

OCSP Stapling

Let the web server protect the users!



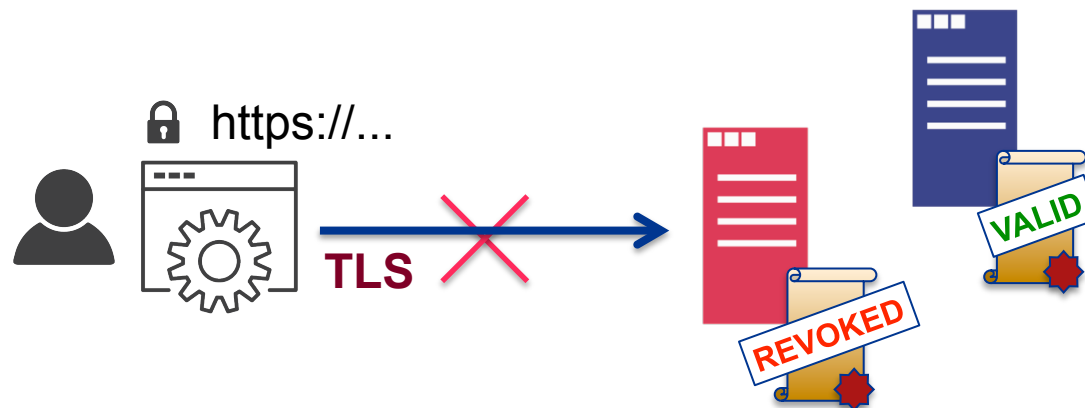
SWITCH

SWITCHpki Team
pki@switch.ch

Bern, 29.03.2017

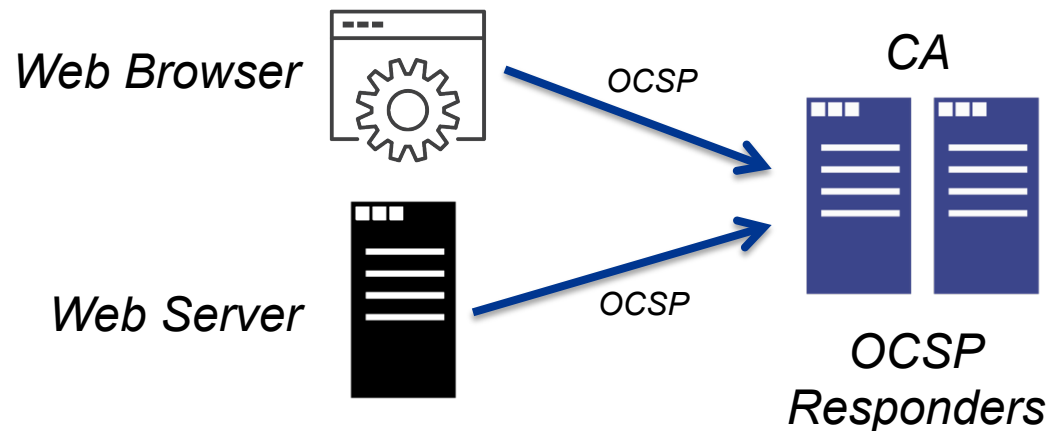
Rejecting Revoked Certificates

- Web browsers should check whether a web server's SSL certificate has been revoked, e.g. because of a stolen private key.
- Such an event is rare, actually. But checking the validity of the certificate is still crucial.
- Web browsers should protect users from accessing sites presenting revoked certificates.



OCSP

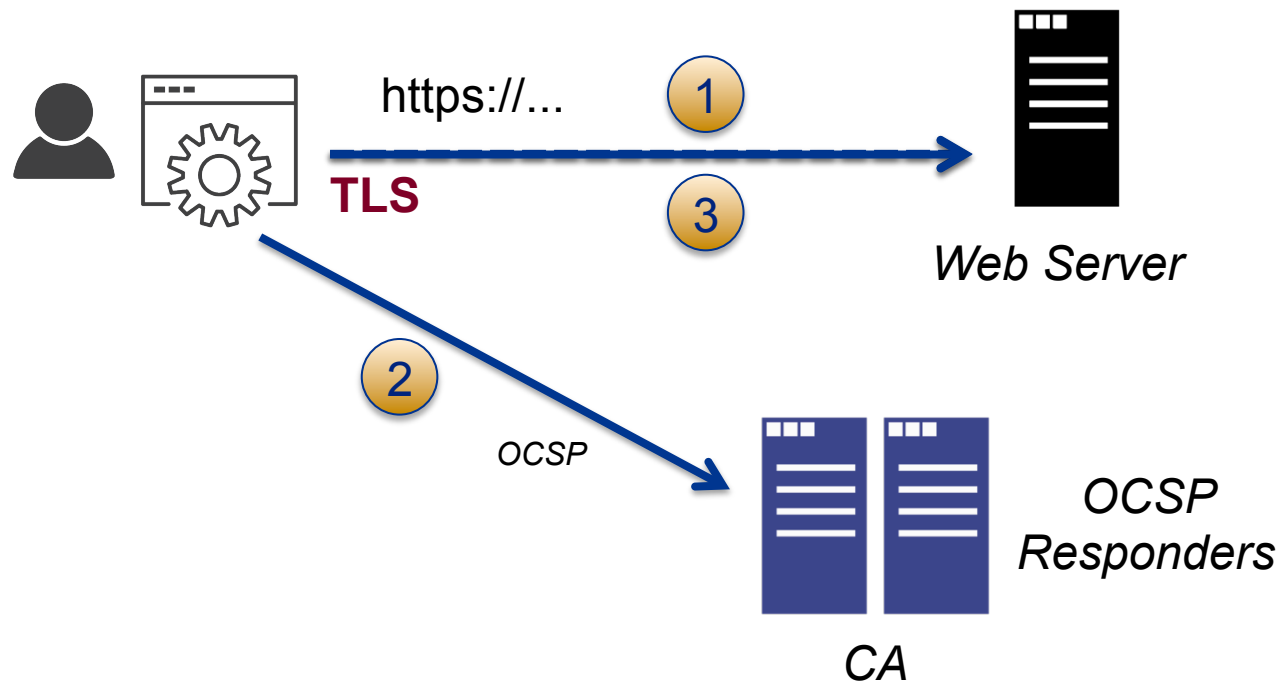
- OCSP (Online Certificate Status Protocol) allows to instantly check a certificate's status.
- Certification Authorities, like QuoVadis for SWITCHpki, run OCSP responders allowing clients to query the status of certificates issued by these CAs.
- OCSP queries are usually run by web browsers or web servers.



OCSP Query by Web Browser

While connecting to a secure web site and setting up the TLS connection, the web browser checks the certificate's status by querying the CA's OCSP responders.

Web Browser



OCSP Query by Web Browser

Security Problems:

- Most browsers just ignore temporary technical problems and establish the TLS connection without knowing the exact status of the certificate.
 - *An attacker might exploit this in a WLAN.*

(Latest IEs and Edge block access to the web site in this case.)
- Mobile clients don't do OCSP queries at all to save bandwidth.
 - *Users are not protected at all.*

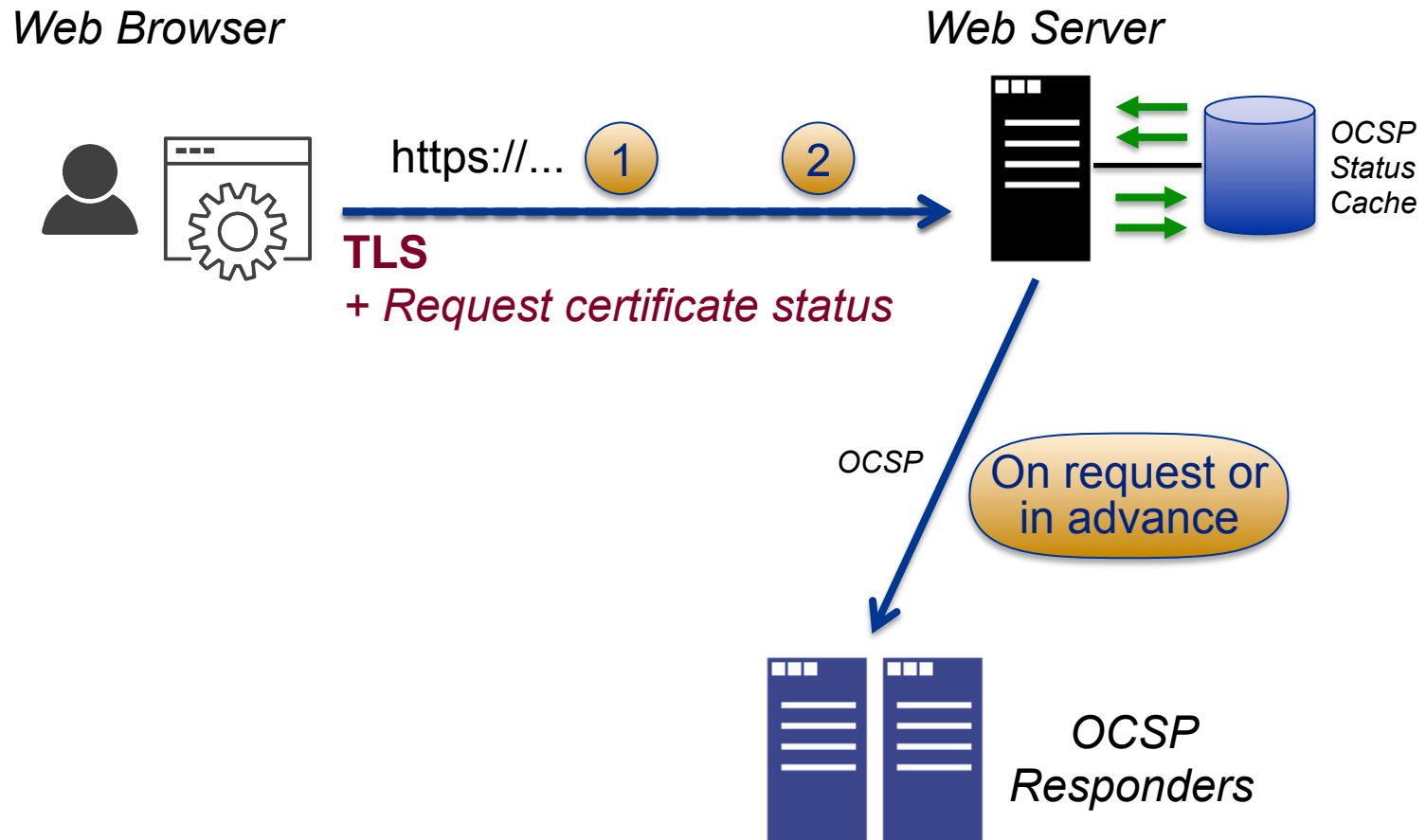
OCSP Query by Web Browser

Data Privacy Problems:

- Clients connect to the CAs' OCSP servers for most TLS connections
 - *CAs can see which web sites users visit (but limited to web sites using certificates of the same CA).*

OCSP Stapling

The OCSP query is done by the web server.



OCSP Stapling

- The web client can request the certificate's status from the web server by an extension of the TLS protocol.
- The web server either fetches the (still valid) certificate status from its local cache or queries the OCSP responders.
- The web server returns the certificate status back to the client as part of the setup of the TLS connection.

OCSP Stapling is usually well supported by desktop web browsers. On newer mobile devices, OCSP Stapling should be supported, too.

Advantages of OCSP Stapling

- Eliminates existing security and data privacy problems.
- Makes HTTPS faster.
- Saves bandwidth at the client side.
 - Good for mobile clients.
- Is mostly prone to short technical problems (e.g. local or remote network problems, short DNS problems, etc.)
 - The web server's configuration specifies whether to ignore the problem and send nothing to the browser or send a "retry-later" status to the browser. Recommended default is to ignore errors to avoid locked out users (Attackers can't easily exploit such situations at the server side).
- System administrator of the web server can partially control the behavior of the web browser regarding OCSP and error handling.

Configuration on Web Server

Apache:

- Available since Apache 2.4
- Disabled by default, must be enabled in the configuration.

IIS on Windows:

- OCSP Stapling is enabled by default (since Windows Server 2008)

Others:

- See the corresponding documentation of your server software.

Enabling OCSP in Apache

Recommended configuration:

Global configuration:

```
SSLStaplingCache shmcb:/run/httpd/ssl_stapling(32768)  
(Example valid for Red Hat)
```

Global configuration or per virtual host:

```
SSLUseStapling on  
# Prevent browsers from blocking access if  
# an OCSP query is temporarily not possible.  
SSLStaplingReturnResponderErrors off  
SSLStaplingErrorCacheTimeout 60  
SSLStaplingFakeTryLater off
```



Enabling OCSP in Apache

Details are available on our website:

https://www.switch.ch/pki/manage/config-apache/#ocsp_stapling

Note:



SWITCH provides this configuration on best effort. Please carefully check whether this configuration suits your needs.

Verifying OCSP Stapling

The *Certificate Chain Test* allows you to check whether OCSP Stapling is enabled and working on your server:

<https://www.switch.ch/pki/manage/certificate-chain-test/>

The option "Advanced mode" needs to be enabled.

Hostname	Port	Starttls	Timeout
<input type="text" value="www.switch.ch"/>	<input type="text" value="443"/>	<input type="text" value="-"/> 	<input type="text" value="5"/>
<input checked="" type="checkbox"/> Advanced mode	<input type="button" value="Submit"/>		
Testing www.switch.ch on port 443 			

Verifying OCSP Stapling

OCSP Stapling is enabled and working:

OCSP Stapling

Enabled. Certificate status: good

OCSP Stapling is not enabled or not configured properly:

OCSP Stapling

Not configured on server