Project Documentation

Security Architecture of the Customer Service System

Paweł Murdzek

January 31, 2026

---

1 Introduction

This document presents a detailed description of the designed security architecture for a modern individual customer service system. The project implements a **Defense in Depth** approach and **Zero Trust Network Access** (ZTNA) principles, ensuring the protection of sensitive data and high service availability.

2 Design Assumptions

2.1 System Characteristics

The customer service system integrates the following key interfaces and access channels:

- **Self-care**: Web and mobile access for end customers.
- **Customer-care**: Internal portal for office employees.
- **POS (Point of Sales)**: Physical points of sale connected via the public Internet.

2.2 Description of the Designed Architecture

The logical structure of the system, divided into isolation zones, is presented below.

2.2.1 Main Components and Network Zones

The designed architecture is based on strict network segmentation to minimize the attack surface. The following zones have been defined:

- **Internet Zone (Untrusted)**: Contains end users and POS points. Incoming traffic is filtered by a **Scrubbing Center** (e.g., CloudFlare) to mitigate volumetric (DDoS) attacks before they reach the company infrastructure.
- **DMZ (Demilitarized Zone)**: A buffer zone for Internet access.
  - **NGFW**: Provides active attack detection.
  - **WAF**: Protects against Layer 7 attacks (SQL Injection, XSS) and implements Rate Limiting.

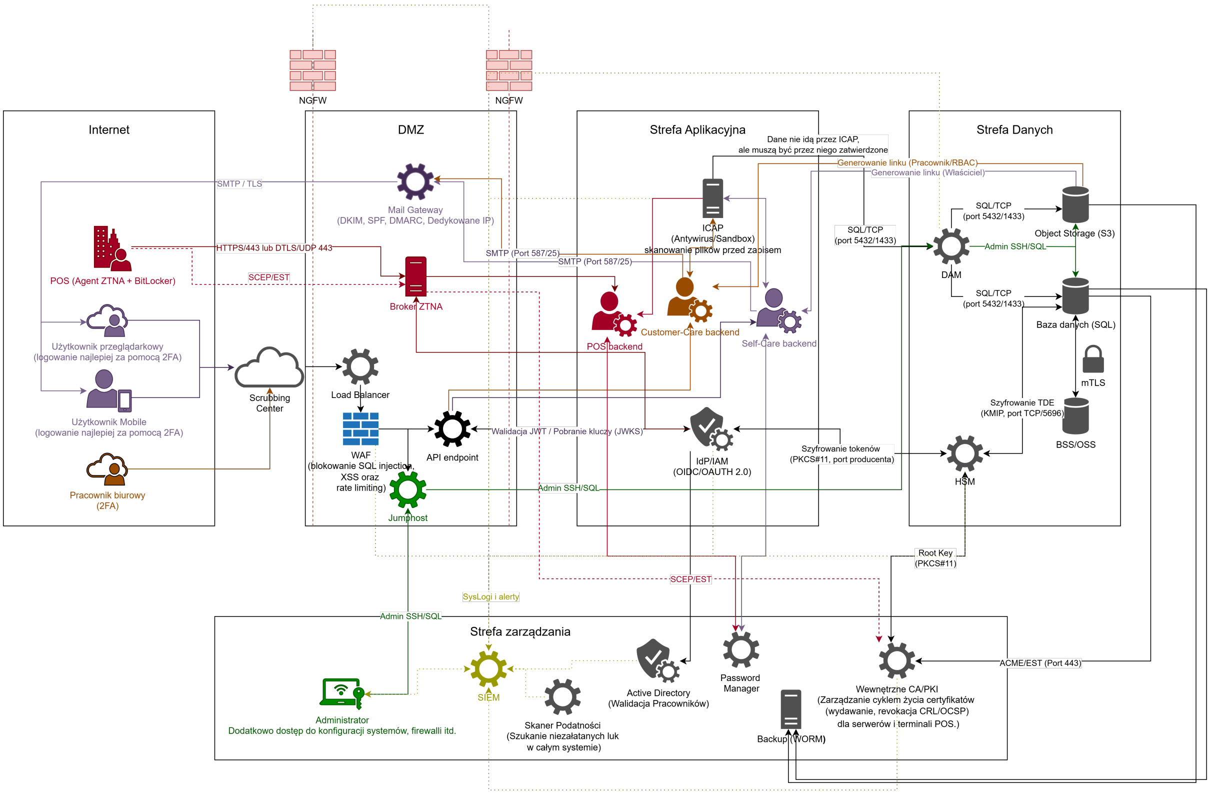

Figure 1: Reference diagram of network segmentation and control mechanisms.

  - **ZTNA Broker**: Used for securely establishing tunnels with POS points. It communicates with the IdP/IAM for user authentication using keys stored in an HSM.
  - **Mail Gateway**: Handles email traffic with DKIM, SPF, and DMARC security; used for invoice distribution.
  - **Jumphost**: Used for secure administrative access (SSH/SQL).
  - **API Gateway/Endpoint**: The central entry point for API queries, performing initial authentication via the IdP/IAM system and schema validation.
- **Application Zone**: This is where the business logic is processed. Traffic reaches this zone only after prior verification in the DMZ.
  - **Backend**: Supports POS, Self-Care, and Customer-Care services.
  - **ICAP Server**: Performs antivirus scanning and sandboxing of files uploaded by users before they are saved to the database.
  - **IdP/IAM**: Central identity system supporting OIDC/OAuth 2.0 protocols.
- **Data Zone**: The most heavily guarded network segment.
  - **SQL Databases and Object Storage (S3)**: Data storage with TDE (Transparent Data Encryption).
  - **BSS/OSS Systems**: Communicate via mTLS.
  - **HSM (Hardware Security Module)**: Secure storage of cryptographic keys (POS, Root CA Key, TDE).
  - **DAM (Database Access Monitoring)**: Real-time control and auditing of database access.
- **Management Zone**: An isolated network for administrators and security tools.
  - **Password Manager**: Central password vault and Privileged Session Management.

- **WORM Backup**: Write Once, Read Many system protecting backups against ransomware.
- **SIEM**: Collects logs and alerts from all systems.
- **Vulnerability Scanners**: Automatic detection of flaws and the latest CVEs.
- **Active Directory**: Authentication for office employees.
- **Internal CA/PKI**: Certificate lifecycle management with revocation capabilities (CRL/OCSP).

3 Applied Security Mechanisms

The project utilizes a **Defense in Depth** approach:

- **Edge Protection**: Scrubbing Center against DDoS and NGFW firewall clusters for L3/L4 traffic filtration.
- **Web Application Security (WAF)**: Blocking attacks from the OWASP Top 10 list and JWT token validation at the API Endpoint level.
- **Zero Trust Network Access (ZTNA)**: A ZTNA agent on the POS workstation (secured with BitLocker) ensures access only to specific applications.
- **Content Inspection (ICAP)**: Sending files to an AV/Sandbox scanner before they are committed to storage.
- **Data Protection**: Database encryption (TDE) using KMIP keys in an external HSM and enforced TLS/mTLS.

4 Secure Development Lifecycle (DevSecOps)

An integral part of the system is a secure CI/CD pipeline implementing the **Shift-Left Security** approach:

- **SAST**: Static Analysis Security Testing at the code commit stage.
- **DAST**: Dynamic Analysis Security Testing (automated penetration tests) run on test environments.
- **Container Security Scanning**: Checking images for known vulnerabilities (CVE) before they reach the registry.
- **Artifact Signing**: Verification of the digital signature of containers before deployment in the Application Zone.