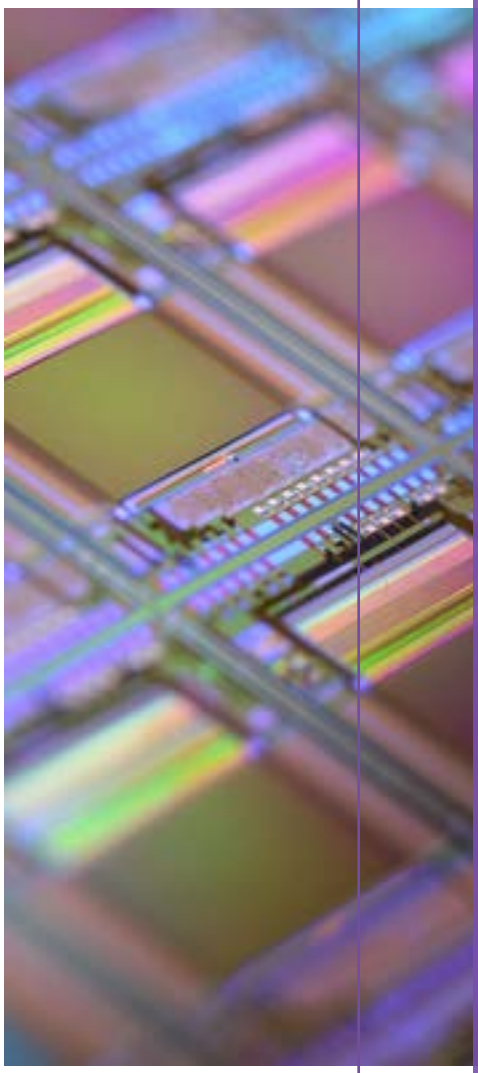


A DID Method Rubric Evaluation of did:web

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:web

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

CONTRIBUTORS:

Kyle Denhartog kyle.denhartog@mattr.global
Orie Steele orie@transmute.industries

EVALUATION DATE

2022-03-01

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

FUNDED BY

MATTR https://mattr.global/ (supported in part by DHS SVIP contract 70RSAT21T00000030)
Transmute https://www.transmute.industries/ (supported in part by DHS SVIP contract 70RSAT21T00000031)

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.
use-case-2	Trusted Key Custody	When the DID Controller is explicitly linked to the Domain Operator (which is the VDR provider for all DIDs under a given domain), but the DID Subject is not. The subject has elected to use an identifier controlled by a service provider they trust, who manages the DID document on their behalf, running web services to publish.
use-case-3	Web Services API	In scenarios where a web-based service API is in use for signing data provided by the web-based service API or invoking authentication to the web-based services API, then did:web is a straightforward mechanism for publishing cryptographic material over https. DID Comm use case using WACI Presentation Exchange. https://github.com/decentralized-identity/waci-presentation-exchange Organizations that already rely on the World Wide Web for presenting authoritative information may feel comfortable with the privacy implications where an individual may have unaddressed concerns. To wit, if the DNS domain is owned by a third party. Such a third party will have full control over and visibility into each individual's DID operations.

Methods Evaluated

	SPECIFICATION	NETWORK	REGISTRY
did:web	did:web is a web-based decentralized identifier method, which uses https webserver and existing DNS infrastructure for resolving DIDs.		
	https://github.com/w3c-ccg/did-method-web	The World Wide Web https://en.wikipedia.org/wiki/World_Wide_Web	Hosted at a https server.

Contents

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)

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:web	A	B	C/D	**Spec** (A): Owned by CCG at W3C, anyone can join. **Net** (B): Most of the network is controlled by public or private entities. **Reg**: Controlled by the Domain Holder, which is a restricted set (C) and in some cases may not be known to the resolving party (D).

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-2	did:web	A-	B-	D	**Spec** (A-): The work occurs mostly in github issues, which are open to be public and retained in perpetuity. However, there are no regular meeti ngs. **Net** (B-): Icann & IANA generally operate in public, although some discussion may be behind closed doors. **Reg** (D): Only the website controller knows the rules they are applying.

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-3	did:web	TLD Control (ICANN / IANA)	https://www.icann.org/ governs the DNS system, operationalized through IANA https://iana.org functions currently performed by PTI https://pti.icann.org/ For our analysis, we treat ICANN, IANA, and PTI as interchangeable terms for the same essential layer.
a-4	did:web	TLD Administrator	https://icannwiki.org/Top-Level_Domain https://www.icann.org/en/icann-acronyms-and-terms/top-level-domain-en A TLD is a domain at the top of the naming hierarchy of the Domain Name System. In a domain name, the TLD appears after the second-level domain. For example, in the domain name icann.org, the characters org identify the TLD. The administrators of a TLD control which second-level domains are recognized within the TLD. TLDs fall into two classes: generic top-level domains (e.g., .com, .net, .edu) and country code top-level domains (e.g., .jp, .de, .in).
a-5	did:web	DNS Registrar	An organization through which individuals and entities (registrants) register domain names. During the registration process, a registrar verifies that the requested domain name meets registry requirements, and submits the name to the appropriate registry operator. Registrars are also responsible for collecting required information from registrants and making the information available through WHOIS. After registration, registrants can make updates to their domain name settings through their registrars.
a-6	did:web	Domain Holder	An individual or entity who registers a domain name. Also called a registrant. To complete a domain name registration, the registrant (Domain Holder) registers the domain name with a registrar. The registrar verifies that the domain name is available in the requested TLD and submits the registration request to the registry operator for that TLD. The registry operator then adds the new domain to the TLD's registry. A registrant can optionally register a domain name through a reseller. Resellers are third-party companies that offer domain name registration services through a registrar.
a-7	did:web	Name Server	A name server provides directory services within the domain name system, matching domain names with their corresponding numerical IP addresses and allowing end users to reach their desired destination on the Internet. Each domain has at least one authoritative name server that publishes information about that domain and the name servers of any domains subordinate to it. The top of the hierarchy is served by the root name servers, the servers to query when looking up (resolving) a TLD.

a-8	did:web	Certificate Authority	https://icannwiki.org/CA A Certificate Authority is a trusted third party company that issues digital certificates and public-private keys as a part of chosen Public Key Infrastructure (PKI). In order to issue these certificates, a CA first consults with a registration authority (RA) such as credit card company to check whether the requester's information is legitimate. Only after the proper verification can the CA issue a certificate claiming that the organization or the individual is the one it claims to be. Having a digital certificate on a website proves the owner's identity, hence developing a trustworthy environment in business. A certificate includes all the information about the owner, including their public key and the expiration date of the certificate. It is also possible to use self-issued certificates, but most browsers will report such efforts as potential security risks, making this approach largely unusable for consumer-facing web applications. Let's Encrypt provides free and easy to use certificates using automated tools. This has the benefit of bypassing the more rigorous and expensive CA process (similar to a self-issued certificate), while still working seamlessly with most browsers.
a-9	did:web	Hosting service	Websites are hosted on some physical server. This hosting can be provided on-premise with a simple network connection or it can be outsourced to any number of hosting services, including Amazon Web Services, Azure, Bluehost, and Linode. Different services provided different levels of security and capability, from Virtual Private Servers, which share a single hardware device amongst many customers to dedicated "raw metal" hardware running whatever the customer installs. The "governance" at this layer is a mix of hosting company policies and software configurations that enable or disable various features for each hosted website.
a-10	did:web	Website owner/ administrator	The owner or administrator of the website controls the content running on the hosting service. For many platforms, this means using services provided by the hosting company to upload and maintain the website, such as FTP or SSH. Within the bounds of the capabilities offered by the hosting server, it is entirely the website owner's decision about what content to host and what software to run. The "governance" for this layer is entirely dependent on the nature of the owner. For many did:web use cases, the website owner is the DID owner, but in cases where the DID document is hosted on someone else's website, the owner of that website's decision making processes should be considered.

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-11	did:web	TLD Control (ICANN / IANA)	E	

a-12	did:web	TLD Administrator	C/F/*	Depends on the TLD. Many TLD Administrators are for-profit (C) while national TLDs like .uk or .jp. are controlled by nation states (F). However, there is no restriction the type of organizations that can qualify as TLD Administrators. (*)
a-13	did:web	DNS Registrar	*/C	Depends on TLD (*), but most are for-profit entities (C). https://www.icann.org/en/accredited-registrars?filter-letter=a&sort-direction=asc&sort-param=name&page=1
a-14	did:web	Domain Holder	*	Any entity may own a domain (*). However, each TLD Administrator may impose additional restrictions, such as doing business in a specific geographic location or operating an accredited educational institution.
a-15	did:web	Name Server	*	DNS servers can be, and are, run by anyone. (*)
a-16	did:web	Certificate Authority	*	Any organization (*). Including self-signed and self-asserted using Let's Encrypt. We expect that the vast majority of use cases rely on top-down CAs.
a-17	did:web	Hosting service	*	Any entity can run a web host (*)
a-18	did:web	Website owner/ administrator	*	Any entity can run a web host (*)

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	Deliberating Body	Cost	Notes
a-19	did:web	TLD Control (ICANN / IANA)	C	Straightforward to get a proposal into ICANN. Not free, but doable. (C)
a-20	did:web	TLD Administrator	D	No formal channels. Each TLD decides who/how they listen. (D)
a-21	did:web	DNS Registrar	C	Typically a customer relationship exists, which provides a framework for negotiating governance policy. (C)
a-22	did:web	Domain Holder	A/D	Entirely up to the Domain Holder whether or not they even want to listen to you (D). However, if you are the Domain Holder, the cost is just the burden of internal decision-making (A)

a-23	did:web	Name Server	A/D	Entirely up to the DNS Server operator whether or not they even want to listen to you (D). If you own the domain, you control which DNS server to use, including running your own (A)
a-24	did:web	Certificate Authority	A/D	Let's Encrypt is FREE. For self-hosted CAs (or Let's Encrypt), it's easy to get changes (A). If your CA is Network Solutions or GoDaddy, they may not have the support infrastructure to seriously consider your request, depending on your relationship with them (D)
a-25	did:web	Hosting service	A/B	It should be easy to get a hosting company to host what you want; if they can't there are a plethora of other providers you can choose from, including yourself. (A) However, some hosting companies may not be able to support particular services, e.g., restricting SSL access to specific subdomains (B).
a-26	did:web	Website owner/ administrator	B	Someone has a relationship with the deliverating body and that implies some mechanism for discussion. (B)

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	Deliberating Body	Cost	Notes
a-27	did:web	TLD Control (ICANN / IANA)	D	ICANN has a Fellowship program that those who wish to take part in discussions may join as well as public meetings. However, ICANN has a complex governance structure and in practice it is very difficult for any single person to be considered a peer without significant investment. (D) https://www.icann.org/en/system/files/files/participating-08nov13-en.pdf
a-28	did:web	TLD Administrator	D	As many TLDs are for-profit companies there is no guaranteed way an individual could be considered a peer in the governance process without joining the organization. (D)

a-29	did:web	DNS Registrar	D	Most DNS Registrars are generally for-profit companies and as such the only real way to be involved in the governance is through a contractual relationship or working directly for a given registrar.
a-30	did:web	Domain Holder	B	Most Domain Holders are private entities that have incentive to respond to requests for changes they can control. It is also not difficult in practice to become a Domain Holder and as such have full control of the governance decisions for a particular domain.
a-31	did:web	Name Server	C	A “peer” means running your own server. (C)
a-32	did:web	Certificate Authority	A/D	It’s easy to act as a CA (A). It’s hard to be accepted by major browsers as such. (D)
a-33	did:web	Hosting service	B	Depends on who controls the hosting service, however, hosting services are effectively commoditized, so switching hosting services is usually a straightforward option. (B)
a-34	did:web	Website owner/ administrator	A	Depends on who controls the website. If you are a member of a collaborative team, it is free to agree to manage the site together (A).

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

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-35	did:web	A	**Spec** (B): did:web, which is based on the World Wide Web and DNS does not rely on any cryptocurrency.

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-36	did:web	B	B	**Net** (B) and **Reg** (B) Every layer in the architecture requires the permission of those above., e.g., website owners need a hosting company. Those permissions can always be revoked.

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-37	did:web	A	A-	A-	**Spec** (A), **Net** (A-) and **Reg** (A-): Web-based wallets may have complications from CORS (cross-origin resource sharing), but in general any “wallet” is compatible. Although a given service (hosting or website, etc.) could add a layer of permissioned restrictions, the did:web method does not require it. Similarly, nation-state level firewalls could restrict access at various layers, but, again, the method does not require it.

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-38	did:web	A/B	A/B	In general, did:web DIDs can be used for anything, by anyone (A). However, some implementers believe did:web should only be used to represent institutional entities (who tend to already have good systemic controls over web infrastructure). (B)

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-39	did:web	B+	The DID controller must be able to communicate with the web server that is hosting the DID document. However, in some configurations, this may not mean accessing the global network. For example, if you are physically present at the hosting server, one can create the DID document files directly without network access. To resolve the DID document those files must be published at an accessible endpoint, but creation doesn't need the network.

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-40	did:web	A	did:web is a partitioned namespace where any given partition could support billions of DIDs. The URL behind the DID could be hosted by a small hosting service that can only handle a limited # of DIDs, but the hosting of a given domain could also be scaled arbitrarily.

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-41	did:web	A	Assuming you already have a hosting provider providing a website, this cost is essentially free. If you don't, you may incur the cost of establishing a website (and perhaps a domain purchase or TLD application).

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-42	did:web	A	Assuming you already have a hosting provider providing a website, this cost is essentially free. If you don't, you may incur the cost of establishing a website (and perhaps a domain purchase or TLD application).

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

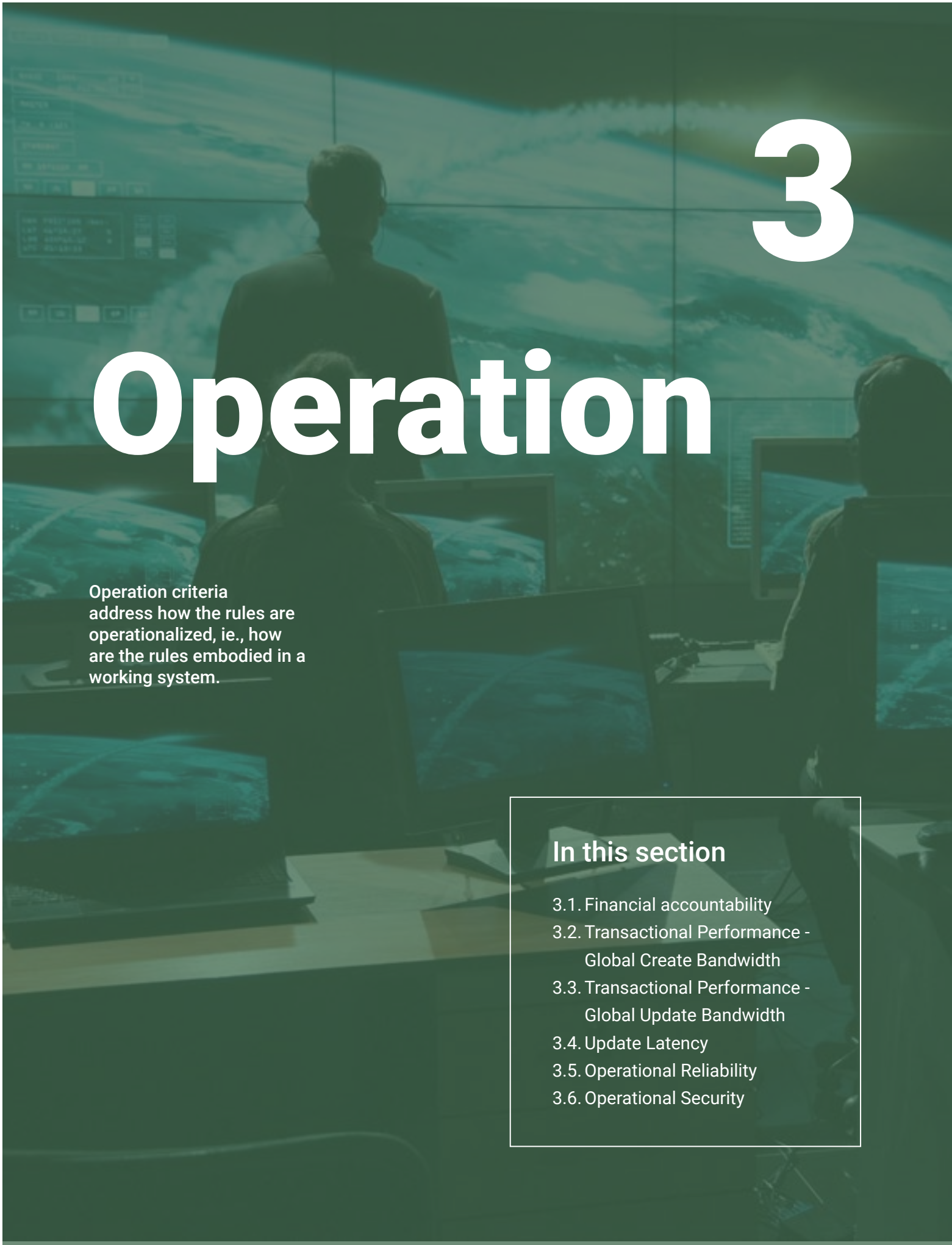
- **A** Only operational costs of running the algorithm (no externalized expense)
- **B** Less than $0.01
- **C** Less than $0.10
- **D** Less than $1
- **E** Less than $10
- **F** $10 or greater

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	Re g.	Notes
a-43	did:web	n/a	The method itself does not provide for in-kind contributions.



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

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-44	did:web	D	D	**Net** (D) and **Reg** (D): The economics of the World Wide Web are a free-for-all by any participating party. Any particular financial arrangements may or may not be visible to DID method users.

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-45	did:web	A	A	**Net** (A) and **Reg** (A): Architecturally, the World Wide Web can easily handle +1,000,000 transactions per second. Thanks to the way domain names can be routed to specific servers in a round-robin fashion, a given domain could, theoretically, reach 1,000,000 TPS. However, we know of no single domain currently engineered to handle that scale.

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-46	did:web	A	DID:web update performance is highly sensitive to both implementation choices (http server, database, etc.) and network latency.

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-47	did:web	B	B	**Net** (B) and **Reg** (B): Depends on your network (and network configuration), but generally, did:web document updates are as fast as updates to any web resource.

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-48	did:web	Root Server	12	As long as at least one root server is functional, DNS lookups work.
a-49	did:web	Registry Operator	NONE	To update or read a given authoritative DNS record for a domain, the Registry Operator for that domain must be operational.
a-50	did:web	Registrar	NONE/ OPTIONAL	**NONE**: To update the ip address for the authoritative DNS server, the registrar must be operational. **OPTIONAL**: However, reads of the DNS record will still work, even if current Registrars are offline.

a-51	did:web	Domain Holder	NONE/ OPTIONAL	**NONE**: Domain Holders SHOULD be involved as the source of all updates to both the Authoritative DNS server and record, but there are no guarantees beyond business processes. **OPTIONAL**: To look up a domain name, the Domain Holder is not involved.
a-52	did:web	Authoritative DNS Server	NONE	To update and read a DNS record, the Authoritative DNS Server must be operational.
a-53	did:web	Recursive DNS Server(s)	NONE/ OPTIONAL	**NONE**: In most cases, if the Recursive DNS fails, the DNS lookup will fail. **OPTIONAL**: However, some software implementations are able to perform the lookup function by 1. going direct to the root zone servers, 2. downloading the root zone file 3. parsing the root zone file 4. finding the TLD Administrator 5. downloading the zone file for the TLD 6. Parsing the TLD zone file 7. Finding the authoritative DNS server 8. Querying the Authoritative DNS server to get the authoritative DNS Record In short, instead of using a recursive DNS server, software can perform the functions from the root servers down. In practice, most software simply relies on a Recursive DNS server to be available.

a-54	did:web	Certificate Authority	OPTIONAL/ ***	**OPTIONAL**: All did:web registry servers must use TLS/ SSL, which requires a certificate signed by a Certificate Authority. If a Domain Holder cannot get a recognized Certificate Authority to issue a TLS certificate, they may go to another CA, including issuing their own. Once the TLS certificate is created, the Certificate Authority has no further operational role, except if they publish some form of revocation list. As such, availability of the CA does not affect the ability to read from the Verifiable Data Registry. ***: However, most software, including web browsers, restrict access in some way to domains with TLS certificates from unknown CAs. As of 24 August 2020, 147 root certificates, representing 52 organizations, are trusted in the Mozilla Firefox web browser,[9] 168 root certificates, representing 60 organizations, are trusted by macOS,[10] and 255 root certificates, representing 101 organizations, are trusted by Microsoft Windows.[11] As of Android 4.2 (Jelly Bean), Android currently contains over 100 CAs that are updated with each release.[12] Similarly, operating systems may be configured to specify additional trusted CAs. In short, web-based applications may struggle to resolve did:web DIDs hosted on https servers configured with CAs outside the commonly recognized set, such as self-signed certificates. However, applications can always be written to support any CA. Note: Certificate Authorities are not involved in the writing of DID documents to the VDR.
a-55	did:web	Hosting service	NONE	If the hosting service is down, did:web DIDs cannot be resolved. Services like Content Distribution Networks and other caching strategies may provide some continuity of service, with a reciprocal tradeoff in latency of updates.
a-56	did:web	Website	NONE	If the website is down, DID documents cannot be resolved.

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.

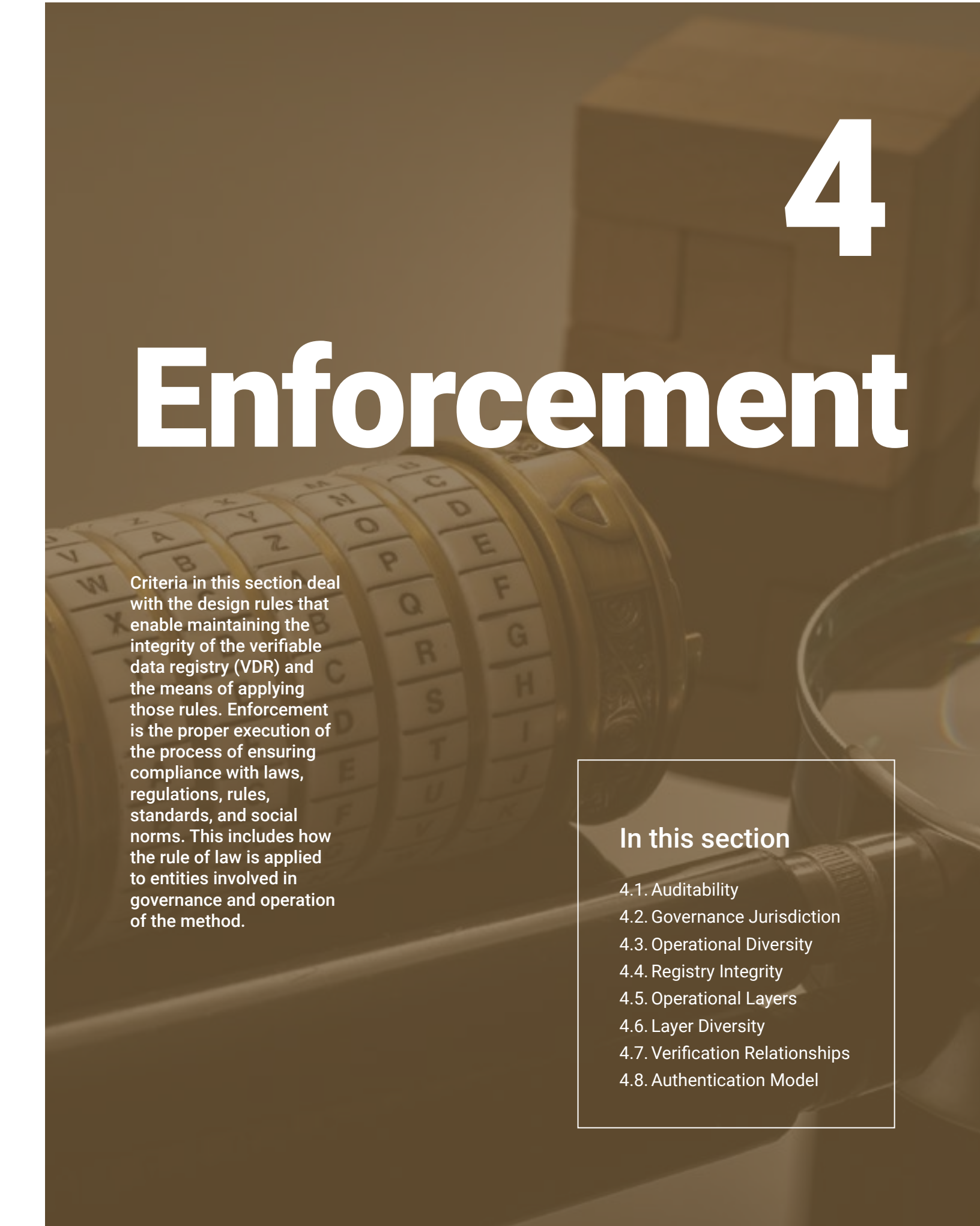
ASSESSMENT

	Method	Layer	Response	Notes
a-57	did:web	Root Server	NONE	Root servers are "guaranteed" to be in a valid state. If the root server a particular application is using has compromised information, DID resolution using that server should also be considered compromised. ICANN uses human processes and governance to correct inconsistencies between root servers. Applications could rely on multiple root servers for extra resilience, but in practice such fail overs are typically for availability rather than integrity and secondary root servers are only checked if the initial check fails.
a-58	did:web	Registry Operator	NONE	If the Registry Operator for a given domain is compromised, did:web DIDs for that entire domain should be considered compromised. However, the failure of one TLD will not affect did:web DIDs using other TLDs.

a-59	did:web	Registrar	NONE	If any Registrar recognized by a given TLD Administrator is compromised, DIDs for that entire TLD should be considered compromised, as Registrars may update any record in the TLD's zone files. One exception occurs when a given domain is locked against changes.
a-60	did:web	Domain Holder	NONE	Domain Holders are the ultimate legal authority over their domain names and all hosted content.
a-61	did:web	Authoritative DNS Server	NONE/ OPTIONAL	**NONE**: Authoritative DNS Servers are expected to be authoritative. Fortunately, only the domain name records authoritatively provided by the compromised service are affected. **OPTIONAL**: If DNSSEC is used to secure the domain records, then even a compromised authoritative DNS server is unable to compromise the DNS record. Unfortunately, both the domain controller and the domain consumer have to opt-in to DNSSEC for it to protect the domain.
a-62	did:web	Recursive DNS Server(s)	NONE/ OPTIONAL	**NONE**: A compromised recursive DNS server can serve false records to any client. **OPTIONAL**: If DNSSEC is used to secure the domain records, then even a compromised authoritative DNS server is unable to compromise the DNS record. Unfortunately, both the domain controller and the domain consumer have to opt-in to DNSSEC for it to protect the domain.
a-63	did:web	Certificate Authority	NONE	If the CA for a given webserver (as well as any CA in its chain of authority) is compromised, then all communication with the webserver should be considered untrustworthy.
a-64	did:web	Hosting service	NONE	If the hosting service for a webserver is compromised, the DID document cannot be considered authentic.
a-65	did:web	Website	NONE	If the website itself is compromised, the DID document cannot be considered authentic, nor should any verification methods in that DID document.

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

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-66	did:web	D	The web server hosting the DID document has no requirement to preserve cryptographic history.

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-67	did:web	TLD Control (ICANN / IANA)	Headquarters of ICANN are in Los Angeles, CA, USA.
a-68	did:web	TLD Administrator	Varies by TLD.
a-69	did:web	DNS Registrar	Could be anywhere. Registrars are chosen by the Domain Holder.
a-70	did:web	Domain Holder	Could be anywhere. Domain Holdership is independent of jurisdiction.
a-71	did:web	Name Server	Could be anywhere.
a-72	did:web	Certificate Authority	Could be anywhere.
a-73	did:web	Hosting service	Could be anywhere.
a-74	did:web	Website owner/ administrator	Could be anywhere.
a-75	did:web	User / DID Controller	Could be anywhere.

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-76	did:web	C	Any of the layers could be compromised by that particular party.

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 Toleran 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-77	did:web	F/G	ICANN sets the specification for consensus (F). DNS works by participants agreeing that ICANN's rules determine global state.

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-78	did:web	Root Server	The authoritative name servers that serve the DNS root zone, commonly known as the “root servers”, are a network of hundreds of servers in many countries around the world. They are configured in the DNS root zone as 13 named authorities. These server names and IP addresses are typically hard coded into software that manages DNS resolution. https://www.iana.org/domains/root/servers
a-79	did:web	Registry Operator	The entity that maintains the master database (the registry) of domain names registered in a particular top-level domain (TLD). Operators run under charter from IANA. See IANA Root Zone Database: https://www.iana.org/domains/root/db
a-80	did:web	Registrar	Registrars operate under charter from IANA, managing ownership of DNS records, subject to IANA policies & procedures. https://www.icann.org/en/accredited-registrars Registrars are involved in updating the authoritative record at the TLD Administrator, but not involved in resolution.
a-81	did:web	Domain Holder	Domain Holders control specific domains, as registered with any approved registrar. Each domain, e.g., “example” in “example.com” may only be registered at one registrar, who ensures that only one party may legitimately claim ownership. Ownership rights are enforced by courts.
a-82	did:web	Authoritative DNS Server	A DNS server (sometimes called a Name Server), pointed to by TLD Administrator database as authoritative for the domain in question, as maintained by registrars under the Domain Holder’s authority. Every DNS zone must be assigned a set of authoritative name servers. This set of servers is stored in the parent domain zone with name server (NS) records.
a-83	did:web	Client DNS Server(s)	Domain Name Servers (DNS servers) may be operated by anyone, however, many individuals rely. Network configuration typically includes default DNS servers and most operating systems allow local operators to set their own DNS servers. Some applications may ignore platform and network settings. DNS servers typically cache records to minimize network traffic and DNS records specify a Time-To-Life for all entries. As a result, changes to DNS records may take time to propagate.

a-84	did:web	Certificate Authority	https://www.icann.org/resources/pages/certificate-authority-2012-02-25-en Certificate Authorities enable the creation of TLS certificates and must be recognized by verification software to be effective. Most software uses a known hierarchy for anchoring trust in a known root authority; many can be configured to accept self-signed certificates or particular, specific Certificate Authorities. In the case of CA hierarchies, each layer in the hierarchy must be trusted to trust the content from the domain. For example, most browsers trigger warnings and errors for TLS certificates issued by unknown parties, such as self-signed certs. In addition, platforms can be configured to recognize proprietary Certificate Authorities under the control of network operators and used to proxy TLS traffic in and out of the network. In this “middlebox” configuration, users must trust the proxy in order to trust the source of TLS traffic.
a-85	did:web	Hosting service	Hosting services, typically provided by ISPs, run a network accessible https server on behalf of customers. Companies or individuals may choose to self-host on-premise; such deployments should still be considered a “hosting service”.
a-86	did:web	Website	Webmasters control individual websites instances of https servers operating on a hosting service.

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-87	did:web	Root Server	B	There are currently 13 root servers. It is understood that the root servers are typically deployed as redundant, round-robin servers, but we consider each of the 13 as a single coherent risk factor. (B)
a-88	did:web	Registry Operator	A/C	Each Registry Operator maintains their own system with variable deployments. They may have multiple, redundant servers (A) or they may not. If a given Registry Operator is non-operational, domain names with that top-level-domain may not be reachable. If the Registry Operator themselves are compromised, the entire top level domain will be suspect. (C)
a-89	did:web	Registrar	C	If the registrar currently on record for a domain name is down, DNS lookup works fine, but changes to the authoritative DNS Server cannot be processed without exceptional handling. (C)

a-90	did:web	Domain Holder	C	Domain Holders are a single point of failure for updates to DNS records. If the Domain Holder refuses or is unable to update DNS records, changes to DNS will not be processed. However, if the domain name is already configured, the method can continue to resolve using current DNS records. In addition, malicious Domain Holders can arbitrarily change the DNS servers for any of their domains, potentially leading to did:web resolution at unexpected servers with arbitrary results. (C)
a-91	did:web	Authoritative DNS Server	A	DNS supports multiple Authoritative DNS servers; many provide two or three for redundancy. However, this is inspectable so a resolving party could determine how many servers are supporting that domain. (A)
a-92	did:web	Client DNS Server(s)	A	End system software can be configured for any number of client DNS servers and many networks run their own. (A)
a-93	did:web	Certificate Authority	A	Software can be configured to accept self-signed certificates, allowing an unlimited number of potential CAs. In practice, most DNS-aware software, such as web browsers, restrict traffic to servers whose certificates can be traced back to a trusted authority. (A)
a-94	did:web	Hosting service	A/C	It is possible to deploy multiple, redundant servers (A). However, many installations reside with a single authoritative host. These hosts must be reachable. (C)
a-95	did:web	Website	C	A webmaster is considered a single point of control over the website (and hence the content of the DID documents), even if realized through a team of collaborating administrators. (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-96	did:web	H	The did:web specification does not restrict Verification Relationships.

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-97	did:web	L	Document updates are secured according to the business rules maintaining the website, allowing effectively any mechanism to be used, including username & password, signed JSON patches, etc. This could also be impacted by the security model of the hosting service, as an improperly configured hosting service could allow an attacker to change the business logic of the website. (L)

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

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-98	did:web	D	A/B/C/D/G	H	**Spec** (D): Specification was developed largely by independent firms using operational budgets . **Net**: The web was funded initially by the US Department of Defense and national TLD Administrators are funded by nation-states (A). Network infrastructure of TLD Administrators, hosting services, etc., have largely been funded by non-profits (B), private firms using either private equity (C), operational budgets (D), or public equity offerings (G). **Reg** (H): Individual websites and network services have been funded in just about every way imaginable.

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-99	did:web	F	A	*	**Spec** (F): did:web specification development began in earnest in 2019 by a variety of interested parties. **Net** (A): The Internet and the World Wide Web have been around for over 20 years. **Reg** (*): The individual web servers that might be used depend on the organizational maturity of the hosting company and the website operator.

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-100	did:web	A	A	**Net** (A) and **Reg** (A): The web has been in general use for 30+ years. Multiple production deployments are in use today.

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-101	did:web	A	D	**Net** (A): The web has been around since 1991. **Reg** (D): We know of no websites that have operationalized did:web earlier than July 2021.

6

Security

Security criteria address how the method is cryptographically secured.

In this section

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-102	did:web	n/a	Although TLS and DNSSec provide significant cryptographic security, the method specification itself does not require web servers to implement any particular security over updates to DID documents. (n/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-103	did:web	A/E	TLS/SSL (a requirement for did:web) is the most widespread adoption of cryptographic technology with well-tested, proven implementations (A). The method itself does not require any additional cryptographic primitives. The did:web method does inherit the known short-comings of DNS, which can be mitigated with DNSSec, in some cases. However, this is not a cryptographic problem. In addition, each webserver is free to use any authentication and authorization technique for creating, updating, and deactivating a DID and DID document. The method relies on this layer to function, but the implementation of this layer may or may not use vetted cryptography (E).

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-104	did:web	A	n/a	**Net** (A): The DNS and TLS systems have been thoroughly reviewed in academic literature in research about the Internet and the World Wide Web. **Reg** (n/a) : The method provides no consensus mechanism with regard to the https server itself. The entity controlling the server operates independently. (n/a)

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-105	did:web	C	There are a number of attack vectors for each layer in the system; however, each layer also has its own mechanisms for addressing disruption. (C)

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-106	did:web	D	The method does not require the website serving the DID document to demonstrate any form of provenance.

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-107	did:web	A	A	A	**Spec** (A), **Net** (A), and **Reg** (A): Due to the flexibility of the underlying web architecture, any layer *might* be non-compliant; However, the web is a mature platform with many years of solutions that do, in fact, meet US federal requirements.

LEGENDARY
REQUIREMENTS