Roll over certificates issues

Chunghwa Telecom Co., Ltd.

Li-Chun CHEN,
Engineer, CISSP, CISM, CISA, PMP
realsky@cht.com.tw

CA/Browser Forum Meeting 34
Cupertino , Host: Trend Micro
March, 11 , 2014

RFC 4210 4.4.1 about Root CA key Update

- To change the key of the CA, the CA operator does the following:
  - 1. Generate a new key pair;
  - 2. Create a certificate containing the old CA public key signed with the new private key (the "old with new" certificate);
  - 3. Create a certificate containing the new CA public key signed with the old private key (the "new with old" certificate);
  - 4. Create a certificate containing the new CA public key signed with the new private key (the "new with new" certificate);

RFC 4210 4.4.1 about Root CA key Update

- 5. Publish these new certificates via the repository and/or other means (perhaps using a CAKeyUpdAnn message);
- 6. Export the new CA public key so that end entities may acquire it using the "out-of-band" mechanism (if required).

- The old CA private key is then no longer required. However, the old CA public key will remain in use for some time. The old CA public key is no longer required (other than for non-repudiation) when all end entities of this CA have securely acquired the new CA public key.

Definition

- Self-issued certificates: Self-issued certificates are generated to support changes in policy or operations.
  - Ex: “old with new” & “new with old” certificates in previous page.
- Self-signed certificates: Self-signed certificates are CA certificates in which the issuer and subject are the same entity
  - Ex: “old with old” & “new with new”
- GRCA: Government Root Certification Authority
- GCA: Government Certification Authority
  - Taiwan NDC outsources the operations of GRCA & GCA to Chunghwa Telecom
    - NDC: National Development Council in Taiwan

Definition

- AIA: Authority Information Access (RFC 5280)
  - The authority information access extension indicates how to access information and services for the issuer of the certificate in which the extension appears.
    - Information and services may include on-line validation services and CA policy data. (The location of CRLs is not specified in this extension; that information is provided by the cRLDistributionPoints extension.)
    - This extension may be included in end entity or CA certificates.
    - Conforming CAs MUST mark this extension as non-critical
  - IE & Chrome on Windows support AIA, so that there is less certificates chaining problem.

BR V1.23 about AIA

- **In BR Appendix B (2) Subordinate CA Certificate & (3) Subscriber Certificate**
- **C. authorityInformationAccess**
- With the exception of stapling, which is noted below, this extension MUST be present. It MUST NOT be marked critical, and it MUST contain the HTTP URL of the Issuing CA’ s OCSP responder (accessMethod

= 1.3.6.1.5.5.7.48.1). It SHOULD also contain the HTTP URL of the Issuing CA’ s certificate

(accessMethod = 1.3.6.1.5.5.7.48.2). See Section 13.2.1 for details.

self-issued certificate as RFC 5280 6.1

- A certificate is self-issued if the same DN appears in the subject and issuer fields (the two DNs are the same if they match according to the rules specified in Section 7.1). In general, the issuer and subject of the certificates that make up a path are different for each certificate. However, a CA may issue a certificate to itself to support key rollover or changes in certificate policies. These self-issued certificates are not counted when evaluating path length or name constraints.

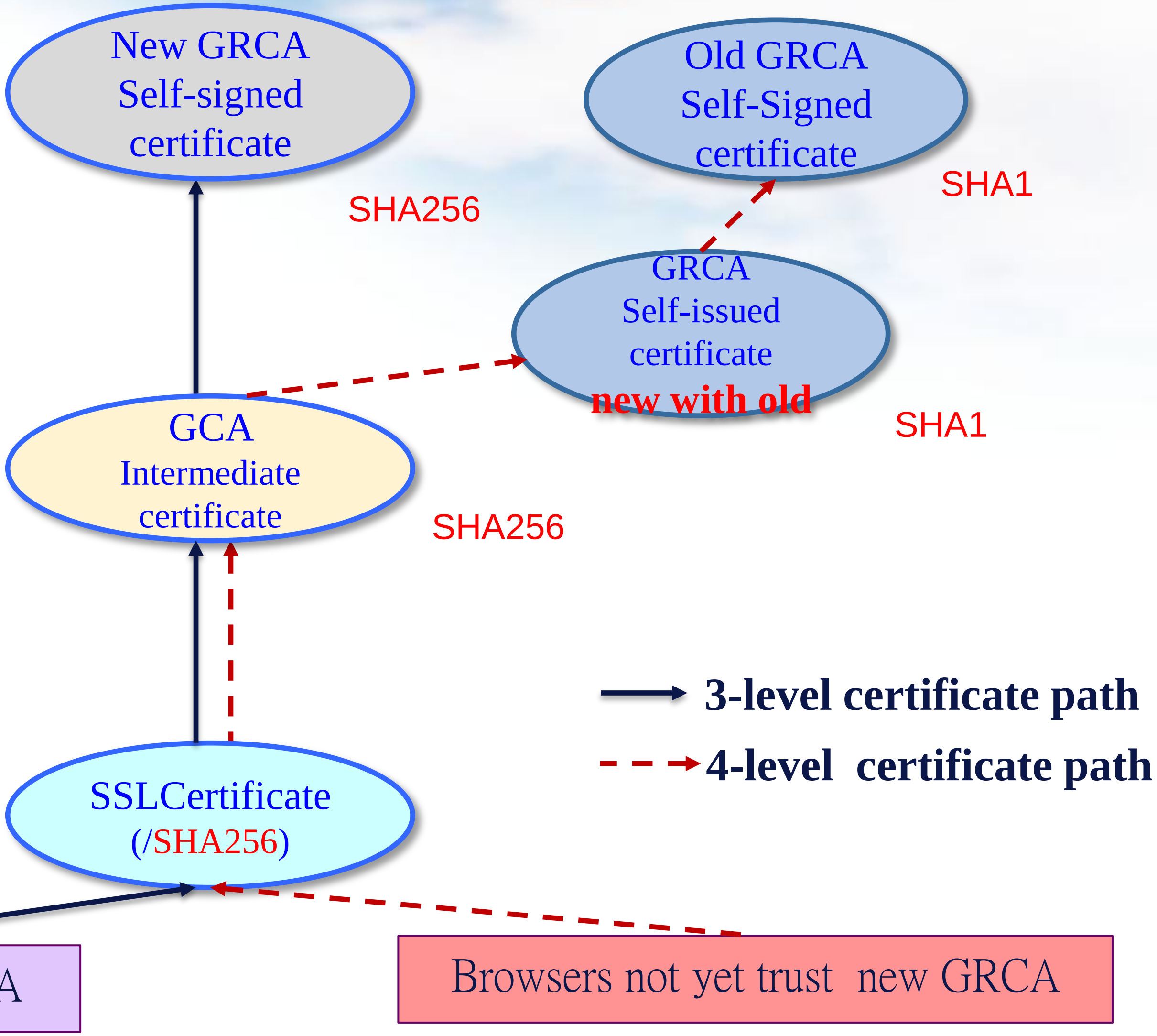
SSL Certificate Path

According RFC 5280,new GRCA & old GRCA have the same DN

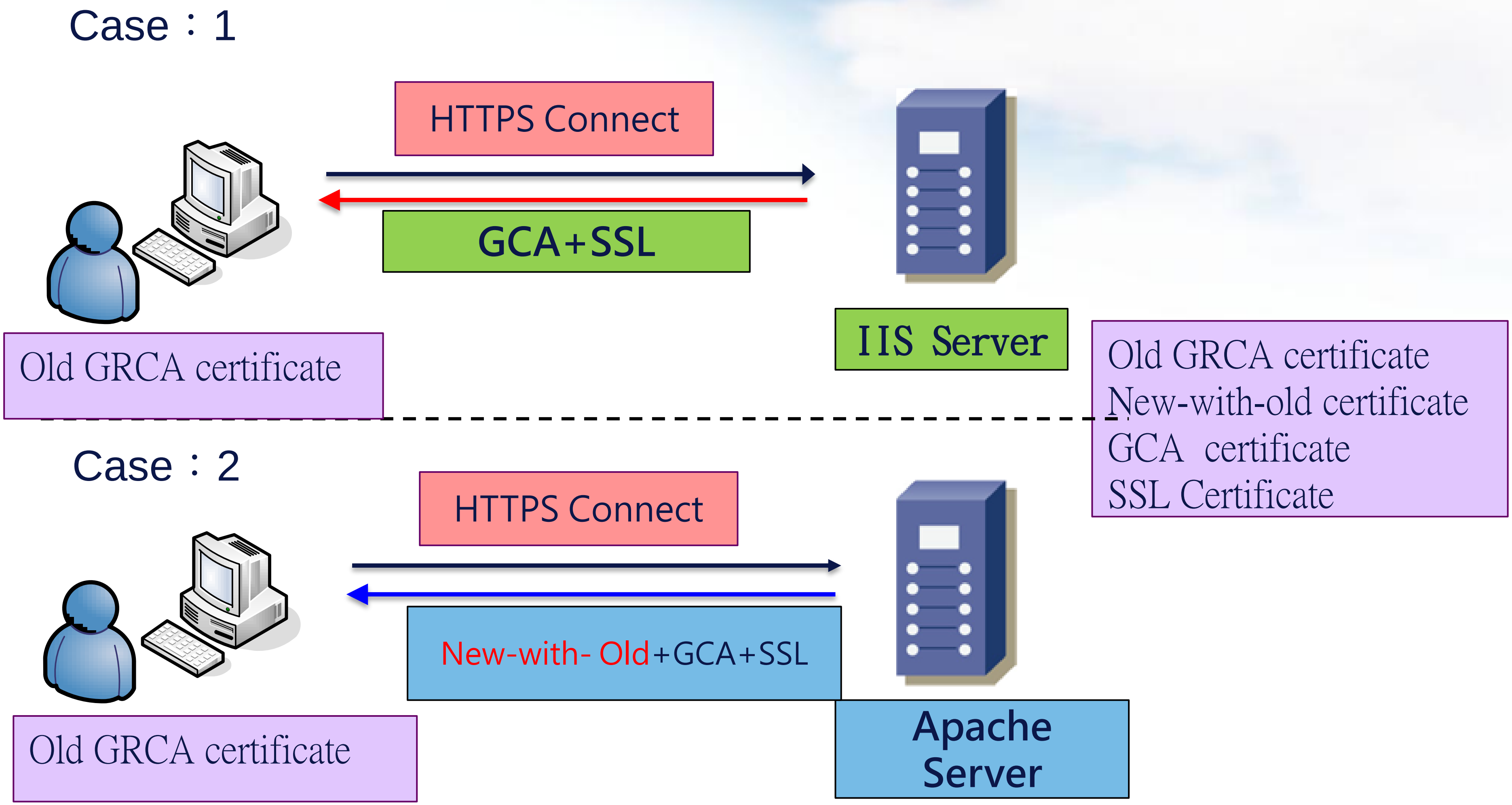
Old GRCA:1st generation of Government Root Certification Authority

New GRCA :2nd generation of Government Root Certification Authority

By GPKI CP, GRCA generate its roll over keys (Root CA Key Update) in 2012.


New GRCA Self-signed certificate
Old GRCA Self-Signed certificate
SHA1
SHA256
GRCA Self-issued certificate
new with old
SHA1
GCA Intermediate certificate
SHA256
3-level certificate path
4-level certificate path
SSLCertificate (/SHA256)
Browsers trust new GRCA
Browsers not yet trust new GRCA

Case Study: Certificate chains transmitted by Web servers



Case：1

HTTPS Connect

GCA+SSL

IIS Server

Old GRCA certificate

Old GRCA certificate
New-with-old certificate
GCA certificate
SSL Certificate

Case：2

HTTPS Connect

New-with- Old+GCA+SSL

Apache Server

Old GRCA certificate

Test result summary (In Jan.,2015)

	Browsers trust new GRCA		Browsers don’ t trust new GRCA		
	Safari	Chrome on MacOS	Firefox	IE	Chrome on Windows
	3-level path validation		4-level path validation		
IIS (Case1)	V	V	X Web server can’t send New –with –old Certificate	V (fetch new-with-old via AIA)	V (fetch new-with-old via AIA)
Apache (Case2)	V	V	V Web server can send New –with –old certificate	V	V

Sites that you can test

- Site powered by IIS 7：
  - https://gcaweb.nat.gov.tw
  - https://www.hrd.gov.tw/
- Site powered by Apache, which will send the entire Certificate Chain：
  - https://www.ncert.nat.gov.tw/

- You could use below pages to test
  - https://www.sslshopper.com/ssl-checker.html
  - https://certlogik.com/ssl-checker/

Finding & Analysis

- IIS 7 falsely treated GRCA’ s Self-Issued certificate (new with old) as a Self-Signed certificate, because it has the same issuer and subject name.
  - So IIS 7 will not send GRCA’ s Self-Issued certificate (new with old) to SSL client.
- Microsoft IE support AIA
  - Even though there is no “new with old” sent by IIS 7, IE can use SSL & GCA certificates’ s AIA to chain up new GRCA .
    - Note that new GRCA was built in Microsoft on Feb,21, 2015.
    - GRCA was built in Microsoft in 2004

Finding & Analysis

- There were lots of complaints for Firefox users connect to Taiwan’ s government organizations or units sites that use IIS. Because
  - IIS do not send a “New-with-Old” certificate to client
  - Firefox has not support AIA yet
  - Firefox uses its own trust list, we had submitted new GRCA certificate to Mozilla for several months, but not sure when it will be added to the trust list.

Suggestions & further discussions

- Request Microsoft to solve the bug of IIS ASAP
  - Chunghwa Telecom had submitted a bug report regarding IIS’ s processing of self-issued certificates through Premium support via Microsoft Taiwan in March, 2015.

- We find there is a bug the same as IIS that Qualays SSL Labs’ s tool can't distinguish self-issued certificate with self signed certificate :
  - https://www.ssllabs.com/ssltest/

Suggestions & further discussions

- We suggest to make AIA mandatory and browsers must support fetching intermediate certificates through AIA
  - In SSL protocol, SSL servers should send intermediate certificate & SSL certificate to SSL client
  - But we see some web site administrators forget to install intermediate certificates to their server follow CA’ s or web server’ s manuals.
  - Some web servers such as IIS have the bug of not sending the complete rollover certificate chain

BR modification Suggestion

- **In BR Appendix B (2) Subordinate CA Certificate & (3) Subscriber Certificate, we suggest to modify as below**

- C. authorityInformationAccess
- This extension MUST be present and MUST NOT be marked critical . With the exception of stapling, which is noted below, it MUST contain the HTTP URL of the Issuing CA’ s OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1). It MUST contain the HTTP URL of the Issuing CA’ s certificate (accessMethod = 1.3.6.1.5.5.7.48.2). From YYMMDD, browsers MUST support fetching intermediate certificates through the HTTP URL of the Issuing CA’ s certificates.

Acknowledgement

- Many thanks to our teams: Dr. Wen-Cheng Wang Wen-hui Tsai, Dr. Pin-Jung Chiang, Yan-Wen Nian, Chia-Hsien Lin ,Hung-Yu Hsu, Pei-yuan, Huang, Sammy Wu in Chunghwa Telecom
- There are testing print screens of in VirtualBox, IIS Servers 7.5 , firefox 36 by Wen-hui Tsai.

(with same DN or different DN of self-issued certificate & self-signed certificates cases)

- Thanks for Gervase, Anoosh,& Erwann's replying before the presentation.

Value Creator for
Investors, Customers, Employees, and Society

Thank you!