Buypass incident report – intermediate certificates not revoked within BR time period

This is an incident report for 2 intermediate certificates not listed in audit reports and not revoked within the BR time period.

The intermediate certificates are 2 of the 8 intermediate certificates not listed in audit reports and should therefore have been revoked. This was reported as a bug earlier; '*Buypass incident report – intermediate certificates not listed in audit reports*' (Bugzilla Bug # 1595113).

===How your CA first became aware of the problem (e.g. via a problem report submitted to your Problem Reporting Mechanism, a discussion in mozilla.dev.security.policy, a Bugzilla bug, or internal self-audit), and the time and date.

We became initially aware of this problem by a discussion on mozilla.dev.security.policy (and subsequently a task in CCADB) and a later clarification from Ryan Sleevi on the same mailing list.

===A timeline of the actions your CA took in response. A timeline is a date-and-time-stamped sequence of all relevant events. This may include events before the incident was reported, such as when a particular requirement became applicable, or a document changed, or a bug was introduced, or an audit was done.

The first incident (8 intermediate certificates not listed in audit reports) was reported Friday November 8th 2019 and at this point in time our intention was to revoke all 8 certificates.

We did revoke 6 of the 8 intermediate certificates Tuesday November 12th. The reason for not revoking the last 2 intermediate certificates is due to the fact that analyzes of OCSP requests made us aware of that the 2 intermediate certificates in question were still extensively used. We decided to do a more thorough investigation in order to not cause any main issues for customers still using these old intermediate certificates.

Friday November 16th Ryan Sleevi clarified on mozilla.dev.security.policy the expectations for a CA with intermediate certificates not listed in the audit report.

Based on this clarification, we decided to create an incident report (this) since the 2 intermediate certificates were not revoked within the BR time period.

===Whether your CA has stopped, or has not yet stopped, issuing certificates with the problem. A statement that you have will be considered a pledge to the community; a statement that you have not requires an explanation.

The 2 intermediate certificates were issued back in time.

We do no longer issue intermediate certificates "within scope" of our audits without including them in the audit reports.

We will also do our best to ensure that any revocation of intermediate certificates will be within the BR time period.

===A summary of the problematic certificates. For each problem: number of certs, and the date the first and last certs with that problem were issued.

The 2 intermediate certificates are issued to two issuing CAs (ICAs) capable of issuing TLS certificates: Buypass Class 2 CA 2 and Buypass Class 3 CA 2.

The 2 intermediate certificates were issued back in September 2012 and was the standard intermediate certificates for the two ICAs until a new set of intermediate certificates were issued in December 2016.

Mozilla introduced a requirement for including the SHA256 hash of intermediate certificates in the audit report in Mozilla Root Store Policy v2.5 in 2017. Since this date, we have included the hash of the latest generations of intermediate certificates for the audited ICAs in the audit report.

===The complete certificate data for the problematic certificates. The recommended way to provide this is to ensure each certificate is logged to CT and then list the fingerprints or crt.sh IDs, either in the report or as an attached spreadsheet, with one list per distinct problem.

The 2 intermediate certificates still under investigation are:

- https://crt.sh/?id=767143
- https://crt.sh/?id=1452271

===Explanation about how and why the mistakes were made or bugs introduced, and how they avoided detection until now.

The main cause of this issue is the same as for the first incident mentioned above:

We consider the ICA to be the main entity when it comes to issuing certificates. An intermediate certificate is not “capable of issuing a certificate” (despite the wording in BR).

Our understanding has always been that it is the ICAs (and corresponding root CAs) which are subject to audits and included in audit reports, not the intermediate certificates for these ICAs.

However, we understand that the expectations from the community differs from our view and respect this.

===List of steps your CA is taking to resolve the situation and ensure such issuance will not be repeated in the future, accompanied with a timeline of when your CA expects to accomplish these things.

We do not consider the failure to include all the intermediate certificates in the audit report to be a security issue. Therefore, we do not consider the failure to revoke these intermediate certificates within the BR time period to be a security issue.

However, we do understand that both failures are compliance issues and will ensure that both intermediate certificates are revoked.

Since both intermediate certificates are still extensively used, we must ensure that revoking them will not cause any main issues for customers still is using these old intermediate certificates.

We have identified customers still using the affected intermediate certificates, are in the process of contacting them, and advise them to replace the intermediate certificates with the latest generation to avoid any issues at time of revocation.