



Dokumentace

k projektu Czech POINT

Příručka pro OTP přihlašování

Vytvořeno dne: 10. 5. 2012

Aktualizováno: 26. 1. 2026

Verze: 1.4

© 2012-2023 MVČR

© 2023-2026 DIA

Obsah

1.	Úvod	4
1.1.	Účel dokumentu	4
1.2.	Princip fungování OTP přihlašování.....	4
1.3.	Definice pojmů	4
1.4.	Technické požadavky	5
2.	Přehled běžných situací a jejich řešení	6
2.1.	Aktivace OTP přihlašování.....	6
	Co potřebuji pro aktivaci OTP přihlašování?	6
	Jak aktivuji OTP přihlašování?	6
	Pro aktivaci OTP přihlašování potřebuji tajný klíč. Kde jej najdu?	6
	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?	6
2.2.	OTP přihlašování obecně	6
	Jak probíhá OTP přihlašování?	6
	Aktivace OTP přihlašování byla úspěšná, ale nemohu se pomocí OTP přihlásit do Správy dat. 6	
	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?	7
2.3.	Konkrétní OTP aplikace	7
	Jakou OTP aplikaci byste mi doporučili?	7
	Chci používat aplikaci Mobile-OTP, ale nedaří se mi úspěšně dokončit aktivaci OTP přihlašování.	7
	Chci používat aplikaci OTP Auth, ale nedaří se mi úspěšně dokončit aktivaci OTP přihlašování.	7
2.4.	Deaktivace OTP přihlašování	7
	Jak zruším OTP přihlašování?	7
	Jak zruším OTP přihlašování, když už nemám příslušné OTP zařízení nebo OTP aplikaci?7	
3.	Nastavení OTP přihlašování	9
3.1.	Aktivace OTP přihlašování – registrace OTP zařízení nebo aplikace	9
3.2.	Registrace nového OTP zařízení nebo aplikace	11
3.3.	Deaktivace OTP přihlašování	12
4.	Přihlašování do aplikací pomocí OTP	15
4.1.	Správa dat.....	15
4.2.	Přihlašování do AIS prostřednictvím JIP/KAAS.....	16
5.	Příklady kompatibilních OTP zařízení a OTP aplikací.....	17
5.1.	Obecné požadavky na OTP zařízení a OTP aplikace	17
5.2.	Které OTP aplikace nelze použít?	17
5.3.	Bezpečnostní doporučení pro používání OTP aplikací	17

5.4.	Přechod na jiný mobilní telefon.....	18
5.5.	Seznam otestovaných OTP aplikací a jakou doporučit?	18
5.6.	OTP aplikace pro Windows	19
5.6.1.	Software602 Form Filler.....	19
5.6.2.	WinAuth	20
5.7.	OTP aplikace pro Android	22
5.7.1.	Mobile-OTP (Android)	22
5.7.2.	Aegis Authenticator (Android).....	24
5.7.3.	Protectimus SMART OTP (Android/iOS)	26
5.7.4.	FreeOTP (Android/iOS)	28
5.7.5.	Google Authenticator (Android/iOS)	30
5.8.	OTP aplikace pro iOS	32
5.8.1.	OTP Auth – 2Step Auth for Pros (iOS).....	32
5.8.2.	Authenticator Plus (iOS)	33
5.8.3.	Protectimus SMART (Android/iOS).....	35
5.8.4.	FreeOTP (Android/iOS)	35
5.8.5.	Google Authenticator (Android/iOS)	35
6.	Přílohy	36
6.1.	Generování tajných klíčů ve formátu Base32	36
6.1.1.	Jednodušší způsob vygenerování tajného klíče.....	36
6.1.2.	Složitější, ale bezpečnější způsob vygenerování tajného klíče	37

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 JIP/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.
DIA	Digitální a informační agentura
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.

Zkratka nebo pojem	Vysvětlení
JIP	Jednotný identitní prostor Zabezpečené adresářové úložiště orgánů veřejné moci a jejich uživatelů
KAAS	Katalog autentizačních a autorizačních služeb Webové služby Czech POINT, provádějící autentizaci uživatelů do externích systémů.
KIVS	Komunikační infrastruktura veřejné správy
MVČR	Ministerstvo vnitra České republiky
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, který zadáte do Správy dat. Tento vymyšlený textový řetězec zakódujete do formátu Base32 a zakódovaný výsledek následně zadáte do OTP aplikace.

Na internetu lze nalézt online nástroje pro zakódování textu 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 přihlášení 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.

Jak zruším OTP přihlašování, když už nemám příslušné OTP zařízení nebo OTP aplikaci?

V takovém případě požádejte lokálního administrátora, aby vašemu účtu odebral OTP přihlašování bez nutnosti zadávání OTP kódů.

Tato změna není ale zcela standardní a občas se mohou vyskytnout problémy. Pokud se stane, že se do takto pozměněného účtu nebudete moci přihlásit, požádejte o pomoc Helpdesk Czech POINT. Informujte Helpdesk Desk, že chyba vznikla při odstranění OTP přihlašování z účtu lokálním administrátorem, a požádejte Helpdesk o odstranění ostatních informací o OTP přihlašování z účtu.

Může také pomoci následující řešení: Dočasně nastavte účtu autentizační certifikát, přihlaste se do účtu pomocí tohoto certifikátu a nakonec certifikát z účtu odstraňte.

3. Nastavení OTP přihlašování

3.1. Aktivace OTP přihlašování – registrace OTP zařízení nebo aplikace

Přihlaste se do aplikace Správa dat na adrese:

Internet: <https://www.czechpoint.gov.cz/spravadat/>

KIVS: <https://www.czechpoint.cms2.cz/spravadat/>

Záložní adresa: <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“:

INFOLINKA: 222 13 13 13 Přihlášený uživatel: MARTIN ŠLANCAR [Odhlásit se](#)

SEZNAM ORGÁNŮ VEŘEJNÉ MOCI

DOMŮ SUBJEKTY VYHLEDÁVÁNÍ

Subjekt: [DETAIL](#) [UŽIVATELÉ](#) [KRIZOVÉ ŘÍZENÍ](#)

VÍTEJTE

Vítejte ve Správě dat, webovém administračním rozhraní Seznamu orgánů veřejné moci.

Svoji práci se Správou dat začněte na stránce [SUBJEKTY](#), kde si vyberte subjekt, jehož krizové řízení chcete spravovat.

JAK SI ZMĚNIT HESLO?

Pomocí funkce „Změna role“ v horním menu se přepnete do role „Uživatel“. Heslo si poté změníte na stránce MŮJ PROFIL, na záložce „Heslo“.

RYCHLÉ ODKAZY

➔ [Detail domovského subjektu \(Vzorov\)](#)

Správa dat se přepne do rozhraní pro běžného uživatele:

INFOLINKA: 222 13 13 13 Přihlášený uživatel: MARTIN ŠLANCAR [Odhlásit se](#)

SEZNAM ORGÁNŮ VEŘEJNÉ MOCI

DOMŮ MŮJ PROFIL

Vzorov:

VÍTEJTE

Vítejte ve Správě dat, webovém administračním rozhraní Seznamu orgánů veřejné moci.

Na tomto místě si můžete změnit heslo ke svému účtu nebo prohlédnout seznam povolených rolí pro přístup do externích systémů a aplikací.

RYCHLÉ ODKAZY

➔ [Detail vlastního účtu \(změna hesla\)](#)

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

DOMŮ
MŮJ PROFIL
Uživatel () Změna role

Vzorov:

CZECH POINT

Obecné
Osobní údaje
Heslo
Správa rolí
Informace o zpracování údajů § 28 z. č. 110/2019 Sb.

ÚDAJ
HODNOTA

Uživatelské jméno ? !
Titul ? Upravit
Jméno ? ! MARTIN
Příjmení ? ! ŠLANCAR
Titul ? Upravit
Fotografie ? Upravit
Blokování účtu ?
AIFO přiděleno ? ANO (CzP, SOVM)
Osoba není evidována v ROB ?
Adresa ? Upravit
Kód adresy: Dočasná adresa
Ulice:
Číslo domovní:
Číslo orientační:
Obec:
Kód obce:
Část obce:
Městská část:
PSČ:
Kraj:
E-mail ? Upravit
oficiální:
Telefony ? Upravit
Krizové telefony ? Upravit
Certifikáty ? Upravit
Typ osoby v OVM ?
Funkce ?
URL WWW ? Upravit
Předchozí zaměstnavatel ?
Osoba uvolněná ze zaměstnání ?
Veřejná osoba ?
Osoba krizového řízení ?
Poznámka ?
Číslo jednací ?
OTP autentizace ? Neaktivní Upravit

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

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

INFOLINKA: 222 13 13 13

Registrace přihlašování OTP

Pro zaregistrování OTP zařízení nebo aplikace zadejte tajný klíč a vygenerujte dva OTP kódy.
V případě zařízení je tajný klíč uveden na přiloženém papíře. V případě aplikace je tajný klíč většinou vygenerován a zobrazen při inicializaci aplikace.

Heslo:

Tajný klíč („seed“):

Formát klíče: Hexadecimální ▾

Kód z bezpečnostního klíče:

Druhý kód z bezpečnostního klíče:

➡ [Registrovat](#)
➡ [Pokračovat](#)

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 těchto dvou 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.

Poznámka: Pokud má váš účet ve Správě dat přiřazeno více rolí (např. uživatel a lokální administrátor), může se stát, že po dokončení aktivace OTP přihlašování se vám zobrazí stránka Správy dat s chybovou hláškou „Pro požadovanou akci nemáte oprávnění“. To je způsobeno tím, že se Správa dat přepnula do role s vyššími právy, která nemá oprávnění zobrazit stránku „Můj profil“. Tuto chybu můžete ignorovat.

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:

Internet: <https://www.czechpoint.gov.cz/spravadat/>

KIVS: <https://www.czechpoint.cms2.cz/spravadat/>

Záložní adresa: <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:

DOMŮ
MŮJ PROFIL
Uživatel () Změna role

Vzorov:

CZECH POINT

Obecné
Osobní údaje
Heslo
Správa rolí
Informace o zpracování údajů § 28 z. č. 110/2019 Sb.

ÚDAJ
HODNOTA

Uživatelské jméno ? !

Titul ? Upravit

Jméno ? ! MARTIN

Příjmení ? ! ŠLANCAR

Titul ? Upravit

Fotografie ? Upravit

Blokování účtu ?

AIFO přiděleno ? ANO (CzP, SOVM)

Osoba není evidována v ROB ?

Adresa ? Upravit

Kód adresy: Dočasná adresa

Ulice:

Číslo domovní: 1

Číslo orientační:

Obec: Praha

Kód obce:

Část obce:

Městská část:

PSČ:

Kraj:

E-mail ? Upravit

Telefony ? Upravit

Krizové telefony ? Upravit

Certifikáty ? Upravit

Typ osoby v OVM ?

Funkce ?

URL WWW ? Upravit

Předchozí zaměstnavatel ?

Osoba uvolněná ze zaměstnání ?

Veřejná osoba ?

Osoba krizového řízení ?

Poznámka ?

Číslo jednacích ?

OTP autentizace ? Aktivováno Upravit

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

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

INFOLINKA: 222 13 13 13

Odregistrace přihlašování OTP

Pro zrušení zabezpečení přihlašování bezpečnostním kódem zadejte znovu Vaše přihlašovací údaje.

Heslo:

Kód z bezpečnostního klíče:

[↔ Odregistrovat](#)
[↔ Pokračovat](#)

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.

Poznámka: Pokud má váš účet ve Správě dat přiřazeno více rolí (např. uživatel a lokální administrátor), může se stát, že po dokončení deaktivace OTP přihlašování se vám zobrazí stránka Správy dat s chybovou hláškou „Pro požadovanou akci nemáte oprávnění“. To je způsobeno tím, že se Správa dat přepnula do role s vyššími právy, která nemá oprávnění zobrazit stránku „Můj profil“. Tuto chybu můžete ignorovat.

Poznámka: Pokud nemůžete provést deaktivaci OTP přihlašování, protože již nedisponujete příslušným OTP zařízením či OTP aplikací, požádejte lokálního administrátora, aby vašemu účtu odebral OTP přihlašování. Pro tuto akci není potřeba generovat žádné OTP kódy.

4. Přihlašování do aplikací pomocí OTP

4.1. Správa dat

Zobrazte si přihlašovací stránku aplikace Správa dat na adrese:

Internet: <https://www.czechpoint.gov.cz/spravadat/>

KIVS: <https://www.czechpoint.cms2.cz/spravadat/>

Záložní adresa: <https://www.czechpoint.cz/spravadat/>

Klikněte na záložku „OTP Autentizace“:

INFOLINKA: 222 13 13 13

SEZNAM ORGÁNŮ VEŘEJNÉ MOCI

DATOVÉ SCHRÁNKY

Přihlášení: Jménem a heslem Certifikátem **OTP Autentizace** NIA Autentizace

ZADEJTE PŘIHLAŠOVACÍ ÚDAJE

Uživatelské jméno

Heslo

Kód:

INFORMACE

Nový uživatel JIP/KAAS
Vzhledem k narůstajícímu počtu uživatelů, kteří se potřebují přihlašovat k agendovým informačním systémům prostřednictvím JIP/KAAS, jsme připravili návod, jak provést základní nastavení účtu. Návod je určen pro úplně začátečníky. [Nový uživatelský účet v JIP/KAAS – základní nastavení](#)

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 kulaté tlačítko **OTP>>**:

Digitální a informační agentura

CZECH POINT

Přihlášení do systému:
RPP AIS Působnostní - A113

Vyberte způsob přihlášení:

Certifikátem	pokud máte zaregistrovaný osobní certifikát ke svému uživatelskému účtu v Jednotném identitním prostoru (JIP)
Jménem a heslem	pokud nemáte zaregistrovaný osobní certifikát ani OTP ke svému uživatelskému účtu v Jednotném identitním prostoru (JIP)
OTP	pokud máte zaregistrováno přihlašování jednorázovým heslem (OTP) ke svému uživatelskému účtu v Jednotném identitním prostoru (JIP)
NIA	pokud se chcete ke svému uživatelskému účtu v Jednotném identitním prostoru (JIP) přihlásit s využitím elektronické identifikace prostřednictvím národního bodu (NIA) podle zákona č. 250/2017 Sb. Váš uživatelský účet v JIP musí být ztotožněn!

Jménem a heslem >>
Certifikátem >>
OTP >>
NIA >>

Přihlašovací jméno:
Heslo:
Kód:
PŘIHLÁSIT

Provozní informace:
Dobrý den,
nedaří-li se Vám přihlášení, tak na adrese:
<https://www.dia.gov.cz/egovernment/navody-ke-stazeni/>
si můžete přečíst tři návody: "JIP_prihlaseni_...".

Správu uživatelských účtů v JIP provádí Váš lokální administrátor na adrese <https://www.czechpoint.cz/spravadat/> .
[Prohlášení o zpracování Vašich osobních údajů](#) .

© 2025 Digitální a informační agentura, všechna práva vyhrazena

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 aplikace, které používají 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 implementovány. U takových aplikací je vhodné jejich spuštění zabezpečit pomocí hesla. K tomu je zapotřebí nainstalovat aplikaci třetí strany (např. AppLock od DoMobile Lab, Norton App Lock apod.). Mobilní zařízení některých výrobců mají funkcionalitu „zamknutí“ aplikací již zabudovanou v systému. Např. Samsung má funkci „Zabezpečená složka“ (Secure Folder). Firmy Huawei, Xiaomi a další používají ve svých zařízeních funkci App Lock.

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 mobilu nainstalovat stejnou aplikaci, přenést na nový mobil vytvořenou zálohu a importovat ji do OTP aplikace.

Součástí mobilních zařízení jsou již specializované aplikace pro zkopírování/naklonování obsahu původního zařízení do nového zařízení. Pomocí těchto aplikací lze přenést kontakty, historii volání a SMS zpráv, ale také nainstalované aplikace a uložená data těchto aplikací. Můžete vyzkoušet, zda se vám pomocí této „kopírovací“ aplikace podaří přenést OTP aplikaci na nové zařízení.

Zaručeně funkčním, ale poněkud složitým (a možná i zdoluhavým) řešením je ve Správě dat deaktivovat OTP přihlašování na starém mobilu (postup je uveden v kap. 3.3), nainstalovat OTP aplikaci na nový mobil, vygenerovat v ní nový OTP profil a ve Správě dat provést novou aktivaci OTP přihlašování za použití nového mobilu (postup je uveden 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 nevdí 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 doporučená v kapitole 5.3. Pokud vám nevdí složitě vytváření klíčů ve formátu Base32, můžeme doporučit velmi povedenou aplikaci Aegis Authenticator (kap. 5.7.2), která podporuje zabezpečení heslem či biometrickou metodou, zálohování dat a navíc je v češtině.

	Bohužel prozatím nemůžeme doporučit aplikaci Google Authenticator, protože jsme během testování narazili na problémy s opětovným vygenerováním OTP kódů. Ikona pro vygenerování nového kódu nefungovala korektně.
iOS	Doporučujeme aplikaci OTP Auth – 2Step Auth for Pros (kap. 5.8.1), která umožňuje rozřadit 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

Vývojář: Software602

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

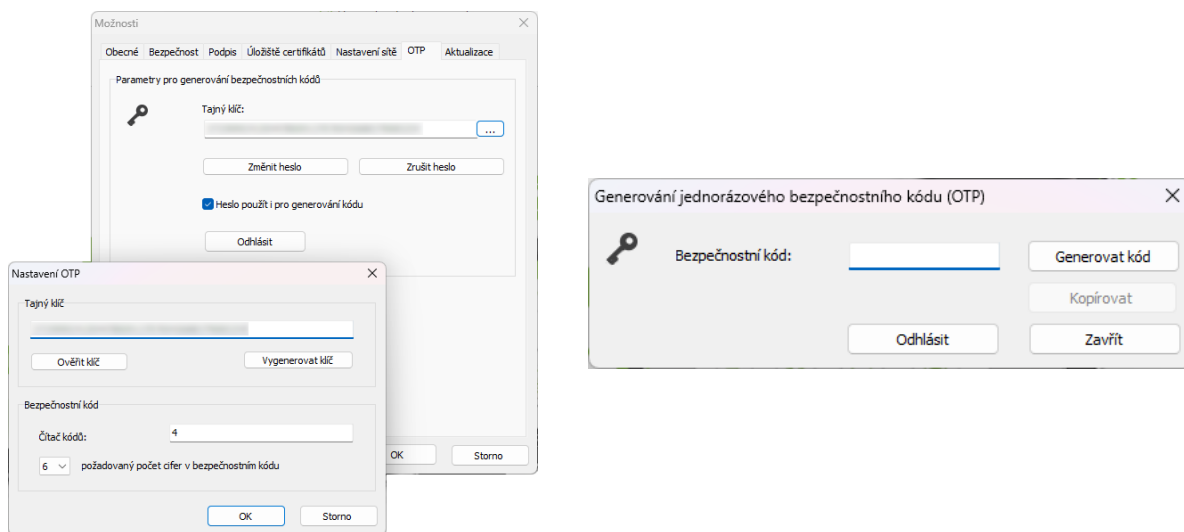
Postup pro **nastavení OTP generátoru a aktivaci OTP přihlašování ve Správě dat** je následující:

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 obsah 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. Spustíte 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

Vývojář: Colin Mackie

WinAuth je open source OTP aplikace určená pro operační systémy Windows a ke svému chodu vyžaduje běhové prostředí .NET Framework 4.5. Je 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>

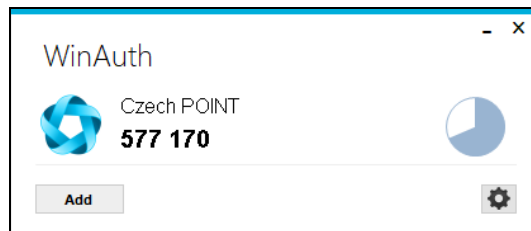
Aplikace podporuje vytváření více profilů, export a import dat a lze nastavit ochranu aplikace heslem.

Tato aplikace vyžaduje zadání tajného klíče ve formátu Base32 (podle RFC 4648). Provedte 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 **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)

Vývojář: Miceli Bros.

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=cs>

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:

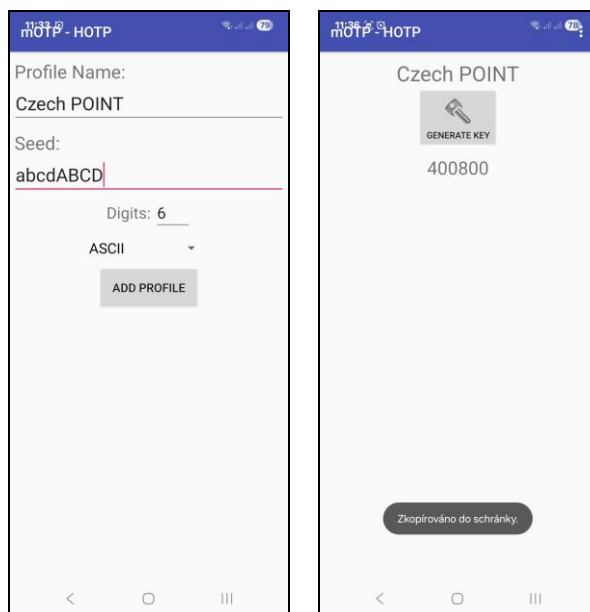
- Do pole „Heslo“ zadejte heslo k vašemu uživatelskému účtu.
 - Do pole „Tajný klíč (seed)“ zadejte stejnou posloupnost znaků, kterou jste zadali do pole „Seed“ v aplikaci Mobile-OTP. **Je přitom potřeba dodržet stejnou velikost písmen!!!**
 - **Důležité: V poli „Formát klíče“ nastavte hodnotu „ASCII“.**
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. Spustíte si aplikaci Mobile-OTP a dlouze ťuknete 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 zahajete 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)

Vývojář: Beem Development

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&hl=cs>

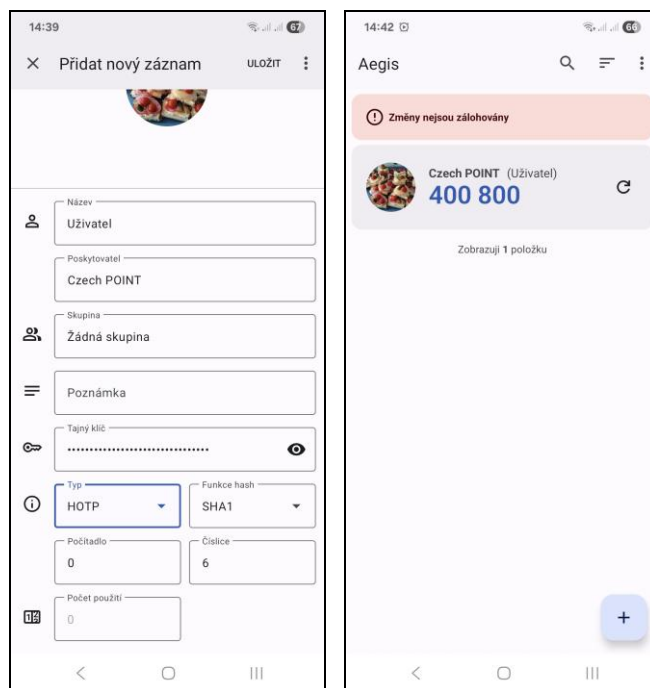
Tato aplikace vyžaduje zadání tajného klíče ve formátu Base32 (podle RFC 4648). Provedte postup v kapitole 6.1, abyste získali tajný klíč ve formátu Base32 pro OTP aplikaci a ve formátu ASCII pro aplikaci Správa dat.

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 kulaté tlačítko „+“ v pravém dolním rohu. Zobrazí se menu 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.

- V dalším poli „Skupina“ pak můžete tento OTP profil zařadit do nějaké skupiny. V dialogovém okně máte možnost vytvořit novou skupinu.
 - Čtvrté pole „Poznámka“ můžete ponechat prázdné.
 - Do pole „Tajný klíč“ zadejte tajný klíč v kódování Base32. Standardně se zapisovaný tajný klíč nezobrazuje, což můžete změnit ťuknutím na ikonu oka v pravé části pole.
 - Ťukněte na text „Pokročilé“, aby se zobrazila pole s dalšími nastaveními.
 - V poli „Typ“ nastavte hodnotu „HOTP“. V druhém poli „Funkce hash“ ponechte přednastavenou hodnotu „SHA1“.
 - Pole „Počítadlo“ ponechte na výchozí hodnotě 0. Pole „Číslice“ slouží pro specifikování délky OTP kódů. Výchozí hodnotu 6 můžete změnit na 7, nebo 8.
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. Protectimus SMART OTP (Android/iOS)

Vývojář: Protectimus Limited

Tato OTP aplikace je určena pro chytré telefony se systémem Android a iOS. Lze ji zdarma stáhnout z obchodů Google Play a Apple iTunes. V Apple obchodu se aplikace jmenuje pouze jako „Protectimus SMART“. Webové adresy mobilní aplikace v obchodech jsou tyto:

<https://play.google.com/store/apps/details?id=com.protectimus.android&hl=cs>

<https://apps.apple.com/cz/app/protectimus-smart/id854508919>

Při **prvním spuštění aplikace** je zobrazen průvodce, ve kterém si můžete zapnout zálohu OTP profilů do cloudu, vygenerovat nový OTP profil nebo importovat stávající profily z Google Authenticatoru.

Doporučujeme přejít do **nastavení aplikace** a aktivovat ochranu aplikace pomocí PIN. V pravém horním rohu ťukněte na ikonu ozubeného kola a ťukněte na položku „App Security“. Budete vyzváni k zadání PIN pro ochranu aplikace. Po zadání PIN budete dotázáni, zda má být pro ochranu aplikace použito biometrické zabezpečení, které je nastaveno v systému.

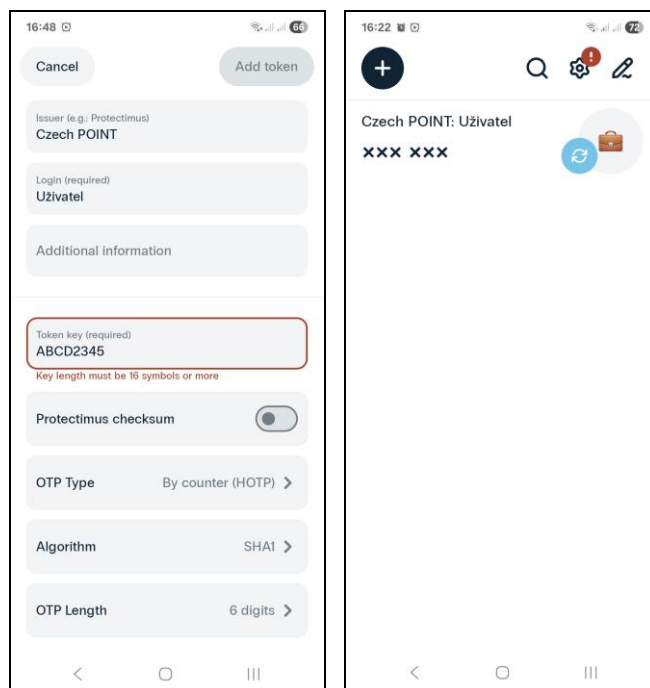
Tato aplikace vyžaduje zadání tajného klíče ve formátu Base32 (podle RFC 4648). Provedte postup v kapitole 6.1, abyste získali tajný klíč ve formátu Base32 pro OTP aplikaci a ve formátu ASCII pro aplikaci Správa dat.

Postup pro **vytvoření nového OTP profilu v aplikaci a zaregistrování OTP přihlášení ve Správě dat** je následující:

1. Spustíte aplikaci. Pokud nezahájíte vytvoření nového OTP profilu v úvodním průvodci, na hlavní obrazovce stiskněte tlačítko **Add token**. Pokud již v aplikaci máte vytvořen OTP profil, ťukněte na ikonu + v levém horním rohu aplikace.
2. Dále vyberte položku „Add token manually“.
3. V dalším okně zadejte parametry nového OTP profilu.
 - Do prvního pole „Issuer“ zadejte např. název informačního systému, ke kterému se budete pomocí OTP přihlašovat.

- Do druhého pole „Login“ zadejte popisný název vašeho uživatelského účtu, pro který hodláte používat OTP přihlašování. Z bezpečnostních důvodů není vhodné sem zadávat skutečné uživatelské jméno.
 - Třetí pole „Additional information“ můžete ignorovat.
 - Do čtvrtého pole „Token key“ zadejte vygenerovaný tajný klíč v kódování Base32. Klíč musí být dlouhý alespoň 16 znaků.
 - **V poli „Protectimus checksums“ deaktivujte přepínač!**
Pokud byste jej nechali zapnutý, aplikace by zadaný tajný klíč považovala za nevalidní.
 - Pole „OTP Type“ nastavte na hodnotu „By counter (HOTP)“.
 - V poli „Algorithm“ nastavte hodnotu SHA-1.
 - V poli „OTP Length“ si volíte délku generovaných OTP kódů. Podle vašich preferencí zvolte délku 6 nebo 8 číslic.
4. Nakonec stiskněte tlačítko **Add token** v pravé horní části okna pro pokračování na další obrazovku.
 5. Na nové obrazovce si můžete pro OTP profil vybrat ikonu a zařadit jej do určité složky. V tomto okamžiku si můžete vytvořit zcela novou složku.
 6. Zobrazí se opět hlavní obrazovka aplikace s vygenerovaným OTP profilem. Místo OTP kódu budou zobrazeny křížky.
 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. Do pole „Kód z bezpečnostního klíče“ zadejte OTP kód, který zobrazíte kliknutím na řádek s OTP profilem.
 9. V mobilní aplikaci vygenerujte nový kód ťuknutím na ikonu se dvěma zakulacenými šipkami. Ikona se nachází u zvoleného obrázku pro daný OTP profil. Zobrazený OTP kód zadejte 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 vyhledáte správný OTP profil (máte-li jich vytvořeno více) a ťuknete na ikonu se dvěma zakulacenými šipkami. Ikona se nachází blízko obrázku daného OTP profilu. Po ťuknutí na ikonu se zobrazí OTP kód a ikona zešedne. Během tohoto stavu ikona nereaguje na ťuknutí. Po chvíli ikona opět zmodrá a vy můžete na ikonu znovu ťuknout pro vygenerování nového OTP kódu.



5.7.4. FreeOTP (Android/iOS)

Vývojář: Red Hat

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=cs>

<https://apps.apple.com/cz/app/freeotp-authenticator/id872559395>

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). Provedte 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 se zobrazí úvodní informace o novinkách ve verzi 2.0 (integrace s Android úložištěm, zálohování a obnova dat). Následně zadáte vlastní heslo pro šifrování záloh dat. Toto heslo není možné později změnit!

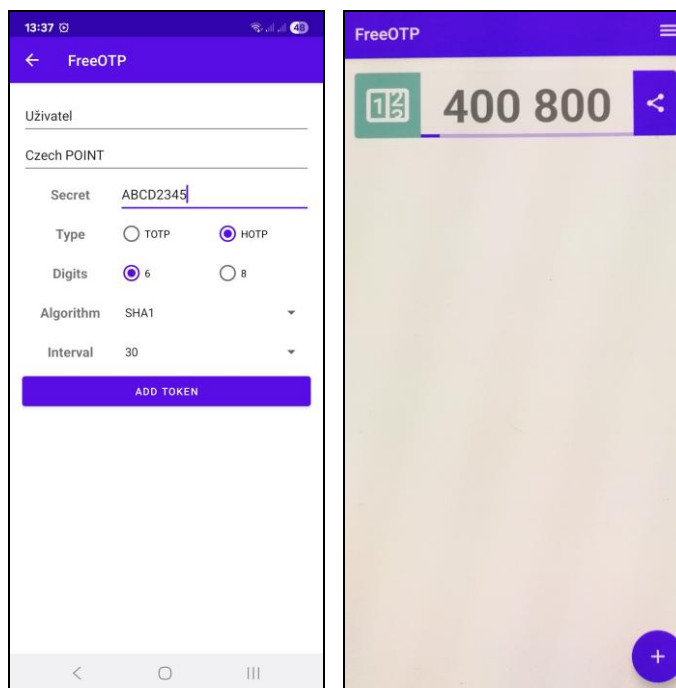
Postup pro **nastavení aplikace** v mobilním zařízení **a zaregistrování OTP přihlášení ve Správě dat** je následující:

1. Spustíte mobilní aplikaci.
2. Vytvoření nového OTP profilu zahájíte ťuknutím na ikonu + v pravém dolním rohu (u verze pro iPhone byla ikona umístěna v horním pruhu). Dále ťukněte na ikonu tužky pro ruční zadání parametrů.
3. V dalším okně zadejte parametry nového OTP profilu.
 - 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.
 - V poli „Algorithm“ nastavte hodnotu „SHA1“.
 - (Pole „Interval“ můžete ignorovat.)
4. Nakonec stiskněte tlačítko **Add Token** pro vytvoření OTP profilu.
 5. Zobrazí se opět 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 FreeOTP nyní ťukněte na řádek s vygenerovaným OTP profilem. 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 včetně časovače¹, 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.

¹ Na Androidu to byl zkracující se proužek, na iOS to byl ubývající kruh.



5.7.5. Google Authenticator (Android/iOS)

Vývojář: Google LLC

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=cs>

<https://apps.apple.com/us/app/google-authenticator/id388497605>

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.

Doporučujeme **aktivovat ochranu aplikace** pomocí zámku obrazovky (PIN, heslo, otisk prstu atd.). Při spuštění aplikace se tak budete muset ověřit stejným způsobem, jako když odemykáte telefon. V levém horním rohu klikněte na ikonu se třemi čárkami a vyberte položku „Nastavení“. Dále zapněte položku „Obrazovka s ochranou soukromí“.

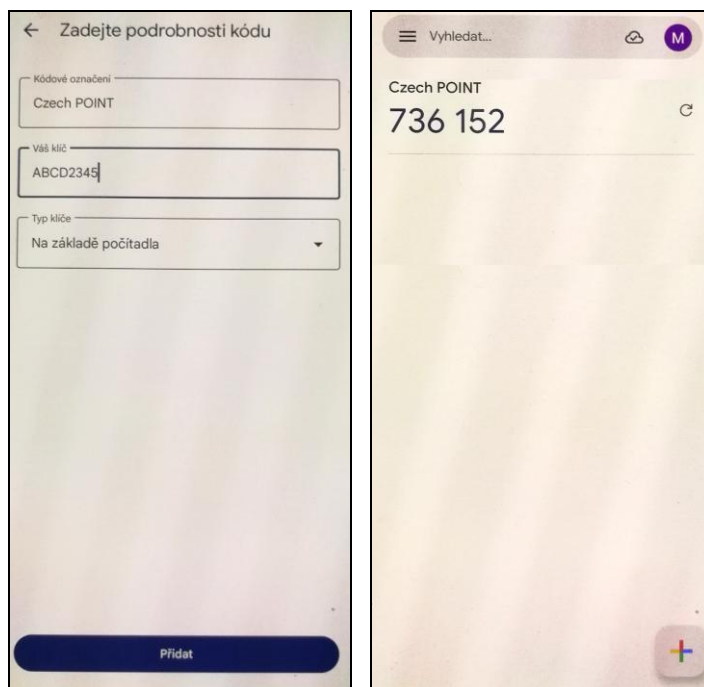
Postup pro **nastavení aplikace** v mobilním zařízení a **zaregistrování OTP přihlášení ve Správě dat** je následující:

1. Spustíte mobilní aplikaci.
2. Na hlavní obrazovce aplikace ťukněte na ikonu + v pravém dolním rohu obrazovky. Z nabídky vyberte položku „Zadat klíč pro nastavení“.
3. Zobrazí se nová obrazovka, ve které se zadávají parametry nového OTP profilu. Jednotlivé položky vyplňte následovně:
 - Do pole „Kódové označení“ 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** ve spodní části obrazovky.
 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 ťukněte v OTP profilu na ikonu zakulacené šipky pro vygenerování druhého OTP kódu. Ten ve Správě dat opište do pole „Druhý kód z bezpečnostního klíče“.
- Poznámka:** Při testování jsme měli problémy s korektním vygenerováním nového kódu. Další informace a způsob řešení tohoto problému naleznete níže v textu.
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 ikonu zakulacené šipky na řádku s vytvořeným OTP profilem. Zobrazí se vygenerovaný OTP kód.

Problémy s vygenerováním nového kódu: Při testování aplikace jsme měli problém s vygenerováním nového kódu. Nový kód by se patrně měl vygenerovat po ťuknutí na ikonu zakulacené šipky. Místo vygenerování kódu se ale pouze stávající kód zkopíroval do schránky. Tento problém se podařilo obejít tak, že před každým vygenerováním nového kódu se aplikace ukončila a znovu spustila. Ve spuštěné aplikaci nebyl zobrazen žádný kód a nový kód se vygeneroval po ťuknutí na ikonu zakulacené šipky.



5.8. OTP aplikace pro iOS

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

Vývojář: Roland Moers

Poznámka: Aplikace byla otestována na telefonu iPhone s iOS 13.3.1.

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>

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

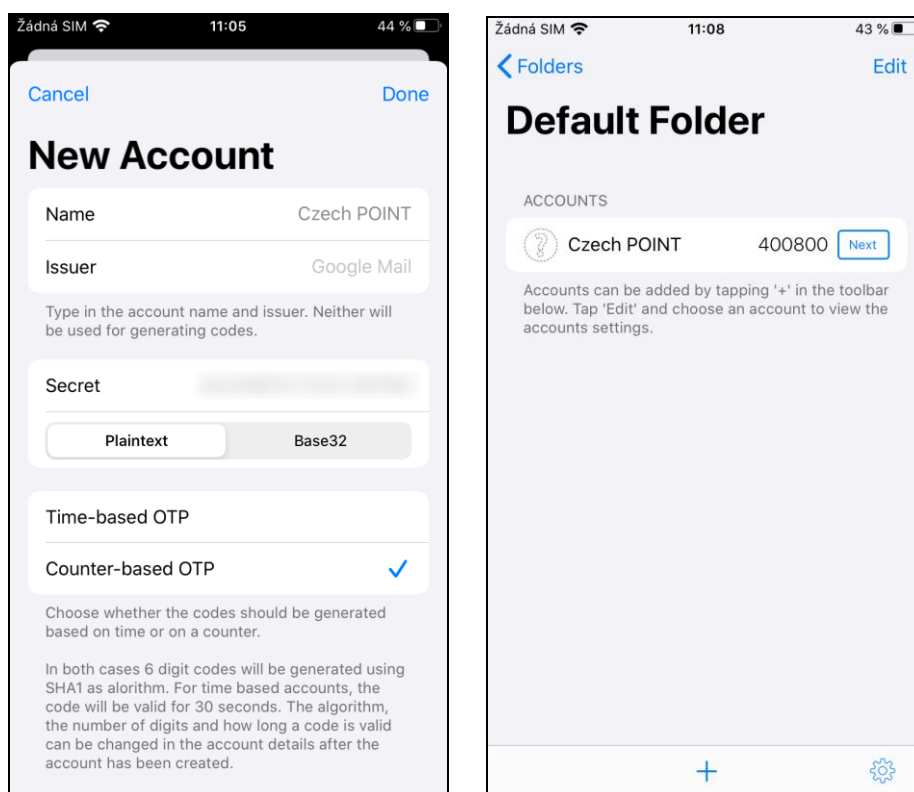
1. Aplikaci nainstalujte standardním způsobem a spusťte ji.
2. Stiskněte tlačítko **Start Setup** pro zahájení nastavování aplikace.
3. Budete vyzváni k zadání hesla pro ochranu OTP aplikace.
4. V dalším kroku si nastavujete způsob zabezpečení aplikace. Buď můžete aktivovat vyžadování hesla po spuštění 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 „+“² si můžete volitelně vytvořit vlastní složku.
7. Zahajte vytvoření nového OTP profilu stisknutím ikony „+“³ a zvolením položky „Enter Credentials“ ze zobrazené nabídky.
8. 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.

² Jsou-li na obrazovce zobrazeny dvě ikony „+“ (zejména na tabletech a zařízeních s větší šířkou displeje), klikněte na ikonu „+“ **vlevo**.

³ 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 (iOS)

Vývojář: Mufliha M

Tato OTP aplikace je dostupná pouze pro mobilní platformu iOS. Je vyžadován alespoň iOS 9. Je dostupná na této webové adrese obchodu Apple iTunes:

<https://itunes.apple.com/app/apple-store/id963496421>

Aplikaci 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 stačí základní, bezplatná verze.

Při **prvním spuštění aplikace** jste dotázáni, zda jste nový uživatel, nebo zda jste aplikaci používali již dříve. V dalším okně jste vyzváni k zadání hlavního hesla (master password). V dalším okně můžete dokoupit dokoupit rozšiřující funkce za 79 Kč, nebo obnovit

předchozí nákup. Ťukněte na „Skip“ pro přeskočení nákupu a poté ťukněte na položku „Go To App“. Zobrazí se hlavní obrazovka aplikace.

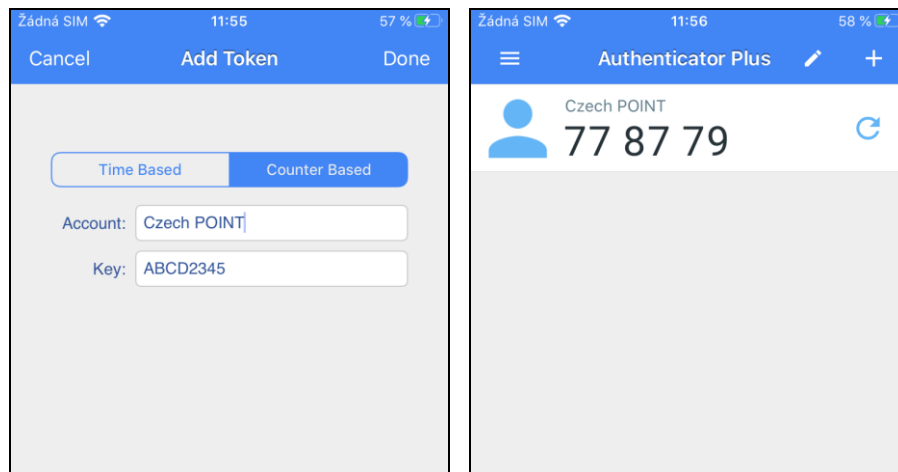
Dále doporučujeme přejít do **nastavení aplikace** a aktivovat ochranu aplikace pomocí PIN. V levém horním rohu ťukněte na ikonu se třemi čarami pro zobrazení postranního panelu. V dolní části panelu ťukněte na položku „Settings“. Dále přejděte do sekce „Security“, kde zapnete přepínač „PIN lock“ a zadejte 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 (položka „Touch ID“). 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.



5.8.3. Protectimus SMART (Android/iOS)

Popis této aplikace naleznete v kapitole 5.7.3.

Funkčnost aplikace byla úspěšně otestována také na iOS.

5.8.4. FreeOTP (Android/iOS)

Popis této aplikace naleznete v kapitole 5.7.4.

Funkčnost aplikace byla úspěšně otestována také na iOS.

5.8.5. Google Authenticator (Android/iOS)

Popis této aplikace naleznete v kapitole 5.7.5.

Tuto aplikaci nebylo možné otestovat na iOS z důvodu příliš staré verze iOS na použitém testovacím iPhoneu.

6. Přílohy

6.1. Generování tajných klíčů ve formátu Base32

Několik popsaných OTP aplikací vyžaduje zadání tajného klíče ve speciálním formátu Base32 podle RFC 4648. Toto kódování umožňuje převést libovolná binární data na textový řetězec složený z vybraných písmen a číslic⁴.

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

The screenshot shows the 'Base32 Encode' web application. On the left is a sidebar with a list of encoding formats: AES, DES, Triple DES, RC4, ECDSA, RSA, Encoding, Hex (Base16), Base32 (highlighted), Base58, Base64, HTML, URL, Format, JSON, and XML. The 'Base32' section is expanded, showing 'Encode', 'Decode', 'File to Base32', and 'Base32 to File'. The main area has a title 'Base32 Encode' and a subtitle 'This online Base32 encoding tool helps you encode text or binary to Base32. You can input UTF-8, UTF-16, Hex, Base64, or other encodings'. Below this are 'Settings' (with 'Auto Update' and 'Remember Input' toggles) and an 'Input' field containing '12345'. An 'Encode' button is positioned between the settings and the input field. The 'Output' field at the bottom displays 'GEZDGNBY'. A 'Share Link' button is visible at the bottom right.

⁴ 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 „emn178“. V případě použití jiného nástroje by ale měl být postup podobný:

1. Do prvního pole „Input“ 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 „Output“ vidíte v reálném čase generovaný zakódovaný text ve formátu Base32. Jinak stiskněte tlačítko **Encode** pro zakódování textu.
3. V prvním poli „Input“ 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 „Output“ 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, z 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 textu 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/downloads/win> si stáhněte 32-bitový nebo 64-bitový balíček „Git for Windows Portable“ podle verze vašich Windows. Pokud se vám při načtení webové stránky 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 souboru⁵ 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. Spustíte 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.

⁵ 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.