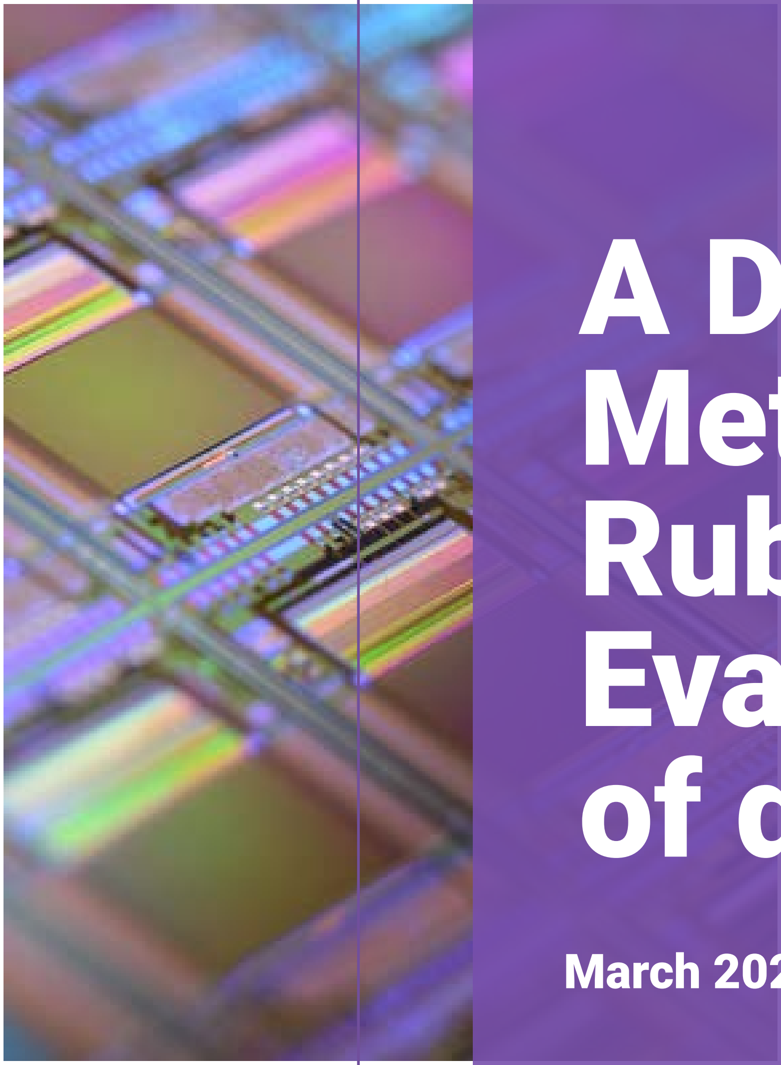


A DID Method Rubric Evaluation of did:v1

March 2022

This evaluation is based on the DID Method Rubric, published by the World Wide Web Consortium https://w3.org/TR/did-rubric

A DID Method Rubric Evaluation of did:v1

This evaluation was compiled in support of the Department of Homeland Security's 2021 and 2022 Silicon Valley Innovation Program.

Prepared by Legendary Requirements
http://legreq.com

EVALUATORS

Joe Andrieu joe@legreq.com
Eric Schuh eric@legreq.com

EVALUATION DATE

2022-03-01

Available at https://didevaluations.com/v1/2022-03-01

FUNDED BY

Digital Bazaar under DHS SVIP contract 70RSAT20T00000029.

COPYRIGHT

© 2022 Legendary Requirements, Inc. All rights reserved.

Use Cases Referenced

LABEL	NAME	DESCRIPTION
use-case-1	Long term verifiable credentials	The use of DIDs as subject identifiers for long term (life-long) verifiable credentials such as a digital Permanent Resident Card from the United States Citizens and Immigration Service.

Methods Evaluated

	SPECIFICATION	NETWORK	REGISTRY
did:v1.testnet	Veres One Testnet is the currently deployed test network for Veres One. It is completely under control of Digital Bazaar and should not be considered for production systems.		
	https://w3c-ccg.github.io/did-method-v1/	https://veres.one/network/	Same as network
did:v1.production	Future version of did:v1. Once Veres One goes into production, governance will be handed off to the Veres Foundation and the Veres Community Group (a W3C community group). These are forward looking statements for pro-forma evaluation of intended deployment.		
	https://w3c-ccg.github.io/did-method-v1/	https://veres.one/network/	Same as network

Contents

1

Rulemaking **5**

1.1 Open contribution (participation) 6

1.2 Transparency 7

1.3 Separation of Power 8

1.4 Decision Making Structures 10

1.5 Cost to introduce rule change 12

1.6 Cost to decide on rule changes 13

2

Design **14**

2.1 Cryptocurrency 15

2.2 Permissioned Operation 16

2.3 Interoperability 17

2.4 Scope of Usage 18

2.5 Offline creation 19

2.6 Update Scalability 20

2.7 Creation Cost 21

2.8 Update & Deletion Cost (out-of-pocket) 22

2.9 Update & Deletion Cost (in-kind) 23

3

Operation **24**

3.1 Financial accountability 25

3.2 Transactional Performance - Global Create Bandwidth 26

3.3 Transactional Performance - Global Update Bandwidth 27

3.4 Update Latency 28

3.5 Operational Reliability 29

3.6 Operational Security 30

4

Enforcement **31**

4.1 Auditability 32

4.2 Governance Jurisdiction 33

4.3 Operational Diversity 34

4.4 Registry Integrity 35

4.5 Operational Layers 36

4.6 Layer Diversity 38

4.7 Verification Relationships 39

4.8 Authentication Model 40

5

Adoption (and diversity) **41**

5.1 Financial Entanglements 42

5.2 Organizational Maturity in Time 43

5.3 Release Status 44

5.4 Maturity 45

6

Security **46**

6.1 Robust Crypto 47

6.2 Expert Review (cryptography) 48

6.3 Expert Review (consensus) 49

6.4 Availability 50

6.5 Provenance 51

6.6 United States Federal Compliance 52

1

Rule making

Rulemaking criteria address who makes the rules and how. Output of rulemaking are the rules.

In this section

1.1. Open contribution (participation)
1.2. Transparency
1.3. Separation of Power
1.4. Decision Making Structures
1.5. Cost to introduce rule change
1.6. Cost to decide on rule changes

1.1 Open contribution (participation)

https://www.w3.org/TR/did-rubric#criteria-1

QUESTION

How open is participation in governance decisions?

POSSIBLE RESPONSES

A Anyone can participate in an open, fair process where all participants have equal opportunity to be heard and influence decisions.

B Anyone can comment and contribute to open debate, but decisions are ultimately made by a closed group.

C Debate is restricted to a selected but known group.

D Debate is conducted in secret by an unknown group.

RELEVANCE

Governance determines how the rules of the underlying network are set and maintained. The more parties that are able to contribute to governance debates, the more decentralized the governance.

ASSESSMENT

	Method	Spec.	Net.	Reg.	Notes
a-1	did:v1. testnet	B	B	B	**Spec** (B), **Net** (B), and **Reg** (B): Created by Digital Bazaar and published on Github Github is open to the public and the spec is a CCG Work Item.
a-2	did:v1. production	A-	A-	A-	**Spec** (A-), **Net** (A-), and **Reg** (A-): The Veres One Community Group is open to participation by anyone and it will be taking over control of the specification. However, the Veres Foundation, which will handle operational control, is likely to have a disproportionate voice in the evolution of the specification, network, and registry.

1.2 Transparency

https://www.w3.org/TR/did-rubric#criteria-2

QUESTION

How visible are rulemaking processes?

POSSIBLE RESPONSES

A Agendas and participation details for all governance discussions are publicly announced, any meetings are broadcast in real-time to any listeners, and all minutes and recordings are captured in realtime and publicly reviewable in perpetuity.

B Minutes of meetings are reviewable by the public, including all votes and who cast them, but real-time observation may be limited.

C All current rules are publicly available.

D Rules may be changed without public notice.

RELEVANCE

While participation measures active contribution, transparency measures the visibility of discussions affecting rule making. If such discussions are only visible to a limited group, it centralizes decision making in ways that Evaluators and users cannot easily see.

ASSESSMENT

	Method	Spec.	Net.	Reg.	Notes
a-3	did:v1. testnet	D	D	D	**Spec** (D), **Net** (D), and **Reg** (D): Operations are not yet transferred to the foundation. Neither a schedule of meetings nor minutes from past meetings were available from Foundation's website.
a-4	did:v1. production	A-	A-	A-	**Spec** (A-), **Net** (A-), and **Reg** (A-): Once the production network is launched, all rule making becomes a matter of public discourse via the Veres One CG. However, decisions about which rules to adopt remain the purview of the Foundation and it is unknown whether or not the Foundation will operate its meetings in as open a fashion as the CG.

1.3 Separation of Power

http://didcriteria.com/criteria/1

QUESTION

What decision making bodies are involved in rulemaking?

POSSIBLE RESPONSES

List all of the deliberating bodies involved in setting or maintaining the method specification. Then, for each decision making body, evaluate criteria 1.4, 1.5, 1.6, and 4.2.

RELEVANCE

Rulemaking rarely occurs in simple structures. Identifying the different organizational entities that participate in setting rules allows evaluators to understand how rules get made. Understanding how rules get helps predict possible future developments.

It is worth noting that all entities who are beholden to sovereign states, which is pretty much all corporations, non-profits, and individuals, have consequences for violating the laws, regulations, and lawful court orders within their jurisdiction. Some decentralized systems go to great lengths to minimize the impact of possible coercion, including actions by nation states. It is understood that any participant in the process may be subject to the rule of law from any number of jurisdictions, e.g., patent law, employment law, financial reporting laws, dumping laws, zoning, environmental regulations, etc. As a result, all decision making bodies are subject to the jurisdictions in which they operate.

This complexity is true for all DID methods and, to our knowledge, most, if not all, DID methods have no intrinsic relationship to any particular jurisdiction. As such, we do not recommend including jurisdictional players, e.g., nation-states, cities, provinces, etc., as distinct operational layers, unless those players have a distinct role to play for that particular DID method.

ASSESSMENT

	Method	Decision Making Body	Notes
a-5	did:v1. testnet	Digital Bazaar	Digital Bazaar created Veres One and is shepherding it through development to production.
a-6	did:v1. production	Veres One Community Group	In production, the Veres One Community Group is the public-facing decision making body designed for discussing technical matters.
a-7	did:v1. production	Veres Foundation Board	The Veres Foundation holds responsibility for the financial and legal decisions necessary to keep the network operational.

SOURCE

New synthesis, in part from DID method Rubric v1.0.0 (draft)
https://www.w3.org/TR/did-rubric#criteria-5

1.4 Decision Making Structures

http://didcriteria.com/criteria/2

QUESTION

How is each decision making body structured?

Evaluate this criteria for each decision making body from 1.3.

POSSIBLE RESPONSES

Describe the governance structure of each decision making body.

A Individual. Sole proprietorship

B Informal Group. Unincorporated Partnership / Open Community

C For-profit formal organization. For-profit Corporation / LLC / Partnership

D Quasi not-for-profit formal organization
a. B-Corp https://bcorporation.net/
b. CIC https://en.wikipedia.org/wiki/Community_interest_company

E Recognized not-for-profit formal organization. Not-for-profit public benefit organization (NGOs, 501c(3/4/6), etc)
a. NGO
b. Trade Association
c. Charity

F Public agency (federal, state, or local)

G Other

RELEVANCE

Different governance structures have different implications for how decisions are made and who wields influence throughout the process.

ASSESSMENT

	Method	Decision Making Body	Governance Structure	Notes
a-8	did:v1. testnet	Digital Bazaar	C	Digital Bazaar is a closely held startup with a seventeen year track record. (C)
a-9	did:v1. production	Veres One Community Group	E	The Veres One Community Group is a community group operating under the rules of the World Wide Web Consortium. Open to the public, self-elected leadership (E)

a-10	did:v1. production	Veres Foundation Board	E	The Veres Foundation operates under the non-profit regulations of Ontario, Canada. Self-propagating board of directors overseeing a non-profit organization. (E)

SOURCE

New synthesis, in part from DID method Rubric v1.0.0 (draft)
https://www.w3.org/TR/did-rubric#criteria-5

1.5 Cost to introduce rule change

http://didcriteria.com/criteria/3

QUESTION

How expensive is it to get a governance decision before each of the deliberating bodies?

Evaluate this criteria for each decision making body from 1.3.

POSSIBLE RESPONSES

A	Free to all
B	Inexpensive, but accessible
C	Modest cost for interested parties
D	Expensive and restricted
E	Not possible to participate because the rules are immutable

RELEVANCE

Governance takes resources, which can limit the ability of interested parties to influence rulemaking. Generally, the more expensive it is to participate, the more governance centralizes to those parties most able to make the investment.

ASSESSMENT

	Method	Decision Making Body	Cost	Notes
a-11	did:v1. testnet	Digital Bazaar	D+	Digital Bazaar is a small development team working with select customers to define Veres One. There is no explicit mechanism for outside participation, however, the governance framework has been developed with high transparency through github and the W3C Veres One Community Group. (D+)
a-12	did:v1. production	Veres One Community Group	B	Community group is open to the public. Any member of the community group can propose changes to the method. Group consensus then determines which proposals advance to the Veres Foundation. (B)
a-13	did:v1. production	Veres Foundation Board	C-	For technical decisions, the Foundation strongly prefers proposals to reach consensus in the community group. For operational, financial, and legal decisions, the board will likely reserve the right to make decisions independent of the community group. Board bylaws are under development as of this evaluation. (C-)

SOURCE

New synthesis, in part from DID method Rubric v1.0.0 (draft)
https://www.w3.org/TR/did-rubric#criteria-5

1.6 Cost to decide on rule changes

http://didcriteria.com/criteria/4

QUESTION

How expensive is it to participate as a peer in a governance decision by the governing body?

Evaluate this criteria for each decision making body from 1.3.

POSSIBLE RESPONSES

A	Free to all
B	Inexpensive, but accessible
C	Modest cost for interested parties
D	Expensive and restricted
E	Not possible to participate because the rules are immutable

RELEVANCE

Governance takes resources, which can limit the ability of interested parties to influence rulemaking. Generally, the more expensive it is to participate, the more governance centralizes to those parties most able to make the investment.

ASSESSMENT

	Method	Decision Making Body	Cost	Notes
a-14	did:v1. testnet	Digital Bazaar	D	The most common way to be involved is by invitation from Digital Bazaar, either as an employee, subcontractor, or advisor. (D)
a-15	did:v1. production	Veres One Community Group	B	The largest cost is time to participate and a track record for credibility. (B)
a-16	did:v1. production	Veres Foundation Board	D	Foundation leadership is initially selected by Digital Bazaar and self-selecting thereafter. (D)

SOURCE

New synthesis, in part from DID method Rubric v1.0.0 (draft)
https://www.w3.org/TR/did-rubric#criteria-5

2

Design

In this section

2.1. Cryptocurrency
2.2. Permissioned Operation
2.3. Interoperability
2.4. Scope of Usage
2.5. Offline creation
2.6. Update Scalability
2.7. Creation Cost
2.8. Update & Deletion Cost (out-of-pocket)
2.9. Update & Deletion Cost (in-kind)

2.1 Cryptocurrency

http://didcriteria.com/criteria/5

QUESTION

What cryptocurrency, if any, is required for method operations?

POSSIBLE RESPONSES

A None

B At least one. [List the required crypto-currencies in the notes.]

RELEVANCE

The use of particular cryptocurrencies create a long term dependency on the viability of those currencies. Such dependency may be a deterrent for some applications. Similarly, if no cryptocurrency is used, there is likely a dependency elsewhere, such as on the organization managing consensus rules and operation.

ASSESSMENT

	Method	Spec.	Notes
a-17	did:v1. testnet	A	**Spec** (A): The V1 DID method operates on its own blockchain with a novel, non-cryptocurrency consensus algorithm.
a-18	did:v1. production	A	**Spec** (A): The V1 DID method operates on its own blockchain with a novel, non-cryptocurrency consensus algorithm.

2.2 Permissioned Operation

http://didcriteria.com/criteria/6

QUESTION

Does one need permission to use the DID method?

POSSIBLE RESPONSES

A Anyone can participate fully (full read/write and participation in consensus).

B Anyone can read/write, but consensus mechanism is permissioned.

C Anyone can read, but writing and consensus is permissioned.

D All participation is permissioned.

RELEVANCE

Permissioned operation impacts the availability of the network to various participants, which can affect inclusivity with regard to underserved or vulnerable populations. Permissioned networks also expose the permission giver to legal or other attacks.

ASSESSMENT

	Method	Net.	Reg.	Notes
a-19	did:v1. testnet	B+	B+	**Net** (B+) and **Reg** (B+)The ledger is available to the public for reading, and anyone can submit a transaction (either through paying an accelerator or in-kind contribution), however, only Witnesses are able to approve updates to the chain. The propagation rules of the peer network restrict the ability for Witnesses to selectively approve transactions, but ultimately, the decision remains with a supermajority of Witnesses.
a-20	did:v1. production	B+	B+	**Net** (B+) and **Reg** (B+)The ledger is available to the public for reading, and anyone can submit a transaction (either through paying an accelerator or in-kind contribution), however, only Witnesses are able to approve updates to the chain. The propagation rules of the peer network restrict the ability for Witnesses to selectively approve transactions, but ultimately, the decision remains with a supermajority of Witnesses.

SOURCE

Iterated from DID method Rubric v1.0.0 (draft) https://www.w3.org/TR/did-rubric#criteria-6.

2.3 Interoperability

https://www.w3.org/TR/did-rubric#criteria-7

QUESTION

Does the DID method restrict access or functionality to particular client software implementations?

POSSIBLE RESPONSES

- **A** Any wallet can work with any resolver on any registry.
- **B** Any wallet can work with multiple resolvers and multiple registries.
- **C** Some implementations of some wallets can work with some resolvers.
- **D** There is a single combined suite of resolver, registry, and wallet.

RELEVANCE

The ability to communicate with different (ideally all) resolvers and registries significantly increases the applicability of a decentralized identity layer / usability of a given wallet. Vice versa, limited capability to work with other methods and registries restrict usage.

ASSESSMENT

	Method	Spec.	Net.	Reg.	Notes
a-21	Did:v1. testnet	A	A	A	**Spec** (A), **Net** (A) and **Reg** (A): Veres One uses 100% W3C conformant representations, without regard to which wallet implementation is used.
a-22	did:v1. production	A	A	A	**Spec** (A), **Net** (A) and **Reg** (A): Veres One uses 100% W3C conformant representations, without regard to which wallet implementation is used.

2.4 Scope of Usage

https://www.w3.org/TR/did-rubric#criteria-8

QUESTION

How widely can DIDs of this method be used?

POSSIBLE RESPONSES

A Universal: DIDs can only be created and used universally, between any number of parties.

B Contextual: DIDs can be created and used contextually, between any set of collaborating parties.

C Paired: DID can be created and used pairwise, between any two parties.

D Central: DIDs can only be created and used with a single, centralized party.

RELEVANCE

Different methods enable different scopes in which a DID might be considered usable or valid. Some DIDs are only resolvable within a limited context, others are suitable for global use. Contextual DIDs are a middle ground that allow a set of parties to use DIDs, while those outside that group cannot meaningfully do so. Finally, central DIDs use the DID syntax and DID documents to establish secure communications, but authority to use these DIDs resides with the central party, who may revoke that ability at their discretion.

EVALUATION

	Method	Net.	Reg.	Notes
a-23	did:v1. testnet	A	A	Veres One DIDs are globally resolvable, without restriction, regardless of context.
a-24	did:v1. production	A	A	Veres One DIDs are globally resolvable, without restriction, regardless of context.

2.5 Offline creation

http://didcriteria.com/criteria/7

QUESTION

Does the method require network communications to create a DID?

POSSIBLE RESPONSES

A No. Creation is expected to be off-line. Only resolution, updates and deactivations require network or registry interaction.

B Yes. Creation requires network coordination with a single party to complete the DID creation.

C Yes. Creation requires network coordination with multiple parties in a known, constrained group to complete the DID creation.

D Yes. Creation requires network coordination with and acceptance by an open, global consensus system to complete DID creation.

RELEVANCE

Communication is costly, with increasing costs the more parties are involved. This cost is not just in terms of the connection expense, but also the latency in processing transactions. The ability to create a DID without registering it on a global shared state greatly reduces the technical and financial cost of the method.

ASSESSMENT

	Method	Spec.	Notes
a-25	did:v1. testnet	A	Veres One DID creation is a local cryptographic process. There is no network or registry involved.
a-26	did:v1. production	A	Veres One DID creation is a local cryptographic process. There is no network or registry involved.

2.6 Update Scalability

http://didcriteria.com/criteria/8

QUESTION

Assuming an average of no more than 1 update per quarter, how many DIDs can this method support?

POSSIBLE RESPONSES

A	Greater than 5 billion
B	Greater than 1 billion
C	Greater than 500 million
D	Greater than 50 million
E	Greater than 5 million
F	Less than 5 million

RELEVANCE

Some DID methods may be able to support the world's population, others may be more suitable to a particular type of use where only a small number of DIDs need to be supported. This gives a rough idea of the population base you may expect a particular DID method to support.

ASSESSMENT

	Method	Reg.	Notes
a-27	did:v1. testnet	C	Veres One can handle ~750 million updates per quarter at the current architecture of 13 witnesses running stock amazon instances. Performance can be improved through a variety of approaches with different cost and engineering tradeoffs.
a-28	did:v1. production	C	Veres One can handle ~750 million updates per quarter at the current architecture of 13 witnesses running stock amazon instances. Performance can be improved through a variety of approaches with different cost and engineering tradeoffs

2.7 Creation Cost

http://didcriteria.com/criteria/9

QUESTION

How much does it cost a DID creator to create a DID?

POSSIBLE RESPONSES

- **A** Only operational costs of running the algorithm (no externalized expense)
- **B** Less than $0.01
- **C** Less than $0.10
- **D** Less than $1
- **E** Less than $10
- **F** $10 or greater

RELEVANCE

Almost all operations are sensitive to the cost of creating the underlying identifiers. If such costs are close to zero, broad use of ephemeral keys is possible. As costs increase, it becomes more and more necessary to limit the number of identifiers created in order to keep systems.

ASSESSMENT

	Method	Reg.	Notes
a-29	did:v1. testnet	A	Creation is FREE
a-30	did:v1. production	A	Creation is FREE

2.8 Update & Deletion Cost (out-of-pocket)

http://didcriteria.com/criteria/10

QUESTION

How much does it cost*, out of pocket, to update or deactivate a DID document?

If the method has a tiered or variable cost structure, list all responses that apply and specify the cost structure in the notes. *This is the cost to the DID document controller.

POSSIBLE RESPONSES

A	Only operational costs of running the algorithm (no externalized expense)
B	Less than $0.01
C	Less than $0.10
D	Less than $1
E	Less than $10
F	$10 or greater

RELEVANCE

Depending on the method and governance, the price of updating and deleting a DID document will inform the cost of doing business with the particular method. Depending on the use case in mind this can be used, along with the scalability questions, to estimate the cost of maintaining a network using this DID method.

ASSESSMENT

	Method	Reg.	Notes
a-31	did:v1. testnet	n/a	Veres One Test Net does not have pricing.
a-32	did:v1. production	D/A	Veres One updates target a retail cost of ~$0.25, which will be set based on operational costs of the Veres Foundation, for wholesale pricing. Accelerators may mark up these prices based on their business model and approach. The estimates for these costs are currently under evaluation. Prices will also vary based on the size of the update, with larger updates costing more. (D) The costs and in-kind requirements will be managed by the Foundation based on market dynamics. (A)

2.9 Update & Deletion Cost (in-kind)

http://didcriteria.com/criteria/11

QUESTION

How much does it cost to update or deactivate a DID document using in-kind contributions?

POSSIBLE RESPONSES

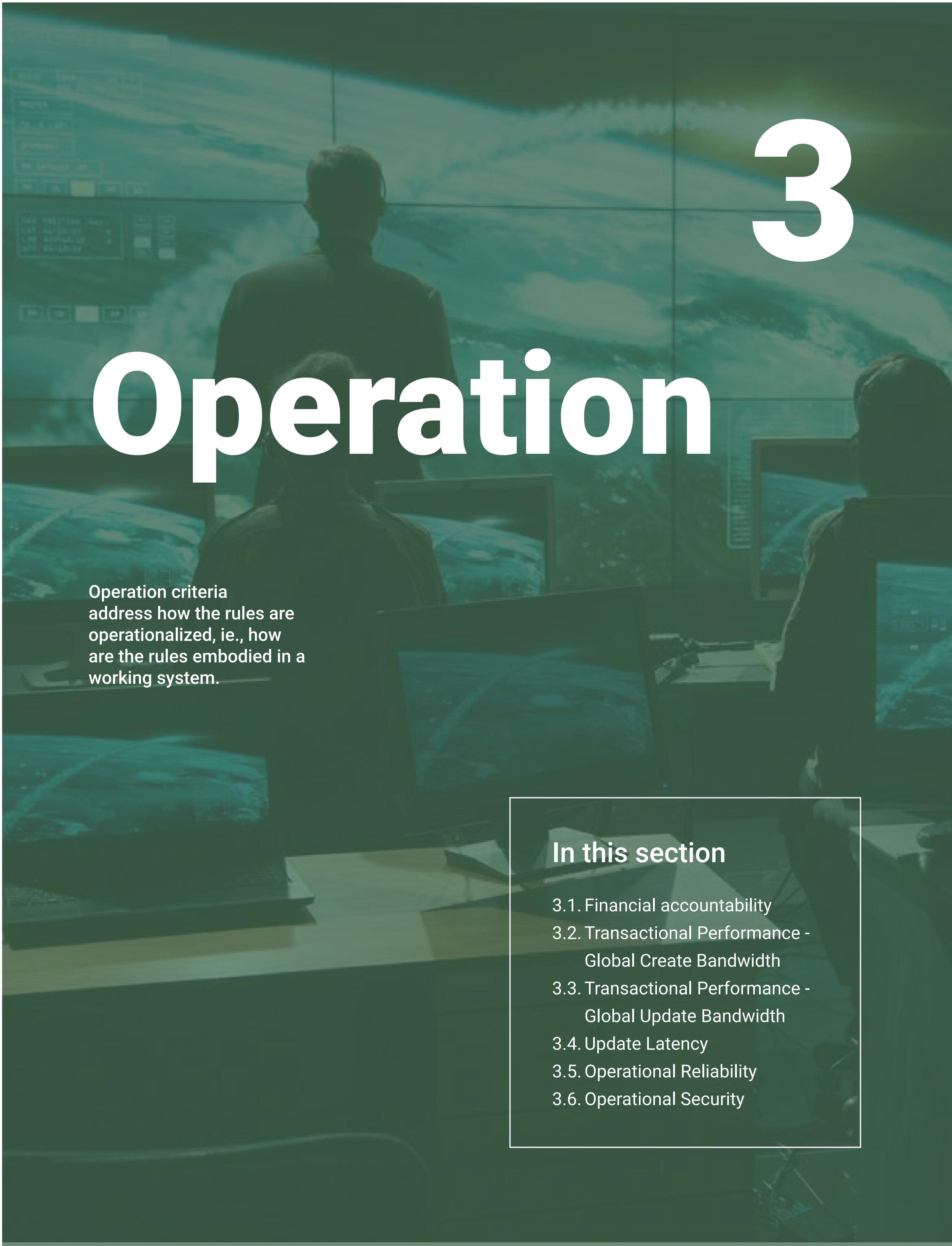
A	Only operational costs of running the algorithm (no externalized expense)
B	Less than $0.01
C	Less than $0.10
D	Less than $1
E	Less than $10
F	$10 or greater

RELEVANCE

Depending on the method and governance, there may be ways of reducing (or removing) the cost of updating or deleting a DID document, such as volunteering with the governance body or doing a set of work the network needs done.

ASSESSMENT

	Method	Reg.	Notes
a-33	did:v1. testnet	n/a	Veres One Testnet does not have pricing.
a-34	did:v1. production	B	The foundation-established cost can be earned by in-kind contributions, allowing hosted participants to post transactions without out-of-pocket expense. The amortized cost of this is expected to be less than “retail” but remain subject to several variables. For this evaluation, we estimate the in-kind costs for Veres One can be reduced to less than $0.01 per update, but ultimately this will be subject both to the foundation’s in-kind rules as well as the marginal cost of satisfying those rules.



3

Operation

Operation criteria address how the rules are operationalized, ie., how are the rules embodied in a working system.

In this section

3.1. Financial accountability

3.2. Transactional Performance - Global Create Bandwidth

3.3. Transactional Performance - Global Update Bandwidth

3.4. Update Latency

3.5. Operational Reliability

3.6. Operational Security

3.1 Financial accountability

http://didcriteria.com/criteria/12

QUESTION

How transparent are the economics of the method?

POSSIBLE RESPONSES

A All operational finances are transparent and accounted for.

B Compensation for primary operators is transparent.

C Some financial flows are visible.

D Operation is privatized with no visibility.

RELEVANCE

Similar to Governance criterion #3, financial accountability reflects the integrity and sustainability of the DID registry. The more open, transparent, and accountable the system, the greater the confidence a DID controller may have that it will remain stable and operational, and therefore continue to provide service.

ASSESSMENT

	Method	Net.	Reg.	Notes
a-35	did:v1. testnet	D	D	**Net** (D) and **Reg** (D): Pre-production operation is essentially in-house at Digital Bazaar.
a-36	did:v1. production	B	B	**Net** (B) and **Reg** (B): Once operations are transferred to the Foundation, finances should be considerably more transparent.

SOURCE

Iteration from DID method Rubric v1.0.0 (draft)
https://www.w3.org/TR/did-rubric#criteria-9

3.2 Transactional Performance - Global Create Bandwidth

http://didcriteria.com/criteria/13

QUESTION

How many DIDs of this method can be created per time period, globally?

POSSIBLE RESPONSES

Methods with offline creation should respond "n/a" to this question.

A	More than 1,000,000 Transactions Per Second
B	100,001 - 1,000,000 TPS
C	10,001 - 100,000 TPS
D	1,001 - 10,000 TPS
E	101 - 1,000 TPS
F	11 - 100 TPS
G	1-10 TPS
H	Less than 1 TPS

RELEVANCE

The number of new DIDs that can be created in a second inform the scalability of the network in regards to onboarding new users and allowing for new uses by existing users.

ASSESSMENT

	Method	Net.	Reg.	Notes
a-37	did:v1. testnet	n/a	n/a	**Net** (n/a) and **Reg** (n/a): Veres One DID creation is a local cryptographic process. There is no network or registry involved.
a-38	did:v1. production	n/a	n/a	**Net** (n/a) and **Reg** (n/a): Veres One DID creation is a local cryptographic process. There is no network or registry involved.

3.3 Transactional Performance - Global Update Bandwidth

http://didcriteria.com/criteria/14

QUESTION

How many DIDs can be updated per second, globally?

POSSIBLE RESPONSES

A	More than 1,000,000 Transactions Per Second
B	10,001 - 1,000,000 TPS
C	101 - 10,000 TPS
D	11 - 100 TPS
E	1-10 TPS
F	Less than 1 TPS

RELEVANCE

Along with creation, update performance of the registry can inform as to how many users make use of the method at any given time.

ASSESSMENT

	Method	Reg.	Notes
a-39	did:v1. testnet	C	Updates on Veres One have been demonstrated at >100 TPS. This could go considerably higher with various technical trade-offs.
a-40	did:v1. production	C	Updates on Veres One have been demonstrated at >100 TPS. This could go considerably higher with various technical trade-offs.

3.4 Update Latency

http://didcriteria.com/criteria/15

QUESTION

How much time does it take for an update to become globally available after submission by the DID controller?

POSSIBLE RESPONSES

A Less than 1 second

B 1 to < 60 seconds

C 1 to < 10 min

D 10 min to < 1 hour

E 1 hour to < 1 day

F 1 day to 2 weeks

G Greater than two weeks

H Updates not guaranteed

RELEVANCE

Different registry mechanisms have different guarantees for some notion of finality. The longer one has to wait for confirmation, the greater the latency for high security transactions. The shorter the duration, the more one has to critically validate the race conditions that may be present in determining finality. Depending on the algorithm, there are likely trade-offs between the stability of consensus and the speed at which consensus is pursued.

ASSESSMENT

	Method	Net.	Reg.	Notes
a-41	did:v1. testnet	B	B	**Net** (B) and **Reg** (B):Provable Finality for Veres One updates ranged from 1 to 60 seconds in testing (1-3 seconds in a single data center)
a-42	did:v1. production	B	B	**Net** (B) and ***Reg*** (B):Provable Finality for Veres One updates ranged from 1 to 60 seconds in testing (1-3 seconds in a single data center)

3.5 Operational Reliability

http://didcriteria.com/criteria/16

QUESTION

For each layer, how many operational components may be offline without that layer losing availability?

Evaluate with layers from 4.5 Operational Layers.

POSSIBLE RESPONSES

Fill in yourself.

Options might be:

- Equation based on the consensus algorithm
- Known number
- Percentage
- NONE (specific components MUST be operational)
- OPTIONAL (operations do not depend on the layer being available)

RELEVANCE

Along with the type of consensus algorithm the number of offline nodes has both security--i.e. DDOS attacks--and reliability implications.

ASSESSMENT

	Method	Layer	Response	Notes
a-43	did:v1. testnet	Witnesses	4	The Byzantine Fault Tolerant consensus algorithm used by Veres One requires a supermajority of 9/13 witness nodes to formulate consensus.
a-44	did:v1. testnet	Peers	N/A	Peer nodes are not needed in the formulation of consensus.
a-45	did:v1. production	Witnesses	4	The Byzantine Fault Tolerant consensus algorithm used by Veres One requires a supermajority of 9/13 witness nodes to formulate consensus.
a-46	did:v1. production	Peers	N/A	Peer nodes are not needed in the formulation of consensus.

3.6 Operational Security

http://didcriteria.com/criteria/17

QUESTION

How many operational components may be compromised without compromising the network?

Evaluate using the layers defined in 4.5 Operational Layers.

POSSIBLE RESPONSES

Fill in yourself. Options might be:

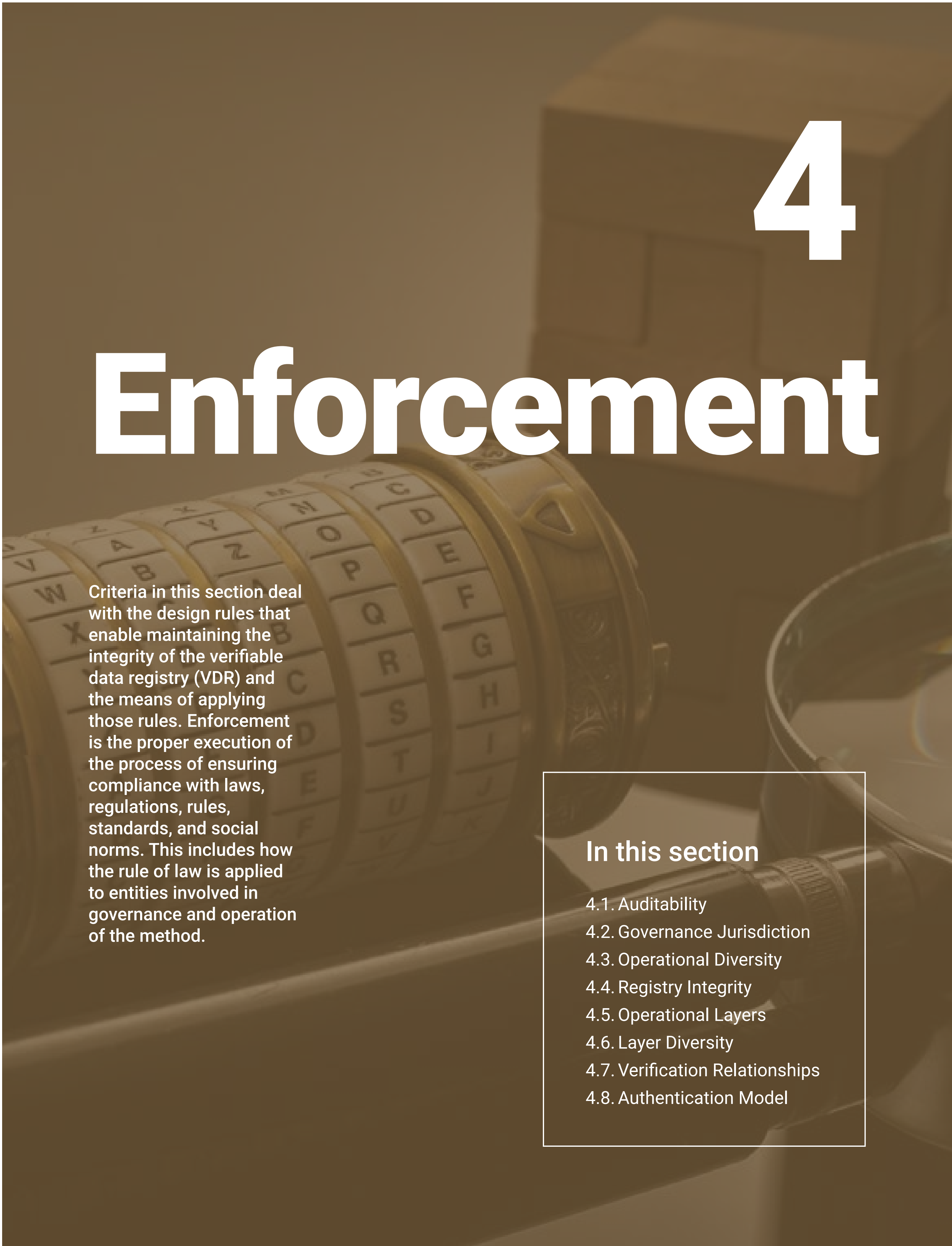
- Equation based on the consensus algorithm
- Known number
- Percentage
- Unknown
- N/A -- If the algorithm isn't dependent on the particular layer

RELEVANCE

Informs how easy it may be to orchestrate a take over of the network and get false transactions accepted by the consensus mechanism.

ASSESSMENT

	Method	Layer	Response	Notes
a-47	did:v1. testnet	Witnesses	4	Since a supermajority of 9/13 witness nodes is needed for consensus to be reached, compromising more than 4 of these nodes means an attacker could halt consensus formulation.
a-48	did:v1. testnet	Peers	N/A	Peers being compromised does not lead to network failure.
a-49	did:v1. production	Witnesses	4	Since a supermajority of 9/13 witness nodes is needed for consensus to be reached, compromising more than 4 of these nodes means an attacker could halt consensus formulation.
a-50	did:v1. production	Peers	N/A	Peers being compromised does not lead to network failure.



4

Enforcement

Criteria in this section deal with the design rules that enable maintaining the integrity of the verifiable data registry (VDR) and the means of applying those rules. Enforcement is the proper execution of the process of ensuring compliance with laws, regulations, rules, standards, and social norms. This includes how the rule of law is applied to entities involved in governance and operation of the method.

In this section

4.1. Auditability

4.2. Governance Jurisdiction

4.3. Operational Diversity

4.4. Registry Integrity

4.5. Operational Layers

4.6. Layer Diversity

4.7. Verification Relationships

4.8. Authentication Model

4.1 Auditability

https://www.w3.org/TR/did-rubric#criteria-12

QUESTION

Who can retrieve cryptographic proof of the history of changes to a given DID document?

POSSIBLE RESPONSES

- **A** Anyone
- **B** Only a select group, including parties not involved in a given DID transaction
- **C** Only parties to the transaction
- **D** Not available

RELEVANCE

Trustlessness is a prerequisite of a decentralized system. If you have to trust the source of a DID document (i.e., if you can't verify cryptographically a DID document that is returned from resolution), then you are at the mercy of a potentially centralized authority. If, instead, you have a cryptographic audit trail, then the current state of a DID cannot be compromised by an intermediary or central party.

ASSESSMENT

	Method	Reg.	Notes
a-51	did:v1. testnet	A	The Veres One ledger is publicly verifiable
a-52	did:v1. production	A	The Veres One ledger is publicly verifiable.

4.2 Governance Jurisdiction

http://didcriteria.com/criteria/18

QUESTION

In which jurisdiction is the governing body located?

Evaluate this criteria for each decision making body from 1.3.

POSSIBLE RESPONSES

Free text. The evaluator should provide the most relevant description of jurisdiction.

RELEVANCE

Different jurisdictions have different laws which may affect the operation of the method.

ASSESSMENT

	Method	Decision Making Body	Notes
a-53	did:v1. testnet	Digital Bazaar, Inc.	Digital Bazaar created Veres One. It is a corporation formed in the commonwealth of Virginia, USA.
a-54	did:v1. production	Veres One Community Group	In production, the Veres One Community Group is the public-facing decision making body designed for discussing technical matters. It operates under the auspices of the World Wide Web Consortium. The W3C does not have a single physical headquarters. There are four institutions that “host” W3C: MIT (in Cambridge, MA, USA), ERCIM (in Sophia-Antipolis, France), Keio University (near Tokyo, Japan), and Beihang University (in Beijing, China).
a-55	did:v1. production	Veres Foundation Board	The Veres Foundation holds responsibility for the financial and legal decisions necessary to keep the network operational. It is based in Ottawa, Canada.

4.3 Operational Diversity

http://didcriteria.com/criteria/19

QUESTION

How many independent legal entities currently maintain the operational integrity of the Verifiable Data Registry?

POSSIBLE RESPONSES

- **A** Open ended, unknown, or unknowable.
- **B** Capped. [State lower and upper bounds in Notes.]
- **C** One
- **D** Zero

RELEVANCE

Singular—or small numbers of—entities controlling the consensus of a network can orchestrate malicious attacks.

ASSESSMENT

	Method	Reg.	Notes
a-56	did:v1. testnet	B [13]	Veres One is designed for 13 Witnesses; only Witnesses are able to approve updates to the chain. The propagation rules of the peer network restrict the ability for Witnesses to selectively approve transactions, but ultimately, the decision remains with a supermajority of nine Witnesses.
a-57	did:v1. production	B [13]	Veres One is designed for 13 Witnesses; only Witnesses are able to approve updates to the chain. The propagation rules of the peer network restrict the ability for Witnesses to selectively approve transactions, but ultimately, the decision remains with a supermajority of nine Witnesses.

4.4 Registry Integrity

http://didcriteria.com/criteria/20

QUESTION

What type of integrity mechanism is used by the method's Verifiable Data Registry?

POSSIBLE RESPONSES

A	Proof of Work
B	Proof of Stake
C	Byzantine Fault Tolerant algorithm based
D	Electoral — Select parties vote with thresholds
E	Unanimous — All parties countersign
F	Unilateral — Latest signed version defined as authentic
G	Standards-based specifications determined by institutional authority, used by anyone
H	Other - Add your own

Note: For registries which use a hybrid of any of the above approaches, select the one that is the closest fit then either denote via slash—e.g. C/A for a hybrid Byzantine Fault Tolerant algorithm that utilizes POW at some layer—and describe in the notes at a high level how the consensus algorithm functions.

RELEVANCE

The consensus mechanism used by the method registry has implications for scalability, speed of operations, security and possibly environmental impact.

ASSESSMENT

	Method	Reg.	Notes
a-58	did:v1. testnet	C	There Veres One registry consensus algorithm uses a Byzantine Fault Tolerant algorithm which formulates consensus through a super majority of witness nodes with any number of peer nodes allowed to participate in the gossip network.
a-59	did:v1. production	C	There Veres One registry consensus algorithm uses a Byzantine Fault Tolerant algorithm which formulates consensus through a super majority of 13 witness nodes with any number of peer nodes allowed to participate in the gossip network.

4.5 Operational Layers

http://didcriteria.com/criteria/21

QUESTION

What layers of operational components establish and maintain integrity of the Verifiable Data Registry?

For each layer, evaluate criteria 3.5, 3.6, and 4.6.

POSSIBLE RESPONSES

A List each layer

RELEVANCE

The manner in which a Verifiable Data Registry (VDR) manages integrity defines how that integrity might be compromised. To understand how the VDR of a given method maintains integrity, this criteria identifies the operational components of the VDR for further evaluation in other criteria, namely 3.5, 3.6, and 4.6.

Unfortunately, network topology inevitably introduces parties that may be able to disrupt or compromise network interactions. For example, DNS servers--often under the control of the user's ISP or the corporate IT department--can return "fake" IP addresses; corporate firewalls can prevent traffic to or from certain addresses; corporate system administrators may prevent users from configuring alternative Certificate Authorities, even international internet traffic can be restricted or denied, purely at the network layer.

Because nearly every DID method known at this point depends on Internet-based networking, every DID method faces these same problems. As such, we don't recommend specifying common network components as distinct layers unless those layers have specific roles unique to the particular DID method.

For this criteria, we are talking about the operational components that have specific, unique, or privileged roles with regard to the evaluated DID method(s). The parties which fulfill said roles should be considered when evaluating the fitness of the given method(s).

ASSESSMENT

	Method	Layer	Notes
a-60	did:v1. testnet	Witnesses	In the test net the number of peer nodes is limited but the same number of witness nodes are used as in production.
a-61	did:v1. testnet	Peers	
a-62	did:v1. production	Witnesses	In production the number of peer nodes is expected to increase greatly.
a-63	did:v1. production	Peers	

4.6 Layer Diversity

http://didcriteria.com/criteria/22

QUESTION

How many operational components need to be compromised to compromise the verifiable data registry?

Evaluate with layers from 4.5 Operational Layers.

POSSIBLE RESPONSES

A Open ended, unknown, or unknowable.

B Capped. [State number in Notes]

C One

RELEVANCE

Depending on the type of integrity mechanism, the number of nodes that may fail without compromising the registries integrity has implications for security and reliability.

ASSESSMENT

	Method	Layer	Response	Notes
a-64	did:v1. testnet	Witnesses	B [4]	Veres One's consensus requires 9 of 13 witness nodes to agree, as such if more than 4 were compromised the network may cease to function. (B)
a-65	did:v1. testnet	Peers	A	Peer nodes are not directly involved in maintaining the verifiable data registry and only propagate state. As such compromising any number of peer nodes does not compromise the network. (A)
a-66	did:v1. production	Witnesses	B [4]	Veres One's consensus requires 9 of 13 witness nodes to agree, as such if more than 4 were compromised the network may cease to function. (B)
a-67	did:v1. production	Peers	A	Peer nodes are not directly involved in maintaining the verifiable data registry and only propagate state. As such compromising any number of peer nodes does not compromise the network. (A)

4.7 Verification Relationships

http://didcriteria.com/criteria/23

QUESTION

What verification relationships are supported by the method per specification?

POSSIBLE RESPONSES

Select all that are supported.

A	None
B	Authentication
C	AssertionMethod
D	Key Agreement
E	CapabilityInvocation
F	CapabilityDelegation
G	Other
H	Any

RELEVANCE

The verification relationships a method supports inform the ways in which DIDs of the method can be used. See section 5.3 of the Decentralized Identifiers specification for details on verification relationships. https://www.w3.org/TR/did-core/#verification-relationships

ASSESSMENT

	Method	Spec.	Notes
a-68	did:v1. testnet	H	The did.v1 specification does not have any restrictions to the Verification Relationships supported.
a-69	did:v1. production	H	The did.v1 specification does not have any restrictions to the Verification Relationships supported.

4.8 Authentication Model

http://didcriteria.com/criteria/24

QUESTION

How does the method authenticate a given DID operation as coming from the legitimate DID controller?

POSSIBLE RESPONSES

Include as many as apply to this method.

A	None
B	Cryptographically signed transactions
C	Cryptographic challenge string & signed response
D	Authenticator App
E	Biometrics
F	Email
G	DNS Record
H	HTML over HTTP
I	SMS/MMS
J	DID document update
K	Other
L	Any

RELEVANCE

The way in which DID updates are authenticated can have implications on not only the trustworthiness of the method but also informs someone who wants to use the method what they may need to implement technologically to properly make use of the method.

ASSESSMENT

	Method	Spec.	Notes
a-70	did:v1. testnet	B	Veres One makes use of signed cryptographic transactions secured by the Ed25519 cryptographic suite. (B)
a-71	did:v1. production	B	Veres One makes use of signed cryptographic transactions secured by the Ed25519 cryptographic suite. (B)

5

Adoption (and diversity)

Adoption criteria address how widely the method and its implementations are used by various parties and systems.

In this section

5.1. Financial Entanglements

5.2. Organizational Maturity in Time

5.3. Release Status

5.4. Maturity

5.1 Financial Entanglements

http://didcriteria.com/criteria/25

QUESTION

How was the method funded?

POSSIBLE RESPONSES

- **A** State-sponsored funding
- **B** Regulated not-for-profit entity
- **C** Private equity
- **D** Operational budget
- **E** Cryptocurrency
- **F** Tokenized Initial Coin Offering
- **G** Initial Public Offering (public equity funding)
- **H** Other -- State what in the notes

RELEVANCE

Funding can create financial entanglements. Those methods that depend on outside financing should be further evaluated to understand the potential consequences of funding to-date.

ASSESSMENT

	Method	Spec.	Net.	Reg.	Notes
a-72	did:v1. testnet	D	D	D	**Spec** (D), **Net** (D), and **Reg** (D): did:v1 was funded by Digital Bazaar through internal operational budgets.
a-73	did:v1. production	D	D	D	**Spec** (D), **Net** (D), and **Reg** (D): did:v1 was funded by Digital Bazaar through internal operational budgets.

5.2 Organizational Maturity in Time

http://didcriteria.com/criteria/26

QUESTION

How long has the organization(s) behind the method been operational?

POSSIBLE RESPONSES

A	Over 20 years
B	Over 10 years
C	Over 5 years
D	Over 1 year
E	Less than 1 year
F	There is no organization per se

RELEVANCE

The age of the organization(s) behind a method can be used to give an idea into organizational maturity. It is not a sole indicator and should be taken as a data point in evaluating the method organization's current state.

ASSESSMENT

	Method	Spec.	Net.	Reg.	Notes
a-74	did:v1. testnet	B	D	D	**Spec**: Digital Bazaar, the team behind the spec has been in business for over 17 years. (B) **Net** (D) and **Reg** (D): The Veres One Foundation was founded in 2019.
a-75	did:v1. production	B	D	D	**Spec**: Digital Bazaar, the team behind the spec has been in business for over 17 years. (B) **Net** (D) and **Reg** (D): The Veres One Foundation was founded in 2019.

5.3 Release Status

http://didcriteria.com/criteria/27

QUESTION

Can the method be used for production today?

POSSIBLE RESPONSES

A A. Yes. A production system is available to the general population.

B B. No. A test network is operational.

C C. No. Only an internal developer network is operational.

D D. No. The software is not yet running on any network.

RELEVANCE

Some errors only become apparent after sufficient time to test edge cases and performance boundaries.

ASSESSMENT

	Method	Net.	Reg.	Notes
a-76	did:v1. testnet	B	B	**Net** (B) and **Reg** (B): The Veres One test network has been operational for over 3 years, in three major release iterations. It is not yet in production.
a-77	did:v1. production	B	B	**Net** (B) and **Reg** (B): The Veres One test network has been operational for over 3 years, in three major release iterations. It is not yet in production.

5.4 Maturity

http://didcriteria.com/criteria/28

QUESTION

How long has the underlying network/registry been available to third parties for non-trivial use?

POSSIBLE RESPONSES

- **A** The network/registry has been operationalized for ten years or more.
- **B** The network/registry has been operationalized for five years or more
- **C** The network/registry has been operationalized for one year or more
- **D** The network/registry has been operationalized for less than one year
- **E** The network/registry is not operationalized for non-trivial use

RELEVANCE

Some errors only become apparent after sufficient time to test edge cases and performance boundaries.

ASSESSMENT

	Method	Net.	Reg.	Notes
a-78	did:v1. testnet	C	C	**Net** (C) and **Reg** (C): The Veres One test network has been operational for over 3 years in three major release iterations.
a-79	did:v1. production	E	E	**Net** (E) and **Reg** (E): The Veres One production network has not yet been released.

6

Security

Security criteria address how the method is cryptographically secured.

In this section

6.1. Robust Crypto
6.2. Expert Review (cryptography)
6.3. Expert Review (consensus)
6.4. Availability
6.5. Provenance
6.6. United States Federal Compliance

6.1 Robust Crypto

https://www.w3.org/TR/did-rubric#criteria-24

QUESTION

What is the lowest security level (“bits of security”) allowed in the processes that ensure integrity of the verifiable data registry?

https://en.wikipedia.org/wiki/Security_level

POSSIBLE RESPONSES

A No combination of required features produces a profile with less than 256 bits of security.

B Less than 128 bits

C Less than 128 bits

D Less than 64 bits

RELEVANCE

A DID method that requires implementations to support something weak (e.g., 1024-bit RSA) is guaranteeing that its users will cooperate by default with encryption that’s relatively easy to crack, with hashing that’s not adequately collision-resistant, etc.

ASSESSMENT

	Method	Reg.	Notes
a-80	did:v1. testnet	A	Veres One uses the Ed25519 public key cryptography scheme(256-bit) to perform all digital signatures. It also uses the SHA-256 hashing algorithm with 256-bits of output to perform all hashing operations performed by the blockchain. (A)
a-81	did:v1. production	A	Veres One uses the Ed25519 public key cryptography scheme(256-bit) to perform all digital signatures. It also uses the SHA-256 hashing algorithm with 256-bits of output to perform all hashing operations performed by the blockchain. (A)

6.2 Expert Review (Cryptography)

https://www.w3.org/TR/did-rubric#criteria-25

QUESTION

Does the system use cryptographic and security primitives that are well vetted by technical experts, and battle hardened in the school of experience?

POSSIBLE RESPONSES

A Experts generally consider the system very secure, and this opinion is reinforced by a track record of secure production use.

B The theoretical security of the system looks excellent, and no known attacks or substantive criticisms are unaddressed. However, limited review or limited experience informs the opinion.

C Credible reports of vulnerabilities or design shortcomings have not been addressed.

D The system actively uses mechanisms that are officially deprecated.

E The system uses mechanisms that have not been vetted.

RELEVANCE

Exotic crypto and other security mechanisms without expert review and a production track record is likely to contain hidden risks.

ASSESSMENT

	Method	Reg.	Notes
a-82	did:v1. testnet	A	Ed25519 and SHA256 are highly regarded cryptographic algorithms and are the only cryptographic primitives used in Veres One. (A)
a-83	did:v1. production	A	Ed25519 and SHA256 are highly regarded cryptographic algorithms and are the only cryptographic primitives used in Veres One. (A)

6.3 Expert Review (Consensus)

http://didcriteria.com/criteria/29

QUESTION

If the method makes use of a distributed consensus mechanism, has the registry's consensus mechanism undergone sufficient review?

POSSIBLE RESPONSES

A Yes. A formal proof has been published in a peer reviewed journal.

B Yes. A formal proof has been published.

C No. An informal argument has been published.

D No. The consensus algorithm is opaque to registry users.

RELEVANCE

Decentralized systems are notoriously difficult to get right. Consensus ordering, in particular, is known to be a hard problem solved by distributed ledgers. Even simpler registries may trade off provable finality with probabilistic finality. It is vital that the method used for high-value or life-critical application be rigorously evaluated for potential flaws.

ASSESSMENT

	Method	Net.	Reg.	Notes
a-84	did:v1. testnet	B	B	**Net** (B) and **Reg** (B): Mathematical proofs have been peer reviewed for publication in a not-yet-published book on consensus algorithms and as a special IEEE journal publication on network consensus algorithms.
a-85	did:v1. production	B	B	**Net** (B) and **Reg** (B): Mathematical proofs have been peer reviewed for publication in a not-yet-published book on consensus algorithms and as a special IEEE journal publication on network consensus algorithms.

6.4 Availability

https://www.w3.org/TR/did-rubric#criteria-28

QUESTION

How robust are protections against attempts to suppress information flow, whether legal (cease and desist) or technical (denial of service)?

POSSIBLE RESPONSES

A The VDR is practically immune from this risk.

B The VDR has reasonable protections in place. However, motivated and well resourced attackers could temporarily disrupt access in a targeted context.

C Attackers could permanently disrupt access in a targeted context.

RELEVANCE

Control over an identifier is far less valuable if the propagation of that control can be limited by someone else.

ASSESSMENT

	Method	Reg.	Notes
a-86	did:v1. testnet	B	Veres One is operated by known parties; if all such parties are attacked, especially via legal means, the network could be shut down or additional rules applied. However, no single party can deny the consensus process. Like any publicly accessible service, Veres One is subject to distributed denial of service attacks. Counter measures are in place, but cannot be 100% ameliorated. (B)
a-87	did:v1. production	B	Veres One is operated by known parties; if all such parties are attacked, especially via legal means, the network could be shut down or additional rules applied. However, no single party can deny the consensus process. Like any publicly accessible service, Veres One is subject to distributed denial of service attacks. Counter measures are in place, but cannot be 100% ameliorated. (B)

6.5 Provenance

https://www.w3.org/TR/did-rubric#criteria-29

QUESTION

Is the current state of a DID document provably correct from a history that's visible to anyone who can resolve the DID?

POSSIBLE RESPONSES

A The update history of the DID document is recorded, accessible, and linked appropriately to its predecessor. Arbitrary versions can be queried and proved correct, and they have a reasonably useful timestamp.

B The update history of the DID document exists, and a forensic analysis could prove correctness. However, it's not exposed for consumption of ordinary resolvers, it lacks supporting metadata, or it's exposed in a very suboptimal way.

C Limited evidence of proper DID document updates exists.

D No evidence of proper DID document updates exist; the user has to trust the system's assertion that the current state resulted from something appropriate.

RELEVANCE

It's possible to tamper with systems that don't actively prove the correctness of their current state. Such tampering is not easy to discover.

ASSESSMENT

	Method	Reg.	Notes
a-88	did:v1. testnet	A	All document updates are recorded in a non-repudiable manner on the Veres One Ledger.
a-89	did:v1. production	A	All document updates are recorded in a non-repudiable manner on the Veres One Ledger.

6.6 United States Federal Compliance

http://didcriteria.com/criteria/30

QUESTION

Is the Method compliant with US Federal requirements for the use of cryptography?

POSSIBLE RESPONSES

A A. Both registry consensus *and* transaction validation are compliant

B B. Transaction validation is compliant but consensus is not

C C. No. Neither consensus nor transactions are compliant

RELEVANCE

Many US Federal programs and projects require use of cryptography according to standards set by the National Institute of Standards and Technology (NIST), such as:

- FIPS 186-5 (https://csrc.nist.gov/publications/detail/fips/186/5/draft)
- NIST 800-131Ar2 (https://csrc.nist.gov/publications/detail/sp/800-131a/rev-2/final)
- SP 800-186 (https://csrc.nist.gov/publications/detail/sp/800-186/draft)
- NIST FIPS 186-4 (https://csrc.nist.gov/publications/detail/fips/186/4/final)
- NIST 800-38D (https://csrc.nist.gov/publications/detail/sp/800-38d/final)
- NIST 800-38F (https://csrc.nist.gov/publications/detail/sp/800-38f/final)
- FIPS 180-4 (https://csrc.nist.gov/publications/detail/fips/180/4/final)
- FIPS 800-107r1. (https://csrc.nist.gov/publications/detail/sp/800-107/rev-1/final)

ASSESSMENT

	Method	Spec.	Net.	Reg.	Notes
a-90	did:v1. testnet	A	A	A	**Spec** (A), **Net** (A), and **Reg** (A): did:v1 was written to be compatible with all NIST requirements, including those specified in the Relevance section (6.8.3)
a-91	did:v1. production	A	A	A	**Spec** (A), **Net** (A), and **Reg** (A): did:v1 was written to be compatible with all NIST requirements, including those specified in the Relevance section (6.8.3)

LEGENDARY
REQUIREMENTS

legreq.com