TURVAKIIBI RAKENDUS JA LIIDES

Security chip
Application and interface

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESSÕNA

Käesolev Eesti standard:

- on kakskeelne väljaanne 2004. aastal avaldatud eestikeelsest standardist EVS 827:2004, millele on lisatud ingliskeelne paralleeltekst;
- on kinnitatud Eesti Standardikeskuse 19.06.2009 käskkirjaga nr 106;
- jõustub sellekohase teate avaldamisel EVS Teataja 2009. aasta juulikuu numbris.

Standardi kakskeelse väljaande koostas AS Sertifitseerimiskeskus, standardi on heaks kiitnud tehniline komitee EVS/TK 4 Infotehnoloogia.

ICS 35.040 Märgistikud ja informatsiooni kodeerimine
Võtmesõnad: turvakiip, sertifikaat, EstEID
Hinnagrupp RQ

FOREWORD

This Estonian standard:

— is bilingual version of standard EVS 827:2004 with added English parallel text;

— is implemented by decree of Estonian Centre for Standardisation 19.06.2009 no 106;

— becomes valid with notice in EVS Teataja, issue July 2009.

Bilingual version of Estonian standard EVS 827:2004 “Security chip – Application and interface” has been prepared by the Estonian Certification Centre (AS Sertifitseerimiskeskus), standard approved by technical committee EVS/TK 4 Infotechnology.

ICS 35.040 Character sets and information coding
Descriptors: security chip, certificate, EstEID
Price group RQ

SISUKORD

TABLE OF CONTENT

1 KÄSITLUSALA

Käesolev standard spetsifitseerib Eesti riikliku avaliku võtme infrastruktuuri (EstEID) turvakiibi liidese ja andmesisu.

2 SEONDUVAD STANDARDID

ISO 7816-1 Identification cards – Integrated circuit(s) cards with contacts – Part 1: Physical Characteristics

ISO 7816-2 Identification cards – Integrated circuit(s) cards with contacts – Part 1: Physical Characteristics

ISO 7816-3 Identification cards – Integrated circuit(s) cards with contacts – Part 3: Electronic signals and transmission protocols

ISO 7816-4 Identification cards – Integrated circuit(s) cards with contacts – Part 4: Interindustry commands for interchange

ISO 7816-5 Identification cards – Integrated circuit(s) cards with contacts – Part 5: Numbering system and registration procedure for application identifiers

ISO 9594-8 Information Technology – Open Systems Interconnection – The Directory: Authentication Framework

PKCS#1 v1.5, RSA Cryptography Standard, November 1, 1993

PKCS#1 v2.0, RSA Cryptography Standard, October 1, 1998

PKCS#5 v2.0, Password-Based Cryptography Standard, March 25, 1999

RFC 3280 Internet X.509 Public Key Infrastructure Certificate and CRL Profile

Micardo 2.1 Chip Card Operating System User Manual

3 KASUTATUD LÜHENDID

APDU	Kiibi rakendusprotokolli ühik
LSB	Noorim bitt
MF	Juurkataloog turvakiibi failisüsteemis
Kaardihalduskeskus	Institutsioon, kes teostab EstEID kaartide haldamise operatsioone kiibi haldaja volitusel
Kaardi haldaja	Institutsioon, kes vastutab EstEID kaardihalduse protseduuride läbiviimise eest

4 EstEID TURVAKIIBI RAKENDUSE OBJEKTID JA OPERATSIOONID

4.1 EstEID turvakiibi objektid

EstEID olevad objektid on kujutatud järgneval joonisel: