

Integračná príručka

ASiC Factory .NET, v1.3, alternatívne API

Projekt	GOV_ZEP	A3019_002
Dokument	Integračná príručka	
Referencia	GOV_ZEP.254	Verzia 5

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	ASiC Factory .NET, v1.3, alternatívne API	
Ref. číslo	GOV_ZEP.254	Verzia 5

Vypracoval	Mikuš Michal	Podpis	Dátum 19. 2. 2025
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 <Objednávateľ>:

Za <Dodávateľ>:.

<Meno zodpovednej osoby>

<Meno zodpovednej osoby>

Projekt	GOV_ZEP	A3019_002
Dokument	Integračná príručka	
Referencia	GOV_ZEP.254	Verzia 5

Záznamy o zmenách

Autor	Popis zmien	Dátum	Verzia
M.Mikuš	Zpracovaná 6.verzia špecifikácie; vzniká v1.1 produktu	19.5.2016	1
R. Vittek	Aktualizácia systémových požiadaviek	18.8.2022	2
M.Mikuš	Aktualizácia systémových požiadaviek	18.2.2025	4

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.254	Verzia 5

Obsah

1.	Úvod	5
2.	Použité zdroje	6
3.	Systémové požiadavky	8
4.	Špecifikácia API.....	9
4.1.	NPAPI	9
4.2.	COM API	9
5.	Návratové kódy.....	11

Projekt	GOV_ZEP	A3019_002
Dokument	Integračná príručka	
Referencia	GOV_ZEP.254	Verzia 5

1. Úvod

Tento dokument je určený pre používateľov softvérového komponentu ASiC Factory .NET a vývojárov aplikácií pre vytváranie a spracovanie zaručených elektronických podpisov formátu XAdES_ZEP.

Komponent ASiC Factory .NET je určený na

- vytváranie kontajnera ASiC v súlade s [1] a [2] pre digitálne podpisy typu CAdES [3],
- spracovanie kontajnera a získavanie informácií o jeho štruktúre a o obsiahnutých podpisoch (CAdES aj XAdES),
- spájanie dvoch kontajnerov do jedného (CAdES aj XAdES).

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 4). Systémové požiadavky sú zhrnuté v časti 3.

Dokument popisuje funkcionality alternatívnych integračných rozhraní komponentu ASiC Factory .NET (COM API a NP API) a tvorí prílohu Integračnej príručky aplikácie ASiC Factory .NET. Tieto rozhrania sú odvodené z .Net API komponentu a sú primárne určené na integráciu komponentu v rámci web stránok portálových riešení.

Projekt	GOV_ZEP	A3019_002
Dokument	Integračná príručka	
Referencia	GOV_ZEP.254	Verzia 5

2. Použité zdroje

- [1] ETSI TS 102 918 v1.3.1 (2013-06). Associated Signature Containers (ASiC). Electronic Signatures and Infrastructures (ESI). http://www.etsi.org/deliver/etsi_ts/102900_102999/102918/01.03.01_60/ts_102918v010301p.pdf
- [2] ETSI TS 103 174 v2.1.1 (2013-06). ASiC Baseline Profile. Electronic Signatures and Infrastructures (ESI). Technical Specification. http://www.etsi.org/deliver/etsi_ts/103100_103199/103174/02.01.01_60/ts_103174v020101p.pdf
- [3] ETSI TS 101 733 V2.2.1 (2013-04). Electronic Signatures and Infrastructures (ESI);. CMS Advanced Electronic Signatures (CADES). http://www.etsi.org/deliver/etsi_ts/101700_101799/101733/02.02.01_60/ts_101733v020201p.pdf
- [4] ETSI TS 103 171 V2.1.1 (2012-03). Electronic Signatures and Infrastructures (ESI);. XAdES Baseline Profile http://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf.
- [5] ETSI TS 101 733 V2.2.1 (2013-04). Electronic Signatures and Infrastructures (ESI);. CMS Advanced Electronic Signatures (CADES). http://www.etsi.org/deliver/etsi_ts/101700_101799/101733/02.02.01_60/ts_101733v020201p.pdf
- [6] ETSI TS 103 173 V2.2.1 (2013-04). Electronic Signatures and Infrastructures (ESI);. CADES Baseline Profile. Technical Specification. http://www.etsi.org/deliver/etsi_ts/103100_103199/103173/02.02.01_60/ts_103173v020201p.pdf
- [7] IETF, RFC 5652, Cryptographic Message Syntax (CMS), <http://tools.ietf.org/html/rfc5652>.
- [8] IETF RFC 3161: "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)", <https://www.ietf.org/rfc/rfc3161.txt>
- [9] PKWARE ".ZIP Application Note". <http://www.pkware.com/support/zip-application-note>
- [10] Odporúčania NIST ohľadom hašovacích funkcií. <http://csrc.nist.gov/groups/ST/hash/policy.html>
- [11] Špecifikácia ASiC Factory, DITEC, a.s., 2015

Projekt	GOV_ZEP	A3019_002
Dokument	Integračná příručka	
Referencia	GOV_ZEP.254	Verzia 5

- [12] OASIS: "Open Document Format for Office Applications (OpenDocument) Version 1.2; Part 3: Packages" 29 September 2011. OASIS Standard.

Projekt	GOV_ZEP	A3019_002
Dokument	Integračná príručka	
Referencia	GOV_ZEP.254	Verzia 5

3. Systémové požiadavky

Alternatívne API komponentu ASiC Factory .NET sú realizované ako nadstavbové knižnice (wrappery) nad .Net implementáciou komponentu ASiC Factory .NET a sú primárne určené na integráciu komponentu ASiC Factory .NET v rámci web stránok portálových riešení.

Systémové požiadavky komponentu ASiC Factory .NET a nadstavbových wrapperov pre jednotlivé alternatívne API sú nasledujúce:

- OS – MS Windows 7 SP1, Windows 8.x, Windows 10, Windows 11,
- platforma – .Net framework, verzia 4.6.2 alebo vyššia,
- web prehliadač – MS Internet Explorer, v7.0 alebo vyššia (len 32 bit), Mozilla Firefox, v45 – v51, resp.v59 ESR(len 32 bit, s podporou NP API)¹
- prístup na internet (prípadne správne nastavenia pre proxy).

Pre komponent ASiC Factory nie sú potrebné vyššie hardwarové požiadavky, ako vyžaduje samotný operačný systém, prípadne platforma .Net framework 4.6.2 alebo vyššia.

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

¹ Pokiaľ je komponent integrovaný v rámci web stránok web portálu.

Projekt	GOV_ZEP	A3019_002
Dokument	Integračná príručka	
Referencia	GOV_ZEP.254	Verzia 5

4. Špecifikácia API

Komponent ASiC Factory .NET tvorí sada DLL knižníc, ktoré poskytujú pre klientske aplikácie nasledujúce integračné rozhrania:

- .Net API – pre .Net aplikácie,
- COM API – wrapper nad .Net API pre iné ako .Net aplikácie,
- NP API – wrapper pre volanie služieb komponentu ASiC Factory .NET z prehliadačov s podporou NPAPI rozhrania.

V nasledujúcich kapitolách sú popísané jednotlivé alternatívne COM API a NP API rozhrania aplikácie. Popis samotných metód a vlastností, ktoré jednotlivé API publikujú, je uvedený v rámci integračných príručiek aplikácie ASiC Factory .NET pre .Net API.

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

4.1. NPAPI

ProgId pre ActiveX:

DTC.AsicFactoryFb

MIME type pre NPAPI:

application/x-ditec.zep.asicfactoryfb

Vlastnosti:

std::wstring JoinedAsicB64;

std::wstring ErrorMessage;

Metódy:

```
void Initialize(const std::wstring& appIdentification);
```

```
void Initialize_2(
    const std::wstring& appIdentification,
    const std::wstring& asicB64
);
```

```
void Initialize_3(
    const std::wstring& appIdentification,
    const std::wstring& asicB64,
    const std::wstring& fileName
);
```

```
std::wstring GetErrorMessage();
std::wstring GetInfo(const long type);
```

```
long GetType();
long CheckContainer();
```

```
bool IsInitialized();
long JoinContainers(
```

```
    const std::wstring& asicAB64,
    const std::wstring& asicBB64
);
```

```
std::wstring GetVersion();
```

4.2. COM API

ProgId:

Projekt	GOV_ZEP	A3019_002
Dokument	Integračná príručka	
Referencia	GOV_ZEP.254	Verzia 5

DTC.AsicFactory

VersionIndependentProgID:

DTC.AsicFactory

Vlastnosti:

BSTR ErrorMessage;

Metódy:

```

BSTR GetErrorMessage();
BSTR GetInfo([in] long type);
AsicType GetType_2();
long CheckContainer();
boolean IsInitialized();
long JoinContainers_2(
    [in] BSTR asicAB64,
    [in] BSTR asicBB64,
    [out] BSTR* joinedAsicB64
);
void Initialize([in] BSTR appIdentification);
void Initialize_2(
    [in] BSTR appIdentification,
    [in] BSTR asicB64
);
void Initialize_3(
    [in] BSTR appIdentification,
    [in] BSTR asicB64,
    [in] BSTR fileName
);
BSTR GetVersion();

```

Projekt	GOV_ZEP	A3019_002
Dokument	Integračná príručka	
Referencia	GOV_ZEP.254	Verzia 5

5. Návrátové kódy

V nasledujúcej tabuľke sú zhrnuté chybové kódy alternatívnych API:

Kód	Popis
0	
-100	Nepodarilo sa vytvoriť inštanciu triedy AsicFactory.

Ostatné funkcie alternatívnych API komponentu ASiC Factory .NET vrátia identickú návratovú hodnotu ako v rozhraní .NET, alebo v prípade chyby prázdny string, resp. hodnotu Null (v závislosti od typu návratovej hodnoty).