



Bundesamt
für Sicherheit in der
Informationstechnik

ICC

Releasebeschreibung für JULIA MailOffice als E-Mail Gateway der Virtuellen Poststelle Version 2.0

ICC GmbH, 30.05.07

Version 2.0

Zusammenfassung

Dieses Dokument enthält eine Release-Beschreibung von JULIA MailOffice, das als Mail-Gateway der Virtuellen Poststelle eingesetzt wird. Die Funktionalität dieser JULIA MailOffice-Version wurde auf der Basis der folgenden Dokumente definiert:

- BA BOL xxxx/03
- Fachkonzept für die Virtuelle Poststelle (VPS) als Basiskomponente Datensicherheit von Bund Online 2005, Version 2.3.1 vom 30.05.2003
- DV-Grobkonzept für die Virtuelle Poststelle, Version 3.6.1 15.12.2003
- Migrationskonzept für das SMTP-Gateway der Virtuellen Poststelle 2.0 (VPS 2.0), Version 1.0 vom 13.05.2004
- Beschlüsse des Lenkungsausschusses
- JULIA MailOffice in der Version vom März 2004

© 2004 BSI Bundesamt für Sicherheit in der Informationstechnologie, Bonn
ICC GmbH, Köln

Version 2.0, Freigabe Juni 2005

Erstellt von:
ICC GmbH, Köln

Dieses Dokument kann bezogen werden über:
Bundesamt für Sicherheit in der Informationstechnik
Referat 111
Postfach 200363
D 53133 Bonn

E-Mail: vps@bsi.bund.de

ICC Solutions GmbH
Luxemburger Straße 79 - 83
D 50354 Hürth

Tel.: +49 (22 33) 9 46 96-0
Fax: +49 (22 33) 9 46 96-33
E-Mail: sales@iccsec.com

Weitere Informationen finden Sie unter:

<http://www.bsi.de/fachthem/vps>
<http://www.iccsec.com>

Inhaltsverzeichnis

1 Einführung.....	1
1.1 Überblick.....	1
2 Releasebeschreibung.....	2
2.1 Überblick.....	2
2.2 Geforderte Funktionalität gemäß Auftrag.....	2
2.2.1 Dokumente.....	2
2.2.2 Funktionsumfang von JULIA MailOffice.....	3
2.3 Zusätzliche Funktionalität.....	5
2.4 Betriebsvoraussetzungen.....	7
2.4.1 Überblick.....	7
2.4.2 Unterstützte Systemumgebungen.....	8
2.4.3 Unterstützte MTAs.....	8
2.4.4 Benötigte Komponenten.....	8
2.4.5 Nicht benötigte Komponenten.....	9
3 Literatur.....	10

1 Einführung

1.1 Überblick

JULIA MailOffice ist ein zentraler Verschlüsselungs- und Signaturproxy für die kryptographische Behandlung ein- und ausgehender E-Mails und operiert als eigenständiges SMTP-Gateway. JULIA MailOffice kann deshalb nahtlos in eine bestehende SMTP-Umgebung integriert werden.

Für die Integration von JULIA MailOffice in die Virtuelle Poststelle 2.0 (VPS 2.0) und um die in [VPS 02/03] und [VPS 03/03] sowie in BA BOL xxxx/03 festgelegte Funktionalität zu implementieren müssen Anpassungen gegenüber der "normalen" JULIA MailOffice-Version vorgenommen werden. Die durchzuführenden Aktivitäten sind im Migrationskonzept für das SMTP-Gateway der Virtuellen Poststelle 2.0 (VPS 2.0) dargestellt. Die Anforderungen an JULIA MailOffice wurden durch entsprechende Beschlüsse in den Lenkungsausschüssen konkretisiert.

Dieses Dokument ist eine Release-Beschreibung zu JULIA MailOffice als Teil der VPS 2.0.

2 Releasebeschreibung

2.1 Überblick

In den folgenden Abschnitten werden die Eigenschaften von JULIA MailOffice beschrieben, welche die Software innerhalb der VPS 2.0 besitzt. Eine genauere Beschreibung der jeweiligen Funktionen ist in [JULIA 03/02] und [JULIA 03/03] zu finden.

2.2 Geforderte Funktionalität gemäß Auftrag

2.2.1 Dokumente

Folgende Dokumente sind Bestandteil der Lieferung von JULIA MailOffice für die Integration in die VPS 2.0:

- Release-Beschreibung: Überblick über die zur Mailkomponente der Virtuellen Poststelle (VPS) gehörenden Komponenten
- Benutzerhandbuch (inklusive Installationsanweisungen): Installationsanweisung für JULIA MailOffice, Beschreibung der Konfigurationsparameter von JULIA MailOffice und den zugehörigen Modulen)
- Installationsanweisung: Installationsanweisung für den VPS-Dispatcher (Installation von JULIA MailOffice ist im Benutzerhandbuch beschrieben), Konfiguration des Kernsystems der VPS für die Zusammenarbeit mit JULIA MailOffice,
- Betriebskonzept: Wie sieht die Betriebsumgebung der Mail-Komponente aus? Wie kann Hoch-Verfügbarkeit realisiert werden? Wie wird JULIA MailOffice in die VPS integriert? Kleine Hilfestellung bei der Fehlersuche
- Feinkonzept: Grobe Beschreibung der Komponenten von JULIA MailOffice, die für die Integration in die VPS relevant sind und im Rahmen der Migration angepaßt bzw. neu erstellt wurden. Komponenten der stand-alone Version von JULIA MailOffice und Komponenten, die nicht verändert wurden, sind in diesem Dokument nicht beschrieben.
- Beschreibung der Schnittstelle(n) für die Erstellung von JULIA MailOffice Plugin-Modulen für Exchange oder Lotus Notes

2.2.2 Funktionsumfang von JULIA MailOffice

Die Software besitzt folgenden Funktionsumfang:

- Verwaltung der Regeln für Verschlüsselung und Signatur innerhalb von JULIA MailOffice:
Die Regeln, die die automatische Verschlüsselung und/oder Signatur von Nachrichten steuern, werden innerhalb von JULIA MailOffice verwaltet. Diese Regeln können sowohl mit Hilfe eines Editors als auch durch ein Web-Frontend administriert werden.
- Erkennung und Behandlung (Signaturprüfung) von PKCS#7 Attachments:
JULIA MailOffice erkennt, ob ein Anhang (Attachment) zu einer Mail signiert wurde und führt in diesem Fall eine Signaturprüfung durch.
- Bezug der Zeitstempel für ein- und ausgehende Mails vom VPS-Kernsystem, konfigurierbar im Regelwerk:
Nachrichten können von JULIA MailOffice mit einem Zeitstempel versehen werden. Dieser Zeitstempel kann auf der Basis der Systemzeit eines Servers („interner Zeitstempel“) bezogen werden. Zeitstempel können jedoch insbesondere für eine qualifizierte Signatur von einem entsprechenden System („externer Zeitstempel“) erhalten werden.
- Signatur des Prüfprotokolls (konfigurierbar):
JULIA MailOffice erstellt zu jeder Nachricht einen Prüfbericht, aus dem hervorgeht, welche kryptographischen Operationen und mit welchem Ergebnis auf die Nachricht angewendet wurden.
- Quittungs-E-mails für externe Benutzer inklusive Prüfprotokoll (Konfigurierbar):
Damit ein externer Benutzer (zum Beispiel ein Bürger) feststellen kann, ob seine Nachricht von der Poststelle angenommen wurde,
- Anbindung des OCSP/CRL-Relays via Document Interface:
Sowohl das OCSP-/CRL-Relay als auch das Kernsystem werden von JULIA MailOffice aus mit Hilfe des Document Interface (DI) angesprochen. Die Umsetzung von JULIA MailOffice-Kommandos auf entsprechende DI-Aufrufe erfolgt mit Hilfe einer Java-Anwendung (VPS-Dispatcher), welcher die JULIA MailOffice-Kommandos über eine Socket-Verbindung entgegen nimmt und DI-Aufrufe übersetzt. Das Ergebnis eines DI-Aufrufs wird ebenfalls über die Socket-Verbindung an JULIA MailOffice weitergereicht. Der VPS-Dispatcher kann auf jedem beliebigen Server installiert und betrieben werden, bevorzugt jedoch auf dem Server des Kernsystems der VPS, da sich dort bereits die benötigte JAVA-Umgebung befindet.
- Log-Funktionalität: Protokoll-Datei und syslog (NG):
Alle Meldungen von JULIA MailOffice können an den Syslog-Daemon geschickt werden, der auf dem JULIA MailOffice-Server läuft. Dieser syslog-Daemon kann so konfiguriert werden, dass die Meldung an einen zentralen Log-Server weitergeleitet werden. Dies erfolgt mit Hilfe UDP-Pakete. Soll die Kommunikation zwischen den Log-Servern über TCP geschehen, ist auf beiden Servern syslog-NG (Syslog Next Generation) einzusetzen.
- Erstellung von Laufzetteln, Integration des Laufzettels der VPS in das Prüfprotokoll von JULIA MailOffice:
Alle von JULIA MailOffice durchgeführten Operationen werden auf einem so genannten Laufzettel zusammengefasst und einer Mail angehängt. Meldungen des VPS-Kernsystems werden integriert.
- Umverschlüsselung eingehender Mails:

Durch eine entsprechende Konfiguration von JULIA MailOffice ist es möglich, vor der Auslieferung einer Mail an einen internen Empfänger diese von JULIA MailOffice erneut verschlüsseln zu lassen. Das bedeutet, eine eingehende verschlüsselte Mail wird, entschlüsselt, geprüft und vor der eigentlichen Zustellung mit einem anderen Schlüssel neu verschlüsselt.

- Erkennung von qualifizierten E-Mails und senden an eine bestimmte Adresse:
Ist eine E-Mail bzw. ein Attachment qualifiziert signiert, wird diese von JULIA MailOffice als solche erkannt und an eine bestimmte Mail-Adresse gesendet. Dieser Mechanismus kann verwendet werden, um zum Beispiel eine Sichtprüfung vornehmen zu lassen oder ein Archivierung durchzuführen.
- Optionale Prüfung, ob Absender und Signierer gleich sind:
JULIA MailOffice stellt fest, ob der Absender einer Email derjenige ist, der diese Email signiert hat.

2.3 Zusätzliche Funktionalität

Folgende Funktionen werden von JULIA MailOffice unterstützt, sind jedoch nicht für den Betrieb zusammen mit der VPS erforderlich bzw. wurden nicht gefordert:

- **Mandantenfähigkeit:**
JULIA Mailoffice kann für mehrere Mandanten betrieben werden. Jedem der Mandaten ist mindestens eine Mail-Domain zugeordnet. Für die Verwaltung von Mandanten (Anlegen von neuen Mandanten, Löschen von Mandanten und Änderung von einer Mandanten-Konfiguration) werden entsprechende Funktionen von JULIA MailOffice bereitgestellt.
- **Cluster-Fähigkeit**
JULIA MailOffice kann in einem Cluster betrieben werden. Die Definition des Clusters erfolgt mit Hilfe der Web-Schnittstelle. Innerhalb des JULIA MailOffice-Cluster gibt es keinen expliziten Master. Die Konfiguration kann auf jedem beliebigen Knoten innerhalb des Clusters definiert werden. Nach der Synchronisation besitzt jeder Knoten die vollständige Information. Auf diese Art und Weise wird die Ausfallsicherheit erhöht. Fällt einer der Knoten aus, besitzen alle übrigen Knoten die vollständige Information über die Struktur des Clusters. Bei der Synchronisation der Knoten werden sowohl Konfigurationsdaten als auch gespeicherte Zertifikate, Schlüssel etc. abgeglichen.

Eine genauere Beschreibung der Cluster-Funktionen ist in [JULIA 02/03] enthalten. Wie ein JULIA MailOffice-Cluster in eine bestehende Mail-Infrastruktur integriert werden kann ist in [JULIA 03/03] beschrieben.

- **Unterstützung von GnuPG**
JULIA MailOffice verwendet eine GnuPG-Instanz für die Implementation von PGP-Funktionen. Das entsprechende JULIA MailOffice-Modul kann per Konfiguration eingeschaltet werden, so dass PGP zusammen mit SMIME verwendet werden kann. Da JULIA MailOffice GnuPG verwendet, wird der IDEA-Algorithmus *nicht* unterstützt.
- **JULIA MailOffice Verifikationsmodul, Bezug von CRLs via http(s)**
JULIA MailOffice kann „stand-alone“ verwendet werden. In diesem Fall werden die kryptographischen Operationen nicht mit Hilfe des Kernsystems der VPS durchgeführt, sondern JULIA MailOffice verwendet eigene Module für diese Operationen. Das JULIA MailOffice-Verifikationsmodul implementiert alle Funktionen für die Prüfung von Zertifikaten.
- **Bezug öffentlicher Schlüssel aus dem Dateisystem**
JULIA MailOffice kann „stand-alone“ verwendet werden. In diesem Fall werden die kryptographischen Operationen nicht mit Hilfe des Kernsystems der VPS durchgeführt, sondern JULIA MailOffice verwendet eigene Module für diese Operationen. Für den Bezug öffentlicher Schlüssel verwendet JULIA MailOffice so genannte Public-Key-Module. Eines dieser Module erlaubt die Speicherung im und den Bezug von öffentlichen Schlüsseln im Dateisystem des JULIA MailOffice-Servers.
- **Bezug öffentlicher Schlüssel von LDAP-Servern**
- **JULIA MailOffice kann „stand-alone“ verwendet werden. In diesem Fall werden die**

kryptographischen Operationen nicht mit Hilfe des Kernsystems der VPS durchgeführt, sondern JULIA MailOffice verwendet eigene Module für diese Operationen. Für den Bezug öffentlicher Schlüssel verwendet JULIA MailOffice so genannte Public-Key-Module. Eines dieser Module erlaubt den Bezug von öffentlichen Schlüsseln von einem LDAP-Server. Es können nahezu beliebig viele LDAP-Server (8192) verwendet werden.

- **Bezug privater Schlüssel aus dem Dateisystem**
JULIA MailOffice kann „stand-alone“ verwendet werden. In diesem Fall werden die kryptographischen Operationen nicht mit Hilfe des Kernsystems der VPS durchgeführt, sondern JULIA MailOffice verwendet eigene Module für diese Operationen. Für den Bezug privater Schlüssel verwendet JULIA MailOffice so genannte Private-Key-Module. Eines dieser Module erlaubt die Speicherung im und den Bezug von privaten Schlüsseln im Dateisystem des JULIA MailOffice-Servers.

2.4 Betriebsvoraussetzungen

2.4.1 Überblick

JULIA MailOffice ist ein zentraler Verschlüsselungs- und Signaturproxy für die kryptographische Behandlung ein- und ausgehender E-Mails und operiert als eigenständiges SMTP-Gateway auf einem oder mehreren (Cluster) eigenen Server. JULIA MailOffice wird in den SMTP-Datenstrom "eingeschleift".

Die Leistungsfähigkeit der Hardware für JULIA MailOffice sollte sich an den bereits verwendeten Mail-Servern orientieren (siehe auch [JULIA 04/04]). Für die Skalierung der Hardware sind Parameter wie

- Anzahl der echt parallel verarbeiteten Mails pro Sekunde
- Durchschnittliche Größe der zu verschlüsselnden Mails

von hoher Bedeutung. Folgende Faustregeln gelten:

- Die Bearbeitungszeit für verschlüsselte Mails steigt um etwa 10 bis 30 Prozent, sofern die kryptographischen Operationen auf dem JULIA MailOffice Server durchgeführt werden. Wird die Kryptographie vom Kernsystem zur Verfügung gestellt, entsteht auf dem JULIA MailOffice Server keine zusätzliche Last, sofern der VPS-Dispatcher nicht auf dem JULIA-Server betrieben wird. Allerdings definieren das Kernsystem und die Qualität der Netzwerkverbindung zwischen JULIA MailOffice und dem Kernsystem der VPS die zusätzliche Latenzzeit, die bei der Verarbeitung signierter oder verschlüsselter Mails entsteht.
Wird der VPS-Dispatcher auf dem JULIA MailOffice Server betrieben, sind $n \times 15$ MB zusätzlich für den RAM-Ausbau zu veranschlagen. Der Parameter "n" bezeichnet die Anzahl der parallel abzuarbeitenden Mails.
- Für jede Mail benötigt JULIA MailOffice etwa 8 MB. Das heißt, Der RAM-Ausbau sollte um $n \times 8$ MB größer sein als der des "normalen" Mail Servers, wobei "n" die Anzahl der parallel verarbeiteten Mails ist.

Das VPS-Kernsystem befindet sich auf einem eigenen Rechner bzw. Cluster. Die Wahl der Hardware sollte gemäß der Dokumentation zur VPS gewählt werden.

2.4.2 Unterstützte Systemumgebungen

- SUN Solaris auf Sparc
 - Solaris 8
 - Solaris 9
- Linux auf Intel-32-Bit-Systemen
 - SuSE, Version 7.3 oder aktueller
 - Redhat, Version 8 oder aktueller
 - Debian, stable Release

Für den VPS-Dispatcher wird auch Windows (2000 oder XP) unterstützt.

2.4.3 Unterstützte MTAs

- sendmail in einer aktuelleren Version als 8.8
- postfix (wird bei Bedarf mit JULIA MailOffice installiert)

2.4.4 Benötigte Komponenten

- JULIA MailOffice
 - syslog oder syslog ng Protokolldienst
 - OpenSSL, Version 0,96 oder aktueller
 - OpenSSH
 - bash, Version 2.04 oder aktueller
- VPS Dispatcher
 - SUN JDK 1.4.2 Release 4 bzw. das für die VPS verwendete JDK
 - VPS 2.0 Class Files, mindestens Release Candidate 4, werden zusammen mit dem VPS-Dispatcher installiert

- VPS
 - VPS mit Kernsystem und OCSP-/CRL-Relay sowie deren Administrationskomponenten, mindestens die Version Governikus 2.0.0.1.b

2.4.5 Nicht benötigte Komponenten

Folgende Komponenten werden von JULIA MailOffice bzw. dem VPS-Dispatcher *nicht* benötigt:

- Application Server (Servlet Engine und/oder EJB-Container)
- Datenbank-System (RDBMS)

3 Literatur

- [JULIA 02/03] JULIA MailOffice Benutzerhandbuch, ICC GmbH, 2003
- [JULIA 03/03] JULIA MailOffice Betriebskonzept, ICC GmbH, 2003
- [JULIA 04/03] JULIA MailOffice Betriebskonzept für VPS, ICC GmbH, 2004
- [JULIA 04/04] JULIA MailOffice Installation mit VPS, ICC GmbH, 2004
-
- [VPS 02/03] Fachkonzept für die virtuelle Poststelle als Basiskomponente
Datensicherheit von Bund Online 2005, V2.3.1, BSI, IBM
- [VPS 03/03] DV-Grobkonzept- Architektur der virtuellen Poststelle
(Version von Dezember 2003), IBM
- [VPS 04/01] BA BOL xxx/03