

PREMIER MINISTRE

Secrétariat général  
de la défense  
et de la sécurité nationale

Agence nationale de la sécurité  
des systèmes d'information

Affaire suivie par : Florence ESSELIN

Paris, le

29 MAI 2012

N° *134* /ANSSI/RELEC

**Le directeur général  
de l'agence nationale de la sécurité des systèmes d'information**

à

**Monsieur Gary KOVACS, directeur général,  
MOZILLA CORPORATION**

Objet : Attestation de réalisation d'audits relatifs à l'IGC/A en 2011.

Références : 1. Politique de certification de l'IGC/A (OID 1.2.250.1.121.1.1.2 et 1.2.250.1.223.1.1.2).  
2. Référentiel général de sécurité ([www.ssi.gouv.fr/rgs](http://www.ssi.gouv.fr/rgs)).  
3. CA/Browser Forum, Baseline requirements for the Issuance and Management of Publicly-Trusted Certificates, v1.0.

Annexe : Courtesy translation.

Monsieur le Directeur,

Conformément à la politique de certification de l'infrastructure de gestion de clés publiques opérée par l'ANSSI, dite « IGC/A » (première référence), l'ANSSI procède systématiquement à l'audit préalable des autorités de certification (AC) demandant à être rattachées à l'IGC/A.

En 2011, il a été procédé à l'audit de certification initiale de l'AC racine du ministère de l'intérieur, de l'outre-mer, des collectivités territoriales et de l'immigration, les 6 et 8 décembre (audit documentaire) et les 12 et 13 décembre (audit sur site). Cet audit a été mené en conformité avec la politique de certification de l'IGC/A, et suivant les critères du référentiel général de sécurité (seconde référence), qui reprend notamment les exigences de l'ETSI TS 102 042.

La conclusion favorable de cet audit a conduit à accepter la demande de certification du ministère.

D'autre part, un exercice a été mené le 15 décembre 2011, dans le but d'éprouver la capacité de l'ANSSI à faire face à un incident majeur affectant son service de publication. Les résultats de cet exercice, mené en collaboration avec certains utilisateurs de l'IGC/A, ont été très positifs.

Enfin, l'audit de surveillance de l'AC racine IGC/A (disposant des certificats RSA2048-SHA1 et RSA4096-SHA2) a été mené les 19 et 21 décembre 2011 en intégrant les exigences du CA/Browser Forum (troisième référence).

Je vous prie d'agréer, monsieur le Directeur, l'expression de mes sentiments les plus distingués.



Patrick PAILLOUX  
Directeur général

Courtesy translation

Subject : 2011 IGC/A - Audits.

Dear Sir,

According to the PKI certification policy (see reference 1) of the French national Public Key Infrastructure “IGC/A”, ANSSI systematically performs a preliminary audit of any Certification Authority (CA) requesting certification by the IGC/A.

In 2011, initial audit of the French Ministry of Interior ' root CA was performed on December the 6<sup>th</sup> and the 8<sup>th</sup> (documentation audit) and on December the 12<sup>th</sup> and the 13<sup>th</sup> (onsite audit). This audit is compliant with the IGC/A's certification policy requirements, and followed the RGS (see reference 2) security standards which includes the ETSI TS 102 042 requirements.

The audit's conclusions have been positive and ANSSI has successfully certified this CA.

In addition, an exercise was led on December the 15<sup>th</sup> in order to test the ANSSI ability to face a major attack on the publication services. The exercise's conclusions have been positive.

At last, a surveillance audit has been performed on the IGC/A's root CA on December the 19<sup>th</sup> and 21<sup>st</sup>, following the CA/browser Forum requirements (see reference 3).

Best regards

Copie

MOZILLA CORPORATION

Kathleen WILSON