

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

**Infineon Technologies (Wuxi) Co.,  
Ltd., Wuxi-Singapore, Industrial  
Park, Wuxi, 214028, China**

to confirm that its Security Management System for the

**Assembly & Final Testing**

fulfils all applicable requirements of the criteria

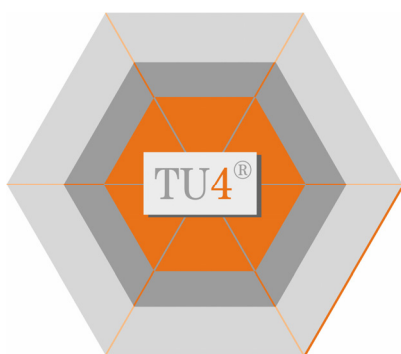
**DeTeCardService/TÜViT TU4<sup>®</sup>, V2.0**

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 Wuxi-200711*, as of 2007-12-07.

The certificate is valid until 2009-11-30.



09  
Certificate Registration No.:  
TUVIT- TUVIT-TU9670.07

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 2007-12-07, audit-ID *S/INF Wuxi-200711*.

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 the audited 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:

4.2 Material Flow: Production Run

4.4 Verification Management

5.8 Security in the IT: Development Environment