Print this page

Mozilla - CA Program

Case Information

Case Number	00000016	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owners/Certificate Name	Government of France (ANSSI, DCSSI)	**Request Status**	CA Action Items from Discussion

Additional Case Information

Subject	IGC/A Root Renewal Request	**Case Reason**	New Owner/Root inclusion requested

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org/show_bug.cgi?id=693450

General information about CA's associated organization

Company Website	http://www.ssi.gouv.fr/	**Verified?**	Verified
Organizational Type	Government Agency	**Verified?**	Verified
Organizational Type (Others)	ANSSI (Agence nationale de la sécurité des systèmes d'information) is the French Network and Information Security Agency, a part of the French Government. It issues certificates for French Government websites, which are used by the general public.	**Verified?**	Verified
Geographic Focus	France French embassies and consulates, French companies abroad and French people abroad, in particular in Europe for cross-border application. There is a growing number of e-services set up in France by French Administration (for people in France and French people abroad, but also for cross-border applications).	**Verified?**	Verified
Primary Market / Customer Base	IGC/A issues certificates to French ministries CAs that issue certificates both for their agents and for websites, which are used by the public. Each department has a sub CA; there are at least 20 at the moment, and potentially up to 60.	**Verified?**	Verified
Impact to Mozilla Users	The Mozilla users impacted will be French Government employees and citizens or companies (national ou international) using an e-service; for instance French people abroad may use electronic vote system in 2012 wherever there are located in the world (https servers doing SSL/TLS). It concerns also national and international contacts of the French governmental employees, which sign e-mails.	**Verified?**	Verified

Response to Mozilla's list of Recommended Practices

Recommended Practices	https://wiki.mozilla.org /CA:Recommended_Practices#CA_Recommended_Practices	**Recommended Practices Statement**	I have reviewed Mozilla's list of Recommended Practices, and confirm that we follow those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Recommended Practices	* Revocation of Compromised Certificates: Yes. See IGC/A root CA CP, page 34, and PC-type Authentication (RGS, annexe7) pages 38-42. * DNS names go in SAN: Yes. RGS_Profils_Certificat_LCR_OCSP_V2-3.pdf, page 19 : "il a DNS is present in the CommonName, RFC1123 section 2,1 must be fulfilled, in addition to be compliant with RFC1034.	**Verified?**	Verified

Response to Mozilla's list of Potentially Problematic Practices

Potentially Problematic Practices	https://wiki.mozilla.org /CA:Problematic_Practices#Potentially_problematic_CA_practices	**Problematic Practices Statement**	I have reviewed Mozilla's list of Potentially Problematic Practices, and confirm that we do not do those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Problematic Practices	* SSL certs are OV, with max lifetime 3 years. * Wildcard DV SSL certs are not allowed. * In the French governmental PKIs, the IT services or ISS agents validate each SSL certificate request. * All subCAs are operated by French governmental IT services and controlled by ISS services, audited by independent party or by ANSSI' auditors. * The Foreign office is the only department that delivers PKCS#12. The delivery is made through the private network of the ministry. The PKCS#12 has a secured password, and can be uploaded on the intranet server only. * communication@ssi.gouv.fr is used for complaints or questions.	**Verified?**	Verified

Root Case Record # 1

Root Case Information

Root Case No	R00000005	**Case Number**	00000016
Request Status	CA Action Items from Discussion	**Root Certificate Name**	IGC/A AC racine Etat francais

Additional Root Case Information

Subject	Include renewed IGC/A root

Technical Information about Root Certificate

O From Issuer Field	ANSSI	**Verified?**	Verified
OU From Issuer Field	0002 130007669	**Verified?**	Verified
Certificate Summary	This is the RSA4096-SHA256 root certificate of the French Government CA. The RSA2048-SHA1 IGC/A root certificate is currently included in NSS, as per bug #368970.	**Verified?**	Verified

Root Certificate Download URL	http://www.ssi.gouv.fr/IMG/crt/igcaRSA4096-072011.crt	**Verified?**	Verified
Valid From	2011 Jul 08	**Verified?**	Verified
Valid To	2028 Apr 15	**Verified?**	Verified
Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	SHA-256	**Verified?**	Verified
Signing Key Parameters	4096	**Verified?**	Verified
Test Website URL (SSL) or Example Cert	https://test4096.igc.agriculture.gouv.fr/	**Verified?**	Verified
CRL URL(s)	http://www.ssi.gouv.fr/fr/sigelec/igca/revocation/igca4096.crl http://igc-crl.agriculture.gouv.fr/crl/crl-ac-serveurs-standard.crl (NextUpdate: 6 days) Variables de Temps document: F_PUB_LCR = Minimal frequency of publication of the CRL = 72 hours or 24h)	**Verified?**	Verified
OCSP URL(s)	NEED -- OCSP URI in AIA of end-entity certs.	**Verified?**	Need Response From CA
Trust Bits	Code; Email; Websites	**Verified?**	Verified
SSL Validation Type	OV	**Verified?**	Verified
EV Policy OID(s)	Not EV	**Verified?**	Not Applicable
EV Tested		**Verified?**	Not Applicable
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	.fr, .gp, .gf, .mq, .re, .yt, .pm, .bl, .mf, .wf, .pf, .nc, .tf	**Verified?**	Verified

Digital Fingerprint Information

SHA-1 Fingerprint	1A:C9:2F:09:EA:89:E2:8B:12:6D:FA:C5:1E:3A:F7:EA:90:95:A3:EE	**Verified?**	Verified
SHA-256 Fingerprint	1E:1A:69:84:B4:E7:6B:D7:09:AE:E3:E9:C9:CF:31:18:EA:C0:96:DA:B9:CC:20:DC:25:FA:AB:67:29:7E:96:5A	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	CA Hierarchy: https://bugzilla.mozilla.org/attachment.cgi?id=566036 This root CA has signed these internally-operated sub-CAs: - AC racine Gendarmerie nationale : Direction générale de la Gendarmerie nationale - 15/04/2010 - OID : 1.2.250.1.223.1.1.1 - AC racine Diplomatie : Ministère des Affaires étrangères et européennes - 21/07/2010 - V1.0 - OID : 1.2.250.1.223.1.1.1 - AC racine ministère en charge de l'agriculture : Ministère de l'agriculture - 08/12/2010 - OID : 1.2.250.1.223.1.1.1 - AC racine Ministère de l'Intérieur : Ministère de l'Intérieur - 22/12/2011 - OID : 1.2.250.1.223.1.1.1	**Verified?**	Verified

Externally Operated SubCAs	None. All subCAs are operated by French governmental IT services and controlled by ISS services.	**Verified?**	Verified
Cross Signing	None	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	The subCA must (legal obligation) be compliant with the "référentiel général de sécurité" or "RGS" - the national IT security reference book. It defines certificates profiles and both technical and organizational constraints. http://www.ssi.gouv.fr/fr/reglementation-ssi/referentiel-general-de-securite/liste-des-documents-constitutifs-du-rgs-v1-0.html	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	Documents are in French. IGCA-PC: http://www.ssi.gouv.fr/IMG/pdf/IGCA_PC_v2-1.pdf This document explains how the root and sub CA certificates are generated. Also explains which type of end-users certificates can be issued by subCA.	**Verified?**	Verified
CA Document Repository	http://www.ssi.gouv.fr/fr/reglementation-ssi/referentiel-general-de-securite/	**Verified?**	Verified
CP Doc Language	French		
CP	http://www.ssi.gouv.fr/IMG/pdf/RGS_PC-Type_Authentification_Serveur_V2-3.pdf	**Verified?**	Verified
CP Doc Language	French		
CPS	http://www.ssi.gouv.fr/IMG/pdf/IGCA_PC_v2-1.pdf	**Verified?**	Verified
Other Relevant Documents	CP for e-sign certs for servers: http://www.ssi.gouv.fr/IMG/pdf/RGS_PC-Type_Cachet_V2_3.pdf CP for email certs: http://crl.diplomatie.gouv.fr/AC_Utilisateurs/AC_UTILISATEURS_PC_Signature_Agent_V1.5.pdf http://crl.diplomatie.gouv.fr/AC_Utilisateurs/AC_UTILISATEURS_PC_Signature_Externe_V1.3.pdf http://www.ssi.gouv.fr/IMG/pdf/RGS_Variables_de_temps_V2-3.pdf FAQ: http://www.ssi.gouv.fr/fr/menu/pied-de-page/aide-et-accessibilite/foire-aux-questions/faq-igc-a.html	**Verified?**	Verified
Auditor Name	French Government	**Verified?**	Verified
Auditor Website	http://www.ssi.gouv.fr/site_rubrique31.html Auditor: French Secretariat Général de la Défense Nationale (French national security authority)	**Verified?**	Verified
Auditor Qualifications	Government	**Verified?**	Verified
Standard Audit	http://www.ssi.gouv.fr/fr/anssi/services-securises/igc-a/attestation-audits.html	**Verified?**	Verified
Standard Audit Type	ETSI TS 102 042	**Verified?**	Verified
Standard Audit Statement Date	11/15/2013	**Verified?**	Verified
BR Audit	NEED -- see https://wiki.mozilla.org/CA:BaselineRequirements#ETSI_BR_Audit_Statement.2FCertificate	**Verified?**	Need Response From CA
BR Audit Type		**Verified?**	Need Response From CA

BR Audit Statement Date		**Verified?**	Need Response From CA
EV Audit		**Verified?**	Not Applicable
EV Audit Type		**Verified?**	Not Applicable
EV Audit Statement Date		**Verified?**	Not Applicable
BR Commitment to Comply	NEED -- see https://wiki.mozilla.org/CA:BaselineRequirements#CA_Conformance_to_the_BRs	**Verified?**	Need Response From CA
SSL Verification Procedures	RGS_PC-Type_Authentification_Serveur_V2-3.pdf is dedicated to SSL authentication and describes the minimum rules imposed on all subCAs regarding verification procedures that must be used by all French administrative CA issuing SSL certificates. Page 25: The recording of a server to which a certificate must be delivered is made via the recording of the corresponding RCAS (i.e. person responsible for the use of the certificate). The RCAS will have to demonstrate that the name of the domain included in the FQDN of the server belongs really to the entity represented by the RCAS. A RCAS can be brought to change during the current validity of the SSL certificate of the corresponding server. In that case, every new RCAS also has to be the object of a recording procedure. The recording of a RCAS, and a corresponding IT server, can be made either directly with the registration authority (RA), or via a representative of certification of the entity (called MC). In the last case the MC must be beforehand recorded by the RA."	**Verified?**	Verified
EV SSL Verification Procedures		**Verified?**	Not Applicable
Organization Verification Procedures	RGS_PC-Type_Authentification_Serveur_V2-3.pdf Page 26: In order for a certificate request to be accepted, the request must include at least: - A written certificate request, dated less than 3 months, signed by a legal representative of the entity, mentioning FQDN concerned ; - A mandate dated less than 3 months, appointing the future RCAS as being authorized to be RCAS for the one or many machines on which will be deployed the SSL certificate. This mandate must be signed by a legal representative of the entity and signed jointly, for acceptance, by the future RCAS; - A document, valid the day of recording, mentioning delegation or sub-delegation of the authority responsible for the administrative entity ; - An official document of identity (id card or passport) of current validity, of the future RCAS, containing a photo, which is presented to the RA which keeps a copy ; - A proof of ownership by the entity of the FQDN of the server; - The e-mail address allowing the RA to contact the RCAS ; - The general conditions of use signed. In addition, French governmental servers must have .gouv.fr domain names, and these domain names are given through a restricted manual procedure. Then there is at least a double control of the ability of a RCAS to manage SSL certificate. Also see IGCA-PC section 3.2.	**Verified?**	Verified
Email Address Verification Procedures	According to IGCA-PC, as far as end entities are administrative agents, the e-mail addresses are stored in Active or e-mail servers directories. PKI refers to these directories for a technical verification. An organizational verification is lead also by the subscriber hierarchy, which validates the certification request, and by the RA which is often the IT service. As an example, see CP for email certs for people working for the Foreign Affairs Ministry: http://crl.diplomatie.gouv.fr/AC_Utilisateurs/AC_UTILISATEURS_PC_Signature_Agent_V1.5.pdf Section 3.1.2: email address must be of the form surname.name@diplomatie.gouv.fr	**Verified?**	Verified

	Section 4.1.2: Information required: · The certificate profile; · The full name of the bearer; · The unique identifier (logon at); · The agent code (identifier at); · The email address of the bearer. Section 4.2.1: Formal validation by the database AROBAS, containing all agents' e-mail addresses. See also AC_UTILISATEURS_PC_Signature_Externe_V1.3.pdf Section 4.2.1: For people of another ministry or organization working with the French foreign office, the certification request is send by paper or electronic mail to a representative of certification of the entity (called MC), who knows the e-mail address of the requestor. MC controls e-mail address, and send the request to the RA. The diagram on page 27 shows that the requestor receive a pkcs#12 encrypted with a password. This password is send to the MC, who sends it then to the requestor.		
Code Signing Subscriber Verification Pro	The code signing subscriber verification procedure must be compliant with the procedure in CP for e-sign certs for servers: http://www.ssi.gouv.fr/IMG/pdf/RGS_PC-Type_Cachet_V2_3.pdf III. IDENTIFICATION AND AUTHENTICATION III.2. Initial validation of the identity III.2.2. Validation of the identity of an organization III.2.3. Validation of the identity of an individual III.2.5. Validation of the authority of the applicant: “This step is performed in conjunction with the validation of the identity of the person (directly by the EA or the MC).”	**Verified?**	Verified
Multi-Factor Authentication	All administrators or operators use a multifactor authentication (smart cards or USB token).	**Verified?**	Verified
Network Security	All governmental PKIs are hosted in secured networks, without any direct access to Internet. These networks are monitored, and ANSSI make regular inspections/technical audits testing weakness and ensuring IDS and other monitoring software are up-to-date, and best practices are in place. Root and first level subCAs are off line, and RGS imposes revocation in case of suspicion of compromise, we can confirm to be able to shut down certificate issuance quickly if alerted of intrusion.	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	http://www.ssi.gouv.fr/fr/anssi/services-securises/igc-a/certificats-et-liste-de-revocation-emis-par-l-igc-a-rsa-2048.html	**Verified?**	Verified