Bugzilla ID: 393166
Bugzilla Summary: Add Certigna certificates to NSS root store

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, as per http://wiki.mozilla.org/CA:Information_checklist.

General Information	Data
CA Name	Certigna of Dhimyotis
Website URL (English version)	http://www.certigna.fr
Organizational type. (E.g., whether the CA is operated by a private or public corporation, government agency, academic institution or consortium, NGO, etc.)	Dhimyotis public corporation Dhimyotis is the name of the company and Certigna is the brand for their certificates.
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?)	Dhimyotis products and services include Certigna ID and Certigna SSL. Certigna is a French CA for European market at the beginning, and expects to server other countries (India, USA, South America ...) soon.

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

Info Needed	Data	Status / Notes
Certificate Name	Certigna	COMPLETE
Cert summary / comments	The Certigna root has three internally operated subordinated CA's: Certigna SSL is for SSL-enabled servers, Certigna ID is for authentication and digitally-signed email, and Certigna Chiffrement is for encrypting email.	COMPLETE
The root CA certificate URL Download into FireFox and verify	http://www.certigna.fr/ca/ACcertigna.crt	COMPLETE
SHA-1 fingerprint.	B1:2E:13:63:45:86:A4:6F:1A:B2:60:68:37:58:2D:C4:AC:FD:94:97	COMPLETE
Valid from	2007-06-29	COMPLETE
Valid to	2027-06-29	COMPLETE
Cert Version	3	COMPLETE

Modulus length / key length	2048	COMPLETE
CRL • URL • update frequency for end-entity certificates	SSL Subordinate CA: http://www.certigna.fr/crl/certignassl.crl ID Subordinate CA: http://www.certigna.fr/crl/certignaid.crl CRL issuing frequency for end-entity certificates: after a certificate's revocation, or every 72 hours.	COMPLETE
OCSP (if applicable) • OCSP Responder URL	SSL Subordinate CA: http://ocsp.certigna.fr/certignassl ID Subordinate CA: http://ocsp.certigna.fr/certignaid	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 CPS, and that any audit covers them as well as the root.	Three subordinates CAs, internally operated: 1) Certigna SSL (SSL CA is TS-102042 compliant) 2) Certigna ID (Authentication and Signing CA is TS-102042 compliant) 3) Certigna Chiffrement (Encryption CA is the complement of Certigna ID) URL of certificate hierarchy diagram: http://www.certigna.fr/chaine_certification.php Certigna SSL and Certigna ID each have their own Certificate Policy document (see links below). The Audit covers both the SSL and ID subordinate CAs: “Certifié conforme ETSI TS 102 042 – Famille CERTIGNA ID (authentification-signature) – Famille CERTIGNA SSL”	COMPLETE
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	No subordinate CAs are operated by third parties.	COMPLETE

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.)		
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 -- identity/organisationally-validated b) CERTIGNA ID CP and CPS "Chapter 3.2.3. Identity validation ... The certificate request file sent to the RA must include : • The Certigna ID certificate request form, available on Certigna Web site, fully filled and signed by the subscriber. It includes: o Acceptance of terms and conditions o First and last name to be included in certificate o Subscriber informations (name, address, e-mail) o Copy of a valid identity document when recording the subscriber In some cases, the request file must include: If the subscriber belongs to an organization: • Proof of attachment to this organization • Authorized representative of the organization informations (name, organization, addresse, phone, e-mail), whose name is mentioned in the certificate request form • Copy of a valid official document when recording the request, including the SIREN number (DUNS equivalent for France), or by default another valid document proving unique identity of the	COMPLETE

	organization."	
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.certigna.fr	COMPLETE
CP/CPS • Certificate Policy URL • Certificate Practice Statement(s) (CPS) URL (English or available in English translation)	SSL Subordinate: http://www.certigna.fr/documents/pc_certigna_ssl.php ID Subordinate: http://www.certigna.fr/documents/pc_certigna_id.php	COMPLETE
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.)	A public statement of compliance with ETSI 102.042 has been provided by their 2008 auditor and posted on Certigna's website: http://www.certigna.fr/downloads/attestation_lsti.pdf I have independently verified this information with the auditor, and have updated the pending list with the new audit info: http://www.mozilla.org/projects/security/certs/pending/ Audit Type: ETSI TS-102042 Auditor: LSTI - La Sécurité des Technologies de l'Information Auditor Website: http://www.lsti.fr Audit Document URL(s): http://www.lsti-certification.fr/images/stories/dhimyotis.pdf	COMPLETE

Review CPS sections dealing with subscriber verification (COMPLETE)

- Verify domain check for SSL

    - Comment #15: Certigna SSL CP and CPS Chapter 3.2.3: “The certificate request file sent to the RA must include: … Proof of possession by the organization of domain name corresponding to the FQDN”
    - Comment #17: Yes, we verify the information in whois registries. This is documented in an internal document.
- 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.
    - Comment #15: Certigna ID CP and CPS Chapter 3.2.3: “The certificate request file sent to the RA must include: … Subscriber informations (name, address, e-mail)”
    - Comment #17: There is a registration form with the email address signed and dispatched to us by the subscriber. We verify that the CSR contains the same address than the one in the form. We send the certificate to the subscriber by mail (to the e-mail address of the form). This is documented in an internal document.
- Verify identity info in code signing certs is that of subscriber
    - Comment #15: No code signing certificates.
    - Comment #17: we have planned to make code signing certificates in the near future. If the need arises our CP/ CPS will have text about : "Verify identity information in code signing certificates is that of subscriber"
- Make sure it’s clear which checks are done for which context (cert usage)
    - Certigna SSL and Certigna ID each have their own Certificate Policy document

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

- Long-lived DV certificates
    - Certs are IV/OV
- Wildcard DV SSL certificates
    - Certs are IV/OV
- Delegation of Domain / Email validation to third parties
    - Not found
- Issuing end entity certificates directly from roots
    - End-entity certs are issued from intermediate CAs
- Allowing external entities to operate unconstrained subordinate CAs
    - Intermediate CAs are internally operated
- Distributing generated private keys in PKCS#12 files
    - Not found
- Certificates referencing hostnames or private IP addresses

    - Not found
- OCSP Responses signed by a certificate under a different root
    - OCSP successfully used in Firefox for the example website
- CRL with critical CIDP Extension
    - CRLs successfully imported into Firefox

Verify Audits (COMPLETE)

- Validate contact info in report, call to verify that they did indeed issue this report.
    - COMPLETE
- For EV CA's, verify current WebTrust EV Audit done.
    - N/A
- Review Audit to flag any issues noted in the report
    - COMPLETE