

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

## **Agencija za komercijalnu djelatnost d.o.o.**

**Savska cesta 31  
10 000 Zagreb, Croatia**

to confirm that its Security Management System for the

## **Chip Card Production**

fulfils all applicable requirements of the criteria

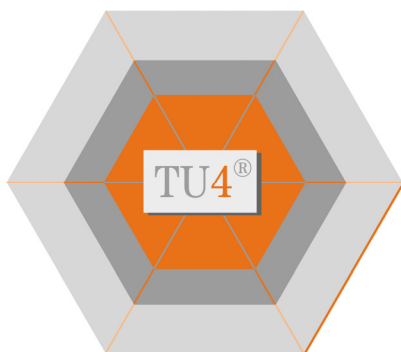
## **DeTeCardService/TÜViT TU4<sup>®</sup>, V2.0**

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 respective audit  
protocol.

The certificate is valid until 2010-10-31.



10  
Certificate Registration No.:  
TUVIT-TU9675.08

Essen, 2008-10-28

Dr. Christoph Sutter  
Head of Certification Body

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



**Certificate**

## Security Audit

TÜV<sup>®</sup>

The certificate is based on the:

- “Audit protocol – Security audit”, version 2.0 as of 2008-10-23, audit-ID “S/AKD-200805”, TÜViT GmbH.

The audit was performed by the following auditor:

- Mr. Blißenbach (TÜViT GmbH)

## DeTeCardService/TÜViT TU4<sup>®</sup> Criteria

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

### Non-applicable requirements of the TU4<sup>®</sup> criteria:

The following requirements of the TU4<sup>®</sup> criteria are not applicable for the present security management system for the Chip Card Production:

- 4.2.2 Production Run Scratch-Off/Voucher Cards
- 5.8 Development Environment

## Summary of the TU4<sup>®</sup> 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 are to be employed.

### 4. Material Flow

Adequate security measures are to be 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 must 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 required.

8. Auditing (external)

In general the auditing is 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.