



UNIVERSITÀ  
DEGLI STUDI  
DI PADOVA

**GLITCHHub**  
TEAM

---

## Verbale esterno 13/01/2026 (M31)

---

### Ordine del giorno

1. Discussione su autenticazione e sicurezza
2. Gestione degli alert di sistema
3. Visualizzazione dei dati e dashboard
4. Impersonificazione degli utenti
5. Audit log
6. Configurazione dei gateway e gestione dei sensori
7. Commissioning e decommissioning dei gateway
8. Monitoraggio del sistema e requisiti non funzionali
9. Tecnologie suggerite

•  
Versione **1.0.0**

**Stato** Verificato

**Partecipanti** Jaume Bernardi  
Alessandro Dinato  
Michele Dioli  
Riccardo Graziani  
Siria Salvalaio  
Elia Ernesto Stellin

**Distribuzione** GlitchHub Team  
M31 SRL

Prof. Cardin Riccardo  
Prof. Vardanega Tullio

## Registro Modifiche

<b>Ver.</b>	<b>Data</b>	<b>Autore</b>	<b>Verificatore</b>	<b>Descrizione</b>
1.0.0	20/01/2026	Hossam Ezzemouri	Alessandro Dinato	Creazione versione stabile del verbale esterno del 13/01/2026
0.0.1	13/01/2026	Hossam Ezzemouri	Alessandro Dinato	Stesura verbale esterno del 13/01/2026

---

---

## Indice

1. Introduzione .....	3
2. Resoconto .....	3
2.1. Discussione su autenticazione e sicurezza .....	3
2.2. Gestione degli alert .....	3
2.3. Visualizzazione dei dati e dashboard .....	3
2.4. Impersonificazione degli utenti .....	3
2.5. Audit log .....	4
2.6. Configurazione dei gateway e gestione dei sensori .....	4
2.7. Commissioning e decommissioning dei gateway .....	4
2.8. Profili GATT e sensori simulati .....	4
2.9. Monitoraggio del sistema e requisiti non funzionali .....	5
2.10. Tecnologie suggerite .....	5
3. Attività conseguenti .....	5

## 1. Introduzione

Il presente verbale attesta che in data 13 gennaio 2026 alle 14:30 si è svolto l'incontro con il **proponente**<sub>G</sub> M31 SRL, in modalità ibrida.

L'incontro ha avuto l'obiettivo di discutere e chiarire alcuni aspetti funzionali del **sistema**<sub>G</sub> sotto studio, con particolare riferimento agli use cases relativi alla gestione degli alert, alla visualizzazione dei dati, all'**impersonificazione**<sub>G</sub> degli utenti, alla configurazione dei **gateway**<sub>G</sub> e alla gestione della sicurezza e dell'osservabilità del **sistema**<sub>G</sub>.

## 2. Resoconto

### 2.1. Discussione su autenticazione e sicurezza

Durante la riunione, il gruppo ha chiesto chiarimenti riguardo l'eventuale utilizzo di meccanismi di autenticazione a due fattori (2FA). Il **proponente**<sub>G</sub> ha specificato che il supporto al 2FA è di interesse marginale e che non è richiesta un'implementazione esplicita di tale funzionalità nell'ambito del progetto.

È stata inoltre discussa la gestione delle **API**<sub>G</sub> Key: l'azienda ha confermato che ha senso mostrare il token una sola volta al momento della creazione, per motivi di sicurezza, lasciando aperta la possibilità di rendere opzionale l'adozione delle **API**<sub>G</sub> Key.

### 2.2. Gestione degli alert

Il gruppo ha presentato la propria interpretazione degli alert di **sistema**<sub>G</sub>.

M31 ha chiarito che:

- la piattaforma non deve occuparsi della **validazione**<sub>G</sub> dei valori oltre soglia;
- la **verifica**<sub>G</sub> di soglie applicative è demandata a piattaforme esterne;
- gli alert gestiti dal **cloud**<sub>G</sub> devono essere principalmente di tipo infrastrutturale o gestionale.

Sono stati ritenuti appropriati:

- alert relativi a **gateway**<sub>G</sub> offline;
- alert relativi ai costi del **tenant**<sub>G</sub>, con invio di una mail al superamento di una soglia (funzionalità opzionale).

Gli alert proposti dal gruppo sono stati giudicati coerenti.

### 2.3. Visualizzazione dei dati e dashboard

La **proponente**<sub>G</sub> ha espresso parere positivo riguardo:

- l'uso di grafici per la visualizzazione dei dati dei sensori;
- la visualizzazione dello storico dei dati;
- il filtraggio dei dati storici;
- la presenza di una dashboard generica per l'utente autenticato.

È stata valutata positivamente l'introduzione di:

- una mappa con la posizione dei **gateway**<sub>G</sub> nella dashboard del **Tenant Admin**<sub>G</sub>
- una visualizzazione analoga nella dashboard del **Super Admin**<sub>G</sub>.

Per le richieste dei **gateway**<sub>G</sub>, è stata ritenuta adeguata una tabella semplice con stato della richiesta e azioni disponibili.

### 2.4. Impersonificazione degli utenti

Il gruppo ha approfondito il tema dell'**impersonificazione**<sub>G</sub>.

---

M31 ha chiarito che:

- impersonare un account significa assumerne completamente il ruolo;
- l'**impersonificazione**<sub>G</sub> è usata dal **Super Admin**<sub>G</sub> per risolvere problematiche operative;
- l'operazione deve avvenire nei **Tenant**<sub>G</sub> che hanno accettato la suddetta clausola.

È stato inoltre specificato che:

- il Super-Admin deve poter accedere agli stessi dati del **Tenant Admin**<sub>G</sub> anche senza **impersonificazione**<sub>G</sub>, con esclusione delle informazioni più sensibili;
- gli use cases possono essere ricondotti a un ruolo di Admin generico, considerando il **Super Admin**<sub>G</sub> come utente fidato.

È stata suggerita la tecnologia open source **Keycloak** per la gestione delle utenze e dell'**impersonificazione**<sub>G</sub>.

## 2.5. Audit log

Il gruppo ha discusso la necessità di introdurre audit log.

M31 ha confermato che:

- gli audit log sono necessari;
- il **Tenant Admin**<sub>G</sub> deve poter visualizzare le operazioni degli operatori del proprio **tenant**<sub>G</sub>
- è sufficiente tracciare chi ha fatto cosa e quando;
- il filtraggio per tipologia di azione è sensato;
- l'esportazione in formato CSV è adeguata.

## 2.6. Configurazione dei gateway e gestione dei sensori

È stata approfondita la gestione della frequenza di invio dei dati e delle tecniche di **normalizzazione**<sub>G</sub>.

M31 ha chiarito che:

- la frequenza di invio dati varia in base alla tipologia di sensore, **ci**<sub>G</sub> sarà un parametro di default per ogni tipologia e successivamente ogni **tenant**<sub>G</sub> potrà personalizzarlo;
- il **gateway**<sub>G</sub> può inviare dati atomici o in pacchetti;
- è possibile definire limiti di invio a livello di **gateway**<sub>G</sub>.

Dal punto di vista del **Tenant**<sub>G</sub>:

- è importante poter modificare la frequenza di invio per tipologia di sensore;
- ogni **gateway**<sub>G</sub> deve avere configurazioni di default e custom;
- le modifiche devono essere inviate al **gateway**<sub>G</sub> tramite comandi;
- le configurazioni custom devono essere tracciate dal **Cloud**<sub>G</sub>.

## 2.7. Commissioning e decommissioning dei gateway

Il commissioning è considerato opzionale:

- per l'**MVP**<sub>G</sub> è sufficiente che il **Super Admin**<sub>G</sub> possa commissionare un numero arbitrario di **gateway**<sub>G</sub>.

Per il decommissioning:

- deve essere possibile specificare quali **gateway**<sub>G</sub> decommissionare;
- il rifiuto della richiesta può essere rimosso.

## 2.8. Profili GATT e sensori simulati

M31 ha confermato che:

- ha senso modellare **gateway**<sub>G</sub> con sensori simulati;

- un singolo **profilo GATT<sub>G</sub>** può fornire più tipologie di dato;
- il **sistema<sub>G</sub>** deve essere consapevole delle diverse misurazioni prodotte.

## 2.9. Monitoraggio del sistema e requisiti non funzionali

Il **requisito<sub>G</sub>** di monitoraggio è da considerarsi obbligatorio.

È sufficiente fare riferimento al capitolato e adottare una soluzione semplice ma scalabile.

Per il **Proof of Concept<sub>G</sub>**:

- non è richiesta una gestione completa di ruoli e permessi;
- è fondamentale dimostrare connessione dei device, transito e crittografia dei dati.

## 2.10. Tecnologie suggerite

M31 ha suggerito:

- **NATS<sub>G</sub>** per la comunicazione;
- **Node.js<sub>G</sub>** per i servizi applicativi, favorendo **JavaScript<sub>G</sub>** o **TypeScript<sub>G</sub>** lungo l'intero stack.

## 3. Attività conseguenti

Task	Assegnatari	Issue
Studio tecnologie suggerite	Alessandro Dinato, Riccardo Graziani	<a href="#"><u>Docs/#165</u></a> , <a href="#"><u>Docs/#169</u></a>
Stesura dei requisiti e realizzazione diagrammi <b>use case<sub>G</sub></b>	Hossam Ezzemouri,Jaume Bernardi, Michele Dioli	<a href="#"><u>Docs/#166</u></a>
Conclusione use cases Visualizzazione	Riccardo Graziani	<a href="#"><u>Docs/#170</u></a>
Approfondimento <b>normalizzazione<sub>G</sub></b> dati	Jaume Bernardi, Alessandro Dinato, Riccardo Graziani, Elia Ernesto Stellin	<a href="#"><u>Docs/#133</u></a>
Approfondimento Grafana+Prometheus	Jaume Bernardi, Alessandro Dinato, Riccardo Graziani, Elia Ernesto Stellin	<a href="#"><u>Docs/#134</u></a>

**Alessandro Dinato**



---

Firma del revisore interno

**Cristian Pirlog**



---

Firma del revisore esterno