Certificate

The certification body of TÜV Informationstechnik GmbH hereby awards this certificate to the company

CoCoNet Computer-Communication Networks GmbH
Parsevalstraße 9 b
40468 Düsseldorf, Germany

to confirm that its software product

MULTIVERSA Token for Mobile, version 2.0.4

fulfils all requirements of the criteria

Security Qualification (SQ), Version 10.0
Security Assurance Level SEAL-3

of TÜV Informationstechnik GmbH. The requirements are summarized in the appendix to the certificate. The appendix is part of the certificate and consists of 7 pages. The certificate is valid only in conjunction with the evaluation report.

Security TÜViT® 2021 Trusted Product

Certificate validity:
2021-07-26 – 2023-07-26

Certificate ID: 6142.21

Essen, 2021-07-26

Dr. Christoph Sutter
Head of Certification Body

TÜV Informationstechnik GmbH
TÜV NORD GROUP
Langemarckstr. 20
45141 Essen, Germany
www.tuvit.de

Certification Scheme

The certification body of TÜV Informationstechnik GmbH performs its certification on the basis of the following certification scheme:

- German document: "Zertifizierungsprogramm (nicht akkreditierter Bereich) der Zertifizierungsstelle der TÜV Informationstechnik GmbH", version 1.1 as of 2020-03-01, TÜV Informationstechnik GmbH

Evaluation Report

- German document: "Prüfbericht Sicherheitstechnische Qualifizierung, MULTIVERSA Token für Smartphones, Version 2.0.4", report version 1.4 as of 2021-07-23, TÜV Informationstechnik GmbH

Evaluation Requirements

- "Trusted Site Security / Trusted Product Security, Security Qualification (SQ) Requirements Catalog for version 10.0, document version 2.8 as of 2020-03-16, TÜV Informationstechnik GmbH
- product-specific security requirements (see below)

The Evaluation Requirements are summarized at the end.

Evaluation Target

The target of evaluation is the software produkt "MULTIVERSA Token for Mobile", version 2.0.4 of CoCoNet Computer-Communication Networks GmbH. It is detailed in the evaluation report.

Evaluation Result

- All applicable evaluation requirements for the security qualification with Security Assurance Level SEAL-3 are fulfilled.
- The product-specific security requirements are fulfilled.

The recommendations of the evaluation report have to be regarded.

Product-specific security requirements

The following product-specific security requirements are the basis of the certification and have been checked.

1 Data storage

The data worth protecting (cryptographic key material, passwords, configuration data) are managed according to best practices of the iOS/Android platforms. The data worth protecting is encrypted using the iOS keychain or Android keystore and stored locally.

2 Cryptography

The encryption of sensitive data is based on symmetric and asymmetric cryptography with dynamically negotiated keys. The cryptographic procedures use current algorithms and procedures that comply with the EBICS specification v2.5.

3 Authentication

The target of evaluation serves as a possession-based 2-factor authentication feature. Before each use, the user must successfully authenticate himself.

If the user is inactive for a specified period of time, the user is forced to successfully authenticate again. Excessive

authentication attempts are prevented. Accepted passwords must meet the complexity of NIST guideline SP 800-63B (appendix A).

4 Transport encryption

Transport encryption is implemented in accordance with the EBICS specification v2.5 for communication with the backend. Data worth protecting (cryptographic key material, user IDs) are not transmitted in plain text. Within the framework of the TLS connection, only server certificates from trustworthy certification authorities are accepted that are stored as trustworthy in the certificate store of the underlying iOS/Android platform. The server certificates of the backend are additionally checked (certificate pinning or certificate transparency) to authenticate the server.

5 Use of platform-specific interfaces

In accordance with best practices of the iOS/Android platforms used, all incoming data is validated. Only request permissions on the iOS/Android platform that are mandatory for the execution of functions are granted. Offered Functions are protected from unauthorised access by other processes by the authorisation concept of the iOS/Android platforms.

6 Code quality and build settings

The app is signed with a valid developer certificate and provisioned in the public app store of the iOS/Android platform. During the compilation process, the code is obfuscated. No debugging symbols are included in the binary code. If errors occur in security functions, they are handled according to best practices of the iOS/Android platform. Automatic memory management and security functions of

the compiler are used according to best practices of the iOS/Android platform.

7 Tamper resistance

A device binding with the mobile device is implemented. A basic detection of untrusted environments (jailbreak/root) comparable to the recommended best practice counter-measures from the OWASP Mobile Security Testing Guide (MSTG-RESILIENCE-1) is implemented. In addition, basic countermeasures are implemented to prevent the use of a debugger, comparable tools and/or an emulator (MSTG-RESILIENCE-2).

Summary of the requirements for the Security Qualification (SQ), version 10.0

1 Technical Security Requirements

The technical security requirements must be documented, consistent and verifiable. The specification must be made in accordance with ISO / IEC 17007. In addition, technical security requirements must be derived in the framework of an individual threat and risk analysis, they must be derived from previously defined protection profiles, or they must conform to published security requirements of recognized authorities or bodies of IT security. Furthermore, they must be appropriate to the intended use of the IT product and meet applicable security demands.

2 Architecture and Design

The IT product must be structured reasonably and under-standable. Its complexity must not have any impact on security. It must not contain any conceptual vulnerability that allows bypassing or disabling security-relevant components.

The hardening and protection measures must be adequate and effective.

3 Development Process

Development of the IT product must follow a defined development life cycle taking into account at least the phases of planning, analysis, design, implementation, testing, deployment and maintenance. The maintenance phase of the development life cycle must consider and eliminate vulnerabilities that allow bypassing or disabling security-relevant components. As part of the testing phase of the development life cycle tests with respect to security functionality of the IT product must be considered.

4 Operating Instructions (as of SEAL-4)

The documentation consisting of security requirements for the operating environment of the product, manuals for installation and administration as well as manuals for the end user must be clearly understandable and comprehensible. The documentation must be known to authorized person and always be readily accessible.

5 Vulnerability Assessment and Penetration Testing

The security measures of the IT product must withstand penetration testing. It must not be possible to break or circumvent security measures. The IT product must be configured securely, must meet all of the defined technical security requirements and must not have any exploitable vulnerability.

6 Source Code Analysis (as of SEAL-4)

The source code must not contain vulnerabilities, errors or inconsistencies, such as e. g. undocumented commands, parameters and test functions.

7 Change Management (as of SEAL-5)

Patch management must be completely documented and suitable for the IT product. The procedure for amendments of the IT product must be clearly defined and appropriate for the IT product. Persons involved must be familiar with it and responsibilities must be clearly defined. Amendments of the IT product must not lead to a reduction of the security level achieved.

Security Assurance Level

The following table shows the applicable criteria for the security assurance level. A certificate can be issued for IT products having successfully passed the evaluation and reaching an overall level of at least SEAL-3.

Security Assurance Level / Evaluation Criteria	SEAL-1	SEAL-2	SEAL-3	SEAL-4	SEAL-5
Technical Security Requirements	X	X	X	X	X
Architecture and Design			X	X	X
Development Process			X	X	X
Operating Instructions				X	X
Vulnerability Assessment and Penetration Testing		X	X	X	X
Source Code Analyse				X	X
Change Management					X

Table: Evaluation Criteria and Security Assurance Level of IT products