OCSP AND CRL PROXY SIGNER

INVENTOR:

MASSIMILIANO PALA

Attorney Docket No: 61879PROV

UNITED STATES PATENT APPLICATION

For

OCSP AND CRL PROXY SIGNER

INVENTOR:

MASSIMILIANO PALA

Description

In this invention, the CRL and OCSP Proxy uses a special certificate that allows it to provide CRLs and OCSP responses for any (or well-identified) PKIS. The produced responses can override the revocation status from the original CA for NetOps purposes (e.g., OCSP not reachable, Ignore of Revocation Status, etc.) - See Attachments (IMG..59 -> IMG..63)

Background

Revocation checking is being built into our networks and we need to provide a mechanism for operators to be able to manage the revocation status independently from the indications from the Certification Authority. This solves many operational uncertainty when it comes to revocation status validation (e.g., number of trust anchors needed on devices, different services offered a different CAs, centrally managing mixed environments).
By adding the possibility of centrally validate the original revocation information, this invention provides a way to mitigate the impact of revocation on live systems and its handling according to the specific needs of the environment where this revocation status is leveraged.

Abstract

This invention provides a mechanism for a full revocation information proxy system that allows deployment administrators to mitigate the impact of revocation (when and if needed) in specific ecosystems/environments. Moreover, this invention can be used in test environments to validate the handling of identities in different statuses - for example, the proxy can be configured to report one, multiple, or all certificates to be revoked to test if a system can correctly process that information (even if the original PKI has not revoked the certificate).

PATENT IDEA

Oct 19, 2021

Massimiliano Pala

OCSP Proxy (Also CRL Proxy - same idea)

→ Today OCSP must be signed by the issuing CA or by an OCSP responder that is issued by the same CA.

→ This invention adds a new option, which is the OCSP Proxy certificate.

The OCSP Proxy certificate must have:

→ The OCSP Proxy OID (i.e. a new OID we define for this) inside the EKU extension

→ (optionally) A new entry in the Subject Alternative Name with

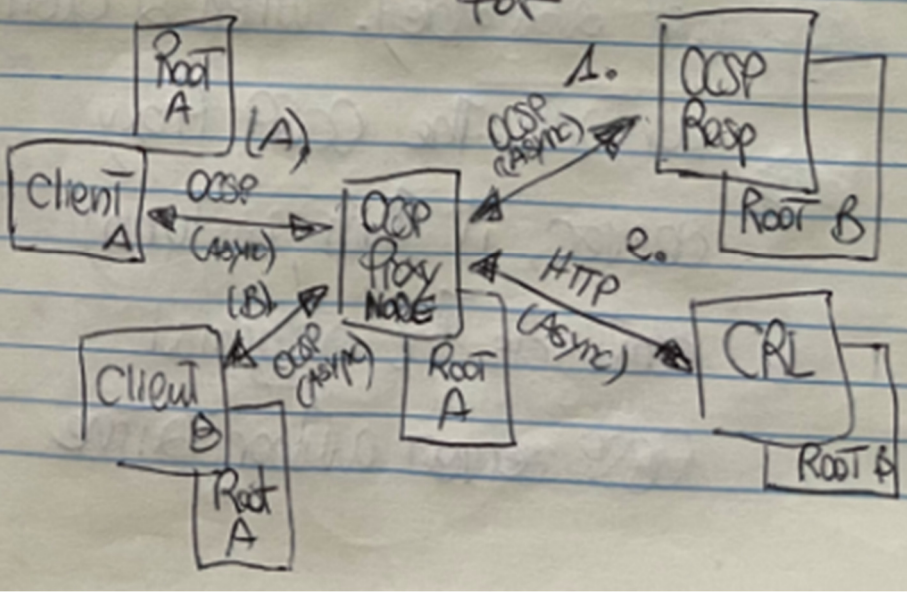
a new access method that indicates the for which the CAs the OCSP responds for.

Multiple entries are possible.

For Example, in a certificate the san can be defined as:

id-ad-ocsp-proxy ::=
certificateIdentifier

As defined in OCSP requests/responses to identify the CA this OCSP can respond for



There are Two main processes. The first one is the one that repeatedly queries the source of revocation information and, if successfully verified, proceeds to update the internal DB as needed.

NOTE: The system can be also implemented synchronously when needed (e.g. CRLs are not available). When a client contacts the OCSP Proxy server, it then, in turn, contacts the original OCSP server authoritative

for the queried certificate and, after validating the response, builds its own response based on the validated information.

- Optionally, the OCSP Proxy can update its internal DB and use it for caching subsequent requests (as indicated by the original response validity times)

The second process is the normal OCSP services to the OCSP clients. In this process, the server side works as a normal OCSP server (no changes there), while on the client side, ~~the client acts as a responder~~ the during the certificate validation of the OCSP responder, the process is changed as follows:

- If the issuer of the OCSP Proxy certificate is not the same of the certificate whose status is

To be checked, the client rejects the signature if the "OCSP-Proxy-OID" is not present in the certificate's EKU.

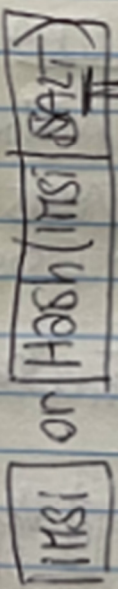
- In addition, if ~~the~~ any "id-ad-ocsp-proxy" access method(s) are used, the client must reject the signature from the server if the CA identifier of the certificate whose status is being queried for is not present in the OCSP Proxy's certificate's SAN extension.

APPLICATIONS:

- Access Networks can use OCSP Proxy to increase PKI reliability when checking credentials:
  - for TLS connections (CORE NETWORK)
  - for Device Authentication

↦ Access Networks can provide Proxy services for their connected users

- → Proxying All (or some) WebPKI CAs / OCSP
- → Proxying All (or some) IoT/Device PKI (as a service - paid by vendors that use this service and/or CA providers)



↦ 5G/3GPP can use this mechanism, together with the OCSP for SM/Revocation idea, to identified compromised identifier and reject malicious/revoked identities

- ↦ Requests from different location can be used to track DUP identities
- ↦ CRLs can be used for privacy concerns

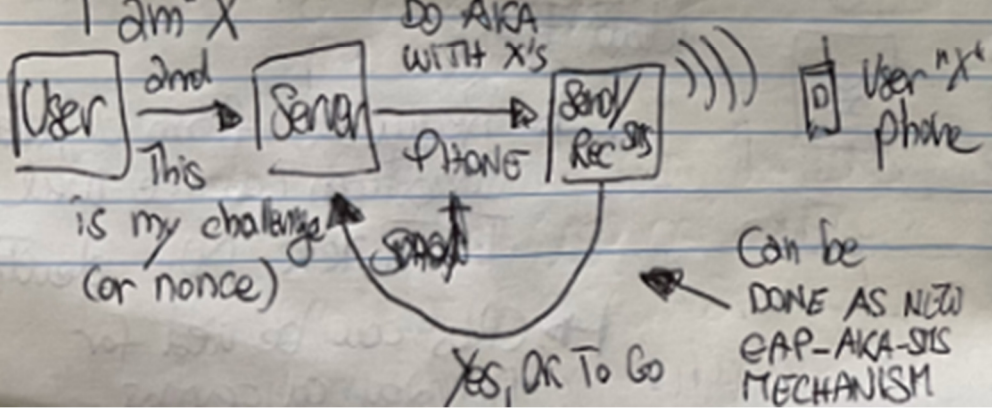
→ Access Networks can use this mechanism to validate SIM-based credentials ~~when~~ for its services, like:

↦ Access or Browse Internet connectivity

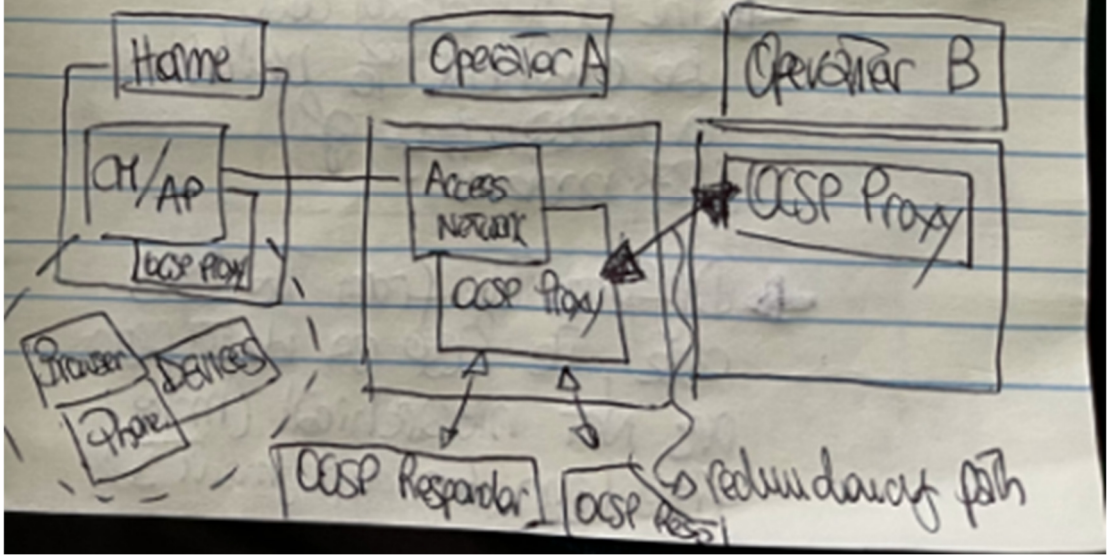
↦ Web Resources (accounts access)

NOTE Possible NEW PATENT IDEA?

→ Performing AKA' Authentications over SMS/MMS as a second (or first) factor of authentication



- Operating Systems can rely on Local OCSP Proxy Nodes That are deployed "locally" (e.g. at an ISP, at an office, or at an home environment)
  - Applications can rely on Operating Systems responders or on the registered Local responder
  - A NEW DHCP OPTION IS DEFINED TO CARRY THE OCSP PROXY URL
- Hierarchies of OCSP Proxies can be used, for example:



The OCSP Proxy can be the first one hit and then the "official" ones can be hit (if the local one(s) do not support such CA)

NOTE **POSSIBLE NEW PATENT IDEA**

A DISTRIBUTED OCSP SYSTEM

Similarly to what we do for the DNS, we can do the same with OCSP

- The OCSP proxy can be enabled to build a hierarchy of responders
- Differently from the DNS case, the OCSP CA identifiers are NOT hierarchical (more freedom for deployment)