Mozilla - CA Program

Case Information

Case Number	00000064	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	WISeKey	**Request Status**	Ready for Public Discussion

Additional Case Information

Subject	Include renewed root	**Case Reason**	

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org /show_bug.cgi?id=1172819

General information about CA's associated organization

CA Email Alias 1	cps@wisekey.com		
CA Email Alias 2			
Company Website	https://www.wisekey.com	**Verified?**	Verified
Organizational Type	Private Corporation	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Not Applicable
Geographic Focus	Global	**Verified?**	Verified
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.	**Verified?**	Verified
Impact to Mozilla Users	Root renewal request. The renewed root cert is SHA-256 and compliant with EV guidelines.	**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	* 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.	**Verified?**	Verified

* 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”).

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	* WISeKey issues SSL certificates with a maximum lifespan of 3 years; except for EV certificates, which are valid for a maximum of one year. * CPS section 14.1.4: It is not permitted to issue Standard SSL certificates containing a “Wildcard character” (*). Only CertifyID Advanced OV SSL Certificates can be issued as “Wildcard SSL Certificates”. * WISeKey currently doesn’t delegate any activity related to the validation of SSL certificate requests. * WISeKey only allows SubCAs operated by external entities if these CAs apply name and policy contraints, in such a way that the entity can only issue certificates for a closed list of pre-authorized domains. * 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. This procedure is implemented by the SSL selling platform (https://reseller.wisekey.com). * WISeKey does 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. * 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. * WISeKey ensures the availability of commercially reasonable resources to attend any request from our subscribers. Main points of contacts are: support@wisekey.com for any issue related to our certification services; and cps@wisekey.com for issues related to our certification policies and practices	**Verified?**	Verified

Root Case Record # 1

Root Case Information

Root Certificate Name	OISTE WISeKey Global Root GB CA	**Root Case No**	R00000087
Request Status	Ready for Public Discussion	**Case Number**	00000064

Additional Root Case Information

Subject	Include OISTE WISeKey Global Root GB CA

Technical Information about Root Certificate

O From Issuer Field	WISeKey	**Verified?**	Verified
OU From Issuer Field	OISTE Foundation Endorsed	**Verified?**	Verified
Certificate Summary	This SHA-256 root cert will eventually replace WISeKey's SHA-1 root cert that was included in NSS via Bugzilla Bug #371362.	**Verified?**	Verified
Root Certificate Download URL	http://public.wisekey.com/crt/owgrgbca.crt	**Verified?**	Verified
Valid From	2014 Dec 01	**Verified?**	Verified
Valid To	2039 Dec 01	**Verified?**	Verified
Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	SHA-256	**Verified?**	Verified
Signing Key Parameters	2048	**Verified?**	Verified
Test Website URL (SSL) or Example Cert	https://goodevssl.wisekey.com	**Verified?**	Verified
CRL URL(s)	http://public.wisekey.com/crl/owgrgbca.crl http://public.wisekey.com/crl/wcidpgbca1.crl http://public.wisekey.com/crl/wcidagbca2.crl	**Verified?**	Verified
OCSP URL(s)	http://ocsp.wisekey.com/ http://ocsp2.wisekey.com	**Verified?**	Verified
Revocation Tested	https://certificate.revocationcheck.com/goodevssl.wisekey.com -- no errors	**Verified?**	Verified
Trust Bits	Code; Email; Websites	**Verified?**	Verified
SSL Validation Type	DV; OV; EV	**Verified?**	Verified
EV Policy OID(s)	2.16.756.5.14.7.4.8	**Verified?**	Verified
EV Tested	// CN=OISTE WISeKey Global Root GB CA,OU=OISTE Foundation Endorsed,O=WISeKey,C=CH "2.16.756.5.14.7.4.8", "WISeKey EV OID", SEC_OID_UNKNOWN, { 0x6B, 0x9C, 0x08, 0xE8, 0x6E, 0xB0, 0xF7, 0x67, 0xCF, 0xAD, 0x65, 0xCD, 0x98, 0xB6, 0x21, 0x49, 0xE5, 0x49, 0x4A, 0x67, 0xF5, 0x84, 0x5E, 0x7B, 0xD1, 0xED, 0x01, 0x9F, 0x27, 0xB8, 0x6B, 0xD6 }, "MG0xCzAJBgNVBAYTAkNIMRAwDgYDVQQKEwdXSVNlS2V5MSIwIAYDVQQLExlPSVNU" "RSBGb3VuZGF0aW9uIEVuZG9yc2VkMSgwJgYDVQQDEx9PSVNURSBXSVNlS2V5IEds" "b2JhbCBSb290IEdCIENB", "drEgUnTwhYdGs/gjGvbCwA==", Success!	**Verified?**	Verified
Root Stores Included In		**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

Digital Fingerprint Information

SHA-1 Fingerprint	0F:F9:40:76:18:D3:D7:6A:4B:98:F0:A8:35:9E:0C:FD:27:AC:CC:ED	**Verified?**	Verified
SHA-256 Fingerprint	6B:9C:08:E8:6E:B0:F7:67:CF:AD:65:CD:98:B6:21:49:E5:49:4A:67:F5:84:5E:7B:D1:ED:01:9F:27:B8:6B:D6	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	There is currently one Policy CA signed by this SHA-256 root cert, and the one Policy CA currently has three active issuing CAs. CA hierarchy diagrams for both the SHA-1 and SHA-256 root certs are provided in section 1.3.1 of the CPS. The root certs sign intermediate certs that sign intermediate certs that sign end-entity certs. CPS section 1.3.1.2: “OWGTM Policy CA G1” is a Certification Authority subordinated to the “OWGTM Root CA GB”. This CA issue certificates for “Issuing CAs” (Certification Authorities that issue certificates for End Entities) dedicated to specific entities and/or purposes, but this CA itself does not issue certificates to end entities. “OWGTM Policy CA G1” can sign: - WISeKey Qualified Issuing CAs - Partner's Qualified Issuing CAs - WISeKey Advanced Issuing CAs - Partner's Advanced Issuing CAs - WISeKey Standard Issuing CAs - Partner's Standard Issuing CAs	**Verified?**	Verified
Externally Operated SubCAs	At this moment, there aren’t externally operated SubCAs under the new SHA-256 root, but this is supported as stipulated in WISeKey's CPS. For the existing SHA-1 root cert's hierarchy, there’s a limited number of CAs operated by external companies, which enforce name constraints. In particular, the currently active SubCAs are: Government of Seychelles (constrained to *.gov.sc), and The Bancorp Inc. (constrained to *.wise-corp.co, *.thebancorp.com, *.wisecorp.us and *.wise-- corp.us)	**Verified?**	Verified
Cross Signing	Not supported	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	Registration Authorities: CPS sections 1.3.2 and 9.6.2 CPS section 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	**Verified?**	Verified

	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. Also see CPS section 12.1.		

Verification Policies and Practices

Policy Documentation	CPS section 1.1: The main information disclosed by the OWGTM in order to expose its practices and policies in the issuance and usages of digital certificates are: - The Certification Practices Statement (CPS) –The CPS is a statement of the practices that every Certification Authority operating under the OWGTM Trust Model employs in issuing, managing, revoking, and renewing or re-keying certificates. - ... The currently approved CPs are incorporated in this version of the CPS, as summarized in Annex B: Approved Certificate Policies and Profiles. Any explicit mention to a CP document must be understood as referring to this document; OWGTM does not maintain separate CP documents.	**Verified?**	Verified
CA Document Repository	http://www.wisekey.com/repository	**Verified?**	Verified
CP Doc Language	English		
CP	https://cdn.wisekey.com/uploads/images/WKPKI.DE001-OWGTM-PKI-CPS.v2.3-CLEAN.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	https://cdn.wisekey.com/uploads/images/WKPKI.DE001-OWGTM-PKI-CPS.v2.3-CLEAN.pdf	**Verified?**	Verified
Other Relevant Documents	Relying Party Agreement: http://www.wisekey.com/Repository/Documents/Relying-Party-Agreement-1.0-wk-signed.pdf?6ecb07	**Verified?**	Verified
Auditor Name	Auren	**Verified?**	Verified
Auditor Website	http://www.auren.com	**Verified?**	Verified
Auditor Qualifications	http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx	**Verified?**	Verified
Standard Audit	https://cdn.wisekey.com/uploads/documents/WISeKey-WebTrust-Audit-Report-2015.pdf?6ecb07	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	6/8/2015	**Verified?**	Verified

BR Audit	https://cdn.wisekey.com/uploads/documents/WISeKey-WebTrust-Audit-Report-2015.pdf?6ecb07	**Verified?**	Verified
BR Audit Type	WebTrust	**Verified?**	Verified
BR Audit Statement Date	6/8/2015	**Verified?**	Verified
EV Audit	https://cdn.wisekey.com/uploads/documents/WISeKey-WebTrust-Audit-Report-2015.pdf?6ecb07	**Verified?**	Verified
EV Audit Type	WebTrust	**Verified?**	Verified
EV Audit Statement Date	6/8/2015	**Verified?**	Verified
BR Commitment to Comply	CPS section 1.7	**Verified?**	Verified
SSL Verification Procedures	CPS section 3.2.2, 3.2.3, 3.2.5: This information is specified in Annex C: Identity Validation Policies CPS section 12 == Annex C CPS section 12.2.2: CertifyID Standard SSL Certificate: The identification data included in the certificate are verified according to the Baseline Requirements made public by the CA/Browser Forum. (For more information, see section 14 "Annex E: Notes on validation methods for SSL and Code Signing certificates") CertifyID Advanced OV SSL Certificate: In addition to the methods indicated for Standard SSL certificates... CPS section 14.1.2 and 14.2.2 For the Fully-Qualified Domain Name listed as SAN in a Certificate, the Agent shall confirm that, as of the date the Certificate was issued, the Applicant either is the Domain Name Registrant or has control over the FQDN by any of the following: 1. Communicating directly with the Domain Name Registrant using the contact information listed in the WHOIS record's "registrant", "technical", or "administrative" field; 2. Communicating with the Domain's administrator using an email address created by pre-pending 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' in the local part, followed by the at-sign ("@"), followed by the Domain Name, which may be formed by pruning zero or more components from the requested FQDN; 3. Relying upon a Domain Authorization Document (See Note); or 4. Having the Applicant demonstrate practical control over the FQDN...	**Verified?**	Verified
EV SSL Verification Procedures	CPS section 12.2.2: CertifyID Advanced EV SSL Certificate: The identification data included in the certificate are verified according to the Baseline Requirements made public by the CA/Browser Forum.	**Verified?**	Verified

	(For more information, see section 14 "Annex E: Notes on validation methods for SSL and Code Signing certificates")		
Organization Verification Procedures	CPS section 14.2.1.2 - Verification of Organization Identity CPS section 14.3 - Verification process for CertifyID Advanced EV SSL Certificates	**Verified?**	Verified
Email Address Verification Procedures	CPS section 12.2.1 -- Personal Certificates Standard -- ID Data Verified: Basic data is verified such as the email address; or in the case of an organisation ownership of the domain names in the certificate, with responsibility to verify the individual entities to which certificates are issued. Method of Verification: - Bounce back email verification procedure proving access to the email account is accepted. - Database (such as existing HR, or IDM) of organisation, with details of organisation's users. - Commonly accepted business methods of identity verification. Advanced -- May be done through database of identity data that is well maintained and was created based on face to face or direct verification using official ID documents. Qualified -- Face to face or direct verification but may be done through database of identity data that is well-maintained and was created based on face to face or direct verification using primary ID documents.	**Verified?**	Verified
Code Signing Subscriber Verification Pro	CPS section 12.2.4: CertifyID Code Signing and CertifyID EV Code Signing Certificates: The identification data included in the certificate are verified according to the Extended Validation Requirements made public by the CA/Browser Forum. (For more information, see section 14 “Annex E: Notes on validation methods for SSL and Code Signing certificates”) CPS section 14.4 - Verification process for CertifyID Code Signing Certificates CPS section 14.5 - Verification process for CertifyID EV Code Signing Certificates	**Verified?**	Verified
Multi-Factor Authentication	CPS section 6.5	**Verified?**	Verified
Network Security	CPS section 6.7	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	https://www.wisekey.com/repository	**Verified?**	Verified