Derrière d'ennuyeuses normes techniques, des enjeux stratégiques (1/18)

Stéphane Bortzmeyer
stephane+ege@bortzmeyer.org

Club Cyber - AEGE, Paris, 26 janvier 2022

Un petit rappel sur l'Internet

Un petit rappel sur l'Internet

- Ce qui caractérise l'Internet, ce n'est pas le datagramme,

Un petit rappel sur l'Internet

- Ce qui caractérise l'Internet, ce n'est pas le datagramme,
- Ni TCP/IP,

Un petit rappel sur l'Internet

- Ce qui caractérise l'Internet, ce n'est pas le datagramme,
- Ni TCP/IP,
- C'est d'être un réseau multi-organisations et multi-fournisseurs,

Un petit rappel sur l'Internet

- Ce qui caractérise l'Internet, ce n'est pas le datagramme,
- Ni TCP/IP,
- C'est d'être un réseau multi-organisations et multi-fournisseurs,
- Il repose sur l'**interopérabilité**.

L'interopérabilité ?

Utilisateur :Kiddo, Public domain, via Wikimedia Commons https ://commons.wikimedia.org/wiki/File :Israeli-type-H-plugs-and-socket.jpg

L'interopérabilité

L'interopérabilité

- Je peux utiliser Microsoft Edge pour regarder un site Web servi par nginx,

L'interopérabilité

- Je peux utiliser Microsoft Edge pour regarder un site Web servi par nginx,
- Je peux envoyer un message avec mutt et Postfix à quelqu'un qui utilise Outlook et Microsoft Exchange,

L'interopérabilité

- Je peux utiliser Microsoft Edge pour regarder un site Web servi par nginx,
- Je peux envoyer un message avec mutt et Postfix à quelqu'un qui utilise Outlook et Microsoft Exchange,
- Par contre, aucune interopérabilité entre messageries instantanées.

Comment assurer l'interopérabilité

Comment assurer l'interopérabilité

- Méthode la plus commune : une **spécification** proprement écrite, décrivant notamment les **protocoles** (HTTP, SMTP, DNS...),

Comment assurer l'interopérabilité

- Méthode la plus commune : une **spécification** proprement écrite, décrivant notamment les **protocoles**,
- Mais parfois, il n'y a pas vraiment de spécification (Bitcoin, BitTorrent).

Qui va écrire la spécification ?

Qui va écrire la spécification ?

- Méthode qui garantit le plus d'ouverture : une organisation de normalisation (SDO, *Standard Development Organisation*),

Qui va écrire la spécification ?

- Méthode qui garantit le plus d'ouverture : une organisation de normalisation,
- Toutes les SDO ne se valent pas : ouverture du processus, publication gratuite des normes. . .

Exemple de norme

INTERNATIONAL STANDARD

ISO/IEC 5218

NORME INTERNATIONALE

First edition
Première édition
2004-07-01

Corrected version
Version corrigée
2004-12-01

Information technology — Codes for the representation of human sexes

Technologies de l'information — Codes de représentation des sexes humains

Mais pourquoi est-ce important ?

Mais pourquoi est-ce important ?

- Ce qui est normalisé sera sans doute plus répandu, plus accessible, notamment aux non-techniciens,

Mais pourquoi est-ce important ?

- Ce qui est normalisé sera sans doute plus répandu, plus accessible, notamment aux non-techniciens,
- Ce qui n'est pas normalisé reste possible mais peut-être plus difficile,

Mais pourquoi est-ce important ?

- Ce qui est normalisé sera sans doute plus répandu, plus accessible, notamment aux non-techniciens,
- Ce qui n'est pas normalisé reste possible mais peut-être plus difficile,
- La normalisation est une bonne chose, elle est efficace. . .

Mais pourquoi est-ce important ?

- Ce qui est normalisé sera sans doute plus répandu, plus accessible, notamment aux non-techniciens,
- Ce qui n'est pas normalisé reste possible mais peut-être plus difficile,
- La normalisation est une bonne chose, elle est efficace. . .
- Et donc elle a des conséquences, bonnes ou mauvaises.

Exemples de conséquences

Exemples de conséquences

- Une technique non-normalisée risque de vous enfermer dans un seul vendeur,

Exemples de conséquences

- Une technique non-normalisée risque de vous enfermer dans un seul vendeur,
- Si la norme ne prévoit pas une fonction (chiffrement...), beaucoup d'utilisateurs n'en disposeront pas,

Exemples de conséquences

- Une technique non-normalisée risque de vous enfermer dans un seul vendeur,
- Si la norme ne prévoit pas une fonction, beaucoup d'utilisateurs n'en disposeront pas,
- Une partie des utilisateurs pourra toujours se débrouiller. Mais la masse ?

Comment fonctionne la normalisation sur l'Internet

Comment fonctionne la normalisation sur l'Internet

- Plusieurs SDO sont impliquées,

Comment fonctionne la normalisation sur l'Internet

- Plusieurs SDO sont impliquées,
- IEEE aux couches basses (Ethernet, WiFi. . .),

Comment fonctionne la normalisation sur l'Internet

- Plusieurs SDO sont impliquées,
- IEEE aux couches basses,
- IETF (*Internet Engineering Task Force*) aux couches moyennes (HTTP, DNS, BGP, QUIC...),

Comment fonctionne la normalisation sur l'Internet

- Plusieurs SDO sont impliquées,
- IEEE aux couches basses,
- IETF aux couches moyennes,
- W3C aux couches hautes (HTML, CSS...).

Plus précisément, l'IETF

Plus précisément, l'IETF

- Organisation internationale ouverte (tout le monde peut participer, tout est public),

Plus précisément, l'IETF

- Organisation internationale ouverte,
- Mais la participation nécessite temps et compétences,

Plus précisément, l'IETF

- Organisation internationale ouverte,
- Mais la participation nécessite temps et compétences,
- Normes librement et gratuitement disponibles (les RFC),

Plus précisément, l'IETF

- Organisation internationale ouverte,
- Mais la participation nécessite temps et compétences,
- Normes librement et gratuitement disponibles,
- Comme les autres SDO, n'a pas de pouvoir légal, pas de « police du protocole »,

Plus précisément, l'IETF

- Organisation internationale ouverte,
- Mais la participation nécessite temps et compétences,
- Normes librement et gratuitement disponibles,
- Comme les autres SDO, n'a pas de pouvoir légal, pas de « police du protocole »,
- L'Internet reste « sans permission ».

Un RFC


https://www.rfc-editor.org/info/rfc9156
RFC Editor
RFC 9156
DNS Query Name Minimisation to Improve Privacy, NOVEMBER 2021
File formats:
HTML
TEXT
PDF
XML
Status:
PROPOSED STANDARD
Obsoletes:
RFC 7816
Authors:
S. Bortzmeyer
R. Dolmans
P. Hoffman
Stream:
IETF
Source:
dnsop (ops)
Cite this RFC: TXT | XML
DOI: 10.17487/RFC9156
Discuss this RFC: Send questions or comments to dnsop@ietf.org

Hackathon de mise en œuvre des normes

Équipe mauritienne travaillant sur TLS 1.3, Wedgeantilles0, CC BY-SA 4.0 via Wikimedia Commons https ://commons.wikimedia.org/wiki/File :Hackers.mu_working_on_TLS_1.3_during_the_IETF_100_Hackathon.jpg

Étude de cas : TLS 1.3

Étude de cas : TLS 1.3

- Les versions précédentes de ce protocole cryptographique avaient des faiblesses,

Étude de cas : TLS 1.3

- Les versions précédentes de ce protocole cryptographique avaient des faiblesses,
- But de la version 1.3 : corriger ces faiblesses,

Étude de cas : TLS 1.3

- Les versions précédentes de ce protocole cryptographique avaient des faiblesses,
- But de la version 1.3 : corriger ces faiblesses,
- Mais certains les utilisaient, par exemple pour surveiller leurs employés,

Étude de cas : TLS 1.3

- Les versions précédentes de ce protocole cryptographique avaient des faiblesses,
- But de la version 1.3 : corriger ces faiblesses,
- Mais certains les utilisaient, par exemple pour surveiller leurs employés,
- Ils réclamaient un mécanisme de « visibilité »,

Étude de cas : TLS 1.3

- Les versions précédentes de ce protocole cryptographique avaient des faiblesses,
- But de la version 1.3 : corriger ces faiblesses,
- Mais certains les utilisaient, par exemple pour surveiller leurs employés,
- Ils réclamaient un mécanisme de « visibilité »,
- Grosse tourmente pendant des années à l'IETF,

Étude de cas : TLS 1.3

- Les versions précédentes de ce protocole cryptographique avaient des faiblesses,
- But de la version 1.3 : corriger ces faiblesses,
- Mais certains les utilisaient, par exemple pour surveiller leurs employés,
- Ils réclamaient un mécanisme de « visibilité »,
- Grosse tourmente pendant des années à l'IETF,
- Le RFC, publié en 2018, ne cède pas aux tenants de la « visibilité ».

Étude de cas : DoH

Étude de cas : DoH

- Le protocole DNS (les noms de domaine) reste un des rares protocoles Internet majoritairement en clair,

Étude de cas : DoH

- Le protocole DNS reste un des rares protocoles Internet majoritairement en clair,
- Deux normes techniques permettent de le chiffrer, DoT et DoH,

Étude de cas : DoH

- Le protocole DNS reste un des rares protocoles Internet majoritairement en clair,
- Deux normes techniques permettent de le chiffrer, DoT et DoH,
- Aucune objection sur le moment, DoT et surtout DoH sont allés très vite à l'IETF (normes simples, pas de questions techniques),

Étude de cas : DoH

- Le protocole DNS reste un des rares protocoles Internet majoritairement en clair,
- Deux normes techniques permettent de le chiffrer, DoT et DoH,
- Aucune objection sur le moment, DoT et surtout DoH sont allés très vite à l'IETF,
- C'est seulement après la parution du RFC en 2018 qu'il y a eu des protestations,

Étude de cas : DoH

- Le protocole DNS reste un des rares protocoles Internet majoritairement en clair,
- Deux normes techniques permettent de le chiffrer, DoT et DoH,
- Aucune objection sur le moment, DoT et surtout DoH sont allés très vite à l'IETF,
- C'est seulement après la parution du RFC en 2018 qu'il y a eu des protestations,
- Les gens qui avaient perdu en contrôle et en visibilité protestaient contre le fait que l'IETF ait normalisé DoH.

Étude de cas : QUIC

Étude de cas : QUIC

- Le principal protocole de transport de l'Internet est TCP (*Transmission Control Protocol*),

Étude de cas : QUIC

- Le principal protocole de transport de l'Internet est TCP,
- Son fonctionnement est en clair, ce qui fait fuiter des informations (même si la charge utile est chiffrée),

Étude de cas : QUIC

- Le principal protocole de transport de l'Internet est TCP,
- Son fonctionnement est en clair, ce qui fait fuiter des informations,
- Son possible successeur QUIC chiffre beaucoup plus,

Étude de cas : QUIC

- Le principal protocole de transport de l'Internet est TCP,
- Son fonctionnement est en clair, ce qui fait fuiter des informations,
- Son possible successeur QUIC chiffre beaucoup plus,
- Débat acharné à l'IETF sur **un seul bit**, le *spin bit*, qui redonnait des informations,

Étude de cas : QUIC

- Le principal protocole de transport de l'Internet est TCP,
- Son fonctionnement est en clair, ce qui fait fuiter des informations,
- Son possible successeur QUIC chiffre beaucoup plus,
- Débat acharné à l'IETF sur **un seul bit**, le *spin bit*, qui redonnait des informations,
- RFC publiés en 2021, pas encore trop de protestations.

En pratique

En pratique

- La normalisation est importante, elle facilite ou décourage certaines choses, elle est politique,

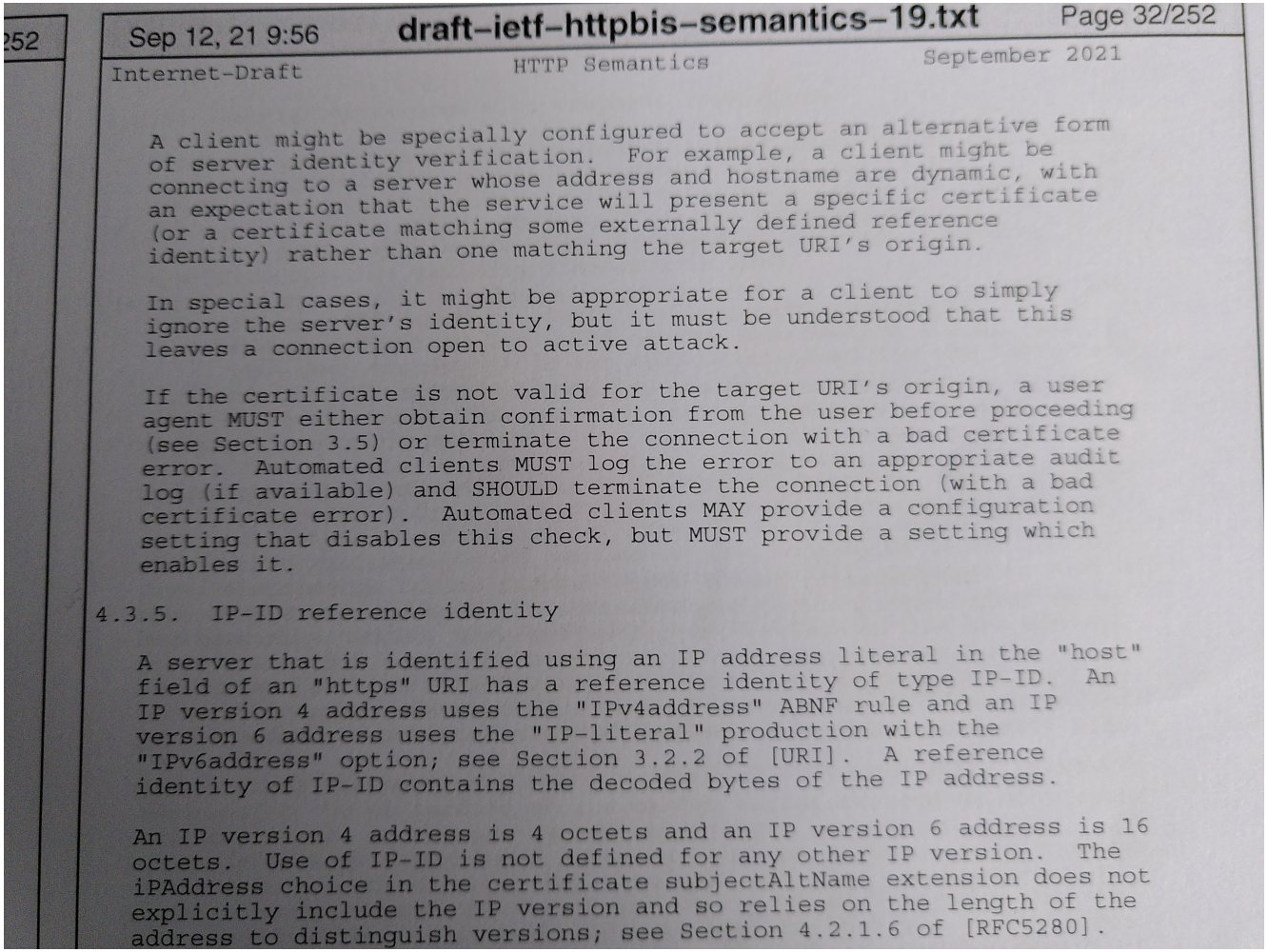
En pratique

- La normalisation est importante, elle facilite ou décourage certaines choses, elle est politique,
- Il est donc important de participer à l'IETF,

En pratique

- La normalisation est importante, elle facilite ou décourage certaines choses, elle est politique,
- Il est donc important de participer à l'IETF,
- Cela nécessite des efforts, et de la compétence technique.

Norme en cours de rédaction



252

Sep 12, 21 9:56 **draft-ietf-httpbis-semantics-19.txt** Page 32/252

Internet-Draft HTTP Semantics September 2021

A client might be specially configured to accept an alternative form of server identity verification. For example, a client might be connecting to a server whose address and hostname are dynamic, with an expectation that the service will present a specific certificate (or a certificate matching some externally defined reference identity) rather than one matching the target URI's origin.

In special cases, it might be appropriate for a client to simply ignore the server's identity, but it must be understood that this leaves a connection open to active attack.

If the certificate is not valid for the target URI's origin, a user agent MUST either obtain confirmation from the user before proceeding (see Section 3.5) or terminate the connection with a bad certificate error. Automated clients MUST log the error to an appropriate audit log (if available) and SHOULD terminate the connection (with a bad certificate error). Automated clients MAY provide a configuration setting that disables this check, but MUST provide a setting which enables it.

4.3.5. IP-ID reference identity

A server that is identified using an IP address literal in the "host" field of an "https" URI has a reference identity of type IP-ID. An IP version 4 address uses the "IPv4address" ABNF rule and an IP version 6 address uses the "IP-literal" production with the "IPv6address" option; see Section 3.2.2 of [URI]. A reference identity of IP-ID contains the decoded bytes of the IP address.

An IP version 4 address is 4 octets and an IP version 6 address is 16 octets. Use of IP-ID is not defined for any other IP version. The iPAddress choice in the certificate subjectAltName extension does not explicitly include the IP version and so relies on the length of the address to distinguish versions; see Section 4.2.1.6 of [RFC5280].