DHS Science & Technology Directorate

SILICON VALLEY INNOVATION PROGRAM

Approach to Developing Security and Privacy Assessment Criteria for Decentralized Identifiers

Deborah Shands

SRI International

Approved for Public Release 20 July 2021

Outline

- Goals of the project
- Standards-based criteria
- Approach to developing criteria
- Example security requirements
- Privacy objectives and example requirements
- Conclusion

Goals of the project

- Develop criteria for individuals/organizations to assess the security/privacy characteristics of Decentralized Identifiers (DID) Method implementations and services.
  - Our report sketches an approach to development of security/privacy objectives and requirements.
- Review draft DID standards to identify potential security/privacy challenges.
  - Our report highlights some potentially challenging criteria for DIDs and DID Methods, based on the V1.0 Core architecture.
- Discuss with SVIP-funded organizations working on decentralized identity management technologies.

Standards-based criteria

- Security criteria development and refinement – one facet of well-established "system security engineering" process.
  - "Common Criteria" [1] protection profiles [2, 3]
    - Used for specifying security requirements for products to be used in national security systems.
    - International agreements to accept results of security assessments performed by licensed laboratories.
  - U.S. National Institute of Standards (NIST) Security and Privacy Controls [4]
    - Used for specifying requirements for mission systems (typically including deployment configurations, operational procedures, and integration with other systems).
- Privacy criteria: no currently well-established approaches to "privacy engineering"
  - NIST's Intro to Privacy Engineering [5] defines three high-level privacy objectives and maps to the Fair Information Practice Principles (FIPPs).
  - FIPPs [6]: set of widely-recognized, high-level privacy principles.

Approach to developing criteria

- Define the system to be evaluated and assumptions about the technology infrastructure (e.g., platform software and hardware, storage systems, network) and operational environment.
- Identify realistic threats and justify them.
- Define the security objectives to counter the expected threats.
- Derive security requirements from the objectives.
  - Which must be addressed by the system under evaluation?
  - [Assumptions] Which are addressed by the technology infrastructure and other elements of the operational environment?
- Define privacy objectives and requirements.
- Recommendation: work collaboratively to develop common security/privacy requirements.
  - Identify requirements that could justify alterations to the emerging standards.
  - Create a security/privacy standard against which all your products/systems/services should be judged.

systems differ; focused on standard

focused on identity fraud

example objectives address identity fraud

requirements that highlight challenges for a government agency or that could suggest changes to the DID standards

Summary of Security and Privacy Objectives Addressed

- Security Objectives
  - Uniqueness
  - Integrity
  - Access control and access policy
  - Accountability
  - Non-repudiation
  - Availability and persistence
- Privacy Objectives
  - Predictability
  - Manageability
  - Disassociability

Expected assessment approaches for requirements

- Red: May be impossible to verify through assessment of the DID Method software and systems.
- Blue: Verifiable during onboarding (i.e., inspect software, operational configurations, administrative processes); may accept only those DID Methods that implement certain optional elements of the specification.
- Green: May be verifiable automatically by a resolver (e.g., table lookup, check a hash value).
- Brown: Not supported by current specification.

Example security objectives and requirements

DID uniqueness

- A DID Method SHALL generate unique method-specific identifiers.
- A DID SHALL resolve to a unique DID document, or the resolver SHALL return an error.
- A DID Method name SHALL be globally unique.

Integrity of DID-related data

- A DID Method SHALL apply tamper protections to DID-related data.
- A DID Method SHALL check DID-related data for evidence of tampering before completing operations. If evidence of tampering is found during a DID Method operation, the DID Method SHALL return an informative error message in response to the operation request.
- DID-related data includes:
  - DIDs
  - DID Documents
  - DID meta-data

Access control and access policy

- A DID Method SHALL ensure that only entities identified as controllers within a DID document can modify that DID document.
- A DID document SHALL explicitly define the extent of a DID controller's authority over specific elements of the DID document.
  - For example, some DID controllers are permitted to add a `verification method` and `verification relationship` and then modify or delete those same elements; other DID controllers are permitted to modify a `Service`.
  - This requires the development of a method for specifying DID controller authorizations within a DID document and a method for policy enforcement through DID Method operations.
- A DID Method SHALL enforce the security policies expressed in a DID document.

Accountability

- DID metadata SHALL include:
  - DID of the DID controller responsible for a DID update.
  - Timestamps applicable to the DID document, identified through the `created` or `updated` properties.
- DID Methods SHALL generate audit records for security-relevant events.
  - Audit records SHALL include at least: date and time of the event; type of event; identity of the subject (e.g., user identifier of a method user, platform-specific identifier of a site administrator, IP address associated with an external request); and outcome of the event.
- Integrity protection SHALL be applied to DID metadata and activity logs and their association with DID Method operations.

Non-repudiation of DID creation and DID document updates

- A request for DID creation SHALL NOT be processed until the DID subject (or legal custodian or guardian) provides external evidence of authorization.
  - Before a new DID/DID document is recorded, the system SHALL verify that an individual who is legally associated with the DID subject has taken an approval action external to the DID Method (e.g., the individual must browse to a web site and enter a PIN code that was delivered by postal mail).
- Any requested DID document updates that are not routine (e.g., key rotation) SHALL NOT be processed until a designated DID controller provides external evidence of authorization.
  - A designated DID controller SHALL be alerted to the requested update.
  - The system SHALL verify that the designated DID controller has taken an approval action external to the DID Method.
- The DID controller designation SHALL be made through a DID document security policy assertion

Availability of DID Method operations and persistence of DID-related data

- A DID Method operator SHALL specify the availability characteristics of its DID Method operations (Create, Resolve, Update, and Deactivate). This specification MAY be expressed through a service level agreement (SLA).
- A DID Method operator SHALL specify the persistence characteristics of DID-related data. This specification MAY be expressed through an SLA.
- DID-related data includes:
  - DIDs
  - DID Documents
  - DID meta-data

Privacy objectives (from NIST [4]) and example requirements

Predictability

- Predictability: enables reliable assumptions by individuals, owners, and operators about PII and its processing by an information system.
- A DID Method operator SHALL provide the capability for a DID controller to request a list of all types of PII maintained by the system and the entities that can view and/or modify each type.

Manageability

- Manageability: capability for granular administration of PII, including alteration, deletion, and selective disclosure.
- A DID Method operator SHALL provide the capability for a DID controller to request and confirm successful modification and/or deletion of PII from the system.

Disassociability

- Disassociability: enables the processing of PII or events without association to individuals or devices beyond the operational requirements of the system.
- The DID Method implementation, including storage systems for DIDs and DID documents SHALL NOT provide capabilities for general-purpose computing and SHALL NOT provide capabilities for other security-critical functions.
  - Platforms, storage systems, verifiable data registries, and other technologies used by DID Method implementations SHALL NOT also enable processing or storage of verifiable credentials.

Conclusion

- Development of security and privacy criteria will enable assessment standards for DID Method technologies (e.g., a DID Method Protection Profile) and services.
- Collaborative development of these criteria can help the DID technology community to:
  - Discuss, debate, and reach agreement on security and privacy fundamentals for DID technologies.
  - Identify requirements that could justify alterations to the emerging standards.
- Existing Common Criteria protection profiles [4] for security-critical systems such as certification authorities, enterprise identity and credential management systems, and electronic signature creation modules can serve as models for developing a DID Method protection profile.

Contact info

Deborah Shands, Ph.D.

Senior Computer Scientist, SRI International

Email: deborah.shands@sri.com

References

1. “Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5,” April 2017. https://commoncriteriaportal.org/cc/
2. Common Criteria Portal. https://commoncriteriaportal.org
3. National Information Assurance Partnership Approved Protection Profiles. https://www.niap-ccevs.org/Profile/PP.cfm
4. National Institute of Standards and Technology (NIST), “Security and Privacy Controls for Information Systems and Organizations, Revision 5, Special Publication 800-53,” September 2020. https://doi.org/10.6028/NIST.SP.800-53r5
5. National Institute of Standards and Technology (NIST), “An Introduction to Privacy Engineering and Risk Management in Federal Systems, Internal Report 8062,” January 2017. https://doi.org/10.6028/NIST.IR.8062
6. Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*, July 2016. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf

Homeland Security

Science and Technology

Thank You

Silicon Valley Innovation Program

DHS-Silicon-Valley@hq.dhs.gov
https://www.dhs.gov/science-and-technology/svip