

EIDAS A VZDÁLENÝ KVALIFIKOVANÝ ELEKTRONICKÝ PODPIS

| Michal Hanzal | Solution Consultant |



VZDÁLENÝ ELEKTRONICKÝ PODPIS JE TREND

Gartner Identity & Access Management Summit 2019 | 7. – 8. 3. 2019 | London



ELEKTRONICKÝ PODPIS

Způsoby elektronického podepisování



Podpis pomocí
čipové karty /
tokenu



Podpis
jako
služba

ELEKTRONICKÝ PODPIS POMOCÍ ČIPOVÉ KARTY / TOKENU

Problémy s využitím

Security Warning

Do you want to run this application?



Your version of Java is out of date and the location below is requesting permission to run on your computer.

Locations: https://[redacted].cvut.cz:443

https://[redacted].cvut.cz:4443

Running unsigned applications like this will be blocked in the future. This is a potentially unsafe and a security risk.

[More Information](#)

Select the box below, then click run to start the application.

1. I accept the risk and want to run this app.

Podepsat dokument

Podepsat jako: Michal Hanzal (PostSignum Qualified CA 2) [v]

Vydal: PostSignum Michal Hanzal (PostSignum Public CA 2) 2019.09.03

Vydal: PostSignum Michal Hanzal (PostSignum Qualified CA 2) 2019.04.25

Michal Hanzal (PostSignum Qualified CA 2) 2019.04.25

Obnovit seznam identifikátorů

Nový identifikátor ...

Vzhled: Standardní

Michal Hanzal Digitálně podepsal Michal Hanzal
Datum: 2019.03.26 08:41:39 +01'00'

Zamknout dokument po podepsání

Nápověda Podepsat Zrušit

Do you want to allow the following application from this web site?

https://[redacted].cvut.cz:4443

DOMApplet

This web site is requesting access and control of the Java application shown above. Allow access only if you trust the web site and know that the application is intended to run on this site.

Do not show this again for this app and web site.

Allow

Do Not Allow



[More information](#)

ELEKTRONICKÝ PODPIS POMOCÍ ČIPOVÉ KARTY / TOKENU

Problémy s využitím podpisu na koncovém zařízení uživatele



vyžaduje čtečku karet
USB pro token



vyžaduje SW
a příslušné ovladače



kompatibilita
prohlížečů



podpis na mobilních
zařízeních



ztráta čipové
karty



možnost jednoduchého
„zapůjčení“

ELEKTRONICKÝ PODPIS

Způsoby elektronického podepisování



Podpis pomocí
čipové karty /
tokenu



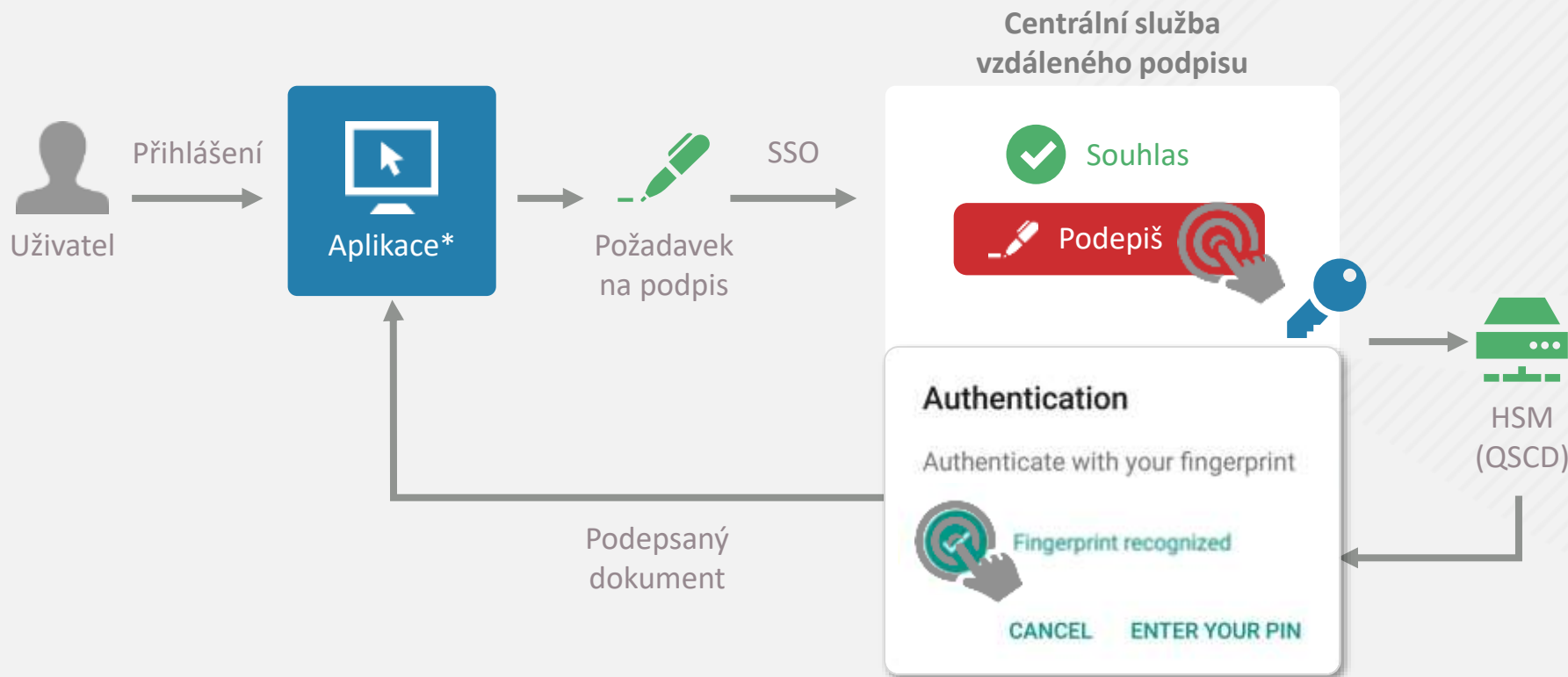
Podpis
jako
služba

ELEKTRONICKÝ PODPIS JAKO SLUŽBA

Až takto jednoduché to může být

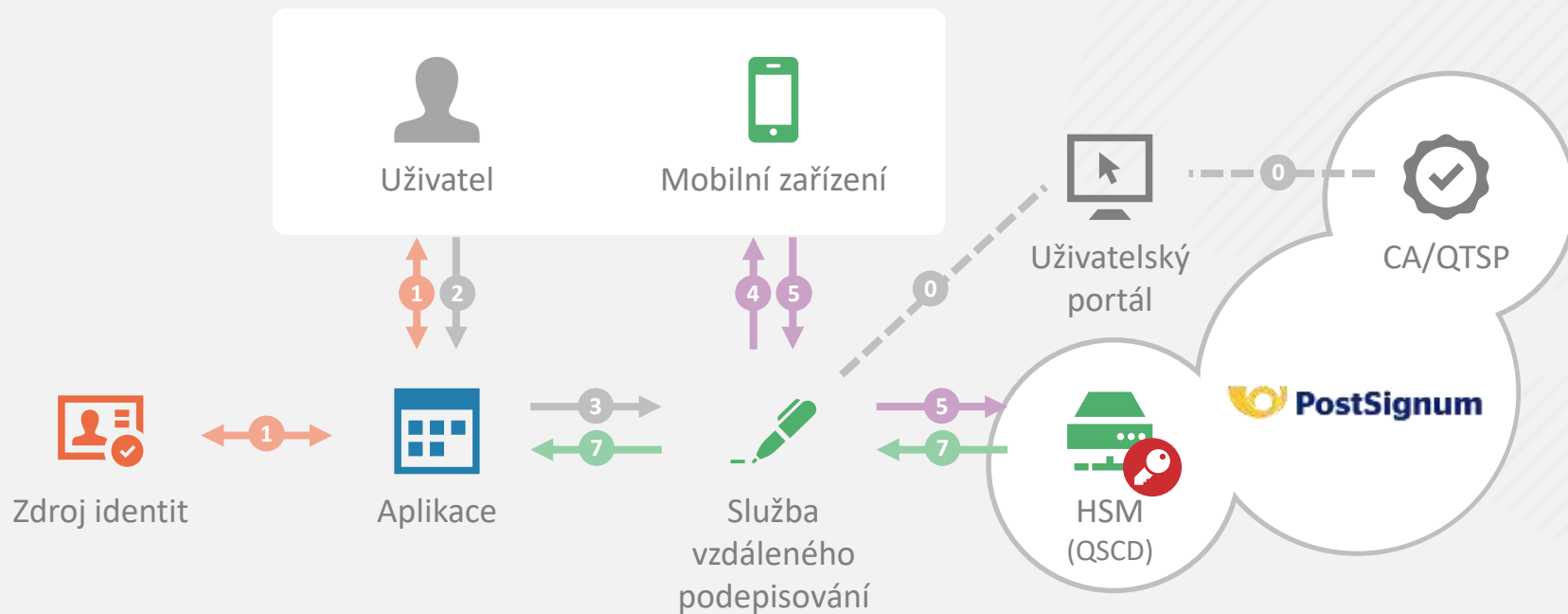


ELEKTRONICKÝ PODPIS JAKO SLUŽBA



* Univerzální aplikace pro všechny PC/mobilní platformy
nezávislá na OS, web prohlížeči či aplikačním toolkitu

ELEKTRONICKÝ PODPIS JAKO SLUŽBA



- 0 Zajištění certifikátu
- 1 Přihlášení do aplikace
- 2 Vyžádání podepsání
- 3 Zahájení procesu podepisování
- 4 Požadavek na autorizaci podepsání
- 5 Aktivace a použití soukromého klíče v HSM
- 6 Vygenerování el. podpisu v HSM
- 7 Vytvoření el. podepsaného dokumentu a jeho předání aplikaci

ELEKTRONICKÝ PODPIS

Srovnání

Podpis pomocí čipové karty/tokenu

Podpis na koncovém zařízení uživatele

- vyžaduje čtečku karet, USB pro token, ...
- vyžaduje příslušné ovladače a SW
- problém s kompatibilitou prohlížečů
- problém s podpisem na mobilních zařízeních
- problém s životností karet a jejich ztrátou
- možnost jednoduchého „zapůjčení“

Podpis jako služba pomocí HSM modulu

Podpis v rámci bezpečné infrastruktury

- podpis vytvořen v HSM modulu (*QSCD*)
- pro libovolné koncové zařízení (*PC, mobil, tablet*)
- uživatelská přívětivost jako internet banking
- využití moderních funkcí smartphonu
- integrace se správou identit (IAM)
- podpora silné autentizace
- až do úrovně kvalifikovaného el. podpisu

PROJEKTY VZDÁLENÉHO PODPISU V ČR



czechtoll



+



ELEKTRONICKÝ PODPIS JAKO SLUŽBA

Hlavní přínosy



User
experience



Kdekoli, kdykoli,
na čemkoli



Kvalifikovaný
podpis



Nasazení
On Premise



Další
využití HSM



Vyšší
bezpečnost

7. ročník konference

DIGITAL TRUST & PAPERLESS

VZDÁLENÝ ELEKTRONICKÝ PODPIS

KVALIFIKOVANÁ PEČEŤ

22. května 2019 | Villa Pellé | Praha

www.sefira.cz

