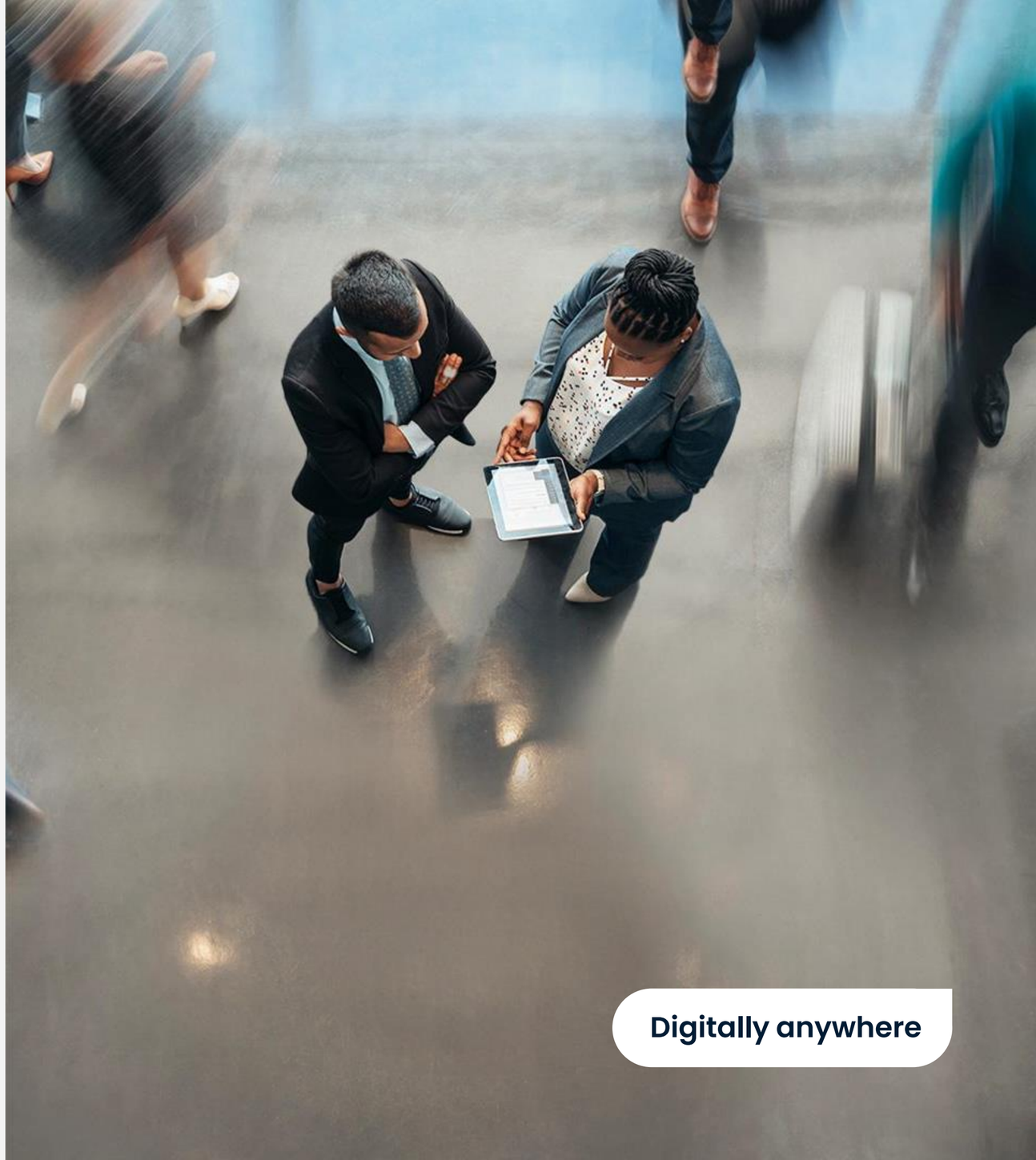
MONET +

Vzdálený elektronický podpis



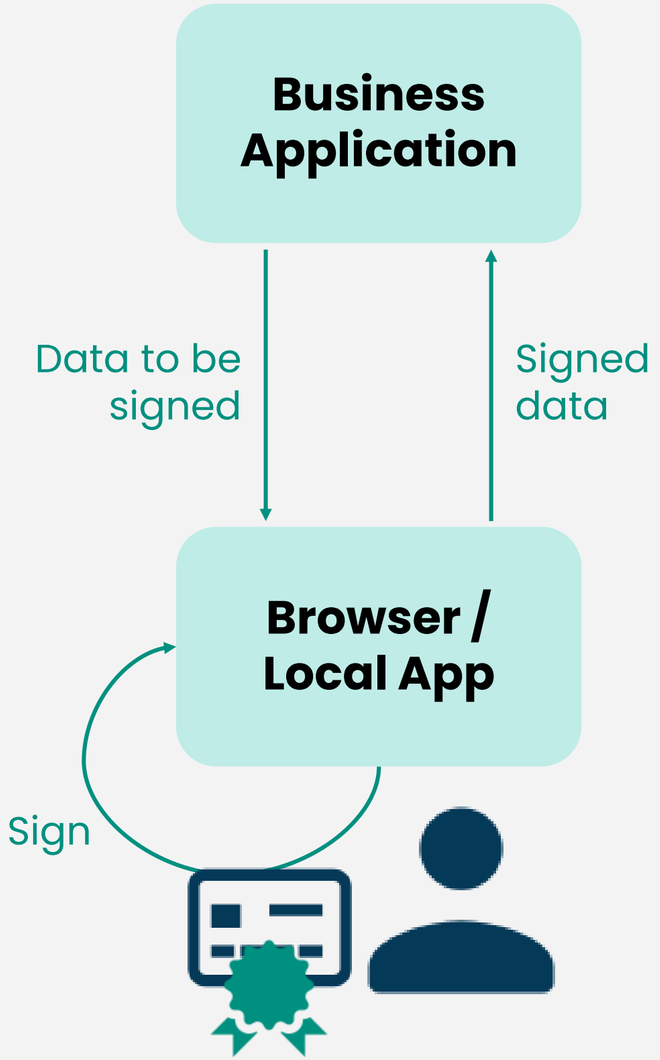
Jiří Kutálek
Solution Architect

Proč elektronicky podepisovat?

- Eliminace papírů (digitalizace)
- Optimalizace nákladů
- Snadný přenos elektronických dat
- Elektronická archivace
- Automatizace procesů

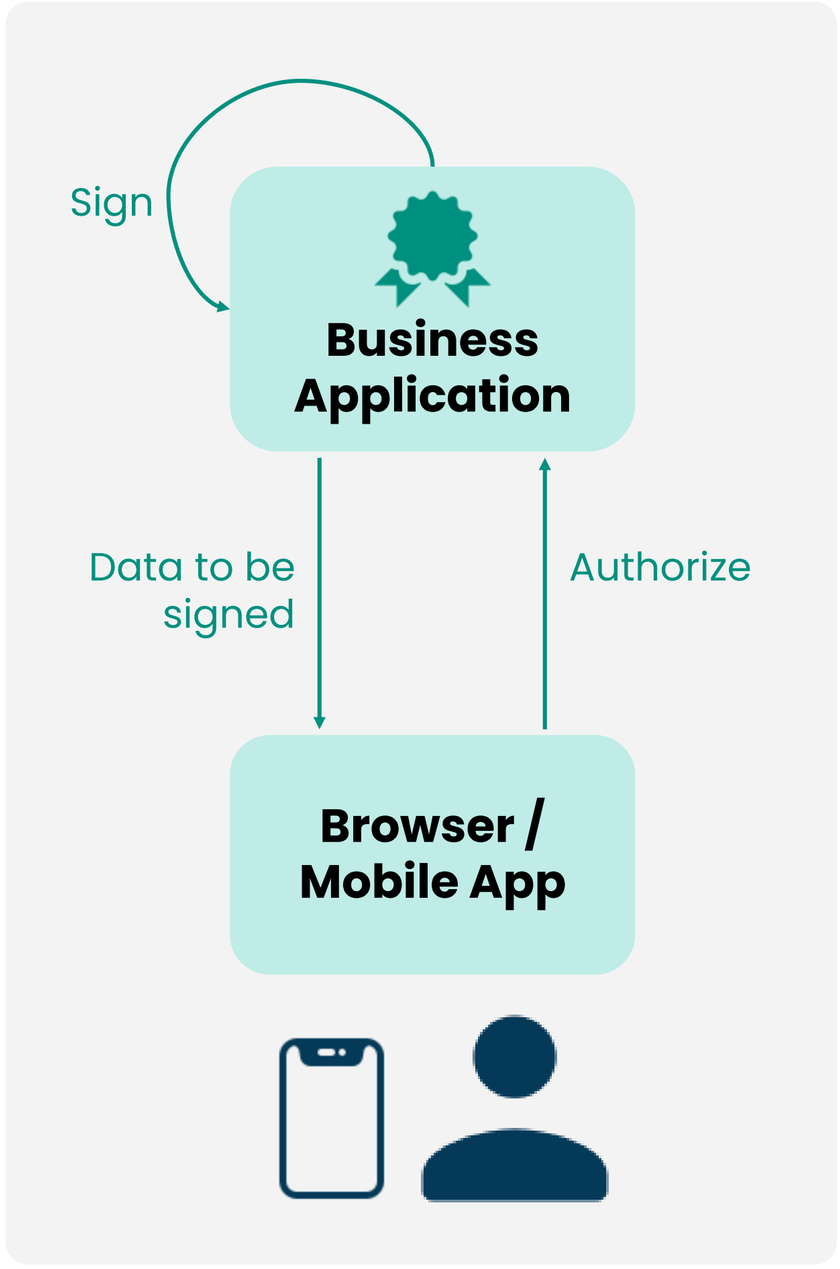
- Záznam souhlasu / neodmítnutelnost zodpovědnosti
- Projev vůle
- Integrita dat
- Odhalení falsa / detekce fraudů
- (Časové razítko)

Lokální elektronický podpis



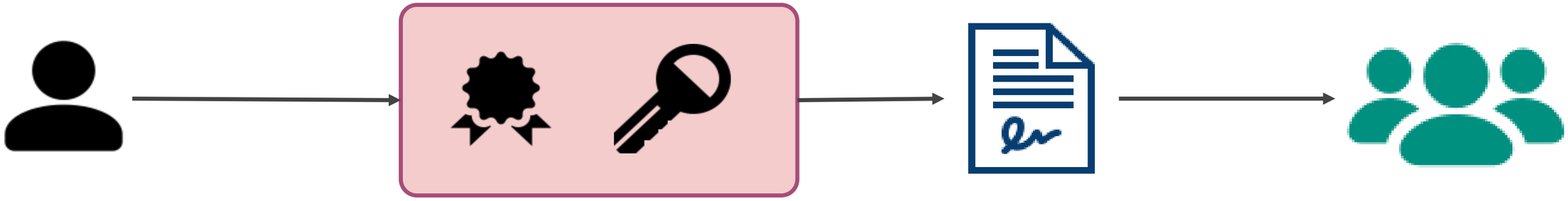
- **Klíč + certifikát lokálně u uživatele**
- **Distribuce tokenu a obslužné aplikace**
- **Vydání / obnova certifikátu**
- **Komplikované na mobilním telefonu**
- **Držitel má klíč pod kontrolou**
- **Přirozený 2-faktor**
- **Průkaz (vizuální / elektronický / bezkontaktní)**

Vzdálený elektronický podpis



- **Klíč + certifikát lokálně na serveru**
- **Distribuce autorizačního předmětu**
- **Automatické vydávání certifikátu**
- **Důvěra v poskytovatele**
- **Vhodné i pro mobily / biometrie**

Důvěryhodnost vzdáleného podpisu



- **Proč věřit, že el.podpis je projevem vůle uživatele?**
- **Proč věřit, že klíč uživatele nezneužije provozovatel?**

Technické řešení systému

- Normy, regulace, legislativa
- Ochrana klíčů vč. přístupu
- Napojení na CA

Kontrola klíče držitelem

- Onboarding, ověření totožnosti
- Aktivace prostředku identifikace
- Autentizace / autorizace

Úroveň kontroly držitele nad podpis.klíčem

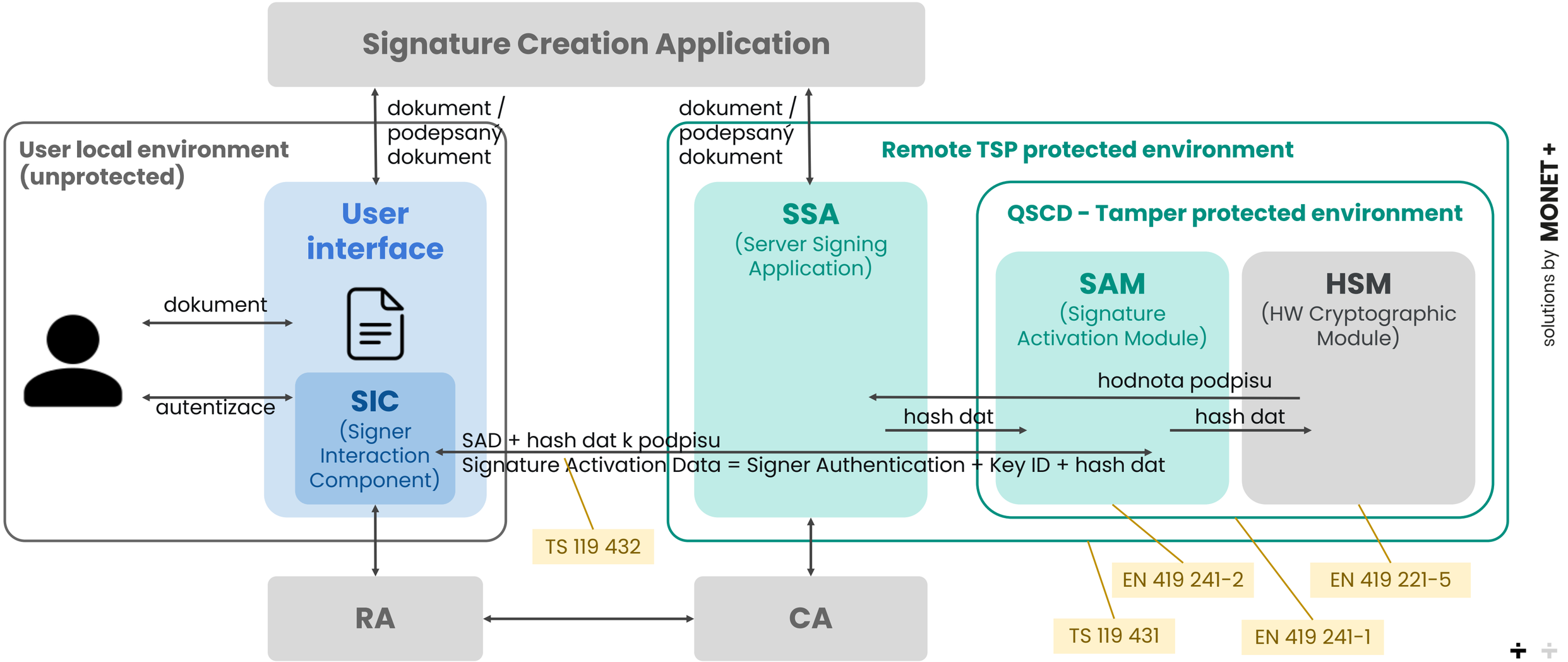
SCAL1 – Sole control assurance level 1

- Nízká úroveň důvěry kontroly podepisujícího nad podpisovým klíčem
- Použití klíče na základě autentizace uživatele
- Prostředek pro elektronickou identifikaci s úrovní záruky nízká
- Lze 1-faktorová autentizace

SCAL2 – Sole control assurance level 2

- Vysoká úroveň důvěry kontroly podepisujícího nad podpis. klíčem
- Použití klíče na základě kryptograficky zabezpečených dat, autorizovaných podepisujícím, na základě hashe dat
- Hardwarová ochrana podpisových klíčů (HSM)
- Prostředek pro elektronickou identifikaci s úrovní záruky značná
- Alespoň 2-faktorová autentizace + dynamická autentizace

Architektura systému vzdáleného podpisu (SCAL2)



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

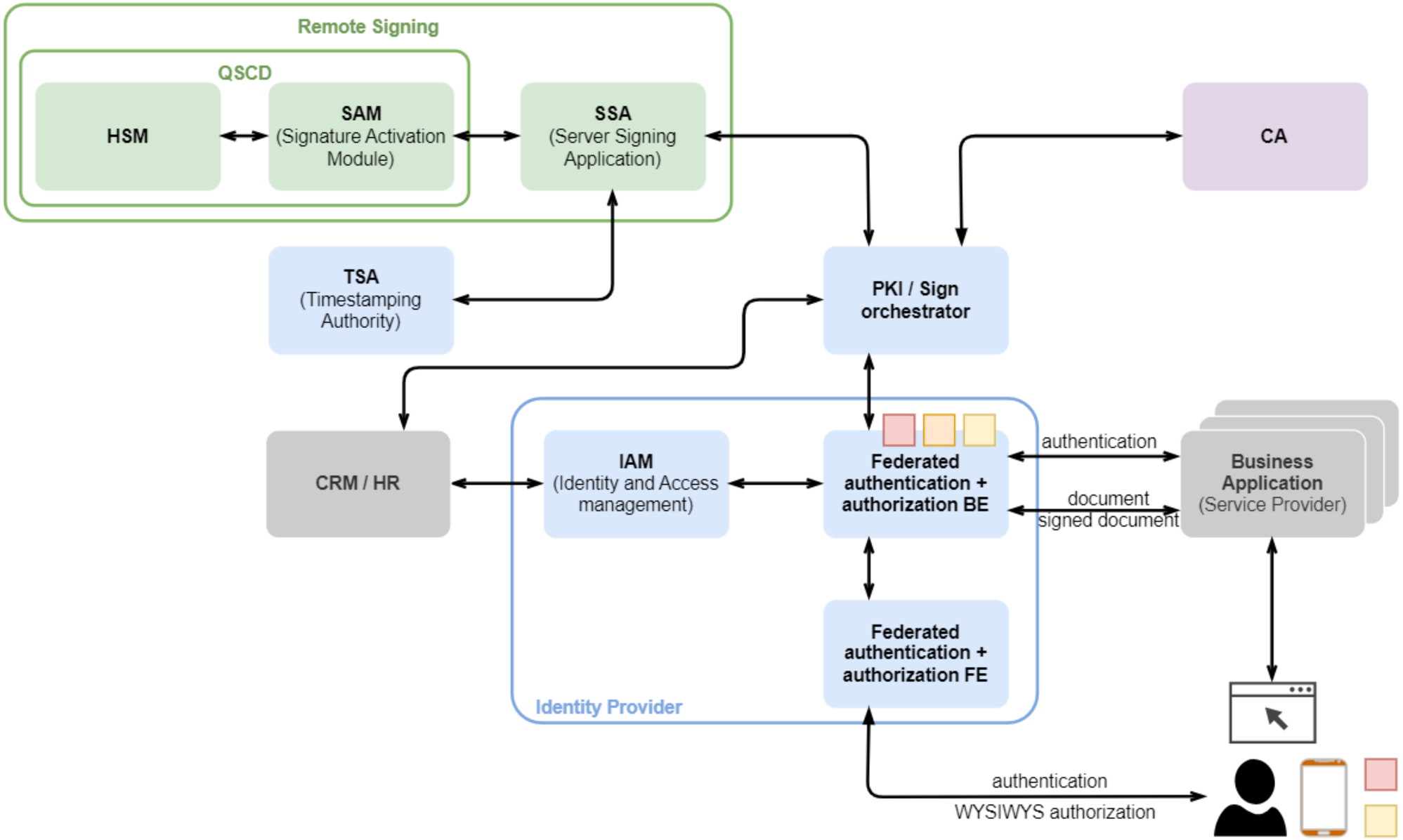
Level B-T
+ časové razítko

Level B-LT
+ CA certifikáty, CRL

Ověření v [ETSI Plugtests]

solutions by **MONET +**

Integrace vzdáleného podpisu - řešení Monet+



Zaručený nebo kvalifikovaný podpis?

Zaručený el. podpis

- Uzavřený systém (např. v rámci organizace)
- Volnost v implementaci norem
- SCAL1 nebo SCAL2
- Ochrana klíčů - doporučeno HSM
- Lze on-premise
- Nevyžaduje hodnocení shody (audit)
- Ne-kvalifikovaná CA a certifikáty
- Volba prostředku a mechanismu identifikace
- Důvěra zakotvena smluvně

Kvalifikovaný el. podpis

- Podepsané dokumenty za hranice organizace, i pro státní správu
- Striktní dodržení norem
- Nutná SCAL2
- QSCD HSM
- Provozuje kvalifikovaný poskytovatel služeb vytvářejících důvěru
- Audit podle eIDAS
- Kvalifikovaná CA a certifikáty
- Nároky na prostředek identifikace a mechanismy autentizace
- Důvěra daná legislativou

Varianty implementace vzdáleného podepisování

	Zaručený podpis	Kvalifikovaný podpis
In-house / on-premise	Doplnění systémů o vzdálený podpis Vlastní CA nebo CA jako služba, Prostředky pro identifikaci / autentizaci	Nutno stát se kvalifikovaným poskytovatelem služeb vytvářejících důvěru, Prostředky pro identifikaci / autentizaci Projít hodnocením shody
Jako služba	Smlouva s poskytovatelem, Nutno předávat identity, Prostředky pro identifikaci / autentizaci	Smlouva s kvalifikovaným poskytovatelem, Nutno řešit identifikaci, autentizaci a autorizaci. Hodnocení shody zajistí poskytovatel.

Rozdíl mezi eIDAS1 a eIDAS2, pro vzdálený podpis

- **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)**

Děkuji!

monetplus.com

proid.tech