

**TVORÍME VEDOMOSTNÚ SPOLOČNOSŤ**

**x104 Integračný manuál pre IS PZS**

Projekt je spolufinancovaný Európskou úniou  
 Európsky fond regionálneho rozvoja

d

dd

Európsky fon

**Elektronické služby zdravotníctva**

kód ITMS projektu: **2110120009**

www.informatizacia.sk  
 www.opis.gov.sk

**Základné informácie o dokumente**

|  |  |
| --- | --- |
| **Šablóna dokumentu** | eSO1\_SB\_Projektovy\_dokument\_20111116\_3.0 |
| **Názov dokumentu** | eZdravie\_Integracny\_manual\_pre\_IS\_PZS\_x104\_v2.29 |
| **Aktuálna verzia** | 2.29 |
| **Status** | Aktualizácia |
| **Vlastník dokumentu** | Integrácia ISPZS |

**História dokumentu**

|  |  |  |  |
| --- | --- | --- | --- |
| **Verzia** | **Dátum** | **Autor** | **Popis verzie a zmien oproti predchádzajúcej verzii** |
| 1.0 | 28.5.2015 | Vladimír Polák | Vytvorenie dokumentu |
| 2.0 | 13.07.2015 | Peter Mešťaník | Úprava dokumentu v súvislosti s rozšírením o prostredie PREPROD |
| 2.1 | 16.07.2015 | Peter Mešťaník | Zapracovanie pripomienok k verzii 2.0 |
| 2.2 | 06.11.2015 | Peter Mešťaník | Rozšírenie dokumentu o prostredie PROD |
| 2.3 | 05.12.2015 | Peter Mešťaník | Zapracovanie pripomienok k verzii 2.2, premiestnenie všetkých binárnych súborov do externej adresárovej štruktúry |
| 2.4 | 25.2.2016 | Peter Mešťaník | Aktualizácia TechnologickyChecklistPripojenieISPZS.docx |
| 2.5 | 10.5.2016 | Gabriel Benko | Aktualizácia TechnologickyChecklistPripojenieISPZS.docx |
| 2.6 | 21.7.2016 | Roland Virág | Aktualizácia umiestnenia príkladu implementácie pre Visual Studio |
| 2.7 | 9.8.2016 | Roland Virág | Aktualizácia CryptoControllera na verziu 4.1.3 |
| 2.8 | 17.8.2016 | Roland Virág | Zmena CryptoControllera na verziu 4.1.1, kvôli chybe vo verzii 4.1.3 |
| 2.9 | 29.9.2016 | Roland Virág | Aktualizácia popisu inštalácie certifikátov a sekcie 7.5; Aktualizácia NzisServicesCertificates.xml pre prostredie PROD |
| 2.10 | 10.10.2016 | Roland Virág | Aktualizácia CryptoControlleru na verziu 4.1.4 |
| 2.11 | 8.11.2016 | Vladimír Polák | Aktualizácia príkladu postupu v Delphi |
| 2.12 | 18.1.2017 | Vladimír Polák | Aktualizované:   * Súbor „NzisServicesCertificates.XML“ pre PROD prostredie * CryptoControlleru na verziu 4.2.1 v prílohách * Doplnený funkčný príklad konfigurácie pre každé prostredie, súbor „Iam.Client.CryptoController.dll.config“ * v kapitole 8.1 doplnená exception z CryptoControlleru * odstránený popis integrácie pre prostredie RIP * pridané do dokumentu TechnologickyChecklistPripojenieISPZS.docx podklady pre integráciu na XP a to: Windows Identity Foundation a knižnicu msvcr120.dll |
| 2.12 | 10.11.2016 | Roland Virág | Aktualizácia textu pre Iam.Client.CryptoController.dll (4.2.4, 5.2.4);  Aktualizácia TechnologickyChecklistPripojenieISPZS.docx |
| 2.13 | 14.2.2016 | Martin Ret | Zlúčenie modifikácií dokumentu |
| 2.14 | 17.2.2016 | Martin Ret | Zapracovanie CR 101429 – pripojenie bez VPN pomocou SSL |
| 2.15 | 30.3.2017 | Vladimír Polák | Doplnená kapitola „8.1 Príloha E1 – Možné issues s konfiguráciou CC.DLL“  Spresnenie formulácie „8.2 Príloha A - Príklad implementácie volania služby vo forme unit testu vo Visual Studio“ |
| 2.16 | 18.5.2017 | Martin Ret | Doplnená informácia o obmedzeniach pri pripojení na PREPROD prostredie pomocou SSL (kap. 0)  V rámci prílohy x104\_Binary.zip aktualizované súbory x104\_Binary\Prostredia\PREPROD\Certificates\services.preprod.npz.sk.crt  A  x104\_Binary\Prostredia\PREPROD\ECC\NzisServicesCertificates.xml |
| 2.17 | 15.8.2017 | Ján Kuruc | Formálne úpravy. Doplnený obrázok mapa dokumentov  Doplnená nová čitačka ePZP kariet  X104\_Binary.zip  nové certifikáty ESB: x104\_Binary\Prostredia\PREPROD\Certificates\services.preprod.npz.sk.der  x104\_Binary\Prostredia\PROD\Certificates\services.prod.npz.sk.der  nové šifrovacie certifikáty:  x104\_Binary\Prostredia\PREPROD\ECC\NzisServicesCertificates\_preprod.xml  x104\_Binary\Prostredia\PROD\ECC\NzisServicesCertificates\_preprod.xml |
| 2.19 | 27.9.2017 | Ján Kuruc | Doplnené koncové body kap 4.1.4 a 5.1.4  Zmena Minidrivra v rámci príloh IDPrime 830 – v 8.5.04 zmena na 8.5.0.5 - x104\_Binary\Install\Gemalto\_Minidriver.zip  Doplnene ID čítačky a navigácie prostredníctvom riadiaceho pavúka |
| 2.20 | 27.12.2017 | Ján Mikolaj | Finalizácia dokumentu – korekcia chýb |
| 2.22 | 31.1.2018 | Ján Mikolaj | Doplnený CC pre HSM |
| 2,23 | 28.3.2018 | Gabriel Benko | Doplenené URL pre SSL, auth. pre eLAB pomocou certifiátov v HSM |
| 2.24 | 26.4.2018 3.10.2018 | Ján Mikolaj Pavol Sidó | Doplnené odkazy na certifikáty a URL adresy pre IAM B2B Finalizácia dokumentu – korekcia chýb a vyrovnanie zmien z dôvodu prehľadnosti |
| 2.25 | 3.7.2019 | Pavol Sidó | Aktualizovaná kapitola eID klient (PPP aplikácia) Aktualizovaný driver pre čítačku REINER SCT a informácia pre inštaláciu na WIN XP a Vista Odstránená kapitola Prostredie DEV |
| 2.26 | 8.9.2020 | Integrácia ISPZS | Aktualizácia dokumentu o nové certifikáty platné pre ePZP karty vydané po 1.7.2020. |
| 2.27 | 13.11.2020 | Integrácia ISPZS | Upravená kapitola 2.2.3 Konfigurácia natavení čítačiek eID v Aplikácii PPP a Aplikácii pre eID (Pôvodný názov kapitoly: Nová funkcionalita)  Doplnené príklady nastavenia Aplikácie PPP a Aplikácie eID pre korektnú komunikáciu s podporovanými čítačkami eID |
| 2.28 | 2.6.2021 | Integrácia ISPZS | Upravená kapitola 2.2. Aplikácia PPP – zmena verzie aplikácie PPP na 1.3.0 |
| 2.29 | 1.11.2021 | Integrácia ISPZS | Upravená kapitola 7.5.2 Zapezpečenie komunikácie medzi IS PZS a NCZI – doplnený návod pre problém s opakovaným vyžadovaným PIN pre ePZP kartu. |
| 2.30 | 25.3.2022 | Integrácia ISPZS | Upravená kapitola 3.4. – zmena end pointov na prostredí preprod |
| 2.31 | 24.1.2023 | Oddelenie IT Štandardov | Upravená kapitola 1.1 Doplnenie integračných manuálov za služby eDPN, eRecept, HoN, eOckovanie.  Dokument: aktulizácia verzie PPP na 4.4  Dokument: Vyradenie nepodporovaných OS win 7, XP, 8  Aktualizácia end pointov PROD |

**Akceptačné riadenie**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Odberateľ** | | | **Dodávateľ** | | |
| **Dátum** | **Meno (Rola)** | **Podpis** | **Dátum** | **Meno (Rola)** | **Podpis** |
|  |  |  |  |  |  |

**Súvisiace produkty a referenčné materiály**

|  |  |
| --- | --- |
| **ID** | **Názov dokumentu a referencia** |
|  | Základne informácie sú dostupné:  https://www.ezdravotnictvo.sk/sk/dodavatel-is/uvod |

# Obsah

[1. Obsah 5](#_Toc125703967)

[1 Úvod 17](#_Toc125703968)

[1.1 Účel dokumentu 17](#_Toc125703969)

[1.2 Rozsah 18](#_Toc125703970)

[1.3 Cieľová skupina 19](#_Toc125703971)

[1.4 Pojmy a skratky 19](#_Toc125703972)

[2 Prerekvizity 20](#_Toc125703973)

[2.1 Technologický checklist 20](#_Toc125703974)

[2.2 Aplikácia PPP 20](#_Toc125703975)

[2.2.1 Defaultne odporovaná čítačká: 20](#_Toc125703976)

[2.2.2 Konfigurácia natavení čítačiek eID v Aplikácii PPP a Aplikácii pre eID: 21](#_Toc125703977)

[2.2.3 ODOSIELANIE LOGOV NA SERVER – DRAFT verzia procesu 22](#_Toc125703978)

[2.2.4 Integrácia 27](#_Toc125703979)

[2.3 Čítačka čipových kariet eID 28](#_Toc125703985)

[2.4 Čítačky čipových kariet ePZP 29](#_Toc125703986)

[2.5 ePZP karta 31](#_Toc125703987)

[2.5.1 Middleware pre čipové karty 31](#_Toc125703988)

[2.5.2 Čipová karta SafeNet eToken 4100 32](#_Toc125703989)

[2.5.3 Čipová karta Gemalto IDPrime 830 32](#_Toc125703990)

[2.5.4 Čipová karta Thales IDPrime 930 32](#_Toc125703991)

[2.6 Sieťový prístup do prostredí 32](#_Toc125703992)

[2.6.1 VPN klient 33](#_Toc125703993)

[2.7 Verejné kľúče 33](#_Toc125703994)

[2.8 IAM B2B Klientsky komponent 33](#_Toc125703995)

[3 Prostredie PREPROD 36](#_Toc125703996)

[3.1 Spôsob prístupu 36](#_Toc125703997)

[3.2 Prerekvizity konektivity – prístupu na PREPROD 36](#_Toc125703998)

[3.2.1 Koreňové certifikáty 36](#_Toc125703999)

[3.2.2 Certifikát ESB 36](#_Toc125704000)

[3.2.3 Certifikáty prostredia PREPROD 36](#_Toc125704001)

[3.2.4 EHealthCryptoController 37](#_Toc125704002)

[3.2.5 Konfigurácia Iam.Client.CryptoController.dll 37](#_Toc125704003)

[3.2.6 Konfigurácia Iam.B2B.Client.CryptoController 37](#_Toc125704004)

[3.2.7 DNS 37](#_Toc125704005)

[3.2.8 VPN 38](#_Toc125704006)

[3.3 Publikačný portál NCZI 39](#_Toc125704007)

[3.4 Overenie prístupu – dostupnosť end pointov 39](#_Toc125704008)

[4 Prostredie PROD 40](#_Toc125704009)

[4.1 Spôsob prístupu 40](#_Toc125704010)

[4.2 Prerekvizity konektivity – prístupu na PROD 40](#_Toc125704011)

[4.2.1 Koreňové certifikáty 40](#_Toc125704012)

[4.2.2 Certifikát ESB 40](#_Toc125704013)

[4.2.3 Certifikáty prostredia PROD 40](#_Toc125704014)

[4.2.4 EHealthCryptoController 40](#_Toc125704015)

[4.2.5 Konfigurácia Iam.Client.CryptoController.dll 40](#_Toc125704016)

[4.2.6 Konfigurácia Iam.B2B.Client.CryptoController 41](#_Toc125704017)

[4.2.7 DNS 41](#_Toc125704018)

[4.2.8 VPN 42](#_Toc125704019)

[4.3 Publikačný portál NCZI 43](#_Toc125704020)

[4.4 Overenie prístupu – dostupnosť end pointov 43](#_Toc125704021)

[5 Nástroje a vstupy pre integráciu 44](#_Toc125704022)

[5.1 Špecifikácia rozhrania IM 44](#_Toc125704023)

[5.2 Nástroj na čítanie archetypov 44](#_Toc125704024)

[5.3 Najzákladnejšie body volania NZIS služby 44](#_Toc125704025)

[5.4 Zoznam služieb a procesov na integráciu 44](#_Toc125704026)

[6 Podpora 44](#_Toc125704027)

[6.1 Kontaktné osoby 44](#_Toc125704028)

[7 Prílohy 46](#_Toc125704029)

[7.1 Príloha E1 – Možné issues s konfiguráciou CC.DLL 46](#_Toc125704030)

[7.1.1 Chyba 1: 46](#_Toc125704031)

[7.1.2 Chyba 2: 46](#_Toc125704032)

[7.2 Príloha A - Príklad implementácie volania služby vo forme unit testu vo Visual Studio 47](#_Toc125704033)

[7.3 Príloha B - Príklad inicializácie CryptoControllera v Delphi 47](#_Toc125704034)

[7.4 Príloha C - Príklad implementácie volania služby v Delphi 52](#_Toc125704035)

[7.5 Príloha D – Technologický checklist 52](#_Toc125704036)

[7.5.1 Technické požiadavky klientských staníc ISPZS 52](#_Toc125704037)

[7.5.2 Zabezpečenie komunikácie medzi IS PZS a NZIS 56](#_Toc125704049)

# Úvod

## Účel dokumentu

Dokument slúži ako sprievodná dokumentácia procesu implementácie integrácie vendorov IS PZS na prostredie PREPROD a PROD v správe NCZI.

Hierarchiu a väzby jednotlivých dokumentov tvoriacich integračné postupy a implementačné štandardy nájdete ako rozcestník v maúovacom pavúku priamo v root adresári IM ( **Mapovaci\_pavuk\_vx.x.x.pptx** ).

Riadiace dokumenty:

Dokument vychádza z podkladov a je plne v súlade s požiadavkami uvedenými v nadradenom dokumente vydávanom NCZI, „**Metodika integrácie informačného systému s NZIS**“ a „**Procesne scenáre služieb**“ dostupnom na webe NCZI <https://www.ezdravotnictvo.sk/sk/dodavatel-is/dokumenty> .

**eZdravie\_Integracny\_manual\_pre\_IS\_PZS\_(x104)\_x\_xx.doc, je vstupným rozcestníkom pre dokumentáciu, obsahuje v zmysle obrázku:**

* Popis integračného prostredia, prístupy cert,
* Prerekvizity – Nástroje (SW – drivery a knižnice, HW-čítačky karty)
* Príklady implementácie
* **TechnologickyChecklistPripojenieISPZS.docx**
  + Podporovane OS
  + SW požiadavky
  + HW požiadavky / drivery / čítačky a karty
* **x104\_Binary\_x\_xx.zip**
  + Príklady implementácie delphi
  + eHealthCryptoConttroller (ECC) knižnica DLL
  + Cert (ECC, ESB, root..) – pre PROD aj PREPROD
  + Inštalačné súbory, drivre pre čítačky

Neoddeliteľnou súčasťou tohto dokumentu sú nasledovné dokumenty aj s prílohami:

* [X070] - špecifikácia rozhrania NZIS, ktorý detailne popisuje rozhranie služieb NZIS.
  + Volanie služieb - Dokument definujúci sadu mechanizmov výmeny správ(**x070E\_RFRS\_Detailna\_specifikacia\_rozhrania\_Volanie\_sluzieb\_x\_xx.docx**)
    - Obsahuje informáciu o princípoch volania služieb, bezpečnostných a autentifikačných mechanizmoch, nutných technických predpokladoch, zoznam generálnych výnimiek a pod.
* ezdravie\_evysetrenie\_IM\_XXXX\_vX.X.docx - Integračný manuál (IM) detailne popisuje rozhranie služieb eVysetrenia
* ezdravie\_elab\_IM\_XXXX\_vX.X.docx -  Integračný manuál (IM) detailne popisuje rozhranie služieb eLab
* ezdravie\_eobjednanie\_IM\_XXXX\_vX.X.docx -  Integračný manuál (IM) detailne popisuje rozhranie služieb eObjednanie
* ezdravie\_eDPN\_IM\_XXXX\_vX.X.docx - Integračný manuál (IM) detailne popisuje rozhranie služieb eDPN
* ezdravie\_HoN\_IM\_XXXX\_vX.X.docx - Integračný manuál (IM) detailne popisuje rozhranie služieb HoN
* ezdravie\_eRecept\_IM\_XXXX\_vX.X.docx - Integračný manuál (IM) detailne popisuje rozhranie služieb eRecept

ezdravie\_eOckovanie\_IM\_XXXX\_vX.X.docx - Integračný manuál (IM) detailne popisuje rozhranie služieb eOckovanie

ezdravie\_xservices\_vX\_IM\_XXXX.docx -  Integračný manuál (IM) detailne popisuje Spoločné služby na podporu procesov PZS.

* ezdravie\_eRecept\_IM\_XXXX\_vX.X.docx eRecept - špecifikácia rozhrania služieb eZdravie\_eRecept
  + Integračný manuál (IM) detailne popisuje rozhranie služieb eRecept (**ezdravie\_erecept\_IM\_YYYMMDD\_vXX.docx**)
  + Číselníky (**ezdravie\_erecept\_IM\_cis\_pre\_Davkovanie\_vXX.xlsx**)
  + Schémy
    - eRecept WSDL
* Prehľad služieb - Dokument popisuje sadu dostupných služieb, ich základné atribúty, popis (**x070E\_RFRS\_Detailna\_specifikacia\_rozhrania\_Prehlad\_sluzieb**)
  + Obsahuje zoznam všetkých WS služieb. Pri každej službe je uvedený účel, popis, odkaz na I/O rozhranie.
* **x070\_Exceptions\_list.xls**
  + Zoznam výnimiek, pre konkrétny službu s uvedením kódu výnimky a dôvodu, pre ktorý môže byť správa odmietnutá.
* **x070E\_Html\_format.xlsx**
  + Povolené HTML tagy v rámci HTML textov.
* **Schémy**
  + Obsahuje zoznam archetypov (\*.adl) a xsd schém (\*.xsd), ktoré špecifikujú štruktúru dátovej časti rozhrania služieb.
  + Špecifikovanie finálnych URL k WSDL schémam bude predmetom integračného balíka. WSDL schémy sú uvedené v prílohe “.\Schemy\COMMON\WSDL”.
  + OID identifikátory jednotlivých entít odkazovaných pri komunikácii sú zverejnené na stránkach www.nczisk.sk.
* **Príklady**
  + Príklady volaní a príklady odpovedí na volanie služieb zaradených do balíkov podľa jednotlivých domén. Názov súboru s príkladu volania korešponduje s názvom služby.
  + Odkazy na kontext používateľa, autentifikačné tokeny, číselníkové položky a dáta v príkladoch su orientačné a nie sú aplikovateľné v reálnej implementácii.

Obsahom tohto dokumentu sú doplňujúce informácie k vyššie uvedenému dokumentu NCZI.

## Rozsah

Cieľom dokumentu je popísať integračné prostredie, prístup na prostredie a spôsob overenia základnej funkcionality.

## Cieľová skupina

Dokument je určený pre vendorov IS PZS, ktorí participujú v procese testovania integrácie.

## Pojmy a skratky

|  |  |
| --- | --- |
| Pojem/Skratka | Definícia |
| NZIS | Národný zdravotnícky informačný systém |
| ISPZS | Informačný systém PZS |
| CC.DLL | EHealthCryptoController |
| ESID | Šifrovaný identifikátor |
| PrZS | Prijímateľ zdravotnej starostlivosti |
| ZPr | Zdravotnícky pracovník |
| ZP | Zdravotná poisťovňa |
| PZS | Poskytovateľ zdravotnej starostlivosti |
| OUPZS | Odborný útvar PZS |
| PPP aplikácia | Potvrdenie prítomnosti pacienta |
| HoN | Hlásenie o narodení |
| eDPN | Elektronická dočasná práce neschopnosť |
| eID | Elektronický občiansky preukaz |
| WIF | Windows Identity Foundation |
| OS | Operačný systém |
| IM | Integračný manuál |
| ePZP | Elektronický preukaz zdravotnického pracovníka |
|  |  |

# Prerekvizity

## Technologický checklist

Technologický checklist je súčasťou **prílohy D** tohto dokumentu popisujúci podrobné požiadavky na pripojenie počítača s nainštalovaným ISPZS k ľubovoľnému z nižšie popisovaných prostredí. Niektoré požiadavky/aplikácie sú v tomto dokumente popísané podrobnejšie.

## Aplikácia PPP

Na využívanie funkcionality eID kariet vo vybraných procesných scenároch je potrebné mať nainštalovanú aplikáciu PPP. Inštalačný súbor samotnej PPP aplikácie verzia 4.4. (Potvrdenie prítomnosti pacienta) je dostupná na integračnom portáli IS PZS (service desk) Samoobslužné centrum/Prehľad dokumenty a formuláre/Aplikácie a nástroje/Aplikácia PPP

Aplikácia PPP zamedzí prístup Aplikácii pre eID k čítačkám vyhradeným pre potvrdzovanie prítomnosti pacienta.

Pozn.: **Podporované od verzie 3.2.1 Aplikácie pre eID**

Podporované OS platformy:Windows 8.1 32/64bit,

Windows 10 32/64bit

Windows 11 32/64 bit

### Defaultne odporovaná čítačká:

Reiner SCT cyberJack one

Poskytnuté ovládače k čítačke Reiner SCT sú funkčné na všetkých podporovaných platformách.

Aplikácia je defaultne nakonfigurovaná tak, aby počúvala iba na čítačke Reiner SCT CyberJack one.

### Konfigurácia natavení čítačiek eID v Aplikácii PPP a Aplikácii pre eID:

**MANUÁLNE ROZŠÍRENIE MNOŽINY ČÍTAČIEK, NA KTORÝCH BUDE APLIKÁCIA PPP POČÚVAŤ:**

Zoznam čítačiek, na ktorých Aplikácia PPP počúva, je definovaný v konfiguračnom súbore readers.ini.

Súbor sa podľa verzie OS môže nachádzať v nasledovných ceste

* C:\ProgramData\Aplikacia\_PPP\readers.ini

Formát súboru:

Parameter includedReaders - ak je špecifikovaný, obsahuje zoznam čítačiek, na ktorých má aplikácia počúvať.

príklad: includedReaders="REINER SCT cyberJack one MF"

Pozn.1: zoznam čítačiek musí byť ohraničený úvodzovkami

Pozn.2: oddeľovačom zoznamu je čiarka bez medzier

Pozn.3: aplikácia kontroluje názov čítačky na "začínajúci reťazec", napr. zadaním len "REINER" sa pridajú všetky čítačky od výrobcu REINER

Pozn.4: aplikácia si súbor readers.ini načíta pri štarte aplikácie

**Príklad pre nastavenie súboru readers.ini v Aplikácii PPP pre použitie čítačky Reiner SCT cyberJack one (default nastavenie po inštalácii):**

[General]

includedReaders="REINER SCT cyberJack one MF"

**Príklad pre nastavenie súboru readers.ini v Aplikácii PPP pre použitie čítačky HID OMNIKEY 3121:**

[General]  
includedReaders="HID Global OMNIKEY 3x21 Smart Card Reader,OMNIKEY CardMan 3x21"

**ZAMEDZENIE PRÍSTUPU APLIKÁCIE PRE EID K ČÍTAČKÁM VYHRADENÝM PRE POTVRDZOVANIE PRÍTOMNOSTI PACIENTA**

Aplikácia PPP pri svojej inštalácii nastaví pre Aplikáciu pre eID špeciálnu konfiguráciu, cez ktorú si rezervuje čítačku Reiner SCT CyberJack One výhradne pre overovanie prítomnosti pacienta.

Uvedenú konfiguráciu inštalátor uloží do súboru

• C:\ProgramData\eID\_klient\readers.ini (vo Windows 10 a vyššie), resp. do súboru

• C:\Documents and Settings\All Users\Application Data\ EAC\_MW\_klient\readers.ini

Formát súboru:

Parameter excludedReaders - ak je specifikovany, obsahuje zoznam citaciek, na ktorych ma aplikacia zakazane pocuvat.

priklad: excludedReaders="REINER SCT cyberJack one MF"

Ak Aplikácia pre eID v systéme nájde uvedenú konfiguráciu, vylúči v nej definované čítačky zo svojho zoznamu čítačiek, na ktorých bude počúvať.

Pozn.1: zoznam čítačiek musí byť ohraničený úvodzovkami.

Pozn.2: oddeľovačom zoznamu je čiarka bez medzier.

Pozn.3: aplikácia kontroluje názov čítačky na "začínajúci reťazec", napr. zadaním len "REINER" sa vylúčia všetky čítačky od výrobcu REINER.

Pozn.4: aplikácia si súbor readers.ini načíta pri štarte aplikácie.

Uvedené riešenie predpokladá:

• u lekárov bude na účel overovania prítomnosti pacientov používaná výhradne čítačka Reiner SCT CyberJack One;

• v lekárňach na predajných PC, aj keď tam môžu byť použité aj iné čítačky (napr. HID OMNIKEY 3121), je predpoklad, že tam Aplikácia pre eID nebude nainštalovaná (kvôli vyskakujúcemu zadávaniu BOK po vložení eID do čítačky);

**V prípade, že sa na PC používa čítačka HID OMNIKEY 3121 a okrem Aplikácie PPP je nainštalovaná aj Aplikácia pre eID, je nutné upraviť súbor readers.ini Aplikácie pre eID nasledovne:**

[General]  
excludedReaders="REINER SCT cyberJack one MF,HID Global OMNIKEY 3x21 Smart Card Reader,OMNIKEY CardMan 3x21"

### ODOSIELANIE LOGOV NA SERVER – DRAFT verzia procesu

Aplikácia umožňuje používateľom odoslať logy na server na „jeden klik“ spôsobom, aký zvládnu aj menej zdatní používatelia. Tým sa postup riešenia incidentov celkovo zjednoduší, zároveň sa zjednodušia úkony pre používateľov a urýchli sa proces vybavovania jednotlivých hlásení.

Poznámka:Tento proces bude odladený počas pilotného testovania a final verzia bude uverejnená v IM.

#### Popis riešenia odosielania logov z PPP aplikácie na server

Cieľom uvedeného riešenia je uľahčenie poskytnutia logov aplikácie operátorkám Centra podpory NCZI (a následne poskytovateľovi podporných služieb) pri riešení incidentov cez centrum podpory. Riešenie umožňuje používateľom aplikácie odoslať logy na server na „jeden klik“ spôsobom, aký zvládnu aj menej zdatní používatelia. Tým sa postup riešenia incidentov celkovo zjednoduší, zároveň sa zjednodušia úkony pre používateľov a urýchli sa proces vybavovania jednotlivých hlásení.

PPP aplikácia poskytuje dva hlavné scenáre, keď bude používateľ môcť odoslať logy na server:

scenár 1: v prípade, keď chyba nastane priamo v aplikácii, napr. v procese overenia prítomnosti pacienta, alebo

scenár 2: v prípade, keď problém alebo chyba nastane v inom prípade súvisiacom s aplikáciou (napr. aplikácia nenačíta kartu, príp. iné)

V jednotlivých scenároch bude odosielanie logov prebiehať nasledovne:

scenár 1: používateľ bude môcť logy odoslať priamo z okna, v ktorom bola chyba zobrazená – viď obr. 1) odoslanie logov pri chybe nižšie,

scenár 2: používateľ bude môcť v menu aplikácie zvoliť možnosť odoslania logov na server – viď obr. 2) odoslanie logov z menu nižšie.

V oboch prípadoch je používateľ po odoslaní logov vedený k tomu, že pre pokračovanie v riešení svojho problému má zavolať na centrum podpory.

Pre párovanie odoslaných logov k hlásenému incidentu je navrhnutý mechanizmus, keď pri odoslaní logov na server bude vygenerovaný špeciálny (pre používateľa ľahko zapamätateľný) kód. Tento kód používateľ jednoducho nadiktuje operátorke (namiesto náročného hľadania lokálnych logov v lokálnej súborovej štruktúre, ich zo-zipovania a posielania emailom).



Obrázok 1



Obrázok 2

### Integrácia

Spôsob integrácie na PPP aplikácie je založený na rovnakých princípoch, ako to bolo v prípade Aplikácie pre eID, t.j. cez lokálne http rozhranie.

**PPP aplikácia však počúva na lokálnom porte 15481** (pre porovnanie, Aplikácia pre eID počúva na porte 15480).

Pre spustenie procesu potvrdenia prítomnosti pacienta prostredníctvom PPP aplikácie je potrebné z eHealth Crypto Controllera na lokálny port **15481** poslať požiadavku http GET v tvare:

http://localhost:15481/?tcTokenUrl=<URL generovaná AS serverom v metóde useID>

Príklad:

http://localhost:15481/?tcTokenUrl=https%3a%2f%2feidas.minv.sk%2fSessionToken%2fTCToken%3ftcTokenId%3d545985be16b4f6f2d0bf

Upozornenie:

Na PREPROD sa môže stať, že sa nedotiahne SNCA2 certifikát medzi dôveryhodné koreňové certifikačné autority. Certifikát je v priložených súboroch eZdravie\_Tech\_manual\x104\_Binary\_2\_23\x104\_Binary\Prostredia\PREPROD\Certificates

## Čítačka čipových kariet eID

Z dôvodu potreby využívania elektronických občianskych preukazov pre získanie potvrdenie prítomnosti pacienta je nevyhnutné mať okrem nainštalovaného eID klienta, mať pripojenú a nainštalovanú aj príslušnú čítačku elektronických občianskych preukazov. Momentálne bola otestovaná kompatibilita nasledovných typov čítačiek eID:

1. HID OMNIKEY 3121 – čítačka bez numerickej klávesnice



Čítačka je funkčná so štandardným driverom dodávaným OS windows

1. ReinerSCT - čítačka s numerickou klávesnicou



Príslušný driver k čítačke je možné nájsť v priložených súboroch na ceste x104\_Binary**\_x\_xx**\Install\16\_bc\_7\_5\_6b.exe

## Čítačky čipových kariet ePZP

Nakoľko sa používajú ePZP karty je potrebné mať nainštalovaný driver pre čítačku čipových kariet.

**Čítačka čipových kariet**

Pre správnu funkciu tejto verzie komponentu je potrebné mať nainštalovanú aspoň jednu čítačku čipových kariet (Smart Card Reaeder)

Aktuálna verzia komponentu CryptoController bola testovaná s  čítačkami

1. „OMNIKEY 3021 USB“ (viď obrázok)



1. Gemalto IDBridge CT30 (pôvodné označenie „Gemalto PC USB TR“)



Pre korektné fungovanie je potrebné mať nainštalovaný aj originálny ovládač k príslušnej čítačke:

* Pre čítačku typ „A“ bol testovaný ovládač HID Global, verzia 1.2.6.5  
  

Driver je možné nájsť na ceste x104\_Binary**\_x\_xx**\Install\OMNIKEY\_3x21\_USB\_CardReader\_Driver.zip

* Pre čítačku typu „B“ bol testovaný ovládač Gemalto, verzia 4.1.3.1  
  

Driver je možné násjť na ceste x104\_Binary**\_x\_xx**\Install\GemPcCCID.exe

UPOZORNENIE

Pri výmene jednotlivých čítačiek je nevyhnutné dbať na to aby boli korektne odinštalované staré ovládače a nainštalované nové. Neodporúčame mať na jednej klientskej stanici nainštalované súčasne ovládače oboch čítačiek kariet.

Komponent môže fungovať aj s inými verziami čítacích zariadení čipových kariet, no jeho správne fungovanie nie je zaručené.

## ePZP karta

### Middleware pre čipové karty

Pre korektnú komunikáciu medzi ISPZS a ePZP kartou je potrebné mať nainštalovaný driver pre ePZP karty. Middleware je popísaný pre príslušnú čítačku kariet.

Ako karty zdravotníckych pracovníkov (ePZP karty) budú použité karty nasledovného typu (rozlíšenie je možné aj vizuálne na základe tvaru plochy elektronického čipu)

1. SafeNet eToken 4100.



1. Gemalto IDPrime 830



1. Thales IDPrime 930



### Čipová karta SafeNet eToken 4100

Pre správne fungovanie čipových kariet SafeNate eToken, používaných ako HPRO karty, je potrebné nainštalovať „mini-driver“, ktorý je umiestnený na „x104\_Binary**\_x\_xx**\Install\CARD-Middleware.zip\CARD-Middleware\SafeNet eToken Minidriver.exe“.

POZOR: Alternatívny middleware výrobcu karty, distribuovaný pod názvom „eToken Authetication Client“ nie je podporovaný! Ak je na pracovnej stanici, na ktorej sa používa EhealthCryptoController, nainštalovaný aj eToken Authentication Client, môže to spôsobovať problémy pri správnom fungovaní komponentu.

### Čipová karta Gemalto IDPrime 830

Pre správne fungovanie uvedených čipových kariet je potrebné nainštalovať príslušný „mini-driver“ pre daný typ karty. Karty typu „C“ boli testované s mini-driverom „Gemalto minidriver for IDPrime MD cards“ verzia „8.5.0.5“. ktorý je umiestnený x104\_Binary**\_x\_xx**\Install\Gemalto\_Minidriver.zip.

UPOZORNENIE

Pre korektné fungovanie tejto čipovej karty je nevyhnutné mať nainštalovanú minimálne verziu eHealthCryptoControllera 5.0.0 (x104\_Binary**\_x\_xx**.zip\Prostredia\PREPROD\ECC\ECC\_20180928\_v5-0-0.zip)

### Čipová karta Thales IDPrime 930

Pre správne fungovanie uvedených čipových kariet je potrebné nainštalovať príslušný „mini-driver“ pre daný typ karty. Karty typu „C“ boli testované s mini-driverom „SafeNet minidriver for IDPrime MD cards“ verzia „10.8.2164“. ktorý je umiestnený x104\_Binary**\_x\_xx**\Install\SafeNet-Minidriver 10.8.2164 R6 Post GA.zip alebo na integračnóm portály IS PZS **Prehľadať dokumenty a formuláre/Informačné systémy PZS/Certifikáty\_ovládače/SafeNet-Minidriver 10.8.2164 R6**

UPOZORNENIE

Pre korektné fungovanie tejto čipovej karty je nevyhnutné mať nainštalovanú minimálne verziu eHealthCryptoControllera 5.0.0 (x104\_Binary**\_x\_xx**.zip\Prostredia\PREPROD\ECC\ECC\_20180928\_v5-0-0.zip)

## Sieťový prístup do prostredí

Prístup do prostredí je možné realizovať jedným z dvoch spôsobov:

1. Pripojenie do dedikovanej privátnej siete (VPN)
2. Pripojenie prostredníctvom siete internet pričom komunikácia je chránená protokolom SSL

(Pripojenie na prostredie PREPROD pomocou SSL bude možné až po povolení zdrojovej IP adresy. Pre povolenie je nevyhnutné kontaktovať NCZI)

### VPN klient

Prístup na všetky prostredia je zabezpečený prostredníctvom dedikovaných VPN sietí. Na prístup do VPN, je potrebné na klientskej stanici mať nainštalovaného VPN klienta. Klienta je možné nájsť na ceste x014\_Binary\Install\anyconnect-win.msi

## Verejné kľúče

Kapitola popisuje kľúče nevyhnutné pre zabezpečenie komunikácie so službami poskytovanými NCZI. Cert súbory sú dostupné v rámci prílohy x104\_Binary**\_x\_xx**.zip

* BspConsultingEcc.cer - verejný kľúč pre podpisovanie komponentov CryptoController
* AuthCA.crt - Verejný kľúč certifikačnej autority, ktorá vydáva autentifikačné certifikáty zdravotníckych pracovníkov, ktoré sú umiestnené na čipovej karte ZPr.
* protectionca.crt - Verejný kľúč certifikačnej autority, ktorá vydáva šifrovacie a podpisové certifikáty zdravotníckych pracovníkov, ktoré sú umiestnené na čipovej karte ZPr
* RootCA.crt - Verejný kľúč hlavnej certifikačnej autority, pod ktorú patria AuthCA, Protection CA a Tech CA.
* TechCA.crt - Verejný kľúč certifikačnej autority, ktorá vydáva šifrovacie certifikáty službám (napr. pre zabezpečenie SSL komunikácie, alebo šifrovacie certifikáty pre JRUZ GW, Autorizáciu, DbIdFuzz atď.)
* b2bca.der – Verejný kľúč certifikačnej autority, ktorá vydáva šifrovacie a podpisové certifikáty pre zdravotníckych pracovníkov, ktoré sú umiestnenné v HSM.

Detailnejší popis je možné nájsť v kapitolách pre príslušné prostredia. Pre inštaláciu kľúčov do úložiska na klientských staniciach s OS Win XP je nevyhnutné mať nainštalovaný AdminPack

## IAM B2B Klientsky komponent

Dokumenty, ktoré popisujú integráciu na servisné rozhrania systému NZIS, konkrétne subsystému IAM pre Business to Business komunikáciu a bezpečnostné mechanizmy ako autentizáciu, podpisovanie a šifrovanie, ktoré musia byť použité, pre úspešnú implementáciu rozhrania sú nasledovné:

* IAM\_B2B\_Klientsky\_komponent\_Integracny\_manual\_vx.x.x.DOCX
* IAM\_B2B\_Klientsky\_komponent\_Manual-pre-administratorov\_vx.x.docx
* HSM-Skolenie.pdf

# Prostredie PREPROD

## Spôsob prístupu

VPN je dostupné z internetu. Príslušné End Pointy prostredia sú zverejnené v rámci VPN a prostredníctvom internetu.

## Prerekvizity konektivity – prístupu na PREPROD

### Koreňové certifikáty

Pre správne fungovanie pripojenia na služby NZIS je nutné zaradiť certifikáty certifikačných autorít NCZI do úložiska dôveryhodných koreňových a sprostredkovateľských certifikátov. Certifikát vydá prevádzkovateľ riešenia.

Je potrebné naimportovať do Trusted Root Certification Authorities (Local computer alebo Current user) nasledovné certifikáty:

x104\_Binary\_x\_xx\Prostredia\PREPROD\Certificates\NCZI\_PreProd\_RootCA-1.crt

Do Intermediate Certification Authorities (Local computer alebo Current user) nasledovné certifikáty:

x104\_Binary\_x\_xx\Prostredia\PREPROD\Certificates\NCZI\_PreProd\_HPRO\_Authentication\_CA R1-1.crt

x104\_Binary\_x\_xx\Prostredia\PREPROD\Certificates\NCZI\_PreProd\_Tech\_CA\_R1-1.crt

x104\_Binary\_x\_xx\Prostredia\PREPROD\Certificates\ NCZI\_ProtectionCA-R1-1.crt

x104\_Binary\_x\_xx\Prostredia\PREPROD\Certificates\ nczi\_b2bca-R1-1.der

x104\_Binary\_x\_xx\Prostredia\PREPROD\Certificates\NCZI\_PreProd\_HPRO\_Authentication\_CA R1-2.cer

x104\_Binary\_x\_xx\Prostredia\PREPROD\Certificates\ NCZI\_PreProd\_HPRO\_ProtectionCA-R1-2.cer

x104\_Binary\_x\_xx\Prostredia\PREPROD\Certificates\ NCZI\_PreProd\_Tech\_CA\_R1-2.cer

### Certifikát ESB

Naimportovať nasledovné certifikáty:

x104\_Binary**\_x\_xx**\Prostredia\PREPROD\Certificates\services.preprod.npz.sk.crt

### Certifikáty prostredia PREPROD

V rámci riešenia ISPZS je potrebné použiť nasledovný súbor. Súbor je možné nájsť na ceste x104\_Binary\_x\_xx\Prostredia\PREPROD\ECC\NzisServicesCertificates\_preprod.xml

### EHealthCryptoController

EHealthCryptoController (popis komponenty viď kapitola *6 Bezpečnostné mechanizmy* dokumentu [X070]).

Súbor je možné nájsť na v x104\_Binary**\_x\_xx**\Prostredia\PREPROD\ECC\ECC\_20190108\_v5-1-0.zip.

### Konfigurácia Iam.Client.CryptoController.dll

Konfigurácia komponentu „Iam.Client.CryptoController.dll“ je realizovaná v rámci štandardného .NET konfiguračného súboru konzumenta – aplikácie, ktorá tento komponent využíva. Vzor konfiguračných kľúčov a ich hodnôt je uvedený v súbore „Iam.Client.CryptoController.dll.SAMPLE.config“.

POZOR: V rámci implementácie podpory eID, musí byť v konfiguračnom súbore definovaný aj nový kľúč „ehealth.iam.cryptoController.eidClientAppUri“, ktorý obsahuje URI lokálne inštalovaného eID klienta (SW tretej strany, nie je dodávkou IAM).

Príklad: „<add key=" ehealth.iam.cryptoController.eidClientAppUri" value="http://localhost:15480"/>“ pre korektnú hodnotu pozri príslušnú dokumentáciu k eID klient.

UPOZORNENIE – Zmena v konfiguračných kľúčoch komponentu

Všetky konfiguračné kľúče v sekcii "appSettings" týkajúce sa komponentu CryptoController sú prefixované "*ehealth.iam.cryptoController*.\*".

Zmena bola zavedená z dôvodu lepšieho "izolovania" konfigurácie komponentu CryptoController pri integrácii do .NET aplikácii.

Možné problémy s konfiguráciou sú popísané v kapitole 8.1 Príloha E1 – Možné issues s konfiguráciou CC.DLL

Prípadne v runtime:

<https://social.msdn.microsoft.com/Forums/vstudio/en-US/d68a872e-14bc-414a-82c4-d1035a11b4a8/how-do-i-updateinsertremove-the-config-file-during-runtime?forum=csharpgeneral>

### Konfigurácia Iam.B2B.Client.CryptoController

V konfiguračnom súbore (app.config / web.config) samotného informačného systému PZS, ktorý integruje klientsky komponent IAM, je potrebné uviesť nasledujúce dva kľúče v rámci sekcie „appSettings“:

<?xml version="1.0" encoding="utf-8" ?>

<configuration>

<appSettings>

<add key="ehealth.iam.b2b.client.nzisCertificatesFile" value="NzisServicesCertificates.xml"/>

<add key="ehealth.iam.b2b.client.iamStsBaseUri" value="https://sts-zpr.preprod.npz.sk/adfs/services/" />

</appSettings>

</configuration>

Kľúč „ehealth.iam.b2b.client.nzisCertificatesFile“ obsahuje cestu k súboru s verejnými kľúčmi vybraných služieb NZIS (viď kap. **Chyba! Nenašiel sa žiaden zdroj odkazov.**) a kľúč „ehealth.iam.b2b.client.iamStsBaseUri“ obsahuje adresu centrálnych služieb IAM.

### DNS

V prostredí preprod sú prostredníctvom DNS zaregistrované nasledovné adresy:

# PREPROD

vpn.preprod.npz.sk

chybna: [ssl-zpr.npz.sk](https://services.infra.npz.sk)– port TCP 443

sslpzs.preprod.npz.sk

sslpzs-b2b.preprod.npz.sk

services.preprod.npz.sk

sts-zpr.preprod.npz.sk

sts-przs.preprod.npz.sk

ocsp.preprod.npz.sk

pki.preprod.npz.sk

cms-zpr-aktiv.preprod.npz.sk

### VPN

Ako end point pre VPN používať „vpn.preprod.npz.sk“

Pre prihlásenie do VPN je potrebné použiť AUTH certifikát zdravotníckeho pracovníka.

V prípade ak nie sú nainštalované ceretifikáty certifikačných autorít z kapitoly 4.2.1 môže pri pokuse o inicializáciu pripojenia k vpn prísť k nasledovnému stavu:



V tomto okamihu je potrebné kliknúť na „Change Setting...“



Kliknúť na „Apply Change“



Zaškrtnúť „Always trust ...“ a kliknúť na „Connect Anyway“

## Publikačný portál NCZI

Publikovanie číselníkov a registrov prebieha v réžii NCZI a čísleníky a registre sú dostupné na integračnom portáli NCZI, ktorý je dostupný na adrese: https://sd.infra.npz.sk/maximo/

## Overenie prístupu – dostupnosť end pointov

Overenie prístupu na prostredie je možné otestovať pomocou

* dostupnosti ESB end pointu prostredníctvom nasledovného URL:
* <http://services2022.preprod.npz.sk/ESB.SyncServiceExt/Service2017.svc?wsdl>
* <https://sslpzs.preprod.npz.sk/ESB.SyncServiceExt/Service2017.svc?wsdl>
* [https://](https://sslpzs-b2b.preprod.npz.sk/ESB.SyncServiceExt/Service.svc?wsdl)*[sslpzs-b2b.preprod.npz.sk](https://sslpzs-b2b.preprod.npz.sk/ESB.SyncServiceExt/Service.svc?wsdl)*[/ESB.SyncServiceExt/Service2017.svc?wsdl](https://sslpzs-b2b.preprod.npz.sk/ESB.SyncServiceExt/Service.svc?wsdl)
* dostupnosťou IAM end pointu:

<https://sts-zpr.preprod.npz.sk/>

# Prostredie PROD

## Spôsob prístupu

VPN je dostupné z internetu. Príslušné End Pointy prostredia sú zverejnené v rámci VPN.

## Prerekvizity konektivity – prístupu na PROD

### Koreňové certifikáty

Pre správne fungovanie pripojenia na služby NZIS je nutné zaradiť certifikáty certifikačných autorít NCZI do úložiska dôveryhodných koreňových a sprostredkovateľských certifikátov. Certifikát vydá prevádzkovateľ riešenia.

Je potrebné naimportovať do Trusted Root Certification Authorities (Local computer alebo Current user) nasledovné certifikáty:

x104\_Binary\_x\_xx\Prostredia\PROD\Certificates\NCZI\_RootCA-1.crt

Do Intermediate Certification Authorities (Local computer alebo Current user) nasledovné certifikáty:

x104\_Binary\_x\_xx\Prostredia\PROD\Certificates\NCZI\_AuthCA-R1-1.crt

x104\_Binary\_x\_xx\Prostredia\PROD\Certificates\NCZI\_ProtectionCA.crt

x104\_Binary\_x\_xx\Prostredia\PROD\Certificates\NCZI\_TechCA-R1-1.crt

x104\_Binary\_x\_xx\Prostredia\PROD\Certificates\ NCZI\_HPRO\_Authentication\_CA R1-2.crt

x104\_Binary\_x\_xx\Prostredia\PROD\Certificates\ NCZI\_HPRO\_ProtectionCA-R1-2.crt

x104\_Binary\_x\_xx\Prostredia\PROD\Certificates\ NCZI\_Tech\_CA\_R1-2.crt

### Certifikát ESB

Naimportovať nasledovné certifikáty:

x104\_Binary**\_x\_xx**\Prostredia\PROD\Certificates\services.infra.npz.sk.crt

### Certifikáty prostredia PROD

V rámci riešenia ISPZS je potrebné použiť nasledovný súbor. Súbor je možné nájsť na ceste x104\_Binary\_x\_xx\Prostredia\PROD\ECC\NzisServicesCertificates.xml

### EHealthCryptoController

EHealthCryptoController (popis komponentu viď kapitola *6 Bezpečnostné mechanizmy* dokumentu [X070]):

Súbor je možné nájsť na ceste x104\_Binary**\_x\_xx**\Prostredia\PROD\ECC\ECC\_20190108\_v5-1-0.zip

### Konfigurácia Iam.Client.CryptoController.dll

Konfigurácia komponentu „Iam.Client.CryptoController.dll“ je realizovaná v rámci štandardného .NET konfiguračného súboru konzumenta – aplikácie, ktorá tento komponent využíva. Vzor konfiguračných kľúčov a ich hodnôt je uvedený v súbore „Iam.Client.CryptoController.dll.SAMPLE.config“.

POZOR: V rámci implementácie podpory eID, musí byť v konfiguračnom súbore definovaný aj nový kľúč „ehealth.iam.cryptoController.eidClientAppUri“, ktorý obsahuje URI lokálne inštalovaného eID klienta (SW tretej strany, nie je dodávkou IAM).

Príklad: „<add key=" ehealth.iam.cryptoController.eidClientAppUri" value="http://localhost:15480"/>“ pre korektnú hodnotu pozri príslušnú dokumentáciu k eID klient.

UPOZORNENIE – Zmena v konfiguračných kľúčoch komponentu

Všetky konfiguračné kľúče v sekcii "appSettings" týkajúce sa komponentu CryptoController sú prefixované "*ehealth.iam.cryptoController*.\*".

Zmena bola zavedená z dôvodu lepšieho "izolovania" konfigurácie komponentu CryptoController pri integrácii do .NET aplikácii.

Možné problémy s konfiguráciou sú popísané v kapitole 8.1 Príloha E1 – Možné issues s konfiguráciou CC.DLL

Prípadne v runtime:

<https://social.msdn.microsoft.com/Forums/vstudio/en-US/d68a872e-14bc-414a-82c4-d1035a11b4a8/how-do-i-updateinsertremove-the-config-file-during-runtime?forum=csharpgeneral>

### Konfigurácia Iam.B2B.Client.CryptoController

V konfiguračnom súbore (app.config / web.config) samotného informačného systému PZS, ktorý integruje klientsky komponent IAM, je potrebné uviesť nasledujúce dva kľúče v rámci sekcie „appSettings“:

<?xml version="1.0" encoding="utf-8" ?>

<configuration>

<appSettings>

<add key="ehealth.iam.b2b.client.nzisCertificatesFile" value="NzisServicesCertificates.xml"/>

<add key="ehealth.iam.b2b.client.iamStsBaseUri" value="https://sts-zpr.infra.npz.sk/adfs/services/" />

</appSettings>

</configuration>

Kľúč „ehealth.iam.b2b.client.nzisCertificatesFile“ obsahuje cestu k súboru s verejnými kľúčmi vybraných služieb NZIS (viď kap. **Chyba! Nenašiel sa žiaden zdroj odkazov.**) a kľúč „ehealth.iam.b2b.client.iamStsBaseUri“ obsahuje adresu centrálnych služieb IAM.

### DNS

Na prostredí PROD sú pre potreby integrácie zaregistrované nasledovné DNS záznamy:

# PROD

vpn.npz.sk

services.infra.npz.sk

services1.infra.npz.sk

[ssl-zpr.npz.sk](https://services.infra.npz.sk)

ssl-zpr-b2b.npz.sk

sts-zpr.infra.npz.sk - pre VPN a SSL komunikáciu sts-przs.npz.sk

ocsp.infra.npz.sk

pki.infra.npz.sk

cms-zpr-aktiv.infra.npz.sk

### VPN

Ako end point pre VPN používať „vpn.npz.sk“

Pre prihlásenie do VPN je potrebné použiť AUTH certifikát zdravotníckeho pracovníka.

V prípade ak nie sú nainštalované certifikáty certifikačných autorít z kapitoly 5.2.1 môže pri pokuse o inicializáciu pripojenia k vpn prísť k nasledovnému stavu:



V tomto okamihu je potrebné kliknúť na „Change Setting...“



Kliknúť na „Apply Change“



Zaškrtnúť „Always trust ...“ a kliknúť na „Connect Anyway“

## Publikačný portál NCZI

Publikovanie číselníkov a registrov prebieha v réžii NCZI a čísleníky a registre sú dostupné na integračnom portáli NCZI, ktorý je dostupný na adrese: https://sd.infra.npz.sk/maximo/

## Overenie prístupu – dostupnosť end pointov

Overenie prístupu na prostredie je možné otestovať pomocou

* dostupnosti ESB end pointu prostredníctvom nasledovného URL:

<http://services.infra.npz.sk/ESB.SyncServiceExt/Service.svc?wsdl>

<https://ssl-zpr.npz.sk/ESB.SyncServiceExt/Service.svc?wsdl>

<https://ssl-zpr-b2b.npz.sk/ESB.SyncServiceExt/Service.svc?wsdl>

* dostupnosťou IAM end pointu:

<https://sts-zpr.infra.npz.sk/>

# Nástroje a vstupy pre integráciu

## Špecifikácia rozhrania IM

Viď samotný pavúk a štruktúra IM

## Nástroj na čítanie archetypov

Pre čítanie EN13606 archetypov vo forme ADL je možné napríklad pomocou nástroja:

<http://www.linkehr.com/>

## Najzákladnejšie body volania NZIS služby

Základným predpokladom volania služby je:

1. SAML token
2. UserContext s vyplneným:
   1. Specialization
   2. IdentifikatorOUPZS
3. Vytvorenie tela správy
   1. Dátové štruktúry služby **sú/nie sú** špecifikované podľa EN13606
   2. Služba **vyžaduje/nevyžaduje** identifikátor zdravotného záznamu
4. Služba je volaná synchrónne a/alebo asynchrónne
   1. MessageInfo.Class = „SluzbaAB\_vX“

## Zoznam služieb a procesov na integráciu

Menný zoznam služieb a procesov pre integráciu je zverejnený na <https://www.ezdravotnictvo.sk/sk/dodavatel-is/dokumenty> v dokumente „Procesné scenáre služieb“

Poznámka2: Ako pomôcku pre integráciu poskytujeme príklad volania týchto služieb vo forme unit testov v prostredí MS Visual Studia. V rámci tohto príkladu sú k dispozícii aj konkrétne requesty pre jednotlivé služby. Príklad je súčasťou prílohy A.

# Podpora

## Kontaktné osoby

|  |  |
| --- | --- |
| Rola | Kontakt |
| |  |  | | --- | --- | | **Nahlasovanie dotazov** |  | | Národné centrum zdravotníckych informácii  Lazaretská 26, 811 09 Bratislava 1  Tel.: +421 2 57 26 91 10  [ispzs@nczisk.sk](mailto:ispzs@nczisk.sk) |

Stránka je úmyselne ponechaná ako prázdna.

# Prílohy

## Príloha E1 – Možné issues s konfiguráciou CC.DLL

### Chyba 1:

System.Exception: Unable to initialize EhealthCryptoController . Current configuration file does not contain the key "nzisServicesCertificatesFile". ---> System.Configuration.ConfigurationException: Current configuration file does not contain the key "nzisServicesCertificatesFile".

Pripadne v event logu ako:



**Riešenie**

Pravdepodobne je chybne nakonfigurovaná cesta k súboru s certifikátmi NZIS prostredia, respektíve daný súbor nie je dostupný pre aplikáciu využívajúcu CC.dll.

### Chyba 2:

System.Exception: Unable to initialize EhealthCryptoController . EventLog source "EhealthCryptoController" does not exists and cannot be created due to following security exception: The source was not found, but some or all event logs could not be searched.  Inaccessible logs… ()

**Riešenie**

Aplikovať postup podľa popisu uvedeného v kapitole “5.5.4.4 Ďalšie predpoklady” uvedeného v dokumente [X070].

## Príloha A - Príklad implementácie volania služby vo forme unit testu vo Visual Studio

Príklad je možné nájsť na [Integračnom portáli](https://sd.infra.npz.sk/maximo/) :Prehľadať dokumenty a formuláre/Aplikácie a nástroje/Visual Studio – ukážka integrácie Priečinok obsahuje príklad vo forme unit testu a príklad pre pripojenie cez SSL.

## Príloha B - Príklad inicializácie CryptoControllera v Delphi

**Nasleduje krátky postup pre Delphi6, Delphi7 a Delphi XE2.   Deplhi priklad nie je kompletný example tak, ako je uvedený example pre Visual Studio v Prilohe A.**

**Delphi6, Delphi7:**

**1.** Ako jednu z alternatív je potrebné vytvoriť COM knižnicu nad eH Cryptocontrollerom (ECC), ktorú je následne možné v prostredí Delphy využiť nasledovným postupom. Takto vytvorenú COM knižnicu pre ilustráciu nazvime „**BspConsulting.Ehealth.CryptoController.dll**“.

**2.** Registrácia  knižnice **BspConsulting.Ehealth.CryptoController.dll , prostredníctvom utility regsvc.exe,**

**Priklad:** D:\Development\JRUZ\Delphi>c:\Windows\Microsoft.NET\Framework\v4.0.30319\Regsvcs .exe BspConsulting.Ehealth.CryptoController.dll

    Počas registrácie sa vygeneruje typová knižnica – potrebná pre Delphi

**3.** **Je** **NUTNE modifikovať tlbimp.sym** súbor v c:\Program Files\Borland\Delphi\Bin . Do tohto súboru je nutné pridať nasledovne deklarácie typov :

;;==============================================;;  
;; Map mscorlib CoClasses to better names       ;;  
;;==============================================;;  
[{BED7F4EA-1A96-11D2-8F08-00A0C9A6186D}:TypeNames]  
Byte=CLRByte  
Double=CLRDouble  
Single=CLRSingle  
Int16=CLRInt16  
Int32=CLRInt32  
Int64=CLRInt64  
String=CLRString  
Object=CLRObject  
Array=CLRArray  
Enum=CLREnum  
Boolean=CLRBoolean  
Char=CLRChar  
Guid=CLRGuid  
Type=CLRType  
Void=CLRVoid  
Pointer=CLRPointer  
Exception=CLRException

4. Vygenerovanú knižnicu **BspConsulting.Ehealth.CryptoController.tlb**   je potrebné neimportovať do projektu Delphi. Vykoná sa to prostredníctvom  menu: Projects\Import Type Library. V rámci okna sa vyberie príslušná TLB a vola sa akcia CreateUnit, ktorá vygeneruje deklaračný .pas file pre danú TLB

5. V Delphi projekte je treba do uses pridať vygenerovanú knižnicu v bode 3

**Priklad**:

                        Uses BspConsulting\_Ehealth\_CryptoController\_TLB,ComObj

  Pozn: comobj je pridávaná z dôvodu vytvárania objektu prostredníctvom CreateComObject,...

6.  Použitie CryptoControllera je napr:

**procedure** TForm1.Button1Click(Sender: TObject);  
**var**  
       ecc: IEhealthCryptoController;  
      token: variant;  
     targetServiceIdentifier: WideString;  
**begin**  
  ecc :=  CreateComObject(CLASS\_EhealthCryptoController) as IEhealthCryptoController;  
  targetServiceIdentifier := 'service1';  
  token := ecc.GetSamlTokenForHealthProfessional (targetServiceIdentifier);  
**end;**

**Delphi XE2:**

**1.** Ako jednu z alternatív je potrebné vytvoriť COM knižnicu nad eH Cryptocontrollerom (ECC), ktorú je následne možné v prostredí Delphy využiť nasledovným postupom. Takto vytvorenú COM knižnicu pre ilustráciu nazvime „**BspConsulting.Ehealth.CryptoController.dll**“.

**2.** Registrácia  knižnice **BspConsulting.Ehealth.CryptoController.dll , prostredníctvom utility regsvc.exe,**

**Priklad:** D:\Development\JRUZ\Delphi>c:\Windows\Microsoft.NET\Framework\v4.0.30319\Regsvcs .exe BspConsulting.Ehealth.CryptoController.dll

    Počas registrácie sa vygeneruje typová knižnica – potrebná pre Delphi

**3.**  Vygenerovanú knižnicu **BspConsulting.Ehealth.CryptoController.tlb**       je potrebné neimportovať do projektu Delphi. Vykoná sa to prostredníctvom  menu: Component\Import Component:

Výstupom je BspConsulting\_Ehealth\_CryptoController\_TLB.pas, ktorá sa použije v danom unite

4. V Delphi projekte je treba do uses pridať vygenerovanú knižnicu v bode 3

**Príklad**:

                        Uses BspConsulting\_Ehealth\_CryptoController\_TLB,ComObj

  Pozn: comobj je pridávaná z dôvodu vytvárania objektu prostredníctvom CreateComObject,...

5.  Použitie CryptoControllera je napr:

**procedure** TForm1.Button1Click(Sender: TObject);  
**var**  
       ecc: IEhealthCryptoController;  
      token: variant;  
     targetServiceIdentifier: WideString;  
**begin**  
  ecc :=  CreateComObject(CLASS\_EhealthCryptoController) as IEhealthCryptoController;  
  targetServiceIdentifier := 'service1';  
  token := ecc.GetSamlTokenForHealthProfessional (targetServiceIdentifier);  
**end;**

## Príloha C - Príklad implementácie volania služby v Delphi

Táto implementácia nie je referenčná, príklad je len ilustratívny. Prílohu je možné nájsť na ceste x104\_Binary**\_x\_xx**\Prilohy\Delphi+dll\_20120731.zip

## Príloha D – Technologický checklist

### Technické požiadavky klientských staníc ISPZS

#### Platforma - Podporované klientske operačné systémy a obmedzenia

Windows 11

Windows 10

Windows 8.1, a 8.1 Update 1 x86 (32-bit) a x64 (64-bit)

Všetky vyššie spomenuté OS sú podporované aktuálnou verziou komponentu EhealthCryptoController.

**Poznámky a obmedzenia:**

* Nekompatibilita produktov tretích strán s Windows 8 môže zabrániť vytvoreniu VPN spojenia cez bezdrôtovú sieť (napr. WinPcap service, staré alebo nepodporované ovládače pre bezdrôtové karty...),
* HP Protect tools nefungujú s AnyConnectom na Windows 8.x
* Pre pripojenie do VPN cez bluetooth alebo USB tethering, Cisco kvalifikovalo iba Apple iPhone, pripojenie cez iné tethered zariadenia nie je garantované,
* Na klientskom PC môže byť počas pripojenia do VPN vytváranej pomocou Cisco Anyconnect prihlásený iba jeden používateľ (lokálny alebo vzdialený), v prípade prihlásenia ďalšieho používateľa, vpn bude ukončená,

Vzhľadom

na vlastnosť OS Windows, ktorý automaticky importuje certifikáty z karty PZS do personálneho certifikačného store prihláseného užívateľa v OS.

Doporučujeme: **Nezdieľať účty vo windows** - t.j. každý, kto vytvára vpnku, má mať vlastný učet do OS, kedže certifikákty sa ukladajú do personal storu vo windowse, takto by sa zamedzilo správaniu OS pri viacerých kartách (s certifikátmi, keďže v personal store by bol vždy iba jeden certifikat0

V prípade že na OS Windows zdieľajú účet v Operačnom systéme viacerí Zprac doporučujeme vykonať nasledovné kroky:

* **vypnúť automatický výber certifikátu v nastaveniach Cisco Anyconnect klienta**



Obrázok 3 - Ikona nastavenia anyconnecta



Obrázok 4 - Vypnutie automatického výberu certifikátu

* **pri pripojení do VPN, manuálne vybrať certifikát podľa aktuálne vloženej smart karty (vo výbere sa budú nachádzať všetky platne certifikáty zo všetkých PZS smart kariet, ktoré boli vložené do čítačky na danom PC),**



Obrázok 5 - Manuálny výber certifikátu

#### Doplnkové SW požiadavky

Microsoft .NET Framework 4

Windows Identity Foundation (WIF)

Windows Identity Foundation (WIF) treba nainštalovať na klientskej stanici. WIF inštalator je možne stiahnuť z <https://www.microsoft.com/en-us/download/details.aspx?id=17331>

Microsoft Installer, version 3.1

### Zabezpečenie komunikácie medzi IS PZS a NZIS

#### Čítačka ePZP kariet

1. Použitý typ čítačky: **Omnikey 3x21 USB**
   * Použitý driver: x104\_Binary\Install\OMNIKEY\_3x21\_USB\_CardReader\_Driver.zip
2. Použitý typ čítačky: **Gemalto IDBridge CT30** (pôvodné označenie „Gemalto PC USB TR“

Použitý driver:x104\_Binary\Install\GemPcCCID.exe

#### Ovládače ePZP kariet

MiddleWare pre použitie čipových kariet - Windows Mini Driver.

1. Čipová karta : **SafeNet eToken 4100.**
   * mini-driver - „x104\_Binary\Install\CARD-Middleware.zip\CARD-Middleware\SafeNet eToken Minidriver.exe“
2. 3.4.3 Čipová karta Gemalto IDPrime 830
   * minidriver - verzia „8.5.0.5- x104\_Binary\Install\Gemalto\_Minidriver.8.5.0.5.zip.

#### . Ovládače čítačiek eID

1. HID OMNIKEY 3121 – čítačka bez numerickej klávesnice
   * Ćítačka je fuknčná so štandardným driverom dodávaným OS windows
2. ReinerSCT –čítačka s numerickou klávesnicou
   * Príslučnbý driver k čítačke je možné nájsť v priložených súboroch na ceste x104\_Binary\Install\16\_bc\_7\_5\_6b.exe

#### Prehľad podporovaných driverov pre rôzne platformy

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Typ/**  **Zariadenie** | **Driver** | **Podporovaná platforma OS** | **Prerekvizity inštalácie** | **Umiestnenie** |
| Omnikey 3x21 USB (čítačka stará) | HID Global 1.2.6.5 | XP, Vista, Windows 7,  Windows 8,  Windows 8.1,  Windows 10 | * Admin prihlásenie | x104\_Binary\Install\OMNIKEY\_3x21\_USB\_CardReader\_Driver.zip |
| Gemalto IDBridge CT30 (čítačka nová) | Gemalto 4.1.2.1 |  | * Admin prihlásenie |  |
| Gemalto 4.1.4.0 | XP, Vista, Windows 7,  Windows 8,  Windows 8.1,  Windows 10 | * Admin prihlásenie | x104\_Binary\Install\GemPcCCID.exe |
| SafeNet eToken 4100 (ePZP starý) | SafeNet eToken Minidriver | XP | * Admin prihlásenie * patch KB909520 | x104\_Binary\Install\CARD-Middleware.zip\SafeNet eToken Minidriver.exe |
| SafeNet eToken Minidriver | Vista, Windows 7,  Windows 8,  Windows 8.1  , Windows 10 | * Admin prihlásenie | x104\_Binary\Install\CARD-Middleware.zip\SafeNet eToken Minidriver.exe |
| Gemalto IDPrime 830 (ePZP nový) | Gemalto.MiniDriver.IDPrime 8.5.0.5 | XP | * Admin prihlásenie * patch KB909520 | x104\_Binary\Install\Gemalto\_Minidriver.zip |
| Gemalto.MiniDriver.IDPrime 8.5.0.5 | Vista, Windows 7,  Windows 8,  Windows 8.1,  Windows 10 | * Admin prihlásenie | x104\_Binary\Install\Gemalto\_Minidriver.zip |
| Minidriver pre karty |  | XP | * patch KB909520 | x104\_Binary\Install\CARD-Middleware.zip\XP-MINI\Windows-KB909520-v1.000-x86-ENU.exe |
| Reiner SCT CyberJack One  (čítačka eID- pinpad) |  | Windows XP,  Windows Vista 32/64bit,  Windows 7 32/64bit,  Windows 8 32/64bit,  Windows 8.1 32/64bit,  Windows 10 32/64bit | * Admin prihlásenie | x104\_Binary\Install\16\_bc\_7\_5\_6b.exe |
| HID OMNIKEY 3121 (bez PIN pad) |  | Windows XP,  Windows Vista 32/64bit,  Windows 7 32/64bit,  Windows 8 32/64bit,  Windows 8.1 32/64bit,  Windows 10 32/64bit | * Admin prihlásenie | x104\_Binary\Install\sfw-01556-rev-2.1.0.71-hid-omnikey-ccid-driver.zip |

Tabuľka 1prehľad potrebných ovádačov a podporovaných platforiem

**Upozornenie: OS Windows 10 v zostave operačného systému 1809 dlhodobo vykazuje nestabilitu pre používanie driverov pre čítačky používané v rámci ezdravie. Odporúčame prehodnotiť prechod na vyššiu zostavu operačného systému Windows 10.**

#### Dôveryhodný certifikát certifikačnej autority NCZI

Pre správne fungovanie pripojenia na služby NZIS je nutné zaradiť certifikáty certifikačných autorít NCZI do úložiska dôveryhodných koreňových a sprostredkovateľských certifikátov. Certifikát vydá prevádzkovateľ riešenia. Vid dokument -eZdravie\_Integracny\_manual\_pre\_IS\_PZS\_x104

#### VPN pripojenie (nie je nevyhnutné v prípade pripojenie pomocou internetu a SSL)

VPN klient: Cisco AnyConnect Secure Mobility Client, Release 4.10

Získanie inštalačného programu: Je súčasťou integračného balíčka

Nastavenie pripojenia: Pri prvom pripojeni VPN klienta na cieľovú IP adresu si VPN klient nastavenia sám stiahne a vynúti.

**Autentifikácia:**

* V prípade pripojenia cez autentizovaný Proxy server, AnyConnect si vyžiada zadať prihlasovacie meno a heslo pre prístup cez proxy server,
* Pre prístup do VPN sa používa certifikát na čipovej karte používateľa. Vyžaduje sa overenie PIN-om,

Ukončenie spojenia: Ukončenie spojenia je vykonané po uplynutí timeoutu – odpojenie od siete, vytiahnutí karty z čítačky alebo manuálny odpojením od VPN.

***Opakované vyžadovanie PIN pre epzp kartu***

Informujeme Vás, že sme obdržali postup od dodávateľa kariet na odstránenie problému s vyžadovaním PIN ePZP karty pre každú operáciu s NZIS. Postup bol overený na nahlásených vybraných prípadoch, avšak v závislosti od heterogenity prostredia je potrebné nám  v prípade pretrvávajúceho problému po  nasadení patchu nahlásiť incident.  Je potrebné aplikovať nasledovné Powershell scripty pod admin účtom

**64 bit OS: spustit v elevated powershell / as admin**

# nastavenie registrov pre 64 bit

Set-ItemProperty -Path 'HKLM:\Software\Microsoft\Cryptography\Calais' -Name "CardDisconnectPowerDownDelay" -Value 28800 -Type DWord

Set-ItemProperty -Path 'HKLM:\Software\Wow6432Node\Microsoft\Cryptography\Calais' -Name "CardDisconnectPowerDownDelay" -Value 28800 -Type DWord

# kontrola

Get-ItemProperty 'HKLM:\Software\Microsoft\Cryptography\Calais\' -Name CardDisconnectPowerDownDelay | select -Property CardDisconnectPowerDownDelay

Get-ItemProperty 'HKLM:\Software\Wow6432Node\Microsoft\Cryptography\Calais\' -Name CardDisconnectPowerDownDelay | select -Property CardDisconnectPowerDownDelay

# restart sluzby

Restart-Service SCardSvr

**32 bit OS: spustit v elevated powershell / as admin**

# nastavenie registrov pre 32 bit

Set-ItemProperty -Path 'HKLM:\Software\Microsoft\Cryptography\Calais' -Name "CardDisconnectPowerDownDelay" -Value 28800 -Type DWord

# kontrola

Get-ItemProperty 'HKLM:\Software\Microsoft\Cryptography\Calais\' -Name CardDisconnectPowerDownDelay | select -Property CardDisconnectPowerDownDelay

# restart sluzby

Restart-Service SCardSvr

 Upozornenie: Registry kľúč nie je dokumentovany na MS