

Questions and Answers Call for Proposals TSec(08)061

Introduction

The following questions with regards to the SCS Call for Proposals (CFP) (TSec(08)061) have been received by TERENA. In order to ensure that all potential bidders have access to the same background information, TERENA publishes the complete set of questions and answers.

Q1. Who is the supplier of SSL certificates for the current SCS service?

A1. The current supplier is GlobalSign BV/SA of Leuven, Belgium. For more information please see the TERENA web site:

<http://www.terena.org/activities/scs>

and

http://www.terena.org/news/fullstory.php?news_id=1509

Q2. Why are you tendering while you have a current contract with GlobalSign?

A1. As mentioned in section 1.3 of the CFP, the current contract with GlobalSign expires in January 2010. After four years TERENA feels it is worth investigating the market again.

Q3. How many websites require SSL certificates for each of the 19 organisations specified in your CFP?

A3. See Annex C of the Call for Proposals for the total number of certificates issued. Please see Q&A6 for more information on the type of servers for which certificates have been issued.

Q4. Are the 19 organisations part of the same organisational group and can their connection be referenced through a third party reference, such as Dun & Bradstreet?

A4. The organisations are all members of TERENA. Because they are located in different countries in Europe and because they all operate in the academic area, it is unlikely that any third party commercial organization can link them in the way suggested by the question.

Please see <http://www.terena.org/about/> for more information about the relationship between TERENA and its members.

Q5. Would each organisation require to manage and purchase their certificates separately?

A5. The organisations requesting and using the certificates are research and educational organisations served by the NRENs. The constraints for the certificate lifecycle management process are laid down in chapter 2 “Services to be contracted”, section 4.2 “Awarding procedure” and chapter 5, “Technical requirements”.

Please take particular note of what is outlined in the CFP, section 2.1, final bullet point: “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.”

Q6. What is the general function of the websites that require certificates?

A6. Generally speaking the websites requiring SSL certificates contain information that ties to the core function of educational and research organisations: public websites with course material, information about projects and research activities, student enrollment websites, intranets, etc.

Please be advised that our community uses SSL server certificates for many purposes other than websites. A list of examples includes, but is not limited to, public websites, intranet websites, project websites, VPN concentrators, print clusters, e-Learning environments, database servers, email servers, collaboration suites. Everywhere in the educational and research community where SSL server certificates are required we can expect the SCS certificates to be used.

Q7. How many websites are publicly facing the Internet and who would typically visit/transact on the websites?

A7. Generally speaking all websites are facing the public Internet. Typical users interacting with these sites (and with other SSL protected services) are students, researchers, university staff and in general everyone interacting with research and education organisations.

Q8. How important is the use of a minimum of 128 bit encryption (versus 40 bit encryption)?

A8. We consider 128 bit encryption essential. We do not consider the use of server gated cryptography relevant for our community.

Q9. Currently TERENA is using a customised issuing CA (SureServerEDU) at GlobalSign. Is there any particular reason this structure was used, or is TERENA happy to have certificates issued from the CA's normal production environment?

A9. This structure was used to allow for a lower liability associated with the SCS certificates than is required for business transactions. Certificates issued from a CA's normal production environment are a viable alternative.

Q10. Does TERENA currently play any role in validating the Organisation and Domain information used in the certificates?

A10. No, TERENA does not play any role in validating the organisations and the related domains.

Q11. Does TERENA prefer that activity to remain totally with the NREN RAs?

A11. TERENA does not want to play any role in validating the organisations and the related domains. However, this does not mandate this activity to totally remain with the NREN RAs. TERENA is also open to other solutions, as outlined in section 2.1 "Background and expectations", in particular the first and second bullet point:

“

- 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.

“

Q12. The CFP mentions the number of 2,225 organisations. Can TERENA provide a breakdown of how many of those organisations have issued SCS certificates, or the number of domains involved?

A12. The number of 2,225 organisations stated in Annex C: “Facts and figures TERENA SCS” is the aggregate number of research and educational organisations that have subscribed to the SCS service via their NREN. Almost all of these organisations will have actually obtained one or more SCS certificates.

The total number of organisations served by the NRENs is higher than 2,225 and therefore the number of organisations subscribed to the SCS service may grow further.

TERENA cannot provide the number of domains involved. The statistics and observations of some of the NRENs suggest that the number of issued certificates per subscribing organisation typically scales with the size of the organisation and that the bigger organisations tend to use sub-domains within their primary domain name.

Q13. Can TERENA provide a breakdown of the certificates issued per year? By validity period? Wildcards?

A13. We cannot provide such a detailed breakdown, but we can provide the following additional information:

- About 3,500 certificates had been issued as per Dec 2006 (at the time 8 NRENs were participating in the service since Jan 2006 and another 3 NRENs joined towards the end of 2006);
- 12,551 certificates had been issued as per Dec 2007 (by then 16 NRENs were part of the service).

The statistics of some of the NRENs suggest that the vast majority of certificates have a validity of 3 years.

Wildcards certificates are used by organisations served by some of the NRENs involved in the SCS service. TERENA has no data about the number of wildcard certificates issued by the SCS service.

Q14. Are TERENA and its NRENs interested in Extended Validation (EV) SSL certificates?

A14. As stated in the CFP, section 2.1:
“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’).”

The Bidder may include Extended Validation SSL certificates in the offer but the financial, technical and procedural consequences have to be clearly specified.

Q15. Section 1.3 of the CFP mentions that 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" and section 2.1 of the CFP states that "each NREN-RA applies a workflow that is optimised to the particular circumstances in its constituency". Please provide information regarding the current vetting processes and workflows so that we can understand the requirements of the NRENs in detail.

A15. The current vetting process is described in detail in Annex B "Current TERENA SCS RA procedure" of the Call for Proposals whereas Annex A, "Current entities and roles" describes the entities involved in this process and their respective roles.

We want to emphasise, as is outlined in Annex A, first sentence, "***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.***"

Section 2.1 also carries particular relevance to this question, in particular the first bullet point:

“

- 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.

“

Q16. With regard to the e-Science certificate profile, are the DN fields required all standard x.509 attributes, and which party sets the field contents: TERENA, the NREN, or the requester?

A16. The e-Science certificate subjects are constructed using attributes defined in RFC 5280, section 4.1.2.4. To ensure global uniqueness, the subjects are constructed with a fixed prefix (e. g. "dc=org, dc=TERENA, dc=scs") followed by the end-entity specific attributes (e. g. country, organizationalName, commonName). The end-entity specific attributes are provided by the requester.

Q17. In Annex B, section 3.2 the CFP states that "...the Registration Authority will verify the ownership of each of the domain names...". Can TERENA please confirm whether it is acceptable for the contracted service provider, and no one else, to perform the domain name pre-validation?

A17. As outlined in Annex B, first sentence, *"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."*

TERENA considers the possibility to have only the contracted service provider perform the domain name validation a viable alternative.

In this context the Bidder is asked to take note in particular of section 2.1, "Background and expectations" and of the award criteria as stated in section 4.2, "Awarding procedure" (in particular the first sentence of section 4.2).

Q18. According to our policy and procedure it is common to sign an NDA in order to disclose company information. Would TERENA be willing to sign an NDA?

A18. The CFP states that all proposals (and more in general, all information) received by TERENA will be treated confidentially. We believe that the information we require does not go beyond the level of 'commercial in confidence' and as such does not require an NDA.