

## TTP.NL SCHEME - GUIDANCE NOTE 2

Subject: **Conformity of Java applets as part of SSCDs**

### 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) shall 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. An SSCD contains a chip with processor, memory, operating system software, and application programs for security and encryption functions (together called "the platform");
  - e. JAVA Cards applied as SSCDs contain in addition to the platform an application program developed in the JAVA programming language, the JAVA applet, installed in the chip's memory for execution of the following functions:
    - i) management of the PKCS #15 Cryptographic Token Information Format on the card,
    - ii) secure communication by means of transportation keys between the Hardware Security Module (HSM) and the JAVA Card during injection of the HSM generated subject's private and public keys,
    - iii) interfacing with the middleware on the subject's computer system for PIN / PUK verification and signing / verification / encryption / decryption operations;
  - f. To assess JAVA Cards applied as SSCD, the audit team shall receive evidence from the Service Provider concerning conformity of the platform as well as the JAVA applet with the requirements for secure signature-creation devices;
  - g. The phrase "wordt vermoed te voldoen" ("is assumed to comply") in article 4 of 'Regeling elektronische handtekeningen' means that certification of an SSCD against CWA 14169 is in general considered as best practice, but does not exclude other means of providing evidence of compliance;

- h. Testing and certification of an SSCD platform is considered an effective and efficient method of providing evidence of security, but testing and certification of JAVA applets could be costly and take long time compared to the relatively low cost and short duration of developing such applets.
3. The open formulation of the phrase in article 4 of 'Regeling elektronische handtekeningen' allows alternative means of providing evidence that a JAVA applet is in conformity with the security requirements. TTP.NL Scheme section 4.1 d) also allows alternative means by stating that "equivalent criteria" can be used in stead of one of the Protection Profiles specified in CWA 14169.

A Certification Body audit team performing an audit of the management system of a Service Provider against ETSI TS 101 456 could be confronted with the situation where the JAVA applet has not been certified for conformity with the requirements of CWA 14169. In such case the audit team should follow the guidance in sections C and D of this Guidance Note, in which alternative means are described for providing evidence that a JAVA applet is compliant.

### C. Testing of the JAVA applet

1. The JAVA applet, applied on a platform that is certified against one of the Protection Profiles specified in CWA 14169 'Secure signature-creation devices "EAL4+" or equivalent criteria, should be tested in accordance with the following minimum requirements:

#### 2. *Commissioning the testing*

- a. Testing of the JAVA applet should be commissioned by the sponsor (e.g. the manufacturer) to a testing laboratory accredited to ISO/IEC 17025 for at least the scope 'testing of Information Technology products'.

NOTE: the testing laboratory may in accordance with the requirements of ISO/IEC 17025:

- subcontract work, or
- make use of competent personnel subcontracted from other organizations and working under supervision of the testing laboratory.

An example of such subcontracted work could be code review of the JAVA applet.

- b. In accordance with the requirements of ISO/IEC 17025, the object of testing shall be identified unambiguously.
- c. The contract for testing should include the assessment objectives specifying at least that testing shall demonstrate that the JAVA applet:
  - i) has been developed using best coding practices;
  - ii) does not contain any cryptographic functions and uses exclusively the secure cryptographic functions of the platform;
  - iii) does not compromise or weaken the security functions of the platform;
  - iv) does not suffer from any vulnerabilities regarding the protection of secret information (PIN, PUK, private keys);
  - v) uses defined rules for managing access and use of critical functionality and data;
  - vi) is, where applicable in combination with the platform, resistant to state-of-art attacks as documented in recent versions of generally accepted reference documents;
  - vii) ensures that after installation of the applet and personalization of the card it is not possible to replace the applet or to install additional applets (i.e. no post-issuance installation of any applets);
  - viii) protects PIN and PUK codes such that these cannot be revealed through e.g. side channel analysis, fault injection, and/or logical attacks;
  - ix) does not, where applicable in combination with the platform, contain logical backdoors;
  - x) has been documented such that, in case the JAVA applet contains personalization options, the accompanying documentation fully and correctly describes the relationship between these personalization options and the security functions of the platform.
- d. The steps and activities required for realizing the assessment objectives should be documented in a testing plan.

### 3. *Performing the testing*

- a. In accordance with the requirements of ISO/IEC 17025, testing personnel shall have relevant technical knowledge in the area of SSCDs.
- b. Testing of the resistance to state-of-art attacks (e.g. side channel analysis, fault injection, and logical attacks) should be performed on the basis of vulnerabilities known at the time of testing and attacks documented in recent versions of generally accepted reference documents.
- c. Testing of the JAVA applet in combination with the platform should include, but not be limited to, testing of the logical security, side channel analysis, and perturbation.

### 4. *Reporting the testing results*

- a. The test report should contain in addition to the requirements specified in ISO/IEC 17025 at least the following:
  - i) an unambiguous identification of the object of testing;
  - ii) the assessment objectives;
  - iii) the description of the software development life-cycle of the JAVA applet and the used coding practices;
  - iv) the description of the attacks used in the testing;
  - v) the testing results specified per assessment objective;
  - vi) the laboratory's opinion concerning the conformity of the JAVA applet in combination with the platform.

## **D. Certification Body actions**

1. In accordance with the requirements of the TTP.NL Scheme, the Certification Body audit team shall verify the evidence concerning the conformity of the SSCD. One of the following situations could occur:
  - a. The presented evidence shows that the platform including JAVA applet is certified to the applicable requirements specified in CWA 14169. The audit team should conclude conformity of the SSCD.
  - b. The presented evidence shows that the platform and the JAVA applet are not certified to the applicable requirements specified in CWA 14169. The audit team should conclude a major nonconformity.
  - c. The presented evidence shows that the platform is certified to the applicable requirements specified in CWA 14169, but the JAVA applet is not certified and has not been tested in accordance with the guidance in section C above. The audit team should conclude a major nonconformity.
  - d. The presented evidence shows that the platform is certified to the applicable requirements specified in CWA 14169 and the JAVA applet is not certified, but has been tested in accordance with the guidance in section C above with a positive opinion in the test report. The audit team should conclude conformity of the SSCD.
2. The Certification Body shall require that the Service Provider eliminates detected nonconformities in accordance with the requirements of section 6.9 of the TTP.NL Scheme.

0 – 0 - 0