Indelli Bridge TOTP

Specifiche Tecniche del Sistema di Autenticazione Zero-Trust

Infrastruttura Multi-Tier, Conformità NIS2, Licenza Apache 2.0

1. Introduzione (Executive Summary)

Il presente documento illustra l'architettura tecnica, sistemistica e legale di un sistema di autenticazione Zero-Trust custom (Identity & Access Management - IAM). Progettato specificamente per proteggere le API e i servizi critici della Pubblica Amministrazione (es. Anonimizzatore Atti PA), il sistema si distingue per l'adozione di un'autenticazione MFA (Multi-Factor Authentication) Context-Aware, basata su token OTP temporali proprietari e principi di Moving Target Defense.

Questa terza revisione del documento cristallizza l'infrastruttura su un modello Multi-Tier blindato, evidenziando la piena rispondenza ai severi requisiti della Direttiva Europea NIS2 e il valore strategico del rilascio del codice sorgente sotto Licenza Open Source Apache 2.0.

2. Architettura del Sistema (Infrastruttura Multi-Tier)

La soluzione adotta una topologia distribuita, disaccoppiando l'interazione pubblica (Frontend) dalla logica applicativa (Backend) per garantire un elevato livello di segregazione e sicurezza.

2.1 Client (Token Generator Air-Gapped)

Un eseguibile portatile compilato residente su una chiavetta USB fisica, concepito per operare in un ambiente Linux dedicato. Agendo offline, interroga il clock di sistema per recuperare parametri temporali (Giorno e Ora) e generare una chiave di salatura concatenata a una passphrase segreta.

2.2 VM di Front-End (Gateway di Autenticazione)

Macchina Virtuale esposta all'esterno che agisce da proxy difensivo. Esegue i seguenti controlli:

- **Filtro (randomname).php:** Applica il Device Fingerprinting bloccando User-Agent commerciali (Windows, Mac, iOS, Android) riceve l'hash ed esegue l'offuscamento dell'identità utente.
- **Autenticatore (randomname2).php:** Decritta l'identità utente tramite compensazione del time-drift (±3 minuti) e valida l'hash temporale prima di instradare la chiamata.

2.3 Server Operativo Core (Backend Privilegiato)

Server isolato (es. connettore1.php) accessibile solo da IP inseriti in Whitelist (tra cui la VM di Front-End). Reitera autonomamente le validazioni (approccio Zero-Trust) e, in caso di successo, istanzia la sessione sicura tramite un ID effimero crittografico a 256 bit (ephemeral_id) e autorizza il servizio.

3. Flussi di Sicurezza e Algoritmi Custom

3.1 Time-Bound Hash Authentication

L'OTP viene calcolato tramite una formula matematica proprietaria con scadenza oraria:

V = Giorno + (Ora * valore numerico)

La variabile V viene concatenata alla passphrase dell'utente e convertita in hash SHA-256. La finestra di validità (massimo 59 minuti) mitiga severamente le possibilità di attacchi di replay a lungo termine.

3.2 Moving Target Defense e Cifratura Polimorfica

Per proteggere l'identificativo utente (es. "stefano"), il sistema converte il nome in valori numerici e li moltiplica per i minuti trascorsi dalla mezzanotte (1-1440). Poiché il parametro moltiplicatore cambia ogni 60 secondi, la stringa intercettabile (payload) muta costantemente. Il backend decritta la stringa iterando i calcoli su una finestra di tolleranza di ±3 minuti per compensare i ritardi di rete. Ogni utente ha il suo generatore di hash key su usb personalizzato e l'accesso **(randomname).php** di cui sopra personalizzato.

4. Infrastruttura Sistemistica e Network Hardening

Entrambi i nodi sono costruiti su uno stack Linux/Open Source blindato per ridurre al minimo la superficie di attacco:

- - Sistema Operativo: Debian 13 (Trixie) in versione minimale.
- - Isolamento VirtualHost: Virtualmin, utilizzato per segregare i domini web in contenitori chroot/PHP-FPM isolati.
- - Regole Firewall (firewalld): Architettura default-deny, con porte esposte limitate al necessario e Backend isolato da Whitelist IP.
- - Intrusion Prevention (fail2ban): Analisi continua dei log per bloccare in tempo reale enumeration, scanning e tentativi brute-force HTTP.

5. Matrice di Conformità: Direttiva NIS2 (Articolo 21)

La soluzione è architettata per rispondere alle rigorose misure di gestione dei rischi imposte dalla Direttiva Europea sulla Cybersicurezza (NIS2) per Soggetti Essenziali e Importanti (PA inclusa).

Requisito NIS2 (Art. 21)	**Misure di Mitigazione Implementate**
Uso di Autenticazione a Più Fattori (MFA)	Adozione di un sistema MFA hardware-based (USB - Qualcosa che hai) + Passphrase (Qualcosa che sai), eliminando il rischio legato alle password statiche.
Politiche Zero-Trust e Controllo Accessi	Segregazione di rete (Whitelist), validazione costante della sessione (nessuna fiducia implicita post-login) e Device Fingerprinting per scartare dispositivi promiscui.
Crittografia e Sicurezza delle Comunicazioni	Hash SHA-256 su credenziali, offuscamento matematico polimorfico dell'identità utente, e comunicazioni vincolate a TLS 1.3 con Apache2.
Sicurezza degli Endpoint	Rifiuto esplicito di OS consumer (Windows/Android). Il sistema impone l'utilizzo dell'ambiente virtuale Linux protetto fornito dall'Ente.

6. Rilascio sotto Licenza Open Source Apache 2.0

Il rilascio del codice e' sotto Licenza Apache 2.0. Questa scelta conferisce al sistema una valenza istituzionale ed Enterprise per i seguenti motivi:

- Trasparenza e Auditabilità:

Il divieto di 'Security by Obscurity' imposto dalle moderne policy (e dalla stessa NIS2) è soddisfatto. Il codice può essere audito, validando la solidità crittografica del sistema.

- Conformità alle Linee Guida AgID (CAD):

Il Codice dell'Amministrazione Digitale (CAD) promuove attivamente il riuso del software. La licenza Apache 2.0 permette l'adozione fluida da parte di altre PA senza iter di acquisto complessi.

- Nessun Effetto Copyleft:

A differenza della licenza GPL, la Apache 2.0 è permissiva. Un Ente può integrare l'autenticatore nei propri gestionali chiusi senza l'obbligo di rilasciare tutto il proprio software proprietario come open source.

- Protezione Legale e Brevetti:

Fornisce una chiara limitazione di responsabilità (liability protection) per gli sviluppatori e una concessione esplicita all'uso di eventuali brevetti software, tutelando sia i creatori che l'Ente utilizzatore.

7. Matrice dei Rischi e Valutazione di Sicurezza

Vettore di Minaccia	**Mitigazione Implementata**	**Efficacia**
Furto di Credenziali (Phishing / Keylogger)	La password statica non viaggia in rete. Il token OTP (SHA-256) intercettabile scade in breve tempo.	Alta
Scraping Identità (Username)	Cifratura mutante (Moving Target Defense) dipendente dal fattore temporale (minuti).	Alta
Lateral Movement	Separazione Gateway Front-End / Server Core. Quest'ultimo autorizza l'accesso solo tramite rigide regole IP di firewall.	Molto Alta
Attacchi Brute-Force L7	Filtri HTTP associati al ban proattivo degli IP abusivi tramite fail2ban e firewalld.	Alta

Altre Caratteristiche :

- Log Centralizzato (SIEM): Invio strutturato dei log di fail2ban e Apache verso un concentratore centrale per auditing continuo.

- Le librerie e/o I pacchetti Debian13 sono esclusivamente Vanilla