

QuoVadis Qualified Certificates Digitary LRA Enrolment Policy – Version 1.0

Overview

This document describes the Enrolment Policy implemented by Digitary as a Local Registration Authority (LRA) for issuing of Qualified Digital Certificates under EU Digital Signature Directive 1999/93/EC through the QuoVadis PKI.

Scope of Operation

The Digitary LRA does **not** currently enrol members of the general public on behalf of the Quo Vadis PKI. The Digitary LRA is currently only open to authorised officials and departments within Higher Education Institutions that have implemented its Digitary secure electronic document solution. The Digitary LRA reserves the right to deny any application for enrolment for a Qualified Certificate.

Legislation, Standards, and Audit

The Digitary LRA enrolls users for Qualified Certificates under 1999/93/EC and in line with the requirements laid down by ETSI TS 101 456. Digitary LRA's procedures are subject to audit by Quo Vadis, which in turn is regularly and independently audited. QuoVadis is an accredited Qualified CSP under ETSI standards. See <http://www.quovadisglobal.com/en-GB/AboutUs/Accreditations.aspx> for more details. Qualified Certificates are issued as Qualified Certificates as defined by EU Digital Signature Directive 1999/93/EC in accordance with the Quo Vadis PKI CPS.

Supported Qualified Certificate Types

The Digitary LRA supports enrolment for the following types of Qualified Certificate:

Type	Description
1	Qualified Certificate where the subject of the certificate is a natural person who is named in the certificate
2	Qualified Certificate where the subject of the certificate is an office or department within an organisation

Type 1 certificates are issued to a natural person who is named in the “common name” attribute of the Subject field of the certificate.

Type 2 certificates are issued to a natural person who acts on behalf of department or office which is named in the “pseudonym” attribute of the Subject field of the certificate.

Delegated signature authority

In certain cases, the Certificate Holder of a Qualified Certificate may be authorised to use the Private Key associated with their Qualified Certificate to sign certain types of official documents on behalf of a party that they represent. In such cases, this is indicated in the “description” attribute of the Qualified Certificate.

Private Key Storage

The Private Keys associated with all Qualified Certificates enrolled through the Digitary LRA are generated by Digitary and stored on a certified Secure Signature Creation Device (SSCD) as defined by the EU Digital Signature Directive 1999/93/EC.

Certificate Holder Enrolment Process

Certificate Holder enrolment is the process of:

1. Vetting the Organisation to be named in the Qualified Certificate
2. Vetting the claimed identity of the Certificate Holder
3. Vetting the claimed role of the Certificate Holder within the Organisation
4. Where, for operational reasons, the Certificate Holder is to use their Qualified Certificate for the purposes of signing documents on behalf of another person, office, or department within the Organisation:
 - a) Vetting the claimed identity of the other person, office or department
 - b) Obtaining confirmation that the Certificate Holder is authorised to use their Qualified Certificate to sign documents on behalf of that other person, office, or department
5. Obtaining the agreement of the Certificate Holder to the terms and conditions of use pertaining to their Qualified Certificate
6. Ensuring that appropriate supporting documentation for 1-5 above is obtained, verified, and securely archived for the long term in the event of any dispute concerning the associated Qualified Certificate

Certificate Holder enrolment must be carried out by an authorised, vetted, and properly trained Enrolment Officer on behalf of the Digitary LRA. Digitary LRA reserves to the right to appoint Enrolment Officers at its discretion.

Organisation vetting

Organisational vetting is carried out in line with the requirements of 1999/93/EC, ETSI TS 101 456, and the Quo Vadis PKI CPS.

Individual vetting

The vetting of individuals is carried out in line with the requirements of 1999/93/EC, ETSI TS 101 456, and the Quo Vadis PKI CPS. Specifically, the enrolment of all Qualified Certificate Holders is subject to face-to-face identity verification involving the checking of passport/national identity documentation in addition to checks regarding the individual's claimed role within the Organisation named in the Qualified Certificate. This checking is performed by an authorised Enrolment Officer on behalf of the Digitary LRA.

Terms and Conditions

Qualified Certificate holders are contractually bound to the terms and conditions of the Digitary /QuoVadis User Subscriber Agreement relating to Qualified Certificates issued through the Quo Vadis EU Qualified Certificate Issuing CA. A copy of these terms and conditions is available from: <http://www.digitary.net/ca.html>