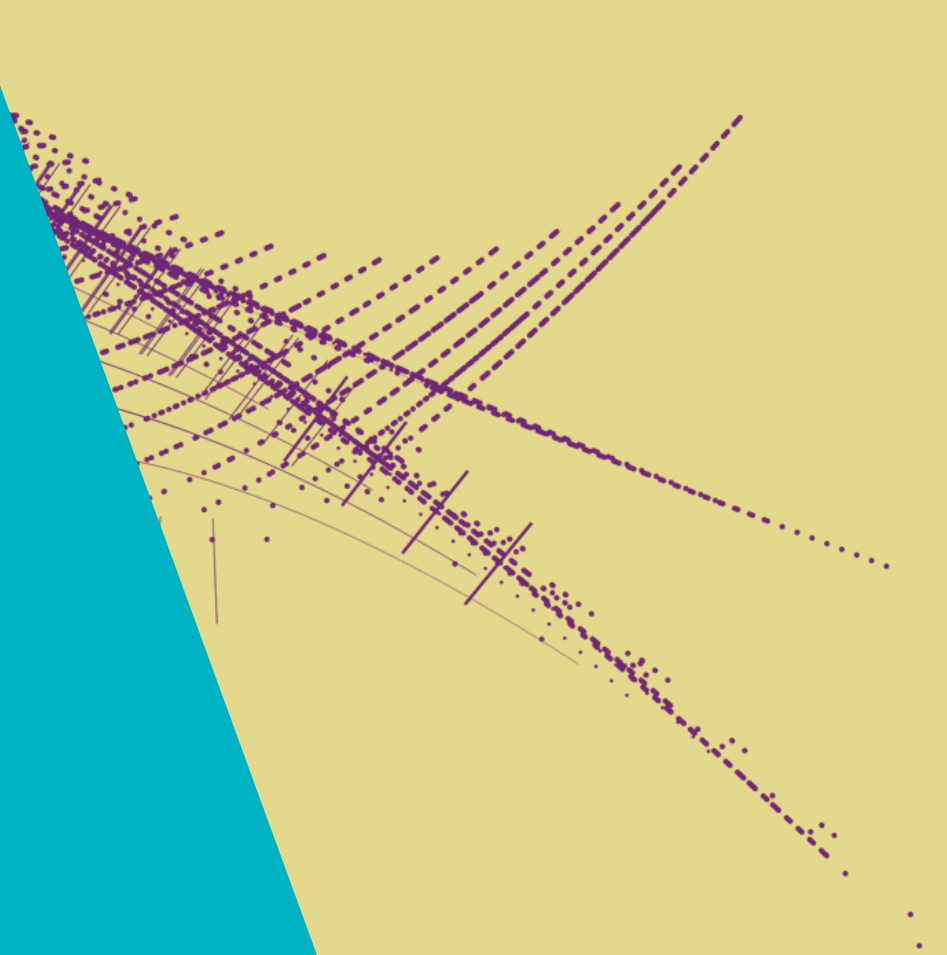
Nikhef

Maastricht University

David Groep



CA/Browser Forum WebPKI and joint trust

October 2022

Joint trust?

Many services today are accessed both by automated agents and (non-interactive) users, but also by eye-balls via browsers

The ‘joint trust’ authorities support that by combining WekPKI trust based on CA/BF Baseline Requirements and IGTF Assurance and PKIX Guidelines that ensure name uniqueness

With cloud (storage) and TPT this is getting very important

name uniqueness is not usually considered in the CA/BF BRs

Joint trust today

DigiCert – OSG, Switzerland, retail

GEANT TCS – Sectigo

InCommon CS – Sectigo

Thanks to the

Hi!

It seems as if CAB/Forum is gaining traction again to fiddle with cert profiles. Apparently they will prohibit all but a limited set of attributes in DNs of publicy trusted certs, and DC is not among them.

Section ##### 7.1.2.7.4 Organization Validated in:
https://github.com/sleevi/cabforum-docs/pull/36/files#diff-e0ac1bd190515a4f2ec09139d395ef6a8c7e9e5b612957c1f5a2dea80c6a6cfeR2266

They even explicitely acknowledge that this will kill current GRID certificates (see slide 6 of the presentation in the attached mail).

Regards

Hi David!

Don't know if you are aware:

CA/B-Forum is working on S/MIME-BRs, which will have severe implications for every user certificate with emailProtection:

https://github.com/cabforum/smime/blob/preSBR/SBR.md

They define a "legacy"-Profile, where things like DC= (or info=) might be acceptable, but in the profiles "strict" and "multipurpose" these things will not be allowed. Goal is to deprecate the legacy-profile pretty soon AFAIK.

They are in the ballot-starting phase. With an adoption date of +8 months after effective date those rules could be in force as early as next July.

I guess that we also need to match the quite specific rules for identification and other stuff to the TCS CPS....

IGTF
Interoperable Global Trust Federation
AP | EU | TAG

IGTF-CABF-DC-response-20220612.docx
Sun, 12 June 2022

Response to the CA/Browser Forum discussion on domainComponent usage

The validation sub-committee of the CA/Browser Forum, during the *Summer 2022 CA/B Forum F2F*, discussed a specific proposal to revise the Baseline Requirements (BR) that, when adopted, would result in serious adverse consequences for the research and education community using certificates for its research infrastructures. Specifically, the proposal

> "Except where explicitly specified, each `Name` MUST NOT contain more than one instance of a given `AttributeTypeAndValue` across all `RelativeDistinguishedName`s." (https://github.com/sleevi/cabforum-docs/pull/36/files#diff-e0ac1bd190515a4f2ec09139d395ef6a8c7e9e5b612957c1f5a2dea80c6a6cfeR3030)

is concerning, since it conflicts with the use of the domainComponent attribute type when used in an RFC-compliant way. It is this 'dc' attribute sequence on which the joint trust mode is based that allows both human researchers to use browsers to access academic research resources, and at the same time enables automated agents to act on those same services for managed data transfers and other research workflow automation tasks.

This was recognised in comments, where "GRID" was highlighted as an active use case that would be impacted, such as https://github.com/sleevi/cabforum-docs/pull/36#discussion_r859176437. The further discussion in that comment does not quite convey the importance of the use case – which is understandable since the research and education user community is not part of those

7.1.4.1 Name Encoding

The following requirements apply to all Certificates listed in Section 7.1.2. Specifically, this includes Technically Constrained Non-TLS Subordinate CA Certificates, as defined in Section 7.1.2.3, but does not include certificates issued by such CA Certificates, as they are out of scope of these Baseline Requirements.

For every valid Certification Path (as defined by RFC 5280, Section 6):

- For each Certificate in the Certification Path, the encoded content of the Issuer Distinguished Name field of a Certificate SHALL be byte-for-byte identical with the encoded form of the Subject Distinguished Name field of the Issuing CA certificate.
- For each CA Certificate in the Certification Path, the encoded content of the Subject Distinguished Name field of a Certificate SHALL be byte-for-byte identical among all Certificates whose Subject Distinguished Names can be compared as equal according to RFC 5280, Section 7.1, and including expired and revoked Certificates.

When encoding a `Name`, the CA SHALL ensure that:

- Each `Name` MUST contain an `RDNSequence`.
- Each `RelativeDistinguishedName` MUST contain exactly one `AttributeTypeAndValue`.
- Each `RelativeDistinguishedName`, if present, is encoded within the `RDNSequence` in the order that it appears in Section 7.1.4.2.
  - For example, a `RelativeDistinguishedName` that contains a `countryName` `AttributeTypeAndValue` pair MUST be encoded within the `RDNSequence` before a `RelativeDistinguishedName` that contains a `stateOrProvinceName` `AttributeTypeAndValue`
- Each `Name` MUST NOT contain more than one instance of a given `AttributeTypeAndValue` across all `RelativeDistinguishedName`s.

Note: Section 7.1.2.2.2 provides an exception to the above `Name` encoding requirements when issuing a Cross-Certified Subordinate CA Certificate, as described within that section.

The rest did not help much

7.1.4.3 Other Subject Attributes

When explicitly stated as permitted by the relavant certificate profile specified within Section 7.1.2, CAs MAY include additional attributes within the `AttributeTypeAndValue` beyond those specified in Section 7.1.4.2.

Before including such an attribute, the CA SHALL:

- Document the attributes within Section 7.1.4 of their CP or CPS, along with the applicable validation practices.
- Ensure that the contents contain information that has been verified by the CA, independent of the Applicant.

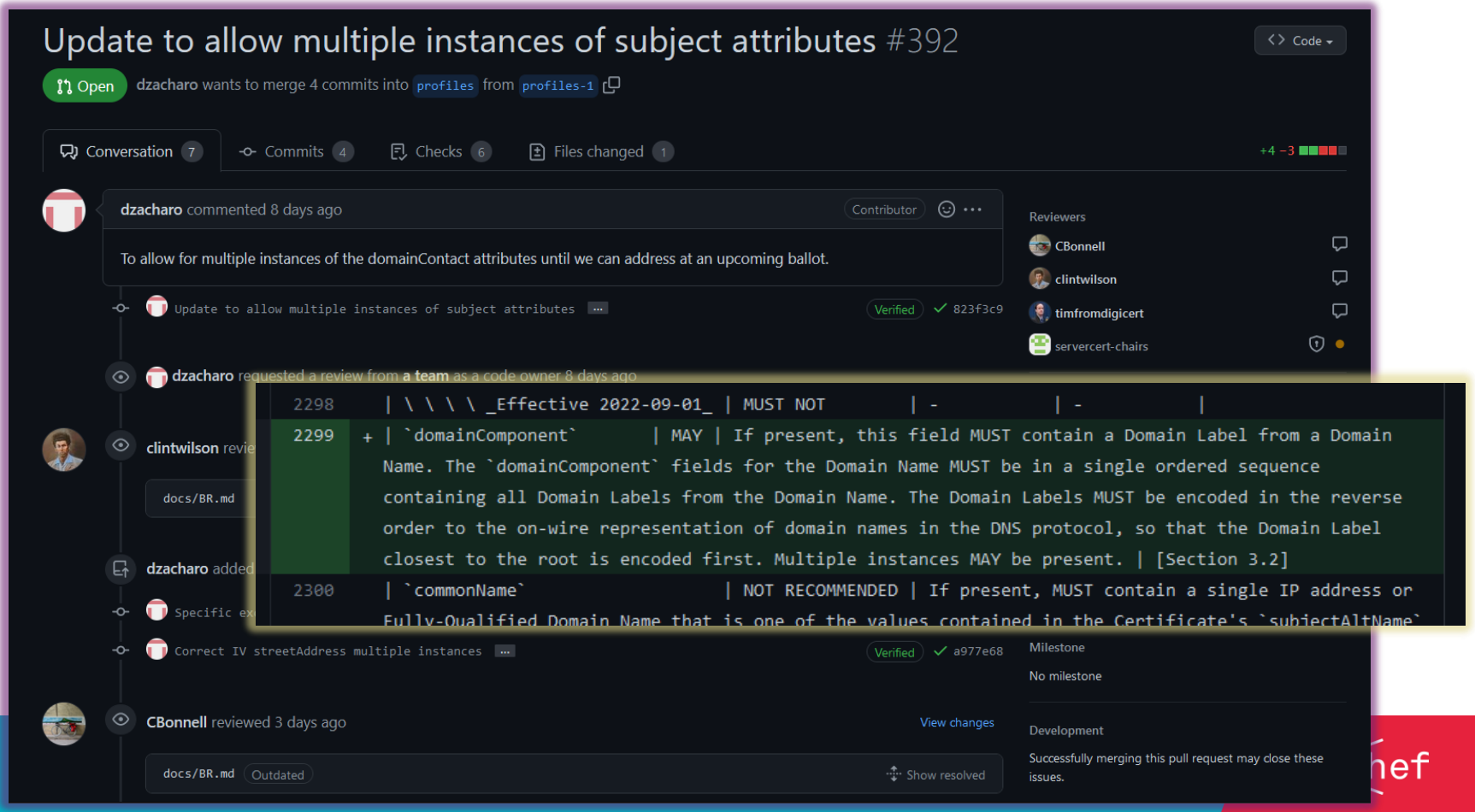
Some frantic discussions

And with great help from (alphabetically :) Clint, Dimitris, and Tim:

- allow domainComponent as per its semantics
- specify very accurately is use cases
- define a validation model (basically: use the DCV methods, but then directed at the responsible org for the scope)

This probably shows the first good mutual interactions – something to foster!

Thanks a million!

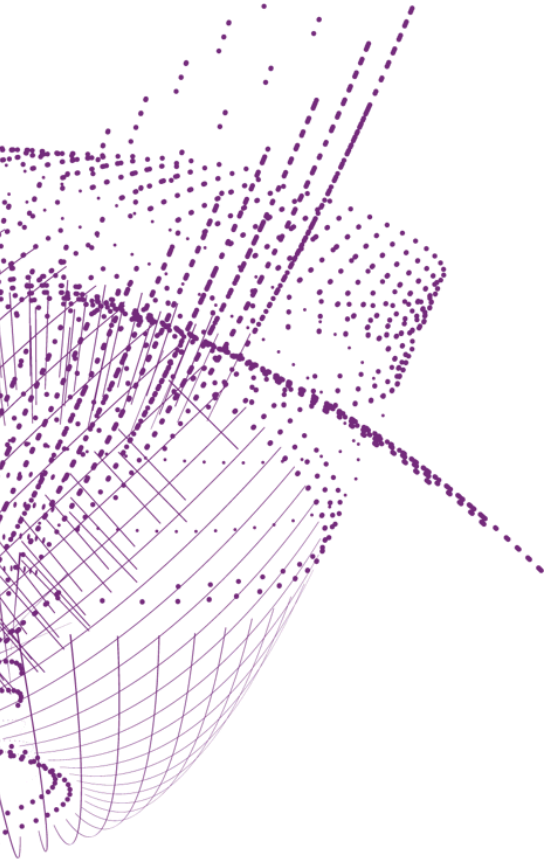


Meanwhile, the discussion brought interesting thoughts

There are more root programmes than just CA/BF …

The separation of transport level trust and authentication trust, and between server-trust and client trust, is also important to the token use cases

Software support for separate trust stores, brought up in the WLCG token context, is worth exploring



Meanwhile in the S/MIME world

S/MIME vs. authentication certificates

Hi David!

Don't know if you are aware:

CA/B-Forum is working on S/MIME-BRs, which will have severe implications for every user certificate with emailProtection:

https://github.com/cabforum/smime/blob/preSBR/SBR.md

They define a "legacy"-Profile, where things like DC= (or info=) might be acceptable, but in the profiles "strict" and "multipurpose" these things will not be allowed. Goal is to deprecate the legacy-profile pretty soon AFAIK.

They are in the ballot-starting phase. With an adoption date of +8 months after effective date those rules could be in force as early as next July.

I guess that we also need to match the quite specific rules for identification and other stuff to the TCS CPS....

https://cabforum.org/2022/07/20/2022-07-20-minutes-of-smime-certificate-working-group/

Here, a private enterprise CA would be fine for auth, separate from email signing
What would be the impact on the IGTF RPs?

S/MIME vs. authentication certificates

The ‘legacy’ profile appears to be marginally OK still, the others forbid domainComponent

Here, a private enterprise CA would be fine for auth, separate from email signing

What would be the impact on the IGTF RPs?

7.1.4.2.5 Subject DN attributes for sponsor-validated profile

Attribute	Legacy (See Note 1)	Multipurpose (See Note 2)	Strict (See Note 2)
commonName	MAY	MAY	MAY
organizationName	SHALL	SHALL	SHALL
organizationalUnitName	MAY	MAY	MAY
organizationIdentifier	SHALL	SHALL	SHALL
givenName	MAY	MAY	MAY
surname	MAY	MAY	MAY
pseudonym	MAY	MAY	MAY
serialNumber	MAY	MAY	MAY
emailAddress	MAY	MAY	MAY
title	MAY	MAY	MAY
streetAddress	MAY	MAY	SHALL NOT
localityName	MAY	MAY	MAY
stateOrProvinceName	MAY	MAY	MAY
postalCode	MAY	MAY	SHALL NOT
countryName	MAY	MAY	MAY
Other	MAY	SHALL NOT	SHALL NOT

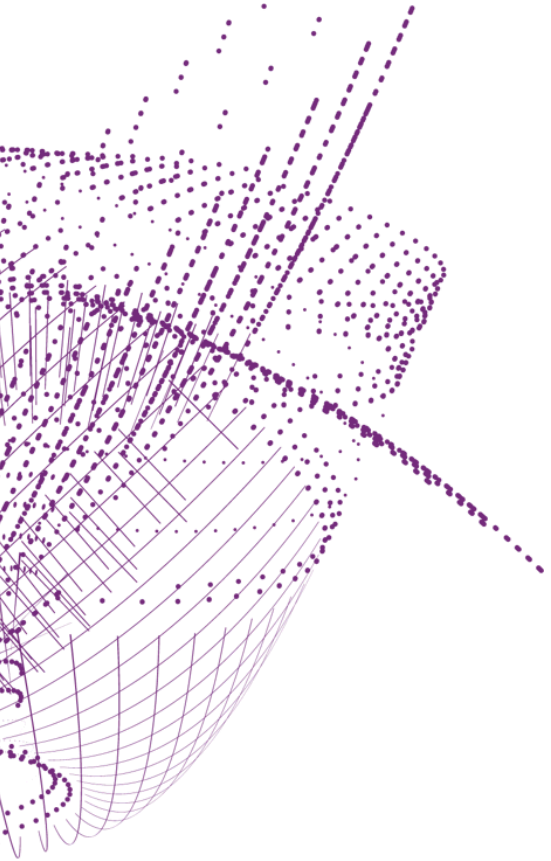
https://github.com/cabforum/smime/blob/preSBR/SBR.md

S/MIME vs. authentication certificates

Here, a private enterprise CA would be fine for auth, separate from email signing

What would be the impact on the IGTF RPs?

Can we add the supporting trust anchors (with minimal CP/CPS updates)
for TCS and InCommon on short notice?



Discussion

TLS BR, S/MIME BR, …

David Groep
davidg@nikhef.nl
https://www.nikhef.nl/~davidg/presentations/
https://orcid.org/0000-0003-1026-6606

Maastricht University

Nikhef