

**STATISTICAL COMMISSION and  
ECONOMIC COMMISSION FOR EUROPE**

**COMMISSION OF THE  
EUROPEAN COMMUNITIES**

**CONFERENCE OF EUROPEAN STATISTICIANS**

**EUROSTAT**

**Joint ECE/Eurostat Work Session on  
Statistical Data Confidentiality**  
(Thessaloniki, Greece, 8-10 March 1999)

Working Paper No. 11 (Summary)  
English only

Topic (ii): software and computing developments

**CRYPTOGRAPHY AS A TOOL TO EXPAND COMMUNICATIONS AND EASE OF ACCESS  
AS WELL AS DATA SECURITY**

Submitted by Statistics Netherlands<sup>1</sup>

**Contributed paper**

**Summary**

1. The greater awareness of the public and governments of the vulnerability of large data collections, at least in the Netherlands, have given rise to increased requirements for the security measures of governmental data bases. Normally, stronger security measures are associated with more difficult and cumbersome access, and an increased burden for the legitimate users of data. Cryptographic techniques can be used however, to realize new ways of access and communication with the same or higher levels of security than with traditional measures.
2. At present, the traditional ways of safeguarding data against unauthorized access and alteration, draw heavily on the physical presence in premises, on the use of passwords, on the assumption that a Local Area Network is hard to eavesdrop, and on the inherent security properties of operating systems. The use of cryptography can improve many of these security ingredients. Moreover, it permits remote access to data at the same level of security as is achieved by local access, i.e. at the workplace.
3. Instead of dividing the world into two groups, the 'ins' and 'outs' (i.e. all NSI employees vs the rest of the world), and building an imaginary 'wall and moat' around the offices of a NSI, the data of an NSI are split into several (3 to 5) categories, with a varying level of security needs and measures. The highest security level is, of course, for identifying data; one step less secure could be e.g. individual but not identifying data; other security categories might be: aggregated statistical data; 'general office' correspondence, and public data and reports. There needs to be some method of communication between the data at different security levels. One of the main issues is how to control and safeguard these communication 'bridges', because they would be among the "weak spots" in the system we propose.

---

<sup>1</sup> Prepared by Leon Willenborg and Jan Kardaun.

4. In the paper we present a model of this hierarchical data access model, taking into account different security levels of data and different employees having access to these data. Within this model, cryptography plays a key role. The advantages of the approach outlined in this paper would be a more flexible form of data access than the one that is traditionally applied, which is an important point in the risk/benefit analysis.

5. The main purpose of this paper is to investigate the possibilities of remote access to data in NSIs. In a modern society where teleworking will be more and more commonplace, NSIs are forced by these developments to explore the possibilities and limitations of remote data access.