

Integračná príručka

D.Sig XAdES Extender .NET, v4.0

Projekt	GOV_ZEP	A3019_002
Dokument	Integračná príručka	
Referencia	GOV_ZEP.201	Verzia 8

Copyright

Všetky práva vyhradené

Tento dokument je vlastníctvom spoločnosti DITEC, a. s. Žiadna jeho časť sa nesmie akýmkoľvek spôsobom (elektronickým, mechanickým) poskytnúť tretej strane, rozmnožovať, kopírovať, vrátane spätného prevodu do elektronickej podoby, bez písomného povolenia spracovávateľa.

Popisné charakteristiky dokumentu

Projekt	GOV_ZEP	A3019_002
Dokument	Integračná príručka	
Podnázov	D.Sig XAdES Extender .NET, v4.0	
Ref. číslo	GOV_ZEP.201	Verzia 8

Vypracoval	Mikuš Michal	Podpis	Dátum 14. 7. 2023
Preveril	Priezvisko Meno	Podpis	Dátum
Schválil	Priezvisko Meno	Podpis	Dátum

Formulár	Dokument		
Ref. číslo	Fo 11	Dátum poslednej aktualizácie	Dátum 03.01.2013

Akceptované dňa : <Dátum akceptácie>

Za <Objednávateľa>:

Za <Dodávateľa>.:

<Meno zodpovednej osoby>

< Meno zodpovednej osoby >

Projekt	GOV_ZEP	A3019_002
Dokument	Integračná príručka	
Referencia	GOV_ZEP.201	Verzia 8

Záznamy o zmenách

Autor	Popis zmien	Dátum	Verzia
M.Mikuš	Súlad so špecifikáciou v.7 zo 4.11.2016 Zmena názvu parametra Class a oiClass v triede MessageContainer. Úprava XML a Json výstupu v metóde GetObjectinfo (tiež MC)	9.1.2017	4
M.Mikuš	Súlad so špecifikáciou v.8. Korekcia terminológie, delenia metód v kapitole 5 (Špecifikácia API) a doplnenie popisov niektorých parametrov. Aktualizácia systémových požiadaviek.	14.7.2023	8

Pripomienkovanie a kontrola

Autor	Stanovisko	Dátum	Verzia

Rozdeľovník

	Priezvisko Meno	Firma, Funkcia
Originál		
Kópia		
Kópia		
Kópia		

Projekt	GOV_ZEP	A3019_002
Dokument	Integračná príručka	
Referencia	GOV_ZEP.201	Verzia 8

Obsah

1.	Úvod	6
2.	Použité zdroje	7
3.	Systémové požiadavky	8
4.	Architektúra	10
4.1.	Postavenie v rámci nadradenej aplikácie	10
4.2.	Vnútorná architektúra.....	10
5.	Špecifikácia API.....	11
5.1.	.NET API	11
5.1.1.	Trieda Extender	11
5.1.1.1.	Triedy použité ako výstupné hodnoty metód	13
5.1.2.	Trieda MessageContainer	15
5.1.2.1.	Triedy použité ako výstupné hodnoty metód	16
5.2.	Trieda Extender.....	17
5.2.1.	Popis vlastností	17
5.2.1.1.	ErrorMessage.....	17
5.2.1.2.	DataSignatures.....	17
5.2.1.3.	DocumentUnauthorized.....	17
5.2.1.4.	Registration	18
5.2.1.5.	RegistrationBase64	18
5.2.2.	Popis spoločných metód	18
5.2.2.1.	konštruktor triedy Extender.....	18
5.2.2.2.	metóda GetDocumentCount.....	18
5.2.2.3.	metóda MoveToDocument	18
5.2.2.4.	metóda GetDocumentType	18
5.2.2.5.	metóda Initialize	19
5.2.2.6.	metóda OpenFile.....	19
5.2.3.	Metódy zloženého elektronického podpisu.....	20
5.2.3.1.	metóda CreateNewDataSignatures.....	20
5.2.3.2.	metóda AddDataEnvelopeToExistingDataSignatures	20
5.2.3.3.	metóda InsertDataSignatures.....	21
5.2.3.4.	metóda GetDataSignaturesInfo	21
5.2.3.5.	metóda GetDataSignaturesInfo	23
5.2.3.6.	metóda VerifyDataSignatures.....	23
5.2.4.	Dokument bez autorizácie	24
5.2.4.1.	CreateNewDocumentUnauthorized.....	24

Projekt	GOV_ZEP	A3019_002
Dokument	Integračná príručka	
Referencia	GOV_ZEP.201	Verzia 8

5.2.4.2. metóda GetDocumentUnauthorizedInfo	24
5.2.4.3. metóda GetDocumentUnauthorizedInfo	25
5.2.5. Podanie	25
5.2.5.1. metóda CreateNewRegistration	25
5.2.5.2. metóda GetRegistrationInfo.....	25
5.2.5.3. metóda GetRegistrationInfo.....	26
5.3. Trieda MessageContainer	26
5.3.1. Popis vlastností a metód.....	27
5.3.1.1. ErrorMessage.....	27
5.3.1.2. konštruktor.....	27
5.3.1.3. metóda Initialize	27
5.3.1.4. metóda AddXObject	27
5.3.1.5. metóda AddBase64Object	28
5.3.1.6. metóda GetMessageContainer.....	28
5.3.1.7. metóda Initialize	28
5.3.1.8. metóda IsInitialized.....	29
5.3.1.9. metóda GetMessageContainerInfo.....	29
5.3.1.10. metóda GetMessageContainerInfo	29
5.3.1.11. metóda GetObjectCount	30
5.3.1.12. metóda GetObjectInfo	30
5.3.1.13. metóda GetObjectInfo	30
5.3.1.14. metóda GetObjectData	31
5.3.1.15. metóda GetVersion	31
6. Scenáre použitia	32
6.1. Scenár 1 – vytvorenie podania	32
6.2. Scenár 2 – zistenie informácií z existujúceho podania/zásielky	33
7. Návratové kódy aplikácie	35

Projekt	GOV_ZEP	A3019_002
Dokument	Integračná príručka	
Referencia	GOV_ZEP.201	Verzia 8

1. Úvod

Tento dokument je určený pre používateľov softvérového komponentu D.Sig XAdES Extender .NET a vývojárov aplikácií pre vytváranie a spracovanie zaručených elektronických podpisov formátu XAdES_ZEP.

Komponent D.Sig XAdES Extender .NET je určený na

- vytváranie štruktúry zloženého elektronického podpisu [6], neautorizovaného dokumentu [7] a podania [8],
- spracovanie podania a získavanie informácií o tejto štruktúre a o obsiahnutých podpisoch,
- vytváranie a spracovávanie elektronických správ vo formáte MessageContainer podľa [10].

Komponent je určený na integráciu do komplexnejších systémov ako pomocná knižnica a neposkytuje užívateľské rozhranie, takže jej popis je zredukovaný na zoznam funkcií a ich vstupno-výstupné charakteristiky (popísané v časti 5).

Systémové požiadavky sú zhrnuté v časti 3 a príklady použitia komponentu sú uvedené v časti 6.

Projekt	GOV_ZEP	A3019_002
Dokument	Integračná príručka	
Referencia	GOV_ZEP.201	Verzia 8

2. Použité zdroje

- [1] Formát jednoduchého elektronického podpisu XAdES_ZEP, verzia 1.0.
http://www.ditec.sk/ep/signature_formats/xades_zep/v1.0/
- [2] Formát jednoduchého elektronického podpisu XAdES_ZEP, verzia 1.1.
http://www.ditec.sk/ep/signature_formats/xades_zep/v1.1/
- [3] Formát jednoduchého elektronického podpisu XAdES_ZEP, verzia 2.0.
http://www.ditec.sk/ep/signature_formats/xades_zep/v2.0/
- [4] Formát zloženého elektronického podpisu XAdES_ZEP, verzia 1.0.
http://www.ditec.sk/ep/signature_formats/xades_zep_data_signatures/v1.0/
- [5] Formát zloženého elektronického podpisu XAdES_ZEP, verzia 1.1.
http://www.ditec.sk/ep/signature_formats/xades_zep_data_signatures/v1.1/
- [6] Formát zloženého elektronického podpisu XAdES_ZEP, verzia 2.0.
http://www.ditec.sk/ep/signature_formats/xades_zep_data_signatures/v2.0/
- [7] XML štruktúra dokumentu bez autorizácie
<http://www.ditec.sk/ekr/unauthorized/v1.0>
- [8] XML štruktúra podania <http://www.ditec.sk/ekr/registration/v1.0>
- [9] Špecifikácia softvérového komponentu XAdES Extender.
GOV_ZEP.161.2.140306.Špecifikácia D.Sig.XAdES.Extender.docx
- [10] Výnos MF SR z 3. apríla 2014 č. MF/009269/2014-173 o jednotnom formáte elektronických správ vytváraných a odosielaných prostredníctvom prístupových miest

Projekt	GOV_ZEP	A3019_002
Dokument	Integračná príručka	
Referencia	GOV_ZEP.201	Verzia 8

3. Systémové požiadavky

Použitie knižnice D.Sig XAdES Extender .NET vyžaduje:

- OS – MS Windows 7, Windows 8.x, Windows 10, Windows 11,
- platforma – .Net framework, verzia 4.5.1 alebo vyššia,

Ak je knižnica D.Sig XAdES Extender .NET spúšťaná z web portálu pomocou aplikácie D.Launcher v1.x, tak požiadavky na web prehliadač sú nasledovné:

- MS Internet Explorer, v7.0 alebo vyššia (IE 7/8/9 len 32 bit, IE 10/11 32 aj 64 bit), Mozilla Firefox, v45 alebo vyššia, Google Chrome v51 alebo vyššia (prípadne Chromium), Opera v38 alebo vyššia, MS Edge v25 alebo vyššia..

Ak je knižnica D.Sig XAdES Extender .NET spúšťaná z web portálu pomocou aplikácie D.Launcher v2 a rozšírenia D.Bridge 2, tak sú podporované tieto prehliadače:

- MS Internet Explorer 11 (len 32bit verzia), Mozilla Firefox 78, 89, 91, 101, Google Chrome 91, 100, 101, Chromium 91, 100, 101, Opera 76, 78, Microsoft Edge 91, 96, 97; vo webovom prehliadači nainštalované a povolené rozšírenie D.Bridge 2, pre MS Internet Explorer sa vyžaduje vypnutý chránený režim.

D.Sig XAdES Extender .NET x64 je možné spúštať výlučne pomocou aplikácie D.Launcher. Systémové požiadavky pre aplikáciu D.Launcher sú špecifikované v rámci používateľskej príručky pre aplikáciu D.Launcher.

Pre aplikáciu D.Sig XAdES Extender .NET nie sú potrebné vyššie hardwarové požiadavky, ako vyžaduje samotný operačný systém, prípadne platforma .Net framework 4.0 alebo vyššia. Požiadavky aplikácie na voľný priestor na disku sú nasledujúce:

Komponent	Veľkosť
D.Sig XAdES Extender .NET, v4.0	5,66 MB

Aplikácia D.Sig XAdES Extender .NET môže byť distribuovaná na inštalačnom CD alebo v rámci klientskej aplikácie, ktorá komponent pre zaručený elektronický podpis používa, či už v rámci jej inštalačných súborov alebo priamo cez Internet na HTTPS stránkach danej web aplikácie. Veľkosť distribučných, resp. inštalačných súborov komponentu D.Sig XAdES Extender .NET je uvedená v nasledujúcej tabuľke.

Komponent	Veľkosť
D.Sig XAdES Extender .NET x86	5,56 MB

Projekt	GOV_ZEP	A3019_002
Dokument	Integračná príručka	
Referencia	GOV_ZEP.201	Verzia 8

D.Sig XAdES Extender .NET x64	4,17 MB
-------------------------------	---------

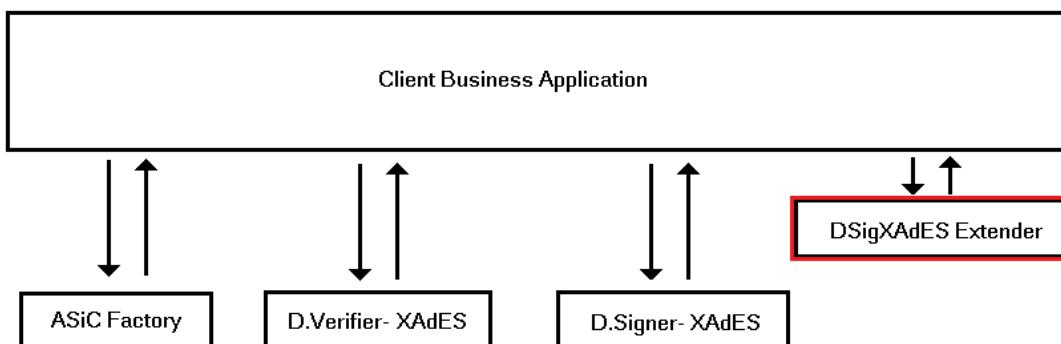
Podrobný popis požiadaviek na prevádzku aplikácie je totožný s požiadavkami na prevádzku, ktoré sú špecifikované v rámci dokumentácie produktu D.Signer/XAdES .NET.

Projekt	GOV_ZEP	A3019_002
Dokument	Integračná príručka	
Referencia	GOV_ZEP.201	Verzia 8

4. Architektúra

4.1. Postavenie v rámci nadradenej aplikácie

Tento komponent poskytuje volajúccej aplikácii rozhranie na vytváranie a spracovanie dátových obálok formátu xzep:DataSignatures a štruktúr podania podľa požiadaviek definovaných v špecifikácii [9]. Volajúca aplikácia ku tomu poskytuje všetky potrebné údaje, takže nie je potrebná interakcia so žiadnymi ďalšími modulmi.



Obr. 1: Postavenie komponentu D.Sig XAdES Extender v rámci širšieho systému na vytváranie a spracovanie elektronicky podpísaných dokumentov. Ostatné komponenty (ASiC Factory, D.Signer-XAdES, ...) sú uvedené ako príklad a nie sú potrebné pre fungovanie D.Sig XAdES Extender.

4.2. Vnútorná architektúra

Vzhľadom na oddelené množiny funkčných požiadaviek postačuje, aby komponent bol tvorený jednou triedou pre základnú funkcionality a jednou triedou pre prácu so štruktúrou MessageContainer.

Metódy týchto tried poskytujú možnosti pre všetky možné scenáre použitia a sú podrobne popísané v nasledujúcej časti.

Projekt	GOV_ZEP	A3019_002
Dokument	Integračná príručka	
Referencia	GOV_ZEP.201	Verzia 8

5. Špecifikácia API

Na základe technológie volajúcej aplikácie je možný prístup k metódam buď priamo referencovaním (.NET trieda Ditec.Zep.DsigXadesExtender.Extender, resp. trieda Ditec.Zep.DsigXadesExtender.MessageContainer), alebo pomocou niektorého rozhrania (NPAPI, COM, COM ATL) uvedeného v samostanom dokumente, ktorý tvorí prílohu tejto príručky.

Rozhranie .NET je popísané nižšie.

Knižnica neposkytuje GUI a teda oznamovanie výstupov z knižnice je plne na strane volajúcej aplikácie.

5.1. .NET API

5.1.1. Trieda Extender

Hlavná trieda:

Ditec.Zep.DsigXadesExtender.Extender

Konštruktor:

Extender();

Vlastnosti:

```
string ErrorMessage { get; }
string DataSignatures { get; }
string DocumentUnauthorized { get; }
string Registration { get; }
string RegistrationBase64 { get; }
```

Metódy:

```
int CreateNewDataSignatures(
    string inDataEnvelope,
    string inURI,
    string inID,
    string inDescription,
    string dataSignaturesVersion = "1.1"
);
int AddDataEnvelopeToExistingDataSignatures(
    string inDataSignatures,
    string inDataEnvelope
);
```

Projekt	GOV_ZEP	A3019_002
Dokument	Integračná príručka	
Referencia	GOV_ZEP.201	Verzia 8

```

DataSignaturesInfo GetDataSignaturesInfo(string inDataSignatures);
string GetDataSignaturesInfo(
    string inDataSignatures,
    int type
);
int VerifyDataSignatures(string inDataSignatures);
int GetDocumentCount();
int MoveToDocument(int index);
int GetDocumentType();
int CreateNewDocumentUnauthorized(
    string inURI,
    string inID,
    string inDescription,
    string objectData,
    string inObjectID,
    string inObjectMimeType,
    string inObjectEncoding,
    string inObjectIdentifier
);
DocumentUnauthorizedInfo GetDocumentUnauthorizedInfo(
    string inDocumentUnauthorized
);
string GetDocumentUnauthorizedInfo(
    string inDocumentUnauthorized,
    int type
);
int CreateNewRegistration(
    string inURI,
    string inID,
    string inDescription,
    string inExternalIdentifier,
    string inBusinessIdentifier
);
RegistrationInfo GetRegistrationInfo(string inRegistration);
string GetRegistrationInfo(
    string inRegistration,

```

Projekt	GOV_ZEP	A3019_002
Dokument	Integračná príručka	
Referencia	GOV_ZEP.201	Verzia 8

```

        int type
    );
    void Initialize();
    string OpenFileDialog(
        string title,
        string filter,
        int readBinary,
        int type
    );
    int InsertDataSignatures(string inDataSignatures);
    string GetVersion();

```

5.1.1.1. Triedy použité ako výstupné hodnoty metód

```

public class DataSignaturesInfo
{
    string Id { get; }
    string Uri { get; }
    string Description { get; }
    string DataSignaturesVersion { get; }
    int SignatureInfoListCount { get; }
    List<SignatureInfo> SignatureInfoList { get; }
    int DispatchObjectInfoListCount { get; }
    List<DispatchObjectInfo> DispatchObjectInfoList { get; }
    int ObjectIdListCount { get; }
    List<string> ObjectIdList { get; }
    int SignatureIdListCount { get; }
    List<string> SignatureIdList { get; }
    int DataEnvelopeListCount { get; }
    List<string> DataEnvelopeList { get; }
}
public class SignatureInfo
{
    string SignatureId { get; }
    int SignedObjectInfoListCount { get; }
    List<SignedObjectInfo> SignedObjectInfoList { get; }
    string X509CertificateDataBase64 { get; }
    string SignatureVersion { get; }
}

```

Projekt	GOV_ZEP	A3019_002
Dokument	Integračná príručka	
Referencia	GOV_ZEP.201	Verzia 8

```

        List<ProductInfo> ProductInfos { get; }

    }
public class SignedObjectInfo
{
    string ObjectId { get; }
    string Description { get; }
    string ObjectIdentifier { get; }
    string MimeType { get; }
    string Data { get; }
    string Encoding { get; }
    string VerifDataObjectVersion { get; }
    Dictionary<string, string> VerifDataObjectParams { get; }
}
public class ProductInfo
{
    string ProductName { get; }
    string ProductVersion { get; }
}
public class DispatchObjectInfo
{
    string ObjectId { get; }
    string MimeType { get; }
    string Data { get; }
    string Encoding { get; }
}
public class DocumentUnauthorizedInfo
{
    string Id { get; }
    string Uri { get; }
    string Description { get; }
    int UnauthorizedObjectInfoListCount { get; }
    List<UnauthorizedObjectInfo> UnauthorizedObjectInfoList { get; }
}
public class UnauthorizedObjectInfo
{
    string Id { get; }

```

Projekt	GOV_ZEP	A3019_002
Dokument	Integračná príručka	
Referencia	GOV_ZEP.201	Verzia 8

```

        string MimeType { get; }
        string Encoding { get; }
        string Identifier { get; }
        string Data { get; }
    }
    public class RegistrationInfo
    {
        string Id { get; }
        string Uri { get; }
        string Description { get; }
        string ExternalIdentifier { get; }
        string BusinessIdentifier { get; }
        int DocumentInfoListCount { get; }
        List<DocumentInfo> DocumentInfoList { get; }
    }
    public class DocumentInfo
    {
        int DocumentType { get; }
        string Data { get; }
    }
}

```

5.1.2. Trieda MessageContainer

Hlavná trieda:

Ditec.Zep.DsigXadesExtender.MessageContainer

Vlastnosti:

```
    string ErrorMessage { get; }
```

Metódy:

```

    void Initialize(
        string messageID,
        string senderID,
        string recipientID,
        string messageType,
        string messageSubject,
        string senderBusinessReference,
        string recipientBusinessReference
    );

```

Projekt	GOV_ZEP	A3019_002
Dokument	Integračná príručka	
Referencia	GOV_ZEP.201	Verzia 8

```

void Initialize(string mc);
bool IsInitialized();
int AddXMLObject(
    string id,
    string name,
    string description,
    string classAttr,
    int isSigned,
    string mimeType,
    string objectData
);
int AddBase64Object(
    string id,
    string name,
    string description,
    string classAttr,
    int isSigned,
    string mimeType,
    string objectDataBase64
);
string GetMessageContainer();
MessageContainerInfo GetMessageContainerInfo();
string GetMessageContainerInfo(int type);
int GetObjectCount();
ObjectInfo GetObjectInfo(int i);
string GetObjectInfo(
    int i,
    int type
);
string GetObjectData(int i);
string GetVersion();

```

5.1.2.1. Triedy použité ako výstupné hodnoty metód

```

public class MessageContainerInfo
{
    string MessageId { get; set; }
    string SenderId { get; set; }

```

Projekt	GOV_ZEP	A3019_002
Dokument	Integračná príručka	
Referencia	GOV_ZEP.201	Verzia 8

```

        string RecipientId { get; set; }
        string MessageType { get; set; }
        string MessageSubject { get; set; }
        string SenderBusinessReference { get; set; }
        string RecipientBusinessReference { get; set; }
    }
    public class ObjectInfo
    {
        string Id { get; set; }
        string Name { get; set; }
        string Description { get; set; }
        string ClassAttr { get; set; }
        bool? IsSigned { get; set; }
        string MimeType { get; set; }
        string Encoding { get; set; }
    }
}

```

5.2. Trieda Extender

Nasleduje stručný popis vlastností a metód triedy Ditec.Zep.DsigXadesExtender.Extender. Metódy sú rozdelené do štyroch množín podľa účelu na: spoločné (pomochné) metódy, metódy zloženého podpisu, metódy dokumentu bez autorizácie a metódy podania.

5.2.1. Popis vlastností

5.2.1.1. ErrorMessage

popis:

Premenná ErrorMessage obsahuje po každom volaní metód triedy Extender prípadné chybové hlásenie.

5.2.1.2. DataSignatures

popis:

Premenná DataSignatures obsahuje (v prípade úspešného volania príslušných metód) štruktúru vytvoreného zloženého elektronického podpisu v súlade s [4] alebo [5] a [6].

5.2.1.3. DocumentUnauthorized

popis:

Táto premenná obsahuje štruktúru dokumentu bez autorizácie podľa [7].

Projekt	GOV_ZEP	A3019_002
Dokument	Integračná príručka	
Referencia	GOV_ZEP.201	Verzia 8

5.2.1.4. Registration

popis:

Premenná Registration obsahuje (v prípade úspešného volania príslušnej metódy) štruktúru podania podľa [8].

5.2.1.5. RegistrationBase64

popis:

Premenná Registration obsahuje (v prípade úspešného volania príslušnej metódy) štruktúru podania podľa [8] v base64 kódovaní.

5.2.2. Popis spoločných metód

5.2.2.1. konštruktor triedy Extender

vstupné parametre: žiadne

výstupné parametre: žiadne

popis:

Vytvorí sa prázdna inštancia triedy Extender. Očakáva sa jeho inicializácia volaním metódy *Initialize()*.

5.2.2.2. metóda GetDocumentCount

vstupné parametre: žiadne

výstupné parametre: žiadne

návratová hodnota: celé číslo

popis:

Metóda vráti počet inštancií dokumentov vytvorených pomocou metód CreateNewDataSignatures alebo CreateNewDocumentUnauthorized (čiže súčet inštancií zložených podpisov DataSignatures a nepodpísaných dokumentov DocumentUnauthorized).

5.2.2.3. metóda MoveToDocument

vstupné parametre: celé číslo

výstupné parametre: žiadne

návratová hodnota: celé číslo

popis:

Metóda nastaví dokument so vstupným indexom ako aktuálny (nad ktorým sa budú vykonávať nasledujúce operácie). Ak je vstupný index mimo rozsahu (menší ako nula, väčší alebo rovný ako počet dokumentov) nevykoná nič a vráti chybu.

5.2.2.4. metóda GetDocumentType

vstupné parametre: žiadne

Projekt	GOV_ZEP	A3019_002
Dokument	Integračná príručka	
Referencia	GOV_ZEP.201	Verzia 8

výstupné parametre: žiadne

návratová hodnota: celé číslo

popis:

Metóda vráti typ aktuálne nastaveného dokumentu. Návratová hodnota:

- 0 zložený elektronický podpis,
- 1 znamená dokument bez autorizácie,
- záporná chyba.

Iné hodnoty sa vrátiť nesmú.

5.2.2.5. metóda Initialize

vstupné parametre: žiadne

výstupné parametre: žiadne

návratová hodnota: žiadna

popis:

Metóda nastaví triedu do iniciálneho stavu:

1. nastaví počet dokumentov na nula,
2. nastaví počet zložených podpisov na nula,
3. všetky interné zoznamy nastaví na prázdne.

5.2.2.6. metóda OpenFile

vstupné parametre:

- textový reťazec `title` – popis v hlavičke dialógu,
- textový reťazec `filter` – umožňuje použiť filter pri výbere súboru,
- celé číslo `readBinary` – či sa načítava binárne (1=áno, inak nie),
- celé číslo `type` – určuje typ výstupu (0=XML, inak JSON) štruktúry `OpenFileInfo`.

výstupné parametre: žiadne

návratová hodnota: štruktúra `OpenFileInfo` (typu string)

Štruktúra `OpenFileInfo` obsahuje:

- textový reťazec `fileExtension` – koncovka súboru,
- textový reťazec `fileName` – meno súboru,
- textový reťazec `fileNameWithPath` – meno súboru vrátane cesty,
- textový reťazec `fileContent` – obsah súboru, v prípade binárnych súborov sa nenapíňa,
- textový reťazec `fileContentBase64` – obsah súboru v base64 kódovaní, v prípade textových súborov sa nenapíňa.

popis:

Projekt	GOV_ZEP	A3019_002
Dokument	Integračná príručka	
Referencia	GOV_ZEP.201	Verzia 8

Metóda zobrazí dialóg pre načítanie súboru podľa vstupných parametrov. Vstupný filter môže byť v tvare „XML File | *.xml | All | *.*“. Ak je nastavený readBinary na jedna, tak sa načítava binárne a výstupný reťazec fileContent* bude prázdny.

5.2.3. Metódy zloženého elektronického podpisu

5.2.3.1. metóda CreateNewDataSignatures

vstupné parametre:

- textový reťazec inDataEnvelope – štruktúra jednoduchého podpisu podľa [1], [2] alebo [3],
- textový reťazec inURI – jednoznačný identifikátor profilu dátovej štruktúry zloženého elektronického podpisu (mal by byť definovaný v rámci príslušného procesu špecifikácie dátových štruktúr na aplikačnej úrovni),
- textový reťazec inID – nepovinný atribút, identifikátor danej inštancie vytvoreného zloženého elektronického podpisu,
- textový reťazec inDescription – nepovinný atribút, popis inštancie alebo profilu zloženého elektronického podpisu,
- textový reťazec dataSignaturesVersion – (nepovinný parameter) označenie formátu vytváraného zloženého el.podpisu (povolené hodnoty sú 1.0, 1.1 a 2.0).

výstupné parametre: žiadne

návratová hodnota: celé číslo

popis:

Parameter dataSignaturesVersion je nepovinný. V prípade absencie je jeho hodnota nastavená na hodnotu „1.1“.

Metóda vytvorí na základe vstupných parametrov štruktúru zloženého elektronického podpisu podľa [4] alebo [5] a [6]. Vytvorená štruktúra bude zaradená na koniec zoznamu dokumentov a bude predstavovať aktuálny dokument, nad ktorým sa budú vykonávať nasledujúce operácie.

V prípade úspechu je návratová hodnota 0, v opačnom prípade číslo rôzne od nuly. Výsledný elektronický podpis bude uložený v DataSignatures vlastnosti..

5.2.3.2. metóda AddDataEnvelopeToExistingDataSignatures

vstupné parametre:

- textový reťazec inDataSignatures – štruktúra zloženého elektronického podpisu verzie 1.0 [4], 1.1 [5] alebo 2.0 [6],

Projekt	GOV_ZEP	A3019_002
Dokument	Integračná príručka	
Referencia	GOV_ZEP.201	Verzia 8

- textový reťazec `inDataEnvelope` – štruktúra jednoduchého zloženého podpisu verzie 1.0 [1], 1.1 [2], alebo 2.0 [3].

výstupné parametre: žiadne

návratová hodnota: celé číslo

popis:

Metóda vloží vstupnú štruktúru `inDataEnvelope` jednoduchého podpisu do zloženej štruktúry `inDataSignatures` a výslednú zloženú štruktúru vloží na aktuálnu pozíciu v zozname zložených elektronických podpisov triedy.

V prípade úspechu je návratová hodnota 0, v opačnom prípade číslo rôzne od nuly. Výsledný elektronický podpis bude uložený v `DataSignatures` vlastnosti.

5.2.3.3. metóda `InsertDataSignatures`

vstupné parametre: textový reťazec `inDataSignatures`

výstupné parametre: žiadne

návratová hodnota: celé číslo

popis:

Metóda vloží vstupný zložený podpis do kolekcie zložených podpisov.

V prípade úspechu je návratová hodnota 0, v opačnom prípade číslo rôzne od nuly. Výsledný elektronický podpis bude uložený v `DataSignatures` vlastnosti.

5.2.3.4. metóda `GetDataSignaturesInfo`

vstupné parametre: textový reťazec `inDataSignatures`

výstupné parametre: žiadne

návratová hodnota: štruktúra `DataSignaturesInfo`

popis:

Metóda vráti informácie o štruktúre aktuálneho zloženého podpisu. Štruktúra `DataSignaturesInfo` obsahuje:

- string `Id` – atribút `Id` z `DataSignatures`,
- string `Uri` – atribút `URI` z `DataSignatures`,
- string `Description` – atribút `Description` z `DataSignatures`,
- int `SignatureInfoListCount` – počet podpisov,
- List<`SignatureInfo`> `SignatureInfoList` – zoznam podpisov,
- int `DispatchObjectInfoListCount` – počet dispatch objektov,
- List<`DispatchObjectInfo`> `DispatchObjectInfoList` – zoznam dispatch objektov,
- int `ObjectIdListCount` – počet objektov (mimo `dispatchnotes` objektov),

Projekt	GOV_ZEP	A3019_002
Dokument	Integračná príručka	
Referencia	GOV_ZEP.201	Verzia 8

- `List<string> ObjectIDList` – zoznam Id atribútov objektov (mimo dispatchnotes objektov),
- `int SignatureIdListCount` – počet podpisov,
- `List<string> SignatureIdList` – zoznam Id atribútov objektov
- `int DataEnvelopeListCount` – počet štruktúr `DataEnvelope` (jednoduchých podpisov),
- `List<string> DataEnvelopeList` – zoznam štruktúr `DataEnvelope`.

Štruktúra `SignatureInfo` obsahuje:

- `string SignatureId` – Id atribút konkrétneho podpisu,
- `int SignedObjectInfoListCount` – počet podpísaných objektov,
- `List<SignedObjectInfo> SignedObjectInfoList` – zoznam podpísaných objektov,
- `string X509CertificateDataBase64` – podpisový certifikát v base64 (vyhľadáva sa postupom špecifikovaným v metóde `VerifyDataSignatures`).
- `string SignatureVersion` – identifikátor verzie podpisu z elementu `xzep:SignatureVersion` v štruktúre `XAdES_ZEP`,
- `List<ProductInfo> ProductInfos` – identifikátory produktov, ktoré boli použité pre vytvorenie podpisu, a ich verzie z elementu `xzep:ProductInfos` v štruktúre `XAdES_ZEP`.

Štruktúra `SignedObjectInfo` obsahuje:

- `string ObjectId` – Id objektu,
- `string Description` – popis objektu,
- `string ObjectIdentifier` – identifikátor objektu,
- `stringMimeType` – mimetype objektu,
- `string Data` – dátá objektu,
- `string Encoding` – kódovanie dát v objekte.
- `string VerifDataObjectVersion` – verzia príslušného dátového objektu s verifikačnými údajmi,
- `Dictionary<string, string> VerifDataObjectParams` – zoznam `<key, value>` pre všetky verifikačné dátá v podpise.

Štruktúra `DispatchObjectInfo` obsahuje informácie o nepodpísaných objektoch:

- `string ObjectId` – Id objektu,

Projekt	GOV_ZEP	A3019_002
Dokument	Integračná príručka	
Referencia	GOV_ZEP.201	Verzia 8

- string `MimeType` – mimetype objektu,
- string `Data` – dátá objektu,
- string `Encoding` – kódovanie dát v objekte.

Štruktúra `ProductInfo` obsahuje:

- string `ProductName` – meno produktu,
- string `ProductVersion` – verzia produktu.

Hodnota `DataSignaturesVersion` je uvedená v atribúte `xmlns` elementu `DataSignatures`. V prípade viacerých `xmlns` atribútov treba zobrať ten, ktorý obsahuje prefix:

"http://www.ditec.sk/ep/signature_formats/xades_zep_data_signatures/v"

5.2.3.5. metóda `GetDataSignaturesInfo`

vstupné parametre:

- textový reťazec `inDataSignatures`,
- celé číslo `type` – určuje požadovaný typ výstupu.

výstupné parametre: žiadne

návratová hodnota: textový reťazec

popis:

Preťažená metóda vráti informácie o štruktúre aktuálneho zloženého podpisu vo formáte XML (vstup `type` = 0), alebo JSON (vstup `type` = 1).

5.2.3.6. metóda `VerifyDataSignatures`

vstupné parametre: textový reťazec `inDataSignatures`

výstupné parametre: žiadne

návratová hodnota: celé číslo

popis:

- Metóda vykoná overenie integrity zloženého elektronického podpisu tak, že overí každý jednoduchý podpis nasledovným spôsobom:
 - i) vezme sa `SignedInfo`, nájdu sa všetky referencie v ňom a skontroluje sa, či každá referencia ukazuje tam kde má a či každá referencia je správna - teda či haš sedí s tým, čo je tam uvedené,

Projekt	GOV_ZEP	A3019_002
Dokument	Integračná príručka	
Referencia	GOV_ZEP.201	Verzia 8

- ii) overí sa podpis elementu SignedInfo voči SignatureValue pomocou nájdeného podpisového certifikatu. Podpisový certifikát sa určí tak, že sa vezmú všetky certifikáty z KeyInfo (v pôdelemente X509Data/Certificate). A z nich sa vráti ten, ktorý je uvedený v xades:SignedSignatureProperties/SigningCertificate (podľa hašu). Ak sa podpisový certifikát nenájde, metóda vráti chybu.
- V prípade úspechu vráti číslo 0, v opačnom prípade vráti číslo rôzne od nuly.

5.2.4. Dokument bez autorizácie

5.2.4.1. CreateNewDocumentUnauthorized

vstupné parametre:

- textové reťazce inURI, inID, inDescription – parametre identifikujúce štruktúru dokumentu bez autorizácie,
- textový reťazec objectData – dáta objektu bez autorizácie,
- textové reťazce inObjectID, inObjectMimeType, inObjectEncoding, inObjectIdentifier – parametre identifikujúce dáta dokumentu bez autorizácie.

výstupné parametre: žiadne

návratová hodnota: celé číslo

popis:

Metóda vytvorí štruktúru dokumentu bez autorizácie v súlade s [7]. Táto štruktúra bude zaradená na koniec zoznamu dokumentov a bude predstavovať aktuálny dokument, nad ktorým sa budú vykonávať ďalšie operácie.

V prípade úspechu vráti číslo 0, v opačnom prípade vráti číslo rôzne od nuly.

5.2.4.2. metóda GetDocumentUnauthorizedInfo

vstupné parametre: textový reťazec inDocumentUnauthorized

výstupné parametre: žiadne

návratová hodnota: štruktúra DocumentUnauthorizedInfo

popis:

Metóda vráti informácie o vstupnom dokumente bez autorizácie. V prípade úspechu vráti nasledovnú štruktúru, v opačnom prípade vráti null.

Štruktúra DocumentUnauthorizedInfo obsahuje:

- string Id – atribút Id z DocumentUnauthorized,
- string Uri – atribút Uri z DocumentUnauthorized,
- string Description – atribút Description z DocumentUnauthorized,

Projekt	GOV_ZEP	A3019_002
Dokument	Integračná príručka	
Referencia	GOV_ZEP.201	Verzia 8

- int UnauthorizedObjectInfoListCount – počet objektov,
- List<UnauthorizedObjectInfo> UnauthorizedObjectInfoList – zoznam objektov.

Štruktúra UnauthorizedObjectInfo obsahuje:

- string Id – atribút Id z konkrétneho objektu,
- stringMimeType – atribútuMimeType z konkrétneho objektu,
- string Encoding – atribút Encoding z konkrétneho objektu,
- string Identifier – atribút Identifier z konkrétneho objektu,
- string Data – dátá konkrétneho objektu.

5.2.4.3. metóda GetDocumentUnauthorizedInfo

vstupné parametre:

- textový reťazec inDocumentUnauthorized,
- celé číslo type – požadovaný typ výstupu

výstupné parametre: žiadne

návratová hodnota: textový reťazec

popis:

Preťažená metóda vráti informácie o vstupnej štruktúre vo formáte XML (ak type=0), alebo vo formáte JSON (ak type=1).

V prípade neúspechu je návratová hodnota prázdny reťazec.

5.2.5. Podanie

5.2.5.1. metóda CreateNewRegistration

vstupné parametre: textové reťazce inURI, inID, inDescription, inExternalIdentifier, inBusinessIdentifier – parametre identifikujúce štruktúru podania podľa [8],

výstupné parametre: žiadne

návratová hodnota: celé číslo

popis:

Metóda vytvorí štruktúru podania podľa [8] z dokumentov, ktoré boli vytvorené v rámci inštancie triedy (pričom zachováva ich poradie). V prípade úspechu je návratová hodnota nula, v opačnom prípade rôzna od nuly. Výsledné podanie bude uložené v Registration a Registration64 vlastnosti.

5.2.5.2. metóda GetRegistrationInfo

vstupné parametre: textový reťazec inRegistration

výstupné parametre: žiadne

Projekt	GOV_ZEP	A3019_002
Dokument	Integračná príručka	
Referencia	GOV_ZEP.201	Verzia 8

návratová hodnota: RegistrationInfo

popis:

Metóda vráti na výstup štruktúru obsahujúcu informácie o vstupnom podaní. Štruktúra obsahuje nasledovné:

- string Id – atribút Id z RegistrationInfo,
- string Uri – atribút Uri z RegistrationInfo,
- string Description – atribút Description z RegistrationInfo,
- string ExternalIdentifier – atribút ExternalIdentifier z RegistrationInfo,
- string BusinessIdentifier – atribút BusinessIdentifier z RegistrationInfo,
- int DocumentInfoListCount – počet dokumentov,
- List<DocumentInfo> DocumentInfoList – zoznam dokumentov.

Štruktúra DocumentInfo obsahuje:

- int DocumentType – typ konkrétneho dokumentu:
 - ◆ 0 – zložený elektronický podpis,
 - ◆ 1 – dokument bez autorizácie,
 - ◆ -1 – neznámy typ dokumentu,
- string Data – dátá konkrétneho dokumentu.

5.2.5.3. metóda GetRegistrationInfo

vstupné parametre:

- textový reťazec inRegistration,
- celé číslo type – požadovaný typ výstupu

výstupné parametre: žiadne

návratová hodnota: textový reťazec

popis:

Preťažená metóda vráti informácie o štruktúre podania v XML (type=0) alebo JSON (type=1) štruktúre.

5.3. Trieda MessageContainer

Trieda MessageContainer slúži na vytváranie štruktúry nového kontajnera podľa špecifikácie [10] a parsovanie už existujúcej štruktúry kontajnera.

Projekt	GOV_ZEP	A3019_002
Dokument	Integračná príručka	
Referencia	GOV_ZEP.201	Verzia 8

5.3.1. Popis vlastností a metód

5.3.1.1. ErrorMessage

popis:

Premenná ErrorMessage obsahuje po každom volaní metód triedy MessageContainer prípadné chybové hlásenie.

5.3.1.2. konštruktor

vstupné parametre: žiadne

výstupné parametre: žiadne

popis:

Vytvorí sa prázdna štruktúra MessageContainer. Očakáva sa jeho naplnenie metódou Initialize().

5.3.1.3. metóda Initialize

vstupné parametre:

- textový reťazec messageId – guid, RFC4122,
- textový reťazec senderId – URI,
- textový reťazec recipientId – URI,
- textový reťazec messageType,
- textový reťazec messageSubject – nepovinný parameter,
- textový reťazec senderBusinessReference – nepovinný parameter,
- textový reťazec recipientBusinessReference – nepovinný parameter.

výstupné parametre: žiadne

návratová hodnota: žiadna

popis:

Metóda vloží zadané parametre do štruktúry MessageContainer-a.

5.3.1.4. metóda AddXMLObject

vstupné parametre:

- textový reťazec id – guid, RFC4122,
- textový reťazec name,
- textový reťazec description,
- textový reťazec classAttr,
- boolean isSigned,
- textový reťazec mimeType,

Projekt	GOV_ZEP	A3019_002
Dokument	Integračná príručka	
Referencia	GOV_ZEP.201	Verzia 8

- textový reťazec `objectData`.

výstupné parametre: žiadne

návratová hodnota: celé číslo

popis:

Metóda skontroluje, či vstupné údaje tvoria platný XML dokument (well-formed) a ak nie, skončí s chybou. Ak je vstupný dokument platný, tak odstráni prípadnú XML deklaráciu a vloží ho do kolekcie objektov v existujúcej štruktúre MessageContainer-a. Atribút Encoding sa nastaví na hodnotu „XML“. Na výstup vráti chybový kód.

5.3.1.5. metóda AddBase64Object

vstupné parametre:

- textový reťazec `id`,
- textový reťazec `name`,
- textový reťazec `description`,
- textový reťazec `classAttr`,
- boolean `isSigned` – true/false,
- textový reťazec `mimeType`,
- textový reťazec `objectDataBase64`.

výstupné parametre: žiadne

návratová hodnota: celé číslo

popis:

Metóda skontroluje, či je vstupný reťazec vo formáte base64 a ak áno, vloží zadané údaje do kolekcie objektov v existujúcej štruktúre MessageContainer-a. Atribút Encoding sa nastaví na hodnotu „base64“. Na výstup vráti chybový kód.

5.3.1.6. metóda GetMessageContainer

vstupné parametre: žiadne

výstupné parametre: žiadne

návratová hodnota: textový reťazec

popis:

Metóda vráti na výstup štruktúru MessageContainer.

5.3.1.7. metóda Initialize

vstupné parametre:

- textový reťazec `mc` – obsah existujúcej štruktúry MessageContainer.

výstupné parametre: žiadne

Projekt	GOV_ZEP	A3019_002
Dokument	Integračná príručka	
Referencia	GOV_ZEP.201	Verzia 8

návratová hodnota: žiadna

popis:

Metóda načíta vstupnú štruktúru kontajnera MessageContainer. V prípade neúspechu sa chyba zaznačí do internej premennej.

5.3.1.8. metóda IsInitialized

vstupné parametre: žiadne

výstupné parametre: žiadne

návratová hodnota: boolean

popis:

Metóda vráti true, ak bol kontajner správne inicializovaný, teda metóda Initialize skončila korektne. Inak vráti false.

5.3.1.9. metóda GetMessageContainerInfo

vstupné parametre: žiadne

výstupné parametre: žiadne

návratová hodnota: štruktúra MessageContainerInfo

popis:

Metóda vráti údaje z načítaného kontajnera. Štruktúra MessageContainerInfo obsahuje:

- textový reťazec MessageId,
- textový reťazec SenderId,
- textový reťazec RecipientId,
- textový reťazec MessageType,
- textový reťazec MessageSubject – nepovinne,
- textový reťazec SenderBusinessReference – nepovinne,
- textový reťazec RecipientBusinessReference – nepovinne.

5.3.1.10. metóda GetMessageContainerInfo

vstupné parametre: celé číslo type – určuje typ výstupu

výstupné parametre: žiadne

návratová hodnota: textový reťazec

popis:

Preťažená metóda vráti údaje z načítaného kontajnera vo formáte XML, ak type bolo rovné nule, alebo vo formáte JSON, ak type bolo rovné jednej. V ostatných prípadoch (hodnoty parametra type) vráti prázdný string a chybu zapíše do internej premennej.

Projekt	GOV_ZEP	A3019_002
Dokument	Integračná príručka	
Referencia	GOV_ZEP.201	Verzia 8

5.3.1.11. metóda GetObjectCount

vstupné parametre: žiadne

výstupné parametre: žiadne

návratová hodnota: celé číslo

popis:

Metóda vráti počet objektov v načítanej štruktúre MessageContainer.

5.3.1.12. metóda GetObjectInfo

vstupné parametre: celé číslo *i*

výstupné parametre: žiadne

návratová hodnota: štruktúra ObjectInfo

popis:

Metóda vráti údaje i-teho objektu z kontajnera. Štruktúra ObjectInfo obsahuje:

- textový reťazec `Id`,
- textový reťazec `Name`,
- textový reťazec `Description`,
- textový reťazec `ClassAttr`,
- boolean `IsSigned`,
- textový reťazec `MimeType`,
- textový reťazec `Encoding`.

Ak je číslo *i* mimo rozsahu, vráti null a do ErrorMessage zapíše chybu.

5.3.1.13. metóda GetObjectInfo

vstupné parametre:

- celé číslo *i* – číslo objektu,
- celé číslo *type* – určuje typ výstupu.

výstupné parametre: žiadne

návratová hodnota: textový reťazec

popis:

Preťažená metóda vráti údaje z načítaného kontajnera vo formáte XML, ak *type* bolo rovné nule, alebo vo formáte JSON, ak *type* bolo rovné jednej. Pri zápisе vlastnosti `ClassAttr` sa do výstupu (XML aj JSON) zapíše označenie `Class`. Štruktúra MessageContainer je totiž definovaná s atribútom `Class`, interne sa však toto označenie premenovalo na `ClassAttr`, pretože „class“ je vyhradené v jazyku Java.

Ak je číslo *i* mimo rozsahu, vráti null a do ErrorMessage zapíše chybu.

Projekt	GOV_ZEP	A3019_002
Dokument	Integračná príručka	
Referencia	GOV_ZEP.201	Verzia 8

5.3.1.14. metóda GetObjectData

vstupné parametre:

- celé číslo i – číslo objektu.

výstupné parametre: žiadne

návratová hodnota: textový reťazec

popis:

Metóda vráti údaje zo zvoleného objektu.

5.3.1.15. metóda GetVersion

vstupné parametre: žiadne

výstupné parametre: žiadne

návratová hodnota: textový reťazec

popis:

Metóda vráti na výstup názov a verziu komponentu D.Sig XAdES Extender.

Projekt	GOV_ZEP	A3019_002
Dokument	Integračná príručka	
Referencia	GOV_ZEP.201	Verzia 8

6. Scenáre použitia

Pre ilustráciu použitia knižnice D.Sig XAdES Extender boli vytvorené dva scenáre, vytvorenie nového podania a zistenie informácií z existujúceho podania. Metódy .NET knižnice sú volané z testovacej C# winforms aplikácie.

6.1. Scenár 1 – vytvorenie podania

Nasledujúca sekvencia predstavuje postupnosť metód, ktoré je potrebné volať pre vytvorenie podania. Pokiaľ skutočný scenár neuvažuje s niektorým krokom, je možné ho vynechať a pokračovať ďalším.

- vytvorenie globálnej inštancie extendera
 - o v c# “`private Extender oExt = new Extender();`”
 - o v javascripte “`var oExt = new ActiveXObject(<progId>);`”, kde progId je uvedené v integračnej príručke alternatívnych rozhrani,
- vytvorenie prvého zloženého el. podpisu s dvoma jednoduchými el. podpismi
 - o metóda “`oExt.CreateNewDataSignatures(inDataEnvelope, inUri, inID, inDescription, inDataSignaturesVersion);`” pričom inDataEnvelope je výstup z podpisovača DSigner, ktorého použitie je mimo tohto dokumentu.
- vloženie druhého jednoduchého el. podpisu
 - o metóda
“`oExt.AddDataEnvelopeToExistingDataSignatures(inDataSignatures, inDataEnvelope)`” pričom inDataSignatures je zložený el. podpis z predošlého kroku a inDataEnvelope je výstup z podpisovača DSigner, ktorého použitie je mimo tohto dokumentu.
- vytvorenie druhého zloženého el. podpisu s jedným jednoduchým el. podpisom
 - o metóda “`oExt.CreateNewDataSignatures(inDataEnvelope, inUri, inID, inDescription, inDataSignaturesVersion);`” pričom inDataEnvelope je výstup z podpisovača DSigner, ktorého použitie je mimo tohto dokumentu.
 - o Tento krok zabezpečil, že inštancia oExt obsahuje už 2 dokumenty typu zložený el. podpis.
- vytvorenie tretieho dokumentu, ktorý bude neautorizovaný
 - o metóda “`oExt.CreateNewDocumentUnauthorized("myDocUri", "myDocID", "myDocDescription", inObjectData, "objID", "application/xml", "", "http://some.uri/someDocIdentifier");`” kde inObjectData sú dátá nejakého xml dokumentu.

Projekt	GOV_ZEP	A3019_002
Dokument	Integračná príručka	
Referencia	GOV_ZEP.201	Verzia 8

- Momentálne nie je možné vkladať viac objektov do jedného neautorizovaného dokumentu.
- Tento krok zabezpečil, že inštancia oExt obsahuje už 3 dokumenty – dvakrát zložený el. podpis a jeden neautorizovaný dokument.
- pridanie tretieho jednočéhho podpisu do prvého zloženého el. podpisu
 - pomocou metódy GetDocumentCount() zistíme počet dokumentov,
 - pomocou metódy MoveToDocument(0) sa nastavime na požadovaný dokument (s poradovým číslom nula),
 - pomocou GetDocumentType môžeme overiť, že naozaj je to dokument typu zložený el. podpis,
 - pomocou vlastnosti DataSignatures získame zložený elektronický podpis z danej pozície (prvý),
 - zavoláme metódu “oExt.AddDataEnvelopeToExistingDataSignatures(inDataSignatures, inDataEnvelope);” pričom inDataEnvelope je výstup z podpisovača DSigner, ktorého použitie je mimo tohto dokumentu a inDataSignatures je výstup metódy DataSignatures nad nastaveným zloženým elektronickým podpisom.
- vytvorenie podania z dvoch zložených el. podpisov a jedného neautorizovaného dokumentu
 - metóda “oExt.CreateNewRegistration("regUri", "regID", "regDesc", "extIdent", "busIdent");”
 - obsah podania vyčítame pomocou metódy Registration alebo RegistrationBase64.

6.2. Scenár 2 – zistenie informácií z existujúceho podania/zásielky

Pre zistenie informácií z podania je možné použiť nasledovnú sekvenciu. Pokiaľ skutočný scenár neuvažuje s niektorým krokom, je možné ho vynechať a pokračovať ďalším.

- vytvorenie inštancie extendera
 - v c# “`private Extender oExt = new Extender();`”
 - v javascripte “`var oExt = new ActiveXObject('DSig.ExtenderAtl');`”
- zistenie informácií o dokumentoch zo vstupného podania
 - pomocou GetRegistrationInfo(inRegistration) je možné zistiť základné informácie o dokumentoch v podaní
 - zistenie typu dokumentu (zložený el. podpis, alebo dokument bez autorizácie),
 - ak je v podaní aj iný element, tak bude ignorovaný a vo výstupe bude označený ako neznámy typ dokumentu,
 - pre známe typy budú vo výstupe aj dátá dokumentu.

Projekt	GOV_ZEP	A3019_002
Dokument	Integračná príručka	
Referencia	GOV_ZEP.201	Verzia 8

- detail pre každý známy typ dokumentu
 - o ak je typ dokumentu zložený el. podpis, bližšie informácie zistíme pomocou metódy `GetDataSignaturesInfo`,
 - o ak je typ dokument bez autorizácie, tak bližšie informácie zistíme pomocou metódy `GetDocumentUnauthorizedInfo`.
- možnosť overenia el. podpisu v rámci zloženého el. podpisu
 - o pokiaľ je typ dokumentu zložený el. podpis, tak je možné overiť matematickú integritu podpisov v ramci zloženého podpisu pomocou metódy `VerifyDataSignatures`.

Projekt	GOV_ZEP	A3019_002
Dokument	Integračná príručka	
Referencia	GOV_ZEP.201	Verzia 8

7. Návratové kódy aplikácie

V nasledujúcej tabuľke sú uvedené návratové kódy funkcie MoveToDocument.

Návratový kód	Popis
0	Operácia bola vykonaná úspešne.
-2	Index je mimo povoleného rozsahu.

V nasledujúcej tabuľke sú uvedené návratové kódy funkcie CreateNewDataSignatures a AddDataEnvelopeToExistingDataSignatures:

Návratový kód	Popis
0	Operácia bola vykonaná úspešne.
-3	Nekorektný vstup XML Xades.
-4	Duplicítne objectID.
-5	Duplicítne signatureID.
-6	Nekorektné XML dátového objektu.
-7	Chýba atribút ID pre dátový objekt.
-8	Chýba namespace pre dátový objekt.
-9	Nekorektný vstup XML DataSignatures.
-10	Nereferencovaný dátový objekt.
-11	Nekonzistentná verzia podpisu v namespace a SignatureProperties.

V nasledujúcej tabuľke sú uvedené návratové kódy funkcie VerifyDataSignatures:

Návratový kód	Popis
0	Operácia bola vykonaná úspešne.
-12	Nesprávna hodnota odtlačku referencovaného objektu s Id={0}.
-13	Chyba počas overovania hodnoty podpisu. Detail: {0}.

V nasledujúcej tabuľke sú uvedené návratové kódy funkcie CreateNewDocumentUnauthorized:

Projekt	GOV_ZEP	A3019_002
Dokument	Integračná príručka	
Referencia	GOV_ZEP.201	Verzia 8

Návratový kód	Popis
0	Operácia bola vykonaná úspešne.
-99	Neočakávaná chyba.

V nasledujúcej tabuľke sú uvedené návratové kódy funkcie CreateNewRegistration:

Návratový kód	Popis
0	Operácia bola vykonaná úspešne.
-14	Zoznam dokumentov je prázdny.
-99	Neočakávaná chyba.

V nasledujúcej tabuľke sú uvedené návratové kódy funkcií AddXMLObject a AddBase64Object:

Návratový kód	Popis
0	Operácia bola vykonaná úspešne.
-20	Inicializácia bola neúspešná.
-15	Vstupný objekt je prázdny.
-99	Neočakávaná chyba.

Ostatné funkcie .Net API vrátia v prípade chyby prázdny string, resp. hodnotu Null (v závislosti od typu návratovej hodnoty). V ErrorMessage je však možné získať detail chyby.