NetSec WG
Cloud Services Subgroup

Update at the CA/B Forum F2F 57

October 2022

Background

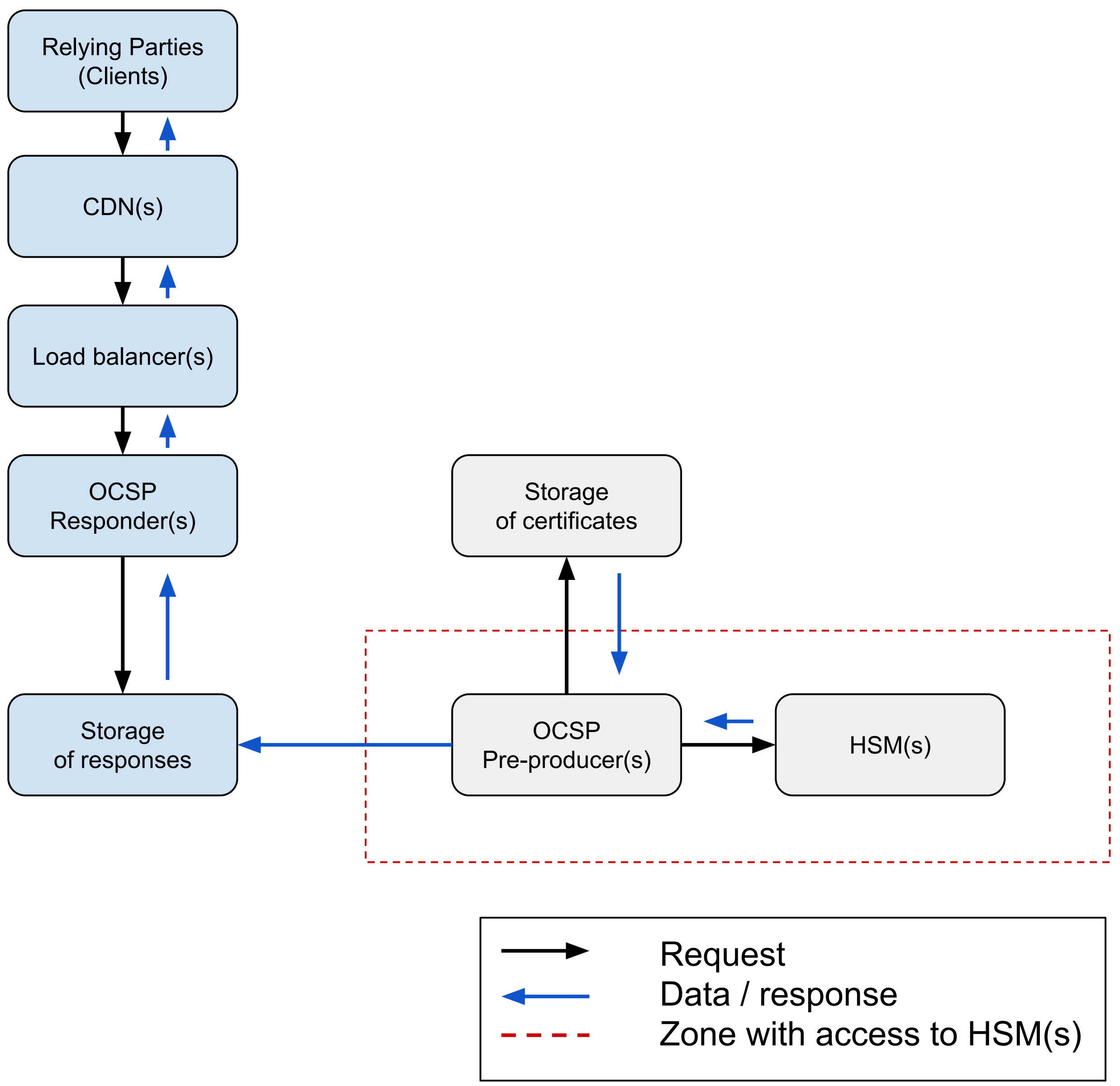
Objective

Within the NetSec WG's mission to improve the NSRs, the Cloud Services subgroup aims to clarify the rules for using cloud services in the CA infrastructure.

In 2022, the subgroup has developed a threat model to support this work and to inform the CA/B Forum's policy decisions.

Methodology

- Assessment based on a model CA architecture
- Design Narrative, Assets, Threats, Mitigations
- Threat assessment by category
- Component by component



Infrastructure components

- OCSP responder
- Certificate storage
- Registration Authority
- Online CAs and their HSMs
- Secure locations
- (offline CAs and HSMs)

Threats

- Spoofing
- Tampering
- Repudiation
- Denial of service
- Elevation of privileges
- Information disclosure

Findings

- Most threats to CA system infrastructure are also common in other high security environments. Our assessment has not identified PKI specific vulnerabilities.
- Summary of common mitigations
  - Individual access with secure authentication mechanisms
  - Full authentication
  - Data encryption
  - Logging + data integrity controls
  - Alerting on security violations (no reliance on “monitoring”)
  - Strong SDLC controls
- Existing security standards address the identified risks (ISO, SOC, PCI DSS and others).
- Due to the high blast radius of CA compromises, CAs must operate security controls on a low margin of error
- The NSRs address CA security threats to a limited extent. (c.f. DigiNotar beach analysis)
- The NSR stipulate only few SDLC controls and focus on vulnerability management in production. No criteria for secure development and acquisition of software.
- Security mitigation is not limited to the network and OS level. On the application level the business logic can be used for security purposes e.g. to detect tampering through data inconsistencies.

Outlook

- **Next Steps:**
  - Clean up the working document
  - Get broad feedback from Forum members and security researchers
  - Resume drafting work
  - For the initial assessment we focused on high level threats. Subsequent revisions should look closer at potential lower level vulnerabilities e.g. those due to faulty implementations.

Links and Reading Material

Links and Reading Material

- Threat modelling document
- Mapping of the NSRs against other common security standards