CertifyID Identity Validation Overview

Version 1.0

Effective Date: 23 July 2007

To issue a CertifyID Subordinate CA license, WISeKey will follow an internal approved procedure to verify an applicant's identity. The submission and validation procedure includes the following steps:

- Submission of subordinate CA applicant data
- Submission of organisation identity documents
- Submission of individual identity documents of proposed CA administrator(s) and organisation's directors, including letters of appointment of CA administrator(s)
- Submission of signed EUA by CA administrator(s)
- Identity Verification and Validation
- Submission of signed contract to WISeKey – stipulating adherence to terms and conditions of usage, obligation to respect WISeKey CPS & CP, and other conditions thereof.
- Submission of pre-issuance audit statement of fulfilment of contract and security requirements
- Submission of certificate request
- Validation of certificate request and license validation - resulting in Denial or Issuance of the CA certificate
- Installation and Post-Audit – including verification of contract compliance, and CRL publishing

To verify and validate the identity of an applicant, WISeKey will collect all documents used for the license approval process, which involves verifying the following:

- That any individual(s) involved in the process are who they purport to be
- That the organization exists and is registered in one or more countries
- That the individual(s) representing the organization has the authority to do so.
- That the nominated CA Administrator requesting a subordinate CA certificate has been given authority to do so by the organization
- That the individual and organization can be located by telephone and by post and has a third party reference that makes its reputable as a trusted entity
- That the domain name(s) for which the organization will be allowed to issue certificates are registered to the organization, or that they have been given permission to use them by the registered owner

WISeKey needs the duly registered statutes or by-laws, together with the registered physical address. In the case of entities that are not registered in the trade registry, other similar documents are also acceptable (e.g. official documents of public entities, notaries, etc.).

Subordinate CA certificates contain naming and domain name constraints, thus commercial registrar records are used to validate Internet Domain Names. The organisation name and address must match the business incorporation papers of the organisation, or the latest data available from the Business Register. A call back must be performed to verify that the individuals with authority in the application work with the organisation, using a telephone number found through public directory services. If its administered by another applicant on behalf of the organisation owning the domain, then a signed letter from the organisation owning the domain must be received granting the certificate applicant the right to use the domain name in their certificates.