NoTIP

NO TESTS IN PRODUCTION

Verbale Esterno del 2026-02-24

Versione	1.0.0
Data Modifica	2026-02-28
Utilizzo	Esterno
Presenze	Francesco Marcon Mario De Pasquale Alessandro Contarini Alessandro Mazzariol Leonardo Preo Matteo Mantoan

Abstract dei contenuti

Il presente documento riporta il resoconto dell'incontro esterno tenutosi in remoto. L'incontro ha avuto come oggetto la discussione per sbloccare i dubbi infrastrutturali sull'implementazione dell'*End-to-End Encryption*$_G$ (E2EE), sulla gestione del Logging e sull'utilizzo di *NATS*$_G$ come motore di comunicazione.

Indice

1. Info e ordine del giorno

Il presente documento attesta formalmente che, in data **24 Febbraio 2026**, si è tenuto un incontro in remoto tramite Microsoft Teams con la proponente *M31*. L'incontro si è tenuto tra le **15:45** e le **16:40**.

A rappresentare l'Azienda era presente Cristian Pirlog e Moones Mobaraki.

2. Discussione

L'incontro è stato dedicato principalmente alla risoluzione di dubbi e blocchi riguardanti l'infrastruttura di comunicazione e la sicurezza dei dati. Il Team ha posto all'Azienda quesiti specifici sulle modalità di distribuzione e mantenimento delle chiavi per la decifrazione dei payload. Questi elementi sono fondamentali in un'architettura che sfrutta la crittografia E2EE.

Durante la riunione si sono anche trattati temi riguardanti l'implementazione di funzionalità accessorie come il Logging e l'Auditing.

2.1. Chiarimenti sull'*End-to-End Encryption*$_G$ (E2EE)

Dibattito:
Il Team ha esposto il problema emerso nelle prime fasi della progettazione. Il problema riguarda il momento e il luogo in cui i dati devono essere decriptati lato utilizzatore. Si è discusso anche come recapitare le chiavi crittografiche al *Gateway*$_G$ (in fase di *provisioning*$_G$) e all'utente finale.

È emerso che l'utilizzo di una API per restituire all'utente la chiave di decifrazione fa venire meno il concetto di E2EE puro.

Si è discusso inoltre del livello di granularità della chiave: per *Tenant*$_G$, per *Gateway*$_G$ o per singolo Utente.

Decisioni:
È stato deciso di non inserire l'E2EE puro come requisito obbligatorio a causa dell'elevata complessità di definizione e progettazione. Come compromesso per gestire il rischio in modo ottimale, è stato concordato di generare chiavi specifiche per ogni *Gateway*$_G$. Le chiavi saranno mantenute in una tabella dedicata. Si rinuncia così alla gestione centralizzata basata sulla singola chiave per *Tenant*$_G$.

2.2. Logging e Auditing

Dibattito:
Il Team ha chiesto all'Azienda indicazioni su come gestire il tracciamento e l'auditing. Si è domandato se fosse preferibile adottare strumenti dedicati oppure integrare i log nel database centrale.

Il referente aziendale ha precisato che l'auditing è una funzionalità opzionale. Ha sconsigliato di investire troppo tempo nell'integrazione con tecnologie esterne complesse.

Decisioni:
Si è convenuto di adottare una soluzione semplice. Si utilizzerà una tabella di log nel database per registrare le operazioni di maggior rilievo (es. creazione di utenti o modifiche a configurazioni critiche). Per ogni evento sarà sufficiente tracciare timestamp, Utente e Azione.

Di conseguenza, il Team manterrà questo requisito con priorità «desiderabile».

2.3. Servizio di Log tramite *NATS$_G$*

Dibattito:
Il Team ha proposto la creazione di un servizio dedicato all'osservazione dei topic *NATS$_G$*. Lo scopo è intercettare le informazioni e inserirle nel database dei log.

Decisioni:
La proposta è stata accolta positivamente. Poiché i servizi comunicano tutti tramite *NATS$_G$*, l'Azienda ha confermato che questo servizio semplifica l'aggregazione e il salvataggio delle informazioni.

2.4. *NATS$_G$* come motore principale e gestione degli Alert

Dibattito:
Il Team ha discusso la validità di *NATS$_G$* come motore principale di comunicazione, portando come esempio il pattern Request-Reply tra i servizi. Successivamente, è stata affrontata la criticità della gestione centralizzata degli alert. A causa della crittografia E2EE, i dati in transito risultano illeggibili per l'infrastruttura centrale. Di conseguenza, intercettare le fluttuazioni dei sensori per generare avvisi automatici risulta molto complesso.

Decisioni:
L'Azienda ha confermato che *NATS$_G$* è una soluzione solida e coerente con i servizi ipotizzati. Per gli alert, si è convenuto di evitare logiche di micro-management interne. L'analisi e la generazione di allarmi sui dati saranno demandate agli utilizzatori terzi tramite API. Il sistema centrale si limiterà a fornire alert di stato o diagnostica (es. disconnessione di un *Gateway$_G$*).

3. Epilogo della Riunione

L'incontro è stato fondamentale per superare alcuni blocchi progettuali. L'abbandono dell'E2EE puro a favore di una crittografia per singolo *Gateway$_G$* riduce la complessità dell'infrastruttura.

Il Team continuerà la progettazione seguendo le indicazioni emerse durante la riunione.

Il prossimo incontro è stato fissato a **martedì 3 marzo**.

4. Approvazione Aziendale

La presente sezione certifica che il verbale è stato esaminato e approvato dai rappresentanti di *M31*. L'approvazione è confermata dalle firme dei referenti aziendali riportate di seguito.