Introduction

Context: EV Guidelines are great, but not every section is necessarily written with automation practices in mind.

- Some sections already support automation today:
  - Example: Use of a signature process that establishes the name and title of the signer in a secure manner, such as through use of an appropriately secure login process that identifies the signer before signing
  - Compared to manual methods: Contacting the Applicant using a Verified Method of Communication for the Applicant, or worse! A letter mailed to the Applicant's or Agent's address

Goal of this initiative: Remove ambiguities that act as barriers to automation.

- Automation can mean two things:
  - Automation of validation – think domain validation
  - Automation of certificate issuance

Method: incremental improvements based on consensus

Main themes for this round

1. Review requirements that imply manual actions
2. Definitions for due diligence and cross-correlation, clarification that:
    1. It must be performed prior to issuance;
    2. It can be re-used (not required for each individual certificate request)
3. Out-scoping domain validation of due diligence & cross-correlation
    1. Out of scope of due diligence because human review does not add value;
    2. Out of scope of cross-correlation because there's nothing to cross-correlate
4. Various improvements

Location

https://github.com/cabforum/servercert/compare/main...chrisbn:servercert:improve-evg-automation-issue-467

Due diligence and domain validation (11.13)

Relevant Clauses:

1. The CA MUST ensure that all information and documentation assembled **as part of the verification processes and procedures** has undergone Due Diligence and Cross-Correlation **prior to issuance of the Certificate.**

Theme:

- Clarification that due diligence and cross-correlation:
  - Must be performed prior to issuance;
  - Can be re-used (not required for each individual certificate request)

Explanation of updates:

- Removal of the reference to EV Certificate application to remove suggestion that these checks must be performed for each certificate (recurring theme);
- Added time element to clarify that this check must be done prior to issuance.

Due diligence and domain validation (11.13)

Relevant Clauses:

- 2. Due Diligence is the process of confirming that each verification process and procedure performed, separately, meets the requirements of these Guidelines. Verification of Domain Name(s), if performed in an automated manner, is out of scope of Due Diligence.

Theme:

- Better definitions of due diligence and cross-correlation
- Domain validation out of scope of due diligence and cross-correlation

Explanation of updates:

Removal of any reference to automated processes, replaced by out-scoping of domain validation if automated.

Question:

Should the definition go into the definition section?

Due diligence and domain validation (11.13)

Relevant Clauses:

- 3. Cross-Correlation is the process of confirming that all Subject information and documentation assembled as part of the verification processes and procedures relates to the same Subject and that there are no discrepancies between the verification elements as they relate to one another. Verification of Domain Name(s) is out of scope of Cross-Correlation.

Theme:

- Better definitions of due diligence and cross-correlation
- Domain validation out of scope of due diligence and cross-correlation

Explanation of updates:

Specific out-scoping of domain validation, regardless of automated or manual, as there isn't anything to cross-correlate ☺

Question:

Should the definition go into the definition section?

Due diligence and domain validation (11.13)

Relevant Clauses:

Removed: In the case of EV Certificates to be issued in compliance with the requirements of [Section 14.2](#142-delegation-of-functions-to-registration-authorities-and-subcontractors), the Enterprise RA MAY perform the requirements of this Final Cross-Correlation and Due Diligence section.

Theme:

- Various improvements

Explanation of updates:

Not sure of appropriateness or added value of the Enterprise RA doing this.

Requirements for Re-use of Existing Documentation (11.14)

Relevant Clauses:
For each EV Certificate Request, including requests to renew existing EV Certificates, the CA MUST ensure all authentication and verification tasks required by these Guidelines have been completed, to ensure that the request is properly authorized by the Applicant and that the information in the EV Certificate is still accurate and valid. This section sets forth the conditions on the re-use of documentation collected by the CA.

The CA MAY rely on previously performed Due Diligence and Cross Correlation for the an Applicant to support multiple EV Certificate Requests for that Subscriber, on the conditions that:

1. the data used to support issuance of an EV Certificate meets the Age of Validated Data requirement as set forth in 11.14.3;

2. a Pre-Authorized Certificate Approver, pre-Authorized in line with 11.8.4 reviewed and approved the EV Certificate Request by use of:

A. 11.10.2. option 2;

B. 11.9.2. option 3, in case the Pre-Authorized Certificate Approver also acts in the capacity of a Certificate Requester

The CA MAY reuse a previously submitted EV Certificate Request, Subscriber Agreement, or Terms of Use, including use of a single EV Certificate Request in support of multiple EV Certificates containing the same Subject to the extent permitted under Section 11.9 and Section 11.10.

Requirements for Re-use of Existing Documentation (11.14) - detail

Relevant Clause: This section sets forth the conditions on the re-use of documentation collected by the CA.

Theme: Various improvements

Explanation of updates:

Previously there was a reference to age as a condition, but other sub-sections are not just about age.

Requirements for Re-use of Existing Documentation (11.14) - detail

Relevant Clause: The CA MAY rely on previously performed Due Diligence and Cross Correlation for an Applicant to support multiple EV Certificate Requests for that Subscriber, on the conditions that:

1. the data used to support issuance of an EV Certificate meets the Age of Validated Data requirement as set forth in 11.14.3;

2. a Pre-Authorized Certificate Approver, pre-Authorized in line with 11.8.4 reviewed and approved the EV Certificate Request by use of:

A. 11.10.2. option 2;

B. 11.9.2. option 3, in case the Pre-Authorized Certificate Approver also acts in the capacity of a Certificate Requester

Theme: Clarification that due diligence and cross-correlation:

- Must be performed prior to issuance;
- Can be re-used (not required for each individual certificate request)

Explanation of updates:

Goal: as long as information is still valid, there's no need to re-do the Due Diligence and Cross Correlation checks **if** the Approval of the newly submitted certificate request has been given in an automated way.

Separation of Duties (14.1.3.)

Relevant Clauses:

- 1. The CA MUST enforce rigorous control procedures for the separation of validation duties to ensure that no one Validation Specialist can single-handedly **complete all verification processes and procedures**. Due Diligence and Cross-Correlation MAY be performed by a single Validation Specialist, however the Validation Specialist MUST not be involved in the processes and procedures performed. For example, one Validation Specialist collects all Applicant information and a second Validation Specialist performs Due Diligence and Cross-Correlation.

Theme:

- Clarification that due diligence and cross-correlation:
  - Must be performed prior to issuance;
- Review requirements that imply manual actions

Explanation of updates:

Removed reference to “validate and authorize the issuance of an EV Certificate” and replaced by “complete all verification processes and procedures” with the reasoning: remove suggestion that these checks must be performed for each certificate

Verification of Approval of EV Certificate Request (11.10)

Relevant Clauses (11.10.1):

- In cases where an EV Certificate Request is submitted by a Certificate Requester, before the CA issues the requested EV Certificate, the CA MUST **ensure** that an authorized Certificate Approver reviewed and approved the EV Certificate Request.

Theme:

- Clarification that due diligence and cross-correlation:
  - Must be performed prior to issuance;
  - Can be re-used (not required for each individual certificate request)

Explanation of updates:

Ensure rather than *verify*, so it is clear that this is not necessarily something that needs to be checked for each certificate.

Question: Is "ensure" still too vague and suggestive? Should we be more explicit with what we want here?

Verification of Signature on Subscriber Agreement and EV Certificate Requests (11.9)

Relevant Clauses (11.10.1):

- The EV Certificate Request MUST be signed by the Certificate Requester submitting the document, unless the Certificate Request has been approved by a Certificate Approver pre-authorized in line with [Section 11.8.4](#1184-pre-authorized-certificate-approver).

Theme:

  - Various improvements

Explanation of updates:

Previous language seemed to suggest that the Certificate Request was pre-authorized, when 11.8.4 is about the pre-authorization of the certificate Approver (who can subsequently post-authorize new requests)

Data Security (16)

Relevant Clauses:

Removed the following: In addition, systems used to process and approve EV Certificate Requests MUST require actions by at least two trusted persons before creating an EV Certificate.

Theme: Clarification that:

- due diligence and cross-correlation must be performed prior to issuance;
- due diligence and cross-correlation is not required after receiving individual certificate requests

Explanation of updates:

Remove the need to have two people involved for the issuance of an EV Certificate (again, remove suggestion that Due Diligence and Cross Correlation checks must be performed for each certificate)