Proof-of-Concept for BR of BRs with requirements Matrix

Paul van Brouwershaven
Director Technology Compliance

CA/Browser Forum F2F#60
October 2023
Location of the Proof-of-Concept

- GitHub username: vanbroup
- Repository: documents
- Branch: brofbr

- [https://github.com/vanbroup/documents/tree/brofbr/](https://github.com/vanbroup/documents/tree/brofbr/)

- Scripts are in the directory “tools” (including a README)
- The unmodified source files in the directory “docs” (as usual)
- The transformed files (the proposed working format) in the directory “structured”
- The example output in the directory “output”
Objective

Streamline and harmonize the existing baseline requirements documents within the CA/Browser Forum, with the aim of reducing duplication and enhancing clarity, by establishing a unified set of baseline requirements applicable to various certificate use cases.

Rationale

The CA/Browser Forum has developed multiple baseline requirements documents, including those for TLS certificates, code signing, S/MIME, and might develop potentially others in the future.

These documents often contain overlapping or redundant content, as they all draw from the same fundamental best practices initially defined in the Baseline Requirements for TLS certificates.

This redundancy results in additional work for Certification Authorities (CAs), web browsers, and auditors, as they must navigate multiple documents with sometimes slightly different wording while addressing common requirements.
Benefits

1. **Maintenance and Updates**: A centralized baseline requirements document will facilitate **easier maintenance and updates**, ensuring that best practices are current and reflective of evolving security needs.

2. **Consistency**: A unified set of baseline requirements will **promote consistency** in certificate issuance and management practices across different use cases, making it **easier to understand and adhere to**.

3. **Efficiency**: With common requirements consolidated, CAs can allocate resources more efficiently, **focusing on specific, detailed requirements for individual use cases** without reiterating shared standards.

4. **Clarity**: With **clearly identified requirements**, and an overview in a spreadsheet, it becomes easy to filter and difficult to miss requirements. It also makes it easier to adopt a Governance Risk and Compliance (GRC) system.
The establishment of a “BR of BRs” will require some changes on how we operate, for example all members might need to be required to participate in a new baseline working group with its own IPR clearance.

• This proposal is not intended to solve that problem
A layered approach

Baseline Requirements (BR)

Extended Validation Certificate

Profile Requirements
TLS, Code Signing, S/MIME, etc.

Level of Assurance
Organization Validated (OV)

Network and Certificate System Security Requirements

Level of Assurance
Domain Validated (DV)

Level of Assurance
Extended Validated (EV)
A layered approach

Organization Validation Certificate

Profile Requirements
TLS, Code Signing, S/MIME, etc.

Level of Assurance
Organization Validated (OV)

Level of Assurance
Domain Validated (DV)

Baseline Requirements (BR)

Network and Certificate System
Security Requirements
A layered approach

Domain Validation Certificate

Profile Requirements
TLS, Code Signing, S/MIME, etc.

Level of Assurance
Domain Validated (DV)

Network and Certificate System
Security Requirements

Baseline Requirements (BR)
Chapter “1. INTRODUCTION” matches the root folder “001 INTRODUCTION”

The subfolder “001 Overview” matches section “1.1 Overview”

The prefix of the folder or file relates back to the section of the document so the path:

```
./001 ***/002 ***/15 ***
```

Translates to section 1.2.15

The zero suffix ensures that files are shown and processed in the correct order.
A small document contains one section

3.2.2.1 Identity

If the Subject Identity Information is to include the name or address of an organization, the CA SHALL verify the identity and address of the organization and that the address is the Applicant’s address of existence or operation. The CA SHALL verify the identity and address of the Applicant using documentation provided by, or through communication with, at least one of the following:

1. A government agency in the jurisdiction of the Applicant’s legal creation, existence, or recognition;
2. A third party database that is periodically updated and considered a Reliable Data Source;
3. A site visit by the CA or a third party who is acting as an agent for the CA; or

The CA MAY use the same documentation or communication described in 1 through 4 above to verify both the Applicant’s identity and address.

Alternatively, the CA MAY verify the address of the Applicant (but not the identity of the Applicant) using a utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that the CA determines to be reliable.
Why a structure with small documents?

A document per type (BR, TLS, DV, etc.)
• Migration is difficult and takes a long time
• Large documents can be hard to navigate
• It can be challenging to identify changes
• It’s easy to mess-up a large document
• Difficult to merge multiple layers into one document

A document per section
• Migration can be done section by section
  – Allows to automatically remove duplicate sections
• Easy to navigate a directory structure
• Easy to identify changes
• Focus on a single section when making updates, which should make it easier to draft ballots
• This enables a layered system where individual sections within a document can be appended or replaced
• Allows the creation of combined and separated documents
How are these layers created

The file name prefix defines the weight and target of the document, for example, a file starting with “000_” has the highest priority, this file normally starts a new section, but a file with a higher weight could contain conditional content.

Example: A file starting with “001_CS”, will only be included if the target document defines the Code Signing requirements. In that case the file will be imported after “000_CS” or “000_BR” if no “000_CS” document exists.

- A file with the prefix 000_CS overrules a file with the prefix 000_BR
- When 000_CS does not exist, 000_BR will automatically be imported
Identifying requirements

Currently the documents contain paragraphs that probably include one or more requirements, depending on the interpretation of the reader.

• In this POC we automatically identify requirements which are indicated using a simple format.

• The paragraph would provide the context to the requirement.

For example, if a document contains a text:

    [001] This is a requirement

This will automatically be detected when building the document, appropriately numbered, and included in the final document and spreadsheet. The requirement number will be based on the location of the requirement, for example, if this requirement was included in section 1.1 of the BRs it would get numbered as “BR-1.1-001” and include the following row in the spreadsheet.

The spreadsheet helps with self-assessments and makes it easier to import and maintain a Governance Risk and Compliance (GRC) system with the corresponding controls.

<table>
<thead>
<tr>
<th>ID</th>
<th>Section</th>
<th>LoA</th>
<th>Type</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>BR-1.1-001</td>
<td>1.1</td>
<td></td>
<td>BR</td>
<td>This is a requirement</td>
</tr>
</tbody>
</table>
Advanced instructions

Frontmatter allows us to include or exclude a document from a certain target document, such as currently used in all the appendix documents.

- It’s not sure if we also need this as the appendix document could simply be called TLS instead of BR in the current cases.

Frontmatter is currently also used to set the LoA to DV, OV or EV, alternatively this could also be done using the filename.

```diff
---
targets:
  included:
    - BR
---

# APPENDIX B - Issuance of Certificates for Onion Domain Names

This appendix defines permissible verification procedures for including one or more Onion Domain Names in a Certificate.
```
Status

• The generated BR document is equal to the source document, except for “No stipulation”, which are removed and some additional new lines.
  − New lines can be removed with automatic markdown formatting
  − "No stipulation“ is less predictable using layers and not consistently used, when do we want this?
  − CS and SMIME include some TLS specific sections which should be moved to TLS specific requirements and removed from the BR to ensure that they are not included in CS or SMIME requirements.
• Review the requirement matrix, do we need to add more information?
• Do we want to move LoA from frontmatter to the filename?
• Create a combined CSV file with all requirements for all document types.
Playing with this Proof-of-Concept

- Check the README:

**Usage**

**Transform documents:**
- py transform.py ../docs/BR.md
- py transform.py ../docs/CS.md
- py transform.py ../docs/SKME.md

**Remove duplicates:**
- py duplicates.py

**Build documents and requirement sheets:**
- py build.py BR
- py build.py CS
- py build.py SKME

**Build documents and requirement sheets including only the following Level of Assurance (LoA):**
- py build.py BR --loa OV
- py build.py BR --loa DV OV EV
Thank You

Paul van Brouwershaven

entrust.com

© Entrust Corporation