



REVOLUČNÍ ŘEŠENÍ NOVÝCH TRENDŮ KYBERNETICKÉ BEZPEČNOSTI

Moderní řešení problematiky autentizace uživatelů, správy životního cyklu digitálních certifikátů, autentizačních zařízení, uživatelů a jejich digitální identity.

Secure

Bold

Trustful

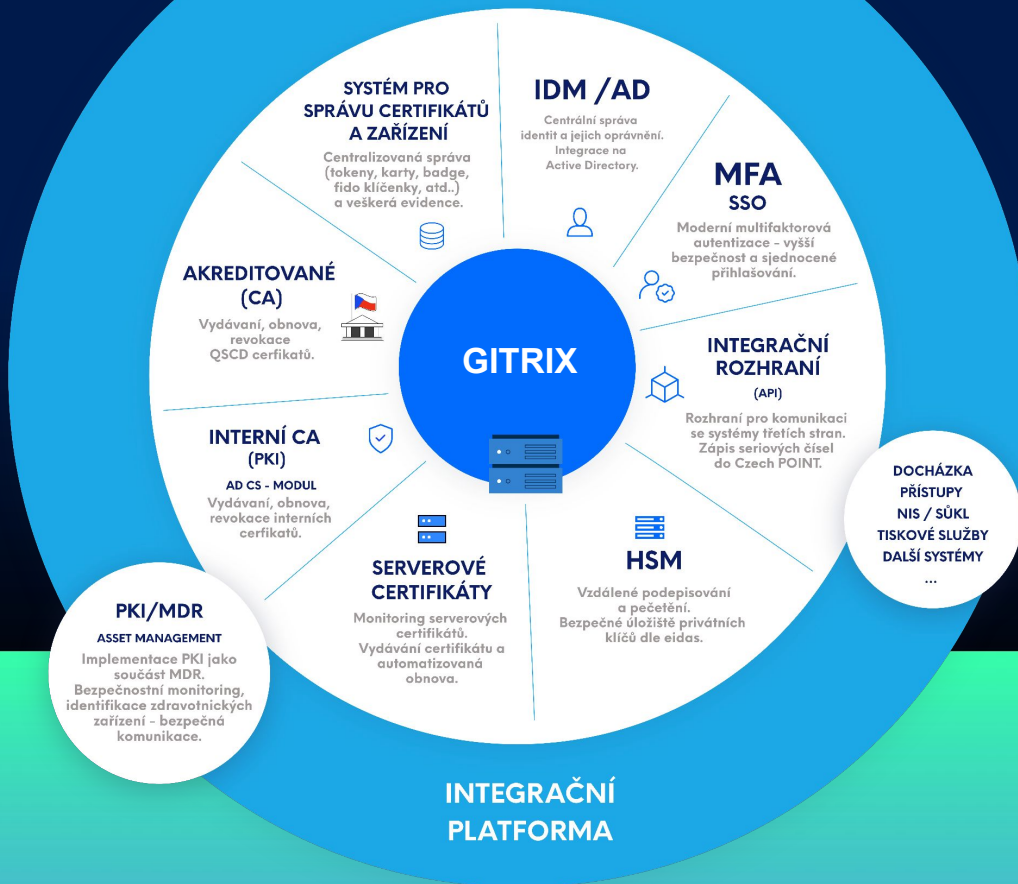
Tech

www.gitrix.cz





KYBERNETICKÁ BEZPEČNOST



MFA

MULTIFAKTOROVÁ AUTENTIZACE



MFA

DRŽITELSKÝ FAKTOR

Mobilní zařízení
Čipová karta
Tokeny a Badge
Certifikát X.509



ZNALOSTNÍ FAKTOR

Uživatelské jméno
+ Heslo
PIN
Hardwarový PIN



BIOMETRICKÝ FAKTOR

Otisk
Obličej
Hlas



MFA - Metody Autentizace GITRIX

Kombinace metod pro komfortní multifaktorovou autentizaci.

1. Mobilní aplikace

- Použití mobilní aplikace pro MFA s PUSH notifikacemi nebo QR kódem (TOTP časově omezený kód) a Face ID / Touch ID tvoří silnou autentizaci.

2. Čipová karta (PKI,QSCD,hybridní)

- Použití PIN a ČK s certifikátem pro MFA tvoří silnou bezheslovou autentizaci.
- Možnost využití bezkontaktní části pro docházku, dveřní vstupy, tisk, parking, atd.

3. Badge (video ukázka)

- Použití Badge s certifikátem a Touch ID nebo Voice ID, případně s HW PIN tvoří extrémně silnou bezheslovou autentizaci.
- **Badge + QSCD Čipová karta = 2+3 v jednom.**

4. FIDO2 - “plán release 2025”, a další...



MATRIX MFA do PC



Znalostní faktor



Držitelský faktor



Biometrický faktor

Windows Login
+ mobilní aplikace

Uživ. jméno
+ Heslo

Mobilní telefon
+ (PUSH notifikace / QR kód TOTP)

Obličej / Otisk

Smart Card logon

PIN

Čipová karta /
Certifikát X.509

-

BADGE

Hardwarový
PIN

Badge / Certifikát X.509

Otisk / Hlas

BADGE + Čipová
karta (QSCD)

PIN /
Hardwarový
PIN

Badge / Čipová karta /
Certifikát X.509

Otisk / Hlas

FIDO2

Plánovaný release 2025

Windows Login
+ mobilní aplikace

Uživ. jméno
+ Heslo

Mobilní telefon
+ (PUSH notifikace / QR kód TOTP)

Obličej / Otisk

GITRIX a jeho konkrétní možnosti jak kombinovat metody autentizace v praxi k využívání extrémně silné autentizace (MFA):

Mobilní aplikace:

- Použití Mobilního telefonu v kombinaci s biometrickými údaji (možnosti telefonu) a PUSH notifikací nebo časově omezeným OTP kódem.
- **Novinka GITRIX***: Použití Mobilního telefonu pro **bezheslové přihlášení (5,6) - iPhone ECC křivky**.
- Přenos dat mezi PC a Telefon pomocí **asymetrické kryptografie**.
- Kombinace znázorněny v tabulce:
- Ukázka prototyp: [Operator](#)

Benefity:

- Nabízí řešení pro multifaktorovou autentizaci s podporou bezheslového přihlašování, biometrie, digitálních certifikátů a SSO s využitím mobilního telefonu. Vyznačuje se vysokou úrovní zabezpečení, pohodlným používáním a vytváří extrémně silnou **vícefaktorovou autentizaci**.

*Nová verze Q1/2025, Ukázka prototypu [Credential provider](#)

MATRIX MFA do PC



MFA Mobilní telefon



Znalostní
faktor



Držitelský
faktor



Biometrický faktor

Varianta 1

Uživ. jméno +
heslo

Mobilní tel. + PUSH notif. +
Otisk prstu

Varianta 2 (Offline)

Uživ. jméno +
heslo

QR kód + Mobilní tel.
+ TOTP (časově omezený) +
Otisk prstu

Varianta 3

Uživ. jméno +
heslo

Mobilní tel. + PUSH notif. +
Obličej

Varianta 4 (Offline)

Uživ. jméno +
heslo

QR kód + Mobilní tel.
+ TOTP (časově omezený) +
Obličej

Offline - pokud se uživatel již někdy v historii přihlásil do PC, je možné se přihlásit přes Offline QR kód

BEZHESLOVÝ MATRIX do PC



MFA Mobilní telefon	 Znalostní faktor  Držitelský faktor  Biometrický faktor  Perimetr faktor			
Varianta 5		QR kód + Mobilní tel. (login certifikát X.509)	Obličej	
Varianta 6 (Q2-2025)		QR kód + Mobilní tel. (login certifikát X.509)	Otisk prstu	
Varianta 7 (Q2-2025) OFFLINE		Mobilní tel. (login certifikát X.509)	Obličej	Automatické zahájení přihlášení
Varianta 8 (Q2-2025) OFFLINE		Mobilní tel. (login certifikát X.509)	Otisk prstu	Automatické zahájení přihlášení
Varianta 9 (Q2-2025) OFFLINE	Passcode (PIN)	Mobilní tel. (login certifikát X.509)		
Varianta 10 (Q2-2025) OFFLINE	Passcode (PIN)	Mobilní tel. (login certifikát X.509)		Automatické zahájení přihlášení

MFA
BADGE



Hardwarový
PIN

Badge / Certifikát X.509

Touch id /
Voice print

GITRIX a jeho konkrétní možnosti jak kombinovat metody autentizace v praxi k využívání extrémně silné autentizace (MFA):

Crayonic Badge:

- Použití Badge s certifikátem, umožňující volbu Touch ID nebo Voice ID, případně volbu kombinace s HW PIN.
- **Další faktor:** Perimetr
- Kombinace znázorněny v tabulce:

Benefity Crayonic Badge:

- Nabízí robustní řešení pro multifaktorovou autentizaci s podporou bezheslového přihlašování, biometrie, digitálních certifikátů a SSO. Jeho největší výhody spočívají ve vysoké úrovni zabezpečení, pohodlném používání a možnosti integrace s různými systémy.

VIDEO UKÁZKA - “Use case hospital”

MATRIX MFA do PC



MFA
BADGE



Znalostní
faktor



Držitelský
faktor



Biometrický faktor

Varianta 1

Hardwarový
PIN

Badge / Certifikát X.509

Touch ID

Varianta 2

Hardwarový
PIN

Badge / Certifikát X.509

Varianta 3

Badge / Certifikát X.509

Touch ID

MFA
Smart Card login

PIN

Čipová karta /
Certifikát X.509



MATRIX MFA do PC



GITRIX a jeho konkrétní možnosti jak kombinovat metody autentizace v praxi k využívání extrémně silné autentizace (MFA):

Čipová karta:

- použití PIN a ČK s certifikátem pro MFA tvoří silnou bezheslovou autentizaci.
- Kombinace znázorněny v tabulce:

Benefity MFA Smart Card login:

- **FIPS 140-2 certifikace:** THALES má vysokou úroveň zabezpečení a splňuje přísné bezpečnostní standardy (FIPS certifikace).
- **Jednoduchá správa:** Je snadno integrován do podnikových prostředí s požadavky na PKI a správu identit.
- **Automatická vzdálená pomoc** s PINem.

MFA
Smart card Login



Znalostní
faktor



Držitelský
faktor



Biometrický faktor

Varianta 1

PIN

Čipová karta PKI /
Certifikát X.509

Varianta 2

PIN

Čipová karta QSCD /
Certifikát X.509

Varianta 3

PIN

Čipová karta PKI -
hybridní / Certifikát
X.509

Varianta 4

PIN

Čipová karta QSCD -
hybridní / Certifikát
X.509

Multifaktorová autentizace - ukázka

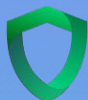
Centrální administrace nastavení MFA z integrační platformy Gitrix

Crayonic badge™

- Přihlašování uživatele certifikátem vydaným do čipu Crayonic badge prostřednictvím konektoru na PKI.
- Přihlášení do operačního systému pouze na základě nastaveného perimetru bez nutnosti zadávat PIN.
- **Crayonic Badge** podporuje **Single Sign-On** (SSO), což znamená, že po jednom ověření může uživatel přistupovat ke všem autorizovaným aplikacím a systémům **bez** potřeby **opětovného zadávání** autentizačních údajů.

Crayonic badge™





(SSO) Jedna karta (a) jeden login = vládne všem!



SMART CARD

Čipová karta
+ Certifikát x.509
+ PIN

MFA: 1. Přihlášení uživatele:
Kerberos login do OS



MOBILE

Uživatelské jméno
+ Heslo

MFA: 1. Přihlášení uživatele:
Kerberos login do OS



BADGE

Badge karta
+ Hardware PIN
+ Certifikát x.509
+ Touch ID

MFA: 1. Přihlášení uživatele:
Kerberos login do OS



GITRIX

Výhody SSO:

- Zjednodušení přihlašování.
- Zvýšení bezpečnosti.
- Centralizovaná správa přístupů.
- Rychlý onboarding a offboarding.

Aplikace (v rámci organizace)

Bez nutnosti
dalšího
přihlašování a
používání hesel

Nemocniční
informační
systém



Agendový
systém (A)



Fortinet FortiGate, Cisco
Any Connect, Microsoft
RDP, Citrix, Check Point,
VPN

Ekonomický
systém
ERP



DMS, Spisová služba

Personální
systém (HR)

Office 365

Google workspace

Dropbox, Slack



Např. **FIDO2, T-OTP**

**Dodatečná autorizace
k vybraným aplikacím**

INTEGRAČNÍ PLATFORMA GITRIX

Vše na jednom místě!

Aplikace a služby

Integrace a konektory



Cílové skupiny

Klíčové oblasti, které jednotlivé skupiny uživatelů řeší:

Pro operátory (desktop aplikace):

- Vydání a recyklace karty.
- Vydání a zneplatnění certifikátů.
- Správa obsahu karty/tokenu.

Pro uživatele (desktop aplikace):

- Vzdálená pomoc se zapomenutým PINem.
- Možnost změnit PINy.
- Obnova certifikátů (na tři kliknutí).

Pro správce a management (webové rozhraní):

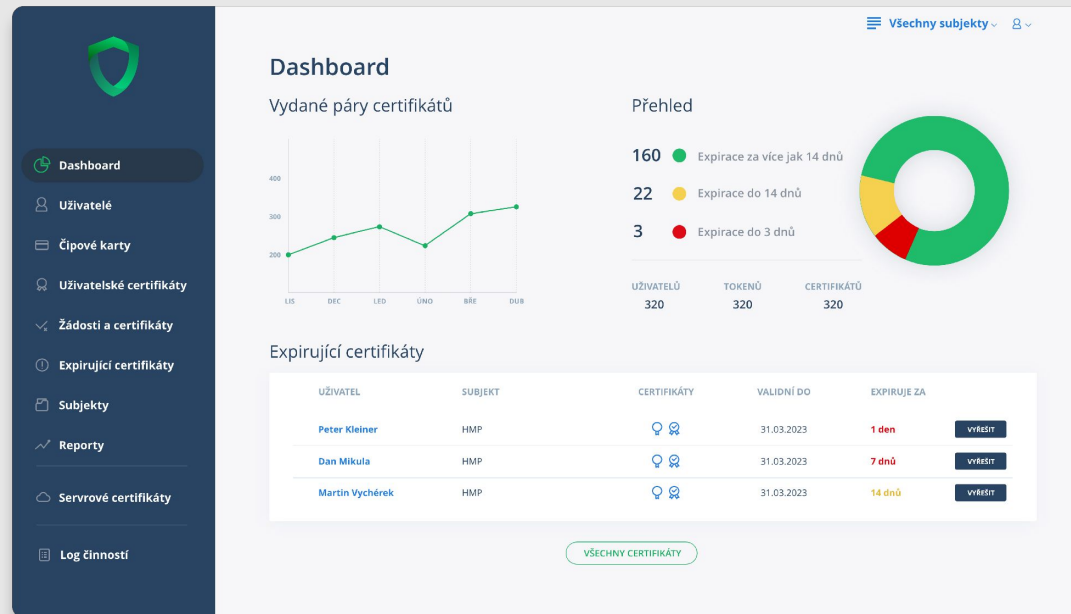
- Manažerský dashboard.
- Veškerá evidence dat a událostí.
- Iniciace obnovy certifikátů.
- Vzdálená revokace certifikátů.
- Auditní stopa (logované události).



Integrační platforma

Webové rozhraní pro správce a management:

- Manažerský dashboard.
- Veškerá evidence dat a událostí.
- Inicie obnovy certifikátů.
- Vzdálená revokace certifikátů.
- Informace o uživateli.
- Informace o tokenech.
- Správa agendy žádostí o certifikáty.
- Reporting.
- **Auditní stopa** (logované události).
- **Monitoring serverových certifikátů** (Server Agent).



Správa životního cyklu certifikátu

Desktop aplikace pro operátory



- Vydání a přiřazení karty / tokenu.
- Vydání certifikátů:
 - ◆ Komerční / kvalifikovaný certifikát.
 - ◆ Interní certifikát.
- Zneplatnění certifikátů (revokace).
- Správa obsahu.
- Recyklace.

OPERÁTORSKÁ APLIKACE - vydání kvalifikovaného certifikátu

Certix Operátor

Ověření
průkazu

Podepsání
žádosti a
smlouvy

Podepsání
předávacích
protokolů

Úspěšně
vydáno

Ověření průkazu žadatele

Opište občanský průkaz, nebo pas žadatele. Údaje pro vytvoření kvalifikovaného certifikátu

OSOBNÍ ÚDAJE

ID zaměstnance: mvyborny, E-mail: franta.prospera@vasecms.cz

Typ dokladu 

Občanský průkaz 

Datum vydání

20.20.2022

Nesprávný formát

ORGANIZAČNÍ JEDNOTKA

☐ Prospera. s.r.o.

Plné jméno žadatele (včetně titulů v dokladu)

Bedřich Smetana, Ing.

☐ Titul není uveden v dokladu, doložen diplomem 

Titul zadán na nesprávné pozici

Ulice č.p./č. o.

Vodičkova 36

PLATNOST CERTIFIKÁTU

1 rok 

ID dokladu

0123654789

ID se neshoduje s CZ ani SK formátem 

Okres / městský obvod

Praha 1

TRVALÝ POBYT

Obec, část obce

Praha

 Neodpojujte kartu od počítače po celou dobu procesu.
Může dojít ke znehodnocení karty.

POKRAČOVAT

OPERÁTORSKÁ APLIKACE - vydání kvalifikovaného certifikátu

Certix Operátor



Vydání certifikátů proběhlo v pořádku!

Nyní kartu odpojte a předejte žadateli

CZECHPOINT

Přejete si zaregistrovat sériová čísla nově vydaných certifikátů do systému Czech POINT?

ANO

NE, ZAVŘÍT OKNO



[Opětovný tisk smlouvy](#) [Opětovný tisk protokolů](#)

OPERÁTORSKÁ APLIKACE - recyklace a správa obsahu karty

 Certix Operátor

Připojená zařízení

**Martin Výborný**
IDPrime MD 840 B

**Jana Novotná**
SafeNet 4000

**Plk. Jaroslav Vomáčl**
Crayonic Badge 450

**#00123695833**
Crayonic KeyVault

Operátor

**Jaroslav Borovička**
Url: <https://app.certix.>
Certifikát: Martin Výborný
Platnost do: 02.09.2025

[→ Odhlásit se](#) [↗ CMS](#)

 Certix Operátor - Obsah tokenů a recyklace

Martin Výborný
ID Zaměstnance: mvyborny
E-mail: martin.prospera@vasecms.cz
Subjekt: Prospera

Sériové číslo tokenu
ECA1D16541E2FE20

RECYKLOVAT TOKEN

Obsah tokenů

Typ	Certifikát	Platný do	Akce
	Martin Výborný Sériové číslo: AED2C73AD171004E97E19526837A796C Vydavatel: CN=Certisys Login ECA1D16541E2FE20	21.01.2027	
	Martin Výborný Sériové číslo: 67A101BA Vydavatel: CN=TEST - CCAeID - C..., O=elidentity a.s.	24.01.2023	
	Martin Výborný Sériové číslo: 0E20A4B0 Vydavatel: CN=TEST - ACAeID - Q..., O=elidentity a.s.	24.01.2023	
	Martin Výborný Sériové číslo: 67A101BA Vydavatel: CN=TEST - CCAeID - C..., O=elidentity a.s.	24.01.2023	
	Martin Výborný Sériové číslo: 0E20A4B0 Vydavatel: CN=TEST - ACAeID - Q..., O=elidentity a.s.	24.01.2023	

Model

IDPrime MD 840 B

certisys.cz)

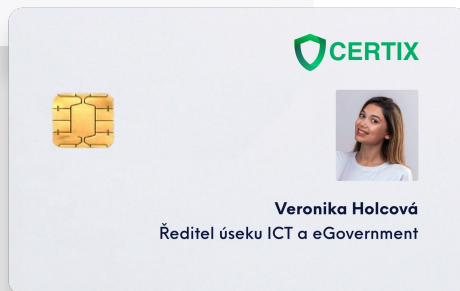
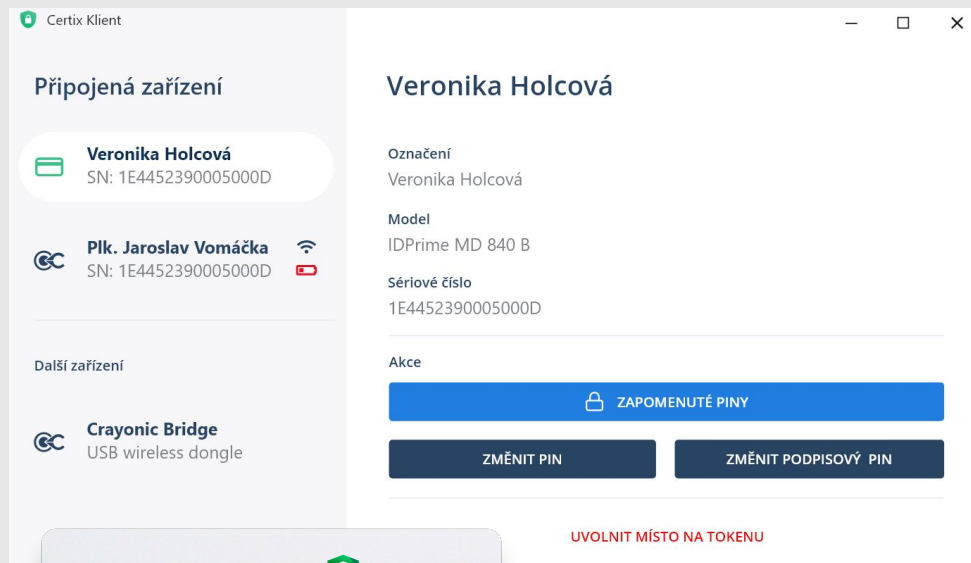
ZOBRAZIT OBSAH TOKENU

T

Správa životního cyklu certifikátu

Desktop aplikace pro uživatele

- Obnova certifikátů (na tři kliknutí)
- Vzdálená pomoc se zapomenutým PINem
- Změna PINů
- Smazání starých certifikátů



Server Agent

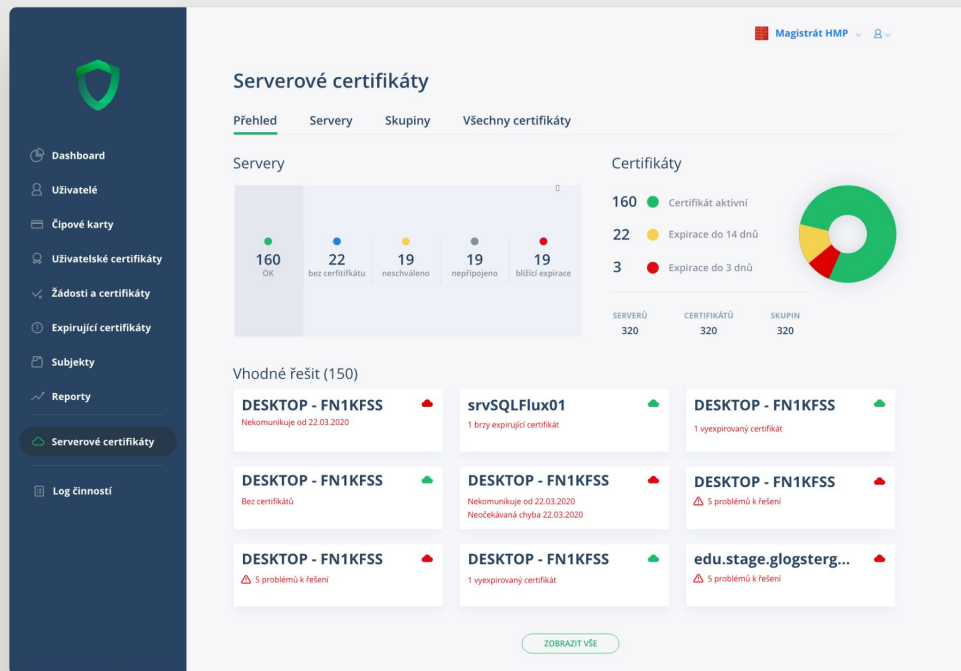
Monitoring serverových certifikátů.

Centralizovaný monitoring serverových certifikátů

- Manažerský dashboard.
- Hlídní platnosti serverových certifikátů.
- Automatická synchronizace nainstalovaných serverových certifikátů.
- Notifikace pro správce a techniky serverů ohledně stavu serverů a nainstalovaných certifikátů.

Realizujeme vydávání a obnovu

- Serverových certifikátů od akreditovaných CA.
- Serverových certifikátů od interních CA.
- Komerčních SSL certifikátů.



Podporované HW prostředky

Integrace řešení na QSCD čipové karty (Gemalto, Starcos), HSM (THALES), bezpečné klíčenky a badge (CRAYONIC)

Crayonic KeyVault™

- Možnost nastavit kombinaci **MFA**.
- **Bezheslové přihlášení**: Proximity Biometric Login & Auto Logout.
- **Unikátní HW zadávání** PINu nebo otisk prstu.
- Úložiště certifikátů (PIV smart karty X.509).
- Podporuje **FIDO/U2F**. [Detailnější informace](#)

Crayonic badge™

- Stejné funkcionality jako výše .
- Možnost autorizovat zařízení na určitou dobu dokud zařízení nepoložíte.
- Připravujeme možnost vložení QSCD karty s kvalifikovaným certifikátem (zároveň funguje jako čtečka). [Detailnější informace](#)

Crayonic badge™



HSM: THALES



nShield Solo Connect XC



Crayonic KeyVault™



Čipové Karty: Gemalto, Starcos



Integrační platforma Certix - HSM

Vzdálené kvalifikované služby v zabezpečeném cloudu.

HSM security modul

- Vstupenka do moderního světa vzdáleného podepisování - HSM jako úložiště soukromých klíčů .
- plná integrace na kvalifikovaného poskytovatele služeb I.CA.

CERTIX nabízí tyto funkcionality prostřednictvím rozhraní REST API:

- Služba vytváření kvalifikovaného el. podpisu na dálku.
- Služba vytváření kvalifikované el. pečete na dálku.
- Kvalifikovaná el. časová razítka (TSA).
- Kvalifikovaná služba ověřování el. podpisů a pečeti (QVerifyTL).
- Služba uchovávání elektronických podpisů (LTA).



nShield Solo Connect XC

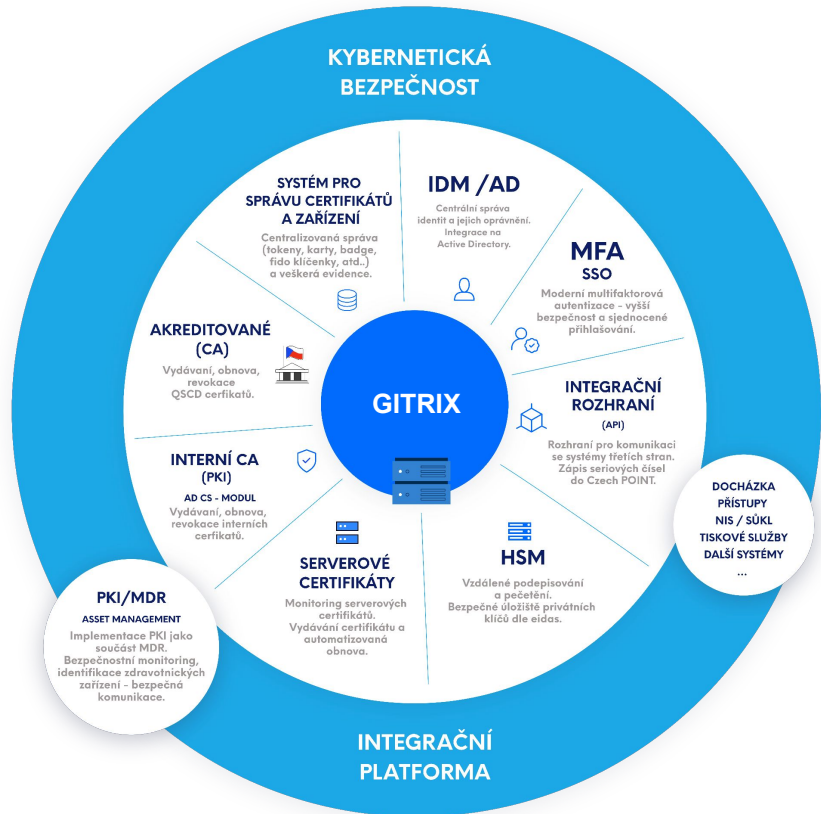


Shrnutí - GITRIX



Hlavní benefity:

1. **Integrační platforma** - koncentruje požadavky na správu digitálních certifikátů do jednoho místa - automatizace firemních procesů.
2. **Flexibilita, škálovatelnost** - nákup a instalace jednotlivých modulů lze realizovat postupně v etapách - jednoduchá rozšiřitelnost.
3. **Centralizovaná správa** - jednotný management HW prostředků, certifikačních autorit, certifikátů a uživatelů.
4. **Moderní MFA & SSO** - zajišťujeme vysoké nároky na kybernetickou bezpečnost v souladu s NIS2 moderními HW prostředky ve spolupráci s partnery GiTy a.s. & Crayonic.
5. **Přímá integrace PKI a akreditované certifikační autority.**
6. **IDM řešení a konektor AD** - centrální správa uživatelů a jejich digitálních identit - obslužíme uživatele jednou návštěvou na personálním oddělení.
7. **Automatizovaný proces** vydávání, obnovy a revokace digitálních certifikátů.
8. **Automatická pomoc s PINem** uživatelům bez nutnosti zásahu administrátora.
9. **Intuitivní uživatelské rozhraní a jednoduché procesy.**
10. **Jednoduchá recyklace HW zařízení**



Hlavním cílem platformy je integrovat veškeré požadavky na správu životního cyklu certifikátů do jednoho místa.





GITRIX

System pro správu digitálních certifikátů, uživatelských identit,
autentizačních prostředků a kyberbezpečnost.

Děkujeme za váš čas.

Neváhejte nás kontaktovat, rádi vám řešení představíme.

www.gitrix.cz