# Často kladené otázky ku kvalifikovanej službe validácie k štruktúre validačného reportu XadesXml

Verzia 1.5

Aktualizované dňa 09.03.2022

Zoznam zmien:

|  |  |  |  |
| --- | --- | --- | --- |
| Dátum | Verzia | Popis zmeny | Poznámka |
| 28.02.2022 | 1.4 | Bod 1 - Doplnený rozdiel medzi parametrami ForSeal a IsQcLegalPerson pre odlíšenie podpisu a pečate. Doplnené nové body:  9. Informácie o podporovaných formátoch podpisov 10. Informácie o výstupných formátoch validačného reportu  11. Informácie o  kvalifikovanej služby validácie v porovnaní s informatívnym overením podpisov |  |
| 09.03.2022 | 1.5 | Doplnené informácie o parametri ExcludeDocuments pre nezahrnutie podpísaných dokumentov do validačného reportu - v bode 2. Zmena poradia bodov v dokumente. |  |

Obsah

[Často kladené otázky ku kvalifikovanej službe validácie k štruktúre validačného reportu XadesXml 1](#_Toc97753379)

[**1. Aký je rozdiel medzi kvalifikovanou službou validácie a informatívnym overením podpisov?** 2](#_Toc97753380)

[**2. V akom formáte poskytuje kvalifikovaná služba validácie validačný report? Je validačný report zapečatený pečaťou kvalifikovanej služby validácie?** 2](#_Toc97753381)

[**3. Overuje služba aj slovenské formáty podpisov XAdES\_ZEP (.xzep/.zepx)?** 3](#_Toc97753382)

[**4. Ako je možné odlíšiť podpis a pečať?** 3](#_Toc97753383)

[**5. Ako je možné odlíšiť jednotlivé legislatívne typy podpisu?** 3](#_Toc97753384)

[**6. Ako je možné odlíšiť kvalifikovanú časovú pečiatku od nekvalifikovanej?** 4](#_Toc97753385)

[**7. Ako je možné odlíšiť mandátny certifikát?** 4](#_Toc97753386)

[**8. Z ktorého elementu je možné získať údaje o držiteľovi certifikátu?** 4](#_Toc97753387)

[**9. Z ktorého elementu je možné získať údaje o vydavateľovi časovej pečiatky?** 4](#_Toc97753388)

[**10. Aký je význam jednotlivých typov časových pečiatok?** 5](#_Toc97753389)

[**11. Aký je význam jednotlivých stavov a výsledkov validácie?** 5](#_Toc97753390)

[**12. Aké hodnoty môže nadobúdať "ValidationResultReason/Code"?** 6](#_Toc97753391)

**1. Aký je rozdiel medzi kvalifikovanou službou validácie a informatívnym overením podpisov?**

Kvalifikovaná služba validácie podlieha pravidelnému povinnému auditu kvalifikovanej dôveryhodnej služby podľa Nariadenia EP a Rady EÚ č. 910/2014 (eIDAS) orgánom posudzovania zhody a dohľadom orgánu dohľadu. Kvalifikovaná služba musí spĺňať povinné podmienky jej poskytovania.

Informatívne overenie podpisov a pečatí používa obdobné postupy pre overovanie ako kvalifikovaná služba validácie, poskytuje však len informatívne overenie vzhľadom na absenciu kvalifikovaného štatútu služby. Vzhľadom na čiastočne odlišné postupy môže v niektorých okrajových prípadoch poskytovať odlišné výsledky validácie.

Používanie kvalifikovanej služby validácie je vyžadované napríklad pri zaručenej konverzii podľa vyhlášky č. 70/2021 Z. z. pre skontrolovanie bezpečnostných prvkov, ktorými sú kvalifikovaný elektronický podpis alebo kvalifikovaná elektronická pečať.

## **2. V akom formáte poskytuje kvalifikovaná služba validácie validačný report? Je validačný report zapečatený pečaťou kvalifikovanej služby validácie?**

Kvalifikovaná služba validácie NASES poskytuje validačný report v troch základných formátoch:

* XadesXml – vhodný pre ďalšie automatizované strojové spracovanie údajov z validačného reportu. Podľa vstupného parametra ExcludeDocuments vo volaní služby môže obsahovať aj podpísané dokumenty z validovaného súboru. Formát je vytvorený v špecifickej štruktúre a vzhľadom na absenciu vykonávacieho rozhodnutia Komisie EÚ nebol zatiaľ zosúladený s existujúcou ETSI špecifikáciou.
* NbuText – čitateľný textový validačný report vytvorený podľa špecifikácie zverejnenej v Schéme dohľadu orgánu dohľadu - Národného bezpečnostného úradu SR. Formát nie je určený na ďalšie strojové spracovanie údajov z validačného reportu a obsahuje zúžený rozsah údajov oproti XadesXml.
* DisigPdf – čitateľný a vizuálne prehľadný validačný report. Formát nie je určený na ďalšie strojové spracovanie údajov z validačného reportu.

Validačný report obsahuje výsledok validácie a detailné informácie o podpisoch, pečatiach, časových pečiatkach a údajoch pre validáciu. Validačný report umožňuje preukazovať platnosť podpisu alebo pečate.

Validačný report vo všetkých troch formátoch TXT (NbuText), PDF (DisigPdf) a XML (XadesXml) je zapečatený pečaťou kvalifikovanej služby validácie s certifikátom zverejneným v dôveryhodnom zozname SR.

Validačný report vo formáte TXT je zapečatený pečaťou vo formáte ASiC-S CAdES.

Validačný report vo formáte PDF je zapečatený pečaťou vo formáte PAdES.

Validačný report vo formáte XML je zapečatený pečaťou vo formáte XAdES (enveloped).

## **3. Overuje služba aj slovenské formáty podpisov XAdES\_ZEP (.xzep/.zepx)?**

Kvalifikovaná služba validácie je určená pre validáciu formátov podpisov vytvorených podľa Nariadenia Európskeho parlamentu a Rady EÚ č. 910/2014 (XAdES, CAdES, PAdES a ASiC). Služba nie je určená pre validáciu formátov podpisov vytvorených podľa legislatívy účinnej pred 1. júlom 2016 ako je napríklad formát XAdES\_ZEP (.zepx, .xzep).

Pre validáciu podpisov vo formáte XAdES\_ZEP je možné používať iné validačné služby.

## **4. Ako je možné odlíšiť podpis a pečať?**

<!-- Príznak určujúci, či sa jedná o podpisový certifikát pre pečať -->

<ForSeal>

<!-- Príznak určujúci, či sa jedná o podpisový certifikát právnickej osoby -->

<IsQcLegalPerson>

Hodnota poľa `IsLegalPerson` sa nastavuje podľa rozšírenia certifikátu zvaného "Qualified Certificate Statements" (oid `1.3.6.1.5.5.7.1.3`) prípadne podľa ekvivalentných údajov z TSL.

Podpisový certifikát v tomto rozšírení nedeklaruje typ certifikátu pomocou QC statementu `qcs-QcType` (oid 0.4.0.1862.1.6), a preto pri certifikáte pre pečať môže byť nastavené `IsLegalPerson = false`.

Hodnota poľa `ForSeal` sa nastavuje o.i. aj pomocou viacerých "heuristických" metód, ktoré zohľadňujú aj národné špecifiká. Napríklad služba vráti `ForSeal = true` ak je použitá certifikačná politika `1.3.158.36061701.0.0.0.1.2.2`, pri ktorej je v `NoticeText` uvedené:

*> Notice Text=EN: A certificate is issued as a qualified certificate for seal pursuant to the Act No. 215/2002 Coll. and the NSA Decree No. 131/2009 Coll. SK: Kvalifikovaný systémový certifikát podľa zákona č. 215/2002 Z. z. a vyhlášky č. 131/2009 Z. z.*

Ak chce klientsky systém pracovať výlučne s informáciami z QC statementov, tak by mal používať hodnotu poľa `IsLegalPerson`.

Ak chce klientsky systém pracovať aj s "kontextovými" informáciami dostupnými mimo QC statementov, tak môže používať hodnotu poľa `ForSeal`.

## **5. Ako je možné odlíšiť jednotlivé legislatívne typy podpisu?**

Postačujúce podmienky:

* zdokonalený elektronický podpis/pečať založený na kvalifikovanom certifikáte

**(IsAdesBes = true alebo IsAdesEpes = true) a zároveň (IsQes = false a zároveň  IsQc = true)**

* zdokonalený elektronický podpis/pečať

**(IsAdesBes = true alebo IsAdesEpes = true) a zároveň (IsQes = false a zároveň  IsQc = false)**

* kvalifikovaný elektronický podpis/pečať:

**IsQes = true**

## **6. Ako je možné odlíšiť kvalifikovanú časovú pečiatku od nekvalifikovanej?**

Validačná služba považuje za dôveryhodné **len kvalifikované služby** časovej pečiatky.

Čiže ak <TimeStampValidationDetail> obsahuje <ValidationResult> a v ňom <Type>**VALID**</Type>, tak to  znamená, že sa jedná o kvalifikovanú časovú pečiatku. V prípade, že sa tam nenachádza **VALID**, jedná sa o nekvalifikovanú časovú pečiatku alebo kvalifikovanú, ale s problémom.

Príklad s časovou pečiatkou je XML dokumente Hello\_report.xml:



## **7. Ako je možné odlíšiť mandátny certifikát?**

Z ktorého elementu je možné získať nasledovné údaje z podpisového certifikátu?

* číslo mandátu - 1.3.158.36061701.1.1.xyz
* UserNotice - textové informácie o mandáte
* údaje o mandantovi - SERIALNUMBER, OrganizationIdentifier, O

Odpoveď:

Údaje je možné získať z elementu SigningCertificate vo vnorených elementoch ako je Mandate a ParsedSubject.

Samotný certifikát sa nachádza v DataObjectId.

## **8. Z ktorého elementu je možné získať údaje o držiteľovi certifikátu?**

Údaje je možné získať z elementu SigningCertificate vo vnorených elementoch Subject a ParsedSubject.

## **9. Z ktorého elementu je možné získať údaje o vydavateľovi časovej pečiatky?**

Element TimeStamps obsahuje TimeStampValidationDetail a ten obsahuje SigningCertificate.

## **10. Aký je význam jednotlivých typov časových pečiatok?**

SignatureTimeStamp, - **Časová pečiatka v podpise**

ArchiveTimeStamp, - **Archívna časová pečiatka**

EscTimeStamp - **Časová pečiatka úplnej informácie na overenie**

CertCrlTimeStamp - **Časová pečiatka odkazov na certifikáty a CRL**

ContentTimeStamp – **Časová pečiatka obsahu**

## **11. Aký je význam jednotlivých stavov a výsledkov validácie?**

**"ValidationResult/Type"** **- Stav validácie podpisu:**

VALID | INDETERMINATE | PARTIAL | INVALID

* VALID  - **Platný (Úplné overenie)**

Popis: Podpis bolo možné plne overiť a bol vyhodnotený ako platný.

* INDETERMINATE -  **Nerozhodnutý**

Popis: Proces overenia použil všetky dostupné údaje, ale napriek tomu nebolo možné jednoznačne automaticky rozhodnúť o platnosti podpisu. Dôvodov môže byť viacero, napr. že niektoré údaje sú dočasne nedostupné, alebo vypršala platnosť podpisového certifikátu a podpis neobsahuje platnú časovú pečiatku.

* PARTIAL – podstav INDETERMINATE - **Platný (Čiastočné overenie)**

Popis: Podpis bol štrukturálne overený ako platný, no zatiaľ nebolo možné plne overiť platnosť všetkých certifikátov, napr. kvôli neaktuálnym údajom o zrušení certifikátov. Po nejakom krátkom čase (typicky pár hodín) bude možné podpis plne overiť ako Platný alebo Neplatný.

* INVALID - **Neplatný**

Popis: Podpis bol overený a je preukázateľné, že je neplatný. Dôvodov môže byť viacero, napr. že bol zmenený obsah dokumentu, podpis bol vytvorený po zrušení certifikátu podpisovateľa a pod.

**"ValidationResultReason/Result" - Výsledok validácie:**

VALID | INDETERMINATE | PARTIAL | INVALID

* + **Jedná sa o sub-výsledky jednotlivých validácií**, ktoré vo výsledku tvoria ValidationResult/Type
  + VALID | INDETERMINATE | PARTIAL | INVALID –  
    **Popis je identický ako pri "ValidationResult/Type"**

**"OverallValidationResult/Type"** **- Celkový výsledok validácie:**

VALID | INDETERMINATE | PARTIAL | INVALID

* + Štruktúra popisujúca celkový výsledok validácie podpisu  
    **(vrátane platnosti časových pečiatok a archívnych časových pečiatok)**
  + VALID | INDETERMINATE | PARTIAL | INVALID –  
    **Popis je identický ako pri "ValidationResult/Type"**

Aké je namapovanie na číselník pri zaručenej konverzii - "platný"/"neplatný"/"nie je možné zistiť"?

**VALID = platný**

**INDETERMINATE | PARTIAL = nie je možné zistiť**

**INVALID = neplatný**

Ktoré z výsledkov uvádzajú konečný stav a pri ktorých je potrebné overenie zopakovať neskôr?

* **Konečné stavy**
  + VALID
  + INVALID
* **Môže/Nemusí nastať zmena pri stavoch a teda nie sú konečné**
  + INDETERMINATE
  + PARTIAL – pričom element <SignatureValidatesAt> udáva odhadovaný čas, kedy je vhodné zopakovať overenie

## **12. Aké hodnoty môže nadobúdať "ValidationResultReason/Code"?**

###############################################

Bližší popis pre ValidationResultReason / Code

###############################################

100 = ReasonCode.INVALID\_SIGNATURE - Low level podpis je neplatný.

101 = ReasonCode.INVALID\_DOCUMENT\_DIGEST - Integrita dokumentu je narušená.

102 = ReasonCode.INVALID\_ALGORITHM - Algoritmus '{0}' nie je podporovaný alebo je v danom kontexte zakázaný.

103 = ReasonCode.MISSING\_ATTRIBUTE - Požadovaný atribút '{0}' chýba.

104 = ReasonCode.UNSUPPORTED\_ATTRIBUTE - Atribút '{0}' nie je podporovaný alebo je v danom kontexte zakázaný.

106 = ReasonCode.MISSING\_CERTIFICATES - Podpis neobsahuje požadované certifikáty.

107 = ReasonCode.MISSING\_CERTIFICATES\_REFERENCES - Podpis neobsahuje požadované referencie na certifikáty.

108 = ReasonCode.NOT\_ALLOWED\_DATA\_ATTACHMENT - Podpis externých údajov nie je podporovaný alebo je v danom kontexte zakázaný.

109 = ReasonCode.SIGNATURE\_POLICY\_EXPIRED - Podpisová politika je použitá mimo dobu svojej platnosti.

110 = ReasonCode.SIGNATURE\_POLICY\_NOT\_FOUND - Podpisová politika '{0}' nebola nájdená.

111 = ReasonCode.INVALID\_PROPERTY - Podpis obsahuje premennú '{0}' s nesprávnou hodnotou '{2}'. Očakávaná hodnota je '{1}'.

112 = ReasonCode.NOT\_RECOGNIZED\_COMMITMENT\_TYPE - Podpis obsahuje záväzok, ktorý nie je povolený podpisovou politikou: {0}

113 - MISSING\_SCHEMA\_OR\_TRANSFORMATION = V podpise uvedená schéma alebo transformácia nie je k dispozícii. Identifikátor: '{0}'. Popis: '{1}'.

114 - REFERENCED\_SIGNATURE\_POLICY\_IGNORED = V podpise referencovaná podpisová politika '{0}' bola v procese overenia ignorovaná.

115 - REFERENCE\_COULD\_NOT\_BE\_PROCESSED = Referencia '{0}' nemohla byť spracovaná.

116 - REFERENCED\_FILE\_NOT\_FOUND = Referencovaný súbor '{0}' nebol v podpisovom kontajneri nájdený.

203 = ReasonCode.CERTPATH\_NOT\_VALID - Certifikačná cesta nie je platná.

300 = ReasonCode.CERTPATHCERT\_VIOLATED\_BASIC\_CONSTRAINT\_MAX\_PATH\_LENGTH - Certifikačná cesta je príliš dlhá.

301 = ReasonCode.CERTPATHCERT\_VIOLATED\_BASIC\_CONSTRAINT\_CA\_CERT - Certifikát nie je certifikátom certifikačnej autority.

302 = ReasonCode.CERTPATHCERT\_VIOLATED\_POLICY\_CONSTRAINT - Certifikát neobsahuje vyžadované certifikačné politiky.

303 = ReasonCode.CERTPATHCERT\_VIOLATED\_CRITICAL\_EXTENSION\_CONSTRAINT - Certifikát obsahuje nepodporované rozšírenie '{0}' označené ako kritické.

304 = ReasonCode.CERTPATHCERT\_VIOLATED\_ISSUER\_SUBJECT\_CONSTRAINT - Názov vydavateľa uvedený v tomto certifikáte sa nezhoduje s názvom subjektu v certifikáte vydavateľa.

305 = ReasonCode.CERTPATHCERT\_VIOLATED\_NAME\_CONSTRAINT - Subjekt certikátu porušuje obmedzenia definované pre jeho obsah.

306 = ReasonCode.CERTPATHCERT\_VIOLATED\_SKI\_AKI\_CONSTRAINT - Rozšírenie "Authority Key Identifier" uvedené v tomto certifikáte sa nezhoduje s rozšírením "Subject Key Identifier" z certifikátu vydavateľa.

307 = ReasonCode.CERTPATHCERT\_EXPIRED\_CERTIFICATE - Certifikát exspiroval.

308 = ReasonCode.CERTPATHCERT\_BAD\_KEY\_USAGE - Certifikát obsahuje nesprávnu hodnotu rozšírenia "Key Usage".

309 = ReasonCode.CERTPATHCERT\_NOT\_TRUSTED - Certifikát nie je dôveryhodný.

310 = ReasonCode.CERTPATHCERT\_INVALID\_REFERENCE - V podpise uvedená referencia na podpisový certifikát nie je platná.

400 = ReasonCode.REVOCATION\_REVOKED - Certifikát je zrušený.

401 = ReasonCode.REVOCATION\_NO\_DATA - Vhodné revokačné údaje nie sú k dispozícii.

403 = ReasonCode.REVOCATION\_OLD\_DATA - Dostupné revokačné údaje nie sú dostatočne aktuálne. Je potrebné počkať na novšie revokačné údaje.

500 = ReasonCode.USED\_ARDACO\_XADES\_HACK - Pri spracovaní atribútu "SigningCertificate" bol použitý mód kompatibility s aplikáciou Ardaco QSign.

501 = ReasonCode.USED\_XADES\_HACK - Pri overení podpisu bol použitý mód kompatibility s aplikáciou Ardaco QSign.

502 = USED\_DISIG\_LEGACY\_NBU\_VALIDATION\_HACK\_FOR\_CERT - Pre overenie platnosti tohto certifikátu bol použitý mód kompatibility so starou NBU validáciou s CautionPeriod=0.

503 = USED\_DISIG\_LEGACY\_NBU\_VALIDATION\_HACK\_FOR\_SIGNATURE - Pre overenie tohto podpisu bol použitý mód kompatibility starou NBU validáciu s CautionPeriod=0.

504 = SKIPPED\_QCSSCD\_CHECK\_IN\_SLOVAK\_SYSTEM\_CERTS - Pri určovaní typu podpisu nebol zohľadnený QcSSCD statement.

505 = USED\_IGNORE\_CAUTION\_PERIOD\_IN\_SIGNATURE\_POLICY\_HACK - Hodnota CautionPeriod definovaná v podpisovej politike bola ignorovaná.

600 = ReasonCode.NOZEP\_NO\_EPES - Podpis nie je ZEP, pretože neobsahuje referenciu na podpisovú politiku vydanú NBÚ SR.

601 = ReasonCode.NOZEP\_NO\_NBU\_TSL - Podpis nie je ZEP, pretože nebol overovaný s Dôveryhodným Zoznamom vydaným NBÚ SR.

700 = ReasonCode.COMMITMENT\_TYPE - V podpise je uvedený záväzok: {0}

701 = ReasonCode.SIGNER\_LOCATION - V podpise je uvedené miesto vzniku podpisu: {0}

900 = ReasonCode.OTHER - Iný bližšie nešpecifikovaný resp. neznámy dôvod.

10109 = ReasonCode.NOT\_VALID\_TIMESTAMP - Časová pečiatka nebola overená ako plne platná.

10110 = ReasonCode.NOT\_VALID\_CERTIFICATE - Podpisový certifikát nebol overený ako plne platný.