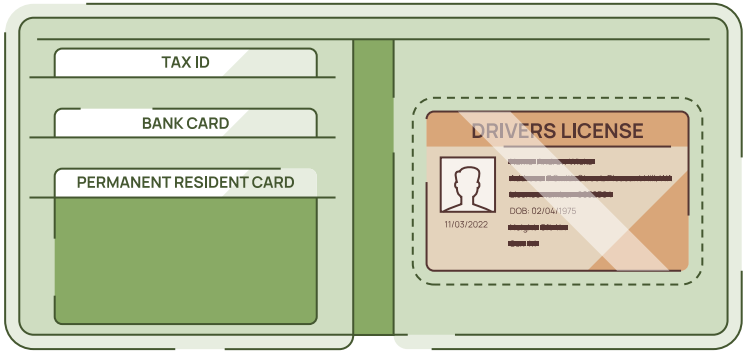
DIGITAL BAZAAR

Selective Disclosure for W3C Data Integrity



Prepared for W3C CCG / VCWG

Date: 2023-03-16

Preface

NOTE

The purpose of this presentation is to introduce the Data Integrity Selective Disclosure schemes and explain the current benefits and drawbacks for this mechanism. A comparison of selective disclosure schemes for W3C Verifiable Credentials will be released at a future date.

DIGITAL BAZAAR

Agenda

What we will cover today.

- Overview of Selective Disclosure
- Selective Disclosure Use Cases
- Data Integrity Selective Disclosure Lifecycle
- How it Works (conceptually)
- How it Works (detail)

DIGITAL BAZAAR

Overview

Selective Disclosure

Digitally signing pieces of data in a document
in a way that empowers the Holder of that document
to only reveal specific information to a Verifier.

DIGITAL BAZAAR

Use Cases

Examples where Selective Disclosure is helpful.

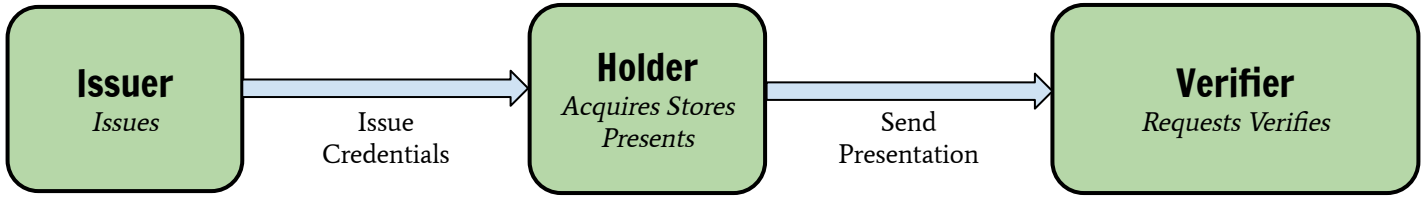
- Prove that you are a citizen of a particular country without revealing your address.
- Prove that you are an employee of a particular company without revealing your name or position.
- Reveal the sender and receiver of a shipment without revealing the contents of a shipment.
- Reveal the sender receiver and payment amount for an invoice without revealing the line items in the invoice.
- Prove that you are over a certain age and are licensed to drive without sharing your PII.

DIGITAL BAZAAR

Data Integrity with Selective Disclosure Journey

1. Issuer creates Verifiable Credential

3. Verifier requests specific claims



2. Issuer signs Verifiable Credential using selective disclosure scheme

4. Holder selectively discloses specific claims

DIGITAL BAZAAR

DIGITAL BAZAAR

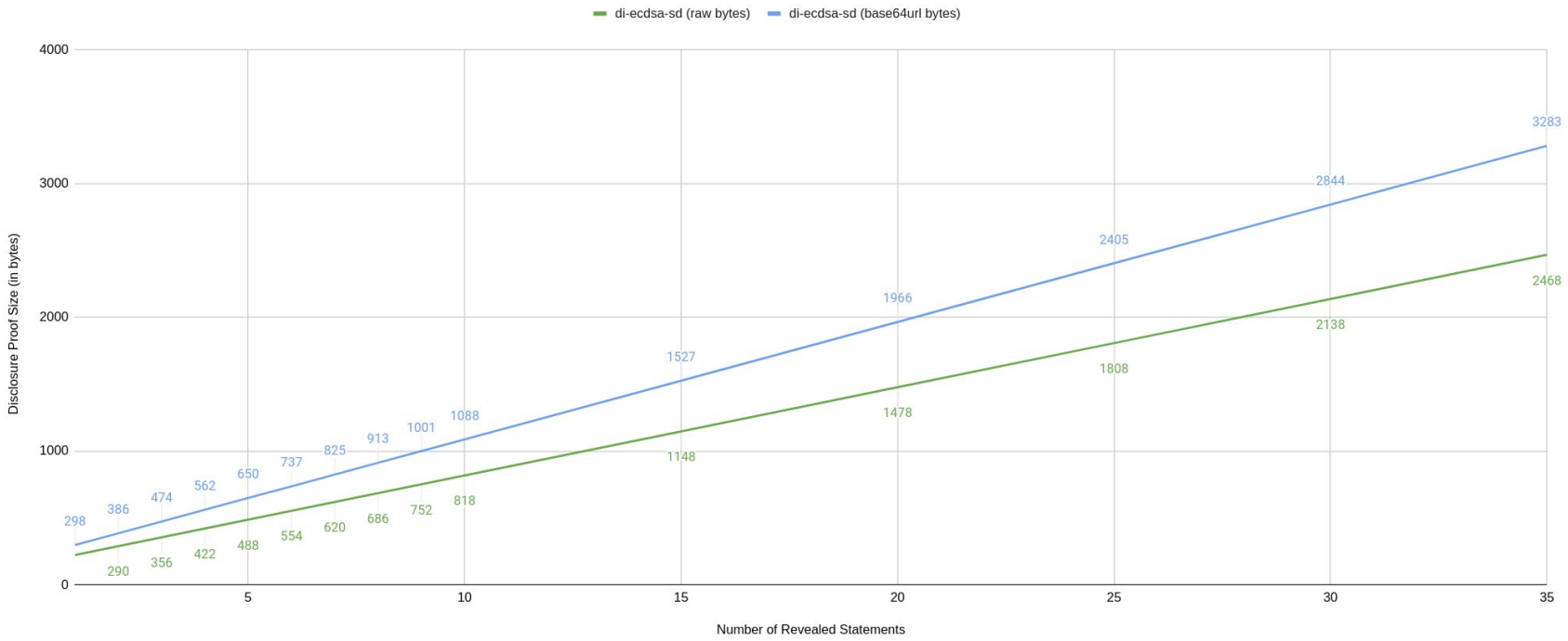
Performance of Selective Disclosure for Data Integrity

Data Integrity Selective Disclosure Scheme Features

- Approach works for NIST-approved cryptography
- Supports mandatory disclosure of specific properties
- Initial proof size is typically between 700-4000 bytes, stored in Digital Wallet (only Holder sees that signature)
- Small disclosure proof sizes (~128 bytes per disclosed claim)
- Disclosure proof size starts small, gets larger as more claims are disclosed
- Approach, or modification thereof, can work for post-quantum cryptography

DIGITAL BAZAAR

Disclosed Proof Size vs. Revealed Statements (smaller size is better)



1. The graph above demonstrates that disclosure proof sizes grow as more claims are disclosed.
2. The green line shows the proof size in raw bytes (e.g., when encoded in CBOR or CBOR-LD).
3. The blue line shows the base64-url encoding overhead for the proof size (e.g., when encoded in JSON or JSON-LD).

DIGITAL BAZAAR

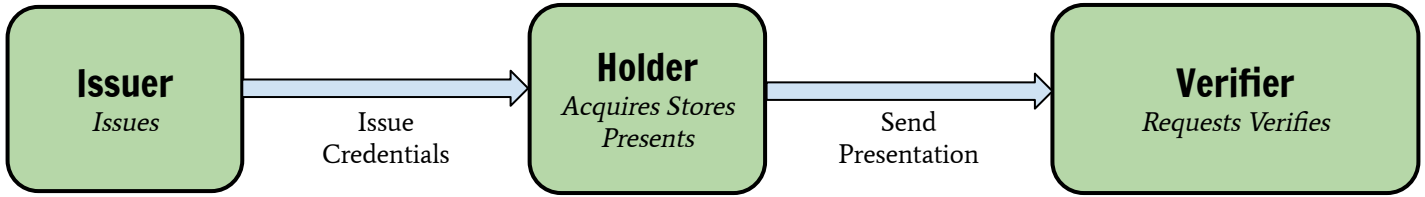
DIGITAL BAZAAR

How it Works: High-level Overview

Data Integrity with Selective Disclosure Journey

1. Issuer creates Verifiable Credential

3. Verifier requests specific claims



2. Issuer signs Verifiable Credential using selective disclosure scheme

4. Holder selectively discloses specific claims

DIGITAL BAZAAR

How it works: Issuer Creates Unsecured Verifiable Credential

```
VC is an Employee Credential.
VC is valid from June 2023.
VC is valid until June 2024.
VC is about Jane Doe.
Jane Does employee ID is YB-38473.
Jane Does job title is Comptroller.
Jane Does division is Accounting.
Jane Does employer is Example Corporation.
```

DIGITAL BAZAAR

How it works: Issuer Canonicalizes Unsecured Verifiable Credential

```
1. Jane Does employer is Example Corporation.
2. Jane Does employee ID is YB-38473.
3. Jane Does job title is Comptroller.
4. Jane Does division is Accounting.
5. VC is about Jane Doe.
6. VC is an Employee Credential.
7. VC is valid from June 2023.
8. VC is valid until June 2024.
```

DIGITAL BAZAAR

How it works: Issuer Digitally Signs Each Claim

```
1. Jane Does employer is Example Corporation.
2. Jane Does employee ID is YB-38473.
3. Jane Does job title is Comptroller.
4. Jane Does division is Accounting.
5. VC is about Jane Doe.
6. VC is an Employee Credential.
7. VC is valid from June 2023.
8. VC is valid until June 2024.
```

DIGITAL BAZAAR

How it works: Holder Receives Secured Verifiable Credential

🔒 VC is an Employee Credential.
🔒 VC is valid from June 2023.
🔒 VC is valid until June 2024.
🔒 VC is about Jane Doe.
🔒 Jane Does employee ID is YB-38473.
🔒 Jane Does job title is Comptroller.
🔒 Jane Does division is Accounting.
🔒 Jane Does employer is Example Corporation.

How it works: Verifier Requests Specific Claims

```
I need an Employee Credential stating your employers name?
```

How it works: Holder Software Selects Claims for Disclosure

```
🔒VC is an Employee Credential.
🔒My employer is Example Corporation.
```

DIGITAL BAZAAR

DIGITAL BAZAAR

How it Works: Excruciating Detail

How it works: Issuer Creates Unsecured Verifiable Credential


```
{
  "@context": [
    "https://www.w3.org/ns/credentials/v2"
    "https://www.w3.org/ns/credentials/examples/v2"
  ]
  "type": ["VerifiableCredential" "ExampleEmployeeCredential"]
  "issuer": "did:example:c276e12ec21ebfeb1f712ebc6f1"
  "validFrom": "2023-06-01T09:25:48Z"
  "validUntil": "2024-06-01T09:25:48Z"
  "credentialSubject": {
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21"
    "name": "Jane Doe"
    "employeeId": "YB-38473"
    "jobTitle": "Comptroller"
    "division": "Accounting"
    "employer": {
      "id": "did:example:c276e12ec21ebfeb1f712ebc6f1"
      "name": "Example Corporation"
    }
  }
}
```

How it works: Issuer Canonicalizes Unsecured Verifiable Credential

```
Mandatory disclosure claims:
  _:uX1Lu5VNvUx…HMYP5VScrM <http://www.w3.org/1999/02/22-rdf-syntax-ns#type> <https://www.w3.org/2018/credentials#VerifiableCredential> .
  _:uX1Lu5VNvUx…HMYP5VScrM <http://www.w3.org/1999/02/22-rdf-syntax-ns#type> <https://www.w3.org/ns/credentials/examples#ExampleEmployeeCredential> .
  _:uX1Lu5VNvUx…HMYP5VScrM <https://www.w3.org/2018/credentials#issuer> <did:example:c276e12ec21ebfeb1f712ebc6f1> .
  _:uX1Lu5VNvUx…HMYP5VScrM <https://www.w3.org/2018/credentials#validFrom> "2023-06-01T09:25:48Z"^^<http://www.w3.org/2001/XMLSchema#dateTime> .
  _:uX1Lu5VNvUx…HMYP5VScrM <https://www.w3.org/2018/credentials#validUntil> "2024-06-01T09:25:48Z"^^<http://www.w3.org/2001/XMLSchema#dateTime> .

Selective disclosure claims:
  <did:example:c276e12ec21ebfeb1f712ebc6f1> <https://www.w3.org/ns/credentials/examples#name> "Example Corporation" .
  <did:example:ebfeb1f712ebc6f1c276e12ec21> <https://www.w3.org/ns/credentials/examples#division> "Accounting" .
  <did:example:ebfeb1f712ebc6f1c276e12ec21> <https://www.w3.org/ns/credentials/examples#employeeId> "YB-38473" .
  <did:example:ebfeb1f712ebc6f1c276e12ec21> <https://www.w3.org/ns/credentials/examples#employer> <did:example:c276e12ec21ebfeb1f712ebc6f1> .
  <did:example:ebfeb1f712ebc6f1c276e12ec21> <https://www.w3.org/ns/credentials/examples#jobTitle> "Comptroller" .
  <did:example:ebfeb1f712ebc6f1c276e12ec21> <https://www.w3.org/ns/credentials/examples#name> "Jane Doe" .
  _:uX1Lu5VNvUx…HMYP5VScrM <https://www.w3.org/2018/credentials#credentialSubject> <did:example:ebfeb1f712ebc6f1c276e12ec21> .
```

How it works: Issuer Digitally Signs Each Claim

```
Base Signature:
          d634b1f975404330ad3febf7bf3e84725bcfd6c5402161244d1f72765c8938c8db6b7d37d6a57ab4aaed682687bb618aac82c7045479185ab4cf55a507d8268d

Ephemeral Public Key:
          did:key:zDnaekGZTbQBerwcehBSXLqAg6s55hVEBms1zFy89VHXtJSa9

HMAC Key (for privacy-preserving blank node IDs):
          431244a601a5507b23b21c263cef965c246a713425c29f85e7a861c822cc30a7

Mandatory disclosure fields (JSON Pointer):
          ["/issuer" "/type" "/validFrom" "/validUntil"]

Selective signatures:
          8468daccca6e1c7afde4574308e3d4ace06ee0c76f2c3038de29bf4cb348939090c0710feb2174306f6dccba8136eb88543371dabca2b9b1267a227ae3e44dcb
          908fe9734a5f94324945533222d3951192f54083323441c74b8a262c30acb7bc283bb1089cc97e3a6f58d67f744ac264612cc3f1c7e73ac23610a63f84b7bd9e
          Ae2b12bbaf88a3770df0e587027315bfaa9700fe8134367b93d88395506d6ebd94ed204a950cbabb217be37f56d6b6dbfade0e48f4e9de48708addd496ca6ddb
          Ec304caebe380353180cbf6cc0944a6e2eed83ee67bfa5577af4ce4d2d3496e38964aaf7572830699ffda5ae06ab9bdda2f4e14c3713075467c0cd0956f07f4c
          7987765b15161e1ada7442c664a862a794a6f59335549f8a30136959adceb7c2b53bde3b8ff02cc4348a322c7851261063e9a1f8446da498a806bc95c996f541
          13cfe730db7a7acbde737407327eeded01666b7549b68301abf9c7bc8050308be0b0913f9c9e9c41bf97226303a41b1c3cb4bc87095032c4eb7df806f13923b9
          db5843a6f720e61f83ae44fdc8c157b9d4e7738c7937d147d51c334d1bcd46535a7476f4243733bee595fecd78770fc8d5d0b6aec709ca675876678f5c27888e

Total Signature Size (P-256 ecdsa-sd):
          643 bytes (859 bytes when encoded in base64url)
```

DIGITAL BAZAAR

How it works: Holder Receives Secured Verifiable Credential


```
{
  "@context": [
    "https://www.w3.org/ns/credentials/v2"
    "https://www.w3.org/ns/credentials/examples/v2"
  ]
  "type": [
    "VerifiableCredential"
    "ExampleEmployeeCredential"
  ]
  "issuer": "did:example:c276e12ec21ebfeb1f712ebc6f1"
  "validFrom": "2023-06-01T09:25:48Z"
  "validUntil": "2024-06-01T09:25:48Z"
  "credentialSubject": {
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21"
    "name": "Jane Doe"
    "employeeId": "YB-38473"
    "jobTitle": "Comptroller"
    "division": "Accounting"
    "employer": {
      "id": "did:example:c276e12ec21ebfeb1f712ebc6f1"
      "name": "Example Corporation"
    }
  }
  "proof": {
    "type": "DataIntegrityProof"
    "created": "2023-06-01T09:25:48Z"
    "verificationMethod": "did:key:zDnaekGZTbQBerwcehBSXLqAg6s55hVEBms1zFy89VHXtJSa9#zDnaekGZTbQBerwcehBSXLqAg6s55hVEBms1zFy89VHXtJSa9"
    "cryptosuite": "ecdsa-sd-2023"
    "proofPurpose": "assertionMethod"
    "proofValue":
"u2V0AhVhA1jSx-XVAQzCtP-v3vz6EclvP1sVAIWEkTR9ydlyJOMjba3031qV6tKrtaCaHu2GKrILHBFR5GFq0z1WlB9gmjVgkge0Pz708xx42eavg6fTXp8AZN-soT1vuxPX3o3pVIbzE31TjWCBDEkSmAaVQ
eyOyHCY875ZcJGpxNCXCn4XnqGHIIswwp4dYQIRo2szKbhx6_eRXQwjj1KzgbuDHbywwON4pv0yzSJOQkMBxD-shdDBvbcy6gTbriFQzcdq8ormxJnoieuPkTctYQJCP6XNKX5QySUVTMiLTlRGS9UCDMjRBx0
uKJiwwrLe8KDuxCJzJfjpvWNZ_dErCZGEsw_HH5zrCNhCmP4S3vZ5YQK4rEruviKN3DfDlhwJzFb-qlwD-gTQ2e5PYg5VQbW69lO0gSpUMurshe-N_Vta22_reDkj06d5IcIrd1JbKbdtYQOwwTK6-OANTGAy_
bMCUSm4u7YPuZ7-lV3r0zk0tNJbjiWSq91coMGmf_aWuBqub3aL04Uw3EwdUZ8DNCVbwf0xYQHmHdlsVFh4a2nRCxmSoYqeUpvWTNVSfijATaVmtzrfCtTveO4_wLMQ0ijIseFEmEGPpofhEbaSYqAa8lcmW9U
FYQBPP5zDbenrL3nN0BzJ-7e0BZmt1SbaDAav5x7yAUDCL4LCRP5yenEG_lyJjA6QbHDy0vIcJUDLE6334BvE5I7lYQNtYQ6b3IOYfg65E_cjBV7nU53OMeTfRR9UcM00bzUZTWnR29CQ3M77llf7NeHcPyNXQ
tq7HCcpnWHZnj1wniI6EZy9pc3N1ZXJlL3R5cGVqL3ZhbGlkRnJvbWsvdmFsaWRVbnRpbA"
  }
}
```

How it works: Verifier Requests Specific Claims

```
{
  "query": [{
    "type": "QueryByExample"
    "credentialQuery": [{
      "reason": "We need you to verify your employer."
      "example": {
        "@context": ["https://www.w3.org/2018/credentials/v2" "https://www.w3.org/ns/credentials/examples/v2"]
        "type": "ExampleEmployeeCredential"
        "credentialSubject": {
          "id": ""
          "employer": {
            "id": ""
            "name": ""
          }
        }
      }
    }]
  }]
  "challenge": "99612b24-63d9-11ea-b99f-4f66f3e4f81a"
  "domain": "sd.example"
}
```

DIGITAL BAZAAR

How it works: Holder Software Selects Claims for Disclosure


```
{
  "@context": [
    "https://www.w3.org/ns/credentials/v2"
    "https://www.w3.org/ns/credentials/examples/v2"
  ]
  "type": [
    "VerifiableCredential"
    "ExampleEmployeeCredential"
  ]
  "credentialSubject": {
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21"
    "employer": {
      "id": "did:example:c276e12ec21ebfeb1f712ebc6f1"
      "name": "Example Corporation"
    }
  }
  "issuer": "did:example:c276e12ec21ebfeb1f712ebc6f1"
  "validFrom": "2023-06-01T09:25:48Z"
  "validUntil": "2024-06-01T09:25:48Z"
  "proof": {
    "type": "DataIntegrityProof"
    "created": "2023-06-01T09:25:48Z"
    "verificationMethod": "did:key:zDnaekGZTbQBerwcehBSXLqAg6s55hVEBms1zFy89VHXtJSa9#zDnaekGZTbQBerwcehBSXLqAg6s55hVEBms1zFy89VHXtJSa9"
    "cryptosuite": "ecdsa-sd-2023"
    "proofPurpose": "assertionMethod"
    "proofValue":
"u2V0BhVhA1jSx-XVAQzCtP-v3vz6EclvP1sVAIWEkTR9ydlyJOMjba3031qV6tKrtaCaHu2GKrILHBFR5GFq0z1WlB9gmjVgkge0Pz708xx42eavg6fTXp8AZN-soT1vuxPX3o3pVIbzE31Tjg1hAhGjazMpu
HHr95FdDCOPUrOBu4MdvLDA43im_TLNIk5CQwHEP6yF0MG9tzLqBNuuIVDNx2ryiubEmeiJ64-RNy1hA7DBMrr44A1MYDL9swJRKbi7tg-5nv6VXevTOTS00luOJZKr3VygwaZ_9pa4Gq5vdovThTDcTB1RnwM
0JVvB_TFhA21hDpvcg5h-DrkT9yMFXudTnc4x5N9FH1RwzTRvNRlNadHb0JDczvuWV_s14dw_I1dC2rscJymdYdmePXCeIjqFlYzE0bjB4LHVYMUx1NVZOdlV4UDdSeDkyQkNsZmxITEFncUhRaGd2d3hITVlQ
NVZTY3JNhQIDBQYH"
  }
}
```


DIGITAL BAZAAR

DIGITAL BAZAAR

Questions and Answers

Read the docs and code at: https://github.com/digitalbazaar/ecdsa-sd-2023-cryptosuite