Cablint Findings for DFN-PKI

1. Introduction

In July and August 2017 multiple parties searched the Certificate Transparency Log system for certificates that violate the CA/Browser Forum Baseline Requirements. Among the reported certificates where several that where issued from the DFN-PKI. Those certificates were/are handled in bug 1391074 (https://bugzilla.mozilla.org/show_bug.cgi?id=1391074)

While handling the problem reports from bug 1391074, we performed a full scan of all non-expired and non-revoked server certificates of the DFN-PKI with cablint on 2017-08-17. This report covers additional findings of this cablint run.

The DFN-PKI is a Sub CA structure under the following two root certificates owned by T-Systems International GmbH:

Root 1:
https://crt.sh/?caid=81 CN=Deutsche Telekom Root CA 2

Sub CAs:
https://crt.sh/?id=393 CN=DFN-Verein PCA Global - G01

https://crt.sh/?id=4749431 CN=DFN-Verein PCA Global - G01

Root 2:
https://crt.sh/?id=8733622 CN=T-TeleSec GlobalRoot Class 2

Sub CA:
https://crt.sh/?id=23908438 CN=DFN-Verein Certification Authority 2

T-Systems and DFN work closely together and are in frequent and regular contact both in daily business as well as in case of incidents.

The Sub CA structure is operated independently from T-Systems by DFN-Verein, and is audited by TÜViT according to ETSI TS 102 042 (next audit will be ETSI EN 319 411). The first audit of the DFN-PKI was performed in 2012. The current audit report is dated 2016-12-15.

DFN-PKI operates a rather large number of issuing CAs, which partly carry the name of German research and education institutions (the constituency of DFN-Verein). All of those Sub CAs are operated in-house by DFN-Verein; no CA private key is handled outside DFN-Verein premises.

DFN-Verein customers have Enterprise RA access to the issuing system, where they can issue certificates for validated and pre-approved authorization domain names and ip addresses, with subject dn values for validated and pre-approved C, ST, L, O values. OU values can be set by Enterprise RA.

2. Further Findings with cablint

The following ERROR-findings were reported by cablint on a full scan of all non-expired and non-revoked server certificates of the DFN-PKI:

(Note: The certificate numbers are not consolidated, e.g., a single certificate with more than one issue is listed multiple times, once under each of its issues.)

2.1. Issue A: Metadata in OU

A set of further 61 certificates was detected. Those certificates are already handled in bug 1391074.

2.2. Issue B: rfc822Name, otherName, uniformResourceIdentifier in server certificate

12045 certificates which were issued up to 12/2014 are still valid, not revoked and contain at least one subject alternative name of the type rfc822Name. 97 of those contain two rfc822Names.

56 certificates which were issued up to 12/2014 are still valid, not revoked and contain a subject alternative name of the type otherName.

34 certificates which were issued up to 12/2014 are still valid, not revoked and contain at least one subject alternative name of the type uniformResourceIdentifier.

2.3. Issue C: DNSName is not in preferred syntax (trailing

dot)

4 further certificates contain DNSName subject alternative names with trailing dots. One of those certificates contains three DNSNames with this error, the others each only one. Those certificates are already handled in bug 1391074.

2.4. Issue D: Invalid Padding in RFC822Name

1 certificate contains an RFC822Name with a mail address with a trailing dot.

2.5. Issue E: DuplicateSANEntry

130 certificates contain at least one duplicate SAN entries. All duplicate SAN entries are of type DNSName, and are only duplicates if case is ignored (e.g. DNS:www.dfn.de and DNS:www.dfn.DE).

3. Root Causes and Remediation

3.1. Issue A: Metadata in OU

This issue has three different causes:

1. Improper validation by Enterprise RAs. Most certificate fields are pre-approved by DFN personnel, like C, ST, L, O, authorization domain names. Values for OU are set by Enterprise RAs. The Enterprise RAs who inspected the OU fields before approving did not catch the improper values.

=> Remediation: Retrain Enterprise RAs to raise awareness for OU validation.
Timeframe: On 2017/08/23, updated documentation was provided and all Enterprise RAs were notified

2. Our PKI systems did not prevent metadata-only OUs.

=> Remediation: Change PKI system to prevent common cases of metadata-only values.
Timeframe: Software fix installed on 2017/08/28

3. Monitoring of issued certificates by DFN did not catch the problem. DFN has a deep 3% audit (as required per BR), and lighter audit of all issued certificates (where certificates are manually inspected, including the OU field). This problem was not caught by both 3% and manual full audit.

=> Remediation:
Check why the problem was not caught by manual full audit.
Timeframe: Audit checklist incomplete, changed audit checklist on 2017/09/06

Handling of affected certificates: This issue does not impair the security of affected certificates and thus does not necessarily warrant revocation in our opinion.

3.2. Issue B: rfc822Name, otherName, uniformResourceIdentifier in server certificate

This issue has to be seen together with Issue D, Invalid Padding in RFC822Name

When preparing the DFN-PKI for CAB/Forum Baseline Requirements compatibility in 2011 and 2012 we misinterpreted the rules for subject alternative names: We gathered that while at least one DNSName or IPAddress was mandatory, additional subject alternative name types were still allowed.

Many certificates where issued with email addresses in rfc822Name, as this was felt an appropriate way of providing contact information of the certificate holders. In addition, some certificate holders felt it necessary to request inclusion of otherNames (e.g. certificates for MS domain controllers) or uniformResourceIdentifier.

In 2014 we noticed by studying the paper „WebPKI: Closing the gap between Guidelines and Practice“, written by authors from Microsoft research, that we missed that BR requirement. We discussed this paper with the authors from Microsoft and changed our PKI software to prevent further inclusion of any other type of subject alternative names than DNSName or IPAddress. The previous BR-nonconformance regarding other subject alternative name type does not raise immediate compatibility or security risks (in our opinion), so it was felt that the old certificates could be grandfathered.

Remediation: Since 2014-12-03 server certificates in the DFN-PKI contain only subject alt name entries DNSName or iPAddress.

Handling of affected certificates: This issue does not impair the security of affected certificates and thus does not necessarily warrant revocation in our opinion.

3.3. Issue C: DNSName is not in preferred syntax (trailing dot)

Up to 2015, the DFN-PKI systems allowed to append a trailing dot to a domain name. This was changed in March 2015. The change was solely motivated to make name handling simpler; it was not detected that trailing dots are actually forbidden according to the BRs via RFC5280=>RFC1034 and trailing dots are technically correct domain names but not “preferred syntax”.

Remediation: Since 2015-03-10 the DFN-PKI software prevents domain names with trailing dots.

Handling of affected certificates: This issue does not impair the security of affected certificates and thus does not necessarily warrant revocation in our opinion.

3.4. Issue D: Invalid Padding in RFC822Name

See Issue B

3.5. Issue E: Duplicate SAN Entry

The software for the DFN-PKI eliminates duplicates in subject alternative names, but does that in a

case-sensitive way.

Remediation: Change the software so that duplicates are eliminated in a case-insensitive way.
Timeframe: Software fix installed on 2017/08/28

Handling of affected certificates: This issue does not necessarily warrant revocation in our opinion.

4. Integrate cablint into toolchain

The last 12 months showed that running a preflight-check to ensure compliance of issued certificates is developing into an industry best practice. DFN had plans to integrate cablint into its workflow for some time now. We will give these plans a much higher priority.

Timeframe: 3 months for full automated integration. Internal development project started on on 2017/08/22

5. Handling of up to now unrevoked certificates from Further Findings

Due to the rather large volume of certificates affected by „Issue B: rfc822Name,otherName, uniFormResourceIdentifer“ , the fact that the current issuing infrastructure is not affected, and the absence of an urgent security risk, no further actions (e.g. revocation) were started for Issues A, B, C, D

All findings and our remediation actions will be indicated to our auditor.

5.1. Expiry timeframes and algorithms

Most certificates, especially with Issue B, C, D, were issued when DFN-PKI still had a validity period of 5 years as the default (which was allowed under BR rules until 2015-04-01), and thus expire only in 2019.

Note, however, that nearly 3/4 of all affected certificates were signed with SHA1 (which was allowed at issuance time), and are not trusted anymore by major browsers.

Numbers only include not yet revoked certificates.

Issue	Expire in 2017	Expire in 2018	Expire in 2019	Expire in 2020
Issue A Metadata in OU	-	-	58	3
Issue B rfc822Name	1431	4069	6545	-
Issue B otherName	26	12	18	-
Issue B URI	5	17	12	-
Issue C DNSName is not in preferred syntax	-	1	3	-

Issue D Invalid Padding	-	-	1	-
Issue E Duplicate SAN	6	24	88	12

Issue	Signed with SHA1	Signed with SHA256
Issue A Metadata in OU	0	61
Issue B rfc822Name	8805	3240
Issue B otherName	16	40
Issue B URI	25	9
Issue C DNSName is not in preferred syntax	1	3
Issue D Invalid Padding	0	1
Issue E Duplicate SAN	29	101

6. Publication of affected certificates

While it has been the position of the Mozilla community for some time that Web PKI certificates are public by nature, German laws, especially data/privacy protection laws, make this situation more complicated. Publication of affected certificates themselves by DFN-PKI is thus subject to prior verification of the lawfulness of such a publication.

The German Federal Data Protection Act states in Section 4 (http://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html#p0061):

"The collection, processing and use of personal data shall be admissible only if permitted or prescribed by this Act or any other legal provision or if the data subject has consented."

Certificate contents such as IP-Addresses, Domain Names and E-Mail Addresses must (in many cases) be considered to be personal data according to German law. The certificates in question do thus have to be considered to be subject to German data protection and privacy laws (which are, as you might know, among the strictest worldwide). We have not been granted explicit consent for publication upon issuance of the certificates in all cases. If there is neither "consent" nor "legal provision", we cannot publish them.

However, some of the certificates are already logged in CT Log because they were used on public web servers. Additionally, we will publish all affected Issuer DNs, serial numbers, fingerprints and

validity dates of the affected certificates.

DFN-PKI is in the progress to establish processes to acquire consent from applicants for publication for each server certificate in the course of introducing certificate transparency later this year 2017, but this work is not finished and does not affect already existing certificates.