Bugzilla ID: 693450
Bugzilla Summary: Add IGC/A RSA4096 SHA256 root certificate

CAs wishing to have their certificates included in Mozilla products must

1) Comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/)
2) Supply all of the information listed in http://wiki.mozilla.org/CA:Information_checklist.
    a. Review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices
    b. Review the Potentially Problematic Practices at https://wiki.mozilla.org/CA:Problematic_Practices

General information about the CA's associated organization

CA Company Name	ANSSI (Government of France)
Website URL	http://www.ssi.gouv.fr/
Organizational type	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. Each department has a sub CA; there are at least 20 at the moment, and potentially up to 60.
Primark Market / Customer Base	IGC/A root CA issues certificates to French ministries CA. These CA issue certificates both for their agents and for websites, which are used by the public. Primary geographical area(s) served : 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). They require more and more electronic certificates. In this perspective, the IGC/A certificate should not be only available in France.
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.
CA Contact Information	CA Email Alias: igca@ssi.gouv.fr CA Phone Number:+33 (0)1 71 75 81 22 Title/Department: SGDSN/ANSSI/ACE/BAC

Technical information about each root certificate

Certificate Name	IGC/A AC racine Etat francais
Certificate Issuer Field	CN = IGC/A AC racine Etat francais OU = 0002 130007669 O = ANSSI C = FR
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. The IGC/A root issues subordinate CAs for government or administrative organizations only. Each of these subordinate CAs may issue end-entity certificates or additional subordinate CAs to be used for divisions within that organization. Each organization is required to follow the CP and the Government RGS, and be audited.

Root Cert URL	http://www.ssi.gouv.fr/IMG/crt/igcaRSA4096-072011.crt
SHA1 Fingerprint	1A:C9:2F:09:EA:89:E2:8B:12:6D:FA:C5:1E:3A:F7:EA:90:95:A3:EE
Valid From	2011-07-08
Valid To	2028-04-15
Certificate Version	3
Signature Algorithm	PKCS #1 SHA-256 With RSA Encryption
Modulus	4096
Test Website URL	https://test4096.igc.agriculture.gouv.fr/
CRL URL	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)
OCSP URL	OCSP not provided
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code Signing
SSL Validation Type	OV
EV Policy OID(s)	N/A

CA Hierarchy information for each root certificate

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
External SubCAs	None. All subCAs are operated by French governmental IT services and controlled by ISS services.
Cross-Signing	None
Technical Constraints on Third-party Issuers	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

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. Section 1.5.1: IGC/A (root CA) delivers CA certificates and CRL only. All IGC/A's subCA must be governmental CA. Any CA that do not belong to the French Administration is not allowed in the IGC/A trust domain. CP/CPS dedicated to some subCA must precise the CA is allowed to deliver certificates to French Administration CA, or people working on behalf of Administration, or servers operated under the Administration responsibility.

	Certificate types can be one of the following, mentioned in the "RGS" which is mandatory for Administration CA: - "authentification" = authentication (human) - "signature" = e-signature (human) - (e-mail signature or any other type of document) - "confidentialité" = enciphering (human) - (e-mail encryption or any other data encryption) - "authentification serveur" = SSL/TLS authentication - "cachet serveur" = e-sign for servers CP for SSL/TLS authentication certs: http://www.ssi.gouv.fr/IMG/pdf/RGS_PC-Type_Authentification_Serveur_V2-3.pdf 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 for people working for the Foreign Affairs Ministry: http://crl.diplomatie.gouv.fr/AC_Utilisateurs/AC_UTILISATEURS_PC_Signature_Agent_V1.5.pdf CP for email certs for people working for another Administration working with the Foreign Affairs Ministry: http://crl.diplomatie.gouv.fr/AC_Utilisateurs/AC_UTILISATEURS_PC_Signature_Externe_V1.3.pdf Variables de Temps: http://www.ssi.gouv.fr/IMG/pdf/RGS_Variables_de_temps_V2-3.pdf IGC/A FAQ: http://www.ssi.gouv.fr/fr/menu/pied-de-page/aide-et-accessibilite/foire-aux-questions/faq-igc-a.html
Audits	Audit Type: ETSI TS 102042 and compliance with IGC/A CP Auditor: French Secretariat Général de la Défense Nationale (French national security authority) Auditor Website: http://www.ssi.gouv.fr/site_rubrique31.html Surveillance Audit Statement: https://bug666771.bugzilla.mozilla.org/attachment.cgi?id=557633 (2010.12.20) Statement about Audits relating to IGC/A: http://www.ssi.gouv.fr/fr/anssi/services-securises/igc-a/attestation-audits.html
SSL Verification Procedures	CP for SSL/TLS authentication certs: http://www.ssi.gouv.fr/IMG/pdf/RGS_PC-Type_Authentification_Serveur_V2-3.pdf This CP 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." 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.
Organization Verification Procedures	See IGCA-PC sections: 3.2 Validation Initial Identity 3.2.2 Validation of the identity of the administrative authority (AA) 3.2.3 Validation of the identity of the root CA 3.2.4 Validation of the identity of the applicant, agent or witness 3.2.6 Validation of Authority of Applicant: "The AE of the IGC/A can contact the FSSI, the HFD or HFDS a relevant ministry to ensure the authority of the applicant with the AA concerned by the application."
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 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 CP for email certs for people working for another Administration working with the Foreign Affairs Ministry: http://crl.diplomatie.gouv.fr/AC_Utilisateurs/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 Procedures	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)."
Multi-factor Authentication	All administrators or operators use a multifactor authentication (smart cards or USB token).
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.

Response to Mozilla's CA Recommended Practices (https://wiki.mozilla.org/CA:Recommended_Practices)

Publicly Available CP and CPS	Yes
CA Hierarchy	Yes
Audit Criteria	Yes
Document Handling of IDNs in CP/CPS	N/A
Revocation of Compromised Certificates	Yes. See IGC/A root CA CP, page 34, and PC-type Authentication (RGS, annexe7) pages 38-42.
Verifying Domain Name Ownership	Yes
Verifying Email Address Control	Yes
Verifying Identity of Code Signing Certificate Subscriber	Yes
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.
Domain owned by a Natural Person	Not allowed.
OCSP	N/A

Response to Mozilla's list of Potentially Problematic Practices (https://wiki.mozilla.org/CA:Problematic_Practices)

Long-lived DV certificates	SSL certs are OV, with max lifetime 3 years.
Wildcard DV SSL certificates	Wildcard DV SSL certs are not allowed.
Email Address Prefixes for DV Certs	N/A
Delegation of Domain / Email validation to	In the French governmental PKIs, the IT services or ISS agents validate each SSL certificate request.

third parties	
Issuing end entity certificates directly from roots	No
Allowing external entities to operate subordinate CAs	All subCAs are operated by French governmental IT services and controlled by ISS services, audited by independent party or by ANSSI' auditors.
Distributing generated private keys in PKCS#12 files	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.
Certificates referencing hostnames or private IP addresses	Not allowed (see RGS annexe 13).
Issuing SSL Certificates for Internal Domains	Not allowed
OCSP Responses signed by a certificate under a different root	N/A
CRL with critical CIDP Extension	No
Generic names for CAs	No
Lack of Communication With End Users	communication@ssi.gouv.fr is used for complaints or questions.