

Distr.
GENERAL

CES/SEM.47/10
19 March 2002

ENGLISH ONLY

**STATISTICAL COMMISSION and
ECONOMIC COMMISSION FOR EUROPE**

**COMMISSION OF THE
EUROPEAN COMMUNITIES**

CONFERENCE OF EUROPEAN STATISTICIANS

EUROSTAT

**Joint UNECE/Eurostat Seminar on Integrated Statistical
Information Systems and Related Matters (ISIS 2002)**
(17-19 April 2002, Geneva, Switzerland)

Topic II: Secure communications and data confidentiality

**SOME LESSONS LEARNED FROM THE
IDA PUBLIC KEY INFRASTRUCTURE PROJECT**

Contributed paper

Submitted by Eurostat¹

***Abstract:** Member States governments are currently implementing security solutions based on public key infrastructures (PKIs). The main objectives are to provide authentication of identity, integrity of information, non-repudiation and security of communications. The IDA programme of the Enterprise Directorate General of the European Commission has operated a PKI since 1998. The purpose of this presentation is to highlight the problems that currently exist in the area of PKI technology. These shortcomings will be based on the practical experience to date of the IDA PKI, and not on theoretical criticism of the standard PKI model (i.e. on X.509 v.3 architectures). Also functional requirements for improved PKI services will be presented. Again these will be based on business requirements that we have identified in the IDA programme and not on theoretical shortcomings of the PKI model.*

I. IDA (Interchange of Data between Administrations)

1. The IDA programme is a strategic EC initiative for 1999 – 2004. Its mission is to coordinate the exchange of information between Member States and the European Commission, as well as between European Institutions, to support the management of the single market, the Community decision making process, and the implementation of a wide range of Community policies, in areas such as agriculture, employment, the environment, statistics, and health and consumer protection, that affect Europe's citizens and enterprises. More information on the IDA programme can be found on the IDA web site at: <http://europa.eu.int/ISPO/ida/>.

¹ Prepared by Paul Murphy (Paul-E.Murphy@cec.eu.int).

The IDA PKI

2. The IDA Public Key Infrastructure for Closed User Groups project (PKI CUG) was launched in 1999. It provides certification services to the members of IDA projects of common interest to exchange information by electronic means securely between Member States, the European Commission and European Institutions.

3. The IDA PKI currently issues server-level, functional, personal and qualified personal electronic certificates. These are used in TLS/SSL and S/MIME v2 applications. Trials of electronic signatures are currently under way. All sectoral networks using an infrastructure able to exploit X.509 certificates can potentially use the IDA PKI. Certificates issued by the IDA PKI for use in a closed user group can also be used in other sectoral projects provided that the administrator of the other network agrees.

II. THE PURPOSE OF THIS PRESENTATION

4. The purpose of this presentation is not so much to describe the IDA PKI, or to present the technical challenges we had to overcome in its implementation. The allocation of time and resources will solve most technical problems. In implementing the PKI, IDA has come across several situations where the business requirements of users do not exactly match with the PKI model. By business requirements here, I mean the way work is actually performed and the way organizations communicate. PKIs are the foundation of electronic ways of working, be they in the private (e.g. e-commerce applications) or public (e.g. e-government services) sectors. Unless these issues are identified and solutions, which need not necessarily be technical solutions, are provided there is a real risk that the lack of congruence between PKIs and operational realities may imperil the roll out of e-services.

5. It should also be pointed out that the IDA PKI operates in an open environment more akin to e-business. We have no control over the technical architectures used by our business partners in the Member States. Many of the problems mentioned below may not exist or may be solvable if you implement a PKI in a single organization, where you can control products, people and processes. This is not the situation within which IDA operates.

Basic requirements for PKIs

6. PKI solutions must comply with various technical specifications for electronic certificates, communications protocols, encryption suites etc. But, at the business level, for PKI solutions to gain widespread acceptance they must:

- provide a real business benefit;
- be cost effective;
- be as easy to operate as their paper-based equivalents;
- be useable by people with little or no training in PKI technologies;
- interoperable;
- work 'out of the box'.

7. A well-defined legal framework is also essential (i.e. it should establish confidence with the electronic signature and provide a true offset to liability).

8. If the above conditions are not met it is unlikely that PKI technologies will gain widespread acceptance outside of large organizations and enterprises. This also means that the benefits of PKIs for the economy as a whole will not be realized and it will make e-business solutions more difficult to implement.

III. PROBLEMS WITH PKIS

9. Let us now examine some problems found with PKIs as they are implemented today.

Problem 1. Authentication and confidentiality

10. Current S/MIME v2 solutions use one key pair for both authentication of identity (i.e. electronic signature) and for confidentiality (i.e. encryption). However, one key pair solutions are not a real solution as you cannot escrow the private confidentiality (i.e. encryption) key. If you do this you cannot have a qualified electronic signature, under the terms of the Electronic Signatures Directive, as the private key is not under the exclusive control of the signatory. You cannot have non-repudiation of transmission for the same reasons. Also one key solutions leave you potentially open to fraud in certain situations where false web servers / malicious code substitutes a signing operation for an authentication operation.

11. You can use two key pairs in S/MIME v2 as you can indicate the functionality of the key by selecting the usage bits in the certificate, but these are not processed in a standard manner or not processed at all. Therefore, it may be possible to implement multiple key pair solutions in house or in other situations where you have control over the technology, but not in the typical e-business environment.

12. Two or multiple key pair solutions also present problems. One relates to the lack of product support and interoperability problems. S/MIME v3 implementations have tended to focus on the use of Cryptographic Message Syntax (CMS) to negotiate encryption suites and not on the support of multiple key pairs. Where this occurs the interoperability problems may occur. This makes life difficult if you are trying to implement PKI solutions in heterogeneous technical environments.

13. If you are implementing a PKI in-house this is not a major problem as you can standardize on a particular product. But if you are dealing with customers and have no control over their technical environment, interoperability problems will occur.

14. Another problem is that X.509 v3 certificates do not support multiple public keys. A key holder must have multiple certificates. This increases the complexity of system design to ensure that the correct certificate is selected. It also makes life extremely difficult for the end-user, in situations where they must select the correct key.

Problem 2 Scalability

15. Do PKIs scale? For the technology the answer clearly is 'Yes'. For the procedures the answer is '?', possibly 'No'.

16. While the PKI technology is scaleable, the organizational model (e.g. Registration Authorities, Local RAs) may not be. In particular, if staff move frequently between organizational units, or if their roles change the administrative burden of large numbers of staff having their certificates revoked, their identity re-validated and new certificates issued will hinder the implementation of PKIs in large organizations.

17. Registration procedures are relatively easy to handle in small pilot projects, but if you have to roll out these procedures, which, by definition, are well-defined and must be strictly adhered to, to cover thousands of

employees this presents new challenges. If employees change roles and acquire new responsibilities, which occurs frequently, their certificate may need to be revoked and another issued. This is particularly important where possession of an electronic certificate defines the access rights the holder has to system resources. I think we need to reflect on the administrative overhead involved in this.

18. If attribute or role-based certificates were available, this problem would be largely solved but these are not available at present. (By 'available' I mean available as standards-based products that are interoperable with similar products from multiple vendors). But even attribute certificates present new problems, with many experts recommending the establishment of parallel Privilege Management Infrastructures to manage the attribute certificates.

19. Scalability may also be a problem, in terms of the administrative overhead required to issue, renew and revoke certificates, if these are issued at the level of society (i.e. to citizens, to enterprises, to people playing a specific and possible volatile role within an enterprise (e.g. the company secretary, the legal representative, etc.)).

Problem 3 –Certificate Policies

20. Certificate policies state the conditions for use of an electronic certificate in creating electronic signatures. The problem with this is that checking the certificate is at present:

- a non-automatic process; and
- certificate policies vary between organizations and Member States.

21. The entitlements of one Class III certificate may not be the entitlement of another Class II certificate. Also, certificate policies tend to focus on the registration process for the identification of the certificate holder. These also vary, but more importantly, place the burden of acceptance of the signature on the signature recipient who may have no idea of what the implications of the various registration procedures entail.

Problem 4 - Interoperability

22. IDA has carried out two studies on interoperability issues relating to S/MIME v2 e-mail exchanges. The results were not particularly encouraging. Only certain products, mainly the market leaders, provided an acceptable degree of interoperability. For others the results were poor or variable. And these were relatively simple interoperability tests. They did not, for example, attempt to follow certification paths, access X.500 directories, or use LDAP, etc.

23. I will not go into technical interoperability issues today – that is a presentation in itself - but simply say that once you are working in a heterogeneous technical environment you currently have interoperability problems, even when you are dealing with standards-based products.

Problem 5 – The way people and organizations actually work

24. While consumers are clearly individual economic agents the same cannot necessarily be said for enterprises or public administrations. Business is generally carried out with the Sales Department of Company Y, you apply to Unit Z of the Taxation Authorities with your tax returns. While a decision on your eligibility for a government subventions may be decided by Mme X, it is in their role as deciding officer and not as an individual that their decision has legal validity.

25. We have a combination of requirements here. The first is for role-based certificates as mentioned above. The second is for 'functional certificates', i.e. electronic certificates issued to a business or organizational unit and not to an individual.
26. Functional certificates, i.e. where the certificate holder is a business function (i.e. the Sales Department, the IDA unit of DG Enterprise, etc) are needed to provide security of communications. You need a certificate on the mailbox to which you are sending your e-mail to encrypt it.
27. However, the use of functional certificates gives rise to additional problems. For example, business functions and organizational units are not legal entities. Therefore, they cannot obtain personal certificates. Functional certificates can support integrity of information and security of communications. They cannot support non-repudiation and electronic signature.
28. However, there is no agreed way in which functional certificates should be issued. For example, even though the business unit is not a legal entity there still should be some 'registration procedure' (perhaps requested out by the manager of the business unit) to ensure that an evidence trail exists showing the request for the functional certificate by authorized personnel.
29. The main problem here is that the PKI model is based on the concept of personal certificates and does not include a framework (e.g. best practice registration procedures, recommended certificate policy, etc.) for shared functional certificates. But this is a major omission as business is typically carried out with business units and not named persons within organizations.
30. Role-based certificates (or attribute certificates) are required for two reasons:
- in many cases a business event is not valid even if it is signed unless the signatory has the authority to transact the business event;
 - in certain situations it is the role and not necessarily the identity of the signatory that determines the validity of a business event;
 - personnel moving rapidly between organizational units should not have to have their entire identity re-validated on such a move. An authentication certificate, authenticating their identity, should be formally issued. This should be supported by locally issued role-based certificates of short duration.
31. However, X.509 v.3 certificate extensions are unlikely to meet these requirements:
- they are, in essence, customized free text making an explicit declaration on the role. In this that are non-standardized. This can give rise to interoperability problems and perhaps language problems.
 - software may reject the certificate or may fail unless it is explicitly programmed to treat certificate extensions.
32. The main problem here really is that at present role-based certificates do not exist (i.e. interoperable standards-based interoperable products with market acceptance are not available from multiple commercial vendors).

Problem 6 – Other problems

33. There are a wide range of other problems, far too numerous to go into today. These include:
- Directory and discovery problems, i.e. not so much problems in accessing directories but in discovering a particular public certificate or CRL;
 - Trust relationships. This is a major problem. Currently you have no way of establishing a trust relationship if you receive an electronic certificate signed by a CA other than your own, or a CA with which it is cross-certified. The problems here relate both to the technical ability to follow a certification path and also to cross-certification issues.
 - Certificate revocation status checking. Problems here include non-automatic procedures for checking certificate revocation status information and, on occasions, the low frequency of CRL update. In the near future we should be able to use OCSP to give revocation status but this does not establish trust, unless you are cross-certified with other CA.

What have you achieved in implementing a PKI?

34. What have you achieved if you have introduced a PKI? Well, you've introduced a PKI. Implementing a PKI is only the start of a series of activities (all of which present new challenges / problems).

35. Like many other business activities, PKIs are introduced to:

- reduce costs or increase profits;
- increase operational efficiency;
- allow organizations to be more effective in achieving their objectives;
- provide value added services that cannot be provided with paper-based ways of working.

36. Unfortunately, introducing a PKI is just the start of a long process required to meet these aims. To obtain the benefits of electronic ways of working you need:

- improvement in the way of working with business partners (e.g. ebXML);
- records management solutions to ensure that your information holdings that are now all / mostly electronic are properly managed;
- improvement of business processes as you are no longer constrained by processes dictated by paper. This may also involve organizational change;
- to introduce knowledge management systems because information that was previously 'locked away' in paper documents is now easily accessible in electronic form.

But there are new challenges / problems presented by each of these areas.

IV. CONCLUSION

37. To sum up:

- PKI solutions present a wide range of challenges. These relate both to technical problems but more importantly to non-congruence between the PKI model and the way business is carried out.

- Most importantly, for PKIs to operate in a business situation where business partners have no prior knowledge of each others' technical configurations (i.e. in typical e-commerce applications) you need standards-based interoperable products from multiple suppliers. This is not the situation today.
- Also, when you implement a PKI there is another set of challenges that must be overcome before the full benefits of electronic ways of working can be achieved.

38. The concluding point is that implementing PKIs, especially where they must interoperate with the PKIs of business partners outside of your organization, presents a series of challenges. Simply implementing a PKI to replace paper-based mail with secure and authenticated e-mail is unlikely to justify the investment required. However, the use of a PKI with other related technologies will allow the introduction of new ways of working with customers, the improvement of business process and the potential to introduce new types of value added services. It is these latter aspects that justify the PKI investment.