Návrh implementace Public Key Infrastructure

Karel Wilhelm

Bakalářská práce
2023

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav automatizace a řídicí techniky

Akademický rok: 2022/2023

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Karel Wilhelm**
Osobní číslo:	**A19489**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Informační a řídicí technologie**
Forma studia:	**Kombinovaná**
Téma práce:	**Návrh implementace Public Key Infrastructure**
Téma práce anglicky:	**Public Key Infrastructure Implementation**

Zásady pro vypracování

1. Vypracujte literární rešerši na dané téma.
2. Zhodnoťte možné praktické problémy související s PKI.
3. Navrhněte vhodný způsob implementace PKI.
4. Proveďte popis implementace v dané instituci.
5. Zhodnoťte dosažené poznatky.

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. ZELENKA, Josef. *Ochrana dat: kryptologie*. Hradec Králové: Gaudeamus, 2003, 198 s. ISBN 8070417374.
2. CIMINO, Al. *Příběh kryptologie: od starověkých šifer po kvantovou kryptografii*. Praha: Dobrovský, 2018, 215 s. Knihy Omega. ISBN 9788073908874.
3. PIPER, F. C. a Sean MURPHY. *Kryptografie*. Praha: Dokořán, 2006, 157 s. Průvodce pro každého. ISBN 8073630745.
4. BURDA, Karel. *Aplikovaná kryptografie*. Brno: Vutium, 2013, 255 s. ISBN 9788021446120.
5. OULEHLA, Milan a Roman JAŠEK. *Moderní kryptografie*. [Praha]: IFP Publishing, 2017, 186 s. ISBN 9788087383674.
6. BURDA, Karel. *Kryptografie okolo nás*. Praha: CZ.NIC, z.s. p.o., 2019, 128 s. CZ.NIC. ISBN 978-80-88168-49-2. Dostupné také z: https://knihy.nic.cz/files/edice/Kryptografie_okolo_nas.pdf

Vedoucí bakalářské práce: **doc. Ing. Roman Šenkeřík, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání bakalářské práce: **16. prosince 2022**
Termín odevzdání bakalářské práce: **24. května 2023**

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

prof. Ing. Vladimír Vašek, CSc. v.r.
ředitel ústavu

Ve Zlíně dne 12. prosince 2022

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 20. května 2023 Karel Wilhelm, v.r.

ABSTRAKT

Tato bakalářská práce se zaměřuje na návrh a implementaci Public Key Infrastructure (PKI). Zahrnuje literární rešerši tohoto konceptu, hodnocení potencionálních praktických problémů spojených s PKI a návrh vhodné implementační strategie. Navrhovaný model PKI bere v úvahu specifické potřeby instituce a poskytuje řešení pro efektivní řízení klíčů, správu certifikátů, autorizaci a autentizaci uživatelů. Práce ukazuje výhody a nevýhody použití PKI a poskytuje doporučení pro další rozvoj PKI v instituci. Celkově tato práce poskytuje ucelený pohled na implementaci PKI a její důležitost při zajištění bezpečnosti a důvěryhodnosti digitálních transakcí a komunikace.

Klíčová slova: Asymetrická kryptografie, Certifikační autorita, eGoverment, Implementace PKI, Public Key Infrastructure, Symetrická kryptografie.

ABSTRACT

This bachelor thesis focuses on the design and implementation of Public Key Infrastructure (PKI). It includes a literature review of the concept, an assessment of potential practical problems associated with PKI, and the design of an appropriate implementation strategy. The proposed PKI model takes into account the specific needs of the institution and provides a solution for efficient key management, certificate management, and user authorization and authentication. The paper highlights the advantages and disadvantages of using PKI and provides recommendations for its further development within the institution. Overall, this thesis offers a comprehensive view of PKI implementation and underscores its importance in ensuring the security and trustworthiness of digital transactions and communications.

Keywords: Asymmetric Cryptography, Certification Authority, eGovernment, PKI Implementation, Public Key Infrastructure, Symmetric Cryptography.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

V dnešním moderním světě, kdy většina našich činností je spojena s ukládáním a přenosem mnohdy citlivých dat, je nezbytné investovat značné prostředky do zabezpečení a autentizace. Jak se technologie vyvíjejí a stávají se stále více součástí našeho každodenního života, stává se problematika kybernetické bezpečnosti nejen důležitější, ale také složitější. Zároveň se zvyšuje počet kybernetických útoků, což představuje vážnou hrozbu pro jednotlivce i organizace.

Legislativa také udává množství opatření, která mohou být pro organizace náročná a zdlouhavá. Tyto požadavky jsou ještě závažnější pro organizace kritické infrastruktury, kde může mít jakýkoliv únik nebo zneužití dat katastrofální důsledky. Nicméně i běžné firmy musí být ostražité a vytvářet robustní systémy a postupy pro zabezpečení svých dat.

Bakalářská práce se zabývá návrhem implementace Public Key Infrastructure (PKI) s cílem zvýšit bezpečnost dat a komunikace. V současné době, kdy kybernetická bezpečnost hraje stále důležitější roli ve společnosti a digitálním světě, je důležité zajistit bezpečnost a ochranu citlivých informací.

V práci je provedena detailní analýza současných studií a odborných článků týkajících se PKI. Cílem je poskytnout čtenáři dostatečný teoretický základ pro pochopení principů fungování PKI, jeho výhod i nevýhod.

V další části je analyzováno několik praktických problémů a výzev, které mohou vzniknout při implementaci PKI, například zabezpečení certifikační autority, správa klíčů a revokace certifikátů.

Na základě získaných poznatků z literární rešerše a analýzy praktických problémů je navržen optimální způsob implementace PKI pro organizaci. Tato část zahrnuje doporučení pro výběr a konfiguraci hardwaru, softwaru a sítě.

Následně se práce věnuje popisu postupu implementace PKI v organizaci, včetně harmonogramu, potřebných zdrojů a zodpovědných osob. Dále je popsán způsob zajištění souladu s legislativou a interními bezpečnostními politikami.

V závěrečné části práce jsou zhodnoceny výsledky dosažené po předložení návrhu a následné implementace PKI. Je zde popsáno, jakým způsobem je zvýšena bezpečnost dat a komunikace v organizaci, jaké přínosy a potenciální rizika přinese implementace PKI a jaké další kroky jsou učiněny pro udržitelnost a zlepšení systému.

Ke zpracování práce jsou využity odborné zdroje, praktické zkušenosti a případové studie, které pomohou při tvorbě návrhu a implementaci PKI v organizaci. Navíc je kladen důraz na soulad s příslušnými normami, standardy a legislativou, aby bylo zajištěno, že navrhované řešení je bezpečné, efektivní a v souladu s požadavky daného prostředí.

Výsledkem této bakalářské práce je komplexní návrh a popis implementace PKI pro vybranou organizaci, který bude sloužit jako základ pro zajištění bezpečnosti a ochrany citlivých dat a komunikace. Práce také poukazuje na potenciální rizika a problémy související s PKI, což umožní čtenářům lépe pochopit tuto problematiku a připravit se na možné výzvy při implementaci vlastního PKI řešení.

I. TEORETICKÁ ČÁST

1 ÚVOD DO KRYPTOGRAFIE A PKI

Kryptografie umožnuje komunikaci velkého množství lidí různými prostředky, jako je e-mail mobilní telefony, sociální sítě, webové stránky, ale také vznik digitálních kryptoměn, např. BitCoinu, kde se transakce ověřují uzly sítě a zaznamenávají v distribuované decentralizované databázi zvané BLOCKCHAIN. Nejdůležitější oblastí použití kryptografie je ochrana důvěrných informací a obchodních transakcí. Pro tyto účely je tedy naprosto nezbytné mít přehled o kryptografických systémech, algoritmech a jejich souvislostech s PKI.

1.1 Vývoj symetrické a asymetrické kryptografie ve vztahu k PKI

Symetrická a asymetrická kryptografie jsou dvě základní kategorie kryptografických systémů. Rozvojem technologií v 70. a 80. letech minulého století tyto dvě kategorie prošly významným vývojem. Symetrická kryptografie je založena na použití společného tajného klíče pro šifrování a dešifrování informací. Z výše uvedeného plyne potřeba před začátkem komunikace, nebo v jejím průběhu důvěryhodným kanálem předat šifrovací klíč druhé straně. Mezi symetrické algoritmy patří například DES[1] (Data Encryption Standard), které byly v roce 1977 zvoleny za standard (dle FIPS 46-3), dále pak nástupce Triple DES a AES[2]. Tyto algoritmy dobře slouží k šifrování velkého objemu dat. Nevýhodou zmíněných algoritmů je nutnost zabezpečeného sdílení klíčů mezi více stranami. Tato podmínka zvyšuje náročnost celého procesu [1].

Asymetrická kryptografie je založena na použití privátního a veřejného klíče. K privátnímu klíči má přístup pouze jeho vlastník. Veřejným klíčem se šifrují zprávy, které může dešifrovat pouze vlastník privátního klíče.

Moderní kryptografické algoritmy jsou postaveny na Kerckhoffově principu, který říká: „*Bezpečnost systému musí záviset výhradně na utajení klíče, nikoli na konstrukci systému.*“[3]

1.2 RSA

RSA (Rivers Shamir Adelman) je asymetrický kryptografický systém, který se používá k šifrování a digitálnímu podepisování dokumentů. Byl publikován v roce 1978 a patří do kategorie kryptografických systémů založených na faktorizaci velkých prvočísel

[1] DES – Data Encryption Standard, FIPS 46-3.
[2] AES – Advance Encryption Standard, FIPS 197.
[3] Zdroj: http://www.crypto-it.net/eng/theory/kerckhoffs.html.

nazývaných IF (Integer Factorization). Bezpečnost tohoto systému spočívá v extrémní složitosti faktorizace velkých prvočísel v reálném čase. RSA algoritmus není absolutně neprolomitelný, především díky prudkému rozvoji výkonnosti výpočetní techniky a rozvoji paralelních architektur je minimální délka klíče 2048 bitů a vyšší. Pro zvýšení bezpečnosti je vhodné použít klíče minimálně o délce 3072 bitů a více [2].

RSA algoritmus byl patentován v roce 1983 na území Spojených států amerických, V mezinárodním prostředí patent nemohl být uznán z důvodu zveřejnění algoritmu před podáním patentu, který vypršel v roce 2000. V roce 2009 bylo dosaženo důležitého milníku, kdy se podařilo provést faktorizaci prvočísla o délce 768 bitů. Tento úspěch zvýšil povědomí o potřebě silnějšího šifrování. Prvočíslo, na kterém byla faktorizace provedena, naleznete v tabulce č. 1 [3].

Tabulka 1 Faktorizace prvočísla v roce 2009 [2]

Faktorizace prvočísla o délce 768 bitů	
RSA - 768	123018668453011775513049495838496272077285356959533479219732 245215172640050726365751874520219978646938995647494277406384 592519255732630345373154826850791702612214291346167042921431 160222124047927473779408066535141959745985690214341 3
RSA - 768	334780716989568987860441698482126908177047949837137685689124 313889828837938780022876147116525317430877378144679994 89 × 367460436667995904282446337996279526322791581643430876426760 322838157396665112792333734171433968102700927987363089 17

V roce 2018 výzkumníci z univerzit v Bonnu a Melbourne dokázali faktorizovat 795bitové prvočíslo pomocí běžného serveru. Tato faktorizace ukázala, že prvočísla o délce 1024 bitů, která byla dříve považována za bezpečná pro použití v RSA kryptografickém systému, mohou být faktorizována s použitím běžně dostupných výpočetních zdrojů. Tento objev znamenal zvýšené obavy o bezpečnost používání RSA s klíči menší délky a poskytl důrazný argument pro používání klíčů o délce 2048 bitů nebo vyšší, jejichž používání je dnes považováno za dostatečně bezpečné [4].

1.2.1 Tvorba klíčového páru

Nejprve je nutné vytvořit dvě velká prvočísla p, q, která je nejvhodnější vygenerovat pomocí Pseudo-Random Number Generators (PRNGs), v lepším případě True Random Number Generators (TRNGs) [5].

Vygenerovaná čísla je nutné otestovat, zda jsou vůbec prvočísla. V současné době jsou známy jen pravděpodobnostní testy, které tvrdí, že testované číslo je prvočíslo s určitou pravděpodobností P.

Dostupné pravděpodobnostní testy:

- FERMATŮV TEST je omezen schopností identifikovat určité typy složených čísel (Carmichaelova čísla)
- MILLER-RABINŮV TEST
- ERATOSTHENOVO SÍTO
- WILSONOVA VĚTA
- CARMICHAELOVA ČÍSLA
- SOLOVAYŮV-STRASSENŮV

Určíme jejich součin (1):

$$n = p \cdot q \tag{1}$$

Vypočítáme hodnotu EULEROVY FUNKCE (2):

$$\phi(n) = (p-1)(q-1) \tag{2}$$

Určíme veřejný exponent e, které musí být nesoudělné s ϕ.

Je vypočítán soukromý exponent d, dle vztahu (3):

$$d = e^{-1} mod\ \phi \tag{3}$$

Veřejný klíč je dvojice (e, n), soukromý klíč je dvojice (d, n) [2].

1.3 ECDSA

ECDSA (Elliptic Curve Digital Signature Algorithm) je asymetrický kryptosystém používaný k podepisování a vytváření klíčů. Jeho bezpečnost je založena na řešení problému diskrétního logaritmu skupiny bodů na eliptické křivce. V roce 1985 Victor S. Miller[4]

[4] *Elliptic Curves and their use in Cryptography*. New York, 1997. Study. Princeton. Vedoucí práce Victor S. Miller.

prezentoval své výsledky na konferenci CRYPTO 85[5]. Kryptosystém EC založený na aditivní grupě bodů eliptické křivky je považován za bezpečný, protože nebylo možné jej prolomit pomocí Pollardova algoritmu[6]. Nicméně, může nastat problém, pokud by byl proveden útok „postranním kanálem“ na elektronický podpis generovaný na přenosném zařízení, kdy by bylo možné detekovat zvýšenou spotřebu elektrické energie [6].

Výhodou ECC jsou podstatně kratší klíče, a tedy vyšší efektivita systému, při zachování bitové bezpečnosti, která je vztahována k symetrickým šifrám (možnostem provedení brute force útoku). Tabulka č. 2 uvádí příklady délky klíčů pro různé úrovně zabezpečení. V dlouhodobém horizontu budou bezpečné klíče s úrovní zabezpečení 128 bitů, což znamená, že RSA bude muset používat klíče o délce 3072bitů a ECC jen 256bitů [3].

Porovnání velikosti klíčů kryptografických systémů:

Tabulka 2 Velikost klíče kryptografického systému [2]

Symetrický	ECDSA	RSA
80	160	1024
112	224	2048
128	256	3072
192	385	7680

1.4 AES

Byla vyvinuta v roce 1998 Belgickými kryptografy pod jménem Rijndael. Tato symetrická bloková šifra zpracovává datové bloky s délkou 128, 192 a 256 bitů a klíči o délce 128, 192, 256 bitů. Šifra je schopna zpracovat i větší délku datových bloků. Šifra Rijndael by přijata NIST (National Institute of Standards and Technology) jako základní šifrovací algoritmus. Algoritmus AES (Advanced Encryption Standard) používají Americká federální ministerstva a agentury k šifrování dat od roku 2002. NIST provádí každých 5 let formální revizi standardu [7].

1.4.1 Popis AES

Vstupní blok má délku 128 bit. To představuje Nb = 4 vyjadřující počet 32bitových slov (sloupců) ve stavu. Šifra AES nepracuje s vektory, ale s maticemi (stavové matice) ve formátu 4 x 4 bajty, ve které jsou definovány čtyři transformace: [3]

[5]Crypto85–Advances in Cryptology: Proceedings of CRYPTO'85.
[6] Pollard, J. (1974). Theorems on factorization and primality testing. *Mathematical Proceedings of the Cambridge Philosophical Society, 76*(3), 521-528. doi:10.1017/S0305004100049252.

- substituce bajtů („SubBytes“),
- rotace řádků („ShiftRows“),
- substituce sloupců ("MixColumns“),
- přičtení iteračního klíče („AddRoundKey“).

Dá se říci, že šifra AES je několik různých šifer. Lze určit tři dílčí šifry v režimu šifrování:

1) Iniciační: AddRoundKey,
2) Hlavní: SubBytes → ShiftRows → MixColumns → AddRoundKey,
3) Závěrečná: SubBytes → ShiftRows → MixColumns.

V tabulce č. 3 naleznete kombinace jednotlivých rund pro různé délky klíčů a velikosti bloků.

Tabulka 3 Kombinace délky klíče, bloku a počtu kol výpočtu v algoritmu AES [8]

Kombinace jednotlivých rund			
	Délka klíče	Velikost bloku	Počet rund
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

1.5 Přehled podporovaných algoritmů projektu NESSIE

EU zahájila v roce 2000 projekt NESSIE[7]s cílem zhodnotit šifrovací algoritmy potřebné k ochraně osobních údajů, on-line bankovnictví a podpoře elektronické veřejné správy. K ukončení a vyhodnocení projektu došlo v roce 2003. Celkem bylo hodnoceno 42 kryptografických algoritmů z více než 10 zemí světa. Z celkového počtu bylo vybráno 17 algoritmů, u kterých nebyly zjištěny nedostatky. Jsou to tyto algoritmy a šifry:

[7] NESSIE – New European Schemes for Signatures, Integrity and Encrypryption

Blokové šifry:

- MISTY1,
- Camellia,
- SHACAL-2,
- AES.

Šifrování s veřejným klíčem:

- ACE Encrypt,
- PSEC-KEM,
- RSA-KEM.

Algoritmy MAC a hašovací funkce:

- Two-Track-MAC,
- UMAC,
- CBC-MAC,
- HMAC,
- Whirlpool,
- SHA-256, SHA-384 a SHA-512.

Algoritmy digitálního podpisu:

- ECDSA,
- RSA-PSS,
- SFLASH,

Identifikační schémata:

- GPS [9].

Zajímavý je přístup EU ke kryptografickým systémům v porovnání s USA. Projekt NIST (National Institute of Standards and Technology) vybíral šifrovací standard jen pro symetrické blokové algoritmy. EU k tomuto přistupovala komplexněji v uvedeném projektu NESSIE [8].

1.6 Zajišťování integrity a důvěry

V dnešním stále více digitalizovaném světě hraje klíčovou roli důvěra v bezpečnost a spolehlivost technologií. Certifikační autority jsou základními pilíři tohoto systému. Poskytují nezbytnou jistotu a zajišťují integritu všech transakcí a komunikace v digitálním prostředí. Tyto instituce vykonávají důležitý úkol tím, že ověřují a potvrzují autenticitu a bezpečnost online služeb, produktů a platforem.

1.6.1 Certifikační autorita

Certifikační autorita (CA) je důvěryhodná entita, vydávající a spravující digitální certifikáty v rámci PKI. Digitální certifikáty jsou elektronické dokumenty používané pro ověření totožnosti subjektů v digitálních sítích. Tyto certifikáty jsou základem pro řadu bezpečnostních služeb, včetně autentizace, integrity dat, důvěrnosti a nepopiratelnosti. CA může také být zodpovědná za další funkce, jako je vydávání certifikátů pro jiné CA, zveřejňování CRL[8] a možnosti online validace certifikátů tzv. OCSP[9].

Důvěryhodnost CA je klíčová, jakákoliv kompromitace její bezpečnosti může vážně narušit důvěru v digitální bezpečnost.

Základní dělení CA je následující [10]:

- Podniková/organizační CA,
- Veřejná CA dále dělená na:
    - CA vydávající kvalifikované certifikáty, na obrázku č. 2 je znázorněna, struktura jednoho z poskytovatelů těchto služeb,
    - CA vydávající komerční certifikáty.

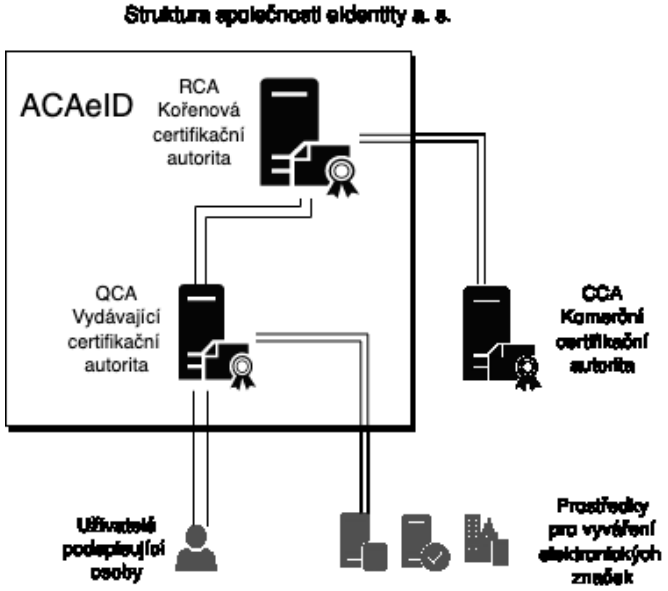
Dále CA dělíme dle typu činnosti, kterou mají vykonávat, a to na atributovou certifikační autoritu (ACA), registrační autoritu (RA) a certifikační autoritu časového razítka (TSA)[10]. Veřejné CA, vydávající kvalifikované certifikáty, čelí značným požadavkům. Jejich povinností je nejen zajistit sledovatelnost poskytovaných služeb, ale také generovat odpovídající dokumentaci pro fakturaci. Kromě výše uvedeného také musí splňovat legislativní požadavky, které jsou stanoveny zákony 297/2016 Sb[11] a 101/2000 Sb[12]. Tyto

[8] CRL – Certificate Revocation List.
[9] OCSP – Online Certificate Status Protocol – Internetový protokol používaný pro získání seznamu revokovaných X.509 certifikátů.
[10] TSA – Time Stamp Authority.
[11] Zákon 297/2016 Sb – Zákon o službách vytvářejících důvěru pro elektronické transakce.
[12] Zákon 101/2000 Sb – Zákon o ochraně osobních údajů.

požadavky jsou nezbytné pro udržení integrity a důvěryhodnosti jejich služeb, které se opírají o vydané certifikáty v souladu se zákony [10].

A dále je vyžadován audit systému dle ČSN ISO/IEL 27001 (369797)[13]. Součástí tohoto auditu jsou následující bezpečnostní dokumenty:

- Certifikační prováděcí směrnice,
- Certifikační politika – ke všem službám musí být vydána samostatná bezpečnostní politika,
- Systémová bezpečnostní politika – v tomto obsáhlém dokumentu je ustanovení bezpečnostních cílů a popsán způsob zajištění IS (Informačních Systémů),
- Celková bezpečnostní politika – stanovuje bezpečnostní cíle a popisuje celkové zajištění bezpečnosti CA.



Obrázek 1 Struktura společnosti eIdentity a. s.

V České republice jsou dostupné tyto CA [11, 12]:

- Česká národní certifikační autorita (CSCA)
- Správa základních registrů
- První certifikační autorita a.s. (I.CA)
- Česká pošta a.s. (PostSignum)
- eIdentity a.s. (ACAeID)
- Software602 a. s.

[13] ČSN ISO/IEL 27001 (369797) Informační technologie, Bezpečnostní techniky, Systémy řízení bezpečnosti informací, Požadavky.

1.6.2 Atributová certifikační autorita

Atributová certifikační autorita (ACA) je součástí infrastruktury veřejných klíčů (PKI) a zajišťuje vydávání atributových certifikátů pro subjekty, jako jsou osoby, organizace nebo zařízení. Tyto certifikáty reprezentují specifické vlastnosti daného subjektu, například jeho role, oprávnění nebo další unikátní charakteristiky. ACA garantuje, že tyto informace jsou distribuovány správným subjektům a používány dle stanovených směrnic.

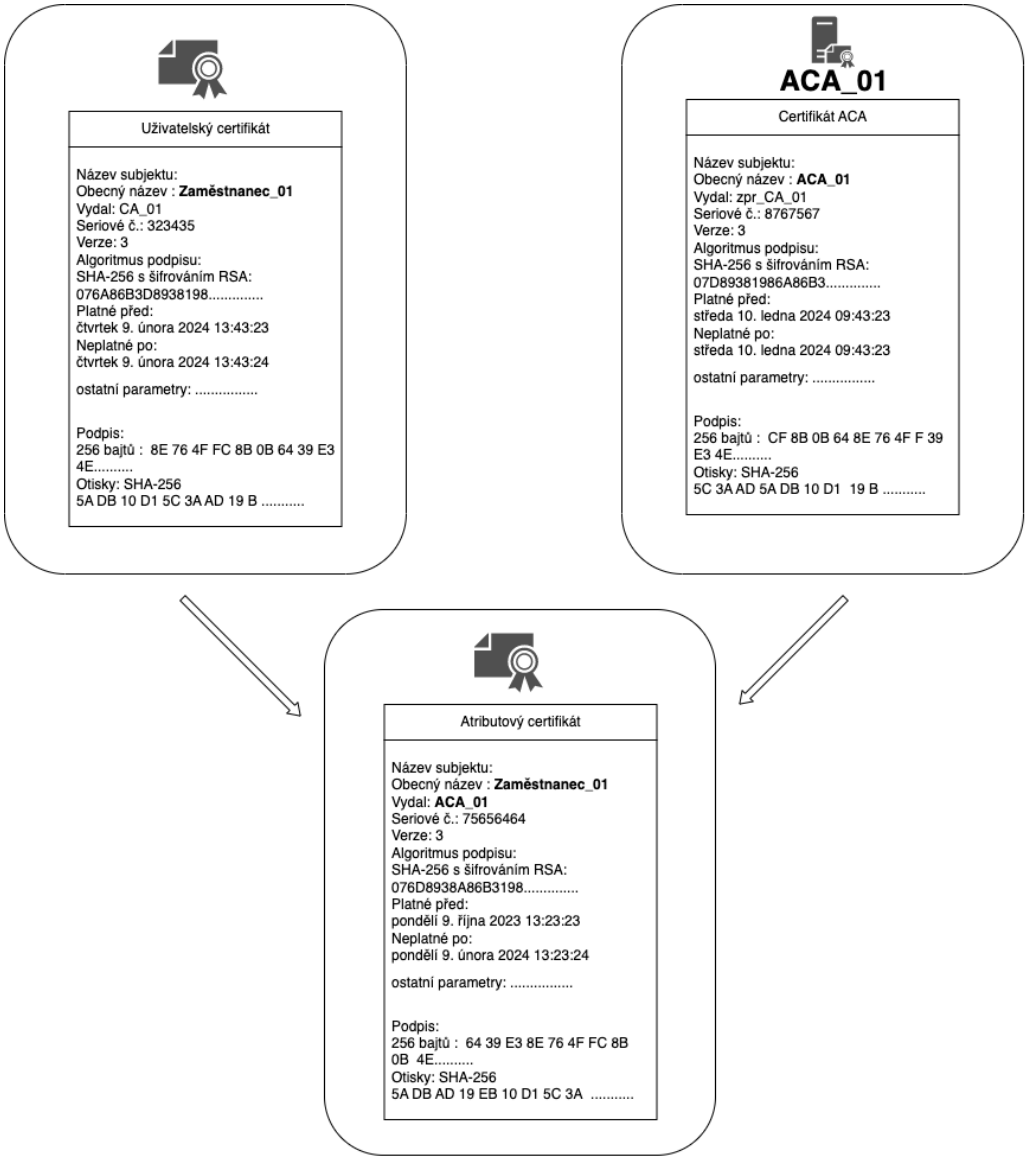
Proces fungování ACA je iniciován při podání žádosti subjektu o vydání atributového certifikátu. Tento požadavek ACA následně vyhodnotí a ověří. V případě schválení žádosti ACA vystaví atributový certifikát s požadovanými údaji.

Při provádění autentizace subjektu vůči autorizačnímu serveru jsou ověřována přístupová práva na základě jeho atributů. Při splnění podmínek je subjektu umožněn přístup k požadovanému systému či službě.

ACA také hraje důležitou roli při správě a revokaci atributových certifikátů, které již nejsou platné. Pokud dojde ke změně vlastností subjektu nebo je odebráno oprávnění, musí být jeho atributový certifikát odvolán.

Na rozdíl od klasických certifikátů, atributové certifikáty neobsahují veřejný klíč držitele, ale informace o něm viz. obrázek č. 2. Tyto certifikáty jsou klíčovým prvkem infrastruktury řízení privilegií (PMI) [14]. Na obrázku č. 3 znázorněno ověření atributového certifikátu [10].

[14] PMI – Privilege Management Infrastructure

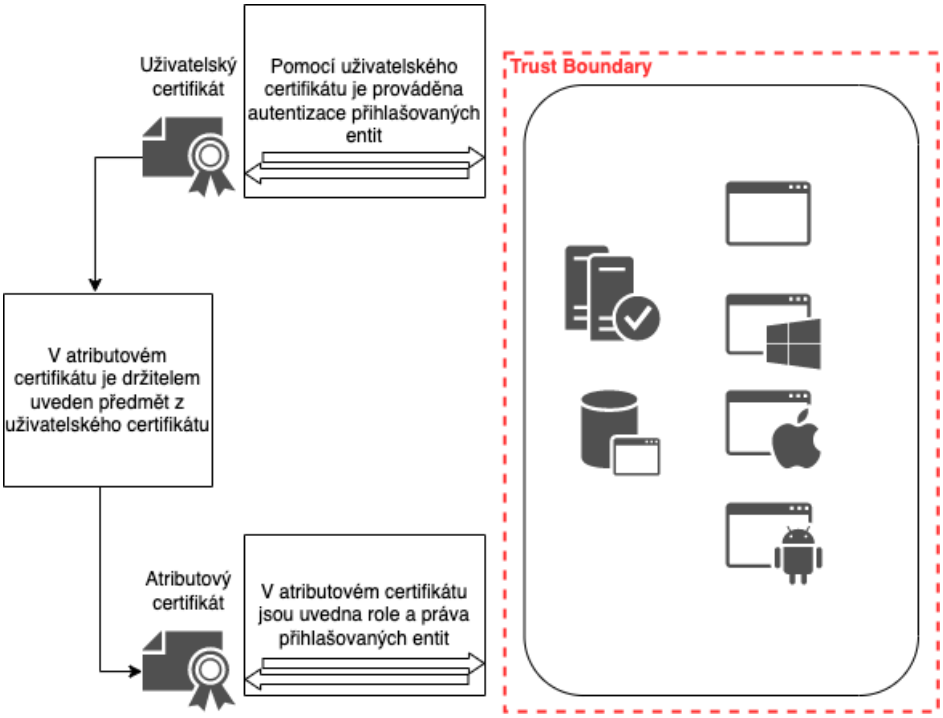


Obrázek 2 Ověření atributového certifikátu

Jak již bylo uvedeno výše, atributový certifikát je úzce spojen s certifikátem veřejného klíče. Může být chápán jako obdoba průkazu zaměstnance, umožňujícího přístup do předem definovaných oblastí. Platnost certifikátu je vydávána zpravidla na kratší časové období (řekněme po setrvávání na určité funkci). Pokud by byly přístupové atributy integrovány do certifikátu veřejného klíče, jakákoliv změna atributu by vyžadovala vydání nového certifikátu. Tento přístup by byl nejen nákladný, ale mohl by způsobit přetížení systému CA. Doporučují se dva způsoby, jakými lze specifikovat držitele atributového certifikátu (AC) v položce držitel (holder) [10]:

- Pomocí položky vydavatel (issuer) a sériového čísla certifikátu (serial number) na certifikátu veřejného klíče,

- Pomocí položky předmět (subject) na certifikátu veřejného klíče. Nevýhodou této volby je, že jiná CA může mít vydán certifikát se stejným předmětem. Naopak výhoda atributového certifikátu, je platnost i při obnovení.



Obrázek 3 Využití atributového certifikátu

1.6.3 Registrační autorita

RA zastává klíčovou roli v ověřování žádostí o certifikáty, které následně předává CA. RA nevytváří ani nevydává certifikáty, ale funguje jako prostředník mezi uživatelem a CA. K plnění svých úkolů shromažďuje RA nezbytné informace a realizuje následující úkoly:

- Přijímá žádosti o certifikáty uživatelů nebo zařízení,
- Provádí ověření a autentizaci uživatelů nebo zařízení,
- Zajišťuje odnětí přístupových oprávnění v případě neplatnosti.

Primárním úkolem RA je zajištění, aby oprávnění uživatelé a zařízení mohli žádat o certifikáty prostřednictvím konkrétních webových stránek nebo aplikací. Po schválení žádosti RA předává požadavek na vydání certifikátu CA [10].

1.6.4 Time Stamp Authority

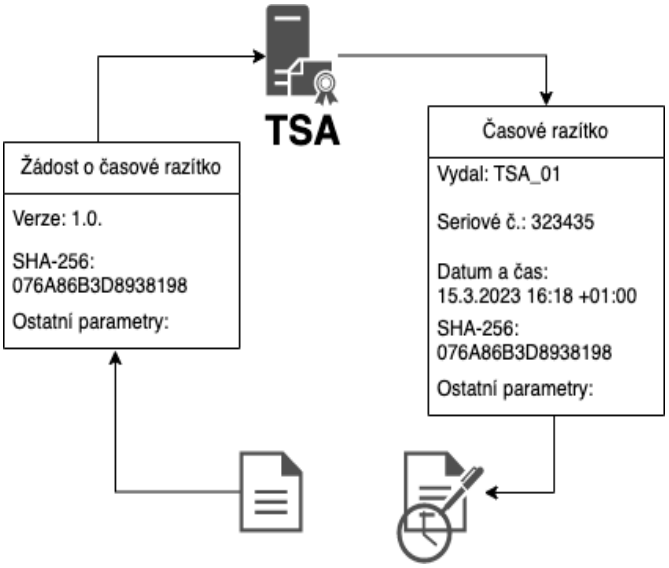
Time Stamp Authority (TSA) je entita, vydávající časová razítka pro digitální dokumenty a další data. Časová razítka jsou důležitá k ověření existence dat v konkrétním časovém

okamžiku. To je nezbytné pro řadu aplikací jako jsou digitální podpisy, elektronické faktury apod.

Funkce TSA spočívá v přijímání požadavků na časové razítko, vytváření časových razítek na základě těchto požadavků a vydávání časových razítek zpět žadatelům.

Při tvorbě časového razítka TSA vytvoří hash daných dat, je přidán aktuální čas minimálně ze dvou ověřených zdrojů času, datum a podepsáno soukromým klíčem TSA. Tím je nezpochybnitelným způsobem zaručena správnost informací uvedených ve vygenerovaném časovém razítku.

Dokument je podepsán TSA (Time Stamping Authority). Postup je zobrazen na obrázku č. 4.



Obrázek 4 Vytvoření časového razítka

Hlavní omezení časového razítka spočívá v tom, že neposkytuje informace o tom, kdo byl držitelem konkrétního dokumentu v daném časovém okamžiku. Tuto mezeru lze vyplnit pomocí certifikátu pro ověření dat (DVC)[15], který může obsahovat položku identifikujícího držitele. Díky tomuto může DVC sloužit jako důkaz o držení daného dokumentu před časovým údajem uvedeným na DVC [10].

1.7 eIDAS

Nařízení Evropské unie č. 910/2014 o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním evropském trhu. Toto nařízení bylo zavedeno pro harmonizaci a posílení důvěry v elektronické transakce mezi členskými státy EU. Nařízení

[15] DVC – Data Validation Certificate.

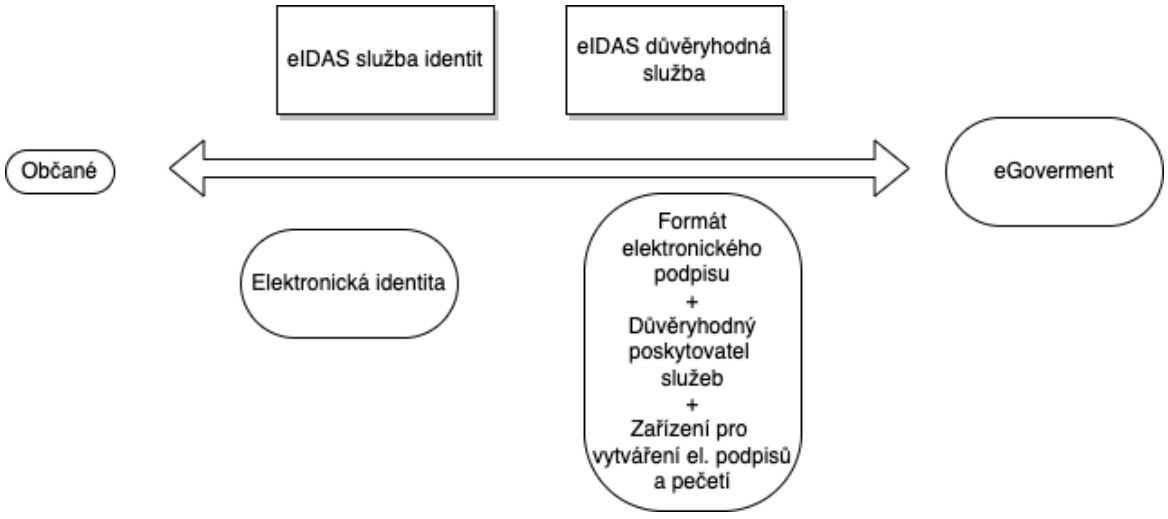
eIDAS stanovuje pravidla a normy pro elektronickou identifikaci, elektronické podpisy, elektronické pečeti, časová razítka, zabezpečené doručování zpráv a certifikační služby.

V současné době digitální a cloudové transformace hraje PKI velmi důležitou roli při vytváření důvěry mezi zúčastněnými subjekty. Za účelem ochrany pravosti a integrity veřejných klíčů je zavedeno mnoho předpisů, prostředků a infrastrukturních zařízení.

PKI je implementováno ve státní správě, eIDAS, různých ziskových i neziskových organizací. Důležité je zajistění bezpečného elektronického podpisu k zajištění integrity a nezpochybnitelnosti dokumentů. Dále pak elektronická identifikace a autentizace pro přístup ke službám eGovermentu [13].

1.7.1 Elektronický podpis

V roce 2014 v EU bylo přijato nařízení eIDAS, které si vzalo za cíl vytvořit důvěru v oblasti elektronických transakcí mezi vládními subjekty v členských státech, organizacemi a jednotlivci. Toto nařízení vstoupilo v platnost v roce 2016. Byla vytvořena pravidla pro elektronickou identifikaci a služby vytvářející důvěru, pro zjednodušení a standardizaci digitálních identifikačních údajů a podpisů v celé EU. eIDAS přineslo mnoho inovací, především nové požadavky na podniky a organizace ve formě NIS 1, NIS 2 [14].



Obrázek 5 eIDAS služby pro identitu i služby vytvářející důvěru

1.7.2 eGovernment

eGoverment představuje koncept, který se vztahuje na použití informačních a komunikačních technologií v poskytování veřejných služeb. Jeho cílem je zlepšit dostupnost a efektivitu těchto služeb pro občany, podniky, vládní organizace a jejich

zaměstnance. eGoverment nabízí široké spektrum online služeb pro občany– např. podávání daní nebo registraci vozidel, ale i podnikatele- např. podávání základních informací o jejich povinnostech a umožňuje kontakt se státem a ostatními podnikateli. Zlepšení vládních operací, jako je správa lidských zdroj, nebo plánování a monitorování projektů.

V rámci eGovernmentu existuje několik způsobů, jak ověřit identitu:

- Státními prostředky:
  - Mobilní klíč eGovernmentu,
  - NIA ID,
  - eObčanka.
- Bankovní identitou.
- Ostatními prostředky:
  - MojeID,
  - První certifikační autorita,
  - IIG.

Použitím těchto prostředků k ověření identity je možné se přihlásit do portálů veřejné správy [15]:

- Portál občana,
- Datová schránka,
- Moje Daně,
- Portál Identity občana,
- ostatní.

Dle hodnocení EU Česká republika vykazuje středně vysokou úroveň penetrace a střední úroveň digitalizace. ČR je zahrnuta mezi země, které jsou stále v procesu digitalizace, ale s vysokým počtem občanů využívajících služby eGovernmentu.

V hodnocení je uvedeno, že ČR je v porovnání se zeměmi s podobným prostředí na dobré cestě v penetraci a že digitalizace je na nedostatečné úrovni [16].

1.8 Adresářové služby

Adresářové služby jsou systémy, které poskytují přístup k atributům spojenými s objekty podle jejich jmen. Tyto služby jsou hierarchické, využívají jmenný kontext a zahrnují uživatele a servery adresářové služby. Služby umožňují jen čtení nebo aktualizaci databáze.

1.8.1 Standard X.500

Standard X.500[16] se zabývá vytvořením globální adresářové struktury, schopné komukoliv přidělit jedinečné jméno (DN – distinguised name). Adresářová struktura začínala úrovní, kde první byla uvedena země (C – Country), dále organizace (O-Organization), organizační jednotka (OU – Organization unit) a na konec jméno držitele (CN – Common Name).

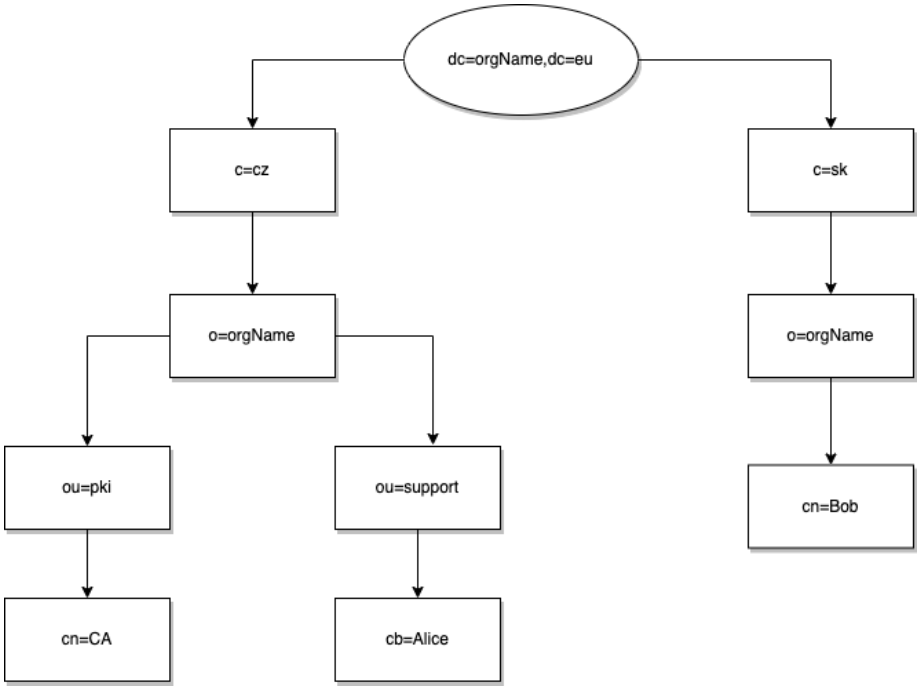
Standard X.509 se stal součástí X.500 a specifikoval formát certifikátů a způsob ověřování podpisů certifikačních autorit v certifikátech. Certifikáty sloužily k zajištění přístupu do globálního adresáře. Dnes je formát X.509 nejběžnější formát certifikátu, který nadále kopíruje strukturu X.500, identifikuje vlastníka certifikátu jedinečným jménem a rozlišuje nadřízené a podřízené certifikační autority [17].

1.8.2 Lightweight Directory Access Protocol

Tento protokol se vyvinul z DAP[17] (Directory Acces Protocol), který byl definován nad protokolem X.500. LDAP[18] je protokolem pro přístup k adresářovým službám, umožňující správu a vyhledávání informací ve struktuře adresářového stromu zobrazena na obrázku č.5.

Tento protokol pro práci s certifikáty používá záznamy typu X.509, uložené v adresářovém stromě. Záznamy obsahují informace o subjektu vlastnícím certifikát, včetně jeho jména a dalších atributů. Informace jsou v hierarchické struktuře organizovány podle rozlišovacího jména DN subjektu. LDAP je využíván v PKI k výměně certifikátů mezi různými subjekty a k ověření platnosti certifikátů. Subjekty mohou v LDAP vyhledávat a získávat certifikáty z adresářového stromu a ověřovat platnost certifikátů při navazování bezpečného spojení. LDAP umožňuje efektivní, centralizovanou správu digitálních certifikátů [18].

[16] Standard X.500 - ISO/IEC 9594, https://www.iso.org/standard/72557.html
[17] DAP – Directory Access Protokol je standard pro počítačové sítě vyhlášený ITU-T a ISO v roce 1988 pro přístup k adresářové službě X.500.
[18] LDAP – Lightweight Directory Access Protocol definovaný protokol pro ukládání a přístup k datům na adresářovém serveru.



Obrázek 5 Struktura adresáře LDAP

2 MOŽNÉ PRAKTICKÉ PROBLÉMY SOUVISEJÍCÍ S PKI

Implementace PKI je komplexní a dlouhodobý proces, který vyžaduje promyšlené rozhodování a důkladnou přípravu. Jakákoliv precipitace v tomto procesu může vést k potencionální kompromitaci bezpečnostního systému. Jedním s častých problémů při implementaci PKI je používání nedostatečně silných klíčů. Délka klíče je kritickým parametrem při výběru kvalifikovaných prostředků, jako jsou například smart cards. Platnost certifikátů je rovněž důležitá proměnná, která by neměla být neúměrně dlouhá. I přes to, že šifrovací metody jako RSA a ECC jsou v současné době efektivní, můžeme očekávat, že budou postupem času zastarávat v důsledku technologického pokroku, zejména v oblasti kvantových počítačů.

Organizace jako je NIST[19] se již zabývají výzkumem a identifikací nových šifrovacích algoritmů, které budou schopny odolat jak kvantovým výpočtům, tak tradičním metodám prolomení šifrování. Toto ukazuje, jak důležité je pro organizace, které implementují PKI, sledovat nejnovější vývoj a inovace v oblasti kryptografie a bezpečnosti informací.

2.1 Komplikace s PKI

PKI je základní komponentou pro zabezpečení digitálních komunikací a transakcí. Nicméně jako u všech technologií i zde existují některé potencionální komplikace při implementaci a provozování.

2.1.1 Cenová náročnost implementace PKI

Náklady spojené s hardwarovou a softwarovou infrastrukturou nezbytnou pro provoz PKI. Toto zahrnuje servery hostující certifikační autority (CA) a další komponenty. Je třeba počítat s náklady na zakoupení a obnovování softwaru pro správu. Kromě tohoto jsou zde náklady spojené s personálem, který bude systém spravovat a podporovat. To zahrnuje nejen platy a benefity, ale také náklady na jejich vzdělávání. Vzhledem k technické složitosti PKI může být nezbytné najmout nebo vyškolit specialisty v oblasti bezpečnosti. Dále je nutné vzít v úvahu náklady na průběžnou správu celého systému, řešení bezpečnostních incidentů nebo výpadků spojených s PKI.

Přestože tyto náklady mohou být vysoké, je důležité si uvědomit, že náklady na odstranění následků nedostatečně zabezpečeného systému mohou být mnohonásobně vyšší.

[19] NIST – National Institute of Standards and Technology

2.1.2 Nedostatečná ochrana klíčů

Správa klíčů je jednou z největších výzev při implementaci a provozování PKI. Tento proces je životně důležitý pro zabezpečení systému. Pro jeho složitost je důležitá jeho velmi důsledná správa.

Vydávání nových klíčů musí být zabezpečeno bezpečným a důvěryhodným procesem, aby se zabránilo jakékoliv kompromitaci již v tomto ranném stádiu.

Dále je důležité řádně spravovat obnovování klíčů. Klíče a certifikáty s omezenou platností musí být pravidelně obnovovány. Pokud není správně implementována správa klíčů a dojde k vypršení jejich platnosti, může to vést k výpadkům v komunikaci nebo, což je ještě horší, mohou být klíče kompromitovány.

V případě kompromitace je bezpodmínečně nutné tyto klíče a certifikáty revokovat. To vyžaduje efektivní a rychlé postupy v detekci bezpečnostních incidentů a reakcích na ně.

Nakonec je důležité zajistit bezpečné uložení klíčů. Soukromé klíče musí být uloženy bezpečně a chráněny před neoprávněným přístupem. To zahrnuje použití Hardware Security Module (HSM)[20].

Případné selhání některého z těchto aspektů správy klíčů může vést ke kompromitaci klíčů a následnému bezpečnostnímu riziku, což může mít vážné důsledky pro organizaci.

2.1.3 Problémy se správou PKI

Účinná správa a provoz PKI vyžaduje dobře definovaný a konzistentní rámec řízení. V případech, kdy takový rámec chybí nebo není jednotně uplatňován, může dojít k nesrovnalostem a potencionálním bezpečnostním rizikům.

Za účelem minimalizace těchto rizik je nezbytné vytvořit a uplatňovat soubor jasně definovaných politik a bezpečnostních směrnic. Tyto dokumenty by měly stanovit standardy a postupy pro všechny aspekty provozu PKI, včetně generování a správy klíčů, vydávání a obnovování certifikátů, zabezpečení a ochrany soukromých klíčů a reakci na bezpečnostní incidenty.

Důsledné dodržování těchto politik a směrnic je nezbytné pro udržení integrity a bezpečnosti PKI. Tím lze nejen předcházet potencionálním škodám, ale také zajistit, že organizace je

[20] HSM – Hardware Security Module je specializovaný kryptografický procesor, speciálně navržen pro ochranu životního cyklu kryptografického klíče.

schopna účinně reagovat na jakékoliv bezpečnostní incidenty nebo výzvy, které mohou nastat v průběhu provozu PKI.

Není možné, aby organizace fungovaly efektivně bez určení pravidel. Nejednotnost je důvodem nesrovnalostí v implementaci PKI. Vytvořením kvalitních politik a bezpečnostních směrnic, které jsou důsledně dodržovány, lze předejít škodám [19].

2.2 Zranitelnosti certifikačních autorit

Jedním z největších možných problémů jsou zranitelnosti. Jako příklad uveďme zranitelnost ROCA (The Return of Coppersmit's Attack) CVE-2017-15361[21] – je to knihovna Infineon RSA 1.02.013 využívána v krypto-čipech ke generování RSA klíčových párů. Využívá algoritmus Fast Prime, problémem nicméně je, že prvočísla nejsou korektně vygenerována. Tím dochází k oslabení generovaných klíčů, které by měly zamezit možnosti odvození privátního klíče [20, 21].

Algoritmická zranitelnost umožňuje faktorizaci klíčů 2048 bitů včetně. Nutnou podmínkou je znalost veřejného klíče, fyzický přístup k zařízení není potřeba. Tato prvočísla mají svou jednoznačnou strukturu, kterou je možno detekovat i v rozsáhlých souborech. Pravděpodobní útočníci si takto mohou snadno určit klíče, na které budou vést útok, a nemusí faktorizovat náhodná prvočísla. Na Amazon AWS c4 lze faktorizovat 1024bitový klíč za 76 $, faktorizace 2048bitového klíče je možná za cca 40000 $.

Toto útočníkovi umožní vydávat se za právoplatného vlastníka soukromého klíče, dešifrovat zprávy, padělat podpisy atd.

Tyto zranitelné klíče byly nalezeny v eIDAS, autentizačních tokenech, TLS/HTTPS, PGP. Je pravděpodobné, že zranitelných klíčů jsou statisíce. Vzhledem k tomu, že byla tato knihovna používána od roku 2012, může jejich počet dosáhnout i miliónů [22].

2.2.1 ROCA (The Return of Coppersmit's Attack)

Zranitelnost ROCA, která byla detekována v lednu 2017 na Slovensku a v Estonsku, spočívala v chybné implementaci RSA klíče v rámci šifrovací knihovny společnosti Infineon Technologies. Tato chyba umožnila útočníkům vypočítat soukromý klíč z veřejného klíče. V uvedených zemích měla tato zranitelnost značný dopad. V Estonsku

[21] CVE-2017-15361 – Knihovna Infineon RSA 1.02.013 ve firmwaru čipu Infineon Trusted Platform Module (TPM), dostupné na https://nvd.nist.gov/vuln/detail/CVE-2017-15361

byly postiženy ID karty vydané mezi říjnem 2014 až říjnem 2017, které pracovaly s chybnou knihovnou společnosti Infineon Technologies. To vedlo k tomu, že estonská vláda musela provést rozsáhlé aktualizace a obnovení ID karet. Na Slovensku zranitelnost ovlivnila eID karty, obsahující chybnou knihovnu. Také zde muselo dojít k aktualizacím a obnovení eID karet. Je zajímavé, jak tyto země přistupovaly k řešení problému.

Slovensko provedlo revokaci certifikátů na přelomu října a listopadu, kdy revokovalo certifikáty vydaných k soukromým klíčům, vygenerovaných krypto-čipem umístěným na kartě využívající chybnou knihovnu. Jednalo se o kvalifikovaný certifikát pro elektronický podpis, certifikát pro elektronický podpis a šifrovací certifikát. Nápravou mělo být vydávání certifikátů ke klíčům o velikosti 3072 bitů, původní plán počítal s vydáváním certifikátů online, pravděpodobně z technických důvodů to nebylo možné, a případní žadatelé o certifikát museli osobně navštívit klientská centra okresních úřadů [23].

Estonsko přistoupilo k revokaci certifikátů podstatně dříve, a to již na konci srpna, a dle mého názoru i zodpovědněji než výše uvedené Slovensko. Důvodem možná bylo to, že Estonsko patří mezi evropské země s největší digitalizací veřejné správy. Téměř okamžitě došlo k znepřístupnění veřejné databáze certifikátů k eID. Z bezpečnostního hlediska byla provedena revokace všech certifikátů [24].

Byla provedena rozsáhlá analýza napadených domén, kterou bylo možné provést pouze pro estonský eID, kvůli adresáři, který byl veřejně dostupný a obsahoval více jak polovinu dokumentů, u kterých byla zjištěna zranitelnost. U vzorků poskytnutých ostatními zeměmi (např. Slovensko) nebylo možné korektně ověřit, zda je zranitelných více dokumentů nebo jen limitovaný počet. Vzhledem k malému množství zranitelných eID, zjištěných v poskytnutém vzorku [24].

Dále se předpokládá, že by touto zranitelností mohly být ovlivněny funkce TPM (Trusted Platform Module)[22] hardwarového kryptografického prvku:

1. Ukládání dešifrovacích a soukromých klíčů,
2. Udržování nedešifrovatelného protokolu aplikací PCR (Platform Configuration Registers),
3. Potvrzování stavu vzdáleného subjektu podpisem PCR.

[22] TPM – Trusted Platform Module.

TPM verze 1.2 pracuje je s RSA s 2048bitovými klíči. Po provedené analýze byl učiněn závěr, že čipy TMP vyrobené před rokem 2013 nejsou touto metodou faktorizovatelné. Předpokládá se, že knihovna Infineon RSA 1.02.013 byla použita v čipu TPM s firmwarem verze 4 a vyšší [25].

2.2.2 Kompromitace certifikačních autorit v EU

Kompromitace PKI ve státní správě se nevyhnula ani jiným evropským zemím. V roce 2011 byla kompromitována CA DigiNotar[23], která vydávala certifikáty doménám nizozemské vlády. SSL certifikáty musely být revokovány. Útok provedla hackerská skupina působící z Íránu. Na webový server vložila škodlivý software, který umožňoval kontrolovat CA a podepisovat vlastní certifikáty pro jakoukoliv doménu. Další incident proběhl ve francouzské CA ANSSI[24] v roce 2013. Útočníci pronikli do sítě CA ANSSI, kde ukradli doménové certifikáty, např. google.com, yahoo.com, skype.com. Útočníci využili malware umožňující vzdálený přístup a mohli tak monitorovat síťový provoz. Získali přístup k privátním klíčům, kterými si podepsaly výše zmíněné domény. CA ANSSI o tomto incidentu informovala měsíce po jeho objevení. Na této CA je názorně ukázáno, že ani velké CA nejsou imunní proti útokům. O rok později v italské CA InfoCert[25], vydávající kvalifikované certifikáty pro el. podpis, získal útočník přístup k privátním klíčům této CA a mohl si podepisovat své certifikáty pro webové stránky, díky čemuž provedl „Man-In-The-Middle“ útok a získal citlivé informace o uživatelích přesměrovaných na jeho falešné stránky. K další kompromitaci, tentokrát estonské CA SK ID Solution, došlo v roce 2016. Tato CA vystavuje certifikáty estonskému e-Governmentu. Občané Estonska mohou díky tomu online volit nebo zakládat firmy. Tato vážná kompromitace certifikátů určených pro el. podpisy a autentizaci byla způsobena chybou kódování, jež umožnila útočníkům vystavit certifikáty s vysokou úrovní důvěryhodnosti. Takto podepsané certifikáty byly použity k podepisování dokumentů a přístupu k citlivým informacím. Tuto kompromitaci objevil estonský tým CERT na konci roku 2017, když bylo odhaleno několik neoprávněně vydaných certifikátů. Z vyšetřování vyplynulo, že tento útok byl velmi sofistikovaný a s velkou pravděpodobností byl veden blíže nespecifikovaným státem. Následně Estonsko zvýšilo bezpečností opatření v rámci celého systému e-Governmentu [26, 27].

[23] DigiNotar – Nizozemská certifikační autorita společnosti VASCO, kterou po kompromitaci, převzala nizozemská vláda provozní řízení systémů DigiNotar.
[24] ANSSI – Agence nationale de la sécurité des systèmes d’information, https://www.ssi.gouv.fr/en/certification/common-criteria-certification/international-agreements/
[25] InfoCert S.p.A. Company Subject to the Management and Coordination of Tinexta S.p.A

2.3 PKI v cloudovém prostředí

PKI hostované v cloudu[26] může nabídnout vyšší úroveň infrastrukturních zdrojů, zabezpečení a odborného know-how, než je tomu v mnoha organizacích. Tato řešené jsou výhodná pro své robustní bezpečnostní politiky, které byly ověřeny skutečným provozem a v dlouhodobém časovém horizontu. V případě útoku na tuto infrastrukturu je třeba obnovit pouze kompromitované systémy. Navíc, umístění PKI v cloudu mimo on-premise[27] infrastrukturu přináší další vrstvu izolace a zabezpečení.

Nicméně je důležité vzít v úvahu možné problémy spojené s integrací on-premise infrastruktury s cloudovým řešením. Synchronizace informačních systémů, které jsou klasifikovány dle § 4 zákona 412/2005 Sb[28]., může být komplikovaná, vzhledem k omezením na provozování těchto systémů na stejné infrastruktuře.

2.3.1 Škálovatelnost a dostupnost

PKI je zásadní pro organizace provozující kritické informační systémy, které vyžadují nepřetržitou dostupnost a schopnost škálovat na tisíce uživatelů a zařízení. Starší implementace PKI, navržené pro omezený počet aplikací, často postrádají podporu pro škálovatelnost a redundanci. I když je například Microsoft CA jednoduchým řešením, nemusí být schopen škálovat tak, aby splnil budoucí požadavky organizace.

Na druhou stranu poskytovatelé cloudových řešení, jako PaaS[29] nebo IaaS[30], disponují hlubokými zkušenostmi a odbornými znalostmi v oblasti škálovatelnosti a standardů. Tito poskytovatelé jsou schopni navrhnout a implementovat PKI, která bude odpovídat aktuálním potřebám organizace a bude připravena na budoucí škálování a rozšíření.

2.3.2 Kontinuita a bezpečnost

Při změně pracovníků, kteří odpovídají za správu PKI, se může zvýšit riziko možných bezpečnostních incidentů. Takové riziko může být způsobeno nepřesnostmi či prodlevami v pravidelných údržbách, automatizaci procesů nebo vydávání certifikátů. Tyto situace

[26] Cloudový hosting je model poskytování infrastruktury pro webové aplikace, webové stránky a další online služby, který využívá cloudové prostředí poskytované poskytovatelem cloudu.
[27] On-premise – provozování vlastní fyzické infrastruktury pro provoz úložišť, zařízení a serverů v prostorách organizace.
[28] Zákon 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, https://www.nbu.cz/cs/pravni-predpisy/1089-zakon-c-4122005/.
[29] PaaS – Platform-as-a-Service.
[30] IaaS – Infrastructure-as-a-Service.

mohou vést k vážným provozním výpadkům, jejichž náprava by větším organizacím zabrala týdny.

Nicméně dobře implementovaná a spravovaná PKI může zajišťovat bezpečné a kontinuální fungování infrastruktury. Důležitým aspektem je zde zavedení standardizovaných postupů pro předávání odpovědnosti, včetně řádného zaškolení nově příchozích pracovníků. Součástí těchto postupů by měla být také revize a aktualizace politik a postupů PKI, aby byly v souladu se současnými bezpečnostními standardy a nejlepšími praxemi.

2.3.3 Automatizace životního cyklu certifikátů

Poskytovatelé PKI jako PaaS mohou efektivně spravovat a automatizovat životní cykly certifikátů a klíčů vydávaných vlastní certifikační autoritou organizace, stejně jako certifikátů certifikačních autorit třetích stran. Automatizace tohoto procesu může výrazně snížit zátěž pracovníků odpovědných za správu PKI a uživatelů certifikátů.

S rostoucí digitalizací a zvyšující se závislosti na bezpečných digitálních transakcích bude role PKI a automatizované správy životního cyklu certifikátů nabývat na významu. Optimalizace spolu s automatizací těchto procesů mohou přinést výhody v oblasti efektivity, bezpečnosti a spolehlivosti digitálních systémů organizace [28, 29].

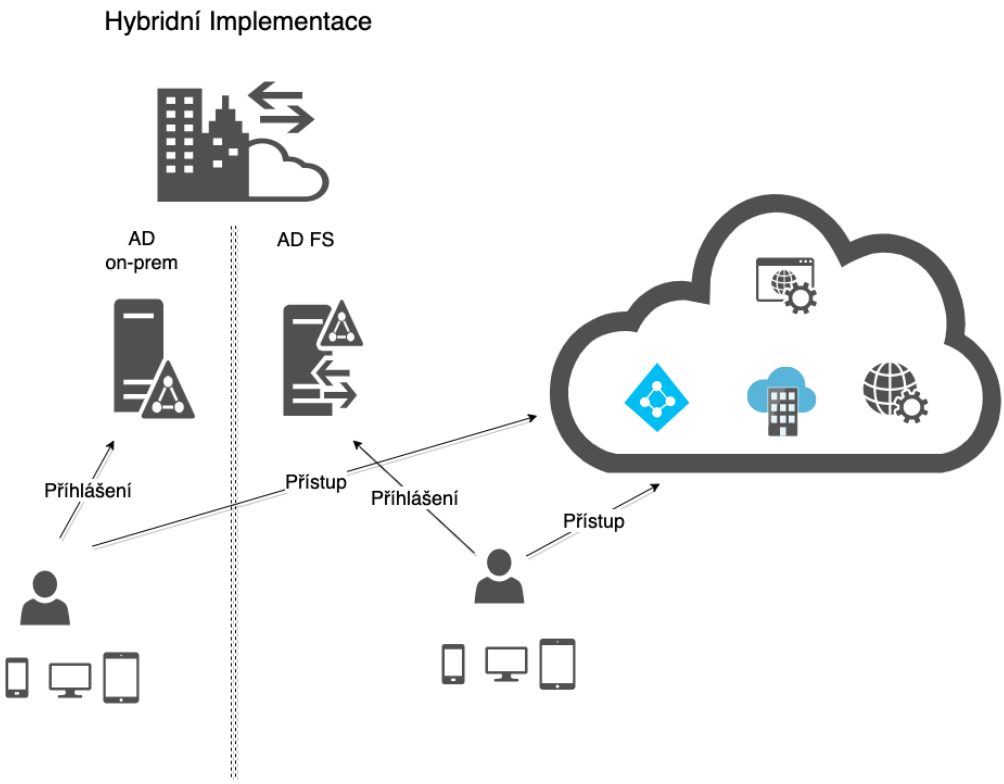
II. PRAKTICKÁ ČÁST

3 NÁVRH IMPLEMENTACE PKI

Tato práce se zabývá implementací PKI v nespecifikované organizaci kritické infrastruktury. Hlavním cílem je navrhnout robustní PKI infrastrukturu, která je schopna efektivně vydávat a spravovat kvalifikované certifikáty na kvalifikovaných prostředcích. Tato infrastruktura by měla zabezpečit integritu, autenticitu a důvěrnost komunikace a transakcí v rámci organizace, přičemž by měla být dostatečně škálovatelná pro budoucí potřeby.

3.1 Struktura organizace

V rámci této studie je přijat hybridní model implementace. Interní systémy a infrastruktura jsou spravovány v rámci on-premise infrastruktury organizace, zatímco další služby jsou provozovány prostřednictvím cloudové platformy Microsoft Azure. Tento model kombinuje výhody obou přístupů on-premise a cloud, umožňuje organizaci efektivně využívat vlastní zdroje a zároveň využívat škálovatelnost, flexibilitu a další výhody, které nabízí cloudové řešení. [30]



Obrázek 6 Hybridní implementace – cloud, on-premise

3.1.1 Předávání požadavků mezi AD DS a AD FS.

Při pokusu uživatele o přihlášení do aplikace nebo služby, je požadavek předán do AD FS[31]. Dále je tento požadavek předán do AD DS, pro autentizaci. Jakmile je uživatel ověřen, AD FS vydá bezpečnostní token, který reprezentuje totožnost a přihlašovací stav uživatele, může obsahovat i další atributy, popisující uživatele nebo jeho práva. Uživatel nebo aplikace použijí tento token k přístupu k aplikaci nebo službě (viz Obr 6). [30]

3.2 Struktura CA

Tříúrovňová hierarchie certifikační autority umožňuje efektivní správu certifikátů a klíčů v rozsáhlé infrastruktuře a zvyšuje bezpečnost systému tím, že izoluje kořenovou CA od přímého kontaktu s koncovými entitami.

Tříúrovňová struktura CA:

a) Kořenová CA (úroveň 1):
    a. vydává kořenové certifikáty pro zprostředkující CA, s platností 10 let,
    b. provozována na stand-alone počítači,
    c. soukromé klíče uchovávány na HSM.
b) Zprostředkující CA (úroveň 2):
    a. vydává certifikáty vydávajícím CA s platností 5 let,
    b. provozována na stand-alone počítači,
    c. soukromé klíče uchovávány na HSM dle (FIPS-140 Level 3).
c) CA vydávající klientské certifikáty (úroveň 3):
    a. kvalifikované certifikáty pro elektronický podpis,
    b. certifikáty určené k autentizaci,
    c. serverové certifikáty.
d) CA vydávající atributové certifikáty (úroveň 3):
    a. uživatelské atributové certifikáty.
e) TSA (úroveň 3):
    a. podepisování dokumentů,
    b. zřízení dostatečného množství TSU (Time Stamp Unit).

[31] AD FS – Active Directory Federated Services

Celá struktura CA je strategicky rozdělena na interní a veřejnou část. Toto oddělení bylo navrženo s cílem posílit bezpečnost interních systémů organizace. Řízení přístupů je realizováno podle principů Zero Trust Access, což přispívá k další vrstvě ochrany.

Interní část:

- Vydává kvalifikované certifikáty na kvalifikovaných prostředcích. Sloužící k autentizaci a podepisování elektronických dokumentů.
- Vydávat CRL[32] seznamy a provozovat OCSP[33] servery.
- Vydávat technologické certifikáty pro zařízení (servery atd.)

Veřejná část:

- Primárně bude používána k vydávání kvalifikovaných certifikátů pro externí zaměstnance a obchodní partnery organizace.
- Vydávat CRL seznamy a provozovat OCSP servery.

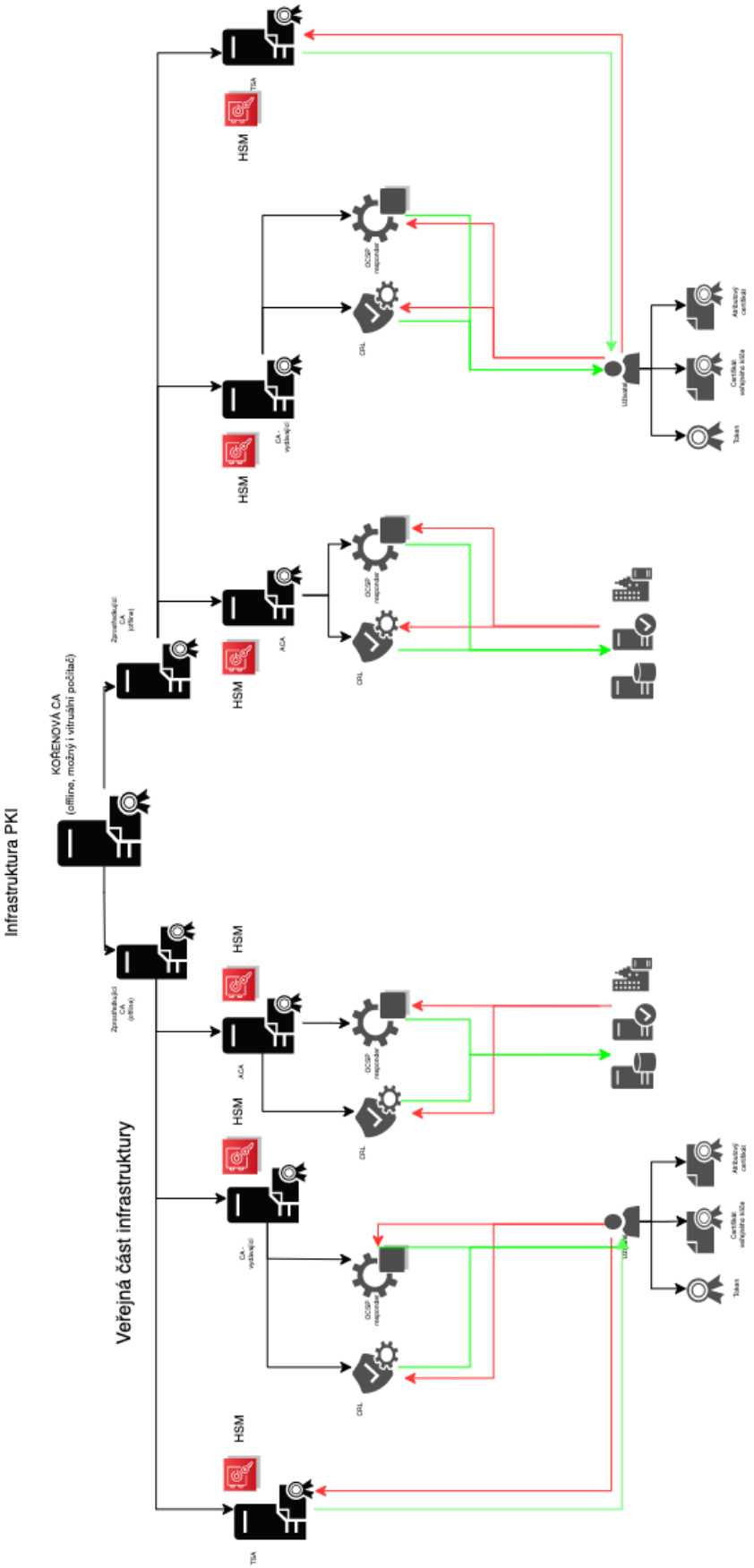
Každá ze zprostředkujících CA provozuje tři CA.

- CA vydávající uživatelské certifikáty,
- CA vydávající atributové certifikáty,
- TSA vydávání časových razítek.

Každá CA ve struktuře organizace bude uchovávat všechny své privátní klíče na HSM. Pro zvýšení bezpečnosti při správě klíčů v jejich životním cyklu. HSM splňuje FIPS-140-3[34].

Dále budou zřízeny záložní CA pro udržení běhu celé infrastruktury PKI k zachování schopnosti online kontroly certifikátů a možnosti používání TSA. Na obrázku č. 10 je customizovaný návrh implementace CA v organizaci. Od běžných řešení se odlišuje rozdílnou strukturou, která je rozdělena na interní a veřejnou část.

[32] CRL – Certificate Revocation List
[33] OCSP – Online Certificate Status Protokol
[34] FIPS-140-3 - Security Requirements for Cryptographic Modules



Obrázek 7 Infrastruktura PKI v dané instituci

Interní RA budou zřízeny na osobních odděleních organizace. Externí RA bude realizovaná na určeném kontaktním místě organizace.

Uživatelé obdrží kvalifikované prostředky, kterými bude zabezpečen fyzický vstup do organizace a jimiž se budou autentizovat, podepisovat dokumenty a přistupovat do Informačních systémů organizace. Vlastní autentizace bude prováděna pomocí multifaktorové autentizace (multi-factor authentication-MFA).

Pro správu koncových bodů je implementován Microsoft Endpoint Manager.

4 POPIS IMPLEMENTACE PKI

V této části práce jsou popsány klíčové prvky implementace PKI v organizaci. Organizace využívá cloudovou službu IaaS (Infrastructure as a Service). Toto řešení vede ke snížení nákladů a nároků na správu lokálních datových center s přístupem k datům v reálném čase. IaaS nabízí pružnost ve zvyšování či snižování IT zdrojů podle aktuálních potřeb organizace.

Cloudový poskytovatel služeb Azure, zajišťuje správu infrastruktury. Organizace spravuje instalace, konfigurace a správu softwaru [31].

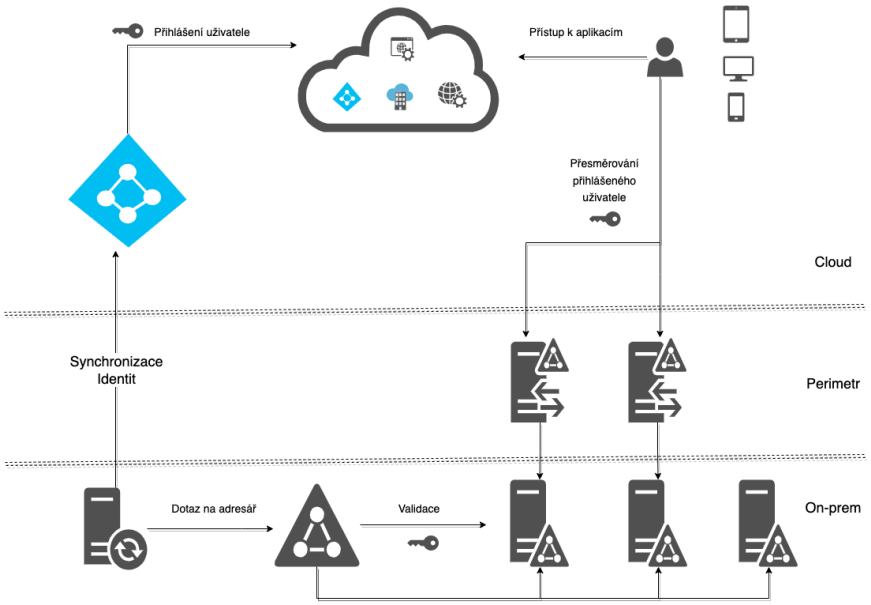
4.1 Struktura organizace a služeb

Identity uživatelů jsou spravovány v místním AD DS[35] a používány pro ověřování uživatelů, kteří se přihlašují ke cloudovým službám. Jedny přihlašovací údaje jsou používány pro přístup jak k místním, tak k cloudovým prostředkům, čímž je proces přihlašování pro uživatele zjednodušen.

Azure AD Connect je nástroj, který zajišťuje synchronizaci účtů mezi místní AD DS a Azure AD[36] (Azure Active Directory). Na lokálním serveru AD DS sleduje změny v účtech a předává je do Azure AD, čímž je zajištěna konzistence účtů a identit napříč oběma prostředími (viz Obr. 11).

V rámci federovaného ověřování je požadováno použití čipových karet. Tento přístup zvyšuje bezpečnost ověřování uživatelů a představuje další úroveň ochrany proti neoprávněnému přístupu. Čipové karty poskytují silnější zabezpečení prostřednictvím dvoufaktorové autentizace. Tímto způsobem je zajištěno, že pouze oprávnění uživatelé mohou přistupovat k citlivým prostředkům a datům.

[35] AD DS – Active Directory Domain Services.
[36] Azure AD – Azure Active Directory.



Obrázek 8 Hybridní identita s federativním ověřováním

4.2 Implementace CA

Software EJBCA[37] byl zvolen jako back-end CA, místo klasické Microsoft CA. Jedním z důvodů bylo snížení organizační náročnosti správy certifikátů. EJBCA bude jediná instance v organizaci, napříč všemi doménami, trees, forrest. Díky tomuto řešení nemusí být v organizaci provozovány Microsoft CA v každé doméně (viz Obr. 12) [32].

4.2.1 Kořenová CA

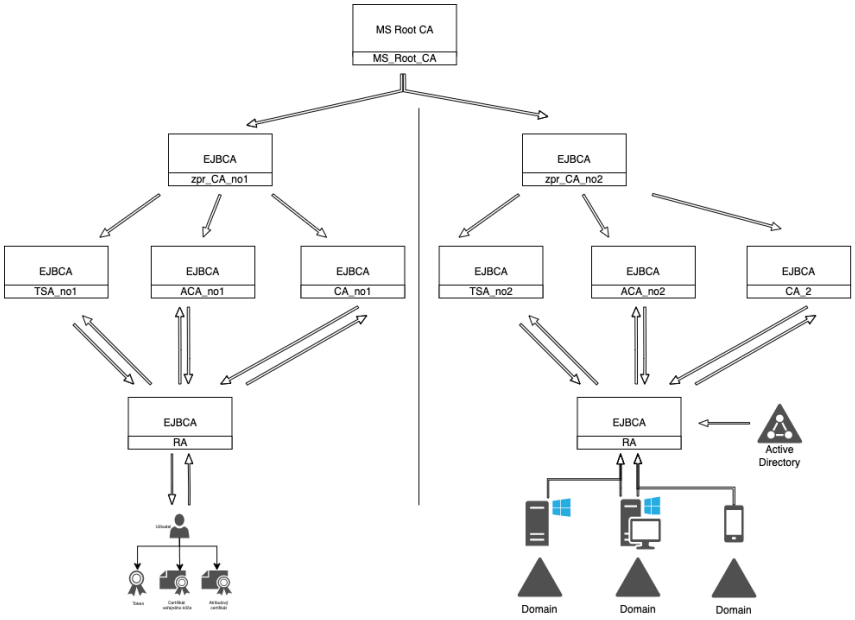
Je základní důvěryhodná kotva v hierarchii PKI (Public Key Infrastructure) organizace. V této organizaci je implementována Microsoft Root CA, která není připojena k Active Directory. Úkolem MS_root_CA je vydávat certifikáty pro tyto certifikační autority zpr_CA_no1 a zpr_CA_no2.

K integrování externích EJBCA do MS_root_CA musí být splněny následující požadavky:

1. Zpr_CA_no1 a zpr_CA_no2 musí být nakonfigurovany jako externí CA v EJBCA, s vygenerovanými žádostmi o podepsání certifikátu (CSR).
2. Microsoft Server 2019 s certifikačními službami nakonfigurovaný jako Microsoft Root CA.

[37] EJBCA – Enterprise Java Beans Certificate Authority, https://doc.primekey.com/.

3. CRL Distribution Point (CDP) na samostatném serveru, protože kořenová CA bude v off-line režimu.
4. Služba OCSP nebude realizována z důvodu off-line režimu.



Obrázek 9 Struktura CA v organizaci

4.2.2 Zprostředkující CA

Zprostředkující CA je nakonfigurována jako externí CA v EJBCA. Tento typ nastavení umožňuje oddělení úrovní důvěry a zodpovědnosti mezi kořenovou CA a vydávající CA. Díky rozdělení na víceúrovňovou hierarchii je zvýšena bezpečnost celého systému.

Zprostředkující CA má podepsaný certifikát od kořenové CA, spolu s řetězcem certifikátů kořenové CA ve formátu PKCS7 (soubory P7B nebo P7C). Tento řetězec certifikátů zajišťuje důvěru v certifikáty vydávané zprostředkující CA, protože mohou být ověřeny až k původní kořenové CA.

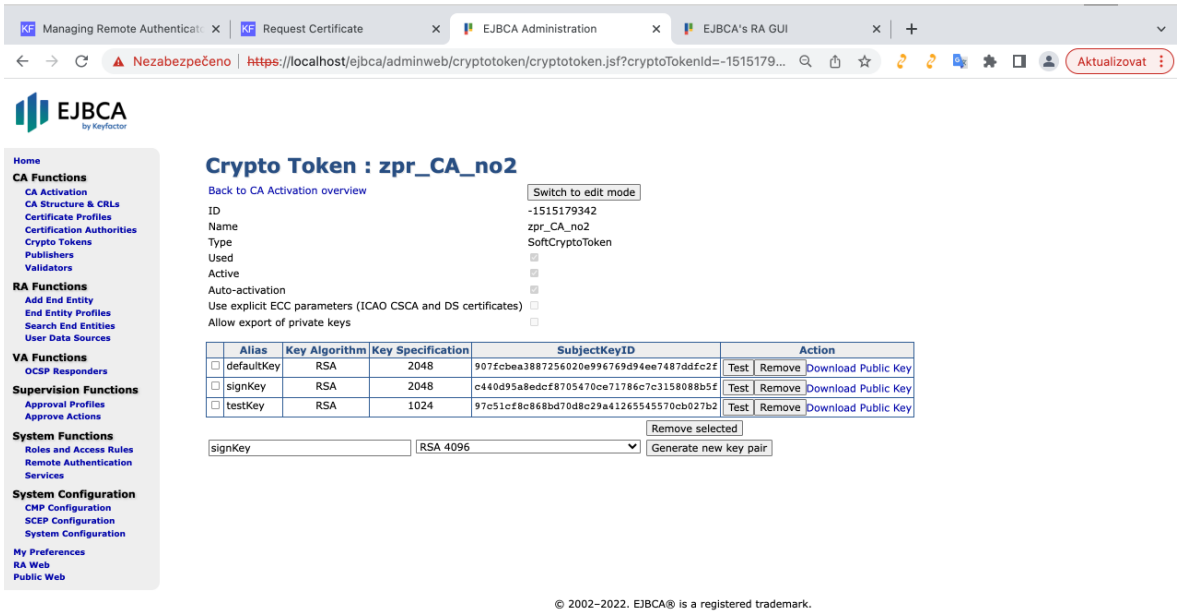
Vydávané CDP[38] a AIA OCSP[39] jsou provozovány na samostatném serveru. CDP je mechanismus umožňující distribuci seznamů zneplatněných certifikátů (Certification Revocation List – CRL). AIA OCSP je protokol poskytující informace o stavu platnosti certifikátu prostřednictvím OCSP (Online Certificate Status Protocol) služeb.

[38] CDP – CRL Distribution Point
[39] AIA OCSP – Authority Information Access Online Certificate Status Protocol

Zprostředkující CA podepisuje certifikáty pro vydávající CA, která vydává certifikáty pro koncové subjekty, jimiž jsou servery, klienti nebo aplikace.

4.2.3 Vydávající CA interní části organizace

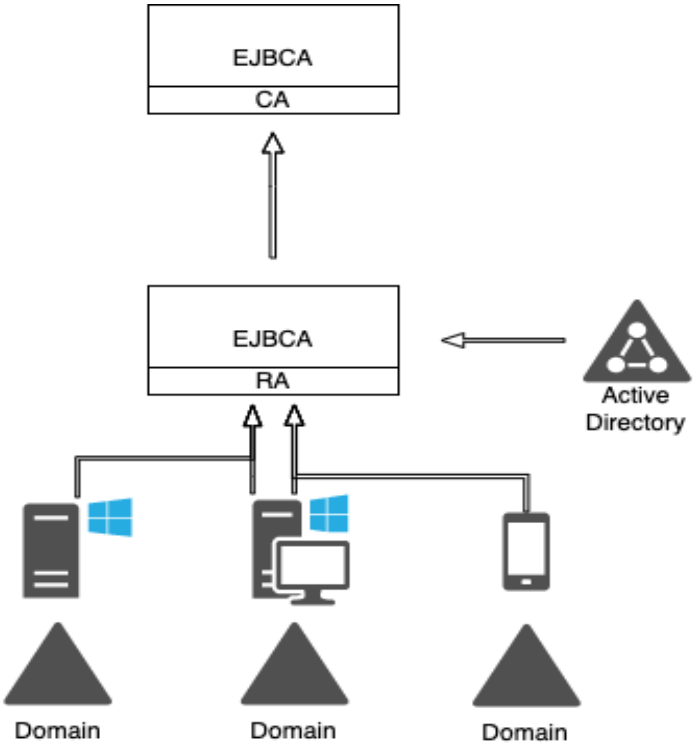
Integrace CA_no2 s AD DS je provedeno pomocí protokolu LDAP, který je podporován jak u CA_no2, tak AD DS. Tímto způsobem může CA_no2 komunikovat s AD DS, a získávat tak potřebné informace o uživatelích a skupinách v AD DS. Automatizace procesů vydávání certifikátů umožní vydávání certifikátů pro uživatele a počítače v AD DS.



Obrázek 10 Webové rozhraní CA v EJBCA

Hlavní funkce vydávající CA:

1. Vydávání certifikátů – generuje a vydává certifikáty koncovým entitám na základě žádostí o certifikáty CSR (Certificate Signing Request).
2. Ověřování identity – Před vydáním certifikátu CA ověří totožnost žadatele. Tento proces zahrnuje různé úrovně ověření podle typu certifikátu.
3. Správa životního cyklu certifikátu: zodpovídá za správu celého životního cyklu certifikátů, včetně jejich vydávání, obnovení, pozastavení a zrušení.
4. Vydávání CRL – pravidelně aktualizuje a publikuje seznam zrušených certifikátů.
5. Podpora OCSP – CA provozuje server s podporou OCSP, umožňující ověření stavu certifikátů v reálném čase.

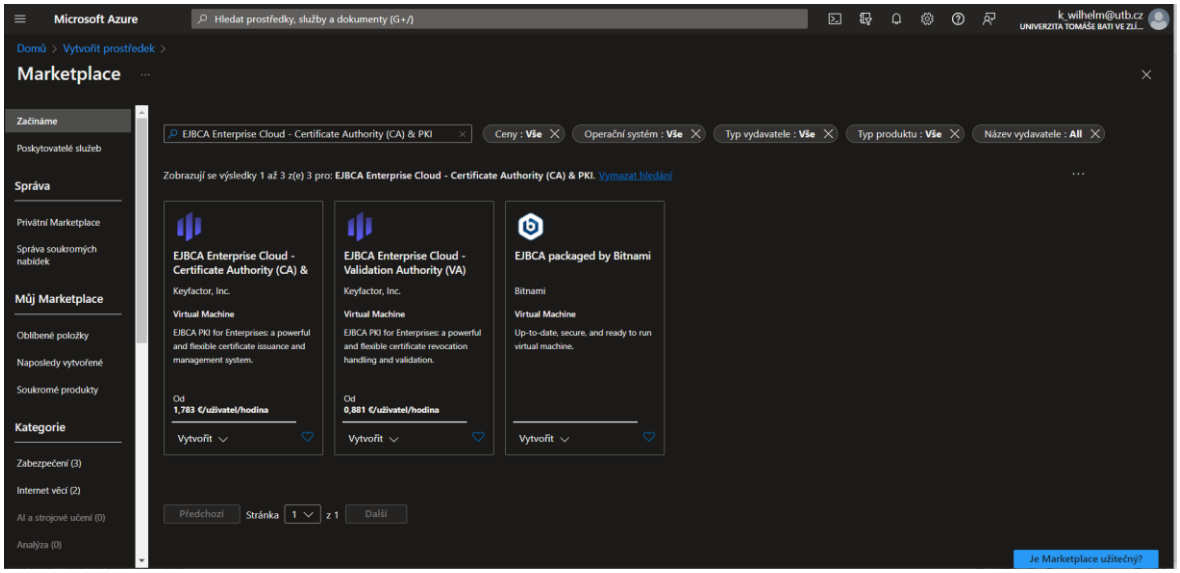


Obrázek 11 Struktura vydávající CA 1

4.2.4 Vydávající CA veřejné části organizace

Pro integraci CA_no1 s Azure AD je třeba provést několik kroků. Zaregistrovat CA_no1 jako aplikaci v Azure AD. V Azure portálu zaregistrovat CA_no1 jako novou aplikaci, aby bylo možné vytvořit propojení mezi CA_no1 a Azure AD. Nakonfigurovat Azure AD pro CA_no1. V Azure AD nastavit potřebné oprávnění pro CA_no1, čtení uživatelských profilů a správu certifikátů. Nastavit synchronizaci uživatelů a skupin. Provést konfiguraci Azure AD Connect pro synchronizaci uživatelů a skupin mezi místním Active Directory a Azure AD.

Vzhledem k nedostatku prostředků a uživatelských práv realizace EJBCA v rámci Microsoft Azure nebyla provedena. Doplňující obrázky byly použity z referenční příručky.



Obrázek 12 EJBCA v MS Azure

4.2.5 Registrační autorita

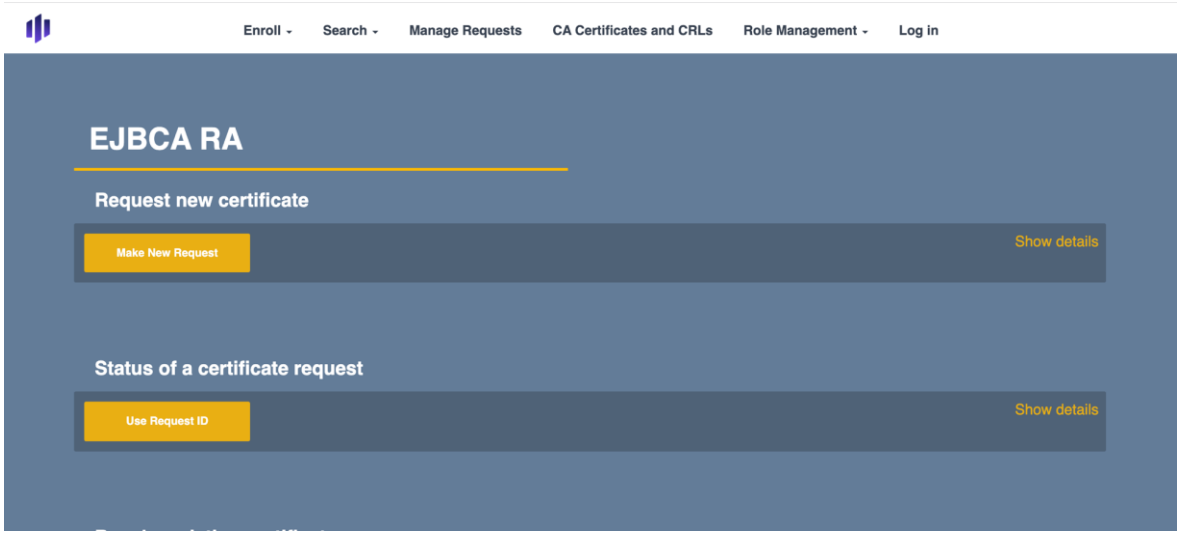
Registrační autorita, je vybavena grafickým uživatelským rozhraním, které je navrženo, aby umožnilo komplexní správu veškerých operací spojených s koncovými entitami a administrátory RA. Tento nástroj zajišťuje plynulý chod celého životního cyklu certifikátů. Od generování klíčů, podepisování CSR[40], až po úpravy konfigurace koncových entit pro budoucí registrace. Pro ověřování v rámci organizace je využíván systém založený na certifikátech.

Správa požadavků se skládá z následujících částí:

1. To Approve (Ke schválení) – Administrátor může schválit nebo zamítnout zobrazené požadavky na certifikáty.
2. Pending Approval (Čeká na schválení) – Nevyřízené žádosti, ke kterým má administrátor přístup a může je schválit.
3. Processed (Zpracováno) – V této části jsou zobrazeny dříve podané žádosti o certifikáty.
4. Custom Search (Vlastní vyhledávání) – Umožňuje administrátorům provádět vlastní vyhledávání certifikátů podle zadaných kritérií.

Na obrázku č. 14 je zobrazení webového rozhraní RA [33].

[40] CSR – Certificate Signing Request

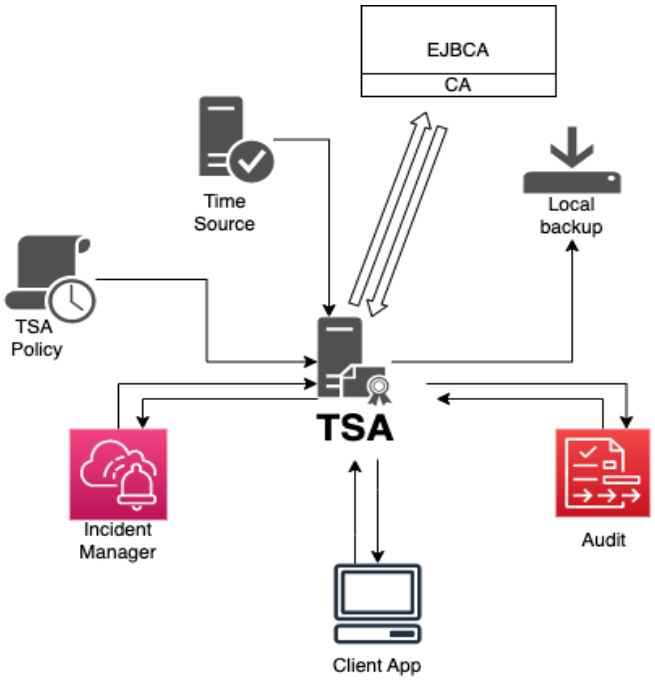


Obrázek 13 Webové rozhraní RA v EJBCA

4.2.6 TSA interní části organizace

Struktura a jednotlivé funkční části jsou zobrazeny na obr. č. 16:

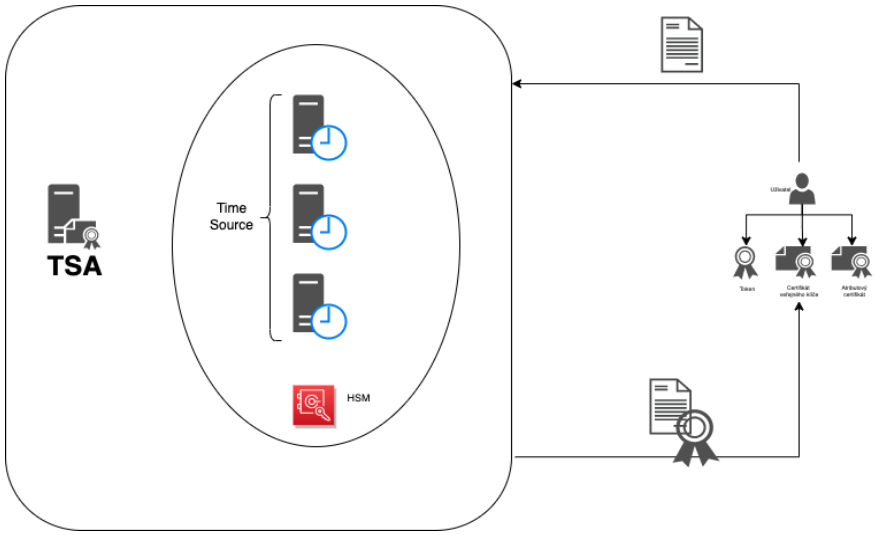
- Time Stamping Server – Centrální server zpracovávající žádosti o časová razítka od uživatelů a generuje časová razítka. Tento server je chráněn a zabezpečen proti neoprávněnému přístupu.
- Time Source – Spolehlivý zdroj času, NTP server, synchronizovaný se standardními časovými servery.
- TSA Policy – Soubor pravidel a postupů, který stanovuje zásady pro vydávání časových razítek.
- Certifikáty pro TSA podepsané vydávající CA, která ověřuje identitu a zajišťuje důvěru ve svá časová razítka.
- Archivace a zálohování – Zálohováním a archivací záznamů o časových razítkách, které zajišťují dlouhodobou dostupnost a integritu dat.
- Audit a kontrola – Pravidelné kontroly a audity pro ověření souladu s TSA Policy a zajištění důvěryhodnosti časových razítek.
- Řízení incidentů a nápravná opatření – Identifikace, řešení a prevence bezpečnostních incidentů a narušení.



Obrázek 14 Struktura TSA

Průběh podepisování dokumentů znázorněn na obr. č. 17:

1. Uživatel odešle žádost o časové razítko na TSA. V žádost obsahuje hash dokumentu.
2. TSA přijme a ověří platnost žádosti. Poté získá aktuální čas ze spolehlivých zdrojů času, které spojí s hash dokumentu. Tuto kombinaci zašifruje pomocí svého soukromého klíče. Výsledkem je časové razítko.
3. TSA odešle časové razítko uživateli.
4. V případě potřeby ověření dokumentu s tímto časovým razítkem, třetí strana použije veřejný klíč TSA k dešifrování razítka.



Obrázek 15 TSA průběh podepisování

.

4.2.7 TSA veřejné části organizace

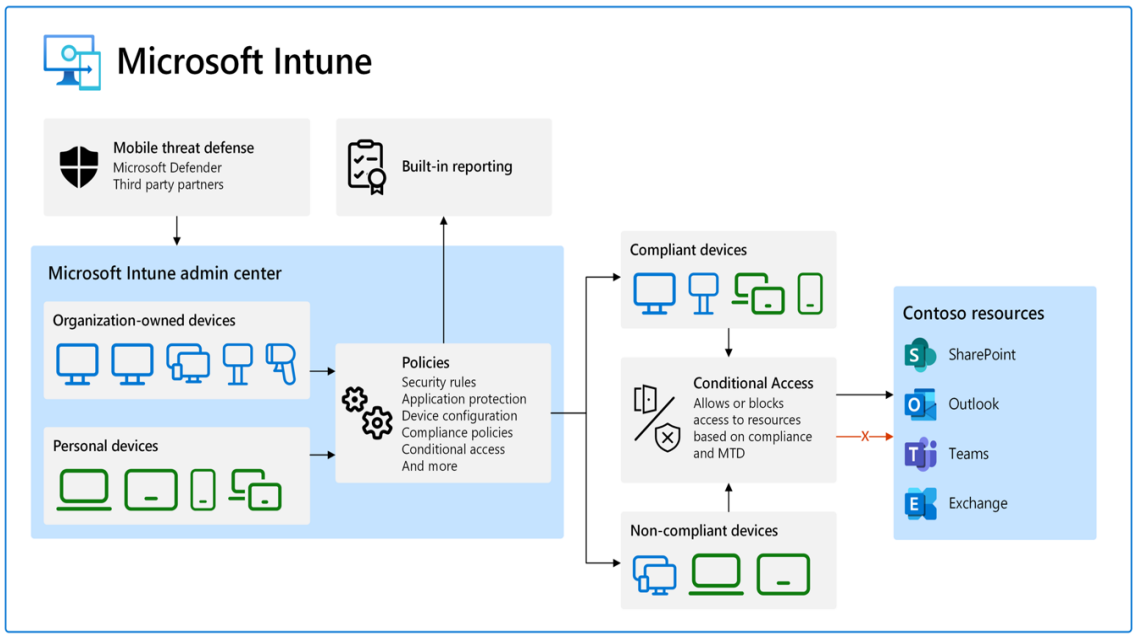
Nastavení TSA_no1 je provedeno tak, aby využíval Azure AD jako zdroj autentizace. Aktivujeme SSO[41], aby bylo uživatelům umožněno využít své přihlašovací údaje Azure AD pro přístup k TSA_no1. Konfigurace TSA_no1 bude zahrnovat generování certifikátu TSA a konfiguraci TSA parametrů.

4.2.8 Microsoft Endpoint Manager

Je integrovaná platforma pro správu koncových bodů v organizaci. Zde je implementováno cloudové řešení Microsoft Intune. Tato cloudová služba se zaměřuje na správu MDM[42]. Byla

[41] SSO – Single Sign-On
[42] MDM – Mobile Device Managment

zvolena z důvodu jednodušší architektury oproti SCCM[43] a také, že nevyžaduje k provozu lokální infrastrukturu. Díky této implementaci je zabezpečeno bezpečné pracovní prostředí. Řízení používání zařízení spolu s návrhem zásad přístupu k zařízením organizace, ale i BYOD[44]. Data organizace jsou oddělena od osobních dat zaměstnanců s BYOD. Intune zajistí splnění požadavků vyžadovaných organizací [34].

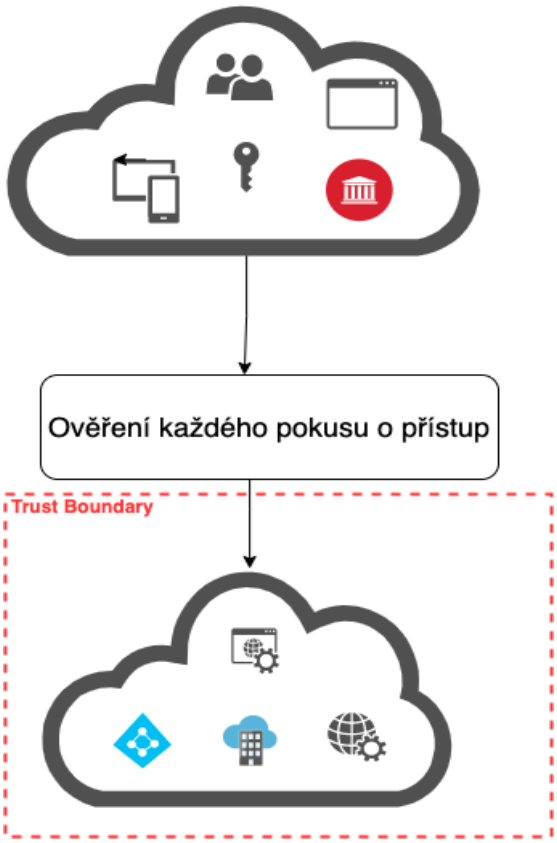


Obrázek 16 Microsoft Intune devices. [34]

Podmíněný přístup je implementován pomocí bezpečnostní politiky, která stanovuje pravidla a podmínky pro přístup ke zdrojům a službám. V případě potřeby je možné tuto politiku přizpůsobit novým požadavkům organizace. Díky podmíněnému přístupu je vynucováno dodržování bezpečnostních zásad, čímž je zajištěna ochrana prostředků organizace.

V případě nesplnění podmínek stanovených v bezpečnostní politice bude odepřen přístup ke všem prostředkům organizace. Tím je zajištěno, že pouze oprávněné osoby mají přístup k citlivým datům a službám. Zásady podmíněného přístupu jsou vynucovány po ověření prvního faktoru. Tím je minimalizováno riziko neoprávněného přístupu [35].

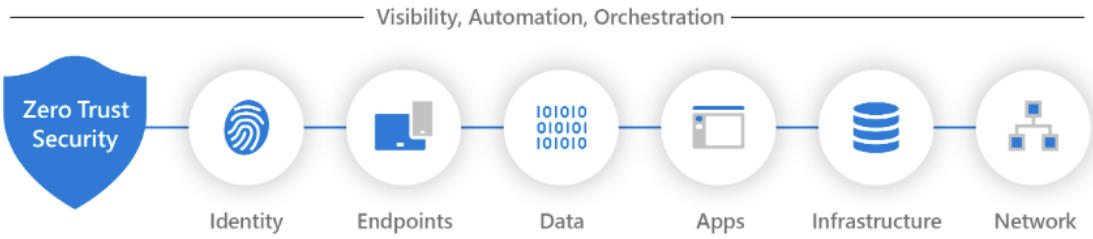
[43] SCCM – System Center Configuration Manager
[44] BYOD – Bring Your Own Device



Obrázek 17 Podmíněný přístup.

4.2.9 Zero Trust

Organizace implementovala ucelenou strategii zahrnující Zero Trust do svých základních prvků. Tato strategie předpokládá, že žádný uživatel, zařízení nebo aplikace nemají automatickou důvěru.



Obrázek 18 Základní prvky Zero Trust [36]

Je vyžadováno, aby byli před získáním přístupu ke zdrojům jednoznačně identifikováni a ověřeni všichni uživatelé, zařízení i aplikace. Průběžné ověřování během celého životního cyklu přístupu ke zdrojům zahrnuje pravidelné sledování a monitorování chování uživatelů a zařízení. Důvodem je rychlá identifikace potenciálních hrozeb a reakce na ně. V rámci této politiky je omezen přístup pouze na zdroje, které jsou nezbytné pro jejich úkoly.

Je vyžadována ochrana dat na všech úrovních. To zahrnuje šifrování dat při ukládání, přenosu i zabezpečení samotných aplikací [36].

Azure Storage

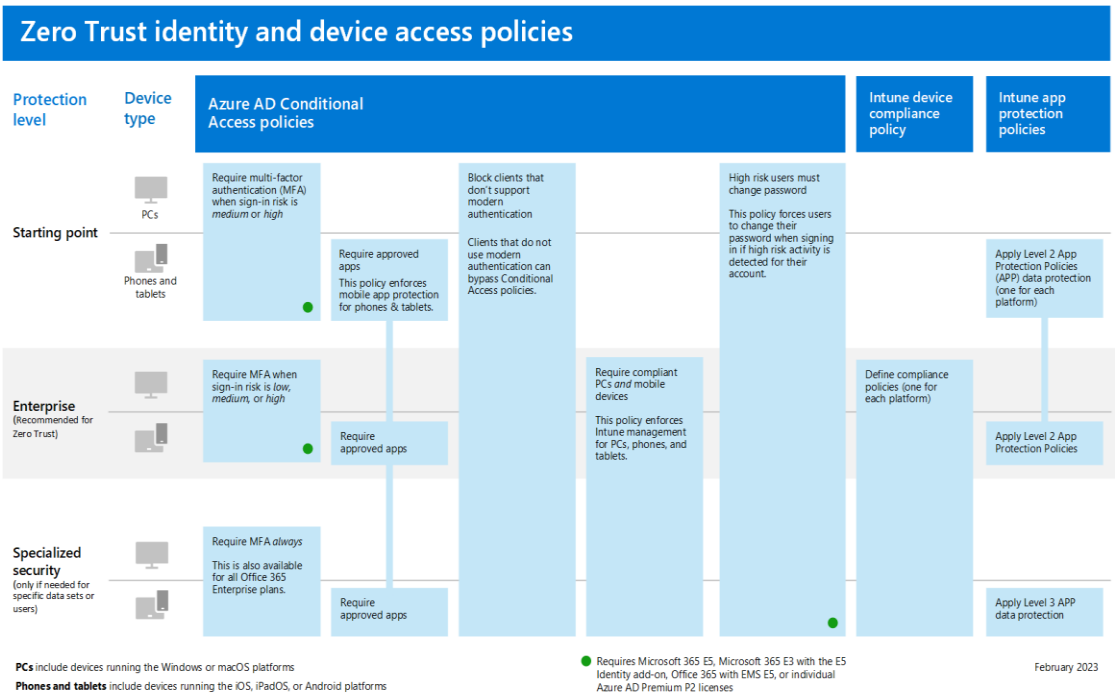
Šifrování přenosu mezi klientem a Azure je postaveno na protokolu HTTPS pro šifrovanou komunikaci mezi uživateli a cloudovými službami. Požadavky pocházející z nezabezpečených připojení jsou bezpodmínečně odmítnuty. Anonymní přístup ke kontejnerům je v Azure zakázán z bezpečnostních důvodů.

K šifrování jsou použity technologie Azure Storage Service Encryption (SSE) s Azure Disk Encryption (ADE), které automaticky šifrují data při ukládání a dešifrují je pouze pro oprávněné uživatele při přístupu [30].

Virtuální počítače

Připojování do systému bude prováděno na základě rolí definovaných v Azure AD s řízením identit a oprávnění. Díky tomuto bude možné přidělovat uživatelům přístup na základě jejich rolí a zodpovědností v organizaci.

Podnikové zásady typu ENTERPRISE – prvky, které vynucují dodržování předpisů týkajících se zařízení a zabezpečení. Zde jsou zahrnuta nastavení pro správu zařízení, šifrování dat, řízení přístupu, sledování hrozeb a další bezpečnostní opatření. V nezbytných případech dojde ke zpřísnění podnikových zásad na typ SPECIALIZED SECURITY – pro zvýšení ochrany určitých datových sad a uživatelů bude uplatněno specializované zabezpečení, zahrnující multifaktorové ověřování a kombinující několik metod ověřování uživatele, konkrétně hesla, tokeny, biometrické údaje a potvrzení prostřednictvím SMS. Administrátoři upraví bezpečnostní politiku na základě různých faktorů, jako je geolokace, typ zařízení, stav zabezpečení zařízení, nebo úrovně rizika uživatele (viz Obrázek č. 15). [36]



Obrázek 19 Virtuální počítač přístupová politika [36].

Celá PKI infrastruktura organizace bude v souladu se směrnicemi kybernetické bezpečnosti Evropské unie. V roce 2023 nabyla účinnost směrnice Evropského parlamentu a Rady (EU) 2022/2555[45] o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii (NIS2). Tato směrnice je navazující na směrnici NIS, kde rozšiřuje kategorie subjektů a stanovuje podrobnější pravidla. Proto bude nutné provést kompletní revizi a doplnění bezpečnostních a organizačních politik. Termín splnění požadavků na podmínek směrnice NIS2 je k 17. říjnu 2024. Nesplnění podmínek této směrnice podmíněni finanční penalizací. Dále se organizace týká také směrnice 2022/2557[46]o odolnosti kritických subjektů. Tato směrnice navazuje na NIS2, hlavně co se týče sdílení informací o kybernetický hrozbách, kybernetických incidentech a bezpečnostních rizicích. Tato náročná opatření budou časově i finančně bezpochyby náročné. Na druhou stranu přínosem vzhledem k množství sdílených informací týkající se výše uvedeného. Lze předpokládat, že vyžadování směrnice NIS2 bude opatřeno i přechodným obdobím kdy bude prováděno vzdělávání a celková osvěta dotčených organizací a zaměstnanců. Pro tuto činnost zřídil NÚKIB[47] informační portál informující širokou veřejnost o této problematice. Je třeba si uvědomit co pro organizaci tato směrnice bude znamenat pro řídící orgány, kteří mít určené povinnosti a osobní zodpovědnost. Bude vyžadováno aby dohlížely na opatření v oblasti kybernetické bezpečnost, schvalovali je a

[45] Zdroj: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32022L2555
[46] Zdroj: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32022L2557
[47] NÚKIB – Národní úřad pro kybernetickou a infomační bezpečnost

samozřejmně byly v této oblasti dostatečně proškoleni. Za porušování těchto povinností mohou být sankcionováni, případně dočasně zdaveni řídících funkcí [37, 38].

ZÁVĚR

Implementace infrastruktury veřejných klíčů (PKI) je komplexní proces, který zahrnuje řadu legislativních, technických a finančních hledisek. Přestože technická implementace není neřešitelným problémem díky dostupným nástrojům, jako jsou OpenSSL, EJBCA a další, pro organizace je mnohem náročnější splnit veškeré legislativní a právní požadavky, které se týkají ochrany dat, soukromí a bezpečnosti.

V rámci legislativního a právního prostředí je třeba řešit problematiku shody s příslušnými zákony a nařízeními, jako je například GDPR v Evropské unii. Součástí tohoto procesu může být také koordinace s regulačními orgány a zajištění potřebných povolení či akreditací.

Finanční aspekt projektu zahrnuje nejen náklady na pořízení a provoz technického vybavení a infrastruktury, ale také náklady na školení zaměstnanců, správu a údržbu PKI a také platby za služby třetích stran, pokud je to nezbytné. Při plánování rozpočtu je důležité vzít v úvahu dlouhodobé náklady spojené s provozem a udržitelností projektu, jako jsou například aktualizace a obnova certifikátů, nákup nového hardwaru či softwaru, a také potřebné personální zdroje.

V případě rozsáhlých organizací, které vydávají velké množství certifikátů, může být vlastní certifikační autorita (CA) efektivním řešením, které snižuje náklady a zároveň zlepšuje kontrolu nad procesem vydávání a správy certifikátů. Nicméně při hledání optimálního řešení je důležité zvážit všechny související náklady, a to včetně těch spojených s časovými razítky a serverovými certifikáty

Při návrhu PKI pro takto rozsáhlou organizaci je tedy nezbytné provést důkladnou analýzu, která zohledňuje technické, legislativní a finanční požadavky. To zahrnuje pečlivý výběr poskytovatelů certifikátů, zhodnocení dostupných technologií a nástrojů a také stanovení optimálního rozpočtu a plánování zdrojů. Součástí tohoto procesu by mělo být také posouzení rizik a potenciálních hrozeb spojených s implementací PKI, jako jsou například útoky na infrastrukturu, zneužití certifikátů nebo ztráta klíčů.

Je důležité také zvážit možnosti outsourcingu některých částí PKI, jako je provoz vlastní certifikační autority nebo zajištění časových razítek. Tímto způsobem může organizace využít odborné znalosti a zkušenosti externích poskytovatelů, čímž sníží zatížení vlastního personálu a zdrojů. Nicméně při outsourcingu je třeba dbát na důkladnou kontrolu bezpečnosti a shody s legislativou ze strany externích dodavatelů.

Při vývoji PKI by měla organizace také zvážit zavedení robustních politik a postupů pro správu certifikátů a klíčů, které zajistí transparentnost a důvěru v systém. To zahrnuje řádné ověřování žadatelů o certifikáty, pravidelné kontroly a revize certifikátů a správné postupy pro revokaci a obnovu certifikátů.

Důležitým aspektem úspěšného nasazení PKI je také školení zaměstnanců a šíření povědomí o bezpečnostních rizicích a postupech spojených s použitím certifikátů a klíčů. Organizace by měla zajistit, že všichni zaměstnanci jsou seznámeni s důležitostí PKI pro ochranu dat a soukromí a že jsou schopni správně používat certifikáty a klíče.

V neposlední řadě by organizace měla zvážit možnost zavedení monitorovacích a auditních nástrojů, které umožní sledování a kontrolu celého životního cyklu certifikátů a klíčů. Tyto nástroje mohou pomoci identifikovat potenciální problémy a rizika včas a zajistit, že PKI splňuje požadavky na bezpečnost a shodu s legislativou.

Závěrem lze říci, že implementace PKI v rozsáhlé organizaci je náročný úkol, který vyžaduje pečlivé plánování a koordinaci technických, legislativních a finančních aspektů. Nicméně správně navržená a implementovaná PKI může přinést řadu výhod, jako je zvýšená bezpečnost, zlepšení ochrany dat a soukromí či efektivnější kontrola a správa vydávání certifikátů.

Aby bylo možné dosáhnout úspěšného nasazení PKI, je důležité provést následující kroky:

1. Důkladná analýza potřeb organizace a požadavků na PKI, včetně zhodnocení technických, legislativních a finančních aspektů.
2. Výběr vhodných technologií, nástrojů a poskytovatelů certifikátů, které nejlépe vyhovují potřebám organizace a zohledňují rozpočet a dostupné zdroje.
3. Zavedení robustních politik a postupů pro správu certifikátů a klíčů, které zajistí transparentnost, důvěru a bezpečnost v rámci PKI.
4. Školení zaměstnanců a šíření povědomí o bezpečnostních rizicích a postupech spojených s použitím certifikátů a klíčů.
5. Implementace monitorovacích a auditních nástrojů, které umožní sledování a kontrolu celého životního cyklu certifikátů a klíčů a zajistí shodu s legislativou a bezpečnostními požadavky.

V průběhu celého procesu je důležité průběžně komunikovat se všemi zúčastněnými stranami, včetně IT oddělení, právního týmu, vedení organizace a zaměstnanců, aby bylo možné řešit případné problémy a otázky včas.

Úspěšná implementace PKI v rozsáhlé organizaci může přinést řadu výhod a zlepšení v oblasti bezpečnosti a ochrany dat a pokud je správně navržena a řízena, může se stát klíčovým prvkem v celkové strategii kybernetické bezpečnosti organizace.

SEZNAM POUŽITÉ LITERATURY

[1] FIPS PUB 46-3. *DATA ENCRYPTION STANDARD (DES)*. 3rd ed. USA: NIST, 1999. Dostupné také z: https://csrc.nist.gov/CSRC/media/Publications/fips/46/3/archive/1999-10-25/documents/fips46-3.pdf

[2] BURDA, Karel. *Aplikovaná kryptografie*. Brno: VUTIUM, 2020. ISBN 978-80-2144-612-0.

[3] OULEHLA, Milan a Roman JAŠEK. *Moderní kryptografie*. Praha: IFP Publishing, 2017. ISBN 978-80-87383-67-4. Dostupné také z: https://www.palmknihy.cz/kniha/moderni-kryptografie-241457

[4] *New RSA factoring challenge solved* [online]. 2019 [cit. 2023-05-08]. Dostupné z: https://www.johndcook.com/blog/2019/12/03/new-rsa-factoring/

[5] MATĚJÍČEK, Jaroslav. *Generátory náhodných čísel pro kryptografii* [online]. Brno, 2012 [cit. 2023-05-08]. Dostupné z: http://hdl.handle.net/11012/53662. Diplomová práce. Vysoké učení technické v Brně. Fakulta informačních technologií. Ústav inteligentních systémů. Vedoucí práce Petr Hanáček.

[6] *Moderní kryptografické metody* [online]. Praha, 2019 [cit. 2023-05-08]. Dostupné z: https://is.ambis.cz/th/x039y/BP_Bilokon_Mariia.pdf. Bakalářská práce. Vysoká škola regionálního rozvoje a Bankovní institut – AMBIS. Vedoucí práce Vladimír Beneš.

[7] *ADVANCED ENCRYPTION STANDARD (AES)*. USA: NIST, 2001. Dostupné také z: https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf

[8] ZELENKA, Josef, Jan ČAPEK, Jiří FRANCEK a Hana JANÁKOVÁ. *Ochrana dat. Kryptologie*. Hradec Králové: GRADEAMUS Univerzity Hradec Králové, 2003. ISBN 80-7041-737-4.

[9] *NESSIE PROJECT ANNOUNCES FINAL SELECTION OF CRYPTO ALGORITHMS* [online]. 2003, 3 [cit. 2023-05-08]. Dostupné z: https://web.archive.org/web/20070628104548/https://www.cosic.esat.kuleuven.be/nessie/deliverables/press_release_feb27.pdf

[10] DOSTÁLEK, Libor, Marta VOHNOUTOVÁ a Miroslav KNOTEK. *Velký průvodce infrastrukturou PKI*. 2. dopl. vyd. Brno: Computer Press, 2015. ISBN 978-80-251-4513-5. Dostupné také z: https://www.palmknihy.cz/ekniha/velky-pruvodce-infrastrukturou-pki-

170207?utm_source=DK&utm_medium=web&utm_campaign=buy_palmknihy_ebook_detail

[11] *TSL ČR* [online]. Praha: Ministerstvo vnitra ČR, 2023 [cit. 2023-05-08]. Dostupné z: https://tsl.gov.cz/tsl_cr.html

[12] *Digital Signature Service (DSS)* [online]. EU: European Commission, 2023 [cit. 2023-05-08]. Dostupné z: https://ec.europa.eu/digital-building-blocks/DSS/webapp-demo/home

[13] *eIDAS, služby vytvářející důvěru a elektronická identifikace* [online]. 2023 [cit. 2023-05-19]. Dostupné z: https://www.mvcr.cz/clanek/eidas-sluzby-vytvarejici-duveru-a-elektronicka-identifikace.aspx

[14] *L 257*. In: . EU: EU, 2014, ročník 2014, číslo 57. ISSN 1977-0626. Dostupné také z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2014:257:FULL&from=P

[15] Identita občana. *Identita občana* [online]. Praha: gov.cz, 2023 [cit. 2023-05-08]. Dostupné z: https://portal.gov.cz/rozcestniky/RZC-104

[16] EGovernment Benchmark 2022 Insight Report. In: *CAPGEMINI* [online]. Milano: CAPGEMINI, 2022, 2022 [cit. 2023-05-08]. Dostupné z: https://prod.ucwe.capgemini.com/wp-content/uploads/2022/07/eGovernment-benchmark-2022-1.-Insight-Report.pdf

[17] ISO/IEC 9594-8:2020. *Information technology — Open systems interconnection — Part 8: The Directory: Public-key and attribute certificate frameworks*. 2020.

[18] BUCHMANN, Johannes A., Evangelos KARATSIOLIS a Alexander WIESMAIER. *Introduction to Public Key Infrastructures*. London: Springer, 2013. ISBN 978-3-642-40656-0.

[19] Top 5 Public Key Infrastructure (PKI) Pitfalls and How to Overcome Them. In: *Top 5 Public Key Infrastructure (PKI) Pitfalls and How to Overcome Them* [online]. 2021, 2021 [cit. 2023-05-08]. Dostupné z: https://www.spiceworks.com/it-security/security-general/guest-article/top-5-public-key-infrastructure-pki-pitfalls-and-how-to-overcome-them/

[20] CVE-2017-15361. *CVE* [online]. 2017 [cit. 2023-05-08]. Dostupné z: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-15361

[21] Infineon RSA library does not properly generate RSA key pairs. *Software Engineering Institute* [online].2017[cit.2023-05-8].Dostupné z: https://www.kb.cert.org/vuls/id/307015

[22] ROCA: Vulnerable RSA generation (CVE-2017-15361). In: *Centre for Research on Cryptography and Security* [online]. 2017 [cit. 2023-05-08]. Dostupné z: https://crocs.fi.muni.cz/public/papers/rsa_ccs17

[23] *Certifikáty na eID budú revokované dnes, osobne sa dajú získať 3072-bitové. Na diaľku nie* [online]. In:. 2017 [cit. 2023-05-08]. Dostupné z: http://www.dsl.sk/article.php?article=20391

[24] Zranitelnost ROCA: co se děje se slovenskými a estonskými e-občankami?. In: *Lupa.cz* [online]. 2017 [cit. 2023-05-08]. Dostupné z: https://www.lupa.cz/clanky/zranitelnost-roca-co-se-deje-se-slovenskymi-a-estonskymi-e-obcankami/

[25] The Return of Coppersmith's A□ack: Practical Factorization of Widely Used RSA Moduli. In: *CCS 2017 - Accepted Papers* [online]. 2017 [cit. 2023-05-08]. Dostupné z: https://acmccs.github.io/papers/p1631-nemecA.pdf

[26] Kauza DigiNotar, aneb: když certifikační autorita ztratí důvěru. In: *Lupa.cz* [online]. 2011, 2011 [cit. 2023-05-19]. Dostupné z: https://www.lupa.cz/clanky/kauza-diginotar-aneb-kdyz-certifikacni-autorita-ztrati-duveru/

[27] Za podvrženými certifikáty pro domény Googlu jsou Francouzi. In: *Lupa.cz* [online]. 2013 [cit. 2023-05-19]. Dostupné z: https://www.lupa.cz/clanky/za-podvrzenymi-certifikaty-pro-domeny-google-je-francouzska-autorita/

[28] Top 5 Public Key Infrastructure (PKI) Pitfalls and How to Overcome Them. In: *Top 5 Public Key Infrastructure (PKI) Pitfalls and How to Overcome Them* [online]. 2021, 2021 [cit. 2023-05-08]. Dostupné z: https://www.spiceworks.com/it-security/security-general/guest-article/top-5-public-key-infrastructure-pki-pitfalls-and-how-to-overcome-them/

[29] 5 Reasons Organizations are Moving PKI to the Cloud. In: *5 Reasons Organizations are Moving PKI to the Cloud* [online]. 2019 [cit. 2023-05-08]. Dostupné z: https://www.spiceworks.com/tech/cloud/guest-article/5-reasons-organizations-are-moving-pki-to-the-cloud/

[30] *Azure Architecture Center* [online]. 2023 [cit. 2023-05-19]. Dostupné z: https://learn.microsoft.com/cs-cz/azure/architecture/

[31] Co je IaaS?: Infrastruktura jako služba. *Co je IaaS?* [online]. Microsoft, 2023 [cit. 2023-05-08]. Dostupné z: https://azure.microsoft.com/cs-cz/resources/cloud-computing-dictionary/what-is-iaas

[32] *Primekey/ejbca-ce* [online]. 2023 [cit. 2023-05-19]. Dostupné z: https://hub.docker.com/r/primekey/ejbca-ce

[33] RA Operations Guide. *EJBCA Documentation* [online]. 2023 [cit. 2023-05-08]. Dostupné z: https://doc.primekey.com/ejbca/ejbca-operations/ejbca-operations-guide/ra-operations-guide

[34] Správa identit uživatelů a skupin v Microsoft Intune. *Dokumentace ke správě koncových bodů* [online]. Microsoft, 2023 [cit. 2023-05-08]. Dostupné z: https://learn.microsoft.com/cs-cz/mem/intune/fundamentals/manage-identities

[35] Co je podmíněný přístup? *Dokumentace k Azure Active Directory* [online]. Microsoft, 2023 [cit. 2023-05-08]. Dostupné z: https://learn.microsoft.com/cs-cz/azure/active-directory/conditional-access/overview

[36] Co je nulová důvěra (Zero Trust)?. *Dokumentace zabezpečení* [online]. Microsoft, 2023 [cit. 2023-05-08]. Dostupné z: https://learn.microsoft.com/cs-cz/security/zero-trust/zero-trust-overview

[37] Použití principů nulová důvěra (Zero Trust) na virtuální počítače v Azure. *Dokumentace zabezpečení* [online]. Microsoft, 2023 [cit. 2023-05-08]. Dostupné z: https://learn.microsoft.com/cs-cz/security/zero-trust/azure-infrastructure-virtual-machines

[38] *Nová směrnice EU o kybernetické bezpečnosti „NIS2“* [online]. 2023 [cit. 2023-05-19]. Dostupné z: https://osveta.nukib.cz/course/view.php?id=145

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

PKI	Public Key Infrastructure
DES	Data Encryption Standard
AES	Advance Encryption Standard
RSA	Rivers Shamir Adelman
IF	Integer Factorization
PRNGs	Pseudo-Random Number Generators
TRNGs	True-Random Number Generators
ECDSA	Elliptic Curve Signature Algorithm
ECC	Eliptic Curve Cryptography
NIST	National Institute of Standards and Technology
NESSIE	New European Schemes for Signatures, Integrity and Encryption
CA	Certifikační autorita
CRL	Certificate Revocation List
OCSP	Online Certificate Status Protocol
ACA	Atributová certifikační autorita
RA	Registrační certifikační autorita
TSA	Time Stamp Authority
PMI	Privileg Managment Infrastructure
DVC	Data Validation Certificate
DAP	Data Access Protocol
LDAP	Lightwieght Directory Access Protocol
HSM	Hardware Security Module
ROCA	The Return of Coppersmit's Attack
TPM	Trusted Platform Module
PaaS	Platform-as-a-Service

IaaS	Infrastructure-as-a-Service
AD DS	Active Directory Domain Services
AD FS	Active Directory Federated Services
TSU	Time Stamp Unit
MFA	Multi-factor Autentication
Azure AD	Azure Active Directory
EJBCA	Enterprise Java Beans Certificate Authority
CDP	CRL Distribution Point
AIA OCSP	Authority Information Access Protocol Online Certificate Status Protocol
CSR	Certificate Signing Request
SSO	Single Sign-On
MDM	Mobile Device Managment
SCCM	Systém Center Configuration Manager
BYOD	Bring Your Own Device
SSE	Storage Service Encryption
ADE	Azure Disk Encryption

NÚKIB NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOSTSEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH