

**1st TF-EMC2 Meeting
3-4 November 2004
Amsterdam, the Netherland**

Welcome and agenda bashing

The first TF-EMC2 meeting was held in Amsterdam on 3 and 4 of November and hosted by the University of Amsterdam. The meeting brought together about 40 people coming from various NRENs in Europe, Internet2 and Grid environment.

Diego welcomed the participants and bashed the agenda, which grouped all PKI-related issues on the first day, whereas the second day was dedicated to other middleware issues.

Agenda and presentations are available at:

<http://www.terena.nl/tech/task-forces/tf-emc2/meetings/nov04/agenda.html>

PKI Related topics

1.TACAR

Diego Lopez

Diego presented the new TACAR web site (<http://www.tacar.org>), set up during the summer. The site contains at the moment 17 certificates (other CAs are in the process of joining), which is more than it was expected in the beginning.

TACAR can be seen as a federated approach to building trust among PKIs.

Diego asked whether statistics could be useful to provide a better view. It was agreed that more than the numbers of download, it would be interesting to know who downloads the certificates.

There are still open issues about TACAR that should be addressed in the near future, which go as follows:

- Downloading certificates. The downloading session of the root CA certificates should be encrypted and for this purpose was proposed to use a self signed certificate, instead than a commercial one (recognized in major browsers). A long discussion followed.

To satisfy the need of encryption while downloading CA certificates, the use of a self-signed certificate or a commercial one makes almost no difference against the threat of a man-in-the-middle attack. The issue is to well protect the server private key and the difficulty of this task does not depend of the nature of the certificate (commercial or self-signed). The need of preventing the www.tacar.org from being tampered with www.tacar.com|net etc remains, using server certificates (either self signed or commercial). Someone can easily register www.tacar.com getting a commercial certificate for it and use the same look and feel as www.tacar.org. Users won't notice any difference, except if they know that they HAVE to check the fingerprint of the certificate against a hard copy or web publication. In this case, having a self-signed certificate which produces a popup is probably slightly better than a browser-recognized certificate, as in the first case users are warned that the certificate is not trusted and consequently more among them will make the effort to check its fingerprint. It would also probably make more sense to certify a non-commercial CA repository website with a self signed certificate. For the reasons listed above a self-signed certificate seems a better solution.

The most important issue remains anyway making sure that potential downloaders of TACAR root CA certificates know exactly the URL of the TACAR repository, where to find the certificate's fingerprint and how to verify it. Keeping in mind that TACAR is not meant for real end users, but for system administrators, enforcing the steps above should not be a problem.

After a long discussion it was agreed to start using a self signed certificate to download the trust anchors.

The fingerprint will be distributed by TERENA to the relaying parties. The first mean of distribution will be the TERENA Annual Report.

This will imply a change of the TACAR policy.

ACTION: LF to update the policy and to circulate it to the tacar list (Jan 05)

ACTION: DL to prepare the self signed certificate (Jan 05)

- Allowing the CP/CPS documents of the CA hosted by TACAR to reside on a site that is different from TACAR. This request came from the EUGridPMA group. The advantage of this approach is that every time the policy is updated there is no need to submit the new document to TACAR, but doesn't solve the problem of resending the finger print of the document, therefore it was agreed to not change the TACAR procedure.
- Information about the security of the web server that hosts the TACAR certificates should be provided on the TACAR web site.

ACTION: LF to update the website

Massimiliano Pala from Politecnico of Torino proposed to add an LDAP backend to the TACAR by the end of year. This would allow for an easier on-line search and an easier management. The LDAP server would be private in the beginning, but in a second moment will become publicly available in read only modality.

ACTION: MP to work on the LDAP back end.

TACAR has proved so far to be a successful initiative; it would be interesting to explore how the repository could be used in other fields.

2. INTERNET2 PKI

Michael Gettes

Michel Gettes presented an update on middleware activities being undertaken by Internet2 as follows:

- Campus

There are currently several infrastructures for High Education (HEBCA/USHER/InCommon/SAML), but nothing at national level.

The academic community is very much in line with what the federal government is doing; namely everything is moving towards a bridge model, which means to trust someone else policy. There are still some problems with the applications that need to be bridge aware.

- Higher Education Bridge Certificate Authority (HEBCA) / US Higher Ed Root (USHER) synergy.

Internet2 has been working on Higher Ed Bridge CA (HEBCA). The new product is called HUSHER, which will be crossed certified with HEBCA. USHER issues only institutional certificates, which can be used for most purposes.

- International Collaboration on Identity Management (I-CIDM)

The rules to get involved span over fields like: citizenship, legal framework, technical issues and of course policy. The principle parties are US Higher education, Federal Bridge CA (FBCA), Pharmaceutical industry (SAFE), commercial aerospace (Joint Striker programme). The federal government requires that the federal bridges have to be run by American citizens.

- Federal eAuthentication effort

There are 24 government programmes funded by the federal government to deal with AA. There is now a move towards USHER and Shibboleth to become part of InCommon federation and to cooperate with the federal government. The recommended approach is to use bridge to leverage global PKIs, which will allow for inter-federation activities. Bridge PKI should be used as means of validating and locating members of other federations. The advantage of a bridge model is that if the root of one of the CAs is compromised it is possible to isolate that CA and still keep using the others.

3. Proposal for a popup-free, flatrate European research and education server-certificate service

Jan Meijer

Jan presented his proposal to acquire a service that offers NRENs a pop-up free X509 server certificates at a flat rate fee for NRENs, with minimum hassle. At the moment server certificates are needed for many applications and NRENs need to buy them from a commercial CA, with the related costs. Jan said that from a rough evaluation SURFnet uses about 600 server certificates per year. The proposal foresees the use of a commercial CA (recognised by the browsers) to issue certificates and to deal with the revocation lists. The NRENs involved would act as RAs; each NREN would manage other sub-RAs, representing institutions related to that NREN. RedIRIS, SWITCH, SURFnet and DFN have expressed their interest in participating.

The proposed roadmap is as follows:

- Sign a consortium agreement (containing information about the budget) with the interested institutions, by December 2004. TERENA would be the legal body to sign the contract. A management board should also be set up to overlook the service.
- Start the process for a tender to commercially acquire the service (December 04)
- Service contracts to be signed by April 2005
- Service available by July 2005
- Service evaluation in July 2006

The financial model agreed consists of a fixed annual fee per participating NREN (at the moment being fixed at 20K Eur). The amount of money agreed is a maximum amount and is intended to be enough to acquire the service for the first year; the real cost will be clear after the service has been contracted. The cost will of course decrease if more NRENs join.

Coordination with other groups

1. EuGridPMA

David Groep

David presented the EUGrid PMA (European Grid Policy Management Authority) group and the model in terms of AA followed by Grid applications.

Grid users join collaboration group, known as virtual organisations (VOs), inside which they can get different privileges and cover different roles. Normally the **VOs** manage the **authorisation**. Users (and resources) are **authenticated** via **digital certificates** provided by CAs. As the Grid grew, the number of CAs grew and coordination between CAs was needed, therefore the EUGridPMA (<http://www.eugridpma.org/>) was born to set minimum requirements for authentication guidelines and a common trust domain for research and academic institutions. The set of minimum requirements guarantees what is needed only for Grid application and in many cases the same CAs have a larger community than Grid (authentication). The EUGridPMA group tries to push countries to have only one CA and ask the institution to run RAs. The root of trust is provided centrally by the CA and it is shared by different institutions

PMA's collaborate bilaterally in an inter-operation framework. There are three main blocks, Europe, Asia-Pacific and Americas. The coordination of these three blocks is still an open issue. Remaining issues faced include better compliance between the minimum requirement and the evolving Grid middleware, industry standards, user's key care (can the user be trusted with key care?), complexity for users, services, online CA methodologies (minimum guidelines, active certificate stores, CA generated key pairs) and ease of use.

It was asked why one of the minimum requirements say that CAs used for Grid purposes should not be hierarchical.

David said that in reality there are a few CA within the EUGridPMA that have hierarchies, but they are static and only the low level generates certificates. The group wants to discourage the use of subordinate CAs, to avoid the distribution of the CRL of all CAs, as this on a big numbers doesn't scale.

2. Liaison with TF-VVC (Task Force, Voice, Video and real time Communication)

Egon Verharen- Surfnet

Egon is the chair of the TF-VVC: Voice, Video, real-time communications taskforce. All collaboration services, like chat, instant messaging, videoconference, need authentication and authorisation standards to control users. Issues like resource discover (users need to know in advance gatekeeper addresses), authentication (not reliable), authorization (all users have the same privileges) and security are still open or partially implemented.

To solve these issues collaboration between the two task forces is important. Egon proposed a collaboration model similar to the Internet2 (I2) working group called vidmic-vc, which produced in the summer 2003 the new videoconference protocol H.350.

As the technology depends a lot on the vendors, it was asked how VVC cope with this. Egon said that the commercial companies follow their trends, but they are willing to listen to the requirements if they come from big and well known communities. Most of the companies know Internet2, but not TERENA which means that it is easier to push forward

requirements coming from I2. Maybe TERENA via TF-EMC2 and TF-VVC should try to get more visibility also outside the academic environment.

3. EuroCAMP: 2-4 March, 2005 (Turin, Italy)

CAMP (Campus Architecture Middleware Planning) workshops have been taking place in the United States for a few years now. Following these examples, TERENA will organise the first CAMP event in Europe on 2,3 and 4 March 2005 in Turin (Torino), hosted by the local university. The target participants of EuroCAMP include CIOs, IT architects and IT managers of universities and research centres across Europe who are involved in designing campus-wide digital ID systems; representatives of national research and education networks in Europe who are involved in harmonising digital ID systems at a national and international level; and any other persons who are involved with digital ID systems in academia.

The programme for the event is being developed by a committee consisting of Licia Florio (TERENA), Ueli Kienholz (SWITCH), Ken Klingenstein (Internet2), Diego Lopez (TF-EMC2, RedIRIS), Miroslav Milinovic (CARNet), Ton Verschuren (SURFnet), Torbjörn Wiberg (Sunet) and Klaas Wierenga (TF-Mobility, SURFnet). Topics to be discussed during the three-day event include: identity management, what is it about and why is it important; federated access to applications; federated access to the network. Because most of the envisaged participants are working in universities and research centres to develop infrastructures and services locally, Licia asked the participants to forward information about the event to those institutions in their own country.

European Updates

1. Sweden, SUNET, Torbjörn Wiberg

Sweden is pushing towards a centralised model, which after the initial costs, will increase efficiency and will make easier the cooperation between different universities. Electronic IDs (meaning in this context one ID per person) would be used to facilitate the process and would be used by different systems. This requires of course harmonisation among the various systems. Sunet has a contract with Umea University to promote a harmonised infraservice -infrastructure within Sweden, also with North Europe and USA.

Sweden has got a CA, SwUPKI which at the moment, issues mainly server certificates. The Swedish government is deploying federal identity.

As far as the Authorisation, SPOCP is mainly used.

There is a Nordic eduperson that includes Norway, Sweden and Finland.

2. UK, JISC, Alan Robbiette

Alan presented the English Middleware development programme, which includes almost 16 projects. The programme targets virtual organization, authorization policies, Grid, e-Learning and other AA issues. UK has just launched an initiative called Virtual Research Environment.

UK would like to move towards a more driven policy authentication model. The integration of PERMIS and Shibboleth is complete and it seems to be quite a flexible platform. JISC is building a production Shibboleth federation which should be in place in 2006, by which time there would be a critical mass of resources by shibbolising existing JISC services. An ATHENS/Shibboleth gateway development activity is underway. The full migration/co-existence strategy is still not defined.

UK is also part of Eduroam, with 29 sites elected for a national trial, a mix of HE and Colleges and mix of network access methods supported. It is expected to have a full service by 2006.

3. France, **CRU Florent Guilleux, Olivier Salaun**

CRU do not operate a national academic network (this is done by Renater), CRU, the Network Committee for French universities, are responsible for coordinating actions among universities and between universities and the ministry for education and research. Middleware current activities are AAI, Directories, Sympa, PKI.

CRU will shortly start an AAI based on Shibboleth, even if at the moment the national schema does not specify all possible values for attributes. A committee has been set up with the aim of defining a full nomenclature of user attributes, which will be based on eduPerson.

CRU has been running a PKI for four years. Server certificates are used mainly by universities (https, imaps, LDAPs). The main problem is popup problem. The options at the moment are either join the TERENA popup-free initiative or wait for a French national PKI recognised by web browsers.

User certificates are not really deployed, due to the fact that have costly registration and revocation process, lots of support is needed because users don't understand PKI concepts, the implementations in web browsers are poor, PKCS#11 devices for mobility secure storage of private keys is also costly. There are also lots of legal constraints to allow safe use of electronic signatures in France.

4. Netherlands **University of Amsterdam, Yuri Demechenko**

Yuri introduced the AIRG (Advanced Internet Research Group), which participates in several projects like Gigaport, collaboratory.nl, the Security Architecture for Open Collaborative Environment and EGEE.

The generic architecture developed by AIRG is now standardized. It intends to separate the policy defined by the resource owner, by the AA technique that is used. He presented also some generic AAA implementations, like bandwidth on demand, access control and privilege management for collaborative environment, Authorisation for web service and Authorisation portType for Grid applications.

AIRG is developing distributed security architecture for collaborative environments based on a job centric model.

Current issues: How to define at the early stage that a private key has been compromised? May require credential storing (not caching) and adding history/evidence

chain to credential format, X509 credentials are not capable of doing this, would SAML have this functionality?

5. Netherlands

Surfnet, Klaas Wierenga

Klaas presented Eduroam and A-Select.

Eduroam, born within TF-Mobility task force, has been very warmly received by the NRENs community, with more than 14 countries connected, with more than 200 institutions. USA and Australia are in the process to set a similar infrastructure. Eduroam can be considered the first federation for network access; the policy framework is nearly in place and some work is being done on attributes and diagnostics. An independent eduroam web site is under development (<http://www.eduroam.org/>), at the moment the information are available on the TF-Mobility web page (<http://www.terena.nl/tech/task-forces/tf-mobility>).

A new release of A-select (1.4), which consolidates functionality and enhances redundancy, is available. Many institutions in the Netherlands use A-Select and it has been selected as the technology for e-federal government service. A-Select is also used in GigaPort –NG project to control access to role-based light path provisioning software.

The University of Amsterdam are starting a Shibboleth pilot

6. Switzerland,

SWITCHaai update Thomas Lenggenhager

SWITCH acts as a federation server provider; the federation membership is based on signed service agreement. There are 50 shibbolised hosts and 5,000 active users, mainly students driven from e-learning initiatives. An example of an open source e-learning solution can be seen at <http://www.olat.unizh.ch/>

Thomas added that SWITCH policy has been developed in independent way; so if there are commonalities with other federations' policy (like InCommon) these are only by chance.

7. Spain

RedIRIS, Diego Lopez

URN (Uniform Resource Name) registry in place under urn:mace:rediris.es. There are namespaces for COPA, LDAP schemas and entitlements. RedIRIS has developed an IRISGRid directory infrastructure. Looking at user ids, user entitlements and user private attribute and are working in the consolidation of use and harmonisation via the IRIS-schema committee.

PAPI is still evolving; the external configuration will be based on a separate XML file. PAPI has been integrated with JNLP and PAPI/Athens connection has been completed. There have been some tests (promising) with RTSP to access videostreams via PAPI. In the near future a PAPI-infrastructure will be developed (following a SAU-WoK proposal) to integrate with library access software for several hundred institutions. RedIRIS is also working on monitoring tools, like RedIRIS weathermap (based on XML <http://www.rediris.es/red/ri2wm/>) and DetectIRIS (Spanish version of the NREN detective produced by SURFnet. Federated web services are being developed based on SOAP +

HTTP (service fed) and RDF+ Dublin Core (semantic model) to be scalable, extensible and simple to configure.

8. Sweden

SPOCP, Roland Hedberg

The SPOCP server is pretty stable and it is starting to slowly add new SPOCP aware applications. SPOCP will be used as a backend for Shibboleth. S-expressions are used to describe information.

In the near future, a UDS (Universal Data Distributor/Dispenser) will be released. This will use SPOCP as route engine, will have a SOAP interface and will use RDF (Resource Description Framework) as data format.

It was asked whether the UDS could be used as middleware diagnostic tool. Roland, said that the Internet2 middleware working group has also expressed interest in using UDS.

9. GEANT2

Juergen Rauschenbach

Juergen presented the JRA5 vision to build a roaming infrastructure which consists of an AA infrastructure with seamless access to e-resources, with the long term aim of a single sign on environment. The vision will also integrate new technologies such as Mobile IPv6.

10. CostWolds Report

Ton Verschuren

Ton reported about the Costworld meeting held on 14-15 October 2004 in Upper Slaughter (UK) and by hosted by the Joint Information Systems Committee (JISC). The meeting was attending by Australia, Finland, the Netherlands, Spain, Switzerland, the UK and the US. CERN also attend as representative of a big scientific community.

The goal of the meeting was to try and establish a framework for further international collaboration of national education authentication and authorisation systems that would lead to convenient interoperable user mechanisms to support international research and education. Participants submitted position papers analyzed by JISC and the results were that each programme was limited initially to one target community and that policies are needed. There are major schemes which target the whole population within these communities, for example, authentication and authorisation schemes for access to digital content.

International collaboration is possible, but there are some things that need to be achieved. The education scheme must support multiple levels of assurance and allow for the use of third party authentication services.

The national schemas set up by the governments to provide electronic identities for citizens are attractive to use, but should be extended. To date there has been little inter-working between these schemes and the national education schemes. Example of government schemas are Finland (the PKI-based electronic passport), the US federal government (has announced a scheme based on smart cards) and in the near future the Netherlands (the government is making e-authorisation a priority to promote e-government and e-commerce).

During the meeting it was agreed to produce a cookbook, containing practical guidance on practical issues, criteria for judging schemas and practical examples.

It was also agreed to have a vehicle for linking authentication systems together, which was agreed to be a super federation.

Directories

1. Directory and schema harmonization

Peter Gietz

Peter provided an update of the Directory Schema Registry (DSR, <http://www.schemareg.org>), which aimed at setting up an LDAP schema registry with easy browsable Web interface and an LDAP interface for retrieval. The policy definition about the standards for inclusion into the registry was also part of the project. To date the project has ran by DAASI at their own cost. A solution to maintain the service alive would be to charge people for its use (either people who download schemas or people who upload schemas), if no organisation volunteers to sponsor it. The estimate cost per year to run the DSR is about 10.000 Eur, which will cover the inclusion of new LDAP schemas and the creation of a committee to evaluate new schemas. As far as the type of information that could be stored in the registry, this should be decided by each virtual organisation in order to have whatr could be useful.

Diego said that in the initial idea of the task force there was a proposal to work on schema in order to harmonise them. The Costworld report emphasises the importance of schemas. It was therefore agreed to have a small group of people within TF-EMC2 to look at schemas definition. Milan Sova, Miroslav Milinovic, Diego Lopez and Peter Gietz volunteer to be part of this group.

ACTION: the people mention above to provide some workplan.

2. FEDERATIONS and PKI

Ken Klingstein

Ken talked about Internet2 activities. Shibboleth as one of the most known activities has been proving to be very successful. A new release SAML-based is available. In the next future Shibboleth will support Grids, as part of an NSF-funded NMI project. The aim is that Globus Toolkit 4 will allow Grid proxies to be Shibboleth targets (do SAML), so that local campus credentials can get access to Grids. The approach should be backwards compatible with the version 2 and 3 of Globus. To allow for integration between Globus and Shibboleth issues like authority management, schema registry and trust coordination among federation need to be addressed.

Ken talked about the differences between federations and PKI. Federations use enterprise-oriented PKI and use SAML as communication language. PKIs use X.509 standard and have more scalability problems. In US Shibboleth is the federating software.

The new federation InCommon (<http://www.incommonfederation.org>), built using Shibboleth AA technologies, operates at a high level of security and trustworthiness and requires its participants to post their relevant operational procedures on identity management, privacy etc. InCommon is used for Institutional users acquiring content from popular providers (Napster) and academic providers (Elsevier, JSTOR, EBSCO, ProQuest, etc.), Institutions working with outsourced service providers, e.g. grading services, scheduling systems and inter-institutional collaborations, including shared courses and students, research computing sharing, etc. Participants have to pay a fee to join.

Ken pointed the attention to diagnostic as a critical part, which can cover different areas, such as network (e2e), desktop tools (like Surfnet detective), policies and so on. Having a standard for the log files would be a first step to solve the problems. Ken envisaged three classes of problems:

- Simple: these are problems related to a single component of a system and should be addressed by a component diagnostic services
- Compound: these are problems that span multiple systems, creating the need for threaded analysis
- inter domain: problems that span multiple domains, creating the need for broad standards, privacy and security tools, etc

The TF-EMC2 could do something in this area. Some elements could be used, for instance the UDS presented by Roland and in some way the AA-RR software developed by RedIRIS.

Conclusions and next meeting

This first meeting gave people the opportunity to present their local activities and in a way gave everybody an occasion to get to know each other, since new people are joining TF-EMC2. The group felt the need to have a more technical meeting in the near future to see how to create a roadmap for common work. Some inputs for possible future activities emerged.

It seems clear that more coordination is needed at global level in terms of creating common schemas and/or harmonize directory. What can be done within TF-EMC2?

Diagnostic is an important issues for many institutions. Could TF-EMC2 start working to explore how feasible is to define a standard for log files?

In terms of PKI, Jan proposal seems a possibility to move forward. The progresses of this initiative will be announced over the TF-EMC2 list. TACAR could be used in a more effective way.

A communication channel with Grids has been open and maybe the moment is mature enough to explore how the NRENs could support Grids.

A better connection between TERENA/TF-EMC2 and other groups, like Liberty Alliance, EUNIS and others would be beneficial.

Summary of the actions

ACTION Description	Name	Deadline
To update the policy and to circulate it to the tacar list.	LF	End of December
To update the website	LF	End of December
To prepare the self signed certificate	DL	End of December
To work on the LDAP back end.	MP	End of December
To provide a workplan for new schema integration in DSR.	MS, DL, MM and DL	End of December

Next meeting will be on the **16 of February 2005**, location to be decided.

Attendees List

<i>Guido Aben</i>	<i>SURFnet</i>
<i>Kristof Bajnok</i>	<i>NIIFI/HUNGARNET</i>
<i>Roberto Cecchini</i>	<i>GARR</i>
<i>Dimitris Daskopoulos</i>	<i>GRNET</i>
<i>Yuri Demchenko</i>	<i>UvA</i>
<i>Ede Fehér</i>	<i>NIIF/Hungarnet</i>
<i>Licia Florio</i>	<i>TERENA</i>
<i>Michael Gettes</i>	<i>Duke University/Internet2/MACE</i>
<i>Peter Gietz</i>	<i>DAASI International Ltd.</i>
<i>Brian Gilmore</i>	<i>University of Edinburgh</i>
<i>David Groep</i>	<i>NIKHEF and EUGridPMA</i>
<i>Florent Guilleux</i>	<i>CRU</i>
<i>Roland Hedberg</i>	<i>Umeå University</i>
<i>Reimer Karlsen</i>	<i>DFN-PCA</i>
<i>Bart Kerver</i>	<i>SURFnet</i>
<i>Ulrich Kiermayr</i>	<i>ACOnet-CERT</i>
<i>Ken Klingenstein</i>	<i>Internet2</i>
<i>Thomas Lenggenhager</i>	<i>SWITCH</i>
<i>Diego Lopez</i>	<i>RedIRIS</i>
<i>Jesus Luna</i>	<i>Polytechnic University of Catalonia</i>
<i>Anders Lund</i>	<i>UNINETT</i>
<i>Jose Manuel Macias</i>	<i>RedIRIS</i>
<i>Miroslav Milinovic</i>	<i>Srce / CARnet</i>
<i>Teun Nijssen</i>	<i>SURFnet-PKI</i>
<i>Massimiliano Pala</i>	<i>Politecnico di Torino</i>
<i>Juergen Rauschenbach</i>	<i>DFN-Verein</i>
<i>Alan Robiette</i>	<i>JISC</i>
<i>Olivier Salaün</i>	<i>CRU</i>
<i>James Sankar</i>	<i>UKERNA</i>
<i>Milan Sova</i>	<i>CESNET</i>
<i>Magnus Strømdal</i>	<i>UNINETT</i>
<i>Alexander Talos</i>	<i>ACOnet / Univie</i>
<i>Egon Verharen</i>	<i>SURFnet</i>
<i>Ton Verschuren</i>	<i>SURFnet</i>
<i>Dick Visser</i>	<i>TERENA</i>
<i>Torbjörn Wiberg</i>	<i>Umeå Universitet</i>
<i>Klaas Wierenga</i>	<i>SURFnet</i>
<i>Jaap van Ginkel</i>	<i>Universiteit van Amsterdam</i>