Distr.
GENERAL

CES/AC.71/2004/3 (Summary)
24 February 2004

Original: ENGLISH

UNITED NATIONS STATISTICAL COMMISSION and ECONOMIC COMMISSION FOR EUROPE (ECE) CONFERENCE OF EUROPEAN STATISTICIANS

EUROPEAN COMMISSION STATISTICAL OFFICE OF THE EUROPEAN COMMUNITIES (EUROSTAT)

ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT (OECD) STATISTICS DIRECTORATE

Joint ECE/Eurostat/OECD Meeting on the Management of Statistical Information Systems (MSIS)
(Geneva, 17-19 May 2004)

Topic (i): Web technology in statistical information systems

USING PUBLIC KEY INFRASTRUCTURE FOR THE CENSUS

Invited Paper

Submitted by Statistics Canada[1]

Summary

1. As Canada's National Statistical Office, Statistics Canada has the responsibility for conducting a census of population every five years. For the next occasion in 2006 we wish to offer all citizens the option of entering their responses on-line and to assure them that their confidentiality is fully protected. This paper explains the Census requirements and the rationale for choosing Public Key Infrastructure (PKI) technology as the solution.

2. The Government of Canada, as part of its Government on-line (GOL) initiative begun in 2000, has established a common infrastructure known as the Secure Channel that is shared by almost 200 operating departments and agencies. This infrastructure provides a secure backbone for delivering electronic services to citizens and businesses over the Internet.

3. In addition to reliable, high-capacity network services, the Secure Channel provides security services that include a PKI and a common Certification Authority (CA). Individual departments are required to use this infrastructure in developing and operating their public services.

4. Statistics Canada has worked closely with Canada's central agencies and the commercial consortium that built the common infrastructure to develop a special PKI service that is suited to the specific requirements of the Census. These requirements and the new service that emerged are described by this paper.

[1] Prepared by Mel J. Turner and Lise Duquet (mel.turner@statcan.ca).

5. This will be one of the first uses of PKI for Census anywhere in the world because the normal registration processes to obtain a PKI certificate are considered too onerous for a one-time operation. Using Entrust TruePass® technology, and a unique approach to reusing certificates, Statistics Canada believes it has developed a practical solution.

6. Our principal requirements for the Census application were:

- Simple, single-step access;
- Convenient and easy to use;
- Capable of securely handling large volumes.

7. The new service was named SEAL for "Session Encryption with Automated Log-in" (en français SCEAU: Session avec Chiffrement et Enregistrement AUtomatique). The automated log-in aspect of the service means that the Census application can request the Secure Channel to establish a secure session without it demanding a log-in dialogue with the user. This met our requirements for a single-step identification process and for an invisible interface. At the same time, it eliminated the overhead directory capacity that would have been needed for a very large number of unique users.

8. Although it is somewhat premature to consider SEAL for use by applications other than the Census, it is important to underline the care that has been taken to develop SEAL as an independent service rather than just a supporting component of the 2006 Census.

9. A partnership agreement between Statistics Canada and the Secure Channel was formed in July, 2003 which included a shared funding approach to develop the SEAL service. The share of costs borne by the common infrastructure reflected the potential of SEAL to be reused by other applications across government.

10. The paper describes the SEAL service, developed for the specific use in the Canadian Census of Population but having potential for many other applications. Although it is particularly appropriate for statistical surveys, it could prove useful for any Internet transaction where confidentiality is the primary goal.

11. Just as this paper is being first delivered (May, 2004) the Census dress rehearsal will be in operation in three locations in Canada. The results of this public exposure will be used to refine our on-line approach to social surveys and to gauge the general acceptability of this approach for data protection. It remains to be seen if the public trust in on-line interaction can be enhanced.

- - - - -