

TÜRKTRUST BİLGİ İLETİŞİM VE BİLİŞİM GÜVENLİĞİ HİZMETLERİ A.Ş

Attn: Dr. T. Tüfekçi
Hollanda Cad. 696.Sok. No:7
06550 Yıldız - Ankara
Turkey

Amsterdam, 7 March 2013

Subject: Summary of results of the special audit

Dear Mr. Tüfekçi,

Introduction

This letter provides a summary of the results of the special audit that we performed in January 2013 as a follow-up of the incident that led to the erroneous issuance of end-user certificates with certificate signing capability. Our detailed audit results have been included in our Assessment Report - Special Audit that has been presented to you separately.

Background

In August 2011 Türktrust issued two erroneous SSL-certificates that were given the technical capability to act as issuing CA certificates. One of these two certificates was revoked in August 2011 due to reported implementation problems at Türktrust's client. The other certificate still remained in operation at another Türktrust client. At this client, on 21 December 2012, during technical configuration activities performed on client's systems, the SSL-certificate was used by the client systems as a CA-issuing certificate and as an automated process a certificate was issued to *.google.com. This was noticed by Google and in response to this, the browser vendors issued a security advisory. In response to this, Türktrust made public announcements on its website concerning the security advisory by Microsoft, Google and other browser vendors and published this on the 3rd of January 2013, after which Türktrust applied updates to the announcements. After intensively communicating with the browser vendors, especially with Mozilla Foundation, Türktrust has been requested to have an additional assessment performed.

Objective and scope

On the request of Türktrust, BSI Group The Netherlands B.V. (hereafter: BSI) was asked to perform a Special Audit, to be performed in addition to the audit cycle of the ETSI TS 102042 conformity certificate (nr. 47421874/ETS 019). The objective of the special audit was to verify the effectiveness of specific control measures

that are important for preventing a similar incident to occur again. The scope area's for the special audit were specifically requested by Mozilla Foundation and comprised the following areas:

- Change management together with release management, emergency software change management, and incident management.
- Internal audit management along with corrective and preventive action management, primarily for CA processes.

Result of the Special Audit

In assessing the effectiveness of the controls for the scope area's identified, we performed a review of selected documentation, we performed site visits at Türktrust premises and we reviewed implemented controls in Türktrust systems. During the performance of our special audit we noted that:

- Türktrust modified its change management and release management process and procedures as a corrective action for the root cause that led to the incident. In addition the incident management procedures were further optimised.
- Türktrust has further optimised its Internal Audit management process. The audit procedures for the review of the CA software components are planned to include the measures taken to prevent the erroneous issuance of certificates.
- Türktrust followed up on the incident by performing an assessment on its database to determine as to whether other certificates with the same error were present. In addition, Türktrust introduced application controls in its CA-software. It involves preventive measures, such as the realtime protection functionality, and repressive measures, such as a nightly cronjob on database contents.
- As part of the corrective actions, Türktrust implemented a new software tool Atlassian Jira to facilitate workflow and registration of activities mentioned in the above areas and updated its documentation.

No new nonconformities were identified during the assessment. As a result of the assessment, the areas assessed during the course of the visit were found to be effective. Based on our assessment, we confirm that the certificate of conformity based on ETSI TS 102042 with number (47421874/ETS 019) continues to maintain its validity.

Enhanced detail relating to the overall assessment findings is contained in the Assessment Report - Special Audit. This report and related documents is prepared for and only for Türktrust and for no other purpose.

The assessment was based on sampling and therefore nonconformities may exist which have not been identified.

Distribution of this letter

BSI grants permission to distribute a copy of this letter only to the designated contact persons at the following organisations:

- Mozilla Foundation
- Microsoft
- Google
- Opera
- Apple

Türktrust and each of the designated persons at the above mentioned organisations will not further distribute the letter, including by disclosing it to the public through physical or electronic means. Notwithstanding the foregoing, upon explicit request of Mozilla, the contact person at Mozilla may disclose the letter on Mozilla's Bugzilla under registration number #835538.

BSI does not accept or assume any responsibility (legal or otherwise) or accept any liability for or in connection with the purpose for which this letter may be used, or to whom the letter is disclosed.

As such, BSI does not accept or assume any responsibility (legal or otherwise) or accept any liability for or in connection with any other purpose for which this letter may be used, or to any other person to whom the letter is shown or in to whose hands it may come, and no other persons shall be entitled to rely on the letter.

BSI, its staff and agents shall keep confidential all information relating to Türktrust and shall not disclose any such information to any third party, except that in the public domain or required by law or relevant accreditation bodies. BSI staff, agents and accreditation bodies have signed individual confidentiality undertakings and will only receive confidential information on a 'need to know' basis.

On behalf of BSI Group The Netherlands B.V.,

Mr. Drs. D.T.P. Hagenaars
Managing Director