

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

Infineon Technologies AG
Wernerwerkstr. 2
93049 Regensburg, Germany

to confirm that its Security Management System for the

Backend Chip Fabrication

fulfils all applicable requirements of the criteria

DeTeCardService/TÜViT TU4[®], V2.0

The requirements are summarized in the appendix to this
certificate.

The appendix is part of the certificate and consists of 2 pages.

The certificate is valid only in conjunction with the audit protocol
S/INF Regensburg-200701, as of 2007-11-12.

The certificate is valid until 2009-07-31.



09
Certificate Registration No.:
TUVIT-TU9667.07

Essen, 2007-12-10 sign. Dr. Sutter

Certification Body

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



Certificate

Security Audit

The certificate is based on the:

- *Audit protocol – Security audit, version 1.1 as of 2007-11-12, audit-ID S/INF Regensburg-200701.*

The audit was performed by the following auditors:

- Mr. Blißenbach (TÜViT GmbH) and
- Mr. Spöner (Deutsche Telekom AG).

DeTeCardService/TÜViT TU4® Criteria

- DeTeCardService/TÜViT TU4® – *Requirements for Security Management Systems, Version 2.0 as of 2001-09-01.*

Summary of the TU4® Requirements

1. Responsibility of the Top Management

The top management is responsible for the definition and documentation of the security policy.

2. Administration

The security representative is responsible for the administration of the security management system.

3. Staff Security

For all security relevant tasks only trustworthy and accordingly qualified staff is employed.

4. Material Flow

Adequate security measures are defined for single materials, (intermediate) products, data and documents in the production.

5. Security in the Information Technology (IT)

Confidentiality, integrity, authenticity and availability of all production and personalising data in all phases have the highest priority.

6. Passive Security Requirements

Passive building security measures have a suitably structured order and resistance quality to represent an effective physical hindrance for potential attackers on their attack path.

7. Active Security Requirements

In order to recognise an attack, if possible in the formation phase, active elements for access control and alerting are in place.

8. Auditing (external)

The external auditing has been carried out on the basis of the current valid version of the TU4®.

The certification confirms that a production facility has installed a security management system according to DeTeCardService/TUVIT TU4® and utilizes it.

Non-applicable TU4® Requirements

The following TU4® Requirements are not applicable:

4. Material Flow: Production Run Scratch-Off / Voucher Cards
5. Security in the IT: Development Environment