EBF Onboarder Security Whitepaper

03 Apr 2024
öffentlich
version 2.2

VERSION	DATE	EDITOR	CHANGES
1.0	15 Mar 2019	Thomas Klütsch	Official Release, error corrections, added PCI certificate
1.1	13 Jan 2020	Thomas Klütsch	Added ISO certificate and more details in several chapters
1.2	15 Jun 2020	Thomas Klütsch	New PlusServer certificates
1.3	09 Jul 2020	Thomas Klütsch	New system architecture image
1.4	17 Dez 2020	Thomas Klütsch	New TÜV certificates (PlusServer), changes in chapter 9
1.5	05 Feb 2021	Thomas Klütsch	Changes in chapter 11 and 12, update PCI certificate, added 9001 certificate.
1.6	20 Jul 2022	Guido Strucksberg	Changes: New EBF Certificate New PCI Certificate PlusServer Format changes Responsible
1.7	24 Aug 2022	Guido Strucksberg	ISO 9001 Certificate PlusServer updated
1.8	23 Jan 2023	Guido Strucksberg	PCI Certificate PlusServer updated
1.9	05 May 2023	Guido Strucksberg	Chapter 02: Diagram updated
2.0	06 Jun 2023	Guido Strucksberg	“ISO 27001 Certificate PlusServer” updated
2.1	1 Jul 2023	Guido Strucksberg	Updating Ch 04.
2.2	**3 April 2023**	**Guido Strucksberg**	**Updated PCI Certificate PlusServer (Ch 16)**

Table of Contents

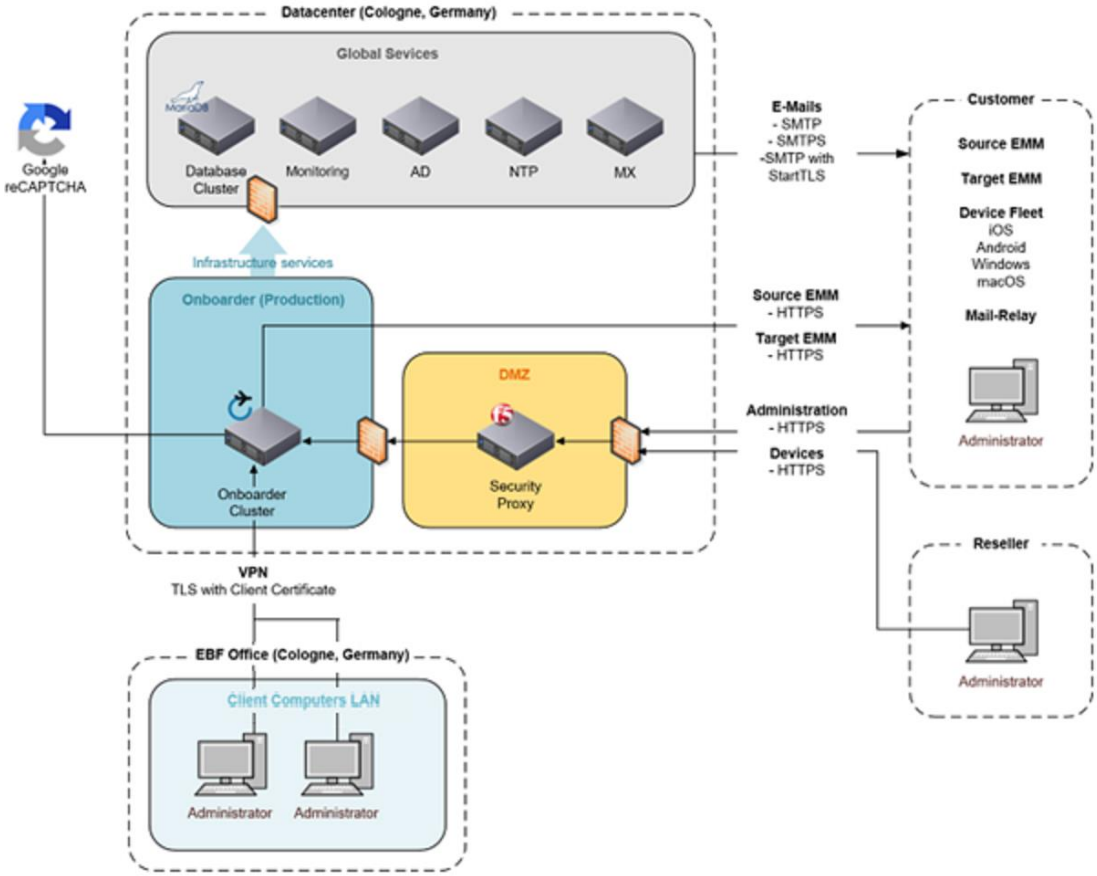
01. General

This Whitepaper provides information about the EBF Onboarder service focusing on security related aspects of the infrastructure, data processing and communication.

EBF GmbH is ISO 27001 certified. The certification is proof that EBF invests sufficiently in information and IT security, protect confidential data sufficiently against misuse, attacks, loss and disclosure and that we guarantee high availability of IT systems at the same time.

02. System Architecture

The following picture gives an overview of the EBF Onboarder system architecture, components, protocols used and communication partners.



03. Hosting

The EBF Onboarder service is hosted in a HA data center provided by PlusServer GmbH in Cologne/Germany. PlusServer is ISO 27001 certified.

04. Firewalls

Incoming communication is allowed only on port 443. Outgoing communication is allowed on ports used by the different API endpoints and additionally SMTP.

Please make sure the Onboarder IP address (out-app.ebf.com; 62.138.245.79) is whitelisted for accessing the source and target EMM systems.

05. Authentication

Each tenant needs to authenticate at the administration console of the EBF Onboarder service. Multi-factor authentication can be enabled for tenant administrators.

06. Role based access control

The EBF Onboarder service users can have different roles:

- Tenant administrator
- Additional tenant administrator

Data visibility and functionality are restricted for each role.

07. Session expiration

User sessions expire after 30 minutes.

08. Personal data handling

08.1. Personal data being stored

The EBF Onboarder service needs to store user data and device data to migrate devices between EMM systems. Data is stored in a MariaDB database. Personal data include the following:

- Name
- Email address
- Device name
- Phone number
- Device serial number / IMEI
- Device ID in source EMM
- Device ID in target EMM

08.2. Data storage duration

Personal data is needed as long as the customer runs the migration projects. After completing the migration, the customer may delete the projects which leads to an anonymization of the personal data stored in database.

PERSONAL DATA FIELDS	ANONYMIZED VALUES
Name	No Name
Email address	noname@ebf.com
Device name	Dummy Device
Phone number	000000
Device serial number / IMEI	XXXXXXXX
Device ID in source EMM	XXXXXXXX
Device ID in target EMM	0

09. Data encryption

Customer admin passwords are salted and hashed when stored in the database. The EMM API passwords for source and target systems and SMTP passwords are encrypted with AES256.

10. External APIs

Communication with related EMM systems is done using the official APIs of the EMM providers. REST communication always uses port 443. SOAP-API ports may vary for different instances of those EMMs.

EMM	API
Afaria (SAP)	SOAP
BlackBerry UEM	SOAP
Good for Enterprise	SOAP
Intune (Microsoft)	REST
jamf	REST
MaaS360 (IBM)	REST
Meraki (Cisco)	REST
MobileIron (Core / Cloud)	REST
Sophos	REST
SOTI	REST
Workspace ONE (VMWare)	REST
XenMobile (Citrix)	REST

11. Logging

The EBF Onboarder service has an audit log stored in the database. It contains information about:

- User logins (available for 5 years)
- User actions (create migration projects, send invitations) (available for 5 years)
- System events (available for 30 days)

Additionally, there is a rolling Tomcat log (available for 7 days), that provides the following information:

- API requests
- Error messages

12. Backups

Automatic backup of data (database dump and log files) is done every night to a SAN. Backups are rolled over after a period of 5 weeks. The backup storage is physically protected within an ISO 27001 certified data center. Encryption of data at rest is not performed on a storage level.

13. ISO 27001 Certificate EBF

Certificate

Standard **ISO/IEC 27001:2013**

Certificate Registr. No. **01 153 1800745**

Certificate Holder:

EBF-EDV Beratung Föllmer GmbH
Gustav-Heinemann-Ufer 120-122
50968 Köln
Germany

Scope: Consulting, development, implementation, hosting and support services for the Digital Workplace and relevant Enterprise Mobility Technologies

Statement of Applicability (SoA): dated 09.03.2022

Proof has been furnished by means of an audit that the requirements of ISO/IEC 27001:2013 are met.

Validity: The certificate is valid from 2022-06-21 until 2025-06-20.

2022-05-05

TÜV Rheinland Cert GmbH
Am Grauen Stein · 51105 Köln

www.tuv.com

DAkkS Deutsche Akkreditierungsstelle D-ZM-16031-01-00

TÜVRheinland®
Precisely Right.

14. ISO 27001 Certificate PlusServer

ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

TÜV SÜD Management Service

CERTIFICATE

The Certification Body
of TÜV SÜD Management Service GmbH

certifies that

plusserver

plusserver gmbh
Venloer Str. 47
50672 Köln
Germany

has established and applies
an Information Security Management System
according to "Statement of Applicability" for

Provisioning and operation of the cloud services 'pluscloud VMware' and 'pluscloud open' and 'Cloud Connect' as well as datacenter capacity and network connections used for cloud and hosting services at the datacenters Cologne (CGN3), Dusseldorf (DUS6), Hamburg/Norderstedt (HAM5) and Hamburg Wilhelmsburg (HAM6)

including the sites see enclosure.

An audit was performed, Order No. **70775393**.

Proof has been furnished that the requirements
according to

DIN EN ISO/IEC 27001:2017

are fulfilled.

The certificate is valid from **2023-06-01** until **2025-10-31**.

Certificate Registration No.: **12 310 40834 TMS**.

Version of the statement of applicability: **V3.03 vom 12.04.2023**.

Head of Certification Body
Munich, 2023-05-23

IAF DAkkS Deutsche Akkreditierungsstelle D-ZM-14143-01-00

Page 1 of 2

TÜV SÜD Management Service GmbH • Zertifizierungsstelle • Ridlerstrasse 57 • 80339 München • Germany
www.tuev-sued.de/certificate-validity-check

TÜV®

MS/01-01/2019

ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

Management Service

Enclosure of Certificate Registration No.: 12 310 40834 TMS

Sites	Scope of application
plusserver gmbh Venloer Str. 47 50672 Köln Germany	Provisioning and operation of the cloud services 'pluscloud VMware' and 'pluscloud open' and 'Cloud Connect'.
plusserver gmbh Welserstraße 14 51149 Köln Germany	Provisioning and operation of datacenter capacity and network connections used for cloud and hosting services at the datacenters Cologne (CGN3), Dusseldorf (DUS6), Hamburg/Norderstedt (HAM5) and Hamburg Wilhelmsburg (HAM6).
plusserver gmbh In der Steele 33a-41 40599 Düsseldorf Germany	Provisioning and operation of datacenter capacity and network connections used for cloud and hosting services (DUS6).
plusserver gmbh Neustädter Neuer Weg 22 20097 Hamburg Germany	Provisioning and operation of datacenter capacity and network connections used for cloud and hosting services at the datacenters Hamburg/Norderstedt (HAM5) and Hamburg Wilhelmsburg (HAM6).
plusserver gmbh Altmarkt 25 01067 Dresden Germany	Customer Support.

Head of Certification Body
Munich, 2023-05-23

Page 2 of 2

TÜV SÜD Management Service GmbH • Zertifizierungsstelle • Ridlerstrasse 57 • 80339 München • Germany
www.tuev-sued.de/certificate-validity-check

MS/01-01/2019

15. ISO 9001 Certificate PlusServer

ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

TÜV SÜD Management Service

ZERTIFIKAT

Die Zertifizierungsstelle
der TÜV SÜD Management Service GmbH
bescheinigt, dass das Unternehmen

plusserver

PlusServer GmbH
Venloer Str. 47 • 50672 Köln • Deutschland
Welserstr. 14 • 51149 Köln • Deutschland
In der Steele 33a-41 • 40599 Düsseldorf • Deutschland
Nagelsweg 33-35 • 20097 Hamburg • Deutschland
Altmarkt 25 • 01067 Dresden • Deutschland

für den Geltungsbereich

Der Lifecycle aller IT-Services des Unternehmens,
von der Entwicklung, über die Beratung und den Vertrieb,
die Bereitstellung und den Betrieb, bis zur
Abrechnung und Außerbetriebnahme

ein Qualitätsmanagementsystem
eingeführt hat und anwendet.
Durch ein Audit, Auftrags-Nr. **70775393**,
wurde der Nachweis erbracht, dass die Forderungen der

ISO 9001:2015

erfüllt sind.
Dieses Zertifikat ist gültig vom **16.08.2022** bis **12.08.2025**.
Vorheriges Zertifikat gültig bis 12.08.2022.
Zertifikat-Registrier-Nr.: **12 100 58433 TMS**.

Leiter der Zertifizierungsstelle
München, 23.08.2022

IAF DAkkS

TÜV SÜD Management Service GmbH • Zertifizierungsstelle • Ridlerstrasse 57 • 80339 München • Germany
www.tuev-sued.de/certificate-validity-check

TÜV®

16. PCI Certificate PlusServer

Certificate

Payment Card Industry Data Security Standard

more security. usd

We hereby confirm

PlusServer GmbH
Venloer Str. 47
50672 Cologne
Germany

successfully provided evidence of compliance according to the Payment Card Industry Data Security Standard (PCI DSS) version 4.0.

The company successfully passed the following PCI DSS assessment measures:

Assessment Measure	Assessment Date	Expiration Date
Onsite Assessment	15-Jan-2024	14-Jan-2025

This confirmation shall be valid only for the assessment objects tested on the date of the test.
The company obligates itself to use the certificate it received and the assessment logo only during the validity period shown above.

more security. usd
JAN-2024
PCI DSS compliant

usd AG
Approved Scanning Vendor
Qualified Security Assessor
P2PE Qualified Security Assessor
3DS Assessor
Qualified PIN Assessor
Software Security Framework Assessor
Neu-Isenburg, Germany

Neu-Isenburg, 15/01/2024
Place, Date

usd AG
Manfred Tubach, CEO