DigTic

DigTic for IT Teams

Technical guide for CTO, architects and integration teams

24 April 2026

Audience	CTO, architects, integration teams, security stakeholders
Purpose	Make the integration model clear and low-risk
Scope	High-level only, no sensitive implementation details

Technical overview

DigTic is API-first: partners integrate once, then issue and validate digital access across multiple use cases.

DigTic exposes a standardized access layer above existing systems. It is designed to integrate with partner platforms, not replace them.

Integration model

- REST-style API for issue, validate, use and revoke flows.
- Partner systems call DigTic from booking, event, access-control or hotel systems.
- Credentials are delivered to Apple Wallet or Google Wallet where relevant.
- Webhooks and lifecycle events can be added for partner workflows.

Security posture

- Tenant isolation is enforced by API authorization and tenant-scoped state.
- Access credentials are signed and validated before use.
- Sensitive implementation details are kept out of public documentation.
- Audit-friendly lifecycle events are stored for issue, validation, use and revoke actions.

Data and GDPR principle

- Use minimal personal data wherever possible.
- Store operational state in the EU.
- Do not put personal data on any public proof layer.
- Keep access decisions tied to tenant, ticket state, validity and usage rules.

What IT teams need to know

- No rip-and-replace is required. DigTic sits above existing systems.
- A pilot can start with one endpoint flow and one defined access scenario.

- The API model is designed to make later integrations faster.
- Physical keycards and access badges can be replaced gradually or complemented during transition.

Next step

Start with a short pilot discussion. Select one concrete use case, one partner flow, and one measurable outcome.