Inhaltsverzeichnis

1 Introduction

In July and August 2017, several certificates were discovered, which did not comply with the CA/Browser Forum Baseline Requirements. Some of these certificates were issued by T-Systems, see:
https://bugzilla.mozilla.org/show_bug.cgi?id=1391074.

We implemented the check-tools (CABlint, X509lint, zlint) to perform further investigations. On 2017-09-19, we scanned all not expired and not revoked server certificates of the PKI hierarchies under the following CA certificates:
CN=TeleSec ServerPass CA 2 (https://crt.sh/?id=4912414)
CN=Shared Business CA 4 (https://crt.sh/?id=4460355)
CN=TeleSec ServerPass Class 2 CA (https://crt.sh/?id=8733623)

As a result, we found additional 24 incorrect certificates. All these certificates were revoked!

2 Further findings with CABlint, X509lint, zlint

2.1 Issue A: Metadata in OU

A set of 2 certificates with empty coded OU was detected.

2.2 Issue B: ST appears to only include metadata

A set of 3 certificates with empty coded ST was detected.

2.3 Issue C: Unallowed key usage for EC public key (Key Encipherment)

A set of 3 certificates with the key usage key Encipherment was detected

2.4 Issue D: No Subject alternative name extension

1 certificate without subject alternative name extension was detected

2.5 Issue E: IP address in dns name

A set of 10 certificates with an IP address coded as dns name was detected.

2.6 Issue F: Invalid country in countryName

A set of 4 certificates was detected

2.7 Issue G: BR certificates with organizationName must include either localityName or StateOrProvinceName

1 certificate was detected.

3 Root Causes and Remediation

3.1 Issue A: Metadata in OU

3.1.1 Cause

This issue has two different causes:

- The PKI system is removing spaces at the end of the OU field but is not checking whether the field is empty afterwards. In these cases the PKI system is coding an empty field into the certificate.
- Monitoring of issued certificates and self auditing (as required per BR) by TSI, did not catch the problem.

3.1.2 Remediation

- Retrain Enterprise RAs to raise awareness for requests with empty OU fields or OU fields with a space within the next 2 weeks.
- A fix of the PKI system is ordered. The PKI system will be fixed within the next 2 months.
- The self audit of issued certificates has been increased. Since 2017-09-21 all issued and non-revoked certificate of the day before are checked with the tools CABlint, X509lint and zlint.

Handling of affected certificates: Both Certificates were revoked on 2017-09-28.

3.2 Issue B: ST appears to only include metadata

3.2.1 Cause

This issue has two different causes:

- The PKI system is removing spaces at the end of the ST field but is not checking whether the field is empty afterwards. In these cases the PKI system is coding an empty field into the certificate.
- Monitoring of issued certificates and self auditing (as required per BR) by TSI, did not catch the problem.

3.2.2 Remediation

- Retrain Enterprise RAs to raise awareness for requests with empty ST fields or ST fields with a space within the next 2 weeks.
- A fix of the PKI system is ordered. The PKI system will be fixed within the next 2 months.
- The self audit of issued certificates has been increased. Since 2017-09-21 all issued and non-revoked certificate of the day before are checked with the tools CABlint, X509lint and zlint.

Handling of affected certificates: 2 Certificates were revoked on 2017-10-02. One certificate of the European Union was revoked on 2017-10-06.

3.3 Issue C: Unallowed key usage for EC public key (Key Encipherment)

3.3.1 Cause

This issue has two different causes:

- The PKI system does not distinguish between certificate requests using an RSA key and a certificate requests using an EC key. For both certificate types the same certificate template was used.
- Monitoring of issued certificates and self auditing (as required per BR) by TSI, did not catch the problem.

3.3.2 Remediation

- Certificate requests with EC keys are refused by the PKI system since 2017-09-20
- The self audit of issued certificates has been increased. Since 2017-09-21 all issued and non-revoked certificate of the day before are checked with the tools CABlint, X509lint and zlint.

Handling of affected certificates: Certificates were revoked on 2017-09-28

3.4 Issue D: No Subject alternative name extension

3.4.1 Cause

- While handling the renewal of very old certificates - caused by a migration error - the PKI system created the renewed certificates without a SAN extension. The error was found in 2016-11 and the affected certificates were revoked, but we missed one certificate.

3.4.2 Remediation

- The error was fixed on 2016-12-06 by a new PKI system version.
- The self audit of issued certificates has been increased. Since 2017-09-21 all issued and non-revoked certificate of the day before are checked with the tools CABlint, X509lint and zlint.

Handling of affected certificates: The certificate was revoked on 2017-09-27.

3.5 Issue E: IP address in dns name

3.5.1 Cause

This issue has two different causes:

- In former days even Chrome, IE and Firefox supported certificates with a Subject Alternative Name (subjectAltName) extension, but only Firefox uses the “IP address” extension correctly for verifying URLs with IP addresses. Chrome and IE both return warnings about invalid domain names, if the IP address of the URL was in the certificate as an IP Address SAN extension. If the IP address from the URL was in the certificate as a dnsName then Chrome and IE stopped their warnings. So we implemented the possibility to the customer to get an IP address as a DNS Name to avoid warnings from Chrome and IE at that time.
- Monitoring of issued certificates and self auditing (as required per BR) by TSI, did not catch the problem.

3.5.2 Remediation

- The possibility to get an IP address as a DNS Name was removed from the PKI system on 2016-12-06.
- The self audit of issued certificates has been increased. Since 2017-09-21 all issued and non-revoked certificate of the day before are checked with the tools CABlint, X509lint and zlint.

Handling of affected certificates: 6 certificates were revoked on 2017-09-25.
4 certificates were used for the elections for the lower house of the German parliament. While this issue does not impair the security of affected certificates we allowed the customer to replace these certificates after the election frozen zone. The certificates were revoked on 2017-10-06.

3.6 Issue F: Invalid country in countryName

3.6.1 Cause

This issue has two different causes:

- Improper validation by Enterprise RAs. The Enterprise RAs who inspected the C fields before approving did not catch the improper values.
- Monitoring of issued certificates and self auditing (as required per BR) by TSI, did not catch the problem.

3.6.2 Remediation

- Retrain Enterprise RAs to raise awareness for country codes and retrain about iso-3166-alpha2-code within the next 2 weeks.
- The self audit of issued certificates has been increased. Since 2017-09-21 all issued and non-revoked certificate of the day before are checked with the tools CABlint, X509lint and zlint.

Handling of affected certificates: 3 Certificates were revoked on 2017-09-25. One certificate of the European Union was revoked on 2017-10-06.

3.7 Issue G: BR certificates with organizationName must include either localityName or StateOrProvinceName

3.7.1 Cause

This issue has two different causes:

- There was a configuration error on the PKI system for a customer group where neither locality nor stateOrProvince were mandatory.
- Monitoring of issued certificates and self auditing (as required per BR) by TSI, did not catch the problem.

3.7.2 Remediation

- The configuration of the PKI system which issued this certificate was updated on 2017-09-08.
- The self audit of issued certificates has been increased. Since 2017-09-21 all issued and non-revoked certificate of the day before are checked with the tools CABlint, X509lint and zlint.

Handling of affected certificates: The Certificate was revoked on 2017-09-20