AUTOMATIC CERTIFICATE REVOCATION PROCESS
WITH SERVICE ASSURANCE NOTIFICATION

INVENTORS:

STEVEN J. GOERINGER

MASSIMILIANO PALA

Description

When a PKI certificate is revoked, impacted subscribers are unable to connect to peers or servers. IT or service provider staff should be made aware of this circumstance so the device can be corrected and service disruption is minimized. Furthermore, to the degree possible, automation of the revocation process can be supported in most circumstances. This invention outlines a process for automatic revocation processing with alerts to support service assurance. Revocation occurs when it is clear the private key of the impacted subscriber (end element, server, RA, CA) is known or suspected to be compromised. Three revocation impacts to service reliability are as follows:

- Self revocation as specified in renewal process (see invention disclosure D4043)
- Revocation by the registration authority or other authorized trusted entity (as reflected by possession by a properly issued certificate and public/private key pair)
- Revocation by a third party

Notification of a management entity should be performed when a certificate is revoked.
Claims:

- A revocation request to a CA or revocation management entity that are signed by the impacted certificate private key OR the responsible registration authority can be automated
- Revocation requests that are not signed by either the impacted certificate entity or the responsible RA must be validate probably using a manual process
- The entity requesting the revocation advises the management entity of the revocation to manage clinical reliability and ensure clinical staff are aware of the revocation

These ideas are illustrated in the attached process flows.

When a PKI certificate is revoked, it is important that IT or service provider staff are made aware so they can mitigate service disruptions that occur as a result. This capability is not available to secure infrastructures based on PKI today.

CableLabs®

Reliability considerations of automated certificate revocation

CableLabs

Max Pala, Steve Goeringer

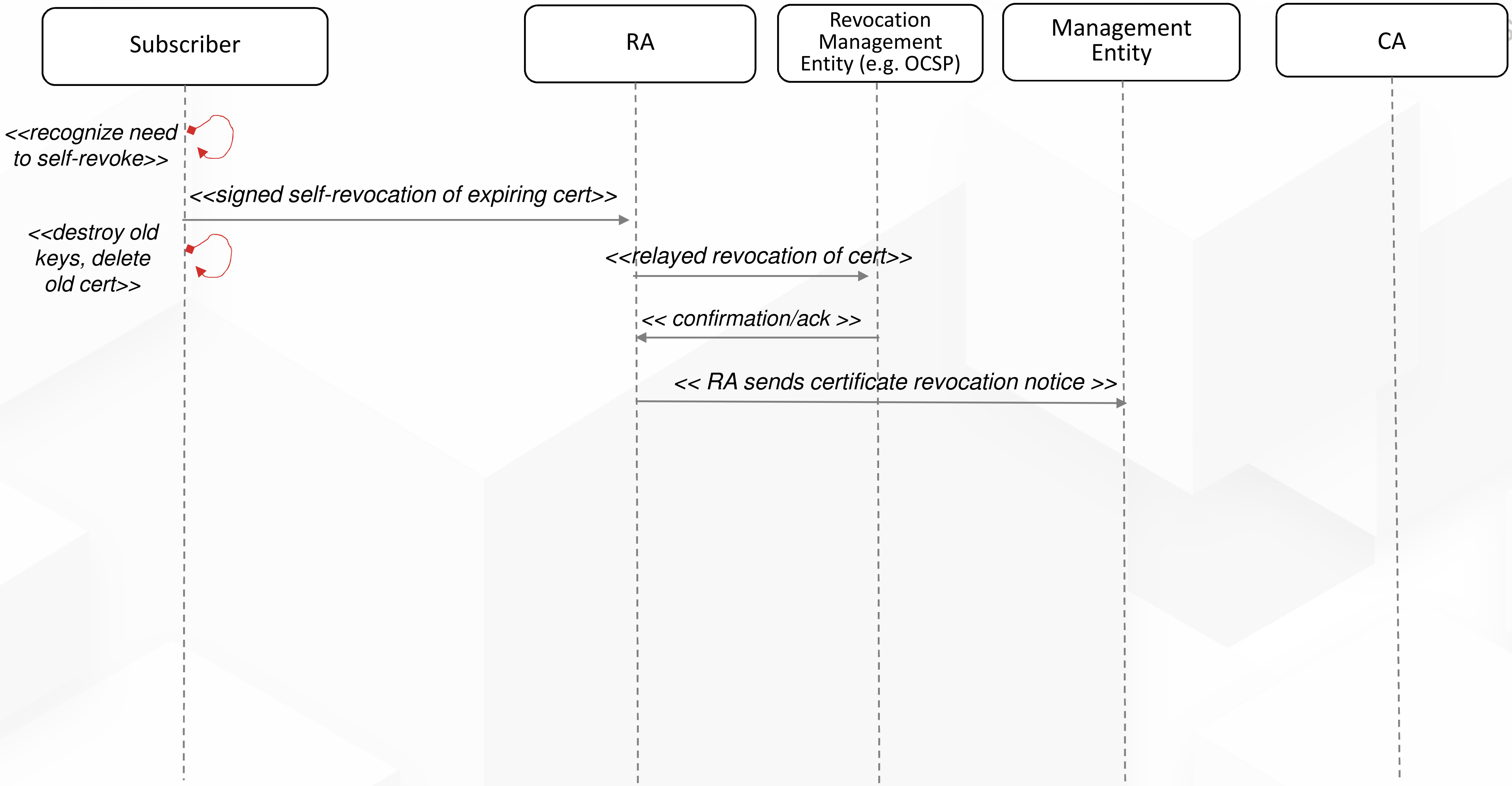
Three revocation impacts to service reliability

- Self revocation as specified in renewal process
- Revocation by the registration authority
- Revocation by a third party

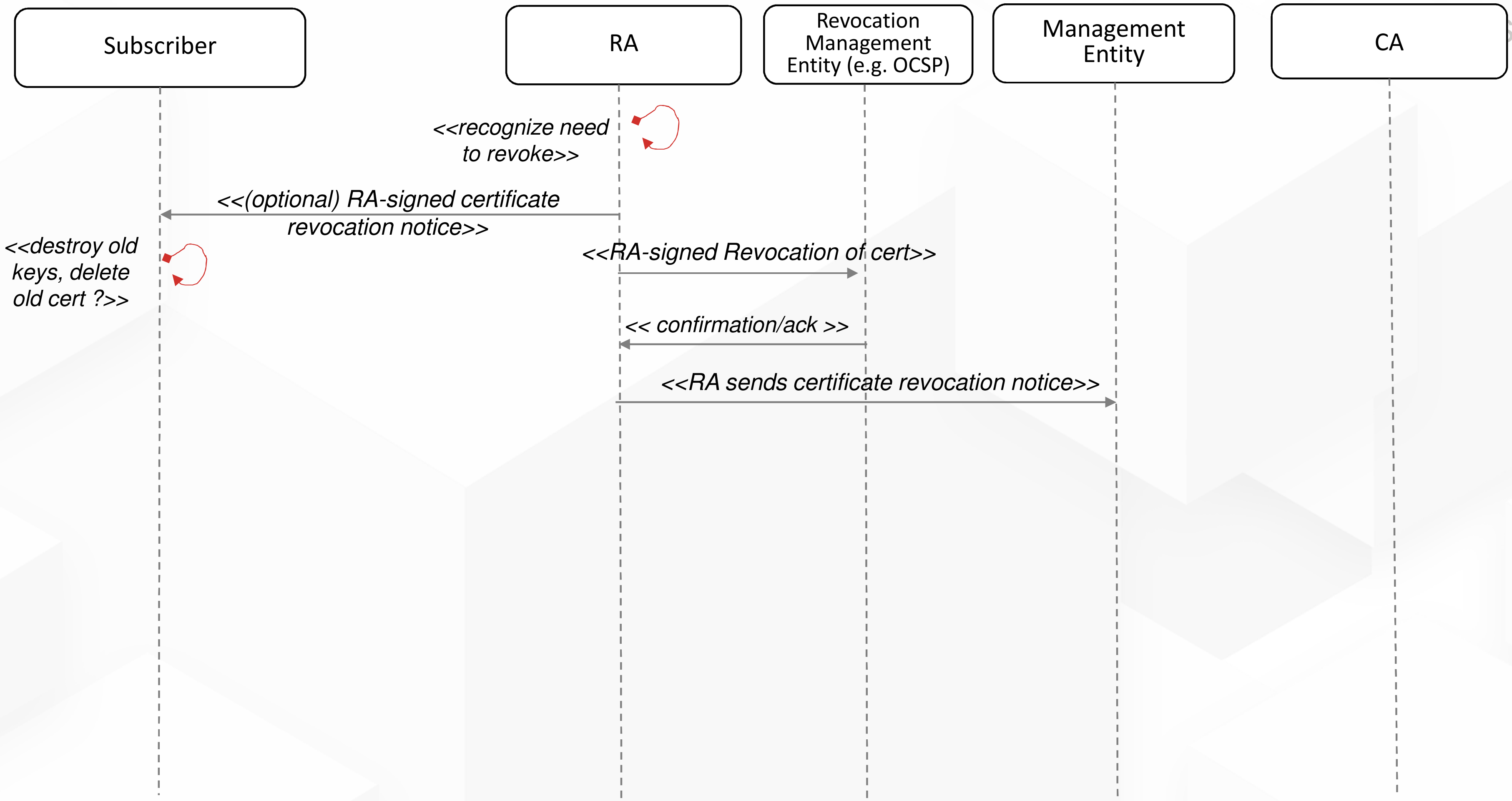
Rationale

- A revocation request to a CA or revocation management entity that are signed by the impacted certificate private key OR the responsible registration authority can be automated
- Revocation requests that are not signed by either the impacted certificate entity or the responsible RA must be validate probably using a manual process
- The entity requesting the revocation advises the management entity of the revocation to manage service reliability and ensure stakeholders aware of the revocation
- RA will send self-signed and RA-signed revocation requests directly to an entity responsible for revocation
  - This entity is usually part of the CA and the CA will implement procedures and practices necessary for processing automatic revocation requests securely to prevent misuse

Revocation by subscriber


Subscriber
RA
Revocation Management Entity (e.g. OCSP)
Management Entity
CA
<<recognize need to self-revoke>>
<<signed self-revocation of expiring cert>>
<<destroy old keys, delete old cert>>
<<relayed revocation of cert>>
<< confirmation/ack >>
<< RA sends certificate revocation notice >>

Revocation by RA



Subscriber

RA

Revocation Management Entity (e.g. OCSP)

Management Entity

CA

<<recognize need to revoke>>

<<(optional) RA-signed certificate revocation notice>>

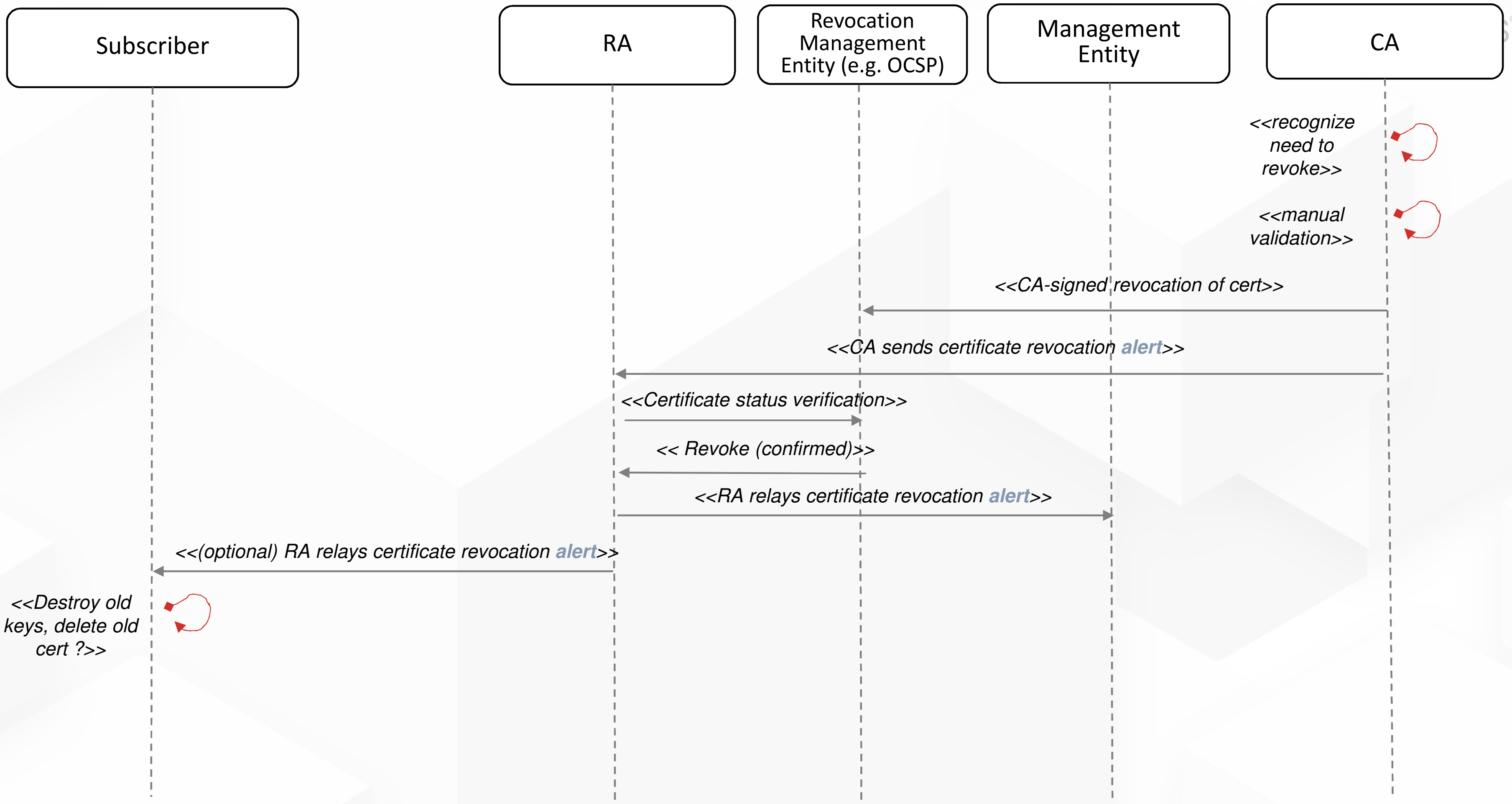
<<destroy old keys, delete old cert ?>>

<<RA-signed Revocation of cert>>

<< confirmation/ack >>

<<RA sends certificate revocation notice>>

Revocation by CA with alerting



Subscriber
RA
Revocation Management Entity (e.g. OCSP)
Management Entity
CA
<<recognize need to revoke>>
<<manual validation>>
<<CA-signed revocation of cert>>
<<CA sends certificate revocation alert>>
<<Certificate status verification>>
<< Revoke (confirmed)>>
<<RA relays certificate revocation alert>>
<<(optional) RA relays certificate revocation alert>>
<<Destroy old keys, delete old cert ?>>