Center: System and Architecture overview

Introduction 🔗

This document provides a system and architecture overview for the Infoniqa Center product, including its web application (🔵 Infoniqa Center) and mobile app (Infoniqa). The assessment details the system architecture, authentication mechanisms, data storage, security measures, and relevant interfaces.

2. System Overview 🔗

2.1 Product Description 🔗

Infoniqa Center provides the following functionalities:

- **Payslips:** Sent from another product and accessible via web and mobile apps. Payslips are stored in the cloud for **2 years**.
- **Expenses Management:** Employees submit expenses, managers approve/reject, and a finance product books approved expenses. Expenses are stored in the cloud for **1 year**.
- **QR Invoices:** Finance personnel scan QR bills via the mobile app and process payments in the finance system. QR invoices remain in the cloud for **7 days**.

2.2 System Architecture 🔗

Infoniqa Center is hosted in Microsoft Azure and utilizes the following components:

- **API Management (APIM):** Secures and manages all API requests from web and mobile apps.
- **Azure Functions:** Handles business logic and communicates with other Azure components.
- **Cosmos DB:** Stores application data securely.
- **ClaimAV Container:** Performs antivirus checks on uploaded files.
- **Azure Storage (Blob Storage):** Stores files securely with encryption at rest.
- **Azure AD B2C (Infoniqa ID):** Manages authentication and authorization.

All requests from mobile and web applications pass through APIM, which validates Infoniqa ID tokens before reaching backend services.

2.3 Hosting and Data Residency 🔗

- The application and data are hosted in **Azure Switzerland (CH)**.
- Azure AD B2C accounts are stored in **Europe**.

- More information on Azure's data residency can be found here:
    - [Azure Data Residency](#)
    - [Azure AD B2C Data Residency](#)
- The system does not enforce any geolocation-based restrictions.

2.4 System Diagram 🔗
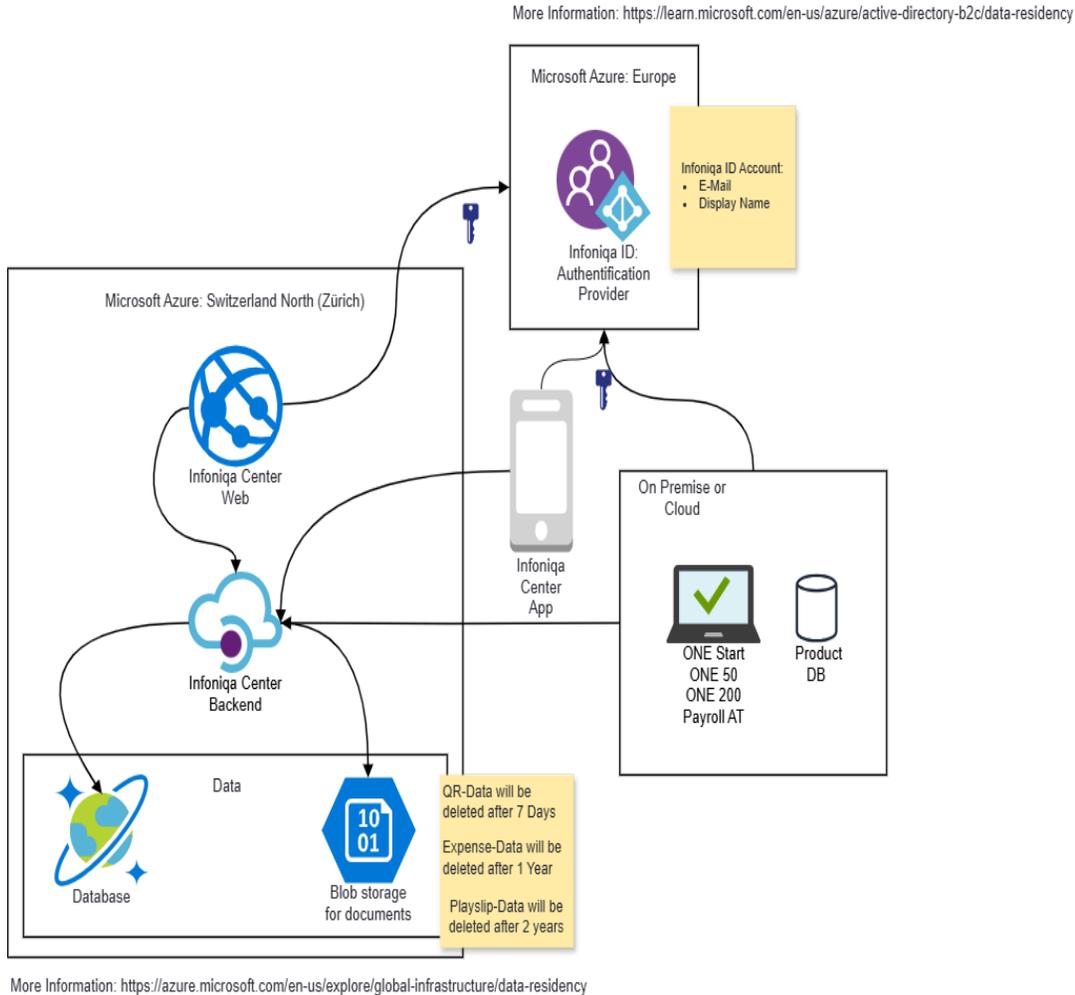
3. Technical Details 🔗

3.1 Cloud Service Model 🔗

Infoniqa Center is built using a **Platform-as-a-Service (PaaS)** model in Azure.

3.2 Technology Stack 🔗

- **Operating System:** Managed Azure services (Linux-based containers for ClaimAV, Windows/Linux for Azure Functions)
- **Database:** Azure Cosmos DB
- **APIs:** Exposed through Azure API Management
- **Authentication:** Azure AD B2C with local and social login support

3.3 Communication and Security Protocols 🔗

- **Network Communication:** HTTPS (TLS 1.2/1.3)
- **Encryption in Transit:** TLS 1.2/1.3 enforced for all API calls

- **Encryption at Rest:**
  - **Cosmos DB:** AES-256 encryption for stored data
  - **Azure Blob Storage:** AES-256 encryption for files stored in the cloud
- **Authentication Methods:**
  - Local accounts (username/password with self-service password reset)
  - Social sign-in via Google and Microsoft
  - Customer-enforced Multi-Factor Authentication (MFA)

3.4 User Account and Access Management 🔗

- **User Database:** Managed within Azure AD B2C.
- **Password Security:** Stored securely with hashing and salting.
- **Access Control:** Enforced via role-based access and token validation at APIM.
- **Account Deactivation:** Customer admins manage user access, including enabling MFA.
- **Audit Logs:** Azure AD B2C logs authentication events.

3.5 Interfaces to Other Systems 🔗

- **Payslips:** Receives data from another payroll system.
- **Expense Management:** Sends approved expenses to a financial system.
- **QR Invoices:** Integrates with financial systems for payment processing.

4. Conclusion 🔗

Infoniqa Center follows industry best practices for security, authentication, and data protection. Hosted in Microsoft Azure, the platform ensures data residency compliance and integrates with enterprise authentication solutions while maintaining strict access controls and encryption standards.