

# WISeKey SA

---

OISTE WISeKey Global Root GB

***Important Notice:** WISeKey SA is already included in Mozilla program for CAs for its “Generation A Root”, named as “OISTE WISeKey Global Root GA CA”. The object of this request is the inclusion of a new “Generation B” root CA, named as “OISTE WISeKey Global Root GB CA”, being the only representative differences the support for SHA-256 algorithm and compliance with “Extended Validation” requirements. Thus, previous compliance with “Mozilla CA Certificate Policy” is maintained or improved.*

**CONTENTS:**

General information about the CA’s associated organization ..... 2

Technical information about each root certificate ..... 2

CA Hierarchy information for each root certificate ..... 5

Verification Policies and Practices ..... 7

Response to Mozilla's CA Recommended Practices..... 9

Response to Mozilla’s list of Potentially Problematic Practices ..... 11

## General information about the CA's associated organization

CA Company Name	WIS@key SA
Website URL	<a href="https://www.wisekey.com">https://www.wisekey.com</a>
Organizational type	Private organization
Primary Market / Customer Base	WIS@key provides worldwide eSecurity services based or related to electronic identities and digital certificates. There's no focus on a particular region or customer profile.
Impact to Mozilla users	<p>WIS@key's portfolio includes the commercialization of SSL and personal certificates. Our previous Root CA (referred to as GA for "Generation A"), already included in Mozilla's product, allows Mozilla's users to benefit the typical uses of trusted certificates (secure web browsing, secure eMail, better authentication...).</p> <p>The new Root CA (referred to as GB for "Generation B"), and the object of this request, will extend these benefits to the use of more secure PKI algorithms, in particular SHA-256, and the use of more reliable services, as EV SSL.</p>
Inclusion in other major browsers	<p>The existing Root for the "Generation A" of our PKI (OISTE WIS@key Global Root GA CA) is already included by:</p> <ul style="list-style-type: none"> <li>• Mozilla (<a href="https://wiki.mozilla.org/CA:IncludedCAs">https://wiki.mozilla.org/CA:IncludedCAs</a>)</li> <li>• Microsoft (<a href="http://download.microsoft.com/download/1/5/7/157B29AB-F890-464A-995A-C87945B28E5A/Windows%20Root%20Certificate%20Program%20Members%20-%20Sept%202014.pdf">http://download.microsoft.com/download/1/5/7/157B29AB-F890-464A-995A-C87945B28E5A/Windows%20Root%20Certificate%20Program%20Members%20-%20Sept%202014.pdf</a>)</li> <li>• Apple (<a href="https://support.apple.com/en-us/HT204132">https://support.apple.com/en-us/HT204132</a>)</li> <li>• ... and others (e.g. Opera, Chrome) which rely directly in Mozilla's or Microsoft programs-</li> </ul>
CA Primary Point of Contact (POC)	<p>WIS@key SA</p> <p>POC Email address alias (preferred): <a href="mailto:cps@wisekey.com">cps@wisekey.com</a></p> <p>Phone: +41 22 594 30 00</p> <p>Post Address:</p> <p>WTC II, 29 route de Pré-Bois, CP 853, CH-1215 Geneva 15, Switzerland</p>

## Technical information about each root certificate

**Important Notice:** only specifying here the new root certificate object of this request. Information already registered for the "Generation A" root CA (**OISTE WIS@key Global Root GA CA**) must be kept as already recorded by Mozilla.

<b>Certificate Name</b>	OISTE WIS@key Global Root GB CA
<b>Certificate Issuer Field</b>	CN = OISTE WIS@key Global Root GB CA OU = OISTE Foundation Endorsed O = WIS@key C = CH
<b>Certificate Summary</b>	Root Certification Authority. This is the first level Certification Authority; its role is to establish the Root of the Trust Model, or <b>OWGTM</b> , as often referred by WIS@key in its CPS. This Certification Authority does not issue certificates for end entities, but only for the Intermediary Certification Authorities (as described in the CPS). The certificates of WIS@key's Root Certification Authorities are self-signed and currently the <b>OWGTM</b> maintains two Root Certification Authorities, in order to provide support for two parallel hierarchies: The already included "Generation A", and the new "Generation B", which implements SHA-256 algorithm. Under the Root CAs, WIS@key deploys an intermediary "Policy CA", which enhances control on the trust model by generating the "Issuing CAs" and the required OCSP/CRL services.
<b>Mozilla Applied Constraints</b>	Does not apply
<b>Root Cert URL</b>	<a href="http://public.wisekey.com/crt/owgrgbca.crt">http://public.wisekey.com/crt/owgrgbca.crt</a>
<b>SHA-1 Fingerprint</b>	0F:F9:40:76:18:D3:D7:6A:4B:98:F0:A8:35:9E:0C:FD:27:AC:CC:ED
<b>Valid from</b>	1-Dec-2014
<b>Valid to</b>	1-Dec-2039
<b>Certificate version</b>	3
<b>Certificate signature algorithm</b>	SHA-256 with RSA encryption
<b>Signing key parameters</b>	RSA Modulus 2048 bits
<b>Test Website URL (SSL)</b>	Standard SSL: <a href="https://goodssl.wisekey.com">https://goodssl.wisekey.com</a> EV SSL: <a href="https://goodevssl.wisekey.com">https://goodevssl.wisekey.com</a>
<b>Example Certificate (non-SSL)</b>	Not available
<b>CRL URL</b>	Root CA: <a href="http://public.wisekey.com/crl/owgrgbca.crl">http://public.wisekey.com/crl/owgrgbca.crl</a> Policy CA: <a href="http://public.wisekey.com/crl/wcidpgbca1.crl">http://public.wisekey.com/crl/wcidpgbca1.crl</a> Issuing CA: <a href="http://public.wisekey.com/crl/wcidagbca2.crl">http://public.wisekey.com/crl/wcidagbca2.crl</a> Issuance frequencies as specified in the CPS
<b>OCSP URL (Required now for end-entity certs)</b>	<a href="http://ocsp2.wisekey.com">http://ocsp2.wisekey.com</a>
<b>Request Trust Bits</b>	Websites (SSL/TLS) Email (S/MIME)

<b>SSL Validation Type</b>	DV (Not yet issued, but supported by the CPS) OV (As currently done in the “Generation A” hierarchy) EV (New)
<b>EV Policy OID(s)</b>	2.16.756.5.14.7.4.8
<b>Non-sequential serial numbers and entropy in cert</b>	The CA software used by WIS@key implements random generation of a serial number of a length greater than 64 bits
<b>Response to Recent CA Communication(s)</b>	Response to communication sent by May 2015, available at: <a href="https://mozillacaprogram.secure.force.com/Communications/CommunicationSummaryReport?CommunicationId=a04o000000M89RCAAZ">https://mozillacaprogram.secure.force.com/Communications/CommunicationSummaryReport?CommunicationId=a04o000000M89RCAAZ</a> Response to communication sent by May 2014, available at: <a href="https://docs.google.com/spreadsheets/d/1v-Lrxo6mYlyrEli_wSpLsHZvV5dJ_vvSzLTAMfxI5n8/pubhtml">https://docs.google.com/spreadsheets/d/1v-Lrxo6mYlyrEli_wSpLsHZvV5dJ_vvSzLTAMfxI5n8/pubhtml</a>

## CA Hierarchy information for each root certificate

<b>CA Hierarchy</b>	<p>The following graphic includes the hierarchies for the already included “Generation A” and the new hierarchy depending on the “Generation B” root, object of this request. Textual descriptions are available in our CPS (“<b>1.3.1. Certification authorities</b>”).</p> <div data-bbox="757 363 1951 1145"> <pre> graph TD     subgraph SHA-1_Hierarchy [SHA-1 Hierarchy]         RootGA[OWGTM Root CA GA] --&gt; WISKeyCertGA[OWGTM Root CA GA]         WISKeyCertGA --&gt; WISKeyCertGA_Q[OWGTM Root CA GA]         WISKeyCertGA --&gt; WISKeyCertGA_A[OWGTM Root CA GA]         WISKeyCertGA --&gt; WISKeyCertGA_S[OWGTM Root CA GA]         WISKeyCertGA_Q --&gt; WISKeyPartnersGA_Q[OWGTM Root CA GA]         WISKeyCertGA_A --&gt; WISKeyPartnersGA_A[OWGTM Root CA GA]         WISKeyCertGA_S --&gt; WISKeyPartnersGA_S[OWGTM Root CA GA]     end      subgraph SHA-2_Hierarchy [SHA-2 Hierarchy]         RootGB[OWGTM Root CA GB] --&gt; PolicyCA[OWGTM Policy CA G1]         PolicyCA --&gt; WISKeyIssuingGB_Q[OWGTM Policy CA G1]         PolicyCA --&gt; WISKeyIssuingGB_A[OWGTM Policy CA G1]         PolicyCA --&gt; WISKeyIssuingGB_S[OWGTM Policy CA G1]         WISKeyIssuingGB_Q --&gt; PartnersIssuingGB_Q[OWGTM Policy CA G1]         WISKeyIssuingGB_A --&gt; PartnersIssuingGB_A[OWGTM Policy CA G1]         WISKeyIssuingGB_S --&gt; PartnersIssuingGB_S[OWGTM Policy CA G1]     end </pre> </div>
<b>Externally Operated SubCAs</b>	<p>At this moment, there aren't externally operated SubCAs under the new “Generation B” root, but this is supported as stipulated in our CPS.</p> <p>For the existing “Generation A” hierarchy, there's a limited number of CAs operated by external companies, which enforce name constraints. In particular, the currently active SubCAs are:</p> <ul style="list-style-type: none"> <li>• Government of Seychelles. Constrained to *.gov.sc</li> <li>• The Bancorp Inc. Constrained to *.wise-corp.co, *.thebancorp.com, *.wisecorp.us and *.wise-corp.us</li> </ul>
<b>Cross-Signing</b>	Not supported

<b>Technical Constraints on Third-party Issuers</b>	<p>As stipulated in our CPS...</p> <p><b>7.1.5 Name constraints</b></p> <p><i>Issuing Certification Authorities not operated by WIS@Key will be constrained for the issuance of certificates under a set of predefined and agreed names (domain names, e-mail suffixes or other name components). For exceptional cases where these constraints aren't applied, these CAs will be included in the external audit for compliance assurance against any applicable requirement (including Baseline and Extended Validation Requirements from the CA/Browser Forum). Domain name constraints can be also applied when using the MPKI RA Interface for Certificate Requests for corporations having access to a dedicated Registration Authority.</i></p>
---	---

## Verification Policies and Practices

<b>Policy Documentation</b>	<p>Language(s) that the documents are in: ENGLISH</p> <p>All documents available at <a href="http://www.wisekey.com/repository">http://www.wisekey.com/repository</a></p> <p>Direct links:</p> <p>CP &amp; CPS: <a href="https://d3o11irj9639cz.cloudfront.net/uploads/images/WKPKI.DE001-OWGTM-PKI-CPS.v2.2-CLEAN.pdf">https://d3o11irj9639cz.cloudfront.net/uploads/images/WKPKI.DE001-OWGTM-PKI-CPS.v2.2-CLEAN.pdf</a></p> <p>Relying Party Agreement: <a href="https://www.wisekey.com/Repository/Documents/Relying-Party-Agreement-1.0-wk-signed.pdf">https://www.wisekey.com/Repository/Documents/Relying-Party-Agreement-1.0-wk-signed.pdf</a></p>
<b>Audits</b>	<p><b>Audit Type:</b></p> <ul style="list-style-type: none"> <li>• WebTrust Principles and Criteria for Certification Authorities 2.0</li> <li>• WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL</li> <li>• WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security</li> </ul> <p><b>Auditor:</b> Auren</p> <p><b>Auditor Website:</b> <a href="http://www.auren.com/en-ES">http://www.auren.com/en-ES</a></p> <p><b>URL to Audit Report and Management’s Assertions:</b>  <a href="https://d3o11irj9639cz.cloudfront.net/uploads/images/WIS@Key-WebTrust-Audit-Report-2015.pdf">https://d3o11irj9639cz.cloudfront.net/uploads/images/WIS@Key-WebTrust-Audit-Report-2015.pdf</a> (all reports and assertions concatenated in a single PDF)</p>
<b>Baseline Requirements (SSL)</b>	<p>Compliance with Baseline Requirements is stated explicitly in several sections of our CPS, and it’s been reviewed and validated by the auditor, as part of their report linked in the above row of this table.</p> <p>In particular, a first statement can be found in section 1.7 of WIS@Key’s CPS (<b>1.7. Statement Compliance with CA/Browser Forum requirements</b>).</p>
<b>SSL Verification Procedures</b>	<p>This information is available in our CPS. Relevant sections are:</p> <ul style="list-style-type: none"> <li>• <b>3. Identification and Authentication</b> (pages 19 to 21)</li> <li>• <b>12. Annex C: Identity Validation Policies</b> (pages 71 to 75)</li> </ul> <p>The verification procedures for SSL certificates have been audited, as included in the reports linked above.</p>
<b>Organization Verification Procedures</b>	<p>In particular to the above-said, please refer to section “<b>12.2.2. Corporate and Server Certificates</b>” in our CPS.</p> <p>Please note that currently all SSL certificates issued by WIS@Key include the verification of the organization. Our CPS supports the future issuance of Domain-validated certificates, although this is</p>

	not practiced yet.
<b>Email Address Verification Procedures</b>	<p>WIS@key CertifyID Personal certificates enforce the validation of Email addresses using different procedures, as stipulated in section “<b>12.2.1. Personal Certificates</b>”. In particular, any enrollment for a CertifyID Account requires a bounce-back Email verification before entitling the subscriber to send a remote (non face-to-face) certificate request. The process can be experienced at <a href="https://www.certifyid.com">https://www.certifyid.com</a></p> <p>The verification procedures for S/MIME-capable certificates have been audited, as included in the reports linked above.</p>
<b>Code Signing Subscriber Verification Procedures</b>	<p>For Code Signing certificates issued to Natural Persons, WIS@key applies the same verification procedures than for the “CertifyID Qualified Personal Certificate” (Section 12.2.1 of the CPS). Alternatively, for Code Signing certificates requested by organizations, the verification will match the stipulations for the “CertifyID Qualified Corporate Certificate” (Section 12.2.2 of the CPS)</p>
<b>Multi-Factor Authentication</b>	<p>Enrollment officers must log-in in the RA interface using strong authentication based on a digital certificate with the profile “CertifyID URA Admin Certificate”. For this certificate profile, WIS@key makes mandatory the use of a cryptographic device (USB Token or Smartcard) to generate and use the private keys linked to the administrator certificate.</p>
<b>Network Security</b>	<p>The Audit reports covering both the existing hierarchy and the new “Generation B” object of this request include the Maintain network security controls published by the CA/Browser forum and considered as part of the “WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security”</p>



## Response to Mozilla's CA Recommended Practices

<b>Publicly Available CP and CPS</b>	<p>WIS@key's CPS integrates the CP-related information and it's publicly available in English language at <a href="http://www.wisekey.com/repository">http://www.wisekey.com/repository</a></p> <p>The CPS is redacted following the RFC3647 and any required information can be found at the corresponding section.</p>
<b>CA Hierarchy</b>	<p>Please refer to the previous section, which includes a graphic and a pointer to the textual description of the hierarchy in the CPS.</p> <p>The CPS itself is applied to the whole hierarchy, and information about the distribution of certificate policies for the different Certification Authorities is described in section "<b>11.1. Issuing CAs and Certificate Policies binding</b>" of the CPS.</p>
<b>Audit Criteria</b>	<p>As described in the above sections, WIS@key conducts annual external audits according to the different WebTrust Principles and Criteria. The results of the audits are made public at <a href="http://www.wisekey.com/repository">http://www.wisekey.com/repository</a></p> <p>The latest audits have been conducted in May 2015, being:</p> <ul style="list-style-type: none"> <li>• WebTrust Principles and Criteria for Certification Authorities 2.0</li> <li>• WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL</li> <li>• WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security</li> </ul>
<b>Document Handling of IDNs in CP/CPS</b>	<p>Currently WIS@key doesn't support IDNs, thus we only admit conventional domain names and we apply the identity validation policies for the domain as specified in the certificate request</p>
<b>Revocation of Compromised Certificates</b>	<p>As stipulated in the CPS (section "<b>4.9.1. Circumstances for revocation</b>"), WIS@key revokes any certificate which is known or suspect to be compromised.</p>
<b>Verifying Domain Name Ownership</b>	<p>WIS@key applies techniques and procedures to verify domain names, which are compliant with the applicable requirements from the CA/Browser Forum. This information is made public in the CPS (Section "<b>12. Annex C: Identity Validation Policies</b>").</p> <p>This, as expected, has been subject to the latest audits to verify adhesion to Baseline and Extended Validation requirements.</p>
<b>Verifying Email Address Control</b>	<p>We reproduce the same answer stated in a previous section...</p> <p>WIS@key CertifyID Personal certificates enforce the validation of Email addresses using different procedures, as stipulated in section "<b>12.2.1. Personal Certificates</b>". In particular, any enrollment for a CertifyID Account requires a bounce-back Email verification before entitling the subscriber to send a remote (non face-to-face) certificate request. The process can be experienced at</p>

	<a href="https://www.certifyid.com">https://www.certifyid.com</a> The verification procedures for S/MIME-capable certificates have been audited, as included in the reports linked above.
<b>Verifying Identity of Code Signing Certificate Subscriber</b>	As responded in the previous section... For Code Signing certificates issued to Natural Persons, WIS@Key applies the same verification procedures than for the “CertifyID Qualified Personal Certificate” (Section 12.2.1 of the CPS). Alternatively, for Code Signing certificates requested by organizations, the verification will match the stipulations for the “CertifyID Qualified Corporate Certificate” (Section 12.2.2 of the CPS).
<b>DNS names go in SAN</b>	WIS@Key makes mandatory to appear the DNS names in the SAN attributes of the certificates, as stipulated in the certificate profiles described in our CPS (Section “ <b>12.2.2. Corporate and Server Certificates</b> ”).
<b>Domain owned by a Natural Person</b>	Currently WIS@Key doesn’t issue SSL certificates to domains owned by Natural Persons, but our internal procedures take in account Mozilla’s requirement in this respect.
<b>OCSP</b>	The requirements for OCSP have been validated as part of the WebTrust Principles and Criteria related to the Baseline and Extended Validation Requirements. A test with Firefox has been performed against the site: <a href="https://goodssl.wisekey.com/">https://goodssl.wisekey.com/</a> , resulting in a satisfactory behavior.

## Response to Mozilla's list of Potentially Problematic Practices

<b>Long-lived DV certificates</b>	WIS@key issues SSL certificates with a maximum lifespan of 3 years (stipulated at section “ <b>11.3. Corporate and Server Certificates</b> ” of the CPS). Except for EV certificates, which are valid for a maximum of one year.
<b>Wildcard DV SSL certificates</b>	All current SSL certificates, including Wildcard, enforce the validation of the organization. WIS@key will support in the future the issuance of SSL certificates not requiring organization validation, but Wildcard certificates won't be supported for those future “domain validation only” certificates.
<b>Email Address prefixes for DV certs</b>	WIS@key observes the Baselines Requirements in its section “ <b>3.2.2.4. Authorization by Domain Name Registrant</b> ”, in what respects to the use of common Email prefixes.
<b>Delegation of Domain / Email validation to third parties</b>	WIS@key currently doesn't delegate any activity related to the validation of SSL certificate requests.
<b>Issuing end-entity certificates directly from roots</b>	As describes in the CPS and in the previous sections (“CA Hierarchy”), WIS@key roots never can't issue end-entity certificates. Issuing CAs are always below a “Policy CA”, which is the only subordinate entity for the Root.
<b>Allowing external entities to operate subordinate CA</b>	As described in the previous section “ <b>Externally Operated SubCAs</b> ”, <b>WIS@key only allows SubCAs operated by external entities if these CAs apply name and policy constraints</b> , in such a way that the entity can only issue certificates for a closed list of pre-authorized domains.
<b>Distributing generated private keys in PKCS#12 files</b>	For personal certificates of classes “Standard” and “Advanced”, WIS@key supports the generation of the key pair by the Registration Authority, and distribute it as a PKCS#12 file to the end user, and always communicating the password to decrypt the file using and out-of-band message (i.e. SMS). For “Qualified” personal certificates the key generation must necessarily occur inside a cryptographic hardware device under sole control of the subscriber. For SSL Certificates, subscribers must generate by their means the key pair and send to WIS@key a certificate request using PKCS#10. This procedure is implemented by the SSL selling platform ( <a href="https://reseller.wisekey.com">https://reseller.wisekey.com</a> ).
<b>Certificates referencing hostnames or private IP addresses</b>	WIS@key doesn't not issue a certificate with an Expiry Date later than 1 November 2015 with a SAN or Subject Common Name field containing a Reserved IP Address or Internal Server Name. WIS@key made an internal audit in this respect, having revoked already any incompliant certificate. This has been verified as part of our last external audit covering the Baseline Requirements.
<b>Issuing SSL certificates for internal domains</b>	As expressed above, WIS@key doesn't allow the issuance of certificates of internal domains. We never considered a “*.int” name as an internal domain. This has been internally verified.

<b>OCSP Responses signed by a certificate under a different root</b>	<p>Reproducing the answer for a similar question in a former section...</p> <p>The requirements for OCSP have been validated as part of the WebTrust Principles and Criteria related to the Baseline and Extended Validation Requirements.</p> <p>A test with Firefox has been performed against the site: <a href="https://goodssl.wisekey.com/">https://goodssl.wisekey.com/</a>, resulting in a satisfactory behavior.</p>
<b>SHA-1 Certificates</b>	<p>The main object of this inclusion request is to enable support to SHA-256 in the certificates issued by WiSeKey. Once the new root is embedded in the browsers, WiSeKey will stop issuing SHA-1 certificates.</p> <p>We have a quality compromise with our customers to replace any existing SHA-1 SSL certificate with a new equivalent SHA256 certificate before 1-January 2016.</p>
<b>Generic Names for CAs</b>	<p>We make mandatory the inclusion of meaningful information in the CN of any CA in our hierarchies. In particular, the new root CA object of this request is named <b>"OISTE WiSeKey Global Root GB CA"</b>.</p>
<b>Lack of Communication with end-users</b>	<p>WiSeKey ensures the availability of commercially reasonable resources to attend any request from our subscribers. In particular, any communication related to the revocation status of our certificates is attended as per the Baseline and EV requirements of the CA/Browser forum. Main points of contacts are:</p> <ul style="list-style-type: none"> <li>• <a href="mailto:support@wisekey.com">support@wisekey.com</a>, for any issue related to our certification services</li> <li>• <a href="mailto:cps@wisekey.com">cps@wisekey.com</a>, for issues related to our certification policies and practices</li> </ul>
<b>Backdating the notBefore date</b>	<p>WiSeKey maintains all reasonable controls to ensure the reliability of the time reference used by the Certification Authority.</p>