DOCUMENTO ISTITUZIONALE — USO RISERVATO

T.T.H.C. OÜ

Sovereign Critical Systems Engineering · Tallinn, Estonia

DOSSIER ISTITUZIONALE

DOSSIER AEGIS-1

Infrastruttura di Autenticazione Forte e Tracciabilità Forense per il Settore Finanziario Europeo

DATA PUBBLICAZIONE	VERSIONE	REGISTRIKOOD	SEDE LEGALE
27 Giugno 2026	2.0	17487615	Tallinn, Estonia

Regolamento (UE) 2022/2554 – DORA Compliant

DOSSIER ISTITUZIONALE AEGIS-1

Infrastruttura di Autenticazione Forte e Tracciabilità Forense per il Settore Finanziario Europeo

---

DISCLAIMER — DA LEGGERE PRIMA DELLA CONSULTAZIONE

AEGIS-1 è un moderno sistema informatico che unisce armoniosamente logica e materia. AEGIS-1 è sistema di autenticazione forte con generazione di token transazionali asincroni progettato per operare come **layer di accesso edge** all'infrastruttura bancaria.

Il sistema AEGIS-1, ad oggi, non sostituisce i sistemi di core banking ma si configura come un **componente di sicurezza perimetrale** specializzato nella: - **Autenticazione dell'utente** all'ingresso dell'APP bancaria; - **Attestazione dell'innesco umano cosciente** di ogni accesso; - **Generazione di token deterministici** senza memorizzazione di PII; - **Fornitura di un audit trail immutabile** per fini forensi e di compliance.

Il sistema AEGIS-1 è progettato per operare **a monte** dei sistemi bancari legacy e, agendo come un componente di sicurezza aggiuntivo, permette di soddisfare i requisiti più critici del Regolamento (UE) 2022/2554 (DORA). A puro titolo esemplificativo e non limitativo si evidenzia il soddisfacimento dell'art. 6 paragrafo 4 "requisito di indipendenza" tramite una segregazione ontologica necessaria per impedire il conflitto di interessi tra controllore e controllato.

INFORMAZIONI SOCIETARIE

Campo	Dettaglio
Ragione Sociale	T.T.H.C. OÜ – Sovereign Critical Systems Engineering
Forma Giuridica	Osaühing (Società a responsabilità limitata, Estonia)
Registrikood	17487615
Sede Legale	Tallinn, Estonia
Registro Imprese	Centro Registri e Sistemi Informativi dell'Estonia (registrikood.e-rik.ee)
Data Pubblicazione Documento	27 giugno 2026
Versione	2.0
Classificazione	Documento Istituzionale – Organi di Vigilanza, Management Body, Funzioni di Compliance e ICT

1. EXECUTIVE SUMMARY

AEGIS-1 è un'infrastruttura tecnica progettata per operare come **layer di autenticazione forte** a supporto delle applicazioni bancarie e finanziarie. Il sistema si posiziona come componente perimetrale (edge authentication layer) che certifica e garantisce il presidio e il rafforzamento del processo di autenticazione e la tracciabilità forense degli accessi.

1.1 Posizionamento

AEGIS-1 interviene esclusivamente nel dominio dell'**autenticazione forte** (Strong Customer Authentication – SCA) e della **generazione di evidenze crittografiche** associate agli eventi di accesso. Il perimetro funzionale è attivo come segue: - **Incluso**: autenticazione a più fattori basata su hardware root-of-trust, generazione di token transazionali asincroni, logging forense strutturato (WORM), reportistica automatica di conformità. - **Escluso**: gestione delle identità (IAM), definizione dei privilegi di accesso, crittografia dei dati a riposo nei sistemi della banca, core banking, sistemi di pagamento, gestione del rischio ICT a livello enterprise.

1.2 Contributo alla Conformità DORA

Il sistema contribuisce al soddisfacimento dei requisiti del Regolamento (UE) 2022/2554 (DORA) e all'attivazione degli articoli pertinenti all'autenticazione forte, alla protezione degli accessi, alla tracciabilità degli eventi ICT e alla gestione degli incidenti correlati all'autenticazione.

1.3 Proposta di Valore

- **Riduzione strutturale dell'esposizione al rischio** di accessi non autorizzati attraverso autenticazione hardware-based.
- **Supporto documentale alla governance ICT** mediante audit trail a elevata integrità crittografica e reportistica automatica.
- **Mitigazione totale del rischio di violazione (data breach) nel processo di autenticazione e di accesso ai sistemi bancari.**

---

2. ARCHITETTURA E PRINCIPI FONDANTI

2.1 Hardware Root-of-Trust

AEGIS-1 impiega un dispositivo indossabile dotato di Secure Element (NTAG 424 DNA) che funge da radice di fiducia hardware. Il chip crittografico genera un Message Authentication Code (MAC) dinamico e univoco per ogni interazione, vincolato a un contatore interno con protezione anti-replay.

Caratteristiche tecniche: - Generazione deterministica di MAC univoci per sessione - Contatore interno hardware per prevenzione del replay - Nessun dato sensibile o chiave privata esposta al dispositivo client

2.2 Architettura Zero-Data

Il sistema è progettato secondo il principio di minimizzazione del dato: AEGIS-1 **non memorizza** dati personali identificabili (PII), token di sessione persistenti o credenziali in chiaro. I MAC sono generati al volo e non vengono conservati in archivi consultabili dal sistema.

> **Nota di qualificazione**: il principio "Zero-Data" si applica al perimetro funzionale di AEGIS-1. I dati gestiti dai sistemi della banca (database, log applicativi, sessioni utente) restano sotto la responsabilità e la governance dell'ente finanziario.

2.3 Protocollo Human-Locked (Air-Gap Biologico)

Il sistema implementa un protocollo di autenticazione che richiede la convergenza sincrona di due elementi:

Fattore	Descrizione
Fattore Silicio	Secure Element hardware (NTAG 424 DNA) con generazione MAC dinamica
Fattore Biologico	Presenza fisica verificata dell'operatore tramite dispositivo indossabile (air-gap biologico)

Questo approccio riduce la superficie di attacco rispetto ai tradizionali sistemi eliminando la dipendenza da canali di comunicazione intercettabili.

2.4 Zero-Inbound Architecture

L'infrastruttura non espone porte in ingresso pubbliche (zero-inbound). Le comunicazioni avvengono esclusivamente tramite connessioni initiate dall'interno, protette da mTLS (Mutual TLS) con certificate pinning e tunnel WireGuard su rete privata.

2.5 Audit Trail WORM

Tutti gli eventi di autenticazione vengono registrati in un audit trail con protezione Write-Once-Read-Many (WORM), corredato da: - Hash-chain sequenziale per verifica di integrità - Timestamp qualificato con ancora temporale deterministica - Struttura machine-readable (formati JSON: `ldg.json`, `aud.json`) compatibile con l'integrazione SIEM

---

3. MAPPATURA DORA: CONTRIBUTO DI AEGIS-1

La seguente mappatura identifica gli articoli del DORA per i quali AEGIS-1 fornisce un contributo tecnico documentabile.

3.1 Articoli a Contributo Diretto

Articolo DORA	Oggetto	Contributo di AEGIS-1	Limiti del Contributo
Art. 9	Protezione e prevenzione	Autenticazione forte hardware-based; segmentazione di rete (zero-inbound, mTLS)	Non copre patch management, crittografia dati a riposo, policy di sicurezza dell'informazione
Art. 10	Individuazione anomalie	Audit trail WORM con hash-chain; integrazione SIEM; soglie di allarme sugli eventi di autenticazione	Non copre il monitoraggio della rete ICT nel suo complesso
Art. 17	Gestione incidenti ICT	Playbook di incident response per eventi di autenticazione; logging WORM per root cause analysis	Non copre la gestione incidenti su sistemi diversi dall'autenticazione
Art. 20	Segnalazione incidenti gravi	Report automatici di conformità (generazione ogni 24h); template conformi ai modelli RTS/ITS	La segnalazione effettiva resta responsabilità dell'ente
Art. 26	Logging e conservazione	Audit trail WORM con hash-chain e timestamp qualificato	Non copre la conservazione di log di altri sistemi

3.2 Articoli a Contributo Indiretto

Articolo DORA	Oggetto	Contributo di AEGIS-1
Art. 6	Quadro di gestione rischi ICT	Supporto documentale tramite evidenze di autenticazione forte; separazione delle funzioni di controllo
Art. 12	Backup e ripristino ICT	Ridondanza geografica infrastruttura AEGIS-1 (server multiregione); RTO < 10 min, RPO < 1 min per il servizio di autenticazione
Art. 25	Contenimento impatto incidenti	Architettura zero-inbound; assenza di dati sensibili in memoria (eliminazione dei danni da blast radius in caso di compromissione)
Art. 28	Rischio ICT di terze parti	Contratti tipo con clausole DORA, SLA con KPI misurabili, diritto di audit, exit strategy documentata

4. EVIDENCE & VERIFICABILITÀ

4.1 Brevetti

Riferimento	Oggetto	Ufficio Brevetti
Brevetto MIMIT N. 102025000033130	Human-Locked Protocol	Ministero delle Imprese e del Made in Italy (MIMIT)
Brevetto MIMIT N. 102025000035566	Hardware Root-of-Trust	Ministero delle Imprese e del Made in Italy (MIMIT)

4.2 Report di Test e Audit

ID Documento	Tipologia	Data
PT-AEGIS-2026-001	Penetration Test su infrastruttura AEGIS-1	21/04/2026
TLPT-AEGIS-2026-001	Threat-Led Penetration Testing (metodologia DORA Art. 26-27)	21/04/2026
VERBALE-AEGIS-2026-001	Verbale delle attività di verifica	21/04/2026
AWS-CONFIG-2026-001	Configurazione (Security Group, VPC)	21/04/2026
CONTROLLI-2026-001	Output dei controlli di sistema	21/04/2026

4.3 Piano di Validazione

Attività	Stato	Timeline Stimata
Pubblicazione numeri di certificato FIPS 140-3 e Common Criteria	Esclusivamente su richiesta dopo sottoscrizione di NDA	Q2 2026
Esercitazione congiunta banca-fornitore (DR/BCP)	Completata Q2 2026	Ricorrente semestrale

5. BENEFICI PER L'ENTE FINANZIARIO

5.1 Sicurezza e Riduzione del Rischio

Beneficio	Dettaglio
Autenticazione hardware-based	Eliminazione della dipendenza dai sistemi vulnerabili a data breach, phishing e MITM
Minimizzazione del dato	Assenza di PII e token persistenti nell'infrastruttura AEGIS-1 riduce la superficie di esfiltrazione
Rete zero-inbound	Assenza di porte pubbliche esposte riduce la superficie di attacco esterno

5.2 Governance e Supporto Documentale

Beneficio	Dettaglio
Audit trail strutturato	Registri WORM con hash-chain, esportabili in formato machine-readable per integrazione SIEM e analisi forense
Report automatici	Generazione ogni 24 ore di report di conformità disponibili per il Management Body e le funzioni di controllo
Registro delle Informazioni (ROI)	Generazione automatica da VM dedicata, allineata al DPM 4.0 ITS 2024/2956
Template di segnalazione	Predisposizione di template conformi ai modelli RTS/ITS per la segnalazione alle autorità di vigilanza

5.3 Gestione del Rischio Terze Parti

Beneficio	Dettaglio
Contratti DORA-compliant	Clausole di conformità, diritto di audit, exit strategy, obblighi di notifica incidenti
SLA con KPI misurabili	Disponibilità 99,99%, latenza < 100ms, RTO < 10 min, RPO < 1 min
Exit strategy documentata	Piano di migrazione e uscita testato, per garantire continuità in caso di sostituzione del fornitore

6. GOVERNANCE E RESPONSABILITÀ

6.1 Separazione dei Domini

Area di Responsabilità	Titolare
Autenticazione forte (SCA)	AEGIS-1 (T.T.H.C. OÜ)
Gestione delle identità (IAM)	Ente finanziario
Autorizzazioni e profili di accesso	Ente finanziario
Crittografia dati a riposo	Ente finanziario
Governance complessiva del rischio ICT	Management Body dell'ente finanziario
Segnalazione alle autorità di vigilanza	Ente finanziario
Conformità normativa complessiva	Ente finanziario

6.2 Supporto al Management Body

L'adozione di AEGIS-1 fornisce al Consiglio di Amministrazione e al Collegio Sindacale: - Evidenza documentale dell'implementazione di autenticazione forte hardware-based (stato dell'arte per il perimetro di pertinenza) - Audit trail a elevata integrità per la ricostruzione forense degli eventi di accesso - Reportistica periodica utilizzabile come supporto alle valutazioni di compliance

7. ANALISI COMPARATIVA SINTETICA: APPROCCI TRADIZIONALI vs. AEGIS-1

Vettore di Rischio	Autenticazione Tradizionale	AEGIS-1
Token intercettabile (MITM, phishing)	Sì – token trasmessi su canali potenzialmente compromessi	Mitigato – MAC generati localmente su Secure Element, non trasmessi in chiaro
Replay attack	Possibile in assenza di contatori robusti	Mitigato – contatore hardware anti-replay integrato nel Secure Element
Esfiltrazione di credenziali	Rischio presente (database, log)	Ridotto – nessun token o PII memorizzato dall'infrastruttura
Brute force	Dipendente dall'implementazione	Mitigato – rate limiting hardware (tick deterministici) con blocco automatico
Tracciabilità forense	Dipendente dal sistema di logging della banca	Audit trail WORM con hash-chain nativo
Disaccoppiamento dell'identità dell'utente dalla transazione finanziaria	Assente – l'identità utente è legata alla sessione	**Applicato – L'identità utente è separata dal token transazionale**

8. DICHIARAZIONE DI PERIMETRO E RESPONSABILITÀ

AEGIS-1 è un'infrastruttura tecnica di autenticazione forte e tracciabilità forense. Il presente documento e il sistema descritto:

1. **Non sostituiscono** la consulenza legale, regolamentare o di compliance.
2. **Non esonerano** l'ente finanziario dalla responsabilità ultima sulla propria conformità normativa complessiva.
3. **Non garantiscono** l'esclusione da incidenti di sicurezza informatica ma garantiscono il disaccoppiamento dell'identità dell'utente dalla transazione finanziaria.
4. **Contribuiscono** alla riduzione del rischio nell'ambito specifico dell'autenticazione forte e della tracciabilità degli accessi.
5. **Richiedono** l'integrazione con il quadro complessivo di governance ICT dell'ente per una copertura DORA completa.

9. CONTATTI E RICHIESTE DI DOCUMENTAZIONE

Canale	Dettaglio
Società	T.T.H.C. OÜ – Sovereign Critical Systems Engineering
Registro Imprese Estonia	registrikood 17487615 – verificabile su e-rik.ee
Richieste di due diligence	Da indirizzare via PEC o comunicazione formale alla sede legale
Documentazione tecnica	Disponibile su richiesta previa sottoscrizione di NDA
Verifica certificazioni	I riferimenti completi (numero di certificato, ente, scadenza) saranno forniti in sede di due diligence formale

DISCLAIMER FINALE

Il presente documento è stato redatto da T.T.H.C. OÜ con finalità informativa e tecnica. I contenuti riflettono lo stato delle conoscenze e delle implementazioni alla data di pubblicazione (27 giugno 2026) e sono soggetti ad aggiornamento. Le affermazioni relative a certificazioni, brevetti e risultati di test si basano sulla documentazione disponibile alla data indicata. AEGIS-1 è un componente tecnico e non costituisce soluzione di compliance autonoma.