Service Description

Conbool

Version 1.0 – As of March 2025

Conbool GmbH
Berlepschweg 11
21079 Hamburg
Germany

info@conbool.com
https://conbool.com

CONBOOL

Content

Conbool GmbH
Berlepschweg 11
21079 Hamburg
Germany

info@conbool.com
https://conbool.com

1. Introduction

Conbool is a state-of-the-art Secure Email Gateway designed to secure business-critical communication. The solution combines enterprise-level cryptographic operations for S/MIME & PGP, certificate and key management, flexible security policies, and more in a modern platform. The goal is to make email communication for companies, Managed Service Providers (MSPs), and authorities efficient, secure, and compliant. The solution is industry-independent and available as both SaaS (Software-as-a-Service) and On-Premise.

2. Main Components

2.1 Supported Protocols

- S/MIME
- PGP

2.2 Absender- und Empfängerdefinition

- Sender:
  - ✓ All senders
  - ✓ Custom sender addresses, including the * operator
  - ✓ User-defined group selection
- Recipient:
  - ✓ All recipients
  - ✓ Custom recipient addresses
  - ✓ User-defined group selection

2.3 Cryptography

The cryptographic functions are based on the proven Bouncy Castle library, known for its flexibility, security, and continuous development. Conbool uses the Java programming language. With support for a variety of modern algorithms and protocols, it meets the highest security standards and enables reliable cryptographic email processing.

Conbool GmbH
Berlepschweg 11
21079 Hamburg
Germany

info@conbool.com
https://conbool.com

2.3.1 Encryption & Signing for Outgoing Emails

- Group Management: Manual assignment of security policies to created groups.

S/MIME (X.509 Certificates)

Encryption:

- Supported encryption rules/policies:
  - ✓ Send without encryption
  - ✓ Encrypt if possible
  - ✓ Send only encrypted
  - ✓ Send only if encryption is possible for all recipients

- Encryption algorithms:
  - ✓ AES-128
  - ✓ AES-192
  - ✓ AES-256
- Encryption modes:
  - ✓ GCM (Galois/Counter Mode)
  - ✓ CBC (Cipher Block Chaining)
- Automatic certificate detection or manual certificate assignment for encryption.
- Notification to the sender in case of a failed operation.

Signing:

- Supported signing rules/policies:
  - ✓ Send without signing
  - ✓ Sign if possible
  - ✓ Send only signed
- Signature algorithms:
  - ✓ SHA-256
  - ✓ SHA-384
  - ✓ SHA-512
- Signature modes:
  - ✓ Detached signature (Detached)
  - ✓ Enveloped signature (Enveloped)
  - ✓ Cleartext signature (Cleartext)
- Automatic certificate detection or manual certificate assignment for signing.
- Notification to the sender in case of a failed operation.

PGP (OpenPGP)

Encryption:

- Supported encryption rules/policies:
  - ✓ Send without encryption
  - ✓ Encrypt if possible
  - ✓ Send only encrypted
  - ✓ Send only if encryption is possible for all recipients
- Encryption algorithms:
  - ✓ AES-128
  - ✓ AES-192
  - ✓ AES-256
- Automatic key detection or manual key assignment for encryption.
- Notification to the sender in case of a failed operation.

Signing:

- Supported signing rules/policies:
  - ✓ Send without signing
  - ✓ Sign if possible
  - ✓ Send only signed
- Signature algorithms:
  - ✓ SHA-256
  - ✓ SHA-384
  - ✓ SHA-512
- Signature modes:
  - ✓ Detached signature (Detached)
  - ✓ Enveloped signature (Enveloped)
  - ✓ Cleartext signature (Cleartext)
- Automatic key detection or manual key assignment for signing.
- Notification to the sender in case of a failed operation.

Conbool GmbH
Berlepschweg 11
21079 Hamburg
Germany

info@conbool.com
https://conbool.com

2.3.2 Decryption & Signature Verification for Incoming Emails

S/MIME (X.509 Certificates)

Decryption:

- Supported decryption rules/policies:
  - ✓ Do not decrypt
  - ✓ Decrypt if possible
- Automatic detection of encryption algorithms
- Automatic detection of encryption modes
- Automatic certificate detection or manual certificate assignment for decryption

Signature Verification:

- Supported signature verification rules/policies:
  - ✓ Do not verify
  - ✓ Verify if possible
- Automatic detection of signature algorithms
- Automatic detection of signature modes
- Automatic certificate detection or manual certificate assignment for signature verification

PGP (OpenPGP)

Decryption:

- Supported decryption rules/policies:
  - ✓ Do not decrypt
  - ✓ Decrypt if possible
- Automatic detection of encryption algorithms
- Automatic key detection or manual key assignment for decryption

Signature Verification:

- Supported signature verification rules/policies:
  - ✓ Do not verify
  - ✓ Verify if possible
- Automatic detection of signature algorithms
- Automatic detection of signature modes
- Automatic key detection or manual key assignment for signature verification

2.4 Certificate & Key Management

- **Key & Certificate Management:**
  - ✓ Management of S/MIME certificates & PGP keys
  - ✓ Import of S/MIME certificates & PGP keys
  - ✓ Software-based encryption & decryption of certificates and keys
- **Corporate PKI:**
  - ✓ Capability to create proprietary Certificate Authorities (CAs)
  - ✓ Issuance of self-generated end-user certificates and keys (S/MIME & PGP), including revocation

2.5 Role-Based Access Control (RBAC)

- Standard Roles:
  - ✓ **Primary Owner:** Full access, including tenant deletion
  - ✓ **Owner:** Full access at the tenant level, excluding tenant deletion
  - ✓ **Operator:** Rule management, log access, certificate management
  - ✓ **Analyst:** Rule management, log access, read-only rights for certificates
  - ✓ **Auditor:** Read-only access to logs/reports
- **Two-Factor Authentication (2FA):** Authenticator app required

2.6 Tracing & Logging

- **Logging Levels:**
  - ✓ Mailflow: Sender/recipient, status, direction, mail size, message ID, envelope status, part status, timestamps
  - ✓ Cryptography: Routing index, cryptographic algorithm used, mode, email address associated with the key, success status
- **Live Dashboard:**
  - ✓ Filterable views:
  - ✓ Time period (last 24 hours/7 days/custom)
  - ✓ Maximum storage duration: 90 days
  - ✓ Metrics overview
- **Export:**
  - ✓ Logs can be exported as CSV files

3. Operating Models

3.1 SaaS Solution (Cloud)

- **Hosting**:
    - ✓ Hosted in ISO 27001-certified EU data centers with a 99.9% SLA.
    - ✓ Redundant server infrastructure.
    - ✓ Automatic scaling to handle peak loads.
- **Database:**
    - ✓ Scalable server infrastructure.
    - ✓ Data storage using PostgreSQL in EU data centers.
    - ✓ SOC2 Type 2 & HIPAA compliance.

- **Compliance & Maintenance:**
    - ✓ Integrated Data Processing Agreement (DPA).
    - ✓ Automatic security patches during maintenance windows (10:00 PM–6:00 AM).

3.2 On-Premise-Lösung

Infrastructure:

- ✓ Templates available for VMware & Proxmox.
- ✓ Full data processing sovereignty on customer systems.
- ✓ Supported operating systems: Linux (RHEL, Ubuntu).

Core Components:

- ✓ Local: Cryptography service & mail server.
- ✓ Centralized: Web interface for homepage & certificate management.

Licensing: Rental license (annual model) with optional premium support.

3.3 Trial Phase

A 7-day full-access trial of the Conbool SaaS solution is available. Conditions are described in the General Terms and Conditions (GTC) under § 4.

4. Technical Features

4.1 Cryptographic Standards

- **Algorithms:**
  - ✓ Symmetric: AES-128, AES-192, AES-256 (GCM & CBC modes).
  - ✓ Asymmetric: RSA, ECC.
  - ✓ Hashing: SHA-256, SHA-384, SHA-512.

4.2 Interoperability

- **Email Systems**:
  - ✓ Google Workspace
  - ✓ Microsoft Exchange
  - ✓ Postfix
  - ✓ Exim
  - ✓ .. and other email systems capable of forwarding emails.
- **Hybrid Environments**: Parallel integration with legacy systems.

4.3 Scalability

- ✓ **SaaS**: Dynamic resource adjustment for peak loads.
- ✓ **Multi-Tenant Capability:** Dedicated namespaces and quota management.

5. Security & Compliance

5.1 Data Security

- **Communication**: HTTPS, TLS 1.3/1.2.
- **Email Processing**: TLS, S/MIME, PGP.
- **Data Encryption**: Software-based encryption.

5.2 Compliance

Data is stored exclusively within the EU; transfers to third countries occur only in compliance with Articles 44 et seq. GDPR (e.g., Standard Contractual Clauses).

- ✓ **Certifications:** ISO 27001 certification of the cloud provider.
- ✓ **GDPR Compliance**: Integrated Data Processing Agreement (DPA); data localization within the EU.

6. Customer Experience & Support

6.1 Self-Service & Documentation

- ✓ User-friendly self-service portal.
- ✓ Comprehensive customer documentation, including step-by-step guides and FAQs.

6.2 Support Models

- **Availability:**
  - ✓ SaaS: 99% annual uptime on average.
  - ✓ On-Premise: Dependent on customer systems (recommendation: redundant infrastructure).
- **Support:**
  - ✓ Standard: Ticketing system with a guaranteed response time of 48 hours on business days.
  - ✓ Enterprise: Customizable phone support with agreed SLA response times.
- **Maintenance Windows:** Regularly scheduled outside business hours (EU: 10:00 PM–6:00 AM).