Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

DecentraSafe

Decentralizovaná architektúra pre bezpečnú správu a manipuláciu s osobnými dátami

Odborný white paper: výskumné východiská, referenčná architektúra, bezpečnostný model a validačný rámec

Prijímateľ	BS partners, s.r.o.
Kód projektu	17I04-04-V05-00078
Komponent / investícia	Komponent 17 – Digitálne Slovensko, Investícia 4
Obdobie realizácie projektu	01.06.2026 – 31.07.2026
Názov projektu	Decentralizovaná architektúra pre ochranu a manipuláciu s osobnými dátami (DecentraSafe)
Výzva	17I04-04-V05 – Výzva na predkladanie žiadostí o poskytnutie prostriedkov mechanizmu na podporu výskumu a vývoja v oblasti digitálnej transformácie Slovenska 2
Vykonávateľ	Ministerstvo investícií, regionálneho rozvoja a informatizácie SR
Napĺňaný merateľný ukazovateľ	Počet odborných publikácií vytvorených v rámci projektu (vedľajší ukazovateľ; východisková hodnota: 0; plánovaná hodnota: 1)
Miesto zverejnenia	*https://www.bspartners.sk/*

Projekt je financovaný Európskou úniou – NextGenerationEU v rámci Plánu obnovy a odolnosti Slovenskej republiky.

O publikácii a úroveň dôkazov

Táto odborná publikácia predstavuje výskumno-vývojový a diseminačný výstup vytvorený v rámci projektu „Decentralizovaná architektúra pre ochranu a manipuláciu s osobnými dátami“ (DecentraSafe). Systematizuje architektonické princípy, návrhové rozhodnutia, bezpečnostný model, metodické postupy a validačný rámec riešenia rozpracované počas realizácie projektu. Text je koncipovaný ako odborné predstavenie vlastného projektového riešenia, nie ako prehľad alebo kompilácia cudzej odbornej literatúry.

Publikácia je súčasne výstupom, ktorým sa napĺňa vedľajší merateľný ukazovateľ projektu **„Počet odborných publikácií vytvorených v rámci projektu“** (merná jednotka: počet; východisková hodnota: 0; plánovaná hodnota: 1) v zmysle časti Monitoring/reporting schváleného opisu projektu. V súlade s definíciou ukazovateľa ide o záznam o publikačnej činnosti v rámci projektu, pričom ukazovateľ zahŕňa všetky druhy publikácií bez ohľadu na typ dokumentu a pre všetky odbory vedy a techniky. Publikácia zároveň napĺňa komunikačný plán projektu, ktorý predpokladá vypracovanie a zverejnenie odborného white paperu o architektúre riešenia a jeho sprístupnenie v sekcii odborných publikácií na webovom sídle projektu, a je diseminačným výstupom pracovného balíka WP10 – Exploitácia, diseminácia a udržateľnosť. Definícia ukazovateľa vychádza z Prílohy 4 výzvy 17I04-04-V05 – Príklady merateľných ukazovateľov [1].

Bibliografická identifikácia výstupu: vydavateľ – BS partners, s.r.o., Liptovský Mikuláš; rok vydania – 2026; forma a miesto zverejnenia – *https://www.bspartners.sk/*; rozsah – *15 strán*

Dokument je určený odbornej verejnosti, integrátorom, bezpečnostným architektom, prevádzkovateľom digitálnych služieb, organizáciám verejnej správy a subjektom pracujúcim s citlivými údajmi. Zámerne neobsahuje interné prístupové údaje, zdrojové kódy, tajomstvá, produkčné adresy, konfigurácie kľúčov ani údaje, ktoré by mohli znižovať bezpečnosť riešenia. Nejde o právne stanovisko ani o náhradu DPIA, penetračného testu, akceptačného protokolu alebo validačnej správy TRL.

Výkonné zhrnutie

DecentraSafe rieši problém dôveryhodnej, auditovateľnej a regulačne preukázateľnej manipulácie s osobnými a inými citlivými údajmi. Základnou architektonickou tézou je striktné oddelenie dátovej a dôkaznej vrstvy: osobné údaje zostávajú v riadených off-chain úložiskách, zatiaľ čo distribuovaný register uchováva iba kryptografické záväzky, revokačné stavy, časové väzby a ďalšie dôkazné artefakty.

- hybridná DLT architektúra: riadená permissioned vrstva doplnená o nezávislé anchoring ukotvenie do verejnej siete;
- privacy-by-design / privacy-by-default: minimalizácia údajov a zákaz ukladania PII do verejne overiteľnej vrstvy;
- zero-trust prístup: žiadna implicitná dôvera na základe siete, zariadenia alebo vlastníctva; rozhodovanie je viazané na identitu, kontext a politiku;
- PQC-ready kryptografický dizajn s migráciou k štandardizovaným post-kvantovým mechanizmom;
- DID/VC model identity a overiteľných poverení s väzbou na európsky rámec digitálnej identity;
- policy-as-code pre verzované a auditovateľné vynucovanie pravidiel, súhlasov a revokácií;
- Data Vaults pre šifrované off-chain uloženie, CRUD, prenositeľnosť a dôkaznú stopu;
- DevSecOps a observabilita ako prierezové bezpečnostné vrstvy od vývoja po prevádzku.

Abstrakt (SK): Publikácia systematizuje výskumno-vývojové východiská a návrhové výsledky projektu DecentraSafe zameraného na bezpečnú a auditovateľnú správu osobných a citlivých údajov. Metodicky vychádza z design science, experimentálneho vývoja, architektonického modelovania, analýzy hrozieb a dôkazne orientovanej validácie. Navrhovaný model oddeľuje šifrovanú off-chain dátovú vrstvu od distribuovanej dôkaznej vrstvy a integruje digitálnu identitu a overiteľné poverenia, policy-as-code, kryptografickú agilitu, zero-trust, observabilitu a obnovu po havárii. Vlastný odborný prínos spočíva v ich syntéze do modulárnej referenčnej architektúry a v matici sledovateľnosti prepájajúcej výskumné otázky, návrhové artefakty a overovacie dôkazy.

Kľúčové slová: decentralizovaná architektúra; ochrana osobných údajov; technológia distribuovaných registrov (DLT); anchoring; post-kvantová kryptografia; overiteľné poverenia (DID/VC); policy-as-code; zero-trust; GDPR; auditovateľnosť.

Abstract (EN): DecentraSafe presents a modular reference architecture for the trustworthy, auditable and regulation-ready management of personal and sensitive data. Its core design principle is a strict separation of the data layer and the evidence layer: personal data remain in governed off-chain vaults, while a hybrid distributed ledger stores only cryptographic commitments, revocation states and time-bound evidence artefacts, periodically anchored to a public network for independent verifiability. The architecture integrates decentralized identity and verifiable credentials (DID/VC) aligned with the European digital identity framework, policy-as-code enforcement of purposes, consents and revocations, post-quantum-ready cryptographic agility (ML-KEM/ML-DSA), zero-trust access control and DevSecOps-based operational security. The paper defines design invariants, a threat model (STRIDE/LINDDUN), a data life cycle with evidential traceability and a validation framework targeting TRL 6 laboratory integration and TRL 7 validation in a relevant environment, including measurable KPIs. The publication is an expert dissemination output of the DecentraSafe project funded by the European Union – NextGenerationEU under the Recovery and Resilience Plan of the Slovak Republic.

Keywords: decentralized architecture; personal data protection; distributed ledger technology; anchoring; post-quantum cryptography; verifiable credentials; policy-as-code; zero trust; GDPR; auditability.

Výskumný charakter projektu

Schválený projektový rámec kvalifikuje činnosti ako experimentálny vývoj a kombinuje design science, iteratívne prototypovanie, laboratórne benchmarky, formálne testovanie politík a validáciu v relevantnom prostredí s cieľom technologickej pripravenosti TRL 7.

1. Výskumný problém, ciele a metodika

1.1 Výskumný problém

Digitalizácia verejných a súkromných služieb zvyšuje objem a citlivosť dátových tokov, pričom paralelne rastie požiadavka na preukázateľnosť účelu spracovania, integritu záznamov, riadenie oprávnení, prenositeľnosť a schopnosť spätne doložiť rozhodovací kontext. Tradičný centralizovaný model sústreďuje dôveru aj riziko do malej skupiny komponentov a často nedokáže oddeliť ochranu obsahu od nezávislej verifikácie procesov.

1.2 Výskumné otázky

- Ako vytvoriť dôkaznú vrstvu, ktorá umožní nezávislé overenie integrity a časovej následnosti operácií bez uloženia osobných údajov na blockchain?
- Ako spojiť permissioned DLT s verejným anchoringom tak, aby sa vyvážili výkon, súkromie, riadenie a nezávislá overiteľnosť?
- Ako formalizovať účel, súhlas, revokáciu a ďalšie pravidlá spracovania do strojovo vyhodnotiteľných, verzovaných politík?
- Ako navrhnúť kryptografickú agilitu umožňujúcu postupný prechod na post-kvantové algoritmy bez technologického lock-inu?
- Ako prepojiť identitu, dátové úložiská a auditnú stopu tak, aby výsledok bol interoperabilný, prenositeľný a validovateľný v relevantnom prostredí?

1.3 Metodický rámec

Metodika je založená na princípoch experimentálneho vývoja a design science: identifikuje problém, formuluje návrhové požiadavky, vytvára technologický artefakt, iteratívne ho implementuje a overuje prostredníctvom experimentov, integračných testov a pilotných scenárov. Projektový rámec počíta s laboratórnym overovaním, benchmarkmi, simuláciami, property-based testingom, bezpečnostným testovaním a validáciou technologickej pripravenosti. [11]

Fáza	Metóda	Predmet hodnotenia	Typ dôkazu
1. Analýza a modelovanie	STRIDE/LINDDUN, DPIA, architektonické modelovanie	aktíva, hrozby, toky, trust boundaries	model hrozieb, referenčný model, politika
2. Návrh artefaktu	design science, modulárna architektúra	DLT, identity, policy engine, vaulty	architektonický návrh, rozhrania, invariants
3. Experimentálny vývoj	iteratívne prototypovanie, Scrum/DevSecOps	funkčné moduly a integračné toky	build artefakty, testy, pipeline záznamy
4. Laboratórne overenie	benchmarky, test vectors, property-based testing	kryptografia, ZKP, DLT, policy engine	výkonnostné a korektnostné výsledky
5. Integračné overenie	end-to-end scenáre	write/read/revoke/export, issuance/verification	integračné logy a test protokoly
6. Pilotná validácia	TRL metodika, relevantné prostredie	výkon, spoľahlivosť, compliance, UX	validačná správa / akceptačný protokol

1.4 Vlastný odborný prínos a výsledok syntézy

Výsledkom spracovania nie je iba opis jednotlivých technológií, ale konzistentný návrhový rámec, v ktorom sú bezpečnostné, regulačné a prevádzkové požiadavky prevedené na overiteľné architektonické invarianty a dôkazné artefakty. Za vlastný projektový prínos sa považuje najmä:

- model oddelenia chráneného obsahu od kryptograficky overiteľnej dôkaznej vrstvy bez ukladania PII do verejne overiteľného registra;
- zjednotenie identity, účelu spracovania, verzie politiky, rozhodnutia a stavu zdroja do auditovateľného rozhodovacieho kontextu;
- crypto-agile integračný model umožňujúci verzovanie a migráciu klasických a post-kvantových kryptografických profilov;

- prepojenie životného cyklu údajov, súhlasov, revokácií a práv dotknutej osoby s end-to-end dôkaznou stopou;
- dôkazne orientovaný validačný rámec, ktorý ku každému tvrdeniu priraďuje merateľnú otázku, testovací artefakt a akceptačný dôkaz.

2. Architektonické požiadavky a návrhové invarianty

Architektonické rozhodnutia sú odvodené z kombinácie bezpečnostných, regulačných, prevádzkových a interoperabilných požiadaviek. Z pohľadu dôveryhodného systému sú dôležitejšie explicitné invarianty ako konkrétna voľba produktu alebo blockchainovej siete.

Požiadavka	Návrhový invariant	Dôsledok pre implementáciu
Minimalizácia PII	PII sa neukladá do verejnej dôkaznej vrstvy.	Hash/commitment musí byť navrhnutý tak, aby nevytváral jednoduchý identifikátor osoby ani spätne rekonštruovateľný obsah.
Auditovateľnosť	Každá významná operácia má mať časovo a kryptograficky viazanú stopu.	Auditný záznam obsahuje identitu/rolu, účel, verziu politiky, výsledok rozhodnutia a referenciu na dôkaz.
Least privilege	Prístup je udeľovaný na minimálny potrebný rozsah a čas.	Autorizácia sa vyhodnocuje per request; oprávnenia a súhlasy sú revokovateľné.
Kryptografická agilita	Algoritmy a kľúčové schémy musia byť vymeniteľné bez prepisu celej platformy.	Abstrakcia KMS, versioning algoritmov, hybridný klasický + PQC režim.
Ledger agnostic	Dôkazný model nesmie byť viazaný na jedinú DLT sieť.	Abstrakčná vrstva, export dôkazov a validovateľná migrácia medzi sieťami.
Regulačná adaptabilita	Zmena pravidla nemá vyžadovať zmenu základnej architektúry.	Policy-as-code, verzovanie politík, testovateľné rozhodovanie a dôkaz verzie pravidla.
Prevádzková odolnosť	Zlyhanie jednej vrstvy nesmie automaticky kompromitovať obsah ani audit.	Segmentácia zón, oddelené KMS domény, zálohy, DR, observabilita a incident response.

3. Hybridná DLT a kryptografická dôkazná vrstva

3.1 Permissioned register a verejný anchoring

Permissioned ledger poskytuje riadenú prevádzku, definované uzly a predvídateľné pravidlá zápisu. Je vhodný pre interné commitmenty, revokačné stavy a evidenciu súhlasu. Periodické ukotvenie kryptografického súhrnu (napr. Merkle root checkpointu) do verejnej siete dopĺňa nezávislú overiteľnosť bez potreby zverejniť PII alebo interný transakčný kontext.

- ledger transakcia obsahuje dôkazný artefakt alebo odkaz, nie citlivý payload;
- anchoring je časovo oddelený od interných operácií a pracuje so súhrnným kryptografickým záväzkom;
- abstrakcia nad ledgerom umožňuje porovnanie a prípadnú migráciu medzi viacerými sieťami;
- validácia musí overovať finalitu, synchronizáciu, fork/stall správanie, záťaž a správnosť verejného ukotvenia.

3.2 Dôkazné artefakty a ich životný cyklus

Dôkazný artefakt môže reprezentovať hash obsahu, commitment k stavu, identifikátor verzie politiky, časový údaj, revokačný stav alebo kryptografický dôkaz vybranej vlastnosti. Jeho návrh musí chrániť pred koreláciou a nesmie umožňovať jednoduchý slovníkový útok na nízko-entropické osobné údaje. Pri citlivých atribútoch je potrebné používať salting, keyed commitments alebo iné mechanizmy podľa konkrétneho use-case.

Dôležité pre GDPR

> Samotný hash nie je automaticky anonymný údaj. Ak ho možno prepojiť s osobou alebo spätne odvodiť z obmedzeného priestoru vstupov, môže naďalej predstavovať osobný údaj alebo pseudonymizovaný identifikátor. Návrh preto musí posudzovať linkovateľnosť, entropiu a kontext použitia.

4. Post-kvantová pripravenosť a kryptografická agilita

Projektový návrh pracuje s post-kvantovými kryptografickými mechanizmami a s hybridným prechodovým modelom kombinujúcim klasickú a post-kvantovú kryptografiu. Kľúčovým návrhovým princípom je kryptografická agilita: kryptografické profily, algoritmy a parametre nesmú byť pevne previazané s aplikačnou logikou, aby ich bolo možné počas životného cyklu riešenia bezpečne meniť bez zásadnej zmeny celej architektúry. [9], [10]

Oblasť	Odporúčaný návrhový princíp	Validačné otázky
Výmena kľúčov / KEM	hybridné spojenie klasického mechanizmu a ML-KEM podľa rizikového profilu	latencia, veľkosť ciphertextu/kľúčov, kompatibilita, failure handling
Digitálne podpisy	algoritmická verzovateľnosť; podpora klasického podpisu a ML-DSA podľa profilu	veľkosť podpisu, výkon, rotácia, dlhodobá verifikácia
KMS/HSM	abstrakcia kľúčového backendu, oddelené domény a politická kontrola exportu	backup/restore, audit kľúčových operácií, separation of duties
Crypto inventory	evidencia algoritmov, kľúčov, verzií a závislostí v softvérovej dodávke	schopnosť identifikovať a nahradiť algoritmus bez redesignu celého systému
Migrácia	verzované dôkazy a metadáta identifikujú použité algoritmy	overiteľnosť historických záznamov po zmene kryptografického profilu

5. Referenčná architektúra a hranice dôvery

Referenčná architektúra je vrstvená tak, aby sa oddelila identita, autorizácia, dátová vrstva, dôkazná vrstva a prevádzková observabilita. Kľúčovou vlastnosťou je, že žiadna jednotlivá vrstva nemá sama o sebe neobmedzenú dôveru ani úplný kontext. Bezpečnostné rozhodnutie vzniká kombináciou identity, politiky, účelu spracovania a stavu chráneného zdroja.

Klienti a integračné systémy	Používateľské aplikácie, EUDI/VC peňaženky, integrační partneri	Externá zóna / nedôveryhodný vstup
Access Gateway & Orchestration	API gateway, policy enforcement point, OPA/Rego, event bus, REST/gRPC/webhook integrácie	Kontrolný bod pre identitu, autorizáciu, rate limiting a routing
Identity & Verifiable Credentials	DID registry/resolver, issuer/verifier, credential status, SDK/peňaženka	Dôveryhodnosť identity a atribútov
Consent & Policy Engine	Policy-as-code, účelové obmedzenia, súhlasy, revokácie, verzie pravidiel	Rozhodovacia vrstva – povoľuje/odmieta operáciu
Data Vaults & Secure Processing	Šifrované off-chain úložiská, CRUD, export, portability, erasure/update workflow	Primárna zóna osobných a citlivých údajov
Core Ledger & Anchoring	Permissioned register, commitmenty, revokačné registre, periodické verejné anchory	Dôkazná vrstva bez PII; integrita a časová následnosť
Observability & Audit	Kryptograficky viazané logy, SIEM, metriky, audit board	Kontrolná a auditná rovina
DevSecOps, KMS a infraštruktúra	CI/CD, IaC, GitOps, SAST/DAST, KMS/HSM domény, Kubernetes/on-prem/EU cloud	Prierezová bezpečnostná a prevádzková rovina

Obr. 1 – Logické vrstvy referenčnej architektúry DecentraSafe a ich bezpečnostná úloha.

Referenčná architektúra je v projektovej dokumentácii rozpracovaná aj vo forme štruktúrovaného architektonického modelu C4 (úrovne L2–L3). Dôkaznú vrstvu dopĺňa transakčný prehliadač (TX Viewer), ktorý umožňuje vyhľadávanie, filtrovanie a nezávislú verifikáciu transakcií vrátane vizualizácie blokov, read/write množín a identifikácie iniciátora operácie; audit podporuje samostatný audit dashboard s exportom dôkaznej stopy pre interné aj externé kontroly.

6. Dátový životný cyklus a dôkazná stopa

Návrh oddeluje obsah spracúvaného údaja od dôkazu o tom, že operácia prebehla za definovaných podmienok. V typickom end-to-end toku sa preto neukladá osobný údaj do distribuovaného registra; ledger obsahuje iba kryptografický záväzok alebo iný overiteľný artefakt.

1. Autentizácia subjektu a zariadenia; získanie kontextu identity a relevantných atribútov.
2. Vyhodnotenie účelu, právneho/procesného základu a aktuálnej verzie politiky v Consent & Policy Engine.
3. Autorizácia operácie na princípe least privilege; vytvorenie rozhodnutia policy enforcement pointom.
4. Vykonanie operácie nad Data Vaultom (write/read/update/revoke/export) bez prenášania PII do ledgeru.
5. Vytvorenie kryptografického dôkazu/commitmentu a auditného záznamu viazaného na identitu, čas a verziu politiky.
6. Zapísanie dôkazného artefaktu do permissioned ledgeru a podľa politiky periodické anchoring ukotvenie checkpointu do verejnej siete.
7. Sprístupnenie auditovateľného pohľadu oprávnenému kontrolórovi bez potreby plošného prístupu k chránenému obsahu.

> **Bezpečnostný invariant**
>
> Obsah PII zostáva v kontrolovanom off-chain prostredí. Verejná alebo zdieľaná dôkazná vrstva nesmie obsahovať údaje, z ktorých je možné priamo alebo nepriamo rekonštruovať osobný údaj bez dodatočných oprávnení a kontextu.

7. Identita, Verifiable Credentials a európska interoperabilita

Identitná vrstva oddeľuje identifikáciu subjektu od rozhodovania o oprávnení. DID registry/resolver poskytuje mechanizmus práce s decentralizovanými identifikátormi; issuer/verifier služby podporujú životný cyklus overiteľných poverení. Návrh je koncipovaný na interoperabilitu s otvorenými modelmi decentralizovanej identity a overiteľných poverení a zároveň s európskym ekosystémom digitálnej identity, tak ako to predpokladá schválený projektový rámec. [6], [7]

Rola	Zodpovednosť	Bezpečnostná kontrola
Issuer	vydáva overiteľné tvrdenie/credential	autentizácia vydavateľa, podpis, politika vydania, revokácia/status
Holder	drží a prezentuje credential	ochrana peňaženky, minimal disclosure, používateľská kontrola
Verifier	overuje credential a jeho status	validácia podpisu, issuer trust, časová platnosť, revokácia, policy rozhodnutie
Resolver / registry	sprístupňuje technické údaje potrebné pre riešenie DID	integrita dokumentu, cache politika, ochrana pred spoofingom
Policy engine	rozhoduje, či je credential/atribút dostatočný pre operáciu	least privilege, purpose binding, verziovanie a audit rozhodnutia

> **Minimal disclosure**
> Overiteľné poverenie nemá byť dôvodom na nadmerné zhromažďovanie atribútov. Pri návrhu prezentačných tokov je potrebné minimalizovať rozsah zdieľaných tvrdení a oddeliť autentizáciu od dokazovania konkrétnej vlastnosti.

8. Consent & Policy Engine: regulačné pravidlá ako vykonateľný artefakt

Policy-as-code transformuje pravidlá z textovej dokumentácie do strojovo vyhodnotiteľnej, verzovanej a testovateľnej formy. V DecentraSafe má policy engine vyhodnocovať nielen rolu používateľa, ale aj účel spracovania, právny/procesný základ, časové obmedzenie, stav súhlasu, citlivosť údajov a kontext operácie.

- každé rozhodnutie musí byť spätne priraditeľné ku konkrétnej verzii politiky;
- revokácia súhlasu alebo credentialu musí mať definovaný účinok na budúce operácie a auditnú stopu;
- konflikty pravidiel a edge cases (retencia, účel, delegácia, núdzový prístup) majú byť pokryté testami;
- property-based testing je vhodné na hľadanie nekonzistentných kombinácií vstupov a pravidiel;
- policy engine nemá nahrádzať právne posúdenie; vykonáva formalizované pravidlá, ktorých obsah musí byť schválený zodpovednou rolou.

8.1 Príklad rozhodovacieho kontextu

Vstup	Príklad	Dôkaz v auditnej stope
Subjekt	DID / enterprise identity / služobný účet	identifikátor a overený autentizačný kontext
Atribúty	rola, profesijné oprávnenie, credential status	overený issuer, čas platnosti, status
Účel	napr. vybavenie žiadosti o prístup k údajom	policy ID + purpose code
Zdroj	konkrétny Data Vault / dátová kategória	resource ID bez PII v zdieľanej vrstve
Operácia	read / update / export / revoke	request ID a výsledok policy rozhodnutia
Čas a prostredie	čas, zariadenie, bezpečnostný posture	timestamp, device/service claims podľa politiky

9. Data Vaults, práva dotknutej osoby a bezpečné spracovanie

Data Vault predstavuje kontrolované off-chain úložisko, v ktorom zostáva samotný obsah osobných a citlivých údajov. Dôkazná vrstva eviduje iba overiteľné artefakty a časové väzby. Tento model podporuje realizáciu životného cyklu údajov bez konfliktu s požiadavkou na nemennosť verejného registra.

Operácia	Kontroly pred vykonaním	Výstup / dôkaz
Create / Write	identita, účel, politika, klasifikácia dát, KMS kontext	šifrovaný stav + commitment/hash + audit event
Read	least privilege, aktuálny súhlas/credential, kontext zariadenia/služby	kontrolovaný prístup + audit event bez zverejnenia obsahu
Update / Rectification	oprávnenie na opravu, väzba na pôvodný stav	nový stav + dôkaz nadväznosti; historická auditná stopa
Erase	právny základ výmazu, retenčné výnimky, schválený workflow	zmazanie/crypto-erasure v dátovej vrstve + dôkaz vykonania
Export / Portability	overenie identity, rozsahu a formátu exportu	prenositeľný balík + manifest + dôkaz integrity

Operácia	Kontroly pred vykonaním	Výstup / dôkaz
Revoke	stav súhlasu/credentialu/prístupu	revokačný záznam a okamžitá zmena budúcich policy rozhodnutí

Nemennosť ≠ nemožnosť výmazu

Nemenná dôkazná stopa nemá obsahovať osobné dáta. Výmaz sa vykonáva v off-chain dátovej vrstve; ledger môže zachovať iba minimálny dôkaz, že riadený proces prebehol, pričom návrh musí zabrániť tomu, aby tento dôkaz sám obsahoval alebo odhaľoval PII.

10. Access Gateway, observabilita a DevSecOps

10.1 Access Gateway & Orchestration

Gateway tvorí centrálny policy enforcement point pre externé a medzislužbové požiadavky. Jeho úlohou je oddeliť autentizáciu, autorizáciu, smerovanie, rate limiting, validáciu vstupov a servisnú observabilitu od aplikačnej logiky jednotlivých modulov. Projektový opis počíta s API bránami, OPA/Rego, event busom a integračnými konektormi REST/gRPC/webhook.

10.2 Observability & Audit

Auditná rovina musí byť schopná rekonštruovať bezpečnostne významnú udalosť bez plošného prístupu k PII. Kryptograficky viazané logy, SIEM, metriky a audit board majú podporovať interný audit, forenznú analýzu, incident response a preukazovanie konzistencie dôkaznej stopy.

10.3 DevSecOps a dodávateľský reťazec

- CI/CD s bezpečnostnými kontrolami pred nasadením a oddelením stage/prod prostredí; [12]
- Infrastructure as Code a GitOps pre reprodukovateľnosť a audit konfigurácie;
- SAST/DAST, fuzzing a penetračné testovanie ako komplementárne techniky;
- kontrola závislostí a softvérového dodávateľského reťazca; požadovaný projektový rámec pracuje aj s konceptom SLSA;
- segmentácia siete, network policies, kontrola egressu a oddelené KMS domény;
- zálohovanie, disaster recovery, RPO/RTO rehearsals a incident response playbooky.

11. Hrozbový model a bezpečnostné mitigácie

Schválený projektový opis predpokladá využitie STRIDE a LINDDUN. Nasledujúca tabuľka uvádza reprezentatívny odborný hrozbový model pre referenčnú architektúru; nejde o náhradu konkrétneho threat registeru alebo penetračného testu produkčnej implementácie.

Kategória	Príklad hrozby	Primárna mitigácia	Overenie
Spoofing / Identifiability	falšovanie identity alebo zneužitie credentialu	MFA/strong auth, DID/VC verifikácia, device/service identity, krátkodobé tokeny	negatívne autentizačné testy, credential status/revocation test
Tampering	zmena auditnej stopy alebo commitmentu	kryptograficky viazané logy, podpisy, ledger anchoring	integrity test, pokus o modifikáciu a re-verifikáciu
Repudiation	spochybnenie vykonanej operácie	časová stopa, policy version, actor/context binding	replay a audit reconstruction
Information disclosure	únik PII cez ledger, logy alebo metadáta	on/off-chain separácia, data minimization, redakcia logov, šifrovanie	privacy review, log inspection, LINDDUN test cases

Kategória	Príklad hrozby	Primárna mitigácia	Overenie
Denial of Service	zahltenie API, DLT alebo policy engine	rate limiting, circuit breaker, horizontálne škálovanie, queueing	load/stress test, chaos-security
Elevation of privilege	obídenie policy engine alebo nadmerné oprávnenie	least privilege, policy enforcement at gateway and service, separation of duties	authorization matrix test, policy bypass attempts
Linkability / Detectability	korelácia transakcií a identifikácia subjektu z metadát	rotácia identifikátorov, minimal metadata, batching/anchoring, selective disclosure	privacy threat modeling, correlation analysis
Non-compliance	nesúlad spracovania s účelom/retenciou	policy-as-code, verzovanie, schvaľovanie pravidiel, DPIA	property-based tests, audit sample, compliance review

12. Validačný rámec a technologická pripravenosť

Cieľom validačného rámca je preukázať nielen funkčnosť jednotlivých modulov, ale aj ich bezpečnostnú konzistenciu a prevádzkovú pripravenosť v integračných a pilotných scenároch. Projektový opis uvádza TRL 6 pre integrovaný prototyp v laboratórnom prostredí a TRL 7 pre validáciu v relevantných prevádzkových podmienkach.

Akceptačný rámec zmluvného výskumu a vývoja v projekte viaže dodávku integrovaného prototypu na preukázanie minimálne TRL 6 v laboratórnom/pilotnom prostredí (východisková úroveň TRL 4), s definovanými akceptačnými ukazovateľmi: 100 % auditovateľnosť relevantných transakcií v demonštračnom scenári, latencia API nad dátovým trezorom p95 ≤ 500 ms v laboratórnom prostredí a RTO ≤ 30 minút v disaster-recovery scenári. Cieľové prevádzkové KPI projektu uvedené v časti 12.2 na tieto akceptačné prahy nadväzujú a predstavujú prísnejšie hodnoty pre relevantné prevádzkové prostredie. Ambiciózna cieľová hodnota a minimálny akceptačný prah pritom nie sú zameniteľné.

12.1 Validačné domény

Doména	Metrika / otázka	Cieľový charakter dôkazu
Kryptografia	test vectors, latencia, veľkosť kľúčov/podpisov, rotácia	reprodukovateľný benchmark + konfiguračný profil
ZKP	korektnosť, veľkosť dôkazu, čas generovania/overenia	PoC test cases + performance log
Policy engine	konflikty pravidiel, edge cases, purpose/retention	property-based tests + rozhodovacie traces
DLT	finalita, synchronizácia, fork/stall, verejné anchoring overenie	load/fault test + nezávislá verifikácia anchoru
GDPR workflow	prístup, oprava, výmaz, prenosnosť	end-to-end scenár + časová a dôkazná stopa
Bezpečnosť	SAST/DAST/fuzz, pen-test, threat model	security report + remediation evidence
Výkon	p50/p95 latencia, throughput, dostupnosť	monitorované testovacie obdobie + dashboard export
Prevádzka	RPO/RTO, backup/restore, incident response	DR rehearsal + incident exercise report

12.2 Cieľové KPI podľa schváleného projektového rámca

KPI	Cieľová hodnota / smer	Účel
Preukázanie integrity a právneho základu	z hodín/dní na minúty	automatizovať zber a prezentáciu dôkaznej stopy
Čas GDPR žiadostí	−40 % oproti baseline	zrýchliť access / portability / deletion workflow
Náklady compliance/audit	−30 až −50 %	obmedziť manuálne dokazovanie a konsolidáciu logov

KPI	Cieľová hodnota / smer	Účel
Dostupnosť core API	≥ 99,9 %	prevádzková spoľahlivosť
p95 latencia čítania	≤ 200 ms	reakčný čas kritického API
Úspešné ZK overenia povinnej politiky	≥ 95 % príslušných transakcií	spoľahlivosť dokazovania policy podmienok
Ledger-agnostic portability	verifikovateľná migrácia dôkazov medzi min. 2 sieťami	eliminácia vendor/ledger lock-in

12.3 Matica sledovateľnosti výskumných otázok a dôkazov

Výskumná otázka	Návrhový výsledok	Overovací dôkaz	Väzba na míľnik
RQ1: dôkaz bez PII na DLT	on-chain/off-chain model a pravidlá minimalizácie	architektonický model, threat model, kontrola obsahu ledgeru	M1–M3
RQ2: permissioned vrstva a verejné ukotvenie	hybridný dôkazný model a anchor checkpoint	verifikácia finality, synchronizácie a verejnej kotvy	M2–M3
RQ3: účel, súhlas a revokácia	verzované policy-as-code rozhodovanie	policy testy, decision traces a audit GDPR tokov	M5, M7
RQ4: kryptografická agilita	verzované klasické/PQC profily a KMS/HSM abstrakcia	test vectors, benchmark, rotácia a inventár algoritmov	M9
RQ5: identita, vault a audit	integrovaný CRUD/revoke/export tok	end-to-end protokoly, audit export a validačná správa	M4, M6–M7, M10

Táto matica je odbornou mapou dôkazov.

13. Regulačná a štandardizačná interoperabilita

Regulačný súlad je v DecentraSafe chápaný ako architektonická vlastnosť podporujúca preukázateľnosť, nie ako automatická právna garancia. Technický systém môže uľahčiť dôkaz o účele, súhlase, revokácii, prístupe a integrite, no právny základ a organizačná zodpovednosť zostávajú na prevádzkovateľovi a príslušných rolách.

Rámec / štandard	Relevantná téma	Architektonická väzba
GDPR – nariadenie (EÚ) 2016/679 [2]	minimalizácia, účel, práva dotknutej osoby, accountability	off-chain PII, purpose binding, policy-as-code, audit trail, export/erase workflow
Európsky rámec digitálnej identity – nariadenie (EÚ) 2024/1183 [3]	EUDI Wallet, dôveryhodná digitálna identita	DID/VC interoperabilita, issuer/verifier, credential lifecycle
W3C DID Core 1.0 [6]	decentralizované identifikátory a resolution model	DID registry/resolver a abstrakcia identitnej vrstvy
W3C Verifiable Credentials Data Model 2.0 [7]	privacy-respecting machine-verifiable credentials	issuer/holder/verifier model, status/revocation, selective disclosure kontext
NIST SP 800-207 [8]	zero trust architecture	per-request authN/authZ, resource-centric security, explicit trust decisions
NIST FIPS 203 / FIPS 204 [9], [10]	ML-KEM / ML-DSA post-kvantové štandardy	PQC-ready kryptografická agilita a hybridný prechod
OECD Frascati Manual 2015 [11]	výskum a experimentálny vývoj	metodické vymedzenie experimentálneho vývoja a tvorby nových aplikácií poznatkov
MiCA – nariadenie (EÚ) 2023/1114 [4]	trhy s kryptoaktívami, dôveryhodnosť a transparentnosť služieb založených na DLT	compliance matica riešenia voči GDPR a MiCA; dôkazná DLT vrstva bez tokenizácie osobných údajov

Rámec / štandard	Relevantná téma	Architektonická väzba
NIS 2 – smernica (EÚ) 2022/2555 [5]	kybernetická bezpečnosť sietí a informačných systémov	zero-trust segmentácia, riadenie zraniteľností a incidentov, observabilita a auditná stopa

14. Referenčné scenáre nasadenia

14.1 Verejná správa

V prostredí verejnej správy je jadrom scenára dôveryhodná evidencia prístupu k údajom občana, účelovo viazané zdieľanie medzi inštitúciami a schopnosť spätne doložiť, na základe akej identity, politiky a právneho/procesného kontextu bola operácia povolená. Verejný anchoring môže poskytnúť nezávislý časový dôkaz bez zverejnenia obsahu registra.

14.2 Finančné služby

Finančný scenár pracuje s overiteľnou identitou klienta, riadeným prístupom k citlivým dokumentom a auditovateľnou výmenou údajov medzi subjektmi. Policy engine môže formalizovať účelové a rolové obmedzenia; credentialy môžu reprezentovať overené atribúty bez potreby kopírovať celý zdrojový dokument.

14.3 Zdravotníctvo

Zdravotnícke nasadenie vyžaduje zvlášť prísne oddelenie identity, oprávnenia a dátovej vrstvy. Vhodné sú časovo a účelovo viazané oprávnenia, audit prístupov, selektívne zdieľanie atribútov a technické mechanizmy na okamžitú revokáciu. Každé konkrétne nasadenie musí mať vlastný právny základ, DPIA a analýzu interoperability s doménovými štandardmi.

14.4 MSP a modulárne zavedenie

Modulárna architektúra umožňuje zavádzať len vybrané komponenty – napríklad Consent Engine, Data Vault alebo auditnú vrstvu – bez nutnosti nasadiť celý ekosystém. Tento prístup znižuje integračné riziko a podporuje postupnú migráciu z existujúcich systémov.

15. Riziká, obmedzenia a otvorené výskumné otázky

Technologická ambícia projektu prináša aj limity, ktoré musia byť explicitne riadené. Profesionálna interpretácia výsledkov preto vyžaduje odlíšiť architektonickú vhodnosť od produkčnej pripravenosti a od právnej akceptácie konkrétneho nasadenia.

Riziko / limit	Dopad	Mitigácia v projektovom návrhu
Regulačný vývoj	potreba meniť pravidlá, credential profily alebo prevádzkové procesy	modulárny policy-as-code, verzovanie a oddelenie pravidiel od jadra architektúry
PQC vývoj a implementačné chyby	výkonové náklady, kryptografická migrácia, riziko nesprávneho profilu	hybridný režim, crypto-agility, test vectors, benchmarky, key inventory
DLT škálovateľnosť a finalita	latencia, dostupnosť, náklady, fork/stall situácie	permissioned jadro, abstrakčná vrstva, multi-ledger anchoring, load/fault testy
Metadátové privacy riziká	linkovateľnosť používateľov aj bez priameho PII	minimal metadata, batching, rotácia identifikátorov, LINDDUN analýza
Zložitosť ZKP	výkon, implementačná náročnosť, auditovateľnosť	selektívna aplikácia len na use-cases s jasnou pridanou hodnotou
Nedostatok expertov	riziko prevádzkovej závislosti od malej skupiny ľudí	dokumentované API, interné know-how, partnerstvá, tréningy

Riziko / limit	Dopad	Mitigácia v projektovom návrhu
Adopcia používateľov	zložité consent/identity flows môžu znižovať použiteľnosť	jasné consent journeys, UX testovanie, postupná adopcia
Dôkaz TRL	white paper sám osebe nepreukazuje TRL 7	samostatná validačná správa, pilotné protokoly, akceptačné a bezpečnostné dôkazy

16. Väzba na pracovné balíky a míľniky projektu

Publikácia nadväzuje na štruktúru pracovných balíkov WP1–WP10 schváleného opisu projektu a systematizuje odborné poznatky rozpracované v ich rámci; jej vypracovanie a zverejnenie je súčasťou diseminačných aktivít pracovného balíka WP10 a komunikačného plánu projektu.

WP	Oblasť	Priamy výstup / míľnik
WP1	Architektúra, bezpečnostný dizajn a compliance	referenčný model, DPIA, STRIDE/LINDDUN, policy model; schválený architektonický a compliance návrh
WP2	Core Ledger & Anchoring	prevádzkovaný permissioned ledger; prvé úspešné anchory do verejnej siete
WP3	Identity & VC	DID registry/resolver, issuer/verifier, peňaženka/SDK; end-to-end issuance/verification flow
WP4	Consent & Policy Engine	policy-as-code, vynucovanie, revokácie, MVP GDPR politiky a dôkazné artefakty
WP5	Data Vaults & Secure Processing	šifrované vaulty, CRUD s dôkazmi, audit trail, export/portability
WP6	Access Gateway & Orchestration	API brány, event bus, konektory; integrované write/read/revoke/export toky
WP7	Observability & Audit	kryptograficky viazané logy, SIEM, metriky, audit board
WP8	DevSecOps & Hardening	CI/CD, IaC, GitOps, SAST/DAST, pen-testy, bezpečnostný release candidate
WP9	Pilotná validácia a TRL overenie	pilotná validácia v dvoch sektoroch; cieľ TRL 7
WP10	Exploitácia, diseminácia a udržateľnosť	go-to-market balík, SLA, roadmapa, správa o dopade a udržateľnosti

17. Záver

DecentraSafe predstavuje výskumno-vývojový rámec pre dôveryhodnú správu osobných a citlivých údajov, v ktorom je bezpečnosť postavená na oddelení dátovej a dôkaznej vrstvy, explicitnom riadení dôvery a kryptografickej preukázateľnosti. Odborná hodnota návrhu spočíva najmä v integrácii hybridného DLT, identity a Verifiable Credentials, policy-as-code, Data Vaults, zero-trust a PQC-ready kryptografickej agility do jedného modulárneho referenčného modelu.

Z pohľadu ďalšieho rozvoja je rozhodujúce, aby architektonické tvrdenia boli doplnené o reprodukovateľné validačné dôkazy: testovacie protokoly, bezpečnostné reporty, benchmarky, pilotné scenáre a dokumentované výsledky TRL overenia. Takýto dôkazný prístup je v súlade so samotnou filozofiou DecentraSafe – dôveryhodnosť nemá byť deklarovaná, ale overiteľná.

18. Normatívne zdroje

Uvedené pramene predstavujú regulačné, štandardizačné a metodické rámce, voči ktorým bolo projektové riešenie navrhované a validované, ako aj dokumenty preukazujúce projektový a evidenčný kontext publikácie; nejde o zdroj samotného výsledného riešenia.

[1] MIRRI SR (2025). Príloha 4 výzvy 17I04-04-V05 – Príklady merateľných ukazovateľov. Dostupné na: https://mirri.gov.sk/wp-content/uploads/2025/08/4_VYZVA_17I04-04-V05_RIS3_Priloha-4-vyzvy_Priklady-meratelnych-ukazovatelov.pdf

[2] Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (všeobecné nariadenie o ochrane údajov, GDPR). https://eur-lex.europa.eu/eli/reg/2016/679/oj

[3] Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1183 z 11. apríla 2024, ktorým sa mení nariadenie (EÚ) č. 910/2014, pokiaľ ide o vytvorenie európskeho rámca digitálnej identity. https://eur-lex.europa.eu/eli/reg/2024/1183/oj

[4] Nariadenie Európskeho parlamentu a Rady (EÚ) 2023/1114 z 31. mája 2023 o trhoch s kryptoaktívami (MiCA). https://eur-lex.europa.eu/eli/reg/2023/1114/oj

[5] Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii (NIS 2). https://eur-lex.europa.eu/eli/dir/2022/2555/oj

[6] W3C (2022). Decentralized Identifiers (DIDs) v1.0. W3C Recommendation, 19 July 2022. https://www.w3.org/TR/did-core/

[7] W3C (2025). Verifiable Credentials Data Model v2.0. W3C Recommendation, 15 May 2025. https://www.w3.org/TR/vc-data-model-2.0/

[8] NIST (2020). Special Publication 800-207: Zero Trust Architecture. https://doi.org/10.6028/NIST.SP.800-207

[9] NIST (2024). FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM). https://doi.org/10.6028/NIST.FIPS.203

[10] NIST (2024). FIPS 204: Module-Lattice-Based Digital Signature Standard (ML-DSA). https://doi.org/10.6028/NIST.FIPS.204

[11] OECD (2015). Frascati Manual 2015: Guidelines for Collecting and Reporting Data on Research and Experimental Development. OECD Publishing. https://doi.org/10.1787/9789264239012-en

[12] NIST (2022). Special Publication 800-218: Secure Software Development Framework (SSDF), Version 1.1. https://doi.org/10.6028/NIST.SP.800-218

[13] Opis projektu „Decentralizovaná architektúra pre ochranu a manipuláciu s osobnými dátami“ (DecentraSafe), kód projektu 17I04-04-V05-00078, výzva 17I04-04-V05, Plán obnovy a odolnosti SR, Komponent 17 – Digitálne Slovensko, Investícia 4 (Príloha č. 2 zmluvy o poskytnutí prostriedkov mechanizmu).

Príloha A – Slovník odborných pojmov

Pojem	Význam v kontexte publikácie
DLT	Distributed Ledger Technology – technológia distribuovaných registrov.
Permissioned ledger	Distribuovaný register s riadeným prístupom a definovanými prevádzkovateľmi uzlov.
Anchoring	Ukotvenie kryptografického súhrnu/checkpointu do inej siete na účely nezávislej overiteľnosti.
Commitment	Kryptografický záväzok k hodnote alebo stavu, ktorý umožňuje neskoršie overenie bez zverejnenia pôvodného obsahu.
DID	Decentralized Identifier – decentralizovaný identifikátor podľa W3C modelu.
VC	Verifiable Credential – kryptograficky overiteľné digitálne poverenie.
PQC	Post-Quantum Cryptography – kryptografia navrhnutá s ohľadom na odolnosť voči útokom využívajúcim kvantový počítač.
ML-KEM / ML-DSA	NIST štandardizované post-kvantové mechanizmy pre zapuzdrenie kľúčov a digitálne podpisy.
ZKP	Zero-Knowledge Proof – dôkaz umožňujúci preukázať tvrdenie bez odhalenia podkladovej citlivej informácie.
Policy-as-code	Pravidlá vyjadrené v strojovo vyhodnotiteľnej, verzovanej a testovateľnej forme.
Data Vault	Riadené šifrované off-chain úložisko pre citlivé údaje.
TRL	Technology Readiness Level – úroveň technologickej pripravenosti.
RPO/RTO	Recovery Point Objective / Recovery Time Objective – cieľ obnovy dát a cieľ času obnovy služby.

Vyhlásenie k odbornému výstupu a odporúčaná citácia

Publikácia je spracovaná ako odborný výstup projektu DecentraSafe a prezentuje vlastné architektonické, bezpečnostné a metodické riešenia rozpracované v rámci jeho realizácie. Odkazy na regulačné, identitné alebo kryptografické rámce uvedené v texte predstavujú požiadavky interoperability, bezpečnosti a regulačného prostredia, voči ktorým bolo projektové riešenie navrhované; nejde o zdroj samotného výsledného riešenia. Verejná verzia zámerne neobsahuje dôverné technické konfigurácie, zdrojové kódy ani interné bezpečnostné údaje. Cieľové KPI a úroveň technologickej pripravenosti je potrebné vyhodnocovať spolu so samostatnými projektovými validačnými a testovacími artefaktmi.

Odporúčaná citácia

BS partners, s.r.o. (2026). DecentraSafe – Decentralizovaná architektúra pre bezpečnú správu a manipuláciu s osobnými dátami. Odborný white paper: výskumné východiská, referenčná architektúra, bezpečnostný model a validačný rámec. Liptovský Mikuláš.