Buypass incident report: Missing NCA identifier in cabfOrganizationIdentifier in PSD2 QWACs

This is an incident report for an issue related to 16 PSD2 QWACs issued by Buypass since the cabfOrganizationIdentifier extension was mandated for EV certificates if the subject.OrganizationIdentifier is present. Buypass use the subject.OrganizationIdentifier in PSD2 QWACs complying with ETSI TS 119 495. The issue is that the NCA identifier included in subject.OrganizationIdentifer is missing in the cabfOrganizatonIdentifier.

1. 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.

Buypass became aware of this by an email received from members of the PSD2 community Thursday 26 March 2020. This was reported as a possible ambiguity in how to carry the PSD2 Authorisation Number in the CA/Browser Forum Organization Identifier Field as defined in EV section 9.8.2. The email also included a recommendation to include the NCA identifier in the registrationReference in the cabfOrganizationIdentifier extension.

2. 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.

2020-02-01: The cabfOrganizationIdentifer extension was mandated in EV certificates if subject.OrganizationIdentifier is present.

Buypass have issued 16 PSD2 QWACs in the period after.

2020-03-26, 13:02: Buypass received the email notifying us about the possible ambiguity.

We started investigating the issue immediately and acknowledged that it probably was an issue with our certificates. The issue was identified to be that the NCA identifier was missing in the cabfOrganizatonIdentifier extension.

We stopped issuance of PSD2 QWACs after identifying this as a potential issue and decided to follow the recommendation from the PSD2 community to include the NCA identifier in the cabfOrganizationIdentifier.

2020-03-27, 16:00 A fix was implemented and verified in test.

2020-03-29, 17:00 The fix was deployed to production and verified before we started issuance of postponed PSD2 QWACs due to this issue.

We also discussed this issue with our ETSI auditor to ensure that we have a common understanding of the issue and how to solve it.

3. 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.

Buypass stopped the issuance of PSD2 QWACs immediately when becoming aware of the issue.

4. 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 16 affected certificates were issued in the period February 4th 2020 to March 20th 2020.

5. 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.spreadsheet, with one list per distinct problem.

The affected certificates are:
https://crt.sh/?id=2557648789
https://crt.sh/?id=2528429797
https://crt.sh/?id=2512093551
https://crt.sh/?id=2503683683
https://crt.sh/?id=2604810665
https://crt.sh/?id=2471346305
https://crt.sh/?id=2599785898
https://crt.sh/?id=2599780360
https://crt.sh/?id=2591181055
https://crt.sh/?id=2591109199
https://crt.sh/?id=2591055509
https://crt.sh/?id=2591042445
https://crt.sh/?id=2591008891
https://crt.sh/?id=2590154860
https://crt.sh/?id=2590152271
https://crt.sh/?id=2414909564

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

The lack of NCA identifier in the cabfOrganizationIdentifier was introduced when the support for this extension was coded into our certificate issuance module. The main focus was on the structure of the extension and not so much of the details within in the RegistrationReference element. The extension includes 3 mandatory elements: 1) the registrationSchemeIdentifier (i.e. 'PSD'), the registrationCountry and the registrationReference.

The registrationReference shall uniquely identify a legal entity and the PSD2 Authorisation Number will fulfill this requirement. Although EVG section 9.8.2 is not very precise on this, we understand (now) that the registrationReference should include both the NCA identifier and the PSD2 Authorisation number.

The cabfOrganizationIdentifier extension is required to identify a legal entity uniquely and this is achieved with or without the NCA identifier, as long as the country code is included (and there is only one NCA per country).

However, after investigating this issue, it is now clear to us that the registrationReference should be “encoded” similarly to the registrationReference in subject.OrganizationIdentifier.

7. 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.

This issue is a detail in an implementation of a certificate profile element which is hard to detect automatically, at least as there are possible ambiguities in the interpretation of the requirements. However, we have now added unit tests for this specific attribute.

We would also recommend providers of linting software to implement controls for new elements introduced in BR/EVG. We do run linters as a part of our certificate issuance processes so this would reduce the risk of such issuances to be repeated in the future.

Buypass analysis and conclusion is that it is not necessary to revoke the affected certificates due to the ambiguity described above. The certificate extension is presumably not used by PSD2 implementations as the same information is available in subject.OrganizationIdentifier. These certificates are used in the PSD2 infrastructure possibly for high volume transaction systems and a revocation will definitely cause harm for the affected customers.