Développement de protocoles à l'IETF ; les RFC

Stéphane Bortzmeyer
AFNIC
bortzmeyer@nic.fr

8 juillet 2009

Le monde merveilleux de la normalisation

- W3C
- OASIS
- ISO (et ANSI et AFNOR)
- IEEE
- IEC
- ECMA
- ETSI
- ITU
- IETF...

Le monde merveilleux de la normalisation

- W3C
- OASIS
- ISO (et ANSI et AFNOR)
- IEEE
- ITU
- IETF...

Ces SDO sont très différentes en rapidité, ouverture, formalisme, statut, elles se distinguent aussi par leur périmètre d'activité...

Mon standard est plus ouvert que le tien

Tout le monde sait ce qu'est un logiciel libre.

Mon standard est plus ouvert que le tien

Tout le monde sait ce qu'est un logiciel libre.

Et une norme ouverte ? PDF, C#, MP3, MPEG4, 3G, SQL, ouverts ?

Mon standard est plus ouvert que le tien

Et une norme ouverte ? PDF, C#, MP3, MPEG4, 3G, SQL, ouverts ?

Critères possibles :

Mon standard est plus ouvert que le tien

Et une norme ouverte ? PDF, C#, MP3, MPEG4, 3G, SQL, ouverts ?

Critères possibles :

- Texte librement disponible

Mon standard est plus ouvert que le tien

Et une norme ouverte ? PDF, C#, MP3, MPEG4, 3G, SQL, ouverts ?

Critères possibles :

- Texte librement disponible
- Implémentable sans problème

Mon standard est plus ouvert que le tien

Et une norme ouverte ? PDF, C#, MP3, MPEG4, 3G, SQL, ouverts ?

Critères possibles :

- Texte librement disponible
- Implémentable sans problème
- Déjà mis en œuvre en logiciel libre

Mon standard est plus ouvert que le tien

Et une norme ouverte ? PDF, C#, MP3, MPEG4, 3G, SQL, ouverts ?

Critères possibles :

- Texte librement disponible
- Implémentable sans problème
- Déjà mis en œuvre en logiciel libre
- Développement et évolution de la norme de manière ouverte

Mon standard est plus ouvert que le tien

Et une norme ouverte ? PDF, C#, MP3, MPEG4, 3G, SQL, ouverts ?

Critères possibles :

- Texte librement disponible
- Implémentable sans problème
- Déjà mis en œuvre en logiciel libre
- Développement et évolution de la norme de manière ouverte

Mais il n'y a pas encore de consensus.

IETF

Internet Engineering Task Force

Responsable de la plupart des protocoles Internet dans les couches 3 à 4 (« TCP/IP »). Également active dans la couche 7.

`http://www.ietf.org/`

RFC

Le produit de l'activité de l'IETF : les *Request For Comments*.

RFC

Le produit de l'activité de l'IETF : les *Request For Comments*.

Quelques exemples :

- RFC 1 : logiciel des machines non-routeuses (à l'époque où les adresses étaient sur 5 bits)
- RFC 791 : IPv4
- RFC 1034/1035 : DNS
- RFC 1149 : IP sur pigeons voyageurs
- RFC 3031 : MPLS
- RFC 5585 : vue générale du protocole de signature du courrier DKIM (le dernier RFC paru à ce jour).

RFC

Le produit de l'activité de l'IETF : les *Request For Comments*.

Distribués librement et redistribuables, lisibles, ils sont un des principaux facteurs du succès de TCP/IP.

Les RFC ne sont pas toujours des normes

Les RFC ont un statut, « **chemin des normes** », mais aussi « pour information », « expérimental », etc.

Sur le chemin des normes, il y a trois étapes : proposition, projet et norme. L'avancement n'est pas automatique et dépend du travail de volontaires intéressés.

Les RFC sont écrits (pour la plupart) par l'IETF mais publiés par le *RFC editor*.

Licence des RFC

RFC 5377 et 5378

Licence des RFC

RFC 5377 et 5378

- Librement distribuable et traduisible

Licence des RFC

RFC 5377 et 5378

- Librement distribuable et traduisible
- Librement implémentable (sauf brevets)

Licence des RFC

RFC 5377 et 5378

- Librement distribuable et traduisible
- Librement implémentable (sauf brevets)
- **Non** modifiable. Plus exactement, seul le **code** est modifiable (ce qui permet son intégration dans les logiciels libres) pas le texte (la séparation est une nouveauté du RFC 5377, avant rien n'était modifiable).

Bureaucratie

Bureaucratie

L'IETF n'existe pas.

Aucune personne morale ne porte ce nom. L'IETF est une étiquette, posée sur une activité de l'ISOC.

Bureaucratie

L'IETF n'existe pas.

Aucune personne morale ne porte ce nom. L'IETF est une étiquette, posée sur une activité de l'ISOC.

Tout le monde peut adhérer, puisqu'il n'y a pas d'adhésion. Je suis donc **membre de l'IETF**.

Bureaucratie

L'IETF n'existe pas.

Aucune personne morale ne porte ce nom. L'IETF est une étiquette, posée sur une activité de l'ISOC.

Tout le monde peut adhérer, puisqu'il n'y a pas d'adhésion. Je suis donc **membre de l'IETF**.

L'administration est assurée par le Secrétariat, supervisé par l'IAOC. Contrairement au W3C, il n'y a pas de permanents.

Bureaucratie

Aucune personne morale ne porte ce nom. L'IETF est une étiquette, posée sur une activité de l'ISOC.

Tout le monde peut adhérer, puisqu'il n'y a pas d'adhésion. Je suis donc **membre de l'IETF**.

L'administration est assurée par le Secrétariat, supervisé par l'IAOC. Contrairement au W3C, il n'y a pas de permanents.

La propriété intellectuelle est gérée par l'*IETF trust*, organisme ISOC/CNRI.

Structuration

Le travail est découpé en **secteurs** (*areas*).

Exemples : Secteur Routage, Secteur Sécurité, Secteur Applications...

Chaque secteur a deux directeurs.

Les directeurs forment l'IESG, qui supervise le travail technique.

Les groupes de travail

Chaque secteur est à son tour découpé en **groupes de travail** (*WG, Working Group*). C'est là que sont développés les protocoles.

La création d'un groupe est souvent précédée d'une BoF (session informelle) et est approuvée par l'IESG.

Chaque groupe a deux présidents.

Les groupes de travail

Chaque secteur est à son tour découpé en **groupes de travail** (*WG, Working Group*). C'est là que sont développés les protocoles.

Par exemple, le secteur Applications comporte, entre autres :

- le groupe LTRU (*Language Tag Registry Update*), étiquettes de langue)
- le groupe SIEVE (langage de filtrage du courrier Sieve)
- le groupe HTTPBIS (révision du protocole HTTP 1.1)

Les groupes de travail

Chaque secteur est à son tour découpé en **groupes de travail** (*WG, Working Group*). C'est là que sont développés les protocoles.

Les groupes ont une durée de vie limitée, bornée par les jalons inscrits dans leur charte.

L'IAB

L'IESG travaille au quotidien, à superviser la production de normes.

L'*Internet Architecture Board* (IAB) regarde de haut et essaie de voir loin.

C'est l'IAB qui impulse les grands travaux et écrit les RFC solennels comme le 4924 sur la **neutralité du réseau**.

Fonctionnement

Un groupe de travail, c'est surtout une liste de diffusion. Le travail se fait là.

Les documents commencent leur vie comme *Internet-Draft*. Tout le monde peut en écrire un.

L'I-D a plusieurs versions, avec un numéro qui augmente (par exemple `draft-ietf-simple-xml-patch-ops-04`).

Après beaucoup de discussions, l'I-D peut être **adopté** par le groupe, ou bien rester document **individuel**.

Fonctionnement, suite

Après un *working group last call*, le document passe à l'IESG, qui peut faire un *IETF-wide last call*.

Une fois approuvé par l'IESG, il est envoyé au *RFC editor* pour publication.

Il n'y a pas de vote

We reject presidents, kings and voting. We believe in rough consensus and running code.

Les outils de travail

- Les listes de diffusion (publiques et archivées)
- Les réunions physiques (en théorie facultatives)
- Un peu d'IM
- `http://tools.ietf.org/`

Les exemples de groupes

Quelques activités intéressantes. . .

NCP

Problème : le DNS permet l'échange de **données** entre les serveurs de noms d'un domaine mais pas l'échange de **configuration**. Si je crée un nouveau domaine, je dois le configurer sur tous les serveurs faisant autorité.

NCP

Problème : le DNS permet l'échange de **données** entre les serveurs de noms d'un domaine mais pas l'échange de **configuration**. Si je crée un nouveau domaine, je dois le configurer sur tous les serveurs faisant autorité.

Solution : un nouveau protocole. La question a été lancée dans le groupe de travail **dnsop** (secteur Gestion & Opérations). Un I-D a été écrit.

NCP

Problème : le DNS permet l'échange de **données** entre les serveurs de noms d'un domaine mais pas l'échange de **configuration**. Si je crée un nouveau domaine, je dois le configurer sur tous les serveurs faisant autorité.

Solution : un nouveau protocole. La question a été lancée dans le groupe de travail **dnsop** (secteur Gestion & Opérations). Un I-D a été écrit.

Les présidents l'ont trouvé trop prématuré $\longrightarrow$ renvoyé à un petit *design team* pour proposer mieux.

NCP

Solution : un nouveau protocole. La question a été lancée dans le groupe de travail **dnsop** (secteur Gestion & Opérations). Un I-D a été écrit.

Les présidents l'ont trouvé trop prématuré $\longrightarrow$ renvoyé à un petit *design team* pour proposer mieux.

Draft du *design team* adopté par le WG. Travail encore en cours.

Cosmogol

Problème : les RFC utilisent souvent des automates à états finis. Mais il n'existe pas de langage formel pour cela. Ils sont en général décrits en art ASCII.

Cosmogol

Problème : les RFC utilisent souvent des automates à états finis. Mais il n'existe pas de langage formel pour cela. Ils sont en général décrits en art ASCII.

Solution : un langage, Cosmogol.
`http://www.cosmogol.fr/`

Cosmogol

Problème : les RFC utilisent souvent des automates à états finis. Mais il n'existe pas de langage formel pour cela. Ils sont en général décrits en art ASCII.

Solution : un langage, Cosmogol.
`http://www.cosmogol.fr/`

Une BoF a eu lieu pour le discuter. Pas assez d'intérêt dans l'IETF.

Cosmogol

Problème : les RFC utilisent souvent des automates à états finis. Mais il n'existe pas de langage formel pour cela. Ils sont en général décrits en art ASCII.

Solution : un langage, Cosmogol.
`http://www.cosmogol.fr/`

Une BoF a eu lieu pour le discuter. Pas assez d'intérêt dans l'IETF.

Projet aujourd'hui en sommeil

ABNF

L'IETF utilise beaucoup des grammaires formelles, écrites en ABNF.

ABNF

L'IETF utilise beaucoup des grammaires formelles, écrites en ABNF.

1. Préhistoire, chaque RFC définissait sa BNF,
2. RFC 2234, novembre 1997, proposition de norme,
3. RFC 4234, octobre 2005, projet de norme,
4. RFC 5234, janvier 2008, norme.

ABNF

1. Préhistoire, chaque RFC définissait sa BNF,
2. RFC 2234, novembre 1997, proposition de norme,
3. RFC 4234, octobre 2005, projet de norme,
4. RFC 5234, janvier 2008, norme.

Le processus a été long et sa dernière étape a nécessité un examen des implémentations, avec un rapport public.

Étiquettes de langue

Plusieurs protocoles ou formats ont besoin d'indiquer la langue comme XML avec `xml:lang` ou HTTP avec `Accept-Language`.

La langue est représentée par une **étiquette de langue** comme `fr` ou `ar-EG` ou `az-Latn-IR`.

Étiquettes de langue

Plusieurs protocoles ou formats ont besoin d'indiquer la langue comme XML avec `xml:lang` ou HTTP avec `Accept-Language`.

La langue est représentée par une **étiquette de langue** comme `fr` ou `ar-EG` ou `az-Latn-IR`.

- RFC 1766, mars 1995
- RFC 3066, janvier 2001
- RFC 4646, septembre 2006. Marque la création du registre des langues et l'ajout des dialectes et des écritures.
- RFC 4646bis, approuvé mais pas encore publié, date inconnue, intégre les macrolangues.

Étiquettes de langue

- RFC 1766, mars 1995
- RFC 3066, janvier 2001
- RFC 4646, septembre 2006. Marque la création du registre des langues et l'ajout des dialectes et des écritures.
- RFC 4646bis, approuvé mais pas encore publié, date inconnue, intégre les macrolangues.

Un travail du groupe LTRU.

MARID

Problème : authentifier le courrier électronique, de manière plus légère qu'avec PGP.

MARID

Problème : authentifier le courrier électronique, de manière plus légère qu'avec PGP.

Propositions sur la table : SPF, Sender-ID

1. Avril 2004 : création du groupe de travail MARID.

MARID

Problème : authentifier le courrier électronique, de manière plus légère qu'avec PGP.

Propositions sur la table : SPF, Sender-ID

1. Avril 2004 : création du groupe de travail MARID.
2. Mai 2004 : le groupe se dispute sur le brevet PRA de Microsoft et sur le choix technique de l'identité à tester.

MARID

Propositions sur la table : SPF, Sender-ID

1. Avril 2004 : création du groupe de travail MARID.
2. Mai 2004 : le groupe se dispute sur le brevet PRA de Microsoft et sur le choix technique de l'identité à tester.
3. Juillet 2004 : beaucoup d'acteurs extérieurs ont une autre solution à proposer et attaquent MARID.

MARID

Propositions sur la table : SPF, Sender-ID

1. Avril 2004 : création du groupe de travail MARID.
2. Mai 2004 : le groupe se dispute sur le brevet PRA de Microsoft et sur le choix technique de l'identité à tester.
3. Juillet 2004 : beaucoup d'acteurs extérieurs ont une autre solution à proposer et attaquent MARID.
4. Septembre 2004 : les discussions sur la licence du brevet PRA n'aboutissent pas. Le groupe est dissous d'autorité par l'IESG.

DNSSEC et la sécurité du DNS

Le DNS n'est pas sûr, on le sait et il est trop facile d'**empoisonner** un résolveur DNS (faille Kaminsky).

Comment le sécuriser ?

DNSSEC et la sécurité du DNS

Le DNS n'est pas sûr, on le sait et il est trop facile d'**empoisonner** un résolveur DNS (faille Kaminsky).

Comment le sécuriser ?

1. Sécuriser le canal entre serveurs de noms, pour être sûr de bien parler avec le bon serveur ?

DNSSEC et la sécurité du DNS

1. Sécuriser le canal entre serveurs de noms, pour être sûr de bien parler avec le bon serveur ?
2. Sécuriser les données DNS transportées, pour être sûr qu'elles ont bien été émises telles quelles par l'origine ? (DNSSEC, RFC 4033)

DNSSEC et la sécurité du DNS

1. Sécuriser le canal entre serveurs de noms, pour être sûr de bien parler avec le bon serveur ?
2. Sécuriser les données DNS transportées, pour être sûr qu'elles ont bien été émises telles quelles par l'origine ? (DNSSEC, RFC 4033)

Le débat existe pour tous les protocoles (PGP vs. SMTP+TLS pour le courrier).

DNSSEC et la sécurité du DNS

1. Sécuriser le canal entre serveurs de noms, pour être sûr de bien parler avec le bon serveur ?
2. Sécuriser les données DNS transportées, pour être sûr qu'elles ont bien été émises telles quelles par l'origine ? (DNSSEC, RFC 4033)

L'IETF (groupe de travail *DNS extensions*, alias *namedroppers*)a toujours privilégié DNSSEC, se méfiant même des solutions partielles comme les *cookies*.

Contournement des NAT

Les routeurs NAT (*Network Address Translation*) sont une des plaies de l'Internet. Fragiles, lents, ils perturbent beaucoup de protocoles (pair-à-pair, VoIP, ...).

Contournement des NAT

Les routeurs NAT (*Network Address Translation*) sont une des plaies de l'Internet. Fragiles, lents, ils perturbent beaucoup de protocoles (pair-à-pair, VoIP, ...).

L'IETF a historiquement estimé qu'ils devaient disparaître, balayés par IPv6.

Contournement des NAT

IPv6 n'ayant pas décollé, les NAT sont restés. Et l'IETF a fini, non sans douleur, par accepter un groupe de travail « Contournement du NAT », le groupe Behave.

- RFC 5389, STUN (trouver son adresse IP publique),
- RFC 5128, documentation des techniques utilisées par les logiciels pair-à-pair pour fonctionner malgré le NAT,
- RFC 4787, comportement des routeurs NAT pour ne pas trop gêner UDP.
- ...

Brevets

Toutes les SDO sont confrontées au problème des brevets. Faut-il normaliser une technologie brevetée ?

Brevets

Toutes les SDO sont confrontées au problème des brevets. Faut-il normaliser une technologie brevetée ?

Du fait de l'existence des **brevets futiles**, tout est breveté, dans au moins un pays. Si on refuse de normaliser ce qui est breveté, on ne normalise plus rien.

Brevets

Toutes les SDO sont confrontées au problème des brevets. Faut-il normaliser une technologie brevetée ?

La politique de l'IETF sur ce point est de **publication** :

1. Si un participant à l'IETF connait un brevet, il doit le dire.
2. L'IETF publie la liste des brevets connus, pour chaque RFC

L'implémenteur doit ensuite consulter son propre avocat :-(

État des lieux

L'IETF reste (avec peut-être le W3C et Oasis) l'organisation de normalisation la plus ouverte, à la fois dans son processus et dans ses résutats.

État des lieux

L'IETF reste (avec peut-être le W3C et Oasis) l'organisation de normalisation la plus ouverte, à la fois dans son processus et dans ses résutats.

Mais l'évolution de l'Internet lui échappe largement. Les vendeurs et FAI déploient le NAT, modifient les réponses DNS pour rediriger vers leur serveur de pub, malgré l'absence de normalisation, ou même en dépit des protestations de l'IETF. À l'inverse, IPv6 n'est pas déployé, malgré les travaux et proclamations de l'IETF.

Conclusion

L'IETF, c'est vous

Conclusion

L'IETF, c'est vous

Le processus est très ouvert, n'hésitez pas à participer. Devenez membre, relisez les *Internet-Drafts*, écrivez-en.