Dokumentace

k projektu Czech POINT

Příručka pro OTP přihlašování

Vytvořeno dne: 10. 5. 2012
Aktualizováno: 16. 4. 2020
Verze: 1.2

Obsah

1. Úvod

1.1. Účel dokumentu

Tato příručka popisuje přihlašování pomocí OTP v prostředí Czech POINT.

Zejména je popsán způsob aktivace a deaktivace OTP přihlašování v aplikaci Správa dat a také postup přihlašování do aplikace Správa dat a externích informačních systémů přes rozhraní KAAS.

1.2. Princip fungování OTP přihlašování

Přihlašování pomocí OTP je založeno na vygenerování jednorázového číselného kódu pomocí specializovaného zařízení nebo aplikace. Tento číselný kód se zadá na přihlašovací obrazovce do systému spolu s uživatelským jménem a heslem. Při každém dalším novém přihlášení do systému se musí na přihlašovací obrazovce zadat vždy nový kód.

Existují dva standardy OTP:

- HOTP (RFC 4226) – číselné kódy se mění na základě čítače, nový kód obvykle vygenerujete stiskem nějakého tlačítka
- TOTP (RFC 6238) – číselné kódy se mění automaticky po uplynutí určitého času (obvykle 30 sekund)

Systém Czech POINT podporuje pouze standard HOTP.

Přidáním proměnných OTP kódů k neměnnému uživatelskému jménu a heslu se zvyšuje zabezpečení přihlašování uživatelů do systémů. Přitom po uživatelích nejsou oproti autentizaci certifikátem vyžadovány žádné velké technické znalosti – stačí vědět jak vygenerovat OTP kód na svém zařízení či v aplikaci.

Pro každý systém, kam se uživatel hlásí, je potřeba mít vlastní specializované zařízení nebo aplikaci pro generování OTP kódů. OTP aplikace však obvykle umožňují vytvořit více tzv. OTP profilů pro přihlašování do různých systémů.

Uživatel musí do systému, kam se přihlašuje, nejprve zaregistrovat tzv. tajný klíč, z nějž jsou generovány OTP kódy. Tím dojde k zaregistrování (aktivaci) OTP přihlašování do daného systému.

1.3. Definice pojmů

Zkratka nebo pojem	Vysvětlení
AIS	Agendový informační systém
ASCII	American Standard Code for Information Interchange
Base32	Kódování, umožňující zakódovat binární data nebo text do textového výstupu složeného z písmen A-Z a číslic 2-7.
EXE	Executable, přípona spustitelných souborů ve Windows.
HEX	Hexadecimální (šestnáctkový) Posloupnost číslic 0-9 a znaků A-F.
HOTP	HMAC-based One-time Password algorithm
ID	Identifikátor
iOS	Operační systém pro mobilní zařízení od Applu.
JIP	Jednotný identitní prostor Zabezpečené adresářové úložiště orgánů veřejné moci a jejich uživatelů

Zkratka nebo pojem	Vysvětlení
KAAS	Katalog autentizačních a autorizačních služeb Webové služby Czech POINT, provádějící autentizaci uživatelů do externích systémů.
OTP	One-Time Password Přihlašování pomocí jednorázových hesel.
PC	Personal Computer
PIN	Personal identification number
QR	Quick response
RFC	Request for comments
SHA1	Secure Hash Algorithm Hashovací funkce pro generování otisků dat
TOTP	Time-based One-time Password algorithm

1.4. Technické požadavky

Pro přihlašování pomocí OTP je potřeba si pořídit:

- specializované OTP zařízení (tzv. OTP token), nebo
- specializovanou OTP aplikaci.

Příklady kompatibilních OTP zařízení a OTP aplikací jsou uvedeny v kapitole 5.

2. Přehled běžných situací a jejich řešení

2.1. Aktivace OTP přihlašování

Co potřebuji pro aktivaci OTP přihlašování?

Potřebujete specializované hardwarové zařízení (tzv. OTP token) nebo specializovanou aplikaci pro generování jednorázových OTP kódů.

Příklady kompatibilních OTP zařízení a aplikací jsou uvedeny v kapitole 5.

Jak aktivuji OTP přihlašování?

Aktivace OTP přihlašování se provádí v aplikaci Správa dat na stránce „Můj profil". K tomu si potřebujete pořídit OTP zařízení nebo si nainstalovat OTP aplikaci a obvykle v ní vytvořit nový OTP profil. Při aktivaci OTP přihlašování ve Správě dat je potřeba zadat tajný klíč a vygenerovat dva OTP kódy.

Podrobný postup je uveden v kapitole 3.1.

Pro aktivaci OTP přihlašování potřebuji tajný klíč. Kde jej najdu?

Tajný klíč k hardwarovému zařízení by měl být uveden na přiloženém papírku.

V případě použití OTP aplikace buď tajný klíč vygeneruje sama aplikace, mnohem častěji je ale potřeba vymyslet náhodný tajný klíč a zadat jej do aplikace. V popisech jednotlivých OTP aplikací v kapitole 5 naleznete pokyny, jak tajný klíč pro danou aplikaci získáte.

V tomto dokumentu je hodně OTP aplikací, které vyžadují tajný klíč ve formátu Base32. Jak jej získám a jak jej zadám při aktivaci OTP přihlášení?

Během aktivace OTP přihlašování ve Správě dat nelze zadat tajný klíč ve formátu Base32. Řešením je vymyslet si náhodný textový řetězec, což bude tajný klíč ve formátu ASCII, a tento řetězec zakódovat do formátu Base32, který se následně zadá do OTP aplikace.

Na internetu lze nalézt online nástroje pro kódování do formátu Base32. Mnohem obtížnější je nalézt důvěryhodné stránky, ze kterých lze stáhnout off-line nástroj (EXE soubor). Uživatelé Linuxu by mohli nalézt nástroj base32 ve své linuxové distribuci. *Podrobnější informace naleznete v kapitole 6.1.*

2.2. OTP přihlašování obecně

Jak probíhá OTP přihlašování?

Na přihlašovací obrazovce zadáte uživatelské jméno a heslo, vygenerujete v OTP zařízení nebo aplikaci OTP kód a ten zadáte do příslušného pole na přihlašovací stránce.

Při každém dalším přihlášení do systému musíte vygenerovat nový OTP kód. S již použitým OTP kódem se podruhé již nepřihlásíte.

Další informace jsou uvedeny v kapitole 4.

Aktivace OTP přihlašování byla úspěšná, ale nemohu se pomocí OTP přihlásit do Správy dat.

Zkontrolujte, jestli nezadáváte špatné heslo (překlep, česká/anglická klávesnice atd.).

OTP přihlašování také nemusí fungovat, protože máte ke svému účtu zaregistrován přihlašovací certifikát. V takovém případě je potřeba z vašeho účtu certifikát odstranit. Do účtu se přihlašte pomocí certifikátu a na stránce „Můj profil" smažte příslušný certifikát. Tuto operaci může za vás provést i lokální administrátor.

Co když se mi omylem podaří vygenerovat dva nebo více OTP kódů za sebou. Podaří se mi přihlásit do systému s posledním vygenerovaným OTP kódem?

Nemusíte se obávat, do aplikace se přihlásíte bez problémů.

Systém OTP přihlašování má určitou toleranci a „přeskočí" nepoužité OTP kódy. Nesmíte však vygenerovat příliš mnoho kódů (řádově desítky); tím byste se dostali mimo toleranční limit a nebyli byste přihlášeni do systému.

2.3. Konkrétní OTP aplikace

Jakou OTP aplikaci byste mi doporučili?

To záleží na tom, jaký operační systém či mobilní platformu používáte, jestli jste pokročilejší uživatel a jaké funkce od OTP aplikace očekáváte (chcete např. českou lokalizaci?). *Naše doporučení pro jednotlivé platformy naleznete v kapitole 5.5.*

Chci používat aplikaci Mobile-OTP, ale nedaří se mi úspěšně dokončit aktivaci OTP přihlašování.

Aktivaci OTP přihlašování ve Správě dat provádějte současně s generováním příslušného OTP profilu v aplikaci Mobile-OTP. Ujistěte se, že v aplikaci Mobile-OTP máte nastaveno „ASCII" a že v aplikaci Správa dat je jako formát tajného klíče nastavena rovněž hodnota „ASCII".

Aplikace Mobile-OTP umožňuje zobrazit tajný klíč u již vygenerovaného OTP profilu (položka „View Secret" po podržení prstu nad profilem). Tajný klíč je v tomto případě zobrazen v hexadecimálním formátu, takže ve Správě dat je při aktivaci OTP přihlašování potřeba ponechat přednastavený hexadecimální formát tajného klíče.

Chci používat aplikaci OTP Auth, ale nedaří se mi úspěšně dokončit aktivaci OTP přihlašování.

Aktivaci OTP přihlašování ve Správě dat provádějte současně s generováním příslušného OTP profilu v aplikaci OTP Auth. Ujistěte se, že v aplikaci OTP Auth máte nastaveno „Plaintext" a že v aplikaci Správa dat je jako formát tajného klíče nastavena hodnota „ASCII".

Aplikace OTP Auth umožňuje zobrazit tajný klíč u již vygenerovaného OTP profilu (položka „Show secret" v editaci profilu), ale tajný klíč je zobrazen ve formátu Base32, takže jej nelze přímo použít pro aktivaci OTP přihlašování ve Správě dat.

2.4. Deaktivace OTP přihlašování

Jak zruším OTP přihlašování?

Zrušení OTP přihlašování se provádí v aplikaci Správa dat a vyžaduje zadání hesla a jednoho OTP kódu.

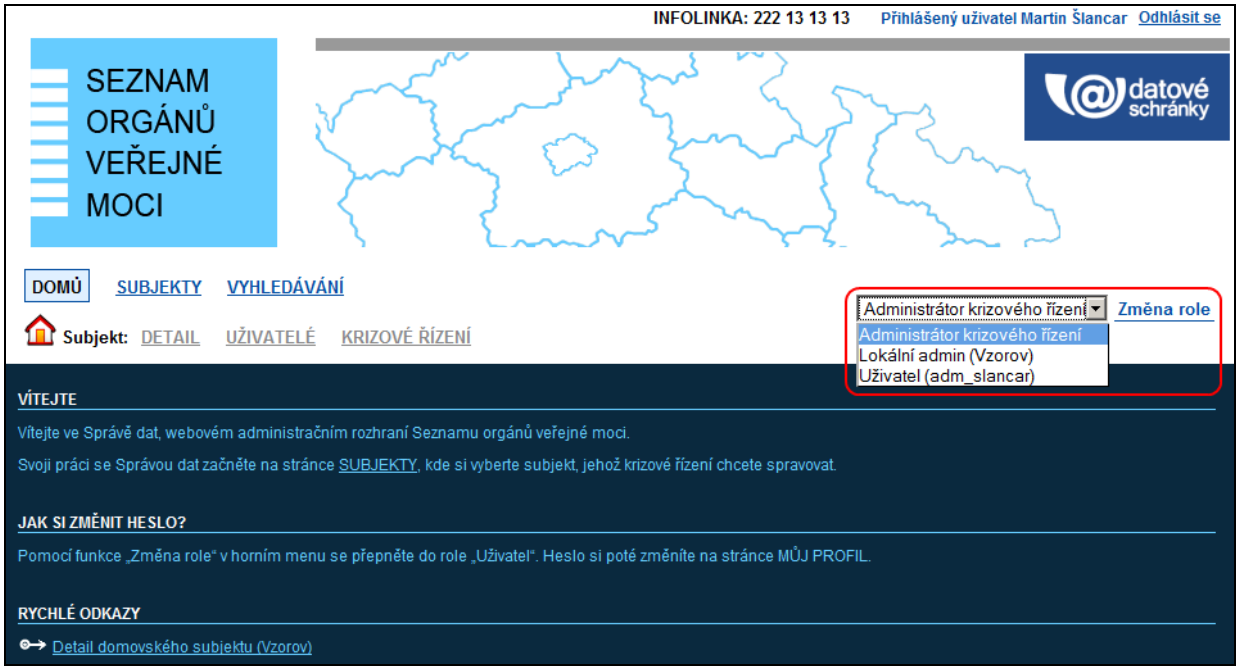
Podrobný postup je uveden v kapitole 3.3.

3. Nastavení OTP přihlašování

3.1. Aktivace OTP přihlašování – registrace OTP zařízení nebo aplikace

Přihlaste se do aplikace Správa dat na adrese: https://www.czechpoint.cz/spravadat/

Pokud vidíte v pravé části horního menu vysouvací seznam s odkazem „Změna role" (viz obrázek níže), vyberte na tomto seznamu roli „Uživatel" a klikněte na odkaz „Změna role":

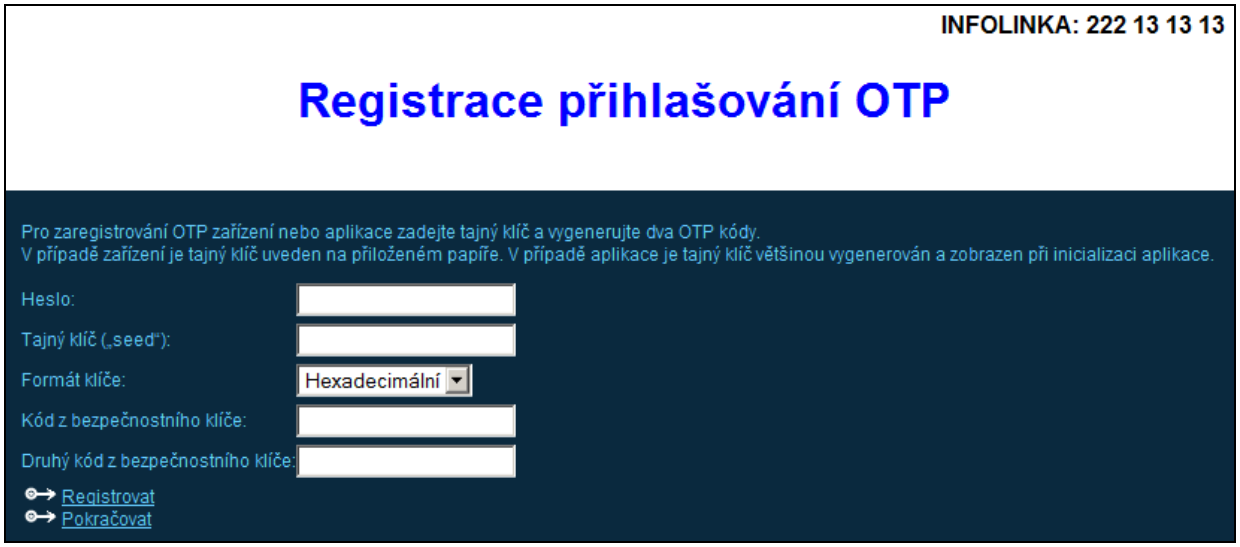


Správa dat se přepne do rozhraní pro běžného uživatele:

V horním menu klikněte na položku „Můj profil". Zobrazí se detail vašeho účtu:

Klikněte na odkaz „Upravit" v řádku „OTP autentizace".

Zobrazí se následující webová stránka pro registraci OTP zařízení nebo aplikace:



Do prvního pole „Heslo" zadejte heslo, kterým jste se přihlásili do Správy dat.

Do druhého pole „Tajný klíč (seed)" zadejte tajný klíč, který je přiložen k OTP zařízení, nebo který jste vygenerovali pro/v OTP aplikaci.

Ve třetím poli „Formát klíče" nastavte formát zadaného tajného klíče. Správa dat podporuje aktuálně pouze hexadecimální formát (v klíči se vyskytují pouze číslice 0-9 a písmena ABCDEF) nebo ASCII formát. Klíče v jiném formátu je zapotřebí zkonvertovat do některého z podporovaných formátů.

Dále postupně vygenerujte na OTP zařízení či aplikaci dva OTP kódy a zadejte je do zbývajících polí.

Klikněte na odkaz „Registrovat". Dojde k zaregistrování OTP zařízení nebo OTP aplikace.

Tímto je OTP přihlašování aktivováno.

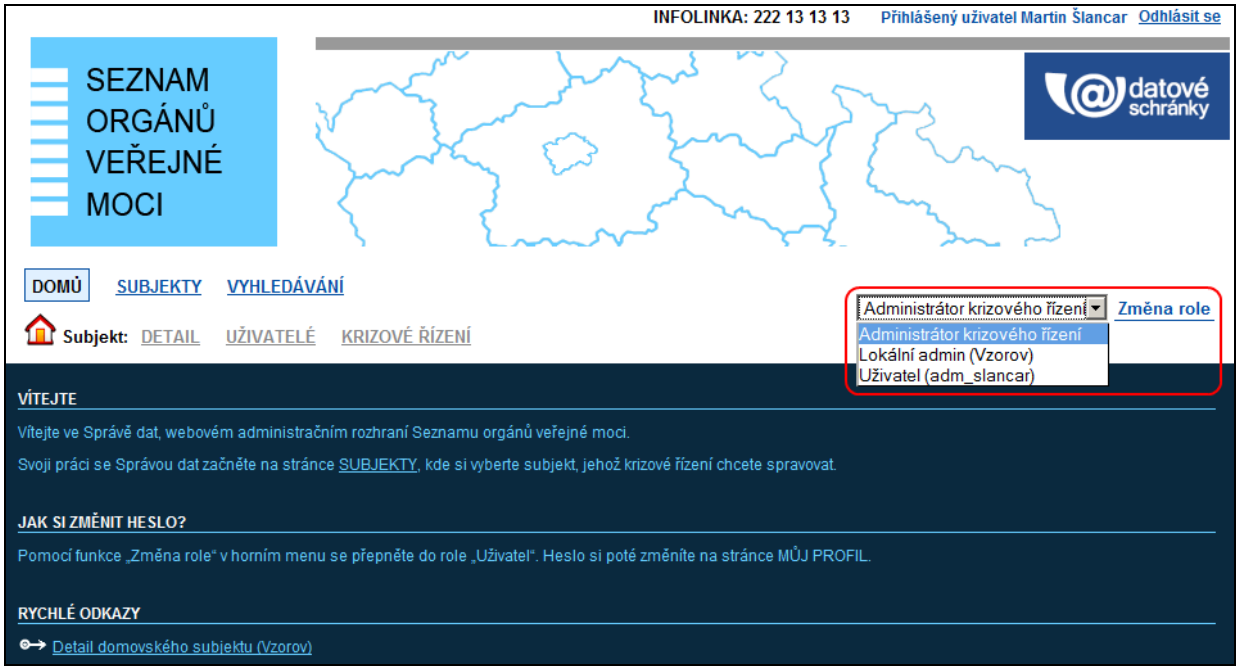
3.2. Registrace nového OTP zařízení nebo aplikace

Nejprve odregistrujte stávající OTP zařízení nebo aplikaci podle postupu v kapitole 3.3. Poté proveďte registraci nového OTP zařízení nebo aplikace podle postupu v kapitole 3.1.

3.3. Deaktivace OTP přihlašování

Přihlašte se do aplikace Správa dat na adrese: https://www.czechpoint.cz/spravadat/

Pokud vidíte v pravé části horního menu vysouvací seznam s odkazem „Změna role" (viz obrázek níže), vyberte na tomto seznamu roli „Uživatel" a klikněte na odkaz „Změna role":

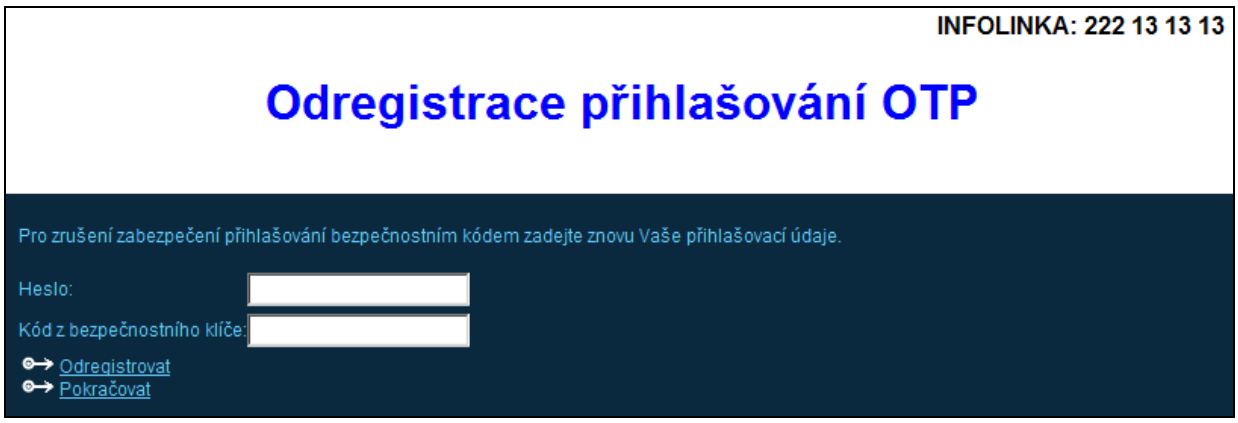


Správa dat se přepne do rozhraní pro běžného uživatele:

V horním menu klikněte na položku „Můj profil". Zobrazí se detail vašeho účtu:

Klikněte na odkaz „Upravit" v řádku „OTP autentizace".

Zobrazí se následující webová stránka pro odregistrování OTP zařízení nebo aplikace:



Do prvního pole „Heslo" zadejte heslo, kterým jste se přihlásili do Správy dat.

Dále vygenerujte na OTP zařízení či aplikaci jeden OTP kód a zadejte jej do druhého pole. Klikněte na odkaz „Odregistrovat".

Dojde k odregistrování OTP zařízení nebo OTP aplikace.

Tímto je OTP přihlašování deaktivováno.

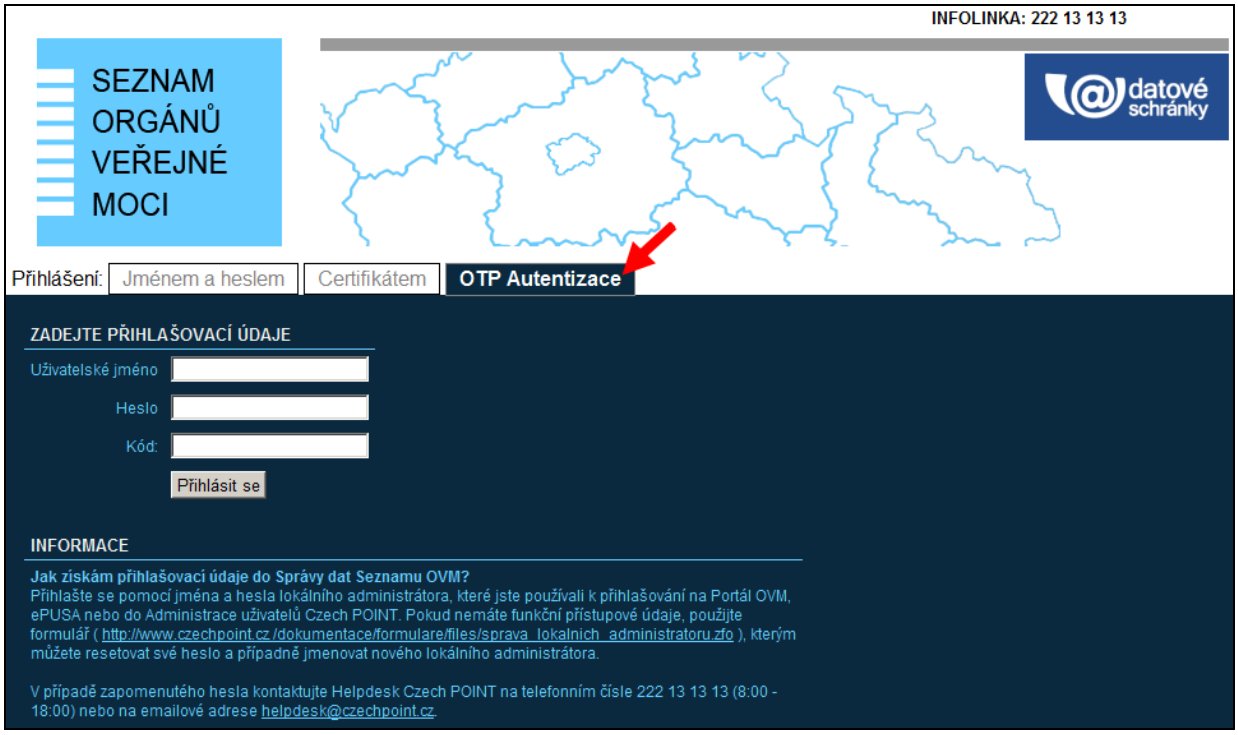
4. Přihlašování do aplikací pomocí OTP

4.1. Správa dat

Zobrazte si přihlašovací stránku aplikace Správa dat na adrese:

https://www.czechpoint.cz/spravadat/

Klikněte na záložku „OTP Autentizace“:



Do prvního pole zadejte své uživatelské jméno. Do druhého pole zadejte heslo.

Na svém OTP zařízení nebo aplikaci, které jste zaregistrovali ve Správě dat, vygenerujte číselný OTP kód. Tento kód zadáte do pole „Kód“.

Stiskněte tlačítko **Přihlásit se**.

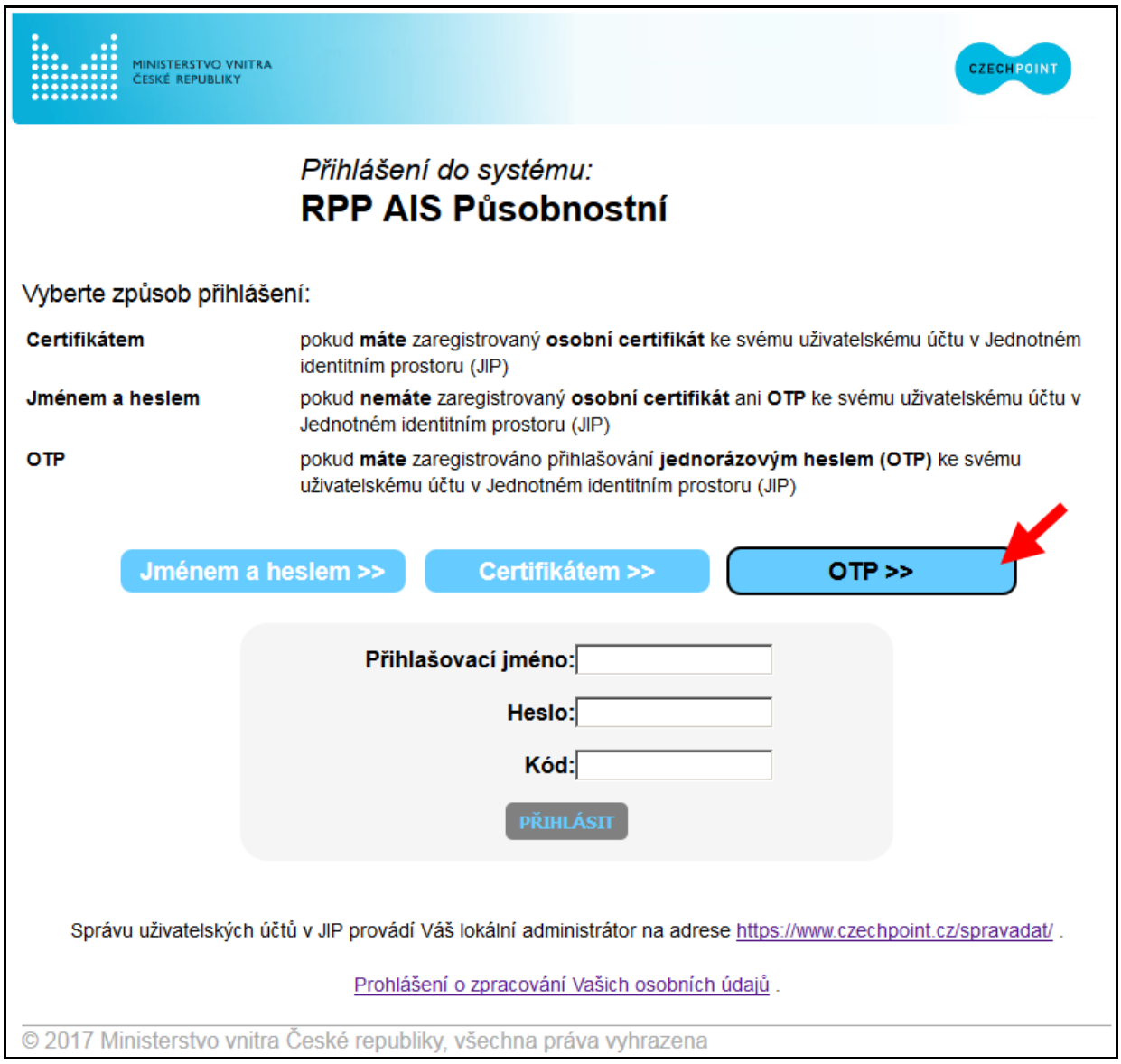
Správa dat ověří vaše přihlašovací údaje. Pokud jsou v pořádku, zobrazí se hlavní stránka Správy dat po přihlášení.

Poznámka: Při každém přihlašování do Správy dat musíte vygenerovat nový OTP kód. Nelze znovu zadat již jednou použitý kód.

Pozor: OTP přihlašování nebude fungovat, pokud máte u svého účtu zaregistrován certifikát. V takovém případě se musíte hlásit pomocí tohoto certifikátu, nebo certifikát smazat z nastavení účtu.

4.2. Přihlašování do AIS prostřednictvím JIP/KAAS

Otevřete si stránku agendového informačního systému. Budete přesměrováni na přihlašovací stránku JIP/KAAS. Klikněte na odkaz „OTP“:



Do prvního pole zadejte své uživatelské jméno. Do druhého pole zadejte heslo.

Na svém OTP zařízení nebo aplikaci, které jste zaregistrovali ve Správě dat, vygenerujte číselný OTP kód. Tento kód zadáte do pole „Kód“.

Stiskněte tlačítko **Přihlásit**.

Dojde k ověření vašich přihlašovacích údajů. Pokud jsou v pořádku, budete přesměrováni do agendového informačního systému.

Poznámka: Při každém přihlašování na přihlašovací stránce JIP/KAAS musíte vygenerovat nový OTP kód. Nelze znovu zadat již jednou použitý kód.

5. Příklady kompatibilních OTP zařízení a OTP aplikací

5.1. Obecné požadavky na OTP zařízení a OTP aplikace

Lze použít libovolné OTP zařízení nebo OTP aplikaci s podporou standardu HOTP – viz standard RFC 4226 dostupný na adrese: http://www.ietf.org/rfc/rfc4226.txt

Další nezbytné podmínky jsou tyto:

1. OTP aplikace musí být schopna ručně generovat tajné klíče, nebo uživateli dovolit je ručně zadat.
2. Tajný klíč musí mít velikost od 16 do 50 bajtů/znaků včetně.
3. Formát tajného klíče musí být hexadecimální nebo ASCII. V případě použití dodatečných nástrojů lze akceptovat i formát Base32.
4. Generovaný OTP kód musí být dlouhý 6, 7 nebo 8 znaků.

5.2. Které OTP aplikace nelze použít?

Na základě praktických zkušeností **nelze použít** takové OTP aplikace, které mají některou z těchto vlastností:

1. OTP aplikace umí vytvořit OTP profil pouze na základě naskenování QR kódu. Nedisponuje ručním vytvořením OTP profilů.
2. OTP aplikace podporuje zadání či vygenerování tajného klíče ve formátu, který aplikace Správa dat nepodporuje. Např. problematický je hojně používaný formát Base32, avšak za použití dodatečných postupů a nástrojů (viz kapitola 6.1) lze použít i takové aplikace.

5.3. Bezpečnostní doporučení pro používání OTP aplikací

Bezpečné používání OTP aplikací je postaveno na předpokladu, že neoprávněná osoba nemá k OTP aplikaci přístup (tj. nemůže vygenerovat OTP kód, nebo dokonce získat přístup k samotné databázi aplikace s uloženými tajnými klíči).

Prvním krokem zabezpečení by mělo být nastavení ochrany pro celé vaše mobilní zařízení. Zapněte odemykání zařízení pomocí alespoň číselného PIN, lepší je však použít heslo. Pro pohodlnější „přihlašování" do zařízení můžete také použít otisk prstu, rozpoznávání obličeje či jinou biometrickou metodu, pokud ji mobilní zařízení podporuje.

Druhým krokem zabezpečení by mělo být zabezpečení přístupu k samotné OTP aplikaci. Velká část testovaných OTP aplikací umožňuje či přímo vyžaduje nastavení PIN nebo hesla pro přístup do aplikace. Některé aplikace podporují také otisk prstu, pokud toto umožňuje dané mobilní zařízení.

Mezi popisovanými OTP aplikacemi jsou ale i takové aplikace, které ochranu PINem nebo heslem nemají implementovánu. V novějších verzích systému Android (patrně od verze 7) lze těmto aplikacím nastavit ochranu heslem v nastavení systému (tato funkce se může jmenovat např. „Zámek aplikace" a v nastavení ji patrně naleznete v sekci „Zabezpečení").

V systému iOS sice existuje podobná funkce „Omezení" (angl. „Restrictions"), ale takto lze uzamknout pouze aplikace vytvořené firmou Apple. Pro ochranu OTP aplikací, vytvořených jinými výrobci, ji nelze bohužel použít.

5.4. Přechod na jiný mobilní telefon

Pořídili jste si např. nový mobilní telefon a nyní řešíte, jak na něj přenést data ze starého telefonu.

Pokud vámi používaná OTP aplikace umí vytvořit zálohu, stačí zazálohovat data, v novém moblu nainstalovat stejnou aplikaci, přenést na nový mobil vytvořenou zálohu a importovat ji do OTP aplikace.

Pokud vámi používaná OTP aplikace nepodporuje zálohu dat, je jedinou možnou cestou deaktivovat OTP přihlašování pomocí OTP aplikace na starém mobilu podle postupu v kap. 3.3, nainstalovat OTP aplikaci na nový mobil, vygenerovat v ní nový OTP profil a provést aktivaci OTP přihlašování podle postupu v kap. 3.1. Pokud máte ve staré aplikaci další OTP profily pro přihlašování do jiných systémů, je potřeba takto „převést" i tyto profily.

5.5. Seznam otestovaných OTP aplikací a jakou doporučit?

Níže následují konkrétní OTP aplikace, u nichž byla otestována jejich kompatibilita se systémem Czech POINT (resp. JIP/KAAS Czech POINT). U každé popsané OTP aplikace byla vyzkoušena aktivace OTP přihlašování, přihlášení pomocí OTP do Správy dat a deaktivace OTP přihlašování.

V následujících kapitolách jsou OTP aplikace rozděleny podle jednotlivých operačních systémů (mobilních platforem) - Windows, Android a iOS. Aplikace, které jsou určeny pro Android i iOS, jsou popsány v kapitole pro Android a v kapitole pro iOS je uveden odkaz na příslušnou kapitolu s popisem aplikace.

V každé kapitole jsou aplikace seřazeny podle našeho subjektivního celkového hodnocení od nejlepší aplikace po „nejméně vhodnou" aplikaci.

Jakou OTP aplikaci si vybrat?

To samozřejmě primárně záleží na operačním systému, pro který OTP aplikaci hledáte:

Operační systém	Doporučení
Windows	Doporučujeme použít **Form Filler** (kap. 5.6.1), abyste nemuseli řešit komplikované vytváření tajných klíčů ve formátu Base32. Navíc se jedná o českou aplikaci. Bohužel však aplikace podporuje pouze jeden OTP profil. Nároční uživatelé, kteří potřebují více OTP profilů a nevadí jim složitější generování tajných klíčů v Base32 kódování, použijí aplikaci **WinAuth** (kap. 5.6.2).
Android	Doporučujeme aplikaci **Mobile-OTP** (kap. 5.7.1), abyste nemuseli řešit komplikované vytváření tajných klíčů ve formátu Base32. Aplikace ale nepodporuje zabezpečení aplikace heslem či jiným způsobem, takže byste měli aplikovat opatření doporučovaná v kapitole 5.3. Pokud vám nevadí složité vytváření klíčů ve formátu Base32, můžeme doporučit velmi povedené aplikace **Aegis Authenticator** (kap. 5.7.2) a **andOTP** (kap. 5.7.3), které obě podporují zabezpečení heslem či biometrickou metodou, zálohování dat a navíc jsou v češtině.
iOS	Doporučujeme aplikaci **OTP Auth – 2Step Auth for Pros** (kap. 5.8.1), která umožňuje roztřídit OTP profily do kategorií, podporuje zálohování a obnovu dat, ale zejména není potřeba složitě generovat tajné klíče ve formátu Base32.

5.6. OTP aplikace pro Windows

5.6.1. Software602 Form Filler

Program Form Filler je určen pro stolní počítače PC a je dostupný jen pro operační systém Windows. Počínaje verzí 4.16 byl do programu implementován generátor OTP kódů. Aplikaci lze zdarma stáhnout z webových stránek firmy Software602:

http://www.602.cz/602xml_filler/download

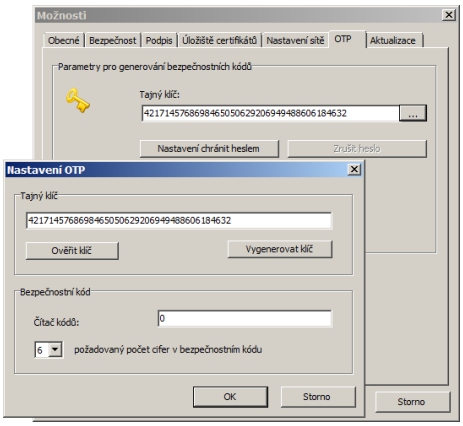
Postup pro **nastavení OTP generátoru a aktivaci OTP přihlašování ve Správě dat** je následující:

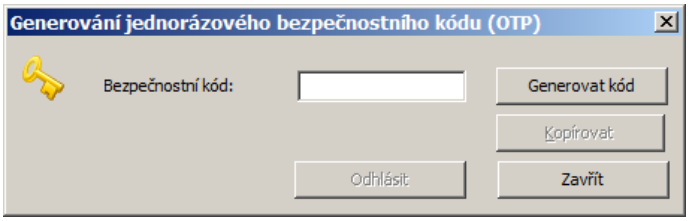
1. Program nainstalujte standardním způsobem a spusťte jej.
2. V menu „Nástroje" klikněte na ikonu  (Možnosti). Zobrazí se okno s konfigurací programu. Přepněte se na záložku OTP.
3. Zobrazí se okno s tajným klíčem.
4. Z bezpečnostních důvodů aktivujte ochranu OTP generátoru heslem. Stiskněte tlačítko **Nastavení chránit heslem** a zadejte dvakrát heslo. Dále zaškrtněte políčko „Heslo použít i pro generování kódu".
5. **Nepovinné:** Po stisknutí tlačítka **...** („tři tečky") napravo od pole s tajným klíčem se dostanete do pokročilých nastavení OTP generátoru. Zde můžete nechat vygenerovat nový tajný klíč, ručně nastavit hodnotu čítače a délku generovaných OTP kódů (6, 7, nebo 8 číslic).

   Pozor! Hodnoty v pokročilém nastavení OTP měňte pouze na začátku, kdy budete provádět aktivaci OTP přihlašování ve Správě dat. Jakmile však začnete OTP generátor používat pro přihlašování, už hodnoty v pokročilém nastavení neměňte.
6. Nyní si ve webovém prohlížeči otevřete aplikaci Správa dat a zahajte aktivaci OTP přihlašování podle postupu v kapitole 3.1. Na webové stránce „Registrace přihlašování OTP" vyplňte jednotlivá formulářová pole následovně:
   - Do pole „Heslo" zadejte heslo k vašemu uživatelskému účtu.
   - Do pole „Tajný klíč (seed)" zkopírujte obah pole „Tajný klíč" ve Form Filleru. Lze použít metodu copy&paste (CTRL+C, CTRL+V).
   - V poli „Formát klíče" ponechte přednastavenou hodnotu „Hexadecimální".
7. Nyní se vraťte do aplikace Form Filler a zavřete okno „Možnosti" stiskem tlačítka **OK**.
8. V menu „Nástroje" klikněte na ikonu  (Generovat bezpečnostní kódy).
9. V nově zobrazeném okně stiskněte tlačítko **Generovat kód**. V poli „Bezpečnostní kód" se zobrazí vygenerovaný OTP kód. Kód opište nebo zkopírujte ve Správě dat do pole „Kód z bezpečnostního klíče".
10. V aplikaci Form Filler znovu stiskněte tlačítko **Generovat kód**. V poli „Bezpečnostní kód" se zobrazí vygenerovaný OTP kód. Kód opište nebo zkopírujte ve Správě dat do pole „Druhý kód z bezpečnostního klíče".
11. Ve Správě dat dokončete aktivaci OTP přihlašování kliknutím na odkaz „Registrovat".
12. V aplikaci Form Filler stiskněte tlačítko **Odhlásit** (lze-li je stisknout), aby program z paměti odstranil vámi zadané heslo. Zavřete okno pro generování OTP kódů stiskem tlačítka **Zavřít**.

Postup pro **vygenerování OTP** v aplikaci je následující:

1. Spusťte aplikaci Form Filler.
2. V menu „Nástroje" klikněte na ikonu (Generovat bezpečnostní kódy).
3. V nově zobrazeném okně stiskněte tlačítko **Generovat kód**. Pokud jste aktivovali ochranu heslem, budete vyzváni k zadání hesla. V poli „Bezpečnostní kód" se zobrazí vygenerovaný OTP kód.
4. Pokud již nechcete generovat další OTP kód, ale chcete dále pracovat v aplikaci Form Filler, z bezpečnostních důvodů stiskněte tlačítko **Odhlásit**, aby program z paměti odstranil vámi zadané heslo.





5.6.2. WinAuth

WinAuth je open source OTP aplikace určená pro operační systémy Windows a ke svému chodu vyžaduje běhové prostředí .NET Framework 4.5. Podle všeho je ale dostupná i verze aplikace, které postačuje .NET Framework 3.5. Aplikace WinAuth je dodávána v ZIP balíčku, není tedy potřeba nic instalovat. Aplikaci lze zdarma stáhnout z webové stránky:

https://winauth.github.io/winauth/index.html

Aplikace podporuje vytváření více profilů, export a import dat a lze nastavit ochranu aplikace heslem.

Tato aplikace vyžaduje zadání tajného klíče ve formátu Base32 (podle RFC 4648). Proveďte postup v kapitole 6.1, abyste získali tajný klíč ve formátu Base32 pro OTP aplikaci a ve formátu ASCII pro aplikaci Správa dat.

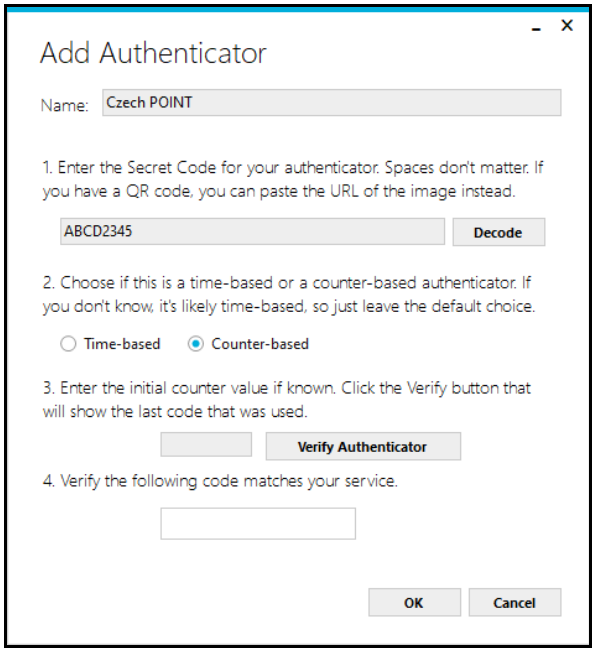
Při **prvním spuštění aplikace** je zobrazen informativní text s doporučeními jak používat aplikaci. Po stisku tlačítka **OK** se zobrazí hlavní okno aplikace.

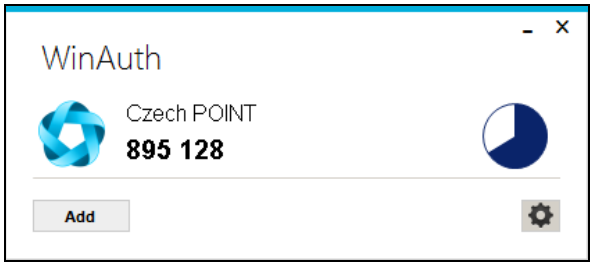
Postup pro **vygenerování OTP profilu** v aplikaci **a aktivaci OTP přihlašování ve Správě dat** je následující:

1. V hlavním okně aplikace stiskněte tlačítko **Add**. Zobrazí se nabídka, v níž vyberte první položku „Authenticator".
2. Zobrazí se nové okno „Add Authenticator", ve kterém vyplníte jednotlivá pole následovně:
   - Do pole „Name" zadejte libovolný název OTP profilu, který např. nějakým způsobem charakterizuje váš účet. Z bezpečnostních důvodů není vhodné zadávat přímo uživatelské jméno účtu.
   - Do pole pod textem „1. Enter the Secret Code..." zadejte tajný klíč v kódování Base32.
   - Do pole pod textem „2. Choose if this is a time-based..." nastavte hodnotu „Counter-based".

3. Stiskněte tlačítko **OK**. V poli pod textem „4. Verify...“ se zobrazí první vygenerovaný OTP kód. Nyní jej můžete ignorovat a znovu stisknout tlačítko **OK**.
4. Pokud jste vygenerovali první OTP profil, zobrazí se nové okno „Protection“, ve kterém si zvolíte způsob ochrany aplikace WinAuth. Ponechte zaškrtnutou první volbu „Protect with my own password“ a zadejte dvakrát heslo do polí „Password“ a „Verify“. Toto heslo bude následně zadávat při každém spuštění aplikace WinAuth. Nakonec stiskněte tlačítko **OK**.
5. Zobrazí se hlavní obrazovka aplikace WinAuth s vytvořeným OTP profilem.
6. Nyní si ve webovém prohlížeči otevřete aplikaci Správa dat a zahajte aktivaci OTP přihlašování podle postupu v kapitole 3.1. Na webové stránce „Registrace přihlašování OTP“ vyplňte jednotlivá formulářová pole následovně:
   - Do pole „Heslo“ zadejte heslo k vašemu uživatelskému účtu.
   - Do pole „Tajný klíč (seed)“ zadejte tajný klíč ve formátu ASCII. **Musíte přitom dodržet velikost písmen!**
   - **Důležité: V poli „Formát klíče“ nastavte hodnotu „ASCII“.**
7. Vraťte se do aplikace WinAuth a klikněte na ikonu kulaté šipky v pravé části OTP profilu. Dojde k zobrazení OTP kódu, který ve Správě dat opište do pole „Kód z bezpečnostního klíče“.
8. V aplikaci WinAuth budete pravděpodobně muset počkat, až v pravé části OTP profilu zmizí kulatý časovač a místo něj se opět zobrazí ikona kulaté šipky. Klikněte na ni. Dojde k zobrazení dalšího OTP kódu, který ve Správě dat opište do pole „Druhý kód z bezpečnostního klíče“.
9. Ve Správě dat dokončete aktivaci OTP přihlašování kliknutím na odkaz „Registrovat“.

Vygenerování OTP kódu v aplikaci provedete kliknutím na ikonu kulaté šipky v pravé části příslušného OTP tokenu. Zobrazí se OTP kód a místo ikony s kulatou šipkou se zobrazí časovač (modrý kruh; viz ilustrační obrázek níže), po jehož uplynutí zobrazený číselný kód zmizí. Nový OTP kód je možné vygenerovat až poté, co uplyne zobrazený časovač.





5.7. OTP aplikace pro Android

5.7.1. Mobile-OTP (Android)

Tato OTP aplikace je určena pro chytré telefony se systémem Android. Lze ji zdarma stáhnout z obchodu Google Play vyhledáním textu „Mobile-OTP". Webová adresa mobilní aplikace v obchodu je tato:

https://play.google.com/store/apps/details?id=org.cry.otp&hl=en

Důležité bezpečnostní upozornění:

Přístup do aplikace není chráněn heslem ani jiným způsobem! Po spuštění aplikace lze ihned generovat OTP kódy. Doporučujeme proto při použití této aplikace aplikovat bezpečnostní doporučení uvedená v kapitole 5.3.

Postup pro **nastavení aplikace** v mobilním zařízení **a aktivaci OTP přihlašování ve Správě dat** je následující:

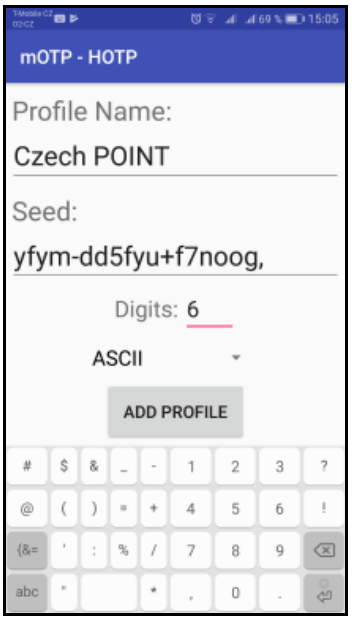
1. Mobilní aplikaci si nainstalujte z Google Play standardním způsobem a spusťte ji.
2. Zobrazí se okno pro výběr typu OTP. Zvolte HOTP.
3. V dalším okně vyplňte jednotlivá pole následovně:
   - Do pole „Profile Name" zadejte libovolný název OTP profilu. Z bezpečnostních důvodů není vhodné zadávat přímo uživatelské jméno účtu.
   - Do pole „Seed" zadejte náhodnou posloupnost znaků, která může obsahovat číslice, malá a velká písmena a další znaky (.,-+/*). Takto zadejte alespoň 16 znaků, maximálně však 50.
   - Hodnotu v poli „Digits" můžete ponechat nastavenou na 6.
   - **Další pole „Hexadecimal" ale změňte na hodnotu „ASCII"!!!!!!!**
4. Nyní si ve webovém prohlížeči otevřete aplikaci Správa dat a zahajte aktivaci OTP přihlašování podle postupu v kapitole 3.1. Na webové stránce „Registrace přihlašování OTP" vyplňte jednotlivá formulářová pole následovně:
   - Do pole „Heslo" zadejte heslo k vašemu uživatelskému účtu.
   - Do pole „Tajný klíč (seed)" zadejte stejnou posloupnost znaků, kterou jste zadali do pole „Seed" v aplikaci Mobile-OTP. **Je přitom potřeba dodržet stejnou velikost písmen!!!**
   - **Důležité: V poli „Formát klíče" nastavte hodnotu „ASCII".**
5. Nyní se vraťte do mobilní aplikace Mobile-OTP, kde stiskněte tlačítko **ADD PROFILE**.
6. Zobrazí se základní obrazovka aplikace s vygenerovaným OTP profilem.
7. Klikněte na vygenerovaný profil a stiskněte tlačítko **GENERATE KEY**. Pod tlačítkem se zobrazí číselný kód, který ve Správě dat opište do pole „Kód z bezpečnostního klíče".
8. V mobilní aplikaci znovu stiskněte tlačítko **GENERATE KEY**. Pod tlačítkem se zobrazí nový číselný kód, který ve Správě dat opište do pole „Druhý kód z bezpečnostního klíče".
9. Ve Správě dat dokončete aktivaci OTP přihlašování kliknutím na odkaz „Registrovat".

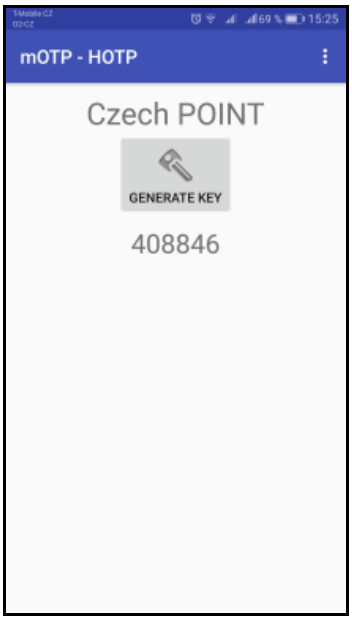
Pokud jste si v aplikaci Mobile-OTP založili OTP profil již dříve, pak **zaregistrování již existujícího OTP profilu do Správy dat** provedete pomocí následujícího postupu:

(Tento postup nemusíte provádět, pokud jste provedli registraci OTP přihlašování pomocí předchozího postupu vygenerováním nového OTP profilu v aplikaci.)

1. Spusťte si aplikaci Mobile-OTP a dlouze ťukněte na OTP profil, který chcete zaregistrovat do Správy dat. Z nabídky vyberte položku „View Secret". Zobrazí se hodnota tajného klíče.
2. Ve webovém prohlížeči si otevřete aplikaci Správa dat a zahajte aktivaci OTP přihlašování podle postupu v kapitole 3.1. Na webové stránce „Registrace přihlašování OTP" vyplňte jednotlivá formulářová pole následovně:
   - Do pole „Heslo" zadejte heslo k vašemu uživatelskému účtu.
   - Do pole „Tajný klíč (seed)" přepište hodnotu tajného klíče, která je zobrazena v aplikaci Mobile-OTP. Není potřeba dodržet velikost písmen.
   - V poli „Formát klíče" ponechte přednastavenou hodnotu „Hexadecimální".
3. Nyní se vraťte do mobilní aplikace Mobile-OTP, kde stiskněte **OK** pro zavření okna se zobrazeným tajným klíčem.
4. Klikněte na OTP profil a stiskněte tlačítko **GENERATE KEY**. Pod tlačítkem se zobrazí číselný kód, který ve Správě dat opište do pole „Kód z bezpečnostního klíče".
5. V mobilní aplikaci znovu stiskněte tlačítko **GENERATE KEY**. Pod tlačítkem se zobrazí nový číselný kód, který ve Správě dat opište do pole „Druhý kód z bezpečnostního klíče".
6. Ve Správě dat dokončete aktivaci OTP přihlašování kliknutím na odkaz „Registrovat".

Vygenerování OTP kódu v aplikaci provedete tak, že na hlavní obrazovce stisknete řádek s názvem vytvořeného tokenu. Zobrazí se nová obrazovka s tlačítkem **GENERATE KEY**. Po stisku tlačítka se pod tlačítkem zobrazí vygenerovaný OTP kód. Opětovným stiskem tlačítka se vygeneruje nový kód.





5.7.2. Aegis Authenticator (Android)

Tato OTP aplikace je určena pro chytré telefony se systémem Android. Většina textů aplikace je lokalizována do **českého jazyka** a aplikace umožňuje provést šifrovanou zálohu dat do souboru. Přístup do aplikace lze zabezpečit heslem i biometrickými metodami, které podporuje daný mobil. Dále lze přepínat mezi světlým a tmavým vzhledem či sdružovat OTP profily do skupin.

Lze ji zdarma stáhnout z obchodu Google Play vyhledáním textu „Aegis Authenticator". Webová adresa mobilní aplikace v obchodu je tato:

https://play.google.com/store/apps/details?id=com.beemdevelopment.aegis

Tato aplikace vyžaduje zadání tajného klíče ve formátu Base32 (podle RFC 4648). Proveďte postup v kapitole 6.1, abyste získali tajný klíč ve formátu Base32 pro OTP aplikaci a ve formátu ASCII pro aplikaci Správa dat.

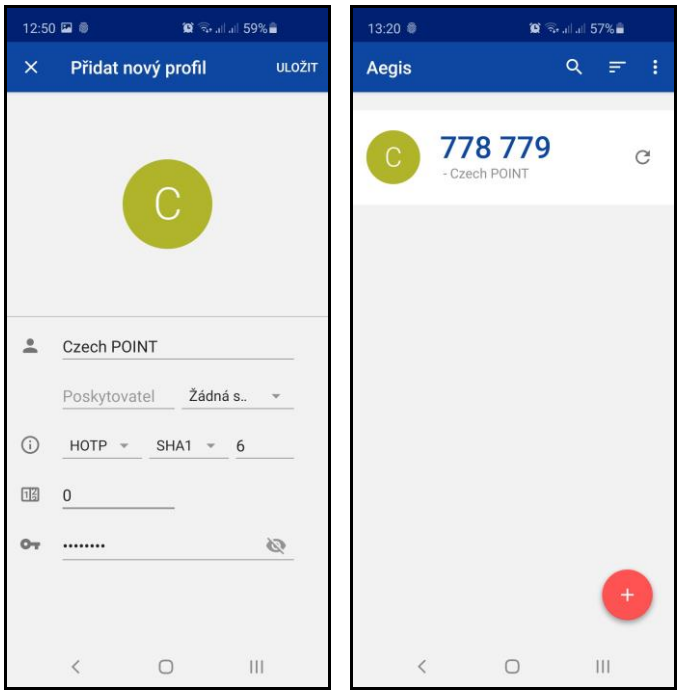
Postup pro **nastavení aplikace** v mobilním zařízení a **aktivaci OTP přihlašování ve Správě dat** je následující:

1. Mobilní aplikaci si nainstalujte z Google Play standardním způsobem a spusťte ji.
2. Při prvním spuštění aplikace se spustí průvodce, v němž si nastavíte způsob šifrování databáze aplikace (žádný, heslem, nebo pomocí biometrie). Následně si případně nastavíte přístupové heslo do aplikace a eventuálně jste vyzváni k otisku prstu. Nakonec se zobrazí hlavní obrazovka aplikace.
3. Na hlavní obrazovce aplikace stiskněte červené kulaté tlačítko „+" v pravém dolním rohu. Nad tlačítkem se zobrazí ikony pro zvolení způsobu založení OTP profilu. Zvolte ikonu „Zadat ručně".
4. V dalším okně zadáváte parametry nového OTP profilu. Vyplňte jednotlivá pole podle těchto pokynů:
   - Po ťuknutí na kulaté logo v horní části obrazovky můžete do OTP profilu přiřadit vlastní obrázek.
   - Do pole „Název" zadejte libovolný název OTP profilu, který např. nějakým způsobem charakterizuje váš účet. Z bezpečnostních důvodů není vhodné zadávat přímo uživatelské jméno účtu.
   - Pole „Poskytovatel" můžete ponechat prázdné. Napravo od tohoto pole pak můžete tento OTP profil zařadit do nějaké skupiny.
   - Ve třetím řádku nastavte v prvním poli hodnotu „HOTP". V druhém poli ponechte přednastavenou hodnotu „SHA1". Poslední pole slouží pro specifikování délky OTP kódů. Výchozí hodnotu 6 můžete změnit na 7, nebo 8.
   - Do pole „Počítadlo" zadejte číslici 0.
   - Do pole „Tajný klíč" zadejte tajný klíč v kódování Base32. Standardně se zapisovaný tajný klíč nezobrazuje, což můžete změnit ťuknutím na ikonu přeškrtnutého oka v pravé části pole.
5. Ťukněte na „Uložit" v pravém horním rohu pro vytvoření OTP profilu.
6. Zobrazí se základní obrazovka aplikace s vygenerovaným OTP profilem, ve kterém je zároveň zobrazen první vygenerovaný OTP kód (v nastavení aplikace je možné aktivovat skrývání OTP kódů pomocí volby „Zobrazit klepnutím").
7. Nyní si ve webovém prohlížeči otevřete aplikaci Správa dat a zahajte aktivaci OTP přihlašování podle postupu v kapitole 3.1. Na webové stránce „Registrace přihlašování OTP" vyplňte jednotlivá formulářová pole následovně:
   - Do pole „Heslo" zadejte heslo k vašemu uživatelskému účtu.

- Do pole „Tajný klíč (seed)" zadejte tajný klíč ve formátu ASCII. **Musíte přitom dodržet velikost písmen!**
- **Důležité: V poli „Formát klíče" nastavte hodnotu „ASCII".**

8. Z mobilní aplikace Aegis Authenticator opište zobrazený OTP kód do Správy dat do pole „Kód z bezpečnostního klíče".
9. V mobilní aplikaci ťukněte v pravé části OTP profilu na ikonu kulaté šipky. Dojde k zobrazení druhého OTP kódu, který ve Správě dat opište do pole „Druhý kód z bezpečnostního klíče".
10. Ve Správě dat dokončete aktivaci OTP přihlašování kliknutím na odkaz „Registrovat".

Vygenerování OTP kódu v aplikaci provedete tak, že na hlavní obrazovce ťuknete na ikonu kulaté šipky v pravé části příslušného OTP profilu.



5.7.3. andOTP (Android)

Tato OTP aplikace je určena pro chytré telefony se systémem Android. Nespornou výhodou této aplikace je, že je lokalizována do **českého jazyka** a umožňuje provést šifrovanou zálohu dat do souboru či využít Android sync.

Lze ji zdarma stáhnout z obchodu Google Play vyhledáním textu „andOTP". Webová adresa mobilní aplikace v obchodu je tato:

https://play.google.com/store/apps/details?id=org.shadowice.flocke.andotp&hl=en

Tato aplikace vyžaduje zadání tajného klíče ve formátu Base32 (podle RFC 4648). Proveďte postup v kapitole 6.1, abyste získali tajný klíč ve formátu Base32 pro OTP aplikaci a ve formátu ASCII pro aplikaci Správa dat.

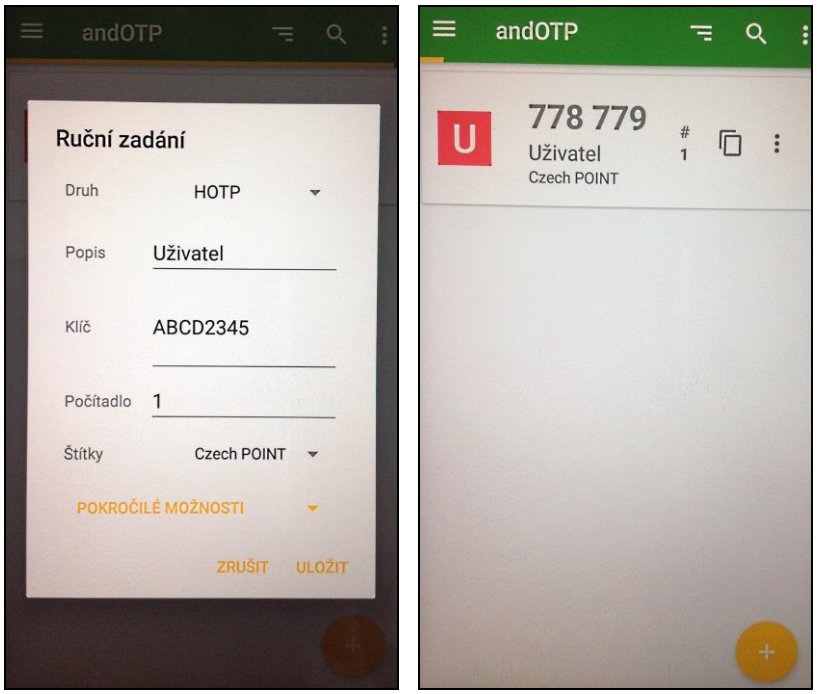
Postup pro **nastavení aplikace** v mobilním zařízení **a aktivaci OTP přihlašování** ve Správě dat je následující:

1. Mobilní aplikaci si nainstalujte z Google Play standardním způsobem a spusťte ji.
2. Při prvním spuštění aplikace se spustí průvodce, v němž si nastavíte způsob šifrování databáze aplikace buď pomocí KeyStore, nebo preferovaného PIN/hesla a následně si nastavíte přístupové heslo do aplikace. Při prvním přihlášení do aplikace

se následně ze zvoleného hesla vygeneruje šifrovací klíč a nakonec se zobrazí hlavní obrazovka aplikace.

3. Na hlavní obrazovce aplikace stiskněte žluté kulaté tlačítko „+" v pravém dolním rohu. Nad tlačítkem se zobrazí zelené ikony pro zvolení způsobu založení OTP profilu. Zvolte ikonu „Zadat detaily".
4. V dalším okně zadáváte parametry nového OTP profilu. Vyplňte jednotlivá pole podle těchto pokynů:
   - V poli „Druh" vyberte hodnotu „HOTP".
   - Pole „Vydavatel" můžete ponechat prázdné.
   - Do pole „Popis" zadejte libovolný název OTP profilu, který např. nějakým způsobem charakterizuje váš účet. Z bezpečnostních důvodů není vhodné zadávat přímo uživatelské jméno účtu.
   - Do pole „Klíč" zadejte tajný klíč v kódování Base32.
   - Pomocí pole „Štítky" můžete přidat další upřesňující text. Pomocí štítku tak lze např. k OTP profilu přidat název informačního syystému, pro který je určen.
   - V poli „Počítadlo" můžete ponechat přednastavenou hodnotu 1.
   - Dále si můžete zobrazit „Pokročilé možnosti" a v nich nastavit délku generovaných OTP kódů – zadejte číslo 6 nebo 8. Ponechte přednastavený algoritmus SHA1.
5. Ťukněte na „Uložit" pro vytvoření OTP profilu.
6. Zobrazí se základní obrazovka aplikace s vygenerovaným OTP profilem, ve kterém je zároveň zobrazen první vygenerovaný OTP kód (v nastavení aplikace je možné aktivovat skrývání OTP kódů pomocí volby „Zobraz klepnutím").
7. Nyní si ve webovém prohlížeči otevřete aplikaci Správa dat a zahajte aktivaci OTP přihlašování podle postupu v kapitole 3.1. Na webové stránce „Registrace přihlašování OTP" vyplňte jednotlivá formulářová pole následovně:
   - Do pole „Heslo" zadejte heslo k vašemu uživatelskému účtu.
   - Do pole „Tajný klíč (seed)" zadejte tajný klíč ve formátu ASCII. **Musíte přitom dodržet velikost písmen!**
   - **Důležité: V poli „Formát klíče" nastavte hodnotu „ASCII".**
8. Z mobilní aplikace andOTP opište zobrazený OTP kód do Správy dat do pole „Kód z bezpečnostního klíče".
9. V mobilní aplikaci ťukněte v OTP profilu do místa, kde se nachází znak „#". Dojde k zobrazení druhého OTP kódu, který ve Správě dat opište do pole „Druhý kód z bezpečnostního klíče".
10. Ve Správě dat dokončete aktivaci OTP přihlašování kliknutím na odkaz „Registrovat".

Vygenerování OTP kódu v aplikaci provedete tak, že na hlavní obrazovce ťuknete na řádek s názvem vytvořeného tokenu. Pozor! Je potřeba ťukat v místě, kde se nachází znak „#" a pod ním číslice. Vygeneruje se (nový) OTP kód. Opětovným ťuknutím do stejného místa se vygeneruje nový kód.



5.7.4. Authenticator Plus (Android/iOS)

Tato OTP aplikace je dostupná pro mobilní platformu Android i iOS. Je vyžadován alespoň iOS 9. Je dostupná na těchto webových adresách obchodů Google Play a Apple iTunes:

https://play.google.com/store/apps/details?id=com.mufri.authenticatorplus&hl=en

https://itunes.apple.com/app/apple-store/id963496421?mt=8

Pozor, tato aplikace je **placená**! U aplikace pro Android je zpoplatněno již její stažení a nainstalování z obchodu. Aplikaci pro iOS lze stáhnout zdarma a následně lze v aplikaci dokoupit rozšiřující funkce, jako je synchronizování dat, automatické zálohování či vytváření vlastních kategorií pro OTP profily. Pro generování OTP kódů či ruční zálohování dat ale postačí základní, bezplatná verze.

Z tohoto důvodu byla otestována jen aplikace pro iOS (konkrétně na iPadu s iOS 9).

Při **prvním spuštění aplikace** jste vyzváni k zadání hlavního hesla (master password). Dále jste informováni, jaké rozšiřující funkce můžete dokoupit.

Dále doporučujeme přejít do **nastavení aplikace** a aktivovat ochranu aplikace pomocí PIN. V levém horním rohu ťukněte na ikonu se třemi čárami pro zobrazení postranního panelu. V dolní části panelu ťukněte na položku „Settings". Dále přejděte do sekce „Security", kde zapněte přepínač „PIN lock" a zadejte nový PIN. Na této obrazovce můžete rovněž změnit PIN nebo hlavní heslo. Na zařízeních s odpovídající hardwarovou podporou zde zřejmě můžete také aktivovat ochranu aplikace pomocí otisku prstu. Sekce „Advanced" v nastavení aplikace slouží pro zálohování a obnovení dat.

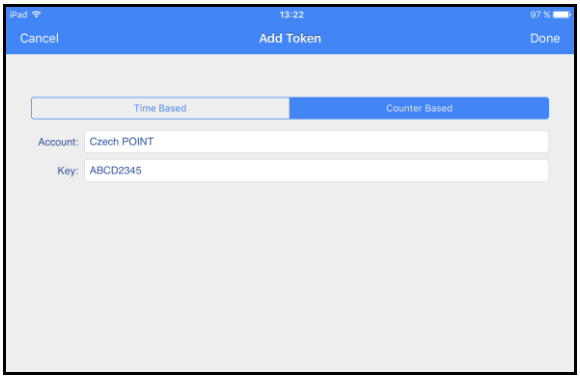
Tato aplikace vyžaduje zadání tajného klíče ve formátu Base32 (podle RFC 4648). Proveďte postup v kapitole 6.1, abyste získali tajný klíč ve formátu Base32 pro OTP aplikaci a ve formátu ASCII pro aplikaci Správa dat.

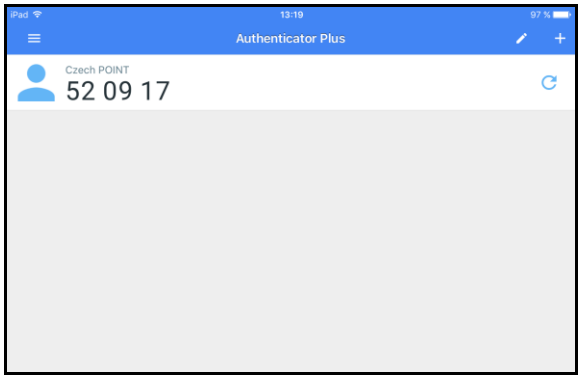
Vytvoření OTP profilu a zaregistrování OTP přihlášení ve Správě dat provedete podle následujícího postupu:

1. Na hlavní obrazovce ťukněte na ikonu „+" v pravém horním rohu.
2. Na nové obrazovce zvolte variantu „Add Manually".

3. Na další obrazovce se přepněte na záložku „Counter Based" a zobrazená pole vyplňte takto:
    - Do pole „Account" zadejte např. popisný název vašeho uživatelského účtu nebo název informačního systému, pro který hodláte používat OTP přihlašování. Z bezpečnostních důvodů není vhodné sem zadávat skutečné uživatelské jméno.
    - Do pole „Key" zadejte vygenerovaný tajný klíč v kódování Base32.
4. Ťukněte na „Done" v pravém horním rohu pro vytvoření OTP profilu.
5. Zobrazí se základní obrazovka aplikace s vygenerovaným OTP profilem.
6. Nyní si ve webovém prohlížeči otevřete aplikaci Správa dat a zahajte aktivaci OTP přihlašování podle postupu v kapitole 3.1. Na webové stránce „Registrace přihlašování OTP" vyplňte jednotlivá formulářová pole následovně:
    - Do pole „Heslo" zadejte heslo k vašemu uživatelskému účtu.
    - Do pole „Tajný klíč (seed)" zadejte tajný klíč ve formátu ASCII. **Musíte přitom dodržet velikost písmen!**
    - **Důležité: V poli „Formát klíče" nastavte hodnotu „ASCII".**
7. V mobilní aplikaci Authenticator Plus nyní v pravé části vygenerovaného OTP profilu ťukněte na symbol kruhové šipky. Zobrazí se OTP kód, který ve Správě dat opište do pole „Kód z bezpečnostního klíče".
8. V mobilní aplikaci znovu ťukněte na symbol kruhové šipky pro vygenerování druhého OTP kódu. Ten ve Správě dat opište do pole „Druhý kód z bezpečnostního klíče".
9. Ve Správě dat dokončete aktivaci OTP přihlašování kliknutím na odkaz „Registrovat".

Vygenerování OTP kódu v aplikaci provedete kliknutím na ikonu se symbolem kruhové šipky, která se nachází v pravé části příslušného řádku představujícího daný OTP profil. Zobrazí se nový vygenerovaný OTP kód.





5.7.5. Google Authenticator (Android/iOS)

Jedná se o jednoduchou OTP aplikaci pro chytré telefony se systémem Android a iOS. Výhodou této aplikace je, že je lokalizována do **českého jazyka**.

Lze ji zdarma stáhnout z obchodů Google Play a Apple iTunes vyhledáním textu „Google Authenticator". Webové adresy mobilní aplikace v obchodech jsou tyto:

https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=en

https://itunes.apple.com/us/app/google-authenticator/id388497605?mt=8

Důležité bezpečnostní upozornění:

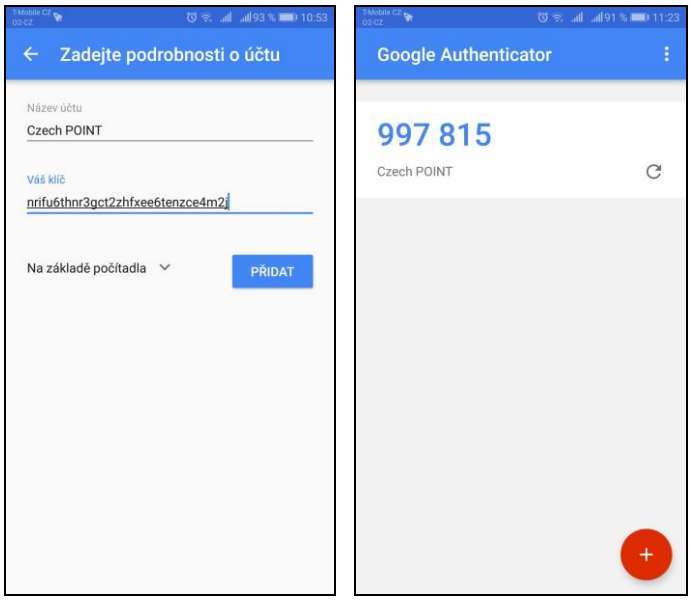
Přístup do aplikace není chráněn heslem ani jiným způsobem! Po spuštění aplikace lze ihned generovat OTP kódy. Doporučujeme proto při použití této aplikace aplikovat bezpečnostní doporučení uvedená v kapitole 5.3.

Tato aplikace vyžaduje zadání tajného klíče ve formátu Base32 (podle RFC 4648). Proveďte postup v kapitole 6.1, abyste získali tajný klíč ve formátu Base32 pro OTP aplikaci a ve formátu ASCII pro aplikaci Správa dat.

Postup pro **nastavení aplikace** v mobilním zařízení **a zaregistrování OTP přihlášení ve Správě dat** je následující:

1. Mobilní aplikaci nainstalujte standardním způsobem a spusťte ji.
2. Při prvním spuštění se spustí průvodce, který vás seznámí s účelem použití aplikace. Na konci průvodce se zobrazí obrazovka „Přidání účtu", ve které ťukněte na „Zadat dodaný klíč".
3. Zobrazí se nová obrazovka, ve které se zadávají parametry nového OTP profilu. Jednotlivé položky vyplňte následovně:
    - Do pole „Název účtu" zadejte název profilu. Můžete sem zadat např. název informačního systému. Z bezpečnostních důvodů není vhodné zadávat skutečné uživatelské jméno.
    - Do druhého pole „Váš klíč" zadejte vygenerovaný tajný klíč v kódování Base32.
    - Ve třetím poli vyberte hodnotu „Na základě počítadla".
4. Nakonec stiskněte tlačítko **PŘIDAT**.
5. Zobrazí se hlavní obrazovka aplikace s vygenerovaným OTP profilem.
6. Nyní si ve webovém prohlížeči otevřete aplikaci Správa dat a zahajte aktivaci OTP přihlašování podle postupu v kapitole 3.1. Na webové stránce „Registrace přihlašování OTP" vyplňte jednotlivá formulářová pole následovně:
    - Do pole „Heslo" zadejte heslo k vašemu uživatelskému účtu.
    - Do pole „Tajný klíč (seed)" zadejte tajný klíč ve formátu ASCII. **Musíte přitom dodržet velikost písmen!**
    - **Důležité: V poli „Formát klíče" nastavte hodnotu „ASCII".**
7. V mobilní aplikaci Google Authenticator nyní ťukněte na vygenerovaný OTP profil. Zobrazí se OTP kód, který ve Správě dat opište do pole „Kód z bezpečnostního klíče".
8. V mobilní aplikaci znovu ťukněte na OTP profil pro vygenerování druhého OTP kódu. Ten ve Správě dat opište do pole „Druhý kód z bezpečnostního klíče".
9. Ve Správě dat dokončete aktivaci OTP přihlašování kliknutím na odkaz „Registrovat".

Vygenerování OTP kódu v aplikaci provedete tak, že na hlavní obrazovce ťuknete na řádek s vytvořeným OTP profilem. Zobrazí se vygenerovaný OTP kód. Na pravé straně OTP profilu se nachází symbol kruhové šipky. Po ťuknutí na profil pro vygenerování OTP kódu tato ikona zešedne a je potřeba počkat, až opět zmodrá, aby bylo možné opětovným ťuknutím na OTP profil vygenerovat další OTP kód.



5.7.6. FreeOTP (Android/iOS)

Tato OTP aplikace je určena pro chytré telefony se systémem Android a iOS. Lze ji zdarma stáhnout z obchodů Google Play a Apple iTunes vyhledáním textu „FreeOTP". Webové adresy mobilní aplikace v obchodech jsou tyto:

https://play.google.com/store/apps/details?id=org.fedorahosted.freeotp&hl=en

https://itunes.apple.com/cz/app/freeotp-authenticator/id872559395?mt=8

Důležité bezpečnostní upozornění:

Přístup do aplikace není chráněn heslem ani jiným způsobem! Po spuštění aplikace lze ihned generovat OTP kódy. Doporučujeme proto při použití této aplikace aplikovat bezpečnostní doporučení uvedená v kapitole 5.3.

Tato aplikace vyžaduje zadání tajného klíče ve formátu Base32 (podle RFC 4648). Proveďte postup v kapitole 6.1, abyste získali tajný klíč ve formátu Base32 pro OTP aplikaci a ve formátu ASCII pro aplikaci Správa dat.

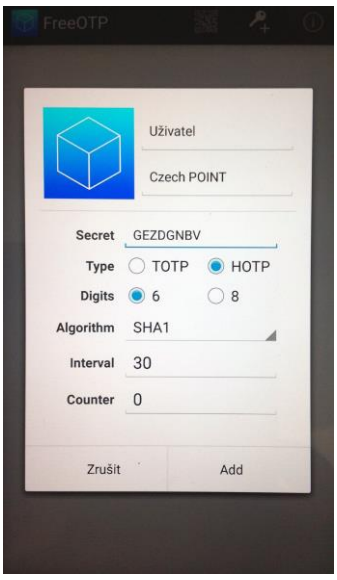
Postup pro **nastavení aplikace** v mobilním zařízení **a zaregistrování OTP přihlášení ve Správě dat** je následující:

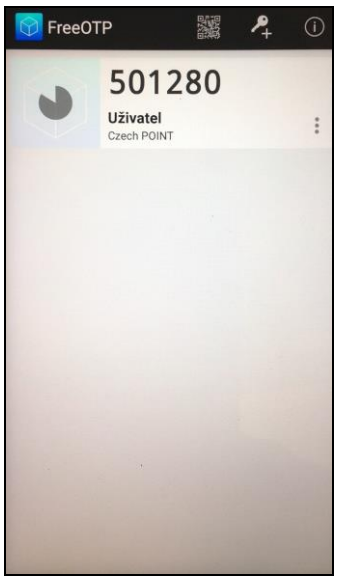
1. Mobilní aplikaci nainstalujte standardním způsobem a spusťte ji.
2. Může se zobrazit výzva pro povolení oprávnění „Fotoaparát" a „Úložiště" mobilní aplikaci. Odsouhlaste povolení těchto oprávnění.
3. Zobrazí se hlavní obrazovka aplikace. Na novějších verzích Androidu se může zobrazit upozornění, že aplikace byla vytvořena pro starší verzi Androidu. Nenarazili jsme však na žádné problémy při používání aplikace.
4. Vytvoření nového OTP profilu zahájíte ťuknutím na ikonu klíčku se znakem + (u verze pro iPad byla pouze ikona +).
5. V dalším okně zadejte parametry nového OTP profilu.
   - Ťuknutím na obrázek můžete nahradit výchozí ikonu některou vaší fotografií.
   - Do prvního pole s ukázkovou e-mailovou adresou „jdoe@example.com" zadejte popisný název vašeho uživatelského účtu, pro který hodláte používat OTP přihlašování. Z bezpečnostních důvodů není vhodné sem zadávat skutečné uživatelské jméno.

- Do druhého pole s posloupností písmen a číslic zadejte např. název informačního systému, ke kterému se budete pomocí OTP přihlašovat.
- Do pole „Secret" zadejte vygenerovaný tajný klíč v kódování Base32.
- Pole „Type" nastavte na hodnotu „HOTP".
- Pole „Digits" určuje délku generovaných OTP kódů. Podle vašich preferencí zvolte délku 6 nebo 8 číslic.
- Pole „Algorithm" ponechte na hodnotě „SHA1".

6. Nakonec stiskněte tlačítko **Add** pro vytvoření OTP profilu.
7. Zobrazí se opět hlavní obrazovka aplikace s vygenerovaným OTP profilem.
8. Nyní si ve webovém prohlížeči otevřete aplikaci Správa dat a zahajte aktivaci OTP přihlašování podle postupu v kapitole 3.1. Na webové stránce „Registrace přihlašování OTP" vyplňte jednotlivá formulářová pole následovně:
   - Do pole „Heslo" zadejte heslo k vašemu uživatelskému účtu.
   - Do pole „Tajný klíč (seed)" zadejte tajný klíč ve formátu ASCII. **Musíte přitom dodržet velikost písmen!**
   - **Důležité: V poli „Formát klíče" nastavte hodnotu „ASCII".**
9. V mobilní aplikaci FreeOTP nyní ťukněte na vygenerovaný OTP profil. Zobrazí se OTP kód, který ve Správě dat opište do pole „Kód z bezpečnostního klíče".
10. V mobilní aplikaci znovu ťukněte na OTP profil pro vygenerování druhého OTP kódu. Ten ve Správě dat opište do pole „Druhý kód z bezpečnostního klíče".
11. Ve Správě dat dokončete aktivaci OTP přihlašování kliknutím na odkaz „Registrovat".

Vygenerování OTP kódu v aplikaci provedete tak, že na hlavní obrazovce ťuknete na řádek s vytvořeným OTP profilem. Zobrazí se vygenerovaný OTP kód včetně kruhového časovače, po jehož uplynutí zobrazený kód zmizí. Opětovným ťuknutím na vytvořený OTP profil se vygeneruje nový kód; není přitom potřeba čekat, až zmizí aktuálně zobrazený OTP kód.





5.8. OTP aplikace pro iOS

5.8.1. OTP Auth – 2Step Auth for Pros (iOS)

Poznámka: Aplikace byla otestována na tabletu iPad s iOS 9 a telefonu iPhone s iOS 11.

Tato OTP aplikace je dostupná pro mobilní platformu iOS. Umožňuje provést zálohu dat, a to buď do iCloudu, nebo do souboru. Je dostupná na této webové adrese obchodu Apple iTunes:

https://itunes.apple.com/us/app/otp-auth-2step-auth-for-pros/id659877384?mt=8

Postup pro **nastavení aplikace** v mobilním zařízení **a zaregistrování OTP přihlášení ve Správě dat** je následující:

1. Aplikaci nainstalujte standardním způsobem a spusťte ji.
2. Stiskněte tlačítko **Start Setup** pro zahájení nastavování aplikace.
3. Budete vyzváni k zadání hesla pro ochranu OTP aplikace.
4. V dalším kroku si nastavujete způsob zabezpečení aplikace. Buď můžete aktivovat vyžadování hesla po spuštění aplikace (položka „Require on start"), nebo aplikaci zabezpečit pomocí Face ID či Touch ID, pokud dané mobilní zařízení tuto možnost podporuje.
5. Tímto je prvotní nastavení aplikace dokončeno a jste vyzváni k přihlášení do aplikace pomocí zvoleného hesla.
6. Po přihlášení do aplikace ťukněte na úvodní obrazovce na název složky, ve které chcete vytvořit nový OTP profil. Například vyberte výchozí složku „Default folder". Stisknutím ikony „+"[1] si můžete volitelně vytvořit vlastní složku.
7. Zahajte vytvoření nového OTP profilu stisknutím ikony „+"[2].
8. Zahajte vytvoření nového profilu (accountu) stisknutím ikony „+" a zvolením položky „Enter Credentials" ze zobrazené nabídky.
9. Na další obrazovce vyplňte jednotlivé údaje podle těchto pokynů:
   - Do pole „Name" zadejte název OTP profilu – např. název informačního systému, ke kterému se budete pomocí OTP přihlašovat. Z bezpečnostních důvodů není vhodné sem zadávat skutečné uživatelské jméno.
   - Pole „Issuer" můžete ponechat prázdné.
   - Do pole „Secret" zadejte náhodnou kombinaci znaků. Můžete použít malá a velká písmena, číslice a neabecední znaky (.,/*+-).Takto zadejte alespoň 16 znaků, maximálně však 50.
   - **V dalším řádku je potřeba nastavit hodnotu „Plaintext"!**
   - Nakonec vyberte možnost „Counter-based OTP".
10. Nyní si ve webovém prohlížeči otevřete aplikaci Správa dat a zahajte aktivaci OTP přihlašování podle postupu v kapitole 3.1. Na webové stránce „Registrace přihlašování OTP" vyplňte jednotlivá formulářová pole následovně:
    - Do pole „Heslo" zadejte heslo k vašemu uživatelskému účtu.

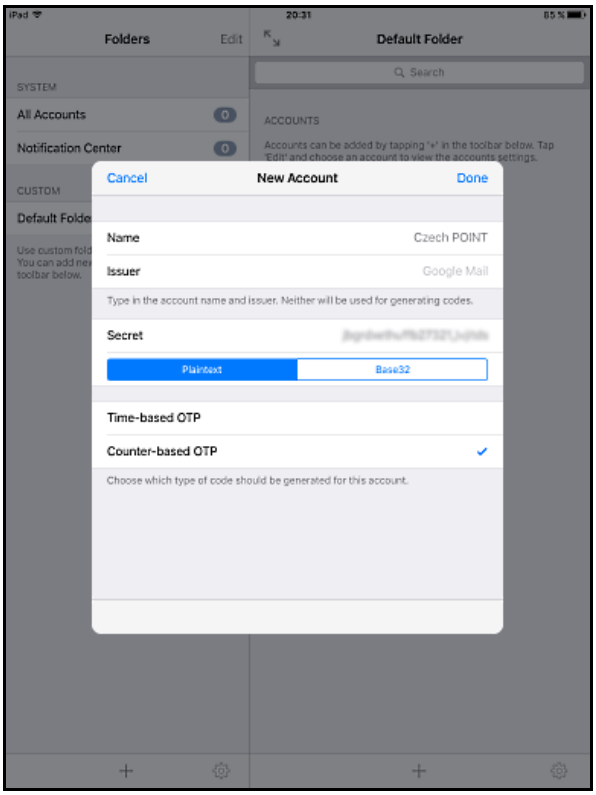
[1] Jsou-li na obrazovce zobrazeny dvě ikony „+" (zejména na tabletech a zařízeních s větší šířkou displeje), klikněte na ikonu „+" **vlevo**.

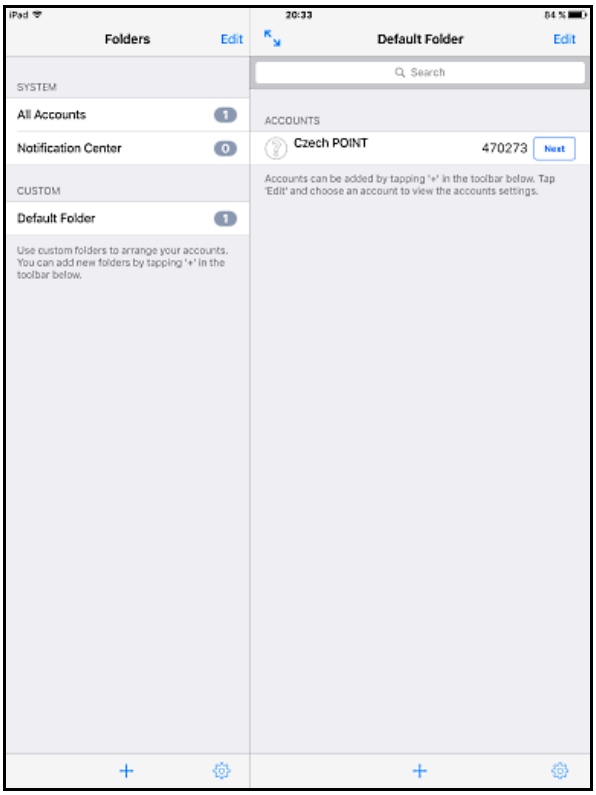
[2] Jsou-li na obrazovce zobrazeny dvě ikony „+", klikněte na ikonu „+" **vpravo**.

- Do pole „Tajný klíč (seed)" zadejte stejnou posloupnost znaků, kterou jste zadali do pole „Secret" v aplikaci OTP Auth. **Je přitom potřeba dodržet stejnou velikost písmen!!!**
- **Důležité: V poli „Formát klíče" nastavte hodnotu „ASCII".**

11. Nyní se vraťte do mobilní aplikace OTP Auth, kde ťukněte na „Done" pro vytvoření OTP profilu.
12. Zobrazí se vytvořený OTP profil, ve kterém bude zobrazen první vygenerovaný OTP kód. Tento kód opište ve Správě dat do pole „Kód z bezpečnostního klíče".
13. V mobilní aplikaci stiskněte tlačítko **Next** v OTP profilu. Zobrazí se nový číselný kód, který ve Správě dat opište do pole „Druhý kód z bezpečnostního klíče".
14. Ve Správě dat dokončete aktivaci OTP přihlašování kliknutím na odkaz „Registrovat".

Vygenerování OTP kódu v aplikaci provedete stisknutím tlačítka **Next** vedle aktuálně zobrazeného OTP kódu.





5.8.2. Authenticator Plus (Android/iOS)

Popis této aplikace naleznete v kapitole 5.7.4.

5.8.3. Google Authenticator (Android/iOS)

Popis této aplikace naleznete v kapitole 5.7.5.

5.8.4. FreeOTP (Android/iOS)

Popis této aplikace naleznete v kapitole 5.7.6.

6. Přílohy

6.1. Generování tajných klíčů ve formátu Base32

Několik popsaných OTP aplikací vyžaduje tajné klíče ve speciálním formátu Base32 podle RFC 4648. Toto kódování umožňuje převést libovolná binární data na textový řetězec složený z vybraných písmen a číslic[3].

V této kapitole naleznete postup, jak pro tyto OTP aplikace získáte požadovaný tajný klíč v Base32 formátu a jak získáte tajný klíč ve formátu ASCII, který budete zase potřebovat pro aplikaci Správa dat, protože ta formát Base32 nepodporuje.

Při přepisování tajného klíče do OTP aplikace i Správy dat je potřeba si dát pozor na správnost přepisovaných znaků. Zejména u přepisování klíče ve formátu ASCII do Správy dat je nutné dodržovat velikost písmen.

Místo přepisování klíče můžete případně využít funkci „copy&paste". Užitečné to může být zejména pro zadání klíče do Správy dat. Označíte a zkopírujete si celý klíč ve formátu ASCII (např. stiskem kláves CTRL+C) a následně jej vložíte do příslušného pole ve Správě dat (např. stiskem kláves CTRL+V).

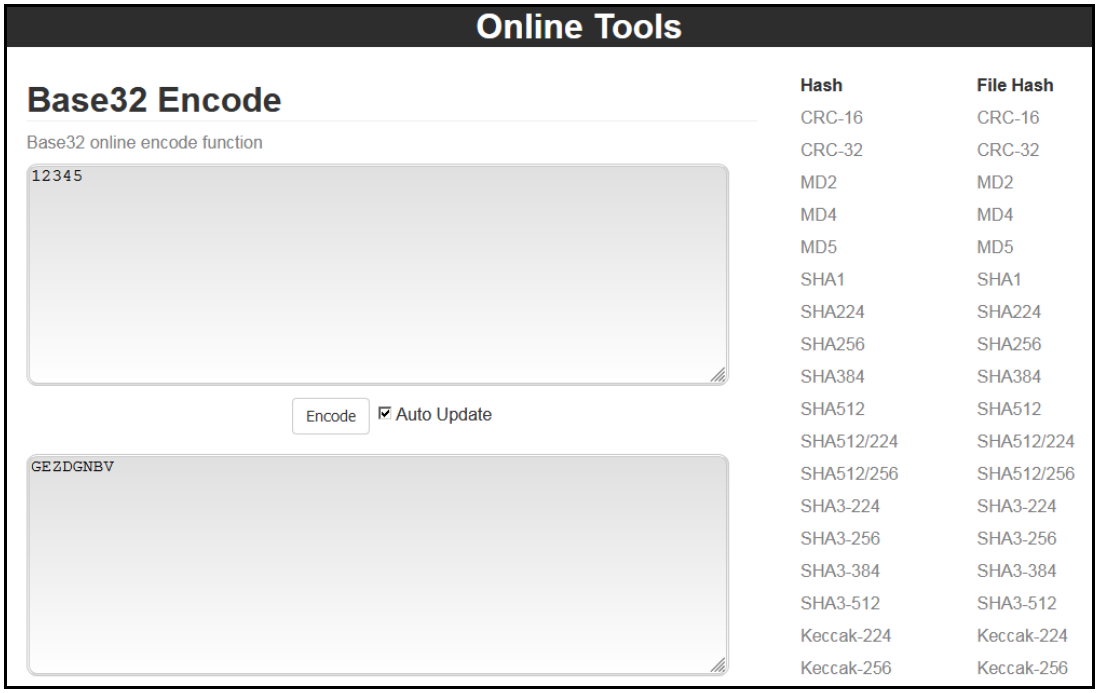
6.1.1. Jednodušší způsob vygenerování tajného klíče

Nejjednodušším způsobem je použít online nástroj pro zakódování textu do formátu Base32 („enkodér"). Tento způsob ale může představovat určité bezpečnostní riziko, protože nikdy nemůžete vědět, co webová stránka dělá s vaším zadaným textem (jestli jej např. neukládá do své databáze nebo neposílá někam jinam).

Base32 enkodér si můžete sami vyhledat pomocí internetového vyhledávače zadáním např. vyhledávacího textu (bez uvozovek): „base32 online encoder".

Lze doporučit např. tento nástroj, který generuje korektní výstupy v Base32:

https://emn178.github.io/online-tools/base32_encode.html



[3] Konkrétně jsou použita pouze velká písmena A-Z a číslice 2-7. Na konci se může případně objevit jeden či více „vyplňovacích" znaků „=".

Pozor: Google nabízí mezi prvními výsledky hledání také nástroj na stránkách „browserling". Podle našich zkušeností tento enkodér negeneruje korektní výstupy podle RFC 4648, a proto jej nelze použít.

Následující postup popisuje použití nástroje „Base32 Encode" z výše uvedené adresy. V případě použití jiného nástroje by ale měl být postup podobný:

1. Do prvního pole zadejte náhodné znaky (nepoužívejte však česká písmena). Zadejte alespoň 16 znaků a maximálně 50 znaků. Čím více znaků zadáte, tím delší budete mít výstup ve formátu Base32 a tím déle potrvá jeho přepsání do OTP aplikace.
2. Je-li zaškrtnuto políčko „Auto Update", ve druhém poli vidíte v reálném čase generovaný zakódovaný text ve formátu Base32. Jinak stiskněte tlačítko **Encode** pro zakódování textu.
3. V prvním poli máte vámi ručně zadaný náhodný text, který představuje tajný klíč ve formátu ASCII. Tento text budete zadávat v aplikaci Správa dat při aktivaci OTP přihlašování (viz kapitola 3.1).
   V druhém poli se nachází zakódovaný tajný klíč ve formátu Base32, který zadáte do OTP aplikace.

6.1.2. Složitější, ale bezpečnější způsob vygenerování tajného klíče

Jak bylo v předchozí kapitole řečeno, online nástroje pro vytvoření klíče v Base32 formátu představují určité bezpečnostní riziko, protože nemůžete vědět, co dělají s vámi zadaným vstupním textem.

Z bezpečnostního pohledu je tedy lepší použít off-line aplikaci. Nicméně ani u stažené aplikace z internetu si nemůžete být zcela jisti její bezpečností (nemůže se jednat např. o virus?). Je tedy potřeba důkladně zvažovat, za jakého zdroje aplikaci stahujete.

Jak uvidíte dále, získání a použití off-line aplikace je mnohem složitější a těžkopádnější než použití online nástroje a vyžaduje pokročilejší počítačové znalosti.

Během našeho průzkumu internetu bylo poměrně problematické najít důvěryhodné stránky nabízející ke stažení aplikaci pro kódování do Base32. Nalezli jsme tyto možnosti, jak získat Base32 aplikaci:

- soubor base32.exe z balíčku „Git for Windows Portable" (https://git-scm.com)
- soubor base32.exe ze softwaru Cygwin (https://cygwin.com); netestováno
- nástroj base32 v linuxových distribucích, patrně součást balíčku GNU Coreutils; netestováno

Ukážeme si, jak **získáte soubor base32.exe z balíčku „Git for Windows portable"**. Tato varianta má tu výhodu (např. oproti Cygwin), že si do počítače neinstalujete žádný software.

1. Z adresy https://git-scm.com/download/win si stáhněte 32-bitový nebo 64-bitový balíček „Git for Windows Portable" podle verze vašich Windows. Pozor, při načtení webové stránky se vám ihned nabídne ke stažení instalátor Git pro vaši verzi Windows. Přerušte stahování souboru a ze stránky ručně stáhněte správný soubor typu „portable".
2. Stažený soubor „PortableGit" je tzv. samorozbalovací archiv. Spusťte jej, zadejte adresář, do kterého má být extrahován obsah balíčku, a počkejte na dokončení operace extrahování souborů. Jedná se skutečně jen o vytváření souborů, ne o instalaci softwaru do Windows. Soubory odstraníte jednoduše tak, že je smažete.
3. Ve vytvořeném adresáři následně naleznete potřebný soubor „base32.exe" v adresáři „usr/bin".

Tip: Můžete ušetřit místo na disku tím, že si ponecháte jen soubor base32.exe a potřebné DLL knihovny. Vytvořte si prázdný adresář a z adresáře „usr/bin" do něj zkopírujte soubory base32.exe, msys-2.0.dll, msys-iconv-2.dll a msys-intl-8.dll. Poté můžete celý adresář „PortableGit" smazat.

Aplikaci base32.exe poté doporučujeme používat následujícím způsobem, který bude pravděpodobně stejný pro všechny výše zmíněné Base32 aplikace:

1. Vytvořte nejlépe v adresáři s aplikací base32.exe nový textový soubor s názvem např. „vstup.txt", do kterého zadejte minimálně 16 a maximálně 50 náhodných znaků. Používejte ideálně písmena, číslice a akceptovatelné jsou i speciální znaky jako ()[]{}<>@#$%&+-_/*,;!?. Nepoužívejte česká písmena. Je důležité, abyste na konci nestiskli klávesu Enter! Textový soubor vytvořte spíše v programu typu Poznámkový blok než ve Wordu, aby bylo zajištěno, že textový soubor bude obsahovat skutečně jen vámi zadaný text.
2. Po vytvoření textového souboru můžete udělat jednoduchou kontrolu, zda jste připravili soubor korektně. Velikost souboru by měla být totožná s počtem znaků, které jste do souboru zadali. Je-li velikost souboru[4] větší, patrně se v zadaných znacích nachází české nebo jiné speciální znaky, nebo jste stiskli klávesu Enter, nebo textový editor přidal do souboru nějaké znaky navíc.
3. Spusťte příkazový řádek a zadejte následující příkaz pro spuštění aplikace base32.exe:

```
cd adresář-kde-se-nachází-base32.exe

base32.exe vstup.txt >vystup.txt
```

4. Měl by se vytvořit textový soubor „vystup.txt" s nenulovou velikostí, který bude obsahovat výsledek ve formátu Base32.
5. V souboru „vstup.txt" máte uložen vámi ručně zadaný náhodný text, který představuje tajný klíč ve formátu ASCII. Tento text budete zadávat v aplikaci Správa dat při aktivaci OTP přihlašování.
   V souboru „vystup.txt" se nachází zakódovaný tajný klíč ve formátu Base32, který zadáte do OTP aplikace.

[4] V detailních informacích o souboru můžete narazit na dvě různé velikosti souboru – velikost souboru a velikost souboru na disku (toto je např. terminologie z Windows). Důležitá je velikost souboru.