Finanzportal

TECHNISCHE DOKUMENTATION

Architekturbeschreibung und Verschlüsselung der Applikation EMMA

Version: D6.1.4
Aktualisiert durch: Michail Kislow
Letzte Aktualisierung: 16.11.2020

VERSIONIERUNG

Datum	Version	Verfasser	Bemerkung
16.11.2020	D6.1.4	Michail Kislow	Initialversion

KONTAKTPERSONEN

Name	E-Mail-Adresse	Telefonnummer	Abteilung
Michail Kislow	michail.kislow@sparkassen-finanzportal.de	030-24636-89956	Emma

INHALT

1 SERVERLANDSCHAFT

1.1 Cloud-Service-Provider

- The unbelievable Machine Company GmbH mit Sitz in Berlin
- ISO-27001 und PCI-DSS Zertifizierung

1.2 Rechenzentrum

- e-shelter
- High-End Rechenzentrumsinfrastruktur (TIER III / V RZ-Klassifizierung)
- Duale Strom- und Notstromversorgung
- Zwei Einspeisungen auf der 10 kV Ebene
- Redundante Versorgung für alle kritischen techn. Gebäudeanlagen
- (Klima-, Kälte-, Lüftungs- und Sicherheitsanlagen)
- Separate Brandschutzzonen
- Rauchmelder mit Brandfrühesterkennung (VESDA)

1.3 Plattformen

- Dedizierte und virtualisierte Server

1.4 Hardware

- Router (redundant)
- A10 Loadbalancer (redundant)
- FortiGate Firewall (redundant)
- Fusion-io SSD Storage (redundant) für Datenbanken
- Zertifizierte Serverhardware mit ILO-Überwachung

1.5 Hochverfügbarkeit

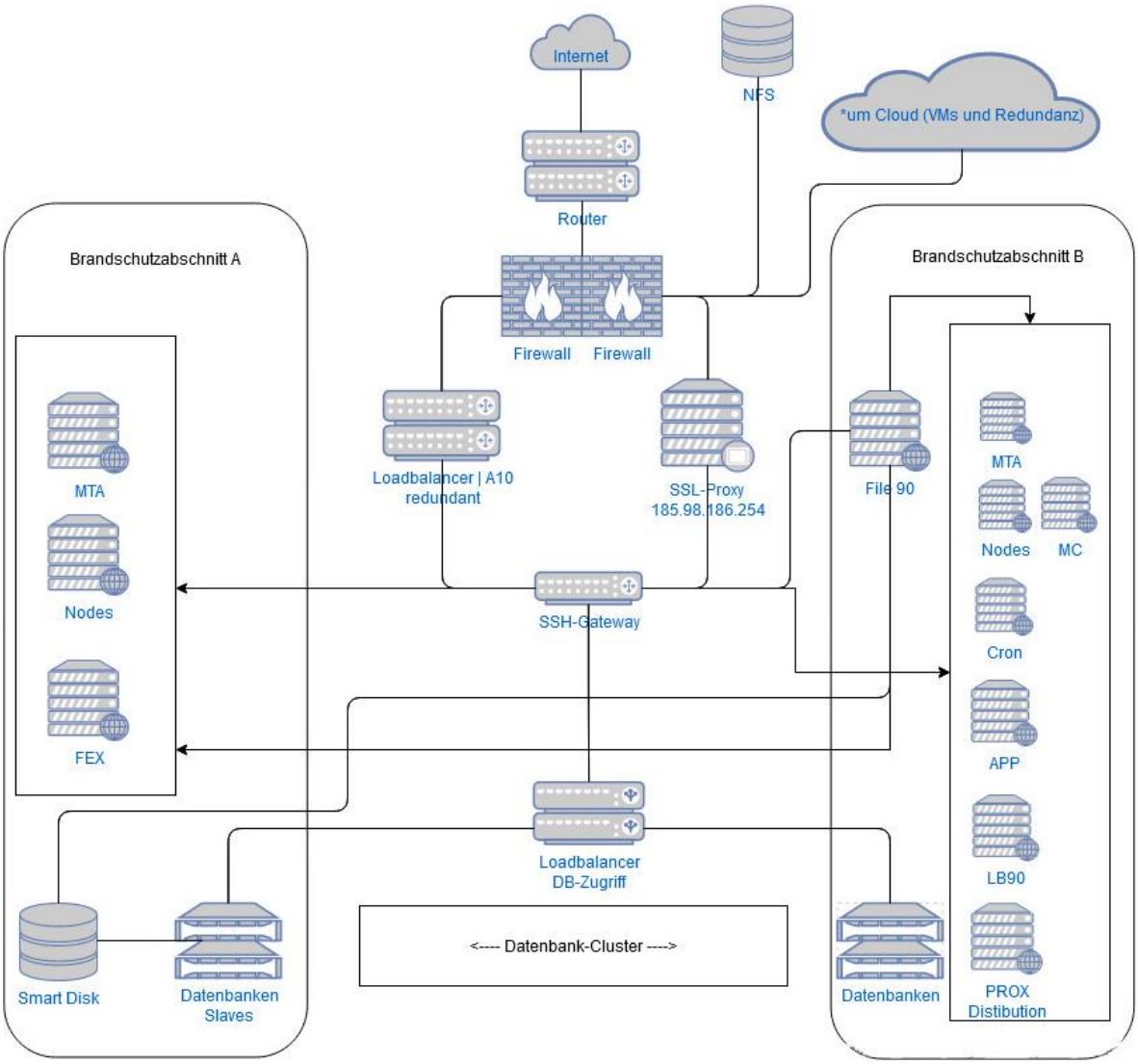
- Getrennte Hypervisor-Zonen
- Getrennte Storage-Systeme (redundant)
- HAProxy (redundant)

1.6 Komponenten

- Datenbankcluster (redundant)
- LB + Application-Server (Oberfläche; redundant)
- Memory-Server (Sessions, Queues; redundant)
- Cronjob-Server (redundant)
- File-Server (Medienverwaltung; Webspace; redundant)
- Versandcluster / MTA (redundant)
- File-Exchange-Server (Dateiaustausch mit Kunden; redundant)
- Fax-Server
- Monitoring-Server
- Backups per Snapshot-Technologien (redundant)

2 TOPOLOGIE

2.1 Topologie Piktogramm



2.2 Topologie Erläuterungen

Die Kommunikation innerhalb der Infrastruktur erfolgt über einzelne segmentierte VLANs. Vor der Kontrolle durch die Firewall regelt ein redundanter Loadbalancer (A10) das Routing und die SSL-Verschlüsselung. Die SSL-Verschlüsselung und Terminierung werden nach aktuellem Stand über 2 Umgebungen betrieben. Genauere Informationen entnehmen Sie bitte dem Punkt 3 „Verschlüsselung“ dieses Dokuments. Anfragen werden über einen weiteren Loadbalancer mit Proxyfunktion an die entsprechenden Server verteilt. Diese sind je nach Funktion in separaten Brandschutzabschnitten platziert. Die Kommunikation dieser Server verläuft untereinander in Abhängigkeit der jeweiligen Funktionen:

- Nodes: Diese Maschinen dienen der Personalisierung während des Versands
- File90: Hierüber werden die Kundendaten (Importfiles | Exportfiles), Mediendaten und der Quellcode der Applikation bereitgestellt
- MTAs: (Mail Transfer Agent) – hierbei handelt es sich um die Versandmaschinen
- FEX: intern bereitgestellter File Exchange Server für den Datenaustausch über (S)FTP
- Cron: Server zur Verarbeitung von Cron-Jobs
- LB90: Interner Loadbalancer mit Proxyfunktion und Webserver-Log
- PROX: Verteilt die Versendungen zu den jeweiligen MTAs und Nodes
- APP: Wird zur Darstellung der Oberfläche und den zugrunde liegenden Prozessen genutzt
- *um Cloud: hier werden alle Maschinen redundant (als VM) gespiegelt
- Smart Disk: Hierbei handelt es sich um einen Backupserver, welcher Daten von den Datenbank-Slaves und dem File90 sichert
- SSH-Gateway: erlaubt eine gesicherte Verbindung zu den einzelnen Servern

Das für die Weiterentwicklung und das Testing der Applikation genutzte DEV-System befindet sich in einem vom Live-System getrennten Netz innerhalb der dargestellten *um-Cloud.

3 VERSCHLÜSSELUNG

3.1 Allgemeine Erläuterungen

Für die SSL/TLS-Verschlüsselung werden nach aktuellem Stand 2 unterschiedliche Systeme betrieben. Diese dienen sowohl dem Zugang zur und der Kommunikation mit der Applikation.

Innerhalb der Applikation als auch bei der Webkommunikation hängt die Verwendung der TLS-Version von der gewählten Umgebung ab. Genauere Informationen können Sie den Punkten 3.4 und 3.5 entnehmen.

3.2 Versandverschlüsselung

Während des Versands über die Applikation EMMA erfolgt die Verschlüsselung je nach Konfiguration der Gegenstelle über SSL respektive TLS. Beim TLS-Handshake werden aktuell die Versionen v1, v1.1 und v1.2 unterstützt. Je nach Konfiguration des gegnerischen Mailservers wird dabei jeweils die höchste Version genutzt. Die Stufe an Sicherheit, die erreicht wird, hängt somit größtenteils von der Gegenstelle ab. Falls die Gegenstelle keine Kommunikation via TLS anbietet, wird standardmäßig unverschlüsselt versendet. Allerdings besteht mandantenbezogen und rekursiv die Möglichkeit, einen Versand ausschließlich via TLS zu erzwingen. Sollte die Gegenstelle in diesem Fall kein TLS unterstützen, wird die E-Mail nicht an den Empfänger versendet und stattdessen ein Bounce erzeugt.

Die am Account hinterlegten Einstellungen für die Versandverschlüsselung und deren Stärke sind komplett unabhängig von der SSL-Terminierung der Webserverabrufe.

3.3 Cipher-Suites

„Cipher-Suites“ – zu Deutsch „Chiffren-Sammlungen“ bezeichnen eine standardisierte Sammlung an kryptografischen Verfahren. Sie bestimmen welche Algorithmen ein Webserver für den Webverkehr akzeptiert. Die aktuell für die Verschlüsselung via TLS verwendeten Cipher-Suites entnehmen Sie bitte dem Anhang unter dem Punkt 5.1 „Unterstützte Cipher-Suites A10“. Sowie dem Punkt 5.2 „Unterstütze Cipher-Suites SSL-Proxy“.

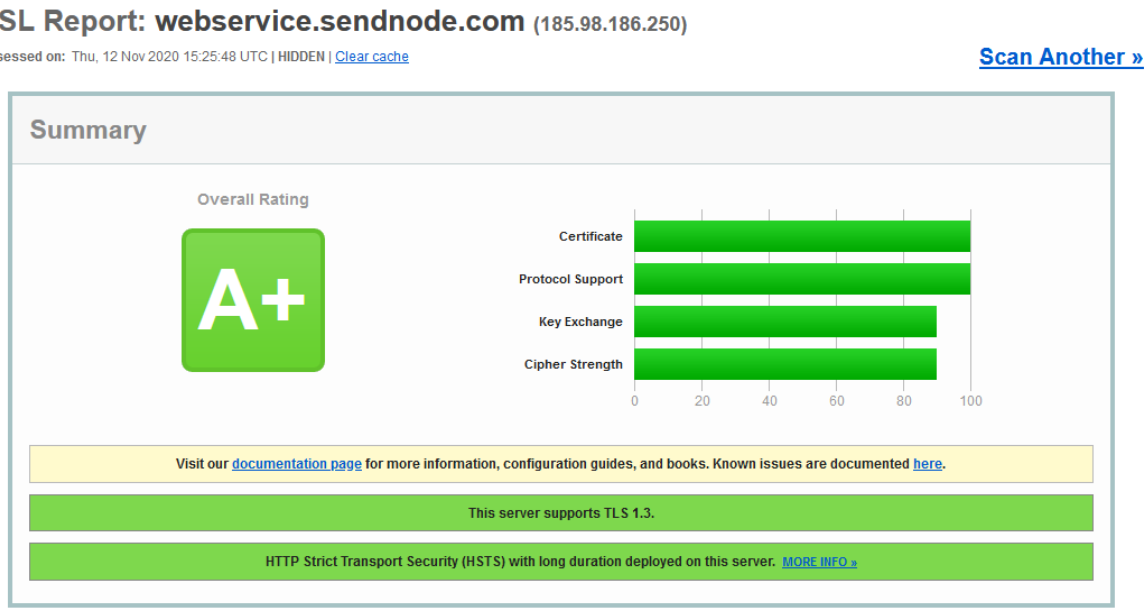
3.4 Verschlüsselung über A10-Loadbalancer

Die A10-Umgebung wird für die Verschlüsselung der in EMMA genutzten Redirect- und Logindomains genutzt und unterstützt aktuell auch Cipher-Suites, die nicht mehr dem Stand der Technik entsprechen. Dies ist dadurch begründet, dass eine Vielzahl an Kunden noch ältere Programmierumgebungen und Systeme verwenden, die einen höheren Verschlüsselungsgrad leider nicht unterstützen.

Um Ihnen das höchste Maß an Sicherheit zu bieten, empfehlen wir Ihnen daher für die Nutzung der Applikation EMMA die Verwendung einer eigenen Redirectdomain über unseren SSL-Proxy. Genauere Informationen entnehmen Sie bitte dem folgenden Punkt.

3.5 Verschlüsselung über SSL-Proxy

Seit September 2020 wird neben der A10-Umgebung ein zusätzlicher Proxy für die SSL/TLS-Terminierung betrieben, welche künftig die A10-Umgebung ablösen wird. Hierbei erfolgt eine ausschließliche Verschlüsselung per TLS 1.2 bzw. TLS 1.3. Für die Verschlüsselung können sowohl speziell von Ihnen bereitgestellte Zertifikate als auch Let's Encrypt-Zertifikate verwendet werden.



Grundsätzlich gilt zu beachten, dass der neue SSL-Proxy zunächst ausschließlich mit SNI-fähigen (Server Name Indication) Browsern kompatibel ist.

4 DKIM-VERSCHLÜSSELUNG | AUTHENTIFIZIERUNG UND PERSISTENZ

Bei DKIM (**D**omain **K**ey **I**dentifier **M**ail) handelt es sich um ein Authentifizierungsverfahren, das entwickelt wurde, um gefälschte Absender-Adressen in E-Mails aufzudecken. Hierbei werden zunächst zwei Schlüssel (Keys) angelegt: ein privater und ein öffentlicher. Der öffentliche Schlüssel wird im DNS unter der Versanddomain hinterlegt. Der private Schlüssel ist nicht öffentlich zugänglich und dient dazu, die digitale Signatur der E-Mail zu erstellen.

Die versendete E-Mail erhält dabei einen **speziellen DKIM-Header**, u.a. bestehend aus dem **Verweis zum öffentlichen Schlüssel im DNS-Eintrag** der Versanddomain, dem **Hashwert über den normalisierten Inhalt des Mailings** sowie der digitalen Signatur über verschiedene Header der E-Mail (From, To, Subject etc., sowie den DKIM-Header selbst).

Der entgegennehmende Server ruft zunächst den öffentlichen Schlüssel der Domain im DNS-Eintrag ab und prüft damit, ob die digitale Signatur gültig ist. Ist diese gültig, wird anschließend der Hashwert des Inhalts der E-Mail berechnet und kontrolliert, ob dieser mit dem Hashwert im DKIM-Header übereinstimmt. **Damit ist sichergestellt, dass der Inhalt der E-Mail auf seinem Weg zum Empfänger unverändert blieb**.

Im Falle einer nach Versand veränderten E-Mail, würde der eigentliche Inhalt der E-Mail nicht mehr mit dem normalisierten Hashwert über den Body der E-Mail übereinstimmen. Somit wäre der DKIM-Header ungültig. Würde der Hashwert im DKIM-Header verändert, wäre die digitale Signatur damit nicht mehr gültig. Ohne den privaten Schlüssel (zu dem niemand Zugang hat, außer dem Inhaber) kann jedoch keine neue gültige Signatur erstellt werden.

Falls durch den Kunden keine eigene Versanddomain inklusive DKIM verwendet wird, wird automatisch der DKIM-Eintrag von EMMA verwendet.

5 ANHANG: UNTERSTÜTZE CIPHER-SUITES

5.1 Unterstütze Cipher-Suites A10-Umgebung

0 AES-128-CBC
1 AES-128-CBC-HMAC-SHA1
2 AES-128-CBC-HMAC-SHA256
3 AES-128-CFB
4 AES-128-CFB1
5 AES-128-CFB8
6 AES-128-CTR
7 AES-128-ECB
8 AES-128-OFB
9 AES-128-XTS
1 0AES-192-CBC
1 1AES-192-CFB
1 2AES-192-CFB1
1 3AES-192-CFB8
1 4AES-192-CTR
15 AES-192-ECB
16 AES-192-OFB
17 AES-256-CBC
18 AES-256-CBC-HMAC-SHA1
19 AES-256-CBC-HMAC-SHA256
20 AES-256-CFB
21 AES-256-CFB1
22 AES-256-CFB8
23 AES-256-CTR
24 AES-256-ECB
25 AES-256-OFB
26 AES-256-XTS
27 BF-CBC
28 BF-CFB
29 BF-ECB
30 BF-OFB
31 CAMELLIA-128-CBC
32 CAMELLIA-128-CFB
33 CAMELLIA-128-CFB1
34 CAMELLIA-128-CFB8
35 CAMELLIA-128-ECB
36 CAMELLIA-128-OFB
37 CAMELLIA-192-CBC
38 CAMELLIA-192-CFB
39 CAMELLIA-192-CFB1
40 CAMELLIA-192-CFB8
41 CAMELLIA-192-ECB

42 CAMELLIA-192-OFB
43 CAMELLIA-256-CBC
44 CAMELLIA-256-CFB
45 CAMELLIA-256-CFB1
46 CAMELLIA-256-CFB8
47 CAMELLIA-256-ECB
48 CAMELLIA-256-OFB
49 CAST5-CBC
50 CAST5-CFB
51 CAST5-ECB
52 CAST5-OFB
53 DES-CBC
54 DES-CFB
55 DES-CFB1
56 DES-CFB8
57 DES-ECB
58 DES-EDE
59 DES-EDE-CBC
60 DES-EDE-CFB
61 DES-EDE-OFB
62 DES-EDE3
63 DES-EDE3-CBC
64 DES-EDE3-CFB
65 DES-EDE3-CFB1
66 DES-EDE3-CFB8
67 DES-EDE3-OFB
68 DES-OFB
69 DESX-CBC
70 RC2-40-CBC
71 RC2-64-CBC
72 RC2-CBC
73 RC2-CFB
74 RC2-ECB
75 RC2-OFB
76 RC4
77 RC4-40
78 RC4-HMAC-MD5
79 SEED-CBC
80 SEED-CFB
81 SEED-ECB
82 SEED-OFB
83 aes-128-cbc
84 aes-128-cbc-hmac-sha1
85 aes-128-cbc-hmac-sha256
86 aes-128-ccm
87 aes-128-cfb
88 aes-128-cfb1

89 aes-128-cfb8
90 aes-128-ctr
91 aes-128-ecb
92 aes-128-gcm
93 aes-128-ofb
94 aes-128-xts
95 aes-192-cbc
96 aes-192-ccm
97 aes-192-cfb
98 aes-192-cfb1
99 aes-192-cfb8
100 aes-192-ctr
101 aes-192-ecb
102 aes-192-gcm
103 aes-192-ofb
104 aes-256-cbc
105 aes-256-cbc-hmac-sha1
106 aes-256-cbc-hmac-sha256
107 aes-256-ccm
108 aes-256-cfb
109 aes-256-cfb1
110 aes-256-cfb8
111 aes-256-ctr
112 aes-256-ecb
113 aes-256-gcm
114 aes-256-ofb
115 aes-256-xts
116 bf-cbc
117 bf-cfb
118 bf-ecb
119 bf-ofb
120 camellia-128-cbc
121 camellia-128-cfb
122 camellia-128-cfb1
123 camellia-128-cfb8
124 camellia-128-ecb
125 camellia-128-ofb
126 camellia-192-cbc
127 camellia-192-cfb
128 camellia-192-cfb1
129 camellia-192-cfb8
130 camellia-192-ecb
131 camellia-192-ofb
132 camellia-256-cbc
133 camellia-256-cfb
134 camellia-256-cfb1
135 camellia-256-cfb8

136 camellia-256-ecb
137 camellia-256-ofb
138 cast5-cbc
139 cast5-cfb
140 cast5-ecb
141 cast5-ofb
142 des-cbc
143 des-cfb
144 des-cfb1
145 des-cfb8
146 des-ecb
147 des-ede
148 des-ede-cbc
149 des-ede-cfb
150 des-ede-ofb
151 des-ede3
152 des-ede3-cbc
153 des-ede3-cfb
154 des-ede3-cfb1
155 des-ede3-cfb8
156 des-ede3-ofb
157 des-ofb
158 desx-cbc
159 id-aes128-CCM
160 id-aes128-GCM
161 id-aes128-wrap
162 id-aes192-CCM
163 id-aes192-GCM
164 id-aes192-wrap
165 id-aes256-CCM
166 id-aes256-GCM
167 id-aes256-wrap
168 id-smime-alg-CMS3DESwrap
169 rc2-40-cbc
170 rc2-64-cbc
171 rc2-cbc
172 rc2-cfb
173 rc2-ecb
174 rc2-ofb
175 rc4
176 rc4-40
177 rc4-hmac-md5
178 seed-cbc
179 seed-cfb
180 seed-ecb
181 seed-ofb

5.2 Unterstütze Cipher-Suites SSL-Proxy

- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCMSHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSACHACHA20-POLY1305
- ECDHE-RSA-CHACHA20-POLY1305
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-CHACHA20-POLY1305
- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES256-GCM-SHA384
- DHERSA-AES256-GCM-SHA384