DQS GmbH
Deutsche Gesellschaft zur Zertifizierung
von Managementsystemen

THE AUDIT COMPANY

Atos Information Technology GmbH
Matthias Moenter
Luxemburger Straße 3
45131 Essen

Our sign : BSH, Phone +49 69 95427-397
E-Mail: bianca.stephan@dqs.de

Frankfurt a. M.,
14.08.2013

Dear Mr. Moenter,

DQS was asked by ATOS to verify in an external audit the issues mentioned in the attached document.

Following statement was made by the auditor Jens Nicolaysen:

The two issues and all related actions have been discussed and reviewed in detail during the audit on the 20th June 2013.

CA-certificates
The issue was not caused by an incident, but rather based on a decision of the Trustcenter. Part of this decision was to consider the risks.
No third party was affected or harmed. In particular the Trustcenter itself had never been out of control of one of its responsibilities, like key usage or the ability to revoke the certificates.

During the audit the steps to adjust the Trustcenter processes were reviewed. In particular the following items have been subject of the audit:

- The whole CA creation process and its documentation have been revalidated.
- All changes and related process documentation have been checked and reviewed.
- The filled checklists and logs of the CA creation process and key generation ceremony have been reviewed for all current CAs.

All in all the changes are considered as sufficient to effectively prevent such an issue from happening again.

OCSP-Get-Requests
During the Audit it was demonstrated that OCSP-Get-Requests are properly handled.

Yours sincerely,
DQS GmbH

Bianca Stephan

Bianca Stephan
Customer Service Representative
Global Account Management

Issues from the Mozilla public discussion

The issues coming out from the Mozilla public discussions are:

- No CRLDP and AIA:OCSP extension in the SSL intermediate cert & intermediate certs were issued with duplicate serial numbers
- Handling of OCSP-Get-Requests

Intermediate certs with duplicate serial numbers & missing CRLDP and AIA:OCSP extension

Background information
The CA-certificates were initially created without CRLDP and AIA:OCSP extension. When the need for these extensions came up the Atos Trustcenter decided to add these information to the already existing CA-certificates. The reason was that no end entity certificates were issued until then. When publishing the CA-certificates (with CRLDP and AIA:OCSP extension) is was missed to update all existing repositories: Two repositories still contained the wrong CA-certificates.

Consequences
Atos Trustcenter has replaced the affected CAs:

- Three new intermediate CAs (Client, SSL and CodeSigning) are created.
- The intermediate CAs (SSL & Codesign) with duplicate CA-Certificates (with/without CRLDP and AIA:OCSP extension) are revoked.
- For the Client-CA: The preparation to switch to the new intermediate CA has started.

Atos Trustcenter has taken the following steps to adjust its processes:

- The process to create a new CA has been reviewed and was improved: Checklist is extended, additional checks are in place, work instructions are revised.
- In particular the checklist which is part of the protocol when creating a new CA has been changed and, among others, a new item was added to explicitly check and confirm that no deviation from the certificate templates have been applied to the certificate data.
- The used software assures that duplicate serial numbers cannot be assigned.
- The issue has been documented and added as a topic for the upcoming ETSI audit.

Handling of OCSP-Get-Requests

During the Mozilla public discussion it came up that the handling of OCSP-Get-Requests did not work properly. The OCSP-Server was then changed, so that the correct functionality is given.