Leistungsbeschreibung

Conbool

Version 1.0 – Stand: März 2025

Conbool GmbH
Berlepschweg 11
21079 Hamburg
Deutschland

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

CONBOOL

Inhalt

Conbool GmbH
Berlepschweg 11
21079 Hamburg
Deutschland

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

1. Einführung

Conbool ist ein hochmodernes **Secure E-Mail Gateway** zur Absicherung geschäftskritischer Kommunikation. Die Lösung kombiniert Enterprise-Level kryptographische Operationen für S/MIME & PGP, Zertifikats- & Schlüsselmanagement, flexible Sicherheitsrichtlinien und mehr in einer modernen Plattform. Ziel ist es die E-Mail Kommunikation von Unternehmen, Managed Service Providern (MSPs) und Behörden effizient, sicher und compliance-konform zu gestalten. Die Lösung ist **branchenunabhängig** und sowohl als **SaaS** (Software-as-a-Service) als auch **On-Premise** verfügbar.

2. Hauptkomponenten

2.1 Unterstützte Protokolle

- S/MIME
- PGP

2.2 Absender- und Empfängerdefinition

- Absender
  - ✓ Alle Absender
  - ✓ Benutzerdefinierte Absenderadressen inkl. *-Operator
  - ✓ Eigendefinierte Gruppenauswahl
- Empfänger
  - ✓ Alle Empfänger
  - ✓ Benutzerdefinierte Empfängeradressen
  - ✓ Eigendefinierte Gruppenauswahl

2.3 Kryptographie

Die Kryptographiefunktionen basieren auf der bewährten Bouncy Castle-Bibliothek, die sich durch ihre Flexibilität, Sicherheit und kontinuierliche Weiterentwicklung auszeichnet. Conbool verwendet die Programmiersprache Java. Mit Unterstützung für eine Vielzahl moderner Algorithmen und Protokolle erfüllt sie höchste Sicherheitsstandards und ermöglicht zuverlässige kryptographische Verarbeitungen von E-Mails.

2.3.1 Verschlüsselung & Signierung bei ausgehenden E-Mails

- Gruppenmanagement: Manuelle Zuweisung von Sicherheitsrichtlinien an erstellten Gruppen.

S/MIME (X.509-Zertifikate)

Verschlüsselung

- Unterstütze Verschlüsselungsregeln/-richtlinien:
  - ✓ Ohne Verschlüsselung senden
  - ✓ Verschlüsseln, wenn möglich
  - ✓ Nur verschlüsselt senden
  - ✓ Nur senden, wenn für alle Empfänger verschlüsselt werden kann
- Verschlüsselungsalgorithmen:
  - ✓ AES-128
  - ✓ AES-192
  - ✓ AES-256
- Verschlüsselungsmodi:
  - ✓ GCM (Galois/Counter Mode)
  - ✓ CBC (Cipher Block Chaining)
- Automatische Zertifikatserkennung oder manuelle Zertifikatszuweisung für Verschlüsselung.
- Benachrichtigung an den Absender bei fehlgeschlagener Operation

Signierung

- Unterstützte Signierungsregeln/-richtlinien
  - ✓ Ohne Signierung senden
  - ✓ Signieren, wenn möglich
  - ✓ Nur signiert senden
- Signaturalgorithmen:
  - ✓ SHA-256
  - ✓ SHA-384
  - ✓ SHA-512
- Signaturmodi:
  - ✓ Abgetrennte Signatur (Detached)
  - ✓ Umschlossene Signatur (Enveloped)
  - ✓ Klartext-Signatur (Cleartext)
- Automatische Zertifikatserkennung oder manuelle Zertifikatszuweisung für Signierung.
- Benachrichtigung an den Absender bei fehlgeschlagener Operation

PGP (OpenPGP)

Verschlüsselung

- Unterstütze Verschlüsselungsregeln/-richtlinien:
  - ✓ Ohne Verschlüsselung senden
  - ✓ Verschlüsseln, wenn möglich
  - ✓ Nur verschlüsselt senden
  - ✓ Nur senden, wenn für alle Empfänger verschlüsselt werden kann
- Verschlüsselungsalgorithmen:
  - ✓ AES-128
  - ✓ AES-192
  - ✓ AES-256
- Automatische Schlüsselerkennung oder manuelle Schlüsselzuweisung für Verschlüsselung.
- Benachrichtigung an den Absender bei fehlgeschlagener Operation

Signierung

- Unterstützte Signierungsregeln/-richtlinien
  - ✓ Ohne Signierung senden
  - ✓ Signieren, wenn möglich
  - ✓ Nur signiert senden
- Signaturalgorithmen:
  - ✓ SHA-256
  - ✓ SHA-384
  - ✓ SHA-512
- Signaturmodi:
  - ✓ Abgetrennte Signatur (Detached)
  - ✓ Umschlossene Signatur (Enveloped)
  - ✓ Klartext-Signatur (Cleartext)
- Automatische Schlüsselerkennung oder manuelle Schlüsselzuweisung für Signierung.
- Benachrichtigung an den Absender bei fehlgeschlagener Operation

2.3.2 Entschlüsselung & Signaturprüfung bei eingehenden E-Mails

S/MIME (X.509-Zertifikate)

Entschlüsselung

- Unterstütze Entschlüsselungsregeln/-richtlinien:
  - ✓ Nicht entschlüsseln
  - ✓ Entschlüsseln, wenn möglich
- Automatische Erkennung der Verschlüsselungsalgorithmen
- Automatische Erkennung der Verschlüsselungsmodi
- Automatische Zertifikatserkennung oder manuelle Zertifikatszuweisung für Entschlüsselung

Signaturprüfung

- Unterstützte Signaturprüfungsregeln/-richtlinien
  - ✓ Nicht verifizieren
  - ✓ Verifizieren, wenn möglich
- Automatische Erkennung der Signaturalgorithmen
- Automatische Erkennung der Signaturmodi
- Automatische Zertifikatserkennung oder manuelle Zertifikatszuweisung für Signaturprüfung

PGP (OpenPGP)

Entschlüsselung

- Unterstütze Entschlüsselungsregeln/-richtlinien:
  - ✓ Nicht entschlüsseln
  - ✓ Entschlüsseln, wenn möglich
- Automatische Erkennung der Verschlüsselungsalgorithmen
- Automatische Schlüsselerkennung oder manuelle Schlüsselzuweisung für Entschlüsselung

Signaturprüfung

- Unterstützte Signaturprüfungsregeln/-richtlinien
  - ✓ Nicht verifizieren
  - ✓ Verifizieren, wenn möglich
- Automatische Erkennung der Signaturalgorithmen
- Automatische Erkennung der Signaturmodi
- Automatische Schlüsselerkennung oder manuelle Schlüsselzuweisung für Signaturprüfung

2.4 Zertifikats- & Schlüsselmanagement

- **Schlüssel- & Zertifikatsverwaltung**
    - ✓ Verwaltung von S/MIME Zertifikaten & PGP Schlüsseln
    - ✓ Import von S/MIME Zertifikaten & PGP Schlüsseln
    - ✓ Softwarebasierte Verschlüsselung & Entschlüsselung von Zertifikaten & Schlüsseln.

- **Unternehmenseigene PKI**
    - ✓ Möglichkeit zur Erstellung eigener Zertifizierungsstellen (Certificate Authorities)
    - ✓ Ausstellung selbstgenerierter Endbenutzerzertifikate und -schlüssel (S/MIME & PGP) einschließlich Widerruf

2.5 Rollenbasierte Zugriffskontrolle (RBAC)

- **Standardrollen**:
    - ✓ **Primary Owner:** Vollzugriff inkl. Tenantlöschung
    - ✓ **Owner:** Vollzugriff auf Tenantebene exkl. Tenantlöschung
    - ✓ **Operator:** Regelverwaltung, Logs-Einsicht, Zertifikatsverwaltung
    - ✓ **Analyst:** Regelverwaltung, Logs-Einsicht, Leserechte Zertifikate.
    - ✓ **Auditor:** Lesezugriff auf Logs/Reports.
- **Zweifaktor Authentifizierung**: Authenticator App.

2.6 Tracing & Protokollierung

- **Protokollierungsebenen**:
  - ✓ Mailflow: Sender/Empfänger, Status, Richtung, Mailgröße, Message ID, Envelope Status, Part Status, Zeitstempel,
  - ✓ Kryptographie: Routing-Index, Kryptographie: Verwendeter Algorithmus, Modi, E-mail adresse des Schlüssels, Erfolgsstatus
- **Live-Dashboard:**
  - ✓ **Filterbare Ansichten:**
  - ✓ Zeitraum (letzte 24h/7 Tage/benutzerdefiniert)
  - ✓ Maximal 90 Tage Speicherung
  - ✓ Metriken
- **Export**:
  - ✓ Export der Logs als CSV.

3. Betriebsmodelle

3.1 SaaS-Lösung (Cloud)

- **Hosting**:
  - ✓ In ISO 27001-zertifizierten EU-Rechenzentren mit 99,9% SLA
  - ✓ Redundanter Aufbau der Serverinfrastruktur
  - ✓ Automatische Skalierung zur Bewältigung von Spitzenlasten.
- **Datenbank:**
  - ✓ Skalierbare Serverinfrastruktur
  - ✓ Speicherung von Daten durch PostgresSQL in EU-Rechenzentren
  - ✓ SOC2 Type2 & HIPPA compliant
- **Compliance & Wartung:**
  - ✓ Integrierte AVV
  - ✓ Automatische Sicherheitspatches (Nachtfenster 22:00-6:00).

3.2 On-Premise-Lösung

- **Infrastruktur:**
  - ✓ Templates für VMware & Proxmox.
  - ✓ Volle Datenverarbeitungshoheit auf Kundensystemen
  - ✓ Linux (RHEL, Ubuntu)
- **Kernkomponenten:**
  - ✓ **Lokal:** Kryptographieservice & Mailserver.
  - ✓ **Zentral:** Webinterface zur Homepage & Zertifikatsverwaltung
- **Lizenzierung:** Mietlizenz (Jahresmodell) inkl. optionalem Premium-Support.

3.3 Testphase

7-tägiger Vollzugriff auf die SaaS-Lösung Conbool. Bedingungen wie in den AGBs unter „§ 4 Testphase des Dienstes“ beschrieben.

4. Technische Merkmale

4.1 Kryptografische Standards

- **Algorithmen:**
  - ✓ Symmetrisch: AES-128, AES-192, AES-256 (GCM- & CBC-Modus).
  - ✓ Asymmetrisch: RSA, ECC.
  - ✓ Hashing: SHA-256, SHA-384, SHA-512.

4.2 Interoperabilität

- **E-Mail-Systeme**:
  - ✓ Google Workspace
  - ✓ Microsoft Exchange
  - ✓ Postfix
  - ✓ Exim
  - ✓ .. und weitere E-Mail-Systeme, die E-Mails weiterleiten können
- **Hybride Umgebungen**: Parallele Integration mit Legacy-Systemen.

4.3 Skalierbarkeit

- ✓ **SaaS**: Dynamische Ressourcenanpassung für Lastspitzen.
- ✓ **Multi-Tenant-Fähigkeit**: Dedizierte Namespaces und Kontingentsteuerung.

5. Sicherheit & Compliance

5.1 Datensicherheit

- **Kommunikation**: HTTPS, TLS 1.3/1.2.
- **Mailverarbeitung**: TLS, S/MIME, PGP.
- **Datenverschlüsselung**: Softwarebasierte Verschlüsselung.

5.2 Compliance

Daten werden ausschließlich innerhalb der EU gespeichert; Drittstaatentransfers erfolgen nur unter Einhaltung der Art. 44 ff DSGVO (z.B., Standardvertragsklauseln).

- ✓ **Zertifizierungen**: ISO 27001 des Cloud Providers.
- ✓ **DSGVO-Konformität**: AVV inkludiert; Datenlokalisierung in der EU.

6. Kundenerlebnis & Support

6.1 Self-Service & Dokumentation

- ✓ Benutzerfreundliches Self-Service Portal
- ✓ Umfangreiche Kundendokumentation samt Schritt-für-Schritt Anleitungen & FAQ

6.2 Supportmodelle

- **Verfügbarkeit**:
  - ✓ SaaS: 99 % im Jahresmittel.
  - ✓ On-Premise: Abhängig von Kundensystemen (Empfehlung: Redundante Infrastruktur).
- **Support**:
  - ✓ **Standard**: Ticketing-System mit garantierter Reaktionszeit von 48 Stunden an Werktagen
  - ✓ **Enterprise**: Individuell vereinbarter Telefonsupport mit abgeschlossener SLA-Response Time Level.
- **Wartungsfenster**: Regulär außerhalb der Geschäftszeiten (EU: 22:00–06:00 Uhr).