# CERTIFICATE

This is to certify that

## Atos Information Technology GmbH

Luxemburger Straße 3
45131 Essen
Germany

has implemented the specification listed below for the following certification services. This certificate is only valid in combination with the respective report.

Scope:
Atos Trusted Certification Authority (ATCA), consisting of

- Atos TrustRoot Server CA
- Atos TrustRoot Client CA
- Atos TrustRoot Codesigning CA

An audit of the certification service, documented in a report, provided evidence that the requirements of the following specification have been fulfilled.

## **ETSI TS 102 042** V2.4.1 (2013-02)

| | |
|---|---|
| Certificate registration no. | 334220 ETSI |
| Date of certification | 2013-07-10 |
| Valid until | 2014-07-09 |

**DQS GmbH**

G. Blechschmidt

Götz Blechschmidt
Managing Director

# Annex to Certificate
# Registration No. 334220 ETSI

## Atos Information Technology GmbH

Luxemburger Straße 3
45131 Essen

### Assessment Requirements

The audit requirements are defined in the technical specification ETSI TS 102 042:

ETSI TS 102 042 V2.4.1 (2013-02): “Electronic Signatures and Infrastructures (ESI); Policy Requirements for certification authorities issuing public key certificates”, Version 2.4.1, 2013-02, European Telecommunications Standards Institute

Including the specification of CA/Browser Forum:

Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.1.3 adopted on 21 Feb. 2013 with an Effective Date of 21 Feb. 2013

The applicable ETSI certification policy is:
NCP in the Variants DVCP and OVCP

The audit object is characterized by the certification information of the reviewed CA:

Atos Trusted Certification Authority (ATCA), consisting of

- Atos TrustRoot Server CA
- Atos TrustRoot Client CA
- Atos TrustRoot Codesigning CA

### Audit Results

- The audit object fulfills all applicable requirements from the audit criteria.
- The certification requirements as defined in the certification assumptions are fulfilled.
- All requirements for a CA Practice according to chapter 7 of the rules and standards together with the therein demanded measures are implemented in terms of the selected Certificate Policy.
- The audited CA also takes the responsibility for the norm requirements’ fulfillment, if CA-functions are taken over by contract partners (at present not relevant).
- The CA provides the certification services according to the definitions of the Certificate Practice Statement.
- The Certificate Policy is part of an effective certificate policy management with regulations concerning responsibilities, communication and PDCA cycle.
- The audit was performed in line with the European standards/specifications, especially in line with the above mentioned standard, the TS 119 403 and were applicable with the requirements of the CA/Browser Forum in the latest version 1.1.3.

# Annex to Certificate
# Registration No. 334220 ETSI

## Atos Information Technology GmbH

Luxemburger Straße 3
45131 Essen

## Summary of audit requirements

The ETSI specification ETSI TS 102 042 contains the following requirements:

### 1 Certification Practice Statement (CPS)

The CA has a presentation of its practices and policies.

### 2 Public Key Infrastructure – key management life cycle

The CA ensures that CA keys are created under controlled conditions. The CA ensures that private CA keys are treated confidentially and that their integrity is maintained. The CA ensures that the integrity and authenticity of the (published) CA public keys together with all associated parameters are preserved during their transfer to relying parties. If the key for electronic signatures is applied in the terms of guideline 1999/93/EG the CA is not entitled to store private signature keys of the certification owner (subject) in a way enabling a decryption (also called key escrow). If a copy of the key remains at the CA the CA takes care that the private key remains secure and is only made accessible to entitled persons.

The CA ensures that private CA signature keys are not used improperly. The CA ensures that private CA signature keys may not be used beyond the end of their life cycle. The CA ensures that the security of cryptographic devices is warranted during their complete life cycle.

The CA ensures that every key created by the CA for a certificate owner (subject) is safely generated and that the non-disclosure of the certificate owner’s private key is guaranteed.

### 3 Public key infrastructure – certificate management life cycle

The CA ensures that the identification confirmation of a participant (subscriber) and of a certificate owner (subject) as well as the correctness of their names and their related data are either checked as part of the defined service or proved by attestations from appropriate and licensed sources. It also ensures that applications for a certificate take place in a correct and authorized way, completely according to the collected proofs respectively attestations.

The CA ensures that the certification applications of certificate owners (subject), who were registered before at the same CA, are authorized completely, correctly and orderly. This implies certificate extensions, anew key generations (rekey) after a blocking or before the expiry date, or updates due to attribute changes of the certificate owner (subject).

The CA ensures that the certificates are handed out in a secure way so that their authenticity is maintained.

The CA ensures that the legal terms and conditions are made available to the participants (subscriber) and to the relying parties.
The CA ensures that certificates are made available to the participants (subscriber), certificate owners (subject) and relying parties to the extent necessary.
The CA ensures that certificates are blocked at short notice using authorized and verified blocking queries.

**4 CA Management und Operation**
The CA ensures that the applied administrative and management methods are appropriate and correspond to acknowledged standards.
The CA ensures that the objects and information worthy of protection receive an appropriate protection.
The CA ensures that the employees and the hiring procedures amplify and support the CA company's trustability.
The CA ensures that physical access to critical services is controlled and that the physical risks for the objects worthy of protection are minimized.
The CA ensures that the CA systems are operated safely, according to specification and with a minimal default risk.
The CA ensures that the access to the CA systems is restricted to appropriate, authorized persons.
The CA is to use trustworthy systems and products that are protected against modifications.
The CA ensures that in case of a catastrophe (including a compromise of the private CA signature key) the operation is restored as soon as possible.
The CA ensures that in case of a cessation of the CA operation the potential interference of users (subscriber) and relying parties is minimized and that the continued maintenance of records that are required as proof of certification in legal proceedings is given.
The CA ensures that statutory requirements are met.
The CA ensures that all relevant information of a certificate is recorded for a reasonable period of time, especially for the purpose of proof of certification in legal proceedings.

**5 Organization**
The CA ensures that its organization is reliable.