Spring 2022 CA/B Forum F2F

Validation Sub-committee Progress Report

digicert®

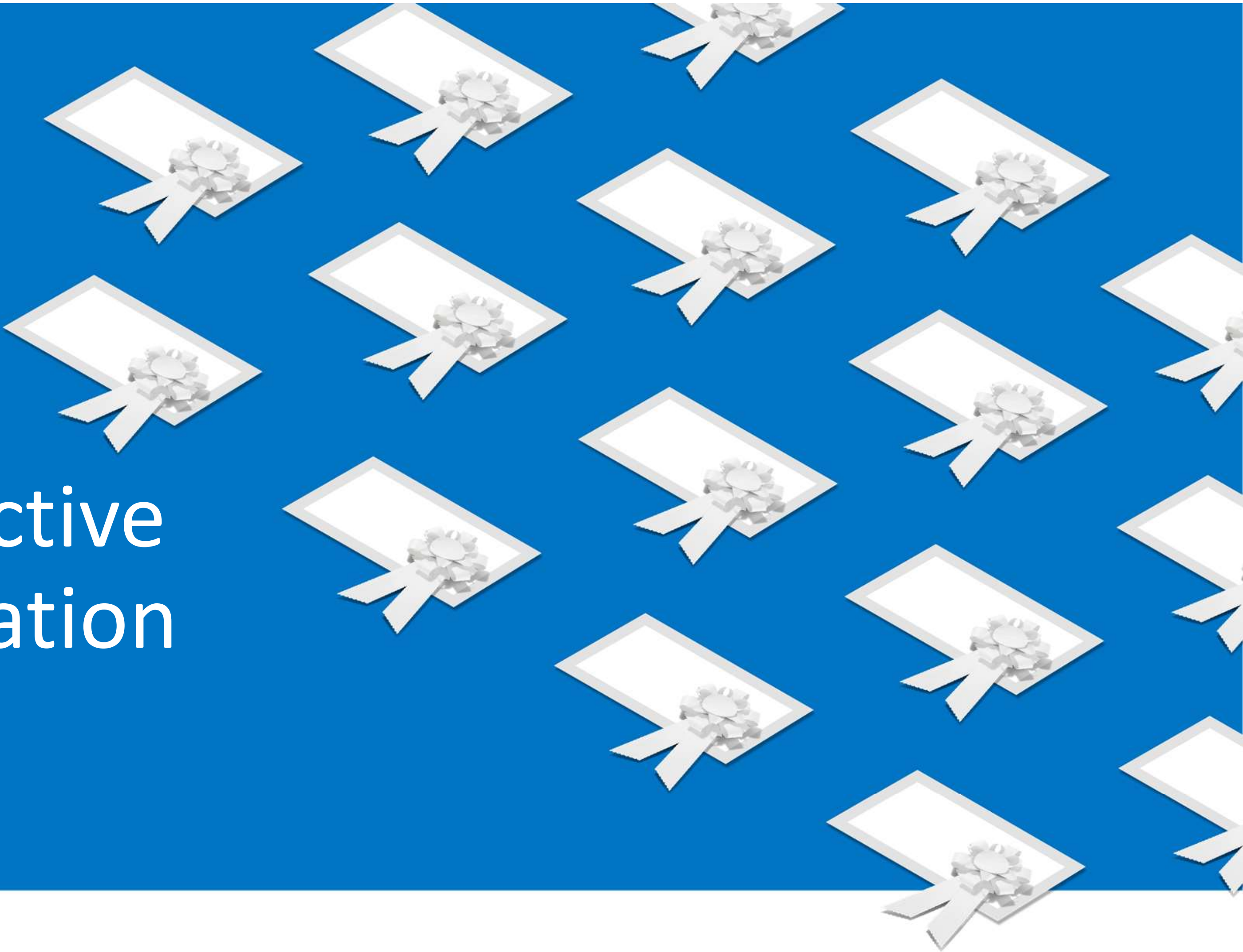
2021 in Review

Ballots

- SC 42: Limit reuse of IP address & domain name validations to 398 days
- SC 43: Clarify acceptable HTTP status codes for method 18 and 19 validations
- SC 45: Sunset use of method 18 and 19 for validation of subdomains and wildcards
- SC 46: Sunset the CAA DNS Operator exception
- SC 47: Sunset the OU subject attribute
- SC 48: Clarify IP address & domain name encoding in Certificates

Topics covered since Fall 2021 F2F

- Certificate profiles
- SC 52: CRL validity period clarification
- Delegating domain validation to a CA-controlled domain name
- Multi-perspective domain validation and RPKI
- Tor cleanup

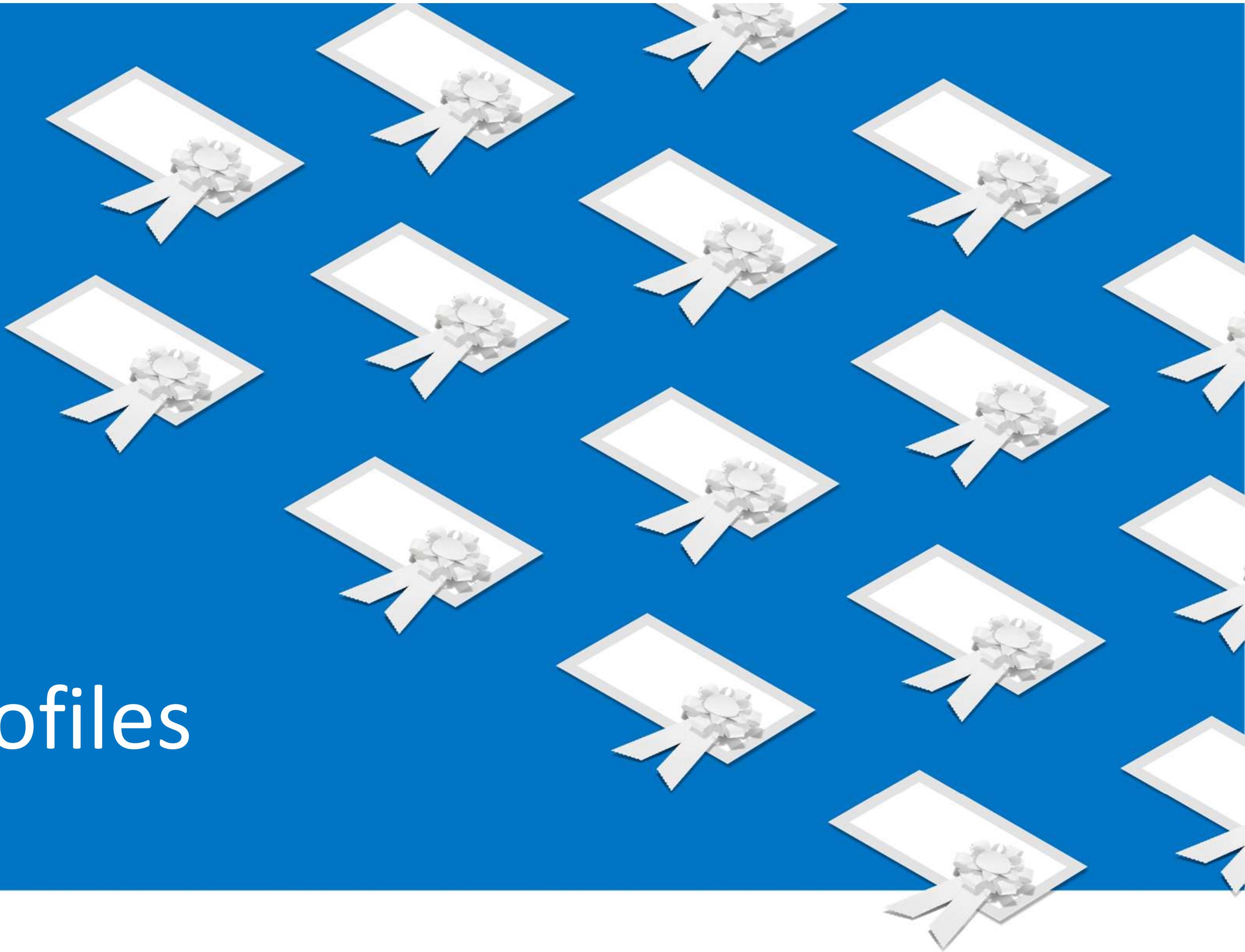


Multi-perspective domain validation and RPKI

digicert

Multi-perspective domain validation

- Princeton study in 2018 highlighted need to perform domain validation from multiple network vantage points to mitigate against BGP hijacks, etc.
- However, 2021 study from Fraunhofer Institute for Secure Information Technology explored downgrade attacks against multi-perspective domain validation
- Long term, RPKI may be the path forward, but still not ubiquitous
- Very recent events highlight critical importance of this area



Certificate Profiles

digicert®

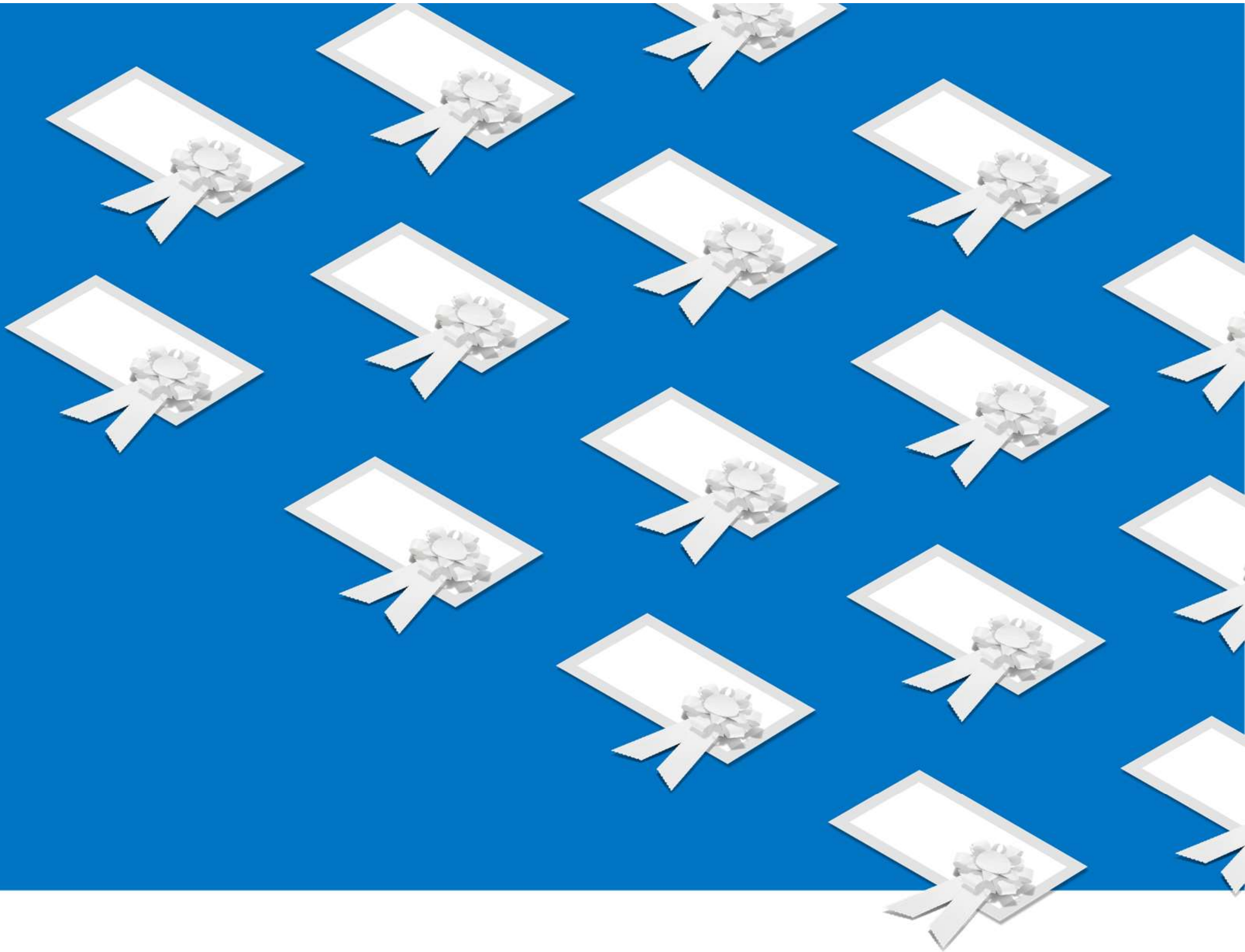
Certificate Profiles

- Consensus to minimize normative changes in initial draft
  - “First Policy OID is a CABF reserved OID” is now a SHOULD
  - Removed requirement for Cross Certificates to include EKU
- Agreed on approach for transition period between current profile and new profile
  - The ballot can allow for the previous version BR profile until the effective date of the new profile

A few open topics, including:

- Back-dating for Subscriber Certificates
- Non-TLS ICA profile (the topic of this meeting’s discussion)

Roadmap



digicert®

Roadmap for 2022

Immediate

- Finish up Certificate profiles v1 ballot

Short/mid term

- Multi-perspective domain validation and RPKI
- Explore validation methods that allow Applicants to passively demonstrate domain control

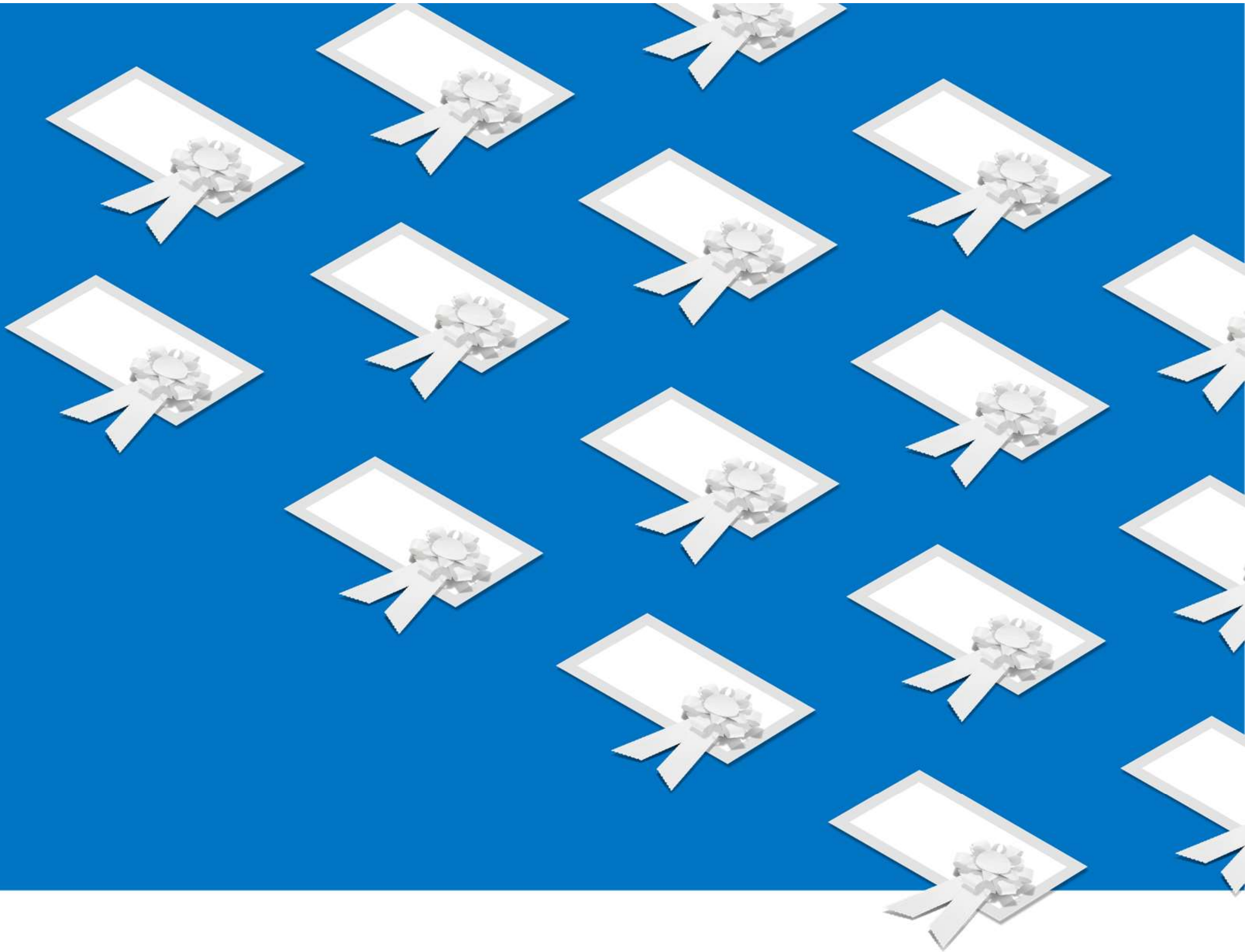
Housekeeping

- Move from Trello to GitHub project

Other items for consideration

- OCSP profile? (may be better addressed in servercert-wg)
- Unicode in subject DN attributes?

Questions?



Discussion topic: Non-TLS ICA profile