SHARED PUBLICLY

CA/Browser Forum
Threat Model for Publicly Trusted CAs

Document Status: work in progress

Version 0.1, last updated Nov 3, 2022

Document Purpose and Objective

The security of publicly trusted certificate authorities (CAs) is governed by a combination of browser root program policies, technical standards and other compliance requirements. Within the WebTrust framework of standards the Principles and Criteria for Certification Authorities require broadly that CAs identify and manage their security risks.[1] The CA/B Forum's Network and Certificate System Security Requirements (NSRs) supplement this principle by providing a specific set of security requirements.[2]

For the ongoing development of the NSRs and the effective application of the WebTrust principles, it is important to analyze and document the prevailing security threats that CAs face and have to protect against.

This document is a collection of common threats and vulnerabilities identified by the CA/B Forum NetSec Working Group based on a model CA architecture. It is open for contributions by CA/B Forum members and other organizations including standards organizations and security interest groups.

The threat assessment will be continuously revised as the threat landscape evolves and the prevailing CA architecture changes.

Contributors

Links and Related Materials

Greg Rubin, Introduction to threat modeling

NetSec Cloud Services Update at the CA/B Forum F2F 57

[1] Principle 3, Principles and Criteria for Certification Authorities
[2] https://cabforum.org/network-security-requirements/

Document Purpose and Objective 2

Contributors 2

Links and Related Materials 2

Registration Authority (RA) 5
- Design Narrative 5
- Assets 5
- Assumptions 5
- Threats 5
  - Spoofing 5
  - Tampering 5
  - Denial of Service 5
  - Elevation of privileges 6
  - Information Disclosure 6
- Mitigations 6

(Online) CAs and their HSMs 6
- Design Narrative 6
- Assets 7
- Assumptions 7
- Threat Identification 7
- Mitigations 8

Physical Security Practices 8
- Design narrative 8
- Assets 8
- Assumptions 8
- Threat Identification 8

Mitigations 8

Storage of Certificates 9
- Design Narrative 9
- Data flow diagram 10
- Assets 10
- Assumptions 10
- Threat Identification 10
- Mitigations 11

OCSP Responder 13
- Design Narrative 13
- Assets 13
- Data flow diagram 13
- Assumptions 15
- Threat Identification 15

Identify Mitigation/Remediation and Controls 18
Spoofing 18
Tampering 18
Repudiation 18
Information Disclosure 18
Denial of Service 18
Elevation of Privilege. 18
Drafting notes for the future 19

Scoping Statements 19

Mitigations 19
Identify Mitigation/Remediation and Controls 21
Spoofing 21
Tampering 21
Repudiation 21
Information Disclosure 21
Denial of Service 21
Elevation of Privilege. 22

Registration Authority (RA)

Design Narrative

The system or component that evaluates certificate signing requests and determines whether the requested certificate should be issued. The RA data is used by the signing CA.

RA systems and services can be implemented in many different ways. They can be located with more or less proximity to the CA and be integrated using different means.

Assets

Validation information (for record keeping)
Validation record which triggers certificate issuance (or not)

Assumptions

1. RA data (validation records) is stored separately from the singing CA
2. All calls to the RA are authenticated
3. The communication from and to the RA is encrypted
4. Changes are logged and the log includes data to identify what changed, when the change was made and who made the change
5. The RA backend systems are located in a secure physical location
6. All access to the RA front-end is authenticated using strong authentication
7. A vulnerability management process has been implemented. Patches that should be installed are installed in a timely manner.
8. Regular vulnerability assessments are performed on the front- and backends including data ingress points. This includes active tests including vulnerability scanning, architecture- and implementation reviews.
9. Changes to the RA systems are controlled through good change management practices.

Threats

Spoofing

Failed authentication could lead to an unauthorized system or service pretending to be the RA.
Unauthorized persons could use authentication failures to act as RA agents without authorization.

Tampering

The input data could be tampered with leading to incorrect issuance decisions.

Repudiation

Due to failures in the logging mechanisms log data is missing or incorrect.
Correct log data has been lost and cannot be restored or regenerated.

Denial of Service

CA is unable to process certificate requests.

RA data is unavailable for the processing of revocation requests.

Elevation of privileges

A failure in the logic of the RA service can lead to unintended issuance decisions where the CA issues certificates based on unauthorized requests.
Other root causes for the same outcome can be failures in the authentication mechanisms or the access management procedures.

Information Disclosure

Disclosure of PII and other confidential information in the certificate request and its associated validation data.
Disclosed authentication data could be leveraged to carry out a subsequent spoofing attack in the CA and cause unauthorized issuance.

Mitigations

Use robust authentication mechanisms and implement them effectively.
- Apply sound SDLC controls
- Apply multi factor authentication

Use separation of duties to limit the impact of compromised authentication factors

Data integrity controls
- Secure data models
- Transaction logging

Data reconciliations

(Online) CAs and their HSMs

Design Narrative

CA systems using intermediate CAs to sign certificates and certificate status information.
Signing CAs use HSM devices via direct connections or the network.
They use RA data or the RA assessment to determine if a certificate should be signed. Issuance logs and certificate data are stored on separate systems or services.
The signing CA produces issuance logs, certificate data and certificate status data.

or

The hardware security module that protects the intermediate CA keys and the software/hardware layer that connects to the HSM to enable use of the keys. This system will produce logs, these logs are stored on a separate system. The CA will have other software such as an issuance system that will request signing from this system or revocation infrastructure that will request signing of certificate revocation status data. The software/hardware layer around the HSM will interact with other systems via direct connections or the network.

The HSM protects signing keys and performs signing operations as instructed by the signing CA. It logs signing operations and other relevant events and can report on its status and integrity.

Assets

Signing keys

Assumptions

1. RA data (validation records) are stored on separate systems
2. All calls to the CA are authenticated.
3. Communication from and to the CA is encrypted
4. Changes are logged and the log includes data to identify what changed, when the change was made and who made the change
5. The CA systems are located in a secure physical location
6. A vulnerability management process has been implemented. Patches that should be installed are installed in a timely manner.

7. The HSM is a physical device (could be a PCI card).
8. HSM conforms to the technical specifications stipulated in the Baseline Requirements (FIPS).
9. Device manufacturer instructions are followed when setting up and operating the device.
10. Device integrity was intact when it was shipped and installed.

Threat Identification

Spoofing
CA: RA, log service, data store, HSM
The impact of a successful spoofing attack on the signing CA or the HSM would be more severe than on most other CA infrastructure components. The RA is a more accessible service, has more users and could therefore be a preferred starting point for a spoofing attack. Similarly the HSM could be spoofed from the CA. Successfully spoofing the CA can lead to incorrect data in logs, data store etc.

Tampering
Insertion of malicious code on the CA
Unauthorized modification of the device firmware

Repudiation
The signing operation cannot be attributed correctly to the CA or an unauthorized actor.

Denial of Service
CA is unable to produce revocation data

Elevation of privileges
Granting the ability to perform unauthorized signing
E.g. by Reconfiguring the HSM to accept signing commands from machines that are not the CA

Information Disclosure
Signing keys extracted from HSM

Mitigations

Physical Security Practices

Design narrative

The physical location where HSMs for online CAs are kept.

Assets

Key material on the HSMs

Assumptions

None

Threat Identification

Spoofing
Unauthorized person enters the space by using someone else's access factors (badges etc.)

Tampering
Devices plugged into HSM to perform unauthorized actions.

Repudiation
Authorized access is used to perform unauthorized actions and cannot be proven or investigated because it was not appropriately logged or alerted.

Denial of Service
Locked out of the secure space

Elevation of privileges
Someone is able to grant themselves access to the secure space
or modify access in an unauthorized manner e.g. disable the two person rule enforcement in the access system or grant access to an unauthorized individual

Information Disclosure
The HSM or key material is removed from the secure location without authorization.

Mitigations

Walls are solid and meet a reasonable security standard
Doors are locked
Two factors

Individual access and access logs
two person rule
Proper logging and alerting
Alarms for forced entry attempts
Cameras and video retention

Storage of Certificates

Design Narrative

Systems where the CA records what certificates it has generated and signed using its online CAs. The Storage of Certificates is part of the online CA infrastructure.

They store:

- certificate serial number
- Certificate type (OV/DV)
- BR Validation method
- Validation result
- Certificate status

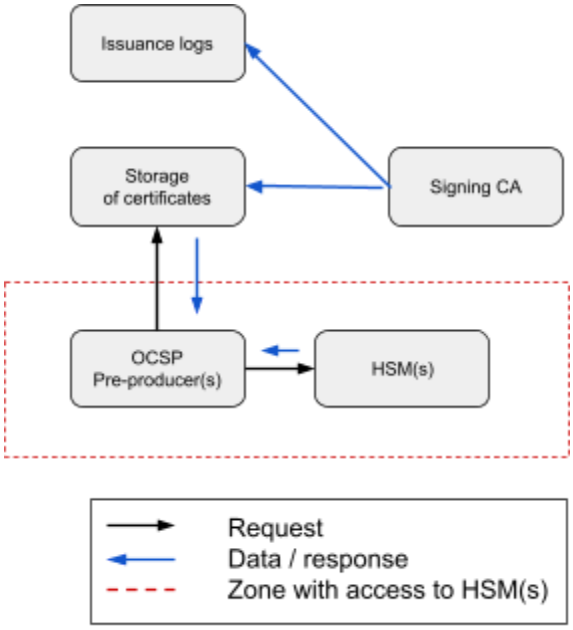
In the same or a separate (RA) system:

- Certificate request details (CSR)
- subscriber information (contact information, email address)
- certificate serial number

The certificate storage contains data that is required by the CA to process a request and the result of the issuance operation. It is the source of information from which the CA generates certificate status information (CRLs and OCSP). It is also consulted to determine who may request certificate revocation i.e. who the subscriber is in relation to a certificate.

The Baseline requirements stipulate that the CA has to keep records of the validation method applied for each certificate request. This (and other) information can be stored in the certificate storage or the issuance logs or both.

Data flow diagram



Assets

- The data

Assumptions

1. All calls to the datastore are authenticated
2. Access is limited to authorized resources that have a valid business reason to connect to it
3. Communication from and to the data store is “properly” TLS encrypted
4. Changes are logged and the log includes data to identify what changed, when the change was made and who made the change
5. The system is located in a secure physical location
6. A vulnerability management process has been implemented. Patches that should be installed are installed in a timely manner.
7. Network boundary controls (physical or logical) are present and the CA restricts network traffic to approved connections.
8. ~~(integrity controls e.g hashing that makes the data tamper evident)~~

Threat Identification

Spoofing

1. An attacker could present itself as an authorized accessor to the datastore allowing them to insert false information. The attacker presents itself as an authenticated user because the authentication mechanism was ineffective.
    a. Attacker could actually have the credentials

   b. Attacker takes over an authenticated client and can exploit existing sessions and/or credentials
   c. Design flaw in the authentication mechanisms
   d. System vulnerability that allows attacker to circumvent the authentication steps

2. An attacker could present themselves as the datastore allowing them to prevent information from being recorded, or queried, or to respond with false information.
   a. Attacker successfully assumes the network identity of the actual datastore.
   b. Attacker get around TLS
   c. Attacker managed to follow the communication protocol conventions that client expects

Tampering

1. An attacker could introduce certificate entries into the data store that were not generated by the CA and thereby cover up mis-issuance that was caused outside the regular issuance workflow. As a consequence the CA would generate status information for the mis-issued certificate, making its existence less obvious.
2. Manipulate validation data to cause the issuance of a requested certificate when the actual validation procedures have not been completed. (successfully)
3. Validation data and status information is deleted making it impossible to account for the validation decisions that have been made.
4. Revoked certificates could be unrevoked.

Repudiation

1. Inability to do reliable identity correlation
2. Tampering cannot be traced back to an actor
3. Validation data is not always tied back to the correct entity

Information Disclosure

- Most certificate and validation information for DV TLS certificates is public information
- Validation information for OV, EV and CS certificates e.g. company records can contain PII and confidential information.
- Disclosure of credentials, authentication information

Mitigations

Spoofing Remediations

1.
a)

- Proper credential management.
- Observing the principle of least privilege
  - Separate accounts for administrative functions, access on demand, …
- Alerting (on the use of credentials)

b)

- Session timeouts
- Replay prevention (as a matter of software or protocol design or added on)

- System hardening including on the client side
- Encrypt connections

c) and d)

- Proper SDLC controls
    - Secure coding
    - Secure systems acquisition processes for commercial off the shelf solutions
    - vulnerability management and patching
- Design and security reviews, penetration tests

2.
a)

- Monitoring DNS records to prevent DNS hijacking
- Use TLS

b)

- Use the most recent version of TLS or an alternative secure method of encryption

Tampering Remediations

1. Reconcile certificate data with issuance logs
2. See above
3. General access controls. Alerting when data is deleted. Rollbacks and restores.
4. See above.

Repudiation Remediations

1. Logging and log data analysis e.g. reviews, alerts
2. See above
3. Data management controls: reconciliations, data checks against business logic of the application

Information Disclosure Remediations
(is the reverse of non-repudiation)

OCSP Responder

Design Narrative

Responding to OCSP requests is an infrastructure component that serves OCSP responses to relying parties. The issuing CA queries certificate status information (e.g. a database) to determine which certificates are valid or have been revoked. It generates OCSP responses for all valid and revoked certificates (and precertificates) and submits them for delivery in response to OCSP requests. A new response is generated before the old one expires.

Pre-produced OCSP responses:

- OCSP response generated before (or without) OCSP request is made, with a CA key*
- Preproduced OCSP response uploaded to a scalable distribution platform (e.g. Content Distribution Network (CDN)

Not a delegated responder

* To simplify the risk model, we assume here that a delegated OCSP responder is not providing OCSP responses “on the fly”.

Assumptions:

- the OCSP responder potentially provides OCSP responses for TLS, S/MIME, and Code Signing certificates (as defined by the CA/B Forum for those respective certificate types)
- the generation and distribution of responses to the storage and OCSP server are not in scope of this model
- the server responding with OCSP responses is secure
- the receipt from OCSP pre-producers is secure
- the storage of responses is secure
- the keys used to sign OCSP responses are securely protected in an HSM
- the storage contains a signed OCSP response for each certificate that requires a response with the correct status of the respective certificate
- the OCSP responder is compliant with the relevant RFCs (typically either 5019 or 6960) and standards
- the responses are not expired
- systems and zones are protected by a firewall
    - only required/known traffic can flow in the directions it needs to flow
- OCSP responder logs are not stored on the OCSP responder

Assets

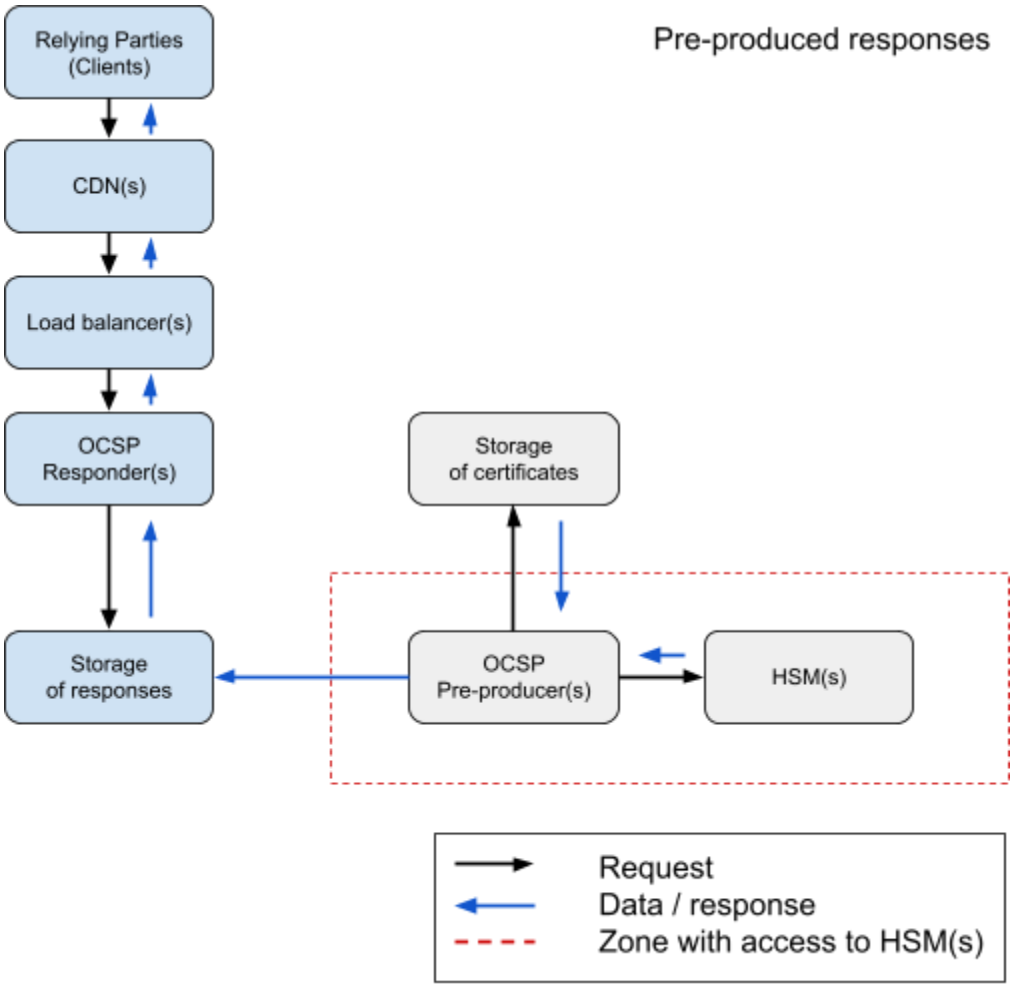
- OCSP responses

Data flow diagram

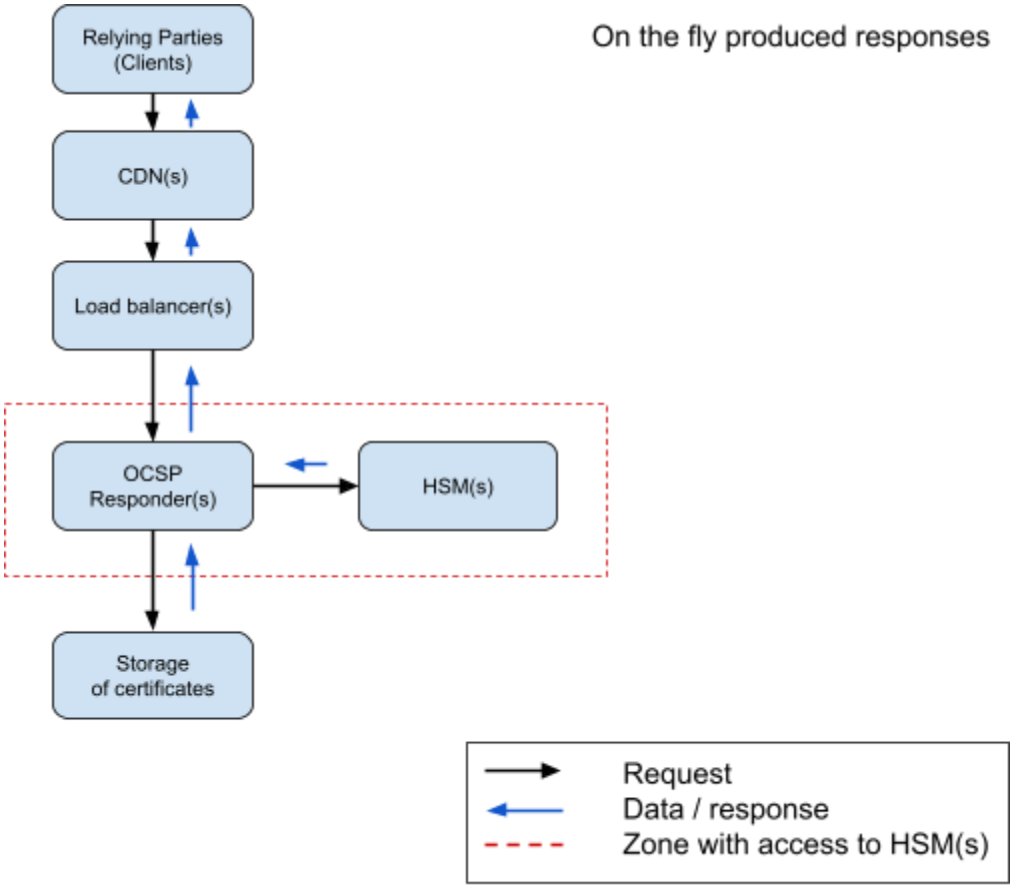
Relying party (client)
CDN

Load Balancers
Responders (http service)
Certificate status data store

Todo: Specify what the arrows mean (data flow or call)
Recommendation: Call out the specific data that is flowing in the diagram to make sure we account for potential different data handling needs. Example: callouts for log data.



Pre-producer (see RFC 5019)
Key storage
Something that uses the keys to sign responses, like a host
Relying Party's Client
Something that informs the configuration of your responder service. Such as what the response types are.



Reference diagrams to help visualize. They do not reflect the design / narrative:

Assumptions

The OCSP Responder operates in a network environment with basic boundary protections such as firewalls.
Traffic is authenticated and encrypted

Threat Identification

Identify and describe the threats. Give industry-standard definition, then provide example(s) of the threat.
TODO: Identify source of definitions (NIST or Threat Modeling Book or https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSDN)
TODO: Build out narrative descriptions of each threat

Spoofing

Threat Definition **:** Pretending to be something or someone other than yourself.

Property Violated: Authentication.

Spoofing is the act of disguising a communication from an unknown source as being from a known, trusted source.
i.e. a response is introduced that was not actually generated by the CA

Assessment:
The responder is not vulnerable to spoofing attacks because for the response to be accepted as valid, the response must be signed by the CA's signing key to which external parties don't have access.
The client validates the signature on the response. The protocol specification prevents MITM attacks where another CA signs a malicious OCSP response.

Since OCSP requests don't have to be signed (and typically are not), these could be spoofed.

Response: ID (cert serial), status, updates
OCSP and CRL requests are not made over TLS to avoid loops

Tampering

Threat Definition **:** Modifying something on disk, on a network, or in memory

Property Violated: Integrity.

Tampering may include a party with access to the OCSP Responder disrupting or corrupting the data of an OCSP response such that it cannot be validated by the client.
Tampering may include parties with access to systems supporting the OCSP Responder, modifying system components such as firewall configuration, access control lists, network identification and allocation, etc. This threat may be best addressed in a separate threat model.

Assessment:
Tampering can lead to various failure scenarios which can eventually lead to unavailability. These will however not change the certificate status e.g. from revoked to good.
Mitigations must be appropriate to ensure service availability sufficient to meet revocation timeline requirements (< 24h pursuant to BR, maybe less pursuant to CA's disclosed SLOs).

Repudiation

Threat Definition **:** Claiming that you didn't do something or were not responsible. Repudiation can be honest or false, and the key question for system designers is, what evidence do you have ?

Property Violated: non-repudiation

E.g. OCSP responder rejecting valid requests
E.g. due to tampering, OCSP responder is configured to not respond to specific requests. No log files, no proof of attack, no evidence left behind.

Assessment:
On the client side, this scenario would lead to the same outcome as an outage. See assessment above.

Information Disclosure

Threat Definition **:** Providing information to someone not authorized to see it.

Property Violated:Confidentiality

E.g. unintentional disclosure of private key due to insufficient protections or incorrect configuration of private key storage.

Assessment:
Extraction of private keys is out of scope for the scope of this assessment because the private keys do not reside on the OCSP responder.

If the OCSP responder holds credentials for reading data from the storage, their disclosure could pose a risk for the storage if they enable an attacker to establish unauthorized or unintended connections.

We assume that such credentials do not facilitate write access because the business logic of the OCSP responder is such that it does not have to push information back to the storage.

OCSP log data can contain PII and its disclosure is a privacy risk. Data privacy is currently not the focus of the BR and the NSR and other compliance frameworks impose privacy requirements on CAs e.g. privacy legislation, PCI DSS, ISO 27000, SOC etc.
Long retention periods for log data increase the risk. The BR should be clear about the scope of logging requirements for OCSP data and not require their retention for longer than necessary especially for troubleshooting.
Section 3(f) NSR currently stipulates that CAs shall “monitor the archival and retention of logs to ensure that logs are retained for the appropriate amount of time in accordance with the disclosed business practices and applicable legislation.”

Propose a ballot to change Section 5.4.3 BR adding a statement along the lines of:
“The retention requirements in this Section do not apply to logs containing queries from relying parties to certificate status services because their retention can cause unnecessary privacy risks.”

Denial of Service

Threat Definition**:** Absorbing resources needed to provide service.

Property Violated: Availability

Primarily at the CDN/edge, nonsense requests, etc.

Assessment:
All online services are in principle susceptible to denial of service attacks. The effect of such an attack on the OCSP service would be increased latency or that it becomes temporarily unavailable.

General consideration: If the revocation services have high latencies and/or periods of unavailability, this could lead to undesired design decisions for user agents. Software providers could design their products to fail open after a certain period or a number of unsuccessful attempts. That is an undesirable outcome for the overall PKI ecosystem.

Elevation of Privilege

Threat Definition: Allowing someone to do something they are not authorized to do.

Property Violated: Authorization

Someone gaining access to system internals and elevating their access, remediation likely includes ensuring blast radius is limited for admin privileges.

Assessment:
If the compromised privileges are limited to the OCSP responder, their elevation could at worst create an outage, which is the same scenario as the ones assessed above.
More problematic would be designs where the OCSP responder is integrated into the CA architecture beyond the degree necessary for its base functionality, for example by sharing access control or configuration management systems or other additional, possibly sensitive systems. If these reside in the same authentication domain, an elevation of privileges on the OCSP responder could grant access on more sensitive parts of the CA such as the storage or the signing infrastructure.

Identify Mitigation/Remediation and Controls

Consider different types of controls:

- *Prevention*
- *Detection*
- *Remediation*

Spoofing

- None.

Tampering

- Implement OCSP monitoring to alert on the status of the service
- Business continuity plan allowing the CA to rebuild the responder infrastructure within less than 24h or any SLO the CA has committed to.
- Note: The BR stipulate in Section 4.9.10 that "The CA SHOULD monitor the OCSP responder for requests for “unused” serial numbers as part of its security response procedures." This requirement aims to identify OCSP requests for certificates that have been issued but not logged in the certificate database (misissuance). It mitigates an impact that occurred on the signing infrastructure.

Repudiation

- OCSP monitoring shall detect if valid requests are rejected
- Logging is enabled and integrity of the log files is maintained

Information Disclosure

- Firewalls
- Process for rotating the OCSP responder credentials

Denial of Service

- Distribution of responses

Elevation of Privilege.

-

Drafting notes for the future

Response 1: Status:good, valid 5d
Response 2: Status:revoked, after day 2

Links and References
https://certificate.revocationcheck.com/

- CA SHALL establish a set of system parameters and other metrics to identify security events and incidents. These shall include at a minimum:
    - patterns of OCSP requests for unused certificate serial numbers
    - <work on this list>

Scoping Statements

- the OCSP responder potentially provides OCSP responses for TLS, S/MIME, and Code Signing certificates (as defined by the CA/B Forum for those respective certificate types)
- the generation and distribution of responses to the storage and OCSP server are not in scope of this model
- ~~the server responding with OCSP responses is secure~~
- ~~the receipt from OCSP pre-producers is secure~~
- ~~the storage of responses is secure~~
- the keys used to sign OCSP responses are securely protected in an HSM
- the storage contains a signed OCSP response for each certificate that requires a response with the correct status of the respective certificate
- the OCSP responder is compliant with the relevant RFCs (typically either 5019 or 6960) and standards
- the responses are not expired
- systems and zones are protected by a firewall
    - only required/known traffic can flow in the directions it needs to flow

Mitigations

Spoofing

Monitoring for unknown requests and alerting on large amounts of unusual requests.

Goals:
- capacity management
- detecting misissuance (is is not a threat to the OCSP responder itself)

Tampering

Prevent:
- Access controls. Only mitigates against threats that do not originate from an authenticated user.

Detect:
- Logging
- System state monitoring

Respond:

- Disaster recovery. Ability to rebuild the system quickly.

Repudiation

Threat Definition **:** Claiming that you didn't do something or were not responsible. Repudiation can be honest or false, and the key question for system designers is, what evidence do you have ?

Property Violated: non-repudiation

E.g. OCSP responder rejecting valid requests
E.g. due to tampering, OCSP responder is configured to not respond to specific requests. No log files, no proof of attack, no evidence left behind.

Assessment:
On the client side, this scenario would lead to the same outcome as an outage. See assessment above.

Information Disclosure

Threat Definition **:** Providing information to someone not authorized to see it.

Property Violated:Confidentiality

E.g. unintentional disclosure of private key due to insufficient protections or incorrect configuration of private key storage.

Assessment:
Extraction of private keys is out of scope for the scope of this assessment because the private keys do not reside on the OCSP responder.

If the OCSP responder holds credentials for reading data from the storage, their disclosure could pose a risk for the storage if they enable an attacker to establish unauthorized or unintended connections.

We assume that such credentials do not facilitate write access because the business logic of the OCSP responder is such that it does not have to push information back to the storage.

Denial of Service

Threat Definition**:** Absorbing resources needed to provide service.

Property Violated: Availability

Primarily at the CDN/edge, nonsense requests, etc.

Assessment:
All online services are in principle susceptible to denial of service attacks. The effect of such an attack on the OCSP service would be increased latency or that it becomes temporarily unavailable.

General consideration: If the revocation services have high latencies and/or periods of unavailability, this could lead to undesired design decisions for user agents. Software providers could design their products to fail open after a certain period or a number of unsuccessful attempts. That is an undesirable outcome for the overall PKI ecosystem.

Elevation of Privilege

Threat Definition: Allowing someone to do something they are not authorized to do.

Property Violated: Authorization

Someone gaining access to system internals and elevating their access, remediation likely includes ensuring blast radius is limited for admin privileges.

Assessment:
If the compromised privileges are limited to the OCSP responder, their elevation could at worst create an outage, which is the same scenario as the ones assessed above.
More problematic would be designs where the OCSP responder is integrated into the CA architecture beyond the degree necessary for its base functionality, for example by sharing access control or configuration management systems or other additional, possibly sensitive systems. If these reside in the same authentication domain, an elevation of privileges on the OCSP responder could grant access on more sensitive parts of the CA such as the storage or the signing infrastructure.

Identify Mitigation/Remediation and Controls

Consider different types of controls:

- *Prevention*
- *Detection*
- *Remediation*

Spoofing

- None.

Tampering

- Implement OCSP monitoring to alert on the status of the service
- Business continuity plan allowing the CA to rebuild the responder infrastructure within less than 24h or any SLO the CA has committed to.
- Note: The BR stipulate in Section 4.9.10 that "The CA SHOULD monitor the OCSP responder for requests for “unused” serial numbers as part of its security response procedures." This requirement aims to identify OCSP requests for certificates that have been issued but not logged in the certificate database (misissuance). It mitigates an impact that occurred on the signing infrastructure.

Repudiation

- OCSP monitoring shall detect if valid requests are rejected
- Logging is enabled and integrity of the log files is maintained

Information Disclosure

- Firewalls
- Process for rotating the OCSP responder credentials

Denial of Service

- Distribution of responses

Elevation of Privilege.

-