

**TVORÍME VEDOMOSTNÚ SPOLOČNOSŤ**

**XX - IAM B2B Klientsky komponent**

**Integračný manuál**

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**

|  |  |
| --- | --- |
| **Názov dokumentu** | eSO1\_SP\_X070E\_Detailna\_specifikacia\_rozhrania\_Volanie\_sluzieb |
| **Aktuálna verzia** | 1.0.4 |
| **Vlastník dokumentu** | Vladimír Turenič |

**História dokumentu**

|  |  |  |  |
| --- | --- | --- | --- |
| **Verzia** | **Dátum** | **Autor** | **Popis verzie a zmien oproti predchádzajúcej verzii** |
| 1.0 | 24.1.2018 | vTUR | Prvotná verzia dokumentu. |
| 1.0.1 | 29.1.2018 | vTUR | Vymedzenie účelu komponentu pre laboratória. Doplnenie podporovanej verzie OS. |
| 1.0.2 | 06.02.2018 | vTUR | Opísaný rozdiel medzi IAM CryptoController-om a IAM B2B klientom.  Doplnená informácia o podporovanom type certifikátov. |
| 1.0.3 | 16.3.2018 | vTUR | Doplnená kapitola 3.2., aktualizácia kap. 4.2. |
| 1.0.4 | 26.4.2018 | vTUR | Doplnené odvolávky na x104 v konfigurácii. |

**Akceptačné riadenie**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Odberateľ** | | | **Dodávateľ** | | |
| **Dátum** | **Meno (Rola)** | **Podpis** | **Dátum** | **Meno (Rola)** | **Podpis** |
|  | Marian Šimegh |  |  | Štefan Gordian |  |

**Súvisiace produkty a referenčné materiály**

|  |  |
| --- | --- |
| **ID** | **Názov dokumentu a referencia** |
| X104 | eZdravie\_Integracny\_manual\_pre\_IS\_PZS\_x104\_v2.23.docx |
| X070 | Detailná špecifikácia rozhrania – volanie služieb |

**Charakteristika dokumentu**

Cieľom dokumentu je popísať integráciu na servisné rozhrania systému NZIS, konkrétne subsystému IAM pre Business to Business komunikáciu.

Dokument popisuje bezpečnostné mechanizmy ako autentizáciu, podpisovanie a šifrovanie, ktoré musia byť použité, pre úspešnú implementáciu rozhrania.

Dokument má byť určený:

Vývojárom - aby vedeli implementovať rozhrania do klientskeho systému v zhode so špecifikáciou rozhrania

Testerom - aby vedeli vyhodnotiť, či implementácia rozhrania klientskeho systému zodpovedá špecifikácii rozhrania

# Manažérske zhrnutie

Dokument je súčasťou širšej sady dokumentov pre integráciu informačných systémov poskytovateľov zdravotnej starostlivosti s elektronickými službami zdravotníctva.

Tento dokument sa sústredí na detailný opis verejného rozhrania klientskeho komponentu IAM pre Business to Business komunikáciu.

Komponent je v tejto verzii určený výlučne len pre laboratória.

# Úvod

Úvodom je dôležité upozorniť na skutočnosť, že IAM B2B klient nie je nástupcom alebo priamou náhradou aktuálneho Iam.Client.CryptoController komponentu. Oba tieto komponenty – Iam.B2B.Client a Iam.Client.CryptoController – koexistujú vedľa seba a sú určené každý pre inú oblasť použitia.

* **Iam.Client.CryptoController** je určený pre implementáciu v ambulanciách a priamo na pracovných staniciach zdravotníckych pracovníkov, ktorí využívajú na komunikáciu s NZIS výlučne čipové karty zdravotníckych pracovníkov.
* **Iam.B2B.Client** je určený pre nasadenie na servre, pričom pre komunikáciu s NZIS nie sú využívané čipové karty zdravotníckych pracovníkov ale príslušné certifikáty uložené v HSM moduloch.

Tento dokument sa venuje opisu výlučne komponentu Iam.B2B.Client. Jednotlivé kapitoly dokumentu postupne prechádzajú od nevyhnutných predpokladov pre správnu integráciu, ako sú platforma a požiadavky na HSM, cez jednoduchý prehľad poskytovanej funkcionality až k detailným opisom jednotlivých metód a stručným príkladom ich implementácie.

# Nevyhnutné predpoklady

## Platforma

Klientsky komponent IAM pre B2B komunikáciu je postavený na platforme Microsoft .NET Framework 4.6.2.

Je realizovaný ako .NET assembly pozostávajúce z nasledujúcich knižníc:

* Iam.B2B.Client.dll
* Iam.B2B.Common.dll
* Iam.B2B.Cryptography.dll
* Iam.B2B.IdentityModel.dll
* BouncyCastle.Crypto.dll

Kľúčovou je knižnica Iam.B2B.Client.dll, ktorá poskytuje triedu Iam.B2B.Client.CryptoController, ktorá implementuj verejné rozhranie pre realizáciu požadovanej funkcionality.

Podporované verzie operačných systémov:

* Microsoft Windows Server 2016 (Standard / Datacenter with GUI)

## Dostupnosť verejných kľúčov Certifikačných autorít NCZI

Správne fungovanie klientskeho komponentu vyžaduje aby boli na serveri, kde bude komponent používaný, naimportované aj všetky verejné kľúče príslušných certifikačných autorít NCZI, najmä

* **NCZI Root CA** (v „Local Computer\Trusted Root Certification Authorities)



* **NCZI B2B CA** (v „Local Computer\Intermediate Certification Authorities“)



Je potrebné zabezpečiť, aby pri danom certifikáte, ktorý má byť B2B klientom použitý, bolo možné korektne overiť celú certifikačnú cestu.

Verejné kľúče príslušných certifikačných autorít sú rôzne pre jednotlivé prostredia (Dev / PrePROD / PROD a pod). Konkrétne certifikáty s verejnými kľúčmi príslušných CA pre jednotlivé prostredia sú uvedené v produkte x104.

## Hardware Security Modul (HSM)

Klientsky komponent počíta s použitím jedného z nasledovných rád HSM modulov na strane laboratórií:

1. THALES nShield Solo
2. THALES nShield Connect

Viac informácií k špecifikáciám jednotlivých typov viď priložené špecifikácie:



Použitie iných typov HSM modulov (model / výrobca) bude znamenať nekompatibilitu, resp. čiastočnú alebo úplnú nefunkčnosť komponentu.

!! UPOZORNENIE !!  
IAM B2B klientsky komponent **nerealizuje** autentifikáciu a autorizáciu pre použitie privátnych kľúčov v HSM.   
  
Nakoľko Informačný systém laboratória si spravuje užívateľské účty samostatne, je povinný zabezpečiť autentifikáciu a autorizáciu používateľa pred použitím konkrétneho certifikátu a zamedziť tak jeho neautorizovanému použitiu.

## Súbor s verejnými kľúčmi služieb NZIS

Kľúčovou súčasťou pre fungovanie komponentu je XML dokument „NzisServicesCertificates.xml“ obsahujúci verejné kľúče vybraných služieb NZIS.

Súbor s verejnými kľúčmi služieb NZIS je rôzny pre jednotlivé prostredia. Konkrétny súbor, s verejnými kľúčmi služieb NZIS pre jednotlivé prostredia je súčasťou produktu x104.

Cestu k tomuto súboru je možné uložiť v rámci konfigurácie informačného systému a následne ju posunúť ako parameter konštruktora triedy Iam.B2B.Client.CryptoController.

## Konfigurácia

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="CESTA\_K\_SUBORU\_S\_VK\_SLUZIEB\_EZDRAVIE"/>

<add key="ehealth.iam.b2b.client.iamStsBaseUri" value="URL\_CENTRALNYCH\_IAM\_SLUZIEB\_EZDRAVIE" />

</appSettings>

</configuration>

Kľúč „ehealth.iam.b2b.client.nzisCertificatesFile“ obsahuje cestu k súboru s verejnými kľúčmi vybraných služieb NZIS (viď kap. 3.3) a kľúč „ehealth.iam.b2b.client.iamStsBaseUri“ obsahuje adresu centrálnych autentizačných služieb IAM. Konkrétna hodnota, URL , je závislá od prostredia voči ktorému prebieha integrácia a je uvedené v produkte x104.

# Verejné rozhranie komponentu

IAM B2B klientsky komponent sprístupňuje požadovanú funkcionalitu pre informačný systém laboratória prostredníctvom klientskej triedy „*Iam.B2B.Client.CryptoController*“.

Verejné rozhranie tejto triedy je zobrazená na nasledujúcom obrázku.



## Návratové hodnoty dávkových operácií

IAM B2B klientsky komponent umožňuje viaceré operácie realizovať v dávkach. Tieto dávkové operácie sa rozdeľujú na dve základné skupiny podľa typu údajov, nad ktorými sú realizované. Operácie nad

1. alfanumerickými znakmi (napr. podpisovanie XML dokumentov) a operácie nad
2. binárnymi dátami (šifrovanie a dešifrovanie dát do/z NZIS).

V prípade dávkových operácií nad alfanumerických dátami je výsledkom množina objektov StringOperationResult a v prípade operácií nad binárnymi dátami je výsledkom množina objektov BinaryOperationResult.

V nasledujúcich podkapitolách sú tieto typy detailnejšie opísané.

### StringOperationResult



V prípade úspechu (IsSuccess = True), bude hodnota „Data" obsahovať alfanumerický reťazec reprezentujúci výsledok danej operácie (napr. podpísaný XML dokument).

V opačnom prípade bude hodnota vlastnosti „Data*“* originálny alfanumerický reťazec (zo vstupu), pri ktorom nastala chyba. Detail vzniknutej chyby je v FaultDetail, pričom sa jedná o objekt typu System.Exception resp. jeho derivát.

### BinaryOperationResult



V prípade úspechu danej operácie (IsSuccess = True), bude hodnota „Data" obsahovať pole bajtov reprezentujúce zašifrované / dešifrované údaje.

V prípade neúspechu danej operácie bude hodnota „Data"

1. NULL pre šifrovacie operácie, z dôvodu ochrany údajov, alebo
2. pôvodné údaje zo vstupu pre dešifrovacie operácie.

Detail vzniknutej chyby je v FaultDetail, pričom sa jedná o objekt typu System.Exception resp. jeho derivát.

## Metóda „GetAvailableCertificates“

Načíta zoznam dostupných certifikátov z Windows Certificate Store, ktorých privátne kľúče sú uložené v HSM a boli vydané príslušnými certifikačnými autoritami IAM.

Certifikáty musia byť uložené vo Windows Certificate Store na ceste „**LocalMachine\My (Personal)**“.

!! UPOZORNENIE !!  
  
IAM B2B klientsky komponent v aktuálnej verzii podporuje **iba certifikáty a privátne kľúče dostupné pomocou nCipher Microsoft CAPI CSP implementácie** .   
  
Certifikáty a privátne kľúče dostupné cez Microsoft Cryptography API: Next Generation (CNG) **nie sú aktuálne podporované** a nebudú teda ani v zozname disponibilných certifikátov.

*Vstupné parametre*

Metóda nemá vstupné parametre.

*Návratová hodnota*

Výsledkom volania je pole objektov štandardného .NET typu

System.Security.Cryptography.X509Certificates.X509Certificate2.

*Výnimky*

| Výnimka | Popis |
| --- | --- |
| CryptographicException | Úložisko s certifikátmi nie je dostupné. |
| SecurityException | Účet, pod ktorým je spustený kód volajúceho komponentu nemá dostatočné oprávnenia na prístup k úložisku s certifikátmi. |

*Príklad*

// ...

using Iam.B2B.Client;

using System.Security.Cryptography.X509Certificates;

using System.Configuration;

// ...

// Vytvorenie inštancie klientskeho komponentu IAM B2B - CryptoController.

CryptoController cc = new CryptoController(

ConfigurationManager.AppSettings["ehealth.iam.b2b.client.nzisCertificatesFile"]

, ConfigurationManager.AppSettings["ehealth.iam.b2b.client.iamStsBaseUri"]

);

);

X509Certificate2[] certs = \_CryptoController.GetAvailableCertificates();

foreach (var cert in certs)

{

Console.WriteLine($"- Certificate:");

Console.WriteLine($"- --- SUBJECT : {cert.Subject}");

Console.WriteLine($"- --- SN : {cert.SerialNumber}");

Console.WriteLine($"- --- ISSUER : {cert.Issuer}");

Console.WriteLine($"- --- THUMBPRINT : {cert.Thumbprint}");

}

## Metóda „SignXmlDocument“

Metóda zabezpečuje realizáciu digitálneho podpisu XML dokumentov v zmysle štandardu XML-DSIG s použitím certifikátu z HSM.

*Vstupné parametre*

|  |  |  |
| --- | --- | --- |
| Parameter | Dátový typ | Popis |
| xmlDataToSign | string[] | Pole alfanumerických reťazcov reprezentujúcich XML dokumenty, ktoré majú byť podpísané špecifikovaným certifikátom (parameter signerCertificateThumbprint. |
| signerCertificateThumbprint | string | Alfanumerický reťazec identifikujúci certifikát, ktorým sa má sada XML dokumentov podpísať.  Tento certifikát musí byť z množiny certifikátov vrátených metódou GetAvailableCertificates (viď kap. 4.2). |

*Návratová hodnota*

Výsledkom volania tejto metódy je pole objektov StringOperationResult (viď kap. 4.1.1), pričom poradie prvkov tejto množiny zodpovedá poradiu prvkov dávky na vstupe. Platí teda, že výsledku operácie nad vstupom xmlDataToSign[n] zodpovedá hodnota result[n]. (viď príklad volania nižšie).

*Výnimky*

V prípade chyby môže hodnota StringOperationResult.FaultDetail obsahovať výnimky uvedené v nasledujúcej tabuľke.

| Výnimka | Popis |
| --- | --- |
| XmlException | Výnimka nastane v prípade syntaktickej chyby v XML dátach špecifikovaných v parametri xmlDataToSign. |
| CertificateNotFoundException | Výnimka nastane v prípade, keď sa medzi disponibilnými certifikátmi nenájde certifikát špecifikovaný v parametri „signerCertificateThumbprint“. |

*Príklad*

Nasledujúci zdrojový kód demonštruje využitie metódy SignXmlDocument na digitálne podpísanie vzorového XML dokumentu.

....

using Iam.B2B.Client;

....

string xmlDoc = @"<?xml version=""1.0"" encoding=""ISO-8859-1""?>

<CATALOG>

<PLANT>

<COMMON>Bloodroot</COMMON>

<BOTANICAL>Sanguinaria canadensis</BOTANICAL>

<ZONE>4</ZONE>

<LIGHT>Mostly Shady</LIGHT>

<PRICE>$2.44</PRICE>

<AVAILABILITY>031599</AVAILABILITY>

</PLANT>

<PLANT>

<COMMON>Columbine</COMMON>

<BOTANICAL>Aquilegia canadensis</BOTANICAL>

<ZONE>3</ZONE>

<LIGHT>Mostly Shady</LIGHT>

<PRICE>$9.37</PRICE>

<AVAILABILITY>030699</AVAILABILITY>

</PLANT>

<PLANT>

<COMMON>Marsh Marigold</COMMON>

<BOTANICAL>Caltha palustris</BOTANICAL>

<ZONE>4</ZONE>

<LIGHT>Mostly Sunny</LIGHT>

<PRICE>$6.81</PRICE>

<AVAILABILITY>051799</AVAILABILITY>

</PLANT>

</CATALOG>

";

// Vytvorenie inštancie klientskeho komponentu IAM B2B - CryptoController.

CryptoController cc = new CryptoController(

ConfigurationManager.AppSettings["ehealth.iam.b2b.client.nzisCertificatesFile"]

, ConfigurationManager.AppSettings["ehealth.iam.b2b.client.iamStsBaseUri"]

);

StringOperationResult[] result = cc.**SignXmlDocument**(

new[] { xmlDoc /\*, xmlDoc2, xmlDoc3 \*/ }

, "VALID\_CERTITICATE\_THUMBPRINT\_FROM\_AVAILABLE\_CERTS"

);

Výsledkom result[0].Data bude:

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

<CATALOG>

  <PLANT>

    <COMMON>Bloodroot</COMMON>

    <BOTANICAL>Sanguinaria canadensis</BOTANICAL>

    <ZONE>4</ZONE>

    <LIGHT>Mostly Shady</LIGHT>

    <PRICE>$2.44</PRICE>

    <AVAILABILITY>031599</AVAILABILITY>

  </PLANT>

  <PLANT>

    <COMMON>Columbine</COMMON>

    <BOTANICAL>Aquilegia canadensis</BOTANICAL>

    <ZONE>3</ZONE>

    <LIGHT>Mostly Shady</LIGHT>

    <PRICE>$9.37</PRICE>

    <AVAILABILITY>030699</AVAILABILITY>

  </PLANT>

  <PLANT>

    <COMMON>Marsh Marigold</COMMON>

    <BOTANICAL>Caltha palustris</BOTANICAL>

    <ZONE>4</ZONE>

    <LIGHT>Mostly Sunny</LIGHT>

    <PRICE>$6.81</PRICE>

    <AVAILABILITY>051799</AVAILABILITY>

  </PLANT>

  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">

    <SignedInfo>

      <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />

      <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />

      <Reference URI="">

        <Transforms>

          <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />

        </Transforms>

        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />

        <DigestValue>kScO3W1gkm3YMDS8ABa++GXyjSI=</DigestValue>

      </Reference>

    </SignedInfo>

    <SignatureValue>EtyoSAzJsKKIDTsJDQQ5MZTiSKYgtFxefKYfr+rPoUY0aZhMPpulxkMUL0KgzPoEDCSWm06Ivs8o89aIMUtseG6Gin7vFvgdIbKXWYFn2Ap/CEKvMMklnCfZkuLKv6n+ys4K2vsj1Yd5TDkbNrK/A5E/67k+4sWn4PTDwE1c5HhghMC9YHa0JP5WoSPOodKtvXXJamHQ5Zplj0Z7rSOu8Y9jvu1uwtew/udc9c318EZk1dis2FkeM4F0CP3wPHESTmAyy9eppRxxEe0tmueCtPyaKhc2Ydg0JBJG02MHnui8SKEpKEDyF1lBEPwSLz3FjdXwYWfsKl8URASddvuxkQ==</SignatureValue>

    <KeyInfo>

      <X509Data>

        <X509Certificate></X509Certificate>

      </X509Data>

    </KeyInfo>

  </Signature>

</CATALOG>

## Metóda „GetAuthenticationToken“

Metóda získa autentizačný SAML token potrebný pre autentizáciu volaní jednotlivých vnútorných služieb NZIS.

*Vstupné parametre*

|  |  |  |
| --- | --- | --- |
| Parameter | Dátový typ | Popis |
| targetServiceIdentifier | string | Alfanumerický reťazec identifikujúci cieľovú službu NZIS, pre ktorú sa žiada vydanie autentizačného tokenu. |
| authenticationCertificateThumbprint | string | Thumbprint X509 certifikátu, ktorý sa má použiť pre identifikáciu pri žiadosti o vydanie autentizačného tokenu.  Tento certifikát musí byť z množiny certifikátov vrátených metódou GetAvailableCertificates (viď kap. 4.2) |

*Návratová hodnota*

Výstupom volania metódy GetAuthenticationTokenje Microsoft .NET Framework objekt typu System.IdentityModel.Tokens.SecurityToken reprezentujúci autentizačný SAML token. Tento objekt sa použije pri volaniach požadovaných služieb NZIS.

*Výnimky*

| Výnimka | Popis |
| --- | --- |
| CertificateNotFoundException | Výnimka nastane v prípade, keď sa medzi disponibilnými certifikátmi nenájde certifikát špecifikovaný v parametri „authenticationCertificateThumbprint“. |
| UnknownServiceIdentifierException | Parameter *targetServiceIdentifier* obsahuje neznámy identifikátor a autentifikačný server nevie identifikovať cieľovú službu pre ktorú je potrebné vystaviť autentifikačný token. |
| UnableContactIdentityProviderException | Nie je možné kontaktovať autentifikačný server z dôvodu uplynutia časového limitu alebo z dôvodu nedostupnosti autentifikačnej služby. |
| TrustFailureException | Nie je možné vytvoriť zabezpečený komunikačný kanál s autentifikačnou službou, pretože klient nedôveruje príslušným certifikačným autoritám IAM. |
| SecureChannelFailureException | Výnimka nastane v prípade, ak počas procesu autentifikácie zlyhá zabezpečenie komunikácie. |
| RequestedOperationFailedException | Nastane v prípade neočakávanej chyby operačného systému alebo sieťovej komunikácie.  Chyba, ktorá túto výnimku spôsobila je zahrnutá ako vlastnosť *InnerException* tejto výnimky. |

*Príklad*

Nesledujúci príklad demonštruje získanie autentizačného tokenu pomocou metódy GetAuthenticationToken pre volanie služby eZdravie.

....

using Iam.B2B.Client;

using Iam.IdentityModel;

....

// Vytvorenie inštancie klientskeho komponentu IAM B2B - CryptoController.

CryptoController cc = new CryptoController(

ConfigurationManager.AppSettings["ehealth.iam.b2b.client.nzisCertificatesFile"]

, ConfigurationManager.AppSettings["ehealth.iam.b2b.client.iamStsBaseUri"]

);

// Reťazec „URL\_ADRESA\_SLUZBY\_EZDRAVIE“ nahradiť konkrétnou hodnotou podľa x104 v závislosti od prostredia

SecurityToken token = cc.**GetAuthenticationToken**(

"URL\_ADRESA\_SLUZBY\_EZDRAVIE"

, "VALID\_CERTITICATE\_THUMBPRINT\_FROM\_AVAILABLE\_CERTS"

);

CallService(tok);

....

Vzorovú implementáciu metódy CallService je možné nájsť v dokumente x070E, „Detailná špecifikácia rozhrania – volanie služieb“.

## Metóda „EncryptForNzis“

Zašifruje bližšie nešpecifikovanú štruktúru dát pre definovanú množinu vnútorných služieb NZIS.

Metóda používa šifrovací algoritmus AES s dĺžkou kľúča 256 bitov v móde CBC (AlgorithmObjectID je „2.16.840.1.101.3.4.1.42“). Výstupné dáta sú následne zabalené do PKCS#7 enveloped message a vrátené ako pole bajtov.

*Vstupné parametre*

| Parameter | Dátový typ | Popis |
| --- | --- | --- |
| dataCollection | IEnumerable<byte[]> | Množina polí bajtov, určených na zašifrovanie. |

*Návratová hodnota*

Výsledkom volania tejto metódy je pole objektov BinaryOperationResult (viď kap. 4.1.2), pričom poradie prvkov tejto množiny zodpovedá poradiu prvkov dávky na vstupe. Platí teda, že výsledku operácie nad vstupom dataCollection[n] zodpovedá hodnota result[n]. (viď príklad volania nižšie).

V prípade úspešnej operácie hodnota BinaryOperationResult.Data obsahuje pole bajtov, reprezentujúce zašifrované dáta v štruktúre PKCS#7.

*Výnimky*

V prípade chyby môže hodnota BinaryOperationResult.FaultDetail obsahovať výnimky uvedené v nasledujúcej tabuľke a hodnota BinaryOperationResult.Data bude NULL.

|  |  |
| --- | --- |
| Výnimka | Popis |
| FileNotFoundException | Nie je možné nájsť lokálny súbor s certifikátmi služieb NZIS. |
| CertificateNotFoundException | Lokálny súbor s certifikátmi služieb NZIS neobsahuje žiadne platné šifrovacie certifikáty služieb NZIS. |
| CryptographicException | Nastane v prípade chyby počas samotného šifrovania údajov pre NZIS.  Chyba, ktorá túto výnimku spôsobila je zahrnutá ako vlastnosť *InnerException* tejto výnimky. |

*Príklad*

Nesledujúci príklad demonštruje zašifrovanie textu „Hello world!” pre služby NZIS volaním metódy *EncryptForNzis*.

....

using Iam.B2B.Client;

....

// Vytvorenie inštancie klientskeho komponentu IAM B2B - CryptoController.

CryptoController cc = new CryptoController(

ConfigurationManager.AppSettings["ehealth.iam.b2b.client.nzisCertificatesFile"]

, ConfigurationManager.AppSettings["ehealth.iam.b2b.client.iamStsBaseUri"]

);

string dataNaZasifrovanie = "Hello world!";

byte[] poleBajtovNaZasifrovanie = Encoding.UTF8.GetBytes(dataNaZasifrovanie);

BinaryOperationResult[] result = cc.**EncryptForNzis**(

new[] { poleBajtovNaZasifrovanie /\*, poleBajtov2, poleBajtov3 \*/ }

);

string zasifrovaneDataBase64 = Convert.ToBase64String(result[0].Data);

## Metóda „CreateEsid“

Metóda vytvorí ASN.1 štruktúru z

1. nešifrovaného identifikátora prijímateľa zdravotnej starostlivosti (parameter identifier),
2. jednoznačných identifikátorov „all\_compositions“ elementov vstupnej eHTalk správy a
3. identifikátorom autentizačného tokenu.

Následne túto štruktúru spolu s ďalšími metadátami digitálne podpíše s použitím privátneho kľúča špecifikovaného certifikátu do formy PKCS#7 štruktúry, ktorú následne celú zašifruje pre cieľové služby NZIS.

Presný popis ASN.1 štruktúry ESID ako aj postup jeho vytvárania je definovaný v technickej špecifikácii ESID, ktorá je samostatným dokumentom.

*Vstupné parametre*

| Parameter | Dátový typ | Popis |
| --- | --- | --- |
| identifier | string | Reťazec znakov predstavujúci identifikátor prijímateľa zdravotnej starostlivosti. |
| token | object | Autentizačný token vrátený metódou GetAuthenticationToken. |
| ehtalkMessage | string | Serialozavaná eHTalk správa s ktorou má byť vytvorený ESID prepojený. |
| esidSignerCertificateThumbprint | string | Alfanumerický reťazec identifikujúci certifikát, ktorým sa má vytvorený ESID podpísať.  Tento certifikát musí byť z množiny certifikátov vrátených metódou GetAvailableCertificates (viď kap. 4.2). |

*Návratová hodnota*

Výstupom volania metódy *CreateEsid* je reťazec znakov (string), reprezentujúci digitálne podpísaný a následne zašifrovaný identifikátor prijímateľa zdravotnej starostlivosti (ESID) transformovaný do Base64 formy.

*Výnimky*

| Výnimka | Popis |
| --- | --- |
| CertificateNotFoundException | Výnimka nastane v prípade, keď sa medzi disponibilnými certifikátmi nenájde certifikát špecifikovaný v parametri „esidSignerCertificateThumbprint“. |
| UnableToLoadEhtalkMessageXmlDataException | Nastane v prípade, ak ako vstupný parameter eHTalkMessage nie je platný XML dokument. |
| RcidNotFoundException | Výnimka nastane, ak sa pri výpočte kontrolného súčtu kompozícii vstupnej eHTalkMessage nepodarí identifikovať/nájsť „rc\_id“ danej kompozície.  Ak nastane táto výnimka, je potrebné skontrolovať, či eHTalkMessage má správnu štruktúru. |
| TooManyRcidException | Výnimka nastane, ak sa pri výpočte kontrolného súčtu kompozícii vstupnej eHTalkMessage nájde viacero „rc\_id“ pre danú kompozíciu a teda nie je možné jednoznačne určiť „rc\_id“ danej kompozície.  Ak nastane táto výnimka, je potrebné skontrolovať, či eHTalkMessage má správnu štruktúru. |
| CryptographicException | Nastane v prípade ak zlyhá samotné zašifrovanie ESID. Detaily chyby, ktorá spôsobila túto výnimku sú obsiahnuté vo vlastnosti *InnerException*. |

*Príklad*

....

using Iam.B2B.Client;

using Iam.IdentityModel;

....

// Vytvorenie inštancie klientskeho komponentu IAM B2B - CryptoController.

CryptoController cc = new CryptoController(

ConfigurationManager.AppSettings["ehealth.iam.b2b.client.nzisCertificatesFile"]

, ConfigurationManager.AppSettings["ehealth.iam.b2b.client.iamStsBaseUri"]

);

string certificateThumbprint = "VALID\_CERTITICATE\_THUMBPRINT\_FROM\_AVAILABLE\_CERTS";

SecurityToken token = cc.**GetAuthenticationToken**(

"https://adfs2.ehealth-iam.local/WSTest/service.svc"

, certificateThumbprint

);

// Vytvorenie príslušnej eHTalk správy a jej serializovanie do premennej ehtalkMsg

string ehtalkMsg = "REPLACE\_THIS\_WITH\_SERIALIZED\_EHTALK\_MESSAGE";

string esid = cc.**CreateEsid**("00000000018", token, ehtalkMsg, certificateThumbprint);

## Metóda „DecryptDataFromNzis“

Dešifruje údaje, zašifrované službami NZIS.

*Vstupné parametre*

| Parameter | Dátový typ | Popis |
| --- | --- | --- |
| encryptedDataCollection | IEnumerable<byte[]> | Množina polí bajtov, reprezentujúcich správy vo forme PKCS#7, určené na rozšifrovanie.  Tieto údaje musia byť šifrované na niektorý disponibilných certifikátov. |

*Návratová hodnota*

Výsledkom volania tejto metódy je pole objektov BinaryOperationResult (viď kap. 4.1.2), pričom poradie prvkov tejto množiny zodpovedá poradiu prvkov dávky na vstupe. Platí teda, že výsledku operácie nad vstupom encryptedDataCollection[n] zodpovedá hodnota result[n]. (viď príklad volania nižšie).

V prípade úspešnej operácie hodnota BinaryOperationResult.Data obsahuje pole bajtov, reprezentujúce rozšifrované dáta.

*Výnimky*

V prípade chyby môže hodnota BinaryOperationResult.FaultDetail obsahovať výnimky uvedené v nasledujúcej tabuľke a hodnota BinaryOperationResult.Data bude obsahovať pôvodné, šifrované údaje pri ktorých chyba nastala.

|  |  |
| --- | --- |
| Výnimka | Popis |
| CertificateNotFoundException | Výnimka nastane v prípade, keď medzi disponibilnými certifikátmi sa nenachádza certifikát žiadneho z cieľových adresátov, ktorým sú šifrované údaje z NZIS adresované. |
| CryptographicException | Nastane v prípade ak zlyhá samotné dešifrovanie správy.  Detaily chyby, ktorá spôsobila túto výnimku sú obsiahnuté vo vlastnosti *InnerException*. |

*Príklad*

....

using Iam.B2B.Client;

....

// Vytvorenie inštancie klientskeho komponentu IAM B2B - CryptoController.

CryptoController cc = new CryptoController(

ConfigurationManager.AppSettings["ehealth.iam.b2b.client.nzisCertificatesFile"]

, ConfigurationManager.AppSettings["ehealth.iam.b2b.client.iamStsBaseUri"]

);

string encDataString = String.Empty;

// 1. Do premennej encDataString načítajte Base64 kódovanú časť zašifrovaných dát z eHTalkMessage

byte[] encData = Convert.FromBase64String(encDataString);

BinaryOperationResult[] result = cc.DecryptDataFromNzis(

new[] { encData /\*, sifrovanaSprava2, sifrovanaSprava3 \*/ }

);

If (

result != null

&& result.Length > 0

&& result[0].IsSuccess

)

{

string strdata = UnicodeEncoding.Default.GetString(result[0].Data);

Console.WriteLine("Rozšifrované údaje z NZIS:");

Console.WriteLine(strdata);

}

## Metóda „ExtractPatientIdentifierFromEsid“

Metóda dešifruje identifikátor prijímateľa zdravotnej starostlivosti z ESID vráteného v odpovedi na volanie NZIS služieb a vráti informáciu o overení digitálneho podpisu na získanom ESID, zoznam kontrolných súčtov elementov „all\_compositions“ pre ktoré bol daný ESID vytvorený a samotný dešifrovaný identifikátor prijímateľa zdravotnej starostlivosti.

*Vstupné parametre*

| Parameter | Dátový typ | Popis |
| --- | --- | --- |
| base64EncodedSsid | string | Reťazec znakov predstavujúci Base64 transformovaný ESID získaný v odpovedi na volanie NZIS služby. |

*Návratová hodnota*

Metóda má nasledovné výstupné parametre:

| Parameter | Dátový typ | Popis |
| --- | --- | --- |
| patientIdentifier | string | Dešifrovaný identifikátor prijímateľa zdravotnej starostlivosti. |
| compositionsHashList | CompositionHashCollection | Zoznam kontrolných súčtov elementov „all\_compositions“, pre ktoré bol daný ESID vytvorený. |
| signatureStatus | EsidSignatureStatus | Enumerácia hodnôt o výsledku overenia digitálneho podpisu na danom ESID. Možné hodnoty:   * „NotVerified“ – podpis nebol overovaný. * „OK“ – všetko je v poriadku (podpis aj podpisovateľ). * „UnableToVerifySigner“ – digitálny podpis je v poriadku ale X.509 certifikát podpisovateľa bol medzičasom exspirovaný, zrušený alebo ho nebolo možné overiť. * „InvalidSignature“ – digitálny podpis nie je platný. |

Nasledujúci obrázok detailnejšie zobrazuje štruktúru „CompositionHashCollection“.



Obr. 18 Štruktúra "CompositionHashCollection"

*Výnimky*

|  |  |
| --- | --- |
| Výnimka | Popis |
| CertificateNotFoundException | Výnimka nastane v prípade, keď medzi disponibilnými certifikátmi sa nenachádza certifikát žiadneho z cieľových adresátov, ktorým sú šifrované údaje z NZIS adresované. |
| CryptographicException | Nastane v prípade ak zlyhá samotné rozšifrovanie ESIDu alebo overovanie elektronického podpisu na ESIDe.  Detaily chyby, ktorá spôsobila túto výnimku sú obsiahnuté vo vlastnosti *InnerException*. |

*Príklad*

// ....

using Iam.B2B.Client;

using eHealth.Security.Esid;

// ....

// Vytvorenie inštancie klientskeho komponentu IAM B2B - CryptoController.

CryptoController cc = new CryptoController(

ConfigurationManager.AppSettings["ehealth.iam.b2b.client.nzisCertificatesFile"]

, ConfigurationManager.AppSettings["ehealth.iam.b2b.client.iamStsBaseUri"]

);

string esidFromNzisReponse;

// 1. Realizácia volania služby NZIS

// 2. Extrahovanie ESIDu z odpovede služby do premennej "esidFromNzisReponse"

// 3. Deklarovanie premenných pre návratové hodnoty metódy "ExtractPatientIdentifierFromEsid".

string przsID;

CompositionHashCollection compositionsHashList;

EsidSignatureStatus signatureStatus;

// Dešifrovanie ESID pomocou " ExtractPatientIdentifierFromEsid".

cc.**ExtractPatientIdentifierFromEsid**(esidFromNzisReponse

, out przsID

, out compositionsHashList

, out signatureStatus

);

// Vypísanie dešifrovaného identifikátora na obrazovku

Console.WriteLine("Identifikátor prijímateľa zdravotnej starostlivosti je: {0}", przsID);