GMO GlobalSign Incident Report

Certificate Revocation Issue

13 October 2016

GlobalSign®

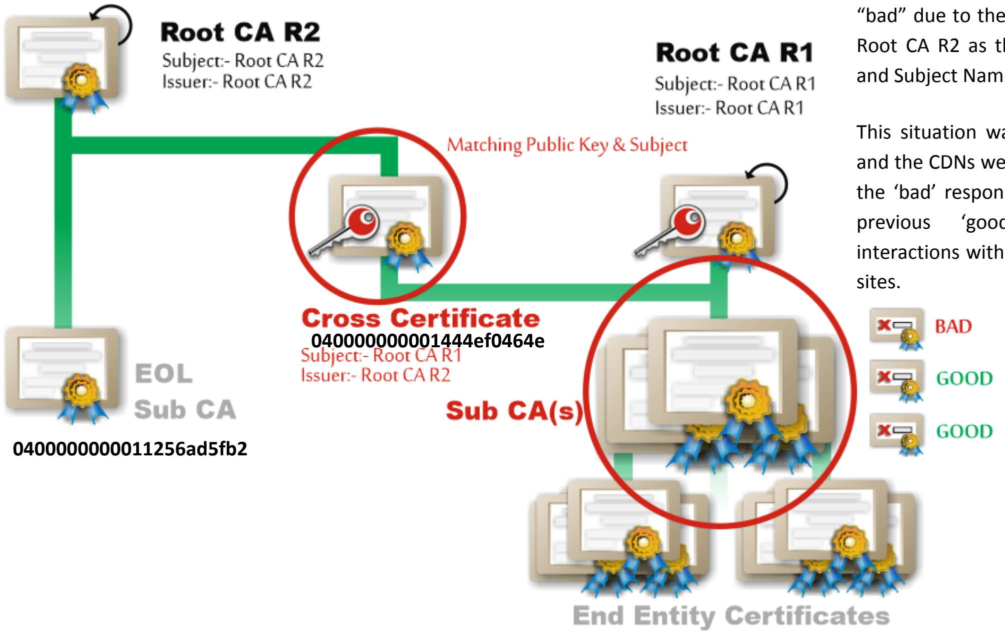
www.globalsign.com

In a revocation exercise which should have been “business as usual” for a Certificate Authority (CA) such as GMO GlobalSign, we published a Certificate Revocation List (CRL) on the 7th October signed by Root CA R2, which listed a Cross Certificate with serial number 040000000001444ef0464e together with another subordinate certificate with serial number 0400000000011256ad5fb2. The latter one being an end of life (EOL) subordinate CA as shown below having previously issued SHA1 Extended Validation SSL certificates – Reason codes in both cases were set to “Cessation of Operation” as there were no risks associated with the Private Keys and no requirements to publish outside of normal procedures. The new CRL remains available, through our Content Distribution Network front end on http://crl.globalsign.com/root-r2.crl. No effect was seen on any clients as the CAs being revoked were effectively not used by any relying parties. The previous CRL would have expired on the 15th October.

At 08:00 BST on the 13th October, the delegated Online Certificate Status Protocol (OCSP) responder database, which serves delegated responses for the Root CA 2 (R2) on http://ocsp2.globalsign.com/rootr2 was updated to include the serial numbers which were included in the CRL. This is where the issue which created the disruption to our customers stemmed.

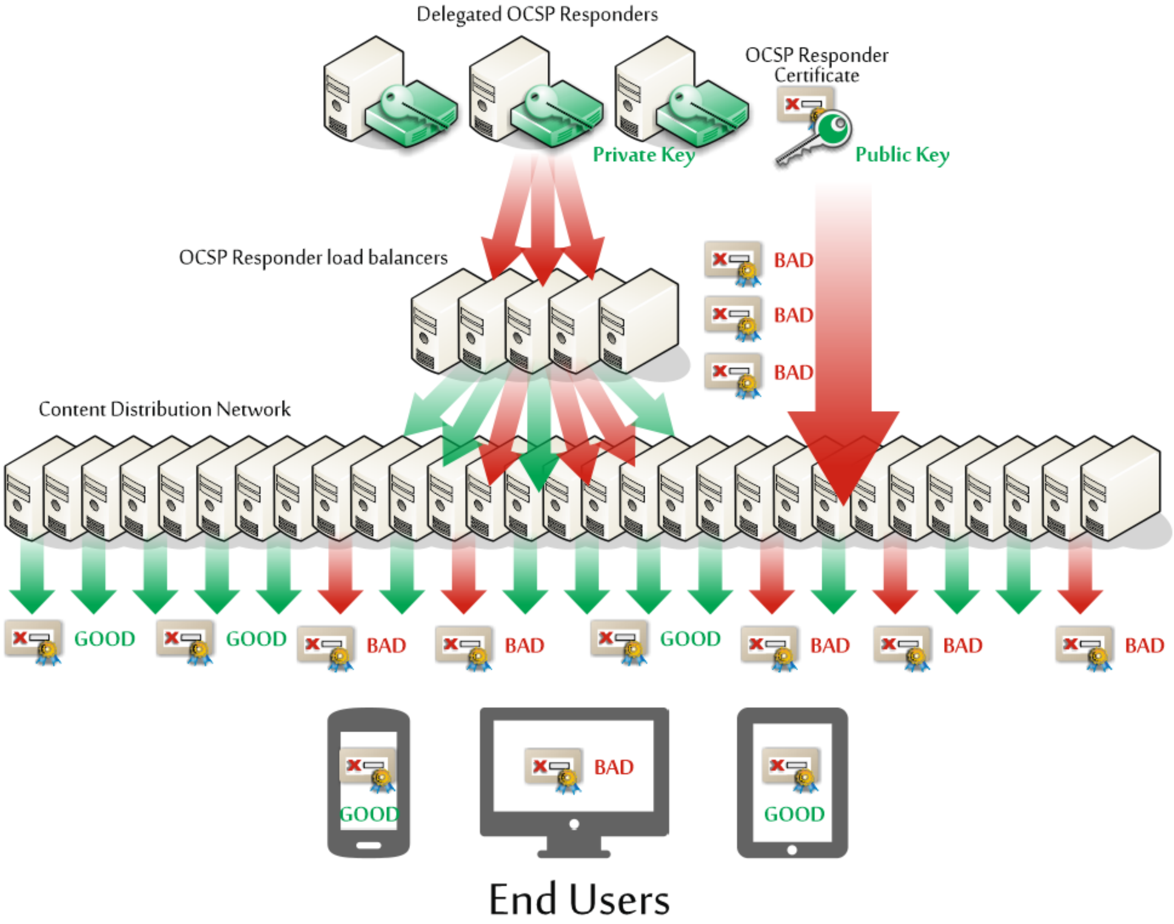
Delegated revocation responders incorrectly determined that all Root CA R1 Intermediates were “bad” due to the cross certificate being revoked by Root CA R2 as the cross had the same Public Key and Subject Name details with a more recent date.

This situation was rolled back and load balancers and the CDNs were purged but some users retained the ‘bad’ response, while many more still had the previous ‘good’ responses from previous interactions with GMO GlobalSign SSL enabled web sites.



GMO GlobalSign uses a third party security accredited load balanced OCSP responder system for provision of delegated responses across the product range and outwards to our community of customers and their relying parties. However, and unfortunately for our ecosystem and our stakeholders and their customers, the logic within the responder code base determined that the revocation of the Cross Certificate, identified by its Public Key and Subject Name in a lookup table, was effectively an instruction to also identify all other subordinate certificate authorities including DomainSSL and AlphaSSL as ‘bad’. The logic took the more recent Not-Before Date (Valid From) of the cross certificate as a later assertion than the original Root CA R1 and therefore determined this as an authoritative instruction to mark all Root CA R1 issued subordinate certificates as ‘bad’. New OCSP requests coming in to the system for any Root CA R1 product after the update were created and pushed to the load balancers as ‘bad’ and onwards out to the CDN and finally out to the platforms of relying parties trying to check the revocation status of Certificates used on SSL/TLS enabled Web Servers of GMO GlobalSign customers. Not all clients will have needed responses at once as some may already have cached the previous good responses. Across the three levels and therefore at any point in time there was a mix of good and bad responses depending on varying circumstances, previously visited web site history, etc.

Initial reports and internal testing incorrectly suggested that the revocation of the cross may have inadvertently affected the logic in some browser platforms and therefore how they determined end entity certificate status. This was clearly an incorrect conclusion but at the time seemed a potential reason for the issue given that both Root CA R1 and Root CA R2 are present in many platforms. The number of client platform types affected was also fairly narrow in the early stages of the incident, which again added to the incorrect assumption it was a client issue.


Delegated OCSP Responders
OCSP Responder Certificate
Private Key
Public Key
OCSP Responder load balancers
BAD
BAD
BAD
Content Distribution Network
GOOD
GOOD
BAD
BAD
GOOD
BAD
BAD
BAD
GOOD
BAD
GOOD
End Users

GMO GlobalSign runs a hierarchical caching system to provide fast responses for users the world over. These caching layers exist in our DCs, in the global CDN, and additionally the user's browser will also cache OCSP responses.

In line with the CA industry standard practice, our OCSP responses are cached for up to 4 days in the user's browser and this is the reason different users saw different effects. The browser loads the response via the CDN network, which provides a lower storage time of 1 hour before refreshing, however the edge load balancers within the GlobalSign infrastructure have a longer cache time of 8 hours to manage load within the internal network.

This multi-layer cache, although now cleaned at the GlobalSign and CDN, levels means that users could see errors for up to 4 days.

GMO GlobalSign takes our Disaster Recovery processes and Risk Mitigation strategy seriously and as such we do try to plan for potential issues by splitting products and services across alternative Root CAs. For this reason our Extended Validation SSL range, AATL and Trusted Root customers were not affected. In addition GlobalSign attempts to maintain backup certificates, issued to the same subordinate Certificate Authority but signed by a different Root CA. We were able to provide two of these certificates for our Organizational SSL and Domain SSL products immediately. Our AlphaSSL and CloudSSL customers had to wait a few hours more while an emergency key ceremony was held to create alternatives.

GlobalSign continues to work with customers affected by this incident and we hope to pass on our experience of this issue to other CAs through our industry associations to help other CAs avoid the same potential issues. As the OCSP responses we issue are valid for a maximum of 4 days, the incident will have fully passed by the 17th October. We will learn from this experience and be stronger as a consequence in our risk mitigation strategy. In addition, our technical teams will be looking at ways to shorten the OCSP validity period to allow users to be protected faster should there be a real need for revocation.

Our teams will also be working with the OCSP responder provider to allow the Cross Certificate to be revoked correctly by the OCSP responders without impacting other CA's. We do not have a final timeline on any patch or workaround for this exercise but recognize that we need to align OCSP and CRL.

GlobalSign has published a support article that we continue to update with resolution instructions and details. Please find the article here: https://support.globalsign.com/customer/portal/articles/2599710-ocsp-revocation-errors---troubleshooting-guide along with a set of FAQs on the incident: https://support.globalsign.com/customer/portal/articles/2599975-ocsp-revocation-errors-faq

Incident Timeline

Date	Time (BST)	Event
7-Oct-16		CRLs for all roots including Root 2 updated
13-Oct-16	08:00	OCSP status updated for The Cross Certificate
13-Oct-16	10:20	Initial reports to support teams of revoked certificates
13-Oct-16	10:40	Growing correlation of Chrome and Safari issues
13-Oct-16	11:07	Determination of R1 chain issues
13-Oct-16	12:02	Confirmation of responder issue from revoked cross signing certificate
13-Oct-16	12:20	Removal of cross signing certificate from the OCSP Database
13-Oct-16	13:20	Initiation of cache flushing
13-Oct-16	14:30	Working with CDN provider to force cache purge
13-Oct-16	18:14	Cache flush complete
13-Oct-16	20:24	Determination of stale cache on load balancer
13-Oct-16	21:19	Confirmation of all caches cleared.

ABOUT GLOBALSIGN

GlobalSign has been a trust service provider since 1996. Its focus has been, and always will be, on providing convenient and highly productive PKI solutions for organizations of all sizes. Its core Digital Certificate solutions allow its thousands of authenticated customers to conduct SSL secured transactions, data transfer, distribution of tamper-proof code, and protection of online identities for secure email and access control. Vision and commitment to innovation led to GlobalSign being recognized by Frost & Sullivan for the 2011 Product Line Strategy Award. The company has local offices in the US, Europe and throughout Asia. For the latest news on GlobalSign visit https://www.globalsign.com or follow GlobalSign on Twitter (@globalsign).

GlobalSign Americas
Tel: 1-877-775-4562
www.globalsign.com
sales-us@globalsign.com

GlobalSign EU
Tel: +32 16 891900
www.globalsign.eu
sales@globalsign.com

GlobalSign UK
Tel: +44 1622 766766
www.globalsign.co.uk
sales@globalsign.com

GlobalSign FR
Tel: +33 9 75 18 32 00
www.globalsign.fr
ventes@globalsign.com

GlobalSign DE
Tel: +49 800 7237980
www.globalsign.de
verkauf@globalsign.com

GlobalSign NL
Tel: +31 85 8882424
www.globalsign.nl
verkoop@globalsign.com

GlobalSign SG
Tel: +65 3158 0349
www.globalsign.com/en-sg/

GlobalSign AU
Tel: +61 3 9988 3988
www.globalsign.com/en-au/

GlobalSign HK
Tel: +852 5808 1867
www.globalsign.com/en-hk/

GlobalSign CN
Tel: +86 21 60762537
cn.globalsign.com

GlobalSign IN
Tel: +91 11 41106000
www.globalsign.com/en-in/

GlobalSign PH
Tel: +63 2 847 4774
www.globalsign.com/en-ph/