MeeSign: Threshold cryptography demonstrator

How to convince decision makers to use threshold cryptography?

Antonín Dufka, Robi Chmelík, Jiří Gavenda, Jakub Janků,
Jan Kvapil, Kristián Mika, Marek Mračna, Petr Švenda
Masaryk University, Czechia

Supported under projects MVČR Impakt VJ01010084, CHESS No. 101087529

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

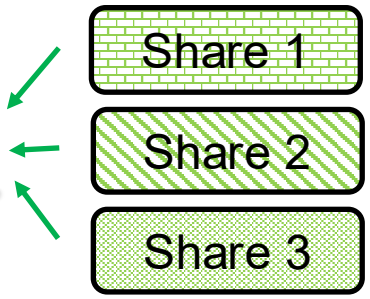
CROCS
Centre for Research on Cryptography and Security

Funded by the European Union

Analogically for decryption and authentication (multiple people to decrypt / authenticate, k-of-n)

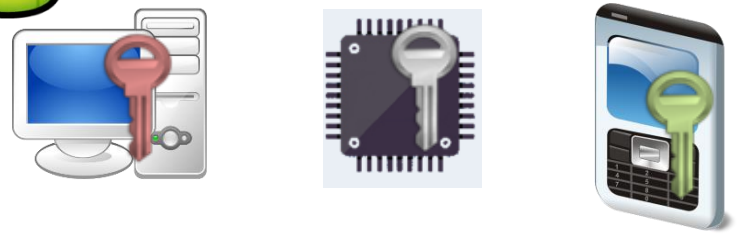
Single signature

Shamir TSS



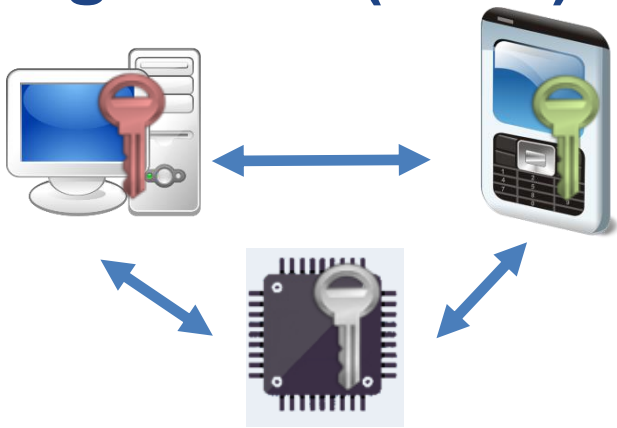
Signature

Multiple signatures



Signature | Signature | Signature

Threshold Signature (MPC)



Signature

Goals of threshold cryptography

1. Remove single point of failure
   - Reduce trust requirements (no single party can fail you)
   - Better protect against attacks like malware (no single device with full key)
2. Provide fault tolerance (n-of-n vs. k-of-n)
   - Perform operation with some parties not available / not cooperating
3. Enable enforcement of signing/decryption policies / rules
   - Regulatory requirements (e.g., “four eyes principle”)
   - Operational requirements (e.g., sign txs only below 10k, only in working hours)

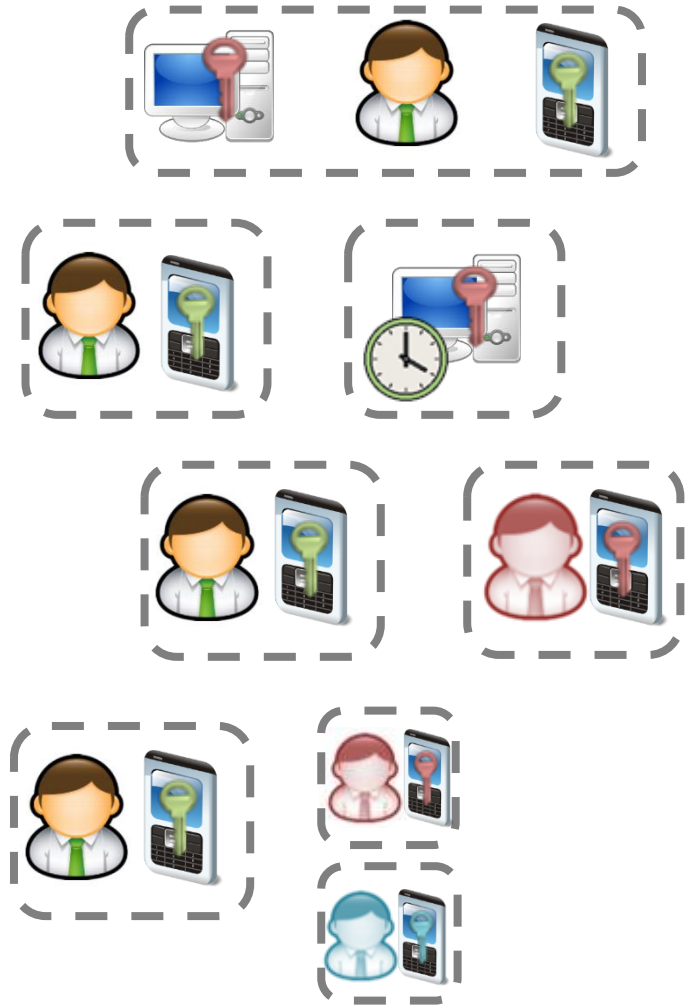
High-level usage scenarios

Backward compatibility with existing deployments (only one side needs change)

1. Digital signature
   - Multiple signers to create signature, single public key to verify
2. User authentication
   - Multiple people to confirm login, single public key to verify
3. Data decryption
   - Single public key to encrypt, multiple participants to decrypt later
4. Key / randomness generation
   - Multiple participants contribute to random number generation

Threshold cryptography – configurations

- 2-of-2: one user, two devices
  - (higher security against device compromise)
- 2-of-2: one user, one server-side automatic process
  - (check time interval when signing is allowed)
- 2-of-2: two users (user, approving controller)
  - (access must be approved by controller)
- 2-of-3: three users (user, redundant approvers)
  - (one user, two controllers – one approval is enough)
- Bonus: Independent log of authentication attempt



How practical is this?

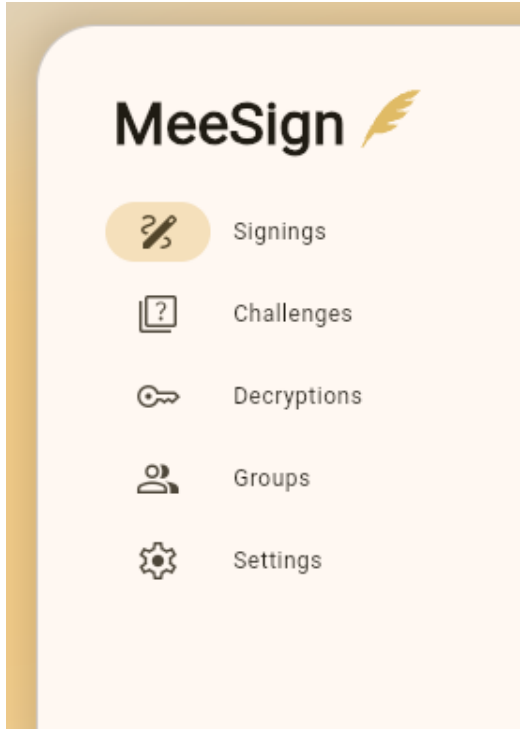
- Smart-ID (2-of-2 RSA signature, phone and server/HSM)
- X-Road (2-of-2 RSA/ECDSA, user and security server)
- Exchanges (2-of-3 ECDSA, 4-of-5, native multisig vs. threshold)
  - BitGo, Unchained Capital, Casa, Blockstream…
- Hardware wallets (2-of-3, e.g., FrostSnap)
- Liquid consortium (11-of-15 native multisig)
- Lighting open channel (2-of-2 Schnorr signature)
- Digitalization of company flow (multiple signatures), Timing-limitation, Third-party confirmation, Geopolitics

MeeSign demonstrator

PROBLEM:
I AM HOOKED,
BUT MY CEO/CTO/HEAD IS NOT

Start your demo client

1. Visit page https://meesign.crocs.fi.muni.cz/client
2. Fill name, click Register, Wait ☺



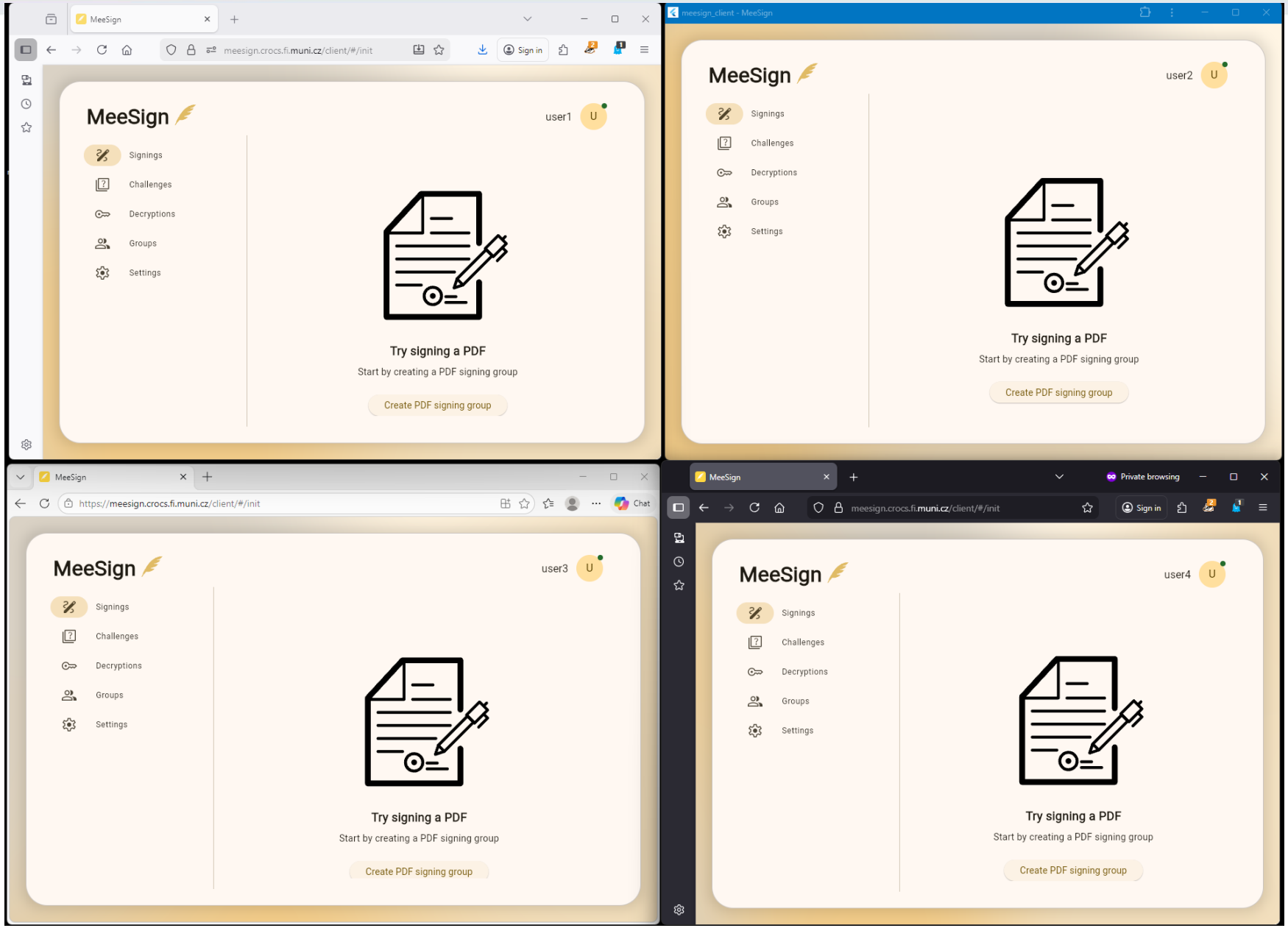
HANDS-ON:
1. LARGE GROUP PDF SIGNING
2. LARGE DATA DECRYPTION
3. SMALLER GROUP PDF SIGNING
4. SSH LOGIN AUTHORIZATION

Task1: Signing as a large group

- New group ‘pdfSigLarge’ created by tutor
  - Threshold set to N-2
  - Participants (signers) added by nickname
- Confirm yourself into group when prompted
- Tutor starts signing of document, you wait for in-app notification

---

- Participant opens pdf document proposed, Sign afterwards
- Wait for the finalization (N-2 people needed)
- Check yourself properties of the resulting multiparty signature
  - E.g., Adobe Reader


MeeSign
meesign.crocs.fi.muni.cz/client/#/init
Sign in
MeeSign
user1
Signings
Challenges
Decryptions
Groups
Settings
Try signing a PDF
Start by creating a PDF signing group
Create PDF signing group
meesign_client - MeeSign
MeeSign
user2
Signings
Challenges
Decryptions
Groups
Settings
Try signing a PDF
Start by creating a PDF signing group
Create PDF signing group
MeeSign
https://meesign.crocs.fi.muni.cz/client/#/init
Chat
MeeSign
user3
Signings
Challenges
Decryptions
Groups
Settings
Try signing a PDF
Start by creating a PDF signing group
Create PDF signing group
MeeSign
Private browsing
meesign.crocs.fi.muni.cz/client/#/init
Sign in
MeeSign
user4
Signings
Challenges
Decryptions
Groups
Settings
Try signing a PDF
Start by creating a PDF signing group
Create PDF signing group

Try signing a PDF

Start by creating a PDF signing g

Create PDF signing group

MeeSign

user1 U

Signings

Challenges

Decryptions

Groups

Settings

Back

New group

Group Name

pdfSigLarge

11/32

Members

Add members

U user1 1

Decrypt

Back

New group

Group Name

pdfSigLarge

11/32

Members

Add members

U user1 1

U user2 1

U user3 1

U user4 1

Threshold

3

Purpose

Sign PDF | Challenge | Decrypt

user1 U

Search for peer

Add | Reload

U user2 | U user3 | U user4

Q quapkaFirefoxMobile

ae00 cab1 ebc8 76bc 62a4 cacf c429 cb70 9ff3 e133

U user2

a324 89b5 fe72 24c2 c013 cf1b c4a4 999b f4d9 51d9

U user3

2173 d0e5 038f 7194 af12 be91 6d6b 9549 ade9 6fd8

U user4

d86b e45b cae5 8c3f 2d74 993f d748 7806 b47e 19ac

MeeSign

user1 U

Signings

Challenges

Decryptions

Groups

Settings

Groups

Search groups by name...

Show only pending

Reload groups

pdfSigLarge

P Sign PDF

Waiting for confirmation

U user3 | U user2 | U user1 | U user4

Join | Decline

New group

Try signing a PDF

Start by creating a new PDF signing task

Create PDF signing

New signature

Back

Create new task

Type of task

Sign PDF | Challe

Select group for the new task

pdfSigLarge

Select PDF

Change file

ee_demo1.pdf

Create PDF signing task

ee_demo1.pdf

Sign PDF

Waiting for confirmation by others

P pdfSigLarge

MeeSign

user1 U

Signings

Challenges

Decryptions

Groups

Settings

Signings

Search tasks by name...

Show only pending

Reload tasks

ee_demo1.pdf

Sign PDF

Waiting for confirmation

P pdfSigLarge

Sign

Decline

Preview Document

New signature

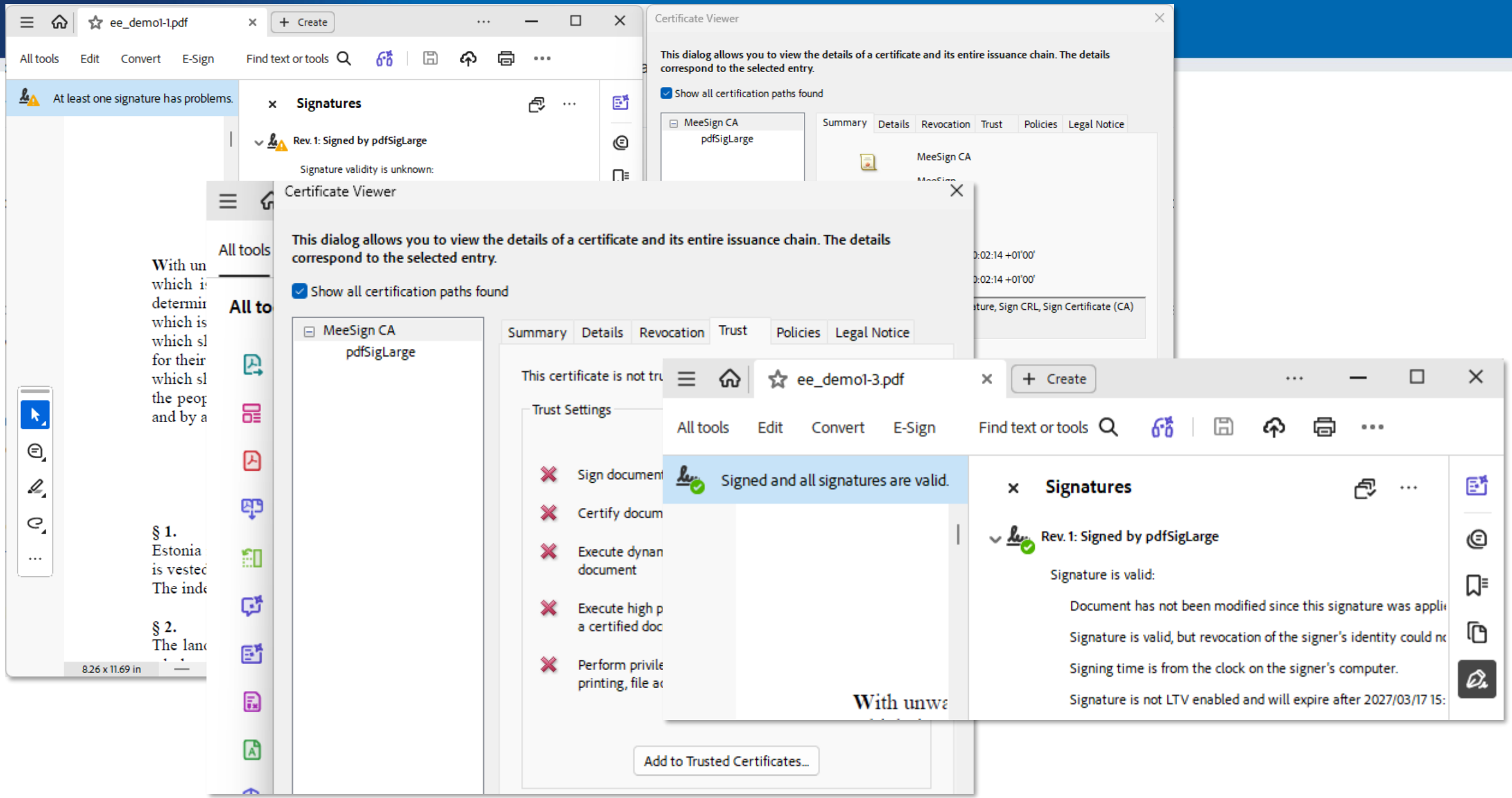
ee_demo1.pdf

Sign PDF

P pdfSigLarge

View

Copy

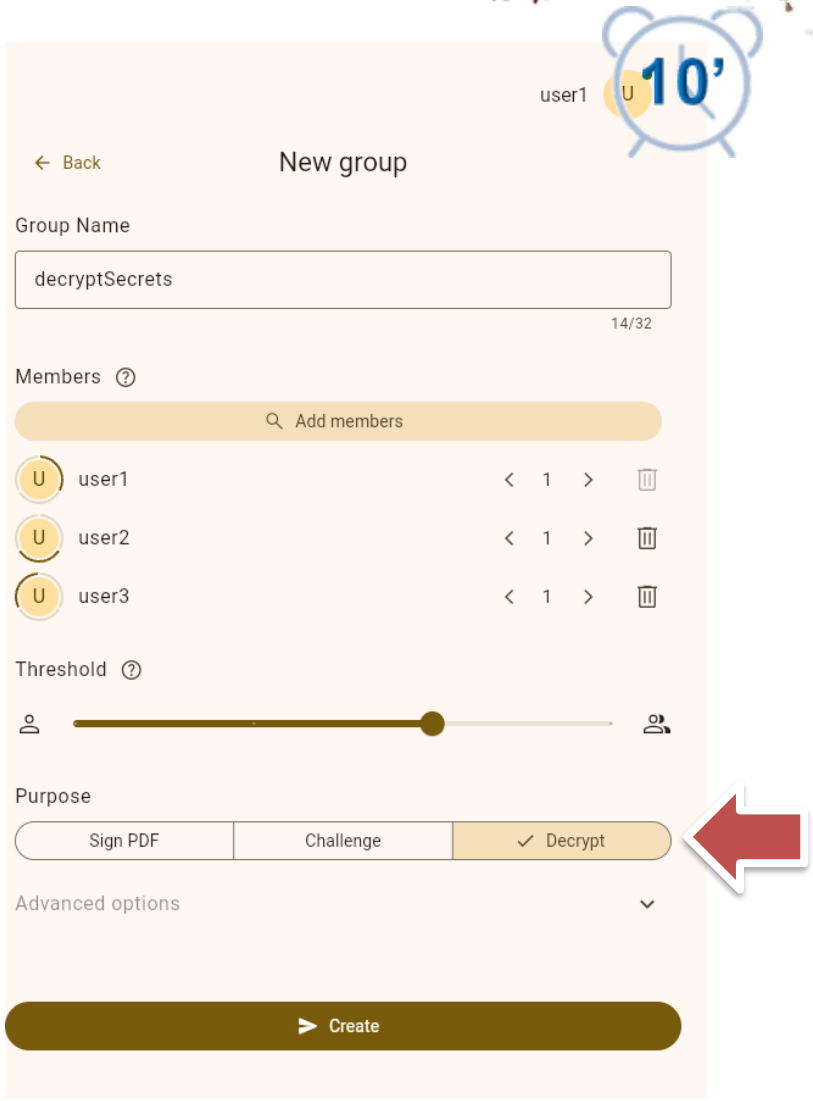

ee_demo1-1.pdf
Create
All tools
Edit
Convert
E-Sign
Find text or tools
At least one signature has problems.
Signatures
Rev. 1: Signed by pdfSigLarge
Signature validity is unknown:
Certificate Viewer
This dialog allows you to view the details of a certificate and its entire issuance chain. The details correspond to the selected entry.
Show all certification paths found
MeeSign CA
pdfSigLarge
Summary
Details
Revocation
Trust
Policies
Legal Notice
Trust Settings
Add to Trusted Certificates...
ee_demo1-3.pdf
Signed and all signatures are valid.
Rev. 1: Signed by pdfSigLarge
Signature is valid:
Document has not been modified since this signature was applie
Signature is valid, but revocation of the signer's identity could nc
Signing time is from the clock on the signer's computer.
Signature is not LTV enabled and will expire after 2027/03/17 15:

Notes for large group signature

- Only one user creates group with given parameters
- User must explicitly participate in group creation (distributed key generation)
  - Can be relaxed, e.g., trusted dealer of participant key shares…
- If enough participants sign, signature is produced and embed into pdf
- Any pdf viewer (Acrobat Reader) can be use to display and validate
  - Group's public key needs to be certified, signed by MeeSign CA for this demo
    => Warning mark on signature, needs set trust to MeeSign CA

Task 2: Multiparty decryption

- New group ‘saySecret’ created by tutor
  - Threshold set to N-2
  - Participants (decryptors) added by nickname
- Confirm yourself into group when prompted
- Outside participant encrypt document, you wait for in-app notification
- Participant agrees for decryption
- Wait for the finalization (N-2 people needed)
- Check the result (View)



← Back

Create new task

Type of task

Sign PDF | Challenge | Decrypt

Select group for the new task

saySecret — Info

Name of the decryption task

meeting notes 2026

Select decryption type

- Decrypt a message
- Decrypt an image

Enter message to be decrypted

The Magic Words are Squeamish Ossifrage

39/100000

Create decryption task

---

meeting notes 2026

Decrypt

Waiting for confirmation

S saySecret

Decrypt | Decline

New encryption

---

user3 U

← Task Detail

Task name Copy

meeting notes 2026

Task value Copy

The Magic Words are Squeamish Ossifrage

Hex value Copy

546865204d6167696320576f726473206172652053717565616d697368204f7373696672616765

Task group

S saySecret

Task 4: Collaborative login to ssh server

- New group ‘sshAuth’ created by tutor
  - Threshold set to N-2
  - Participants (guardians) added by nickname
- Confirm yourself into group when prompted
- When prompted, confirm authentication request

- SSH client → PKCS#11 library → MeeSign → login / command

Task 5: Policy enforcement

- New group ‘oddMinuteSigning’ created by tutor
  - Threshold set to 2-of-2
  - Second participant is auto-signing bot on server (but only in odd minutes)

What to do after this presentation

1. Think about use-case with threshold crypto relevant for your company
   – Leverage its backward compatibility! (RSA, ECDSA…)
2. Use MeeSign demonstrator to convince your decision makers
3. Build your own application for your specific use-case
   – Do not use MeeSign directly – is not security-hardened product
   – Use existing audited libraries like Binance's tss-lib, ZenGo-X's multi-party-ecdsa, Coinbase's Kryptology…

- Thank you for your attention ❤️

MeeSign is open-source and more

- Flutter-based multiplatform demonstration client
- Backend coordination server
- “Bridge” into operating system (PKCS#11, FIDO2…)
- Concrete protocols included, extensible
- Supports also cryptographic smartcards
- Incorporates research and libraries of others
- Utilizes also our own research (e.g., 2-of-2 ECDSA on smartcard)

Two-party ECDSA with JavaCard-based smartcards

Antonin Dufka, Peeter Laud and Petr Svenda,

Applied Cryptography and Network Security: 23rd International Conference on Applied Cryptography and Network, Springer, 2025.

Keywords: smartcards, smpc, ecdsa, javacard, DOI website, paper website, BibTeX

The Power of Many: Securing Organisational Identity Through Distributed Key Management

Mariia Bakhtina, Jan Kvapil, Petr Svenda and Matulevicius Raimundas,

Advanced Information Systems Engineering, Springer Nature Switzerland, 2024, 475–491.

Keywords: distributed control, key management, organisational digital identity, security, threshold signatures, zero trust, pre-print PDF, DOI website,