HTTP Security Primer

Dominick Baier
http://leastprivilege.com
@leastprivilege

pluralsight
hardcore dev and IT training

Agenda

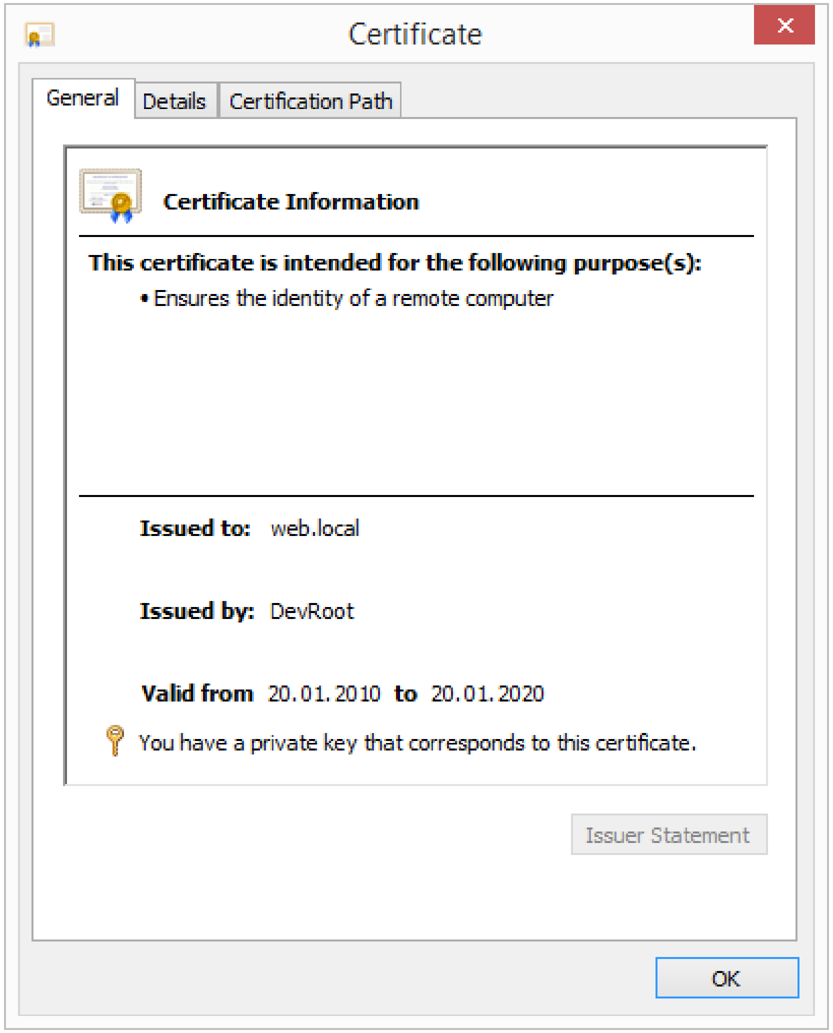
- Transport security
- X.509 Certificates
- Setting up TLS endpoints
- HTTP authentication framework
- APIs & Tools
- Resources

Transport security

- **HTTPS == HTTP over TLS**
  - RFC 2818

- **Tunnels unprotected HTTP and adds**
  - server authentication
  - integrity protection
  - replay protection
  - confidentiality

X.509 Certificates



Certificate Information

This certificate is intended for the following purpose(s):

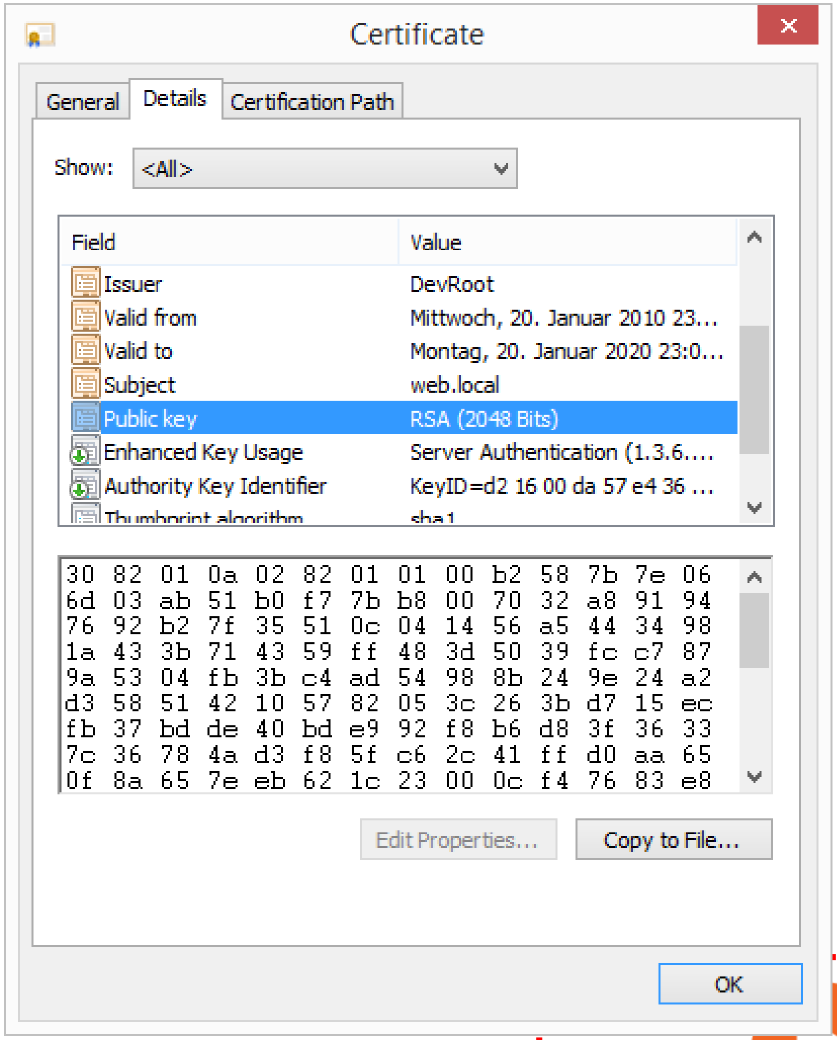
- Ensures the identity of a remote computer

Issued to: web.local

Issued by: DevRoot

Valid from 20.01.2010 **to** 20.01.2020

You have a private key that corresponds to this certificate.

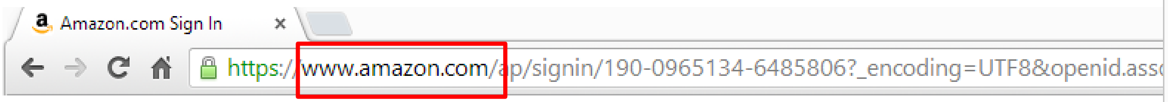


Show: <All>

Field	Value
Issuer	DevRoot
Valid from	Mittwoch, 20. Januar 2010 23...
Valid to	Montag, 20. Januar 2020 23:0...
Subject	web.local
Public key	RSA (2048 Bits)
Enhanced Key Usage	Server Authentication (1.3.6....
Authority Key Identifier	KeyID=d2 16 00 da 57 e4 36 ...
Thumbprint algorithm	sha1

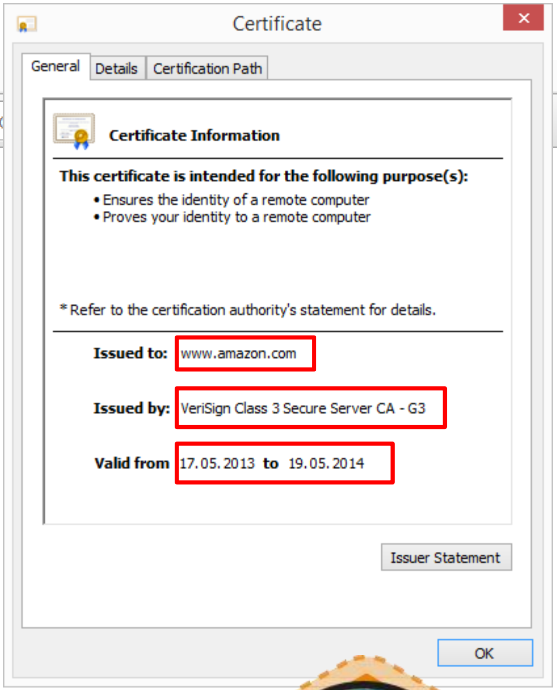
```
30 82 01 0a 02 82 01 01 00 b2 58 7b 7e 06
6d 03 ab 51 b0 f7 7b b8 00 70 32 a8 91 94
76 92 b2 7f 35 51 0c 04 14 56 a5 44 34 98
1a 43 3b 71 43 59 ff 48 3d 50 39 fc c7 87
9a 53 04 fb 3b c4 ad 54 98 8b 24 9e 24 a2
d3 58 51 42 10 57 82 05 3c 26 3b d7 15 ec
fb 37 bd de 40 bd e9 92 f8 b6 d8 3f 36 33
7c 36 78 4a d3 f8 5f c6 2c 41 ff d0 aa 65
0f 8a 65 7e eb 62 1c 23 00 0c f4 76 83 e8
```

Simplified SSL handshake



Amazon.com Sign In

https://www.amazon.com/ap/signin/190-0965134-6485806?_encoding=UTF8&openid.ass



Certificate

Certificate Information

This certificate is intended for the following purpose(s):

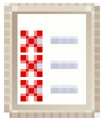
- Ensures the identity of a remote computer
- Proves your identity to a remote computer

* Refer to the certification authority's statement for details.

Issued to: www.amazon.com

Issued by: VeriSign Class 3 Secure Server CA - G3

Valid from 17.05.2013 **to** 19.05.2014



CRL check

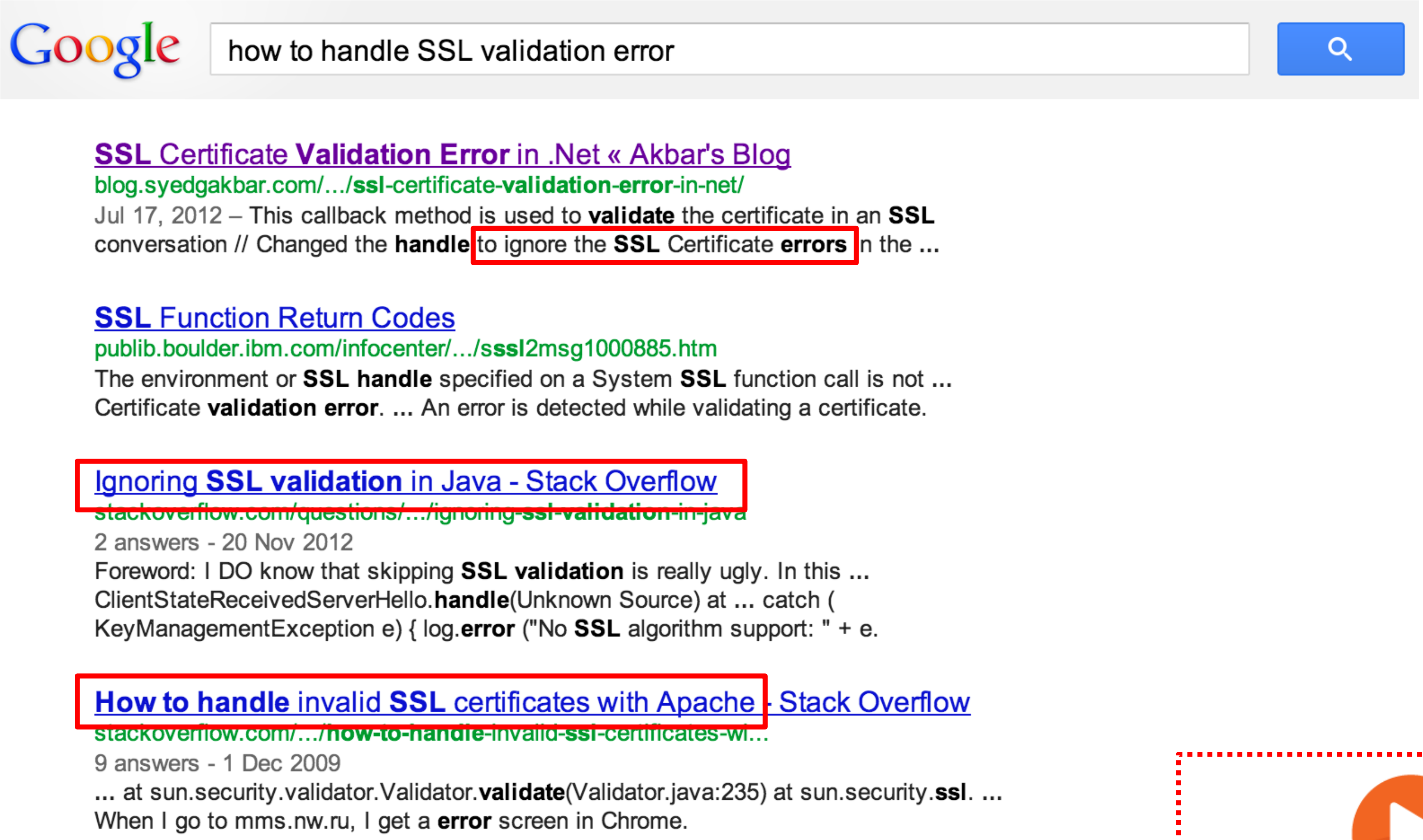
connect →

← send certificate

generate session key & encrypt with public key →

http://www.moserware.com/2009/06/first-few-milliseconds-of-https.html

Developers & SSL



how to handle SSL validation error

SSL Certificate **Validation Error** in .Net « Akbar's Blog
blog.syedgakbar.com/.../**ssl**-certificate-**validation**-**error**-in-net/
Jul 17, 2012 – This callback method is used to **validate** the certificate in an **SSL** conversation // Changed the **handle** to ignore the **SSL** Certificate **errors** in the ...

SSL Function Return Codes
publib.boulder.ibm.com/infocenter/.../s**ssl**2msg1000885.htm
The environment or **SSL handle** specified on a System **SSL** function call is not ... Certificate **validation error**. ... An error is detected while validating a certificate.

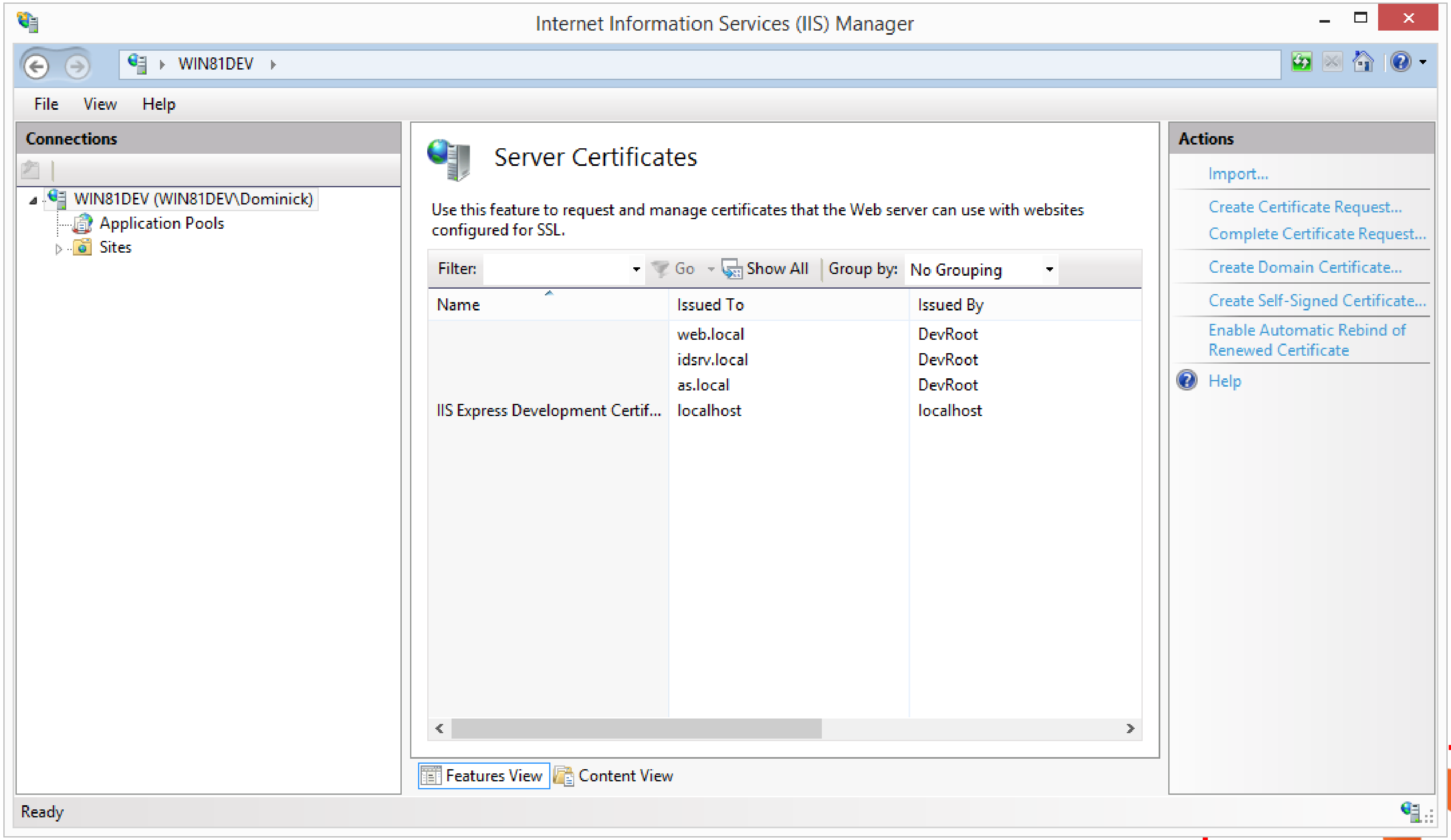
Ignoring **SSL validation** in Java - Stack Overflow
stackoverflow.com/questions/.../ignoring-**ssl**-**validation**-in-java
2 answers - 20 Nov 2012
Foreword: I DO know that skipping **SSL validation** is really ugly. In this ... ClientStateReceivedServerHello.**handle**(Unknown Source) at ... catch (KeyManagementException e) { log.**error** ("No **SSL** algorithm support: " + e.

How to handle invalid **SSL** certificates with Apache - Stack Overflow
stackoverflow.com/.../**how-to-handle**-invalid-**ssl**-certificates-wi...
9 answers - 1 Dec 2009
... at sun.security.validator.Validator.**validate**(Validator.java:235) at sun.security.**ssl**. ... When I go to mms.nw.ru, I get a **error** screen in Chrome.

Where to get certificates from?

- **Buy**
  - Verisign etc…
- **Corporate PKI**
  - Windows Certificate Services
- **Create yourself**
  - makecert.exe
  - OpenSSL

Creating/requesting certificates with IIS



Internet Information Services (IIS) Manager
WIN81DEV
File
View
Help
Connections
WIN81DEV (WIN81DEV\Dominick)
Application Pools
Sites
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Enable Automatic Rebind of Renewed Certificate
Help
Features View
Content View
Ready

Server Certificates

Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

Filter: Go Show All | Group by: No Grouping

Name	Issued To	Issued By
	web.local	DevRoot
	idsrv.local	DevRoot
	as.local	DevRoot
IIS Express Development Certif...	localhost	localhost

Creating a root certificate

```
makecert.exe

   -r                 // self signed
   -n "CN=DevRoot"    // name
   -pe                // exportable
   -sv DevRoot.pvk    // name of private key file
   -a sha1            // hashing algorithm
   -len 2048          // key length
   -b 01/21/2010      // valid from
   -e 01/21/2030      // valid to
   -cy authority      // certificate type
   DevRoot.cer        // name of certificate file
```

Creating an SSL certificate

```
makecert.exe

    -iv DevRoot.pvk           // file name of root priv key
    -ic DevRoot.cer           // file name of root cert
    -n "CN=web.local"         // name
    -pe                       // mark as exportable
    -sv web.local.pvk         // name of private key file
    -a sha1                   // hashing algorithm
    -len 2048                 // key length
    -b 01/21/2010             // valid from
    -e 01/21/2020             // valid to
    -sky exchange             // certificate type
    web.local.cer             // name of certificate file
    -eku 1.3.6.1.5.5.7.3.1    // extended key usage
```

Setting up SSL

- **Establish trust**
  - Windows certificate store

- **Bind SSL certificate to port / host name**
  - IIS
  - netsh.exe
  - httpconfig.exe

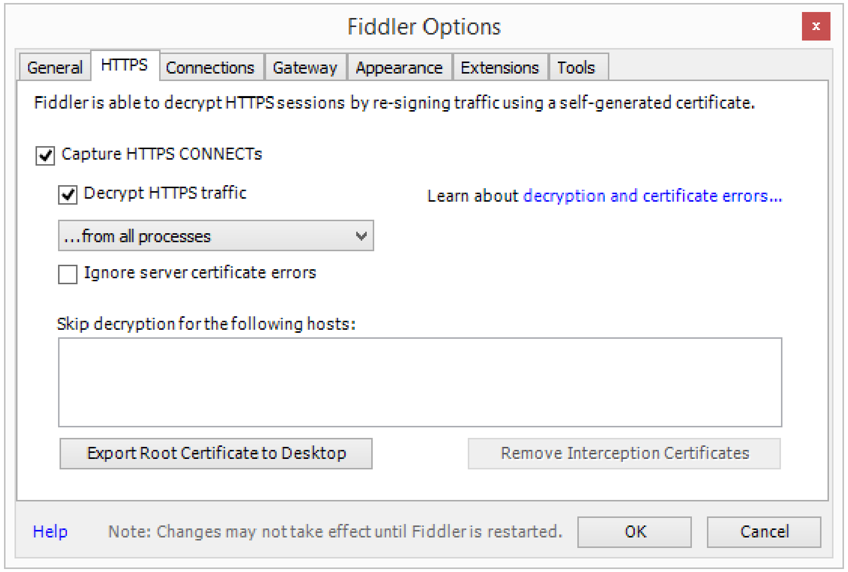
Using code to validate certificates

```
private bool ValidateUsingValidator(X509Certificate2 cert)
{
    var validator = X509CertificateValidator.ChainTrust;

    try
    {
        validator.Validate(cert);
        return true;
    }
    catch (SecurityTokenValidationException)
    {
        return false;
    }
}
```

Useful tools

- **Fiddler**
  - HTTP proxy
  - mainly for debugging purposes
  - Can "sniff" HTTPS connections



Fiddler is able to decrypt HTTPS sessions by re-signing traffic using a self-generated certificate.

☑ Capture HTTPS CONNECTs

☑ Decrypt HTTPS traffic

Learn about decryption and certificate errors...

...from all processes

☐ Ignore server certificate errors

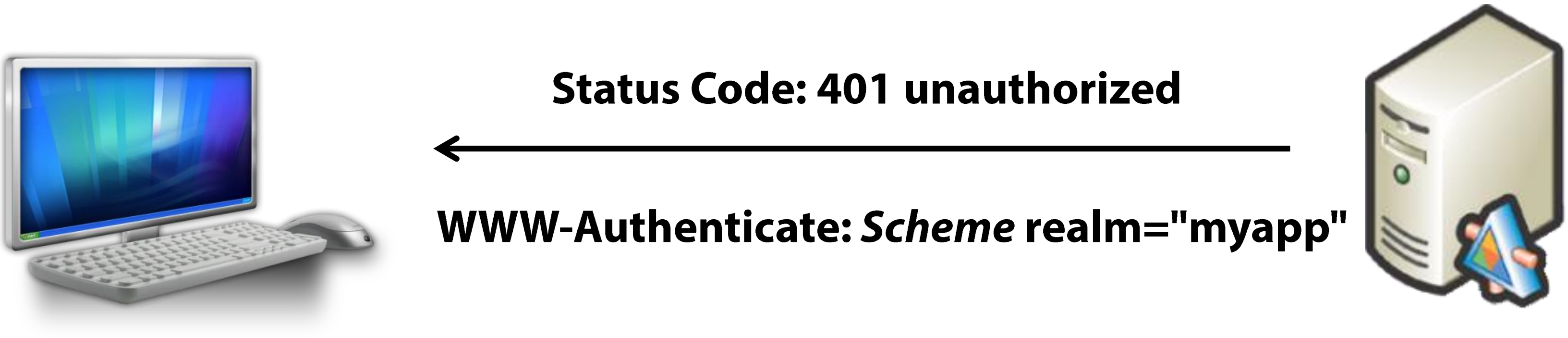
Skip decryption for the following hosts:

Export Root Certificate to Desktop
Remove Interception Certificates
Help

Note: Changes may not take effect until Fiddler is restarted.

HTTP Authentication Framework

- **Whenever authentication is required**
  - Status code of 401 indicates *unauthorized*
  - *WWW-Authenticate* response header indicates preferred authentication method

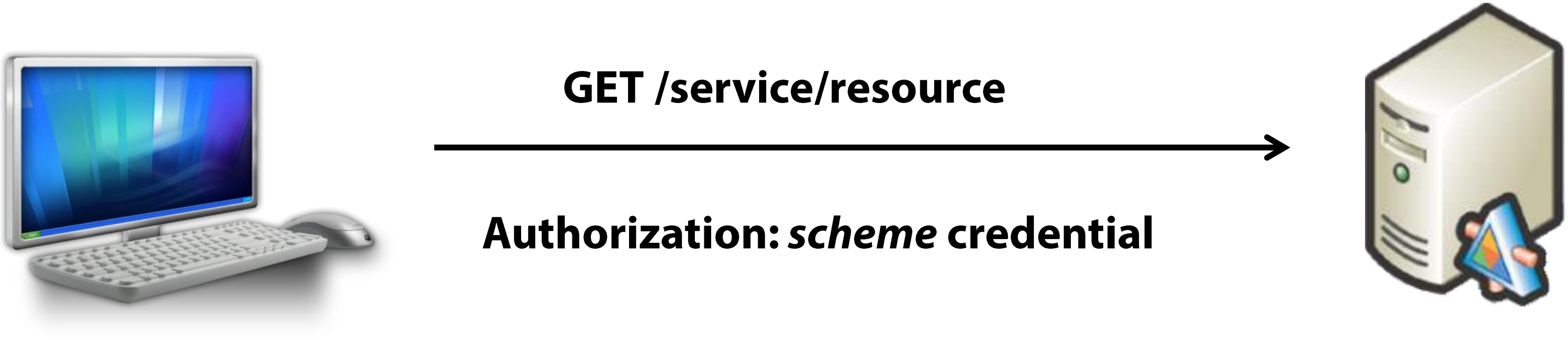


Status Code: 401 unauthorized

WWW-Authenticate: *Scheme* realm="myapp"

Authentication for HTTP-based services

- **Credentials transmitted (typically) via *Authorization* header**
  - e.g. Basic authentication, access tokens…
  - sometimes other means (query string, cookie…)



GET /service/resource

Authorization: *scheme* credential

Summary

- **HTTP has no transport security on its own**
  - SSL/TLS layer protects data on the wire
- **Every developer should understand how SSL/TLS works**
  - at least the simple rules
    - common name has to match DNS name
    - expiration
    - trusted root
  - don't disable SSL validation
- **HTTP authentication is simple**
  - challenge via status code 401 / WWW-authenticate header
  - send credentials via Authorization header

Resources

- **Thinktecture.IdentityModel**
  - https://github.com/thinktecture/Thinktecture.IdentityModel
- **HttpConfig**
  - http://www.stevestechspot.com/ABetterHttpcfg.aspx
- **Netsh documentation**
  - http://msdn.microsoft.com/en-us/library/windows/desktop/cc307236(v=vs.85).aspx
- **Fiddler**
  - http://www.telerik.com/download/fiddler

Resources II

- **PluralSight:**
  - HTTP Fundamentals - Scott Allen
  - Introduction to IIS Certificates - Paul Lemmers
  - IIS for Developers - Steven Evans