

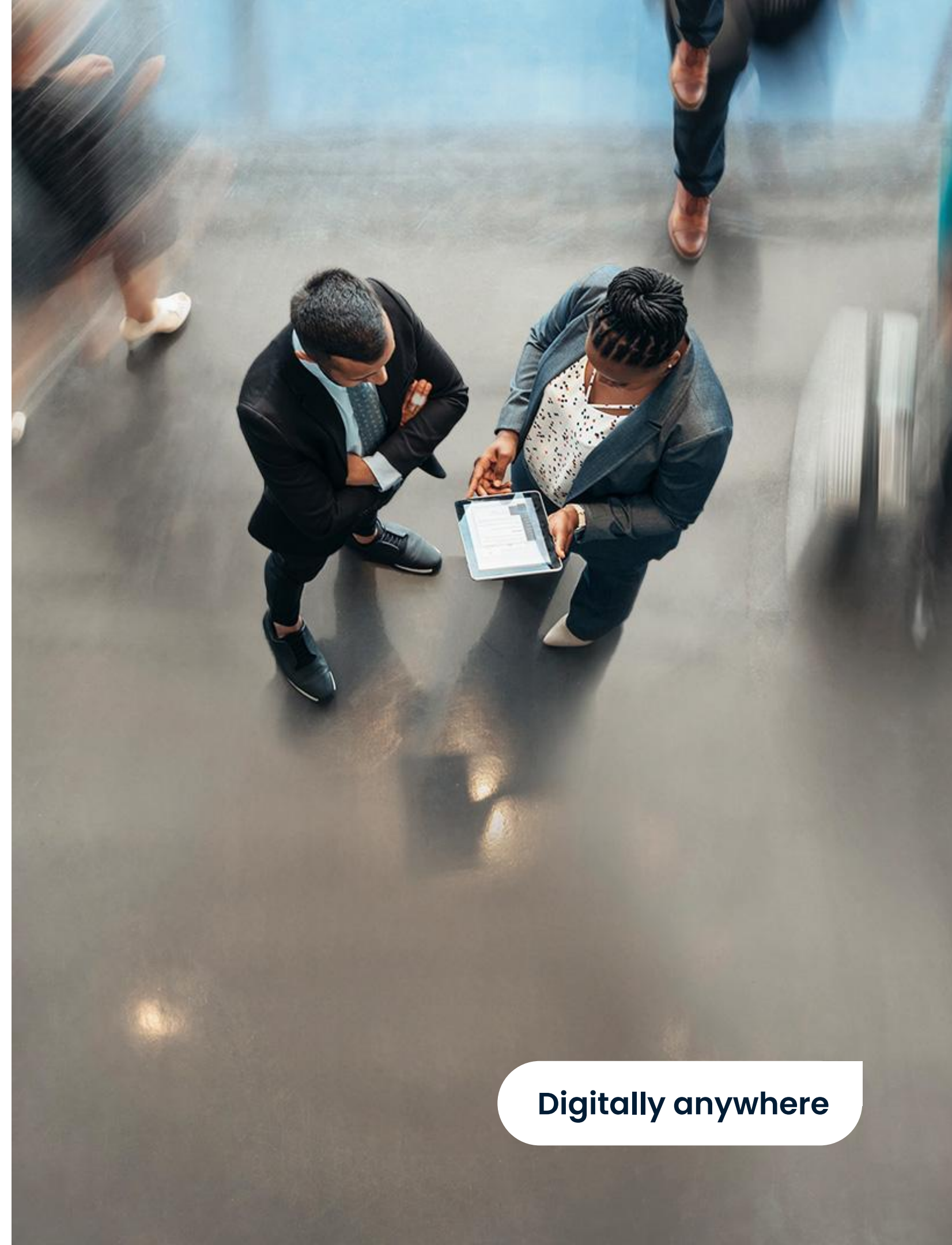
**MONET +**

**System Architecture for**

# **qualified el. signature & document digitization**

**Jiri Zmelik**  
Sales

**Digitally anywhere**



# Why sign electronically?

**Paperless  
(digitization)**

**Cost reduction**

**Easy data transfer**

**Electronic archive**

**Process automation**

**Consent record /  
non-repudiation of liability**

**Expression of Will**

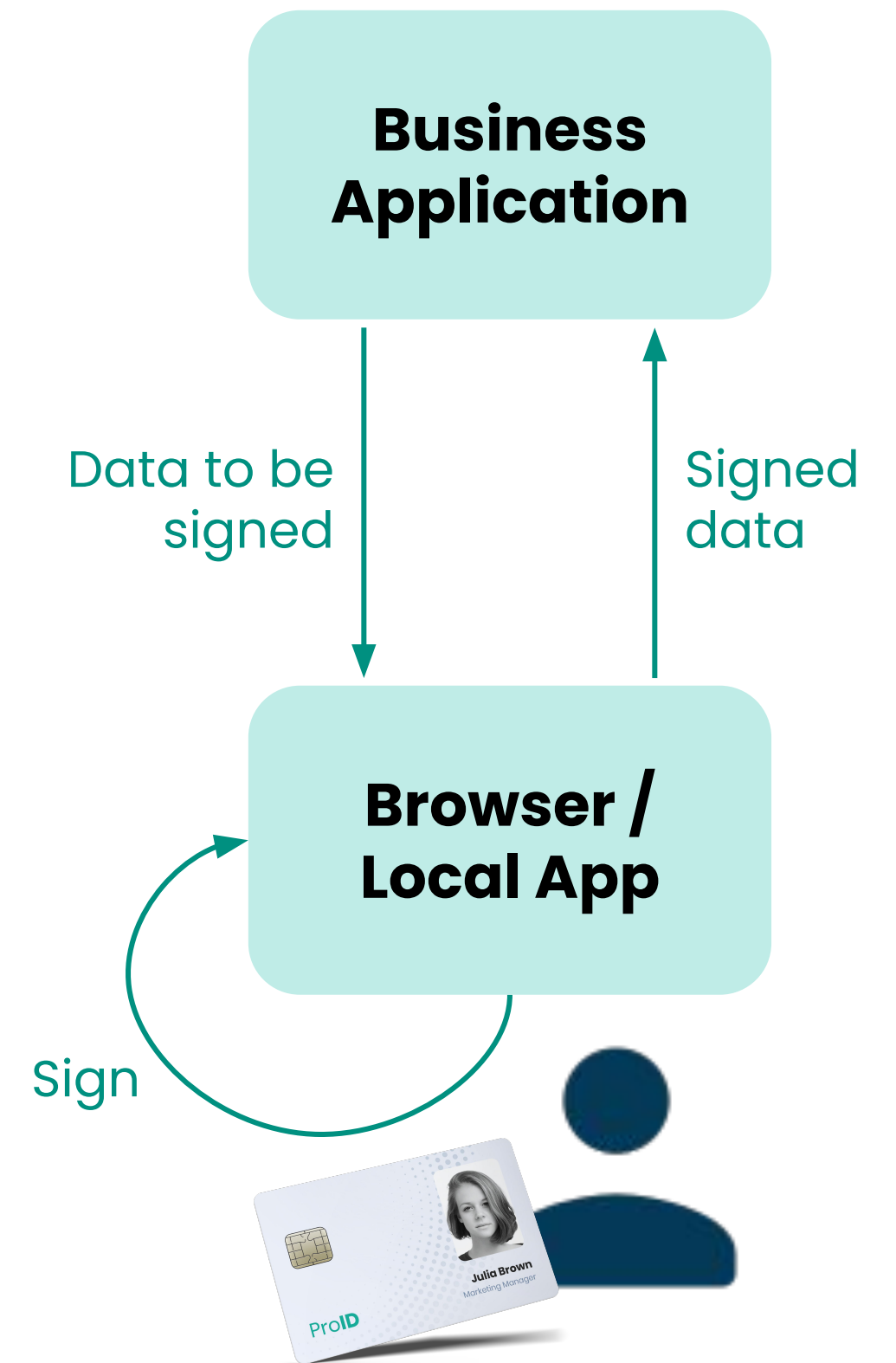
**Data integrity**

**Exposing the falsetto /  
fraud detection**

**Timestamp**

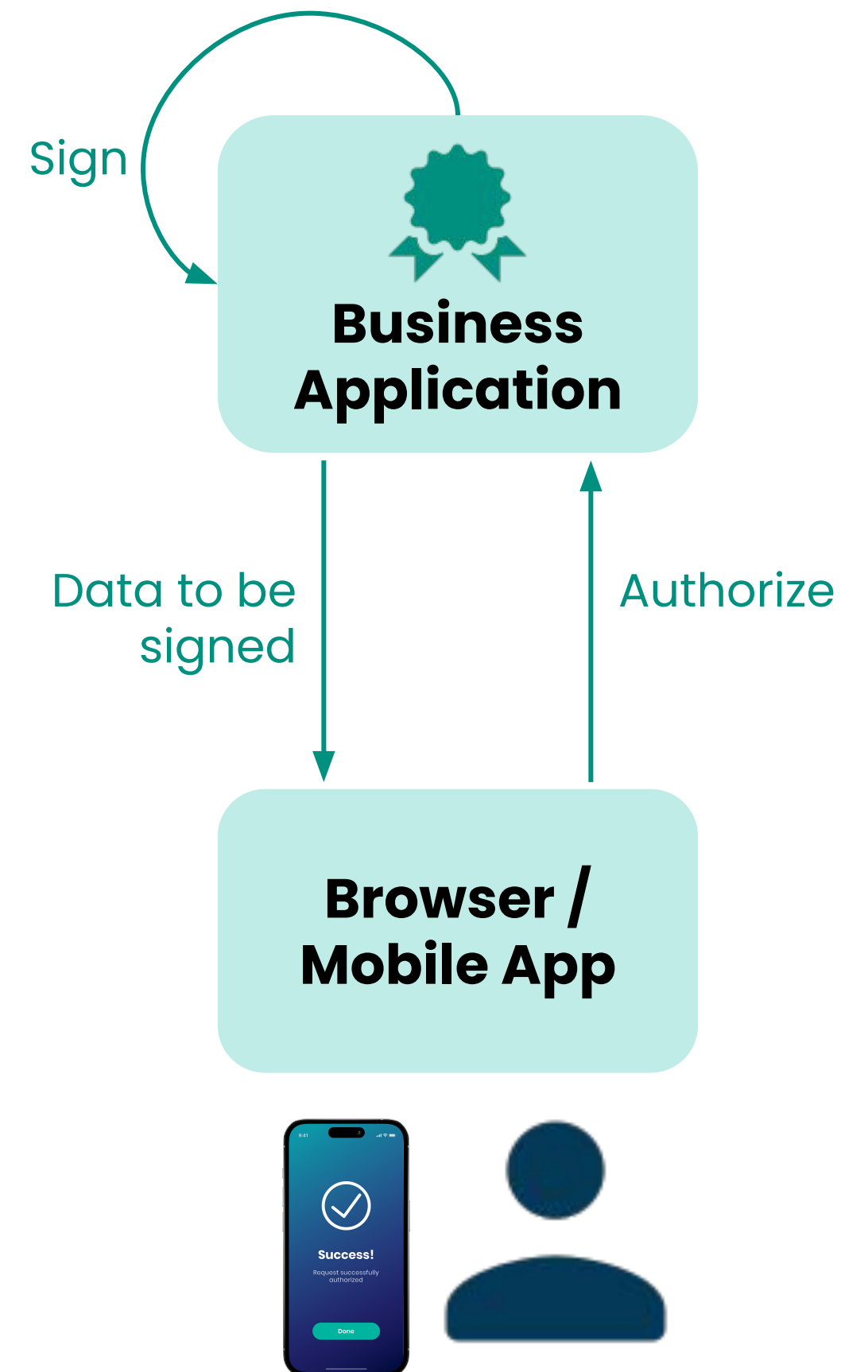
# LOCAL electronic signature

- Key + certificate hold by user
- Token and service application distribution
- Certificate issuance / renewal
- The holder controls the key
- Natural 2-factor
- Badge (visual / electronic / contactless)



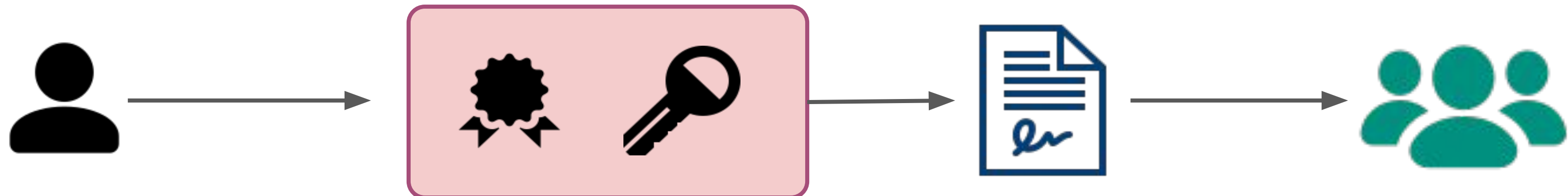
# REMOTE electronic signature

- Key + certificate on the server
- Distribution of the authorisation tool
- Automatic certificate issuance
- Trust in the provider
- Suitable for mobiles / biometrics



# Credibility of remote signature

- Expression of the user's will
- Misuse prevention



## System tech solution

- Standards, regulation, legislation
- Key protection including access
- Connection to CA

## Holder's level of control over key

- Onboarding, identity verification
- Identification tool activation
- Authentication / authorization

# Holder's level of control over the signature key

## SCAL1

### Sole control assurance level 1

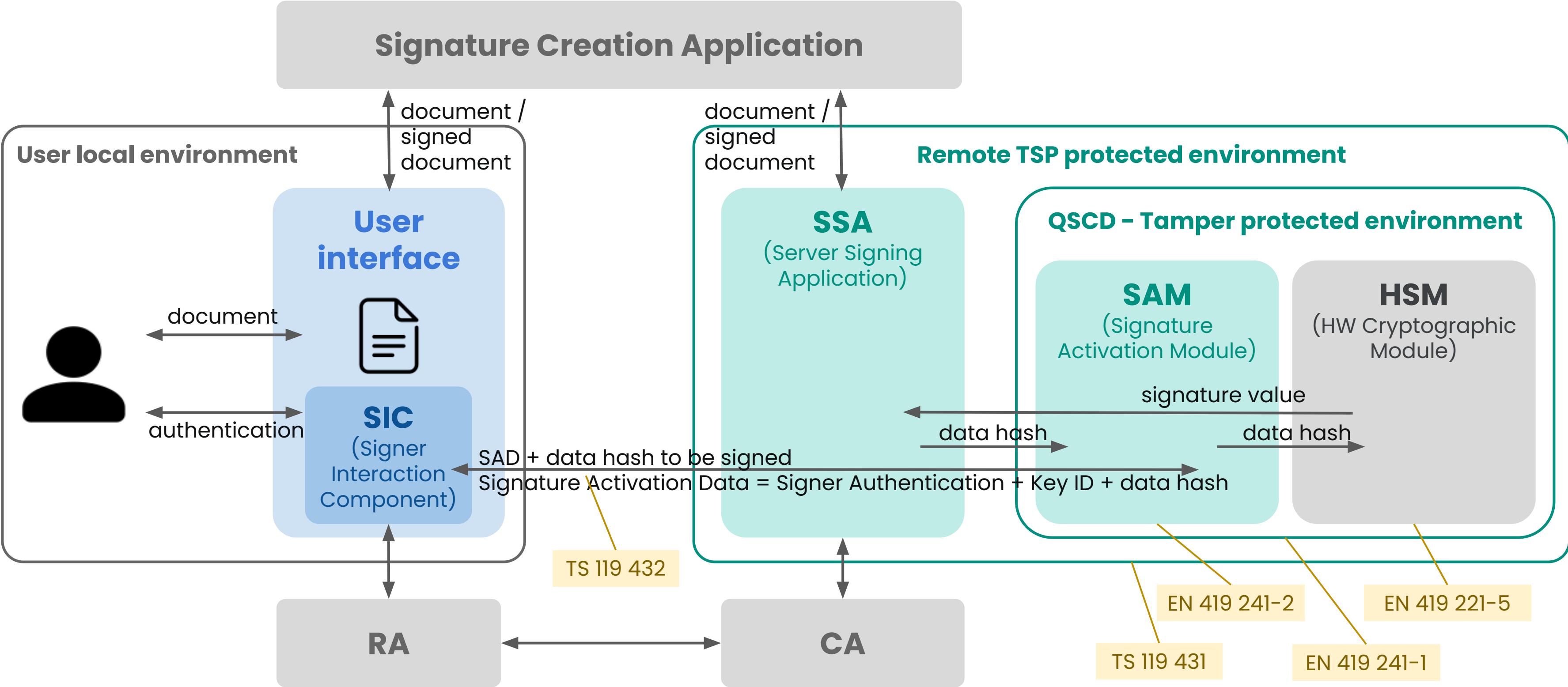
- **Low level** of trust in the signer's control over the signing key
- Use of key based on user authentication
- **Low assurance** level electronic identification tools
- **1-factor** authentication possible

## SCAL2

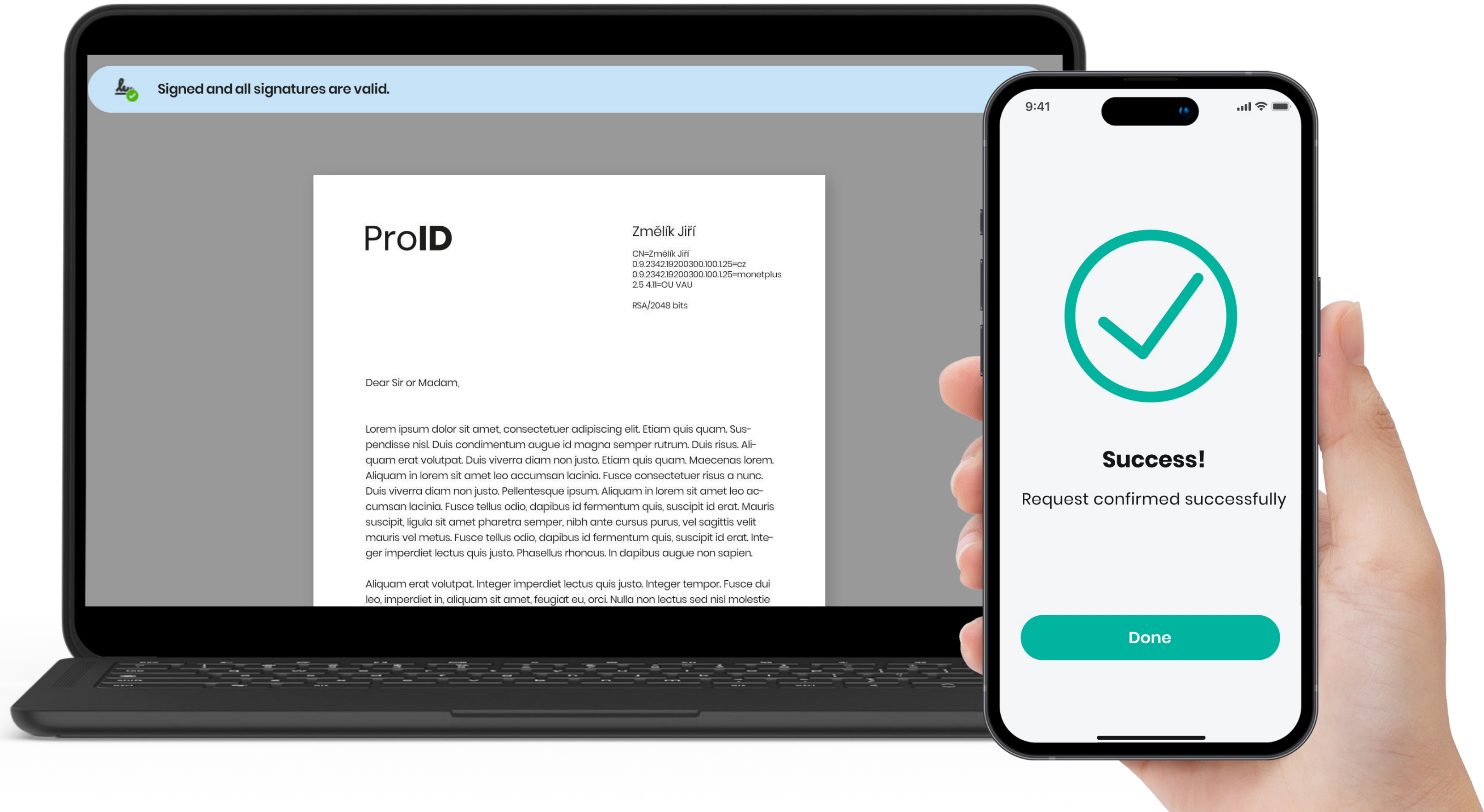
### Sole control assurance level 2

- **High level** of trust in the signer's control over the signing key
- Use of a key based on cryptographically secure data, authorized by the signer
- Hardware Signing Key Security (**HSM**)
- **"Substantial" level** of assurance electronic identification tool
- **At least 2-factor** authentication + dynamic authentication

# Remote signing - system architecture (SCAL2)



# Signature flow



 Signed and all signatures are valid.

## ProID

Změlík Jiří

CN=Změlík Jiří  
0.9.2342.19200300.100.1.25=cz  
0.9.2342.19200300.100.1.25=monetplus  
2.5.4.11=OU VAU  
RSA/2048 bits

Dear Sir or Madam,

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Etiam quis quam. Suspendisse nisl. Duis condimentum augue id magna semper rutrum. Duis risus. Aliquam erat volutpat. Duis viverra diam non justo. Etiam quis quam. Maecenas lorem. Aliquam in lorem sit amet leo accumsan lacinia. Fusce consectetur risus a nunc. Duis viverra diam non justo. Pellentesque ipsum. Aliquam in lorem sit amet leo accumsan lacinia. Fusce tellus odio, dapibus id fermentum quis, suscipit id erat. Mauris suscipit, ligula sit amet pharetra semper, nibh ante cursus purus, vel sagittis velit mauris vel metus. Fusce tellus odio, dapibus id fermentum quis, suscipit id erat. Integer imperdiet lectus quis justo. Phasellus rhoncus. In dapibus augue non sapien.

Aliquam erat volutpat. Integer imperdiet lectus quis justo. Integer tempor. Fusce dui leo, imperdiet in, aliquam sit amet, feugiat eu, orci. Nulla non lectus sed nisl molestie

9:41



**Success!**

Request confirmed successfully

Done

# Signed data - formats

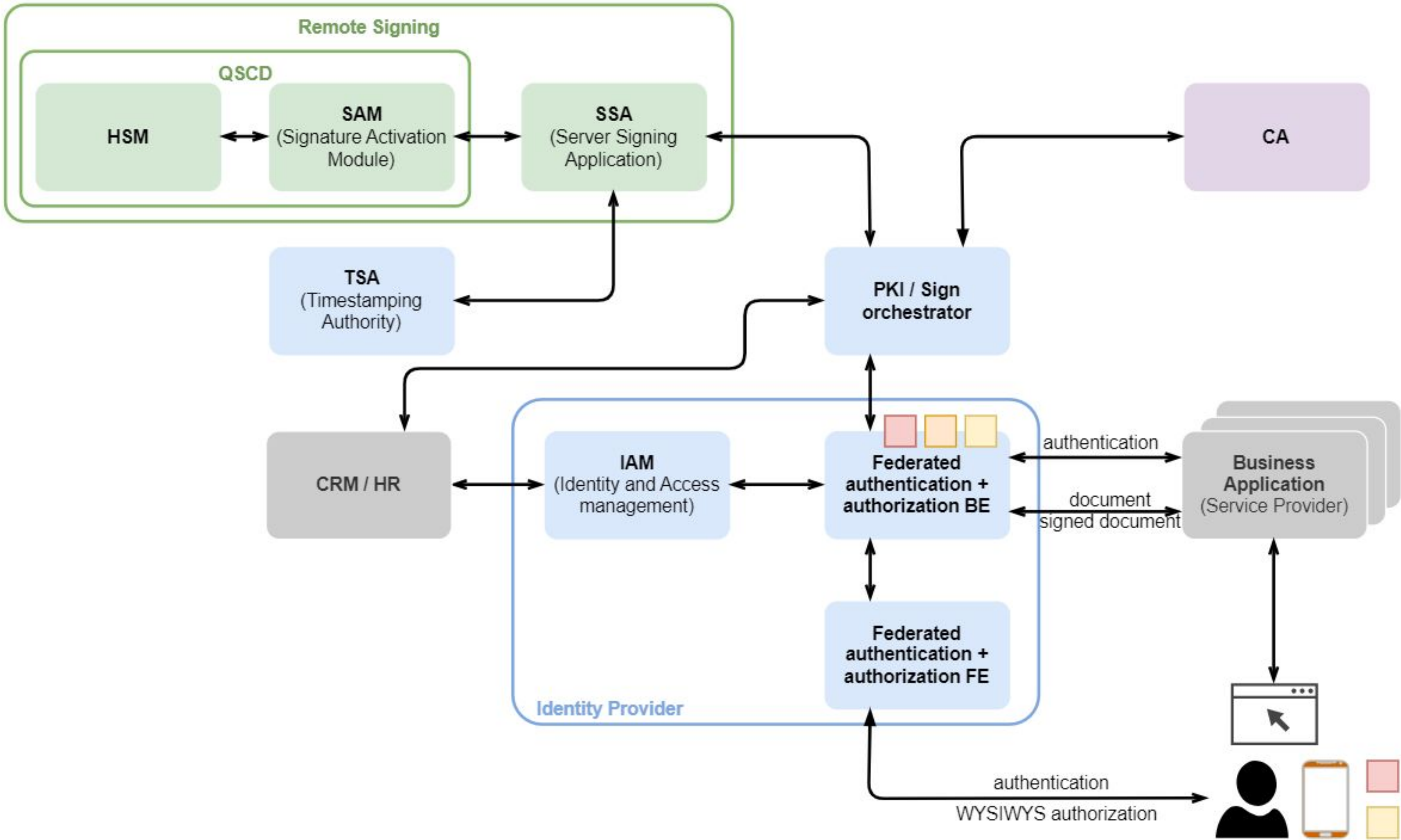
## File type:

- **PDF** (PAdES)
- **CMS** (CAdES)
- **XML** (XAdES)
- **Sets of documents** (ASiC)

## Signature type:

- **Level B-B**
  - Signature with certificate
- **Level B-T**
  - Same + timestamp)
- **Level B-LT**
  - Same + CA certificates, CRL

# Remote signing (integration) - modular solution by Monet+



# Advanced or Qualified signature?

## Advanced el. signature

- Closed ecosystem (signing within organization)
- No implementation standards??
- SCAL1 nebo SCAL2
- Key protection – HSM recommended
- On-premise possible
- No audit required
- Non-qualified CA & certificates
- Choice of tool and identification mechanism
- Contract-based trust

## Qualified el. signature

- Signing beyond organization ecosystem, Public Administration
- Mandatory standards compliance
- SCAL2 only
- Key protection – in certified QSCD HSM
- Operated by a qualified TSP
- Audit according to eIDAS
- Qualified CA & certificates
- Specification of tool and identification mechanism
- Legislation-based trust

# Monet+ Remote Signing Ecosystem

## Remote Signing

ProID  
Orchestrator

SAM Module

Server Signing  
Application

## Authorization Service

Mobile  
method

Smart  
card

Authorization  
Service

## Time Stamping Authority (TSA)

Time Stamping  
Authority (TSA)

Time Stamping  
Unit (TSU)

## Public Key Infrastructure

HSM

# Monet+ Remote Sign

The logo for ASIT, featuring the letters 'A-SIT' in a bold, blue, sans-serif font. The letter 'S' is stylized with a red keyhole icon inside its center.

[Certified by ASIT](#)



[Trusted List](#)



[Entrust N-Shield XC HSM](#)



[ETSI Plugtests](#)

# Jiri Zmelik

Sales Manager

[jzmelik@proid.tech](mailto:jzmelik@proid.tech)

+420 777 213 990

[proid.tech](https://proid.tech) | [monetplus.com](https://monetplus.com)

**Thank you!**



# Thank you!

[monetplus.com](https://monetplus.com)

[proid.tech](https://proid.tech)

# Main changes in remote signature (eIDAS1 vs eIDAS2)

- **Identifikace / autentizace prostřednictvím peněženky digit. identity**
- **Čl.3 bod 16: Správa prostředků pro vytváření el.podpisů na dálku, nově jako služba vytvářející důvěru**
- **Nový čl. 23a) s def. prostředku pro vytváření kval.podpisů na dálku**
- **Čl. 24 – změna požadavků na ověření identity žadatele o kval.certifikát**
  - Zpřísnění oznámených prostředků a změna pořadí způsobu ověření
- **Čl. 29, 1a) Klíče pro vytváření kval.podpisů může spravovat pouze kvalifikovaný poskytovatel (poskytující příslušnou službu – viz výše)**
- **Čl. 29a) Požadavky na kval. službu správy prostředků pro vytváření el.podpisů na dálku**
  - Do 12 měsíců budou stanoveny normy pro hodnocení shody
- **Certifikace QSCD platná 5 let (každé 2 roky hodnocení zranitelnosti)**

# Formáty podepsaných dat (Advanced Electronic Signatures)

## **PAdES**

(PDF Advanced Electronic Signature)

## **CAdES**

(CMS Advanced Electronic Signature)

## **XAdES**

(XML Advanced Electronic Signatures)

## **ASiC**

(Associated Signature Container)

**Level B-B**  
podpis s certifikátem

**Level B-T**  
+ časové razítko

**Level B-LT**  
+ CA certifikáty, CRL

Ověření v [ETSI Plugtests](#)