

0101UZI0100REGISTER10111

Applicable Standards

UZI-register

Published by : Central Agency for Information on Healthcare Professions (CIBG)

Version : 1.1 Def. (Eng)

Date : 2-5-2005

© 2005 CIBG, Den Haag

All rights reserved. No part of this publication may be reproduced, stored in an automated datafile or made public in any form or in any way, whether electronically, mechanically, by photocopy, recording or any other means, without the prior written permission of the publisher: CIBG, telephone + 31 (0)70 340 7446.

Contents

1	Applicable standards	4
1.1	Introduction	4
1.2	Certification and legal framework	4
1.3	Smart card	5
1.4	Card reader.....	6
1.5	PKI middleware.....	6
1.6	Dissemination Service	6
1.7	Browser interoperabiliteit.....	7
1.8	Ondersteunde client platform	7
1.9	Certificate and CRL profiles.....	7
1.10	Cryptographic Algorithms	8
1.11	Registration system	8

1 Applicable standards

1.1 Introduction

This document contains a summary of the standards with which the UZI-register complies. Where possible, the standards have been grouped around the components of the UZI-register to which they relate. A summary of standards, guidelines and legislation is then given for each group so formed.

1.2 Certification and legal framework

ETSI TS 101 456 v1.2.1 (2002-04), Policy requirements for certification authority issuing qualified certificates.

Schedule of requirements from the PKI for the government, www.pkioverheid.nl:

- SoR part 2b Certificate Policy - Government domain, version 5.0, September 2003
- SoR part 2d Certificate Policy - Services, appendix to CP Business and CP Government, version 2.0, September 2003

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures. These guidelines were implemented in the Dutch Electronic Signatures Act [*Wet elektronische handtekeningen*] on 8 May 2003.

Dutch Electronic Signatures Act [*Wet elektronische handtekeningen*], the Act of 8 May 2003 modifying Book 3 and Book 6 of the Dutch Civil Code [*Burgerlijk Wetboek*], the Telecommunications Act [*Telecommunicatiewet*] and the Economic Offences Act relating to Electronic Signatures [*Wet op de economische delicten inzake elektronische handtekeningen*] in the context of the implementation of Directive 1999/93/EC of the European Parliament and the Council of the European Union of 13 December 1999 on a Community Framework for Electronic Signatures (OJ EC L13) (Electronic Signatures Act), www.overheid.nl.

Individual Healthcare Professions Act [*Wet Beroepen in de individuele Gezondheidszorg Wet*, BIG Act], law passed on 11 November 1993, which sets down rules on the provision of healthcare services by professional practitioners, www.overheid.nl.

Quality of Healthcare Institutions Act [*Kwaliteitswet zorginstellingen*, KwZ], law passed on 18 January 1996 which regulates the quality of healthcare institutions, www.overheid.nl. Article 1 of this Act defines a "healthcare institution" as a hierarchical arrangement for the purpose of providing healthcare services.

1.3 Smart card

The UZI-register has opted for the following smart card:

Smart card features	Specifications
Microprocessor:	Philips P8WE5033; 32 k Eeprom
Operating system:	IBM JCOP 21 id
Manufacturer:	Trüb

The smart card (a combination of a microprocessor and an operating system) has been independently certified in accordance with the following standards:

- [Common Criteria EAL4+] : Common Criteria for Security Evaluation (Version 2.1, ISO/IEC 15408: 1999), Evaluation Assurance Level 4+ (EAL4+), <http://www.commoncriteriaportal.org/>
- [FIPS 140-2 level 3] : Federal Information Processing Standards Publication, Security Requirements for Cryptographic Modules, National Institute of Standards and Technology, <http://csrc.nist.gov>

According to independent testing, the smart card hardware (Philips P8WE5033; 32 k Eeprom, Triple-DES coprocessor, FameX RSA coprocessor) complies with the following standards:

- Supply voltage: tests indicate that the card functions properly with a supply voltage of both 5V and 3V.
- [ISO7816-1 t/m 3] Information technology - Identification cards - Integrated circuit(s) cards with contacts:
Part 1: Physical characteristics
Part 2: Dimensions and location of contacts
Part 3: Electronic signals and transmission protocols
- [ISO/IEC 7816-3 Amd. 1] This is an asynchronous, half-duplex smart card communications protocol, generally known as the T=1 protocol.

The smart card uses [IBM JCOP 21 id] as its Card Operating System, a system which is based on open standards.

- [JCOP 21 id] is an IBM implementation of the [JavaCard 2.1.1] and the [GlobalPlatform Card Specification v2.1.1] basic specifications. Further information is available via www.ibm.com, key search words 'JCOP21id Technical Brief'.
- [Java Card v2.1.1] : JavaCard specifications from Sun: <http://java.sun.com/products/javacard/>.
- [GlobalPlatform Card Specification v2.1.1] : GlobalPlatform Card Specification v2.1.1 - published March 2003, <http://www.globalplatform.org/>.
- [ISO7816-1 t/m 3] Information technology - Identification cards - Integrated circuit(s) cards with contacts:
Part 4: Interindustry commands for interchange
Part 8: Commands for security operations
- [PKCS #15 v1.1] : Cryptographic Token Information Syntax Standard (6 June 2000) , RSA Laboratories, www.rsasecurity.com.

1.4 Card reader

The UZI-register has subjected the following card readers to interoperability tests.

Product	Specifications
Readers, Omnikey	CardMan 3121 USB
Readers, Omnikey	CardMan 4040 PCMCIA
Gemplus	GemPC TWIN USB
Gemplus	GemPC 400 (PCMCIA)

Note: In principle, the selected PKI Middleware worked satisfactorily with all [PC/SC v1.0] compliant card readers. However, in an endeavour to avoid problems, the reader must have be capable of producing 60mA.

Standards supported for the card reader

- [PCMCIA] : PC Card standard, developed by the Personal Computer Memory Card International Association, <http://www.pcmcia.org>
- [PC/SC v1.0] : Personal Computer/Smart Card interface specifications, <http://www.pcscworkgroup.com/>
- [USB] : Universal Serial Bus, www.usb.org

1.5 PKI middleware

The UZI-register has opted for SafeSign (www.aeteurope.com) as PKI middleware. The following versions of PKI middleware have been tested by the UZI-register in regard to interoperability with card readers and smart card.

Product	Specifications
PKI middleware AET	SafeSign version 2.0.14 (for the Windows platform)
PKI middleware AET	SafeSign version 2.0.14 for MacOS X
PKI middleware AET	SafeSign version 2.0.x for Linux

There are two standards which relate to the applications which make use of SafeSign:

- [CryptoAPI] : Microsoft Crypto API, www.microsoft.com
- [PKCS#11] : Public-Key Cryptography Standards. PKCS #10 v2.11: Cryptographic Token Interface Standard, RSA Laboratories, www.rsasecurity.com.

In addition, SafeSign also supports the following standard:

- [PKCS#12] : Personal Information Exchange Syntax v1.0, RSA Laboratories, www.rsasecurity.com.

1.6 Dissemination Service

Certificates and CRLs can be called up using the [HTTP] protocol. [SSL] is used to secure this protocol and also communications with the directory service (LDAP).

- [HTTP]: RFC 2616, Hypertext Transfer Protocol -- HTTP/1.1, www.ietf.org.
- [SSL]: SSL3.0 Specification, www.netscape.com

The LDAP directory service meets the following standards:

- [X.509v3] : ISO/IEC 9594-8, 4th edition, 2002 (=ITU-T Rec. X.509): Information Technology – Open Systems Interconnection – The directory: Public-key and attribute certificate framework
- [X.520] : ITU/X.520 Attribute types

- [X.521] : ITU/X.521 Object Classes
- [RFC 2798] : IETF/RFC 2798, Definition of the inetOrgPerson LDAP Object Class
- [RFC 2251] : IETF/RFC 2251, Lightweight Directory Access Protocol (v3)

OCSP services which will comply with the following standard are currently in preparation:

- [RFC 2560]: Online Certificate Status Protocol – OCSP, <http://www.ietf.org/>

1.7 Browser interoperabiliteit

In the dissemination service (www.uzi-register) the following browsers can be used.

Operating System	Browser
Windows 2000	Microsoft Internet Explorer 5.x and next
	Netscape 6.0 and higher
	Mozilla 1.3 en hoger (inclusief Firefox)
Windows XP	Microsoft Internet Explorer 5.x and next
	Netscape 6.0 and next
	Mozilla 1.3 en hoger (inclusief Firefox)
Mac OS X	Microsoft 5.2 and next
	Safari
Linux	Mozilla 1.3 and next (inclusief Firefox)

1.8 Ondersteunde client platform

De clients (PC's) tested with the UZI card are:

Product	Specificaties
Windows 2000	Service Pack 4
Windows XP	Service Pack SP2
Mac OS X	Versie 10.2
Linux	Linux Fedora Core 1

1.9 Certificate and CRL profiles

The profiles meet the following standards:

- [X.509v3] : ISO/IEC 9594-8, 4th edition, 2002 (=ITU-T Rec. X.509): Information Technology – Open Systems Interconnection – The directory: Public-key and attribute certificate framework
- [ISO8825] : ISO/IEC 8825-1: 1995 Information technology - ASN.1 encoding rules - Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)
- [RFC3280] : Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile, April 2002
- [RFC2279] : UTF-8, a transformation format of ISO 10646, January 1998

Signature certificates classify as what are known as qualified certificates and accordingly comply with the following additional standards:

- [ETSI 101 862] : ETSI TS 101 862 - Qualified Certificate Profile
- [RFC3739] : Internet X.509 Public Key Infrastructure Qualified Certificates Profile, March 2004

1.10 Cryptographic Algorithms

All the cryptographic algorithms used for the UZI-register comply with [ETSI SR 002 176]. Algorithms and Parameters for Secure Electronic Signatures, v1.1.1 (2003-03)

- [ETSI SR 002 176] only describes the algorithms for electronic signature and not the trust function (by encrypting messages) and authenticity. The same algorithms as are used for the electronic signature are also used for authentication. Symmetric algorithms which are not included in [ETSI SR 002 176] are often used to encrypt messages. For that reason, and until standardization has been achieved at European level, the [3DES] and [AES] variants have been chosen.
- [3DES] : Triple-DES, defined in the Federal Information Processing Standards Publication 46-3, Data Encryption Standard, National Institute of Standards and Technology, <http://csrc.nist.gov>, and in the standard ANSI X.9.52 'Triple Data Encryption Algorithm Modes of Operation' (American Bankers Association, 1998).
- [AES] : Advanced Encryption Standard, Federal Information Processing Standards Publication 197, <http://csrc.nist.gov>.

In the context of the permitted algorithms, it has been decided to further opt for:

- PKCS #1 V1.5: Nov. 1993, V2.0: July, 1998
- V2.1 June 2002: RSA Cryptography Standard, RSA Laboratories, www.rsasecurity.com.
- [SHA-1] : Federal Information Processing Standards Publication 180-1, 1995 April 17, Secure Hash Standard.

RSA keys with a length of 1024 bits are used for users; the RSA keys of CAs have a length of 2048 bits.

1.11 Registration system

[PKCS#10] is used for requesting services certificates.

- Public-Key Cryptography Standards. PKCS #10 v1.7: Certification Request Syntax Standard, RSA Laboratories, www.rsasecurity.com.

The character set defined in [NEN1888] is supported for registration in the UZI-register.

- NEN 1888 (nl) General personal data - Definitions, character sets and interchange formats.