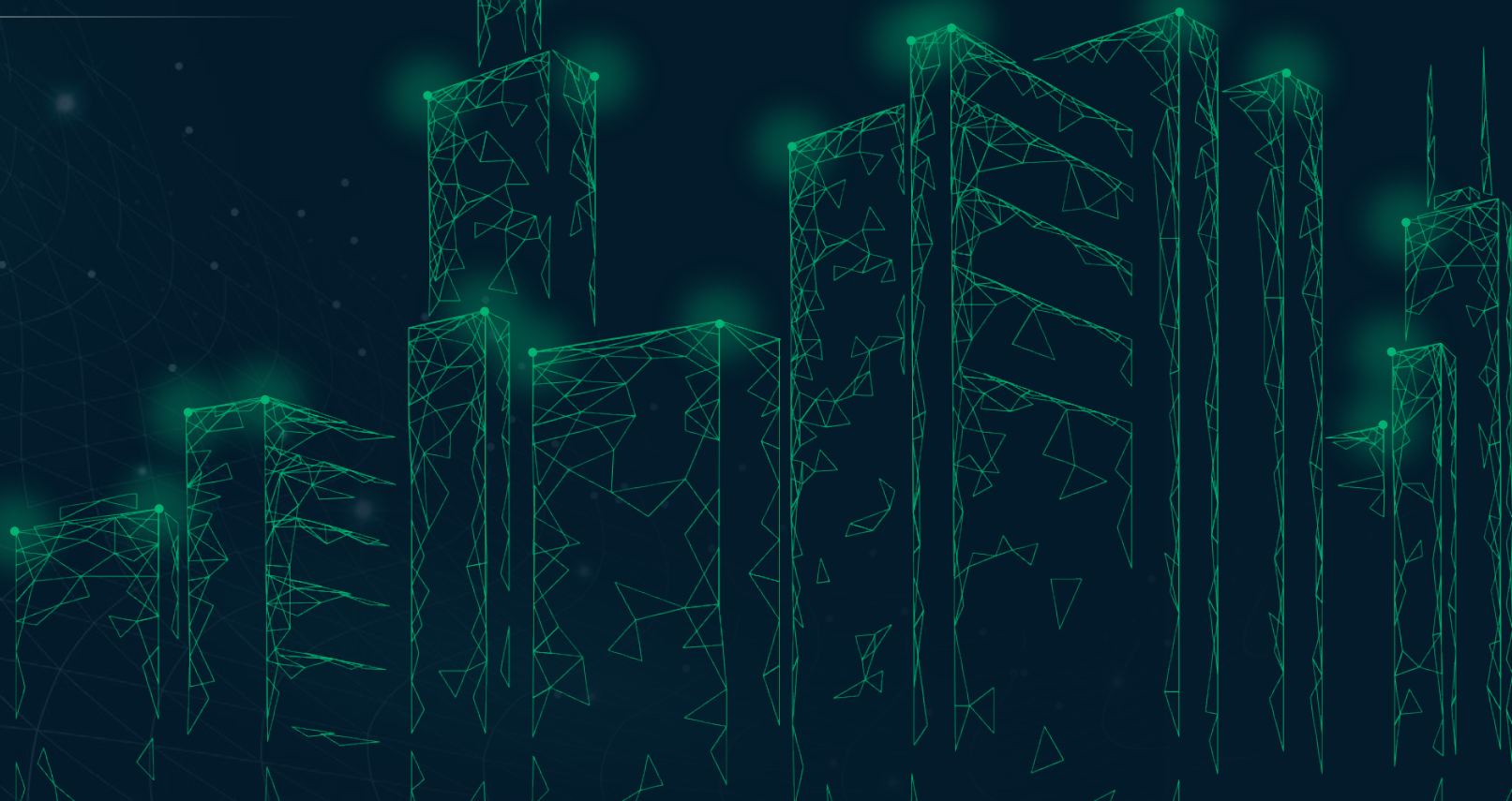
Better Alignment of Remedies with BR Violations

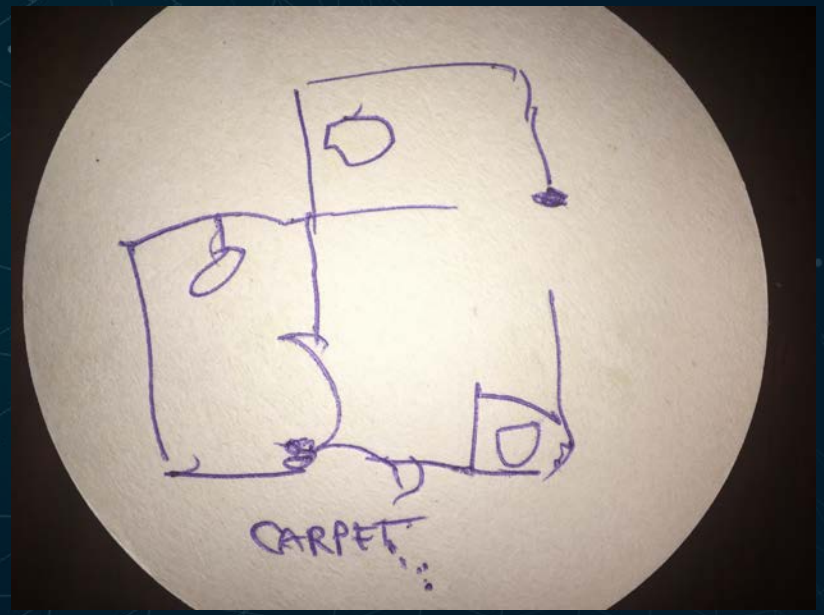
SECTIGO

September 2019

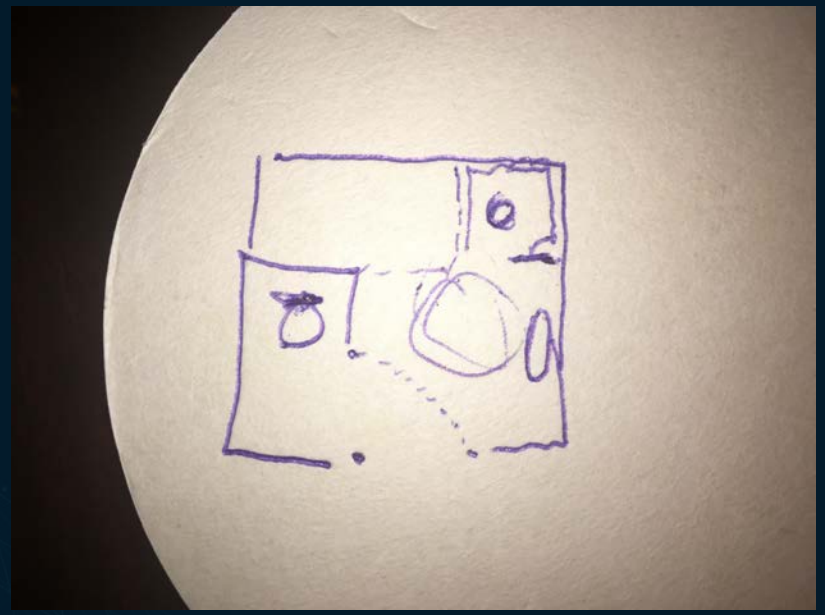


A discrepancy

1



2



https://pollev.com/timcallan192

We believe these statements to be true

- Subscribers are essential to our digital ecosystems. To the degree that the system fails subscribers, it lessens its ability to serve the needs of relying parties.
- We should seek to avoid unnecessary harm to subscribers.
- While we must have rules that can occasionally harm individual subscribers, harm that is disproportionately large compared to the trust benefit it brings can and should be eschewed.

We believe these statements to be true

- We should follow the rules we create for ourselves.
- When these rules fail our objectives for the ecosystem, we should change them until they meet those objectives.

The BRs contain broad language for when leaf certificate revocation is required

From Baseline Requirements 1.6.7 section 4.9.1.1

The CA SHOULD revoke a certificate within 24 hours and MUST revoke a Certificate within 5 days if one or more of the following occurs:

…

7. The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement;
8. The CA determines or is made aware that any of the information appearing in the Certificate is inaccurate;

This language prescribes the same remedy for any misalignment of certificate information, regardless of severity or risk

Forced revocation can have negative consequences

- Bad for subscribers
  - Potential outage or breach
  - Sudden reallocation of resources
  - Distraction
- Bad for relying parties
  - Potential outage or breach
  - Short or long term service quality
- Bad for CAs
  - Poor customer experience
  - Sudden reallocation of resources
  - Distraction

Our rules should not create forced revocation events that do more harm than good.

In 2019 we started to see a pattern of behavior

- Individual writes a script to search CT logs for some kind of mismatch between certificate details and BR requirements
- Individual mass reports all mismatches at one time
- CA and affected subscribers must scramble to respond within 5 days
- Even when there is no apparent fraud or security risk

We believe it is possible…

- To minimize the damage caused by forced revocations without meaningfully compromising security or identity
- To find improvements that a voting majority in this forum will support in an initial ballot
- To continuously improve over time with further scrutiny and new revelations

We proposed to distinguish two revocation time periods based on level of risk

Meaningful fraud or security risk exists

- Same as today

5 days

No meaningful fraud or security risk exists

- Codify error types that meet this criterion
- “White list”
- Can expand over time

30 days

Example candidates for 30-day revocation

- Simple misspellings of place names where the intended meaning is obvious
- Too-precise information in JOI fields
- Purely syntactic mistakes (e.g. 65 characters in an OU field)

Let’s put some errors to the test

Event:	NewYork instead of New York
Is security meaningfully weakened?	No
Is identity meaningfully weakened?	No
Revocation period:	30 days

Let’s put some errors to the test

Event:	State abbreviation substituted for state name
Is security meaningfully weakened?	No
Is identity meaningfully weakened?	No
Revocation period:	30 days

Let’s put some errors to the test

Event:	Autheticated, accurate local name included in JOI fields for Dutch certs
Is security meaningfully weakened?	No
Is identity meaningfully weakened?	No
Revocation period:	30 days

Let’s put some errors to the test

Event:	OU field contains 65 characters
Is security meaningfully weakened?	No
Is identity meaningfully weakened?	No
Revocation period:	30 days

Let’s put some errors to the test

Event:	Requester name in City field
Is security meaningfully weakened?	No
Is identity meaningfully weakened?	Yes
Revocation period:	5 days

Let’s put some errors to the test

Event:	2040 bit key
Is security meaningfully weakened?	Yes
Is identity meaningfully weakened?	No
Revocation period:	5 days

Let’s put some errors to the test

Event:	Serial number entropy falls below prescribed threshold
Is security meaningfully weakened?	Yes
Is identity meaningfully weakened?	No
Revocation period:	5 days

Anticipating some of the potential objections…

Objection: Just don’t issue certificates with errors

- That’s everyone’s goal
- That’s a lot like saying “Just don’t ship software with bugs”
- The BRs acknowledge that errors are a possibility
- Ambiguities still exist in the BRs and interpretations have shifted over time

Objection: Solve it through automation

- Automation goes a long way in minimizing one-off human errors
- Both CAs and subscribers have strong built-in motivations to automate these processes
- Delivery of roadmap items is not instant
  - Legacy systems can be complex
- Production systems contain unknowns
- Automated systems can produce errors as well

Objection: CAs are demotivated to revoke certificates

- Responses will have been prescribed in the BRs
- 30-day revocation events will those which the CABF as a body has deemed appropriate for that level of response

Objection: CAs won’t be motivated to improve

- Every CA views forced revocation as a bad outcome
  - Bad customer experience
  - Reputational damage
  - Taxing on the CA
- The deterrent effect remains

Objection: This proposal doesn’t handle unknown cases

- Yes, and that’s unfortunate
- However, it is still better than what we have today
- As we become aware of these cases we can add them in future ballots
- Let’s embrace improvement rather than being paralyzed by the idea of perfection