Certificate

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

Vodafone GmbH
Ferdinand-Braun-Platz 1
40549 Düsseldorf, Germany

to confirm that its product

Vodafone Secure SIM (VSS) – Secure Login, V1.0

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 this certificate. The appendix is part of the certificate and consists of 7 pages.

The certificate is valid only in conjunction with the corresponding evaluation report until 2015-09-30.

Security PQ6122.13 TÜViT® 2013 Trusted Product

Voluntary Validation

Certificate-Registration-No.:
TUVIT-PQ6122.13

Essen, 2013-09-09

Dr. Christoph Sutter
Head of Certification Body

TÜV Informationstechnik GmbH
Member of TÜV NORD Group
Langemarckstr. 20
45141 Essen, Germany
www.tuvit.de

Certification System

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

- German document: ”Zertifizierungsschema für TÜViT Trusted-Zertifikate der Zertifizierungsstelle TÜV Informationstechnik GmbH“, version 1.0 as of 2010-05-18, TÜV Informationstechnik GmbH

Evaluation Report

- German document: “Vodafone Secure SIM (VSS) – Secure Login“, V1.0, report version 1.3 as of 2013-09-02 TÜV Informationstechnik GmbH.

Evaluation Requirements

- German document: “Sicherheitstechnische Qualifizierung (SQ)® der TÜV Informationstechnik GmbH”, version 10.0 as of 2011-03-21, TÜV Informationstechnik GmbH
- Product-specific security requirements (see below)

The evaluation requirements are listed at the end.

Evaluation Target

The target of evaluation "Secure Vodafone SIM (VSS) - Secure Login", V1.0 of Vodafone GmbH consists of the following components:

- VSS infrastructure components, Release 1.0, which are operated as core systems in the data centre of Vodafone GmbH.
- Customer Administration Portal, Release 1.0, which is operated as WebAccess portal at the site of a service provider of Vodafone GmbH.

- SIM applet, Release 1.0, which is integrated in the SIM card of the mobile phone of the customer.

The VSS infrastructure components are centrally installed and operated in the data centre of Vodafone GmbH. The Customer Administration Portal is operated centrally, depending on the use case, by a service provider of Vodafone GmbH used by the customer. The SIM applet in the SIM card of the mobile phone is used by customers of Vodafone GmbH.

The target of evaluation allows the customers of Vodafone GmbH to carry out a two-factor authentication based on knowledge (SIM applet PIN) and possession (SIM). It includes the following two use cases:

- VPN gateway, 2-factor authentication with RADIUS at the VPN authentication server of the customer or service provider and
- Web portal, 2-factor authentication with SAML at the WebAccess portal of the customer or service provider.

The components VPN gateway and Web portal of the use cases are with the responsibility of the customer and are not in the scope of evaluation. A detailed description of the target of evaluation is included in the evaluation report.

Evaluation Result

- All applicable evaluation requirements for the Security Qualification (SQ) 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 were basis of the certification and have been checked.

1 Identification & Authentication

The IT product must uniquely identify and authenticate the user, taking into account the SIM applet as security token. The authentication data of the 2-factor authentication must be sufficiently strong to withstand common attacks long enough.

2 Access Control

The IT product must provide functions that make it possible to restrict users' access rights. This particularly applies to the multi-client capability of the Customer Administration Portal in the context of use cases: VPN authentication server / WebAccess portal. A customer cannot access data from other customers.

An attacker must not be able to gain unauthorized privileges on the central VSS server components of the IT product with possible effort. The VSS server components in the dedicated VSS network of the datacenter of Vodafone GmbH and the service providers have no known exploitable vulnerabilities.

3 Encrypted Communication Path

Data communication via insecure networks (as e. g. the internet) must be performed via a trustworthy channel/path that ensures the confidentiality of the transmitted data.

4 Data Flow Control

The IT product must ensure that only connections needed for operation are possible. This is valid for the connections between

- the central VSS-server components and the VPN gateway/web access portal on customer's side,
- the central VSS-server components and the Customer Administration Portal,
- the central VSS-server components and the IT-infrastructure as VSS-environment and
- the central VSS-server components and the administrators.

5 Logging

Security-relevant events must be logged by the security components of the IT infrastructure and flow into a reporting and alerting system.

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 understandable. 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 of 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 or 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 Analysis				X	X
Change Management					X

Table: Evaluation Criteria and Security Assurance Level