# Mozilla - CA Program

## Case Information

| | | | |
|---|---|---|---|
| **Case Number** | 00000079 | **Case Record Type** | CA Owner/Root Inclusion Request |
| **CA Owner/Certificate Name** | Dhimyotis / Certigna | **Request Status** | Need Information from CA |

## Additional Case Information

| | | | |
|---|---|---|---|
| **Subject** | Include renewed Certigna Root | **Case Reason** | |

## Bugzilla Information

| | |
|---|---|
| **Link to Bugzilla Bug** | https://bugzilla.mozilla.org /show_bug.cgi?id=1265683 |

## General information about CA's associated organization

| | | | |
|---|---|---|---|
| **CA Email Alias 1** | security@dhimyotis.com | | |
| **CA Email Alias 2** | | | |
| **Company Website** | http://www.certigna.fr/ | **Verified?** | Verified |
| **Organizational Type** | Private Corporation | **Verified?** | Verified |
| **Organizational Type (Others)** | | **Verified?** | Not Applicable |
| **Geographic Focus** | France, Europe | **Verified?** | Verified |
| **Primary Market / Customer Base** | Dhimyotis is the name of the company and Certigna is the brand for their certificates. | **Verified?** | Verified |
| **Impact to Mozilla Users** | DHIMYOTIS is one of the biggest French CAs which issues qualified certificates for general public, public administrations and privates companies. The CA focus its activities in France and worldwide. DHIMYOTIS has already sold certificates to more than 10,000 customers worldwide. . | **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** | NEED CA's response to each of the items listed in https://wiki.mozilla.org /CA:Recommended_Practices#CA_Recommended_Practices<br>1) Publicly Available CP and CPS: Yes<br>2) CA Hierarchy: Yes<br>3) Audit Criteria: Yes | **Verified?** | Need Response From CA |

4) Document Handling of IDNs in CP/CPS: ???
5) Revocation of Compromised Certificates: ???
6) Verifying Domain Name Ownership: Yes
7) Verifying Email Address Control: Yes
8) Verifying Identity of Code Signing Certificate Subscriber: Not applicable. Mozilla is no longer enabling the Code Signing trust bit for root certificates.
9) DNS names go in SAN: ???
10) Domain owned by a Natural Person: ???
11) OCSP: ERRORS IN TESTING
12) Network Security Controls: ???

### 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** | NEED CA's response to each of the items listed in https://wiki.mozilla.org/CA:Problematic_Practices#Potentially_problematic_CA_practices<br><br>1) Long-lived DV certificates: ???<br>2) Wildcard DV SSL certificates: Wildcard OV SSL certs are issued.<br>3) Email Address Prefixes for DV Certs: ???<br>4) Delegation of Domain / Email validation to third parties: No<br>5) Issuing end entity certificates directly from roots: No<br>6) Allowing external entities to operate subordinate CAs: No<br>7) Distributing generated private keys in PKCS#12 files: ???<br>8) Certificates referencing hostnames or private IP addresses: ???<br>9) Issuing SSL Certificates for Internal Domains: ???<br>10) OCSP Responses signed by a certificate under a different root: No<br>11) SHA-1 Certificates: No<br>12) Generic names for CAs: No<br>13) Lack of Communication With End Users: ???<br>14) Backdating the notBefore date: ??? | **Verified?** | Need Response From CA |

# Root Case Record # 1

### Root Case Information

| | | | |
|---|---|---|---|
| **Root Certificate Name** | Certigna Root CA | **Root Case No** | R00000114 |
| **Request Status** | Need Information from CA | **Case Number** | 00000079 |

### Additional Root Case Information

| | |
|---|---|
| **Subject** | Include Renewed Certigna Root CA |

### Technical Information about Root Certificate

| | | | |
|---|---|---|---|
| **O From Issuer Field** | Dhimyotis | **Verified?** | Verified |
| **OU From Issuer Field** | 0002 48146308100036 | **Verified?** | Verified |

| | | | |
|---|---|---|---|
| **Certificate Summary** | This SHA-256 root certificate will eventually replace the SHA-1 Certigna root certificate that was included via Bugzilla Bug #393166. | **Verified?** | Verified |
| **Root Certificate Download URL** | http://autorite.certigna.fr /certignarootca.der http://autorite.dhimyotis.com /certignarootca.der | **Verified?** | Verified |
| **Valid From** | 2013 Oct 01 | **Verified?** | Verified |
| **Valid To** | 2033 Oct 01 | **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://test.dhimyotis.com/ | **Verified?** | Verified |
| **CRL URL(s)** | http://crl.certigna.fr/certignarootca.crl https://www.certigna.fr/autorites /index.xhtml CP/CPS section 4.9.6 next update: 6 days but they are published every 24 hours or after a certificate's revocation. Frequency of updating CRL is described in chapters 2.3 and 4.9.6 of the CP/CPS | **Verified?** | Verified |
| **OCSP URL(s)** | URI for SSL certificate: http://servicesca.ocsp.certigna.fr/ Frequency of updating OCSP is described in chapter 4.9.6 of the CP/CPS. The maximum time elapsing from the revocation of an end entity or CA certificate until OCSP responders are updated to reflect that revocation : 1 hour | **Verified?** | Verified |
| **Trust Bits** | Email; Websites | **Verified?** | Verified |
| **SSL Validation Type** | OV | **Verified?** | Verified |
| **EV Policy OID(s)** | Not EV | **Verified?** | Not Applicable |
| **Root Stores Included In** | Apple; Microsoft | **Verified?** | Verified |
| **Mozilla Applied Constraints** | NEED: Mozilla has the ability to name constrain root certs; e.g. to *.gov or *.mil. CAs should consider if such constraints may be applied to their root certs. https://dxr.mozilla.org/mozilla-central /source/security/nss/lib/certdb /genname.c#1551 | **Verified?** | Need Response From CA |

## Test Results (When Requesting the SSL/TLS Trust Bit)

| | | | |
|---|---|---|---|
| **Revocation Tested** | NEED: Resolve all errors https://certificate.revocationcheck.com /test.dhimyotis.com error: OCSP signing certificate does not contain the OCSP No Check extension | **Verified?** | Need Response From CA |

| | | | |
|---|---|---|---|
| **CA/Browser Forum Lint Test** | NEED: resolve x509lint errors in crt.sh<br>crt.sh Run cablint: no errors<br>Run x509lint: ERROR: Subject with organizationName but without stateOrProvince or localityName | **Verified?** | Need Response From CA |
| **Test Website Lint Test** | http://cert-checker.allizom.org/<br>run certlint<br>no errors | **Verified?** | Verified |
| **EV Tested** | Not requesting EV treatment | **Verified?** | Not Applicable |

## Digital Fingerprint Information

| | | | |
|---|---|---|---|
| **SHA-1 Fingerprint** | 2D:0D:52:14:FF:9E:AD:99:24:01:74:20:47:6E:6C:85:27:27:F5:43 | **Verified?** | Verified |
| **SHA-256 Fingerprint** | D4:8D:3D:23:EE:DB:50:A4:59:E5:51:97:60:1C:27:77:4B:9D:7B:18:C9:4D:5A:05:95:11:A1:02:50:B9:31:68 | **Verified?** | Verified |

## CA Hierarchy Information

| | | | |
|---|---|---|---|
| **CA Hierarchy** | URL of certificate hierarchy diagram :https://www.certigna.fr/autorites/index.xhtml<br>The Certigna root has 7 internally operated subordinated CAs :<br>- Identity CA : encipherment, authentication and/or digitally-signed email<br>- Identity Plus CA : authentication and/or digitally-signed email<br>- Entity CA : seal (EKU : emailProtection or timeStamping)<br>- Entity Code signing CA : seal (EKU : codeSigning)<br>- Services CA : SSL (EKU : authServer or authClient)<br>- Wild CA : SSL (EKU : authServer and authClient)<br>- FR03 : Seal | **Verified?** | Verified |
| **Externally Operated SubCAs** | No any external operated SubCAs | **Verified?** | Verified |
| **Cross Signing** | The intermediate CA certificates signed by our new root certificate «Certigna Root CA» are also signed by the root certificate «Certigna» already included in Mozilla program. | **Verified?** | Verified |
| **Technical Constraint on 3rd party Issuer** | No third-parties can directly cause the issuance of certificates.<br>Several External Delegued Registration Authorities are working with DHIMYOTIS but all registrations are validated by the RA of DHIMYOTIS. | **Verified?** | Verified |

## Verification Policies and Practices

| | | | |
|---|---|---|---|
| **Policy Documentation** | Documents are provided in French<br>Root CP: http://politique.certigna.fr/PCcertignarootca.pdf<br>Services CP: http://politique.certigna.fr/PCcertignaservicesca.pdf | **Verified?** | Verified |

| | | | |
|---|---|---|---|
| **CA Document Repository** | https://www.certigna.fr/autorites/index.xhtml | **Verified?** | Verified |
| **CP Doc Language** | French | | |
| **CP** | http://politique.certigna.fr/PCcertignaservicesca.pdf | **Verified?** | Verified |
| **CP Doc Language** | French | | |
| **CPS** | http://politique.certigna.fr/PCcertignarootca.pdf | **Verified?** | Verified |
| **Other Relevant Documents** | Identity CP : http://politique.certigna.fr/PCcertignaidentityca.pdf<br>Identity Plus CP: http://politique.certigna.fr/PCcertignaidentityplusca.pdf<br>Entity CP: http://politique.certigna.fr/PCcertignaentityca.pdf<br>Entity Code signing CP: http://politique.certigna.fr/PCcertignaentitycsca.pdf<br>Wild CP: http://politique.certigna.fr/PCcertignawildca.pdf<br>FR03 CP: http://politique.certigna.fr/PCfr03.pdf | **Verified?** | Verified |
| **Auditor Name** | LSTI | **Verified?** | Verified |
| **Auditor Website** | http://lsti-certification.fr/ | **Verified?** | Verified |
| **Auditor Qualifications** | http://www.cofrac.fr/en/activites/certification.php<br>https://portal.etsi.org/TBSiteMap/ESI/TrustServiceProviders.aspx | **Verified?** | Verified |
| **Standard Audit** | https://bugzilla.mozilla.org/attachment.cgi?id=8742753 | **Verified?** | Verified |
| **Standard Audit Type** | ETSI TS 102 042 | **Verified?** | Verified |
| **Standard Audit Statement Date** | 2/15/2016 | **Verified?** | Verified |
| **BR Audit** | http://www.lsti-certification.fr/images/liste_entreprise/Liste%20PSCe | **Verified?** | Verified |
| **BR Audit Type** | ETSI TS 102 042 | **Verified?** | Verified |
| **BR Audit Statement Date** | 2/15/2016 | **Verified?** | Verified |
| **EV Audit** | Not EV | **Verified?** | Not Applicable |
| **EV Audit Type** | | **Verified?** | Not Applicable |
| **EV Audit Statement Date** | | **Verified?** | Not Applicable |
| **BR Commitment to Comply** | Services CP and Wild CP section 1.1.1. | **Verified?** | Verified |
| **SSL Verification Procedures** | NEED: Where in the Services and Wild CP documentation does it say *how* the domain name included in the certificate is verified to be owned/controlled by the certificate subscriber?<br>Need to have documentation in the CP/CPS that we can confirm meets the requirements of section 3.2.2.4 (Authorization by Domain Name Registrant) of the CA/Browser Forum's Baseline Requirements.<br><br>In other words, where in the Services CP | **Verified?** | Need Response From CA |

| | | | |
|---|---|---|---|
| | and Wild CP can we find the following? "WHOIS and AFNIC website are used by RA for checking ownership/control of the domain name for SSL certificate applications."<br>And *how* WHOIS and AFNIC are used. | | |
| **EV SSL Verification Procedures** | Not requesting EV treatment. | **Verified?** | Not Applicable |
| **Organization Verification Procedures** | Translation of Service CA and Wild CA Certification Policy, section 3.2.3 :<br><br>« The RC must demonstrate that he has the right to use the domain included in the FQDN (ownership rights over the domain or right to use the part of the entity right holder). The registration of the futur RC requires the verification of the legal person's identity, RC's identity, and the relationship between the RC and the legal person.<br><br>The certificate requestfile, send to RA, shall include :<br>- The certificate request (template available on certigna website : http://www.certigna.fr), dated within 3 months,<br>completed and co-signed by a legal representative and the RC, with especially :<br>o The acceptance of the terms and conditions ;<br>o The identity of the server to be used the certificate (FQDN) ;<br>o Identification personal data of the RC ;<br>o Identification information of the legal person ;<br>o Contact information of a legal representative of the entity (name, entity, address, phone number, email) ;<br>o Contact information of the future RC (name, entity, address, phone number, email) ;<br>- A mandate signed and dated less than 3 months, by a legal representative of the entity, designating the future RC as eligible to be RC for the service to which the certificate should be issued. This mandate must be signed for acceptance by the future RC. | **Verified?** | Verified |
| **Email Address Verification Procedures** | NEED: Where does it say in the Identity CP and Identity Plus CP that the email address to be included in the certificate is *used* by Certigna RA to verify that the certificate subscriber owns/controls that email address?<br><br>i.e. where does the CP actually say the following?<br>Subject's email is controlled during the registration phase, through the exchange of several emails in particular to create the customer account and manage his certificate. If the subject provide a wring email he can not obtain his certificate. Furthermore the email used for registration is always the one inserted in the subject certificate. | **Verified?** | Need Response From CA |

| | | | |
|---|---|---|---|
| **Code Signing Subscriber Verification Pro** | Mozilla is no longer accepting requests to enable the Code Signing trust bit. | **Verified?** | Not Applicable |
| **Multi-Factor Authentication** | Administrators and operators intervening within the CA system are identified with certificates on token from Certigna Identity Plus CA.<br>Relevant events involved in the management and operation of the IGC are recorded in handwritten form or electronically (by seizure or by automatic generation) and, for purposes of audit.<br>The means for event logs management were checked during the certification audit and are described in the Certification Policies at the section 5.4. | **Verified?** | Verified |
| **Network Security** | Services CP section 6.7<br>DHIMYOTIS confirms the following :<br>- Maintain network security controls that at minimum meet the Network and Certificate System Security Requirements.<br>- Check for mis-issuance of certificates, especially for high-profile domains.<br>- Review network infrastructure, monitoring, passwords, etc. for signs of intrusion or weakness.<br>- Ensure Intrusion Detection System and other monitoring software is up-to-date.<br>- Confirm that you will be able to shut down certificate issuance quickly if you are alerted of intrusion.<br>Means are especially described in section 6.7 of Ccertification policies :<br>« Interconnection to public networks is protected by security gateways configured to accept only the necessary protocols to the desired operation by AC. The network features include two firewalls (clustered on) with integrated intrusion detection system (IPS with alerting).<br>The CA guarantees that the components of the local network are kept in a physically secure environment and their configurations are periodically audited for compliance with the requirements specified by the AC. » | **Verified?** | Verified |

## Link to Publicly Disclosed and Audited subordinate CA Certificates

| | | | |
|---|---|---|---|
| **Publicly Disclosed & Audited subCAs** | https://www.certigna.fr/autorites/index.xhtml | **Verified?** | Verified |