BR of BRs with requirements Matrix

Paul van Brouwershaven

Director Technology Compliance

CA/Browser Forum F2F#61
February 2024

ENTRUST

SECURING A WORLD IN MOTION

Location

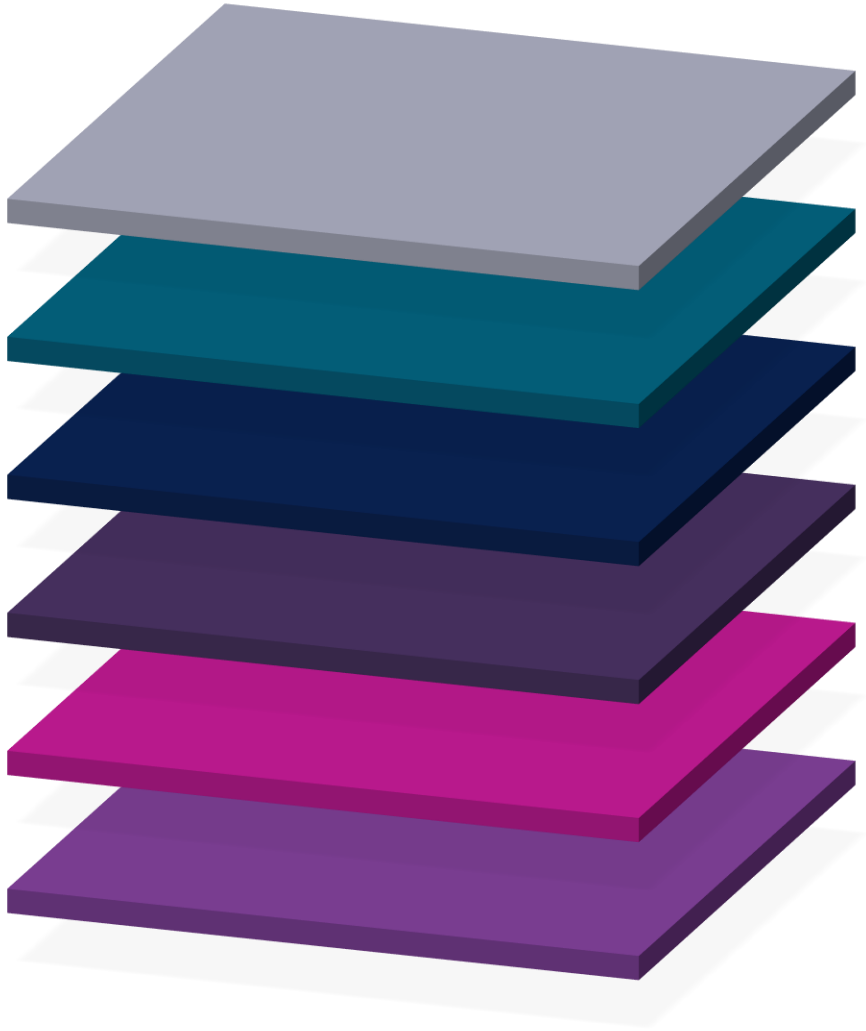
- **GitHub username**: vanbroup
- **Repository**: documents
- **Branch**: brofbr

- 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”

A layered approach

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
Extended Validated (EV)

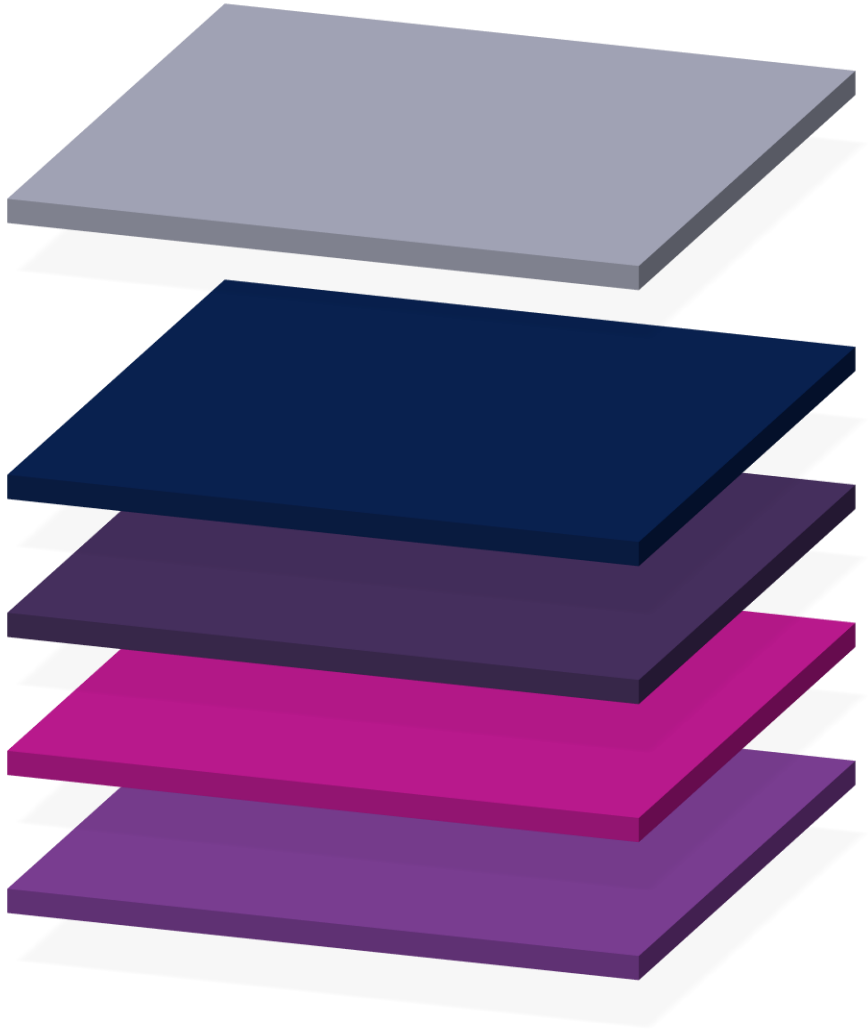
Level of Assurance
Domain Validated (DV)

Baseline Requirements (BR)

ENTRUST

A layered approach

Organization Validation Certificate



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

Level of Assurance
Organization Validated (OV)

Network and Certificate System Security Requirements

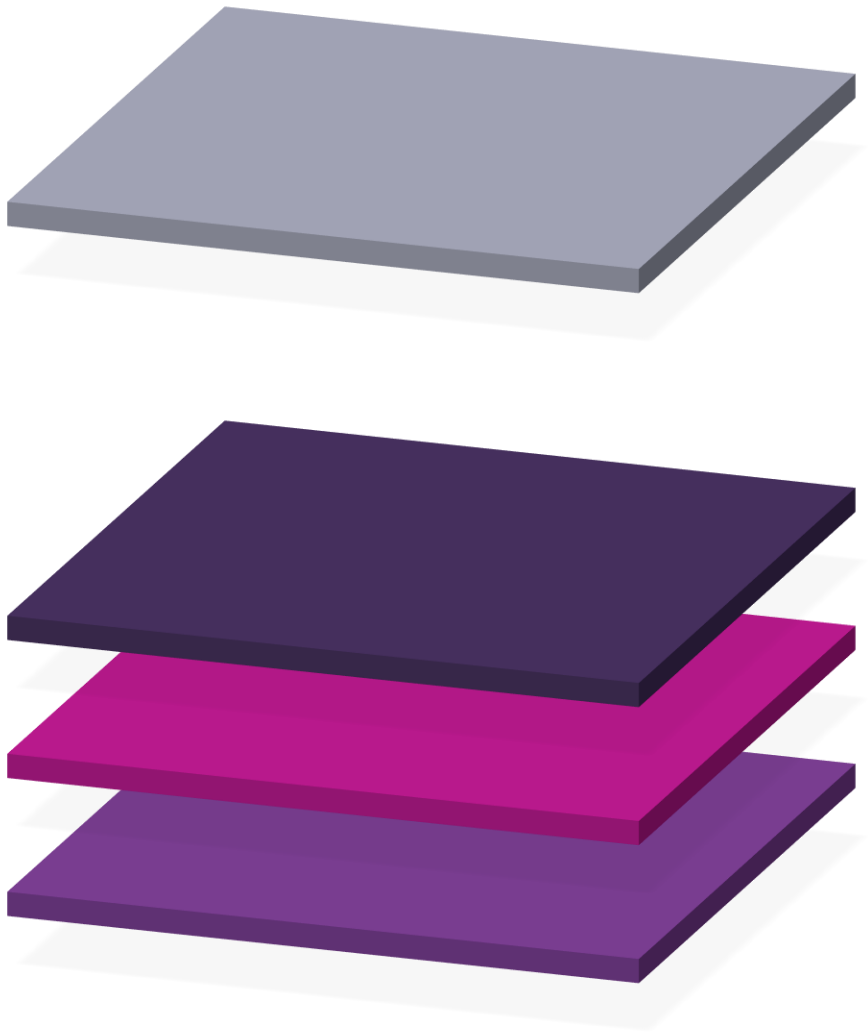
Level of Assurance
Domain Validated (DV)

Baseline Requirements (BR)

ENTRUST

A layered approach

Domain Validation Certificate



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

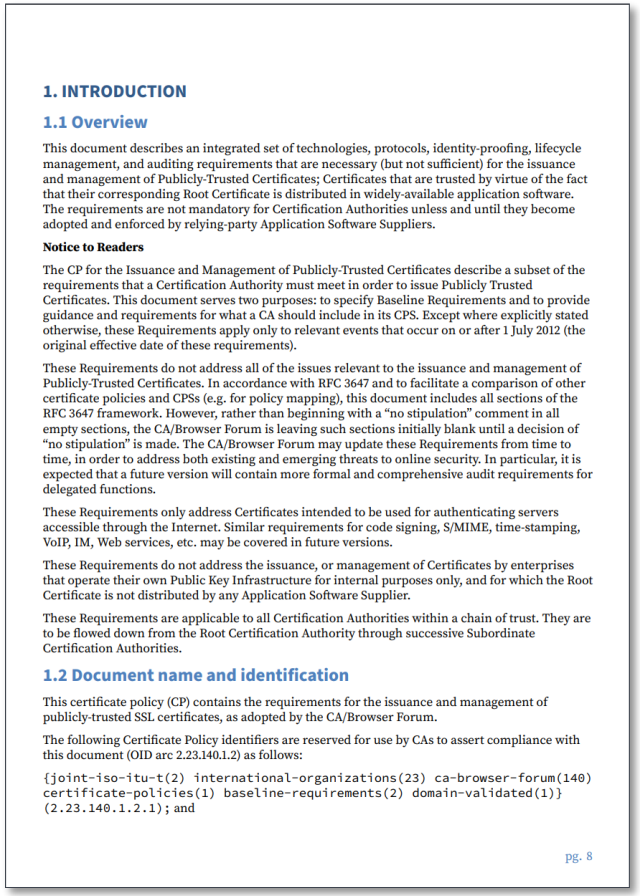
Level of Assurance
Domain Validated (DV)

Network and Certificate System Security Requirements

Baseline Requirements (BR)

ENTRUST

Transforming the RFC 3647 formatted documents



1. INTRODUCTION

1.1 Overview

This document describes an integrated set of technologies, protocols, identity-proofing, lifecycle management, and auditing requirements that are necessary (but not sufficient) for the issuance and management of Publicly-Trusted Certificates; Certificates that are trusted by virtue of the fact that their corresponding Root Certificate is distributed in widely-available application software. The requirements are not mandatory for Certification Authorities unless and until they become adopted and enforced by relying-party Application Software Suppliers.

Notice to Readers

The CP for the Issuance and Management of Publicly-Trusted Certificates describe a subset of the requirements that a Certification Authority must meet in order to issue Publicly Trusted Certificates. This document serves two purposes: to specify Baseline Requirements and to provide guidance and requirements for what a CA should include in its CPS. Except where explicitly stated otherwise, these Requirements apply only to relevant events that occur on or after 1 July 2012 (the original effective date of these requirements).

These Requirements do not address all of the issues relevant to the issuance and management of Publicly-Trusted Certificates. In accordance with RFC 3647 and to facilitate a comparison of other certificate policies and CPSs (e.g. for policy mapping), this document includes all sections of the RFC 3647 framework. However, rather than beginning with a "no stipulation" comment in all empty sections, the CA/Browser Forum is leaving such sections initially blank until a decision of "no stipulation" is made. The CA/Browser Forum may update these Requirements from time to time, in order to address both existing and emerging threats to online security. In particular, it is expected that a future version will contain more formal and comprehensive audit requirements for delegated functions.

These Requirements only address Certificates intended to be used for authenticating servers accessible through the Internet. Similar requirements for code signing, S/MIME, time-stamping, VoIP, IM, Web services, etc. may be covered in future versions.

These Requirements do not address the issuance, or management of Certificates by enterprises that operate their own Public Key Infrastructure for internal purposes only, and for which the Root Certificate is not distributed by any Application Software Supplier.

These Requirements are applicable to all Certification Authorities within a chain of trust. They are to be flowed down from the Root Certification Authority through successive Subordinate Certification Authorities.

1.2 Document name and identification

This certificate policy (CP) contains the requirements for the issuance and management of publicly-trusted SSL certificates, as adopted by the CA/Browser Forum.

The following Certificate Policy identifiers are reserved for use by CAs to assert compliance with this document (OID arc 2.23.140.1.2) as follows:

```
{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140)
certificate-policies(1) baseline-requirements(2) domain-validated(1)}
(2.23.140.1.2.1); and
```

pg. 8

Chapter "1. INTRODUCTION" matches the root folder "001 INTRODUCTION"

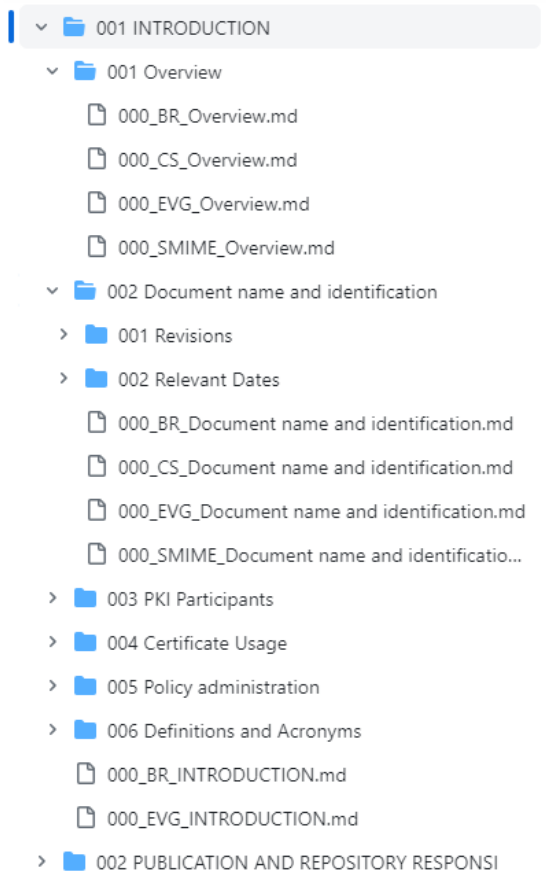
The subfolder "001 Overview" matches section "1.1 Overview"

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

"./001 ****/002 ***/015 ***"

Translates to section 1.2.15

The zero suffix ensures that files are shown and processed in the correct order.



ENTRUST

One section per document

Preview | Code | Blame | 13 lines (8 loc) · 1.1 KB | Code 55% faster with GitHub Copilot | Raw

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:

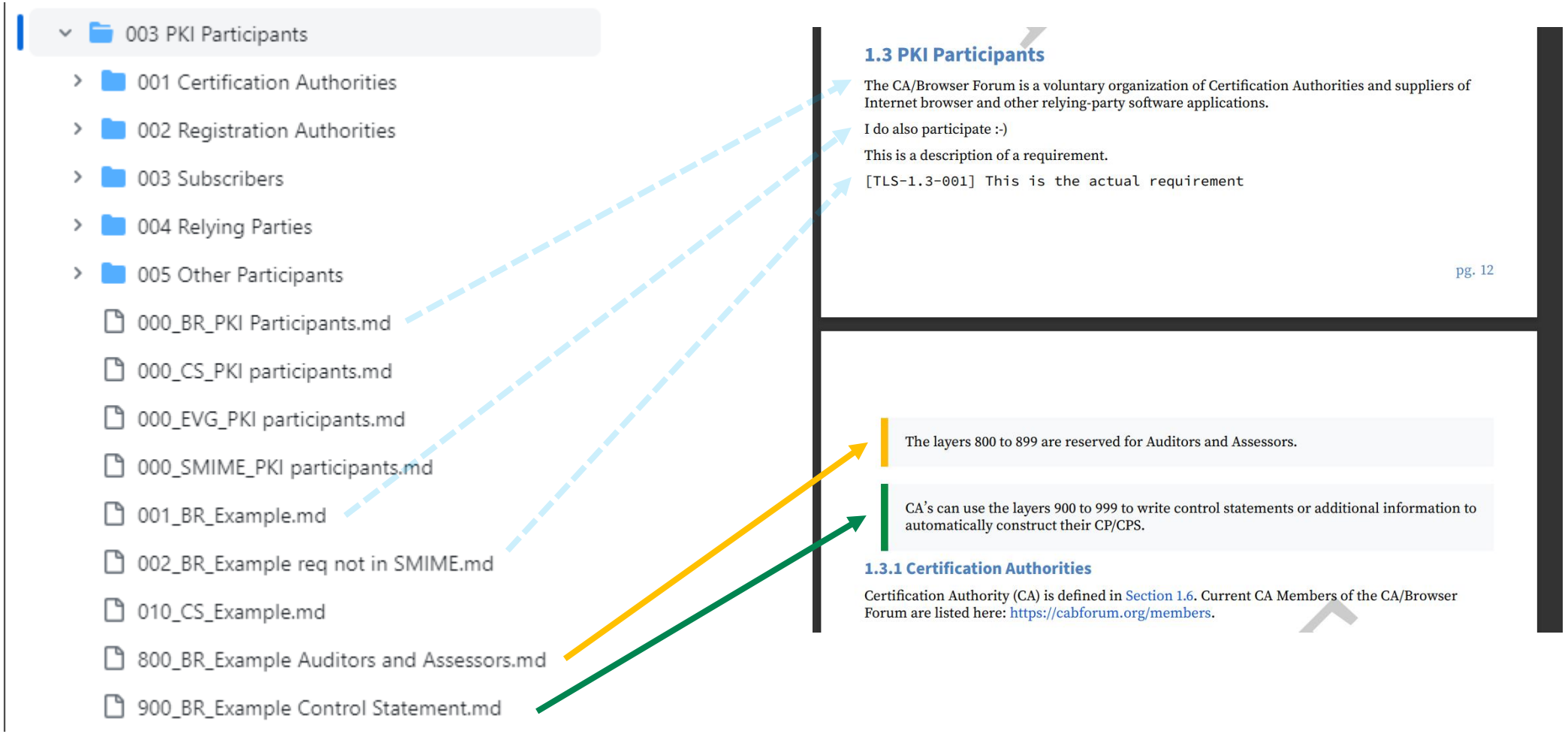
1. A government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;
2. A third party database that is periodically updated and considered a Reliable Data Source;
3. A site visit by the CA or a third party who is acting as an agent for the CA; or
4. An Attestation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

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.

ENTRUST

Sections **can** be combined from multiple layers (documents)



ENTRUST

Layers can have custom styles

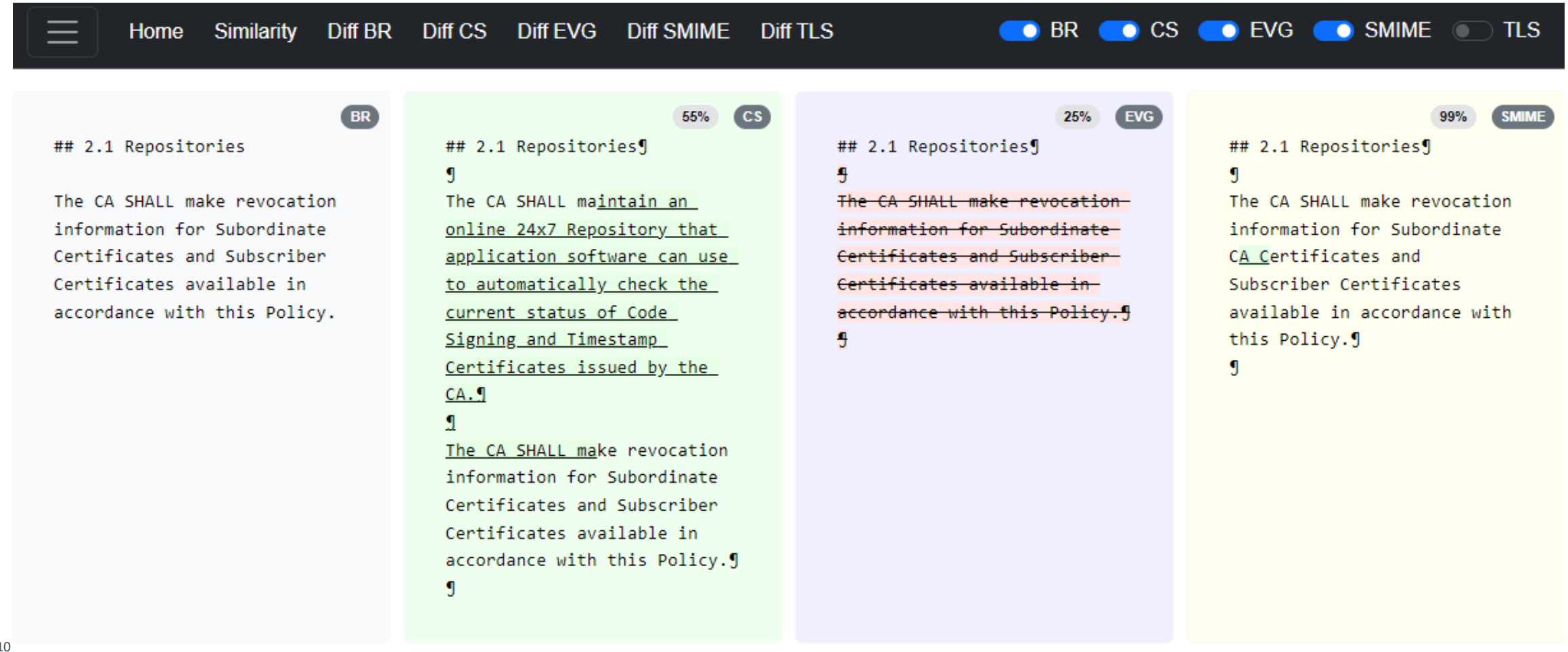
The layers 800 to 899 are reserved for Auditors and Assessors.

CA's can use the layers 900 to 999 to write control statements or additional information to automatically construct their CP/CPS.

ENTRUST

Supporting Interface

- https://vanbroup.github.io/documents/



Deduplication and Similarity

- A lot of duplication is automatically detected and removed
- Similarity to the Baseline Requirements:

	100%	>= 90%	>= 75%	>= 50%	>= 25%	Average	Average incl. 100%
		&& != 100					
	(Sections)					*(%)*	*(%)*
CS (295)	190	14	25	36	56	**39%**	78%
EV (294)	168	2	12	17	41	**23%**	76%
S/MIME	176	23	43	62	87	**49%**	79%

https://vanbroup.github.io/documents/similarity/

ENTRUST

Consistency

- The similarity report also includes some basic information about consistency
  - Does the title match the title of the Baseline Requirements?
  - If this is a section defined by RFC 3647, does the title match?

ENTRUST

Creation of the TLS Baseline Requirements

- Automatically includes all sections of the BRs that appear in other documents (CS and S/MIME) but are not supposed to be included.
- Hardcoded to move the following sections from the BRs to the TLS BRs
  - '3.2.2.3','3.2.2.4','3.2.2.5','3.2.2.6','3.2.2.7','3.2.2.8','7.1.2'

https://vanbroup.github.io/documents/diff-tls.html

ENTRUST

Discussion items

- Currently **all documents** are based on the **latest BRs**
  - This allows CAs to implement TLS, CS and S/MIME without having to deal with different effective dates for different certificate types.
- The BRs of BRs should be managed and have IPR reviewed in a new BR working group that consists of **all forum members**.
- The Validation subcommittee should become a subcommittee of the new BR working group.
- The TLS, CS and S/MIME working groups would focus on the specifics for the issuance of those certificate types, such as:
  - Additional requirements
  - Certificate profiles
  - Which LoA (OV, EV) and methods (DCV, ECV, etc.) will be supported and specify any additional requirements for certain methods (by adding paragraphs on the BRs using document specific layers).

ENTRUST

Discussion items

- Numbering scheme (use RFC 3647 outline but extend and lock down the numbers). Try not to overlap sections in different Guidelines.
- All WGs must commit that they will do efforts to align with the BR of BRs, override only in a justified and documented way and avoid duplication.

ENTRUST

Thank You

Paul van Brouwershaven

entrust.com

ENTRUST

SECURING A WORLD IN MOTION