



Certificate Revocation With OCSP



Copyright © www.ine.com

Keith Bogart

CCIE #4923



-  kbogart@ine.com
-  [@keithbogart1](https://twitter.com/keithbogart1)
-  [linkedin.com/in/keith-bogart-2a75042](https://www.linkedin.com/in/keith-bogart-2a75042)

CCIE Routing & Switching



Copyright © www.ine.com



Topic Overview

- ▷ OCSP Definition & Functionality
- ▷ OCSP Browser Support
- ▷ OCSP Stapling
- ▷ OCSP Must-Staple

OCSP

- ▶ Online Certificate Status Protocol
- ▶ Web Client submits a request to a CA server, that returns a signed response with certificate current status.
- ▶ Problem areas;
 - ▶ OCSP Query between client and CA servers during TLS handshake increases latency.
 - ▶ Relies on CA infrastructure making it prone to availability problems.
 - ▶ Privacy compromise. Browser leaks what website is being accessed and who accesses it to CA servers.
 - ▶ Tremendous load on CA Servers to respond to gazillions of OCSP Requests.

Field	Value
Subject	ine.com
Public key	RSA (2048 Bits)
Public key parameters	05 00
Enhanced Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1)
Subject Key Identifier	bcc970e4ef1936806ef5d3ae3...
Authority Key Identifier	KeyID=a84a6a63047ddd8ae6...
Authority Information Access	[1]Authority Info Access: Acc...
Subject Alternative Name	DNS Name=ine.com

[1]Authority Info Access
Access Method=On-line Certificate Status Protocol
(1.3.6.1.5.5.7.48.1)
Alternative Name:
URL=http://ocsp.int-x3.letsencrypt.org
[2]Authority Info Access
Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)
Alternative Name:
URL=http://cert.int-x3.letsencrypt.org/

Copyright © www.ine.com



To use OCSP, the CA must encode the OCSP server location into the certificates that it signs. The “Authority Information Access” extension is used for this.

-
- OCSP requests contains the Serial number of the Certificate in question.
-
- Notice that OCSP Response is “signed” by the CA. This prevents anyone else from spoofing the CA and spoofing an OCSP Response.
-
- CA Servers are a ripe target for malicious actors to attack because they are known, public sources of critical data.
-
- OCSP does not mandate encryption, everything is sent in cleartext. When an OCSP Request is sent:
----The CA knows that a specific website Certificate was just viewed and your IP address

OCSP Browser Support

▷ OCSP is supported by the following Web Browsers:

- ▶ Internet Explorer (starting in Windows Vista)
- ▶ All versions of Mozilla Firefox (on by default in Firefox 3 and later)
- ▶ Safari on MacOS (on by default as of Mac OS X 10.7)
- ▶ Opera starting with version 8.0
- ▶ Microsoft Edge

▷ OCSP Soft Fail

- ▶ Failure to receive OCSP Response doesn't mean Certificate is invalid...just that CA is unreachable/unresponsive.
- ▶ Most browsers simply treat the Certificate as valid in this case...this is called, "Soft Fail"

▷ Google Chrome does not support OCSP but instead implements its own revocation-checking mechanism.

OCSP Capture

[ip.addr eq 72.21.91.29 and ip.addr eq 192.168.200.34] and (tcp.port eq 80 and tcp.port eq 54890)

No.	Time	Source	Destination	Protocol	Length	Info
7130	30.517613	192.168.200.34	72.21.91.29	TCP	66	54890 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
7135	30.544270	72.21.91.29	192.168.200.34	TCP	66	80 → 54890 [SYN, ACK] Seq=0 Ack=1 Win=5535 Len=0 MSS=1460 SACK_PERM=1 WS=512
7136	30.544403	192.168.200.34	72.21.91.29	TCP	54	54890 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
7137	30.544485	192.168.200.34	72.21.91.29	HTTP	288	GET /MFewTzBNIEswSTA3BgUrdgMCGgUABBTfghLjKLEJQZPIn0KCzkdAqVYowQUsT7DaQP4v0cB1JgmGggC72NkK8MCEAKXB1YH1KnrVx2Bjy8eCv2I13D HTTP/1.1r\n
7148	30.582245	72.21.91.29	192.168.200.34	TCP	60	80 → 54890 [ACK] Seq=1 Ack=235 Win=147456 Len=0
7149	30.584088	72.21.91.29	192.168.200.34	OCSP	842	Response
7165	30.624409	192.168.200.34	72.21.91.29	TCP	54	54890 → 80 [ACK] Seq=235 Ack=789 Win=64768 Len=0

> Frame 7137: 288 bytes on wire (2304 bits), 288 bytes captured (2304 bits) on interface 0
> Ethernet II, Src: AsustekC_9d:45:66 (f8:32:e4:9d:45:66), Dst: Ubiquiti_f0:c6:13 (80:2a:a8:f0:c6:13)
> Internet Protocol Version 4, Src: 192.168.200.34, Dst: 72.21.91.29
> Transmission Control Protocol, Src Port: 54890, Dst Port: 80, Seq: 1, Ack: 1, Len: 234
▼ Hypertext Transfer Protocol
> GET /MFewTzBNIEswSTA3BgUrdgMCGgUABBTfghLjKLEJQZPIn0KCzkdAqVYowQUsT7DaQP4v0cB1JgmGggC72NkK8MCEAKXB1YH1KnrVx2Bjy8eCv2I13D HTTP/1.1r\n
Connection: Keep-Alive\r\nAccept: */*\r\nUser-Agent: Microsoft-CryptoAPI/10.0\r\nHost: ocsp.digicert.com\r\n\r\n[Full request URI: http://ocsp.digicert.com/MFewTzBNIEswSTA3BgUrdgMCGgUABBTfghLjKLEJQZPIn0KCzkdAqVYowQUsT7DaQP4v0cB1JgmGggC72NkK8MCEAKXB1YH1KnrVx2Bjy8eCv2I13D]
[HTTP request 1/1]
[Response in frame: 7149]

OCSP Stapling

- ▶ Normal OCSP protocol requires Web Client to directly query the Certificate Authority (using OCSP) for status of website Certificate.
- ▶ OCSP Stapling moves this responsibility to the Web Server itself.
 - ▶ Web Server will periodically poll CA (via OCSP) for revocation status of its own Certificate.
 - ▶ Web Server will “staple” this OCSP Response along with certificate to the client during TLS handshake in a “ServerCertificateStatus” message.
 - ▶ In this way, the CA will not know when a Client is visiting any particular website.
- ▶ **Downsides: OCSP-Stapling is not mandatory, and clients don't know when to expect it.**
 - ▶ When Cert is received without an OCSP Staple, web-client proceeds to using normal OCSP (if anything at all) to verify revocation status.

Copyright © www.ine.com



OCSP Stapling would be great if EVERY website did it. Then, browsers could be programmed that if they connected to a website, downloaded its Cert and there WASN'T a staple...game over! That site must be a fake!

-

Most websites that utilize HTTPS also implement OCSP Stapling.

OCSP Staple Capture

The image shows a Wireshark capture of an OCSP Staple message. The packet list shows three packets: 82 (Certificate Status), 83 (TCP ACK), and 84 (Client Key Exchange). The details pane shows the Certificate Status message structure, including the Handshake Protocol, Certificate Status Type, OCSF Response, and Certificate Status fields. A Wireshark filter 'ocsp!' is applied, and a small table shows the filtered packets.

No.	Time
82	1.525580
92	1.532310

OCSP Wireshark Filter

Copyright © www.ine.com



How can you tell that this is an OCSP-Staple (as opposed to a normal OCSP transaction between a Client and a CA)?? Two indicators:

----OCSP is sent using HTTP...not HTTPS (so it wouldn't show up in Wireshark as TLS)

----Take a look at the IP Source Address of the "Certificate Status" message. It is the same source IP as the website itself.

OCSP Must-Staple

- ▶ OCSP-Stapling is not mandatory, and clients don't know when to expect it.
- ▶ OCSP Must-Staple is an extension to a Digital Certificate
 - ▶ Must be requested in CSR (Certificate Signing Request)
 - ▶ Certificate Authority will append OCSP Must-Staple to Certificate
 - ▶ Added as X.509v3 Extension
- ▶ When Server Certificate is presented to Web Client, presence of this extension indicates (to the Client) that the Cert is ONLY valid if an OCSP Status Response immediately follows.
- ▶ More details: RFC 7633


Copyright © www.ine.com



In this way, even if someone did steal the private key and Certificate of a website...and even IF they did manage to convince you to navigate to their spoofed website...the moment you received a copy of the Cert you would wait (for a few milliseconds) for an OCSP Response...which of course they couldn't give you. And then your browser would block this website and declare it to be unsafe.

OCSP Responses are digitally signed by the CA with the CA's private key and contain the Serial number of the Cert. There is no way to spoof them. And if a Malicious Actor tries to remove this extension from a Cert...then the Signature of that Cert will no longer be valid.

OCSP Must-Staple

Authentication	
 Server Key and Certificate #1	
Subject	scottheime.co.uk Fingerprint SHA1: R0b0b1888049c6ad0733d39840950771e31043 Pin SHA256: 9dNZZueK2hyatSpT1X0aDgOclLjK6H-Nzaa0ACF5SDwep
Common names	scottheime.co.uk
Alternative names	rsa2048.scottheime.co.uk scottheime.co.uk scottheime.com strongssl.scottheime.co.uk weakssl.scottheime.co.uk www.scottheime.co.uk www.scottheime.com xn--l8haa.scottheime.co.uk
Valid from	Sun, 23 Oct 2016 16:21:00 UTC
Valid until	Sat, 21 Jan 2017 16:21:00 UTC (expires in 2 months and 28 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	Let's Encrypt Authority X3 AIA: http://cert.int-x3.letsencrypt.org/
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	No
OCSP Must Staple	Supported
Revocation information	OCSP OCSP: http://ocsp.int-x3.letsencrypt.org/
Revocation status	Good (not revoked)
Trusted	Yes

Copyright © www.ine.com





Thanks for watching!