verifier)[nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ay hindi "binabawi nang may dahilan ng [nagbigay](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) ". credentialStatus

### **A.7Fitness para sa Layunin**

Ang seksyong ito ay hindi normatibo.

Ang fitness for purpose ay tungkol sa kung ang mga custom na [property](https://www.w3.org/TR/vc-data-model/#dfn-property) sa [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ay angkop para sa layunin ng [verifier .](https://www.w3.org/TR/vc-data-model/#dfn-verifier)Halimbawa, kung kailangang tukuyin ng isang [verifier kung ang isang](https://www.w3.org/TR/vc-data-model/#dfn-verifier)[paksa](https://www.w3.org/TR/vc-data-model/#dfn-subjects) ay mas matanda sa 21 taong gulang, maaari silang umasa sa isang partikular na birthdate [property](https://www.w3.org/TR/vc-data-model/#dfn-property) , o sa higit pang abstract na mga [katangian](https://www.w3.org/TR/vc-data-model/" \l "dfn-property) , gaya ng ageOver.

Ang nag- [isyu](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) ay pinagkakatiwalaan ng [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) na gawin ang mga [claim](https://www.w3.org/TR/vc-data-model/#dfn-claims) sa kamay. Halimbawa, pinagkakatiwalaan ng isang naka-franchise na lokasyon ng fast food na restaurant ang mga [claim](https://www.w3.org/TR/vc-data-model/#dfn-claims) sa discount coupon na ginawa ng corporate headquarters ng franchise. Ang impormasyon ng patakaran na ipinahayag ng nag- [isyu](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) sa [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ay dapat na igalang ng mga may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) at taga- [verify](https://www.w3.org/TR/vc-data-model/#dfn-verifier) maliban kung tinatanggap nila ang pananagutan ng pagbalewala sa patakaran.

## B.Mga Konteksto, Uri, at Mga Schema ng Kredensyal

Ang seksyong ito ay hindi normatibo.

### **B.1Batayang Konteksto**

Ang seksyong ito ay hindi normatibo.

Ang batayang konteksto, na matatagpuan sa https://www.w3.org/2018/credentials/v1may SHA-256 digest ng **ab4ddd9a531758807a79a5b450510d61ae8d147eab966cc9a200c07095b0cdcc**, ay maaaring gamitin upang ipatupad ang isang lokal na naka-cache na kopya. Para sa kaginhawahan, ang batayang konteksto ay ibinibigay din sa seksyong ito.

{

"@context": {

"@version": 1.1,

"@protected": true,

"id": "@id",

"type": "@type",

"VerifiableCredential": {

"@id": "https://www.w3.org/2018/credentials#VerifiableCredential",

"@context": {

"@version": 1.1,

"@protected": true,

"id": "@id",

"type": "@type",

"cred": "https://www.w3.org/2018/credentials#",

"sec": "https://w3id.org/security#",

"xsd": "http://www.w3.org/2001/XMLSchema#",

"credentialSchema": {

"@id": "cred:credentialSchema",

"@type": "@id",

"@context": {

"@version": 1.1,

"@protected": true,

"id": "@id",

"type": "@type",

"cred": "https://www.w3.org/2018/credentials#",

"JsonSchemaValidator2018": "cred:JsonSchemaValidator2018"

}

},

"credentialStatus": {"@id": "cred:credentialStatus", "@type": "@id"},

"credentialSubject": {"@id": "cred:credentialSubject", "@type": "@id"},

"evidence": {"@id": "cred:evidence", "@type": "@id"},

"expirationDate": {"@id": "cred:expirationDate", "@type": "xsd:dateTime"},

"holder": {"@id": "cred:holder", "@type": "@id"},

"issued": {"@id": "cred:issued", "@type": "xsd:dateTime"},

"issuer": {"@id": "cred:issuer", "@type": "@id"},

"issuanceDate": {"@id": "cred:issuanceDate", "@type": "xsd:dateTime"},

"proof": {"@id": "sec:proof", "@type": "@id", "@container": "@graph"},

"refreshService": {

"@id": "cred:refreshService",

"@type": "@id",

"@context": {

"@version": 1.1,

"@protected": true,

"id": "@id",

"type": "@type",

"cred": "https://www.w3.org/2018/credentials#",

"ManualRefreshService2018": "cred:ManualRefreshService2018"

}

},

"termsOfUse": {"@id": "cred:termsOfUse", "@type": "@id"},

"validFrom": {"@id": "cred:validFrom", "@type": "xsd:dateTime"},

"validUntil": {"@id": "cred:validUntil", "@type": "xsd:dateTime"}

}

},

"VerifiablePresentation": {

"@id": "https://www.w3.org/2018/credentials#VerifiablePresentation",

"@context": {

"@version": 1.1,

"@protected": true,

"id": "@id",

"type": "@type",

"cred": "https://www.w3.org/2018/credentials#",

"sec": "https://w3id.org/security#",

"holder": {"@id": "cred:holder", "@type": "@id"},

"proof": {"@id": "sec:proof", "@type": "@id", "@container": "@graph"},

"verifiableCredential": {"@id": "cred:verifiableCredential", "@type": "@id", "@container": "@graph"}

}

},

"EcdsaSecp256k1Signature2019": {

"@id": "https://w3id.org/security#EcdsaSecp256k1Signature2019",

"@context": {

"@version": 1.1,

"@protected": true,

"id": "@id",

"type": "@type",

"sec": "https://w3id.org/security#",

"xsd": "http://www.w3.org/2001/XMLSchema#",

"challenge": "sec:challenge",

"created": {"@id": "http://purl.org/dc/terms/created", "@type": "xsd:dateTime"},

"domain": "sec:domain",

"expires": {"@id": "sec:expiration", "@type": "xsd:dateTime"},

"jws": "sec:jws",

"nonce": "sec:nonce",

"proofPurpose": {

"@id": "sec:proofPurpose",

"@type": "@vocab",

"@context": {

"@version": 1.1,

"@protected": true,

"id": "@id",

"type": "@type",

"sec": "https://w3id.org/security#",

"assertionMethod": {"@id": "sec:assertionMethod", "@type": "@id", "@container": "@set"},

"authentication": {"@id": "sec:authenticationMethod", "@type": "@id", "@container": "@set"}

}

},

"proofValue": "sec:proofValue",

"verificationMethod": {"@id": "sec:verificationMethod", "@type": "@id"}

}

},

"EcdsaSecp256r1Signature2019": {

"@id": "https://w3id.org/security#EcdsaSecp256r1Signature2019",

"@context": {

"@version": 1.1,

"@protected": true,

"id": "@id",

"type": "@type",

"sec": "https://w3id.org/security#",

"xsd": "http://www.w3.org/2001/XMLSchema#",

"challenge": "sec:challenge",

"created": {"@id": "http://purl.org/dc/terms/created", "@type": "xsd:dateTime"},

"domain": "sec:domain",

"expires": {"@id": "sec:expiration", "@type": "xsd:dateTime"},

"jws": "sec:jws",

"nonce": "sec:nonce",

"proofPurpose": {

"@id": "sec:proofPurpose",

"@type": "@vocab",

"@context": {

"@version": 1.1,

"@protected": true,

"id": "@id",

"type": "@type",

"sec": "https://w3id.org/security#",

"assertionMethod": {"@id": "sec:assertionMethod", "@type": "@id", "@container": "@set"},

"authentication": {"@id": "sec:authenticationMethod", "@type": "@id", "@container": "@set"}

}

},

"proofValue": "sec:proofValue",

"verificationMethod": {"@id": "sec:verificationMethod", "@type": "@id"}

}

},

"Ed25519Signature2018": {

"@id": "https://w3id.org/security#Ed25519Signature2018",

"@context": {

"@version": 1.1,

"@protected": true,

"id": "@id",

"type": "@type",

"sec": "https://w3id.org/security#",

"xsd": "http://www.w3.org/2001/XMLSchema#",

"challenge": "sec:challenge",

"created": {"@id": "http://purl.org/dc/terms/created", "@type": "xsd:dateTime"},

"domain": "sec:domain",

"expires": {"@id": "sec:expiration", "@type": "xsd:dateTime"},

"jws": "sec:jws",

"nonce": "sec:nonce",

"proofPurpose": {

"@id": "sec:proofPurpose",

"@type": "@vocab",

"@context": {

"@version": 1.1,

"@protected": true,

"id": "@id",

"type": "@type",

"sec": "https://w3id.org/security#",

"assertionMethod": {"@id": "sec:assertionMethod", "@type": "@id", "@container": "@set"},

"authentication": {"@id": "sec:authenticationMethod", "@type": "@id", "@container": "@set"}

}

},

"proofValue": "sec:proofValue",

"verificationMethod": {"@id": "sec:verificationMethod", "@type": "@id"}

}

},

"RsaSignature2018": {

"@id": "https://w3id.org/security#RsaSignature2018",

"@context": {

"@version": 1.1,

"@protected": true,

"challenge": "sec:challenge",

"created": {"@id": "http://purl.org/dc/terms/created", "@type": "xsd:dateTime"},

"domain": "sec:domain",

"expires": {"@id": "sec:expiration", "@type": "xsd:dateTime"},

"jws": "sec:jws",

"nonce": "sec:nonce",

"proofPurpose": {

"@id": "sec:proofPurpose",

"@type": "@vocab",

"@context": {

"@version": 1.1,

"@protected": true,

"id": "@id",

"type": "@type",

"sec": "https://w3id.org/security#",

"assertionMethod": {"@id": "sec:assertionMethod", "@type": "@id", "@container": "@set"},

"authentication": {"@id": "sec:authenticationMethod", "@type": "@id", "@container": "@set"}

}

},

"proofValue": "sec:proofValue",

"verificationMethod": {"@id": "sec:verificationMethod", "@type": "@id"}

}

},

"proof": {"@id": "https://w3id.org/security#proof", "@type": "@id", "@container": "@graph"}

}

}

### **B.2Mga Pagkakaiba sa pagitan ng Mga Konteksto, Uri, at CredentialSchemas**

Ang seksyong ito ay hindi normatibo.

Ang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) at nabe-verify na mga modelo ng data ng [presentasyon ay gumagamit ng iba't ibang pinagbabatayan na teknolohiya kabilang ang [](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-presentations)[JSON-LD](https://www.w3.org/TR/vc-data-model/#bib-json-ld) ] at [ [JSON-SCHEMA-2018](https://www.w3.org/TR/vc-data-model/#bib-json-schema-2018) ]. Magbibigay ang seksyong ito ng paghahambing ng @context, type, at mga credentialSchema katangian, at sumasaklaw sa ilan sa mga mas partikular na kaso ng paggamit kung saan posibleng gamitin ang mga feature na ito ng modelo ng data.

Ginagamit ang typeproperty upang natatanging tukuyin ang uri ng [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) kung saan ito lumalabas, ibig sabihin, upang isaad kung aling hanay ng mga claim ang nilalaman ng [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) . Ang property na ito, at ang value VerifiableCredentialsa loob ng set ng mga value nito, ay mandatory. Bagama't magandang kasanayan na magsama ng isang karagdagang value na naglalarawan sa natatanging subtype ng [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) na ito, pinahihintulutan itong alisin o isama ang mga karagdagang value ng uri sa array. Maraming mga verifier ang hihiling ng isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ng isang partikular na subtype, pagkatapos ay ang pag-alis sa subtype na halaga ay maaaring maging mas mahirap para sa mga verifier na ipaalam sa may-ari kung aling [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ang kailangan nila. Kapag a[Ang nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ay may maraming mga subtype, ang paglista sa lahat ng mga ito sa type property ay makatuwiran. Bagama't pareho ang mga semantiko sa parehong representasyon ng [ [JSON](https://www.w3.org/TR/vc-data-model/#bib-json) ] at [ [JSON-LD](https://www.w3.org/TR/vc-data-model/#bib-json-ld) ], ang paggamit ng typeproperty sa isang representasyon ng [ [JSON-LD](https://www.w3.org/TR/vc-data-model/#bib-json-ld) ] ng isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ay mas nagagawang ipatupad ang mga semantika ng [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) kaysa sa isang [ [JSON](https://www.w3.org/TR/vc-data-model/#bib-json) ] representasyon ng parehong kredensyal dahil nasusuri ng makina ang mga semantika. Kasama si [ [JSON-LD](https://www.w3.org/TR/vc-data-model/#bib-json-ld)], ang teknolohiya ay hindi lamang naglalarawan sa pagkakategorya ng hanay ng mga paghahabol, ang teknolohiya ay naghahatid din ng istruktura at semantika ng sub-graph ng mga katangian sa graph. Sa [ [JSON-LD](https://www.w3.org/TR/vc-data-model/#bib-json-ld) ], kinakatawan nito ang uri ng node sa graph kung kaya't ang ilang [ [JSON-LD](https://www.w3.org/TR/vc-data-model/#bib-json-ld) ] na representasyon ng isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ay gagamit ng typeproperty sa maraming bagay sa na- verify na [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-credentials) .

Ang pangunahing layunin ng @contextproperty, mula sa pananaw ng [ [JSON-LD](https://www.w3.org/TR/vc-data-model/#bib-json-ld) ], ay ihatid ang kahulugan ng data at mga terminong kahulugan ng data sa isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) , sa paraang nababasa ng machine. Kapag nag-e-encode ng purong [ [JSON](https://www.w3.org/TR/vc-data-model/#bib-json) ] representasyon, @contextnananatiling mandatory ang property at nagbibigay ng ilang pangunahing suporta para sa pandaigdigang semantics. Ginagamit ang @context property para imapa ang mga pandaigdigang natatanging URI para sa mga property sa mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) at [nabe-verify na mga presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) sa mga short-form na pangalan ng alyas, na ginagawang parehong makatao ang mga representasyong [ [JSON](https://www.w3.org/TR/vc-data-model/#bib-json) ] at [ [JSON-LD ] na basahin.](https://www.w3.org/TR/vc-data-model/#bib-json-ld)Mula sa isang [ [JSON-LD](https://www.w3.org/TR/vc-data-model/#bib-json-ld)] perspective, pinapayagan din ng pagmamapa na ito ang data sa isang [kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-credential) na mamodelo sa isang network ng data na nababasa ng machine, sa pamamagitan ng pagpapahusay kung paano nauugnay ang data sa [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) o na-verify na [presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) sa isang mas malaking graph ng data na nababasa ng makina. Ito ay kapaki-pakinabang para sa pagsasabi sa mga makina kung paano iugnay ang kahulugan ng data sa iba pang data sa isang ecosystem kung saan ang mga partido ay hindi makapag-coordinate. Ang property na ito, na ang unang value sa set https://www.w3.org/2018/credentials/v1ay , ay mandatory.

Dahil ang @contextproperty ay ginagamit upang i-map ang data sa isang graph data model, at ang typeproperty sa [ [JSON-LD](https://www.w3.org/TR/vc-data-model/#bib-json-ld) ] ay ginagamit upang ilarawan ang mga node sa loob ng graph, ang typeproperty ay nagiging mas mahalaga kapag ginagamit ang dalawang property sa kumbinasyon. Halimbawa, kung ang typeproperty ay hindi kasama sa naresolbang @contextresource gamit ang [ [JSON-LD](https://www.w3.org/TR/vc-data-model/#bib-json-ld) ], maaari itong humantong sa pagtanggal ng mga claim at/o hindi na protektado ang kanilang integridad sa panahon ng paggawa at paggamit ng [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) . Bilang kahalili, maaari itong humantong sa mga error na itinaas sa panahon ng produksyon o paggamit ng isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials). Ito ay depende sa mga pagpipilian sa disenyo ng pagpapatupad at ang parehong mga path ay ginagamit sa mga pagpapatupad ngayon, kaya mahalagang bigyang-pansin ang mga katangiang ito kapag gumagamit ng isang [ [JSON-LD](https://www.w3.org/TR/vc-data-model/#bib-json-ld) ] na representasyon ng isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) o na-verify na [presentasyon](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-presentations) .

Ang pangunahing layunin ng credentialSchemaproperty ay tukuyin ang istruktura ng [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) , at ang mga datatype para sa mga value ng bawat property na lalabas. Ang A credentialSchemaay kapaki-pakinabang para sa pagtukoy sa mga nilalaman at istraktura ng isang hanay ng mga claim sa isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) , samantalang ang [ [JSON-LD](https://www.w3.org/TR/vc-data-model/#bib-json-ld) ] at a @contextsa isang na-verify na [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-credentials) ay pinakamahusay na ginagamit lamang para sa paghahatid ng mga semantika at terminong mga kahulugan ng data, at maaaring gamitin para tukuyin din ang istruktura ng [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) .

Bagama't posibleng gumamit ng ilang feature ng [ [JSON-LD](https://www.w3.org/TR/vc-data-model/#bib-json-ld) ] para tukuyin ang mga nilalaman ng [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) , hindi ito karaniwang iminumungkahi na gamitin @contextupang hadlangan ang mga uri ng data ng modelo ng data. Halimbawa, "@type": "@json"ay kapaki-pakinabang para sa pag-iwan sa mga semantika na bukas at hindi mahigpit na tinukoy. Maaari itong maging mapanganib kung ang tagapagpatupad ay naghahanap upang hadlangan ang uri ng data ng mga claim sa [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) , at inaasahang hindi gagamitin.

Kapag pinagsama-sama ang mga credentialSchemaat @contextproperty, maaaring maging mas kumpiyansa ang mga producer at consumer tungkol sa mga inaasahang nilalaman at uri ng data ng [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) at [nabe-verify na presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) .

## C.Relasyon ng May-hawak ng Paksa

Ang seksyong ito ay hindi normatibo.

Inilalarawan ng seksyong ito ang mga posibleng ugnayan sa pagitan ng isang [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) at isang may- [ari](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) at kung paano ipinahahayag ng Modelo ng Data ng Na-verify na Kredensyal ang mga kaugnayang ito. Ang sumusunod na diagram ay naglalarawan ng mga ugnayang ito, kasama ang mga kasunod na seksyon na naglalarawan kung paano pinangangasiwaan ang bawat isa sa mga ugnayang ito sa modelo ng data.

Chart, radar chart

Description automatically generated

(img src: <https://www.w3.org/TR/vc-data-model/diagrams/subject-ne-holder.svg>)

*Pigura*13*Mga Relasyon ng May-hawak ng Paksa sa Mga Na-verify na Kredensyal.*

### **C.1Ang paksa ay ang May hawak**

Ang seksyong ito ay hindi normatibo.

Ang pinakakaraniwang relasyon ay kapag ang isang [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) ay ang may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) . Sa kasong ito, madaling mahihinuha ng isang [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) na ang isang [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) ang may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) kung ang [nabe-verify na presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) ay digital na nilagdaan ng may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) at ang lahat ng nilalamang [napapatunayan na mga kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-credentials) ay tungkol sa isang [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) na maaaring matukoy na kapareho ng may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) .

Kung ang credentialSubjectpinapayagan lang na maglagay ng [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) sa isang [nabe-verify na presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) , maaaring ipasok ng [tagabigay ang](https://www.w3.org/TR/vc-data-model/#dfn-issuers)nonTransferable [property](https://www.w3.org/TR/vc-data-model/#dfn-property) sa [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) , gaya ng inilarawan sa ibaba.

#### C.1.1Hindi Naililipat na Ari-arian

Ang seksyong ito ay hindi normatibo.

Isinasaad ng nonTransferable [property](https://www.w3.org/TR/vc-data-model/#dfn-property) na ang isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ay dapat lamang isama sa isang [nabe-verify na presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) na ang patunay ay ibinigay ng credentialSubject. Ang isang [nabe-verify na presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) na naglalaman ng isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) na naglalaman ng ari- nonTransferable [arian](https://www.w3.org/TR/vc-data-model/" \l "dfn-property) , na ang patunay na lumikha ay hindi ang credentialSubject, ay hindi wasto.

[HALIMBAWA40](https://www.w3.org/TR/vc-data-model/#example-usage-of-the-nontransferable-property): Paggamit ng hindi naililipat na ari-arian

{

"@context": [

"https://www.w3.org/2018/credentials/v1",

"https://www.w3.org/2018/credentials/examples/v1"

],

"id": "http://example.edu/credentials/3732",

"type": ["VerifiableCredential", "ProofOfAgeCredential"],

"issuer": "https://example.edu/issuers/14",

"issuanceDate": "2010-01-01T19:23:24Z",

"credentialSubject": {

"id": "did:example:ebfeb1f712ebc6f1c276e12ec21",

"Lagpas sa edad": 21

},

"nonTransferable": totoo,

"patunay": { ..

"verificationMethod": "did:example:ebfeb1f712ebc6f1c276e12ec21",

... }

}

### **C.2Ang Kredensyal ay Natatanging Tinutukoy ang isang Paksa**

Ang seksyong ito ay hindi normatibo.

Sa kasong ito, maaaring maglaman ang credentialSubject [property ng maraming property](https://www.w3.org/TR/vc-data-model/#dfn-property) , bawat isa ay nagbibigay ng aspeto ng isang paglalarawan ng [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) , na pinagsama-sama upang malinaw na matukoy ang [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) . Ang ilang mga kaso ng paggamit ay maaaring hindi nangangailangan na kilalanin ang may [hawak](https://www.w3.org/TR/vc-data-model/#dfn-holders) , gaya ng pagsuri upang makita kung ang isang doktor (ang [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) ) ay sertipikado ng board. Maaaring kailanganin ng ibang mga kaso ng paggamit ang [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) na gumamit ng out-of-band na kaalaman upang matukoy ang kaugnayan sa pagitan ng [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) at ng may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) .

[HALIMBAWA41](https://www.w3.org/TR/vc-data-model/#example-a-credential-uniquely-identifying-a-subject): Isang kredensyal na natatanging nagpapakilala sa isang paksa

{

"@context": ["https://www.w3.org/2018/credentials/v1", "https://schema.org/"]

"id": "http://example.edu/credentials/332",

"type": ["VerifiableCredential", "IdentityCredential"],

"issuer": "https://example.edu/issuers/4",

"issuanceDate": "2017-02-24T19:73:24Z",

"credentialSubject": {

"pangalan": "J. Doe",

"address": {

"streetAddress": "10 Rue de Chose",

"postalCode": "98052",

"addressLocality": "Paris",

"addressCountry": "FR"

},

"birthDate": "1989-03-15"

...

},

"patunay": { **...** }

}

Ang halimbawa sa itaas ay natatanging kinikilala ang [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) gamit ang pangalan, address, at petsa ng kapanganakan ng indibidwal.

### **C.3Ipinapasa ng Paksa ang Nabe-verify na Kredensyal sa May-hawak**

Ang seksyong ito ay hindi normatibo.

Karaniwan ang mga [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ay iniharap sa mga [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) ng [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) . Gayunpaman, sa ilang sitwasyon, maaaring kailanganin ng [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) na ipasa ang kabuuan o bahagi ng isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) sa isa pang may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) . Halimbawa, kung ang isang pasyente (ang [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) ) ay masyadong may sakit para kumuha ng reseta (ang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ) sa parmasyutiko (ang [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) ), maaaring kunin ng isang kaibigan ang reseta upang kunin ang gamot.

Ang modelo ng data ay nagbibigay-daan para dito sa pamamagitan ng pagpayag sa [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) na mag -isyu ng bagong [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) at ibigay ito sa bagong may- [ari](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) , na maaaring magpakita ng parehong [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) sa [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) . Gayunpaman, ang nilalaman ng pangalawang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) na ito ay malamang na tukoy sa aplikasyon, kaya hindi ma-standardize ng detalyeng ito ang mga nilalaman ng pangalawang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) na ito . Gayunpaman, ang isang hindi normatibong halimbawa ay ibinigay sa Appendix [C.5Ipinapasa ng Paksa ang isang Nabe-verify na Kredensyal sa Iba](https://www.w3.org/TR/vc-data-model/#subject-passes-a-verifiable-credential-to-someone-else) .

### **C.4Kumikilos ang May-ari sa ngalan ng Paksa**

Ang seksyong ito ay hindi normatibo.

Sinusuportahan ng Verifiable Credentials Data Model ang may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) na kumikilos sa ngalan ng [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) sa kahit man lang sa mga sumusunod na paraan. Ang:

* [Maaaring](https://www.w3.org/TR/vc-data-model/#dfn-issuers) isama ng tagabigay ang relasyon sa pagitan ng may- [ari](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) at ng [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) sa ari- credentialSubject [arian](https://www.w3.org/TR/vc-data-model/" \l "dfn-property) .
* [Maaaring](https://www.w3.org/TR/vc-data-model/#dfn-issuers) ipahayag ng tagabigay ang ugnayan sa pagitan ng may- [ari](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) at ng [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) sa pamamagitan ng pagbibigay ng bagong [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) , na ginagamit ng may- [ari](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) .
* Maaaring ipahayag ng [paksa ang kanilang kaugnayan sa may-](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects)[ari](https://www.w3.org/TR/vc-data-model/#dfn-holders) sa pamamagitan ng pagbibigay ng bagong [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) , na ginagamit ng may- [ari](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) .

Ang mga mekanismong nakalista sa itaas ay naglalarawan ng ugnayan sa pagitan ng may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) at ng [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) at tinutulungan ang [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) na magpasya kung ang relasyon ay sapat na ipinahayag para sa isang partikular na kaso ng paggamit.

TANDAAN

Ang mga karagdagang mekanismong ginagamit ng [issuer](https://www.w3.org/TR/vc-data-model/#dfn-issuers) o ng [verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) para i-verify ang kaugnayan sa pagitan ng [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) at ng may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) ay nasa labas ng saklaw ng detalyeng ito.

[HALIMBAWA42](https://www.w3.org/TR/vc-data-model/#example-the-relationship-property-in-a-child-s-credential): Ang pag-aari ng relasyon sa kredensyal ng isang bata

{

"@context": [

"https://www.w3.org/2018/credentials/v1",

"https://www.w3.org/2018/credentials/examples/v1"

],

"id": "http://example.edu/credentials/3732",

"type": ["VerifiableCredential", "AgeCredential", "RelationshipCredential"],

"issuer": "https://example.edu/issuers/14",

"issuanceDate": "2010-01-01T19:23:24Z",

"credentialSubject": {

"id": "did:example:ebfeb1f712ebc6f1c276e12ec21",

"edad sa ilalim": 16,

"magulang": {

"id": "did:example:ebfeb1c276e12ec211f712ebc6f",

"type": "Ina"

}

},

"patunay": { **...** } **// ang patunay ay nabuo ng DMV**

}

Sa halimbawa sa itaas, ipinahayag ng [tagabigay](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) ang ugnayan sa pagitan ng bata at ng magulang nang sa gayon ay malamang na tanggapin ng isang [verifier ang](https://www.w3.org/TR/vc-data-model/#dfn-verifier)[kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-credential) kung ito ay ibinigay ng bata o ng magulang.

[HALIMBAWA43](https://www.w3.org/TR/vc-data-model/#example-a-relationship-credential-issued-to-a-parent): Isang kredensyal ng relasyon na ibinigay sa isang magulang

{

"@context": [

"https://www.w3.org/2018/credentials/v1",

"https://www.w3.org/2018/credentials/examples/v1"

],

"id": "http://example.edu/credentials/3732",

"type": ["VerifiableCredential", "RelationshipCredential"],

"issuer": "https://example.edu/issuers/14",

"issuanceDate": "2010-01-01T19:23:24Z",

"credentialSubject": {

"id": "did:example:ebfeb1c276e12ec211f712ebc6f",

"bata": {

"id": "did:example:ebfeb1f712ebc6f1c276e12ec21",

"type": "Bata"

}

},

"patunay": { **...** } **// ang patunay ay nabuo ng DMV**

}

Sa halimbawa sa itaas, ipinahayag ng [tagabigay](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) ang ugnayan sa pagitan ng bata at ng magulang sa isang hiwalay na [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) upang malamang na tanggapin ng isang [verifier ang alinman sa mga](https://www.w3.org/TR/vc-data-model/#dfn-verifier)[kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-credential) ng bata kung ang mga ito ay ibinigay ng bata o kung ang [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) sa itaas ay ibinigay kasama ng alinman sa mga [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) ng bata .

[HALIMBAWA44](https://www.w3.org/TR/vc-data-model/#example-a-relationship-credential-issued-by-a-child): Isang kredensyal ng relasyon na ibinigay ng isang bata

{

"@context": [

"https://www.w3.org/2018/credentials/v1",

"https://www.w3.org/2018/credentials/examples/v1"

],

"id": "http://example.org/credentials/23894",

"type": ["VerifiableCredential", "RelationshipCredential"],

"issuer": "http://example.org/credentials/23894",

"issuanceDate": "2010-01-01T19:23:24Z",

"credentialSubject": {

"id": "did:example:ebfeb1f712ebc6f1c276e12ec21",

"magulang": {

"id": "did:example:ebfeb1c276e12ec211f712ebc6f",

"type": "Ina"

}

},

"patunay": { **...** } **// ang patunay ay nabuo ng bata**

}

Sa halimbawa sa itaas, ipinahayag ng bata ang ugnayan sa pagitan ng bata at ng magulang sa isang hiwalay na [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) upang malamang na tanggapin ng isang [verifier ang alinman sa mga](https://www.w3.org/TR/vc-data-model/#dfn-verifier)[kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-credential) ng bata kung ibinigay ang [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) sa itaas.

Katulad nito, ang mga diskarte na inilalarawan sa mga halimbawa sa itaas ay maaaring gamitin para sa maraming iba pang uri ng mga kaso ng paggamit, kabilang ang kapangyarihan ng abogado, pagmamay-ari ng alagang hayop, at pagkuha ng reseta ng pasyente.

### **C.5Ipinapasa ng Paksa ang isang Nabe-verify na Kredensyal sa Iba**

Ang seksyong ito ay hindi normatibo.

Kapag ang isang [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) ay nagpasa ng isang [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) sa isa pang may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) , ang [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) ay maaaring mag-isyu ng isang bagong na-verify na [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-credentials) sa may- [ari](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) kung saan ang:

* [Tagapagbigay](https://www.w3.org/TR/vc-data-model/#dfn-issuers) ay ang [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) .
* [Ang paksa](https://www.w3.org/TR/vc-data-model/#dfn-subjects) ay ang may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) kung kanino ipinapasa ang [nabe](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) -verify na kredensyal.
* Naglalaman ang [claim ng mga](https://www.w3.org/TR/vc-data-model/#dfn-claims)[property](https://www.w3.org/TR/vc-data-model/#dfn-property) na ipinapasa.

Ang may- [ari](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) ay maaari na ngayong lumikha ng isang [nabe-verify na presentasyon](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations) na naglalaman ng dalawang na-verify na [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-credentials) upang ma - [verify ng](https://www.w3.org/TR/vc-data-model/#dfn-verify)[verifier](https://www.w3.org/TR/vc-data-model/#dfn-verifier) na ang [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) ay nagbigay ng orihinal na na-verify na [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-credentials) sa may- [ari](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) .

[HALIMBAWA45](https://www.w3.org/TR/vc-data-model/#example-a-holder-presenting-a-verifiable-credential-that-was-passed-to-it-by-the-subject): Isang may hawak na nagpapakita ng nabe-verify na kredensyal na ipinasa dito ng paksa

{

"@context": [

"https://www.w3.org/2018/credentials/v1",

"https://www.w3.org/2018/credentials/examples/v1"

],

"id": "https://example.com/VP/0987654321",

"type": ["VerifiablePresentation"],

"napapatunayang kredensyal": [

{

"@context": [

"https://www.w3.org/2018/credentials/v1",

"https://www.w3.org/2018/credentials/examples/v1"

],

"id": "http://pharma.example.com/credentials/3732",

"type": ["VerifiableCredential", "PrescriptionCredential"],

"issuer": "https://pharma.example.com/issuer/4",

"issuanceDate": "2010-01-01T19:23:24Z",

"credentialSubject": {

"id": "did:example:ebfeb1f712ebc6f1c276e12ec21",

"reseta": {....}

},

"CredentialStatus": {

"id": "https://pharma.example.com/credentials/status/3#94567",

"type": "RevocationList2020Status",

"revocationListIndex": "94567",

"revocationListCredential": "https://pharma.example.com/credentials/status/3"

},

"patunay": {....}

},

{

"@context": [

"https://www.w3.org/2018/credentials/v1",

"https://www.w3.org/2018/credentials/examples/v1"

],

"id": "https://example.com/VC/123456789",

"type": ["VerifiableCredential", "PrescriptionCredential"],

"issuer": "did:example:ebfeb1f712ebc6f1c276e12ec21",

"issuanceDate": "2010-01-03T19:53:24Z",

"credentialSubject": {

"id": "did:example:76e12ec21ebhyu1f712ebc6f1z2",

"reseta": {....}

},

"patunay": {

"type": "RsaSignature2018",

"nilikha": "2018-06-17T10:03:48Z",

"proofPurpose": "assertionMethod",

"jws": "pYw8XNi1..Cky6Ed=",

"verificationMethod": "did:example:ebfeb1f712ebc6f1c276e12ec21/keys/234"

}

}

],

"patunay": [{

"type": "RsaSignature2018",

"nilikha": "2018-06-18T21:19:10Z",

"proofPurpose": "pagpapatunay",

"verificationMethod": "did:example:76e12ec21ebhyu1f712ebc6f1z2/keys/2",

"hamon": "c0ae1c8e-c7e7-469f-b252-86e6a0e7387e",

"jws": "BavEll0/I1..W3JT24="

}]

}

Sa halimbawa sa itaas, ang isang pasyente (ang orihinal na [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) ) ay nagpasa ng isang reseta (ang orihinal na [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ) sa isang kaibigan, at nag-isyu ng bagong na-verify na [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-verifiable-credentials) sa kaibigan, kung saan ang kaibigan ang [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) , ang [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) ng orihinal na [nabe-verify na kredensyal](https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials) ay ang [nagbigay](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers) , at ang [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) ay isang kopya ng orihinal na reseta.

### **C.6Pinapahintulutan ng Tagapagbigay ang May-ari**

Ang seksyong ito ay hindi normatibo.

Kapag gusto ng [issuer](https://www.w3.org/TR/vc-data-model/#dfn-issuers) na pahintulutan ang isang may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) na magkaroon ng [kredensyal](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential) na naglalarawan sa isang [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) na hindi ang may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) , at ang may [hawak](https://www.w3.org/TR/vc-data-model/" \l "dfn-holders) ay walang alam na kaugnayan sa [paksa](https://www.w3.org/TR/vc-data-model/" \l "dfn-subjects) , maaaring ipasok ng [tagabigay ang kaugnayan ng may](https://www.w3.org/TR/vc-data-model/" \l "dfn-issuers)[hawak](https://www.w3.org/TR/vc-data-model/#dfn-holders) sa sarili nito sa [kredensyal ng](https://www.w3.org/TR/vc-data-model/" \l "dfn-credential)[paksa](https://www.w3.org/TR/vc-data-model/#dfn-subjects) .

TANDAAN

Ang mga nabe-verify na kredensyal ay hindi isang balangkas ng awtorisasyon at samakatuwid ang delegasyon ay nasa labas ng saklaw ng detalyeng ito. Gayunpaman, nauunawaan na ang mga nabe-verify na kredensyal ay malamang na gagamitin upang bumuo ng mga sistema ng pahintulot at pagtatalaga. Ang sumusunod ay isang diskarte na maaaring naaangkop para sa ilang mga kaso ng paggamit.

[HALIMBAWA46](https://www.w3.org/TR/vc-data-model/#example-a-credential-issued-to-a-holder-who-is-not-the-only-subject-of-the-credential-who-has-no-relationship-with-the-subject-of-the-credential-but-who-has-a-relationship-with-the-issuer): Isang kredensyal na ibinigay sa isang may hawak na hindi (tanging) paksa ng kredensyal, na walang kaugnayan sa paksa ng kredensyal, ngunit may kaugnayan sa nagbigay

{

"@context": [

"https://www.w3.org/2018/credentials/v1",

"https://www.w3.org/2018/credentials/examples/v1"

],

"id": "http://example.edu/credentials/3732",

"type": ["VerifiableCredential", "NameAndAddress"],

"issuer": "https://example.edu/issuers/14",

"may hawak": {

"type": "Pagpapatupad ng Batas",

"id": "did:example:ebfeb1276e12ec21f712ebc6f1c"

},

"issuanceDate": "2010-01-01T19:23:24Z",

"credentialSubject": {

"id": "did:example:ebfeb1f712ebc6f1c276e12ec21",

"name": "Mr John Doe",

"address": "10 Some Street, Anytown, ThisLocal, Country X"

},

"patunay": {

"type": "RsaSignature2018",

"nilikha": "2018-06-17T10:03:48Z",

"proofPurpose": "assertionMethod",

"verificationMethod": "https://example.edu/issuers/14/keys/234",

"jws": "pY9...Cky6Ed = "

}

}

### **C.7Kumikilos ang May-ari sa Ngalan ng Verifier, o walang Relasyon sa Paksa, Tagabigay, o Verifier**

Ang seksyong ito ay hindi normatibo.

Kasalukuyang hindi sinusuportahan ng Verifiable Credentials Data Model ang alinman sa mga sitwasyong ito. Ito ay para sa karagdagang pag-aaral kung paano sila maaaring suportahan.

## D.Mga Pagsasaalang-alang ng IANA

Ang seksyong ito ay hindi normatibo.

Ang seksyong ito ay isusumite sa Internet Engineering Steering Group (IESG) para sa pagsusuri, pag-apruba, at pagpaparehistro sa IANA sa "JSON Web Token Claims Registry".

* Pangalan ng Claim: "vc"
* Paglalarawan ng Claim: Nabe-verify na Kredensyal
* Baguhin ang Controller: W3C
* (Mga) Dokumento ng Pagtutukoy: [Seksyon 6.3.1.2: Mga Extension ng JSON Web Token ng Nabe-verify na Modelo ng Data ng Mga Kredensyal 1.0](https://www.w3.org/TR/vc-data-model/)
* Pangalan ng Claim: "vp"
* Paglalarawan ng Claim: Na-verify na Presentasyon
* Baguhin ang Controller: W3C
* (Mga) Dokumento ng Pagtutukoy: [Seksyon 6.3.1.2: Mga Extension ng JSON Web Token ng Nabe-verify na Modelo ng Data ng Mga Kredensyal 1.0](https://www.w3.org/TR/vc-data-model/)

## E.Kasaysayan ng Pagbabago

Ang seksyong ito ay naglalaman ng mga makabuluhang pagbabago na ginawa mula noong ilathala ang v1.0 ng detalyeng ito bilang isang Rekomendasyon ng W3C .

Mga pagbabago mula noong [Rekomendasyon](https://www.w3.org/TR/2019/REC-vc-data-model-20191119/):

* Idagdag ang seksyong ito ng kasaysayan ng rebisyon.
* I-update ang mga nakaraang normative reference na tumuturo sa RFC3339 para sa mga detalye ng datetime upang normal na ma-reference ngayon ang mga detalye ng datetime na inilalarawan sa XMLSCHEMA11-2 na mas tumpak na nagpapakita ng paggamit sa mga halimbawa at library.
* Paluwagin ang pangangailangang gumamit ng mga URL para gumamit ng mga [URI](https://www.w3.org/TR/vc-data-model/#dfn-uri) sa id property ng credentialStatusat mga refreshService seksyon ng modelo ng data.
* Paluwagin ang mga normative statement sa seksyong zero-knowledge proofs para ma-enable ang pagsunod sa mga bagong zero-knowledge proof scheme, gaya ng BBS+, na ginawa mula noong na-publish ang v1.0 specification bilang Rekomendasyon.
* I-update ang lahat ng mga sanggunian upang tumuro sa pinakabagong bersyon ng mga tinukoy na detalye. Ayusin ang mga sirang link sa mga papel na naging hindi available sa mga na-update na lokasyon kung saan available ang mga papel.
* Dagdagan ang accessibility ng mga SVG diagram.
* Ayusin ang mga editoryal na bug sa ilang halimbawang nauugnay sa issuer, issuanceDate, credentialStatus, mga petsa, patay na link, at maliliit na syntax error.
* Ilipat ang mga pagkilala mula sa seksyong Status ng Dokumento papunta sa apendiks ng Mga Pagkilala.

## F.Mga Pasasalamat

Ang seksyong ito ay hindi normatibo.

Ang Working Group ay nagpapasalamat sa mga sumusunod na indibidwal hindi lamang para sa kanilang mga kontribusyon sa nilalaman ng dokumentong ito, ngunit para din sa trabaho ni yeoman sa komunidad ng mga pamantayang ito na nagdulot ng mga pagbabago, talakayan, at pinagkasunduan sa iba't ibang opinyon: Matt Stone, Gregg Kellogg, Ted Thibodeau Jr, Oliver Terbu, Joe Andrieu, David I. Lehn, Matthew Collier, at Adrian Gropper.

Ang paggawa sa detalyeng ito ay suportado ng komunidad ng Rebooting the Web of Trust na pinangasiwaan ni Christopher Allen, Shannon Appelcline, Kiara Robles, Brian Weller, Betty Dhamers, Kaliya Young, Manu Sporny, Drummond Reed, Joe Andrieu, Heather Vescent, Kim Hamilton Duffy , Samantha Chase, at Andrew Hughes. Sinuportahan din ng mga kalahok sa Internet Identity Workshop, na pinangasiwaan nina Phil Windley, Kaliya Young, Doc Searls, at Heidi Nobantu Saul, ang pagpipino ng gawaing ito sa pamamagitan ng maraming sesyon ng pagtatrabaho na idinisenyo upang turuan ang tungkol, debate sa, at pahusayin ang detalyeng ito.

Ang Working Group ay nagpapasalamat din sa aming mga Tagapangulo, Dan Burnett, Matt Stone, Brent Zundel, at Wayne Chang, pati na rin ang aming W3C Staff Contacts, Kazuyuki Ashimura at Ivan Herman, para sa kanilang ekspertong pamamahala at matatag na paggabay ng grupo sa pamamagitan ng proseso ng standardisasyon ng W3C .

Ang mga bahagi ng trabaho sa detalyeng ito ay pinondohan ng Departamento ng Homeland Security ng Science and Technology Directorate sa ilalim ng kontrata HSHQDC-17-C-00019. Ang nilalaman ng detalyeng ito ay hindi kinakailangang sumasalamin sa posisyon o patakaran ng US Government at walang opisyal na pag-endorso ang dapat na ipahiwatig.

Nais pasalamatan ng Working Group ang mga sumusunod na indibidwal para sa pagsusuri at pagbibigay ng feedback sa detalye (sa alpabetikong pagkakasunud-sunod):

Christopher Allen, David Ammouial, Joe Andrieu, Bohdan Andriyiv, Ganesh Annan, Kazuyuki Ashimura, Tim Bouma, Pelle Braendgaard, Dan Brickley, Allen Brown, Jeff Burdges, Daniel Burnett, ckennedy422, David Chadwick, Chaoxinhu, Kim (Hamilton) Duffy, Lautaro Dragan, enuoCM, Ken Ebert, Eric Elliott, William Entriken, David Ezell, Nathan George, Reto Gmür, Ryan Grant, glauserr, Adrian Gropper, Joel Gustafson, Amy Guy, Lovesh Harchandani, Daniel Hardman, Dominique Hazael-Massieux, Jonathan Holt, David Hyland-Wood, Iso5786, Renato Iannella, Richard Ishida, Ian Jacobs, Anil John, Tom Jones, Rieks Joosten, Gregg Kellogg, Kevin, Eric Korb, David I. Lehn, Michael Lodder, Dave Longley, Christian Lundkvist, Jim Masloski, Pat McBennett, Adam C. Migus, Liam Missin, Alexander Mühle, Anthony Nadalin, Clare Nelson, Mircea Nistor, Grant Noble, Darrell O'Donnell,Nate Otto, Matt Peterson, Addison Phillips, Eric Prud'hommeaux, Liam Quin, Rajesh Rathnam, Drummond Reed, Yancy Ribbens, Justin Richer, Evstifeev Roman, RorschachRev, Steven Rowat, Pete Rowley, Markus Sabadello, Kristijan Sedlak, Tzviya Seigman, Reza Soltani, Manu Sporny, Orie Steele, Matt Stone, Oliver Terbu, Ted Thibodeau Jr, John Tibbetts, Mike Varley, Richard Varn, Heather Vescent, Christopher Lemmer Webber, Benjamin Young, Kaliya Young, Dmitri Zagidulin, at Brent Zundel.Richard Varn, Heather Vescent, Christopher Lemmer Webber, Benjamin Young, Kaliya Young, Dmitri Zagidulin, at Brent Zundel.Richard Varn, Heather Vescent, Christopher Lemmer Webber, Benjamin Young, Kaliya Young, Dmitri Zagidulin, at Brent Zundel.

## G.Mga sanggunian

### **G.1Mga sanggunian sa normatibo**

**[JSON-LD]**

[JSON-LD 1.1: Isang JSON-based na Serialization para sa Linked Data](https://www.w3.org/TR/json-ld11/) . Gregg Kellogg; Manu Sporny; Dave Longley; Markus Lanthaler; Pierre-Antoine Champin; Niklas Lindström. W3C JSON-LD 1.1 Working Group. W3C Working Draft. URL:<https://www.w3.org/TR/json-ld11/>

**[RFC2119]**

[Mga pangunahing salita para sa paggamit sa mga RFC upang Ipahiwatig ang Mga Antas ng Kinakailangan](https://www.rfc-editor.org/rfc/rfc2119) . S. Bradner. IETF. Marso 1997. Pinakamahusay na Kasalukuyang Kasanayan. URL:<https://www.rfc-editor.org/rfc/rfc2119>

**[RFC3986]**

[Uniform Resource Identifier (URI): Generic Syntax](https://www.rfc-editor.org/rfc/rfc3986) . T. Berners-Lee; R. Fielding; L. Master. IETF. Enero 2005. Internet Standard. URL:<https://www.rfc-editor.org/rfc/rfc3986>

**[RFC7515]**

[JSON Web Signature (JWS)](https://www.rfc-editor.org/rfc/rfc7515) . M. Jones; J. Bradley; N. Sakimura. IETF. Mayo 2015. Iminungkahing Pamantayan. URL:<https://www.rfc-editor.org/rfc/rfc7515>

**[RFC7519]**

[JSON Web Token (JWT)](https://www.rfc-editor.org/rfc/rfc7519) . M. Jones; J. Bradley; N. Sakimura. IETF. Mayo 2015. Iminungkahing Pamantayan. URL:<https://www.rfc-editor.org/rfc/rfc7519>

**[RFC8174]**

[Kalabuan ng Malaking titik kumpara sa Maliit na titik sa RFC 2119 Key Words](https://www.rfc-editor.org/rfc/rfc8174) . B. Leiba. IETF. Mayo 2017. Pinakamahusay na Kasalukuyang Kasanayan. URL:<https://www.rfc-editor.org/rfc/rfc8174>

**[RFC8259]**

[Ang Format ng Pagpapalitan ng Data ng JavaScript Object Notation (JSON)](https://www.rfc-editor.org/rfc/rfc8259) . T. Bray, Ed.. IETF. Disyembre 2017. Internet Standard. URL:<https://www.rfc-editor.org/rfc/rfc8259>

**[XMLSCHEMA11-2]**

[W3C XML Schema Definition Language (XSD) 1.1 Bahagi 2: Mga Uri ng Data](https://www.w3.org/TR/xmlschema11-2/) . David Peterson; Sandy Gao; Ashok Malhotra; Michael Sperberg-McQueen; Henry Thompson; Paul V. Biron et al. W3C. 5 Abril 2012. Rekomendasyon ng W3C. URL:<https://www.w3.org/TR/xmlschema11-2/>

### **G.2Mga sanggunian na nagbibigay-kaalaman**

**[CL-SIGNATURES]**

[Isang Signature Scheme na may Mahusay na Protocol](https://www.researchgate.net/publication/220922101_A_Signature_Scheme_with_Efficient_Protocols) . Jan Camenisch; Anna Lysyanskaya. Pananaliksik sa IBM. Peer Reviewed Paper. URL:<https://www.researchgate.net/publication/220922101_A_Signature_Scheme_with_Efficient_Protocols>

**[INTEGRIDAD NG DATOS]**

[Integridad ng Data](https://w3c-ccg.github.io/data-integrity-spec/) . Manu Sporny; Dave Longley. Pangkat ng Komunidad ng Mga Kredensyal. CG-DRAFT. URL:<https://w3c-ccg.github.io/data-integrity-spec/>

**[DEMOGRAPHICS]**

[Ang mga Simpleng Demograpiko ay Kadalasang Nakikilala ang mga Tao na Natatangi](https://dataprivacylab.org/projects/identifiability/paper1.pdf) . Latanya Sweeney. Data Privacy Lab. URL:<https://dataprivacylab.org/projects/identifiability/paper1.pdf>

**[HASHLINK]**

[Mga Cryptographic Hyperlink](https://datatracker.ietf.org/doc/draft-sporny-hashlink/) . Manu Sporny. Internet Engineering Task Force (IETF). Internet-Draft. URL:<https://datatracker.ietf.org/doc/draft-sporny-hashlink/>

**[IPFS]**

[InterPlanetary File System (IPFS)](InterPlanetary%20File%20System%20(IPFS)) . Wikipedia. URL:<https://en.wikipedia.org/wiki/InterPlanetary_File_System>

**[JSON]**

[Ang Format ng Pagpapalitan ng Data ng JavaScript Object Notation (JSON)](https://www.rfc-editor.org/rfc/rfc8259) . T. Bray, Ed.. IETF. Disyembre 2017. Internet Standard. URL:<https://www.rfc-editor.org/rfc/rfc8259>

**[JSON-SCHEMA-2018]**

[JSON Schema: Isang Uri ng Media para sa Paglalarawan sa Mga Dokumento ng JSON](https://datatracker.ietf.org/doc/draft-handrews-json-schema/) . Austin Wright; Henry Andrews. Internet Engineering Task Force (IETF). Internet-Draft. URL:<https://datatracker.ietf.org/doc/draft-handrews-json-schema/>

**[LDP-REGISTRY]**

[Naka-link na Data Cryptographic Suite Registry](https://w3c-ccg.github.io/ld-cryptosuite-registry/) . Manu Sporny; Drummond Reed; Orie Steele. Pangkat ng Komunidad ng Mga Kredensyal. CG-DRAFT. URL:<https://w3c-ccg.github.io/ld-cryptosuite-registry/>

**[NA-LINKED-DATA]**

[Mga Isyu sa Disenyo ng Naka-link na Data](https://www.w3.org/DesignIssues/LinkedData.html) . Tim Berners-Lee. W3C. 27 Hulyo 2006. W3C-Internal Document. URL:<https://www.w3.org/DesignIssues/LinkedData.html>

**[RFC7049]**

[Concise Binary Object Representation (CBOR)](https://www.rfc-editor.org/rfc/rfc7049) . C. Bormann; P. Hoffman. IETF. Oktubre 2013. Iminungkahing Pamantayan. URL:<https://www.rfc-editor.org/rfc/rfc7049>

**[RFC7516]**

[JSON Web Encryption (JWE)](https://www.rfc-editor.org/rfc/rfc7516) . M. Jones; J. Hildebrand. IETF. Mayo 2015. Iminungkahing Pamantayan. URL:<https://www.rfc-editor.org/rfc/rfc7516>

**[RFC7797]**

[JSON Web Signature (JWS) Unencoded Payload Option](https://www.rfc-editor.org/rfc/rfc7797) . M. Jones. IETF. Pebrero 2016. Iminungkahing Pamantayan. URL:<https://www.rfc-editor.org/rfc/rfc7797>

**[RFC8471]**

[Ang Token Binding Protocol Bersyon 1.0](https://www.rfc-editor.org/rfc/rfc8471) . A. Popov, Ed.; M. Nystroem; D. Balfanz; J. Hodges. IETF. Oktubre 2018. Iminungkahing Pamantayan. URL:<https://www.rfc-editor.org/rfc/rfc8471>

**[STRING-META]**

[Mga String sa Web: Metadata ng Wika at Direksyon](https://www.w3.org/TR/string-meta/) . Addison Phillips; Richard Ishida. Internationalization Working Group. W3C Working Draft. URL:<https://www.w3.org/TR/string-meta/>

**[VC-EXTENSION-REGISTRY]**

[Na-verify na Registry ng Extension ng Mga Kredensyal](https://w3c-ccg.github.io/vc-extension-registry/) . Manu Sporny. Pangkat ng Komunidad ng Mga Kredensyal. CG-DRAFT. URL:<https://w3c-ccg.github.io/vc-extension-registry/>

**[VC-IMP-GUIDE]**

[Mga Alituntunin sa Pagpapatupad ng Mga Napapatunayang Kredensyal 1.0](https://w3c.github.io/vc-imp-guide/) . Andrei Sambra; Manu Sporny. Pangkat ng Komunidad ng Mga Kredensyal. Draft ng W3C Editor. URL:<https://w3c.github.io/vc-imp-guide/>

**[VC-USE-CASES]**

[Mga Na-verify na Kredensyal sa Paggamit ng Mga Kaso](https://www.w3.org/TR/vc-use-cases/) . Shane McCarron; Joe Andrieu; Matt Stone; Tzviya Siegman; Gregg Kellogg; Ted Thibodeau. W3C. 24 Setyembre 2019. Tala ng W3C Working Group. URL:<https://www.w3.org/TR/vc-use-cases/>

**[WCAG21]**

[Web Content Accessibility Guidelines (WCAG) 2.1](https://www.w3.org/TR/WCAG21/) . Andrew Kirkpatrick; Joshua O'Connor; Alastair Campbell; Michael Cooper. W3C. 5 Hunyo 2018. Rekomendasyon ng W3C. URL:<https://www.w3.org/TR/WCAG21/>