

See dokument on EVS-i poolt loodud eelvaade

TURVAKIIBI RAKENDUS JA LIIDES

**Security chip
Application and interface**

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

Standardite reprodutseerimis- ja levitamiseõigus kuulub Eesti Standardikeskusele

Andmete paljundamine, taastekitamine, kopeerimine, salvestamine elektroonilisse süsteemi või edastamine ükskõik millises vormis või millisel teel on keelatud ilma Eesti Standardikeskuse poolt antud kirjaliku loata.

Kui Teil on küsimusi standardite autorikaitse kohta, palun võtke ühendust Eesti Standardikeskusega:
Aru 10 Tallinn 10317 Eesti; www.evs.ee; Telefon: 605 5050; E-post: info@evs.ee

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

Right to reproduce and distribute belongs to the Estonian Centre for Standardisation

No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, without permission in writing from Estonian Centre for Standardisation.

If you have any questions about standards copyright, please contact Estonian Centre for Standardisation:
Aru str 10 Tallinn 10317 Estonia; www.evs.ee; Phone: 605 5050; E-mail: info@evs.ee

SISUKORD

1	KÄSITLUSALA	6
2	SEONDUVAD STANDARDID	6
3	KASUTATUD LÜHENDID	6
4	EstEID TURVAKIIBI RAKENDUSE OBJEKTID JA OPERATSIOONID.....	6
4.1	EstEID turvakiibi objektid.....	6
4.2	EstEID turvakiibi operatsioonid	16
4.3	EstEID failisüsteem	22
4.4	Objektid EstEID kaardil väljaandmise hetkel.....	26
5	EstEID ABIPROTSEDUURID.....	26
5.1	EstEID turvaline kommunikatsioon.....	26
5.2	3DESKey tuletamine paroolausest.....	26
6	EstEID KAARDI TURVASTRUKTUUR	26
6.1	Turvakeskkondade ja operatsioonide risttabel.....	26
6.2	Kommentaariid turvakeskkondade kohta.....	30
7	JUHISEID KAARTI KASUTAVATE RAKENDUSTE KIRJUTAJALE.....	30
7.1	EstEID kiibi käsustik	30
7.2	EstEID kiibi ATR ajaloolised baidid	30
7.3	EstEID kiibi erinevused standardsest MICARDO 2.1st.....	32
7.4	Üldisi juhiseid.....	32

TABLE OF CONTENT

1	SCOPE	7
2	REFERENCE STANDARDS	7
3	ABBREVIATIONS	7
4	ESTEID SECURE TOKEN OBJECTS AND OPERATIONS	7
4.1	EstEID secure token objects	7
4.2	EstEID secure token operations	17
4.3	Overview of EstEID Files	23
4.4	Objects on EstEID token in moment of issuing	27
5	ESTEID PROCESS	27
5.1	EstEID secure messaging	27
5.2	3DESKeys derivation from passphrases	27
6	SECURITY FRAMEWORK OF ESTEID SECURE TOKEN	27
6.1	Cross-table of security environments and operations	27
6.2	Comments on security environments	31
7	GUIDELINES FOR APPLICATION DEVELOPERS	31
7.1	EstEID secure token command interface	31
7.2	EstEID secure token ATR historical bytes	31
7.3	EstEID token variations from MICARDO 2.1	33
7.4	General guidelines	33

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: