Buypass incident report – intermediate certificates not listed in audit reports

This is an incident report for 8 intermediate certificates not listed in audit reports

===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 aware of this problem by a discussion on mozilla.dev.security.policy (and subsequently a task in CCADB).

===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.

We became aware of the issue when reading a posting from Kathleen to mozilla.dev.security.policy October 16th. We logged into CCADB, but misinterpreted what this was about and postponed any further action until the week after.

We started investigations October 22nd. We did not quite understand the issue, so we asked Kathleen for clarifications by email on October 25th.

Based on Kathleen's reply we discussed the options with our auditors October 29th during an onsite visit. The same day Kathleen posted an email clarifying the options on mozilla.dev.security.policy.

We discussed this further with our auditors on October 30th and realised that revocation was the only feasible option.

We have initiated some activity to find out if any of the intermediate certificates are still used. Based on the result from these activities, we will prepare a plan for revocation of the intermediate certificates.

===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.

All intermediate certificates involved were issued back in time.

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

===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 intermediate certificates in question are related to two issuing CAs (ICAs) capable of issuing TLS certificates: Buypass Class 2 CA 2 and Buypass Class 3 CA 2.

Both ICAs were established in 2010 and we issued multiple intermediate certificates for these two ICAs during the first period after establishment. All intermediate certificates issued have been compliant with relevant requirements at time of issuance.

There are 4 intermediate certificates for each ICA, in total 8 intermediate certificates.

The first set of intermediate certificates were issued in October 2010 and the last set of certificates in question were issued in September 2012.

===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 intermediate certificates not listed in audit reports are:

For Buypass Class 2 CA 2:
https://crt.sh/?id=12629289
https://crt.sh/?id=12629290
https://crt.sh/?id=767143
https://crt.sh/?id=23234308

For Buypass Class 3 CA 2:
https://crt.sh/?id=23234307
https://crt.sh/?id=12624719
https://crt.sh/?id=1452271
https://crt.sh/?id=7634742

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

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.

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 last email from Kathleen on mozilla.dev.security.policy regarding this topic defined the options and we would have preferred to include the hash of the intermediate certificates in the audit reports.

However, audit reports (at least those issued by our auditors) is a time stamped statement and it is not possible for our auditors to reissue audit reports back in time including the intermediate certificates.

===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.

The situation described by this incident report is based on our understanding of the relation between an ICA and its intermediate certificates.

We realise that our understanding differs from the expectations of members in the community. We will make our best effort to interpret relevant requirements more literally and not so much using our own judgement.