DIGITÁLNÍ
A INFORMAČNÍ
AGENTURA_

DIAPX001VHQM

DIAPX001VHQM

prvotní identifikátor

ČÍSLO JEDNACÍ

DIA- 498-1/EG-2024

Dokument upřesňující problematiku zápisu údajů o čísle a typu dokladu do kvalifikovaného certifikátu pro elektronický podpis.

Verze	Popis
1.0	První verze dokumentu.

DIGITÁLNÍ
A INFORMAČNÍ
AGENTURA_

Obsah

DIGITÁLNÍ
A INFORMAČNÍ
AGENTURA_

1. Manažerské shrnutí

Dokument obsahuje informace a doporučení pro QTSP v případě, kdy se rozhodne podporovat možnost uvádět ve vydaném QC údaje o čísle a typu dokladu. Pokud ve vydaném QC budou tyto údaje uvedeny, pak lze za splnění podmínek uvedených v § 6 odst. 2 zákona č. 12/2020 Sb. přisoudit uznávanému elektronickému podpisu založeného na tomto QC, právní účinky úředně ověřeného.

Pro zajištění využívání údajů o čísle a typu dokladu ve vydaném QC v praxi je klíčové, aby pokud možno, údaje o čísle a typu dokladu QTSP uváděli ve vydaných QC jednotným způsobem. Z tohoto pohledu je zásadní zejména kapitola týkající se způsobu zápisu údajů o čísle a typu dokladu ve vydaném QC.

2. Zkratky

Zkratka	Význam
QC	Kvalifikovaný certifikát pro elektronický podpis
Nařízení eIDAS	Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.
QTSP	Kvalifikovaný poskytovatel služeb vytvářejících důvěru.
CIS	Cizinecký informační systém
DIA	Digitální a informační agentura
MRZ	Machine Readable Zone, strojově čitelné údaje
Zákon č. 297/2016 Sb.	Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, v platném znění.
Zákon č. 12/2020 Sb.	Zákon č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů, v platném znění.
Uznávaný elektronický podpis	zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis nebo kvalifikovaný elektronický podpis

ETSI EN 319 412-1	ETSI EN 319 412-1 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
ROB	Registr obyvatel

3. Celkový kontext

Zákon č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů, zavedl v rámci § 6 odst. 2 právo na nahrazení úředně ověřeného podpisu s využitím uznávaného el. podpisu. Základním předpokladem je, že požadavek na úřední ověření podpisu je stanoven právním předpisem. Splnění požadavku na úřední ověření podpisu je realizováno pomocí uznávaného elektronického podpisu, pokud lze s využitím údajů základního registru obyvatel ověřit, že kvalifikovaný certifikát pro elektronický podpis, na jehož základě podepisující vytvořil uznávaný elektronický podpis na dokumentu, patří jemu (tedy podepisujícímu).

Právo na nahrazení úředně ověřeného podpisu nebo uznávaného elektronického podpisu bylo doposud realizováno prostřednictvím zápisu údajů o QC do ROB – v rámci Portálu občana je implementována možnost pro identifikovaného a autentizovaného uživatele nahrát údaje o QC vydaném pro jeho osobu do ROB. Pro využití této možnosti je potřeba po přihlášení v úvodním menu kliknout na „Více“, otevřít sekci „Profil“ a následně odkaz „Certifikáty“. Uživatel pouze nahraje veřejnou část svého certifikátu a následně se údaje o sériovém číslu, vydavateli a platnosti QC nahrají do ROB k příslušné fyzické osobě. Orgány veřejné moci mají následně možnost tyto údaje z registru obyvatel využít tak, aby mohly ztotožnit podepisující osobu vůči záznamu v ROB v rámci příslušné agendy.

Výkladem ustanovení § 6 odst. 2 zákona č. 12/2020 Sb. lze také dojít k dalšímu řešení, které spočívá v tom, že pro dosažení právního účinku úředně ověřeného podpisu dle § 6 odst. 2 zákona č. 12/2020 Sb., není nezbytně nutné, aby údaje o kvalifikovaném certifikátu pro el. podpis musely být evidovány v ROB, ale naopak pomocí údajů o podepisující osobě uvedených v QC, nalézt a ztotožnit tuto podepisující osobu (na straně ověřovatele uznávaného el. podpisu) v ROB a to s využitím údajů o čísle a typu dokladu.

DIA zveřejnila informace o právu na nahrazení úředně ověřeného podpisu dle § 6 odst. 2 zákona č. 12/2020 Sb. na následující webové stránce: https://www.dia.gov.cz/egovernment/eidas-sluzby-vytvarejici-duveru-a-elektronicka-identifikace/informace-pro-uzivatele/pravo-na-nahrazeni-uredne-overeneho-podpisu-dle-%c2%a7-6-odst-2-zakona-c-12-2020-sb/. Tato informační stránka byla aktualizována o informace, že dosažení právního účinku úředně

ověřeného podpisu dle § 6 odst. 2 zákona č. 12/2020 Sb., je možné realizovat rovněž s využitím údajů o čísle a typu dokladu podepisující osoby uvedenými v QC, pomocí nichž by bylo možné nalézt a jednoznačně ztotožnit tuto podepisující osobu (na straně ověřovatele uznávaného el. podpisu) v ROB. Je vhodné dále poznamenat, že v ROB jsou uváděny pouze údaje o dokladech, které byly vydány Českou republikou, u cizinců tak v ROB jsou uvedeny pouze doklady, které mu jsou vydány v rámci pobytu na území České republiky.

4. Ověření údaje o čísle a typu dokladu podepisující osoby

QTSP při vydání prvotního QC kontroluje osobní údaje budoucí podepisující osoby v rámci procesu kontroly totožnosti osoby (ať už prezenční či distanční), QTSP má tak k dispozici údaje o čísle a typu dokladu podepisující osoby při vydání prvotního QC.

V případě vydání následného QC uživatel potvrzuje, že údaje uvedené ve QC jsou nadále aktuální. QTSP by měl nicméně i tak ověřit, že údaje o čísle a typu dokladu jsou nadále platné, např. prostřednictvím ověřovacího portálu NIA, viz níže. Pokud podepisující osoba indikuje, že se změnily její údaje o čísle a typu dokladu, pak musí dojít k ověření nových údajů o čísle a typu dokladu. Tj. stávající podepisující osoba by podstoupila stejný proces jako při vydání prvotního QC nebo by QTSP musel před vydáním následného certifikátu ověřit, že nové číslo a typ dokladu se vztahují stále ke stejné fyzické osobě. Této kontroly může být dosaženo s využitím údajů vedených v základních registrech a dalších evidencích a to jak „přímým“ přístupem QTSP dle oprávnění uvedeném v § 4a zákona č. 297/2016 Sb. nebo s využitím tzv. ověřovacího portálu NIA (https://info.identitaobcana.cz/OverovaciPortal/) dle § 12a zákona č. 12/2020 Sb.

5. Aktuálnost údajů o čísle a typu dokladu podepisující osoby

Aktuálnost údaje o čísle a typu dokladu QTSP ověřuje při vydání QC, ale v průběhu platnosti QC nemusí QTSP proaktivně zjišťovat aktuálnost údaje, pokud nevyužívá svého oprávnění dle § 4a zákona č. 297/2016 Sb. – v takovém případě má QTSP možnost přihlásit se k notifikacím a zjistit tak možnou změnu v čísle a typu dokladu uvedeného ve vydaném QC. V případě QC, kde budou uvedeny informace o čísle a typu dokladu, se nadále bude uplatňovat povinnost podepisující osoby zakotvená v certifikační politice informovat QTSP o změně údajů uvedených ve vydaném QC. Pokud je QTSP informován ze strany podepisující osoby o skutečnosti, že se změnily údaje o čísle a typu dokladu

uvedené v QC, pak vydaný QC zneplatní z důvodu neaktuálnosti údajů uvedených ve vydaném QC. Podobně rovněž v případě, pokud se QTSP dozví hodnověrným způsobem o tom, že se údaje o čísle a typu podepisující osoby změnily, certifikát zneplatní.

V případě, kdy na straně spoléhající se strany bude zjištěno, že číslo a typ dokladu neodpovídají údajům v ROB, tak takovému uznávanému el. podpisu spoléhající se strana nepřisoudí právní účinky úředně ověřeného podpisu, tj. bude se jednat „jen o standardní" uznávaný el. podpis. Pozn.: tento stav lze zhojit nahráním údajů o QC do ROBu popisovaným v bodu 3.

6. Informování podepisující osoby

QTSP vydávající se QC se řídí nařízením eIDAS, zákonem č. 297/2016 Sb. a dalšími právními předpisy. Přesné podmínky, za kterých QTSP vydávají QC se řídí příslušnou certifikační politikou pro vydávání QC, kde podepisující osoba může nalézt přesné podmínky pro vydání QC včetně povinností, které plynou pro ni samotnou.

Jestliže údaje o čísle a typu dokladu budou uvedeny ve vydaném QC, vždy se tak musí dít se souhlasem samotné budoucí podepisující osoby. Tato osoba musí být seznámena s tím, jaké skutečnosti pro ni mohou plynout z faktu, že údaje o čísle a typu dokladu budou uvedeny ve vydaném QC, tj. že elektronickému podpisu založenému na QC, jenž obsahuje údaje o čísle a typu dokladu, mohou být přisouzeny právní účinky úředně ověřeného podpisu (je možné odkázat na webovou stránku https://www.dia.gov.cz/egovernment/eidas-sluzby-vytvarejici-duveru-a-elektronicka-identifikace/informace-pro-uzivatele/pravo-na-nahrazeni-uredne-overeneho-podpisu-dle-%c2%a7-6-odst-2-zakona-c-12-2020-sb/). Je tak ještě více důležité, aby podepisující osoba dbala důsledné ochrany proti zneužití soukromého klíče příslušného k veřejnému klíči uvedenému v QC.

Pokud QTSP zveřejňuje vydané QC, tak **v případě, kdy ve vydaném QC budou uvedeny informace o čísle a typu dokladu, podepisující osoba by měla učinit aktivní krok k tomu, aby případně její certifikát byl zveřejněn v rámci veřejné databáze vydaných QC – tj. v průběhu žádosti o vydání certifikátu by měla být volba zveřejnění vydaného QC ve výchozím stavu „NE"** a až v případě, že podepisující osoba učiní aktivní krok (tj. zvolí volbu zveřejnění vydaného QC) by vydaný QC byl následně zveřejněn v rámci veřejné databáze vydaných QC daného QTSP.

7. Způsob zápisu údajů o čísle a typu dokladu do QC

V případě, že QTSP se rozhodne podporovat možnost uvádění informací o čísle a typu dokladu do vydaného QC, pak by QTSP měl uvádět tyto informace v atributu „serialNumber" v poli Předmětu certifikátu v souladu s kap. 5.1.3. ETSI EN 319 412-1. Tento standard se dále zmiňuje o sémantickém identifikátoru „id-etsi-qcs-SemanticsId-Natural", a v případě, kdy je tento sémantický identifikátor uveden ve vydaném QC, pak musí být údaje uvedené v jakémkoliv atributu serialNumber v souladu s formátem popsaným v kap. 5.1.3. ETSI EN 319 412-1.

Aktuálně QTSP využívají atribut „serialNumber" zejména pro uvádění interního identifikátoru umožňující jednoznačnou identifikace podepisující osoby v rámci databáze QTSP. V případě, že se QTSP rozhodne podporovat možnost uvádění informací o čísle a typu dokladu v QC, pak tyto informace může uvést v další instanci tohoto atributu. V tom případě by ale existovalo více instancí atributu „serialNumber" ve vydaném QC a není možné dle standardu v certifikátu uvádět sémantický identifikátor „id-etsi-qcs-SemanticsId-Natural", jelikož struktura „serialNumber" s uvedením interního identifikátoru by nebyla v souladu s kap. 5.1.3. ETSI EN 319 412-1. Nicméně i tak je vhodné se držet způsobu, jakým tento standard předpokládá zápis údaje o čísle a typu dokladu v atributu „serialNumber", až na to, že v QC nebude uveden sémantický identifikátor „id-etsi-qcs-SemanticsId-Natural".

Struktura zápisu údajů o čísle a typu dokladu v atributu „serialNumber" by měla být dle kap. 5.1.3. ETSI EN 319 412-1 následující:

- jestliže by v QC byla uvedena informace o čísle občanského průkazu, pak struktura záznamu by měla odpovídat formátu: "IDCCZ-123456789".
- jestliže by v QC byla uvedena informace o čísle pasu, pak struktura záznamu by měla odpovídat formátu: "PASCZ-12345678".
- Pro ostatní typy dokladů standard neuvádí konkrétní identifikátory, nicméně připouští možnost používat vlastní dvouznakové identifikátory následované dvojtečkou s identifikací země, pomlčkou a vlastní hodnotou – například „EI:CZ-200007292386". Identifikátor, který se má použít pro konkrétní typ dokladu uvádí tabulka níže a je dán kódem typu dokladu, pod kterým je tento kód veden v ROB, případně kódem, který je definován ve standardu ETSI EN 319 412-1. Například číslo vízového štítku by se mělo uvádět ve tvaru: „VS:CZ-123456789".
- Čísla některých identifikačních dokladů nemusí obsahovat jen číslice.

Převodní tabulka kódů typů dokladů v ROB na kódy uváděné v certifikátu:

Kód typu dokladu v ROB	**Kód uváděný v certifikátu**	**Formát uváděný v certifikátu (délka znaků čísla dokladu může být různá pro ten který typ dokladu)**	**Název typu dokladu**
ID	IDC	IDCCZ-xxxxxxx	občanský průkaz
OP	IDC	IDCCZ-xxxxxxx	občanský průkaz bez MRZ
P	PAS	PASCZ-xxxxxxx	cestovní pas
IR	IR	IR:CZ-xxxxxxx	Povolení k pobytu/Pobytová karta/Karta trvalého pobytu s biometrickými údaji (forma: plastiková karta s čipem)
VS	VS	VS:CZ-xxxxxxx	vízový štítek (forma: nálepka do pasu)
PS	PS	PS:CZ-xxxxxxx	pobytový štítek (forma: nálepka do pasu)
CA	CA	CA:CZ-xxxxxxx	cestovní průkaz
IX	IX	IX:CZ-xxxxxxx	Forma: knížečka (označení CIS: PB - povolení k pobytu, PE - průkaz o povolení k trvalému pobytu obč. EU, PO - průkaz o povolení k trv. pobytu - vazba EU, PP - průkaz o povolení k pobytu, PR - průkaz o pobytu rod. př. obč. EU - přech. pobyt)
IE	IE	IE:CZ-xxxxxxx	Forma: tiskopis (označení CIS: PM - potvrzení o přechodném pobytu na území, OR - Osvědčení o registraci občana EU k přechodnému pobytu)