Print this page

Mozilla - CA Program

Case Information

Case Number	00000165	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	WISeKey	**Request Status**	In Detailed CP/CPS Review

Additional Case Information

Subject	Add OISTE WISeKey Global Root GC CA root certificate	**Case Reason**	

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org /show_bug.cgi?id=1403591

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?**	Verified
Geographic Focus	Switzerland, 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

Required and Recommended Practices

Recommended Practices	https://wiki.mozilla.org /CA/Required_or_Recommended_Practices	**Recommended Practices Statement**	I have reviewed Mozilla's lists of Required and 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	Page 8 of https://bug1403591.bmoattachments.org/attachment.cgi?id=8912719	**Verified?**	Verified

Forbidden and Potentially Problematic Practices

Potentially Problematic Practices	https://wiki.mozilla.org/CA/Forbidden_or_Problematic_Practices	**Problematic Practices Statement**	I have reviewed Mozilla's lists of Forbidden and 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	Page 10 of https://bug1403591.bmoattachments.org/attachment.cgi?id=8912719	**Verified?**	Verified

Root Case Record # 1

Root Case Information

Root Certificate Name	OISTE WISeKey Global Root GC CA	**Root Case No**	R00000405
Request Status	In Detailed CP/CPS Review	**Case Number**	00000165

Certificate Data

Certificate Issuer Common Name	OISTE WISeKey Global Root GC CA
O From Issuer Field	WISeKey
OU From Issuer Field	OISTE Foundation Endorsed
Valid From	2017 May 09
Valid To	2042 May 09
Certificate Serial Number	212a560caeda0cab4045bf2ba22d3aea
Subject	CN=OISTE WISeKey Global Root GC CA, OU=OISTE Foundation Endorsed, O=WISeKey, C=CH

Signature Hash Algorithm	ecdsaWithSHA384
Public Key Algorithm	EC secp384r1
SHA-1 Fingerprint	E0:11:84:5E:34:DE:BE:88:81:B9:9C:F6:16:26:D1:96:1F:C3:B9:31
SHA-256 Fingerprint	85:60:F9:1C:36:24:DA:BA:95:70:B5:FE:A0:DB:E3:6F:F1:1A:83:23:BE:94:86:85:4F:B3:F3:4A:55:71:19:8D
Certificate Fingerprint	7A:FC:85:4B:65:6E:7D:F8:E1:05:EA:76:A5:01:26:BA:A4:E0:BA:E4:C8:C1:10:0C:4E:B1:2F:8C:A8:4F:9F:A3
Certificate Version	3

Technical Information about Root Certificate

Certificate Summary	This is WISeKey's Generation C root certificate. Their Generation A and B root certificates are currently included in Mozilla's root store. This ECC root cert will be used in “Internet of Things” (IoT) environments, client auth, SSL, and S/MIME.	**Verified?**	Verified
Root Certificate Download URL	https://bugzilla.mozilla.org /attachment.cgi?id=8912737	**Verified?**	Verified
CRL URL(s)	http://public.wisekey.com /crl/wcidgcas1.crl	**Verified?**	Verified
OCSP URL(s)	http://ocsp.wisekey.com	**Verified?**	Verified
Mozilla Trust Bits	Email; Websites	**Verified?**	Verified
SSL Validation Type	DV; OV	**Verified?**	Verified
Mozilla EV Policy OID(s)	Not EV	**Verified?**	Not Applicable
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints		**Verified?**	Not Applicable

Test Websites or Example Cert

Test Website - Valid	https://gcvalidssl.hightrusted.com/	**Verified?**	Verified
Test Website - Expired	https://gcexpiredssl.hightrusted.com/		
Test Website - Revoked	https://gcrevokedssl.hightrusted.com/		

Example Cert	
Test Notes	

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

Revocation Tested	https://certificate.revocationcheck.com/gcvalidssl.hightrusted.com no errors	**Verified?**	Verified
CA/Browser Forum Lint Test	https://crt.sh/?caid=64091&opt=cablint,zlint,x509lint&minNotBefore=2000-01-01 no errors	**Verified?**	Verified
Test Website Lint Test	see above	**Verified?**	Verified
EV Tested	Not EV	**Verified?**	Not Applicable

CA Hierarchy Information

CA Hierarchy	CPS section 1.3.1. https://www.wisekey.com/cacertificates/#cidcrl Currently this root cert has one internally-operated issuing intermediate cert, WISeKey CertifyID Advanced GC CA 1.	**Verified?**	Verified
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 the CPS, using a "Name constraint" and/or "EKU constraint" approach.	**Verified?**	Verified
Cross Signing	None	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	CPS section 7.1.5. 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	**Verified?**	Verified

	access to a dedicated Registration Authority. External RAs are also allowed, but are legally bound to comply with the documented verification procedures.		

Verification Policies and Practices

Policy Documentation	Documents are in English	**Verified?**	Verified
CA Document Repository	https://www.wisekey.com/repository/	**Verified?**	Verified
CP Doc Language	English		
CP	https://cdn.wisekey.com/uploads/images/WKPKI.DE001-OWGTM-PKI-CPS.v2.9-CLEAN.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	https://cdn.wisekey.com/uploads/images/WKPKI.DE001-OWGTM-PKI-CPS.v2.9-CLEAN.pdf	**Verified?**	Verified
Other Relevant Documents	https://www.wisekey.com/repository/	**Verified?**	Verified
Auditor (New)	Auren	**Verified?**	Verified
Auditor Location (New)	Spain	**Verified?**	Verified
Standard Audit	https://cdn.wisekey.com/uploads/images/Audit-Report-and-Management-Assertions-Webtrust-CA-GC.pdf	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	12/5/2017	**Verified?**	Verified
BR Audit	https://cdn.wisekey.com/uploads/images/Audit-Report-and-Management-Assertions-Webtrust-BR-GC.pdf	**Verified?**	Verified
BR Audit Type	WebTrust	**Verified?**	Verified
BR Audit Statement Date	12/5/2017	**Verified?**	Verified
EV SSL Audit	Not EV	**Verified?**	Not Applicable
EV SSL Audit Type		**Verified?**	Not Applicable
EV SSL Audit Statement Date		**Verified?**	Not Applicable
BR Commitment to Comply	CPS section 1.7	**Verified?**	Verified

BR Self Assessment	https://bug1403591.bmoattachments.org/attachment.cgi?id=8912732	**Verified?**	Verified
SSL Verification Procedures	Domain Verification is in CPS section 14.1.2, 14.1.3, 14.2.2, 14.2.3 CPS section 3.2 points to section 12, Annex C: Identity Validation Policies. Section 12.1 is about subCA certs, technically constraining such certs, and verifying that the organization owns the domain names to be in the constraints. Section 12.2 is about verifying personal and server certificates. Points to section 14, Annex E for details.	**Verified?**	Verified
EV SSL Verification Procedures	Not requesting EV treatment.	**Verified?**	Not Applicable
Organization Verification Procedures	CPS sections 14.2.1.2, 14.3.2.1, 14.3.2.2, 14.3.2.3, 14.3.2.4, 14.3.3, 14.3.5 CPS section 3.2.2 points to Annex C (section 12). CPS section 12.2.2 points to section 14, Annex E.	**Verified?**	Verified
Email Address Verification Procedures	CPS section 12.2.1.	**Verified?**	Verified
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	**Verified?**	Not Applicable
Multi-Factor Authentication	CPS section 5.2.3	**Verified?**	Verified
Network Security	CPS section 6.7	**Verified?**	Verified