37. Саветовање CIGRE Србија 2025
СИГУРНОСТ, СТАБИЛНОСТ, ПОУЗДАНОСТ И RESILIENCE ЕЛЕКТРОЕНЕРГЕТСКОГ СИСТЕМА
МУЛТИСЕКТОРСКО ПОВЕЗИВАЊЕ У ЕНЕРГЕТИЦИ И ПРИВРЕДИ
26 - 30. мај 2025, Копаоник

DOI: 10.46793/CIGRE37.C2.25

**C2.25**

# PROVERA INTEGRITETA MREŽNIH MODELA SA ASPEKTA INFORMACIONE BEZBEDNOSTI

# VALIDATION OF GRID MODEL INTEGRITY FROM THE INFORMATION SECURITY ASPECT

**Dušan Prešić, Andrijana Prešić, Marija Miljuš, Srđan Subotić***

**Kratak sadržaj:** Poverljivost-integritet-dostupnost (*Confidentiality, Integrity, Availability* – CIA) trijada je vodeći model koji se koristi za pronalaženje ranjivosti i metoda za minimiziranje pretnji u vezi sa bezbednošću informacija. U slučaju operativnog planiranja elektroenergetskog sistema (EES), ključni skupovi podataka su individualni mrežni modeli (*Individual Grid Model* – IGM) i spojeni mrežni modeli (*Common Grid Model* – CGM), pošto se podaci sadržani u ovim modelima mreže koriste za predviđanje očekivanog ponašanja EES-a u budućnosti. U okviru ENTSO-E zajednice sprovedeno je mnogo različitih kontrolnih mera kako bi se zaštitila poverljivost i dostupnost pomenutih mrežnih modela, dok integritet ovih modela nije bio toliko u fokusu.
Kao deo R²D² (*Reliability, Resilience and Defense technology for the griD*) projekta, finansiranog kroz program *Horizon Europe*, implementiran je KSI (*Keyless Signature Infrastructure*) sistem koji proverava integritet IGM-a i CGM-a. Koristeći specifičnu *blockchain* tehnologiju, KSI sistem je u poziciji da obradi ove modele mreže i kreira datoteku potpisa koja predstavlja dokaz integriteta podataka.
U radu su opisani opšti koncepti u vezi sa KSI sistemom i KSI *blockchain* tehnologijom, kako se može dokazati integritet podataka i kako se KSI sistem primenjuje u procesu kreiranja CGM-a.

***Ključne reči:*** *CIA trijada, Bezbednost informacija, Operativno planiranje, Blockchain tehnologija, R2D2, Horizon Europe*

**Abstract:** The CIA (Confidentiality, Integrity, Availability) triad is a guiding model used to find vulnerabilities and methods to minimize threats related to information security. In the case of operational planning of the Electrical Power and Energy System (EPES), the key datasets are Individual Grid Models (IGMs) and Common Grid Models (CGMs), since data contained in these grid models is used to forecast expected EPES behavior in the future.

* Dušan Prešić, Security Coordination Centre SCC Ltd. Belgrade, dusan.presic@scc-rsci.com
Andrijana Prešić, Security Coordination Centre SCC Ltd. Belgrade, andrijana.presic@scc-rsci.com
Marija Miljuš, EMS AD, marija.miljus@ems.rs
Srđan Subotić, EMS AD, srdjan.subotic@ems.rs

Many different control measures have been implemented within the ENTSO-E community to protect the confidentiality and availability of the mentioned grid models, while the integrity of these models was not so much the focus.
As part of the R²D² (Reliability, Resilience and Defense technology for the griD) project, funded through the Horizon Europe program, the KSI (Keyless Signature Infrastructure) system was implemented to validate the integrity of IGMs and CGMs. Using specific blockchain technology, the KSI system is in a position to process these grid models and create a signature file, which represents a proof of data integrity.
The paper describes general concepts related to the KSI system and KSI blockchain technology, how the integrity of data could be proved, and how the KSI system is implemented in the CGM building process.

***Key words:*** *CIA triad, Information security, Operational planning, Blockchain technology, R2D2, Horizon Europe*

## 1 UVOD

Sa rastućom digitalizacijom, zaštita informacija postala je prioritet za kompanije, vlade i pojedince. Poverljivost-integritet-dostupnost (*Confidentiality, Integrity, Availability* – CIA) trijada predstavlja osnovni model u informacionoj bezbednosti, koji usmerava razvoj bezbednosnih politika, strategija upravljanja rizikom i mehanizama odbrane. Poverljivost osigurava da osetljive informacije budu dostupne samo ovlašćenim korisnicima, integritet štiti podatke od neovlašćenih izmena, dok dostupnost garantuje da informacije i sistemi ostanu pristupačni kada su potrebni.

Pri operativnom planiranju elektroenergetskog sistema (EES), ključne informacije su sadržane u individualnim mrežnim modelima (*Individual Grid Model* – IGM) i spojenim mrežnim modelima (*Common Grid Model* – CGM). S obzirom na to da se ove informacije koriste za predviđanje budućeg ponašanja EES-a, u ENTSO-E zajednici preduzete su brojne tehničke mere kako bi se osigurala poverljivost i dostupnost datih mrežnih modela na OPDE (*Operational Planning Data Environment*) platformi, dok je integritet ostao u drugom planu. Integritet podataka znači da su oni pouzdani, potpuni i da ih neovlašćeni korisnik nije menjao ili modifikovao. Integritet podataka se održava samo ako su podaci autentični, tačni i pouzdani. Nedostatak adekvatnih mehanizama za zaštitu integriteta podataka može dovesti do ozbiljnih posledica u operativnom planiranju EES-a. Greške u unosu, neusklađenost između IGM-ova i CGM-ova koji se odnose na isti vremenski trenutak, nenamerne ili zlonamerne izmene podataka mogu ugroziti tačnost predikcija i donošenje odluka zasnovanih na tim podacima. Bez adekvatnih kontrola integriteta, postoji rizik da se odluke donose na osnovu netačnih ili nepotpunih informacija, što može negativno uticati na sigurnost i efikasnost rada EES-a. Stoga je neophodno uvesti strože mere zaštite integriteta podataka, uključujući napredne metode provere tačnosti, automatizovane sisteme detekcije anomalija i uspostavljanje jasnih standarda za razmenu podataka unutar ENTSO-E zajednice.

U okviru *Horizon Europe* programa Evropske unije za istraživanje i inovacije, finansiran je R²D² (*Reliability, Resilience and Defense technology for the griD*) projekat (ID: 101075714), koji ima za cilj jačanje pouzdanosti i otpornosti EES-a u Evropi. Kroz razvoj inovativnih alata za procenu rizika, prevenciju pretnji i unapređenje održavanja infrastrukture, R²D² projekat pomaže u zaštiti elektroenergetske mreže od fizičkih i sajber pretnji, čime se obezbeđuje sigurniji i otporniji EES, što doprinosi stabilnosti snabdevanja i jačanju evropske energetske bezbednosti.

U okviru srpskog testnog okruženja (*Serbian pilot site*) implementiran je KSI (*Keyless Signature Infrastructure*) sistem koji proverava integritet IGM-a i CGM-a. Koristeći KSI *blockchain* tehnologiju, KSI sistem je u poziciji da obradi ove modele mreže i kreira datoteku potpisa koja predstavlja dokaz integriteta podataka. Dodatna vrednost ove provere integriteta za operatore prenosnog sistema (*Transmission System Operator* – TSO) i regionalne koordinacione centre (*Regional Coordination Centre* – RCC) mogla bi biti sledeća:

- Sposobnost reagovanja na zlonamerne aktivnosti, ljudsku grešku i opštu korupciju podataka kada je operativno planiranje zasnovano na lažnim ili pokvarenim podacima – ovo dovodi do smanjenja prekida energetskih usluga i poremećaja;

- Pruža dokaze koji se mogu koristiti za rešavanje sporova između uključenih strana u slučaju neovlašćene modifikacije podataka;

- Pruža zadovoljenje nekih regulatornih aspekata bezbednosti informacija (na nacionalnom nivou ili nivou EU).

Cilj ovog rada je da prikaže kako se KSI *blockchain* tehnologija može koristiti za kontrolu integriteta mrežnih modela – skupova poverljivih podataka koji se svakodnevno koriste od strane TSO-a i RCC-a za procese operativnog planiranja EES-a. U okviru Poglavlja 2 prikazani su osnovni koncepti vezani za *blockchain* tehnologiju uopšte, ali i za specifičnu KSI *blockchain* tehnologiju koja se koristi za proveru integriteta mrežnih modela sa aspekta informacione bezbednosti. Poglavlje 3 opisuje na koji način je KSI sistem implementiran u srpsko testno okruženje R²D² projekta, da bi Poglavlje 4 dalo opis na koji način je KSI sistem integrisan u proces prognoze zagušenja za dan unapred (*Day-Ahead Congestion Forecast* – DACF). Poglavlje 5 daje zaključke rada, a poslednje dve celine predstavljaju Zahvalnicu i Literaturu.

## 2 KSI BLOCKCHAIN TEHNOLOGIJA

*Blockchain* predstavlja distribuiranu repliciranu bazu podataka, koja je organizovana u formi jednostruko spregnute liste (lanac) [1]. Karike u ovom lancu predstavljaju blokove sa podacima, koji se posle grupisanja štite kriptografskim metodama. Otuda i naziv *blockchain*, odnosno „lanac blokova“. U poređenju sa klasičnim bazama podataka, *blockchain* tehnologija nema centralno mesto čuvanja podataka, već se za to koristi čvor-na-čvor komunikacija (*Peer to peer* – P2P) u okviru distribuirane *blockchain* mreže. Čvorovi mreže koji učestvuju u realizaciji servisa poseduju kopiju svih zapisa, te stalno međusobno komuniciraju i sinhronizuju zapise [1]. Pored toga, uloga pojedinih čvorova je i da stalno vrše verifikaciju autentičnosti zapisa koji se nalaze u lancu, te da odbace predložene blokove podataka, ukoliko ne prođu verifikaciju [1]. Zahvaljući P2P arhitekturi, poverenje u ispravnost podataka na datoj *blockchain* mreži se ne dobija od nekog centralnog autoriteta (banka, vladina služba, notar, itd.), već se to poverenje ostvaruje validacijom novog bloka korišćenjem mehanizma konsenzusa koji mora biti potvrđen od 51% čvorova u datoj mreži. Svaki validiran blok dobija svoju jedinstvenu vremensku oznaku (*eng. timestamp*) i potpis (*eng. hash*), te se kao takav propagira na ostale čvorove u mreži [1]. Pri dodavanju svakog narednog validiranog bloka, inkrementira se brojač potvrda za prethodno upisane blokove, te se dalje smanjuje verovatnoća da su oni lažni [1]. Dakle, protokom vremena i povećanjem broja čvorova u mreži raste pouzdanost zapisanih podataka, tj. poverljivi podaci sadržani u blokovima se mogu smatrati nepromenljivim.

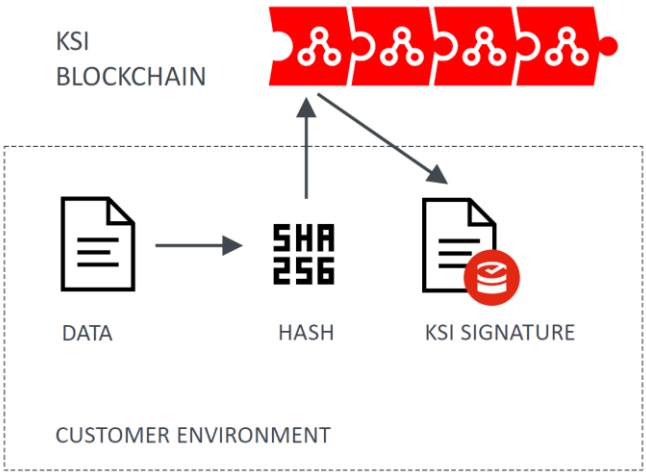
Estonija je jedno od vodećih informacionih društava u svetu. Više od dve decenije, ova zemlja unapređuje digitalizaciju svog društva. Još 2000. godine, Estonija je proglasila pristup internetu ljudskim pravom, što je podstaklo širenje internet pristupa u ruralnim oblastima i omogućilo

inovativnu upotrebu digitalnih tehnologija. Estonija teži širenju digitalnih usluga i implementaciji tehničkih i pravnih rešenja koja podržavaju digitalne interakcije između građana i države. Kriptografske tehnologije predstavljaju osnovu sigurnosti takvih interakcija. Još jedan važan deo pravnog okvira jeste obavezno sprečavanje dupliranja podataka u bazama (*eng. once-only writing*) – nijedna informacija se ne skladišti dva puta, a svaka izmena mora biti izvršena na glavnom zapisu. Ovakav sistem omogućava precizno evidentiranje i reviziju pristupa podacima i upita koji se odnose na lične zapise. Iz tog razloga postoji jasna motivacija za korišćenje *blockchain* tehnologije, koja garantuje otkrivanje pokušaja manipulacije podacima, bilo da dolaze od internih ili eksternih aktera, pa čak i od potencijalnih državnih entiteta sa značajnim računsko-logističkim resursima. [2]

U estonskim primenama *blockchain* tehnologije, KSI *blockchain* tehnologija zauzima centralno mesto. KSI generiše i održava *blockchain* koji sadrži distribuiranu glavnu knjigu (*eng. ledger*). Ova tehnologija je integrisana u ključne državne registre, uključujući poslovni registar, registar nepokretnosti, nasledni registar, digitalne sudske spise i zvanična saopštenja. KSI *blockchain* se koristi za interne i eksterne procese kako bi se očuvao integritet podataka i omogućilo efikasno otkrivanje namernih i nenamernih izmena u podacima u stanju mirovanja (*eng. data-at-rest*). Pored toga, upotreba KSI *blockchain* omogućava nezavisnu verifikaciju od strane trećih lica i služi kao dugoročni forenzički dokaz postojanja podataka. [2]

KSI *blockchain* tehnologija, koju je razvila kompanija Guardtime za pomenute potrebe estonskog društva, predstavlja specifičnu *blockchain* tehnologiju osmišljenu za obezbeđivanje integriteta podataka bez oslanjanja na tradicionalne PKI (*Public Key Infrastructure*) sisteme. Za razliku od PKI, koji zahteva složeno upravljanje ključevima, KSI omogućava proveru integriteta podataka bez potrebe za korišćenjem ključeva ili pouzdanih autoriteta. Osnovni princip rada KSI *blockchain* tehnologije (prikazan na Slici 1) sastoji se od sledećih koraka:

- U okviru korisničkog okruženja, podaci se šifruju pomoću određenog kriptografskog *hash*-algoritma, koji podacima proizvoljne dužine dodeljuje *hash*-kod fiksne dužine;
- *Hash*-kod se onda posebnim tehnikama ugrađuje u KSI *blockchain*;
- KSI *blockchain* generiše datoteku potpisa (*eng. signiture file*) koja predstavlja dokaz integriteta inicijalnih podataka, vremenskog trenutka kada su podaci upisani i entiteta koji ih je upisao.




Slika 1: Pojednostavljeni princip rada KSI *blockchain* tehnologije [3]

Ovakav koncept obezbeđuje visok nivo privatnosti korisničkih podataka, jer oni nikada ne izlaze van korisničkog okruženja, pošto se šifrovanje podataka vrši isključivo u okviru korisničkog okruženja, a samo *hash*-kod se prosleđuje spolja u KSI *blockchain* mrežu. Proces generisanja datoteke potpisa detaljno je opisan u okviru literature [4], a suštinski se sastoji od sledećih koraka (prikazanih na Slici 2):

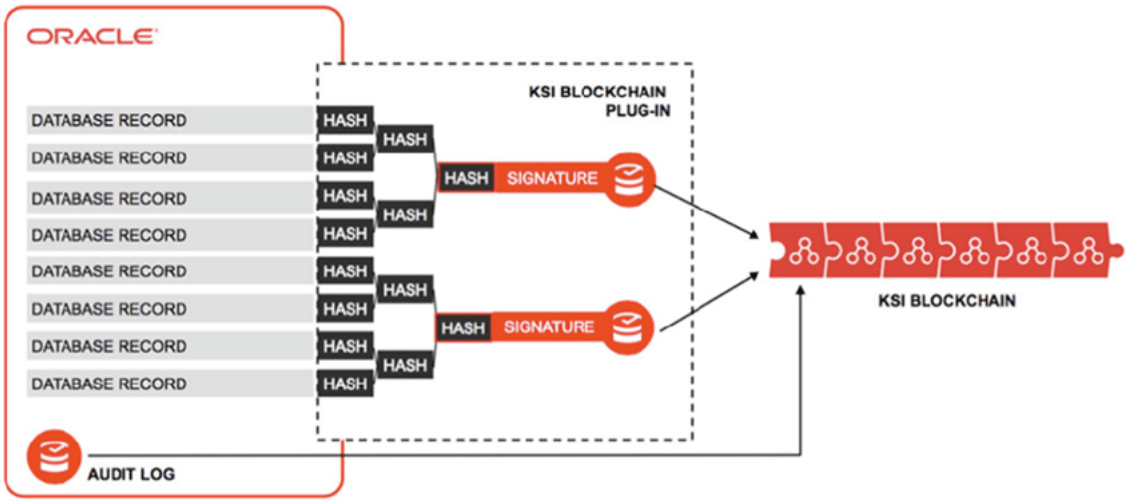
- Šifrovanje podataka – Svaki deo podataka se transformiše u jedinstveni *hash*-kod pomoću kriptografskih *hash*-algoritama. Ovaj *hash*-kod služi kao digitalni otisak podataka;

- Konstrukcija Merklovog stabla – Pojedinačni *hash*-kodovi podataka organizuju se u hijerarhijsku strukturu poznatu kao Merklovo stablo. U ovom stablu, *hash*-kodovi podataka predstavljaju „list“ čvorove, a svaki čvor koji nije „list“ (a koji se naziva grana, unutrašnji čvor ili inod) je označen kriptografskim *hash*-kodom njegovih podređenih čvorova. Krajnji rezultat je jedinstveni *hash*-kod „korena“ Merklovog stabla, koji predstavlja ceo skup podataka;

- Agregacija – H*ash*-kodovi „korena“ Merklovog stabla iz više klijenata se prikupljaju i dodatno agregiraju na hijerarhijski način. Ovaj proces sprovode specijalizovani čvorovi unutar KSI infrastrukture, čime se osigurava skalabilnost i efikasnost sistema;

- Vremensko označavanje (*eng. timestamping*) i integracija u kalendarsku bazu podataka (*eng. calendar database/archive*) – Agregirani *hash*-kod se kombinuje sa vremenskim pečatom i integriše u KSI *blockchain*. Ovaj korak omogućava nezavisnu verifikaciju postojanja i integriteta podataka u određenom vremenskom trenutku;

- Verifikacija – Da bi se proverio integritet podataka, može se ponovo izračunati *hash*-kod podataka, pratiti kroz Merklovo stablo do agregiranog *hash*-koda „korena“ Merklovog stabla koji je smešten u okviru KSI *blockchain*-a i onda taj *hash*-kod podataka uporediti sa *hash*-kodom datoteke potpisa. Ako su ova dva *hash*-koda ista onda se može tvrditi da podaci nisu izmenjeni od trenutka vremenskog obeležavanja.




Slika 2: Prikaz načina generisanja datoteke potpisa [2]

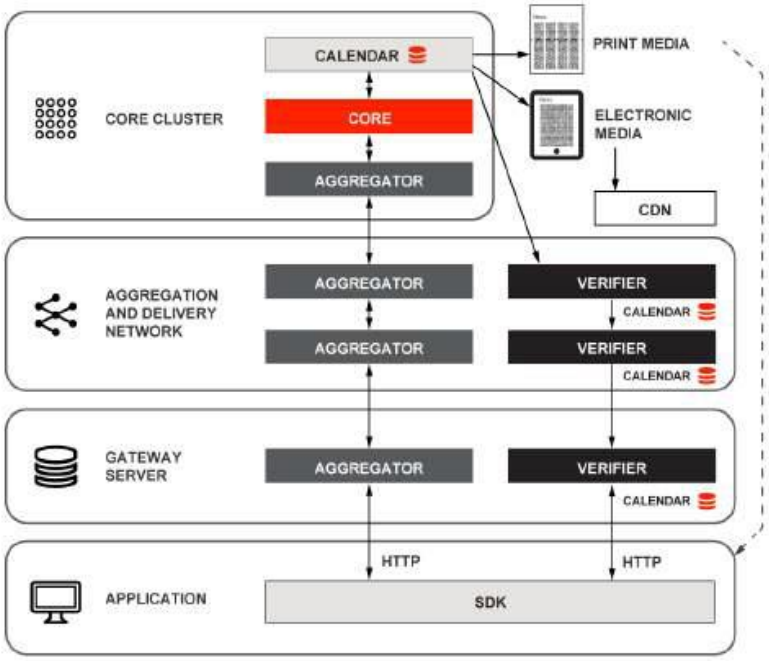
Da bi se efikasno izvršilo generisanje datoteke potpisa, koristi se arhitektura KSI sistema prikazanog na Slici 3. Ovaj sistem se sastoji od četiri ključne komponente:

- Lokalna korisnička aplikacija koja proizvodi poverljive podatke se pomoću paketa za razvoj softvera (*Software Development Kit* – SDK) integriše sa KSI sistemom. Alternativno se može koristiti grafički korisnički interfejs koji je implementiran kao veb-servis koji se pokreće putem internet pretraživača (ovo rešenje je razvijeno u okviru R²D² projekta i biće detaljnije objašnjeno u Poglavlju 3);

- *Gateway server* je hardverska ili softverska komponenta na lokaciji korisnika, koja omogućava pristup KSI usluzi. *Gateway server* je protokolni adapter koji služi kao interfejs za različite aplikacije koje koriste KSI *blockchain*. On implementira prvi nivo agregacije, jer se opterećenje može predvideti i ne zahteva kanale velike propusnosti. Pored toga, *Gateway server* sadrži i *extender servis*, koji omogućava verifikaciju potpisa ; [5]

- *Aggregation and delivery network* sastavljena je od geografski rasutih skupova agregacionih servera koji se koriste za kreiranje Merklovog stabla na osnovu dolaznih zahteva [2]. Ova komponenta sistema omogućava skalabilnost, redundantnost i globalni domet u isporuci KSI usluga [5];

- *Core Cluster* su distribuirani sinhronizovani sistemi odgovorni za postizanje konsenzusa o vrednostima gornjih *hash*-kodova iz agregacionih perioda. *Core Cluster* trajno skladišti ove gornje *hash*-kodove u bazu podataka kalendara i vraća ih *Aggregation and delivery network* kao deo datoteke potpisa. Takođe, *Core Cluster* je zadužen za vremensku sinhronizaciju, koja određuje vreme izdavanja svake datoteke potpisa. [2]




Slika 3: Arhitektura KSI sistema [5]

Ključne karakteristike KSI *blockchain* tehnologije su:

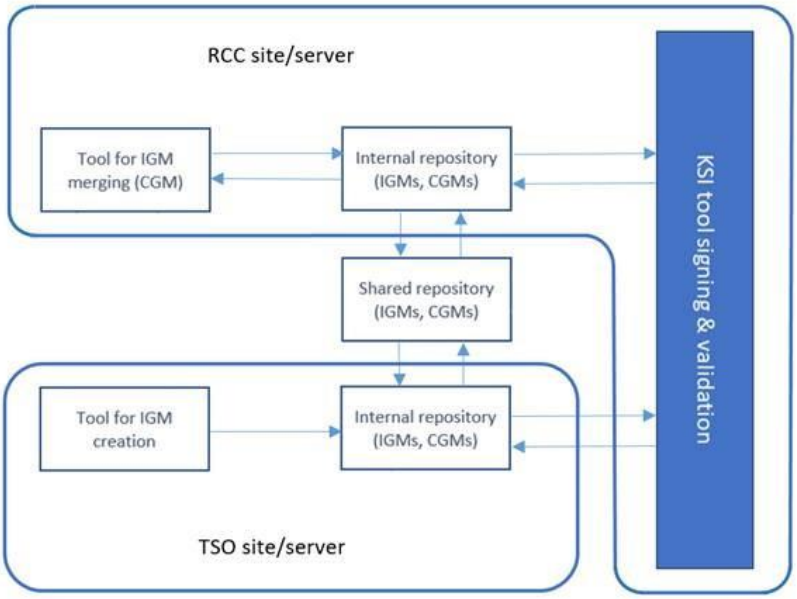
- Skalabilnost – KSI sistem može obrađivati ogromne količine podataka (milione događaja u sekundi), što ga čini pogodnim za primenu u javnom i privatnom sektoru. Takođe, prevazilazi tehnička ograničenja drugih *blockchain* tehnologija (npr. vremena potvrde transakcija);

- Nezavisna verifikacija – Vremenske oznake kreirane putem KSI sistema mogu se nezavisno verifikovati, bez potrebe za oslanjanjem na bilo kog trećeg provajdera, čime se povećavaju poverenje i transparentnost;

- Dugoročni integritet – KSI vremenske oznake su dizajnirane tako da budu neograničeno upotrebljive, bez potrebe za složenim upravljanjem kriptografskim životnim ciklusom. One ne ističu, pružaju dugoročni forenzički dokaz i otporne su na napade kvantnim računarima, čime se obezbeđuje dugoročna sigurnost podataka.

## 3 IMPLEMENTACIJA KSI SISTEMA U R²D² TESTNOM OKRUŽENJU

Pristup KSI sistemu za potrebe R²D² projekta u okviru srpskog testnog okruženja se ostvaruje putem veb-servisa koji se pokreće preko internet pretraživača. Lokalni *Gateway server* implementiran je u prostorijama SCC-a na virtuelnoj mašini, koja je izolovana od ostatka IT okruženja. Takođe, u SCC IT okruženju implementiran je i *Proxy* servis, koji se pokreće u *Docker container*-u. Ovaj servis omogućava sigurnu konekciju sa internetom i primenu CORS (*Cross-Origin Resource Sharing*) zaglavlja, koja su neophodna za rad KSI sistema. Arhitektura lokalnog IT okruženja, sa jednom instancom KSI sistema postavljenom u SCC prostorijama, kojoj pristupaju i korisnici iz SCC-a i EMS-a, prikazana je na Slici 4. [6]

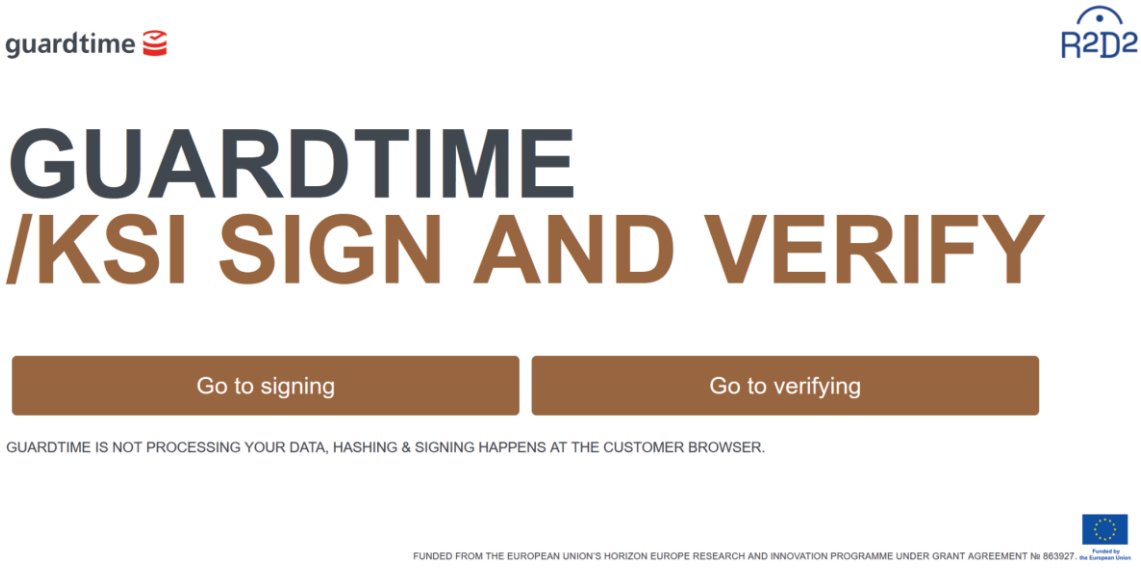



Slika 4: Arhitektura lokalnog IT okruženja u koje je implemetiran KSI sistem [6]

Interni repozitorijum se koristi za skladištenje IGM-ova, CGM-ova i datoteka potpisa. Deljeni repozitorijum obezbeđuje treća strana, u skladu sa postojećim poslovnim procesom razmene IGM/CGM podataka. RCC strana (SCC) poseduje alat za kreiranje CGM-ova, dok TSO strana (EMS) poseduje alat za kreiranje IGM-ova i da bi imala pristup KSI sistemu mora pre toga da ostvari VPN pristup na SCC-ovu IT mrežu.

Arhitektura u kojoj TSO strana ima sopstveni pristup KSI sistemu je takođe inicijalno razmatrana kao realistična situacija u praksi, ali se od nje odustalo samo zbog uštede resursa prilikom implementacije KSI sistema u okviru R²D² projekta, jer se i sa datom arhitekturom može dokazati koncept.

Slika 5 prikazuje glavni ekran korisničkog interfejsa veb-servisa KSI sistema, koji omogućava ručno potpisivanje i verifikaciju podataka. Izborom dugmeta *Go to signing*, korisnik otvara ekran za potpisivanje, gde bira fajlove koji će biti potpisani. Nakon potpisivanja, korisnik može preuzeti generisane datoteke potpisa. Isti princip se primenjuje i kod verifikacije. Izborom dugmeta *Go to verifying*, korisnik otvara ekran za verifikaciju, gde bira fajlove i pripadajuće datoteke potpisa kao ulazne podatke za proces verifikacije, koji se završava prikazom rezultata verifikacije. U zavisnosti od toga da li je bilo modifikacije mrežnih modela ili ne, status verifikacije može da bude uspešan (*Success*) ili neuspešan (*Failure*).




Slika 5: Glavni ekran korisničkog interfejsa veb-servisa KSI sistema

## 4 INTEGRACIJA KSI SISTEMA U DACF PROCES

Kako bi se unapredila sajber bezbednost mrežnih modela, TSO-i i RCC-i mogu koristiti KSI *blockchain* tehnologiju za kreiranje datoteke potpisa, koja predstavlja jedinstven kriptografski dokaz koji štiti integritet, vreme potpisivanja i identitet potpisnika mrežnog modela. Primalac modela koristi kriptografske dokaze sadržane u datoteci potpisa za verifikaciju modela, kako bi se osiguralo da je mrežni model originalan i da nije izmenjen, bilo slučajno, zlonamerno, usled *bit-flip* greške ili korupcije podataka [7]. Ako je čak i jedan bit u modelima ili datoteci potpisa izmenjen, verifikacija će prikazati grešku sa odgovarajućom porukom, omogućavajući primaocu (ili bilo kome ko vrši verifikaciju) da započne istragu [7].

Za testiranje primene KSI sistema u okviru operativnog planiranja EES-a izabran je DACF proces, gde operatori TSO-a kreiraju IGM-ove za naredna 24 sata, koristeći najbolje prognoze proizvodnje, potrošnje, topologije i prekograničnih razmena. Ovi modeli se zatim dostavljaju RCC-ima. Operatori RCC-a validiraju IGM-ove na osnovu sintakse, semantike i pravila tokova snage, a zatim ih objedinjuju u CGM-ove, koji se vraćaju TSO-ima. IGM-ovi i CGM-ovi u UCTE formatu se razmenjuju putem *Electronic Highway* (EH) platforme i predstavljaju osnovu za dalje poslove u okviru operativnog planiranja rada EES-a, kao što su: analiza sigurnosti sistema, proračun prekograničnih kapaciteta, koordinacija planova isključenja, itd.

S obzirom na to da su IGM-ovi ključni ulaz za kreiranje CGM-ova i da se oba tipa modela skladište u deljenim repozitorijumima kako bi bili dostupni RCC-ima i TSO-ima, izuzetno je važno osigurati integritet podataka u IGM-ima i CGM-ima.

Preliminarna demonstracija KSI sistema u okviru DACF procesa izvedena je tokom pet radnih dana decembra 2024. godine, i obuhvatala je proveru integriteta IGM-ova koje je EMS kreirao, kao i proveru integriteta CGM-ova koje je SCC kreirao. Provera integriteta IGM-ova svakodnevno je rađena na sledeći način:

- Operator EMS-a je kreirao 24 DACF IGM-a koristeći eTNA (*enterprise Transmission Network Analyzer*) alat i prosleđivao ih je SCC-u putem EH (u skladu sa postojećom procedurom);

- Nakon toga, operator EMS-a je IGM-ove ručno učitavao u KSI sistem, kako bi on automatski potpisivao učitane IGM-ove i kreirao 24 datoteke potpisa IGM-ova;

- Po završetku prethodnog koraka, operator EMS-a je preuzimao datoteke potpisa IGM-ova, a zatim ih postavljao na repozitorijum *Alfresco*;

- Operator SCC-a je preuzimao IGM-ove sa EH i odgovarajuće datoteke potpisa IGM-ova sa repozitorijuma *Alfresco*, a zatim ih skladištio na lokalnom repozitorijumu;

- Zatim su IGM-ovi verifikovani pomoću KSI sistema, tako što ih je operator SCC-a ručno učitavao zajedno sa pripadajućim datotekama potpisa IGM-ova;

- Na kraju se u interfejsu KSI sistema prikazivao status verifikacije pored imena svakog IGM-a.

Nakon završetka procesa verifikacije integriteta IGM-ova, operator SCC-a je koristio EMS-ove IGM-ove i IGM-ove ostalih TSO-a Kontinentalne Evrope da kreira CGM-ove. Provera integriteta CGM-ova svakodnevno je rađena na sledeći način:

- Operator SCC-a je kreirao 24 DACF CGM-a koristeći alat eTNA i prosleđivao ih EMS-u putem EH (u skladu sa postojećom procedurom);

- Nakon toga, operator SCC-a je CGM-ove ručno učitavao u KSI sistem, kako bi on automatski potpisivao učitane CGM-ove i kreirao 24 datoteke potpisa CGM-ova;

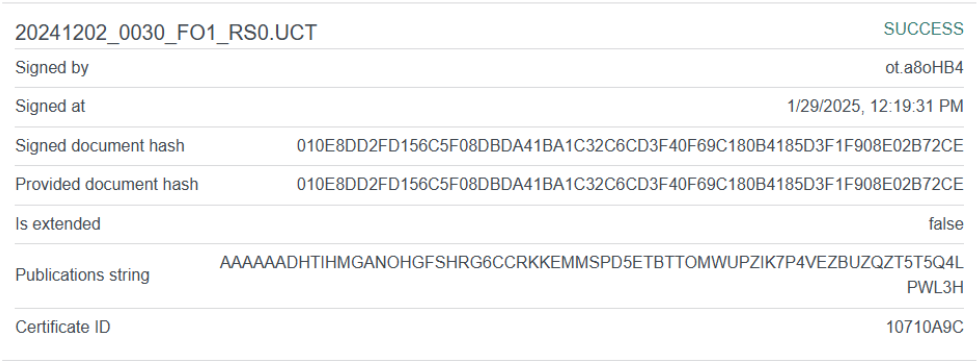
- Po završetku prethodnog koraka, operator SCC-a je preuzimao datoteke potpisa CGM-ova, a zatim ih postavljao na repozitorijum *Alfresco*;

- Operator EMS-a je preuzimao CGM-ove sa EH i odgovarajuće datoteke potpisa CGM-ova sa repozitorijuma *Alfresco*, a zatim ih skladištio na lokalnom repozitorijumu;

- Zatim su CGM-ovi verifikovani pomoću KSI sistema, tako što ih je operator EMS-a ručno učitavao zajedno sa pripadajućim datotekama potpisa CGM-ova;

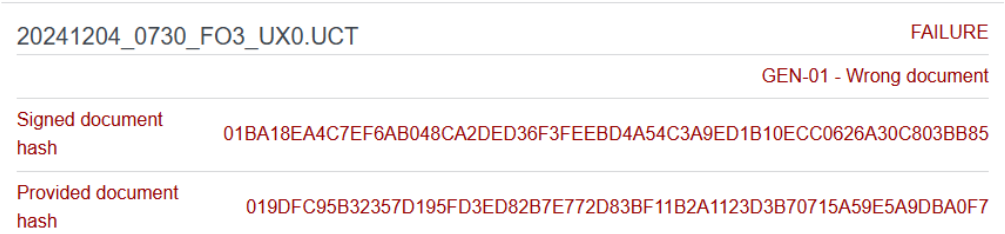
- Na kraju se u interfejsu KSI sistema prikazivao status verifikacije pored imena svakog CGM-a.

Tokom testiranja primene KSI sistema u okviru DACF procesa ukupno je verifikovano nekoliko stotina IGM-ova i CGM-ova, pri čemu su određeni mrežni modeli bili namerno modifikovani da bi se testiralo da li je KSI sistem u stanju da prepozna situacije u kojima je integritet modela ugrožen. U slučajevima kada je status verifikacije uspešan, kao što je prikazano na Slici 6, interfejs KSI sistema prikazuje izveštaj verifikacije u kome se navodi: entitet koji je izvršio potpisivanje, vremenski trenutak potpisivanja, vrednosti *hash*-kodova mrežnog modela i datoteke potpisa, informaciju da nije bilo proširenja, string publikacije i identifikacioni broj sertifikata.




Slika 6: Izveštaj nakon uspešne verifikacije integriteta mrežnog modela

U slučajevima kada je status verifikacije neuspešan, kao što je prikazano na Slici 7, interfejs KSI sistema prikazuje izveštaj verifikacije u kome se navodi: razlog neuspešne verifikacije, kao i vrednosti *hash*-kodova mrežnog modela i datoteke potpisa. Očigledno je da se prilikom modifikacije mrežnog modela promeni njegov *hash*-kod u odnosu na onaj koji je zapisan u datoteci potpisa i da se na osnovu toga može detektovati ugrožavanje integriteta mrežnih modela.




Slika 7: Izveštaj nakon neuspešne verifikacije integriteta mrežnog modela

Ove namerne modifikacije su obuhvatile promene naziva i promene sadržaja datoteke mrežnog modela. Zanimljivo je naglasiti da nakon ispravke greške u mrežnom modelu, dati mrežni model i dalje nije mogao da prođe verifikaciju, bez obzira na to što on u sebi ima iste informacije kao i u trenutku potpisivanja. Razlog tome je što se vreme čuvanja mrežnog modela (zajedno sa ostalim tzv. meta-podacima) koristi prilikom kreiranja *hash*-koda. Zato ispravka modifikacije u okviru mrežnog modela ne pruža povratak integriteta podataka i to KSI sistem odlično detektuje – jednom narušen integritet podataka ostaje trajno narušen bez obzira na ispravku modifikacije. KSI sistem je tokom čitavog perioda testiranja uspešno detektovao sve modifikacije mrežnih modela nakon potpisivanja.

## 5 ZAKLJUČAK

U ovom radu je prikazana integracija KSI sistema u okviru DACF procesa operativnog planiranja rada EES-a, sa ciljem da se omogući provera integriteta mrežnih modela sa aspekta informacione bezbednosti, s obzirom da to nije trenutna praksa u okviru ENTSO-E zajednice. Da bi pomenuto ispitivanje bilo moguće sprovesti izvršena je implementacija KSI sistema u srpsko testno okruženje u okviru R²D² projekta. Na osnovu prikazanih rezultata preliminarne demonstracije KSI sistema u okviru DACF procesa, mogu se izvesti sledeći zaključci [8]:

- KSI sistem je uspešno implementiran u IT okruženje SCC-a;
- KSI sistem je lako integrisan u DACF proces na strani TSO-a i RCC-a;
- Sve ključne funkcionalnosti KSI sistema rade u skladu sa očekivanjima.

Ovo konceptualno testiranje je pokazalo potencijal primene KSI *blockchain* tehnologije u cilju potvrde integriteta mrežnih modela, te se ovo rešenje može primeniti na OPDE platformu koja se koristi za razmenu mrežnih modela u CGMES (*Common Grid Model Exchange Standard*) formatu, tako što se KSI sistem iskoristi za potpisivanje svih mrežnih modela neposredno pre nego što budu objavljeni na OPDE platformi. Na taj način, integritet mrežnih modela bi mogao biti proveren i dokazan u svakom trenutku, što danas nije slučaj.

Sa KSI *blockchain* tehnologijom implementiranom u IT okruženju TSO-a i RCC-a, istorija podataka ne može biti izmenjena od strane bilo koga, a autentičnost mrežnih modela može se matematički dokazati. To znači da niko – ni hakeri, ni sistemski administratori, pa čak ni sami vlasnici mrežnih modela – ne može manipulisati podacima, a da to ostane neprimećeno.

## ZAHVALNICA

Rad je deo *Horizon Europe* projekta R²D² (*Reliability, Resilience and Defense technology for the griD*, ID: 101075714). Ovaj dokument je urađen uz finansijsku pomoć Evropske Unije. Sadržaj ovog dokumenta je isključivo odgovornost autora i ni pod kojim okolnostima se ne može smatrati da odražava stav Evropske Unije.

## LITERATURA

[1] Miroslav Minović, „Blockchain tehnologija: mogućnosti upotrebe izvan kripto valuta“, INFOTECH 2017, Aranđelovac, jun 2017;

[2] Ivan Martinović, Lucas Kello, Ivo Sluganović, „Blockchains for Governmental Services: Design Principles, Applications, and Case Studies“, Oxford University’s Centre for Technology and Global Affairs, Working Paper Series – No. 7, decembar 2017;

[3] Blockchain in Estonia & project PRIVILEDGE H2020, https://northsearegion.eu/media/11757/20191217-guardtime.pdf, 28.03.2025;

[4] Ahto Buldas, Andres Kroonmaa, Risto Laanoja, „Keyless Signatures' Infrastructure: How to Build Global Distributed Hash-Trees“, Cryptology ePrint Archive, 2013/834, decembar 2013;

[5] Keyless Signature Infrastructure – Massive-Scale System Integrity, https://m.guardtime.com/files/KSI_data_sheet_201509-2.pdf, 28.03.2025;

[6] R²D² project consortium, „D5.2 Final Version of the Prevention Systems For Energy Infrastructures Security“, septembar 2024;

[7] R²D² project consortium, „D2.3 Final version of the R2D2 Requirements and Detailed Architecture Design“, januar 2024;

[8] R²D² project consortium, “D7.3 R²D² ecosystem integration and testing”, mart 2025.