

Data Access & Privacy Architecture — Validation Application

Target Audience: Enterprise IT Security, Architecture Review Board (ARB), and Data Privacy Teams

Compliance Standards Addressed: ISO/IEC 27001, SOC 2 Type II, GDPR (Data Minimization & Purpose Limitation)

System Classification: Non-retaining Processing Agent (Zero Engineering Data Persistence)

Executive Summary & Non-Persistence Declaration

The Validation Application is designed as a **zero-retention, pass-through validation engine**.

[!IMPORTANT] Data Non-Copy / Non-Persistence Guarantee:

The application **never copies, replicates, stores, or warehouses customer proprietary engineering data** (CAD files, 3D geometry, BIM models, element properties, or spatial databases). All engineering data remains exclusively in Bentley's authoritative cloud repositories and is queried transiently in-memory via the official Bentley iTwin API using the user's delegated Identity Management System (IMS) token.

Core Architecture Pillars

1. User Engineering Data Access:

Accessed **exclusively** via the Bentley iTwin Platform API (<https://api.bentley.com>) over TLS 1.3, authenticated directly by the end-user's Bentley IMS OAuth 2.0 / OIDC Bearer Token. Permissions and Role-Based Access Controls (RBAC) are evaluated and enforced by Bentley Systems at query time.

2. Configuration & Rule Storage (User Store):

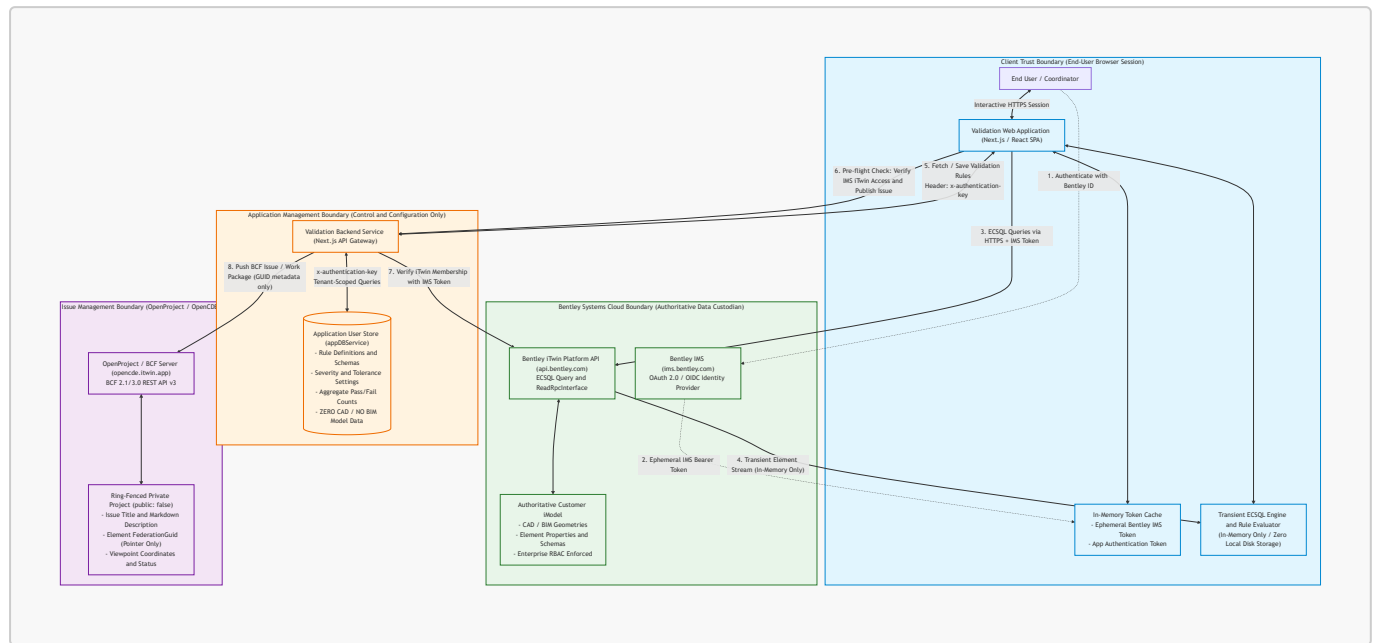
Application configurations (validation rules, severity thresholds, regex patterns, and aggregate run metrics) are stored in the application's configuration user store ([appDBService](#)). Access is strictly guarded and requires an authenticated application token ([x-authentication-key](#)). **No engineering data is stored in this database.**

3. OpenProject BCF Bridge Publishing:

Publishing issues or tasks to OpenProject (<https://opencde.itwin.app> or Bring-Your-Own OpenProject) is an optional, user-initiated action. Publishing is **strictly contingent on verifying that the user holds an active, authorized Bentley IMS token for the target iTwin**. Only lightweight issue metadata (element GUID, issue title, severity, camera viewpoint) is transmitted into ring-fenced private projects ([public: false](#)).

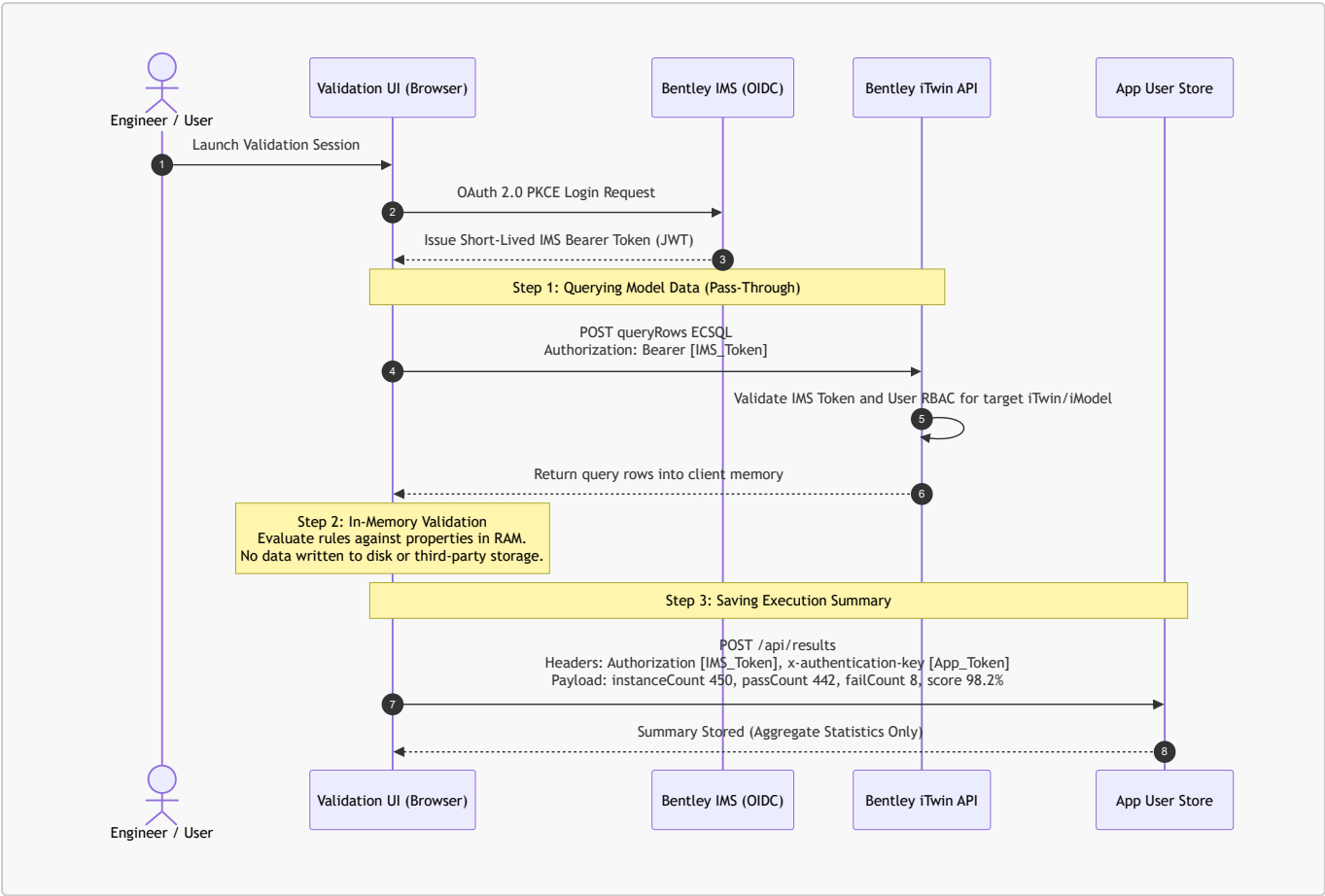
1. Data Access & Trust Boundary Diagram

The following diagram illustrates the network boundaries, trust domains, authentication handshakes, and data flows. Notice the explicit isolation between transient model processing and persistent configuration storage.

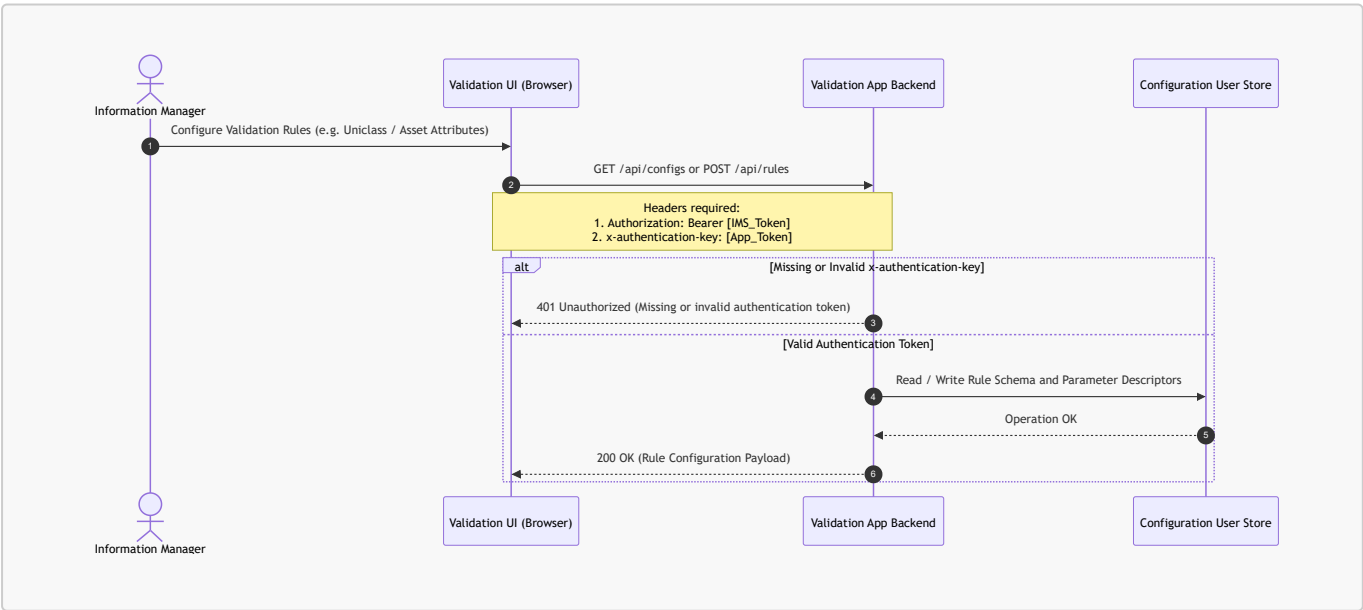


2. End-to-End Sequence & Data Lifecycle Flows

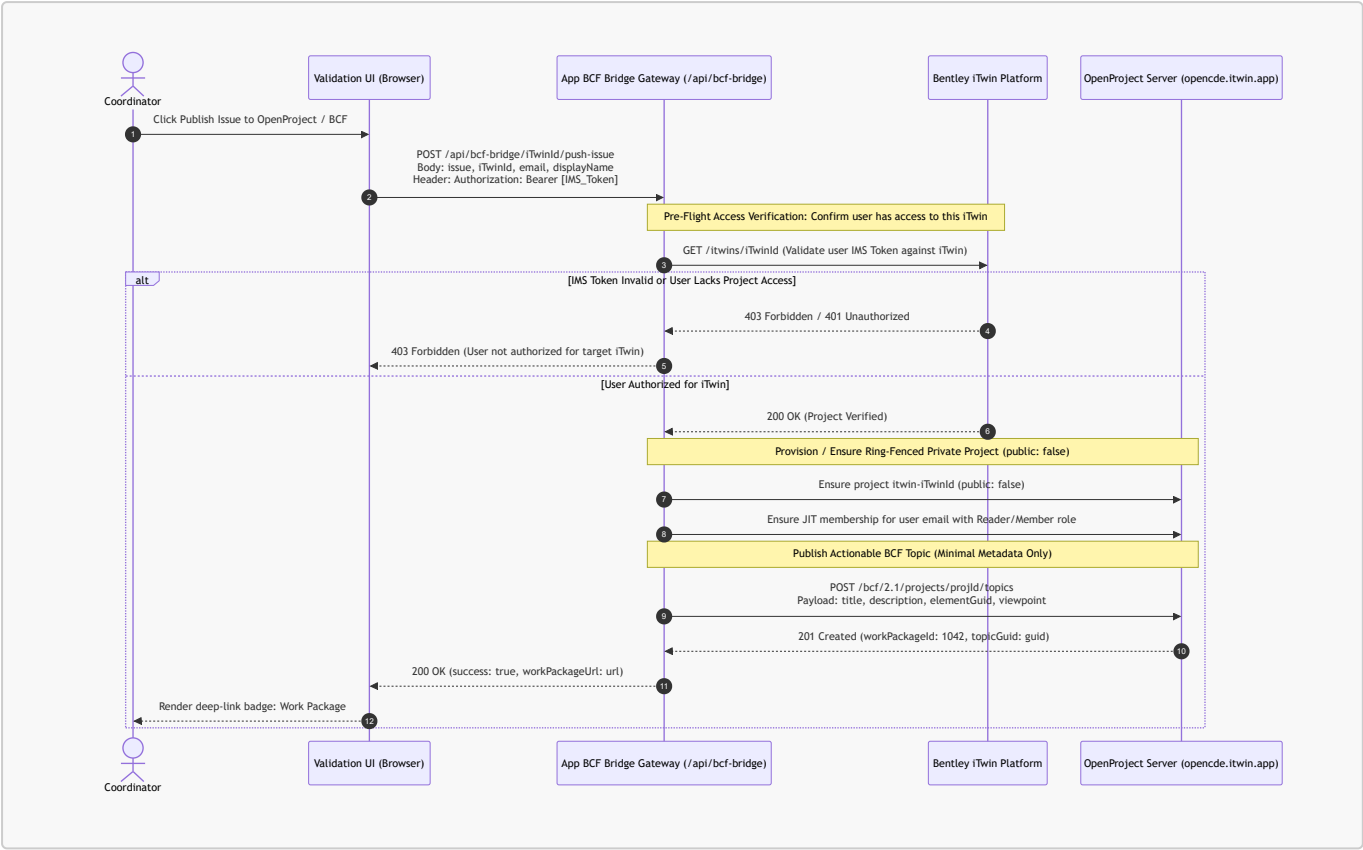
Flow A: User Model Data Access & Validation (Zero Copy Guarantee)



Flow B: Configuration & Rule Management (User Store Authentication)



Flow C: Optional Publishing to OpenProject with Pre-Flight Access Check



3. Data Classification & Storage Matrix

Data Category	Examples / Payload	Authoritative Storage Location	Retention Policy in Validation App	Protection & Security Controls
Class A: User Engineering & Model Data	3D CAD geometries, BIM elements, spatial coordinates, ECClass schemas, physical asset attributes.	Bentley Systems Cloud (api.bentley.com) exclusively.	Zero Retention (0 seconds). Processed strictly in volatile browser RAM. Discarded immediately after rule evaluation.	Encrypted in transit (TLS 1.3). Direct delegated authentication via user's Bentley IMS token. Enforces enterprise RBAC.
Class B: Validation Configurations & Rules	Rule types (REQUIRED_BUT_BLANK), property target filters, regex patterns, parameter defaults, weightings.	Application User Store (appDBService).	Persistent (as configured by project administrator).	Gated by x-authentication-key / license header and tenant identifier. Isolated per customer/tenant partition.
Class C: Execution Metrics	Total elements checked, pass count, fail count, compliance score %, timestamp.	Application User Store (appDBService).	Persistent (historical trend audit trail).	High-level summary metrics only. Contains zero element properties, zero CAD geometry, zero model content.
Class D: Published Issue Trackers	Work Package title, status, severity, target element GUID pointer, viewpoint camera vector.	OpenProject / OpenCDE BCF Server.	Persistent in OpenProject (lifecycle managed by issue tracker).	Ring-fenced private project (public: false). Requires verified IMS iTwin authorization before push.

4. Key IT Review & Security Assurances

1. No Data Duplication / Shadow Repository

- **Assertion:** The application does **not** create a secondary database or copy of customer models.
- **Technical Guarantee:** The application acts as a client querying Bentley's `IModelReadRpcInterface-3.8.0-queryRows` over HTTPS. Query results are parsed directly into memory data structures in the user's browser, evaluated against client-side or backend validation rules, and garbage-collected. No raw model dumps or geometry blobs are written to any local or remote database.

2. Delegated Identity & Access Management (Zero Shared Credentials)

- **Assertion:** The application never bypasses Bentley security policies or uses a generic service account to access engineering data.
- **Technical Guarantee:** All iModel queries inherit the authenticated user's permissions via their Bentley IMS token (OAuth 2.0 PKCE / OIDC). If a user does not have permission in Bentley to view an iTwin or iModel, the Bentley API rejects the request with `403 Forbidden`, and the validation application cannot access any data.

3. Application User Store Access Control

- **Assertion:** The configuration repository cannot be accessed anonymously or cross-tenant.
- **Technical Guarantee:** Requests to `appDBService` are inspected for the `x-authentication-key` header. If the key is missing, expired, or invalid, the request is immediately aborted before any configuration read/write operations can take place.

4. Controlled Issue Publishing (OpenProject BCF Bridge)

- **Assertion:** Data cannot be leaked to an issue tracker without verified project rights.
 - **Technical Guarantee:**
 - **Access Gate:** The BCF Bridge backend requires an active Bentley IMS token and explicitly validates that the requesting user belongs to the associated `iTwinId`.
 - **Ring-Fencing:** Projects in OpenProject are provisioned with `public: false` so that only verified project team members can view work packages.
 - **Data Minimization:** Only references (element `FederationGuid`, classification code, and anomaly description) are published. The proprietary BIM/CAD model is never attached or exported.
-

5. Security & IT Review Sign-Off Checklist

Review Dimension	Status	Architecture Evidence
Engineering Data Persistence	 NONE	No CAD/BIM model databases exist in the application stack. All model data is queried on-demand from Bentley API.
In-Transit Encryption	 PASS	TLS 1.2 / TLS 1.3 enforced for all communication (Bentley API, App DB, OpenProject).
User Authentication	 PASS	Bentley IMS OAuth 2.0 / OpenID Connect with short-lived tokens and in-memory caching.
Configuration Store Security	 PASS	Dedicated API token authentication (x-authentication-key) required for all rule & config operations.
Third-Party Publishing	 PASS	User authorization validated against Bentley IMS prior to publishing; private ring-fenced projects; minimal metadata only.
Tenant Isolation	 PASS	Strict partitioning by iTwinId and tenant credentials across all services.