

ELEKTRONICKÝ PODPIS V PRAXI

Petr Chlumský



DIGITÁLNÍ DŮVĚRA



DŮVĚRA VE FYZICKÉM SVĚTĚ



DŮVĚRA A JEJÍ NÁSTROJE VE FYZICKÉM SVĚTĚ



DIGITÁLNÍ DŮVĚRA



[illegible]

ZROVNOPRÁVNĚNÍ DŮVĚRY V DOKUMENTY



Papírový
dokument



Elektronický
dokument



El. podpis



El. pečeť



Čas. razítko

PROSTŘEDKY PRO VYTVÁŘENÍ DIGITÁLNÍ DŮVĚRY

dle nařízení eIDAS



Elektronický
podpis



Elektronická
pečeť



Elektronické
časové razítko

ELEKTRONICKÝ PODPIS



TYPY ELEKTRONICKÝCH PODPISŮ



Prostý
elektronický podpis



Biometrický
podpis



Podpis
založený na certifikátu

ÚČEL ELEKTRONICKÉHO PODPISU



Projev vůle

Vnáší do dokumentu nezměnitelné informace o projevu vůle podepisující osoby



Zajištění integrity

Umožňuje detekci neautorizovaných změn v dokumentu opatřeného elektronickým podpisem

TYPY ELEKTRONICKÝCH PODPISŮ

založených na certifikátu



Zaručený podpis

je založen na interním nebo
komerčním certifikátu



Uznávaný podpis

je založen na kvalifikovaném
certifikátu pro elektronický podpis



Kvalifikovaný podpis

je založen na kvalifikovaném
certifikátu pro elektronický podpis

a

vytvořen pomocí kvalifikovaného
prostředku pro vytváření podpisů

POVINNOSTI POUŽITÍ EL. PODPISU

dle zákona 297/2016 Sb. o službách vytvářejících důvěru

✓ §5

K podepisování elektronickým podpisem lze použít pouze kvalifikovaný elektronický podpis, podepisuje-li elektronický dokument, kterým právně jedná, veřejnoprávní podepisující.

✓ §6

(1) K podepisování elektronickým podpisem lze použít pouze uznávaný elektronický podpis, podepisuje-li se elektronický dokument, kterým se právně jedná vůči veřejnoprávnímu podepisujícímu nebo jiné osobě v souvislosti s výkonem jejich působnosti.

(2) Uznávaným elektronickým podpisem se rozumí zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis nebo kvalifikovaný elektronický podpis.

✓ §7

K podepisování elektronickým podpisem lze použít zaručený elektronický podpis, uznávaný elektronický podpis, případně jiný typ elektronického podpisu, podepisuje-li se elektronický dokument, kterým se právně jedná jiným způsobem

TYPY ELEKTRONICKÝCH PODPISŮ

a povinnost jejich použití v praxi dle zákona 297/2016 Sb.

Původce \ Příjemce	Veřejná správa	Ostatní původci
	Veřejná správa	Ostatní původci
Veřejná správa	Kvalifikovaný	Kvalifikovaný
Ostatní původci	Uznávaný	Libovolný typ

ELEKTRONICKÁ PEČEŤ



ÚČEL ELEKTRONICKÉ PEČETI



Prokázání původu

Vnáší do dokumentu nezměnitelné informace o původci dokumentu opatřeného elektronickou pečeti



Zajištění integrity

Umožňuje detekci neautorizovaných změn v dokumentu opatřeného elektronickou pečeti

ČASOVÉ RAZÍTKO



ČASOVÉ RAZÍTKO



Existence v čase

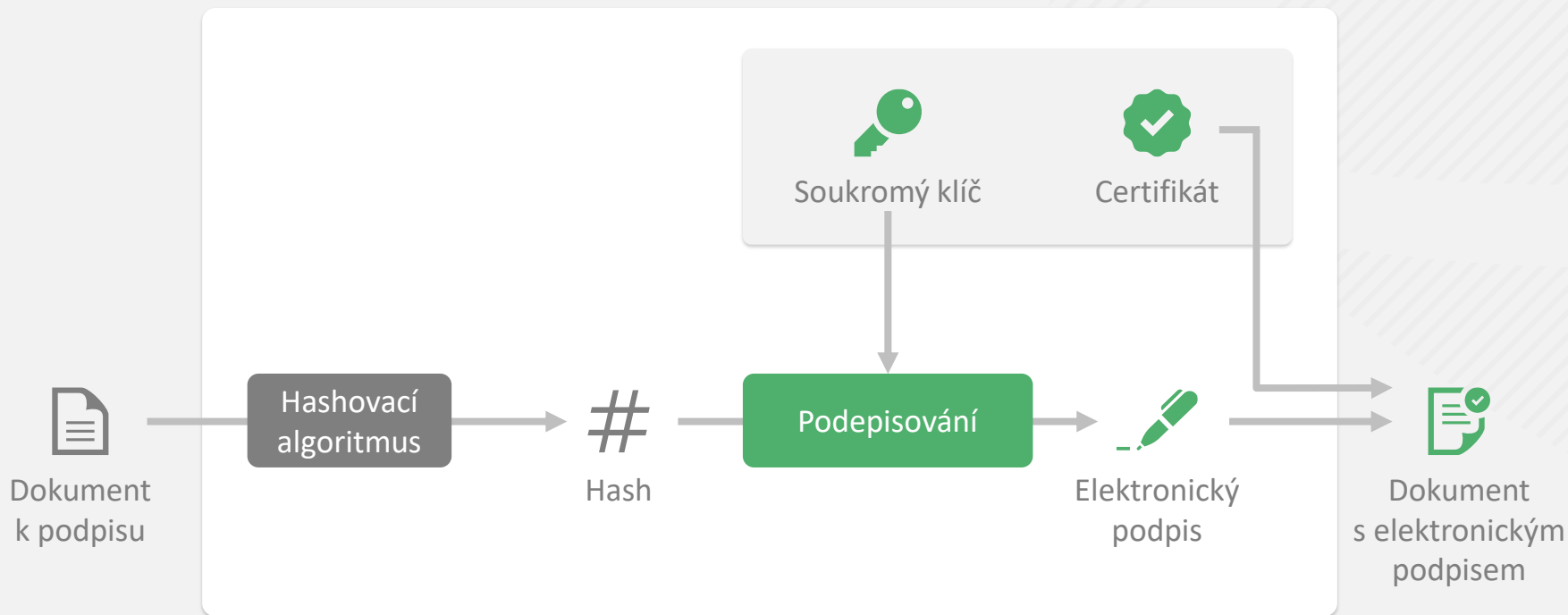
Prokazuje existenci dokumentu
v dané podobě a v daném čase

ELEKTRONICKÝ PODPIS V PRAXI



ELEKTRONICKÝ PODPIS

založený na certifikátu



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.

Locations: <https://...cvut.cz:443>

<https://...cvut.cz:4443>

Running unsigned applications like this will be blocked by Java security. This is 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.

Podpsat dokument

Podpsat jako: Michal Hanzal (PostSignum Qualified CA 2) 2019.09.03
Michal Hanzal (PostSignum Public CA 2) 2019.09.03
Michal Hanzal (PostSignum Qualified CA 2) 2019.04.25
Michal Hanzal (PostSignum Qualified CA 2) 2019.04.25
Obnovit seznam identifikátorů
Nový identifikátor ...

Vydal: PostSignum

Vzhled: Standard

Michal Hanzal

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

☐ Zamknout dokument po podepsání

Nápověda Podpsat Zrušit

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

<https://...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



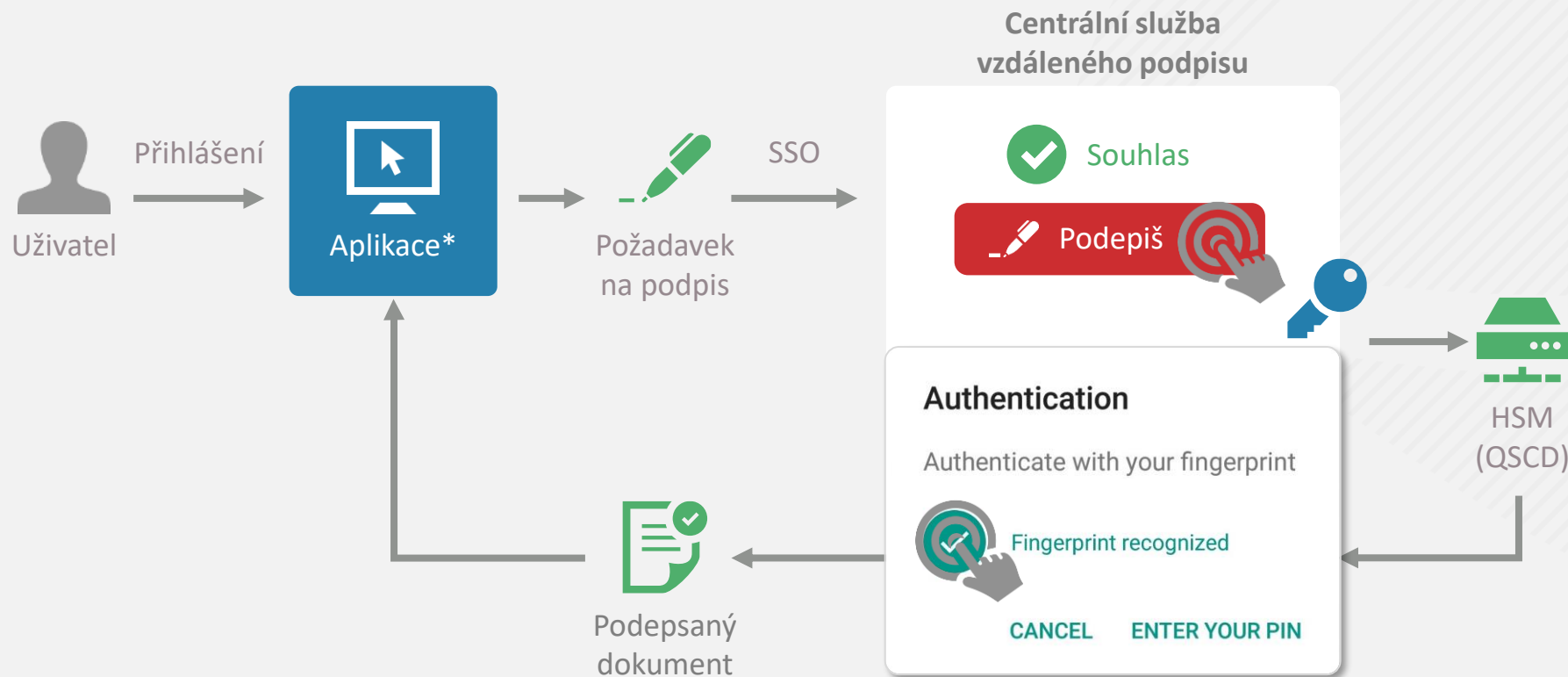
Podpis
jako
služba

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

Hlavní přínosy



Intuitivní a snadné
ovládání



Elektronický podpis
kdykoli a odkudkoli



Nezávislost na typu
zařízení

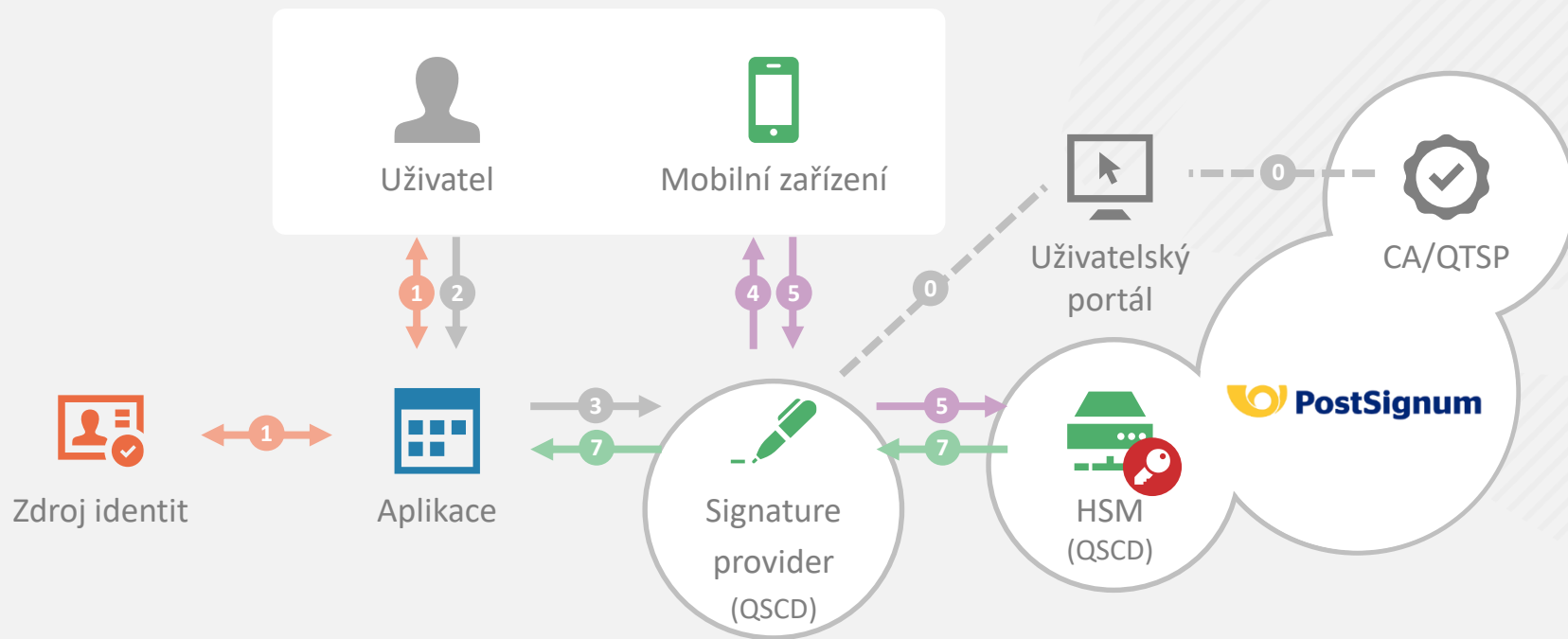


Vyšší bezpečnost



Audit a monitoring

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

VÍCEFAKTOROVÁ AUTENTIZACE / AUTORIZACE

Bezpečné ověření identity uživatele a autorizace podpisu



PIN



Heslo

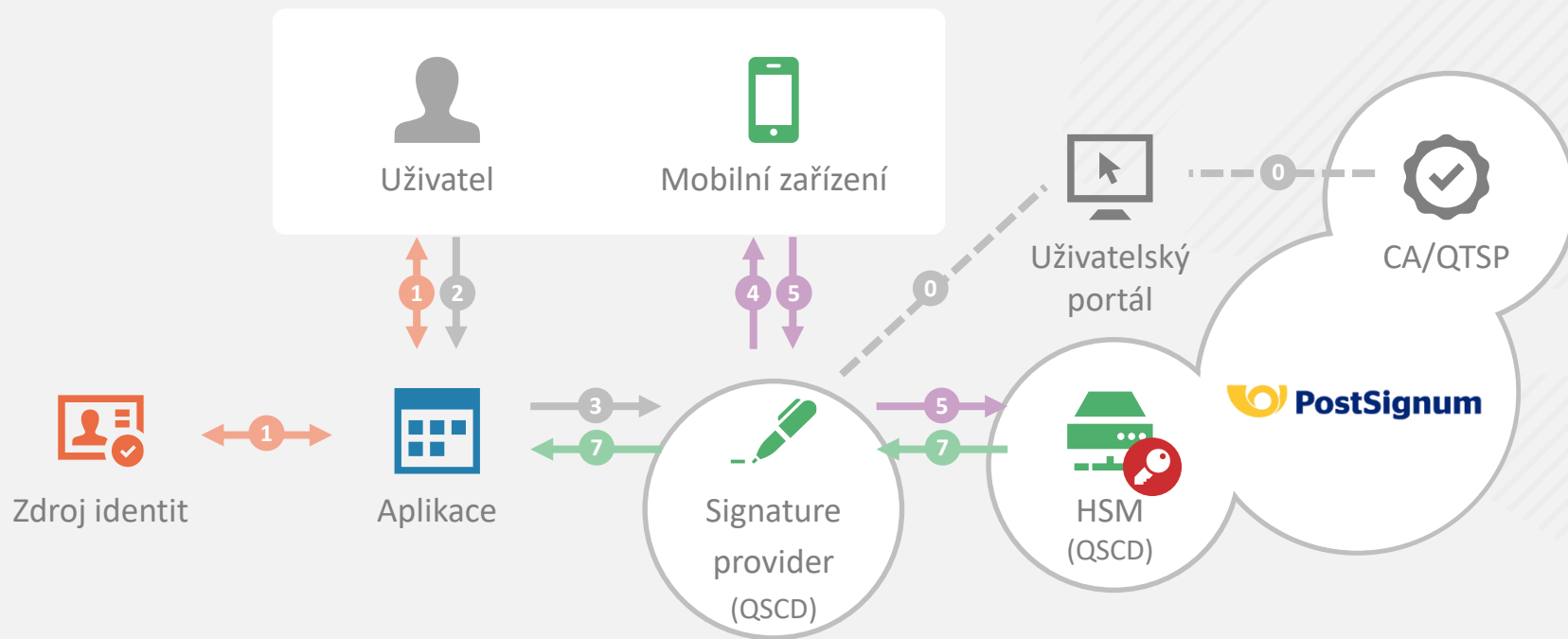


One-Time Password
emailem nebo SMS



Autentizace
mobilním telefonem

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

BEZPEČNÉ ULOŽENÍ KLÍČŮ

HSM jako kvalifikovaný prostředek (QSCD)

- ✓ Certifikace jako QSignCD
- ✓ Certifikace FIPS 140-2 Level-3, Common Criteria EAL4+

- ✓ Co to vlastně je Hardware Security Module?
 - specializované vysoce bezpečné zařízení pro:
 - generování silných kryptografických klíčů
 - ochranu privátních klíčů
 - poskytování šifrovacích služeb
 - správu a archivaci kryptografických klíčů



VIRTUÁLNÍ ČIPOVÁ KARTA

Užitečná aplikace služby pro vzdálený elektronický podpis

- ✓ Náhrada fyzické karty pro lokální aplikace
 - chování obdobné jako při vložení fyzické čipové karty do čtečky
- ✓ Aplikace není nutné jakkoliv upravovat
 - pokud již dnes podporují podepisování pomocí standardních rozhraní OS
- ✓ Vzdálený podpis jako přímá náhrada fyzické karty
 - vhodné například i do prostředí s virtualizovanými desktope
- ✓ Překlenovací řešení do přechodu na aplikace s podporou mobilních platforem
 - s klasickou službou vzdáleného podpisu



OBELISK SIGNING PORTAL

OBELISK Signing Portal – systém pro centrální zpřístupnění elektronického podepisování informačním systémům a koncovým uživatelům.

PODPISOVÁ FLOW



Online podpis

- ✓ Uživatelské podepsání bez čekání v rámci jednoho volání webové služby



Odložený podpis

- ✓ Shromáždění požadavků na podpis v podpisovém portálu
- ✓ Uživatelé jsou dokumenty k podepsání dostupné po přihlášení

UŽIVATELSKÉ GUI

Dokumenty k podpisu

Signing Portal

Řešitel

Přijaté

6

Zpracovává se

Historie přijatých

Úlohy

2

Přijaté požadavky

Signing Portal > Přijaté

← Zpět

Otevřít v náhleduPodepsatX Odmítnout

Výsledková sada záznamů (6)

První

Předchozí

1

Následující

Poslední

		Název dokumentu	Typ dokumentu	Datum zadání		Termín pro splnění		Žadatel	
		83552561 Pracovní smlouva zam. 45684	Testovací požadavek	09.04.2020		10.04.2020		Michal Hanzal	
		83552550 Smlouva k podpisu	Testovací požadavek	09.04.2020		16.04.2020		Michal Hanzal	
		83552551 Směrnice ke schválení	Testovací požadavek	09.04.2020		16.04.2020		Michal Hanzal	
		83552552 Platový výměr zaměstnance 58213	Testovací požadavek	09.04.2020		16.04.2020		Michal Hanzal	
		83552553 Nákup kancelářských potřeb 04/2020	Testovací požadavek	09.04.2020		16.04.2020		Michal Hanzal	
		83552555 Pracovní smlouva zam. 45678	Testovací požadavek	09.04.2020		16.04.2020		Michal Hanzal	

První

Předchozí

1

Následující

Poslední

Zobrazeny záznamy 1 až 6 z 6 nalezených.

UŽIVATELSKÉ GUI

Obrazovky dle rolí uživatelů

Signing Portal

+ Vytvořit požadavek

Resitel

Přijaté2

Zpracovává se

Historie přijatých

Úlohy

Zadatel

Vytvořené3

Nesplněné2

Historie vytvořených

Přijaté požadavky

Signing Portal > Přijaté

← Zpět

Otevřít v náhleduPodepsatX Odmítnout

Výsledková sada záznamů (2)

PrvníPředchozí1NásledujícíPoslední

☐	Název dokumentu	Typ dokumentu	Datum zadání	Termin pro splnění	Žadatel
☐	Testovací požadavek 088_2581835	Testovací požadavek	12.05.2020	19.05.2020	Michal Hanzal
☐	Testovací požadavek 088_2581875	Testovací požadavek	12.05.2020	19.05.2020	Michal Hanzal

PrvníPředchozí1NásledujícíPoslední

Zobrazeny záznamy 1 až 2 z 2 nalezených.

HROMADNÉ ZPRACOVÁNÍ

Podpis / schválení / odmítnutí více dokumentů najednou

Signing Portal

Řešitel

Přijaté 6

Zpracováva se

Historie přijatých

Úlohy 2

Přijaté požadavky

← Zpět

Otevřít v náhledu

Podepsat

✕ Odmítnout

Výsledková sada záznamů (6)

3

První

Předchozí

1

Následující

Poslední

	Název dokumentu	Typ dokumentu	Datum zadání	Termín pro splnění	Žadatel
	83552561 Pracovní smlouva zam. 45684	Testovací požadavek	09.04.2020	10.04.2020	Michal Hanzal
	83552550 Smlouva k podpisu	Testovací požadavek	09.04.2020	16.04.2020	Michal Hanzal
	83552551 Směrnice ke schválení	Testovací požadavek	09.04.2020	16.04.2020	Michal Hanzal
	83552552 Platový výměr zaměstnance 58213	Testovací požadavek	09.04.2020	16.04.2020	Michal Hanzal
	83552553 Nákup kancelářských potřeb 04/2020	Testovací požadavek	09.04.2020	16.04.2020	Michal Hanzal
	83552555 Pracovní smlouva zam. 45678	Testovací požadavek	09.04.2020	16.04.2020	Michal Hanzal

První

Předchozí

1

Následující

Poslední

Zobrazeny záznamy 1 až 6 z 6 nalezených.

PROHLÍŽEČ DOKUMENTŮ

 OBELISK

 < 1 / 1 >

sealed.pdf

  1 / 1  Pracovní smlouva zam...

 Zpět

DOKUMENT

 Podepsat

 Odmítnout

SOUBOR

 Otočit doprava

 Otočit doleva

 Zmenšit velikost

 Zvětšit velikost

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Curabitur a dui mattis, pellentesque ante id, porttitor metus. Integer ut tortor sed massa semper condimentum. Donec sed urna at tellus laoreet viverra ac eu dui. Donec leo sem, dictum in velit nec, aliquet interdum lacus. Quisque massa nisl, sagittis quis ornare pharetra, ultrices porttitor ligula. Vestibulum orci massa, fermentum id tincidunt non, molestie sit amet dolor. Sed consectetur vestibulum pellentesque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Donec tincidunt dolor augue, in bibendum dolor mattis sit amet. Vestibulum scelerisque ipsum non risus eleifend porta. Sed a placerat nisl. Proin at volutpat nulla. Quisque congue quam non massa mollis, at tincidunt ante scelerisque. Curabitur porttitor facilisis pharetra. Sed gravida tortor in elit venenatis dignissim. Curabitur et nisi mauris.

Sed enim ipsum, efficitur quis convallis non, dictum vitae massa. Nam ex dui, luctus sit amet nibh nec, cursus interdum libero. Nunc semper tellus ac pretium blandit. Pellentesque libero diam, varius sit amet massa non, aliquam porta mi. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec non est a odio viverra sagittis. Nam aliquam placerat justo. Quisque tincidunt mauris leo, quis lobortis metus lobortis id. Etiam at tellus non est cursus luctus sit amet bibendum ante. Donec laoreet tortor a dolor dapibus, in viverra eros cursus. Ut sollicitudin sagittis velit vitae luctus. Vestibulum pellentesque volutpat turpis, finibus tristique nunc lobortis faucibus. In rhoncus mollis accumsan. Nam commodo consectetur finibus.

Elektronicky opečetěno,
SEFIRA spol. s r. o.

NOTIFIKACE & UPOMÍNKY



Notifikace

- ✓ Přizpůsobitelné notifikované události
- ✓ Přizpůsobitelní příjemci notifikací
- ✓ Přizpůsobitelný obsah sdělení



Upomínky

- ✓ Podpisový požadavek je opatřen očekávaným datumem splnění
- ✓ Při překročení termínu jsou řešiteli odesílány upomínky

AUDIT A MONITORING



Monitoring

- ✓ Sleduje se:
 - Celkový stav systému
 - Stav jednotlivých komponent
 - Průchod požadavků systémem
- ✓ Stav je dostupný přes webové GUI nebo přes SNMP
- ✓ Lze definovat vlastní semaforey



Audit

- ✓ Záznam celého procesu podepisování
- ✓ Dostupnost logů:
 - Ve webovém GUI
 - Přes dedikovaný databázový pohled

PŘÍNOSY



Podpora různých
způsobů podpisu



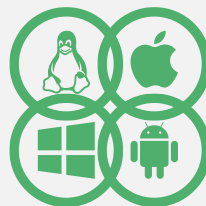
Hromadné
podepisování



Přidání pečeti
s časovým razítkem



Nezávislost na
business systémech



Nezávislost na
operačním systému



Přihlášení pomocí
Single Sign On

INTEGRACE S PRODUKTY DIGITÁLNÍ DŮVĚRY

Podpisem to teprve začíná



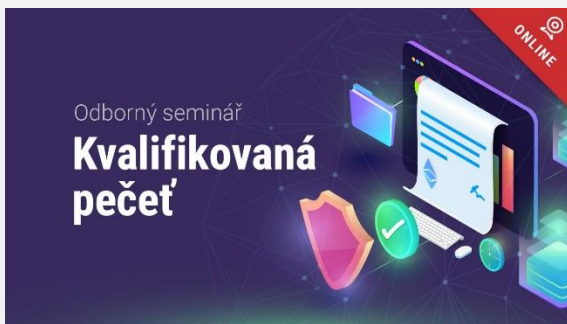
ONLINE SEMINÁŘE



28. 5. 2020



2. 6. 2020



9. 6. 2020



4. 6. 2020



| 25
LET |

www.sefira.cz