WISeKey SA

OISTE WISeKey Global Root GB

Important Notice: *WISeKey SA is already included in Mozilla program for CAs for two Root CAs, named as "OISTE WISeKey Global Root GA CA" and "OISTE WISeKey Global Root GB CA". The object of this request is the inclusion of a new "Generation C" root CA, named as "OISTE WISeKey Global Root GC CA", being the only representative differences the use of ECC algorithms in the full certification chain. Thus, previous compliance with "Mozilla CA Certificate Policy" is maintained or improved.*

CONTENTS:

General information about the CA's associated organization

CA Company Name	WISeKey SA
Website URL	https://www.wisekey.com
Organizational type	Private organization
Primary Market / Customer Base	WISeKey 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	WISeKey's portfolio includes the commercialization of SSL and personal certificates. Our previous Root CAs (referred to as GA and GB, for "Generation A" and "Generation B" respectively), 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…). The new Root CA (referred to as GC for "Generation C"), and the object of this request, aims specifically to its use in "Internet of Things" (IoT) environments, that require the use of ECC algorithms for the full certification chain. Thanks to the inclusion of this new Root, WISeKey will be able to deploy trusted digital identities to connected devices, enhancing the security of IoT projects. The main uses of these certificates would be for client authentication, digital signature and data encryption. We need to enable also the SSL and S/MIME trust bits for this root to ensure that, when needed, a browser can also securely connect to a device featuring a web interface (i.e. management console of a device), and also to enable secure email messages sent by these intelligent objects (i.e. sending authenticated critical messages). The reason of requesting the inclusion of this new root is to enable a full certification chain using only ECC algorithms. Most IoT deployments, due to the computing and memory size constraints, only support these algorithms, which allow higher security levels with smaller key lengths. Please note that WISeKey doesn't aim to issue commercial "general purpose" SSL certificates under this Root. The main focus for this Root is currently IoT.
Inclusion in other major browsers	The existing Root for the GA and GB of our PKI (OISTE WISeKey Global Root Gx CA) are already included by: • Mozilla (https://ccadb-public.secure.force.com/mozilla/IncludedCACertificateReport) • Microsoft (https://social.technet.microsoft.com/wiki/contents/articles/31634.microsoft-trusted-root-certificate-program-participants.aspx#Participants_list) • Apple (https://support.apple.com/es-es/HT208125) • … and others which rely directly in Mozilla's or Microsoft programs-

CA Primary Point of Contact (POC)	WISeKey SA – Pedro Fuentes (CSO) POC Email address – Preferred: cps@wisekey.com; Direct: pfuentes@wisekey.com Phone: +41 22 594 30 00 Post Address: WTC II, 29 route de Pré-Bois, CP 853, CH-1215 Geneva 15, Switzerland

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" and "Generation B" root CAs (**OISTE WISeKey Global Root GA/GB CA**) must be kept as already recorded by Mozilla.*

Certificate Name	OISTE WISeKey Global Root GC CA
Certificate Issuer Field	CN = OISTE WISeKey Global Root GC CA OU = OISTE Foundation Endorsed O = WISeKey C = CH
Certificate Summary	Root Certification Authority. This is the first level Certification Authority; its role is to establish the Root of the Trust Model, or **OWGTM**, as often referred by WISeKey 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 WISeKey's Root Certification Authorities are self-signed and currently the **OWGTM** maintains three Root Certification Authorities, in order to provide support for three parallel hierarchies: The already included "Generation A" (SHA-1) and "Generation B" (SHA-256), and the new "Generation C", which implements ECC algorithms. Under the Root CAs, WISeKey deploys the "Issuing CAs" and the required OCSP/CRL services.
Root Cert URL	http://public.wisekey.com/crt/owgrgc.crt
SHA-1 Fingerprint	E0 11 84 5E 34 DE BE 88 81 B9 9C F6 16 26 D1 96 1F C3 B9 31
Valid from	9-May-2017
Valid to	9-May-2042
Certificate version	3
Certificate signature algorithm	ECDSA with SHA-384
Signing key parameters	ECC NIST P-384, 384 bits

Test Website URL (SSL)	Valid: https://gcvalidssl.hightrusted.com Expired: https://gcexpiredssl.hightrusted.com Revoked: https://gcrevokedssl.hightrusted.com
Example Certificate (non-SSL)	Not available
CRL URL	Root CA: http://public.wisekey.com/crl/owgrgc.crl Issuing CA: http://public.wisekey.com/crl/wcidgcas1.crl Issuance frequencies as specified in the CPS
OCSP URL	http://ocsp.wisekey.com
Request Trust Bits	Websites (SSL/TLS) Email (S/MIME)
SSL Validation Type	DV (Not yet issued, but supported by the CPS) OV (As currently done in the "Generation A" and "Generation B" hierarchies)
EV Policy OID(s)	N/A

CA Hierarchy information for each root certificate

CA Hierarchy	The following list represents the current hierarchy: • CN=OISTE WISeKey Global Root GC CA, OU=OISTE Foundation Endorsed, O=WISeKey, C=CH Thumbprint: e8 11 84 5 e34 de be88 81 b9 9c f6 16 16 26 d1 96 1f c3 b9 31 Valid From :9 th May2017 Valid To :9 th May2042 • Issuing CAs ○ WISeKey CertifyID Advanced GC CA 1 Thumbprint: bb f9 b6 91 8b 63 e4 b4 13 36 69 0f d6 92 21 3c 19 5f 39 40 Valid From: June 19, 2017 Valid To :May 9 ,2042 Complete description of all the WISeKey hierarchies is available in our CPS ("**1.3.1. Certification authorities**").
Externally Operated SubCAs	At this moment, there aren't externally operated SubCAs under the new "Generation C" root, but this is supported as stipulated in our CPS, using a "Name constraint" and/or "EKU constraint" approach.
Cross-Signing	Not supported

Technical Constraints on Third-party Issuers	As stipulated in our CPS… ***7.1.5 Name constraints*** *Issuing Certification Authorities not operated by WISeKey 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.*

Verification Policies and Practices

Policy Documentation	Language(s) that the documents are in: ENGLISH All documents available at http://www.wisekey.com/repository Direct links: CP & CPS: https://cdn.wisekey.com/uploads/images/WKPKI.DE001-OWGTM-PKI-CPS.v2.8-CLEAN1.pdf Relying Party Agreement: https://www.wisekey.com/Repository/Documents/Relying-Party-Agreement-1.0-wk-signed.pdf
Audits	**Audit Type:** • WebTrust Principles and Criteria for Certification Authorities 2.0 • WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security **Auditor:** Auren **Auditor Website:** http://www.auren.com/en-ES **URL to Audit Report and Management's Assertions:** available at http://www.wisekey.com/repository (also attached separately to this inclusion request)
Baseline Requirements (SSL)	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. In particular, a first statement can be found in section 1.7 of WISeKey's CPS (**1.7. Statement Compliance with CA/Browser Forum requirements**).
SSL Verification Procedures	This information is available in our CPS. Relevant sections are: • **3. Identification and Authentication** (pages 19 to 21) • **12. Annex C: Identity Validation Policies** (pages 71 to 75) The verification procedures for SSL certificates have been audited, as included in the reports linked above.
Organization Verification Procedures	In particular to the above-said, please refer to section "**12.2.2. Corporate and Server Certificates**" in our CPS. Please note that currently all SSL certificates issued by WISeKey include the verification of the organization. Our CPS supports the future issuance of Domain-validated certificates, although this is not practiced yet.

Email Address Verification Procedures	WISeKey CertifyID Personal certificates enforce the validation of Email addresses using different procedures, as stipulated in section "**12.2.1. Personal Certificates**". 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 https://www.certifyid.com The verification procedures for S/MIME-capable certificates have been audited, as included in the reports linked above.
Code Signing Subscriber Verification Procedures	N/A
Multi-Factor Authentication	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, WISeKey makes mandatory the use of a cryptographic hardware device (USB Token or Smartcard) to generate and use the private keys linked to the administrator certificate, except if the administrator is only entitled to generate certificates for a set of pre-authorized domains, being admissible in these cases the use of a software-based client certificate.
Network Security	The Audit reports covering both the existing hierarchy and the new "Generation C" 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"

Response to Mozilla's CA Recommended Practices

Publicly Available CP and CPS	WISeKey's CPS integrates the CP-related information and it's publicly available in English language at http://www.wisekey.com/repository The CPS is redacted following the RFC3647 and any required information can be found at the corresponding section.
CA Hierarchy	Please refer to the previous section, which includes a graphic and a pointer to the textual description of the hierarchy in the CPS.
Audit Criteria	As described in the above sections, WISeKey conducts annual external audits according to the different WebTrust Principles and Criteria. The results of the audits are made public at http://www.wisekey.com/repository For this new Root, we are attaching to this inclusion request the "Point in time" audit reports corresponding to: • Webtrust Principles and Criteria for Certification Authorities 2.0 • Webtrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security
Document Handling of IDNs in CP/CPS	Currently WISeKey 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
Revocation of Compromised Certificates	As stipulated in the CPS (section "**4.9.1. Circumstances for revocation**"), WISeKey revokes any certificate which is known or suspect to be compromised.
Verifying Domain Name Ownership	WISekey 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 "**12. Annex C: Identity Validation Policies**"). This, as expected, has been subject to the latest audits to verify adhesion to Baseline and Extended Validation requirements.
Verifying Email Address Control	We reproduce the same answer stated in a previous section… WISeKey CertifyID Personal certificates enforce the validation of Email addresses using different procedures, as stipulated in section "**12.2.1. Personal Certificates**". 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 https://account.wisekey.com The verification procedures for S/MIME-capable certificates have been audited, as included in the reports linked above.

Verifying Identity of Code Signing Certificate Subscriber	N/A
DNS names go in SAN	WISeKey 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 "**12.2.2. Corporate and Server Certificates**").
Domain owned by a Natural Person	Currently WISeKey doesn't issue SSL certificates to domains owned by Natural Persons, but our internal procedures take in account Mozilla's requirement in this respect.
OCSP	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 sites, resulting in a satisfactory behavior.
Baseline Requirements Self-Assessment	The latest self-assessment document is attached separately to this inclusion request.

Response to Mozilla's list of Potentially Problematic Practices

Long-lived DV certificates	WISeKey issues SSL certificates with a maximum lifespan of 3 years (stipulated at section "**11.3. Corporate and Server Certificates**" of the CPS). This will be reduced according to the new requirements.
Wildcard DV SSL certificates	All current SSL certificates, including Wildcard, enforce the validation of the organization. WISeKey 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.
Email Address prefixes for DV certs	WISeKey observes the Baselines Requirements in its section "**3.2.2.4. Authorization by Domain Name Registrant**", in what respects to the use of common Email prefixes.
Delegation of Domain / Email validation to third parties	WISeKey currently doesn't delegate any activity related to the validation of SSL certificate requests.
Issuing end-entity certificates directly from roots	As describes in the CPS and in the previous sections ("CA Hierarchy"), WISeKey roots never can't issue end-entity certificates, but through Issuing CAs.
Allowing external entities to operate subordinate CA	As described in the previous section "**Externally Operated SubCAs**", **WISeKey only allows SubCAs operated by external entities if these CAs apply name and policy constraints**, in such a way that the entity can only issue certificates for a closed list of pre-authorized domains.
Distributing generated private keys in PKCS#12 files	For personal certificates of classes "Standard" and "Advanced", WISeKey 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 WISeKey a certificate request using PKCS#10, using the certificate management platform.
Certificates referencing hostnames or private IP addresses	WISeKey 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. WISeKey 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.
Issuing SSL certificates for internal domains	As expressed above, WISeKey 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.
OCSP Responses signed by a certificate under a different root	Reproducing the answer for a similar question in a former section… 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: https://goodssl.wisekey.com/, resulting in a satisfactory behavior.
SHA-1 Certificates	WISeKey doesn't issue SSL certificates using SHA-1.
Generic Names for CAs	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 "**OISTE WISeKey Global Root GC CA**".
Lack of Communication with end-users	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: • support@wisekey.com, for any issue related to our certification services • cps@wisekey.com, for issues related to our certification policies and practices
Backdating the notBefore date	WISeKey maintains all reasonable controls to ensure the reliability of the time reference used by the Certification Authority.