Network Security Subcommittee

F2F 51 - October 2020

Overall Strategy and Goals

Problem Statement and Objectives

1. NCSSRs are ambiguous at times.
This creates uncertainty as to whether a particular implementation meets the requirements and/or the expectations of browsers.

2. NCSSRs stand in the way of newer technology.
Updates are recommended **BUT** they have to take into account possible dependencies that impact the security posture of Certificate Systems.
NCSSRs must be technology neutral: it is not the job of the requirements to stipulate “approved” technology architectures.

Objective
Update the NCSSRs and/or introduce new Guideline documents for new technologies.

Problem Statement (continued)

- Example
  - CA wishes to use multi-aspect DNS lookup to address potential spoofing attacks (for zones not protected via DNSSEC)
  - CA can buy and operate hardware in multiple data centers and use quorum-based approach (all data centers in audit scope)
  - Could CA use a public cloud service (eg Lambda, Cloud Functions)?
    - Does cloud provider DC need to be audited to same standard?
    - If using multiple providers in quorum - does that reduce the threat of hostile provider spoofing results? Is that an effective control?
    - How is NCSSRs 2. (m)(n)(o) measured in a shared responsibility model?

Considerations for the NetSec Team

- Ensure that the language of the NCSSRs pertains to System Architectures and Deployments
  - Not practice requirements for certificate issuance (belongs in the BRs)
    - Example: Trusted Role description - BRs dictate that they must exist, but NCSSRs shouldn't be dictating what they are, only that sensitive operations are conducted under the authority of such roles
- Clarify terms which "everybody knows what they mean" (when we don't)
  - eg "System Accounts"
    - All accounts on a particular host ("system") ?
    - Or those accounts which are for pseudo-users running services on the "system"?
    - Application-level accounts, e.g. "users" in a webservice running on the "system"?

Practice Goals of the NetSec Team

- Reach out earlier
  - Where a ballot has got past primary drafting, reach out to the SCWG prior to a ballot being redlined and finalized, in order to solicit feedback and concerns
- Ensure that dependencies are explored in the discussion documents
  - Newer deployments should not weaken security properties that were in place
    - Unless those properties can be shown to be unnecessarily strict
- Still drive towards greater automation in monitoring and reporting
  - But recognize that the configuration of the automated system becomes a critical component, and is itself subject to periodic (human) review and reporting
  - CAs still need to be certain that all anomalies which would have been discovered by periodic human review will be discovered OR also conduct human reviews

Practice Goals of the NetSec Team (cont)

- Take a slightly more cynical view of the CA community
  - With each change, discuss
    - Does it open up any new behaviors that a bad actor might want to exploit?
    - Is it practical to close off such behaviors?
  - Recognize that utterly pathological misreadings of the BRs/NCSSRs cannot be prevented
    - Auditor role remains to determine whether a CA policy effects a substantive control or is syntactic adherence only

Subgroups/Teams

Document Structuring Team

- **“Zones” Ballot** - rewriting with a goal of strengthening requirements for logical and physical security while preserving distinction for CA systems to be appropriately protected (if we’re removing the “zones” concept, something needs to replace it)
- **Offline CA Ballot** - we will soon start a broader public discussion of ballot’s objectives
- Improve BR section 5 (e.g. physical security, trusted roles, etc.)
- Continue efforts to improve NCSSR document structure

Threat Modelling Team

- Our current work mostly is focused on discussing risks
  - Shared accounts problem (they are sometimes necessary but should be prohibited)
  - Identified 6 main requirements for Zones
  - Discussed CA Equipment risks
- The newest idea is to preparing “risk analysis” section which could be included in Ballots
  - The main goal is to show each time which risks will be mitigated/avoided thanks to new proposals

Pain Points Team Update

Authentication control rules outdated. **(Ballot SC3-Passwords and Ballot SC3X-Account Lockout)**

Increased scalability and effectiveness of log integrity controls, and system configuration reviews by reducing reliance on human element.

Extension to System Account Management being discussed **(Ballot SC34)**

Reduced excessive log data retention requirements from 7 to 2 years **(Ballot SC 28)**

Clarified the applicability of various NCSSR provisions to offline equipment - **(Offline CAs Ballot)**

Timing requirements for remediation of critical vulnerabilities. → not addressed. Draft Ballot was not provided. Assumed to be obsolete.

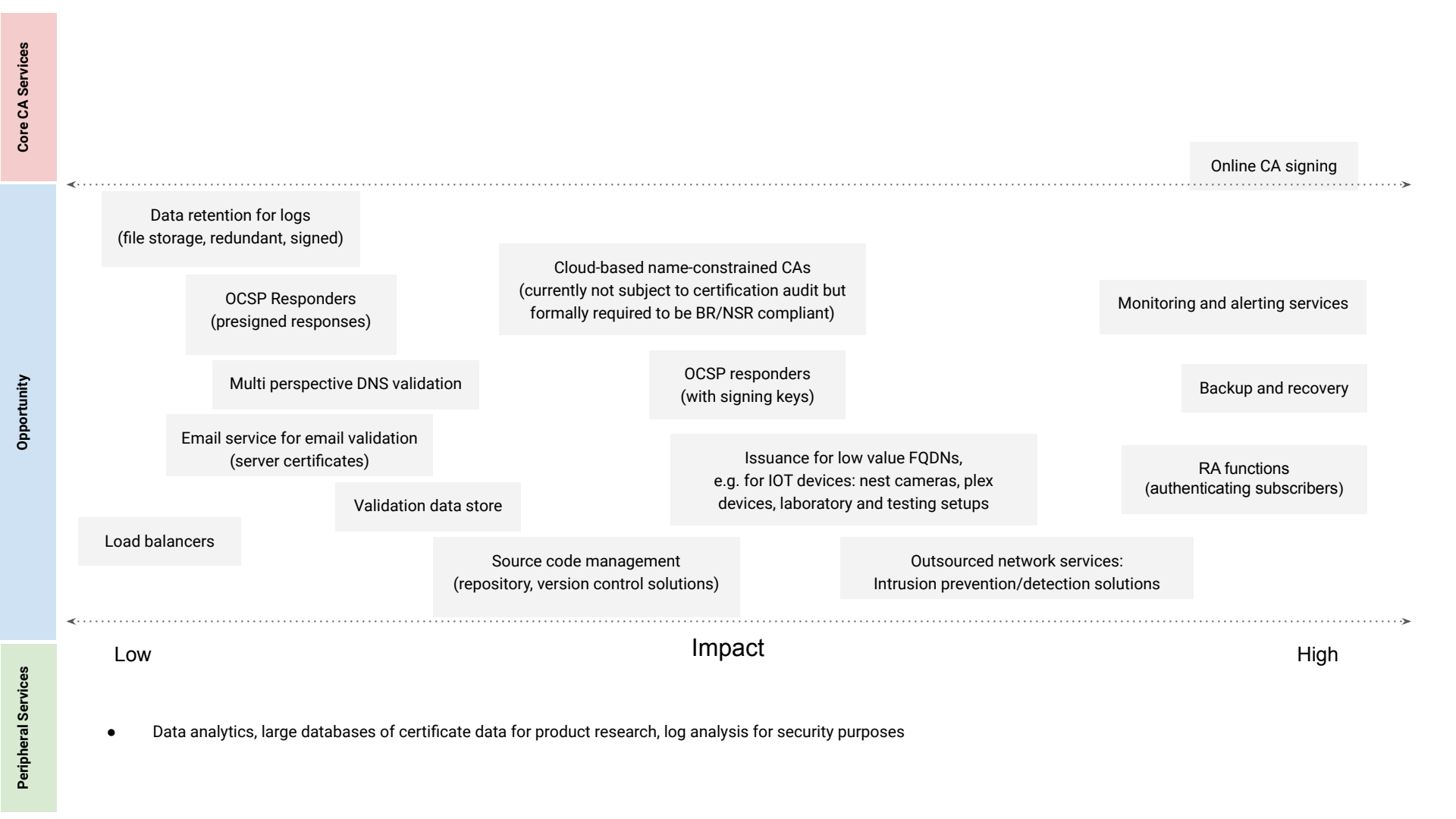
Ballots were prepared for all pain points. They are addressed to the extent possible.
Pain point subgroup meetings will be put on hold to focus on other topics. It may be resumed when required.

Using Cloud Service Providers

We will be forming a new sub group to focus on the use of cloud service providers by certificates authorities. Questions we are examining:

- What do the BRs allow today?
- Are there services CAs operate that are improved by taking advantage of cloud service providers?
- Are there CA functions that are risky/riskier in a non-on-premise environment and options for mitigating the risky sufficiently?
- How do we divide responsibilities and ensure that the responsible party is meeting the necessary requirements?

On the next slide is output from a brain storming exercise to identify functions that could leverage cloud services.



- Data analytics, large databases of certificate data for product research, log analysis for security purposes

Ballots

Ballot	Title	Status
SC28	Logging and Log Retention	Passed
SC32	Elimination of Zones	Abandoned - Redrafting
SCYY	Offline CA Provisions	Seeking broader discussion
SC34	Account Management	Redrafting

Thanks!

Mailing lists:

Main:
netsec@cabforum.org

Non-archived:
netsec-management@cabforum.org