A Rubric Evaluation of Veres One *DRAFT*

This evaluation of Veres One is compiled for the Department of Homeland Security's 2021 Silicon Valley Innovation Program.

Rubric Evaluation			
Evaluators	Joe Andrieu <joe@legreq.com>, Eric Schuh <eric@legreq.com>		
Evaluation Date	2021-04-20		
Funding	Funded by Digital Bazaar under DHS SVIP contract 70RSAT20T00000029.		
Use Cases	**Long term verifiable credentials.** The use of DIDs as subject and identifiers for long term (life-long) verifiable credentials such as a digital Permanent Resident Card from the United States Citizens and Immigration Service.		
Report URL	http://legreq.com/media/v1.rubric.2021.04.20		
Methods Evaluated			
	Specification	**Network**	**Registry**
did:v1.testnet	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.		
Criteria Sources			
Veres One Rationale Presentation	https://docs.google.com/presentation/d/1jOozLjbdepazamhtKld69bDi-kmuUddBFBjbjoap7P4/edit#slide=id.g9fc1a283da_1_87		
DID Method Rubric v1.0.0	https://w3c.github.io/did-rubric		

THE CRITERIA

1 Rulemaking

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

1.1 Open contribution (participation)

1.1.1 Question

How open is participation in governance decisions?

1.1.2 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.

1.1.3 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.

1.1.4 Evaluation

Method	Spec.	Net.	Reg.	Notes.
did:v1.testnet	B	B	B	Spec was created by Digital Bazaar, network and registry rules are managed by the Veres One Foundation Github is open to the public and the spec is a CCG Work Item.
did:v1.production	A-	A-	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.

1.1.5 Source

DID Method Rubric v1.0.0 (draft) §2.1.1
https://w3c.github.io/did-rubric/#open-contribution-participation

1.2 Transparency

1.2.1 Question

How visible are rulemaking processes?

1.2.2 Possible Responses

A. Agendas and participation details for all meetings are publicly announced, the 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.

1.2.3 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.

1.2.4 Evaluation

Method	Spec.	Net.	Reg.	Notes
did:v1. testnet	D	D	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.
did:v1. production	A-	A-	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.

1.2.5 Source

DID Method Rubric §https://w3c.github.io/did-rubric/#transparency

1.3 Separation of Power

1.3.1 Question

What deliberating bodies are involved in rulemaking?

1.3.2 Possible Responses

List all of the deliberating bodies involved in setting or maintaining the Method specification. Then, for each deliberative body, evaluate criteria 1.4, 1.5, 1.6, and 4.3.

1.3.3 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.

1.3.4 Evaluation

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

1.3.5 Source

New synthesis, in part from DID Method Rubric v1.0.0 (draft) §https://w3c.github.io/did-rubric/#cost

1.4 Deliberation Mechanisms

Evaluate this criteria for each deliberative body from 1.3.

1.4.1 Question

How is each deliberative body structured?

1.4.2 Possible Responses

Describe the governance structure of each deliberative body.

1.4.3 Relevance

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

1.4.4 Evaluation

Method	Deliberating Body	Governance Structure	Notes
did:v1.testnet	Digital Bazaar	For-profit business	Digital Bazaar is a closely held startup with a seventeen year track record.
did:v1.production	Veres One Community Group	W3C Community Group, open to the public, self-elected leadership.	The Veres One Community Group is a community group operating under the rules of the World Wide Web Consortium.
did:v1.production	Veres Foundation Board	Self-propagating board of directors overseeing a non-profit organization.	The Veres Foundation operates under the non-profit regulations of Ontario, Canada.

1.4.5 Source

New synthesis, in part from DID Method Rubric v1.0.0 (draft) §https://w3c.github.io/did-rubric/#cost

1.5 Cost to introduce rule change

Evaluate this criteria for each deliberative body from 1.3.

1.5.1 Question

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

1.5.2 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

1.5.3 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.

1.5.4 Evaluation

Method	Deliberating Body	Cost	Notes
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.
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.
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.

1.5.5 Source

New synthesis, in part from DID Method Rubric v1.0.0 (draft) §https://w3c.github.io/did-rubric/#cost

1.6 Cost to decide on rule changes

Evaluate this criteria for each deliberative body from 1.3.

1.6.1 Question

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

1.6.2 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

1.6.3 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.

1.6.4 Evaluation

Method	Deliberating Body	Cost	Notes
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.
did:v1.production	Veres One Community Group	B	The largest cost is time to participate and a track record for credibility.
did:v1.production	Veres Foundation Board	D	Foundation leadership is initially selected by Digital Bazaar and self-selecting thereafter.

1.6.5 Source

New synthesis, in part from DID Method Rubric v1.0.0 (draft) §https://w3c.github.io/did-rubric/#cost

2 Design

2.1 Cryptocurrency

2.1.1 Question

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

2.1.2 Possible Responses

A. None
B. [List of currencies]

2.1.3 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.

2.1.4 Evaluation

Method	Spec.	Net.	Reg.	Notes.
did:v1. testnet	A	A	A	The V1 DID Method operates on its own blockchain with a novel, non-cryptocurrency consensus algorithm.
did:v1. production	A	A	A	No change between did:v1.testnet and did:v1.production

2.1.5 Source

Derived from Veres One Rationale Presentation

2.2 Permissioned Operation

2.2.1 Question

Does one need permission to use the DID Method?

2.2.2 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.

2.2.3 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.

2.2.4 Evaluation

Method	Net.	Reg.	Notes
did:v1.testnet	B+	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.
did:v1.production	B+	B+	Same as did:v1.testnet

2.2.5 Source

Iterated from DID Method Rubric v1.0.0 (draft)
§https://w3c.github.io/did-rubric/#permissioned-operation

2.3 Interoperability

2.3.1 Question

Does the DID Method restrict access or functionality to particular wallet implementations per the specification?

2.3.2 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.

2.3.3 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.

2.3.4 Evaluation

Method	Net.	Reg.	Notes
Did:v1. testnet	A	A	Veres One uses 100% W3C conformant representations, without regard to which wallet implementation is used.
did:v1. production	A	A	No change between did:v1.testnet and did:v1.production

2.3.5 Source

DID Method Rubric v1.0.0 (draft) §https://w3c.github.io/did-rubric/#interoperability

2.4 Scope of Usage

2.4.1 Question

How widely can DIDs of this Method be used?

2.4.2 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.

2.4.3 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.

2.4.4 Evaluation

Method	Net.	Reg.	Notes
did:v1. testnet	A	A	Veres One DIDs are globally resolvable, without restriction, regardless of context.
did:v1. production	A	A	No change between did:v1.testnet and did:v1.production

2.4.5 Source

DID Method Rubric v1.0.0 (draft) §https://w3c.github.io/did-rubric/#scope-of-usage

2.5 Off-ledger creation

2.5.1 Question

Does the Method require network communications to create a DID?

2.5.2 Possible Responses

A. No. Creation is entirely off-line. Only updates and deactivations require network or registry interaction
B. Yes. Creation requires network communication with a single party, but not consensus
C. Yes. Creation requires network coordination with multiple parties in a constrained group
D. Yes. Creation requires global consensus

2.5.3 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.

2.5.4 Evaluation

Method	Spec.	Net.	Reg.	Notes.
did:v1.testnet	A	n/a	n/a	Veres One DID creation is a local cryptographic process. There is no network or registry involved.
did:v1.production	A	n/a	n/a	Same as did:v1.testnet

2.5.5 Source

Derived from Veres One Rationale Presentation

2.6 Update Scalability

2.6.1 Question

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

2.6.2 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

2.6.3 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.

2.6.4 Evaluation

Method	Reg.	Notes
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.
did:v1. production	C	Same as did:v1.testnet

2.6.5 Source

Derived from Veres One Rationale Presentation

2.7 Creation Cost

2.7.1 Question

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

2.7.2 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

2.7.3 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.

2.7.4 Evaluation

Method	Reg.	Notes
did:v1. testnet	A	Creation is FREE
did:v1. production	A	Same as did:v1.test.net

2.7.5 Source

Derived from Veres One Rationale Presentation

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

2.8.1 Question

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

2.8.2 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

2.8.3 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.

2.8.4 Evaluation

Method	Reg.	Notes
did:v1. testnet	n/a	Veres One Test Net does not have pricing.
did:v1. production	D	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 is currently under evaluation. Prices will also vary based on the size of the update, with larger updates costing more. The costs and in-kind requirements will be managed by the Foundation based on market dynamics.

2.8.5 Source

Derived from Veres One Rationale Presentation

2.9 Update & Deletion Cost (in-kind)

2.9.1 Question

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

2.9.2 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

2.9.3 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.

2.9.4 Evaluation

Method	Reg.	Notes
did:v1.testnet	n/a	Veres One Testnet does not have pricing.
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.

2.9.5 Source

Derived from Veres One Rationale Presentation

3 Operation

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

3.1 Financial accountability

3.1.1 Question

How transparent are the economics of the Method?

3.1.2 Answers

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.

3.1.3 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.

3.1.4 Evaluation

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

3.1.5 Source

Iteration from DID Method Rubric v1.0.0 (draft)
§https://w3c.github.io/did-rubric/#financial-accountability

3.2 Transactional Performance - Global Create Bandwidth

3.2.1 Question

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

3.2.2 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

3.2.3 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.

3.2.4 Evaluation

Method	Spec.	Net.	Reg.	Notes.
did:v1.testnet	n/a	n/a	n/a	Veres One DID creation is a local cryptographic process. There is no network or registry involved.
did:v1.production	n/a	n/a	n/a	No change between did:v1.testnet and did:v1.production

3.2.5 Source

Derived from Veres One Rationale Presentation

3.3 Transactional Performance - Local Create Bandwidth

3.3.1 Question

How many DIDs of this method can be created per time period, on a single device using the Method's best reference implementation? Reference device is Microsoft Azure Standard_D8as_v4 8vCPUs, 32 GiB RAM, and 1024 GiB Disk.

3.3.2 Possible Responses

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

3.3.3 Relevance

In high volume or low-processor applications, it is vital to be able to estimate how many resource DID creation requires. In some cases, a single local device can serve an entire enterprise deployment. In other situations, multiple servers may be required to meet demand. This criteria uses a stock Amazon Web Services instance to calibrate computational requirements across different methods.

3.3.4 Evaluation

Method	Spec.	Net.	Reg.	Notes.
did:v1. testnet	D	D	D	2,850 DID Creations/sec
did:v1. production	D	D	D	No change between did:v1.testnet and did:v1.production

3.3.5 Source

Derived from Veres One Rationale Presentation

3.4 Transactional Performance -- Update

3.4.1 Question

How many DIDs can be updated per unit time?

3.4.2 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

3.4.3 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.

3.4.4 Evaluation

Method	Reg.	Notes
did:v1. testnet	C	Updates on Veres One have been demonstrated at >100 TPS. This could go considerably higher with various technical trade-offs.
did:v1. production	C	No change between did:v1.testnet and did:v1.production

3.4.5 Source

Derived from Veres One Rationale Presentation

3.5 Update Latency

3.5.1 Question

How long does it take until updates are authoritatively final?

3.5.2 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

3.5.3 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.

3.5.4 Evaluation

Method	Net	Reg	Notes
did:v1. testnet	B	B	Provable Finality for Veres One updates ranged from 1 to 60 seconds in testing (1-3 seconds in a single data center)
did:v1. production	B	B	No change between did:v1.testnet and did:v1.production

3.5.5 Source

Derived from Veres One Rationale Presentation

3.6 Operational Reliability

Evaluate with layers from 4.6 Consensus Layers.

3.6.1 Question

How many nodes may be offline without compromising the network?

3.6.2 Possible Responses

Fill in yourself. Options might be:

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

3.6.3 Relevance

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

3.6.4 Evaluation

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

3.6.5 Source

Derived from Veres One Rationale Presentation

3.7 Operational Security

Evaluate using the layers defined in 4.6 Consensus Layers.

3.7.1 Question

How many nodes may be compromised without compromising the network?

3.7.2 Possible Responses

Fill in yourself. Options might be:

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

3.7.3 Relevance

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

3.7.4 Evaluation

Method	Layer	Response	Notes
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.
did:v1. testnet	Peers	50%-1	If half or more of the peer nodes have been compromised an attacker could convince a supermajority of witnesses to accept their transactions.
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.
did:v1. production	Peers	50%-1	If half or more of the peer nodes have been compromised an attacker could convince a supermajority of witnesses to accept their transactions.

3.7.5 Source

Derived from Veres One Rationale Presentation

4. Enforcement

4.1 Auditability

4.1.1 Question

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

4.1.2 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

4.1.3 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.

4.1.4 Evaluation

Method	Reg.	Notes
did:v1. testnet	A	The Veres One ledger is publicly verifiable.
did:v1. production	A	No change between did:v1.testnet and did:v1.production

4.1.5 Source

DID Method Rubric v1.0.0 (draft) §https://w3c.github.io/did-rubric/#auditability

4.2 Proof of Control

4.2.1 Question

How can one prove control over DIDs of the Method?

4.2.2 Possible Responses

A. Cryptographic challenge string & signed response
B. Authenticator App
C. Biometrics
D. Email
E. DNS Record
F. HTML over HTTP
G. SMS/MMS
H. DID Document update
I. Other

4.2.3 Relevance

The ability to change a DID Document implies the permission to do so. How is this permission determined? Cryptographic proof of control is typical for crypto-currency-based Methods, but other means may be employed.

4.2.4 Evaluation

Method	Spec.	Notes
did:v1. testnet	A	Veres One requires a signed challenge string, using private key material associated with the DID.
did:v1. production	A	No change between did:v1.testnet and did:v1.production

4.2.5 Source

Derived from Veres One Rationale Presentation

4.3 Governance Jurisdiction

4.3.1 Question

In which jurisdiction is the governing body located?

4.3.2 Possible Responses

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

4.3.3 Relevance

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

4.3.4 Evaluation

Method	Deliberating Body	Notes
did:v1.testnet	Digital Bazaar, Inc.	Digital Bazaar created Veres One. It is a corporation formed in the commonwealth of Virginia, USA.
did:v1.production	Veres One Community Group	In production, the Veres One Community Group is the public-facing deliberative 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).
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.

4.3.5 Source

Derived from Veres One Rationale Presentation

4.4 Operational Diversity

4.4.1 Question

How many independent legal entities determine consensus?

4.4.2 Possible Responses

A. Open ended. Currently estimated at greater than 1 million
B. Over 100,000
C. Over 10,000
D. Over 1,000
E. Over 100
F. Over 10
G. Less than 10

4.4.3 Relevance

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

4.4.4 Evaluation

Method	Reg.	Notes
did:v1. testnet	F	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 Witnesses.
did:v1. production	F	No change between did:v1.testnet and did:v1.production

4.4.5 Source

Derived from Veres One Rationale Presentation

4.5 Registry Consensus

4.5.1 Question

What type of consensus mechanism is used by the method registry?

4.5.2 Possible Responses

A. Proof of Work
B. Proof of Stake
C. BFT algorithm based
D. Electoral - Select parties vote with thresholds
E. Unanimous - All parties countersign
F. Unilateral - Latest signed version defined as authentic

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 parenthesis–e.g. C(A) for a hybrid BFT algorithm that utilizes POW at some layer–and describe in the notes at a high level how the consensus algorithm functions.

4.5.3 Relevance

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

4.5.4 Evaluation

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

4.5.5 Source

Derived from Veres One Rationale Presentation

4.6 Consensus Layers

4.6.1 Question

What different layers contribute to the consensus mechanism (list all that apply)?

For each layer, evaluate criteria 4.7, 3.6, and 3.7.

4.6.2 Possible Responses

A. Miners -- Perform proof of work
B. Witnesses -- Select transactions
C. Functionaries -- Select transactions and snapshot chain states
D. Peers -- Maintain peer-to-peer gossip network
E. Transactioners -- Can post transactions
F. Auditors -- Can read and validate state
G. Other -- Add your own

4.6.3 Relevance

The ways in which an entity can participate in the consensus algorithm inform the general security and reliability of the actualization of the consensus algorithm.

4.6.4 Evaluation

Method	Reg.	Notes
did:v1. testnet	Witnesses, Peers	In the test net the number of peer nodes is limited but the same number of witness nodes are used as in production.
did:v1. production	Witnesses, Peers	In production the number of peer nodes is expected to increase greatly.

4.6.5 Source

Derived from Veres One Rationale Presentation

4.7 Layer Diversity

4.7.1 Question

How many nodes currently contribute to operational reliability?

4.7.2 Possible Responses

A. Open ended. Currently estimated at greater than 1 million
B. Over 100,000
C. Over 10,000
D. Over 1,000
E. Over 100
F. Over 10
G. Less than 10

4.7.3 Relevance

Along with the type of consensus algorithm, the number of nodes that can participate in consensus has implications towards network security and reliability.

4.7.4 Evaluation

Method	Layer	Response	Notes
did:v1. testnet	Witnesses	F	Veres One uses 13 witness nodes in both testnet and production.
did:v1. testnet	Peers	F	The testnet is configured with 50 peer nodes.
did:v1. production	Witnesses	F	Veres One uses 13 witness nodes in both testnet and production.
did:v1. production	Peers	E	The number of nodes is expected to grow to several hundred nodes in the first year.

4.7.5 Source

Derived from Veres One Rationale Presentation

5. Adoption (and diversity)

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

5.1 Public Funding

5.1.1 Question

If the Method is based on a cryptocurrency, did that currency have an Initial Coin Offering or other public funding mechanism?

5.1.2 Possible Responses

If the method is not based on a cryptocurrency, respond with “n/a”

A. No.
B. Yes.

5.1.3 Relevance

Public 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.

5.1.4 Evaluation

Method	Spec.	Net.	Reg.	Notes.
did:v1. testnet	n/a	n/a	n/a	did:v1 is not based on any cryptocurrency
did:v1. production	n/a	n/a	n/a	No change between did:v1.testnet and did:v1.production

5.1.5 Source

Derived from Veres One Rationale Presentation

5.2 Organizational Maturity in Time

5.2.1 Question

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

5.2.2 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

5.2.3 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.

5.2.4 Evaluation

Method	Spec.	Net.	Reg.	Notes.
did:v1. testnet	B	D	D	Digital Bazaar, the team behind the spec has been in business for over 17 years. The Veres One Foundation was founded in 2019.
did:v1. production	B	D	D	No change between did:v1.testnet and did:v1.production

5.2.5 Source

Derived from Veres One Rationale Presentation

5.3 Test Coverage

5.3.1 Question

How rigorously tested is the proposed consensus implementation?

5.3.2 Possible Responses

A. Continuous integration tests evaluate all known failure modes across multiple nodes.
B. Nightly automated tests evaluate failure modes on a single node
C. Occasional automated tests are run and results published
D. Human-mediated tests have been run, and the result published
E. Testing is performed by evaluating the system in production

5.3.3 Relevance

Robust testing helps ensure that the method has been thoroughly vetted against issues. Both malicious attacks or internal code errors could cause problems which should be found through testing and not in a live system.

5.3.4 Evaluation

Method	Net.	Reg.	Notes
did:v1.testnet	B	B	The Veres One Software contains nightly test suites, simulation suites, and other continuously running correctness tests implemented as code to ensure that the implementation is aligned with the mathematical proof of correctness.
did:v1.production	B	B	No change between did:v1.testnet and did:v1.production

5.3.5 Source

Derived from Veres One Rationale Presentation

5.4 Release Status

5.4.1 Question

Is the registry in general release?

5.4.2 Possible Responses

A. Yes. A production system is available to the general population.
B. No. A test network is operational.
C. No. Only an internal developer network is operational.
D. No. The software is not yet running on any network.

5.4.3 Relevance

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

5.4.4 Evaluation

Method	Net.	Reg.	Notes
did:v1. testnet	B	B	The Veres One test network has been operational for over 3 years, in three major release iterations. It is not yet in production.
did:v1. production	B	B	No change between did:v1.testnet and did:v1.production

5.4.5 Source

Derived from Veres One Rationale Presentation

5.5 Maturity

5.5.1 Question

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

5.5.2 Possible Responses

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

5.5.3 Relevance

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

5.5.4 Evaluation

Method	Spec.	Net.	Reg.	Notes
did:v1.testnet	C	C	C	The Veres One test network has been operational for over 3 years, in three major release iterations.
did:v1.production	C	E	E	No change between did:v1.testnet and did:v1.production

5.5.5 Source

Derived from Veres One Rationale Presentation

6 Security

Security criteria address how the method is cryptographically secured.

6.1 Robust Crypto

6.1.1 Question

What is the lowest security level ("bits of security") provided by the combination of algorithms and key types that the method requires its implementations to support?

6.1.2 Possible Responses

A. No combination of required features produces a profile with less than 256 bits of security.
B. Between 128 and 256 bits
C. Less than 128 bits
D. Less than 64 bits

6.1.3 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.

6.1.4 Evaluation

Method	Reg.	Notes
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.
did:v1. production	A	No change between did:v1.testnet and did:v1.production

6.1.5 Source

DID Method Rubric v1.0.0 (draft) §https://w3c.github.io/did-rubric/#robust-crypto

6.2 Expert Review (Cryptography)

6.2.1 Question

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

6.2.2 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.

6.2.3 Relevance

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

6.2.4 Evaluation

Method	Reg.	Notes
did:v1. testnet	A	Ed25519 and SHA256 are highly regarded cryptographic algorithms
did:v1. production	A	No change between did:v1.testnet and did:v1.production

6.2.5 Source

DID Method Rubric v1.0.0 (draft) §https://w3c.github.io/did-rubric/#expert-review

6.3 Expert Review (Consensus)

6.3.1 Question

Has the registry's consensus mechanism undergone sufficient review?

6.3.2 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.

6.3.3 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.

6.3.4 Evaluation

Method	Net.	Reg.	Notes
did:v1.testnet	B	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.
did:v1.production	B	B	No change between did:v1.testnet and did:v1.production

6.3.5 Source

Derived from Veres One Rationale Presentation

6.4 Future Proofing

6.4.1 Question

How friendly is the system to adopting post-quantum crypto, larger hashes, or other measures that upgrade its security?

6.4.2 Possible Responses

A. Any user of the system can easily upgrade their crypto at any time
B. No code changes are needed, but the whole system needs to be reconfigured to allow new crypto.
C. Code changes must be implemented before new crypto is possible.
D. Code changes must be implemented, and migration of all existing data must be performed, before new crypto is possible.

6.4.3 Relevance

A DID method that is hard to upgrade with respect to crypto creates incentives to remain with deprecated algorithms beyond their useful lifespan.

6.4.4 Evaluation

Method	Reg.	Notes
did:v1.testnet	D	The Veres One network does not provide for adjustable or modular cryptography. Changes must be made through API updates propagating via manual updates to the software running the network.
did:v1.production	D	No change between did:v1.testnet and did:v1.production

6.4.5 Source

DID Method Rubric v1.0.0 (draft) §https://w3c.github.io/did-rubric/#future-proofing

6.5 Availability

6.5.1 Question

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

6.5.2 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.

6.5.3 Relevance

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

6.5.4 Evaluation

Method	Reg.	Notes
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 measurers are in place, but cannot be 100% ameliorated.
did:v1.production	B	No change between did:v1.testnet and did:v1.production

6.5.5 Source

DID Method Rubric v1.0.0 (draft) §https://w3c.github.io/did-rubric/#availability

6.6 Provenance

6.6.1 Question

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

6.6.2 Possible Responses

A. Every evolution of state 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. Adequate evidence of proper evolution 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 evolution exists.
D. No evidence of proper evolution exists; the users have to trust the system's assertion that the current state resulted from something appropriate.

6.6.3 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.

6.6.4 Evaluation

Method	Reg.	Notes
did:v1. testnet	A	All document updates are recorded in a non-repudiable manner on the Veres One Ledger.
did:v1. production	A	No change between did:v1.testnet and did:v1.production

6.6.5 Source

DID Method Rubric v1.0.0 (draft) §https://w3c.github.io/did-rubric/#evolution

6.7 Many Eyes

6.7.1 Question

Is the code of the method published, does it have many contributors, and does it have a published vulnerability reporting (responsible disclosure) mechanism?

6.7.2 Possible Responses

A. The code is public. It has hundreds of contributors. Common Vulnerability and Exposures (CVEs) or similar reports have been published and handled appropriately.
B. The code is public, but the list of contributors is small. No vulnerability reporting mechanism has been announced, or it's been announced but has no demonstrable track record.
C. The code is partly private.
D. The code is entirely private.

6.7.3 Relevance

Security vulnerabilities tend to be found and fixed best in code that has many active contributions and a strong history of correctly handled responsible disclosure.

6.7.4 Evaluation

Method	Reg.	Notes
did:v1. testnet	B	There is a reference implementation available, created and maintained by Digital Bazaar with limited contributions from the public.
did:v1. production	B	No change between did:v1.testnet and did:v1.production

6.7.5 Source

DID Method Rubric v1.0.0 (draft) §https://w3c.github.io/did-rubric/#many-eyes

6.8 United States Federal Compliance

6.8.1 Question

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

6.8.2 Possible Responses

A. Both registry consensus *and* transaction validation are compliant
B. Transactions validation are compliant but consensus is not
C. No. Neither consensus nor transactions are compliant

6.8.3 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)

6.8.4 Evaluation

Method	Spec.	Net.	Reg.	Notes.
did:v1. testnet	A	A	A	did:v1 was written to be compatible with all NIST requirements, including those specified in the Relevance section (6.8.3)
did:v1. production	A	A	A	No change between did:v1.testnet and did:v1.production

6.8.5 Source

Derived from Veres One Rationale Presentation