

Britenet - MVP Software Requirements Specification (SRS) v4.0)

Document Purpose: This document provides the definitive and complete Software Requirements Specification (SRS) for the Minimum Viable Product (MVP) of the Britenet platform. It serves as the single source of truth for all teams. **This document is self-contained and supersedes all previous versions.**

1. Guiding Philosophy & Strategic Goal

- **Philosophy:** We are building an **intelligent operating system** for the construction project supply chain, founded on an unbreakable layer of trust. Our system must respect the chaotic reality of our users' workflows while providing an unparalleled layer of order, intelligence, and control.
- **MVP Goal:** To build and validate the core, **three-sided workflow** between the **Consultant** (the source of specifications), the **Contractor** (the source of pricing requests), and the **Supplier** (the engine of commerce).

2. Core User Personas & Roles (MVP Scope)

This MVP will focus on five primary user personas.

2.1. Britenet Platform Admin ("The Architect")

- **Objective:** To manage the entire platform ecosystem, control platform-wide standards, and manage commercial relationships with all member companies.
- **Core Permissions:**
 - Manage company subscriptions and access levels.
 - Invite and onboard new companies and their initial Admin users.
 - Control and define the master catalog structures (Categories, Families).
 - Manage the global attributes and fields available in the Datasheet templates.
 - Define catalog segments and standards for different supplier types.
 - **Access** and monitor any project or quotation package from any member **on the platform for support and auditing purposes.**

2.2. Britenet Operations Team ("The Librarian")

- **Objective:** To act as a "model supplier" by building and maintaining a trusted, high-quality library of international catalogs. This serves as a benchmark for quality and a foundational dataset for the platform's matching engine.
- **Core Permissions:** Possesses all the same permissions as a **Supplier Company Admin**.

2.3. The Supplier Company ("The Vendor")

- **Objective:** To manage their digital presence, build and control their interactive catalogs, and empower their internal teams to respond to sales opportunities with maximum speed and accuracy.
- **Persona: Supplier Admin ("The Manager")**

- **Core Permissions:** Full CRUD on catalogs, pricing control, commercial management, team & authorization rules, and profile management.
- **Persona: Supplier Team Member ("The Operator")**
 - **Core Permissions:** Granted and restricted by their Admin to perform specific roles like catalog building or quotation preparation.

2.4. The Consultant Company ("The Specifier")

- **Objective:** To create accurate, standardized technical specification packages and perform value engineering.
- **Core Permissions:** Create projects, build & send RFQs, apply a "**Digital Stamp of Approval**," and use the "Magic Button."

2.5. The Contractor Company ("The Builder")

- **Objective:** To manage the quotation process from receiving specs to securing pricing from suppliers.
- **Core Permissions:** Create projects, receive RFQs, build & send RFQs to suppliers, and use the "Magic Button."

3. Core Platform Modules (MVP Scope)

3.1. My Products - The Interactive Catalog Engine

- **Key Features:** ERCO-style Structure, Product Card Control, Structured Datasheet, Pricing Engine, Accessory Linking, Quotation Description Field.

3.2. My Projects - The Operational Workspace

- **Key Features:** Project Card / RFQ Card Structure, "Smart Triage" Workflow, Interactive Quotation Transcript, ID Generation System (v4.0).

3.3. The "Magic Button" & Workbench

- **Key Features:** Query-based Matching Engine, "Generate Alternative" Action, The "Quick Compare Workbench" with a "Mandatory On-Ramp".

4. Core Platform Rules & Permissions (The Trust Protocol)

This section defines the non-negotiable business logic and data access rules that govern the platform. These rules are the foundation of our promise of security, neutrality, and trust.

4.1. Data Privacy & Competition Firewall

- **Rule 4.1.1: Supplier Catalog Secrecy.** A user from a Supplier company is strictly forbidden from viewing the catalogs or pricing of any competing Supplier company.
- **Rule 4.1.2: Client Catalog Visibility.** A Consultant or Contractor can view all public supplier catalogs. A Supplier Admin can manage a "Visibility List" to explicitly hide their catalog from specific clients.

4.2. Internal Company Permissions & Visibility

- **Rule 4.2.1: The Admin's "God-View".** Within a single company, the "Admin" can view all Project Cards created by their team.
- **Rule 4.2.2: RFQ Access Control.** Access to a specific RFQ and its "Interactive Quotation Transcript" is strictly limited to the Admin, the creator, and any explicitly assigned team members.

4.3. "Magic Button" (Generate Alternative) - The Ethical Firewall

This protocol is the platform's most critical security feature. It prevents the misuse of our most powerful tool for corporate espionage. The backend must enforce these rules before any quotation data (the JSON file) is retrieved or processed.

- **Rule 4.3.1: Supplier Self-Analysis Only.**
 - **Condition:** When a user from a Supplier company (e.g., "Philips") uses the "Magic Button," the system **MUST** restrict the "Generate Alternative from..." option to catalogs that exist **only within their own company's domain**.
 - **Rationale:** This allows them to perform value engineering on their own product lines (e.g., comparing their premium brand vs. their budget brand) but explicitly forbids them from analyzing a competitor's products.
- **Rule 4.3.2: The "Chain of Custody" Protocol.**
 - **Principle:** A user can only access and analyze a quotation's data if they are a legitimate party in that specific transaction.
 - **The Check:** Before retrieving any quotation data from the database via its ID, the system **MUST** perform a non-negotiable permissions check. The system will ask: **"Is the current authenticated user either the original SENDER or a direct RECIPIENT of this specific quotation ID?"**
 - **Allowed Scenario:** Orascom (Contractor) receives quotation QT-000123 from Philips. Orascom logs in and uses the ID QT-000123 to import the quotation for analysis. The system checks: Is Orascom a recipient of QT-000123? **Yes**. Access is **Granted**.
 - **Forbidden Scenario (The Firewall in Action):** Orascom gives the quotation ID QT-000123 to a sales rep at El Sewedy (a competitor). The El Sewedy rep logs in and attempts to import QT-000123. The system checks: Is El Sewedy the sender? **No** (Philips is). Is El Sewedy a recipient? **No** (Orascom is). Access is **Denied**. The system must display a clear message stating that the user does not have permission to access this document.
 - **Rationale:** This protocol is our core ethical guarantee to our paying customers (the suppliers). It makes it technically impossible for their competitors to use our platform to reverse-engineer their proposals.