První certifikační autorita, a.s.

Uživatelská příručka

Mobilní aplikace I.CA RemoteSign

datum vytvoření:	30.9.2019
datum změny:	25.6.2020
verze:	1.3
počet stran:	21

OBSAH

1. ÚVOD

I.CA RemoteSign (dále jen „RemoteSign“) je aplikace pro platformy Google Android a Apple iOS tvořící klientskou část systému RemoteSign určeného pro elektronické podepisování v mobilním zařízení.

Požadavky na mobilní zařízení:

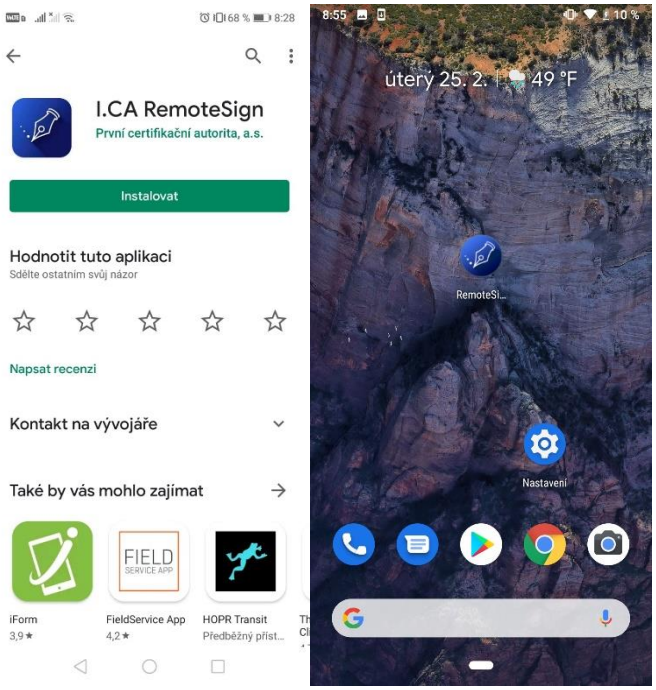
- mobilní telefon nebo tablet s operačním systémem Android verze 6.0 a vyšší nebo iOS 10.0 a vyšší
- mobilní telefon nemůže mít provedený root nebo jailbreak a nemůže obsahovat instalace z neověřených zdrojů
- alespoň 100 MB volného místa v interní paměti telefonu (aplikaci nelze přesunout na externí úložiště)
- připojení k internetu

Ostatní požadavky/předpoklady pro aktivaci aplikace:

- uzavřená smlouva o vydání certifikátu
- aktivační obálka

2. INSTALACE

Aplikaci je možné zdarma stáhnout a nainstalovat z obchodu Google Play (Android) nebo App Store (iOS) pod názvem „I.CA RemoteSign“. Během instalace bude mezi ikony pro spuštění aplikací přidána nová ikona pro RemoteSign.



Bezprostředně po instalaci aplikace do zařízení je nejprve nutné projít procesem Aktivace a následně v již aktivované aplikaci podepsat smlouvu o používání služby I.CA RemoteSign (pouze při elektronickém vydávání, jinak se smlouva podepisuje v tištěné podobě). Bez provedení předchozích kroků není možné aplikaci plnohodnotně používat.

3. PRVOTNÍ SPUŠTĚNÍ

Po prvním spuštění aplikace se zobrazí obrazovka se základními informacemi, jak dále postupovat. Aktivace služby probíhá na obchodním místě První certifikační autority, a.s. nebo u poskytovatelů služeb, kteří provozují aktivační místa služby. Zde je provedeno ověření totožnosti uživatele (žadatele o službu), jeho registrace a podepsání smlouvy o vydání certifikátu v případě volby tištěné smluvní dokumentace. Po provedení registrace uživatel získá podklady pro aktivaci služby (aktivační obálku).

V aktivační obálce uživatel setře bezpečnostní potisk pro zpřístupnění aktivačního kódu a poté může přejít k aktivaci aplikace v zařízení.

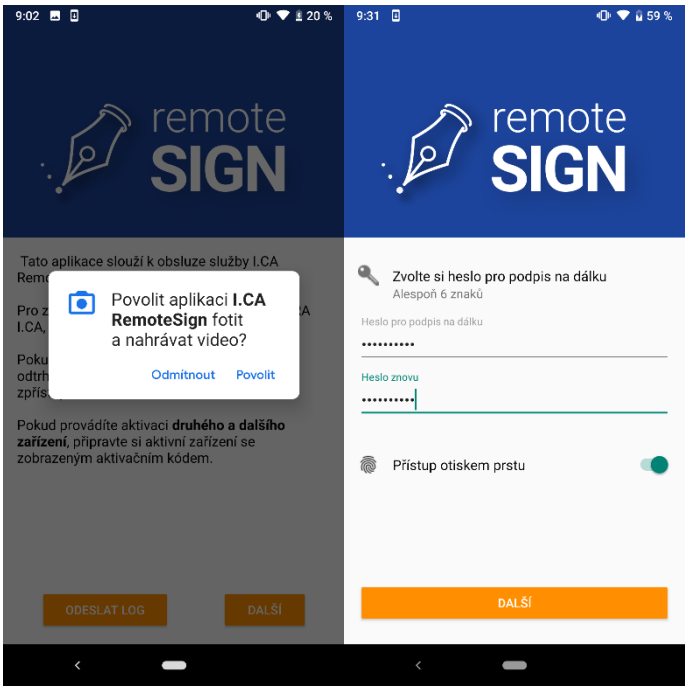
Důležitá informace:

Aktivační obálku důkladně uschovejte, můžete ji v budoucnu potřebovat např. při resetu hesla nebo při aktivaci zařízení ze zálohy.

4. AKTIVACE ZAŘÍZENÍ

Aktivace mobilní aplikace probíhá v těchto krocích:

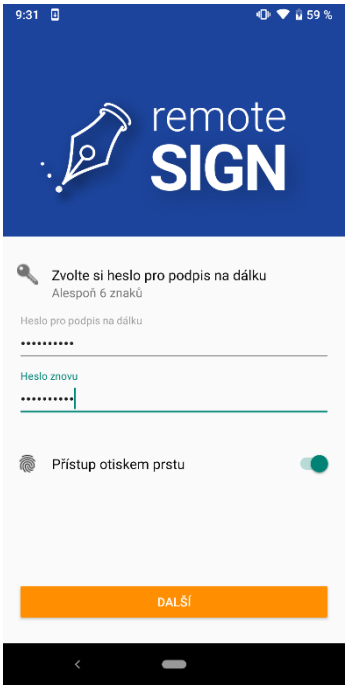
1. Skenování aktivačního kódu (2D barcode) z aktivační obálky. Skenování je realizováno skenerem integrovaným v aplikaci (nejdříve je nutné povolit aplikaci možnost používat fotoaparát).
2. Volba a zadání hesla pro budoucí podepisování a autentizaci do aplikace, aktivace použití biometriky.
3. Elektronický podpis smlouvy o užívání služby I.CA RemoteSign (v případě elektronické dokumentace).



4.1 Nastavení hesla, aktivace biometriky

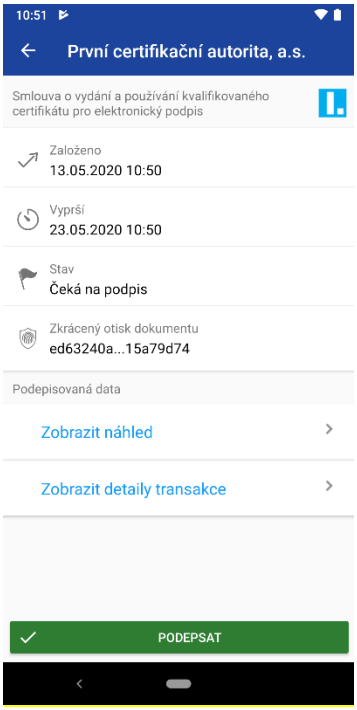
Heslo se zadává pro kontrolu 2x a musí být dlouhé alespoň 6 alfanumerických znaků (A-Z, 0-9), přičemž musí obsahovat alespoň jedno písmeno (rozlišují se velká a malá písmena).

Po zadání hesla je, na podporovaných zařízeních, možné aktivovat i biometriku. Na zařízeních, která biometriku nepodporují je volba biometriky nedostupná.



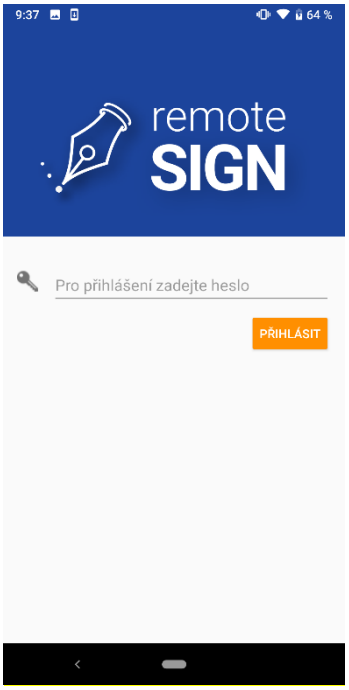
4.2 Aktivace dokončena, podpis smlouvy

Aby bylo možné zahájit používání aplikace pro podepisování dokumentů, musí být Aktivace dokončena podpisem smlouvy o užívání služby I.CA RemoteSign (v případě, kdy na obchodním místě nebyla podepsána papírová verze smlouvy). Proces podpisu smlouvy je shodný s podpisem běžného dokumentu/transakce s tím rozdílem, že podpis smlouvy nelze odmítnout. Bez tohoto kroku nelze zařízení používat. O úspěšné aktivaci je uživatel informován zobrazením příslušné obrazovky.



5. PŘIHLÁŠENÍ DO APLIKACE

Pro přihlášení do aplikace a zobrazení transakcí (požadavků na podepsání) může uživatel volit mezi autentizací heslem a biometrikou (pokud je zařízením podporována).



Typy spuštění aplikace:

- **Standardní** (ikonou) – po přihlášení se zobrazí obrazovka se seznamem transakcí.
- **Z push notifikace** – po přihlášení se přejde na detail konkrétní transakce.

5.1 Přihlášení – biometrikou

Pokud má uživatel povolené přihlašování pomocí biometriky, přihlásí se přiložením prstu na čtečku otisků prstů, nebo použitím *faceID*.

5.2 Přihlášení – heslo

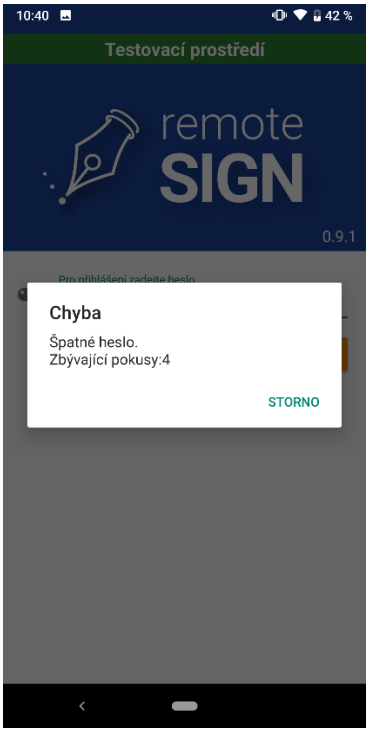
Pokud uživatel nemá povolené přihlašování biometrikou, musí se přihlašovat pomocí zvoleného hesla.

5.3 Přihlášení – chybně zadané heslo

5.3.1 Zbývá "n" pokusů

Uživatel má 5 pokusů pro zadání správného hesla.

Pokud uživatel chybně zadá heslo, zobrazí se mu informace o chybně zadaném heslu a počtu zbývajících pokusů.



5.3.2 Zablokované heslo, možnost resetu hesla

Pokud uživatel vyčerpal všechny pokusy (zapomněl heslo), zobrazí se obrazovka, ve které lze vybrat možnost obnovy hesla.

6. OBNOVA HESLA

V případě, že uživatel heslo zapomene, je k dispozici funkčnost pro obnovu hesla. K obnově hesla je nutno znovu načíst aktivační kód (2D barcode) z aktivační obálky.

6.1 Nastavení nového hesla

Pokud načtení kódu z aktivační obálky proběhlo úspěšně, pokračuje se nastavením nového hesla.

6.1.1 Neplatné heslo

Pokud se zadaná hesla neshodují (pro kontrolu se zadává 2x) nebo nesplňují bezpečnostní podmínky, je zobrazena informace, že heslo není akceptováno (nutno zadat správně).

7. TRANSAKCE

Každý požadavek na podpis, obnovu certifikátu apod., se nazývá transakce.

Pro uživatele se budou jednotlivé transakce jevit obdobně jako emaily. Každá transakce bude z pohledu uživatele mít:

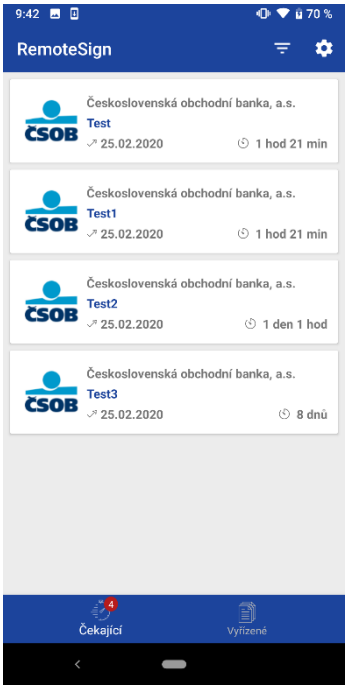
- svého (ověřeného) zadavatele (poskytovatele služeb)

- datum a čas založení
- platnost
- předmět transakce (nešifrovaný)
- náhled nebo odkaz na stažení celých podepisovaných dat (šifrované)
- hash (otisk) podepisovaných dat
- stav (nepřečtená/přečtená/podepsaná/odmítnutá/expirovaná)

Uživatel si bude moct označit každou jednotlivou transakci jako přečtenou/nepřečtenou a po zobrazení detailu transakce ji podepsat nebo odmítnout.

7.1 Seznam transakcí

V obrazovce se seznamem transakcí jsou transakce rozdělené na čekající a na vyřízené. K přepnutí mezi seznamy dojde po kliknutí na příslušnou volbu ve spodní části obrazovky. U čekajících transakcí je uveden počet nepřečtených transakcí.



7.1.1 Zobrazené transakce

Ke každé transakci je zobrazeno logo zadavatele (poskytovatele služeb), název zadavatele, předmět transakce, datum založení transakce a zbývající čas do expirace transakce.

Nepřečtená transakce je znázorněna pomocí tučného písma a zobrazením počtu nepřečtených transakcí u možnosti „čekající“. Seznam čekajících transakcí je řazen podle data a času expirace transakce od nejbližšího termínu expirace (nahoře) po nejpozdější termín expirace (dole).

Seznam vyřízených transakcí je řazen podle data a času vyřízení (tj. podepsání, odmítnutí nebo expirování transakce) od nejaktuálněji vyřízených transakcí (nahoře) po nejstarší vyřízené transakce (dole). Historie transakcí je udržována minimálně 1 měsíc.

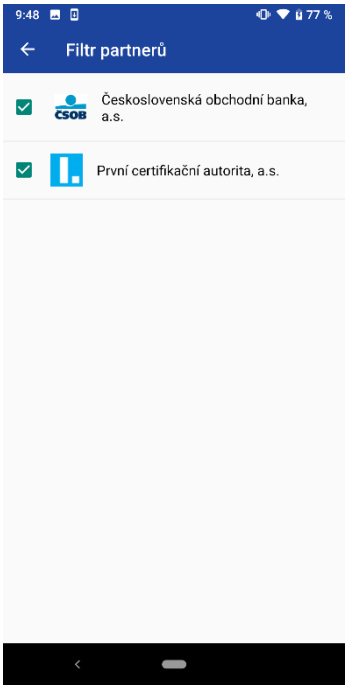
Seznam transakcí je možné obnovit (znovu načíst ze serveru) „stažením“ (swipem) seznamu směrem dolů. V případě posouvání seznamu směrem nahoru (tj. rolováním seznamu směrem dolů) dochází v případě většího počtu transakcí v seznamu k postupnému načítání dalších transakcí ze serveru. Pokud se v tomto případě čeká na stažení dalších transakcí ze serveru pro jejich zobrazení, je po dobu čekání na konci seznamu zobrazena informace „Načítání, čekejte prosím“. Tato je po stažení informací o další transakci nahrazena příslušnou transakcí.

Po kliknutí na konkrétní transakci dojde k zobrazení jejího detailu.

7.1.2 Nastavení filtru v seznamu transakcí

V seznamu transakcí je možné filtrovat podle partnerů (I.CA, ČSOB).

Ve výchozím nastavení je filtr nastaven tak, aby zobrazoval vše. Jiné nastavení filtru je platné pouze pro danou relaci. S ukončením aplikace se neukládá.



7.2 Detail transakce

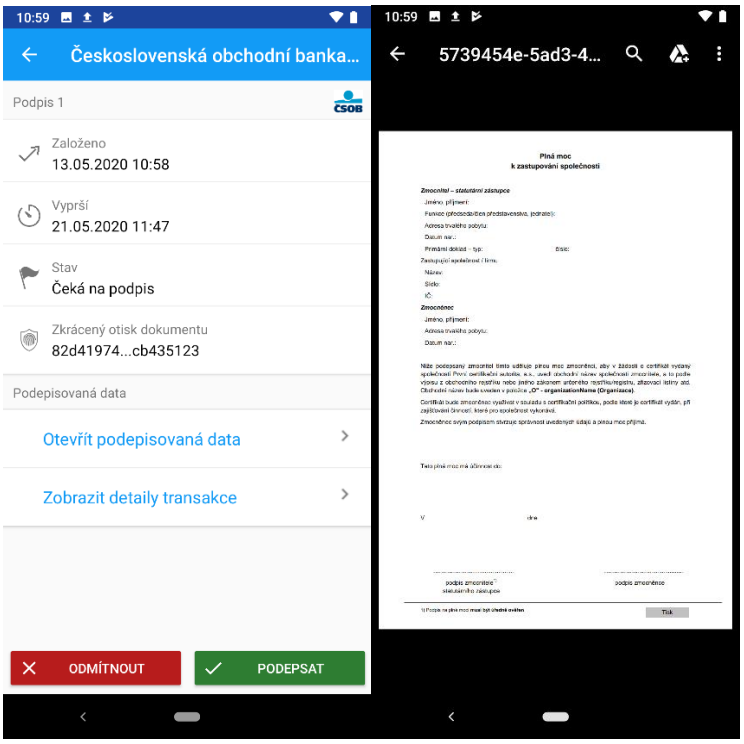
V detailu transakce je možné transakci podepsat nebo odmítnout. Tlačítko „*Odmítnout*“ může být pro specifické transakce neaktivní (např. pro podpis smlouvy o používání I.CA RemoteSign).

Detail transakce obsahuje volbu pro zobrazení náhledu podepisovaných dat nebo ke stažení a zobrazení podepisovaných dat v asociované aplikaci.

Pro každou transakci jsou k dispozici detailní informace, které si může uživatel v případě zájmu zobrazit zvolením možnosti „Zobrazit detail transakce“, zde je uveden kompletní hash (otisk) dokumentu a ID transakce.

Po kliknutí na tlačítko „*Podepsat“* je nutné operaci autorizovat:

- První podpis v řadě – nutné zadat heslo.
- Další podpis v řadě – lze využít biometriku (pokud je aktivní)



7.2.1 Vyřízené transakce

Zde má uživatel možnost zobrazit vyřízené transakce.

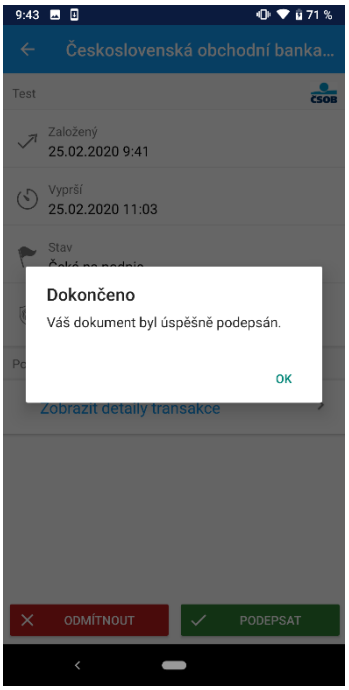
7.2.2 Transakci nelze podepsat na daném zařízení

Obrazovka s touto informací je zobrazena v případech, kdy není z technických důvodů možné provést podpis konkrétní transakce na konkrétním zařízení (např. když transakce vznikla před aktivací (klonováním) dané mobilní aplikace).

Uživatel je přesměrován zpátky na seznam transakcí.

7.2.3 Úspěšně podepsáno

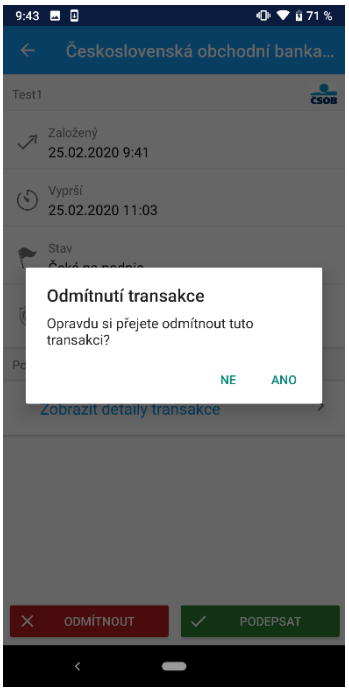
O úspěšném dokončení podpisu transakce je uživatel informován pomocí vyskakovacího okna, po jehož odkliknutí je vrácen na seznam čekajících transakcí.



7.2.4 Odmítnout transakci

Odmítnutí transakce se provede stisknutím tlačítka *„Odmítnout“,* poté je zobrazeno vyskakovací okno s výzvou, zda si uživatel skutečně přeje transakci odmítnout.

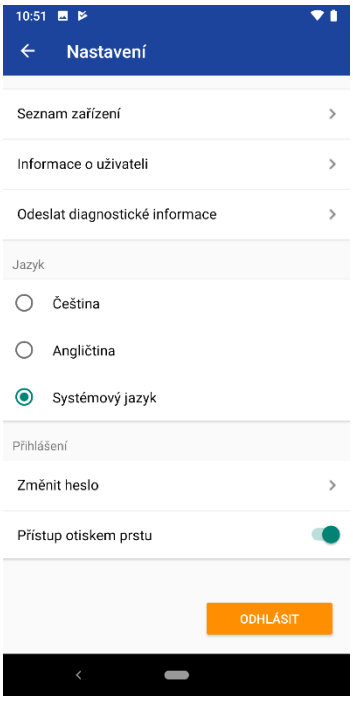
Odmítnutí transakce je nevratné.



7.2.5 Expirovaná transakce

Při expiraci transakce se zobrazí informace o expiraci a není možné transakci podepsat.

8. NASTAVENÍ

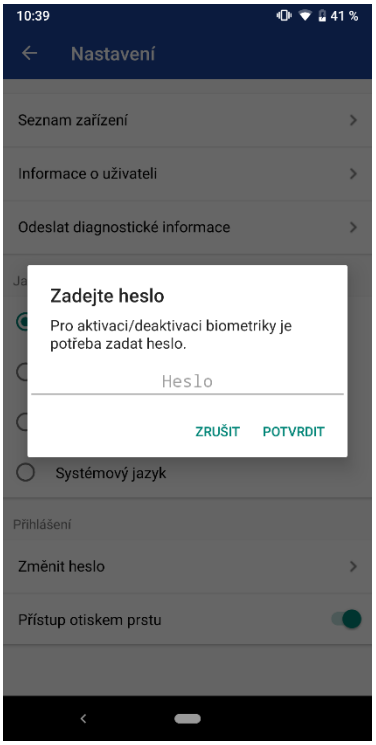


8.1 Nastavení – hlavní obrazovka

Hlavní obrazovka nastavení aplikace, ve které lze vybrat jednu z akcí:

- zobrazit informace o uživateli a zařízení
- změnit heslo
- aktivovat biometriku
- deaktivovat biometriku (deaktivace biometriky je provedena okamžitě bez dotazu na heslo)
- odeslat diagnostické informace
- zobrazit seznam zařízení

8.1.1 Aktivace biometriky – zadání hesla



Změnou stavu přepínače aktivace biometriky dojde k zobrazení nového okna pro zadání hesla pro autorizaci aktivace biometriky.

8.1.2 Informace o uživateli a zařízení

Aplikace zobrazí informace o uživateli a zařízení.

Tato obrazovka je určena spíše pro diagnostické účely v případě řešení problémů.

8.1.3 Odeslat diagnostické informace

Skrze tuto obrazovku lze jednorázově odeslat diagnostické informace na technickou podporu (HelpDesk) I.CA.

Diagnostické informace neobsahují žádné citlivé údaje, jako jsou hesla, klíče, podepisovaná data, náhled podepisovaných dat, odkaz, ani autentizační hlavičky na podepisovaná data. Diagnostické informace jsou před odeslání zašifrovány kvůli utajení přenášených logů mezi mobilní aplikací a I.CA.

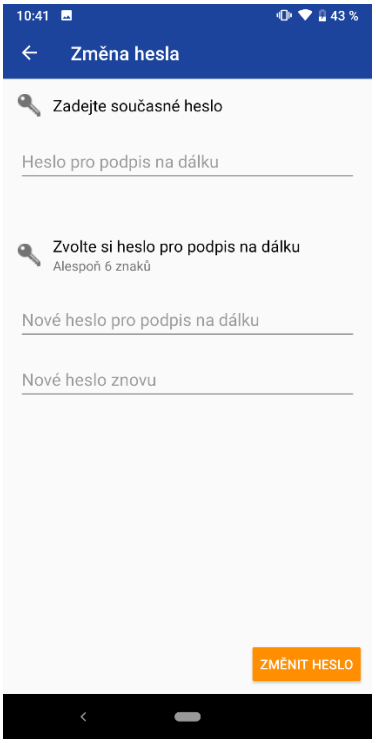
9. ZMĚNA HESLA

Změnu hesla může uživatel zvolit na obrazovce s nastavením.

V případě, že uživatel heslo zapomene, je k dispozici funkčnost pro obnovu hesla. K obnově hesla je nutno znovu načíst aktivační kód (2D barcode) z aktivační obálky.

Heslo musí být dlouhé alespoň 6 alfanumerických znaků (A-z, 0-9), přičemž musí obsahovat alespoň jedno písmeno. Rozlišují se malá a velká písmena.

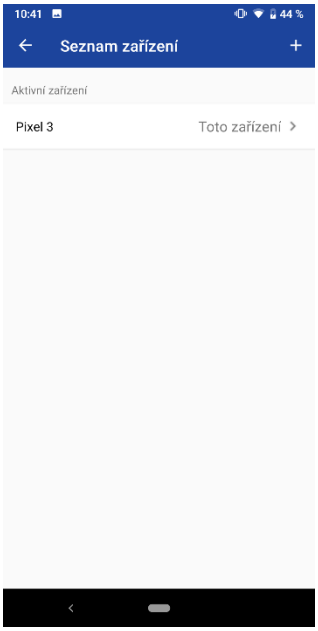
9.1 Změna hesla



Na této obrazovce je potřeba zadat původní heslo a nové heslo (2x pro kontrolu).

10. ZAŘÍZENÍ

10.1 Seznam zařízení

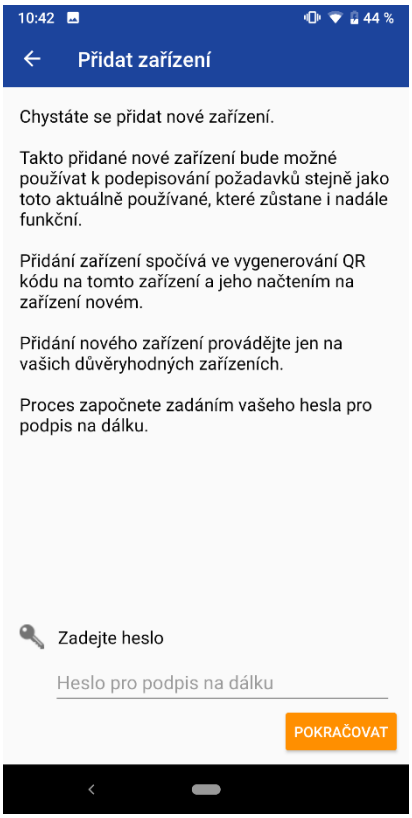


Seznam zařízení se nachází v nastavení.

Zobrazuje seznam v minulosti aktivovaných zařízení (aktivní, blokovaná (i na stanovený časový úsek), zrušená).

Umožňuje přidat další zařízení nebo zobrazit detail konkrétního zařízení.

10.2 Přidat zařízení



Možnost přidat zařízení je dostupná v seznamu zařízení.

Informuje o způsobu a důsledcích klonování zařízení s možností zadat heslo pro pokračování.

10.2.1 Aktivační QR-kód pro nové zařízení

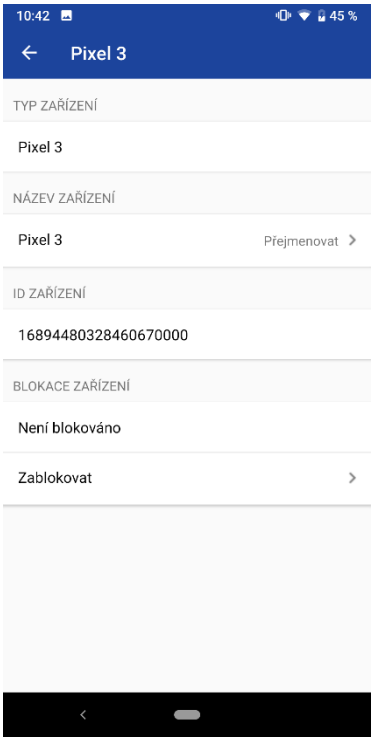
Aplikace vytvoří aktivační QR-kód, který slouží k aktivaci dalšího zařízení.

10.2.2 Varování – pokus o storno nedokončeného klonování

Pokud se uživatel pokusí stornovat nedokončené klonování, je zobrazeno varování o důsledcích s dotazem, zda se má klonování skutečně stornovat:

- ANO – klonování bude zrušeno
- NE – pokračuje se v klonování

10.3 Detail zařízení



Na této obrazovce jsou zobrazeny detaily o zařízení:

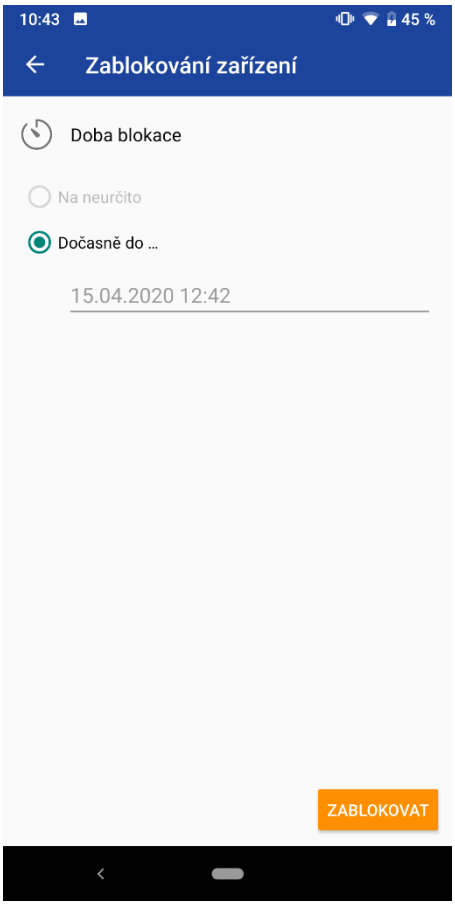
- *Typ zařízení*
- *Název zařízení*
- *ID zařízení*
- *Stav zařízení*

Lze zde vybrat akce:

- Přejmenovat zařízení
- Blokace zařízení:
    - zablokovat po stanovenou dobu
    - zablokovat na dobu neurčitou
    - trvale zrušit
    - odblokovat

10.3.1 Zablokovat

Zařízení je možné blokovat na stanovenou dobu nebo na dobu neurčitou. V případě blokace na stanovenou dobu zadává uživatel datum a čas, do kdy má být zařízení zablokované. Po uplynutí tohoto času dojde k automatickému odblokování zařízení.



10.3.2 Zablokovat – úspěšně zablokováno

Obrazovka informuje o úspěšném zablokování zařízení (je zde zobrazen čas, do kdy je zařízení zablokováno, pokud se jedná o blokaci na stanovenou dobu).

10.3.3 Zrušit

Obrazovka zobrazuje dopady, které zrušení zařízení obnáší a zároveň slouží pro zadání hesla, které je ke zrušení zařízení potřeba. Zrušení zařízení je možné pouze v případě dvou (nebo více) aktivovaných zařízení, jinak je tato volba deaktivována a zařízení lze přes mobilní aplikaci pouze zablokovat.

11. NÁSLEDNÝ CERTIFIKÁT

60 dnů před vypršením platnosti certifikátu do zařízení dojde požadavek „Žádost o prodloužení certifikátu RemoteSign“. Po podepsání tohoto požadavku se odešle žádost o vydání následného certifikátu. Jakmile se následný certiifkát vydá, je poté automaticky používán pro další podepisování, není nutné ze strany klienta nic dalšího dělat.

Pokud se požadavek nepodepíše hned, aplikace 30 dnů před vypršením platnosti RemoteSign certifikátu nedovolí podepsat jinou transakci než je žádost o následný certifikát.

12. HLÁŠENÍ O PÁDU APLIKACE

Na této obrazovce se nachází možnost pro odeslání diagnostických dat i na technickou podporu (HelpDesk I.CA/ČSOB).

13. PUSH NOTIFIKACE

Po založení transakce na straně zadavatele (poskytovatele služeb) dojde k přijmutí push notifikací na všech aktivních zařízeních daného účtu. Push notifikace informuje o nové transakci k podpisu a nehledě na zadávajícího poskytovatele služeb vystupuje pod ikonou RemoteSign. „Rozliknutí“ push notifikace otevře aplikaci RemoteSign na stránce přihlášení, po přihlášení dojde k zobrazení detailu konkrétní transakce.

Po dokončení transakce a jejím označení na serveru RemoteSign jakožto „Finalized“ dojde k odeslání push notifikace informující o úspěšném dokončení podpisu.

14. AKTIVACE ZAŘÍZENÍ ZE ZÁLOHY

Opakovanou aktivaci zařízení (např. po restartu do továrního nastavení), je možné pouze v případě, že je účet uživatele zálohovaný. Prostředky OS zajistí přenesení vybraných dat instalovaných aplikací do nového zařízení. Aplikace RemoteSign nebude ihned fungovat, jelikož nedochází k přenosu tajných bezpečnostních klíčů. Je nutné využít původní aktivační kód (obálku) ke zprovoznění aplikace.