Зборник радова Факултета техничких наука, Нови Сад

УДК: 4.4
ДОИ: https://doi.org/10.24867/35BE29Unkovic

Управљање сертификатима у модерним индустријским системима

Certificate Management in Modern Industrial Systems

Јелена Унковић, *Факултет техничких наука, Нови Сад*

Студијски програм – ПРИМЕЊЕНО СОФТВЕРСКО ИНЖЕЊЕРСТВО

Кратак садржај – *Овај рад обрађује концепт управљања дигиталним сертификатима у индустријским системима, са фокусом на хибридна рјешења која комбинују локалну и cloud инфраструктуру. Кроз теоријске основе, архитектуре, аутоматизацију и мониторинг, приказује се како се сертификатима може ефикасно управљати у сложеним техничким окружењима. Студија случаја производне фабрике и имплементација система за управљање сертификатима илуструју практичну примјену концепта. Као закључак, рад доноси свеобухватну анализу предности хибридног приступа у погледу безбједности и оперативности.*

Кључне ријечи: *дигитални сертификати, хибридно рјешење, cloud, on-premise, SCADA*

Abstract – *This thesis explores the concept of digital certificate management in industrial systems, with a focus on hybrid solutions that combine on-premises and cloud infrastructure. Through theoretical foundations, architectural models, automation, and monitoring, it demonstrates how certificates can be efficiently managed in complex technical environments. A case study of a metal processing factory and the implementation of a custom Certificate Management solution illustrate the practical application of the concept. In conclusion, the thesis provides an analysis of the security and operational advantages of the hybrid approach.*

Keywords: *digital certificates, hybrid solution, cloud, on-premise, SCADA*

НАПОМЕНА: Овај рад проистекао је из мастер рада чији ментор је био др Бојан Јелачић, доцент

1. УВОД

Индустријски контролни системи (*Industrial Control Systems – ICS*), укључујући систем за надзор и прикупљање података (*Supervisory Control and Data Acquisition - SCADA*) и савремену индустријску мрежу паметних уређаја (*Industrial Internet of Things - IIoT*), представљају основу модерне производње и инфраструктуре. Са све већом повезаношћу *ICS* система са мрежама информационих технологија (*Information Technology - IT*) и интернетом расту и сајбер ризици. За разлику од класичне *IT* безбједности, *ICS* нагласак ставља на доступност и интегритет, док застарјела опрема и дуг животни циклус отежавају примјену савремених механизама. Традиционални локални модели (*on-premise*) нуде контролу, али су ограничени у скалабилности, док рјешења у рачунарском облаку (*cloud*) доносе аутоматизацију уз изазове усклађености. Хибридни приступ, који комбинује локалну инфраструктуру и *cloud* сервисе, намеће се као оптимално рјешење. Циљ рада је приказати савремене приступе управљању дигиталним сертификатима (*certificate management*) у индустријским системима, са фокусом на хибридна рјешења и практичну имплементацију у погону за обраду метала.

2. ТЕОРИЈСКЕ ОСНОВЕ

2.1 Дигитални сертификати

Дигитални сертификати су кључни механизам за заштиту комуникације и интегритет података у дигиталном окружењу. Њихова основна улога је аутентикација идентитета, обезбјеђивање интегритета путем дигиталних потписа и повјерљивости кроз енкрипцију. У индустријским системима користе се за аутентикацију уређаја, контролу приступа *SCADA* и човјек-машина интерфејсима (*Human-Machine Interface - HMI*), као и за потписивање софтвера. Најчешће се примјењује формат *X.509* [1], који дефинише кључне елементе сертификата [2].

2.2 Компоненте *PKI* система

Инфраструктура јавног кључа (*Public Key Infrastructure – PKI*) омогућава безбједну размјену информација коришћењем асиметричне криптографије, повезујући јавни кључ са идентитетом субјекта путем дигиталног сертификата који издаје поуздано сертификационо тијело (*Certificate Authority – CA*). *PKI* обезбјеђује аутентикацију, енкрипцију и дигитално потписивање, а *CA* има кључну улогу у верификацији идентитета, издавању сертификата и управљању њиховим животним циклусом. Како број сертификата расте, користи се хијерархијска структура са главним (*root*) и подређеним (*subordinate*) *CA*, уз механизме провјере валидности као што је протокол за провјеру статуса сертификата (*Online Certificate Status Protocol – OCSP*) или путем листе опозваних сертификата (*Certificate Revocation List – CRL*) [3].

2.3 Типови сертификата

Дигитални сертификати се класификују према намјени и нивоу повјерења, а најчешће категорије су сервер сертификати за безбједну комуникацију путем протокола *Transport Layer Security / Secure Sockets Layer (TLS/SSL)*, клијентски сертификати за аутентикацију корисника и уређаја, сертификати за потписивање кода (*code-signing*), те сертификати за потписивање и енкрипцију електронске поште (*e-mail*) [4]. Ове врсте сертификата обезбјеђују аутентикацију, интегритет и повјерљивост комуникације, као и заштиту од неауторизованих измјена софтвера и напада посредника („*man-in-the-middle*“).

2.4 Рок трајања, обнављање и опозив сертификата

Рок трајања дигиталног сертификата дефинише временски период у којем је сертификат важећи. Кратки рок повећава безбједност, али захтијева аутоматизацију процеса обнављања путем система за управљање животним циклусом сертификата (*Certificate Lifecycle Management – CLM*). У случају компромитације или промјене статуса, сертификати се опозивају коришћењем механизама *CRL* и *OCSP* за провјеру валидности у реалном времену [5].

2.5 Регулаторни захтјеви

Управљање дигиталним сертификатима у индустријским окружењима мора бити усклађено са регулаторним оквирима који дефинишу техничке стандарде и процесе безбједности. Кључне регулативе укључују директиву за критичну инфраструктуру *(Network and Information Security Directive 2 – NIS2*), за информациону безбједност (*International Organization for Standardization / International Electrotechnical Commission 27001 – ISO/IEC 27001*), за индустријску аутоматизацију (*International Electrotechnical Commission 62443 – IEC 62443*) и за безбједну обраду података (*General Data Protection Regulation – GDPR*).

2.6 Управљање великим бројем сертификата

У савременим индустријским системима број дигиталних сертификата може достићи стотине или хиљаде због раста IIoT уређаја, микросервиса и потребе за безбједном комуникацијом. Ручно управљање постаје неодрживо, па су неопходни скалабилни системи који омогућавају аутоматизовано издавање, обнављање и опозив сертификата, уз интеграцију са платформама за континуирану интеграцију и испоруку (*Continuous Integration / Continuous Deployment – CI/CD*) и *cloud* сервисима.

3. КОРИШЋЕНЕ ТЕХНОЛОГИЈЕ

У развоју софтверског рјешења за управљање дигиталним сертификатима коришћене су модерне технологије које обезбјеђују сигурну имплементацију. *Backend* је развијен у *.NET Core* платформи, *frontend* у *React* библиотеци, док је *Azure Key Vault* коришћен за безбједно управљање сертификатима у *cloud* окружењу и *Microsoft Entra ID* за аутентикацију корисника. Ова комбинација омогућава високе перформансе, сигурну комуникацију и интеграцију са савременим безбједносним протоколима.

4. ТИПОВИ АРХИТЕКТУРЕ ЗА УПРАВЉАЊЕ СЕРТИФИКАТИМА

4.1 *On-premice* рјешење

On-premise рјешења за управљање дигиталним сертификатима подразумевају да се сви елементи *PKI* инфраструктуре, укључујући *CA*, базе података, политике и алате за мониторинг, налазе унутар локалне мреже организације, што омогућава потпуну контролу над безбједносним процесима. Овај приступ је погодан за индустријска окружења са високим захтјевима за приватност и усклађеност са стандардима, али захтијева значајне ресурсе за имплементацију, одржавање и обуку особља.

4.2 *Cloud* рјешење

Cloud рјешења за управљање дигиталним сертификатима ослањају се на сервисе попут *Azure*, *Amazon Web Services (AWS)* и *Google Cloud*. Интеграција са софтверским алатима који омогућавају аутоматизацију, интеграцију и надзор процеса развоја, тестирања и испоруке апликација (*DevOps*) и *CI/CD* процесима обезбјеђује континуитет безбједности, док сервиси као што су *Azure Key Vault* и *AWS* менаџер сертификата нуде централизовано управљање, ротацију кључева и аудит активности.

4.3 Хибридно рјешење

Хибридна архитектура управљања сертификатима комбинује локална и *cloud* рјешења како би организацијама омогућила контролу над критичним компонентама уз коришћење флексибилности и скалабилности које пружају *cloud* сервиси. Сертификати за интерне системе издају се и чувају локално, док се они за апликације које комуницирају са екстерним сервисима ефикасно управљају кроз *cloud* алате. Постојећа рјешења која се користе у хибридним моделима укључују *Microsoft Intune* у комбинацији са *ADCS* (*Active Directory Certificate Services*), *AWS* менаџер сертификата повезан са *Windows ADCS*, *HashiCorp Vault* интегрисан са *Azure Key Vault*-ом, *Enterprise Java Beans Certificate Authority* (*EJBCA*) *Hybrid PKI* за индустријске системе, као и *CertAccord Enterprise* који омогућава аутоматизовано управљање сертификатима. Ова рјешења потврђују да хибридни модел није теоријски концепт, већ практичан приступ који омогућава постепену миграцију ка *cloud*-у, оптимизацију ресурса, смањење трошкова и повећање отпорности система на безбједносне инциденте [6].

5. МЕХАНИЗМИ И АЛАТИ ЗА АУТОМАТСКО УПРАВЉАЊЕ СЕРТИФИКАТИМА

Аутоматизација процеса издавања, обнављања и опозива сертификата повећава безбједност, смањује ризик људске грешке и омогућава скалабилност система, уз коришћење специјализованих механизама и алата.

5.1 *ACME* протокол

ACME (*Automatic Certificate Management Environment*) је стандардизовани протокол за потпуно аутоматско управљање дигиталним сертификатима од генерисања захтјева (*Certificate Signing Request – CSR*), верификације, издавања до аутоматског обнављања. Развијен од стране *Internet Security Research Group (ISRG)* за *Let's Encrypt*, *ACME* смањује људске грешке, убрзава *TLS* имплементацију и омогућава скалабилност у динамичним окружењима. Валидација се врши преко *HyperText Transfer Protocol – 01 (HTTP-01)* или *Domain Name System – 01 (DNS-01)* механизама [7].

5.2 Аутоматизација издавања, обнављања и опозива

Аутоматско издавање сертификата обухвата генерисање *CSR*-а са јавним кључем, верификацију идентитета и издавање без мануелне интервенције, користећи алате као што су *HashiCorp Vault*, *Microsoft ADCS* и *ACME* протокол. Сертификати се обнављају помоћу заказаних задатака (*cron job*), механизама за аутоматско обавјештавање преко веба (*webhook*) или алата попут *Certbot*-а. У случају компромитације, аутоматизовани опозив ажурира *CRL* или *OCSP* у реалном времену, уз подршку алата као што су *Vault*, *ADCS* и *Security Information and Event Management (SIEM)* системи.

5.3 Интеграција са *CI/CD* алатима

У *CI/CD* окружењима сертификати обезбјеђују аутентикацију, потписивање артефаката и сигурну комуникацију током „*build*“ и „*deployment*“ процеса, уз аутоматизацију кроз алате попут *Jenkins* и *GitHub Actions*.

5.4 Аутоматизација у *cloud* окружењу

Cloud платформе као што су *Microsoft Azure, AWS* и *Google Cloud* нуде сервисе за управљање сертификатима без сопствене *PKI* инфраструктуре. *Azure Key Vault* омогућава генерисање и обнављање сертификата, *AWS* менаџер сертификата аутоматски издаје *SSL/TLS* сертификате, а *Google Cloud* менаџер сертификата подржава аутоматско управљање.

6. ЦЕНТРАЛИЗОВАНО УПРАВЉАЊЕ И МОНИТОРИНГ

6.1 Централна тачка за издавање и ревокацију

Централизована тачка за издавање и опозив сертификата обезбјеђује досљедну примјену правила, праћење и брзу реакцију на инциденте. Рјешења попут *Microsoft ADCS* и *HashiCorp Vault* омогућавају аутоматско управљање сертификатима уз интеграцију са *Active Directory*, *cloud* сервисима и *DevOps* алатима.

6.2 Мониторинг и аудитинг сертификата

Мониторинг прати рок важења, открива неауторизоване сертификате и валидира конфигурацију, док аудитинг биљежи и анализира све активности ради форензике и транспарентности. Интеграција са *SIEM* системима омогућава централизовано прикупљање логова и корелацију догађаја за већу безбједност.

6.3 Алати за управљање животним циклусом сертификата

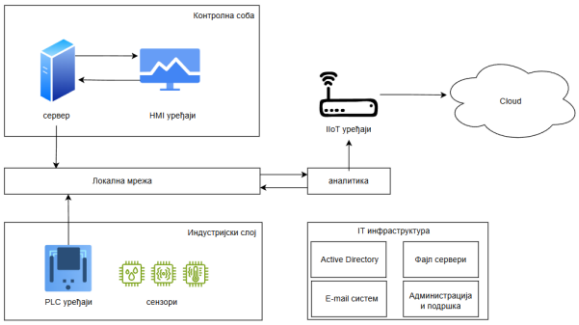
Алати за управљање сертификатима као што су *Venafi*, *Keyfactor* и *Certbot* аутоматизују издавање, обнављање, опозив и надзор. *Venafi TLS Protect* и *SSH Protect* нуде напредну ротацију и валидацију, *Keyfactor* управља *PKI* инфраструктуром уз подршку за *cloud* и *DevOps*, док је *Certbot* алат отвореног кода (*open-source*) за *ACME* протокол, идеалан за мање системе.

7. АРХИТЕКТУРА ХИБРИДНОГ РЈЕШЕЊА ЗА УПРАВЉАЊЕ СЕРТИФИКАТИМА ЗА ПОТРЕБЕ ПОГОНА ЗА ОБРАДУ МЕТАЛА

Избор хибридне архитектуре комбинује локални *CA* (*Microsoft ADCS*) за управљање сертификатима у затвореним мрежама оперативних технологија (*Operational Technology – OT*) и *Azure Key Vault* за *cloud* окружење. Овакав приступ омогућава централизовано, аутоматизовано и безбједно управљање сертификатима за *SCADA, HMI,* програмабилни логички контролер (*Programmable Logic Controller – PLC*) и *IIoT* уређаје, уз смањење трошкова и ризика. Систем подржава аутентикацију, енкрипцију комуникације, контролу приступа и аудит у складу са стандардима као што је *IEC 62443*.

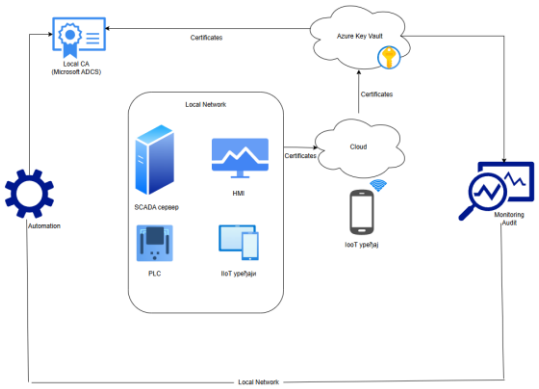
7.1 Опис индустријског система

Студија случаја приказује средње велику фабрику за обраду метала која користи *SCADA* систем за надзор и управљање производњом. Техничка архитектура система укључује *SCADA* сервер, *HMI* терминале, *PLC* уређаје, *IIoT* сензоре, локалну индустријску мрежу и *IT* инфраструктуру, што је приказано на Слика 1.



Слика 1. Техничка архитектура система

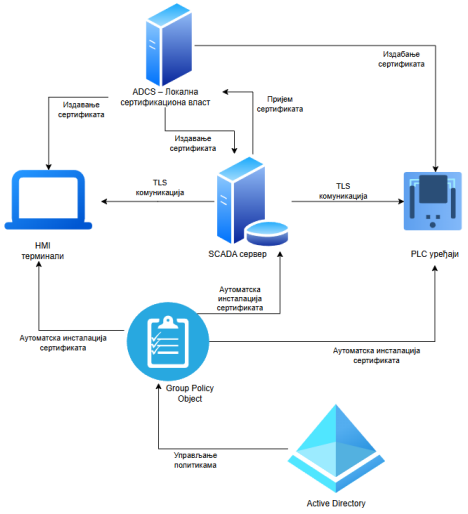
За управљање дигиталним сертификатима примјењена је хибридна архитектура која комбинује *Microsoft ADCS* за *SCADA*, *HMI* и *PLC* компоненте, и *Azure Key Vault* за *IIoT* уређаје и *cloud* сервисе. Токови сертификата, аутоматизација процеса и надзор у реалном времену приказани су на Слика 2.



Слика 2. Архитектура система

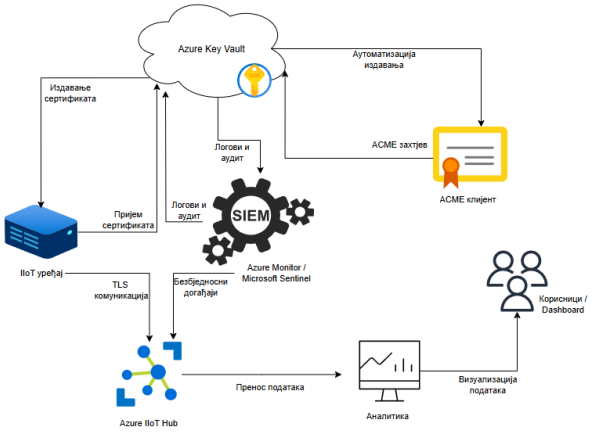
7.2 Архитектура хибридног рјешења за управљање сертификатима

У циљу обезбјеђивања безбједне комуникације и управљања идентитетима у сложеном индустријском окружењу, имплементирано је хибридно рјешење које комбинује локалну инфраструктуру (*Microsoft ADCS*) и *cloud* сервисе (*Azure Key Vault*), омогућавајући централизовано, аутоматизовано и скалабилно управљање сертификатима за *SCADA, HMI, PLC* и *IIoT* уређаје. Слика 3 приказује токове сертификата у локалној мрежи, укључујући издавање путем *ADCS*-а, дистрибуцију преко *Group Policy* објеката (*GPO*) и *PowerShell* скрипти, те аутентикацију корисника кроз *Active Directory*.



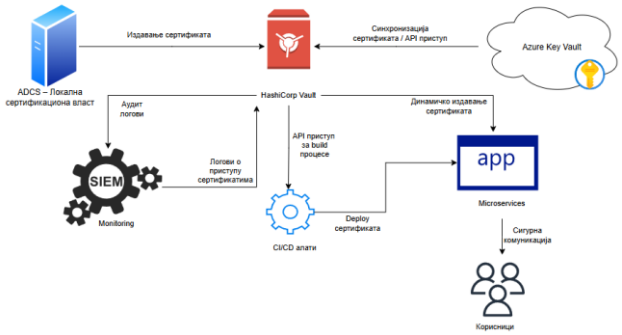
Слика 3. Архитектура локалне компоненте

За *cloud* компоненту, Слика 4 илуструје како *Azure Key Vault* управља сертификатима за *IIoT* уређаје, омогућава аутоматско издавање путем *ACME* протокола и интеграцију са *Azure IoT Hub*-ом, уз мониторинг кроз *Azure Monitor* и *Microsoft Sentinel*.



Слика 4. Архитектура *cloud* компоненте

Слика 5 приказује интеграциони слој са *HashiCorp Vault*-ом који повезује локални *CA* и *cloud* сервисе, омогућава динамичко издавање сертификата за микросервисе и *CI/CD* алате, те централизовану евиденцију и аудит. Аутоматизација се додатно подржава алатима као што је *Certbot*, скриптама и *webhook*-овима, док *SIEM* системи омогућавају надзор и детекцију инцидената.



Слика 5. Архитектура интеграционог слоја

Резултати имплементације укључују смањење броја инцидената, повећану ефикасност тимова, усклађеност са безбједносним стандардима и спремност система за будуће ширење.

8. ИМПЛЕМЕНТАЦИЈА ХИБРИДНОГ РЈЕШЕЊА ЗА УПРАВЉАЊЕ СЕРТИФИКАТИМА

У оквиру мастер рада развијено је софтверско рјешење засновано на *.NET Core* и *React* технологијама које омогућава хибридну архитектуру за управљање дигиталним сертификатима, комбинујући локалну инфраструктуру и *cloud* компоненту *Azure Key Vault*. Систем обезбјеђује генерисање, управљање, складиштење и дистрибуцију сертификата уз подршку за реалне индустријске сценарије, а архитектура је подијељена на *backend* који обрађује логику сертификата и *frontend* који пружа интерактивни интерфејс за управљање. На Слика 6 приказан је централни дио апликације са прегледом сертификата и акцијама као што су обнова, опозив, извоз и слање у *Azure Key Vault*.

Слика 6. Интерфејс апликације

Слика 7 показује *Azure* портал на коме је сертификат успјешно синхронизован, што потврђује исправност интеграције и безбједан пренос података.

Слика 7. Приказ сертификата на *Azure Key Vault*-у

Имплементација је довела до смањења инцидената везаних за истекле сертификате, повећања ефикасности *IT* и *OT* тимова, усклађености са безбједносним стандардима и спремности система за проширење на нове производне линије и *cloud* сервисе.

9. ПРЕДНОСТИ ХИБРИДНОГ РЈЕШЕЊА

Имплементација хибридног система за управљање дигиталним сертификатима комбинује локалну контролу преко *Microsoft ADCS*-а и *cloud* флексибилност *Azure Key Vault*-а. Рјешење засновано на *.NET* и *React* технологијама омогућава централизовано и аутоматизовано управљање сертификата, уз минималну ручну интервенцију. Систем доноси безбједносне предности као што су *TLS* енкрипција, јединствени сертификати и брза реакција на инциденте, као и оперативне предности попут скалабилности, интеграције са *DevOps* алатима и централизованог надзора. На Табела 1 приказана је компаративна анализа кључних параметара различитих рјешења за управљање дигиталним сертификатима, а плавом бојом је означено рјешење описано у овом раду.

Табела 1. Компаративна анализа хибридних рјешења

Критеријум	Описано рјешење	Microsoft Intune + ADCS	AWS ACM + ADCS	HashiCorp Vault + Azure KV	EJBCA Hybrid PKI	CertAccord Enterprise
Локални CA	ADCS	ADCS	ADCS	Опционо	EJBCA	ADCS
Cloud сервис	Azure Key Vault	Microsoft Cloud PKI	AWS ACM + HSM	Azure Key Vault	AWS/Azure/GCP	Опционо
Интеграциони слој	HashiCorp Vault	Не	Не	Vault као примарни	Опционо	Не
Аутоматизација	Висок - ACME, CI/CD	Средњи - Intune, GPO	Средњи - API	Висок - API, ACME	Средњи	Средњи
DevOps интеграција	Да	Ограничено	Ограничено	Да	Да	Не
OT/SCADA фокус	Да	Не	Не	Не	Ограничено	Не
SIEM/Мониторинг	Да - Sentinel	Основни	Основни	Основни	Основни	Основни
IoT подршка	Да	Ограничено	Да	Да	Да	Ограничено
Усклађеност	IEC 62443, NIS2	GDPR	GDPR	GDPR	IEC 62443	GDPR

Представљено рјешење се истиче интеграцијом *OT/SCADA* и *IIoT* компоненти, напредном аутоматизацијом кроз *ACME* и *CI/CD* процесе, мониторингом и *SIEM* интеграцијом, као и усклађеношћу са *IEC 62443* и *NIS2*.

10. ЗАКЉУЧАК

У овом раду обрађена је тема управљања дигиталним сертификатима, са фокусом на хибридна рјешења. Дигитални сертификати играју кључну улогу у аутентикацији, енкрипцији и контроли приступа у *SCADA* и *IIoT* системима. Аутоматизација управљања сертификатима, интеграција са *CI/CD* алатима и примјена *DevSecOps* приступа постају стандард, док се истовремено развијају рјешења за динамичко управљање у изворним *cloud* окружењима (*cloud-native*) и аутоматизовану усклађеност са регулативама. *DevSecOps* омогућава безбједност кроз све фазе развоја. Будућа истраживања усмјерена су ка отпорности на квантне пријетње, анализи ризика помоћу вјештачке интелигенције, стандардизацији протокола и проширењу функционалности апликација.

11. ЛИТЕРАТУРА

[1] https://www.sectigo.com/blog/x509-certificate-management (pristupljeno u aprilu 2022.)

[2] https://www.okta.com/identity-101/digital-certificate/ (pristupljeno u avgustu 2024.)

[3] A. Albarqi, E. Alzaid, F. Al Ghamdi, S. Asiri, J. Kar, "Public Key Infrastructure: A Survey", *J. Inf. Secur.*, vol. 6, pp. 31–37, January 2015.

[4] N. Ricchizzi, C. Schwinne, J. Pelzl, "Applied Post Quantum Cryptography: A Practical Approach for Generating Certificates in Industrial Environments", *arXiv preprint*, May 2025.

[5] N. Korzhitskii, N. Carlsson, "Revocation Statuses on the Internet", *Proc. of Passive and Active Measurement Conference (PAM 2021)*, pp. 175–191, April 2021.

[6] https://learn.microsoft.com/en-us/intune/intune-service/protect/microsoft-cloud-pki-deployment (pristupljeno u aprilu 2025.)

[7] D. A. Cordova Morales, A. S. Wazan, D. W. Chadwick, R. Laborde, A. R. R. Maramara, K. Cabral "Enhancing the ACME Protocol to Automate the Management of All X.509 Web Certificates", *IFIP Adv. Inf. Commun. Technol.*, vol. 679, pp. 265–278, April 2024.

Кратка биографија:

Јелена Унковић рођена је у Бањој Луци 2000. год. Мастер рад на Факултету техичких наука из области Електротехнике и рачунарства - Примењено софтверско инжењерство одбранила је 2026. год.
Контакт: jelenaad26@gmail.com