

TTP.NL SCHEME - GUIDANCE NOTE 1

Subject: ***Conformity of the use of a trusted channel between signature-creation application (SCA) and secure signature-creation device (SSCD)***

A. Introduction

This Note provides guidance for Certification Bodies performing management system certification audits of Service Providers in accordance with the requirements of the TTP.NL Scheme.

The word "shall" is used to indicate mandatory requirements strictly to be followed in order to conform to the requirements of the TTP.NL Scheme or the specified standard.

The word "should" is used to indicate that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required.

B. Background

1. TTP.NL Scheme section 4.1 d) requires that secure signature-creation devices (SSCDs) must be certified against one of the Protection Profiles specified in CWA 14169 'Secure signature-creation devices "EAL4+" or equivalent criteria. This is based on the requirements for SSCDs which are specified in article 5 of 'Besluit elektronische handtekeningen' and, in addition, article 4 of 'Regeling elektronische handtekeningen' where it is stipulated that in case an SSCD complies with the requirements of CWA 14169, compliance with the requirements of 'Besluit elektronische handtekeningen' is assumed.
2. With regard to the audit of the management system of a Service Provider issuing qualified certificates for electronic signatures, the following considerations apply:
 - a. In accordance with the requirements of ETSI TS 101 456 and the additional requirements of 'Besluit elektronische handtekeningen', the object of the audit is the applicable component services of the Service Provider's management system;
 - b. During the audit of the Service Provider's management system, the Certification Body audit team performs limited testing of SSCDs and this only as far as specific requirements of ETSI TS 101 456 are concerned;
 - c. In order to assess conformity of SSCDs with the requirements of CWA 14169 or equivalent, the audit team requests the Service Provider to present the necessary evidence;
 - d. For assessing conformity with the specific requirements of CWA 14169 concerning the use of a trusted channel between the signature-creation application (SCA) and the SSCD, the audit object would be the subject's computer system environment in which the SSCD is used;
 - e. The subject's computer system environment can be very different from case to case, depending upon the hardware, operating system, signature-creation application, cryptographic interface, and SSCD middleware and drivers;
 - f. ETSI TS 101 456 requires Service Providers in clause 7.3.4 a) to make available to subscribers and relying parties the terms and conditions regarding the use of certificates including (in the third bullet) the subscriber's obligation concerning the use of an SSCD, but ETSI TS 101 456 does not require Service Providers to inform subscribers and/or subjects on how the SSCD shall be used;
 - g. Verifying and assessing the use of a trusted channel at computer system environments of subjects as part of a management system audit of a Service Provider would be an impossibility due to factors as logistics, access rights, audit time, and costs, and would be impractical since

Service Providers have no means to ensure correction of possible nonconformities found at subjects;

- h. As far as known, audits of Service Providers in other European Member States do not include verification and assessment of the requirements for the use of a trusted channel. Some Member States, e.g. Germany, make assumptions concerning the security of computer system environments of subjects using SSCDs.

C. Certification Body action

- 1. Based on above considerations, the requirements in CWA 14169 concerning the use of a trusted channel for communication between the signature-creation application (SCA) and the secure signature-creation device (SSCD) should not be verified and assessed as part of management system audits against ETSI TS 101 456.

0 – 0 - 0