

# **Call for Proposals TERENA SCS**

**23 September 2008**

## 1 Introduction

### 1.1 Contracting authority

TERENA (the Trans-European Research and Education Networking Association) is a European organisation whose principal members are the National Research and Education Networking organisations (NRENs) from countries in and around Europe. For more information see [www.terena.org/](http://www.terena.org/).

In the remainder of this document, the term 'NREN' is used to indicate a TERENA national member organisation and/or another national organisation representing the education and research community in its country.

TERENA is the contracting authority for this procurement. For this procurement, TERENA acts on behalf of a number of NRENs. The NRENs participating in this joint procurement are:

ACOnet	Austria
ARNES	Slovenia
BELNET	Belgium
CARNet	Croatia
CESNET	Czech Republic
FCCN	Portugal
GARR	Italy
HEAnet	Ireland
HUNGARNET	Hungary
JANET(UK)	United Kingdom
LITNET	Lithuania
PSCN	Poland
RedIRIS	Spain
RENATER / CRU	France
SUNET	Sweden
SURFnet	Netherlands
SWITCH	Switzerland
UNI•C	Denmark
UNINETT	Norway

### 1.2 Purpose of the Call for Proposals

The purpose of this Call for Proposals is to procure a managed Secure Sockets Layer (SSL) server certificate service that will provide the European education and research community with SSL server certificates that are recognised by popular web browsers, mobile devices and other user applications.

### 1.3 The TERENA Server Certificate Service

European NRENs had been involved for many years in running Public Key Infrastructures (PKIs) when in 2005 a number of NRENs joined forces and set out to create the right circumstances that would allow for a massive rollout of SSL server certificates in their constituencies. They found two problems that hindered such a massive rollout of SSL server certificates in the European education and research community:

- the per-certificate pricing of commercially available certificates;
- lacking browser recognition of server certificates issued by NRENs' PKIs.

The group of NRENs asked TERENA to explore the possibility of a joint procurement of a managed SSL server certificate service to provide browser-recognised server certificates to education and research organisations served by these NRENs. After a tender procedure, TERENA awarded the contract for a managed SSL server certificate service at the beginning of 2006, with the service becoming operational starting in March 2006.

After the service proved to fulfil its potential during the first year of operations, the contract was extended for a three-year period starting January 2007. The current service uses the existing contractual relationships between NRENs and the organisations in their constituencies, resulting in a highly optimised, scalable and efficient certificate request vetting process that is tailored to the requirements of the participating NRENs.

As a result of the TERENA Server Certificate Service (SCS), the barriers for large-scale use of SSL server certificates in the European education and research community have effectively been removed.

Therefore, on behalf of the 19 NRENs that will be participating in the TERENA SCS by the end of 2008, TERENA now seeks to prolong the service.

The desired future service will allow NRENs, in their role as service providers for their constituencies, to continue providing their communities with a functionally unlimited number of browser-recognised SSL server certificates.

This Call for Proposals is targeted at acquiring a managed SSL server certificate service to allow for the continuation of the TERENA SCS<sup>1</sup>.

---

<sup>1</sup> Note that TERENA is looking to establish a new contract early in 2009, with the associated service starting shortly afterwards. That service is therefore expected to run in parallel with the service under the current contract for a period of approximately ten months, allowing for a smooth transition.

## 2 Services to be contracted

Bidders are invited to submit an offer for a managed SSL server certificate service that will allow the NRENs acting as service providers to their constituencies to provide the European education and research community with a functionally unlimited number of *SSL server certificates that are recognised by popular web browsers, mobile devices and other user applications* (hereafter in this document, these will be referred to as 'SSL server certificates').

### 2.1 Background and expectations

Bidders are asked to take the following background and expectations into consideration when formulating their proposal:

- TERENA is open to novel approaches to solve the challenge of providing large numbers of SSL server certificates to the European education and research community. However, solutions presented must be available at the time that they are offered. TERENA is not willing to embark on a potentially long development project.
- Due to its position in the education and research community in its country and the existing (contractual) relationships that each NREN has with the organisations that it serves, each NREN is well suited to play a role in efficiently organising the Registration Authority (RA) process for that community. Note that this does not imply that the NREN must be involved in the vetting process of each individual certificate request.
- In the current service, each NREN-RA applies a workflow that is optimised to the particular circumstances in its constituency, while adhering strictly to the Certification Authority (CA) policies. This has led to a highly optimised, scalable and efficient certificate vetting process executed by the NREN-RAs, which uses the existing contractual relationships that NRENs have with the organisations that they serve. The NRENs expect a future service to give their users a similar experience of an optimal certificate request vetting process.
- The NRENs expect to be able to offer their users a completely digital certificate request vetting process.
- A proposal that assumes that a financial transaction (payment) will take place for each individual certificate request is not considered to be a viable option.

### 3 The tender procedure

#### 3.1 Type of procedure

The service requested under this Call for Proposals is to be classified as an 'electronic signature certification service'<sup>2</sup> and is listed in Annex 2B of the European Directive<sup>3</sup>. The Directive prescribes only very limited regulations for tendering such so-called Annex 2B services, i.e. common rules in the technical field and certain publication rules.

Because TERENA is committed to business transparency, it has decided to:

- send this Call for Proposals to all established CA providers that are currently known to TERENA;
- publish the Call for Proposals on the TERENA website; and
- apply the procedure as described below.

TERENA thus creates a level playing field in tendering the requested service. TERENA emphasises that the procedure does not classify as one of the award procedures laid down in the Directive and that such was expressly not the intention of TERENA.

If the procedure leads to successful granting of the contract, TERENA will submit the outcome to the Publication Office of the European Commission for publication in the Official Journal of the European Union ('S series'). The name of the successful bidder and the value of the contract will be made public, unless the company winning the contract explicitly expresses to TERENA legitimate commercial interests to remain anonymous.

#### 3.2 General terms and conditions regarding the Call for Proposals

Proposals from bidders must explicitly indicate the extent to which the proposal meets the mandatory and optional requirements listed in section 5. TERENA reserves the right to exclude a bidder whose proposal does not meet the mandatory requirements. The final agreement will be based on the content of this Call for Proposals (CfP), only taking into account reservations that the bidder may list in a dedicated chapter in his proposal, provided that both parties agree on these reservations.

In case of any discrepancy between the text of this CfP and information in other documents, the text of this CfP takes precedence, unless explicitly stated otherwise.

The technical expressions and abbreviations used in this document are considered to be known to the bidder. Special expressions and abbreviations are explained in Annex D.

TERENA does not assume any liability, regardless of the grounds, for costs or damages incurred by the bidder in relation to this procurement procedure, including but not limited to the costs of the preparation of the proposal.

TERENA will award the economically most advantageous proposal. TERENA reserves the right not to accept any offer, without providing explanation. TERENA reserves the right to accept more than one offer. In case TERENA awards more than one proposal, the accepted offers will be the economically most advantageous ones.

#### 3.3 Time schedule

All proposals must be received on paper at the address mentioned below no later than the **deadline for submission of proposals of 10 November 2008 at 12:00 hrs Central European Time**.

In addition, the bidder must submit an electronic version of his proposal; see below for details. The electronic version must also be received no later than the deadline mentioned above. In case of any differences between the paper version and the electronic version, the paper version will prevail.

The prospective overall time schedule is as follows (all times are Central European (Summer) Time):

---

<sup>2</sup> Please see numerical code 74113210-9 of the Common Procurement Vocabulary.

<sup>3</sup> European Council Directive 2004/18/EC of 31 March 2004.

Deadline for questions	20 October 2008, 12:00 hrs
Last date for answers and corrections	27 October 2008, 14:00 hrs
<b>Deadline for submission of proposals</b>	<b>10 November 2008, 12:00 hrs</b>
End of selection and awarding process	End December 2008
Two-week period for objections	First half of January 2009
Estimated contract date	Mid January 2009
Start of service	1 March 2009

Bidders may be invited to a meeting with TERENA representatives to discuss their proposal. These meetings, if any, are expected to take place in the second half of November 2008.

### **3.4 Address data – contact information**

The proposal must be sent by mail, messenger or hand delivered to:

TERENA Secretariat  
attn. Dr. Karel Vietsch  
Singel 468D  
1017 AW Amsterdam  
The Netherlands

During the whole procedure, Ms. Licia Florio will be the liaison person on behalf of TERENA. Her contact details are:

Ms. Licia Florio  
TERENA Secretariat  
Singel 468D  
1017 AW Amsterdam  
The Netherlands  
E-mail: [florio@terena.org](mailto:florio@terena.org)  
Phone: +31 20 530 44 88  
Fax: +31 20 530 44 99

### **3.5 Additional information, Questions and Answers**

Any questions and remarks concerning the Call for Proposals must be sent to the liaison person mentioned above, through e-mail. Questions must be asked before **20 October 2008 at 12:00 hrs Central European Summer Time**. TERENA reserves the right not to answer questions received after this deadline.

Answers that are considered to be corrections or extensions to the Call for Proposals will be anonymised and will be published on the TERENA website and sent to all Parties to which TERENA has sent this Call for Proposals. Both answers and questions will be issued no later than **27 October 2008 at 14:00 hrs Central European Time**.

### **3.6 Corrections, additions or changes to the Call for Proposals**

TERENA reserves the right to make non-substantial corrections, additions or changes to the tender documents until the last date for answers and corrections: **27 October 2008 at 14:00 hrs Central European Time**.

These corrections, additions or changes will be published on the TERENA website and sent to all Parties to which TERENA has sent this Call for Proposals.

### **3.7 Opening of Tenders**

Immediately after the **deadline for submission of proposals of 10 November 2008 at 12:00 hrs Central European Time**, TERENA will inspect all proposals that have been submitted, and will generate a list containing all bidders for this CfP. This inspection will take place at the TERENA offices in Amsterdam, the Netherlands. This is a closed procedure.

Each proposal will be treated confidentially.

Each item of the proposals sent to TERENA is considered to become the property of TERENA unless

otherwise specified and agreed by the bidder and TERENA.

### **3.8 Period for objections**

After having selected a preferred supplier, TERENA will notify all other bidders that have submitted a proposal of TERENA's intention to formally reject their offers. If bidders have objections with respect to that decision, these bidders should submit their objections to TERENA substantiated and in writing and commence interlocutory proceedings by submitting a writ of summons, all within 15 days of the date on which the notification was sent. After expiration of the 15 days without any objections being raised, TERENA will enter into a contract with the preferred supplier.

### **3.9 About the proposal**

The proposal must be written in the English language.

The proposal must be valid for a period of at least six (6) months, after the submission deadline of 10 November 2008.

The proposal must consist of four (4) identical paper copies, and must be delivered to TERENA in a closed envelope or box. At the same time, the bidder must submit an electronic version of the proposal in PDF, HTML or Microsoft Word format to TERENA. This can be done, for example, by submitting the proposal on CD-ROM (together with the paper version) or through email to the TERENA liaison person.

### **3.10 Terms of Agreement**

The contractual agreements governing the service are expected to include provisions to the following effect:

1. The contract period for the service shall be at least two years, with the possibility of renewal.
2. That possible renewal will be for yearly periods, with a maximum of three years.
3. The Call for Proposals, the Questions & Answer document(s) and any additional correspondence shall form part of the final agreements.
4. The law of the Netherlands shall apply to these agreements. Any dispute arising between the parties over the application or interpretation of the agreements shall be settled between the parties. Should the parties fail to settle the dispute, then it shall be resolved by the competent Court in Amsterdam, the Netherlands.
5. The agreements shall include liability clauses that as a minimum entitle TERENA to reimbursement of any fees that it has paid up-front, in case the contract is terminated early due to circumstances regarding the provision of the service.
6. If the provider fails to deliver the service according to the contracted schedule, TERENA shall be entitled to claim compensation equal to the contracted price of the missing service, on a daily basis, without prejudice to its rights for compensation for other losses and damages.
7. If the provider fails to deliver the service within two months after the contracted date, TERENA shall be entitled to terminate the contract with immediate effect, without penalty or other claims from the provider, and without prejudice to its rights for compensation for other losses and damages.

The terms listed above as numbers 1 and 7 are mandatory.

## 4 Selection and awarding procedure

### 4.1 Selection procedure

All bidders that meet the selection criteria<sup>4</sup> qualify for the awarding procedure. TERENA reserves the right to exclude a bidder that does not meet the selection criteria.

The selection criteria are:

- The proposal from the bidder contains a letter duly signed by an authorised representative of the bidder stating that:
  - the bidder is not bankrupt or being wound up, is not having its affairs administrated by the courts, has not entered into an arrangement with creditors, has not suspended its business activities, is not the subject of proceedings concerning these matters, and is not in any analogous situation arising from a procedure provided for in national legislation or regulations;
  - the bidder has not been convicted of an offense concerning its professional conduct;
  - the bidder has not been guilty of grave professional misconduct proven by any means that the bidder cannot justify;
  - the bidder has fulfilled its obligations relating to the payment of social security contributions and the payment of taxes in accordance with the legal provisions of the country where the bidder is legally established or where the service is to be provided;
  - the bidder has not been the subject of a judgement for fraud, corruption, involvement in a criminal organisation or any other illegal activity detrimental to TERENA's financial interests.
- The proposal from the bidder contains a copy of the bidder's registration in the professional or trade registers.
- The proposal from the bidder contains a description of the bidder's technical capacity.
- The proposal from the bidder contains a description of the financial status of the bidder, including the bidder's annual financial reports for 2006 and 2007.

The selection procedure will be carried out a by a committee consisting of TERENA staff members and selected representatives of the participating NRENs.

### 4.2 Awarding procedure

TERENA is looking for a solution that provides SSL server certificates that are recognised by a wide range of applications and platforms, that has a very efficient way of issuing certificates at low cost per certificate and that brings attractive Total Cost of Ownership to the participating NRENs.

TERENA will award the most economically advantageous proposal(s).

The key awarding criteria will be:

1. costs of the proposed service *<very important>*;
2. favourableness of the contractual terms *<important>*; and
3. quality of the proposed service *<very important>*.

The key criteria are listed in no particular order, and the list is not exhaustive.

For the information of the bidders, the sub-criteria into which these awarding criteria can be broken down are listed below. The sub-criteria are listed in no particular order, and the list of sub-criteria is not exhaustive.

1. Costs for the proposed service:
  - annual service fee *<very important>*; and
  - certificate lifecycle management cost per certificate, both for the NREN and for the certificate holder *<very important>*.
3. Quality of the proposed service:
  - technical quality of the proposed solution (see the mandatory and optional requirements in section 5) *<very important>*;
  - coverage of recognition of the SSL server certificates by applications and platforms *<very important>*;

---

<sup>4</sup> Note that the selection criteria only take into account the qualifications of the bidder, not its proposal.

- o vendor competence <important>; and
- o quality of support < important>.

A clarification round may be part of the procedure. TERENA reserves the right to exclude a bidder at any time, if the bidder proves unwilling or unable to provide the requested information or clarifications.

TERENA reserves the right, at any stage during this procurement procedure, to subject any information that has been provided by the bidders initially or at a later stage, to investigation concerning the correctness of the information. If this verification procedure demonstrates, in the opinion of TERENA, that any of the information provided by a bidder, regardless of the nature of the information, is incorrect, then TERENA reserves the right to exclude such a bidder from the procurement procedure.

The awarding procedure will be carried out a by a committee consisting of TERENA staff members and selected representatives of the participating NRENS.

## 5 Technical requirements

### Mandatory requirements:

#### M1. Popular browser support

The service must provide SSL server certificates that are recognised by current versions (i.e., versions considered to be current at the time that the offer is submitted) of the Microsoft Internet Explorer and Mozilla (Firefox) families of web browsers.

#### M2. Support by other platforms/applications

The offer must specify any other platforms/applications that recognise the SSL server certificates issued by the service.

#### M3. Validity of issued SSL server certificates upon contract end

SSL server certificates issued under the service that are valid (as is defined in paragraph 4.1.2.5 *Validity* of RFC5280, specifically "The validity period for a certificate is the period of time from notBefore through notAfter, inclusive.") when the contract ends must remain valid, and revocable by the RAs, until the end of their validity period.

#### M4. Ensuring future recognition by browsers and other applications/platforms

The offer must specify how the recognition by the web browsers referred to in M1, and by any other applications/platforms as indicated in M2, of SSL server certificates issued by the service will be maintained and ensured throughout their validity period.

#### M5. End-user interfaces

Interfaces must be provided for end users that allow:

- a. requesting and obtaining certificates;
- b. revoking certificates.

#### M6. Interface response times

The offer must specify the typical average response times and maximum response times of the end-user interfaces as specified in mandatory requirement M5 and of any administrative interfaces operated by NREN staff members. The bidder is asked to take into consideration that NRENs typically use very high speed, congestion-free networks.

#### M7. Certificate request processing

The service must support an efficient and effective process to handle certificate requests that minimises the per-certificate request handling cost and per-certificate request handling effort, both for the entities involved in processing the request and for the certificate holder. The process can use the existing relationships between NRENs and the organisations served by them. The process must meet the following conditions:

- a. fully electronic certificate request processing must be supported;
- b. certificate request processing must not require face-to-face meetings.

Note that additionally a conventional way of processing certificate requests (i.e. fax) may also be supported.

The offer must specify the process by which certificate requests will be processed, including (but not limited to) the entities involved and any means of authentication needed by those entities.

#### M8. Certificate profiles

The offer must specify which certificate profiles (used for issuing the SSL server certificates) are supported by the service. Sufficient detail must be included to allow an evaluation of the (settings of) individual fields (such as Extended Key Usage, Key Usage, Basic Constraints, etc.). Examples of certificates may be included.

#### M9. subjectAltName

The service must support the use of the *subject alternative name* extension. At a minimum, the *dNSName* subjectAltName must be supported. The service must support multiple instances of each supported alternative name (i.e. two *dNSName* entries and two *rfc822Name* entries). The interfaces mentioned in mandatory requirement M5 must fully support the use of the subject alternative name extension. The offer must describe which subject alternative names are supported.

**M10. Multiple valid certificates**

The service must support having multiple valid certificates with the same subject.

**M11. Internationalisation**

The service must support the use of internationalised names in general, and specifically the use of UTF8STRING and PRINTABLESTRING in the subject name components.

**M12. Support**

The service must provide helpdesk services to the NREN staff members involved and per-NREN reporting services. The offer must specify:

- a. the support function and the maximum response time for helpdesk queries;
- b. the fault reporting point, its maximum response times and opening hours;
- c. the maximum delivery times of different steps in the workflow;
- d. the frequency and content of per-NREN statistical reports and how these will be delivered;
- e. the method and timescales for notification of service changes, and planned and unplanned outages.
- f. the escalation contact point and escalation process.

**M13. Auditing**

The offer must specify details of any current audit arrangements mandated by the proposed service. These details must include the process by which NRENs are notified of such audits.

**M14. Training**

If the proposed solution requires training, then the service must provide a training process for the NREN staff members involved. This process should use a "train the trainer" approach, allowing selected NREN staff members to provide the training.

**M15. Certificate lifetime**

The service must support a certificate lifetime of at least 2 years.

**Optional requirements:**

The proposal should specify which of the following requirements can be met, and at what extra cost (if any):

**O1. Alternative certificate lifetimes**

The service should support alternative certificate lifetimes of 1 year and of 3 years or more.

**O2. End-user interface for certificate renewal**

The service should provide an end-user interface for renewing certificates.

**O3. Branding**

The service should permit separate branding by each NREN for the interfaces mentioned in mandatory requirement M5 and optional requirement O2.

**O4. Additional certificate profiles**

The service should support the implementation of additional certificate profiles.

**O5. e-Science Grid server certificate support**

The service should support the following requirements that allow the use of the SSL server certificates in e-Science Grid environments:

- a. ability to specify the values of certain Distinguished Names within the subject field for a certificate profile that is specific to e-Science Grids;
- b. ability to specify a certificate lifetime of at most 13 months for a certificate profile that is specific to e-Science Grids.

**O6. API**

The service should be provided with an API that allows NRENs to develop and provide their own customised end-user interfaces for the functionality as defined in mandatory requirement M5 and optional requirement O2.

**O7. Wildcard certificates**

The service should allow wildcard certificates to be issued.

**O8. OCSP support**

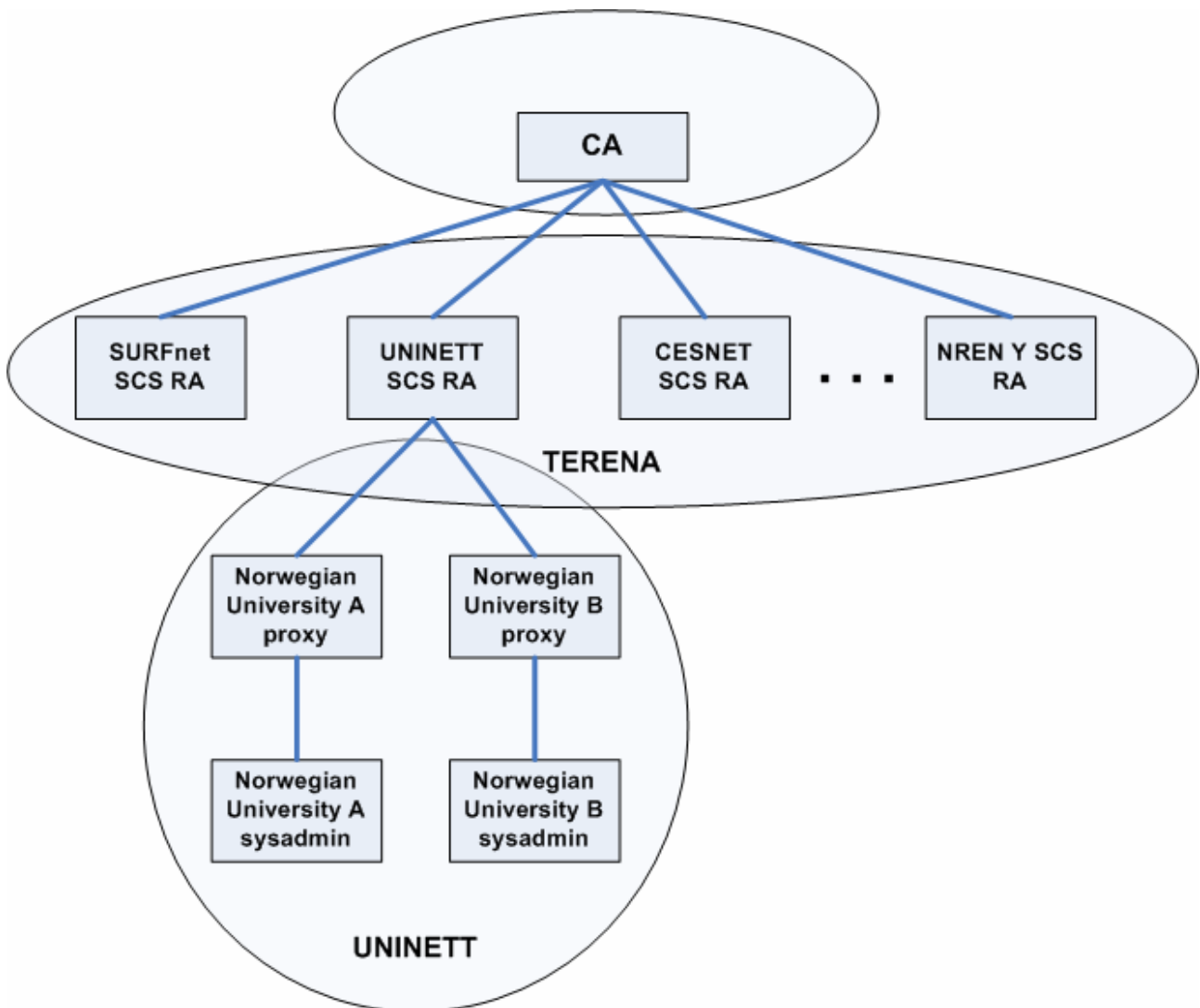
The service should support the use of Online Certificate Status Protocol (OCSP). Various implementations can be considered, including options that use the NREN infrastructure for the OCSP responders.

**O9. Extensive reporting**

The service should support extensive per-NREN reporting (a list of certificates issued, denied, etc.) in an easily exchangeable format, e.g. XML.

## Annex A. Current entities and roles

*This annex describes the entities currently involved in the TERENA SCS and the roles that they fulfil. This annex is included to illustrate how a possible solution can function, not to mandate how a possible solution must function.*



**Figure 1: TERENA SCS - Organisational entities and roles**

### TERENA:

- is the legal entity contracting the service with the Supplier;
- coordinates the service;
- acts as administrative single point of contact for the Supplier on behalf of the NRENs;
- carries out certain operational tasks that it is well suited for due to its place in the NREN world;
- does not perform any operational tasks directly related to certificate requests or certificate revocation requests;
- interacts with the Supplier of the CA and with the NREN-RAs.

### CA:

- is an automated certificate factory;
- issues certificates on instruction of the RAs;
- revokes certificates on instruction of the RAs or certificate holders;
- involves no per-certificate human handling;
- interacts with the NREN-RAs.

**NREN-RA:**

- performs the validation of organisational proxies for its constituency;
- performs the validation of every certificate request for its constituency;
- performs certificate revocation on behalf of the subscriber upon a request by the proxy;
- maintains the archive for the validation processes that it performs;
- is usually run as a centralised unit by the NREN but in some cases is set up in a more distributed way using subRAs;
- has direct access to the CA backend to authorise issuing certificates or revoking certificates;
- is responsible for ensuring adherence to policies and procedures for every certificate issued and revoked;
- interacts with TERENA and with the organisational proxies;
- delivers technical support to the certificate holders;
- facilitates auditors.

**Organisational proxy:**

- is officially appointed by a organisation served by an NREN (university, university college, research institution, etc.);
- acts on behalf of that organisation in the process of requesting a certificate or revoking a certificate within the context of the TERENA SCS;
- is a role usually fulfilled by at least two persons, depending on the size of the organisation and the number of certificates that it typically requests;
- interacts with the NREN-RA and with the certificate holder.

**Certificate holder**

- is the person responsible for the certificate;
- is typically a member of technical staff within an organisation: system administrator etc.;
- interacts with the organisational proxy from a procedural point of view and with the NREN-RA for technical support.

## Annex B. Current TERENA SCS RA procedure

*This annex describes the current procedure used by TERENA SCS RAs to verify certificate requests and certificate revocation requests. It is included to illustrate how a possible solution can function, not to mandate how a possible solution must function.*

### 1. Introduction

The procedure to submit and validate a TERENA SCS 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 that the organisation on behalf of which an Applicant requests a TERENA SCS certificate exists and at the same time that the organisation operates within the education or research environment that resides under the NREN umbrella;
- assure that an Applicant for a TERENA SCS certificate is authorised to act on behalf of his organisation;
- assure for each certificate that the Applicant agrees with the subscriber agreement;
- assure for each certificate that the requesting organisation is authorised to request a TERENA SCS certificate for the requested domain name(s);
- assure for each certificate the Applicant's identity;
- assure for each certificate that the RA acts according to the CPS (Certification/Certificate Practice Statement) of the service.

The procedures operate within the following limitations:

- the Registration Authority will only accept TERENA SCS certificate requests from organisations 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 the Supplier for the term of retention of records as specified below (under 3.3 – Archiving);
- following pre-approval from the Supplier, 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 Organisation:** the organisation on behalf of which a TERENA SCS certificate is requested.

**Applicant:** a person officially appointed by the Applying Organisation representing the Applying Organisation and authorised by that organisation to bind that organisation to the Supplier subscriber agreement and to perform all required actions to validate TERENA SCS 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 organisation validation

Assuring Applicant authority and Applying Organisation existence, option 1:

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

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

## Assuring Applicant authority and Applying Organisation existence, option 2:

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

A list of registries accepted by the Supplier will be maintained by TERENA.

### **3.2. Domain ownership validation**

#### **Pre-validated domain names**

The representatives of the Applying Organisation 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 [www.icann.org/registries/listing.html](http://www.icann.org/registries/listing.html);
- ccTLD domain names can be verified using registries listed at [www.iana.org/cctld/cctld-whois.htm](http://www.iana.org/cctld/cctld-whois.htm).

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

### **3.3. Request validation**

#### **Per-certificate validation procedure**

Each TERENA SCS 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;
- by signed fax;
- by email with a scan of the signed form;
- by digitally signed email.

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

- that the Applying Organisation is present in the appropriate pre-validation registry of that Registration Authority;
- that the Applicant is (one of) the representative(s) according to the pre-validation registry of that Registration Authority (name and email-matching);
- that the signature of the Applicant on the email challenge matches the name of the registered representative for the Applying Organisation;
- that the certificate request in the registration form is equal to the request online (cross-check);
- for signed email: that the digital signature is correct (name, organisation, message content 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.

At any time and for each certificate request, the Supplier must 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**

Digital signatures for email may be created using X.509 client certificates or PGP keys. To ensure an adequate assurance level for the X.509 certificates or PGP keys used, the identity of the certificate holder needs to be verified (although not necessarily in a face-to-face meeting), as well as the relationship between the certificate holder and his employer. The procedures for maintaining an adequate assurance level on these client certificates or PGP keys will be submitted to the Supplier for approval. TERENA will maintain a list of accepted procedures.

1. The way in which the assurance level is maintained (the client certificates are issued, or the PGP keys are signed) MUST be documented in a CPS.
2. The Supplier 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 the Supplier of any significant changes of the CPS and/or procedures.

An example of an accepted CPS can be found at [www.cesnet.cz/pki/CPS/2.0/CPS.pdf](http://www.cesnet.cz/pki/CPS/2.0/CPS.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) and be only accessible to the accredited NREN RA administrators.

Electronic documents must be stored in a format that can be expected to withstand six years of archiving (.txt or .pdf). Availability must be ensured to enable possible ad-hoc checks by the Supplier. Paper documents must be archived for six years.

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

## **Annex C: Facts and figures TERENA SCS**

The numbers are per 1 August 2008. At that time, 18 NRENS were participating in the TERENA SCS, of which 3 had only recently joined.

<b>Number of participating NRENS:</b>	<b>18</b>
<b>Aggregate number of certificates issued:</b>	<b>19,400</b>
<b>Aggregate number of participating organisations:</b>	<b>2,225</b>
<b>Aggregate number of proxies:</b>	<b>3,800</b>

## Annex D: Glossary of Terms

### CA

Certification Authority

### e-Science Grid

Computational and storage Grid environment used by researchers. The EGEE web site contains relevant information for the European e-Science Grid ([www.eu-egee.org/](http://www.eu-egee.org/)). The EUGridPMA website contains relevant information on the X.509 certificates used in this environment ([www.eugridpma.org/](http://www.eugridpma.org/)).

### OCSP

Online Certificate Status Protocol

### PKIX

The Public Key Infrastructure working group of the IETF (Internet Engineering Task Force) and the standards it produces

### RA

Registration Authority

### RFC5280

Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC 5280) as defined by the PKIX working group of the IETF

### SSL Server Certificates

X.509v3 certificates that function in a typical PKIX environment

### subjectAltName

As defined in paragraph 4.2.1.6. "Subject Alternative Name" of RFC5280 "the PKIX Certificate and CRL Profile"

*Excerpt: "The subject alternative name extension allows identities to be bound to the subject of the certificate. These identities may be included in addition to or in place of the identity in the subject field of the certificate."*

## **Annex E: Statements of compliance with requirements**

This Annex summarises the requirements of this Call for Proposals in a table. Every bidder is required to state compliance to each of the requirements in the table, which must be included with the offer. Partial compliance should be annotated and explained in detailed documentation, which must be included with the offer.

R: Requirement  
M: Mandatory technical requirement  
O: Optional technical requirement  
FC: Full Compliance  
PC: Partial Compliance  
NC: Non-Compliance

	Description	FC/PC/NC	Remarks
R1	Name and contact details of the contact person for this offer		
	<b>Selection criteria (see section 4.1):</b>		
R2	Letter from authorised representative		
R3	Copy of registration in trade registers		
R4	Description of technical capability		
R5	Annual financial reports		
	<b>Technical requirements (see section 5):</b>		
M1	Popular browser support		
M2	Support by other platforms/applications		
M3	Validity of issued SSL Server Certificates upon contract end		
M4	Ensuring future recognition by browsers and other applications/platforms		
M5	End-user interfaces		
M6	Interface response times		
M7	Certificate request processing		
M8	Certificate profiles		
M9	subjectAltName		
M10	Multiple valid certificates		
M11	Internationalisation		
M12	Support		
M13	Auditing		
M14	Training		
M15	Certificate lifetime		
O1	Alternative certificate lifetimes		
O2	End-user interface for certificate renewal		
O3	Branding		
O4	Additional certificate profiles		
O5	e-Science Grid server certificate support		
O6	API		
O7	Wildcard certificates		
O8	OSCP support		
O9	Extensive reporting		