Bugzilla ID: 368970
Bugzilla Summary: Add French Government (DCSSI) CA certificate

CAs wishing to have their certificates included in Mozilla products must comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/) and must supply the information necessary to determine whether or not the policy's requirements have been satisfied.

General Information	**Data**
CA Name	DCSSI (Central Information Systems Security Division)
Website URL (English version)	http://www.ssi.gouv.fr/fr/sigelec/igca/
Organizational type. (E.g., whether the CA is operated by a private or public corporation, government agency, academic institution or consortium, NGO, etc.)	DCSSI is a part of the French Government.
Primary market / customer base. (Which types of customers does the CA serve? Are there particular vertical market segments in which it operates? Does it focus its activities on a particular country or other geographic region?)	DCSSI issues certificates to 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. Primary geographical area(s) served : France, French ambassadies and PCs of French people abroad, 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

Comment #25: Please close our request for the DSA certificate – the key was created for backup purpose in case of a cryptographic matter with RSA. It hasn't be used yet, and we will soon use another key for this purpose. Then there is no need to include the DSA certificate anymore.

For Each Root CA whose certificate is to be included in Mozilla (or whose metadata is to be modified)

Info Needed	**RSA Cert**	**Status / Notes**
Certificate Name	IGC/A	COMPLETE
Cert summary / comments	This is the root certificate of the French Government CA. The IGC/A root issues a subordinate CA for each organization, which can be only a government or an administrative organization. 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/PRIS, and be audited.	COMPLETE
The root CA certificate URL	http://www.ssi.gouv.fr/fr/sigelec/igca/cert_igca_rsa.crt	COMPLETE

SHA-1 fingerprint.	60:D6:89:74:B5:C2:65:9E:8A:0F:C1:88:7C:88:D2:46:69:1B:18:2C	COMPLETE
Valid from	2002-12-13	COMPLETE
Valid to	2020-10-17	COMPLETE
Cert Version	3	COMPLETE
Modulus length / key length	2048	COMPLETE
CRL - URL - update frequency for end-entity certificates	http://www.ssi.gouv.fr/fr/sigelec/igca/revocation/igca.crl For end-entities, the CRLs frequency update is 24h (as specified in http://www.synergies-publiques.fr/IMG/pdf/RGS_Variables_de_temps_V2.1.pdf).	COMPLETE
OCSP (if applicable) - OCSP Responder URL - Max time until OCSP responders updated to reflect end-entity revocation	Not Applicable	COMPLETE
List or description of subordinate CAs operated by the CA organization associated with the root CA. (For example, this might include subordinate CAs created to issue different classes or types of end entity certificates: Class 1 vs. class 2 certificates, qualified vs. non-qualified certificates, EV certificates vs. non-EV certificates, SSL certificates vs. email certificates, and so on.) For internally-operated subordinate CAs the key is to confirm that their operation is addressed by the relevant CP/CPS, and that any audit covers them as well as the root.	Cert Hierarchy diagram is on page 15 of the CP: http://www.ssi.gouv.fr/fr/sigelec/igca/igca-pc-v2.pdf See IGC/A CP, ch.1.4.PKI Participants, especially p. 18, 1.4.3.End entity certificates. In a nutshell: Subordinate CAs are only governmental CAs (current) and administrative authorities* CAs (planned). * as defined in the order no.2005-1516 of 8th December 2005. [verified via Google Translate] Governmental CAs must respect the following rules : - the subscriber must be a French official - the CA must federate all subordinated CA belonging to the administrative authority involved ; exceptions can't be accepted without the agreement of the Defense and Security Officer of the authority involved - CA must have an auto-signed certificate and sign ARL - CA must be able to audit the PKI and to allow DCSSI to audit or make audit the statements. IGC/A CP, §1.5.1 – certificate usage (short translation):	COMPLETE

	As a condition for IGC/A issuing certificates, all CA certificates chaining up to IGC/A root CA must belong to one or more French administrative authority (AA). Subordinate CAs must restrict certificate issuance to : - CA of an Administrative Authority; - person for authentication, e-signature and confidentiality in applications on the authority's duty - servers under the exclusive authorities' responsibility for SSL/TLS authentication, signature and timestamp ; - authorities for code signing. *** N.B. : Certificates are not used for commercial purposes. They are used only for administrative exchanges.	
For subordinate CAs operated by third parties, if any: General description of the types of third-party subordinates that exist, and what the general legal/technical arrangements are by which those subordinates are authorized, controlled, and audited. (For example, contractual arrangements should require third-party subordinates to operate in accordance with some CPS/CP. Technical arrangements might include name constraints, not allowing them to create their own subordinates, etc.)	The IGC/A root does not sign sub-CAs for private companies. The IGC/A root issues a subordinate CA for each organization, which can be only a government or an administrative organization. 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/PRIS, and be audited. Some sub-CAs may be operated on behalf of the French administration. The RGS compels private operators to conform to RGS/PRIS profiles and to be referenced (certified by an accredited certification body). Under French Law they would have to comply with RGS: http://www.ssi.gouv.fr/fr/RGS/index.html PRIS: http://www.synergies-publiques.fr/article.php?id_article=945 And http://www.synergies-publiques.fr/IMG/pdf/061129_PRIS_US_ENISA.pdf	COMPLETE
List any other root CAs that have issued cross-signing certificates for this root CA	None	COMPLETE
Requested Trust Bits One or more of: • Websites (SSL/TLS) • Email (S/MIME) • Code (Code Signing)	Websites Email Code	COMPLETE

If SSL certificates are issued within the hierarchy rooted at this root CA certificate: • Whether or not the domain name referenced in the certificate is verified to be owned/controlled by the certificate subscriber. (This is commonly referred to as a DV certificate.) • Whether or not the value of the Organization attribute is verified to be that associated with the certificate subscriber. (This is commonly referred to as an OV certificate.) • Whether verification of the certificate subscriber conforms to the Extended Validation Certificate Guidelines issued by the CAB Forum. (This is commonly referred to as an EV certificate.)	IV/OV Identities of persons are verified as described in chapter 3.2 and 4.2 of the PRIS documents. The FQDN is also verified.	COMPLETE
Example certificate(s) issued within the hierarchy rooted at this root, including the full certificate chain(s) where applicable. • For SSL certificates this should also include URLs of one or more web servers using the certificate(s). • There should be at least one example certificate for each of the major types of certificates issued, e.g., email vs. SSL vs. code signing, or EV vs. OS vs. DV. • Note: mainly interested in SSL, so OK if no email example.	https://www.journal-officiel.gouv.fr	COMPLETE

CP/CPS • Certificate Policy URL • Certificate Practice Statement(s) (CPS) URL (English or available in English translation)	About DCSSI http://www.ssi.gouv.fr/en/dcssi/index.html Policies and other useful information specific to this root http://www.ssi.gouv.fr/fr/sigelec/igca/ Certificate Policy: http://www.ssi.gouv.fr/fr/sigelec/igca/igca-pc-v2.pdf Repository General Security (RGS) Website: http://www.ssi.gouv.fr/fr/RGS/index.html French law (order no.2005-1516 of 8th december 2005 – on electronic exchanges between users and administrative authorities and between administrative authorities) compels CAs delivering end-entity certificates to be compliant with the IT security general referential. PRIS = Politique de Référencement Intersectorielle de Sécurité = Policy List Intersectoral Security The page where all documents of PRIS 2.2 are now available : http://www.synergies-publiques.fr/article.php?id_article=945 Summary of PRIS: http://www.synergies-publiques.fr/IMG/pdf/061129_PRIS_US_ENISA.pdf A brief presentation of the requirements and the scheme to agree trustworthy service providers (administrative authorities as well as private companies delivering certificates for exchanges between users and the French administration). Variables de temps (for CRL frequency update) http://www.synergies-publiques.fr/IMG/pdf/RGS_Variables_de_temps_V2.1.pdf PC-Type authentification servers (for SSL) http://www.synergies-publiques.fr/IMG/pdf/RGS_Service_Authentification_Serveur_V2.2.pdf PC-Type authentification http://www.synergies-publiques.fr/IMG/pdf/RGS_PC-Type_Authentification_V2.2.pdf Profiles de certificats, LCR et OCSP	COMPLETE

	http://www.synergies-publiques.fr/IMG/pdf/RGS_Profils_Certificat_LCR_OCSP_V2_2.pdf PC-Type cachet server http://www.synergies-publiques.fr/IMG/pdf/RGS__PC-Type_Cachet_Serveur_V2.2.pdf PC-type signature : http://www.synergies-publiques.fr/IMG/pdf/RGS_PC-Type_Signature_V2.2.pdf (PRIS 2.1 documents I mentionned are still available : http://www.synergies-publiques.fr/IMG/pdf/PRISv2.1_-_PC-Type_Signature.pdf)	
AUDIT: The published document(s) relating to independent audit(s) of the root CA and any CAs within the hierarchy rooted at the root. (For example, for WebTrust for CAs audits this would be the “audit report and management assertions” document available from the webtrust.org site or elsewhere.)	Audit Type: WebTrust CA Equivalent Auditor: French Secretariat Général de la Défense Nationale, which acts as the French national security authority Auditor Website: http://www.ssi.gouv.fr/fr/RGS/index.html Official decision for IGC/A homologation: http://www.ssi.gouv.fr/fr/sigelec/igca/igca-homologation.pdf IGC/A has been accredited by the ISS central director (he is the French INFOSEC authority for UE). The statement of this accreditation can be transmitted to you. Compared to the initial audit, this process implies regular audits to maintain the accreditation, giving an assurance that the level of security is maintained.	COMPLETE

Review CPS sections dealing with subscriber verification (COMPLETE – verified using Google Translate)
(Section 7 of http://www.mozilla.org/projects/security/certs/policy/)

- Verify domain check for SSL
    - http://www.synergies-publiques.fr/IMG/pdf/RGS__PC-Type_Authentification_Serveur_V2.2.pdf
    - http://www.references.modernisation.gouv.fr/sites/default/files/RGS_%20PC-Type_Authentification_Serveur_V2_2.pdf
    - Page 26
    - [Server-server] means the sentence concerns SSL/TLS servers, and “RCAS” means the one responsible for the SSL certificate as mentioned page 12
    - Chapter III.2 explains conditions about identity. It precises that the RCAS must prove that the server belongs to the entity the RCAS represents, and that the domain name belongs to this entity.
    - Chapter IV explains that the RA must verify identity as defined in chapter III.2, and must check the FQDN
        - 4.2.1.Identication and validation of application process
            - Identities of persons are verified as described in chapter 3.2.

        - RA must: - validate FQDN of the server the certificate delivered refers to
- Verify the email account associated with the email address in the cert is owned by the subscriber. In addition to verification of subscriber's legal identity.
    - The RA (AE in French) is responsible of verifying information concerning the certificate holder, then this include verifying the association with email address - see section 4.2.1 of http://www.synergies-publiques.fr/IMG/pdf/RGS_PC-Type_Signature_V2.2.pdf The RA must "vérifier la cohérence des justificatifs présentés" = check the consistency of the evidence
    - Comment #27: "I translated "vérifier la cohérence des justificatifs présentés" as "check coherence of relevant documents". These "relevant documents" are in fact all pieces of the registration file, including e-mail adress. Consequently the RA verify e-mail address like any other information about end-entity and about the organization or company the end-entity belongs to; an end-entity submitting the request can't give an e-mail address without the agreement of the legal representative of the organization the end-entity belongs to and vice-versa.
- Verify identity info in code signing certs is that of subscriber
    - PRIS , PC-Type cachet serveur
    - http://www.synergies-publiques.fr/IMG/pdf/RGS__PC-Type_Cachet_Serveur_V2.2.pdf
        - 3.2 Initial identity validation
        - 3.2.3 Subscriber identity validation
        - 4. Certificate Life-Cycle Operational Requirements
        - 4.2. Certificate Application Processing
- Make sure it's clear which checks are done for which context (cert usage)
    - There are different PRIS documents based on cert usage.

Flag Problematic Practices
(http://wiki.mozilla.org/CA:Problematic_Practices)

- 1.1 Long-lived DV certificates
    - No. SSL certs are IV/OV.
- 1.2 Wildcard DV SSL certificates
    - No. SSL certs are IV/OV.
- 1.3 Issuing end entity certificates directly from roots
    - No. IGC/A root delivers only CA certificates.
- 1.4 Allowing external entities to operate unconstrained subordinate CAs
    - Yes. The external entities (government or an administrative organization) are required to follow the CPS and the Government Laws of RGS/PRIS and be audited. See information provided above.
- 1.5 Distributing generated private keys in PKCS#12 files
    - No
- 1.6 Certificates referencing hostnames or private IP addresses
    - No
- 1.7 OCSP Responses signed by a certificate under a different root

  - Not applicable
- 1.8 CRL with critical CIDP Extension
  - No. CRL successfully downloaded into Firefox.

Verify Audits (COMPLETE)

- Validate contact info in report, call to verify that they did indeed issue this report.
  - Information is posted on the official French government website.
- For EV CA's, verify current WebTrust EV Audit done.
  - Not EV.
- Review Audit to flag any issues noted in the report
  - No issues noted in audit statements.