MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Upřesnění ke kap. 2.3. a kap. 3 dokumentu DKP verze 4

- ***Ověření totožnosti žadatelů o vydání QC pomocí prostředků pro elektronickou identifikaci v souladu s čl. 24 odst. 1 písm. d) nařízení eIDAS.***

Verze	Autor	Popis
0.1	FB	První návrh v závislosti na připomínkách QTSP a CAB.
0.2	FB	Aktualizace na základě došlých připomínek.
0.3	FB	Aktualizace dokumentu na základě jednání dne 16.3.2022
0.9	FB	Před-finální verze.
1.0	FB	Ke zveřejnění (MV- 61410-9/EG-2022).

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Obsah

1. Manažerské shrnutí:

Účelem dokumentu je upřesnit kap. 2.3 a kap. 3 dokumentu DKP verze 4, pokud jde o kritéria, která subjekt posuzování shody ověří při tvorbě zprávy o posouzení shody v případě, kdy k ověření totožnosti žadatelů o vydání QC poskytovatel plánuje použít identifikační metodu v souladu s čl. 24 odst. 1 písm. d) nařízení eIDAS a kdy je použit prostředek pro elektronickou identifikaci, který nesplňuje požadavky čl. 24 odst. 1 písm. b) nařízení eIDAS (tj. nejedná se o prostředek se značnou či vysokou úrovní záruky, který je vydáván v rámci oznámeného systému el. identifikace a u něhož byla před vydáním QC ověřena totožnost za fyzické přítomnosti). Účelem zprávy o posouzení shody je potvrdit, že použitá identifikační metoda poskytuje záruku spolehlivosti rovnocennou fyzické přítomnosti.

Tento upřesňující dokument pokrývá aktuálně problematiku ověřování totožnosti pomocí prostředků pro el. identifikaci používaných mimo rámec kvalifikovaného systému el. identifikace (tj. **BankID**) a používání prostředků pro el. identifikaci v rámci kvalifikovaného systému el. identifikace s úrovní záruky **vysoká**. Otázka použití prostředků pro el. identifikaci v rámci kvalifikovaného systému el. identifikace s úrovní záruky značná pro účely ověření totožnosti při vydání QC, může být řešena aktualizací tohoto dokumentu (zejména s ohledem na skutečnost, že prostředky se značnou úrovní záruky mohou být vydány díky použití datových schránek (např. mojeID s úrovní záruky značná, NIA ID a Mobilní klíč eGovernmentu) a tomu, že aktuálně není implementována možnost, aby service provider (QTSP) mohl obdržet informaci o tom, zda byla při vydání prostředku pro el. identifikaci ověřena fyzicky totožnost osoby.

2. Zkratky:

Zkratka	Význam
DKP	Dokument konkretizující požadavky na kvalifikované poskytovatele služeb vytvářejících důvěru a jimi poskytované kvalifikované služby vytvářející důvěru, jehož aktuální verze je zveřejněna na webu: https://www.mvcr.cz/sluzba/docDetail.aspx?docid=22021695&docType=ART
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.
QC	Kvalifikovaný certifikát ve smyslu nařízení eIDAS (kvalifikovaný certifikát pro el. podpis/el.pečeť/ pro autentizaci internetových stránek).
CAB	Subjekt posuzování shody.
CAR	Zpráva o posouzení shody.
NIA	Národní bod pro identifikaci a autentizaci dle zákona č. 250/2017 Sb.
BankID	Agregátor služby elektronické identifikace, přes kterého banky nabízejí služby bankovní identity pro subjekty spadající mimo kategorii státních orgánů a orgánů územně samosprávných celků.
SeP	Service provider, poskytovatel online služeb. V závislosti na kontextu se jedná buď o kvalifikovaného poskytovatele ve smyslu zákona č. 250/2017 Sb., který je připojen na NIA, případně poskytovatel online služeb připojený k BankID.
IdP	Podle kontextu buď kvalifikovaný správce v rámci NIA nebo banka zapojená v rámci BankID
BSI	Bezvýznamový směrový identifikátor
AISEO	Agendový informační systém evidence obyvatel
AISC	Agendový informační systém cizinců
AISEOP	Agendový informační systém evidence občanských průkazů
AISECD	Agendový informační systém evidence cestovních dokladů
RUIÁN	Registr územní identifikace, adres a nemovitostí

3. Legislativní rámec – ověření totožnosti žadatelů o vydání QC:

Nařízení eIDAS definuje ve čl. 24 odst. 1 možné způsoby, jak může QTSP ověřit totožnost osoby a případně zvláštní znaky fyzické nebo právnické osoby, jíž je kvalifikovaný certifikát vydáván:

Článek 24 - Požadavky na kvalifikované poskytovatele služeb vytvářejících důvěru

1. Při vydávání kvalifikovaného certifikátu pro službu vytvářející důvěru ověří kvalifikovaný poskytovatel služeb vytvářejících důvěru pomocí vhodných prostředků a v souladu s vnitrostátním právem totožnost a případně zvláštní znaky fyzické nebo právnické osoby, jíž je kvalifikovaný certifikát vydáván.

Kvalifikovaný poskytovatel služeb vytvářejících důvěru ověří informace uvedené v prvním pododstavci přímo nebo tím, že se v souladu s vnitrostátním právem spolehne na třetí osobu:

a) na základě fyzické přítomnosti fyzické osoby nebo oprávněného zástupce právnické osoby; nebo
b) na dálku s využitím prostředku pro elektronickou identifikaci, u něhož byla před vydáním kvalifikovaného certifikátu zajištěna fyzická přítomnost fyzické osoby nebo oprávněného zástupce právnické osoby a jenž splňuje požadavky stanovené v článku 8, pokud jde o značnou nebo vysokou úroveň záruky; nebo
c) pomocí certifikátu kvalifikovaného elektronického podpisu nebo kvalifikované elektronické pečeti, vydaného v souladu s písmenem a) nebo b); nebo
d) pomocí jiných identifikačních metod uznávaných na vnitrostátní úrovni, které poskytují záruku spolehlivosti rovnocennou fyzické přítomnosti. Tuto rovnocennou záruku musí potvrdit subjekt posuzování shody.

Možnost využít prostředky pro elektronickou identifikaci pro účely ověření totožnosti žadatele o vydání QC lze zařadit pod písm. b) a písm. d) výše uvedeného čl. 24 odst. 1 nařízení eIDAS.

Varianta pod písm. b) se týká situace, kdy je možné použít pro ověření totožnosti prostředek pro el. identifikaci vydaný v rámci oznámeného systému el. identifikace s úrovní záruky značná a vysoká a zároveň u něhož byla před vydáním kvalifikovaného certifikátu zajištěna fyzická přítomnost fyzické osoby nebo oprávněného zástupce právnické osoby. Zde nařízení eIDAS nepožaduje doložení zprávy o posouzení shody.

Variantu pod písm. d) lze pak aplikovat na případy, kdy je k ověření totožnosti použit prostředek pro el. identifikaci, který neodpovídá požadavkům podle písm. b) například z toho důvodu, že prostředek pro el. identifikaci není vydáván v rámci oznámeného systému el. identifikace. Tzn. použití prostředku pro el. identifikaci v rámci kvalifikovaného systému el. identifikace v souladu se zákonem č. 250/2017 Sb. nebo použití prostředku pro elektronickou identifikaci mimo rámec kvalifikovaného systému el. identifikace dle § 38ac zákona č. 21/1992 Sb., o bankách, spadá zejména pod toto písmeno.

Předpokladem pro možnost aplikovat ověření totožnosti dle písm. d) je, že tato metoda musí být uznávána na vnitrostátní úrovni a zároveň musí identifikační metoda poskytovat záruku spolehlivosti

rovnocennou fyzické přítomnosti a tuto rovnocennou záruku musí potvrdit subjekt posuzování shody (CAB). Tento materiál se bude dále věnovat použití prostředků pro el. identifikaci v režimu dle čl. 24 odst. 1 písm. d) nařízení eIDAS, kde je stanoven požadavek na potvrzení ze strany subjektu posuzování shody o tom, že identifikační metoda poskytuje záruku spolehlivosti rovnocennou fyzické přítomnosti. S ohledem na dosavadní zvyklosti, toto potvrzení by mělo mít formu zprávy o posouzení shody (CAR).

4. Ověření totožnosti

V případě, kdy QTSP ověřuje totožnost žadatelů o vydání QC pomocí prostředků pro el. identifikaci, **musí být v certifikační politice, podle které se QC vydává, jednoznačně stanoveno, pomocí jakých prostředků pro el. identifikaci je možné prokázat totožnost** – musí být uvedena požadovaná úroveň záruky prostředku pro el. identifikaci a seznam či odkaz na seznam prostředků pro el. identifikaci, které lze použít v případě konkrétního QTSP.

Na úrovni NIA je možné manuálně pro každého SePa definovat kvalifikovaného správce, pomocí kterého je povoleno se ke službě přihlásit v případě, kdy lze nalézt odůvodnění pro toto nastavení v právním předpise. Na úrovni BankID toto selektivní nastavení IdP je možné také, nicméně z principu nesmí docházet k diskriminaci žádného IdP zapojeného v rámci BankID a tak eventualita omezení konkrétního IdP v rámci BankID, musí být rovněž odůvodněná.

Jak uvedeno v kap. 1**, současný dokument řeší možnost použití prostředku pro el. identifikaci používaný v rámci kvalifikovaného systému el. identifikace (tj. prostřednictvím NIA) s úrovní záruky vysoká, nebo prostředek pro el. identifikaci sice vydaný v rámci kvalifikovaného systému el. identifikace, ale používaný mimo rámec kvalifikovaného systému el. identifikace (tj. BankID) s úrovní záruky značná.**

Prostředky pro elektronickou identifikaci s úrovní záruky značná a vysoká, mohou být vydány buď na základě osobní přítomnosti, nebo na základě využití jiných prostředků pro elektronickou identifikaci (tj. řetězení – jeden prostředek pro el. identifikaci je vydán na základě jiného prostředku pro el. identifikaci), případně na základě dalších definovaných postupů (zejména s využitím datových schránek – platí pro úroveň záruky značná). Informaci o tom, zda došlo k vydání prostředku za fyzické přítomnosti identifikovaného, není v tuto chvíli součástí předávaných dat v rámci NIA. V rámci BankID platí, že pro vydání prvotního prostředku BankID musela banka fyzickou osobu ztotožnit na základě fyzické přítomnosti. V rámci BankID lze získat informaci, kdo provedl prvotní fyzické ztotožnění osoby, v případě zřetězení prostředků BankID je součástí předávaných dat jednak informace, kdo ručí za identitu osoby (tj. konkrétní banka, která vydala zřetězený prostředek pro el. identifikaci), tak i informaci, jaká banka provedla prvotní fyzické ověření totožnosti dané osoby.

S ohledem na závažnost právního jednání učiněného na základě elektronického podpisu založeného na vydaném kvalifikovaném certifikátu pro el. podpis a **s přihlédnutím k tomu, že za určitých okolností může mít uznávaný el. podpis právní účinek úředně ověřeného el. podpisu, je nutné**, aby totožnost fyzické osoby byla dostatečně prokázána. Při použití prostředku pro el. identifikaci **se značnou úrovní** záruky (tj. pro účely současné verze dokumentu se má na mysli BankID) musí QTSP zajistit snížení rizika, že prostředek pro el. identifikaci byl použit (zneužit) jinou osobou. V případě použití prostředku pro el. identifikaci s vysokou úrovní záruky není nezbytně nutné bezpečnostní pojistky aplikovat, nicméně samozřejmě QTSP se může na dobrovolné úrovni rozhodnout bezpečnostní pojistky také aplikovat (ani sebebezpečnější prostředek el. identifikace nemůže zcela zabránit situacím zneužití prostředku).

Příklady těchto "bezpečnostních pojistek“ (výčet příkladů nelze brát taxativně, mohou existovat i další metody):

Před vydáním QC:

- video-hovor s žadatelem o vydání QC,
- přiložení skenu sekundárního dokladu (např. řidičský průkaz),
- telefonický hovor se žadatelem za účelem ověření znalosti základních osobních údajů,
- odeslání dopisu na adresu žadatele o certifikát s jednorázovým kódem a až po zadání tohoto jednorázového kódu dojde k vystavení certifikátu, případě odeslání jednorázového kódu jiným kanálem, který je pod kontrolou žadatele o vydání QC,
- umožnění v procesu vydání QC, aby žadatel zadal bezpečnostní kód, který by byl distribuován žadateli ze strany vydavatele prostředku pro el. identifikaci (znalostní kód by byl smluven např. v průběhu fyzického ověřování totožnosti pro účely vydání prostředku pro el. identifikace nebo byl předán jiným kanálem - např. doporučenou poštou),
- úhrada za vydání QC zaplacená bankovním převodem z účtu vedeného na jméno žadatele o vydání QC se zprávou pro příjemce např. „Souhlasím s vydáním QC pro svoji osobu, [JMÉNO PŘÍJMENÍ]“, „Platba za vydání QC pro [JMÉNO PŘÍJMENÍ]“, apod. přičemž QTSP může žadateli v procesu vydání QC zobrazit přímo QR kód pro platbu za vydání QC,
- vzdálené biometrické ověření osoby, např. porovnání fyzické podoby obličeje žadatele o vydání QC s podobiznou osoby, kterou QSTP nebo třetí strana hodnověrně ověřili (např. z dokladu totožnosti), včetně ověření živosti žadatele o QC,
- použití dodatečného prvku pro jednoznačnou vzdálenou identifikaci uživatele, který se nepoužívá v rámci prostředků pro elektronickou identifikaci; např. pokud žadatel o QC autorizuje žádost o vydání QC pomocí mobilního tokenu a hesla, je přípustné použít jako bezpečnostní pojistku jednorázový kód zaslaný žadateli formou SMS na dříve evidovaný primární telefon žadatele a odeslání informativního emailu na dříve evidovanou emailovou adresu žadatele.

Po vydáním QC:

- odeslání korunové platby na účet žadatele o vydání QC s informací o tom, že QTSP danému žadateli vydal QC (při použití BankID ve variantě IDENTIFY AML je součástí předávaných dat rovněž informace o čísle účtu),
- informování o vydání QC na kontaktní údaje žadatele obdržené prostřednictvím BankID.

Výše uvedená opatření lze dělit na opatření **před** vydáním QC, a **po** vydání QC. Zatímco opatření před vydáním QC míří na dodatečné ověření totožnosti osoby tak, aby bylo sníženo riziko možného vydání QC útočníkovi, tak smyslem opatření po vydáním QC je informovat osobu, na kterou byl certifikát vydán o tom, že došlo k vydání certifikátu a případná opatření ponechat na této osobě (v případě, že se stala předmětem podvodu okamžitě požádat o zneplatnění QC). **QTSP by měl podle analýzy rizik zvolit opatření před vydáním QC nebo opatření po vydání QC, přičemž minimálně by měl zajistit opatření po vydání QC. QTSP musí konkrétní implementaci bezpečnostních pojistek uvést v certifikační politice, podle které se QC vydává. V případě vydání QC na základě použití prostředku mimo rámec kvalifikovaného systému, tj. BankID, mohou být bezpečnostní pojistky implementovány nejen na straně QTSP, ale rovněž na straně banky jakožto vydavatele prostředku pro el. identifikaci, případně rovněž na straně BankID[1].**

QTSP musí pro každého klienta, jemuž vydal QC a ověřil totožnost prostřednictvím prostředku pro el. identifikaci v souladu pomocí čl. 24 odst. 1 písm. d) nařízení eIDAS, vést dokumentaci, ze které bude patrno, jaké údaje obdržel za použití prostředku pro el. identifikaci, jakým způsobem byla ověřena totožnost klienta, jaké bezpečnostní pojistky byly pro tohoto konkrétního klienta aplikovány (pokud nebyl použit prostředek s vysokou úrovní záruky) a jakým způsobem byla zaručena aktuálnost osobních údajů (k aktuálnosti osobních údajů viz následující kapitola).

Je dále účelné, aby **QTSP vydávající QC informovali vhodnou formou své klienty, že za určitých okolností může jejich uznávaný elektronický podpis mít právní účinky úředně ověřeného** – toto by mělo být učiněno nezávisle na způsobu, jakým dojde k ověření totožnosti. QTSP může odkázat na informace, které připraví MV a zveřejní na webových stránkách MVČR.

Činnosti CAB:

- ověřit, že budou akceptovány ze strany QTSP vydávající QC pouze prostředky pro el. identifikaci použité v rámci kvalifikovaného systému el. identifikace s úrovní záruky vysoká (seznam kvalifikovaných správců, seznam udělených akreditací pro správu kvalifikovaného systému el. identifikace), nebo prostředky vydané v rámci kvalifikovaného systému el.

[1] Pokud se prostředek pro el. identifikaci používá v rámci kvalifikovaného systému, kvalifikovaný správce nemá možnost zjistit, pro jakou službu byl prostředek využit.

identifikace, ale použité mimo rámec kvalifikovaného systému el. identifikace (tj. BankID) s úrovní záruky minimálně značná,

- ověřit, jaké a jakým způsobem jsou implementovány bezpečnostní pojistky (bezpečnostní pojistky je povinnost implementovat v případě použití BankID) a ty blíže popsat v CAR a ověřit, zda jsou definovány v certifikační politice.

5. Aktuálnost údajů

Zde je třeba reflektovat situaci, zda prostředek pro elektronickou identifikaci byl **použit v rámci kvalifikovaného systému el. identifikace** (tj. prostřednictvím NIA) nebo **mimo rámec kvalifikovaného systému el. identifikace (v případě prostředků BankID)**.

V případě, že prostředek byl použit v rámci kvalifikovaného systému el. identifikace, jsou předané osobní údaje **navázány na referenční údaje v registru obyvatel** a jsou tedy považovány v daném okamžiku za platné. Pro úplnost je vhodné dodat, že součástí předaných údajů mohou být také tzv. subjektem definované údaje - uživatelem definované telefonní číslo a emailová adresa.

V případě, kdy prostředek byl použit **mimo rámec kvalifikovaného systému** el. identifikace (tj. prostředky BankID), předané osobní údaje pocházejí od konkrétní banky a jsou předané danému SeP prostřednictvím BankID. Tyto údaje jsou rovněž navázány na základní registry s tím, že k aktualizaci údajů dochází jednou za 24 hodin. **Povinností QTSP je zajistit vlastními silami nebo smluvně, že pro vydání QC budou použity aktuální údaje o fyzické osobě.** Existují zejména tři možnosti, jak zajistit aktuálnost údajů pro účely vydání QC (či kontroly, zda budou použity aktuální osobní údaje) v případě, kdy k ověření totožnosti byl použit prostředek použitý mimo rámec kvalifikovaného systému el. identifikace:

1. QTSP vydávající QC mají dle § 4a zákona č. 297/2016 Sb. oprávnění využívat údaje ze základních registrů a dalších napojených evidencí. Při využití tohoto práva mohou tak QTSP ověřit platnost předaných údajů na základě využití prostředků bankovní identity. V případě nalezené neshody pak QC nevydat. Nicméně je třeba upozornit, že se jedná pouze o právo pro QTSP vydávají QC přistupovat do ZR (a dalších evidencí), nikoliv o povinnost být připojen do ZR a dalších AIS.

2. QTSP může smluvně zavázat BankID, aby banka, která bude ručit za korektní autentizaci a osobní údaje o fyzické osobě, provedla ověření aktuálnosti osobních údajů v ZR v případě, kdy budou tyto údaje použity pro účely vydání QC (fakticky tak každé vydání QC za použití BankID by znamenalo jeden dotaz do ZR). BankID může rovněž na základě souhlasu klienta a smluvního ujednání s daným service providerem notifikovat tohoto service providera o případných změnách v údajích daného klienta (model, kdy service provider dostane notifikaci o změně a je na service providerovi, aby zavolal dedikovanou službu BankID, která mu sdělí konkrétní změny).

3. Poslední možností, jak QTSP může ověřit správnost údajů obdržených prostřednictvím BankID je využít ustanovení § 12a zákona č. 12/2020 Sb., které nabylo účinnosti dne 1. července 2022. Za účelem implementace tohoto ustavení vznikl portál pro online ověřování. Fyzické osobě nebo podnikateli (tj. podnikající fyzické osobě nebo právnické osobě) je umožněno ověřit kombinaci identifikačních údajů, které o sobě sdělila fyzická osoba v roli původce údajů. V případě, kdy osobní údaje souhlasí s referenčními údaji v ROB, nebo souhlasí s daty vedenými v dalších vybraných agendách (AISEO, AISC, AISEOP, AISECD) – tj. jedná se o starší již neaktuální data (předcházející současný stav), je přiděleno BSI. Volající osoba je v případě přidělení BSI informována, zda osobní údaje sloužící pro vydání BSI souhlasily s referenčními údaji v ROB, nebo zda shoda byla nalezena na starších datech (v příslušných evidencích). Více viz popis pro vývojáře[2]. Samozřejmě platí, že přidělené BSI by nebylo součástí vydaného QC.

V souvislosti s problematikou aktuálnosti údajů, je vhodné na tomto místě rovněž uvést **pro doplnění kontextu** následující informace týkající se prokazování totožnosti pomocí občanského průkazu, respektive databáze neplatných dokladů:

Může se stát, že když fyzická osoba prokazuje svoji totožnost pomocí občanského průkazu v době časové platnosti, a občanský průkaz nemá ustřižené rohy (a tak osoba kontrolující doklad nemá indikovánu žádnou změnu), tak že základní osobní údaje (jméno, adresa, datum a místo narození, trvalý pobyt) uvedené na občanském průkaze nesouhlasí s údaji vedenými v ROB?

- *principálně vyloučit to nelze, nicméně se jedná o okrajové případy typu:*
  - *sňatek v zahraniční, kdy oddací list je zpracován zvláštní matrikou (na základě toho se zaktualizují údaje v ROB) a zároveň občan nenahlásí na ohlašovně změnu jména. Pokud došlo ke sňatku před 1/8/2021, občanský průkaz je stále platný, ale údaje v ROB budou odlišné (jméno, rodinný stav). Pokud ke sňatku došlo po 2/8/2021, pak takový občanský průkaz ztrácí platnost po 45 dnech, ale v rámci těchto 45 dnů nemusí souhlasit jméno či rodinný stav se jménem vedeným v ROB.*
  - *rozhodnutí o zrušení trvalého pobytu, a to po nabytí právní moci (tento doklad by měl být veden v seznamu neplatných dokladů, více viz níže) – na dokladu bude uveden trvalý pobyt, v ROB ale bude adresa úřadu,*
  - *dojde k přejmenování ulice, kdy údaje na občanském průkazu nemusí odpovídat údajům v ROB, který odkazuje na příslušnou novou adresu v RUIÁN. Obecní úřad obce s rozšířenou působností má technický nástroj k tomu, aby změnil adresu trvalého pobytu, aniž by byla spuštěna funkcionalita ukončení platnosti občanského průkazu po uplynutí 45 dnů. Pokud úřad využije standardní proces změny trvalého pobytu, tak po 45 dnech by nicméně měla skončit platnost dokladu (tento doklad by měl být veden v seznamu neplatných dokladů, více viz níže),*

[2] https://dev.azure.com/SpravaZakladnichRegistru/NIA%20pro%20v%C3%BDvoj%C3%A1%C5%99e/_wiki/wikis/NIA-pro-v%C3%BDvoj%C3%A1%C5%99e.wiki/68/P%C5%99id%C4%9Blov%C3%A1n%C3%AD-BSI-dle-%C2%A712a

- *změna rodinného stavu – např. rozvod - soud rozhodne o rozvodu a zároveň rodinný stav je uveden na občanském průkaze. Po 45 dnech by nicméně měla skončit platnost dokladu (tento doklad by měl být veden v seznamu neplatných dokladů, více viz níže).*

Databáze neplatných dokladů (https://aplikace.mvcr.cz/neplatne-doklady/)

- *v databázi jsou evidovány občanské průkazy evidované jako ztracené, odcizené, ze zákona neplatné a neplatné na základě rozhodnutí, včetně data ohlášení ztráty nebo odcizení a data neplatnosti v ostatních případech a to do doby, kdy by jim skončila jejich řádná platnost uvedená na občanském průkazu (tj. kolonka „PLATNOST DO“) případně do doby než bude doklad navrácen správnímu úřadu a vyznačena skartace v informačním systému, tj. například:*
  - *pokud byla nahlášena ztráta nebo krádež dokladu a zároveň takovýto občanský průkaz není navrácen správnímu úřadu, bude uveden v evidenci a to do doby, než skončí jeho původní udávaná časová platnost nebo do doby, než byl odevzdán (tj. někdo jej nalezl) správnímu orgánu,*
  - *pokud skončí platnost občasného průkazu z důvodu ohlášení změny trvalého bydliště (po uplynutí 45 dnů ode dne ohlášení změny), bude uveden v evidenci a to do doby, než skončí jeho původní udávaná časová platnost nebo do doby, než bude předán správnímu orgánu, zpravidla dochází k tomu, že občan podá žádost o vydání nového občanského průkazu a při převzetí odevzdá občanský průkaz s nesprávnou adresou trvalého pobytu.*
  - *… viz § 34 zákona č. 269/2021 Sb., o občanských průkazech*

Zapisují se data nového občanského průkazu do ROB po výrobě, nebo až po potvrzení fyzického převzetí držitelem?

- *Číslo občanského průkazu se propíše do ROB až s okamžikem předání občanovi.*

Činnosti CAB:

- ověřit v případě, kdy je použit prostředek mimo rámec kvalifikovaného systému el. identifikace (tj. prostředky bankovní identity), že vždy bude zajištěno, že QTSP vydávající QC použije aktuální údaje o fyzické osobě pro níž má být QC vydán – tj. ověřit způsob, jak bude zajištěna aktuálnost osobních údajů (QTSP může tuto povinnost smluvně přenést na BankID viz bod č. 2 z výše uvedených možností, jak zajistit aktuálnost údajů pro účely vydání QC),
- ověřit v případě, kdy je použit prostředek mimo rámec kvalifikovaného systému el. identifikace (tj. prostředky bankovní identity), že poskytovatel údajů přijímá odpovědnost za to, že osobní údaje předané QTSP vydávajícímu QC jsou svázány s osobou držitele prostředku pro elektronickou identifikaci.

6. Odpovědnost

Opět je třeba reflektovat situaci, zda prostředek pro elektronickou identifikaci byl **použit v rámci kvalifikovaného systému el. identifikace** (tj. prostřednictvím NIA) nebo **mimo rámec kvalifikovaného systému el. identifikace (v případě prostředků BankID)**.

V případě, že prostředek byl použit v rámci kvalifikovaného systému el. identifikace, muselo se jednak o prostředek vydaný státním orgánem nebo akreditovanou osobou (neplatí pro bankovní identitu, tu lze použít prostřednictvím NIA jen vůči online službám státních orgánů a orgánů územně samosprávných celků). Zatímco v případě státního orgánu není stanovena povinnost mít uzavřeno pojištění odpovědnosti, tak v případě akreditované osoby, je tato povinnost stanovena v § 9 zákona č. 250/107 Sb. Akreditovaná osoba je dále povinna nahradit škodu způsobenou při správě kvalifikovaného systému bez ohledu na sjednaný limit pojistného plnění. V případě použití prostředku pro el. identifikaci v rámci kvalifikovaného systému el. identifikace je tedy problematika odpovědnosti řešena zákonem. Na webové stránce[3] jsou zveřejněny minimální doporučené výše pojištění pro žadatele o akreditaci dle zákona č. 250/2017 Sb. Připravuje se rovněž vyhláška dle zmocnění uvedeného v § 9 zákona č. 250/2017 Sb.

Pokud je prostředek pro el. identifikaci **použit mimo rámec** kvalifikovaného systému el. identifikace (platí pro bankovní identitu), pak problematika odpovědnosti musí být upravena ve smluvním vztahu mezi QTSP vydávajícím QC a BankID, případně s konkrétní bankou. **Odpovědnost musí být upravena obdobně**, jako odpovědnost akreditované osoby v zákoně č. 250/2017 Sb. Tj. neomezená odpovědnost a existence pojištění, které lze použít pro případnou úhradu škody při vzniku škody vlivem předání nesprávných osobních údajů ze strany banky či BankID (příčina předání nesprávných osobních údajů může být značně rozlišná – nesprávná data, chyba v autentizaci osoby,...). V případě, kdy vydané jednorázové QC budou využity v rámci uzavřených use casů, kde všechny strany budou informovány o vymezeném účelu použití QC a případnému omezení odpovědnosti ze strany QTSP podle čl. 13 odst. 2 Nařízení eIDAS, pak odpovědnost BankID, případně konkrétní banky, nemusí být nutně neomezená, ale musí minimálně odpovídat omezení odpovědnosti stanovené ze strany QTSP v souvislosti s vydaným QC.

V rámci smluvního vztahu mezi QTSP a BankID (případně s konkrétní bankou) musí být jednoznačně stanoveno, jaký subjekt odpovídá za co, tj. kde začíná a končí odpovědnost bank/BankID (např. odpovědnost za korektní autentizaci osoby a bezpečnou komunikaci mezi BankID a QTSP) a kde začíná a končí odpovědnost QTSP (např. korektní implementace a zabezpečení „end pointu" pro komunikaci s BankID).

[3] Minimální doporučené výše pojištění pro žadatele o akreditaci dle zákona č. 250/2017 Sb., https://www.mvcr.cz/clanek/minimalni-doporucene-vyse-pojisteni-pro-zadatele-o-akreditaci-dle-zakona-c-250-2017-sb.aspx

Činnosti CAB:

- ověřit v případě, kdy je použit prostředek mimo rámec kvalifikovaného systému el. identifikace (tj. prostředky bankovní identity), že jsou jasně stanoveny hranice odpovědnosti jednotlivých aktérů (QTSP, BankID, případně konkrétní banky),
- ověřit v případě, kdy je použit prostředek mimo rámec kvalifikovaného systému el. identifikace (tj. prostředky bankovní identity), že odpovědnost zapojených subjektů není limitována a rovněž, že existuje pojištění pro úhradu případných škod, kdy pojistné částky musí odpovídat částkám zveřejněných na webové stránce[2], případně v připravované vyhlášce.

7. Logování a zabezpečení komunikace

Pokud jde o problematiku logování, CAB musí ověřit, že QTSP vydávající QC má adekvátně zabezpečeno logování komunikace jak s NIA, tak i s BankID, případně komunikaci s jednotlivými bankami. Komunikace musí být zachycena tak, aby byla zjištěna důvěrnost, integrita a autenticita komunikace. Musí být uchovávána celá komunikace včetně requestů o autentizaci a to po dobu stanovenou v § 3 zákona č. 297/2016 Sb. – tj. po dobu 25 let od skončení platnosti QC.

V případě, kdy je použit prostředek pro el. identifikaci mimo rámec kvalifikovaného systému el. identifikace, CAB ověří zabezpečení způsobu komunikace s BankID, případě s jednotlivými bankami tak, aby bylo s vysokou úrovní spolehlivosti zajištěno, že je vysoce nepravděpodobně narušení této komunikace ze strany útočníka (šifrování, parametry použitých kryptografických algoritmů).

Činnosti CAB:

- ověřit, že QTSP vydávající QC má korektně implementováno logování a archivování komunikace jak s NIA, tak i s BankID, případně komunikaci s jednotlivými bankami,
- ověřit způsob předání QC žadateli o vydání QC,
- ověřit komunikaci s BankID, případně s jednotlivými bankami, zda je komunikace zabezpečena tak, aby bylo zajištěno, že je vysoce nepravděpodobně narušení této komunikace ze strany útočníka (důvěrnost, autenticita a integrita komunikace) včetně následného uložení této komunikace – CAB může při přezkoumání využít reporty pravidelných bezpečnostních auditů spol. BankID, pokud audity proběhly v souladu s mezinárodními normami a pokud spol. BankID výsledky bezpečnostních auditů CAB poskytne.

8. Implementace ověřování totožnosti pomocí prostředků pro el. identifikaci

CAB v souvislosti se zpracováním CAR rovněž ověří, zda QTSP vydávající QC implementoval ověřování totožnosti pomocí prostředků pro el. identifikaci korektně.

Činnosti CAB:

- QTSP musí demonstrovat celý proces vydání QC (včetně ověření totožnosti pomocí prostředku pro el. identifikaci),
- ověřit ukázku logů komunikace s NIA nebo BankID a celkový soubor údajů o klientovi (dokumentace, ze které bude patrno, jaké údaje obdržel za použití prostředku pro el. identifikaci, jakým způsobem byla ověřena totožnost klienta [BankID/prostřednictvím NIA s využitím prostředku s vysokou úroveň záruky], jaké bezpečnostní pojistky byly pro tohoto konkrétního klienta aplikovány (pokud nebyl použit prostředek s vysokou úrovní záruky) a jakým způsobem byla zaručena aktuálnost osobních údajů),
- ověřit chování při nestandardních situacích – žadatel o vydání QC neposkytne souhlas s předáním požadovaných údajů, přerušení online komunikace mezi QTSP a žadatelem o vydání QC v procesu vydání QC.