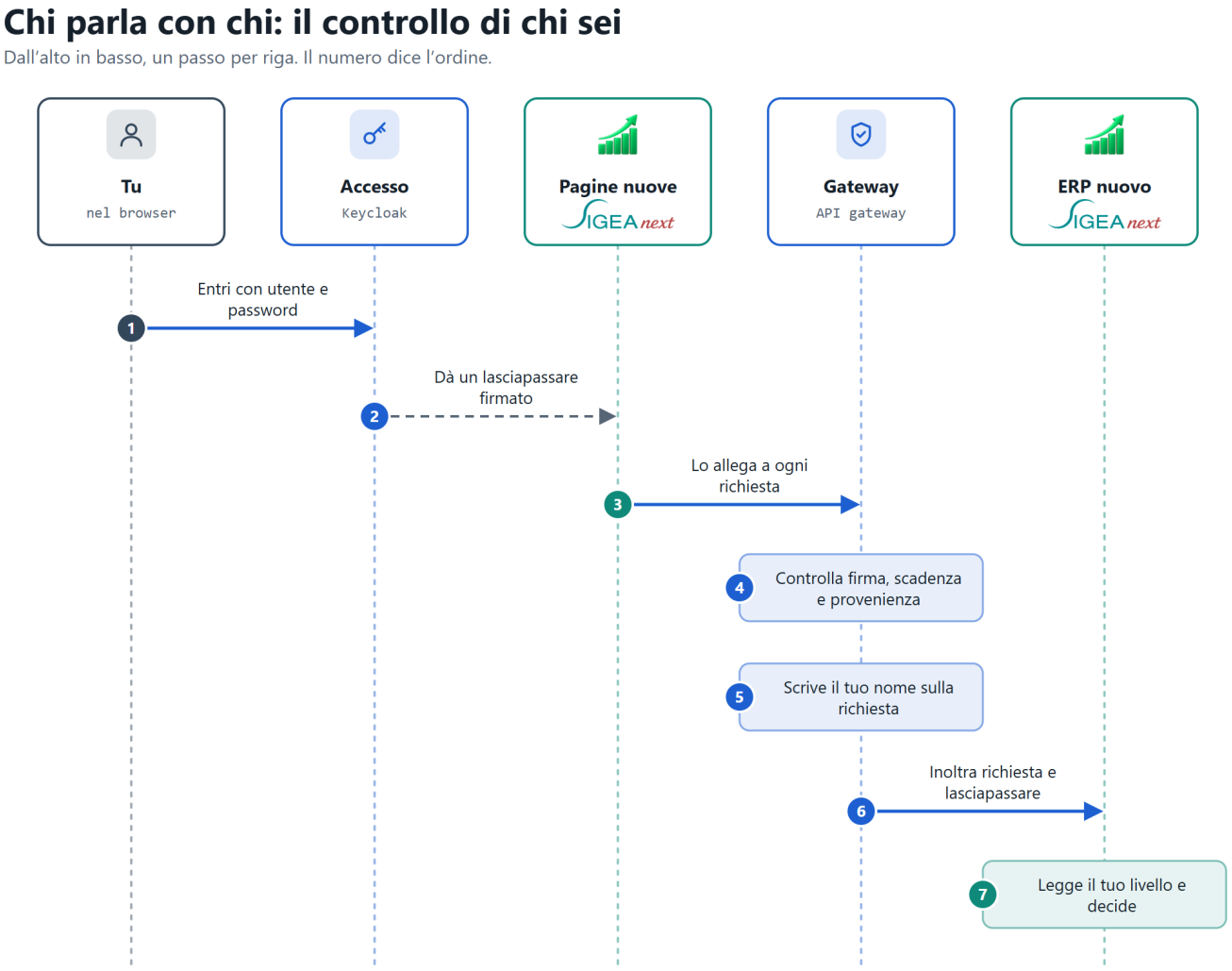
JC2.2 - Come si controlla chi sei

In una frase. Il Gateway non ti chiede la password: controlla il lasciapassare che hai ricevuto entrando, e passa ai servizi il tuo nome.

Utente e password li scrivi una volta sola, nella pagina dell'Accesso. In cambio ricevi un **lasciapassare**: un piccolo documento firmato che dice chi sei e che livello hai, e che scade dopo poco. Da quel momento la pagina lo allega a ogni richiesta. La password non viaggia più.



Il controllo di chi sei: l'Accesso firma il lasciapassare, il Gateway lo verifica, il servizio legge il livello

Per ogni richiesta il Gateway controlla quattro cose:

- che la **firma** sia quella dell'Accesso, quindi che il lasciapassare non sia stato fabbricato o ritoccato;
- che non sia **scaduto**;
- che venga dall'**Accesso di questa installazione** e non da un altro;
- che l'abbia chiesto un **programma ammesso**, cioè l'app web o uno dei servizi.

Se una sola non torna, la richiesta si ferma con l'errore 401 e nessun servizio la vede.

Se tutto torna, il Gateway scrive sulla richiesta il tuo **nome utente** e la inoltra insieme al lasciapassare. Prima però cancella qualunque nome fosse già scritto: così nessuno può presentarsi ai servizi con il nome di un altro.

Il **livello** (lettore, base, avanzato, staff) sta dentro il lasciapassare. Lo legge il servizio che riceve la richiesta, e decide lui se quella cosa la puoi fare. Se non puoi, risponde con l'errore 403. I livelli sono spiegati in Lettore, base, avanzato, staff (libro «JB - Accesso e permessi», pagina «JB3.1 - Lettore, base, avanzato, staff»).

> **Nota.** Poche cose passano senza lasciapassare, perché chi le chiede non può averlo: il controllo «sei acceso?» che il server fa ai servizi, le immagini dentro una stampa, la procedura di prima installazione.

> **Per chi sviluppa.**
> • Il controllo è in `SecurityConfig` e `SsoConfig` del Gateway: firma verificata con le chiavi pubbliche dell'Accesso (JWKS), poi scadenza, emittente e programma che ha chiesto il lasciapassare (`SSO_CLIENT_AMMESSI`).
> • `AuthenticationFilter` scrive `X-User-Id` con il nome utente del lasciapassare e toglie sempre quello arrivato dal client.
> • L'interruttore è `AUTH_ENABLED`. Spento serve solo in sviluppo: il Gateway lascia passare tutto e scrive un utente di comodo. Se è acceso ma mancano gli indirizzi dell'Accesso, il Gateway rifiuta ogni lasciapassare.
> • Anche i servizi verificano il lasciapassare per conto loro: una richiesta che non passa dal Gateway non entra.

> **Per approfondire.**
> • Integrazione Autenticazione JWT Angular + API Gateway: `docs/guide/sviluppo/GUIDA-AUTENTICAZIONE-JWT.md` (descrive una versione precedente, in cui si entrava dal Gateway: oggi si entra dall'Accesso)
> • Il disegno di oggi: `docs/devops/auth/AUTENTICAZIONE.md`

Revisione #2
Creato 17 novembre 2026 07:56:37 da Giuseppe Anelli
Aggiornato 17 novembre 2026 09:34:37 da Genesys Software