Call for Proposals

TERENA Certificate Service 2014

Table of Contents

1. Introduction and Background 2
2. General Information 2
2.1 Contracting Authority 2
2.2 Type of Procedure 3
2.3 Time Schedule 3
2.4 Language and Currency 4
2.5 Clarification and Questions 4
2.6 Opening of Tenders 4
2.7 Evaluation and Decision 4
2.8 Period for Objections 5
2.9 Applicable Law 5
2.10 Terms of Agreement 5
3. Pre-Requisites 6
4. Requirements and Approach 6
Annex A: Technical Requirements 8
Annex B: eScience Profile 13
Annex C: Participating NRENS 18

1. Introduction and Background

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

Since 2005, TERENA[1] has coordinated a joint procurement on behalf of European NRENs to provide TLS certificates to their constituencies. Initially, this service focused on server certificates but in recent years has been expanded to include certificates to support personal certificates and code-signing certificates. 29 European NRENs currently take advantage of the TERENA Certificate Service (TCS)[2], whilst a further 44 NRENs have the option to sign-up to the service (see Annex C). Bidders are encouraged to review the information on the existing TERENA TCS website regarding the existing service before submitting a bid.

Bidders are invited to submit an offer for a managed TLS 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 certificates as described in the technical requirements for this tender.[3]

The primary aim of the joint procurement is to reduce the per-certificate cost for organisations and as such, TERENA is seeking a fixed priced core service. A proposal that assumes that a financial transaction will take place for each individual certificate request is not considered to be a viable option, although additional services may be charged individually as 'add-on' features.

TERENA is open to novel approaches to solve the challenge of providing large numbers of 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 and therefore seeks proven technology.

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 as part of the offered service. TERENA will create a Certificate Practice Statement to establish policies and procedures for the validation and issuance of certificates as part of this agreement.

2. General Information

2.1 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

[1] TERENA: www.terena.org.
[2] TERENA Certificate Service: www.terena.org/activities/tcs.
[3] Please see Annex C for historical facts and figures. Note that no rights may be derived from the stats and figures provided.

organisations (NRENs) from countries in and around Europe. For more information see: http://www.terena.org. 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, acting on behalf of the NRENs listed in Annex C and their users.

The contact details for this Call are:

TERENA
468D Singel
Amsterdam 1017 AW
Contact person: Nicole Harris
e-mail: procurement@terena.org
phone: +31(0)20 5304488

2.2 Type of Procedure

Under the Common Procurement Vocabulary ("CPV"), i.e. a European classification system for public procurement, the TCS qualifies as a 'certification service' (Classification 79132000-8 of the CPV). Because certification services in turn are listed in Annex IIB to the Procurement Directive the TCS is to be regarded as a B service. The Directive prescribes only very limited regulations for tendering Annex 2B services, i.e. common rules in the technical field and certain publication rules. Due to the cross border character of the service (and the related cross border interest of bidders to participate in this tender procedure), TERENA 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;
- Advertise the tender procedure on TenderNed and TED.

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[4].

If the procedure leads to successful granting of the contract, TERENA will notify the European Commission within 48 days of awarding a contract through the relevant submission form on TenderNed.

2.3 Time Schedule

All proposals must be sent to procurement@terena.org no later than 18 April 2014 at 12:00 hrs Central European Summer Time.

Call for proposals issued	24 February 2014
Deadline for questions and clarifications	14 March 2014, 12:00 hrs CET

[4] Within the context of the Dutch Public Procurement Act 2012 the award procedure only classifies as a 'procedure for B-services' and not as one of the other award procedures described therein.

Response to questions and clarifications	21 March 2014, 12:00 hrs CET
Deadline for submission	18 April 2014, 12:00 hrs CEST
Interview of bidders	Week 26 May 2014
End of selection and awarding process	06 June 2014
Stand-still period of 20 days	30 June 2014 - 18 July 2014
Estimated contract date	End July 2014
Start of service	TBD

2.4 Language and Currency

All questions, clarifications and proposals should be submitted in English. The preferred currency for the tender is euros, although TERENA is willing to consider working in other currencies if it is advantageous to do so. TERENA reserves the right to request bidders which have chosen an alternative currency, to adjust their proposals to euros against the applicable exchange rate of 18 April 2014, 12:00 hrs CEST.

2.5 Clarification and Questions

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 14 March 2014, 12:00 hrs CET. 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 21 March 2014, 12:00 hrs CET.

2.6 Opening of Tenders

Immediately after the deadline for submission (18 April 2014, 12:00 hrs CEST) TERENA will inspect all proposals that have been submitted, and will generate a list containing all bidders for this Call for Proposals. 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.

2.7 Evaluation and Decision

TERENA has appointed a committee of community experts to undertake the evaluation against the criteria outlined in sections 3 and 4 below. The following process will be followed:

- TERENA staff will review each proposal against the pre-requisites. Any proposal that fails to meet the pre-requisites will be rejected at this stage.
- The TCS Tender Committee will assess the cost of the proposal against the affordability criteria.
- The TCS Tender Committee will be invited to mark each proposal against the technical requirements described in Annex A. All proposals that fail to meet the minimum technical score of **25 marks** will be rejected at this stage.
- Bidders with the highest scoring proposals may be invited to interview at the TERENA Offices in Amsterdam during the week of 26 May 2014.

- The TCS Tender Committee will meet to review the remaining proposals in light of the financial score and the technical score awarded. The contract award criteria will be "the most economically advantageous tender". This will include a full review of the combined technical and financial score in relation to the full service offer.

2.8 Period for Objections

After the decision of the TCS Tender Committee has been announced, a stand-still period of 20 days will be put in to effect. During this period any objections to the process of evaluation and award may be raised with TERENA.

2.9 Applicable Law

This award procedure is governed exclusively by the law of the Netherlands. Any dispute shall be adjudicated, in the first instance, by the District Court of Amsterdam. Should a bidder object to any action and/or decision of TERENA with regard to the award procedure, such bidder must initiate interim injunction proceedings against such action or decision within 20 calendar days after the day that the decision or action became known to the bidder or could reasonably have become known. If a bidder does not actually file for preliminary injunction within such 20 calendar days, such bidder shall have forfeited any rights in this respect towards TERENA (including any right to claim damages).

2.10 Terms of Agreement

The contract period for the service shall be two years, with the possibility of renewal. That possible renewal will be for yearly periods, with a maximum of three years. The maximum contract period will therefore be 5 years. The service will run in conjunction with the existing TCS service for a period of 10 months to ensure effective hand-over of the service.

TERENA will provide a model contract for the service that will at least contain the terms described below. The application of any general terms and conditions of the provider is hereby expressly excluded. No minimum purchase obligation will apply.

The law of the Netherlands shall apply to the agreement. 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 by the competent Court in Amsterdam, the Netherlands.

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.

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.

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. Should this occur, TERENA shall be entitled to contract with the follow-up winner from this call procedure.

The provider will be expected to support TERENA in migrating the service to a new supplier as appropriate when the contract period is complete.

3. Pre-Requisites

All proposals submitted must meet the following pre-requisites. Bidders are invited to signal their compliance with these pre-requisites in their response to TERENA:

- The proposal must be valid and irrevocable for a period of at least 6 months from the submission deadline date.
- The proposal must include a statement that the bidder has read and agreed to the Terms of Agreement in section 2.9 above.
- 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 judgment for fraud, corruption, and / or 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 financial status of the bidder, including the bidder's annual financial reports for 2011 and 2012.

4. Requirements and Approach

All proposals must meet the pre-requisites outlined in section 3 above. All proposals that meet these pre-requisites will then move forward to the second stage of the marking process, which is divided into a financial review and a technical review.

For the financial review, TERENA will review the total cost of the service against affordability criteria. The following formula will be used: Score = 30 * (Min / Cost), where Maximum Score = 30, Lowest cost bid = Min, cost bid = Cost and Score bid = Score.

Annex A details the technical requirements for the tender. **For each criterion, bidders are invited to provide a written explanation as to how the proposed service will meet this requirement. Each criteria will be assessed by the Tender Committee and given a score on a scale of 0 – 5 (see Annex A). Answering a requirement with 'compliant' or similar one word reply will not provide enough information for the review and may result in a failing score. Instead the bidder will provide a complete explanation of how the service will fulfil each requirement.**

If a requirement cannot be met by the proposed service, please explain this in full against the appropriate criterion.

The TCS Tender Committee will evaluate each bid against the requirements, using the weighted criteria shown in Annex A. The maximum total that can be achieved by any bidder against the technical requirements is 50 marks (weighted). Any proposal scoring less than 25 marks (weighted) in the technical assessment will be automatically rejected from the process. All other proposals will then be assessed against the score received for service cost before a final decision is made.

Annex A: Technical Requirements

The following Annex details the Technical Requirements for the tender. For each criterion, bidders are invited to provide a written explanation as to how the proposed service will meet this requirement. Each criteria will be assessed by the Tender Committee and given a score on a scale of 0 – 5. Answering a requirement with 'compliant' or similar one word reply will not provide enough information for the review and may result in a failing score. Instead the bidder will provide a complete explanation of how the service will fulfil each requirement. The weighting shows the importance given to each requirement as part of this tender.

A.1 Scoring Criteria

The scoring criteria to be used are as follows:

Score	Criteria	Judgment
5	The response could be regarded as a perfect model that will significantly exceed requirements in all respects, and bring significant added value and benefit to the project.	Excellent
	The response is fully detailed, with appropriate explanations and supporting evidence, and there are no identified issues.	
	The response does not give any indication that there is a risk the Bidder cannot support the achievement of the intended outcomes of the project.	
4	The response exceeds requirements, and will bring some added value and benefit to the Project.	Good
	The response is detailed, with appropriate explanations and supporting evidence. There are a number of minor issues, but no major issues.	
	The response does not give any indication that there is a risk the Bidder cannot support the achievement of the intended outcomes of the project.	
3	The response satisfactorily meets requirements.	Fair
	The response is sufficiently detailed, with some appropriate explanations and supporting evidence. There are a significant number of minor issues, and a small number of major issues.	
	The response indicates there is limited risk that the Bidder cannot support the achievement of the intended outcomes of the project, but the risk is manageable.	
2	The response meets some requirements, but falls short of meeting all requirements.	Doubtful

	The response has insufficient detail, with limited appropriate explanations and supporting evidence. There are a significant number of minor issues, and a significant number of major issues.	
	The response indicates there is some risk that the Bidder cannot support the achievement of the intended outcomes of the project, and there is doubt that the risk is manageable.	
1	The response meets some requirements, but falls short of meeting most of the requirements.	Poor
	The response has limited detail, with limited appropriate explanations and supporting evidence. There are many minor issues and a significant number of major issues.	
	The response indicates there is significant risk that the Bidder cannot support the achievement of the intended outcomes of the project, and it is unlikely that the risk is manageable.	
0	The response does not meet requirements.	Unacceptable
	The response has insufficient detail, with virtually no appropriate explanations and supporting evidence. There are many minor issues, and many major issues.	
	The response indicates there is significant risk that the Bidder cannot support the achievement of the intended outcomes of the project, and the risk is not manageable.	

A2. Technical Requirements

Bidders may use the table below as a template or use an alternative form, however requirements should be easily identifiable against each section as shown.

1	**Certificate Types**	**Weight**
1.1	The offered service should allow organisations to request OV certificates.	0.6
1.2	The offered service should allow organisations to request EV certificates.	0.6
1.3	The offered service should allow users to request personal certificates.	0.3
1.4	The offered service should allow users to request DV certificates in cirucmstances where OV and EV cannot be used.	0.3
1.5	The offered service should allow users to request code signing certificates.	0.3
1.6	The offered service should allow organisations to request a range of other certificate type (e.g. robot, pdf etc.)	0.2

1.7	The offered service should allow certificates with a range of validity periods (between 1 and 3 years).	0.2
1.8	Certificates issued by the service within the contract period should remain valid and revokable beyond the lifetime of the contract.	0.4
1.9	The offered service should allow wildcard certificates to be issued.	0.2
2	**Certificate Profiles**	**Weight**
2.1	The offered service should meet the eScience requirements (as per the specification in Annex B).	0.5
2.2	The offered service should allow certificates profiles to be created during the service lifetime, e.g. profiles relating to specific values in extendedKeyUsage and subjectAltName.	0.1
2.3	The offered service should support profiles accepting at least RSA Key Lengths between 2048 bits and 8192 bits and support SHA-1, SHA-256 and SHA-512,and have appropriate migration plans in place for SHA-1 obsolescence.	0.15
3	**Service Scope**	**Weight**
3.1	The offered service should be available to an agreed list of NRENS and their customers.	0.2
3.2	The offered service should support an efficient and effective process to handle certificate request 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.	0.5
3.3	The offered service should support a fully electronic certificate request process - certificate requests should not require face-to-face meetings.	0.4
3.4	The offered service should make good use of the existing relationship between NRENS and their member organisations to maximise service efficiency - e.g. NRENS acting as Registration Authorities.	0.4
3.5	The bidder should be willing to support the effective migration of the service to a new provider once the contract period is complete. Key material relating to trust anchors created as part of the contract shall be permitted to be exported to a similarly secure environment after the end of the service. IP in the certificates shall be held by TERENA.	0.5
4	**Interfaces**	**Weight**
4.1	The system should provide a central portal that allows for organisations and end users to request, obtain, renew and revoke certificates, including end-of-life notifications for certificates.	0.6
4.2	NRENS should be able to appropriately brand the central portal interface.	0.4
4.3	The user interface should support web accessibility best practice.	0.05

4.4	The offered service should provide usage statistics using an API and/or the HTML-base user interface.	0.05
4.5	The vendor should provide an API for user interfaces to NRENS as an alternative to the central portal.	0.2
4.6	The offered service interface should support authentication using SAML WebSSO or equivalent.	0.4
4.7	The system should be highly available to end users and offer excellent response times.	0.2
4.8	The system should provide an effective API for provisioning users in to the system.	0.2
5	**Support and Training**	**Weight**
5.1	The vendor should provide full end-user support or escalation through customer help desk during normal business hours.	0.1
5.2	The offered service should provide a written user guide in English.	0.05
5.3	The vendor should provide a training program for NREN staff members.	0.05
5.4	The vendor should continuously perform maintenance and support of the offered service.	0.1
5.5	The vendor should notify customers 10 business days in advance about planned maintenance with significant affect on offered service performance.	0.05
6	**Standards and Compliance**	**Weight**
6.1	The offered service should provide certificates that are recognised by the current versions of the most popular families of web browsers, software and mobile clients throughout the lifetime of the contract.	0.4
6.2	The vendor should be willing to work with standards organisations (such as the CA/B Forum) and reflect best practices from these organisations in to service offerings and be willing to represent the needs of the TERENA community to these organisations as appropriate.	0.2
6.3	The offered service should support the use of the subject alternative name extension, including domains owned by different organisations in different countries, for which CA/Browser Forum compliant Domain Validation suffices	0.2
6.4	The offered service should support multiple valid certificates with the same subject.	0.2
6.5	The audit practices of the offered service should be appropriate for the community in question.	0.3
6.6	The vendor should explain if the service can support the secure hosting of additional enterprise-specific trust anchors, subordinate CAs and end-entity issuing CAs.	0.05
6.7	The offered service should support characters that cannot be represented in PrintableString and names that exceed PrintableString limitations with minimal possible encoding.	0.05

6.8	The offerd service should include 'CRL Distribution Point URLs' in each issued TERENA certificate. The services should include 'Authority Information Access, AccessMethod=OCSP in each issued TERENA certificate.	0.05
6.9	The bidder shall provide online CRL services and online OCSP services as supported by all major browsers. New CRLs should be issued each 24 hours or at most 1 hour after a revocation. OCSP information should be updated immediately after every revocation.	0.05
6.10	The offered service should support extended key usage (eKU).	0.2

Annex B: eScience Profile

This section describes the requirements for TLS certificates that compatible with the technical specifications as defined by the International Grid Trust Federation (IGTF).

B.1 eScience Profile

The vendor must support a certificate profile that is compliant with the Grid Certificate Profile[5] (GFD.125) or - at the discretion of the vendor - its successor version.

Certificates issued for the eScience Profiles should also support a validity period of 13 months. It should be possible to restrict eScience certificates to only this validity period for those certificates issued through the offered central web portal.

B.2 OID

The certificate profile should allow for OIDs to be added to the certificatePolicies extension on request of TERENA, where TERENA can demonstrate compliance to these listed Policies:

- For certificates issued to servers, this shall be 1.2.840.113612.5.2.2.1.
- For certificates issued to clients, this shall be 1.2.840.113612.5.2.2.5.

It should be possible to add additional OIDs that reflect compatible policies at the request of TERENA for specific purposes at a later time.

B.3 Certificates types

It shall be possible for a client of this service to hold multiple certificates with distinct subject names and profiles for different purposes. These purposes shall be reflected in the permitted keyUsage and extendedKeyUsage extensions, and the certificates may have distinct subject name.
The vendor shall indicate if and how the following use cases are addressed.

It shall be possible to issue certificates that are solely used and usable for TLS Client Authentication, and thus *not* for emailSigning or contentConfirmation. These may be issued to for automated software agents ("Robots"[6]) that act on behalf of a human client, or whose life cycle is securely controlled and managed on behalf of the users by an appropriate qualified and auditable system.

For example, a user called "John Doe" should be able on hold an additional certificate with the subject name "/DC=org/DC=terena/DC=tcs/C=NL/O=Stichting FOM Nikhef/CN=Robot – client auth – John Doe jdoe@nikhef.nl", whose keyUsage contains solely "Digital Signature, Key Encipherment" and whose extendedKeyUsage contains solely "TLS Web Client Authentication", even though an emailAddress is present in the subjectAltName extension.

[5] Grid Certificate Profile: www.ogf.org/documents/GFD.125.pdf or at the vendors discretion the latest Recommendation draft at http://redmine.ogf.org/dmsf_files/25.
[6] For a reference description of this use case, see http://www.eugridpma.org/guidelines/robot/

B.4 subjectDN elements

B.4.1 X.500 subject Distinguished Name directoryName namespace slicing

It should be possible to prepend to the sequence of relative distinguished names in the certificate subject distinguished name a series of specific 1-element sets in order to 'namespace' the subject names. These subjectDN elements must be in the very first elements of the sequence.
The vendor should indicate if the use of the TERENA owned and managed sequence of 1 element domainComponent sets "/DC=org/DC=terena/DC=tcs", whose corresponding subdomain name "terena.org" is owned by TERENA, can be used for the purpose stated.

For more information please refer to the use cases mentioned in GFD.189[7].

B.4.2 subject DN name representation

The relative distinguished name elements of the subject distinguished name (subjectDN) subject to the condition that this name is representable as a PrintableString or T61String for commonName and organisationName elements, and IA5String for domainComponent elements. The transliteration shall be a reasonable representation of the original name, and shall not be excessively long: it should be possible to represent the entire subjectDN in a string no more than approximate 200 characters.

The following fictitious examples are indicative[8] of the intended transliteration and representation (the subjectDN is here given in OpenSSL x509_name_oneline format):

Original name	Seán Ó Nualláin
Original Incorporated Organisation name	The Provost, Fellows and Scholars of the College of the Holy and Undivided Trinity of Queen Elizabeth near Dublin
Original Country	Republic of Ireland
Expected subjectDN	/DC=org/DC=terena/DC=tcs/C=IE/O=Trinity College Dublin/CN=Sean O Nuallain son.example@tcd.ie
RDN Encodings used	dc:IA5String, c:PrintableString, o:PrintableString, cn:T61String
Comment	The formal organisation name is excessively long and shortened to the conventional name. The diacritical marks in the name cannot be presented and are ignored in the transliteration.

Original name	Παναγιώτης κανελλοπουλος
Original	Εθνικό Δίκτυο Έρευνας και Τεχνολογίας

[7] GFD.189: http://www.ogf.org/documents/GFD.189.pdf.
[8] These examples are indicative, and variants are allowed as long at the variants meet the requirements of GFD.125 or as the vendors discretion its successor version http://redmine.ogf.org/dmsf_files/25

Incorporated Organisation name	
Original Country	Ελλάς
Expected subjectDN	/DC=org/DC=terena/DC=tcs/C=GR/O=Greek Research and Technology Network/CN=Panagiotis Kanellopoulos author@grnet.gr
RDN Encodings used	dc:IA5String, c:PrintableString, o:PrintableString, cn:T61String
Comment	Greek characters cannot be encoded in Printable or T61 strings, and an appropriate English translation of the organisation name is available. The name of the individual is transliterated.

Original name	Albrecht Dürer
Original Incorporated Organisation name	Friedrich-Alexander-Universität Erlangen-Nürnberg
Original Country	Deutschland
Expected subjectDN	/DC=org/DC=terena/DC=tcs/C=DE/O=Friedrich-Alexander-Universitaet Erlangen-Nuernberg/CN=Albrecht Duerer aduerer@fau.eu
RDN Encodings used	dc:IA5String, c:PrintableString, o:PrintableString, cn:T61String
Comment	Diacritical marks not supported in the encoding, a transliteration common in the country of origin is used

B.5 Certificate Profile Extensions

B.5.1 Server authentication certificate profile

A prototypical certificate issued to a server (TLS networked listening end-point) will include the following elements. Those elements which will be specific to the chosen vendor are italicised. Bold elements are those required in GFD.125 or necessary for IGTF operational reasons. Other and additional elements may be included as long as they do not conflict with the guidance given in GFD.125.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            78:e9:4d:1d:c0:2a
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=NL, O=TERENA, CN=TERENA eScience SSL CA G2
        Validity
            Not Before: Feb 12 00:00:00 2013 GMT
            Not After : Mar 14 23:59:59 2014 GMT
        Subject: DC=org, DC=terena, DC=tcs, C=NL, O=Stichting FOM Nikhef, CN=stremsel.nikhef.nl
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c2:fa:ff:ee:ef:de:f1:c2:fa:02:62:71:32:36:…
                Exponent: 65537 (0x10001)
        X509v3 extensions:
             X509v3 Basic Constraints: critical
                 CA:FALSE
             X509v3 Key Usage: critical
                 Digital Signature, Key Encipherment
```

```
          X509v3 Extended Key Usage:
              TLS Web Server Authentication, TLS Web Client Authentication
          X509v3 Certificate Policies:
              Policy: 1.3.6.1.4.1.10434.99.667
              Policy: 1.2.840.113612.5.2.2.1
              Policy: 2.23.140.1.2.2
          X509v3 Authority Key Identifier:
              keyid:23:D3:97:BD:…
          X509v3 Subject Key Identifier:
              4A:51:AA:…

          X509v3 CRL Distribution Points:
              Full Name:
                URI:http://crl.tcs.terena.org/TERENAeScienceSSLCA.crl

          Authority Information Access:
              CA Issuers - URI:http://crt.tcs.terena.org/TERENAeScienceSSLCA.crt
              OCSP - URI:http://ocsp.tcs.terena.org

          X509v3 Subject Alternative Name:
              DNS:stremsel.nikhef.nl, DNS:ce03.nikhef.nl
    Signature Algorithm: sha1WithRSAEncryption
         22:62:8b:73:f9:dd:4c:dc:8e:4b:22:7b:5d:e3:90:88:29:b0:…
```

Policy OIDs 2.23.140.1.2.1 (DCV) or 2.23.140.1.2.2 (OV) should be used as appropriate.
The server certificate should also contain clientAuth in the extendedKeyUsage extension.
The signature algorithm and RSA key length used are for this example only: all algorithms and key lengths requested in section 3 should be supported.

The subjectDN is given in default OpenSSL format, where the first element of the sequence of RDN sets is printed first in the string representation; the RFC2253 representation of this same name is "CN=stremsel.nikhef.nl, O=Stichting FOM Nikhef, C=NL, DC=tcs, DC=terena, DC=org"

B.5.2 Client authentication certificate profile

A prototypical certificate issued to a client (human end-users) will include the following elements. Those elements that will be specific to the chosen vendor are italicised. Bold elements are those required in GFD.125 or necessary for IGTF operational reasons. Other and additional elements may be included as long as they do not conflict with the guidance given in GFD.125.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            e2:2a:2f:be:81:1e:3a
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=NL, O=TERENA, CN=TERENA eScience Personal CA G2
        Validity
            Not Before: Apr 11 00:00:00 2013 GMT
            Not After : May 11 23:59:59 2014 GMT
        Subject: DC=org, DC=terena, DC=tcs, C=NL, O=ExampleUni, CN=Jan Klaassen s1243112@example.nl
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:db:ab:4d:8c:64:b6:03:e0:f2:66:27:e1:93:d2:…
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                E-mail Protection, TLS Web Client Authentication
            X509v3 Authority Key Identifier:
                keyid:C8:89:73:99:A7:…
            X509v3 Subject Key Identifier:
                F8:55:76:3F:38:3D:F1:…
            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.10434.99.666
                Policy: 1.2.840.113612.5.2.2.5

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://crl.tcs.terena.org/TERENAeSciencePersonalCA.crl

            Authority Information Access:
                CA Issuers - URI:http://crt.tcs.terena.org/TERENAeSciencePersonalCA.crt
```

```
            OCSP - URI:http://ocsp.tcs.terena.org

        X509v3 Subject Alternative Name:
            email:j.klaassen@example.nl
Signature Algorithm: sha256WithRSAEncryption
     27:dd:91:c1:40:77:0f:7b:f3:c9:b9:84:3e:cf:10:c2:69:09:…
```

The signature algorithm and RSA key length used are for this example only: all algorithms and key lengths requested in the Technical Requirements should be supported. The subjectDN is given in default OpenSSL format, where the first element of the sequence of RDN sets is printed first in the string representation.

Annex C: Participating NRENS

The following NRENS are currently actively participating in TCS:

Albania (ANA), Austria (ACOnet), Azerbaijan (AZSCIENCENET), Belgium (BELNET), Croatia (CARNet), Cyprus (CYNET), Czech Republic (CESNET), Denmark (UNI.C), Estonia (EENet), Finland (CSC), France (RENATER), Greece (GRNET), Hungary (HUNGARNET), Ireland (HEAnet), Italy (GARR), Israel (IUCC), Lithuania (LITNET), Malta (UoM), The Netherlands (SURFnet), Norway (UNINETT), Poland (PSNC), Portugal (FCCN), Romania (ROEduNet), Serbia (AMRES), Slovakia (SANET), Slovenia (ARNES), Spain (RedIRIS), Sweden (SUNET), United Kingdom (Janet).

The following list includes all the countries that are permitted to sign up to the current TCS:

Albania, Algeria, Andorra, Armenia, Austria, Azerbaijan, Bahrain, Belarus, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Egypt, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Iran, Iraq, Ireland, Israel, Italy, Jordan, Kazakhstan, Kosovo, Kuwait, Kyrgyzstan, Latvia, Lebanon, Libya, Liechtenstein, Lithuania, Luxembourg, Macedonia (Former Yugoslav Republic of), Malta, Moldova, Monaco, Montenegro, Morocco, Netherlands, Norway, Oman, Palestine, Poland, Portugal, Qatar, Romania, Russia, San Marino, Saudi Arabia, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Syria, Tajikistan, Tunisia, Turkey, Turkmenistan, Ukraine, United Arab Emirates, United Kingdom, Uzbekistan, Vatican City, Yemen.

As of December 2013, there were 50,718 active certificates within the TERENA Certificate Service across 28 NRENs. 86% of these are server certificates, and 10% are personal certificates. The remaining 4% represents other certificate types such as wildcard, email and code signing.