Katalog Služeb BankID

Tento Katalog Služeb tvoří přílohu Smlouvy o poskytování služeb IdP (dále jen „**Smlouva IdP**“) a zároveň Smlouvy o poskytování služeb BankID (dále jen „**Smlouva SeP**“ a společně se Smlouvou IdP také jen „**Smlouvy**“, jednotlivě „**Smlouva**“) a stanoví popis a parametry Služeb BankID a Služeb poskytovaných dle těchto smluv a předpoklady jejich poskytování.

Společnost Bankovní identita, a.s. nabízí následující Služby BankID a Služby ve smyslu Smluv:

1. Přihlášení (CONNECT);
2. Identifikace (IDENTIFY, IDENTIFY PLUS, IDENTIFY AML);
3. Podpis/Autorizace (SIGN)

(dále společně jen „**Služby**“ nebo samostatně „**Služba**“).

Rozsah poskytovaných Služeb se může v budoucnu rozšiřovat. Zároveň předpokládáme budoucí změny Služeb proti stávajícímu popisu, a to především v zájmu naplnění potřeb SeP a Zákazníků ve smyslu Smluv (dále společně jen „**SeP**“), podle trendů a novinek v oblasti identitních služeb i pro zlepšení zákaznické zkušenosti Koncového uživatele.

Základní pojmy:

Nestanoví-li tento Katalog Služeb jinak, pojmy s velkým písmenem použité v tomto Katalogu Služeb mají svůj význam stanovený ve Smlouvě IdP nebo Smlouvě SeP, Smluvních podmínkách, SLA nebo jiných dokumentech, na které tyto dokumenty výslovně odkazují.

Pro tento Katalog Služeb se dále definují následující výrazy:

1. **API**: aplikační programové rozhraní;
2. **Aplikace**: koncová služba nebo její část vymezená nastavením SeP v samoobslužné platformě BankID, která umožňuje SeP aktivaci, deaktivaci a konfiguraci Služeb a která je dostupná na developer.bankid.cz;
3. **Ceník BankID**: Ceník tvořící přílohu Smlouvy SeP;
4. **Claim**: jednotlivý Osobní údaj specifikovaný v [Tabulce č. 2](#Table03) v příloze tohoto Katalogu Služeb;
5. **Consent** **screen**: obrazovka IdP žádající souhlas Koncového uživatele se zpracováním Osobních údajů;
6. **Dokument**: PDF dokument podepisovaný pomocí služby BankID SIGN. V případě, že je v tomto Katalogu služeb uvedeno „Dokumenty“ v množném čísle, rozumí se tím i jeden samostatný Dokument, není-li řečeno jinak;
7. **Flow**: postup kroků z pohledu Koncového uživatele při použití Služby Koncovým uživatelem popisovaný tímto Katalogem Služeb pro Služby v části Popisu Služby;
8. **LoA**: úroveň záruky ve smyslu čl. 8 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; pojem může odkazovat na úroveň záruky ve smyslu standardu ISO/IEC 29115:2013, v rozsahu dle Technické specifikace, je-li to u pojmu výslovně uvedeno;
9. **Nabídka aktivních Identity providerů**: rozhraní BankID, ve kterém jsou zavedeni IdP a Identity provideři a ke kterému přistupuje Koncový uživatel;
10. **Metadata**: metadata Dokumentu tvořená jedinečným matematickým otiskem (hashem) a názvem Dokumentu, který poskytuje SeP obojí ve formátu dle Technické specifikace. Dochází-li k podpisu sady Dokumentů, jsou Metadata tvořena jedinečným matematickým otiskem (hashem) Obálky a názvem Obálky, který poskytuje SeP, obojí ve formátu dle Technické specifikace;
11. **Obálka**: elektronická sada obsahující jeden a více Dokumentů podepisovaných pomocí služby BankID SIGN;
12. **PEI**: prostředek pro elektronickou identifikaci vydaný Koncovému uživateli ze strany IdP;
13. **Prohlášení**: dvojice textových hodnot obsahující
    1. prohlášení Koncového uživatele (například pokyn k nákupu určitého počtu akcií); a
    2. název tohoto prohlášení (například „Pokyn k nákupu akcií“).

Prohlášení je podepisováno pomocí služby BankID SIGN.

1. **Rozhraní Služeb**: API BankID prostřednictvím kterého jsou Služby poskytovány;
2. **Scope**: kategorie Osobních údajů Koncového uživatele zpracovávaných při užití Služeb specifikovaných v [Tabulce č. 1](#Table02) v příloze tohoto Katalogu Služeb, zahrnující Claimy specifikované v [Tabulce č. 2](#Table03) v příloze tohoto Katalogu Služeb.
3. Přihlášení (CONNECT)

|  |
| --- |
| **POPIS SLUŽBY** |
| Služba je určena pro SeP, kteří vyžadují přihlášení Koncového uživatele. Služba je alternativou ke službám Google ID / Facebook ID / Moje ID nabízející ovšem ověřenou identitu – osobní a kontaktní údaje o Koncovém uživateli. Služba nabízí možnost dvoufaktorové autentizace pro lepší zabezpečení účtů Koncových uživatelů.  Aplikace SeP může být jakákoliv webová/mobilní aplikace, která vyžaduje/nabízí možnost registrace a přihlašování a ve které může Koncový uživatel na místo nové registrace či přihlášení využít přihlášení přes BankID.  **Z pohledu Koncového uživatele:**   1. Koncový uživatel zvolí přihlášení prostřednictvím BankID; 2. kliknutím na logo své banky v Nabídce aktivních Identity providerů je přesměrován na přihlašovací stránky IdP; 3. na login stránce IdP provádí autentizaci pomocí PEI; 4. při prvním přihlášení je Koncový uživatel požádán IdP o souhlas s poskytnutím svých údajů ve prospěch SeP; 5. po potvrzení souhlasu Koncovým uživatelem poskytuje IdP data SeP pro registraci a Koncový uživatel je přesměrován zpět na stránku SeP, kde je přihlášený.   *Poznámka:*  *V rámci souhlasu může IdP Koncovému uživateli poskytnout možnost zrušit předání nepovinných údajů nebo potvrdit trvalé přihlášení. Služba podporuje možnost trvalého přihlášení bez nutnosti opakované autentizace a souhlasu s předáním údajů (platnost tokenu pro trvalé přihlášení je 365 dní).*  *V rámci Služby je možné ze strany SeP nastavit vlastní parametr na požadovanou úroveň autentizace. Použití PEI LoA vyšší než byl požadovaný ze strany SeP je v rámci Služby povoleno (např. pokud IdP nepodporuje).*  *SeP si může vzhled Flow přizpůsobit své vlastní potřebě v rozsahu, v jakém to Smluvní podmínky nevylučují.*  *Pro druhé a další přihlášení se Koncový uživatel, popř. vybraná banka z Nabídky aktivních Identity providerů uloží do cookies a výše uvedené Flow se zjednoduší (dle řešení daného IdP), jak je blíže specifikováno v doporučených UX standardech Služeb BankID.* |
| **PŘEDÁVANÉ ÚDAJE** |
| **Údaje Koncového uživatele, které lze poskytnout v rámci Služby, specifikuje** [Tabulka č. 1](#Table02) **a** [Tabulka č. 2](#Table03) **v příloze tohoto Katalogu Služeb.**  *Poznámka:*  *SeP vybírá z uvedených Scopes (viz.* [Tabulka č. 1](#Table03) *v příloze tohoto Katalogu Služeb). Rozsah Scopes v mezích* [Tabulky č.](#Table03) 1 *určuje SeP v rámci volání na Rozhraní Služeb. Zároveň určuje, jaké Claims jsou povinné/volitelné z pohledu Koncového uživatele. Je-li v Portálu pro Aplikaci zvolena Služba Identifikace (IDENTIFY, IDENTIFY PLUS, nebo IDENTIFY AML), je možné pomocí odpovídajícího (menšího) rozsahu Scopes volat i Službu CONNECT.*  *IdP sestavuje Consent screen dle zaregistrovaných Scopes popř. omezuje seznam dle konkrétního volání SeP.*  *V případě IdP umožňujících propojení identit, uvedených na seznamu zpřístupněném pro tento účel na Portálu, je ve vztahu ke Koncovému uživateli předáván Scope ID uživatele s jednotným identifikátorem* sub*, bez ohledu na to, jakého IdP pro využití Služeb Koncový uživatel zvolí. Scope ID je v tomto případě předáván způsobem, který umožní SeP spojit identifikátory* sub *přidělené Koncovému uživateli v minulosti při využití různých IdP ze strany Koncového uživatele při přístupu ke službám tohoto SeP.* |
| **DODATEČNÉ PODMÍNKY a INFORMACE** |
| Z pohledu věku Koncového uživatele není poskytnutí Služby Koncovému uživateli ze strany BankID omezeno. Službu může použít Koncový uživatel s platným PEI vydaným IdP, a to dle vlastní obchodní politiky IdP. |
| **VARIANTY SLUŽBY** |
| 1. **CONNECT – jednorázové použití/transakce**   V Ceníku BankID je definována cena za jednorázové použití Služby CONNECT, a to bez ohledu na použitý PEI (LoA 2 / LoA 3). Možnost trvalého přihlášení Koncového uživatele s max. dobou platnosti 365 dní.   1. **CONNECT – předplatné na Koncového uživatele**   V Ceníku BankID je definována cena za předplatné pro Koncového uživatele Služby CONNECT, a to bez ohledu na použitý PEI (LoA 2 / LoA 3). Možnost trvalého přihlášení Koncového uživatele s max. dobou platnosti 365 dní.  Cena je za neomezené použití Služby pro daného Koncového uživatele dle zvolené varianty předplatného (bez ohledu na počet použití Služby). Po uplynutí této doby je účtována další platba v momentě dalšího použití Služby ze strany Koncového uživatele. |

1. Identifikace (IDENTIFY, IDENTIFY PLUS, IDENTIFY AML)

|  |
| --- |
| **POPIS SLUŽBY** |
| Služba je určená pro SeP, kteří potřebují identifikovat Koncového uživatele na základě bankou ověřené identity – tzn. jako kdyby byl Koncový uživatel fyzicky přítomen a před uzavřením smluvního vztahu/získáním služby použil k identifikaci např. platný doklad totožnosti.  Rozsah dat v rámci Služby se odvíjí od standardních právních předpisů a obchodní politiky SeP. Službu lze využít k identifikaci osoby v souladu se zákonem č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu.  **Z pohledu Koncového uživatele:**   1. Koncový uživatel chce sjednat službu (produkt/uskutečnit objednávku) u SeP; 2. zvolí si možnost ověření identity pomocí BankID; 3. kliknutím na logo své banky v Nabídce aktivních Identity providerů je přesměrován na přihlašovací stránky IdP; 4. na login stránce IdP provádí Koncový uživatel autentizaci pomocí PEI; 5. Koncový uživatel je IdP požádán o souhlas s poskytnutím svých údajů ve prospěch SeP (obsahuje i souhlas pro BankID); 6. po potvrzení souhlasu poskytuje IdP data SeP; 7. Koncový uživatel je přesměrován zpět na stránku SeP.   *Poznámka:*  *SeP definuje rozsah dat předávaných v rámci Služby dle nabízených variant Služby, včetně označení povinných/volitelných položek. Rozsah předávaných osobních a kontaktních údajů požadovaných SeP v rámci Služby lze ze strany Koncového uživatele upravit pouze v rámci volitelných položek a dle realizace konkrétním IdP.*  *O zakomponování Služby Identifikace v rámci procesu nákupu/objednávky rozhoduje SeP.*  *SeP si může rovněž vzhled Flow přizpůsobit své vlastní potřebě v rozsahu, v jakém to Smluvní podmínky nevylučují.* |
| **PŘEDÁVANÉ ÚDAJE** |
| **Údaje Koncového uživatele, které lze poskytnout v rámci Služby Identifikace, specifikuje** [**Tabulka č. 1**](#Table02) **a**[**Tabulka č. 2**](#Table03) **v příloze tohoto Katalogu Služeb.**  Je-li v rámci volání na Rozhraní Služeb požadován Scope Doklad a Koncový uživatel není státním občanem České republiky, je IdP povinen předat BankID údaje v rozsahu dle Technické specifikace o   1. dokladu Koncového uživatele vydaném orgánem státní správy České republiky, jehož údaje lze ověřit v registru obyvatel, má-li IdP k dispozici údaje o takovémto platném dokladu, a zároveň 2. údaje o dokladu Koncového uživatele, který je průkazem totožnost ve smyslu § 4 odst. 6 zákona č. 253/2008, o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů (dále jen „**AML zákon**“).   Splňuje-li jeden doklad obě podmínky (tj. jedná se o doklad ověřitelný v registru obyvatel a zároveň je průkazem totožnosti dle AML zákona), může IdP předat BankID pouze údaje o takovém jednom dokladu.  *Poznámka:*  *Variantu Služby Identifikace (IDENTIFY, IDENTIFY PLUS, IDENTIFY AML) vybírá SeP pomocí volby Scopes v rámci volání na rozhraní Služeb (viz.* [Tabulka č. 1](#Table02) *v příloze tohoto Katalogu Služeb). Zároveň určuje, jaké Claims jsou povinné/volitelné z pohledu Koncového uživatele. Volat lze však pouze Službu se stejným nebo menším rozsahem Scopes než jaký* [Tabulka č. 1](#Table02) *určuje pro Službu, kterou má SeP nastavenu v Portálu pro Aplikaci, která zasílá volání na Rozhraní Služeb. Je-li v Portálu pro Aplikaci zvolena Služba Identifikace (IDENTIFY, IDENTIFY PLUS, nebo IDENTIFY AML), je možné pomocí odpovídajícího (menšího) rozsahu Scopes volat i Službu CONNECT.*  *IdP sestavuje Consent screen dle zaregistrovaných Scopes popř. omezuje seznam dle konkrétního volání SeP.*  *V případě IdP* *umožňujících propojení identit, uvedených na seznamu zpřístupněném pro tento účel na Portálu, je ve vztahu ke Koncovému uživateli předáván Scope ID uživatele s jednotným identifikátorem* sub*, bez ohledu na to, jakého IdP pro využití Služeb Koncový uživatel zvolí. Scope ID je v tomto případě předáván způsobem, který umožní SeP spojit identifikátory* sub *přidělené Koncovém uživateli v minulosti při využití různých IdP ze strany Koncového uživatele při přístupu ke službám tohoto SeP.* |
| **DODATEČNÉ PODMÍNKY a INFORMACE** |
| V rámci Služby Identifikace IdP nepředává SeP kopii dokladu totožnosti Koncového uživatele.  Poskytnutí Služby je ze strany BankID omezeno pro Koncové uživatele starší 18 let.  Autentizace Koncového uživatele je v rámci Služby Identifikace možná pouze prostřednictvím PEI LoA 3. |
|  |
| **VARIANTY SLUŽBY** |
| **Možné varianty Služby Identifikace dle rozsahu poskytovaných dat (Scope) dle** [**Tabulky č. 1**](#Table02)**:**   1. **IDENTIFY;** 2. **IDENTIFY PLUS;** 3. **IDENTIFY AML.**   Služba zahrnuje možnost opakovaného přihlášení, předání údajů (bez ohledu na počet použití Služby) a možnost trvalého souhlasu s předáním údajů Koncového uživatele s max. dobou platnosti 365 dní. BankID může nastavit max. dobu předplatného v délce 730 dní v případě Služby IDENTIFY AML.  V Ceníku BankID je definována cena Služby za Koncového uživatele dle jednotlivých variant Služby Identifikace. Po uplynutí doby předplatného je účtována další platba v momentě dalšího použití Služby ze strany Koncového uživatele. |

1. Notifikace (není samostatná Služba)

|  |
| --- |
| **NOTIFIKACE** |
| Jako doplňkovou vlastnost Služeb CONNECT a Identifikace ve variantě „předplatné na Koncového uživatele“ si lze sjednat zasílání notifikací o změně poskytnutých údajů Koncového uživatele. Podmínkou zaslání notifikací je souhlas Koncového uživatele.  Pokud je Služba CONNECT nebo Identifikace poskytnuta se sjednanými notifikacemi, Koncový uživatel k nim udělí souhlas a dojde ke změně údajů Koncového uživatele evidovaných IdP, kterého Koncový uživatel zvolil pro Službu CONNECT, resp. Identifikace, IdP zašle BankID změnovou notifikaci. BankID následně zašle změnovou notifikaci SeP. Notifikace neobsahuje změněné údaje, pouze informuje SeP, že ke změně údajů došlo. IdP zasílá změnové notifikace i v případě, kdy dojde k vypršení platnosti tokenu dle následujícího odstavce.  Pokud Koncový uživatel udělil pro SeP souhlas s trvalým přihlášením do Koncové služby SeP, získá SeP token s platností 365 dnů. Souhlas může Koncový uživatel odvolat. V případě odvolání souhlasu se platnost tokenu a zasílání notifikací ukončí. S platným tokenem může SeP po obdržení změnové notifikace bezplatně vyžádat od BankID poskytnutí aktualizovaných údajů Koncového uživatele, které BankID vyžádá od IdP. Pokud SeP nemá platný token, může následně Službu CONNECT, resp. Identifikace využít pro získání aktualizovaných údajů (s novým souhlasem Koncového uživatele). Úhrada za další poskytnutí Služby CONNECT, resp. Identifikace záleží na zvoleném modelu úhrady, případně na existenci předplatného pro daného Koncového uživatele.  IdP zasílá změnovou notifikaci na základě získání aktualizovaných údajů z informačních systémů veřejné správy podle § 38af zákona č. 21/1992 Sb., o bankách, nebo jiným způsobem (např. sdělením Koncového uživatele). |

1. Podpis/Autorizace (SIGN)

|  |
| --- |
| **POPIS SLUŽBY** |
| Služba SIGN je určena pro zaručený elektronický podpis ve vztahu Koncového uživatele a SeP.  Služba je určena pro podpis PDF Dokumentů při sjednávání produktů/služeb u SeP, kde je třeba ověřovat identitu Koncového uživatele při podpisu příslušné smlouvy včetně možnosti tento podpis zpětně doložit/verifikovat. Službu lze využít rovněž pro podpis Prohlášení.  K podpisu lze současně zaslat:   * jeden PDF Dokument nebo Obálku obsahující jeden až deset PDF Dokumentů; a * až 20 Prohlášení.   Podpis jednoho PDF Dokumentu a podpis Obálky se pro účely odst. 4.9 Smluvních podmínek pro SeP považují za samostatné Služby.  **Proces podpisu prostřednictvím Služby SIGN:**   1. SeP vygeneruje obsah Dokumentů a Prohlášení, jež mají být podepsány, a zobrazí je Koncovému uživateli; 2. Koncový uživatel vybírá možnost podepsat Dokumenty a/nebo Prohlášení pomocí BankID; 3. SeP zašle Dokumenty a/nebo Prohlášení spolu s Metadaty dle Technické specifikace do BankID; 4. Koncový uživatel vybírá IdP; 5. BankID zobrazí Koncovému uživateli Metadata a odkaz na prohlédnutí či stažení Dokumentů a/nebo Prohlášení z prostředí BankID; současně Koncového uživatele informuje o obchodních podmínkách poskytování služby BankID SIGN pro Koncového uživatele a způsobu jejich akceptace; 6. Po potvrzení seznámení s Dokumenty a/nebo Prohlášeními a záměru je podepsat je Koncový uživatel přesměrován na stránky IdP; 7. BankID zašle IdP:    1. Metadata a odkaz na Dokumenty dočasně uložené v systémech BankID a/nebo    2. Prohlášení. 8. V prostředí IdP Koncový uživatel uděluje pokyn připojit podpis Koncového uživatele k Dokumentům s předanými Metadaty a/nebo Prohlášení a dává souhlas IdP s předáním Osobních údajů BankID a bere na vědomí, že Osobní údaje v rámci certifikátu Koncového uživatele budou zpřístupněny SeP; pokyn Koncového uživatele podepsat Dokumenty a/nebo Prohlášení je ověřován dvěma faktory; v prostředí IdP provádí Koncový uživatel také autentizaci pomocí PEI; pokynem připojit podpis Koncového uživatele k Dokumentům a/nebo Prohlášením a udělením souhlasu IdP s předáním Osobních údajů BankID Koncový uživatel současně akceptuje podmínky poskytování služby BankID SIGN pro Koncového uživatele; 9. IdP předá BankID zpět Prohlášení a/nebo Metadata jako potvrzení, že Koncový uživatel udělil pokyn BankID podepsat Dokumenty a/nebo Prohlášení. 10. BankID opatří Dokumenty vizuální značkou symbolizující podpis Koncového uživatele (pokud je to možné), opatří elektronickým podpisem Dokumenty a/nebo Prohlášení pomocí certifikátu Koncového uživatele pro elektronický podpis, který vydává BankID, a opatří Dokumenty a/nebo Prohlášení kvalifikovanou elektronickou pečetí BankID a zpřístupní Dokumenty a / nebo Prohlášení SeP; certifikát Koncového uživatele se neuchovává dlouhodobě a je vytvářen při každém použití Služby. V okamžiku uložení Dokumentů a/nebo Prohlášení s elektronickým podpisem v prostředí BankID jsou Dokumenty a/nebo Prohlášení podepsány.   *Poznámka:*  *SeP si může vzhled Flow přizpůsobit své vlastní potřebě (např. výběr bank, komponenty pro rychlé přihlášení). O zakomponování Služby SIGN v rámci procesu rozhoduje SeP.*  *SeP může odeslat odkazy na podpis konkrétních Dokumentů a/nebo Prohlášení Koncovému uživateli na email nebo pomocí SMS a umožnit tak využití služby BankID později nebo z jiného zařízení.*  *IdP nedisponuje podepsanými Dokumenty a/nebo Prohlášeními.*  *V případě, kdy je třeba Dokumenty a/nebo Prohlášení opatřit podpisy více osob, je třeba Službu volat opakovaně (samostatně pro každou podepisující osobu).* |
| **POVINNOSTI SEP A IDP** |
| **SeP:**  SeP je v rámci procesu podpisu prostřednictvím Služby SIGN povinen:   1. Zobrazit obsah Dokumentů a/nebo Prohlášení v rozhraní Koncové služby Koncovému uživateli (tuto skutečnost potvrzuje SeP v rámci volání Služby SIGN).   *Poznámka: Umožnění seznámení se s obsahem Dokumentů nebo Prohlášení Koncovému uživateli před jeho podpisem je povinností SeP. Neposkytnutí Služby (nedokončení Transakce) nebo budoucí rozporování platnosti podpisu Koncovým uživatelem plynoucí z nedodržení této povinnosti jde k tíži SeP.*   1. Zaslat Dokumenty spolu s Metadaty, případně zaslat Prohlášení do BankID ve formátu odpovídajícím Technické specifikaci; Dokumenty je třeba zaslat ve verzi PDF/A; Metadata musí odpovídat Dokumentu nebo Obálce zaslaným BankID. 2. Uložit si podepsané Dokumenty a/nebo Prohlášení poskytnutý ze strany BankID.   *Poznámka: Podepsané Dokumenty* *a/nebo Prohlášení bude na straně BankID k dispozici ke stažení po dobu 3 dnů. Po uplynutí této doby budou Dokumenty a/nebo Prohlášení smazány a SeP k nim nebude mít dále přístup.*   1. Zpřístupnit Koncovému uživateli podepsané Dokumenty a/nebo Prohlášení způsobem umožňujícím uchování a opakované zobrazení.   *Poznámka: BankID nezajišťuje stažení a poskytnutí Dokumentů a/nebo Prohlášení Koncovému uživateli v textové podobě podle § 1827 odst. 2 zákona č. 89/2012 Sb., občanský zákoník. Za splnění povinností v souvislosti s uzavřením smlouvy ve vztahu ke Koncovému uživateli odpovídá výhradně SeP.*  **IdP:**  IdP je v rámci procesu podpisu prostřednictvím Služby SIGN povinen:   1. Zobrazit Koncovému uživateli    1. Metadata a/nebo    2. Prohlášení a společný hash všech Prohlášení vypočtený BankID, pomocí SHA-512 funkce serializací všech Prohlášení vzestupně podle pořadí. 2. Informovat uživatele, že potvrzením pokynu připojit podpis Koncového uživatele k Dokumentům a/nebo Prohlášení a udělením souhlasu IdP s předáním Osobních údajů BankID v prostředí IdP uděluje pokyn připojit podpis k Dokumentům nebo Prohlášením prostřednictvím BankID. 3. Na základě autentizace a autorizace pomocí PEI ověřit totožnost Koncového uživatele a jeho pokyn k podpisu Dokumentů a/nebo Prohlášení prostřednictvím BankID.    1. Využívá-li IdP v rámci svého technického řešení ke dvoufaktorovému ověření pokynu Koncového uživatele k připojení podpisu k Dokumentům a/nebo Prohlášení SMS zprávy nebo jiné metody s podstatným omezením délky zobrazovaného textu, je povinen   v autorizační SMS zprávě či zprávách nebo jiné metodě s podstatným omezením délky uvést minimálně   * + 1. prvních 30 znaků názvu Dokumentu, posledních 10 znaků jeho hashe a informaci o použité metodě k vytvoření hashe dle Technické specifikace, pokud je podepisován jeden Dokument; nebo     2. 25 znaků názvu Obálky, posledních 10 znaků hashe Obálky a informaci o použité metodě k vytvoření hashe dle Technické specifikace, pokud je podepisováno více Dokumentů; a/nebo     3. počet podepisovaných Prohlášení a posledních 10 znaků společného hashe všech těchto Prohlášení a informaci o použité metodě k vytvoření hashe dle Technické specifikace, pokud je podepisováno alespoň jedno Prohlášení.   1. Využívá-li IdP v rámci svého technického řešení ke dvoufaktorovému ověření pokynu Koncového uživatele k připojení podpisu k Dokumentů a/nebo Prohlášení jiné technické postupy, je povinen při v rámci ověřovacího procesu v rámci druhého faktoru uvést minimálně      1. název Dokumentu, jeho hash a informaci o použité metodě k vytvoření hashe dle Technické specifikace, pokud je podepisován jeden Dokument; nebo      2. název Obálky, její hash a informaci o použité metodě k vytvoření hashe dle Technické specifikace, pokud je podepisováno více Dokumentů; a/nebo      3. počet podepisovaných Prohlášení a posledních 10 znaků společného hashe všech těchto Prohlášení a informaci o použité metodě k vytvoření hashe dle Technické specifikace, pokud je podepisováno alespoň jedno Prohlášení.  1. Předložit Koncovému uživateli souhlas s předáním Osobních údajů pro BankID potřebných k vydání Certifikátu a provedení podpisu dle Technické specifikace a informovat jej o předání těchto údajů SeP. 2. Předat BankID Metadata a/nebo Prohlášení jako potvrzení, že Koncový uživatel udělil pokyn podepsat Dokument a/nebo Prohlášení. 3. Poskytnout BankID osobní údaje Koncového uživatele potřebné k vydání certifikátu a vytvoření podpisu Koncového uživatele. 4. Archivovat po dobu 15 let od provedení Transakce Auditní logy dokládající autorizaci podpisové transakce ze strany Koncového uživatele. |
| **ZÁZNAMY O TRANSAKCÍCH** |
| **Údaje ukládané v rámci Služby:**  BankID bude v databázi udržovat záznamy o podpisových Transakcích, včetně data, času a hashe Obálky, Dokumentů a/nebo Prohlášení přijatých od SeP a zaslaných zpět a hashe certifikátu veřejného klíče, odpovídajícího certifikátu použitému pro vytvoření podpisu daných Dokumentů a/nebo Prohlášení. SeP (případně libovolná třetí osoba disponující podepsaným Dokumentem nebo Prohlášením) si bude moci prostřednictvím API BankID po stanovenou dobu zpětně ověřit podpis Dokumentu, a to nahráním Dokumentu přes API do BankID, na základě čehož BankID ověří a případně potvrdí platnost certifikátu a že příslušný Dokument byl podepsán pomocí Služby SIGN.  Záznamy o podpisových Transakcích bude BankID uchovávat 15 let od provedení Transakce.  **Údaje Koncového uživatele nezbytné pro podpis Dokumentů a/nebo Prohlášení specifikuje** [**Tabulka č. 1**](#Table02) **a**[**Tabulka č. 2**](#Table03) **tohoto Katalogu služeb. Uvedené Scopes poskytuje IdP BankID pro vytvoření podpisu. Údaje se v rámci Služby SIGN předávají SeP pouze v rámci certifikátu Koncového uživatele.** |
| **DODATEČNÉ PODMÍNKY a INFORMACE** |
| Poskytnutí Služby SIGN je ze strany BankID omezeno pro Koncové uživatele starší 18 let.  Autentizace Koncového uživatele je v rámci Služby SIGN možná pouze prostřednictvím PEI LoA 3.  Záznam o uskutečněné transakci je na straně BankID a bank uchovávaná po dobu 15 let. |
| **VARIANTY SLUŽBY** |
| **1. SIGN – jednorázové použití/transakce**  Služba slouží k jednorázovému úkonu Koncového uživatele, nikoliv k pravidelným úkonům Koncového uživatele.  V Ceníku BankID je definována cena za jednorázové použití Služby SIGN.  **2. SIGN – předplatné na Koncového uživatele**  V Ceníku BankID je definována cena za předplatné pro Koncového uživatele pro Službu SIGN jako doplněk pro službu CONNECT.  Cena je za neomezené použití Služby pro daného Koncového uživatele dle doby předplatného (bez ohledu na počet použití Služby). Po uplynutí této doby je účtována další platba v momentě dalšího použití Služby ze strany Koncového uživatele. |

Příloha

**Tabulka č. 1: Dostupnost jednotlivých Scopes v rámci Služeb**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Scope** | **CONNECT** | **IDENTIFY** | **IDENTIFY PLUS** | **IDENTIFY AML** | **SIGN[[1]](#footnote-2)** |
| ID uživatele | ü | ü | ü | ü | ü |
| Jméno a příjmení | ü | ü | ü | ü | ü |
| Telefon | ü | ü | ü | ü | ü |
| Email | ü | ü | ü | ü | ü |
| Adresy |  | ü | ü | ü | ü |
| Datum narození | ü | ü | ü | ü | ü |
| Tituly |  | ü | ü | ü | ü |
| Pohlaví |  | ü | ü | ü |  |
| Rodné číslo |  | ü | ü | ü |  |
| Místo narození |  |  | ü | ü |  |
| Stav |  |  | ü | ü |  |
| Doklad |  |  | ü | ü |  |
| Právní status |  |  | ü | ü | ü |
| Bankovní účet |  | ü | ü | ü |  |
| AML ověření |  |  |  | ü |  |

**Tabulka č. 2: Scope a Claimy**

|  |  |  |  |
| --- | --- | --- | --- |
| **Název scope** | **Označení Scope dle Technické specifikace** | **Claimy** | |
| ID uživatele | - | sub | |
| Jméno a příjmení | profile.name | given\_name3  family\_name3  middle\_name3, 7  nickname4, 7  preferred\_username4, 7 | |
| Telefon | profile.phonenumber | phone\_number4, 7  phone\_number\_verified4, 7 |
| Email | profile.email | email4, 7  email\_verified4, 7 |
| Adresy | profile.addresses | addresses.type5  addresses.street5, 7  addresses.buildingapartment5, 7  addresses.streetnumber5, 7  addresses.city5  addresses.zipcode5  addresses.country5  addresses.ruian\_reference5, 7 |
| Datum narození | profile.birthdate | Birthdate  age  date\_of\_death3, 7 |
| Tituly | profile.titles | title\_prefix3, 7  title\_suffix3, 7 | |
| Pohlaví | profile.gender | gender4 | |
| Rodné číslo | profile.birthnumber | birthnumber3, 8 | |
| Místo narození | profile.birthplaceNationality | birthplace3  birthcountry3, 9  primary\_nationality3, 7  nationalities3 | |
| Stav | profile.maritalstatus | maritalstatus4, 7 | |
| Doklad | profile.idcards | idcards.type3  idcards.description3, 7  idcards.country3  idcards.number3  idcards.valid\_to3  issuer3, 7  issue\_date3, 7 | |
| Právní status | profile.legalstatus | majority4  pep4  limited\_legal\_capacity6 |
| Bankovní účet | profile.paymentAccounts | paymentAccounts4, 7 | |
| AML ověření[[2]](#footnote-3) | profile.verification | verification.trust\_framework  verification.time7  verification.verification\_process | |

1. Uvedené Scopes poskytuje IdP BankID pro vytvoření podpisu. SeP se předávají pouze vybrané údaje se SeP, a to pouze jako součást podpisového certifikátu. [↑](#footnote-ref-2)
2. Údaje profile.verification IdP předává v povinném rozsahu bez ohledu na variantu služby vždy, v souladu s Technickou specifikací.

   3 Údaje, které IdP notifikuje na základě změny v Informačních systémech veřejné správy

   4 Údaje, které IdP notifikuje na základě změny ve svých systémech.

   5 Údaje o adrese trvalého pobytu notifikuje IdP na základě změny v Informačních systémech veřejné správy, údaje o kontaktní adrese IdP notifikuje na základě změny ve svých systémech.

   6 Údaje, které IdP notifikuje na základě změny ve svých systémech. Po zpřístupnění těchto údajů z v Informačních systémů veřejné správy IdP notifikuje tyto údaje na základě změny v Informačních systémech veřejné správy.

   7 Údaje, které není IdP povinen předávat BankID a BankID předávat SeP. To platí pouze v případě, že IdP takové údaje nemá k dispozici. Pokud IdP má údaje k dispozici, je povinen je předat BankID (a BankID dále SeP), dle obecných pravidel stanovených v Katalogu služeb.

   8 U občanů České republiky se předává vždy, u ostatních osob není IdP povinen předávat BankID a BankID předávat SeP, nemá-li je IdP k dispozici.

   9 U tohoto claimu mohou být předávány také nestandardní hodnoty jako "N/A" nebo "Mimo území státu". [↑](#footnote-ref-3)