

QuoVadis Email Certificates (Non-Qualified) Digitary LRA Enrolment Policy – Version 1.0

Overview

This document describes the Enrolment Policy implemented by Digitary as a LRA for the issuing of digital certificates for use with digitally signed (S/MIME) emails. These digital certificates are issued through the QuoVadis PKI.

Scope of Operation

The Digitary LRA does **not** currently enrol members of the general public on behalf of the QuoVadis PKI. The Digitary LRA is currently only open to Higher Education Institutions that have implemented its Digitary secure electronic document solution. Digitary LRA reserves the right to approve or deny any application for a digital certificate from any party.

Legislation, Standards, and Audit

The Digitary LRA enrolls users for email certificates in line with the requirements laid down by the QuoVadis CPS. Digitary LRA's procedures are subject to audit by QuoVadis, which in turn is regularly and independently audited. QuoVadis is an accredited CA under relevant standards. See <http://www.quovadisglobal.com/en-GB/AboutUs/Accreditations.aspx> for more details.

Email digital certificates issued under this policy are NOT issued as Qualified Certificates under EU Digital Signature Directive 1999/93/EC.

Supported Email Certificate Types

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

Type	Description
1	Email Certificate where the subject of the certificate is a natural person
2	Email Certificate where the subject of the certificate is an electronic entity controlled by the organisation specified in the subject field of the certificate.

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, directly or indirectly, uses the email address referenced in the certificate, and who is an authorised representative of the organisation referenced in the certificate for this purpose.

Private Key Storage

The Private Keys associated with email certificates issued under this policy are stored in encrypted software format (i.e. PKCS#12 standard). Access to private keys is restricted as follows:

Type	Description
1	Access to the Private Key is restricted to the person named in the certificate
2	Access to the Private Key is restricted to systems controlled by the organisation named in the subject field of the certificate

Certificate Enrolment Process

Certificate enrolment is the process of:

1. Vetting the Organisation to be named in the Email Certificate
2. Vetting one of the following in accordance with the requirements of the Digitary/QuoVadis User Subscriber Agreement and the QuoVadis PKI CP/CPS:
 - a) The individual named in the certificate (for Type 1 certificates)
 - b) An authorised representative of the Organisation (for Type 2 certificates)
3. Obtaining the agreement of the person in (2) to the terms and conditions of use pertaining to the Email Certificate
4. Ensuring that appropriate supporting documentation for 1-3 above is obtained, verified, and securely archived for the long term in the event of any dispute concerning the associated Email Certificate

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 and Individual vetting

Organisational and individual vetting is carried out in line with the requirements of the Digitary/QuoVadis User Subscriber Agreement and and the Quo Vadis PKI CP/CPS.

Terms and Conditions

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