Università degli Studi di Padova

GlitchHub TEAM

Verbale esterno 03/02/2026 (M31)

Ordine del giorno

1. Dubbi sulla classificazione dei **requisiti**$_G$
2. Crittografia **NATS**$_G$
3. Scambio di chiavi tra **NATS**$_G$ e **Gin**$_G$
4. Gestione dell'autenticazione tramite **Keycloak**

•

Versione **1.0.0**

Stato	Verificato
Partecipanti	Alessandro Dinato Riccardo Graziani Elia Ernesto Stellin Jaume Bernardi
Distribuzione	GlitchHub Team M31 SRL Prof. Cardin Riccardo Prof. Vardanega Tullio

Registro Modifiche

Ver.	Data	Autore	Verificatore	Descrizione
1.0.0	04/02/2026	Riccardo Graziani	Alessandro Dinato	Versione stabile verbale esterno 03/02/2026
0.1.0	04/02/2026	Riccardo Graziani	Alessandro Dinato	Stesura verbale esterno del 03/02/2026
0.0.1	04/02/2026	Riccardo Graziani	Alessandro Dinato	Bozza iniziale verbale esterno del 03/02/2026

Indice

1. Introduzione

Il presente verbale attesta che in data 3 febbraio 2026 dalle 14:40 alle 15:15, si è svolto l'incontro con la proponente **M31 SRL**, in modalità remota.

L'incontro ha avuto l'obiettivo di discutere e chiarire:

- il livello di importanza di alcuni **requisiti**$_G$
- come gestire la crittografia lato **NATS**$_G$
- come gestire lo scambio di chiavi di cifratura tra **NATS**$_G$ e **Gin**$_G$
- come gestire l'autenticazione usando **Keycloak**.

2. Resoconto

2.1. Classificazione dei requisiti

Durante la riunione, il gruppo ha chiesto dei chiarimenti riguardo il livello di importanza di alcuni **requisiti**$_G$, in particolare:

- **filtraggio** dei dati storici;
- la possibilità di **sospendere** l'invio di dati da parte di un **gateway**$_G$
- la possibilità di **sospendere** l'invio di dati da parte di un sensore;
- la visualizzazione delle richieste di **commissioning/decommissioning** in corso;
- la visualizzazione delle **metriche di sistema**;
- la presenza di **alert** di base riguardanti gateway non funzionanti o non raggiungibili;

La proponente ha chiarito che:

- il filtraggio dei dati storici è da considerarsi come **requisito**$_G$ **obbligatorio**;
- la possibilità di **sospendere** l'invio di dati da parte di un **gateway**$_G$ è da considerarsi come **requisito**$_G$ **desiderabile**;
- la possibilità di **sospendere** l'invio di dati da parte di un sensore è da considerarsi come **requisito**$_G$ **opzionale**;
- la visualizzazione delle richieste di **commissioning/decommissioning** in corso è da considerarsi come **requisito**$_G$ **opzionale**;
- la visualizzazione delle **metriche di sistema**, in generale, è da considerasi come **requisito**$_G$ **obbligatorio**, ma le seguenti metriche hanno un'importanza minore:
  - il **throughput dei dati** è **desiderabile**;
  - l'uso delle **risorse** dei nodi cloud è **opzionale**;
  - la **frequenza di disconnessione** dei gateway è **desiderabile**;
  - il **numero** di valori **out-of-range** è **opzionale**;
- la presenza degli **alert** di base è da considerarsi **requisito**$_G$ **obbligatorio**.

2.2. Crittografia NATS

Il gruppo ha esposto i propri dubbi su come gestire la crittografia dei dati su **NATS**$_G$. Il problema principale riguarda il salvataggio di tali dati su **TimescaleDB**$_G$: salvare tutti i dati crittografati nel database causerebbe un'importante perdita di performance, in quanto il server **Gin**$_G$ dovrebbe richiedere tutti i dati e decrittarli in memoria prima di poter eseguire qualsiasi operazione di filtro o aggregazione.

La proponente ha dichiarato che la soluzione va determinata con uno studio più approfondito delle tecnologie ed ha consigliato di esporre questo dubbio attraverso una mail in maniera da poter fornire una risposta più completa.

2.3. Scambio di chiavi di cifratura

In relazione al precedente dubbio, il gruppo ha individuato un problema riguardo allo scambio di chiavi di cifratura. In particolare il gruppo non ha chiaro come le istanze di **Gin**$_G$ possano avere tutti le chiavi private di cifratura per poter decrittare i dati ricevuti da **NATS**$_G$ o da **TimescaleDB**$_G$, senza però esporre tali chiavi in chiaro sul network.
La proponente ha invitato ad esporre questo dubbio attraverso una mail in maniera da poter fornire una risposta completa.

2.4. Gestione dell'autenticazione

Lo studio di preliminare di **Keycloak** ha evidenziato come una sua implementazione come sistema di autenticazione non sarebbe fattibile tenendo conto dei tempi di sviluppo del **PoC**$_G$. La soluzione proposta dal gruppo sarebbe di implementare un database **PostgreSQL**$_G$ che separi gli utenti in diversi **tenant**$_G$.
La proponente ha dichiarato che tale soluzione è accettabile nell'ambito del **PoC**$_G$, e che lo studio di **Keycloak** può essere approfondito in vista dell'**MVP**$_G$.

3. Attività conseguenti

Task	Assegnatari	Issue
Login con dashboard Angular	Elia Ernesto Stellin	**PoC/#16**
Sviluppo crittografia, autenticazione e account con NATS	Alessandro Dinato	**PoC/#2**
Sviluppo API di autenticazione	Elia Ernesto Stellin	**PoC/#8**

Alessandro Dinato

Firma del revisore interno

Cristian Pirlog

Firma del revisore esterno