Napotki za razvijalce v zvezi z obstoječimi funkcionalnostmi in novimi karticami KZZ in PK

Nove kartice KZZ in PK zagotavljajo vse do sedaj obstoječe funkcionalnosti na hitrejšem in sodobnejšem čipu, uvajajo pa tudi številne novosti kot so brezstični vmesnik, podpora za eliptične algoritme, biometrijo. Za podporo novih kartic v obstoječih sistemih in na obstoječih funkcionalnostih so potrebne določene prilagoditve, ki jih bomo skušali zajeti v pričujočem dokumentu.

Glavne uporabniku oz. razvijalcu vidne spremembe obstoječih funkcionalnosti na novih PK/KZZ karticah v primerjavi s starimi:

* na kartice PK in KZZ je omogočen dolg zapis imena in priimka (do 130 znakov tako za ime kot za priimek) ter njegovo kodiranje po UTF-8
* na karticah PK in KZZ sta za vsako staro vrsto nekvalificiranega potrdila po novem zapisani po 2 potrdili (eno za uporabo za kriptiranje RSA in eno za eliptične krivulje), kar se lahko vidi v medprogramju Classic Client. Kvalificirano potrdilo na PK je še vedno eno samo za namene RSA kriptiranja dokumentov (npr. e-bolniški listi). Nekvalificirana potrdila imajo naslednji namen:
  + eno potrdilo na PK za prijavo v on-line sistem
  + eno potrdilo na KZZ za avtentikacijo zahtevkov v imenu zavarovanca
  + drugo potrdilo na KZZ za prijavo v zdravstveni portal (ta funkcionalnost se več ne uporablja, potrdilo pa je ohranjeno za morebitne razširitve v prihodnosti)
* nove KZZ ne podpirajo več kompatibilnostnega načina (delovanja kot kartice prve generacije brez digitalnih potrdil) zato morajo tudi v primeru izbire kompatibilnostnega načina uporabljati digitalna potrdila in ne smejo prožiti medsebojne avtentikacije za ponastavljanje števca dostopov do stare KZZ
* novo medprogramje ClassicClient je podprto na Windows sistemih ki so trenutno pod podporo Microsoft (Windows 10, 8.1, Server 2012/R2, Server 2016). Razvoj za Windows XP ter Windows 7 tako ni več relevanten.

Podpora in testiranje je smiselno za vse kombinacije kartic:

* nova PK in nova KZZ
* nova PK in stara KZZ
* nova PK in KZZ prve generacije (t.j. kartice brez digitalnih potrdil, če so le-te na voljo)
* stara PK in nova KZZ
* stara PK in stara KZZ
* stara PK in KZZ prve generacije (t.j. kartice brez digitalnih potrdil, če so le-te na voljo)

Dostop do kartic je v splošnem možen v povezavi z medprogramjem proizvajalca (Thales Classic Client) preko različnih tehnologij:

* MS CryptoAPI – podpira trenutne funkcionalnosti (RSA algoritmi) tako na starih kot novih KZZ in PK
* MS CNG (CryptoAPI Next Generation/CryptoAPI2) – nujen za uporabo eliptičnih algoritmov, vendar ne podpira trenutnih funkcionalnosti kartice
* PKCS#11 – podpira funkcionalnosti obeh generacij

Tu je potrebno opozoriti na izziv s katerim se bodo soočale vse rešitve, ki bazirajo na MS tehnologi CryptoAPI za uporabo RSA kritografije. Ob vpeljavi podpore za eliptične krivulje jih bo treba dopolniti še s CNG, saj vsaka tehnologija podpira svoj nabor kriptografskih algoritmov. Da bi torej delali hkrati z RSA in eliptičnimi algoritmi, je potrebno implemenitrati rešitev hkrati z CryptoAPI in CNG, ali pa rešitev enotno izvesti s pomočjo PKCS#11. Priporočamo da se zaradi hitrejše integracije začetno prilagoditev naredi samo v okviru podpore že obstoječih RSA funkcionalnosti.

V rešitvah je običajen tudi dostop do kartic preko nizkonivojskih ukazov APDU, s katerimi so realizirane nekatere operacije specifične za ZZZS KZZ in PK, ki jih splošna funkcionalnost medprogramja in zgoraj navedenih tehnologij ne podpira.

Prilagoditve so potrebne v odvisnosti od trenutne implementacije rešitve – če se uporabljajo posamezne operacije, je potrebno zanje narediti za nove kartice določene prilagoditve, kar skušamo ponazoriti v naslednjih razdelkih. Pri tem je potrebno poudariti da morajo stare kartice še vedno delovati na enak način kot doslej, zato se pri teh funkcionalnostih uvaja dualnost, t.j. različno delovanje za stare in nove kartice. Predlagamo da dokument uporabite tako da za vsako operacijo oz. tehnologijo v naslednjih razdelkih identificirate ali se uporablja v vaši rešitvi in preučite potrebne prilagoditve.

# APDU: Procesiranje vsebine datoteke EF.GDO in EF.HPD

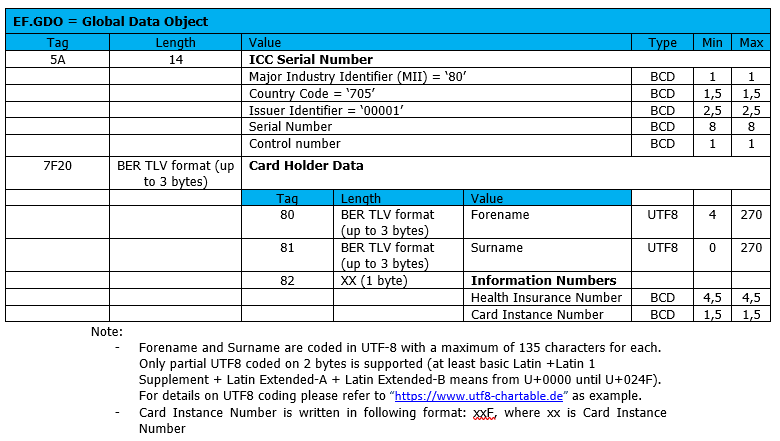
Ozadje:

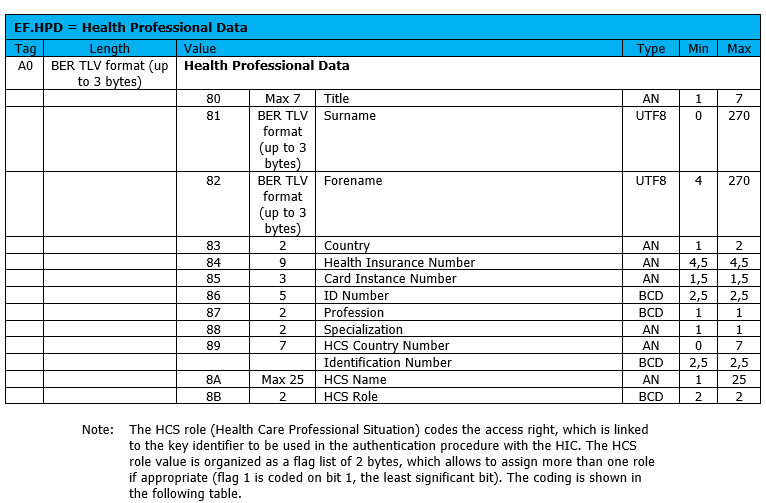
* Datoteki EF.GDO ter EF.HPD sta se na novih karticah spremenili tako, da podpirata dolga imena in priimke ter jih kodirata v UTF-8 zapisu.
* Datoteki sta na novih karticah dostopni šele po eksplicitnem izboru IASE aplikacije
* Datoteka GDO se uporablja za pridobitev podatkov o uporabniku kartice, HPD pa o izvajalcu storitev, uporablja se npr. za pridobitev reference ključa za resetiranje števca dostopov do 3DES ključa na prvi generaciji KZZ oz. v kompatibilnostnemu načinu delovanja starih KZZ.

Potrebne prilagoditve:

* z ukazom SELECT FILE je potrebno najprej narediti izbor IASE aplikacije šele nato izbor datotek GDO ali HPD
* uvesti je treba APDU veriženje (chaining) odziva kartice, da se lahko prebere vsebina datoteke, ki je dolga več kot 127 bajtov. Veriženje uvedemo s pomočjo izbire datoteke EF.GDO (SELECT FILE 2F 02) oz. EF.HPD (DD 01) in preberemo vsebino v več iteracijah (READ BINARY), kjer naslavljamo s parametroma P1 in P2 vsebino v datoteki. Več informacij na: <https://stackoverflow.com/questions/11297880/use-read-binary-to-read-more-than-256-bytes>
* Branje dolžine obeh datotek je potrebno izvesti tako, da najprej preberemo dolžino (max 3 bajti) s fiksne pozicije (v specifikacijah označena kot BER TLV format) in iz njega izračunamo dolžino preostanka datoteke (torej vsebina oz. value za Card Holder Data ter Health Professional Data), po TLV kodiranju, več na <https://stackoverflow.com/questions/60792080/how-to-parse-3-byte-length-ber-tlv-tag>. Dolžino variabilnega dela seštejemo z dolžino fiksnega dela in šele nato lahko z dobljeno pričakovano dolžino (Le) preberemo celotno datoteko

Nova specifikacija obeh datotek:





# APDU: Izbira IASE aplikacije

Ozadje: IASE ID aplikacije (AID) se je spremenil.

Potrebne prilagoditve:

* Za nove kartice je potrebno izbrati (SELECT FILE) novi AID – A0 00 00 00 18 40 00 00 01 63 42 00

# Branje ATR odziva kartic

Ozadje: vsaka vrsta kartice se sistemu identificira z edinstvenim ATR (Answer-To-Reset), novi PK in KZZ imata vsaka svoj nov ATR odziv, ki je drugačen od odzivov kartic prejšnjih generacij. Če uporablja rešitev odločanje glede na ATR odziv, je takšno logiko potrebno prilagoditi.

Potrebne prilagoditve:

* Rešitev naj predvidi ATR za nove kartice in sicer:
  + KZZ: 3B 7F 96 00 00 80 31 80 65 B0 85 04 01 20 F2 00 01 82 90 00
  + PK: 3B 7F 96 00 00 80 31 80 65 B0 85 04 01 20 F2 00 02 82 90 00

# Odstranitev kompatibilnostnega načina iz novih KZZ

Ozadje: nove KZZ ne uporabljajo več kompatibilnostnega načina, v katerem simulirajo delovanje prve generacije KZZ, ki še niso imele digitalnih potrdil. Kompatibilnostni applet ZZZS je bil z novih KZZ fizično odstranjen in ga ni mogoče več izbrati (SELECT FILE). Na novih PK je kompatibilnostni applet še vedno prisoten, saj morajo podpirati tudi KZZ starejših generacij.

Potrebne prilagoditve:

* Če aktiviramo v rešitvi kompatibilnostni applet je potrebno predvideti, da ta več ne obstaja, in da bo poskus izbire (SELECT FILE) vrnil odziv z napako.
* Potrebno je poskrbeti za vse kombinacije kartic, z novo KZZ kompatibilnostni način ne deluje, z vsemi ostalimi kombinacijami pa.

# PKCS#11: Uporaba varnega vnosa PIN preko zunanje tipkovnice (PinPada)

Ozadje: novo medprogramje ne dopušča več vnosa -1 kot dolžine PIN-a, da sproži varni vnos preko hardverske naprave (PinPad čitalca, če ta obstaja), potrebno je uporabiti dolžino 0.

Potrebne prilagoditve:

* V klicu funkcije C\_Login je potrebno podati kot parameter ulPinLen vrednost 0 in ne -1, kot je bilo možno pri prejšnji različici medprogramja.

# Sprememba referenčne številke podpisnega PIN-a

Ozadje: nove PK imajo referenčno številko podpisnega PIN-a za kvalificirano potrdilo zamaknjeno na številko HEX 82 v primerjavi s številke HEX 83 na starih PK. Pregled PINov na starih in novih PK je v naslednji tabeli:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Stara PK | Stara PK brez KDP | Nova PK | Nova PK brez KDP |
| Globalni PIN (Uporabniški PIN za HPC-Entry) | HEX 11 | HEX 11 | HEX 11 | HEX 11 |
| SO PIN (PUK/Skrbniški PIN za HPC-Entry) | HEX 82 | HEX 81 | HEX 81 | HEX 81 |
| BioPIN (prstni odtis za HPC-Entry) | Brez | Brez | HEX 21 | HEX 21 |
| Podpisni PIN (Uporabniški PIN za HPC-Qualified) | HEX 83 | Brez | HEX 82 | Brez |
| Transportni PIN | HEX 84 | Brez | HEX 83 | Brez |

Potrebne prilagoditve:

* Če rešitev uporablja delo s podpisnim PINom za PK (bodisi preko APDU, PKCS#11 ali CAPI), je potrebno reference za nove PK prestaviti iz 0x83 na 0x82.
* Če rešitev naslavlja še katere od v tabeli navedenih spremenjenih PIN-ov je treba tudi zanje narediti ustrezno razlikovanje

# PKCS#11/CAPI: Naslavljanje slotov/containerjev kartice

Ozadje: nove kartice imajo dodatne slote (v PKCS#11 svetu) oz. containerje (v CAPI svetu) za vsa dozdajšnja nekvalificirana potrdila. Poleg »HIC-Entry«, »HPC-Entry«, »HIC-Portal« slotov imamo še dodatne slote za nekvalificirana potrdila ki omogočajo podpisovanje z algoritmi kriptografije eliptičnih krivulj, z imeni po vrsti »HIC-Entry-EC«, »HPC-Entry-EC«, »HIC-Portal-EC«. Dvojna potrdila omogočajo postopen prehod na uporabo kritpografijo z eliptičnimi krivuljami. Kvalificirano potrdilo ostaja na PK le eno, ker izdajatelj za zdaj še ne ponuja kvalificiranih potrdil s podporo za eliptične krivulje.

Potrebne prilagoditve:

* Načeloma nič, iskanje containerjev/slotov eksplicitno po imenu ali enumeriranje vseh containerjev/slotov na kartici in sprehod po njih bi morala zagotoviti da se iskano potrdilo najde, pozornost je treba nameniti le performansam (ali je enumeracija in sprehod po potrdilih dovolj hitro, načeloma je eksplicitno nalaganje po imenu hitrejše) in pravilnosti (da se eliptična potrdila zaenkrat preskočijo, saj je v prvi fazi potrebna prilagoditev aplikacij da v njih delujejo že obstoječe funkcionalnosti tudi z novimi karticami)