

SCHEDULE 1

TERENA RA VERIFICATION PROCEDURE FOR SERVERSIGN EDU

1. Introduction

The procedure to submit and validate a ServerSign EDU (also referred to as SureServer EDU) request consists of two parts:

- an initial, one-time pre-validation procedure
- a per-certificate validation procedure
 - for pre-validated domain names
 - for other domain names

The purpose of the two procedures combined is to:

- Assure the organization on behalf of which an Applicant requests a ServerSign EDU certificate exists and at the same time that the organization operates within the educational or research environment that resides under the NREN umbrella;
- Assure an applicant for a ServerSign EDU certificate is authorized to act on behalf of his organization;
- Assure for each certificate the Applicant agrees with the subscriber agreement;
- Assure for each certificate the requesting organization is authorized to request a ServerSign EDU certificate for the requested domain name(s);
- Assure for each certificate the Applicant's identity.

The procedures operate within these limitations:

- The Registration Authority will only accept ServerSign EDU certificate requests from organizations that have been pre-validated;
- All (pre-validation) registries and verification documents and proof of validation (paper or electronic) [must be open to inspection and/or verification by GlobalSign for the term of retention of records as specified under 3.3 - Archiving](#).
- Following pre-approval from GlobalSign, individual RAs MAY extend on the procedures defined in this document and define additional procedures to which their Applicants need to adhere.

2. Roles and terminology

Applying Organization: The organization on behalf of whom a ServerSign EDU certificate is requested.

Applicant: A person officially appointed by the Applying Organization representing the Applying Organization and authorized by that organization to bind that organization to the GlobalSign subscriber agreement and perform all required actions to validate ServerSign EDU requests to the Registration Authority.

Validation: This term is used to indicate a verification step in the procedure.

3. Pre-validation procedure

The pre-validation procedure uses one of these two options:

3.1. Applicant and Organization Validation

Assuring Applicant authority and Applying Organization existence, option 1:

The Applying Organization submits a proxy, in paper and signed by a legal representative of the Applying Organization, to the Registration Authority in which the representatives who can apply for certificates on behalf of the Applying Organization are appointed. The agreement will have sufficient safeguards to assure proper maintenance of the representatives.

With the agreement the Applying Organization submits its Articles of Association/Incorporation or any other official document proving the legal existence of the Applying Organization.

Assuring Applicant authority and Applying Organization existence, option 2:

The Registration Authority uses an existing registration of representatives that is actively maintained and backed by formal agreements with the Applying Organizations. These formal agreements MUST include the Articles of Association/Incorporation or any other official document proving the legal existence of the Applying Organization.

A list of registries accepted by GlobalSign will be maintained by TERENA

3.2. Domain Ownership Validation

Pre-validated domain names

The representatives of the Applying Organization can submit domain names to the Registration Authority to be pre-validated. Upon receipt of such a request the Registration Authority will verify the ownership of each of the domain names, the appropriate official domain name registry for that particular domain name and maintain proper records of this verification. Pre-validated domain names must be re-validated when indications of change of ownership have been received. To make sure ownership has not changed since pre-validation, the RA administrator must always perform a brief check of domain name ownership in the pre-validation registry before issuance of the server certificate.

Non pre-validated domain names

For domain names that have not been pre-validated the domain name ownership will be checked through querying the appropriate official registry:

- gTLD domain names can be verified using registries listed at <http://www.icann.org/registries/listing.html>
- ccTLD domain names can be verified using registries listed at <http://www.iana.org/cctld/cctld-whois.htm>

Registries not listed above need to be approved by GlobalSign. TERENA will maintain this list and hand it to the NREN-RAs upon change.

3.3. Request Validation

Per certificate validation procedure

Each ServerSign EDU certificate request results in an email challenge sent to the Applicant, containing details of both the certificate request (such as the DN) and the Applicant.

The Applicant must sign and return this email challenge to the Registration Authority. The available methods are:

- by signed postal mail;
- a signed fax;
- an email with a scan of the signed form;
- a signed email.

Upon receipt of the signed email challenge, the Registration Authority verifies:

- The Applying Organization is present in the appropriate pre-validation registry of that Registration Authority;
- The Applicant is (one of) the representative(s) according to the pre-validation registry of that Registration Authority (name and email-matching);
- The signature of the Applicant on the email challenge matches the name of the registered representative for the Applying Organization;
- The certificate request in the registration form is equal to the request online (cross-check);
- For signed email: verify the correctness of a digital signature (name, organization and certificate validity);
- The ownership of each of the domain names in the request via either the appropriate official domain name registry for that particular domain name or an internal registry of pre-validated domain names.

GlobalSign must at any time and for each certificate request be able to check whether or not the verification steps described above have been performed (i.e. ask for paper proof or electronic proof).

The Applicant accepts the subscriber agreement upon using the issued certificate.

Signed email

Email signatures can be set using x.509 client certificates or PGP keys. The x.509 certificates or PGP keys used need to have an assurance level comparable with that of the **GlobalSign PersonalSign 2 Pro** certificates. The procedures for maintaining an adequate assurance level on these client certificates or PGP keys will be submitted to GlobalSign for approval. TERENA will maintain a list of accepted procedures.

1. The way the assurance level is maintained (the client certificates are issued or the PGP keys are signed) **MUST** be documented in a CPS;
2. GlobalSign must at any time be able to check whether or not the procedures as described in the CPS are indeed respected (i.e. ask paper proof);
3. the NREN has an obligation to inform GlobalSign of any significant

changes of the CPS and/or procedures.

An example of an accepted CPS is <<http://igc.cru.fr/references/pc.pdf>>

Archiving

All relevant verification documents must be treated as 'confidential data'. Access to this sensitive information is restricted to the accredited NREN RA administrators.

The folder (digital or paper) must be clearly labeled 'confidential' and must contain specifications of the data within.

The documents must be stored in a secure manner (Access Control Lists for file access or in a personal file cabinet) only accessible to the accredited NREN RA administrators.

Electronic documents must be stored in a format which can be expected to withstand 6 (six) years of archiving (.txt or .pdf). Availability must be ensured to enable possible adhoc checks by GlobalSign. Paper documents must be archived for 6 (six) years.

After the archival period the documents must be destroyed in a way appropriate for confidential information.