ČESKÁ TECHNICKÁ NORMA

ICS 35.240.15 **Březen 2010**

Aplikační rozhraní pro čipové karty používané jako zařízení pro vytváření bezpečného podpisu – Část 1: Základní služby

ČSN EN 14890-1
36 9710

Application Interface for smart cards used as Secure Signature Creation Devices – Part 1: Basic sevices

Interface applicative des cartes a puces utilisées comme dispositifs de création de signature numérique sécurisés – Partie 1: Services de bases

Anwendungsschnittstelle für Chipkarten, die zur Erzeugung qualifizierter elektronischer Signaturen verwendet werden – Teil 1: Allgemeine Dienste

Tato norma je českou verzí evropské normy EN 14890-1:2008. Překlad byl zajištěn Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví. Má stejný status jako oficiální verze.

This standard is the Czech version of the European Standard EN 14890-1:2008. It was translated by Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN EN 14890-1 (36 9710) z června 2009.

Národní předmluva

Změny proti předchozím normám

Proti předchozí normě dochází ke změně způsobu převzetí EN 14890-1:2008 do soustavy norem ČSN. Zatím co ČSN EN 14890-1 z června 2009 byla převzata schválením k přímému používání jako ČSN oznámením ve Věstníku, tato norma ji přejímá překladem.

Informace o citovaných normativních dokumentech

EN ISO 3166-1 zavedena v ČSN EN ISO 3166-1 (97 1002) Kódy pro názvy zemí a jejich částí – Část 1: Kódy zemí (idt ISO 3166-1:2006)

ISO/IEC 7816-4:2005 zavedena v ČSN ISO/IEC 7816-4:2006 (36 9205) Identifikační karty – Karty s integro-vanými obvody – Část 4: Organizace, bezpečnost a příkazy pro výměnu

ISO/IEC 7816-6 dosud nezavedena v ČSN ISO/IEC 7816-6 (36 9205) Identifikační karty – Karty s integrovanými obvody – Část 6: Mezioborové datové prvky pro výměnu

ISO/IEC 7816-8:2004 dosud nezavedena

ISO/IEC 7816-11:2004 zavedena v ČSN ISO/IEC 7816-11:2005 (36 9205) Identifikační karty – Karty s integro-vanými obvody – Část 11: Ověřování osob biometrickými metodami

ISO/IEC 7816-15:2004 zavedena v ČSN ISO/IEC 7816-15:2004 (36 9205) Identifikační karty – Karty s integro-vanými obvody – Část 15: Aplikace kryptografické informace

ISO/IEC 9796-2:2008 dosud nezavedena

ISO 11568-2:2005 dosud nezavedena

ISO/IEC 14888-2:2008 dosud nezavedena

ISO/IEC 15946-1 zavedena v ČSN ISO/IEC 15946-1 (36 9794) Informační technologie – Bezpečnostní techniky – Kryptografické techniky založené na eliptických křivkách – Část 1: Všeobecně

ISO/IEC 18033-3 dosud nezavedena

Vysvětlivky k textu převzaté normy

Český překlad vychází z anglické verze, místy upřesněné podle německé verze.

Rozsah „českých slov“ v softwarové části textu odpovídá „německým slovům“ v německé verzi téže části.

anglický termín	**obvyklé termíny**	**použitý termín**
administrator	• administrátor • správce (sítě)	administrátor (bezpečnostní)
a in F (viz tabulku 126)	• *a* z F • *a* Î F • *a* je prvkem F	• *a* z F • *a* Î F
• advanced electronic signature • qualified electronic signature	• kvalifikovaný elektronický podpis • zaručený elektronický podpis (starší verze směrnice 1999/93)	kvalifikovaný elektronický podpis
authentication key	• autentizační klíč • klíč pro autentizaci	autentizační klíč
big edian	• big endian • „velký konec první“	big endian
• certificate field • cert field	• pole s certifikátem • pole cert	• pole s certifikátem • pole cert
credentials	• pověření • doklady	pověření
• data field - empty • data field - absent	• datové pole - prázdné • datové pole – nevyskytuje se	• datové pole - prázdné • datové pole – nevyskytuje se
device	• zařízení • součástka • prostředek (zákon o el. podpisu)	zařízení (zařízení IFD i karta ICC)
discretionary data	• volně použitelná data • data podle uvážení	volně použitelná data
ephemeral public key	• dočasný veřejný klíč • efemerální veřejný klíč	dočasný veřejný klíč

flag	• flag • příznak	flag
hash	• hash (název operace) • hašování (název činnosti) • výsledek operace hašování	• hash (název operace) • hašování (název činnosti)
hash code	• hodnota hash • hash • výsledek operace hašování	hodnota hash
hash value	• hodnota hash • digitální otisk • výsledek operace hašování	hodnota hash
• KA • K_A	klíč entity A	klíč entity A
key seed	• výchozí materiál klíče • počáteční klíč	výchozí materiál klíče
key token	• token klíče • token s klíčem	token klíče
mechanism	• mechanizmus • ustálený způsob provádění	mechanizmus
mode	• režim • mode	režim
notation	• notace • zápis	• notace • zápis
padding	• vyplňování, výplň • vycpávka	vyplňování; výplň
personal card data	• osobní údaje na kartě • osobní data na kartě	osobní údaje na kartě
prime fields (elliptic curves over prime fields)	• prvočíselná tělesa • prvočíselná pole	prvočíselná tělesa (eliptické křivky nad prvočíselnými tělesy)
retail	• retail • bankovní služby pro drobnou klientelu	retail
root	• kořen, kořenová (autorita) • root	kořen, kořenová (autorita)
secure messaging (SM)	• bezpečné předávání zpráv • bezpečná výměna zpráv	• bezpečné předávání zpráv • SM
security environment	• bezpečnostní prostředí • bezpečné prostředí	bezpečnostní prostředí
stage	• etapa • fáze	etapa
signature password	• podpisové heslo • heslo pro podpis	podpisové heslo
signer	• podepisující se strana • podepisující	podepisující se strana
tag	• tag • příznak	tag
transport	• přenos • transport	přenos
variable; var.	• variable; var. • proměnná	variable; var.
verify certificate	• ověření certifikátu • proveď ověření certifikátu	ověření certifikátu

Vypracování normy

Zpracovatel: Anna Juráková, Praha, IČ 61278386, RNDr. Karel Jurák, PhD.

Technická normalizační komise: TNK 42 Výměna dat

Pracovník Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví: Ing. Petr Wallenfels

EVROPSKÁ NORMA EN 14890-1
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM Prosinec 2008

ICS 35.240.15 Nahrazuje CWA 14890-1:2004

Aplikační rozhraní pro čipové karty používané jako zařízení pro vytváření bezpečného podpisu – Část 1: Základní služby

Application Interface for smart cards used as Secure Signature Creation Devices – Part 1: Basic services

Interface applicative des cartes a puces utilisées comme dispositifs de création de signature numérique sécurisés – Partie 1: Services de bases

Anwendungsschnittstelle für Chipkarten, die zur Erzeugung qualifizierter elektronischer Signaturen verwendet werden – Teil 1: Allgemeine Dienste

Tato evropská norma byla schválena CEN 2008-09-27.

Členové CEN jsou povinni splnit Vnitřní předpisy CEN/CENELEC, v nichž jsou stanoveny podmínky, za kterých se musí této evropské normě bez jakýchkoliv modifikací dát status národní normy. Aktualizované seznamy a bibliografické citace týkající se těchto národních norem lze obdržet na vyžádání v Řídicím centru nebo u kteréhokoliv člena CEN.

Tato evropská norma existuje ve třech oficiálních verzích (anglické, francouzské, německé). Verze v každém jiném jazyce přeložená členem CEN do jeho vlastního jazyka, za kterou zodpovídá a kterou notifikuje Řídicímu centru, má stejný status jako oficiální verze.

Členy CEN jsou národní normalizační orgány Belgie, Bulharska, České republiky, Dánska, Estonska, Finska, Francie, Irska, Islandu, Itálie, Kypru, Litvy, Lotyšska, Lucemburska, Maďarska, Malty, Německa, Nizozemska, Norska, Polska, Portugalska, Rakouska, Rumunska, Řecka, Slovenska, Slovinska, Spojeného království, Španělska, Švédska a Švýcarska.

CEN

Evropský výbor pro normalizaci

European Committee for Standardization

Comité Européen de Normalisation

Europäisches Komitee für Normung

Řídicí centrum: rue de Stassart 36, B-1050 Brusel

Předmluva

Tento dokument (EN 14890-1:2008) byl vypracován v technické komisi CEN/TC 224 „Identifikace osob, elektronický podpis a karty a příslušné systémy a operace“, jejíž sekretariát je při AFNOR.

Této evropské normě musí být dán status národní normy buď zveřejněním identického textu nebo převzetím nejpozději do června 2009 a národní normy, které jsou s touto normou v rozporu, musí být zrušeny nejpozději do června 2009.

Je nutné upozornit na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. CEN [a/nebo CENELEC] neodpovídají za identifikování jednotlivých nebo všech souvisejících patentových práv.

Tento dokument nahrazuje CWA 14890-1:2004.

Tato norma dále poskytuje základní popis služeb identifikace, autentizace a digitálního podpisu (IAS), a obsahuje tedy všechny doplňkové kryptografické služby specifikované v EN 14890-2.

Tato norma umožňuje vývoj interoperabilních karet vydávaných libovolným sektorem kartového obchodu.
Norma popisuje aplikační rozhraní a chování SSCD, tj. mělo by být možné implementovat ji například do nativních karet nebo do karet založených na interpretaci.

Tato norma je ve shodě s dalšími evropskými normami, které byly vypracovány v rámci Evropské směrnice 1999/93.

Tato norma *Aplikační rozhraní pro čipové karty používané jako zařízení pro vytváření bezpečného podpisu* sestává ze dvou částí:

- Část 1: "Základní služby" popisuje povinné specifikace pro SSCD jako část obecně použitelných služeb IAS, které mají být použity ve shodě s požadavky 5.1 Směrnice o zásadách Společenství pro elektronické podpisy
- Část 2: "Další služby" popisuje zbývající služby IAS.

V souladu s Vnitřními předpisy CEN/CENELEC se národní normalizační organizace následujících zemí zavazují, že vyhlásí tuto evropskou normu: Belgie, Bulharska, České republiky, Dánska, Estonska, Finska, Francie, Irska, Islandu, Itálie, Kypru, Litvy, Lotyšska, Lucemburska, Maďarska, Malty, Německa, Nizozemska, Norska, Polska, Portugalska, Rakouska, Rumunska, Řecka, Slovenska, Slovinska, Spojeného království, Španělska, Švédska a Švýcarska.

Obsah

Strana

Předmluva 6

1 Předmět normy 12

2 Citované normativní dokumenty 12

3 Termíny a definice 13

4 Značky a zkratky 15

5 Aplikace podpisu 18

5.1 Průběh aplikace 18

5.2 Důvěryhodné prostředí a nedůvěryhodné prostředí 19

5.3 Volba aplikace ESIGN 20

5.3.1 Všeobecně 20

5.3.2 Výjimky pro bezpečné předávání zpráv 20

5.4 Volba aplikace kryptografické informace 20

5.5 Současné použití aplikací podpisu 21

5.5.1 Všeobecně 21

5.5.2 Metody volby kanálu 21

5.5.3 Bezpečnostní problémy s více kanály 21

5.6 Volba bezpečnostního prostředí 21

5.7 Volba klíčů 21

5.8 Základní bezpečnostní služby 21

6 Ověření uživatele 22

6.1 Všeobecně 22

6.2 Ověření uživatele založené na znalosti 22

6.2.1 Všeobecně 22

6.2.2 Explicitní ověření uživatele 22

6.2.3 Mechanizmy založené na heslu 23

6.2.4 Formáty prezentace 24

6.2.5 Čítače opakovaných pokusů (RC) 24

6.2.6 Změna hesla 24

6.2.7 Resetování RC a ustavení nového hesla 25

6.3 Biometrické ověřování uživatele 26

6.3.1 Všeobecně 26

6.3.2 Získání šablony biometrické informace (*Biometric Information Template*) 26

6.3.3 Provádění biometrického ověřování uživatele 27

6.3.4 Resetování RC 29

7 Služba digitálního podpisu 29

7.1 Algoritmy pro generování podpisů 29

7.2 Aktivace služby digitálního podpisu 29

7.3 Všeobecné aspekty 29

7.4 Generování podpisu 31

7.4.1 Žádné hašování na kartě 31

7.4.2 Dílčí hašování 31

7.4.3 Všechno hašování na kartě 32

Strana

7.5 Volba různých klíčů, algoritmů a vstupních formátů 33

7.5.1 Obnovení existujícího SE 34

7.5.2 Změna šablony HT aktuálního SE 34

7.5.3 Změna šablony DST aktuálního SE 35

7.6 Čtení certifikátů a informací, které se vztahují k certifikátům 35

7.6.1 Čtení objektů CIO, které se vztahují k certifikátům 35

7.6.2 Čtení certifikátu podpisující se strany z karty ICC 36

7.6.3 Získání certifikátu podepisující se strany ze služby adresáře *(directory service)* 37

8 Autentizace zařízení 37

8.1 Certifikační autority a certifikáty 38

8.1.1 Řetězce certifikátů 38

8.1.2 Používání křížových certifikátů 38

8.2 Autentizační prostředí 39

8.2.1 SCA v důvěryhodném prostředí 39

8.2.2 SCA v nedůvěryhodném prostředí 39

8.2.3 Specifikace prostředí 40

8.2.4 Mechanizmus zobrazování zprávy 40

8.2.5 Další autentizační prostředí 40

8.3 Mechanizmy přenosu klíče a dohody na klíči 40

8.4 Protokol přenosu klíče založený na RSA 40

8.4.1 Kroky autentizace 42

8.4.2 Vytvoření klíče relace 49

8.5 Autentizace zařízení s ochranou osobních údajů 49

8.5.1 Kroky autentizace 50

8.6 Modulární EAC protokol (mEAC) s nevysledovatelností pro ochranu soukromí (založený na eliptických křivkách) 62

8.6.1 Případ sledovatelnosti – příklad 62

8.6.2 Notace 62

8.6.3 Kroky autentizace 63

8.7 Přehled asymetrické autentizace 72

8.8 Schéma symetrické autentizace 72

8.8.1 Kroky autentizace 72

8.8.2 Vytvoření klíče relace 75

8.9 Výpočet klíčů relace z výchozího materiálu klíče *(Key Seed)* $K_{IFD/ICC}$ 76

8.9.1 Výpočet klíčů relace TDES 76

8.9.2 Výpočet AES-128 klíčů relace pro CBC mode a EMAC 77

8.9.3 Výpočet AES-128 klíčů relace pro CBC mode a CMAC 77

8.10 Výpočet hodnoty čítače posloupnosti odesílání SSC 77

8.11 Post-autentizační fáze 77

8.12 Ukončení bezpečné relace 77

8.12.1 Příklad zakončení bezpečné relace 78

8.12.2 Pravidla pro ukončení bezpečné relace 78

8.13 Čtení zobrazené zprávy *(Display Message)* 78

8.14 Aktualizace zobrazené zprávy 80

Strana

9 Bezpečné předávání zpráv 81

9.1 Bajt CLA 81

9.2 Kódování TLV příkazu a zprávy odezvy 81

9.3 Ošetření chyb SM 82

9.4 Vyplňování pro výpočet kontrolního součtu *(checksum calculation)* 82

9.5 Čítač posloupnosti odesílání (SSC) 82

9.6 Struktura zprávy v jednotkách APDU bezpečného předávání zpráv 82

9.6.1 Kryptogramy 82

9.6.2 Kryptografický kontrolní součet 85

9.6.3 Konstrukce APDU posledního příkazu 88

9.7 Ochrana APDU odezvy 89

9.8 Používání TDES a AES 95

9.8.1 Zašifrování/dešifrování TDES/AES 95

9.8.2 Režim CBC 95

9.8.3 Retail MAC pomocí TDES 96

9.8.4 EMAC pomocí AES 96

9.8.5 CMAC pomocí AES 97

10 Generování klíče 97

10.1 Generování klíče a export pomocí PrK.ICC.AUT 98

10.2 Generování klíče a export pomocí dynamické nebo statické SM 98

10.3 Zapsání certifikátu 98

10.4 Ustavení klíčů při statickém bezpečném předávání zpráv 98

11 Identifikátory a parametry klíčů 98

11.1 Identifikátory klíčů (KID) 98

11.2 Parametry veřejného klíče 99

11.3 Algoritmus DSA s ELC parametry veřejného klíče 99

11.4 Parametry pro výměnu RSA klíčů podle Diffie-Hellmana 100

11.5 Parametry pro výměnu ELC klíčů 100

12 Datové struktury 101

12.1 Šablony CRT 101

12.1.1 CRT AT pro volbu klíčů pro interní autentizaci 101

12.1.2 CRT pro volbu $PuK.CA_{IFD}$.CS_AUT pro zařízení IFD 101

12.1.3 CRT pro volbu PuK.IFD.AUT pro zařízení IFD 101

12.1.4 CRT AT pro volbu parametrů veřejného DH klíče 102

12.1.5 Parametry DH klíče pro GENERAL AUTHENTICATE 102

12.1.6 CRT AT pro volbu soukromého autentizačního klíče karty ICC 102

12.1.7 CRT pro volbu PuK.IFD.AUT pro zařízení IFD 102

12.1.8 Šablona CRT pro volbu PrK.ICC.KA 103

12.2 Protokol přenosu klíče pro autentizaci zařízení 103

12.2.1 EXTERNAL AUTHENTICATE 103

12.2.2 INTERNAL AUTHENTICATE 104

12.3 Protokol pro autentizaci zařízení s ochranou soukromí 104

12.3.1 EXTERNAL AUTHENTICATE 104

Strana

12.3.2 INTERNAL AUTHENTICATE 105

13 Identifikátory AlgID, formáty HASH a DSI 106

13.1 Identifikátory algoritmů a identifikátory objektů OID 106

13.2 Vstupní formáty pro hašování 107

13.2.1 PSO:HASH bez řetězení příkazů 107

13.2.2 PSO:HASH s řetězením příkazů 108

13.3 Formáty vstupu pro digitální podpis (DSI) *(Digital Signature Input)* 108

13.3.1 DSI podle ISO/IEC 14888-2 (schéma 2) 108

13.3.2 DSI podle PKCS #1 V 1.5 109

13.3.3 Digest Info pro SHA-X 110

13.3.4 DSI podle PKCS #1 V 2.x 111

13.3.5 DSA s parametry DH klíče 113

13.3.6 Algoritmus digitálního podpisu založený na eliptických křivkách – ECDSA 113

14 CV_certifikáty a správa klíčů 113

14.1 Důvěryhodnost certifikátů 113

14.2 Správa klíčů *(Key Management)* 113

14.3 Kartou ověřitelné certifikáty 114

14.3.1 Podpisy certifikátů 114

14.3.2 Cerifikáty autentizace 114

14.4 Použití veřejného klíče extrahovaného z certifikátu 114

14.5 Platnost klíče extrahovaného z certifikátu 115

14.6 Struktura CVC 115

14.6.1 Nesamopopisné certifikáty 116

14.6.2 Samopopisné certifikáty 116

14.7 Obsah certifikátu 116

14.7.1 CPI – Identifikátor profilu certifikátu 117

14.7.2 CAR – Odkaz na certifikační autoritu *(Certification Authority Reference)* 117

14.7.3 CHR – Odkaz na držitele certifikátu 119

14.7.4 CHA – Autorizace držitele certifikátu 119

14.7.5 Specifikace identifikátoru role 120

14.7.6 CHAT – Šablona pro autorizaci držitele karty 122

14.7.7 OID – Identifikátor objektu 122

14.7.8 CED – Datum začátku platnosti certifikátu 124

14.7.9 CXD – Datum ukončení platnosti certifikátu 124

14.8 Podpis certifikátu 124

14.8.1 Nesamopopisné certifikáty 124

14.8.2 Samopopisné certifikáty 126

14.9 Kódování obsahu certifikátu 126

14.9.1 Nesamopopisné certifikáty 126

14.9.2 Samopopisné certifikáty 127

14.9.3 Samopopisné certifikáty pro kryptografii založené na eliptických křivkách 127

14.10 Kroky ověřování CVC 129

14.10.1 První cyklus: Ověřování CVC z kořenového PuK 130

14.10.2 Následující cyklus (cykly) 130

14.11 Příkazy pro manipulaci s CV certifikáty 131

14.12 C_CV.IFD.AUT (nesamopopisné) 131

14.13 C_CV.CA.CS-AUT (nesamopopisné) 132

14.14 C.ICC.AUT 133

14.15 Samopopisné CV certifikáty (Příklad) 133

14.15.1 Veřejný klíč 133

15 Soubory 134

15.1 Struktura souboru 134

15.2 Identifikátory ID souborů 135

15.3 EF.DIR 135

15.4 EF.SN.ICC 136

15.5 EF.DH 136

15.6 EF.ELC 137

15.7 EF.C.ICC.AUT 137

15.8 EF.C.CA_{ICC}.CS-AUT 138

15.9 EF.C_X509.CH.DS 138

15.10 EF.C_X509.CA.CS (DF.ESIGN) 138

15.11 EF.DM 139

16 Aplikace poskytující informaci o kryptografických objektech 139

16.1 Příklad rozvržení kryptografické informace ESIGN 140

16.1.1 EF.CIAInfo 141

16.1.2 EF.AOD 142

16.1.3 EF.PrKD 144

16.1.4 EF.PuKD 146

16.1.5 EF.CD 146

16.1.6 EF.DCOD 147

Příloha A (informativní) Autentizace zařízení – Kryptografické hledisko 150

A.1 Algoritmy pro autentizaci s výměnou klíče nebo dohodou na klíči 150

A.2 Autentizace zařízení s přenosem klíče 150

A.2.1 Podle ISO/IEC 11770-3 150

A.2.2 Použití min(SIG, N-SIG) pro token podpisu 152

A.3 Autentizace zařízení s dohodou na klíči 152

A.3.1 Výměna klíče podle Diffie-Hellmana 153

A.4 Autentizace zařízení s ochranou osobních údajů 154

A.4.1 Autenticita veřejných DH parametrů 157

A.5 Autentizace zařízení s nevysledovatelností 158

A.5.1 Výměna klíče podle Diffie-Hellmana 158

A.6 Útok šachového velmistra *(Grandmaster Chess Attack)* 160

Příloha B (informativní) Scénáře personalizace 161

Příloha C (informativní) Schéma vytváření identifikátorů objektů mEAC 163

Bibliografie 165

1 Předmět normy

Část 1 tohoto souboru specifikuje aplikační rozhraní čipových karet v průběhu jejich používání jako zařízení pro vytváření bezpečného podpisu (SSCD - *Secure Signature Creation Devices*) ve shodě s evropskou směrnicí
o elektronickém podpisu 1999/93, aby se umožnila interoperabilita a používání jako SSCD na národní nebo evropské úrovni.

Tento dokument popisuje povinné služby pro používání čipové karty jako SSCD založené na EN 14890 (všechny části). Toto pokrývá funkci podpisování, uchovávání certifikátů, příslušné ověřování uživatele, zřizování a používání důvěryhodné cesty a kanálu, požadavky na generování a přidělování klíče a na formát zdrojů požadovaných pro provádění těchto funkcí a příslušných informačních kryptografických tokenů.

Funkčnost CWA 14890-1 je tedy posílena v následujících oblastech:

- autentizace zařízení založená na eliptických křivkách (ELC) pro existující asymetrické autentizační protokoly (Přenos RSA, Protokol s ochranou soukromí),
- zesílení existujících asymetrických autentizačních protokolů s nevysledovatelností pro ochranu soukromí,
- formáty certifikátů (samopopisné) ověřitelných kartou (CV) založené na ELC pro všechny typy autentizačních a autorizačních protokolů,
- tagy bezpečného předávání zpráv a používání příkazů s lichým-INS kódem ve shodě s aktuální verzí ISO/IEC 7816-4,
- další hašovací algoritmy (rodina SHA2) s příslušným identifikátorem objektu a odkazy na algoritmy,
- používání AES v autentizačních protokolech,
- používání AES pro bezpečné předávání zpráv.

Následující položky přesahují předmět tohoto dokumentu:

1. fyzikální a elektrické charakteristiky karty a charakteristiky protokolu přenosu,
2. proces externího vytváření podpisu a prostředí podpisu,
3. prvky požadované pro ověřování elektronického podpisu vytvořeného kartou použitou jako SSCD,
4. procesy pro ošetření chyb.