Amsterdam, 4 August 2005
Ref.: TSec(05)074
Subject: Call for Proposals

Dear Sir/Madam,

This letter is to inform you that TERENA, on behalf of a number of National Research and Education Network organisations (and similar national organisations), is intent to acquire an X.509 PKI service, according to a procedure as well as a set of requirements laid out in the attached Call for Proposals.

In this respect, TERENA would like to invite your Party to put forward a proposal to set up and provide such a service.

Yours sincerely,

Karel Vietsch
TERENA Secretary General

CALL FOR PROPOSALS

Introduction

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.nl/.)

NRENs are currently witnessing an increase in the need for SSL server certificates in their own organisation and within their user communities. This increase is due to both an increased awareness for the need of encrypted channels (webmail etc.) and the rollout of authentication and authorisation middleware. Organisations typically want to keep using username/passwords for some years to come but do not want those passwords to be exposed to sniffing. Furthermore, as more and more servers need to be able to communicate to one another in a secure, authenticated way there is a move away from shared secrets and towards a scalable X.509 certificate infrastructure.

NRENs find that two problems hinder the massive rollout of server certificates:
- the per-certificate pricing of commercially available certificates
- the 'browser-popup[1]' problem in server certificates issued by NREN PKIs.

A number of NRENs[2] have banded together and are seeking to contract, through TERENA, and using TERENA as a contracting party, a commercial CA provider to issue server certificates to these NRENs and their user communities either by establishing and running a dedicated CA or by other means. This should take away the barriers for large-scale use of SSL server certificates in these communities (any usage, not limited to the usage-cases briefly mentioned above) through CA services from a commercial CA provider that allow the NRENs involved to act as service providers for their constituency and issue an unlimited (or close to that) number of SSL certificates per year.

[1] This problem refers to the 'the issuer of this certificate is not trusted' when a browser encounters a server certificate issued by a CA that is not available in the browsers' Root-CA certificate repository, as is the case with all European NREN PKIs.

[2] The term 'NREN' is used throughout this document to indicate a TERENA national member and/or another national organisation representing the academic community in its country. The following NRENs and national organisations are currently participating in this procurement procedure: ACOnet (Austria), CARNet (Croatia), CESNET (Czech Republic), CRU (France), RedIRIS (Spain), SURFnet (the Netherlands), SWITCH (Switzerland) and UNI•C (Denmark).

Requirements

Mandatory requirement

- A server-certificate should not result in a 'The issuer of this certificate is not trusted' pop-up at the end-users' client; it is sufficient if this requirement is satisfied for the versions of the Microsoft Internet Explorer and Mozilla/Netscape families of browsers that are in use at the time the service becomes operational.

Optional requirements

The proposals should specify whether the following requirements can be met, and if so, at which extra cost:

- PKIX compliance (especially RFC 3280)

- Flexibility for the Certificate Authority Policy (CP) and Certificate Authority Practice Statements (CPS). A policy document that follows the RFC 3647 structure will be considered a plus. Within a reasonable time after the service enters its production phase it should become possible to define custom certificate profiles enabling the use of, for example, extendedKeyUsage. As another example, the requester should be free to choose the value for the subject's CN attribute within specified limits. These requirements translate into a general flexibility in the usage of the attributes.

- Enforce that all End Entities Subject DNs start with a unique prefix ('dc=org,dc=scs' would be a perfect example), with the possibility of using other attributes (dc, o, c, ou, cn) for constructing the DN after the prefix.

- Enable NREN-specific branding and localisation of the proposed service.

Background and expectations

- Each NREN is best equipped to create the proper level of Registration Authority (RA) delegation needed for its own community; many NRENs will already have one or more contact persons appointed at each connected site that could easily be used as such, many NRENs with already established PKIs will be able to re-use their existing delegated RA/CA infrastructure. Where a delegated structure is in place it is usually already supported by contracts.

- Combined buying power plus their position in the academic world are expected to allow NRENs to acquire the service cheaper through a joint procurement.

- NRENs wish to enable large-scale rollout of server-certificates by moving from a per-certificate/per-DNS-domain fee to a per-NREN fee.

Proposed architecture

Every X.509 certificate service consists of a CA that issues certificates and of a (hierarchy of) RA(s) that verifies the requests and instructs the CA to issue or revoke a certificate. The CA acts as a dumb signing-/revocation-engine on the orders of the RA.

It is preferred to have a hierarchical RA structure which (where possible and feasible) follows existing contractual relationships, especially the relationships between organisations[3] and their NREN (e.g. those established by existing academic PKIs).

This would result in a single RA per participating NREN communicating with the (outsourced) CA.

The organisations represented by an NREN should be able to set up their own sub-RA, hierarchically positioned under the NREN-RA, resulting in the process of verifying the binding between machine-identity, public key and organisation being put as close to the subject as possible.

The NREN-RA is responsible for setting up a procedure for issuing and revoking certificates that satisfies the requirements of the CA provider. The NREN-RA is also responsible for ensuring that this procedure is adhered to.

The service should comprise the whole path from the system-administrator who generates the certificate request through the RA/CA structure back to the system-administrator with a certificate. All the work per transaction effort for issuing or revoking certificates is performed by the organisations and their NREN.

Services to be contracted

The following services will be contracted from a well established CA provider:

- **CA platform**: This comprises the backend CA and associated requirements (e.g. CP and the related CPS) and interfacing specifications (API) towards the RA infrastructure. It must be demonstrated that it is possible to change the CA provider while keeping the RA platform. The interface towards the RA needs to be documented and should follow applicable standards (if available). The CP/CPS of the CA provider must be published and operations must periodically be audited through a reliable audit process.

[3] The term 'organisation' is hereafter used to indicate an organisation being represented by an NREN or by a national organisation representing the academic community in its country.

- **RA platform**: This comprises the RA backend infrastructure offering the RA interfaces and associated procedure specifications. The RA set-up including the RA platform forms a major investment in terms of manpower and this investment needs to be properly protected by making it as independent from the CA service as possible. The interface towards the CA service needs to be documented and should follow applicable standards (if available).

Procedure and timeline

The services requested under this Call for Proposals are to be classified as "electronic signature certification services"[4] and are listed on Annex I B of the European Services Directive[5]. The Services Directive prescribes only very limited regulations for tendering such so-called Annex 1 B 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 which 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 services. TERENA emphasises that the procedure does not classify as one of the award procedures laid down in the Services 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, except if the company winning the contract explicitly expresses to TERENA legitimate commercial interests to remain anonymous.

All proposals must be received no later than 30 September 2005 at 11:00 hrs Dutch local time. TERENA reserves the right but does not assume the obligation not to consider proposals received after this deadline.

All proposals must be received on paper at the address mentioned below no later than the deadline mentioned above. 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.

[4] Please see numerical code 74113210-9 of the Common Procurement Vocabulary (2003 version).
[5] European Council Directive 92/50/EC as amended by European Parliament and Council Directive 97/52/EC.

Any questions concerning the Call for Proposals must be sent to the liaison person mentioned below, through e-mail. Questions must be asked before 15 September 2005 at 12:00 hrs Dutch local 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 forwarded to all Parties to which TERENA has sent this Call for Proposals. Both answers and questions will be issued no later than 24 September 2005 at 14:00 hrs Dutch local time.

After TERENA has selected a preferred supplier, all other Bidders which have submitted a proposal will be notified 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 two weeks after the date of the notification. After expiration of the two-week period without any objections being raised, TERENA will enter into a contract with the preferred supplier.

The prospective overall time schedule is as follows (all times in Dutch local time):

Deadline for questions from interested parties	15 September 2005, 12:00 hrs
Deadline for answers and corrections by TERENA	24 September 2005, 14:00 hrs
Deadline for submission of proposals	30 September 2005, 11:00 hrs
Appointing preferred supplier	end October 2005
Two-week period for objections	first half of November 2005
End of awarding process by signing contract	mid November 2005
Start of service	1 January 2006

Bidders may be invited to a meeting with TERENA representatives to discuss their proposal. These meetings, if any, are expected to take place between 10 October 2005 and 21 October 2005.

The mandatory and optional requirements of the requested service are listed above. Every Bidder is requested to use this list in his proposal, to reflect compliance to each of the requirements. Partial compliance or non-compliance should be annotated and explained in documentation to be included with the proposal.

The service requested in this Call for Proposals is divided into one lot. TERENA aims to grant contract to a single Bidder whose proposal offers technical soundness and feasibility within TERENA's budget constraints.

The proposals will be assessed on the following criteria (non-exhaustive, not described in details and not listed in any order of importance):
- price;

- extent to which the optional technical requirements are met; and
- favourableness of the contractual terms.

TERENA reserves the right to not award contract at all.

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

The proposal must be written in the English language.

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 either 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 liaison person (see contact details below).

The proposal must be valid for a period of at least six (6) months, after the submission deadline of 30 September 2005.

Each proposal will be treated confidentially.

Each item of the proposal sent to TERENA is considered to become the property of TERENA unless otherwise specified and agreed by the Bidder and TERENA.

Terms of Agreement

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

1. The law of the Netherlands applies to these agreements.

2. The agreements should include liability clauses that as a minimum entitle TERENA to reimbursement of any fees it has paid up-front, in case the agreement is terminated early, due to circumstances regarding the provider of the service.

3. The Call for Proposals, the Question & Answer document(s) and any additional correspondence shall form part of the final agreement.

4. Any dispute arising between the parties over the application or interpretation of the agreement shall be settled between the parties. Should the parties fail to settle the dispute, it shall be resolved with the Court in Amsterdam, the Netherlands.

5. The contract period for the service shall be one year, with the possibility of renewal.

6. The provider of the service has the right to commence invoicing for the contracted service from the day on which the acceptance test has been passed.

7. Any recurring costs will be paid one period in advance. The length of the period must never exceed three months.

8. Any compensation due to failure of services shall be subtracted from the next invoice or settled separately if agreed thus by the parties.

9. If the provider fails to deliver the services according to the contracted schedule, TERENA is entitled to claim compensation equal to the contracted price of the missing services, on a daily basis rounded down to the nearest full day, without prejudice to its right for compensation for other losses and damages.

10. If the provider fails to deliver the service within two months after the contracted date, TERENA is 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 3, 5 and 10 are mandatory.

Contact details

The proposal shall be addressed 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: licia@terena.nl
Phone: +31 20 5304488
Fax: +31 20 5304499