European Federated Validation Service Study

Solution Profile – TERENA Academic CA Repository (TACAR)

July 2009

This report / paper was prepared for the IDABC programme by:

Author's name: Indicated in the solution profile below, under '*contact information*'

Coordinated by: Hans Graux (time.lex), Christian Staffe (Siemens), Eric Meyvis (Siemens)

Contract No. 1, Framework contract ENTR/05/58-SECURITY, Specific contract N°14

Disclaimer

The views expressed in this document are purely those of the writer and may not, in any circumstances, be interpreted as stating an official position of the European Commission.

The European Commission does not guarantee the accuracy of the information included in this study, nor does it accept any responsibility for any use thereof.

Reference herein to any specific products, specifications, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favouring by the European Commission.

All care has been taken by the author to ensure that s/he has obtained, where necessary, permission to use any parts of manuscripts including illustrations, maps, and graphs, on which intellectual property rights already exist from the titular holder(s) of such rights or from her/his or their legal representative.

This paper can be downloaded from the IDABC website:

http://europa.eu.int/idabc/
http://ec.europa.eu/idabc/en/document/7764

Executive summary

The European Federated Validation Service (EFVS) Study was initiated by IDABC in order to assess the feasibility of specific measures to ensure the availability of a European scale federated electronic signature verification functionality. As a first step in the EFVS Study, information has been collected on twenty existing solutions that already provide all or some of the functionalities associated with European signature verification functionality, or that could provide valuable insights on how such an EFVS could be organised.

This has been done by drafting standardised profiles of the identified solutions, focusing specifically on how each of these solutions (a) determine the validity of signature certificates; (b) verify electronic signatures created using these certificates; and (c) provide specific guarantees to their customers on the outcomes of these processes.

The present document contains the solution profile for: TERENA Academic CA Repository (TACAR).

Table of Contents

1 Documents

1.1 Applicable Documents

[AD1]	Framework Contract ENTR/05/58-SECURITY

1.2 Reference Documents

[RD1]	Project Management and Quality Plan (EFVS SC14 PMQP)
[RD2]	DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures http://europa.eu/information_society/eeurope/i2010/docs/esignatures/esignatures_en.pdf
[RD3]	Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications http://ec.europa.eu/idabc/en/document/6485/5938

2 Glossary

2.1 Definitions

In the course of this report, a number of key notions are frequently referred to. To avoid any ambiguity, the following definitions apply to these notions and should also be used by the correspondents.

- *Entity:* anyone or anything that is characterised through the measurement of its attributes in an eIDM system. This includes natural persons, legal persons and associations without legal personality; it includes both nationals and non-nationals of any given country.

- *eIDM system*: the organisational and technical infrastructure used for the definition, designation and administration of identity attributes of entities. This Profile will only elaborate on eIDM systems that are considered a key part of the national eIDM strategy. Decentralised solutions (state/region/province/commune…) can be included in the scope of this Profile if they are considered a key part of the national eIDM strategy.

- *eIDM token (or 'token')*: any hardware or software or combination thereof that contains credentials, i.e. information attesting to the integrity of identity attributes. Examples include smart cards/USB sticks/cell phones containing PKI certificates, …

- *Authentication*[1]: the corroboration of the claimed identity of an entity and a set of its observed attributes. (i.e. the notion is used as a synonym of "entity authentication").

- *Authorisation*: the process of determining, by evaluation of applicable permissions, whether an authenticated entity is allowed to have access to a particular resource.

- *Unique identifiers*: an attribute or a set of attributes of an entity which uniquely identifies the entity within a certain context. Examples may include national numbers, certificate numbers, etc.

- *Official registers*: data collections held and maintained by public authorities, in which the identity attributes of a clearly defined subset of entities is managed, and to which a particular legal of factual trust is attached (i.e. which are generally assumed to be correct). This includes National Registers, tax registers, company registers, etc.

- *eGovernment application*: any interactive public service using electronic means which is offered entirely or partially by or on the authority of a public administration, for the mutual

[1] For the purposes of this Profile, the notion of authentication is considered to be synonymous with 'entity authentication', as opposed to 'data authentication'. The notion of 'identification should be avoided to avoid confusion.

benefit of the end user (which may include citizens, legal persons and/or other administrations) and the public administration. Any form of electronic service (including stand-alone software, web applications, and proprietary interfaces offered locally (e.g. at a local office counter using an electronic device)) can be considered an eGovernment application, provided that a certain degree of interactivity is included. Interactivity requires that a transaction between the parties must be involved; one-way communication by a public administration (such as the publication of standardised forms on a website) does not suffice.

- *eSignature*: data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication with regard to this data. Note that this also includes non-PKI solutions.

- *Advanced electronic signature*: an electronic signature which meets the following requirements:

  (a) it is uniquely linked to the signatory;

  (b) it is capable of identifying the signatory;

  (c) it is created using means that the signatory can maintain under his sole control; and

  (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

  Again, this definition may cover non-PKI solutions.

- *Qualified electronic signature*: advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device, as defined in the eSignatures Directive[2].

- *Validation*: the corroboration of whether an eSignature was valid at the time of signing.

[2] See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML

2.2 Acronyms

A2A ..... Administration to Administration

A2B ..... Administration to Businesses

A2C ..... Administration to Citizens

CA ..... Certification Authority

CRL ..... Certificate Revocation Lists

CSP ..... Certificate Service Provider

eID ..... Electronic Identity

eIDM ..... Electronic Identity Management

IAM ..... Identity and Authentication Management

IDM ..... Identity Management

OCSP ..... Online Certificate Status Protocol

OTP ..... One-Time Password

PKCS ..... Public-Key Cryptography Standards

PKI ..... Public Key Infrastructure

SA ..... Supervision Authority

SOAP ..... Simple Object Access Protocol

SCVP ..... Server-based Certificate Validation Protocol

SSCD ..... Secure Signature Creation Device

USB ..... Universal Serial Bus

TTP ..... Trusted Third Party

XAdES ..... XML Advanced Electronic Signature

XML ..... eXtensible Markup Language

XML-DSIG ..... XML Digital Signature

3 Solution Profile – TERENA Academic CA Repository (TACAR)

Name and organisation
TACAR – the TERENA Academic CA Repository TACAR is a trusted repository of verified root-CA certificates, originally proposed by members of TF-AACE, a Task Force on Authentication and Authorisation Coordination for Europe. It is currently coordinated by the non-profit TERENA organisation (Trans-European Research and Education Networking Association – www.terena.org), of which the TF-AACE was a part.
Reference (on-line source)
http://www.tacar.org/
Contact information
• Licia Florio - licia@terena.org • Diego R. Lopez, TF-EMC2 chairman - diego.lopez@rediris.es

Scope of the solution

Services offered
(What services does the solution offer to a relying party? This should include most notably the three basic services above – validation of certificates, verification of the signature, and ensuring trustworthiness and legal liability – but may also cover additional services – e.g. semantic services, archiving of documents/signatures, maintenance, time stamping, security/reliability metrics for the security level of the signature and the certificate,…Services that are not currently available but which are planned for the future may also be indicated.) TERENA is a European non-profit organisation established as an association under Dutch law and focused on collaboration and knowledge sharing related to Internet technology, infrastructure and services to be used by the research and education community. TACAR is TERENA's model to address some of the interoperability issues arising when using multiple PKI solutions in a variety of academic environments. TACAR consists principally of a trusted repository of verified root-CA certificates. The scope of the repository is limited to: • CAs managed by TERENA member NRENs (National Research and Education Networks), • CAs belonging to a National Academic PKI in the TERENA member countries (NPKIs), • CA's managed by institutions to support non-profit research projects that involve the academic community. The repository of currently integrated CAs can be found on-line (https://www.tacar.org/repos/), including links to the CA policies. Through this list, TACAR mainly aims to make it easier to identify and download trustworthy root CAs in order to install them in end users' browsers and applications, such as mail clients. The added value from TACAR stems mostly from the adherence of all participating CAs to the TACAR policy (http://www.tacar.org/docs/TACAR-Policy-v1.4.3.pdf). In addition, it should be noted that most CAs in the repository have been accredited by the IGTF (International Grid Trust Federation), which comprises three Grid PMAs (Policy Management Authorities): EuGridPMA, TAGPMA, APGridPMA. Via the repository, users can see which CAs are compliant with a specific IGTF profile. TACAR intends to also work with other PMAs in the future, such as the one that is being created under the GN3 framework[3]. However, TACAR does not use cross-certification, accept liability with regard to the CA's policies or the information in the TACAR repository itself, or offer signature

[3] See http://www.geant2.net/server/show/nav.2309

validation services.

Application domain (e.g. sector or application types)

(Is the solution usable in any sector or application field (i.e. is it generic in scope), or is it currently limited to a specific sector, application or domain? If it is currently restricted, would it be possible to extend the solution to other sectors, applications or domains? What would need to be changed?)

While the solution has been developed with the TERENA community in mind and is only intended for this community, there is no inherent restriction in the application domain. This would of course require an amendment of the TACAR policy.

CAs covered by the solution

(How many CAs are presently covered by the solution, and which ones? Do they include CAs established in multiple countries or states?)

Currently 55 CAs are listed in the TACAR repository, which can be found on-line (https://www.tacar.org/repos/), including references to the applicable policies. Through this list, TACAR mainly aims to make it easier to identify and install trustworthy root CAs in the end users' browsers.

The list comprises CAs from both European (EU and non-EU) and non-European countries, including several in South America.

Extensibility of the solution

(Can additional CAs be integrated into the solution? If so, are there restrictions? Have such extensions been done in the past yet, or are any extensions currently planned?)

Yes, any CA within the scope of TACAR may request to be included in the repository, subject to the policies defined by TACAR (see http://www.tacar.org/docs/TACAR-Policy-v1.4.3.pdf). The procedure is explained on-line (http://www.tacar.org/join.html), and will be further commented below.

It should be noted that TACAR does not provide and it is not meant for CA policy evaluation. Therefore, there are no policy or technical minimum requirements a CA has to comply with to be accepted in TACAR. The reason for this is that TACAR is a repository, whereas policy

assessment should be done by a dedicated body such as a PMA (Policy Management Authority). In the current situation, policy evaluation for TACAR is done by the EuGridPMA/ IGTF (International Grid Trust Federation) for all Grid CAs. It is possible that other PMAs will evaluate other CAs policies. For instance, there are plans to establish a PMA for the GN3 Project, which will evaluate CAs operating for the GN3 service.

As noted above, however, the envisaged scope of the repository is limited to:

- CAs managed by TERENA member NRENs (National Research and Education Networks),
- CAs belonging to a National Academic PKI in the TERENA member countries (NPKIs),
- CA's managed by institutions to support non-profit research projects that involve the academic community.

This restriction is a part of the TACAR policy.

Business model/cost model of the solution

(How is the solution funded? Is it envisaged as a for-profit model? Who pays contributions, and for what type of services? What profits (if any) are made with the services provided by the solution? Upon request of the correspondent, any communicated price information or other commercially sensitive information will not be disclosed.)

TERENA is a non profit organization, and bears the costs for the maintenance of the repository. Given that no liability is accepted for information within the repository and that no ancillary services are offered, costs are limited.

Technical approach

Validation approach
(Does the solution validate signature certificates, electronic signatures based on a hash value of the signed document(s), or signed documents with embedded signatures?) Not applicable. As noted above, TACAR is a repository of trusted root CAs; there is no validation component.
With regard to certificates
(How does the validation of certificates work – based on OCSP, CRLs, or both? What certificate profiles are supported by the solution?) Not applicable. As noted above, TACAR is a repository of trusted root CAs; there is no validation component. It is worth noting however that whenever a root needs to be revoked or replaced, the TACAR administrator must be notified by the CA representative with a signed email.
With regard to signatures
(What signature formats are supported by the solution - PKCS #7, CMS, XML signatures, PDF signatures, XAdES, CAdES, or others?) Not applicable. As noted above, TACAR is a repository of trusted root CAs; there is no validation component.
Multi-signatures
(Is the solution capable of validating multiple signatures on a document?) Not applicable. As noted above, TACAR is a repository of trusted root CAs; there is no validation component.
Logging and auditing
(Is the use of the solution logged, and if so, to what extent? Do users of the solution have the

possibility to perform audits or to gain access to independent auditing reports?)

Not applicable. As noted above, TACAR is a repository of trusted root CAs; there is no validation component to be logged.

Restrictions imposed on CAs

(What technical requirements are imposed on CAs, e.g. with regard to standards, formats or certificate profiles that they need to adopt? This includes e.g. the inclusion of certain information in signature certificates that is necessary in specific sectors.)

Conditions for inclusion are defined in the TACAR policy (http://www.tacar.org/docs/TACAR-Policy-v1.4.3.pdf). However, it should be noted that TACAR does not provide and it is not meant for CA policy evaluation. Therefore, there are no policy or technical minimum requirements a CA has to comply with to be accepted in TACAR.

Usage of the solution by relying parties

(How do relying parties use the solution? Are there software components which they need to integrate into their own systems, is it a web service, etc.)

Not applicable. As noted above, TACAR is a repository of trusted root CAs; it is up to the participants to decide if/how they want to use the information in the repository.

Technical flexibility

(Given the technical characteristics outlined above, could the technical requirements of the solution be changed to increase its flexibility (e.g. by supporting other signature standards, validation methods, certificate profiles, etc.).

The only limitation in flexibility is the need for a common policy that is considered to be sufficiently trustworthy by the participants. From a technical perspective, this implies no real restriction. TACAR emphasises explicitly in its policy that there are no policy or technical minimum requirements a CA has to comply with to be accepted in TACAR.

Status of the project/Actual usage of the solution

(What is the status of the project (e.g. in development, prototyped, in production, etc.).

What is the actual usage of the solution (e.g. in terms of relying parties adopting the solution to

validate electronic signatures) and what are the impacts of its use? How many transactions, how many certificates does it handle?)

The solution is currently in active use, and will likely be expanded in the future to also host CAs that will be adopted by GN3 services..

Legal approach

Relationship with the CAs[4]

(What requirements does a CA need to meet before being able to accede to the solution? Specifically, which processes and procedures have been foreseen to 'vet' CAs? What kind of agreements are put in place with the CAs, and what are the main issues addressed in these agreements?)

In order to accede to the repository, a CA has to send an application to TACAR (a letter of registration containing general information about the CA, the key and the CP/CPS; see http://www.tacar.org/docs/AnnexI.doc), participate in a face-to-face meeting, and sign a letter committing it to maintain the information published in the repository in accordance with the changing circumstances, and ensuring that applicable practices remain compliant with the TACAR policy (a letter of accreditation identifying the people who are authorised in the CA to update the documents and their PGP keys; see http://www.tacar.org/docs/AnnexII.doc).

The process is initiated via a face-to-face meeting, during which the applying organisation hands the annexes (i.e. the two letters mentioned above) and the trust-anchor (a CD containing the electronic version of the registration letter, the electronic version of the accreditation letter, and the related PGP key) to the TERENA representative or to a so-called Trusted Introducer, i.e. a specific representative who is considered to be trustworthy enough to assist in the inclusion in the TACAR Repository on behalf of TERENA. Criteria for becoming a Trusted Introducer are specified in the TACAR policy. The current Trusted Introducers are:

- David Groep (NIKHEF) representing the EUGridPMA
- Yosho Tanaka (AIST) representing the APGrid PMA
- Mike Helm (EsNET) representing the TAG PMA

Once the process has commenced after the first meeting, PGP may be used as trusted

[4] Within the EU, the term 'CA' should be taken to mean a certification service provider as defined in article 2.11 of the eSignatures Directive (Directive 1999/93/EC) and outside the EU, this means a Certification Authority in the technical sense, i.e. an entity issuing signature certificates to third parties.

mechanism to electronically submit updates.

No further auditing or verification of the acceding CA's practices is undertaken by TACAR.

Relationship with the relying parties

(How does a relying party get the right to use the solution? What kind of agreements are put in place in relation with the relying parties, and which services can be offered to the relying parties via these agreements?)

Anyone is free to install and use the root CA certificates offered through the TACAR repository. However, this is done at one's own risk; TACAR does not accept any liability in this respect.

The TACAR Policy specifies explicitly that TERENA will provide a copy of any CP/CPS associated with any CA root certificate in the repository, and that it is therefore the user's responsibility to check the respective CA policies before using the CA root certificate.

Reliability of the signature certificates

(What procedures does the solution put in place to determine the reliability of signature certificates? Are certificate policies checked? Are supervision/accreditation schemes considered? Have specific security criteria been defined, and does the solution support multiple levels of reliability? If so, can the solution distinguish between qualified and nonqualified signature certificates?)

As noted above, each CA in the repository must sign an agreement with TACAR. However, no further verification takes place. Only a single TACAR policy is defined, which specifies some fundamental obligations for the CAs (specifically the obligation to keep the information in the repository up to date). Supervision/accredition is not considered in this policy, and neither is the status of qualified/nonqualified certificates.

Legal value of the signatures

(Can the solution make a statement on the legal value of signatures? If so, what factors are taken into account? If multiple degrees of validity are supported by the system (i.e. a statement on the reliability of the signature as a whole is provided), then how are these 'reliability levels' defined and communicated to the relying party? Can the solution identify if a signature can be considered a qualified signature (i.e. if it is an advanced electronic signature based on a qualified certificate created by using a secure signature creation device, as defined in the eSignatures Directive)? Finally, if the certificate policies contain restrictions on the use of the signatures (e.g. limitation to transactions of a certain amount or exclusion of certain sectors), then are these restrictions taken into account when communicating the legal value of the signature?)

The TACAR is merely intended as a repository of trustworthy CAs, based on the criteria which TACAR sets forth in its policy. TACAR makes no statement on the legal value or validity of any

signatures created using certificates issued by a CA participating in the repository.

Liability of the solution provider

(What liability (if any) does the solution provider accept with regard to its services? Specifically, if the signatures rely on qualified certificates as defined under the European eSignatures Directive (if this is applicable to the solution), then how does the solution address its liability for providing guarantees to the public in relation to such certificates?)

While TERENA takes responsibility for undertaking the identification/authorisation procedures as described in the TACAR policy document, it accepts no liability in this regard. As noted on the TACAR home page:

"Compliance with the TACAR does not imply that the submitting body has passed any evaluation of its policy, but merely that the root-CA was submitted to TERENA by a bona-fide member of that organisation who identified him or herself to TERENA with a legally-recognised means of personal identification.

TERENA makes no warranty, express or implied, including the warranties of fitness for a particular purpose, or assumes any legal liability or responsibility for the information hosted in the repository."

The status of qualified or nonqualified certificate is not considered by the TACAR policy, and TERENA does not consider itself to be providing any guarantees in relation to qualified certificates (indeed, it explicitly disclaims this role, as noted above).

Quality of service and availability

(Does the solution provide any guarantees with regard to the quality of its service (i.e. the reliability of the information it provides) and its availability to relying parties, other than already mentioned above?)

No, as noted above, no responsibility or liability is accepted by TERENA in this respect.

Independence of the solution

(Is the solution fully unaffiliated (legally unrelated) with all of the CAs that are integrated into the solution? If not, then how is trust created towards the relying party for affiliated CAs?)

Yes: TACAR is coordinated by TERENA, which is fully unaffiliated with the CAs in the repository.

Compliance with the provisions of the eSignatures Directive

(Does the solution support signatures from CAs established in countries that are not subjected to the provisions of the eSignatures Directive (Directive1999/93/EC)? If so, how are they integrated and how does the solution address their legal value?)

As noted above, CAs from non-European countries are already included in the TACAR repository. This is possible due to the fact that TACAR provides no judgment on the value of any signatures created using certificates issued by the participating CAs.

Suitability of the solution at the European level

Assessment of the solution owner

(Does the solution owner feel that the solution could be adapted to operate at the European level – not applicable if the solution already functions at the European level?)

As noted above, TACAR is already used in academic environments across Europe.

Issues to be addressed

(Which issues does the solution owner feel would still need to be addressed before the solution could be made to operate at the European level?)

Not applicable. Considering its scope and goals – providing a repository of trusted CAs – there are no further issues to be addressed. However, to grow beyond its current context, it is likely that some form of guarantees/liabilities would be required to increase trustworthiness of TACAR to outside parties.

Integration with other validation solutions

(Is there any strategy to allow the solution to interoperate with other validation solutions, i.e. can the solution connect to other 'islands of trust'?)

Any solution that is covered by an identifiable root CA can be integrated. It would thus also be possible to integrate e.g. PKI bridges or hierarchies, provided that a root CA can be identified.
Market Impacts
(How could the solution impact or influence the European market?) TACAR is interesting as a trust model; however, it does not accept any liabilities as it stands, nor does it distinguish between different levels of trustworthiness of certificates issued to the public, which is an inherent limitation of the scope and approach.
Any other comments?
(The solution owner can provide any other comments that (s)he feels were not adequately covered elsewhere) Not applicable.