CA's Self-Assessment of CP/CPS documents to CA/Browser Forum Baseline Requirements (BRs)

Introduction:

1) CA's Legal Name: WISeKey SA
2) PKI Hierarchy in scope of this assessment:

```
ROOT 1: OISTE WISeKey Global Root GB CA / 0F:F9:40:76:18:D3:D7:6A:4B:98:F0:A8:35:9E:0C:FD:27:AC:CC:ED
    INTERMEDIATE: WISeKey CertifyID Policy GB CA 1 / 63:8E:F7:24:26:BD:7A:8F:61:A5:78:CD:F3:C6:29:57:EE:03:8F:32 - CAN ISSUE SSL, EV ENABLED
        ISSUING: WISeKey CertifyID Advanced GB CA 1 / DA:69:96:C8:60:97:A9:3E:36:FF:7A:36:90:DC:29:96:7D:07:9A:8C - DEPRECATED, NOT USED ANYMORE
        ISSUING: WISeKey CertifyID Advanced GB CA 2 / 5B:DE:30:A0:26:C7:5C:36:C8:50:E3:26:68:E2:96:C8:19:A0:E2:D3
    INTERMEDIATE: WISeKey CertifyID Qualified GB CA 2 / 49:52:95:70:02:8B:30:F8:8F:D7:AA:AF:49:CF:42:92:C6:74:11:FA
        (No issuing CAs under this Intermediate)
    INTERMEDIATE: WISeKey CertifyID Standard GB CA 2 / 97:C6:45:22:1C:68:B8:74:EB:E8:A3:1B:0F:4A:F1:67:C8:8F:0E:BC
        (No issuing CAs under this Intermediate)
ROOT 2: OISTE WISeKey Global Root GA CA / 59:22:A1:E1:5A:EA:16:35:21:F8:98:39:6A:46:46:B0:44:1B:0F:A9
    INTERMEDIATE: WISeKey CertifyID Advanced G1 CA / 9C:EF:ED:B3:3C:24:8D:16:FC:CF:D0:8C:62:CD:44:BC:56:A0:D5:F0
        ISSUING: WISeKey CertifyID Advanced Services CA 2 / 04:97:A1:0D:77:5E:09:87:3B:A6:FF:84:D7:79:9C:F3:D7:E0:A1:A9 - DOESN'T ISSUE SSL
    INTERMEDIATE: WISeKey Qualified Services CA 2 / 73:72:B2:A6:F8:E7:DA:8C:C7:4E:A3:4C:3E:64:92:DB:43:4D:09:CE
        ISSUING: WISeKey CertifyID Qualified G1 CA / BD:59:C8:B9:E2:76:CC:0E:EC:EF:03:26:3B:A6:63:C1:7D:AE:FA:98 - DOESN'T ISSUE SSL
    INTERMEDIATE: WISeKey CertifyID Standard G1 CA / 9D:72:1A:47:CB:CA:CD:D7:FE:10:DE:A0:6C:EB:3C:99:21:6D:46:15
        ISSUING: WISeKey CertifyID Standard Services CA 2 / 04:C8:4E:53:F0:22:A5:3F:72:1E:32:B8:12:28:6B:87:21:58:AE:E3 - DOESN'T ISSUE SSL
    INTERMEDIATE: WISeKey CertifyID Policy GA CA 1 / 6C:C2:74:33:26:8F:ED:1F:91:37:E5:5F:80:8F:58:0D:2D:2F:B8:1B
        (No issuing CAs under this Intermediate)
    ISSUING: WISeKey CertifyID Advanced Services CA 3 / F5:C7:14:E6:88:19:83:3D:DD:A1:88:28:3C:88:24:9E:82:FA:3E:3B - DEPRECATED, NOT USED ANYMORE
    ISSUING: WISeKey CertifyID Advanced Services CA 4 / DF:02:FB:DE:A8:20:AC:7E:D7:5E:4B:EF:AE:A5:09:7E:A6:44:01:D2 - MAIN CA FOR SSL CERTIFICATES
ROOT 3: OISTE WISeKey Global Root GC CA / E0:11:84:5E:34:DE:BE:88:81:B9:9C:F6:16:26:D1:96:1F:C3:B9:31
    ISSUING: WISeKey CertifyID Advanced GC CA 1 / 13:A1:8A:B2:90:58:BC:34:63:64:07:52:E7:3F:0B:58:54:81:7D:96
```

3) BR version 1.4.2, with the exception of the Domain Validation section 3.2.2.4 for which we used BR version 1.4.1.
4) Related CP/CPS document: CPS Version x.x, available at https://www.wisekey.com/repository (WISeKey CPS integrates also the CP estipulations).
5) No further update is deemed necessary after this self-assessment.

Referenced Documents:
CPS: Certificate Practices Statement
SECPOL: Corporate Security Policy
SLA: Standard SLA Agreement

BR Section Number	Documents and section numbers of those documents which meet the requirements of each BR section	Explain how the CA's listed documents meet the requirements of each BR section.
1.2.1. Revisions Note the Effective Date for each item in the table. Certificates created after each Effective Date are expected to be in compliance with the item. Make sure your CA is in compliance with each of these items. After careful consideration, indicate if your CA is fully compliant with all items in the table, or clearly indicate action that your CA is taking to improve compliance.	CPS: Version 2.8	We consider the current CPS compliant with the requirements
1.2.2. Relevant Dates Note the Compliance date for eachitem in the table. Those are the dates by which your CP/CPS and practices are expected to be updated to comply with the item. Make sure your CA is in compliance with each of these items. After careful consideration, indicate if your CA is fully compliant with all items in the table, or clearly indicate action that your CA is taking to improve compliance.	CPS: 19 June 2017	We don't consider immediate chages as result of this assessment
1.3.2. Registration Authorities Indicate whether your CA allows for Delegated Third Parties, or not. Indicate which sections of your CP/CPS specify such requirements, and how the CP/CPS meets the BR requirements for RAs.	CPS Section 1.3.2 Registration authorities	WISeKey only delegates the issuance of Personal Certificates
2.1. Repositories Provide the direct URLs to the CA's repositories	CPS Section 2.1 Repositories	Policies and public documents repository: http://www.wisekey.com/repository. Public access to certificate download: http://trustcenter.certifyid.com/ura/public/
2.2. Publication of information "The CA SHALL publicly give effect to these Requirements and represent that it will adhere to the latest published version." --> Copy the specific text that is used into the explanation in this row. (in English)	CPS Section 1.7 Statement on Compliance with CA/Browser Forum requirements	WISeKey, as operator of the OWGTM ensures the compliance with industry best practices and security controls. In particular, OWGTM enforces regular review and compliance with the latest version of the “Baseline Requirements” and “Extended Validation Requirements” for the certificate profiles to which these regulations apply.
2.2. Publication of information "The CA SHALL host test Web pages that allow Application Software Suppliers to test their software with Subscriber Certificates that chain up to each publicly trusted Root Certificate. At a minimum, the CA SHALL host separate Web pages using Subscriber Certificates that are (i) valid, (ii) revoked, and (iii) expired." --> List the URLs to the three test websites (valid, revoked, expired) for each root certificate under consideration. If you are requesting EV treatment, then the TLS cert for each test website must be EV.	This is not included in the CPS	The test URLs are: https://gXvalidssl.hightrusted.com https://gXexpired.hightrusted.com https://gXrevoked.hightrusted.com Where X is "a", "b" or "c", to reference the three current roots (GA, GB and GC)
2.3. Time or frequency of publication Indicate your CA's policies/practices to ensure that the BRs are reviewed regularly, and that the CA's CP/CPS is updated annually.	CPS Section 1.5.4 CPS approval procedures	It’s required to issue new CP/CPS versions at least once a year.
2.4. Access controls on repositories Acknowledge that all Audit, CP, CPS documents required by Mozilla's CA Certificate Policy and the BRs will continue to be made publicly available.	CPS Section 2.1 Repositories	We don't apply access controls to the documents published in the Repository
3.2.2.1 Identity If the Subject Identity Information in certificates is to include the name or address of an organization, indicate how your CP/CPS meets the requirements in this section of the BRs.	CPS Section 14.1.2	We verify the name and address in the public registris (e.g. Chamber of Commerce)
3.2.2.2 DBA/Tradename If the Subject Identity Information in certificates is to include a DBA or tradename, indicate how your CP/CPS meets the requirements in this section of the BRs.	Does not apply	
3.2.2.3 Verification of Country If the subject:countryName field is present in certificates, indicate how your CP/CPS meets the requirements in this section of the BRs.	CPS Section 14.1.3	We verify the country that sources the validation documents
3.2.2.4 Validation of Domain Authorization or Control Indicate which of the methods of domain validation your CA uses, and where this is described in your CP/CPS. The CA's CP/CPS must clearly describe the acceptable methods of domain validation. It is *not* sufficient for the CP/CPS to merely reference the BRs. Enough information must be directly provided in the CP/CPS for the reader to be able to understand how the CA performs domain validation.	CPS Section 14.2.2	We allow two main methods: 1. We send a random code and the customer must create a file in a given URL including the code 2. We request an authorization letter sent from the registered Fax

3.2.2.4.1 Validating the Applicant as a Domain Contact If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	Not used	
3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	CPS Section 14.2.2	We request to use a formal letterhead that gives assurance on the source
3.2.2.4.3 Phone Contact with Domain Contact If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	CPS Section 14.2.2	This is not a common practice for WISeKey
3.2.2.4.4 Constructed Email to Domain Contact If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	Not used	
3.2.2.4.5 Domain Authorization Document If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	CPS Section 14.2.2	WISeKey provides a template letter, which must be completed and signed by the owner of the domain
3.2.2.4.6 Agreed-Upon Change to Website If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	CPS Section 14.2.2	We send a random code and the customer must create a file in a given URL including the code
3.2.2.4.7 DNS Change If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	Not used	
3.2.2.4.8 IP Address If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	Not used	
3.2.2.4.9 Test Certificate If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	Not used	
3.2.2.4.10. TLS Using a Random Number If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	Not used	
3.2.2.5 Authentication for an IP Address If your CA allows IP Addresss to be listed in certificates, indicate how your CA meets the requirements in this section of the BRs.	Not used	
3.2.2.6 Wildcard Domain Validation If your CA allows certificates with a wildcard character (*) in a CN or subjectAltName of type DNS-ID, then indicate how your CA meets the requirements in this seciton of the BRs.	CPS Section 14.2.4	The CertifyID Reseller Portal implements automated CSR validation rules to ensure that only valid SAN are accepted, this also covers the case of Wildcard certificates
3.2.2.7 Data Source Accuracy Indicate how your CA meets the requirements in this section of the BRs.	CPS Section 14.2.2	We only accept official document sources
3.2.3. Authentication of Individual Identity	CPS Section 14.2	We request copy of a valid official ID document (Passport, National ID, Drivers License)
3.2.5. Validation of Authority	CPS	Same as 2.2.4.5
3.2.6. Criteria for Interoperation or Certification Disclose all cross-certificates in the CA hierarchies under evaluation.	Does not apply	
4.1.1. Who Can Submit a Certificate Application Indicate how your CA identifies suspicious certificate requests.	CPS Section 4.1.1	A certificate application can be submitted by the subject of the certificate or by an authorized representative of the subject.
4.1.2. Enrollment Process and Responsibilities	CPS Section 4.1.2 and 12	WISeKey defines the role of the "Enrolment Agent" as the main responsible of the process. It may be delegated to authorized third parties
4.2. Certificate application processing		
4.2.1. Performing Identification and Authentication Functions Indicate how your CA identifies high risk certificate requests.	CPS Sections 4.2.1 and 4.2.2	As noted in the CPS: "A rejection of a certificate application results in a notification being sent to the applicant by appropriate means, and is registered for further reference." Any high risk request would be denied and kept in a list, which is controlled by the enrollment agent
4.2.2. Approval or Rejection of Certificate Applications	CPS Section 4.2.2	As described in the CPS
4.3.1. CA Actions during Certificate Issuance	CPS Section 4.3.1 and 4.3.2	A Certification Authority adhering to the OWGTM proceeds with the issuance of a certificate only after executing the necessary measures to verify that the request received by a Registration Authority is genuine, by verifying the signatures of the CSR. The CA will publish the certificate and the RA will notify the user by email.
4.9.1.1 Reasons for Revoking a Subscriber Certificate Reasons for revoking certificates must be listed in the CA's CP/CPS.	CPS Section 4.9.1	This information is included in the CPS
4.9.1.2 Reasons for Revoking a Subordinate CA Certificate	CPS Section 4.9.1	This information is included in the CPS
4.9.2. Who Can Request Revocation	CPS Section 4.9.2 Who can request revocation	Subscriber or authorized representative.
4.9.3. Procedure for Revocation Request	CPS Section 4.9.3 Procedure for revocation request	• Remote requests sent by e-mail or via a web page or service, appropriately authenticated by the subscriber or its representative. • Face-to-face requests addressed to an official Registration Authority representative and the identity of the requestor is proved by the same means as used for certificate registration. • Revocation requests sent by an official Registration or Certification representative operating under the OWGTM Trust Model.
4.9.5. Time within which CA Must Process the Revocation Request	CPS Section 4.9.5	We don't set an specfic time. We specify "Revocation requests are processed by the CA within the shortest possible period."
4.9.7. CRL Issuance Frequency	CPS Section 4.9.7	The stipulated frequencies are: • The OWGTM Root CAs issue a full CRL every year, with a typical overlapping period of one week. This CRL will contain the revoked, if any, certificates for OWGTM Policy CAs or Issuing CAs, as appropriate for the hierarchy. New CRLs are published immediately if a new subordinated CA is revoked. • The OWGTM Policy CAs issue a full CRL every month, with a typical overlapping period of 3 days. This CRL will contain the revoked, if any, certificates for OWGTM Issuing CAs. New CRL are published immediately if a new subordinated CA is revoked. • The OWGTM Issuing CAs issue a full CRL every up to three days, with a maximum latency of two additional days in case of service disruption. This CRL will contain the revoked, if any, certificates for OWGTM end-users / subscribers.
4.9.9. On-line Revocation/Status Checking Availability	CPS Section 4.9.9	The Issuing Certificate Authorities in the OWGTM provide an OCSP service that is typically available on a 24x7 basis. The OCSP service availability is not mandatory for low assurance certificates, as the “CertifyID Standard Personal Certificate” and some types of device or personal certificates. NOTE: There's a DR Site to ensure the capability to provide revocation services
4.9.10. On-line Revocation Checking Requirements Indicate how your CA meets all of the requirements listed in this section, including support of GET, update frequency, preventing errounious return of "good" status.	Not in the CPS	We implement the EJBCA OCSP Responder, which implements properly GET and the responses for non-existent certificates
4.9.11. Other Forms of Revocation Advertisements Available Indicate if your CA supports OCSP stapling.	Does not apply	
4.10.1. Operational Characteristics	CPS Section 4.10.1	Certificate Status Services are accessible through HTTP servers owned by the OWGTM Certification Authorities. The Services can be accessed by downloading revocation lists (CRL) or by sending requests to OCSP servers. The appropriate certificate revocation information service URLs are included in standard extensions within the issued certificates. Other services could be available, as stipulated in the corresponding End User Agreement.
4.10.2. Service Availability	CPS Section 4.10.2	The Certificate Status Services are available on a 24x7 basis. As explained in 4.9.9
5. MANAGEMENT, OPERATIONAL, and Physical CONTROLS		

5.2.2. Number of Individuals Required per Task	CPS Sections 5.2.2 and 5.2.4	
5.3.1. Qualifications, Experience, and Clearance Requirements	CPS Section 5.3.1 and WISeKey Trusted Personnel Policy (not public)	We implement a trusted personnel policy to ensure compliance with the best practices and Webtrust requirements
5.3.3. Training Requirements and Procedures	CPS Section 5.3.3	New employees or third parti enrollment agents are training before starting their duties
5.3.4. Retraining Frequency and Requirements	CPS Section 5.3.4	We don't specify retraining frequencies, only "as required"
5.3.7. Independent Contractor Controls	CPS Section 5.3.7	We base these controls in the acceptance of the Security Policy and the signature of an NDA. Note: these controls will be improved in the next audit period
5.4.1. Types of Events Recorded	CPS Section 5.4.1	All the events are listed in the CPS and are part of the sudit scope
5.4.3. Retention Period for Audit Logs	CPS Section 5.4.3	We specify that the retention period is the validity of the involved certificate
5.4.8. Vulnerability Assessments	CPS Section 5.4.8	We execute annual external penetration tests and internal tests. The frequency of the internal tests must be increased to improve compliance
5.5.2. Retention Period for Archive	CPS Section 5.5.2	Archived records and audit logs are kept Records are retained for at least the validity of the involved certificates.
5.7.1. Incident and Compromise Handling Procedures	CPS Section 5.7.1, SECPOL, SLA	WISeKey discloses public information about these procedures in the CPS, which are enforced and audited
6.1.1. Key Pair Generation	CPS Section 6.1.1	Apart of the stated in the CPS, WISeKey doesn't provide key generation services for SSL subscribers, who must provide a valid CSR
6.1.2. Private Key Delivery to Subscriber	CPS Section 6.1.1	WISeKey doesn't support key generation for SSL Certificates, so the private key is not sent to the subscriber, for other certificate types, different types are supported, as stated in the CPS
6.1.5. Key Sizes	CPS Section 6.1.5	The OWGTM enforces the use of minimum length 2048-bit RSA and ECC NIST P-256, P-384 for key pairs at all levels of the hierarchy.
6.1.6. Public Key Parameters Generation and Quality Checking	CPS Section 6.1.6	The algorithm used in the OWGTM for key generation is RSA or ECC.
6.1.7. Key Usage Purposes	CPS Section 6.1.7, Section 11	The detailed KU and EKU combinations are detailed for each certificate type at Section 11. CA and SSL Certfificates are checked to be compatible with CA. There are some old CAs in the hierarchy that were created before the BR specification, thus can't be changed
6.2. Private Key Protection and Cryptographic Module Engineering Controls	CPS Section 6.2	Certification Authorities in the OWGTM are required to use Hardware Security Modules, at least compliant with FIPS 140-2 Level 2 for PKI components. Requirements for End-User cryptographic devices (if any) can vary in terms of the expected assurance level.
6.2.5. Private Key Archival	CPS Section 6.2.5	The Private Keys are never archived for any PKI participant.
6.2.6. Private Key Transfer into or from a Cryptographic Module	CPS Section 6.2.6	For Certification Authorities operating under the OWGTM Trust Model it is mandatory that key pairs are operated in Hardware Security Modules as defined in section 6.2.1. Private Keys can be transferred to adequate hardware security modules for back-up and recovery operations.
6.2.7. Private Key Storage on Cryptographic Module	CPS Section 6.2.7	CA or RA private keys held on hardware cryptographic modules are stored in an encrypted form supported by the HSM vendor. End-entity private keys must use encrypted containers compliant at least with FIPS 140-1 Level 1.
6.3.2. Certificate Operational Periods and Key Pair Usage Periods	CPS Section 6.3.2	OWGTM Root CA GA (SHA-1) 32 years OWGTM Root CA GB (SHA-2) 25 years OWGTM Root CA GC (SHA-2) 25 years Policy and Issuing Certification Authority Up to the entire life time of the Root CA upon issuance End-Entity Certificate Up to 3 years
6.5.1. Specific Computer Security Technical Requirements	CPS Section 6.5.1, SECPOL	As disclosed in the CPS. The internal security documentation details the implementation. Internal audits are done to check compliance
7.1. Certificate profile	CPS Section 7.1 and Section 11	The CPS details teh different certificate profiles in Annex B
7.1.1. Version Number(s)	As per CPS	OK
7.1.2. Certificate Content and Extensions; Application of RFC 5280	As per CPS	OK
7.1.2.1 Root CA Certificate	As per CPS	OK
7.1.2.2 Subordinate CA Certificate	As per CPS	OK
7.1.2.3 Subscriber Certificate	As per CPS	OK
7.1.2.4 All Certificates	As per CPS	OK
7.1.2.5 Application of RFC 5280	Does not apply	We don't issue pre-certificates
7.1.3. Algorithm Object Identifiers	As per CPS	OK
7.1.4. Name Forms	As per CPS	OK
7.1.4.1 Issuer Information	As per CPS	OK
7.1.4.2 Subject Information	As per CPS	OK
7.1.4.3 Subject Information - Subordinate CA Certificates	As per CPS	OK
7.1.5. Name Constraints	As per CPS	WISeKey enforces the use of Name constraints in subordinate CAs not owned and operated by WISeKey. This is under tha audited scope
7.1.6. Certificate Policy Object Identifier	As per CPS	OK
7.1.6.1 Reserved Certificate Policy Identifiers	As per CPS	OK
7.1.6.2 Root CA Certificates	As per CPS	OK
7.1.6.3 Subordinate CA Certificates	As per CPS	OK
7.1.6.4 Subscriber Certificates	As per CPS	OK
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS	CPS Section 8	
8.1. Frequency or circumstances of assessment	CPS Section 8.1	All Certification Authorities and dependent Registration Authorities must follow the adequate assessment program (as stipulated in section 8.4 of the CPS) on an annual frequency.
8.2. Identity/qualifications of assessor	Section 8.2	External audits are performed by AUREN (Spain)
8.4. Topics covered by assessment	Section 8.4	The OWGTM establishes two levels of audit and accreditation. • The Root CA, Policy CAs and Issuing CAs owned or operated by WISeKey. These services are audited against the WebTrust criteria and commonly accepted industry accreditation standards. Issuing CAs operated by third parties which don't enforce name constraints must be included in this assessment. • The Issuing CAs owned and/or operated by third parties enforcing name constraints. These services must meet the practices stipulated in this CPS, and the CPs that are entitled to issue, and are audited and accredited by the OWGTM by means of an internal audit executed by WISeKey or other authorized auditor.
8.6. Communication of results	Section 8.6	The summarized report is deemed public and is only published in the OWGTM Repository. Also communicated as required by the different CA Programs (i.e. Mozilla CA Database)
8.7. Self-Audits	Not disclosed in the CPS as a separate section	WISeKey does an internal audit covering the full list of SSL certificates and a sample (5%) of personal certificates issued by external RAs.

9.6.1. CA Representations and Warranties	CPS Section 9.6.1	OWGTM Root CAs will: • Establish a chain of trust by issuing a certificate, which is a self-signed certificate • Ensure that the Root signs any subordinate CAs issued under the OWGTM hierarchy • Properly conduct the verification process described in section 3.2 • Ensure the accuracy and completeness of any part of the certificate information which is generated or compiled by the OWGTM, according to the applicable Certification Policy • Ensure that all relevant information concerning a certificate is recorded (electronically or otherwise) for an appropriate period of time, and in particular, for the purpose of providing evidence for the purposes of legal proceedings • Utilise trustworthy systems, procedures and human resources in performing its services • Comply with any other relevant provisions of the relevant CP or CPS, and other approved documents. All CAs in the OWGTM will: • Operate according to the requirements of this CPS and any applicable SLA. • Ensure at the time it issues a certificate, that the certificate contains all the elements required by the CP or PDS. • Manage their keys in accordance with Section 6.2 Private Key Protection and Cryptographic Module Engineering Controls. • Ensure the availability of a Certificate Directory and CRL • Promptly revoke a certificate if required. • MITM / traffic management policy: Explicitly, the CAs will not issue a certificate that can be used for MITM or “traffic management” of domain names or IPs that the certificate holder does not legitimately own or control. Therefore, the Issuing CA will be required to diligently execute the appropriate proofs of ownership or representation in the certificate issuance process. • In particular and where applicable, CAs will respect the warranties and obligations set by the CA/Browser Forum Baseline and EV Requirements.
9.6.3. Subscriber Representations and Warranties	CPS Section 9.6.3	The Subscribers of certificates issued under the OWGTM must warrant that: • All information supplied by the Subscriber and contained in the Certificate is true and valid. • All representations made by the Subscriber in the submitted Certificate Application are true and valid. • His or her private key is protected and that no unauthorized person has ever had access to the Subscriber’s private key. • An obligation and warranty that it will not install and use the Certificate(s) until it has reviewed and verified the accuracy of the data in each Certificate. • An obligation and warranty to install the Certificate only on the server accessible at the domain name listed on the Certificate, and to use the Certificate solely in compliance with all applicable laws, solely for authorized company business, and solely in accordance with the Subscriber Agreement. • The Certificate is being used exclusively for authorized and legal purposes, consistent with this CPS. • Each digital signature created using the private key corresponding to the public key listed in the Certificate is the digital signature of the Subscriber and the Certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created. • The Subscriber is an end-user Subscriber and not a CA, and is not using the private key corresponding to any public key listed in the Certificate for purposes of digitally signing any Certificate (or any other format of certified public key) or CRL, as a CA or otherwise. • An obligation and warranty to promptly cease using a Certificate and its associated Private Key, and promptly request that the Certification Authority revokes the Certificate, in the event that: (a) any information in the Certificate is or becomes incorrect or inaccurate, or (b) there is any actual or suspected misuse or compromise of the Subscriber’s Private Key associated with the Public Key listed in the Certificate. • An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key listed in an Certificate upon expiration or revocation of that Certificate.
9.8. Limitations of liability	CPS Section 9.8	(Verified by external audit) Liability limitations are regulated in the contractual agreement between the concerned parties. If applicable such concepts are specified in the Subscriber, Relying Party or other commercial agreements made among the participants. Subject to the foregoing limitations, WISeKey’s aggregate liability limit towards all End users, Relying Parties and any other entities that are not Subordinate PKI Entities for the whole of the validity period of certificates issued by the Root CA (unless revoked or suspended prior to its expiry) towards all persons with regard to such certificates is CHF 5,000,000.00 (Five Million Swiss Francs), with a maximum aggregate per year liability on such certificates of CHF 500,000.00 (Five Hundred and Thousand Swiss Francs).
9.9.1. Indemnification by CAs	CPS Section 9.9	Indemnities are regulated in the contractual agreement between the concerned parties. If applicable such concepts are specified in the Subscriber, Relying Party or other commercial agreements made among the participants. NOTE: For third-party owned CA, WISeKey enforces the signature of a provate agreement which establishes the indemnification aspects
9.16.3. Severability	CPS Section 9.16.3	Should individual provisions of this CPS prove to be ineffective or incomplete, this shall be without prejudice to the effectiveness of all other provisions. The ineffective provision will be replaced by an effective provision deemed as most closely reflecting the sense and purpose of the ineffective provision. In the case of incomplete provisions, amendment will be agreed as deemed to correspond to what would have reasonably been agreed upon in line with the sense and purposes of this CPS, had the matter been considered beforehand.