MeeSign

Platforma pro vícestranné podepisování dokumentů

Antonín Dufka, Jakub Janků, Jiří Gavenda, Petr Švenda

CROCS
Centre for Research on Cryptography and Security

Osnova

- Motivace
- Prahová kryptografie
  - Příklady užití
- MeeSign
  - Architektura platformy
  - Použití platformy
- Demo

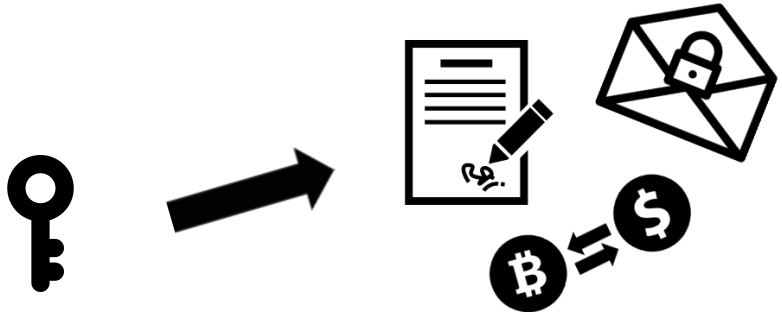
Motivace

- Scénáře z reálného světa často vyžadují podpis dokumentu více stranami
  - Dva podpisy na smlouvě
  - Schválení dokumentu skupinou (nadpoloviční většina)
  - Petice
  - …
- Standardní nástroje pro práci s digitálními podpisy tyto scénáře mnohdy neuvažují
  - Lze přidat nanejvýš jeden podpis k dokumentu
  - Nástroje pro ověřování podpisu často podporují ověření jen jednoho podpisu
  - Dokument nelze podepsat se zachováním anonymity podepisujících stran

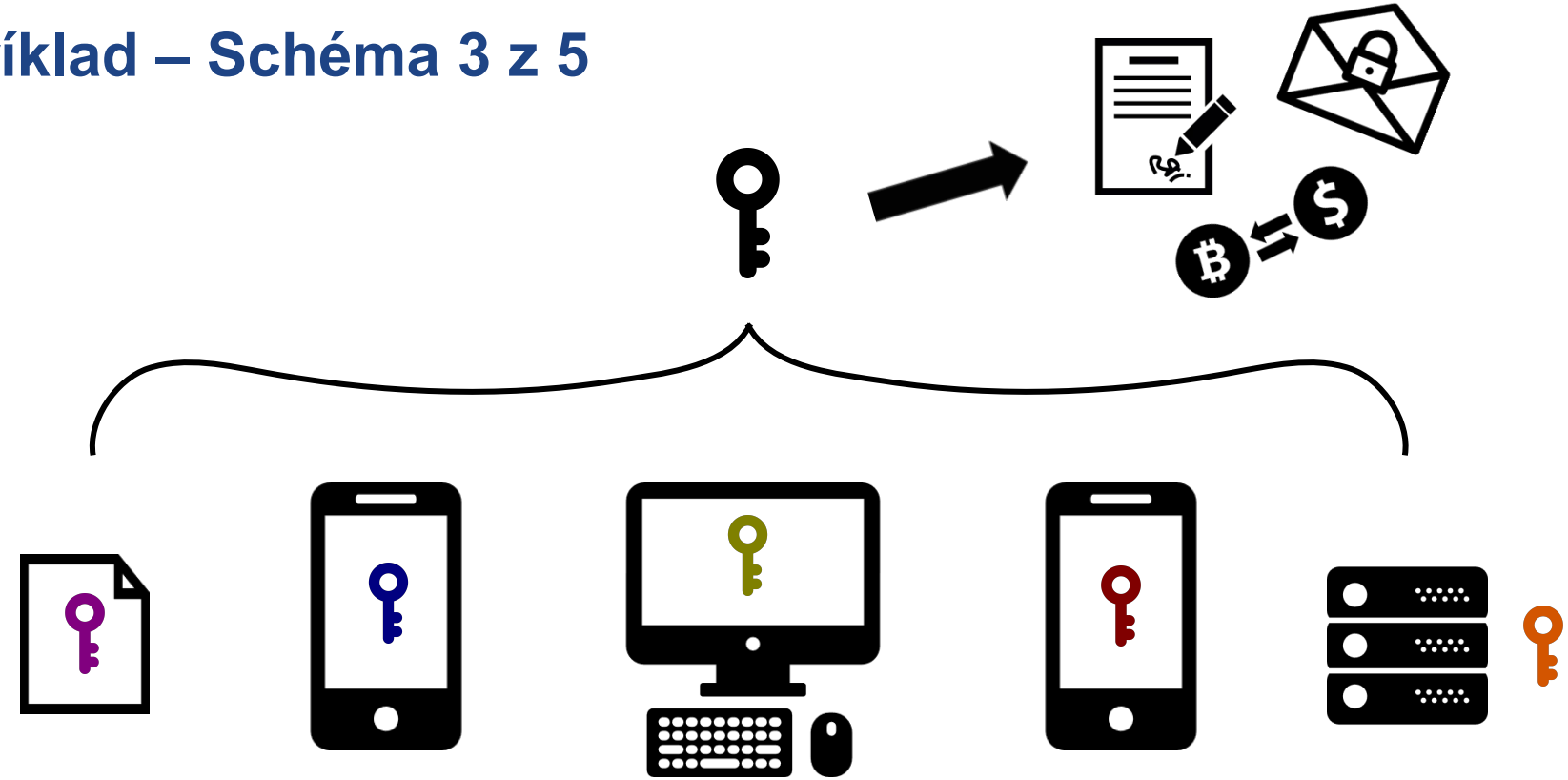
Prahová kryptografie (threshold cryptography)

- Navržena v roce 1987 profesorem Yvo Desmedtem
- Významný vývoj v souvislosti se zabezpečením kryptoměnových aplikací
- Princip
  - Privátní klíč je rozdělen na více částí
  - Tyto části se využívají v protokolu za účelem provedení kryptografické operace
  - Při použití dostatečného počtu částí klíče se operace úspěšně dokončí
- Vlastnosti
  - Vyšší zabezpečení klíče (odstraněn single point of failure)
  - Klíč může být rozdělen mezi více stran (samostatný proces schvalování)
  - Výsledný podpis může být nerozlišitelný od standardního podpisu (zpětně kompatibilní)

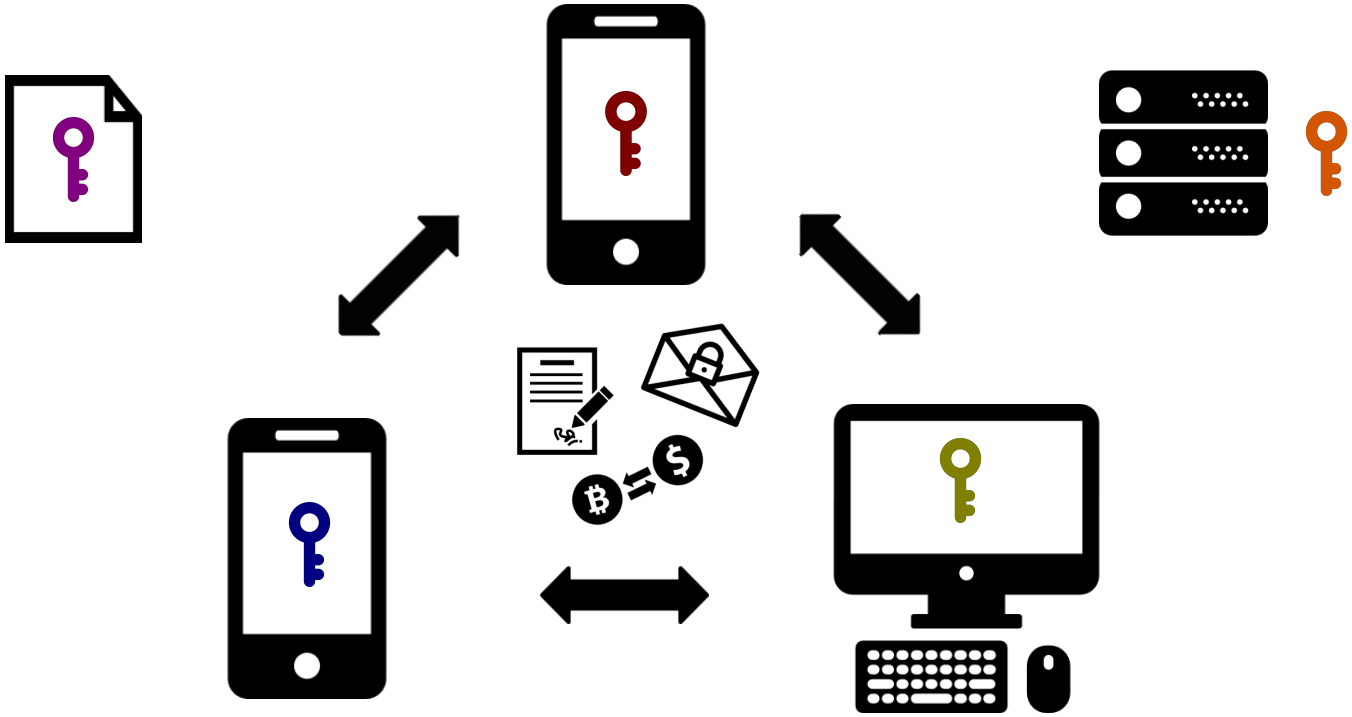
Příklad – Schéma 3 z 5



Příklad – Schéma 3 z 5



Příklad – Schéma 3 z 5



Příklady užití – prahové podepisování

- 2-ze-2 (dva podepisující)
  - dvoustranná autorizace
- 2-ze-3 (tři podepisující, alespoň dva vyžadováni)
  - dvoustranná autorizace se zálohou
- 3-z-5 (pět podepisujících, alespoň tři vyžadováni)
  - hlasování s různou prioritou hlasů (vedoucí dvě části klíče, ostatní jen jednu)
- 11-z-15 (patnáct podepisujících, alespoň jedenáct vyžadováno)
  - vysoká garance bezpečnosti i zálohy
  - Liquid konsorcium (podepisování bloků na sidechainu Bitcoinu)

Příklady užití – prahové podepisování s politikou

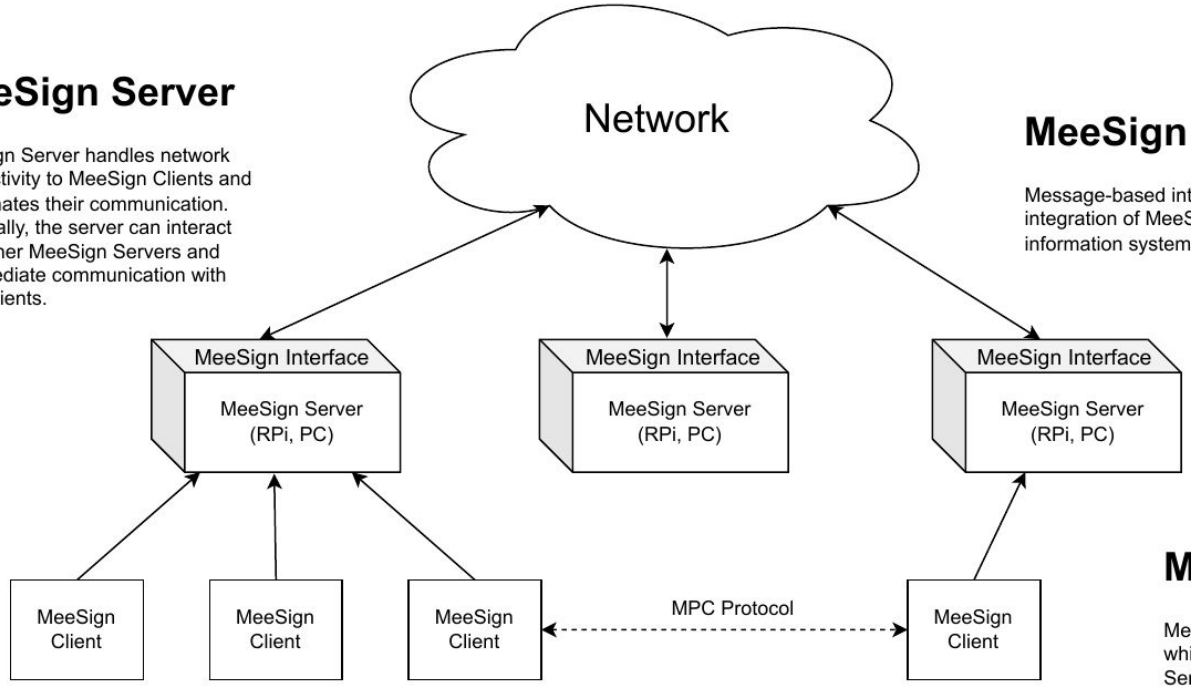
- Podepisující strany mohou být automatizované a vynucovat určitou politiku
- 2-ze-2 s politikou
  - jedna fyzická osoba, druhá strana automatizovaná po splnění určité politiky (podpis vznikne jen v určitém čase, v návaznosti na nějakou událost, po určitém čase po podání žádosti o podpis, …)
- 2-ze-3 s politikou
  - dvě fyzické osoby dokáží vytvořit podpis vždy, jedna strana s automatizovaným serverem s politikou pouze za určitých podmínek
- 3-ze-3 s politikou
  - automatizované zařízení podepisuje pouze pokud vznikly předchozí dva podpisy od fyzických osob a podpis vydá až po uplynutí určitého času

MeeSign (Multiparty electronic evidence Signing)

- Platforma pro vícestranné podepisování dokumentů
- Využívá prahové kryptografie pro vytváření podpisů
  - Podpisy nerozlišitelné od standardních jednostranných podpisů (zpětně kompatibilní, verifikovatelné standardními nástroji)
  - Možnost doplnění o podepisování serverem za splnění určité politiky
- Další cíle
  - Uživatelsky přívětivé rozhraní pro vytváření podpisů
  - Podpora různých dokumentových formátů
  - Snadná integrovatelnost do stávajících systémů (Informační systémy, standardní softwarová rozhraní – PKCS#11, HWI)
- Provoz zamýšlen v interním prostředí organizace
  - Možnost propojení s jinými instancemi systému

MeeSign Server

MeeSign Server handles network connectivity to MeeSign Clients and coordinates their communication. Optionally, the server can interact with other MeeSign Servers and intermediate communication with their Clients.



MeeSign Interface

Message-based interface (gRPC) for easy integration of MeeSign with preexisting information systems.

MeeSign Client

MeeSign Client is an application which is registered with a MeeSign Server. The application has access to private keys and uses them in MPC protocols with other MeeSign Clients.

MPC Protocols

Various MPC protocols for signing, decryption, randomness generation running on MeSign Clients coordinated by MeeSign Server.

MeeSign server

- Implementace MeeSign serveru v jazyce Rust
  - https://github.com/crocs-muni/meesign-server
- Funkce
  - Udržování informací o registrovaných zařízeních, skupinách, dokončených podpisech i běžících úlohách
  - Rozhraní pro konfiguraci, registraci nových zařízení, správu skupin a zadávání úloh
  - Zprostředkovávání komunikace mezi klientskými zařízeními
  - Vydávání certifikátů pro klientské zařízení i skupiny
  - Integrace podpisů do podepisovaných dokumentů
- Možná integrace s existujícími systémy přes gRPC rozhraní

MeeSign klient

- Implementace multiplatformního (Android, Linux, Windows) MeeSign klienta v jazyce Dart s frameworkem Flutter
  - https://github.com/crocs-muni/meesign-client
- Funkce
  - Uživatelské rozhraní pro interakci se systémem MeeSign
    - Registrace zařízení, vytváření skupin, účast ve skupinách, zadávání a vykonávání podepisovacích úloh
  - Bezpečné uchování privátního identitního klíče i klíčů pro účast ve skupinách
  - Síťová komunikace se serverem a upozornění uživatele na příchozí požadavky
  - Realizace kryptografických operací s privátními klíči při vykonávání protokolů
- Pro vykonávání kryptografických operací se používá implementace protokolu GG18 z knihovny ZenGo X

Použití platformy – Registrace

- Uživatel se připojí ke svému lokálnímu (organizačnímu) serveru
- Aplikace na zařízení vygeneruje svůj identitní klíčový pár
  - Veřejný klíč je zaslán společně s názvem zařízení na server
  - Server vydá certifikát zařízení
    - Může být podmíněno ověřením identity vlastníka (podobně jako v případě CA)
- Pozdější autentizace probíhá pomocí privátního identitního klíče

Použití platformy – Podepisovací skupiny

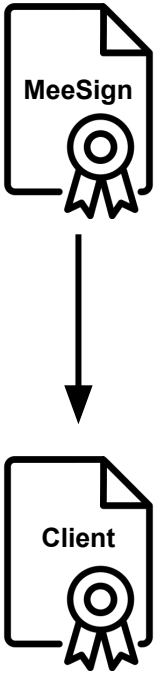
- Registrovaná zařízení mohou být organizována do podepisovacích skupin
  - Tvorba skupiny může být iniciována buď centrálně (administrátorem) nebo samotnými uživateli
  - Je potřeba zvolit:
    - Název skupiny
    - Členy skupiny
    - Práh (hranici nezbytnou pro vznik podpisu)
- Vznik skupiny
  - Uživatelé nejprve musí souhlasit s účastí ve skupině
  - Poté se spustí proces generování skupinového klíče s požadovanými parametry
  - Na závěr server vydá certifikát veřejného klíče dané skupiny

Použití platformy – Podepisování dokumentu

- Vzniklé skupiny se mohou účastnit podepisování
  - Žádost o podpis dokumentu může být zaslána centrálně nebo jednotlivými členy skupiny
  - Je potřeba zvolit:
    - PDF dokument
    - Podepisující skupinu
- Vznik podpisu
  - Uživatelé obdrží žádost o podpis dokumentu
  - Tento dokument si mohou zobrazit a rozhodnout se, zda souhlasí s jeho podpisem
  - Jakmile s podpisem souhlasí dostatečný počet stran, spouští se podepisovací protokol
  - Výsledkem podepisovacího protokolu je podpis PDF dokumentu
  - Server integruje tento podpis v PDF a rozešle jej všem zúčastněným stranám

Poznámka o certifikátech

- MeeSign server si generuje vlastní certifikát pro vydávání certifikátů (CA)
  - Nejedná se o běžně důvěřovaný certifikát – nemáte jej nainstalovaný jako důvěřovaný na svých zařízeních
  - Pro úspěšnou verifikaci včetně certifikačního řetězce až k důvěřovanému certifikátu je potřeba importovat MeeSign certifikát
    - Stačí importovat pouze jeden MeeSign certifikát – slouží k vydávání všech dalších
    - Bez importovaného certifikátu verifikace podpisu uspěje, ale verifikační nástroje zobrazí ikonu s varováním
  - Pro interní použití v organizaci se nejedná o problém



MeeSign Demo

Demo – Instalace

1. Stáhněte a spusťte si klientskou aplikaci MeeSign pro vaši platformu
   - Android
     - Potřeba povolit instalaci APK souborů z externích zdrojů
   - Linux
     - Stažený tar archiv je potřeba extrahovat
   - Windows
     - Stažený zip archiv je potřeba extrahovat
   - Sources
     - README.md

https://meesign.crocs.fi.muni.cz/

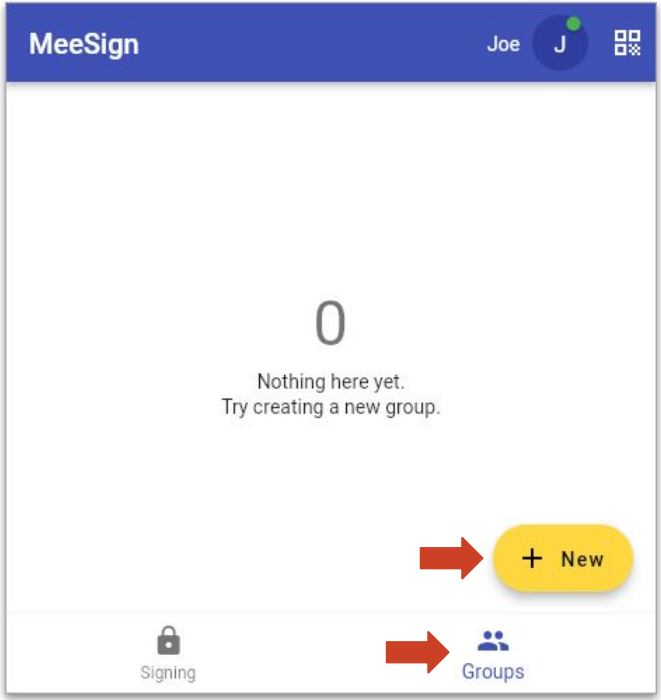
Demo – Registrace

2. Připojte se na lokální WiFi **`meesign`**
   - Přístup bez hesla
   - Pro ověření úspěšného připojení lze navštívit adresu http://192.168.1.2/

3. Registrujte se na serveru MeeSign
   - Zvolte si své uživatelské jméno
   - Adresa **meesign.local** (192.168.1.2)
   - Stisknout Register
   - (Od této chvíle prosím nevypínejte aplikaci)

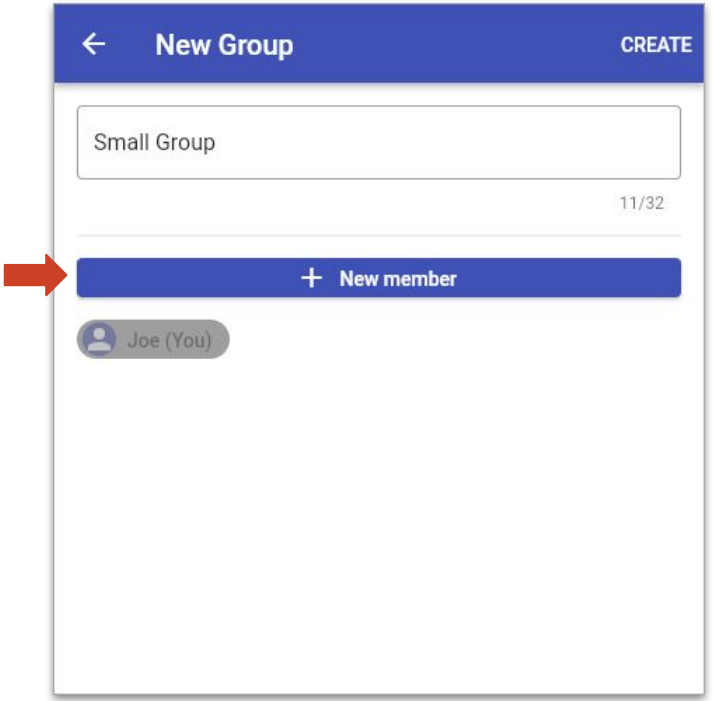
Demo – Vytvoření skupiny

4. Vytvořte skupiny ze dvou účastníků
   - Nabídka Groups → New (vpravo dole)
   - Zvolte název skupiny
   - Přidejte členy pomocí New member jedním ze způsobů:
     - Načíst QR kód (Scan QR code)
     - Vyhledávat podle jména (Search peer)
   - Stisknout Create (vpravo nahoře)
   - Potvrdit notifikaci o účasti v nové skupině (zobrazí se jen ostatním členům)



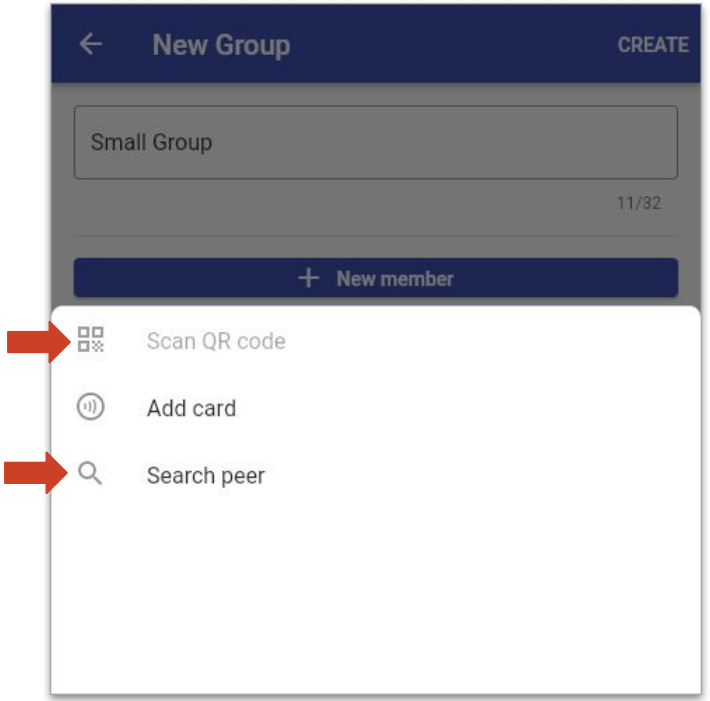
Demo – Vytvoření skupiny

4. Vytvořte skupiny ze dvou účastníků
   - Nabídka Groups → New (vpravo dole)
   - Zvolte název skupiny
   - Přidejte členy pomocí New member jedním ze způsobů:
     - Načíst QR kód (Scan QR code)
     - Vyhledávat podle jména (Search peer)
   - Stisknout Create (vpravo nahoře)
   - Potvrdit notifikaci o účasti v nové skupině (zobrazí se jen ostatním členům)



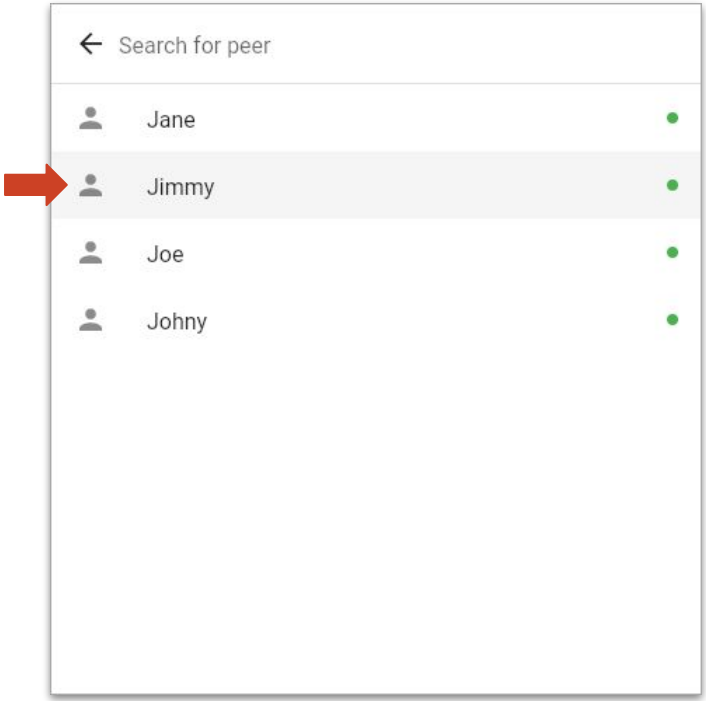
Demo – Vytvoření skupiny

4. Vytvořte skupiny ze dvou účastníků
   - Nabídka Groups → New (vpravo dole)
   - Zvolte název skupiny
   - Přidejte členy pomocí New member jedním ze způsobů:
     - Načíst QR kód (Scan QR code)
     - Vyhledávat podle jména (Search peer)
   - Stisknout Create (vpravo nahoře)
   - Potvrdit notifikaci o účasti v nové skupině (zobrazí se jen ostatním členům)



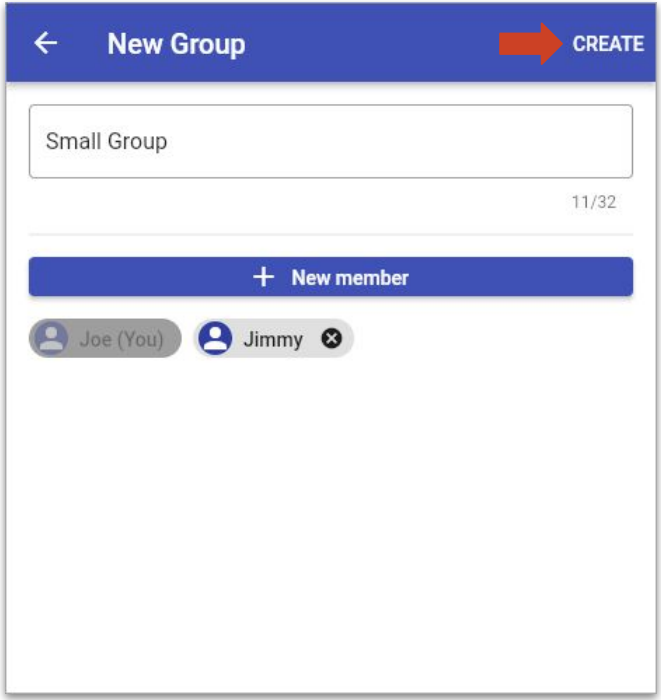
Demo – Vytvoření skupiny

4. Vytvořte skupiny ze dvou účastníků
   - Nabídka Groups → New (vpravo dole)
   - Zvolte název skupiny
   - Přidejte členy pomocí New member jedním ze způsobů:
     - Načíst QR kód (Scan QR code)
     - Vyhledávat podle jména (Search peer)
   - Stisknout Create (vpravo nahoře)
   - Potvrdit notifikaci o účasti v nové skupině (zobrazí se jen ostatním členům)



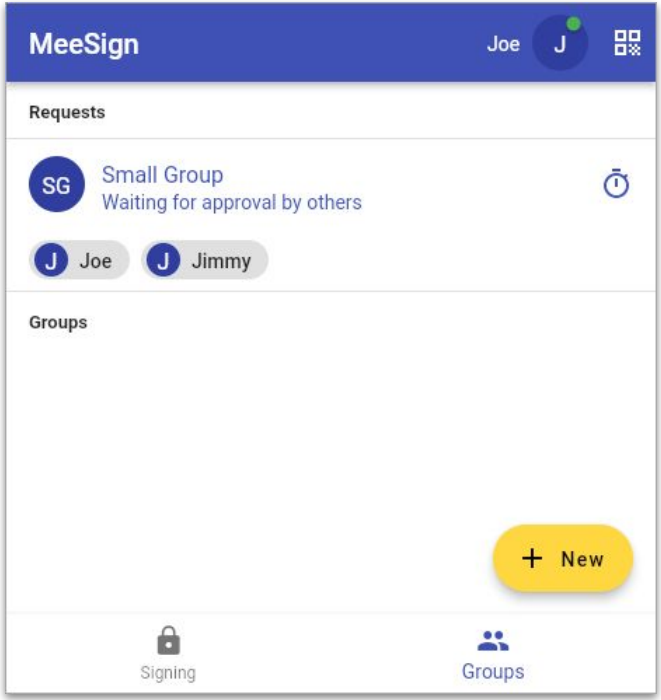
Demo – Vytvoření skupiny

4. Vytvořte skupiny ze dvou účastníků
   - Nabídka Groups → New (vpravo dole)
   - Zvolte název skupiny
   - Přidejte členy pomocí New member jedním ze způsobů:
     - Načíst QR kód (Scan QR code)
     - Vyhledávat podle jména (Search peer)
   - Stisknout Create (vpravo nahoře)
   - Potvrdit notifikaci o účasti v nové skupině (zobrazí se jen ostatním členům)



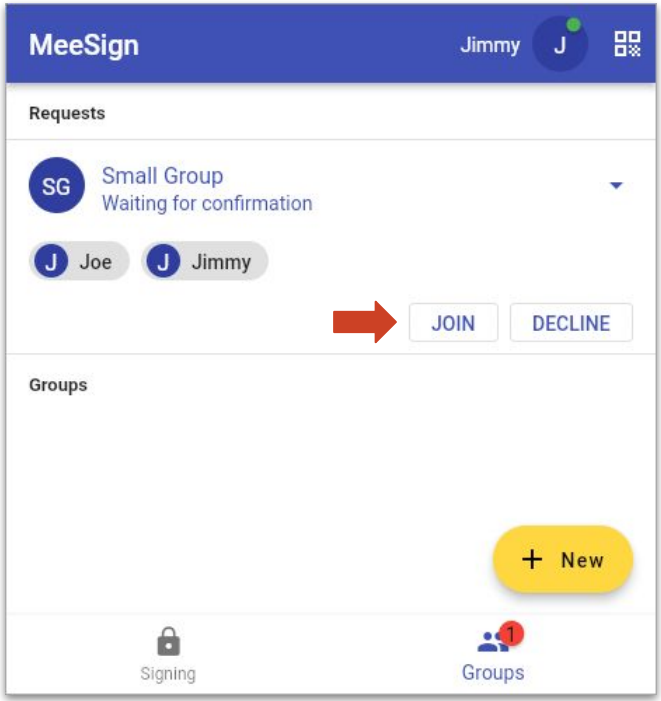
Demo – Vytvoření skupiny

4. Vytvořte skupiny ze dvou účastníků
   - Nabídka Groups → New (vpravo dole)
   - Zvolte název skupiny
   - Přidejte členy pomocí New member jedním ze způsobů:
     - Načíst QR kód (Scan QR code)
     - Vyhledávat podle jména (Search peer)
   - Stisknout Create (vpravo nahoře)
   - Potvrdit notifikaci o účasti v nové skupině (zobrazí se jen ostatním členům)



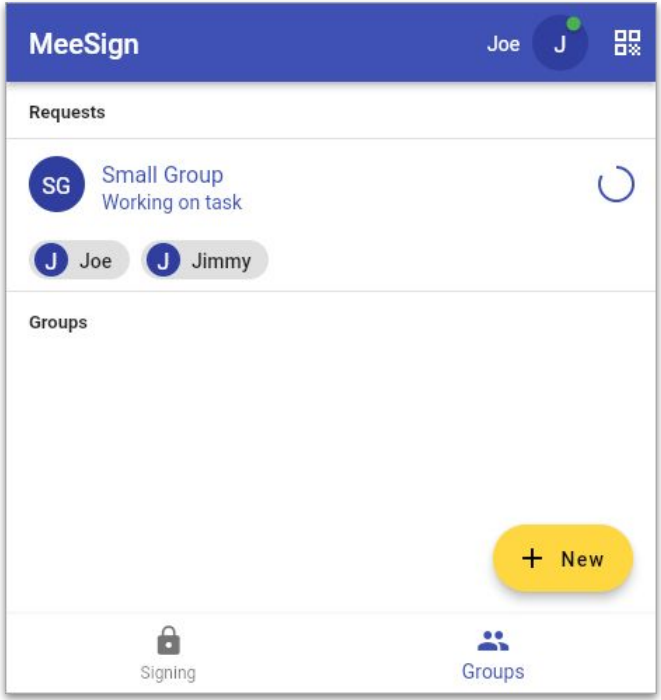
Demo – Vytvoření skupiny

4. Vytvořte skupiny ze dvou účastníků
   - Nabídka Groups → New (vpravo dole)
   - Zvolte název skupiny
   - Přidejte členy pomocí New member jedním ze způsobů:
     - Načíst QR kód (Scan QR code)
     - Vyhledávat podle jména (Search peer)
   - Stisknout Create (vpravo nahoře)
   - Potvrdit notifikaci o účasti v nové skupině (zobrazí se jen ostatním členům)



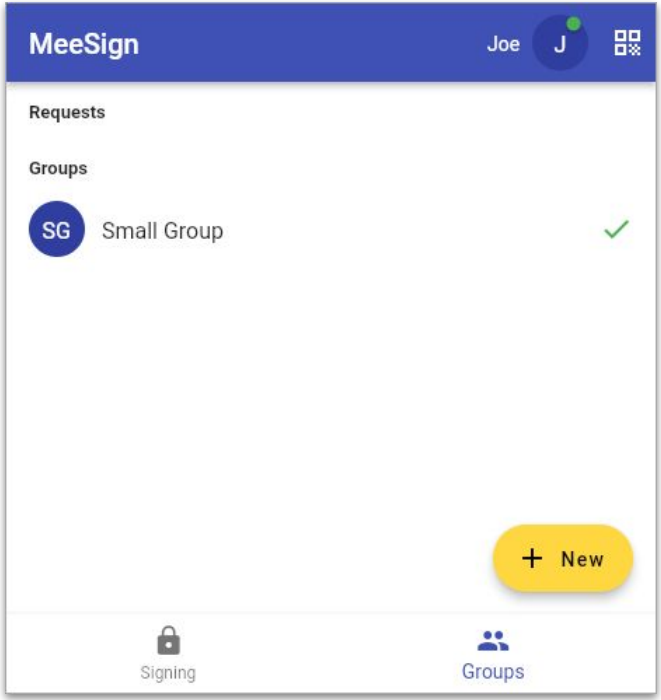
Demo – Vytvoření skupiny

4. Vytvořte skupiny ze dvou účastníků
   - Nabídka Groups → New (vpravo dole)
   - Zvolte název skupiny
   - Přidejte členy pomocí New member jedním ze způsobů:
     - Načíst QR kód (Scan QR code)
     - Vyhledávat podle jména (Search peer)
   - Stisknout Create (vpravo nahoře)
   - Potvrdit notifikaci o účasti v nové skupině (zobrazí se jen ostatním členům)



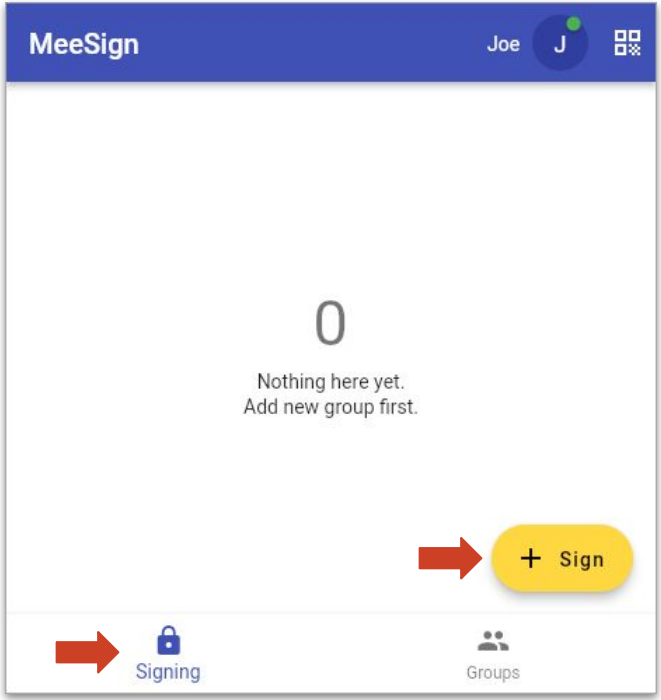
Demo – Vytvoření skupiny

4. Vytvořte skupiny ze dvou účastníků
   - Nabídka Groups → New (vpravo dole)
   - Zvolte název skupiny
   - Přidejte členy pomocí New member jedním ze způsobů:
     - Načíst QR kód (Scan QR code)
     - Vyhledávat podle jména (Search peer)
   - Stisknout Create (vpravo nahoře)
   - Potvrdit notifikaci o účasti v nové skupině (zobrazí se jen ostatním členům)



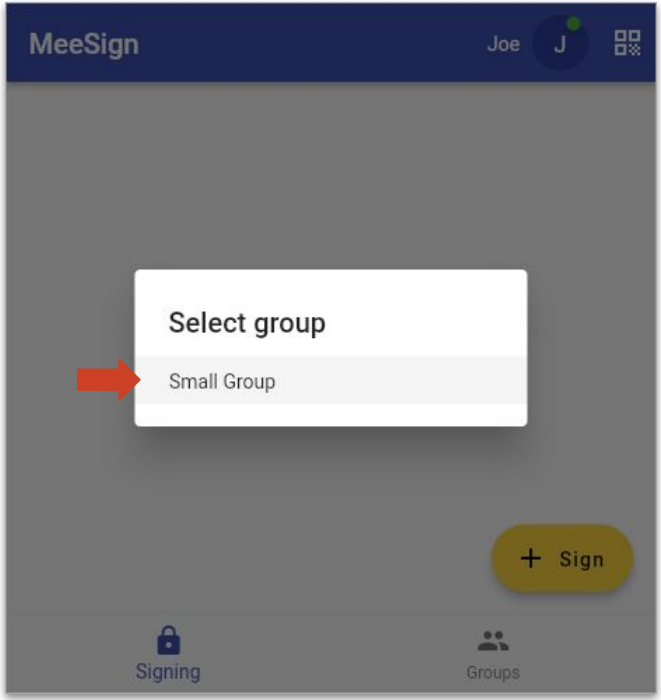
Demo – Podpis dokumentu

5. Skupinově podepište PDF dokument
   - Nabídka Signing → Sign (vpravo dole)
   - Zvolte PDF dokument z vašeho zařízení
     - Ukázkové PDF ke stažení na http://192.168.1.2/
   - Zvolte podepisující skupinu
   - Členům skupiny přijde notifikace s žádostí o podpis dokumentu
     - Zobrazit před podepsáním
     - Podepsat
     - (Zamítnout)
   - Zobrazit podepsaný dokument



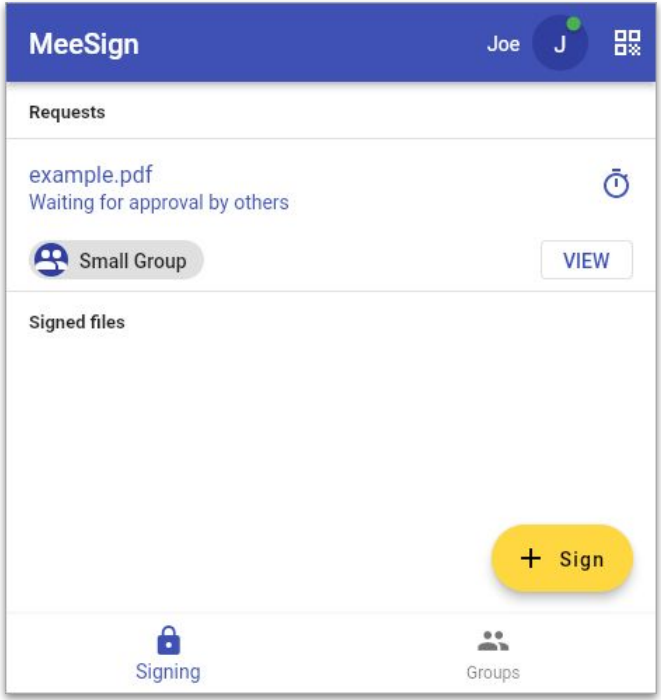
Demo – Podpis dokumentu

5. Skupinově podepište PDF dokument
   - Nabídka Signing → Sign (vpravo dole)
   - Zvolte PDF dokument z vašeho zařízení
     - Ukázkové PDF ke stažení na http://192.168.1.2/
   - Zvolte podepisující skupinu
   - Členům skupiny přijde notifikace s žádostí o podpis dokumentu
     - Zobrazit před podepsáním
     - Podepsat
     - (Zamítnout)
   - Zobrazit podepsaný dokument



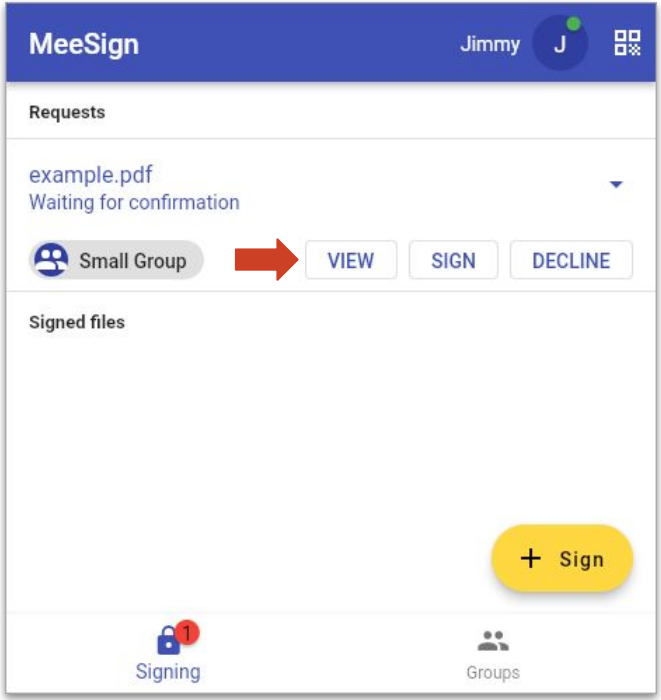
Demo – Podpis dokumentu

5. Skupinově podepište PDF dokument
   - Nabídka Signing → Sign (vpravo dole)
   - Zvolte PDF dokument z vašeho zařízení
     - Ukázkové PDF ke stažení na http://192.168.1.2/
   - Zvolte podepisující skupinu
   - Členům skupiny přijde notifikace s žádostí o podpis dokumentu
     - Zobrazit před podepsáním
     - Podepsat
     - (Zamítnout)
   - Zobrazit podepsaný dokument



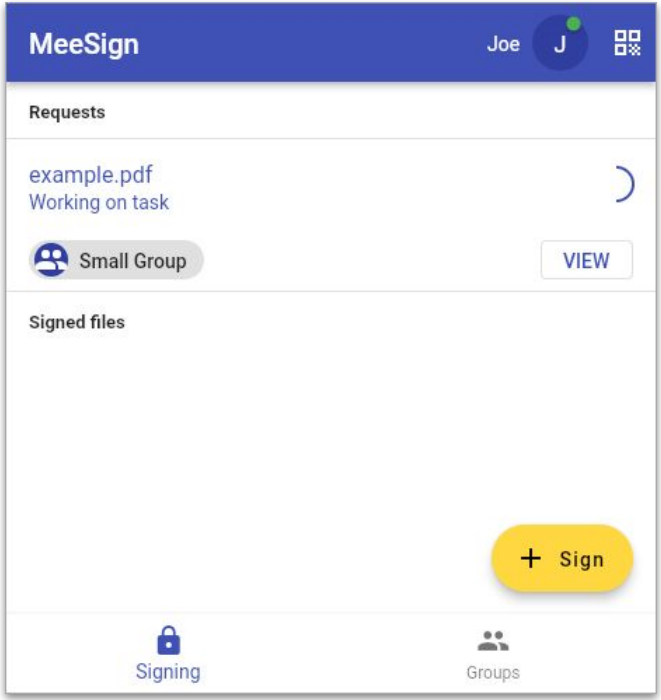
Demo – Podpis dokumentu

5. Skupinově podepište PDF dokument
   - Nabídka Signing → Sign (vpravo dole)
   - Zvolte PDF dokument z vašeho zařízení
     - Ukázkové PDF ke stažení na http://192.168.1.2/
   - Zvolte podepisující skupinu
   - Členům skupiny přijde notifikace s žádostí o podpis dokumentu
     - Zobrazit před podepsáním
     - Podepsat
     - (Zamítnout)
   - Zobrazit podepsaný dokument



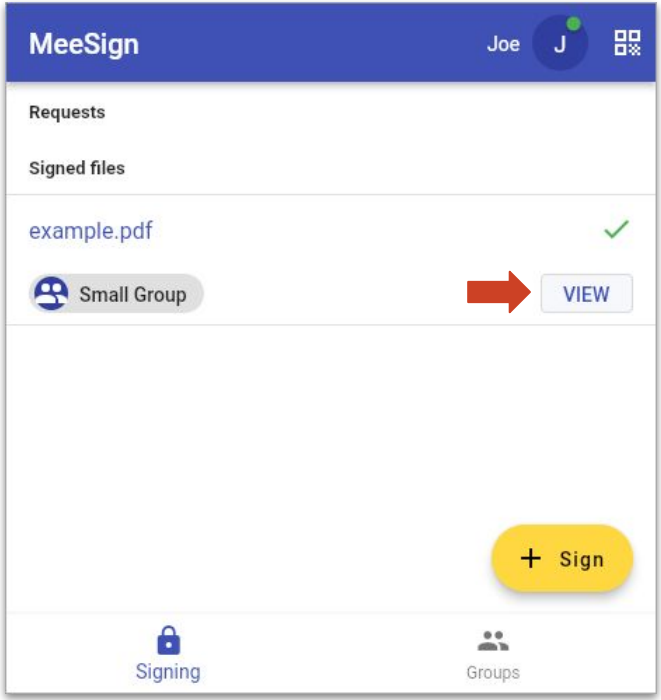
Demo – Podpis dokumentu

5. Skupinově podepište PDF dokument
   - Nabídka Signing → Sign (vpravo dole)
   - Zvolte PDF dokument z vašeho zařízení
     - Ukázkové PDF ke stažení na http://192.168.1.2/
   - Zvolte podepisující skupinu
   - Členům skupiny přijde notifikace s žádostí o podpis dokumentu
     - Zobrazit před podepsáním
     - Podepsat
     - (Zamítnout)
   - Zobrazit podepsaný dokument



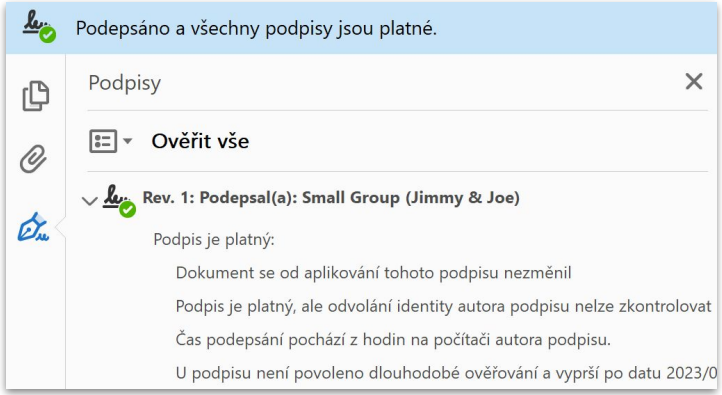
Demo – Podpis dokumentu

5. Skupinově podepište PDF dokument
   - Nabídka Signing → Sign (vpravo dole)
   - Zvolte PDF dokument z vašeho zařízení
     - Ukázkové PDF ke stažení na http://192.168.1.2/
   - Zvolte podepisující skupinu
   - Členům skupiny přijde notifikace s žádostí o podpis dokumentu
     - Zobrazit před podepsáním
     - Podepsat
     - (Zamítnout)
   - Zobrazit podepsaný dokument

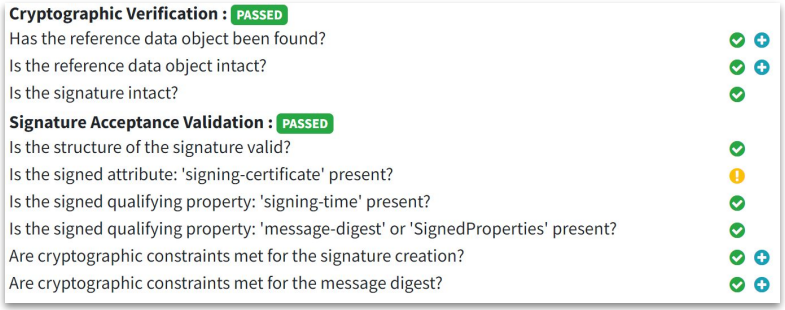


Demo – Verifikace podpisu dokumentu

6. Ověřte výsledný podpis dokumentu
   - Adobe Acrobat Reader
   - pdfsig (poppler-utils)
   - Online nástroj https://ec.europa.eu/digital-building-blocks/DSS/webapp-demo/validation

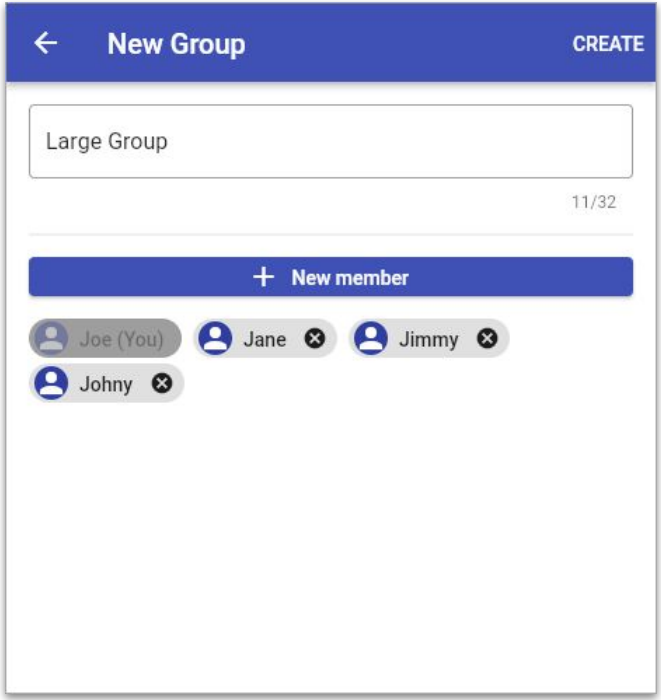



```
↳ pdfsig example.pdf
Digital Signature Info of: example.pdf
Signature #1:
  - Signer Certificate Common Name: Small Group (Jimmy & Joe)
  - Signer full Distinguished Name: CN=Small Group (Jimmy & Joe)
  - Signing Time: May 27 2022 09:05:26
  - Signing Hash Algorithm: SHA-256
  - Signature Type: adbe.pkcs7.detached
  - Signed Ranges: [0 - 106317], [125263 - 125849]
  - Total document signed
  - Signature Validation: Signature is Valid.
  - Certificate Validation: Certificate issuer isn't Trusted.
```



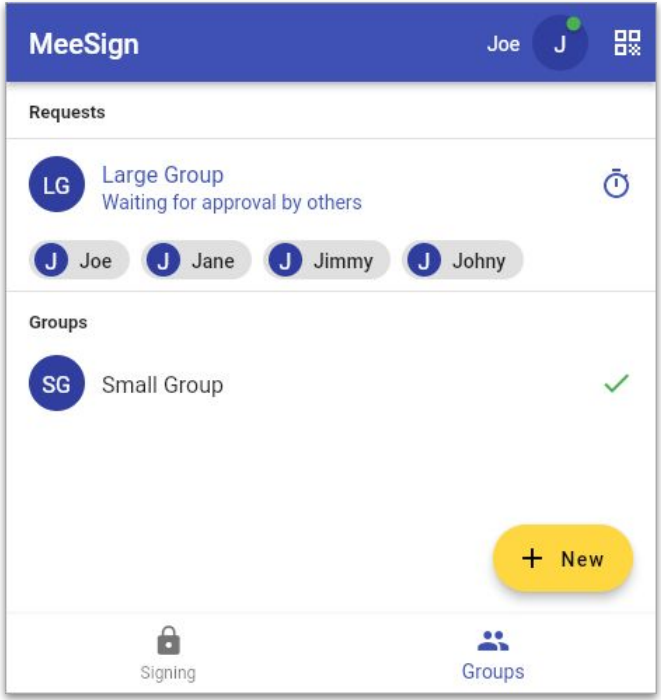
Demo – Podpis větší skupinou

7. Zopakujte vytváření skupiny a podpis s více účastníky (alespoň 8)



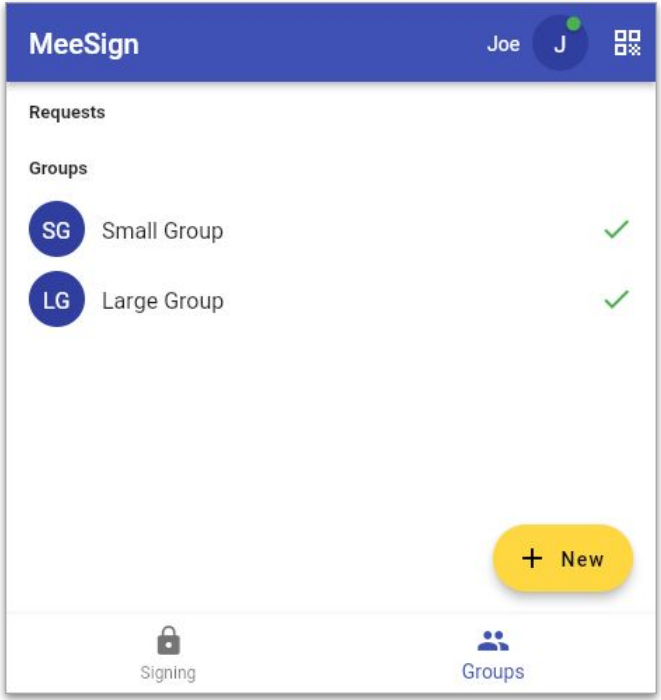
Demo – Podpis větší skupinou

7. Zopakujte vytváření skupiny a podpis s více účastníky (alespoň 8)



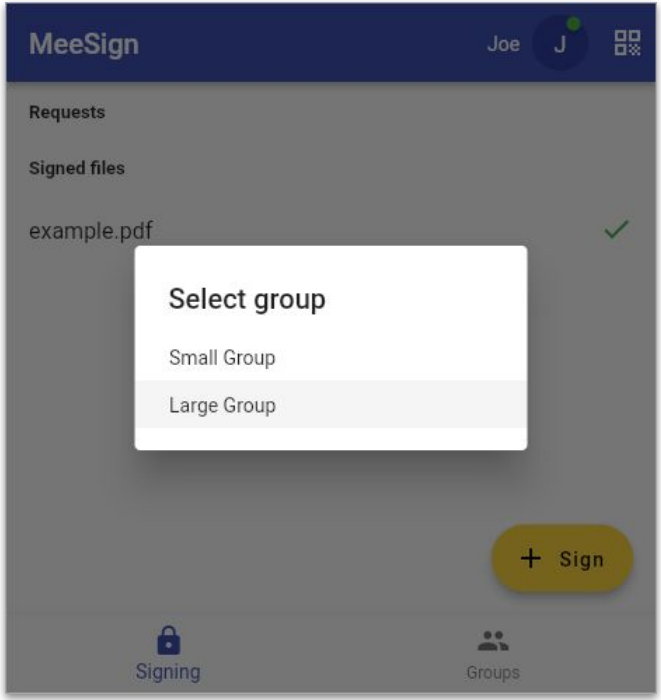
Demo – Podpis větší skupinou

7. Zopakujte vytváření skupiny a podpis s více účastníky (alespoň 8)



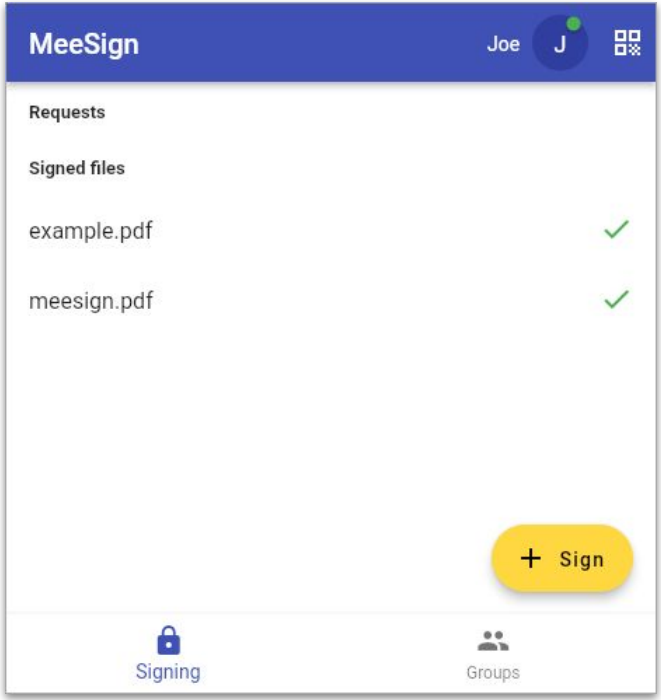
Demo – Podpis větší skupinou

7. Zopakujte vytváření skupiny a podpis s více účastníky (alespoň 8)



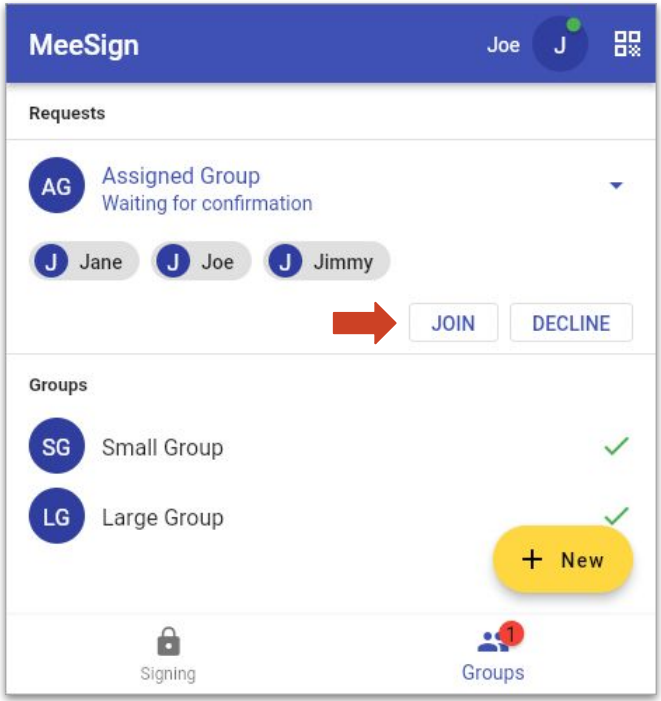
Demo – Podpis větší skupinou

7. Zopakujte vytváření skupiny a podpis s více účastníky (alespoň 8)



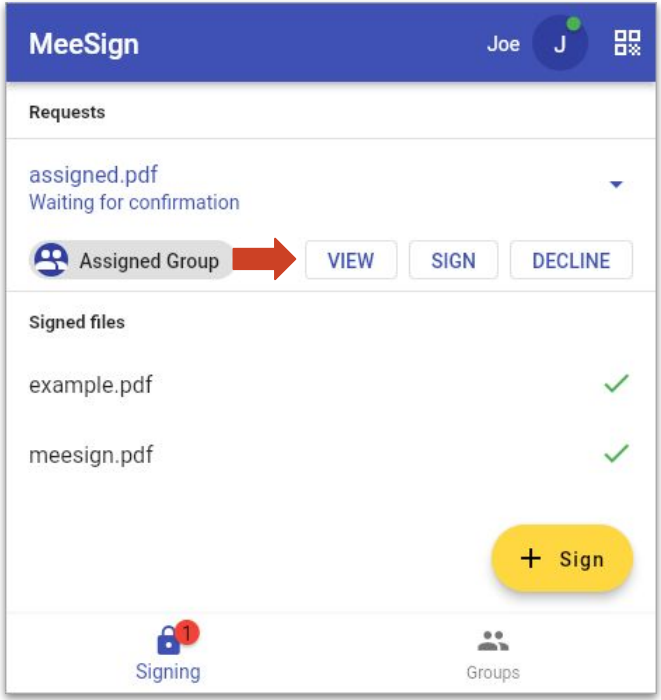
Demo – Přiřazená skupina

8. Připojte se do centrálně vytvářené skupiny
   - Žádosti mohou být zasílány například informačním systémem
   - Potvrďte příchozí notifikaci



Demo – Přiřazené podepisování

9. V rámci vytvořené skupiny podepište dokument
   - Žádosti mohou být opět zasílány například informačním systémem
   - Prohlédněte si podepisovaný dokument a podepište jej



Děkujeme za pozornost

Antonín Dufka
dufkan@mail.muni.cz

Jakub Janků
514496@mail.muni.cz

Jiří Gavenda
484647@mail.muni.cz

Petr Švenda
svenda@fi.muni.cz

MVČR Impakt VJ01010084

https://meesign.crocs.fi.muni.cz/