

TF-AACE Deliverable B.5

A reported on authentication practices in the European NRENs

Diego R. Lopez, RedIRIS

Licia Florio, TERENA

Abstract

This document presents a short review of the current authentication practices followed by the European NRENs in their AA pilots or running infrastructures and it is only a case study, not an exhaustive description of authentication practices.

The information contained in this document was provided by the NRENs, but as there was not detailed questionnaire to be filled in, in many cases the response was quite general. Extra information has been added on the basis of personal knowledge.

Czech Republic

Finland

Germany

Greece

The Netherlands

Norway

Poland

Spain

Sweden

Switzerland

United Kingdom

1. Introduction

When talking about authentication is important to establish a distinction between authentication procedures and authentication schemas. Authentication procedures deal with the process of establishing user's identity and identifying the appropriate identity attributes. Authentication schemas determine the components providing the authentication service, the interactions between the user and the service, and the interactions among the different components.

The first section provides several criteria for classifying authentication schemas, while the rest of this document deals directly with the different authentication procedures that have been reported by the participating NRENs. Our experience is that most (if not all) of the authentication procedures currently in use are compatible with any authentication schema. The rest of sections of this document describe these procedures, grouped according to structural criteria, including remarks for specific authentication schemas where appropriate.

It is also worth noting that we are not considering in this survey the procedures used for establishing the appropriate authentication service for a given user from a target site, generally known as WAYF (an acronym for *Where Are You From invented by the Shibboleth* team). These services are considered to mostly belong to the authorization services.

2. Authentication Schemas. A Classification

Three independent criteria can be established to classify the authentication schemas that European NRENs currently use:

- Whether the authentication procedures are applied by specific (middleware or application) services, or at the network access points. In the first case, identity attributes are usually provided to the authorization elements by means of middleware components known as the AAI (*Authentication and Authorization Infrastructure*). In the second case, user's identity is usually linked (by some automatic procedure or by means of log entries) to the address assigned at the network access point.

A special situation that is being considered in several NRENs (and within the TF-Mobility group) is the case of mobile users employing wireless network access. Several initiatives to unify authentication procedures in a single middleware layer are under development.

- Whether the user's identity (and/or attributes) is determined by means of local sources of data, or it is possible to use external sources for this. The latter case introduces the need for trust models at the authentication phase.
- Whether the exchange of user's credentials must take place in well-defined and controlled points, or it is allowed to use any (possibly registered) point to request these credentials, forwarding them to the authentication service.

As said above, any of the authentication procedures discussed in the following sections can be applied to any kind of schema (as described by the above criteria). For example, it is possible to establish an authentication service for network access based on smartcards and only using corporate directories and access points, or an LDAP-based service that uses institutional directory servers and allows applications to ask users for their username/password, forwarding it to the authentication service.

3. Authentication Procedures. A Structural Survey

Although the degree of deployment and maturity of the different infrastructures varies very much from one country to another, it is possible to identify four different approaches to authentication procedures inside the institutions served by European NRENs. All of them try to keep authentication data management within the scope of the institutions, while they differ in the way in which data are exchanged to authenticate users, and in the formal requirements and procedures to grant users for authentication accounts. The following sections tries to make a distinction among specific authentication procedures (such as smartcards and the like), more practical approaches using ad-hoc pre-existing methods (there is a great variety of them) and those that combine local ad-hoc methods with some central service.

3.1 Central Authentication Servers

This approach implies the existence of a central server holding all user data (identifiers, passwords, and, possibly, access rights) and has been the common authentication method of the better established AA infrastructure, the Athens AMS in use in the UK, until the so-called "devolved authentication" procedures (that fit into the fourth category described in this document) were implemented.

As said above, to keep authentication management at a reasonable level of complexity, administrative procedures are left to the individual institutions: one (or several) accounts with special privileges are allocated per each participating institutions. These accounts can be used to add, delete or modify data pertaining users at the corresponding institutions.

Obviously, this approach has the appeal of simpler interactions inside the AA infrastructure and the guarantee of unique identifiers. But the drawbacks are also evident: a central point of failure (that can be alleviated by using replicas) and the great loss of privacy for users, whose identity can be tracked by a third party outside their institutions.

3.2 PKI-based Authentication

Although they are not well deployed yet, and their use is often mentioned as a future approach. In those cases (a couple of them) where PKI is mentioned as an actual alternative, its deployment is not reported to be very advanced.

Very few institutions (such as RedIRIS, SURFnet and DFN), although some of them are reported, have a well deployed PKI based on smartcards, not only in

pure technological terms (availability of card readers in campus equipment, crypto libraries, procedures for RA and CA operation, etc.), but also in the sense of a widespread use among their communities (use for library loans, sport facility reservation, etc.). In these cases, the obvious choice for performing user authentication is the combination of smartcard possession and knowledge of its PIN. In addition to the use of a central corporate directory (for certificate revocations, special user management, etc.), this is the strongest approach to authentication currently available in the European Academic Community. Institutional PKIs are usually integrated into national PKIs, either within NRENs or any other structure, like a governmental infrastructure. Policies are well-established and according to the relevant standards in this field.

The usual procedure is the generation of certificates and their storage in smartcards along with the enrollment process of any individual belonging to the institution (faculty, staff, alumni). Enrollment processes are strongly formal and require the presentation of national identity documents (or equivalent: passport or driving license), so user's identity is well established, according with legal regulations, in the moment of generating the certificates. Policies require similar procedures for certificate renewal (because of smartcard damage, loss, etc.) and revocation.

3.3 Authentication Based on Pre-existing Services

The common approach to user authentication in those institutions not running a operative PKI has been to employ a service that requires user identification (typically, by means of an username/password pair) and that was already offered at a institutional level. Examples of these services are LDAP, e-mail access (POP and/or IMAP), and remote network access (via RADIUS). A paradigm of this approach is SURFnet's A-Select, that allows the use of several (currently, 6) different authentication methods, from RADIUS or LDAP, to the use of SMS in mobile phones.

The use of these services, well known to the user community, is a rather pragmatic approach that enables for a real seamless deployment of the authentication infrastructure, allowing users to employ an identification they were acquainted with, and not requiring (ideally) an additional effort on the IT staff. Nevertheless, it shows certain technical and organizational flaws that must be addressed in order to build a reliable authentication system:

- Although the process for including users in these services is usually as formal as in the case above (requiring photo identification with an official document), too many times the procedures for changing its parameters (essentially, passwords) are not so strict as they should.
- In many cases, the inclusion of users for the service used in authentication procedures is automatic and performed at the same time of enrollment, but in some others it is an on-demand service. The extension of the service to general user authentication causes an extra demand that implies an additional pressure

on the people in charge of service management, thus risking the degradation of that service.

- Many of these alternative services do not provide for more than pure binary user identification (users are valid or not), without providing further information about their attributes. This imposes the use of flat authorization schemas, thus compromising the goals of any AA infrastructure. The use of directories, either as authentication method or as a attribute repository, constitutes the simplest solution to this.

3.4 Central Directories plus Local Identity Services

A solution that has been described in several cases consists of the combination of a central directory with local identity services (as described in the point above). The central directory may be constructed as an actual centralized directory service, or by means of a combination of indexing and searching procedures on locally managed directory servers.

This approach is applied in the Athens Devolved Authentication, an attempt for de-centralizing the existing Athens infrastructure, key in the efforts to make Athens interoperable with the other AAI initiatives now being established across Europe. Another approach that fits in this category is the FEIDE project: FEIDE is based on local information in local directories being indexed and searchable, with no central storage of information about users.

This is also the case of the greater PAPI installation in Spain, operated by the National Council for Scientific Research (CSIC). This institution has very special characteristics, notably a very wide geographic distribution (covering almost the whole territory of Spain or one of its parts), and a very much decentralized structure for IT, without any central service. A central directory service (hosted at the infrastructure provider) has been established, including data about users that are allowed to use the authentication system, their affiliation, etc. One of these pieces of information is the local identification procedure and server. When an user wants to use the authentication systems, s/he must provide their identification inside the system. The system will carry out any required procedures at the corresponding identity server to perform user authentication. This is an approach dictated by strict practical reasons, although it has obvious advantages, not only for those institutions with the characteristics described above, but also for very small ones, where there is difficult to find enough resources to start an authentication service.

As in the structures described in the above section, the main advantages are that users continue employing already-known credentials and that it does not impose heavy requirements on the institution IT resources. Furthermore, since a pre-existing service is also used to perform user identification, its flaws are the same as above, although mitigated by the fact that the use of the central directory permits a better control and formalization of user enrollment, and avoids the lack of data about user attributes.

3.5 Wireless Network Access

The common authentication standard in wireless access, 802.1x, defines the roles of a client (called the supplicant), the authentication pass-through component of an access point (the authenticator), and a back-end authentication server. This technology is closely related to another protocol called Extensible Authentication Protocol (EAP), which provides a generic architecture for passing messages among parties.

The way 802.1X works is quite simple: the supplicant provides his/her credential (digital certificate, username and password, etc..) to the authenticator, which transfers this information to an authentication server.

If access is approved, the authenticator hands over a unique per-supplicant master key. When the user has been authenticated, EAP is used to refresh the master key, to reduce the possibility that the packets are intercepted.

As EAP does not have a built-in encryption method, it has to be used in combination with something else, typically Transport Layer Security (TLS) Tunneled Transport Layer Security (TTLS) and Protected Extensible Authentication Protocol (PEAP). The first one TLS is complicated because it requires a client side public key certificate (so basically it is PKI-based). The other two protocols, TTLS and PEAP, are very similar as both of them build a tunnel within an existing tunnel.

Appendix: Responses from NRENs

Country / NREN	Data Provided on Authentication Practices
Spain RedIRIS	<p>Three different approaches for authentication:</p> <ul style="list-style-type: none"> ⓂPKI-based ⓂBased on pre-existing services ⓂCentral directories plus local identity services <p>A project for integrating the AAI infrastructure (PAPI) and wireless access in the Spanish campuses is planned to start in the fourth quarter of 2003. More information at: http://www.rediris.es</p>
Germany DFN	<p>Authentication practices defined by the policies. Before the certificates are issued a staff member has to meet personally with the applicant and check her/his ID-card or Passport. DFN has a combined CP/CPS not RFC formatted. More information at: http://www.dfn-pca.de/certification/policies/</p>
Switzerland SWITCH	<p>Authentication is a local matter for each organization participating in AAI. SWITCH has not collected the details about authentication practices yet, so a detailed report is not available. More information at: http://www.switch.ch/aa1/docs/AA1_Policy.pdf</p>
UK UKERNA	<p>The only national authentication method in use in the UK is the ATHENS system. For details of this please see their web site. At institutional level, the methods of authentication is a policy for the institution. More information at: http://www.athens.ac.uk/</p>
Finland FUNET	<p>Passwords and authentication databases are directly managed by institutions. With respect to PKI, Funet does not have a CA of its own. The few certificates in the (web) servers maintained by Funet/CSC have server certs issued by the Population Registration Center, the CA maintained by the government. Many institutes have an own CA for server certificates. The focus of Feidhe has been not on authentication but on identity management. More information at: http://www.csc.fi/suomi/funet/middleware/english/gnomis/slides/gnomis_HAKA.ppt</p>
Greece GRNET	<p>No established authentication infrastructure yet. There are plans to set-up a PKI for authentication purposes</p>
Sweden Sunet	<p>There is no centralized authentication practices and policies in Sweden. All users that uses Sunet must be identifiable by the local HEI, which have their local policies and practises.</p>
Poland	<p>A 2-years project, "Deployment of LDAP service in Polish academic network" will be finished in August 2003 and is mainly focused on using LDAP service for authentication in network services. Using LDAP and PAM for authentication opens broad possibilities to extend network services in multi-servers environment without the need to copy user credentials between servers. LDAP authentication is used for granting permission to network resources in Web and Samba services as well.</p> <p>Within the project entitled "Building Trust in networking in Newly Associated States through the use of secure information society technologies (NASTEC)" in the 5-th Frame Programme of European Union in which the Technical University in Wroclaw is taking part, The Polish EuroPKI Certification Authority has been established (http://www.europki.pl).</p> <p>Within the Polish Research Community there is a strong need toward newer and more secure AA mechanisms. Therefore a project is planned which will take many possible aspects into consideration and will be mostly focused on building common infrastructure for authentication and authorisation. The PKI environment will be tested and used, but only as one of authentication and authorisation methods and as a platform to experiment, not as the base of this project. The results from PSNC</p>

Country / NREN	Data Provided on Authentication Practices
	<p>projects will be adapted with the aim to make these solutions universal for the academic community.</p> <p>The evaluation of free products to support authentication and authorisations, as PAPI and Shibboleth is planned as well.</p>
Czech Republic CESNET	<p>Distributed authentication services in CESNET are based on pre-existing services (NetWare, Kerberos, LDAP).</p> <p>The "origin sites" provide for basic authorization for individual services. The authorization process is "hidden" (its result is provided as a result to the authentication request).</p> <p>The registration and attribute setting/changing policies are not dealt with.</p>
Netherlands SURFnet	<p>As far as we know no institution is doing smartcard-based authentication. There have been attempts to do this on a national scale for higher education in the mid 90's, but this has failed horribly.</p> <p>Most organizations use username/password based authentication. SURFnet has started pilots for authentication with one-time passwords via SMS and using authentication that uses the chip on banking cards with a random reader.</p> <p>In the Netherlands, all banking cards have a chip on it, and this is used with a standalone device for a challenge-response when internet banking. SURFnet uses the Internet banking authentication as a service. This is currently deployed on two sites.</p> <p>Using the A-Select authentication middleware organizations can choose 6 types of authentication, namely:</p> <ul style="list-style-type: none"> - username/password from a RADIUS server - username/password from an LDAP server - SMS via GSM - Banking card - Software certificates - IP address <p>What we see is that username/password from LDAP or a relational database is used in most cases. An interesting observation that we have made while deploying and promoting the A-Select infrastructure is that the single sign-on aspects and the migration path to stronger forms of authentication is more important to organizations than the actual authentication method.</p> <p>The need for stronger forms of authentication is recognized but the single sign-on aspects seem to have more priority.</p>