Allegato K – API & Personalizzazioni

Definizioni

- **Backoff esponenziale**: strategia di retry che aumenta progressivamente l'intervallo tra i tentativi (es. 1s, 2s, 4s, …) per ridurre la pressione sul sistema ricevente.
- **Breaking change**: modifica incompatibile con client esistenti (es. rimozione/cambio semantica di campi/endpoint) introdotta solo in major version.
- **Changelog**: registro delle modifiche rilasciate (nuove funzioni, fix, deprecazioni, cambi di schema/endpoint).
- **Dead-Letter Queue (DLQ)**: coda che riceve messaggi/eventi non consegnabili dopo i retry, per analisi e ri-processamento.
- **Firma HMAC**: firma del payload con chiave condivisa (Hash-based Message Authentication Code) per garantire integrità/autenticità delle notifiche (es. webhooks).
- **Hypercare**: finestra di assistenza rafforzata immediatamente post go-live, focalizzata su stabilizzazione e tuning.
- **Idempotenza**: proprietà per cui ripetere la stessa richiesta produce sempre lo stesso effetto (evita duplicazioni su retry).
- **iPaaS/ESB**: piattaforme di integrazione (Integration-Platform-as-a-Service / Enterprise Service Bus) usate per orchestrare e trasformare flussi tra sistemi.
- **mTLS (mutual TLS)**: autenticazione a doppio verso (client e server) tramite certificati durante la connessione TLS.
- **Near-real-time (NRT)**: scambio dati con latenza bassa ma non istantanea (es. secondi/minuti), tipicamente tramite webhooks/code.

- **OpenAPI/Swagger**: specifica e strumenti per descrivere formalmente le API REST (endpoint, metodi, schemi, esempi) e generare client/server.
- **Payload**: contenuto della richiesta/risposta (es. JSON) trasmesso da/verso un'API o in un evento.
- **Piano di Integrazione**: documento progettuale che definisce perimetro flussi, mappature, sicurezza, KPI, volumi, finestre e responsabilità.
- **Retry**: ritentativo automatico di consegna/esecuzione dopo un errore temporaneo, spesso con backoff esponenziale e limiti massimi.
- **SCIM**: standard per provisioning/de-provisioning utenti e gruppi tra sistemi di identità (System for Cross-domain Identity Management).
- **SFTP / S3-compatibile**: protocolli/servizi per trasferimento e deposito sicuro di file; SFTP usa SSH, S3-compatibile espone API tipo-S3 per oggetti.
- **Versioning semantico (SemVer)**: schema di versioni MAJOR.MINOR.PATCH; compatibilità garantita su minor/patch, cambi incompatibili solo su major con coesistenza/deprecazione.

1. Scopo e ambito

Il presente Allegato disciplina integrazioni, uso API, webhooks/eventi, personalizzazioni e connettori per WMP/VMP, inclusi perimetro, deliverable, governance tecnica e oneri economici. Si applica salvo diversa pattuizione in Ordine/SoW.

2. Oggetto

API: REST/JSON su HTTPS.

Webhook/Eventi: notifiche push server-to-server verso endpoint Cliente.

Connettore: componente batch o NRT verso terze applicazioni.

Personalizzazione: estensioni o configurazioni avanzate extra-standard.

3. Catalogo API e modelli dati

API REST documentate (OpenAPI) per domini, a titolo esemplificativo: *projects, company, users, jobSector, services, technology, languages, certifications* (CRUD ove applicabile). L'elenco puntuale e gli schemi sono pubblicati nel tenant del Cliente e nel documento "TimeFlow – API List". Gli endpoint possono evolvere; non costituiscono impegno a esporre ogni operazione su tutti i tenant.

4. Webhooks/Eventi

Attivabili su richiesta per eventi (es. CRUD su progetti/esigenze, profili/risorse, candidature, utenti, stati trattativa).

Sicurezza: firma HMAC opzionale, IP allowlist/mTLS su richiesta.

Affidabilità: retry con backoff esponenziale; DLQ opzionale.

Dettagli (payload, headers, tempi) nel Piano di Integrazione.

5. Sicurezza e controlli di accesso

Autenticazione: bearer token; su richiesta OAuth2/OIDC con IdP Cliente (SAML/OIDC) per flussi server-to-server; API key per integrazioni tecniche.

Autorizzazione: scoping per tenant/ruoli/permission (least-privilege).

Hardening & logging: audit trail, logging applicativo e telemetria.

Rate limiting & throttling: limiti per client/tenant e burst-control; in caso di superi non occasionali può essere applicato throttling o sospensione mirata degli endpoint, in coerenza con MSA §2.4 e AUP.

Misure aggiuntive: IP allowlist e mTLS su richiesta.

Ulteriori misure in Allegato D – TOMs & BC/DR.

6. Ambienti, versioning e compatibilità

Ambienti: produzione UE/SEE; eventuale test/staging su richiesta (no dati reali salvo accordo e misure dedicate – cfr. MSA §2.8 e Allegato D §2.6).

Versioni API: versioning semantico (path vN).

Compatibilità: backward-compat su minor/patch; breaking changes solo su major.

Deprecazioni: comunicate con preavviso adeguato; coesistenza versioni major per un periodo compatibile con l'impatto. Change management e preavvisi si coordinano con MSA §9.5 (processo di change) e con le manutenzioni di SLA – Allegato C §5.

7. Modelli di integrazione supportati

- Pull via API REST (cron o near-real-time).
- Push via webhooks/eventi.
- Exchange file (CSV/JSON) su SFTP/S3-compatibile; schema concordato.
- iPaaS/ESB (es. MuleSoft, Boomi, ecc.) tramite connettori generici HTTP/REST.
- Single Sign-On per utenti interattivi (SAML/OIDC) e SCIM opzionale per provisioning.

8. Onboarding tecnico & deliverable

- Kick-off integrazione e raccolta requisiti.
- Piano di Integrazione (perimetro flussi, mappature campi, KPI, volumi, finestre).
- Specifica tecnica (OpenAPI + esempi payload; schemi file; contratti webhook).
- Configurazione (credenziali, allowlist, parametri sicurezza).
- Collaudo tecnico: test di connettività, autenticazione, flussi end-to-end e resilienza (retry/idempotenza).
- Go-live e Hypercare (ove previsto dall'Ordine).

Per WMP non è prevista UAT di processo: la piattaforma viene configurata e resa disponibile; il Cliente procede al caricamento dei propri profili/dati. Eventuali UAT si applicano esclusivamente se espressamente previste da Ordine/SoW per altri moduli (es. VMP).

9. Oneri economici

Gli oneri di seguito sono "a catalogo" e si applicano salvo diversa pattuizione nell'Ordine/SoW o Listino Enterprise vigente:

- Setup integrazione standard API/Webhook (una tantum): attivazione credenziali, profili sicurezza, rate-limit, test con esempi payload.
- Connettori e mapping: sviluppo/adeguamento di connettori, trasformazioni dati, mapping campi.
- Personalizzazioni applicative: estensioni UI/API, logiche specifiche, nuovi eventi.
- Exchange file gestito: definizione schema, validatori, controlli di qualità, schedulazioni.
- Supporto & Hypercare: assistenza post go-live entro la finestra concordata.

- Manutenzione evolutiva: adeguamenti a modifiche normative/tecniche di terzi.

La valorizzazione è come da Ordine (forfait o T&M) e, in assenza di diversa indicazione, a consuntivo secondo il listino Enterprise vigente (giornate/uomo o canoni mensili per connettori gestiti).

10. Assunzioni e prerequisiti Cliente

- Disponibilità di un IdP per SSO (se richiesto), endpoint di integrazione raggiungibili e documentazione dei sistemi terzi.
- Dati di prova non sensibili o mascherati, utenti tecnici, referenti IT e processo.
- Finestra di test e, ove necessario, sandbox dei sistemi terzi.

11. Limiti ed esclusioni

Salvo diverso accordo, restano esclusi: sviluppo ETL complessi fuori perimetro, migrazioni dati storici, test di sicurezza/penetration test, licenze di terze parti, connettori "premium" di fornitori terzi, ambienti supplementari, monitoraggio enterprise esteso (SIEM del Cliente), attività onsite.

12. Variazioni (Change Request)

Qualsiasi modifica a perimetro, tempi, deliverable o prerequisiti di integrazione è gestita tramite Change Request (CR). La CR descrive oggetto e motivazione della variazione, impatti tecnici ed economici, piano e tempi, rischi e dipendenze. L'esecuzione è subordinata ad approvazione scritta del Cliente; fino a tale approvazione restano validi perimetro e tempi originari. Le attività oggetto di CR sono valorizzate a forfait o a tempo e materiali secondo offerta/quotazione; le variazioni possono comportare adeguamenti a prezzo e milestone. Le CR urgenti possono essere avviate su e-mail di autorizzazione del Cliente con formalizzazione a seguire. Restano esclusi dagli SLA standard gli elementi non ancora approvati o in corso di variazione, salvo diverso accordo scritto.

13. Accettazione e messa in esercizio

Integrazioni standard: accettazione tecnica al superamento dei test concordati nel Piano di Integrazione; messa in esercizio a esito positivo.

UAT di processo: non prevista per WMP salvo diversa pattuizione; per VMP/personalizzazioni si applica solo se indicata in Ordine/SoW (cfr. MSA §4.5).

14. Supporto e SLA

API e connettori rientrano nel perimetro dello SLA – Allegato C (finestre di manutenzione §5, esclusioni §6, gestione incidenti §7).
Per componenti ospitati su infrastrutture del Cliente si applicano i livelli di servizio del Cliente; i rimedi SLA (Service Credits) operano limitatamente ai componenti erogati/ospitati da TimeFlow (cfr. MSA §3.1 e Allegato C §3-4).

15. Documentazione e tracciabilità

TimeFlow fornisce documentazione tecnica (OpenAPI), esempi request/response, guide d'integrazione e changelog. Le chiamate API sono soggette ad audit trail e logging; è disponibile telemetria per troubleshooting e KPI di integrazione (cfr. Allegato D §2.5).

16. Prevalenza e aggiornamenti

Prevalenza documentale: Ordine → MSA → Allegato C (SLA) → Allegato D (TOMs & BC/DR) → Allegato K (cfr. MSA §18.4).

Aggiornamenti: TimeFlow può aggiornare il presente Allegato nei limiti di MSA §18.3 (nessun peggioramento sostanziale, preavviso 30 giorni); variazioni materiali richiedono accordo ai sensi di MSA §18.4 o adeguamenti strettamente necessari per conformità legale ai sensi di MSA §18.3. Nessun effetto retroattivo su attività già erogate.

Ultima modifica: 18/11/2025 – **Versione API-2025-11-18**