RFC 6730 : Requirements for IETF Nominations Committee tools

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 27 septembre 2012

Date de publication du RFC : Septembre 2012

https://www.bortzmeyer.org/6730.html

L'IETF dispose d'une institution curieuse, le **NomCom** ("*Nominations Committee*") qui est chargée de sélectionner des candidats pour des postes à l'IESG, l'IAB ou l'IAOC. Sa tâche d'examen des noms et de sélection nécessite un certain nombre d'outils informatiques, qui n'existent pas forcément tous à l'heure actuelle. Ce RFC est le cahier des charges des outils, pour servir de base aux futurs développements.

Tous les détails sur le NomCom et son fonctionnement sont spécifiés dans le RFC 7437[1]. On peut aussi consulter le site officiel <https://www.ietf.org/nomcom/>. Le NomCom dispose déjà d'un outil (accessible via le Web pour sa partie publique <https://www.ietf.org/group/nomcom/2012/>, mais il a aussi une partie privée <https://www.ietf.org/group/nomcom/2012/private/>, réservée aux membres du NomCom) mais qui est insuffisant. Notre nouveau RFC liste les nouveautés nécessaires pour cet outil. La première exigence, étiquetée META-001 est que le nouvel outil devra reprendre toutes les fonctions de l'ancien.

Ensuite, comme le NomCom travaille avec des données personnelles, la plupart des exigences du cahier des charges concernent la sécurité. Le logiciel stockera des noms, des appréciations, des opinions sur des personnes, etc, toutes choses assez sensibles. Il faudra un système d'authentification (exigences AUTH-001 à AUTH-003), capable de distinguer trois rôles (membre ordinaire de l'IETF, membre du NomCom, président du NomCom). Les membres ordinaires n'ont accès qu'à la partie publique. Ils se servent pour cela de leur compte `datatracker.ietf.org` (cf. RFC 6175, tout le monde peut se créer un compte avec cet outil puisque tout le monde peut participer à l'IETF).

Toutes les communications seront évidemment chiffrées et l'exigence SEC-001 demande que les données stockées le soient de telle façon qu'on minimise même leur exposition accidentelle (même

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc7437.txt`

l'administrateur ne doit les voir que sur une action explicite de sa part). Les données seront stockées chiffrées avec la clé publique du NomCom (exigences SEC-002 à SEC-005) et seront détruites à la fin de la sélection (toutes les données ne sont pas concernées, voir plus loin).

Moins cruciales, les autres exigences portent sur le processus de désignation des candidats (exigences NOM-001 à NOM-011) et sur l'enregistrement de l'acceptation ou du rejet car un candidat peut ne pas accepter sa désignation, qui a pu être faite par un tiers (exigences AD-001 à AD-007).

Enfin, l'outil devra gérer les réponses des candidats aux questionnaires qui leur seront soumis (≪ que ferez-vous si vous êtes élu à l'IAB ? ≫ (exigences QR-001 à QR-007) et surtout les retours des membres sur les candidatures (exigences FB-001 à FB-006). Ces retours, avis, et opinions forment une part essentielle du processus mais, malheureusement, les exigences d'ouverture et de sécurité ne sont pas faciles à concilier. Ainsi, les messages envoyés au NomCom par les membres sont archivés, contrairement aux autres données collectées par le NomCom (exigence FB-005).

On peut finir avec l'amusante annexe A de ce RFC, qui décrit les commandes OpenSSL nécessaires pour la gestion de la cryptographie dans l'outil du NomCom. La configuration (le fichier `nomcom-config.cnf`) ressemble à :

```
[ req ]
distinguished_name = req_distinguished_name
string_mask        = utf8only
x509_extensions    = ss_v3_ca

[ req_distinguished_name ]
commonName           = Common Name (e.g., NomcomYY)
commonName_default   = Nomcom12

[ ss_v3_ca ]

subjectKeyIdentifier = hash
keyUsage = critical, digitalSignature, keyEncipherment, dataEncipherment
basicConstraints = critical, CA:true
subjectAltName = email:nomcom12@ietf.org
extendedKeyUsage= emailProtection
# modify the email address to match the year.
```

Et on peut générer le certificat avec :

```
openssl req -config nomcom-config.cnf -x509 -new -newkey rsa:2048 \
   -sha256 -days 730 -nodes -keyout privateKey.pem \
   -out nomcom12.cert
```