Root CA Certificate Rekeying in the Scenario of Post Quantum Migration

IETF 121, LAMPS

Guilin Wang, Yanjiang Yang, and Jie Zhang

Wang.guilin@Huawei.com

Root CA Certificate Rekeying

❑ Information of our daft

- **Title**: Root CA Certificate Rekeying in the Scenario of Post Quantum Migration (draft-wang-lamps-root-ca-cert-rekeying-00)
- **Author**: Guilin Wang, Yanjiang Yang, and Jie Zhang
- **Date submitted**: v00 on 2024-07-05
- https://datatracker.ietf.org/doc/draft-wang-lamps-root-ca-cert-rekeying/

❑ Motivation

- **RFC4210** gives two approaches for old entities acquiring the new root CA public key via **NewWithNew or NewWithOld**.
- Our draft proposes a one-way link certificate based solution such that old entities are transparent to root CA certificate rekeying.
- The solution is beneficial for scenarios where old entities are not ware of the existence of new root CA certificate or cannot update correspondingly.
- In some scenarios, the certificate lifetime of devices can be longer than 10 years.
- Logically, the proposed solution does not rely on which cryptographic algorithms are used to verify the certificate chains.
- So, the proposed solution works in traditional, pure PQ, or hybrid PKIs.
- **This version v01: Added Section 5 for our testing results.**

Root CA Certificate Rekeying

How to Update Root CA Certificate?
Basically, two approaches only …

- **<u>Rekeying</u>: Issue a brand new root CA certificate**
  - May use different key length or even new algorithms
  - How to manage two root CA certificates during the overlapping period (20 years)?

Challenges!

- Some old devices cannot install the new root CA certificate …
- So, how do they verify a new certificate chain?
- May need to update software or even the logic of certificate management…

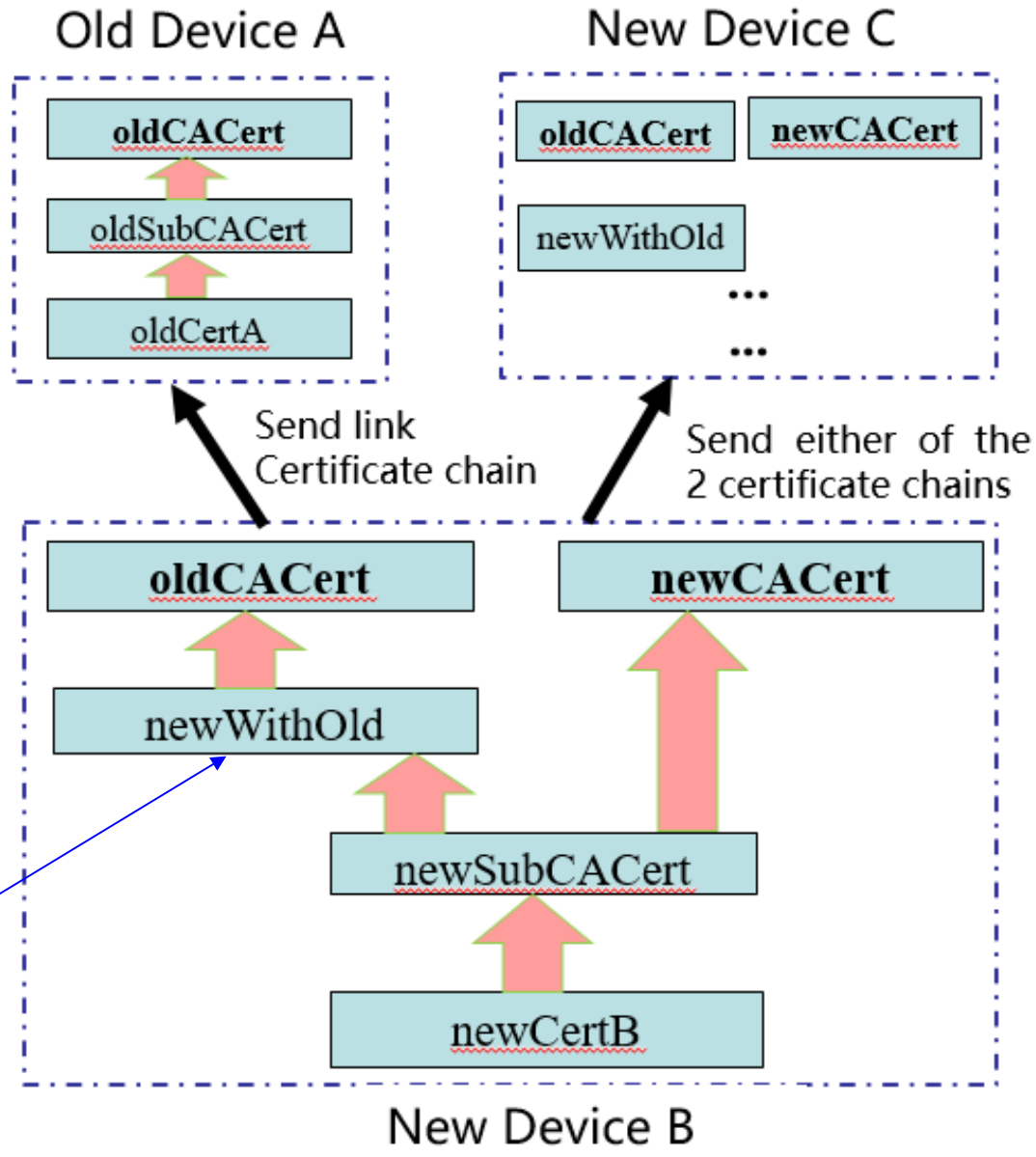
- **Renewing: Extend the validity of existing CA certificate**
  - Still the same key pair
  - But longer validity
  - But attackers have longer time to cryptanalyze the same key pairs
  - Still need to issue a brand new CA certificate, soon or later…

Root CA Certificate Rekeying: The Proposed Solution

❑ Basic Ideas

- o **Use a link certificate,** called **NewWithOld**
- o It certifies the new root key by the old one.
- o So, during the overlapping period, old devices can verify a link certificate chain from a new device by using the old root CA certificate as the trust anchor.
- o Other cases are simpler …

The link certificate **NewWithOld** (specified in RFC4210) is used to introduce the new root key to old devices, which may be not equipped with the new root CA certificate



Root CA Certificate Rekeying: Testing

- 3 generations of root CA certificates: G1 (2016-2025), G2 (2018-2027), and G3 (2020-2029)
- Cross verifying tests among OpenSSL 1.0.1c, OpenSSL 1.0.2u 、 OpenSSL 1.1.1g and JDK 8u251
- G1 and G2 implements RSA, with RSA 4096 for root CA certificate, RSA 3092 for subject CA certificate, and RSA 2048 for end entity certificate.
- G3 implements ECDSA, with ECDSA 384 for root CA certificate, and ECDSA 256 for both subject CA certificate and end entity certificate.
- Cross verifying tests are experimented among implementations of running OpenSSL 1.0.1c, OpenSSL 1.0.2u 、 OpenSSL 1.1.1g and JDK 8u251. More specifically, G1 implements RSA with all these four software packages, while G2 and G3 implement RSA and ECDA respectively in the last three software packages, but not OpenSSL 1.0.1c. This is because OpenSSL 1.0.1c is a relatively old version of openSSL, so new system may not employ it.

Root CA Certificate Rekeying: Testing

	2018					2020					
	G1 Client		G2 Client		G3 Client		G1 Client		G2 Client		G3 Client	
	Cli.	Ser.	Cli.	Ser.	Cli.	Ser.	Cli.	Ser.	Cli.	Ser.	Cli.	Ser.
G1 Server	OK	OK	OK	OK	-	-	OK	OK	OK	OK	OK	OK
G2 Server	OK	OK	OK	OK	-	-	OK	OK	OK	OK	OK	OK
G3 Server	-	-	-	-	-	-	OK	OK	OK	OK	OK	OK

Root CA Certificate Rekeying: Testing

	2015			2016		
	G1 Client	G2 Client	G3 Client	G1 Client	G2 Client	G3 Client
	Cli. / Ser.	Cli. / Ser.	Cli. / Ser.	Cli. / Ser.	Cli. / Ser.	Cli. / Ser.
G1 Server	- / -	- / -	- / -	OK / OK	- / -	- / -
G2 Server	- / -	- / -	- / -	- / -	- / -	- / -
G3 Server	- / -	- / -	- / -	- / -	- / -	- / -

	2025			2026		
	G1 Client	G2 Client	G3 Client	G1 Client	G2 Client	G3 Client
	Cli. / Ser.	Cli. / Ser.	Cli. / Ser.	Cli. / Ser.	Cli. / Ser.	Cli. / Ser.
G1 Server	OK / OK	OK / OK	OK / OK	NO / NO	NO / NO	NO / NO
G2 Server	OK / OK	OK / OK	OK / OK	NO / NO	OK / OK	OK / OK
G3 Server	OK / OK	OK / OK	OK / OK	NO / NO	OK / OK	OK / OK

	2028			2030		
	G1 Client	G2 Client	G3 Client	G1 Client	G2 Client	G3 Client
	Cli. / Ser.	Cli. / Ser.	Cli. / Ser.	Cli. / Ser.	Cli. / Ser.	Cli. / Ser.
G1 Server	NO / NO	NO / NO	NO / NO	NO / NO	NO / NO	NO / NO
G2 Server	NO / NO	NO / NO	NO / NO	NO / NO	NO / NO	NO / NO
G3 Server	NO / NO	NO / NO	NO / NO	OK / OK	NO / NO	NO / NO

Conclusion: Our testing results show positive answers for all the cases that should be considered

Root CA Certificate Rekeying

Comments received by 17 July 2024

Michael Richardson

- The problem of updating root CAs is particularly acute in IoT devices …
- draft-ietf-anima-constrained-voucher … has a section 6.5 that deals with how to do RFC4210 transition
- You may find some of the terminology from draft-irtf-t2trg-taxonomy-manufacturer-anchors useful
- What is unclear to me from reading the document is how/if it differs from the 4210 process?

Russ Housley

- Can you summarize how this is different that OldWithNew and NewWithOld as described in RFC 4210?
- There are other parts of CMP and CMC that allow the client to request certificates. CMP has certificate announcements (Section 5.3.14). CMC has the Get Certificate Control (Section 6.9) …

David von Oheimb

- please explain clearly what your approach is helpful for. It assumes that old devices cannot upgrade their trust anchor, …, the described approach is not helpful.
- CMP meanwhile also has support for clients requesting root CA updates and getting (intermediate) CA certs. See RFCs 9480 and 9483.

Hendrik Brockhaus

- The draft rfc4210bis updated the section on root CA key update (… #section-4.4), specifies a CA key update announcement message (… #section-5.3.1) and root CA update (… #section-5.3.19.5) messages.

Our Feedback

- We are not going to assume that the old entities will be able to acquire the new CA public key by themselves.
- Therefore, the process of CA root key pair update is transparent to old entities
- (The solution aims for scenarios where old devices will expire when or before their old certificates

Further Actions

- To check more details and make further comparison suggested by the above experts
- All suggestions, comments and reviews are welcome!

Wang.guilin@Huawei.com

Thanks!