

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

Swiss Post Solutions GmbH
Kronacher Straße 61
96052 Bamberg, Germany

to confirm that its Security Management System for the

**Production of Chip Cards and of
Scratch-Off-/Voucher Cards**

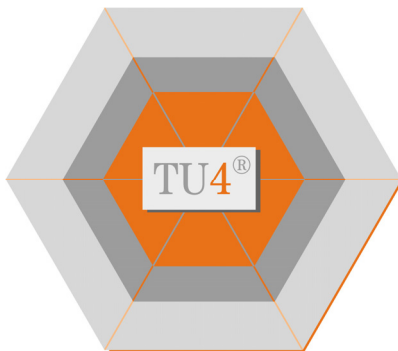
fulfils all applicable requirements of the criteria

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 3 pages.

The certificate is valid only in conjunction with the corresponding
audit report until 2013-07-31.



13
Certificate-Registration-No.:
TUVIT-TU9695.11

Essen, 2011-07-15

Dr. Christoph Sutter
Head of Certification Body

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



Certificate

Certification System

The certification body of TÜV Informationstechnik GmbH performs its certifications 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, TÜViT GmbH

Audit Report

- "Audit protocol – Security audit – SMS for Chip Card Production of Eurochip cards, eGK, KVK health cards and scratch cards", version 1.0 as of 2011-07-05, audit ID S/11041513, TÜViT GmbH

The audit was performed at the site 96052 Bamberg, Germany.

Audit Requirements

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

The Audit Requirements are listed at the end.

Audit Target

The target of the audit is the security management system for the "Production of Chip Cards and of Scratch-Off-/Voucher Cards" at the company Swiss Post Solutions GmbH, Kronacher Straße 61, 96052 Bamberg Germany.

Audit Result

The certification confirms that the audited company has installed for the audit target a security management system according to DeTeCardService/TÜViT TU4® and utilizes it.

The audit target fulfils all applicable audit requirements.

Summary of the Audit 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.



Member of
TÜV NORD Group

TÜV®

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®.