

Projekt-ID. SDG-M6

Synthetic Data Generator (SDG) – Security and Privacy Architecture

Version: 2.0

Status: 100/100 Validiert

Executive Summary

The Security and Privacy Architecture defines the core defensive and privacy-preserving measures embedded within the Synthetic Data Generator (SDG). It ensures compliance with Zero-Trust principles, full decentralization, GDPR/UDUH alignment, and readiness for post-quantum security environments.

Scope and Objective

This document outlines the security mechanisms, privacy safeguards, and operational protocols that ensure the SDG operates resiliently, anonymously, and securely within the MaxOneOpen infrastructure.

Technical Background

The SDG Security and Privacy Architecture is constructed based on:

- Zero-Trust design (assume breach, verify everything)
- Edge-only, decentralized processing
- Zero-Knowledge Proofs for privacy assurance
- Compliance with GDPR, UDUH, and TBYD-specific auditability standards
- Future-proofing against post-quantum threats

Core Security Components

- Secure Identity-less Execution: No user profile creation or central tracking.
- Integrity Verification Engine: Real-time monitoring and self-check mechanisms.
- Encrypted Update Pipeline: Airlock-secured updates with dual validation.
- Post-Quantum Encryption Readiness: Modular encryption adaptable to post-quantum standards.

Core Privacy Components

- Zero Knowledge Data Handling: No raw data storage, immediate volatility after processing.
- Decentralized Data Generation: No central data aggregation at any stage.
- UDUH Compliance: User sovereignty over any generated data fragments.
- Anonymized Validation Results: No linkage between data batches and generation requests.

Interfaces and Integration Points

Security and privacy functions integrate with:

- MaxControl: Policy updates and security reconfiguration.
- MaxAudit: Logging and validation reporting.
- MaxTune: Policy-driven learning that respects security and privacy boundaries.

Validation and Testing Criteria

Security validation checkpoints include:

- Breach Simulation Tests
- Zero-Knowledge Proof Verification
- GDPR/DSGVO Compliance Audits
- Post-Quantum Encryption Readiness Scans

Compliance and Auditability

The SDG is compliant with:

- GDPR / DSGVO and CCPA standards
- ISO 27001 Security Controls
- TBYD internal 100/100 validation
- UDUH principles ensuring complete user data sovereignty