STATISTICAL COMMISSION and
ECONOMIC COMMISSION FOR EUROPE

Working Paper No. 13
English only

CONFERENCE OF EUROPEAN STATISTICIANS

Joint UNECE/EUROSTAT Work Session on Electronic Data Reporting
(Geneva, Switzerland, 13-15 February 2002)

Topic (ii): Security, confidentiality and privacy issues

SECURE COMMUNICATIONS IN THE NATIONAL STATSTICAL INSTITUTE OF ITALY

Submitted by ISTAT, Italy [1]

Contributed paper

ABSTRACT

Statistical production has changed in parallel with information technology (IT) evolution. In the past it was based on paper: information was collected on paper and processed by large systems with terminals. Only recently has digital information begun, in some cases, to replace paper publications. At the same time the IT environment has changed, introducing network centric architectures and permitting the introduction of new methods of data collection, processing and dissemination. New technologies offer opportunities to grasp new challenges, to offer new services to customers or to improve statistics quality. But the risk connected to these new technologies increases with the necessity of new and stronger security measures.

In this paper three examples of security solutions adopted in the National Statistical Institute of Italy are given. The Secure Regional Network of ISTAT, based on the frame-relay network of the Public Administration, uses an IPsec solution to improve strong authentication between the trusted entities (Regional offices or single users in some Provincial offices) and the headquarters of the Institute. The Secure Interviewers' Network, the second example, has been designed, tightly integrated into the Regional Network to conduct the continous EU Labour Force survey and the consequent development of the interviewers' network. This solution is based on the use of IPsec clients and smart-cards with X.509 digital certificates given to the interviewers who carry out the face-to-face interviews to the households. The third one is the development of a Public Key Infrastructure with an internal CA planned for the next year, to introduce new methods of access control, a wide use of digital signature for the internal personnel and to enforce security on communications with the exterior.

We consider these solutions a basis on which to build a security infrastructure for the flow of data between entities involved in statistical processes, but at the same time we don't believe they are the only solution to the security needs.

I. INTRODUCTION

1. The National Statistical Institute of Italy (ISTAT) is a research Institute in which researchers represent an important motivation for innovation in statistics and in IT.

2. ISTAT, with its 1900 employees and 600 researchers, evenly covers all Italian territory, divided into 18 regional sites and 8 sites in Rome: this is not a functional choice but rather one justified by the

[1] Prepared by M.I. Balla, C. Catalano and A. Guarino.

increase in personnel in the past. This distribution in the capital city represents a point of complexity for the IT infrastructure, which has been affected by the changes both in IT and in statistical production. Statistical production has changed parallel with IT evolution. In the past it was based on paper: information was collected on paper and processed by large systems with terminals. The output was only on paper, such as publications, books, tables and so on. Recently floppy disks and CDs have begun to be associated with paper, to complete but not to substitute for paper publications.

3. The IT environment has changed, introducing network centric architectures. So paper data collection has been gradually replaced with a collection made in digital format, which can be directly processed by production sectors. The output has changed too, favouring digital publications such as CDs, dissemination via the web, or e-books.

4. In the future digital information will be the main method used, and paper will only represent a useful copy, while the same dissemination on Internet is changing from a static representation of data, to which users have to adapt, to dynamic information that will follow the users' requests.

5. Table 1 shows the evolution of statistical processes in the three phases of collection, processing and dissemination of the statistical information. You can see how paper has been gradually, but at the moment not completely, replaced by digital information.

	From	**To**
Collection	Surveys/Questionnaires on paper	Public registers, administrative archives / Electronic questionnaires
	editing by hand	CAI, CASIC, primary and secondary EDI
Processing	Sequential by survey	Integrated to produce systems from surveys and public registers
Production of information deposits	Sequential data files from surveys	Integrated databases for large populations individuals/families, factories/industries
Dissemination of statistical information	Dissemination on paper	Data-warehouse, dissemination of databases for paper and e-publishing.

Table 1 – Evolution of statistical processes

6. Another important element of the evolution of statistical processes is the increasing trend to use administrative archives and public registers to collect data, and from them to develop databases of virtual respondents for large populations.

7. Because of this trend and also because of the development of integrated databases of data and metadata and of dissemination databases built to deliver static or dynamic information, the entire cycle of the production of the statistical information is changing.

II. IT EVOLUTION IN ISTAT

8. ISTAT has gradually adapted its methodologies and its IT and telecommunications infrastructures. In the years 1996-1999 ISTAT changed IT architecture from a host centric system (2 Mainframes VM - MVS - SNA network - 3270 terminals) to a network centric one. In Table 2 are shown

some interesting steps made in ISTAT in the recent past up to December 31st 1999, the date on which the old centralised systems were disengaged.

October 95 - March 99	Installation of new hw & sw systems (AIX, Oracle, SAS, Windows client).
February 96	Istat on the WWW internet.
April 97	Workshop on IT security in Istat.
November 97	Internal seminars on RSA, digital signature, authentication.
May 98	First applications of electronic certificates using digital signature.
July 98 - December 99	Complete transfer of the applications into new systems according to Y2K and Euro.
December 31st 99	The old centralised system was disengaged

Table 2 – Steps of technological evolution in ISTAT

9. At the moment the IT system consistence, based on AIX servers, Oracle DB, SAS and Windows Clients, is the following:

- ?? 1 SP server (6 nodes)
- ?? 35 UNIX servers
- ?? 306 UNIX Workstation
- ?? 2300 PC Windows/Linux

} ??5 TB

10. The ISTAT network (Fig. 1) is composed of a Metropolitan Area Network in Rome (from 256 kb/s to 2 Mb/s), which connects the Local Area Networks (LAN) of all the ISTAT buildings and a Wide Area Network (WAN), connecting the LANs of the Regional offices to the head-office in Rome, based on the Public Administration (PA) network. In this way, all the sites have access to all the services available on the ISTAT network.

11. The communications towards the exterior are based on two input/output gates that collect separately the traffic to/from Internet and the traffic to/from certain public and private organisations. The two points of communications are protected by firewall systems that control access from outside to the servers in the Demilitarised Zones (servers for specific functions and users on one side and public servers on the other).

12. The communications play a fundamental role in the phases of statistical production (data collection, dissemination and delivery), because ISTAT is in the middle of a large network of information exchange, with two main organisations (Eurostat and SISTAN, which is the National Statistical System of Italy) and some other entities.

13. In this context of communications among different actors, opportunities given by new technologies are very important and new challenges offer new services to the customers or improve statistics quality. But it's essential to evaluate the risk connected to these new technologies, because a non-evaluated risk can also damage the image of the Institute.

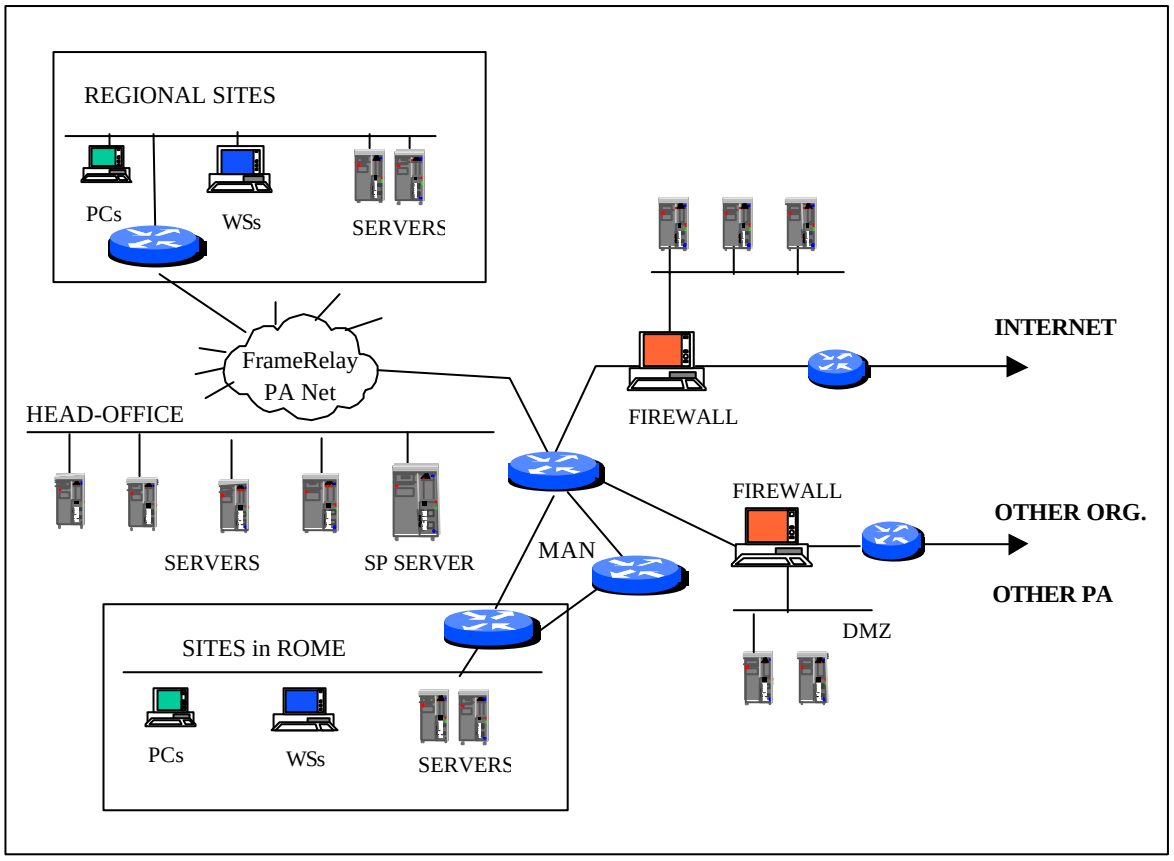

Figure 1 - IT infrastructure

14. If we consider the evolution of the IT technologies - and the consequent growth of new opportunities - we can show, as in Figure 2, that the connection in a closed environment such as a LAN has evolved to the present techniques of e-commerce, opening more and more services to the customers, but at the same time the increased risk necessitates new and stronger security measures.

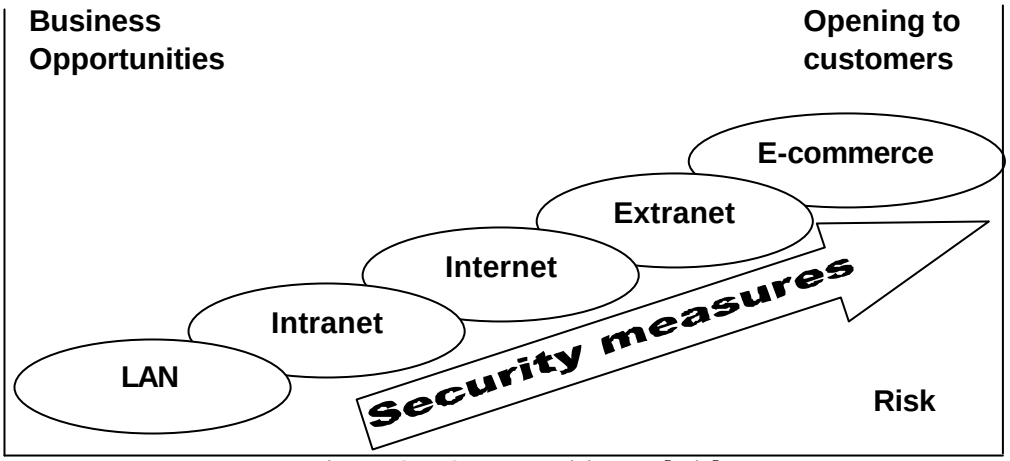

Figure 2 – Opportunities and risks

15. In fact, traditionally security has been seen as a protection of the IT system boundary, with rules which allowed internal users to access external resources, and at the same time denied any access from outside. New functions override such a vision and security is evolving into a policy of authorisation

where external users can access internal services and resources. This is possible only if the security level increases covering authentication, integrity and privacy.

16. The answers may come from the standard IPsec and the Public Key Infrastructure (PKI), which allow the development of a Secure VPN to protect the Intranet and to open it to extranets.

III. EXAMPLES OF SECURITY SOLUTIONS

III.1 The Secure Regional Network

17. The design of the Secure Wide Area Network of ISTAT had to deal with two different kinds of requirements. On one hand, because the network is based on a public frame-relay network, the connection with the ISTAT Regional offices requires the introduction of authentication and privacy services between the border routers. On the other hand, to allow the connection to our head-office of some users connected to untrustworthy networks in provincial offices, it is necessary to introduce encryption of the connection and user authentication.

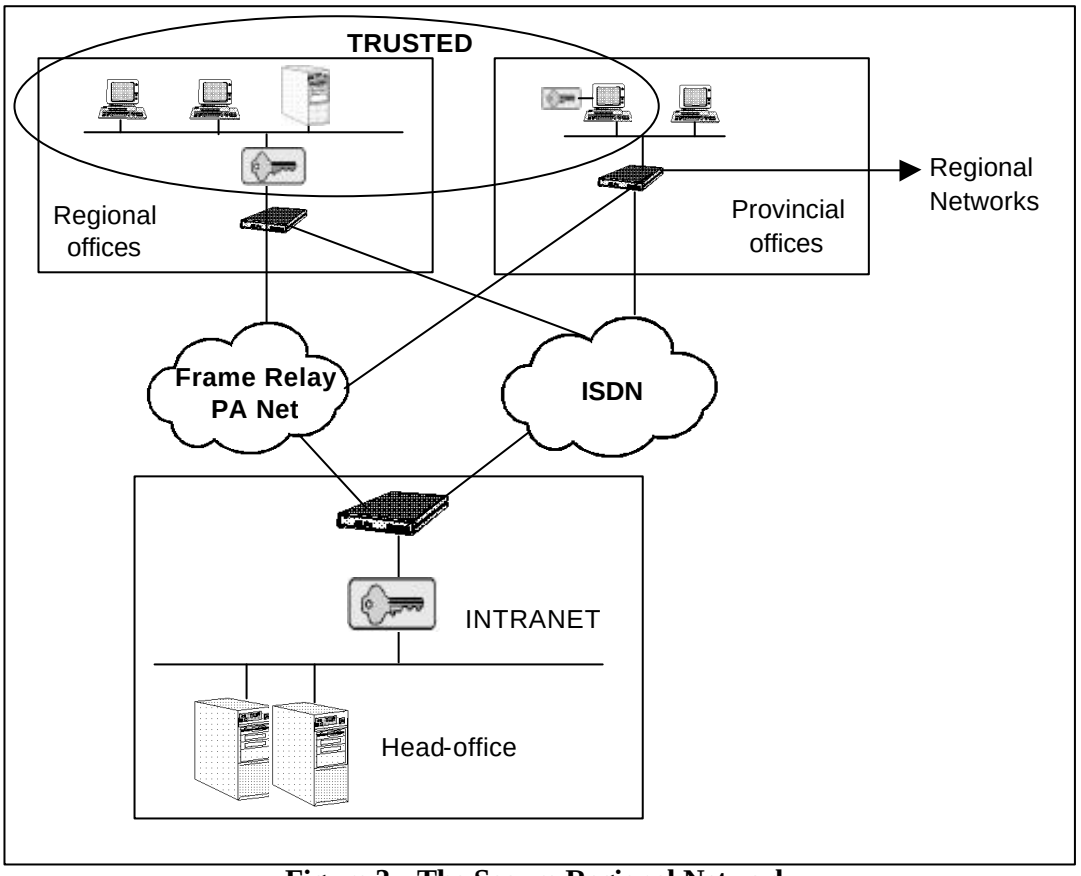

Figure 3 - The Secure Regional Network

18. In both cases the IPsec standard has been used: in gateway-to-gateway mode for the Regional offices and in host-to-gateway mode for the Provincial offices. In this way the security services are completely transparent for the Regional offices users, while the others need to authenticate themselves to establish a connection to ISTAT, but at the same time they can continue to use their own network and its services.

19. The solution adopted (Fig. 3) is based on the introduction of a security server at headquarters dedicated to the authentication and encryption of the communication with Regional and Provincial

offices. In the Regional offices, IPsec systems have been added to the routers, while in the Provincial offices IPsec clients have been installed on the PCs of trusted personnel, using smart-card for security matters. The X.509 digital certificates used in the secure communications are issued by an internal Certification Authority (CA).

20. The technical characteristics of this solution are the following:
- ?? hardware random number generation;
- ?? private key based on RSA 1024/2048 bit;
- ?? encryption 3DES with key up to 192 bit.

21. This solution is based on the separation of the routing functions from the security ones, making them completely independent from the communications matter and allowing to change the network without involving security.

22. The solution based on the hardware level allows:
- ?? more availability because the security functions are controlled on specific equipment;
- ?? best performances because difficult operations, like the encryption, are made separately from the communication ones;
- ?? easier management, different groups that can more easily isolate different problems.

23. On the basis of separation between routing and security functions, the Secure Intranet of ISTAT is ready for future evolution to a broadband network for the integration of data and voice.

III.2 The Secure Interviewer's Network

24. A first example of utilisation of these new technologies, shown below in Figure 4, is the new method of conducting the continuous EU Labour Force survey and the consequent development of the Interviewers' network.

25. It has been necessary to review the methodology of this survey in order to answer a European recommendation, which requires a survey throughout the year. At the moment we are developing a prototype of the system and we have planned its complete implementation for the first half of 2002.

26. The different actors who participate in the survey are:
- ?? 350 interviewers who carry out the "Computer Assisted Personal Interviewing" (CAPI) face-to-face interviews of households and send the information to the head-office;
- ?? the regional supervisors who monitor the interviewers' activities;
- ?? the head-office, which manages the entire network, receives and processes the information and sends to the interviewers the lists of new households to be contacted.

27. The entire flow of information on the network requires strong-authentication of the interviewers and the head office, integrity and privacy, because the information sent to and from the head office is confidential.

28. The solution is tightly integrated into the Secure Regional Network of ISTAT. Each interviewer has a notebook with an integrated modem and a smart-card where keys and the X.509 certificate, issued by an internal CA, are stored. On the PC an IPsec client for authentication and encryption is installed. At the head-office level there is a Remote access system and an IPsec server dedicated to client authentication and to code/decode the information. When the interviewer ends his interviews he needs to send them to the head-office and to collect new addresses. He can do it indifferently by PSTN or ISDN or with a mobile phone. After the phase of in-depth authentication with the control of the Certificate Revocation List, the interviewer is connected to an internal server CAPI and directly transmits and

receives information in a strong secure way. A test for the use of transmission via GPRS has also been planned.

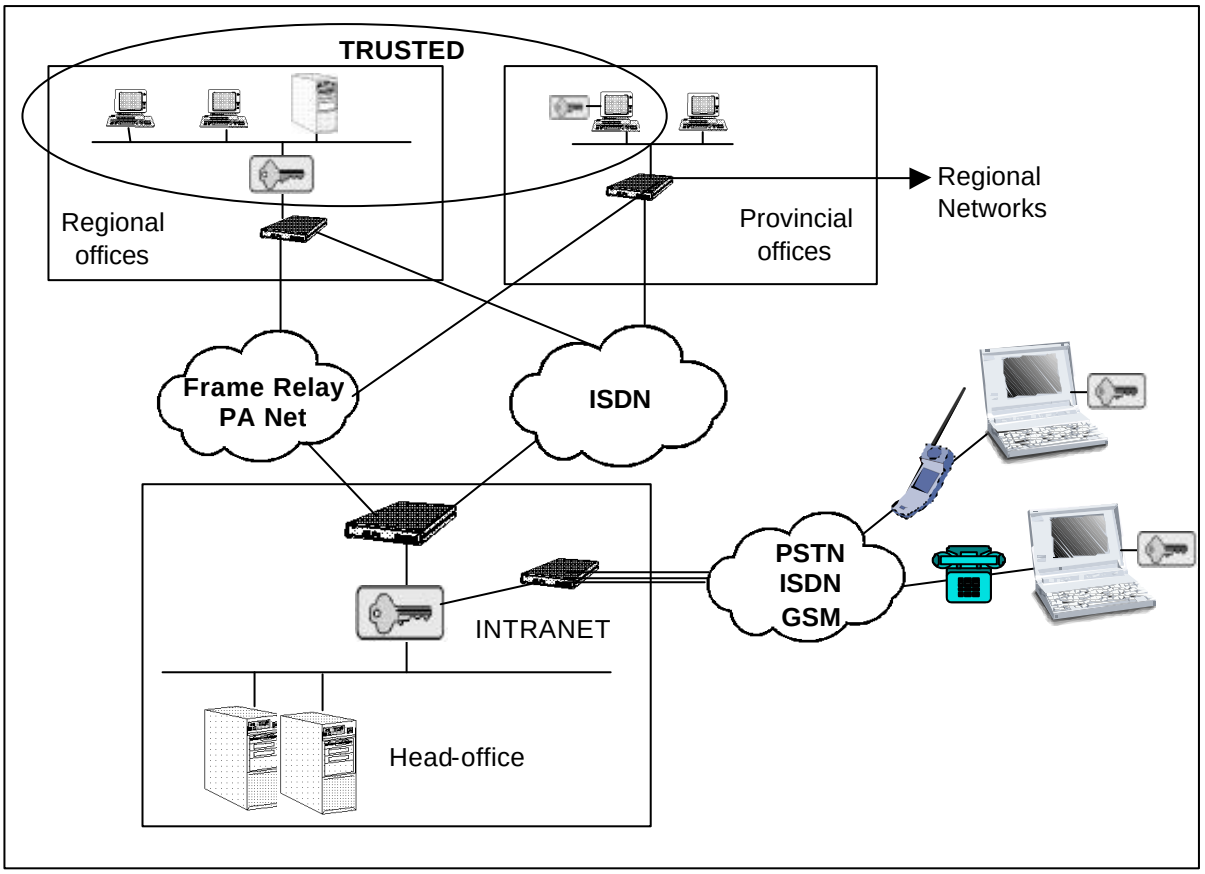

Figure 4 - The Secure Interviewer's Network

29. The interviewers' network is a useful test field for new security techniques because there are some interesting problems peculiar to remote users working in the field, who can only be contacted with difficulty.

30. The management of such personnel needs to define precisely the persons, distributed over the whole territory, delegated to contact and control them. And at the same level there is the problem of the smart-cards distribution and substitution in case of failure or change of an interviewer. We have chosen our Regional offices for the role of Registration Authority, because they have a regular distribution on Italian territory. They will have ready but not active smart-cards to give personally to the interviewers in the above-mentioned cases.

31. One of the greatest problems is the security awareness of the interviewers. Far from the head office and its control, they might not pay attention to data confidentiality and to security, for instance leaving the smart-card in the PC or even writing the PIN on it, making any security measure superfluous. The Regional offices are also responsible for contacting households for confidential information, in which role they represent the whole institute, with its image of total confidentiality. It is for this reason that education on security aspects becomes vital, essential before the production starts.

III.3 Digital signature

32. Another important aspect of use of new security technologies is the data exchange with other organisations and generally all exterior relations of the institute.

33. One of the most important phases is data collection, for which an increasingly large number of actors send data to ISTAT through the Internet to make the respondents' activities and their transmission systems as easy and friendly as possible. There are different methods for data-collection (WEB-form, FTP, E-mail, etc.), but once again the problems are the same: we have to ensure authenticity, integrity and privacy for confidential data.

34. The solution that our Institute considers the most viable at the moment is the development of a PKI that ensures the requested level of security. This solution may not be the only security solution but it can represent the basis on which to develop other services and products.

35. Such a solution can present not technical but organisational problems. Those previously mentioned relating to our 350 interviewers can rapidly expand when the number of the users increases to 25.000.

36. In ISTAT there is a project for the introduction of a PKI both for internal activities and for data exchange with the exterior.

37. In order to better understand what we have planned, it is necessary to briefly explain the Italian legislation on digital signature.

38. In Italy digital signature is completely legal and now digitally signed electronic documents have the same value as those signed by hand. The Authority for IT in the PA has recently decided to distinguish between interior relations and legal documents. Concerning interior relations, and not legal relations with others, a PA can use a "Weak signature". This involves the possibility to use different media to store keys and certificates and the possibility to have a private CA, without following the strict rules of the public CA.

39. For legal documents, the use of the "Strong signature" following all the rules of the Authority is of great importance. Smart-cards are necessary to store key and certificate and the signature must be certified by one of the Italian Certification Authorities, at present twelve of them.

40. Following these rules, ISTAT intends to realise an infrastructure of Digitalcertificates for the purpose of data exchange with other organisations and to allow access from the exterior to Web applications for authorised persons.

41. The PKI will also involve the entire internal personnel in order to introduce new methods of access control and a wide use of digital signature in order to automate the document flow management. For this reason we are planning to create and manage our own CA.

42. For all the legal aspects, such as signing legal documents and their delivery to users, ISTAT adopts strong digital signatures directly certified by the CA of PA IT Authority; for this purpose an inner Registration Authority has been constituted that manages the certificate requests of ISTAT personnel.

REFERENCES

M.I. Balla. Conference “La Pubblica Amministrazione tra esigenze di trasparenza e sicurezza delle informazioni” , November 1994

Various Authors. ISTAT – Conference “Problemi di sicurezza nel trattamento dei dati statistici” – April 1997

G. Carchesio, A. Guarino. “Certificazione elettronica degli indici dei prezzi” XXXVII conference AICA – September 1999

M.I. Balla. “Riservatezza e autenticità nei servizi telematici al cittadino” – Italian magazine of public communication - n.1 1999

AIPA Linee guida per la definizione di un piano per la sicurezza”. Magazine “Informazioni AIPA” Supplement to n.9-10/1999

J. Harry, D. Crowther. “Securing your e-business” IBM White paper - May 2000

Various Authors. V National statistical conference – Workshop “Connessione in rete: sicurezza informatica e riservatezza” - November 2000

S. Bergamasco, G. Budano, A. Toma. Business process reengineering aimed to re-design a statistical process: a case study the “new interviewers’ network” – Conference NTSS & ETK 2001 – June 2001-10-15

S. Bergamasco, G. Budano, L. Quattrociocchi, A. Toma. The new ISTAT network for capturing interview data: “The technological architecture”