

Distr.
GENERAL

CES/SEM.47/12 (Summary)
5 February 2002

ENGLISH
Original: FRENCH

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

PUBLIC KEY INFRASTRUCTURE USE AT INSEE

Invited paper

Submitted by the National Institute of Statistics and Economic Studies (INSEE), France¹

SUMMARY

1. Like any statistical office, INSEE collects, processes, stores and disseminates large amounts of data, and for that purpose has to support many different information flows with a wide range of partners. These data and information flows require services offering various forms of security, including data confidentiality and integrity. In particular, the secrecy of some kinds of information is guaranteed by law.
2. With the dematerialization of exchanges, fundamentally new questions of security have to be addressed: relatively informal systems of confidence, such as those based on the written word and postal or telephone services, will need equivalents in the digital world, and electronic certification techniques are certain to play a key role, in this change.

¹ Prepared by Franck Cotton (franck.cotton@insee.fr).

3. INSEE has therefore decided to invest in such technologies to keep pace with ongoing developments in French society as a whole and especially in public administration. The national context is marked by the incorporation of the EC Electronic Signature Directive into French law, a process that is currently under way, and also by numerous State initiatives taken under a Government plan announced in 1998.

4. These initiatives notably include action by the Ministry of Economy, Finance and Industry, to which INSEE belongs, to implement a very voluntarist policy on developing “teleservices”, the largest enterprises now being required by law to declare and pay their VAT on line.

5. Under this policy, rather than itself attributing certificates to enterprises, MEFI has developed a system of accreditation of external certificates based on a standard certification policy combined with a process of evaluating certification services. This initiative has contributed greatly to developing the market, and there are now about twenty commercial certification service providers in France, most of them being banks.

6. INSEE, for its part, naturally follows MEFI policy. An internal public key infrastructure (PKI) has been established and various applications using certification techniques have been developed or are being studied. A number of guidelines have been laid down to provide for new developments in this fairly new area.

7. As regards strictly internal needs, it is intended to use INSEE’s PKI to certify staff and information resources. In particular, the Institute has recently improved the formalization of its data classification policy; in this new framework, only persons strongly authenticated (with a certificate and smart card) will be able to access data under high protection. File encryption services supported by the internal PKI will also be employed.

8. To meet the requirements for secured exchanges with identified partners, especially information providers, INSEE gives precedence to solutions involving the accreditation of external certification systems. By way of example, reference may be made to a project now under way to assign identification numbers (SIREN numbers) in real time to newly created enterprises. This necessitates establishing secure links with the enterprise registration centres to which enterprises apply to complete their respective administrative formalities (for example, chambers of commerce and industry, or trade or professional chambers). In this connection, INSEE provides guidance on the establishment of certification systems for these centres by their supervisory bodies.

9. However, in some cases, and as an interim measure, INSEE is itself having to certify those partners whose certification schemes are not sufficiently developed. For example, as part of a pilot project for on-line transmission of civil registry data, the Institute plans to attribute certificates making it possible to authenticate the town councils taking part in the experiment: a certifying authority has been created for that purpose within the internal PKI framework. Nevertheless, it is not part of INSEE’s mission to act as a body responsible for certifying town councils, and some systems run by the Ministry of the Interior are in any case now being set up: when the project reaches the actual delivery stage, it is these systems which will be used.

10. Regarding its own needs for communication with the general public or enterprises, INSEE is making use of commercial certificates for its servers: this is being done in particular to secure its electronic commerce web sites or sites for retrieving information from some enterprises surveyed. On the other hand, strong authentication is not for the time being planned for customers: both in the examples mentioned above and in the Internet survey projects currently under way, password authentication seems to be sufficient.

11. Nevertheless, there will clearly be a need to cater quickly for requests from customers or respondents wanting their security level to be increased and to be authenticated with a certificate. In particular, enterprises supplied with a certificate recognized by MEFI for paying their VAT on line may legitimately ask to use that same certificate to respond to an INSEE telesurvey. In anticipation of this demand, INSEE is taking part in MEFI discussions on the implementation within the ministry of mutually agreed certificate validation services, as it is essential for MEFI accreditation policy to be translated into uniform practices relating to acceptance or refusal of certificates in all services.

12. More generally, INSEE is for its part contributing to the various discussions under way, in particular on the organization of certification services within the State system. It can draw on its theoretical and practical expertise in the definition of concepts, identification or naming and other services vital for the success of electronic certification systems. Many new developments can still be expected with regard to the dematerialization of exchanges, and any organization whose mission is to handle information, as is the case with a statistical office, is bound to find itself at the centre of these changes.
