IBM ITSO Poughkeepsie
OS/390 in an e-business environment

Domino Go Webserver V5 SSL Client Authentication

Roland Trauner
trauner@us.ibm.com

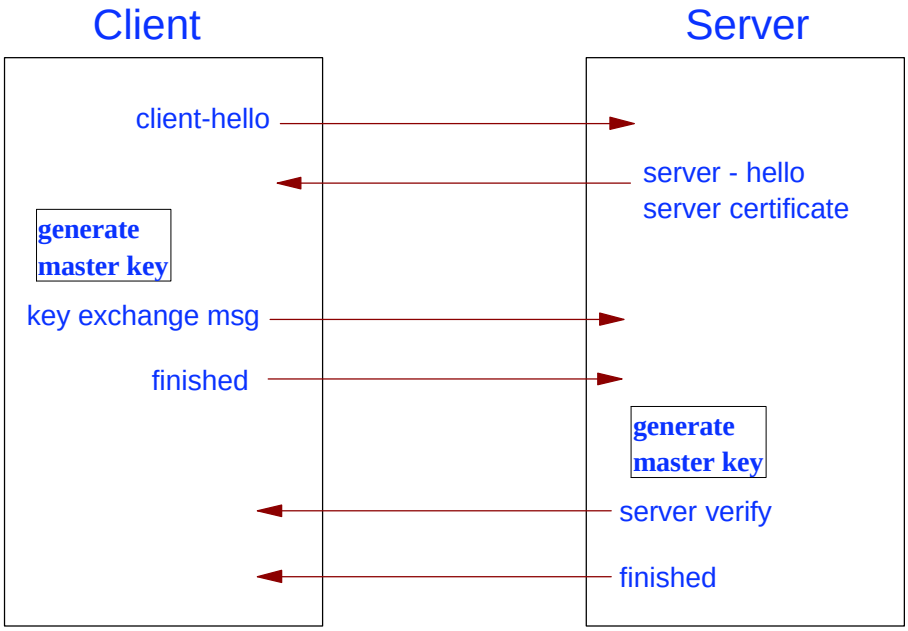
SSL Client Authentication

- **SSL allows encrypted communication with or without client authentication**
- **SSL client authentication requires the client to present a certificate**
- **DGW can be configured to require client authentication**
  - With client authentication, the server can control the access of resources by using the client certificate information instead of challenging for user ID/password.

Roland Trauner trauner@us.ibm.com

SSL Client Authentication

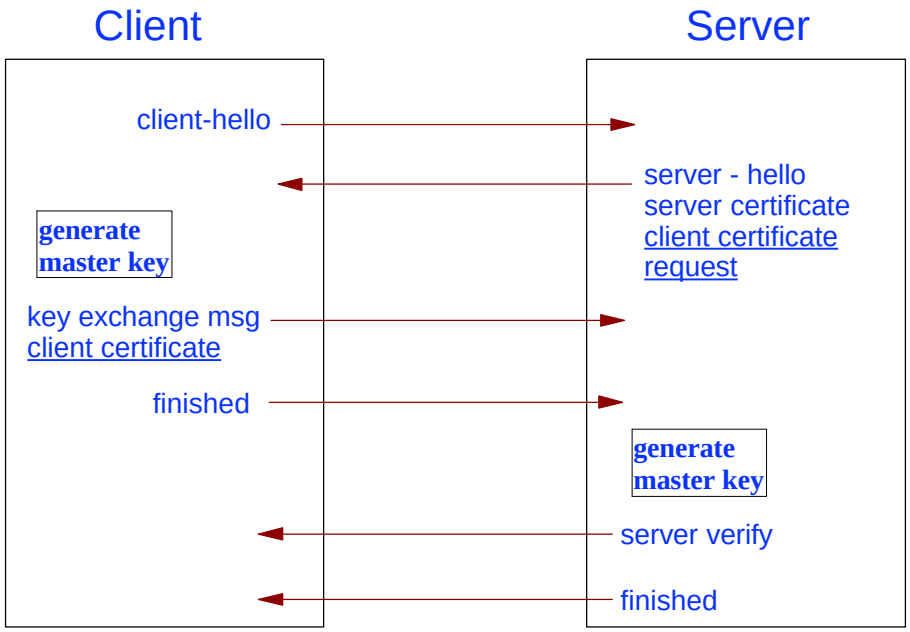
SSL handshake without client authentication



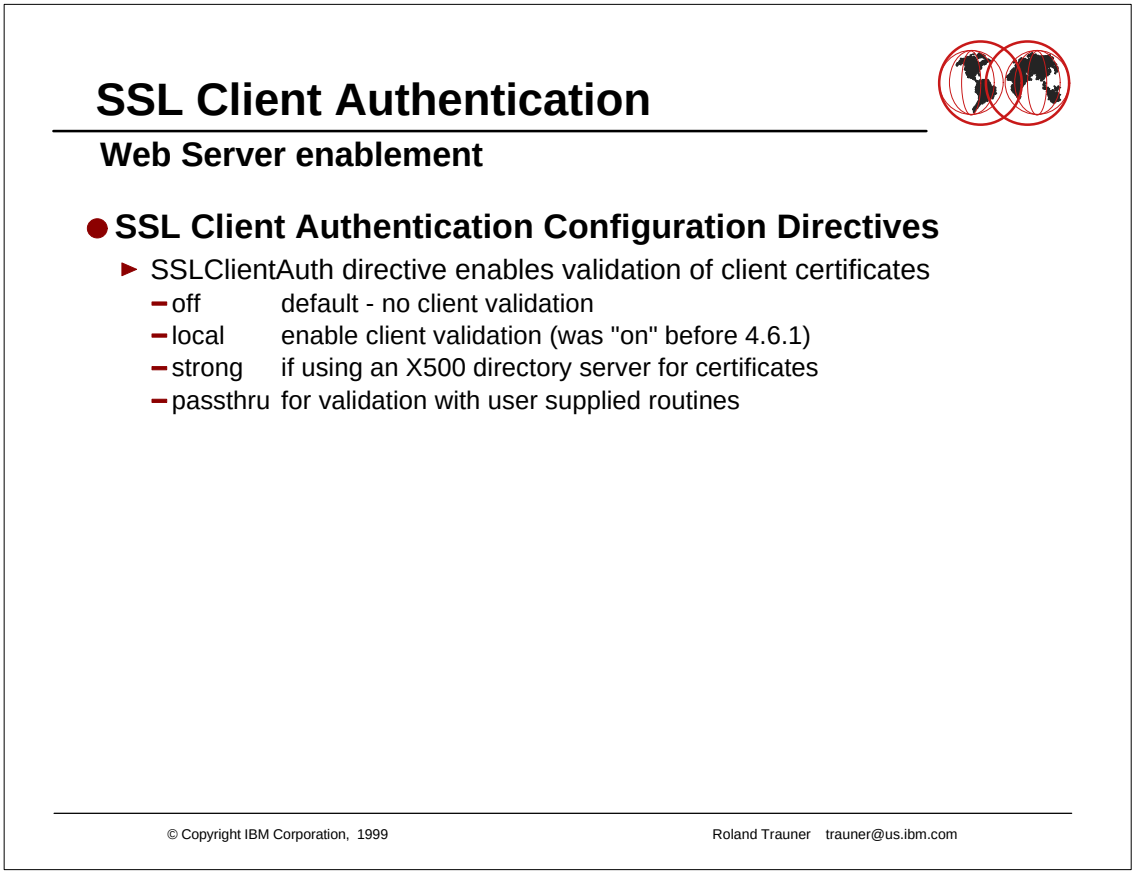
Roland Trauner trauner@us.ibm.com

SSL Client Authentication

SSL handshake with client authentication



Roland Trauner trauner@us.ibm.com



- passthru is the right spelling for the option - even if webmasters guide suggests passthrough

SSL Client Authentication

Web Server enablement

- **Protection based on client authentication**
  - The following protection directive can be used to protect a resource using certificate information

```
Protection Prot2 {
 ServerId           Candy_Prot_Test2
  AuthType           Basic
   CommonName         "Roland Trauner"
   Locality           "Internet"
   Organization       "VeriSign, Inc."
   OrgUnit            "Digital ID Class 1 - Netscape"
   IssuerLocality     "Internet"
   IssuerOrganization "VeriSign, Inc."
   IssuerOrgUnit      "VeriSign Class 1 CA - Individual Subscriber"
  Mask               anybody@*
}

Protect /sec2/*       Prot2
```


Roland Trauner trauner@us.ibm.com

SSL Client Authentication

Web Server enablement

- **Some Remarks:**
  - Caution:
    - If you set up a protection directive like the example and forget to define *SSLClientAuth on*, then the certificate related parameters (CommonName etc.) will be ignored and the access is simply granted by Mask anybody@*
    - Accessing the directory like the example above requires HTTPS protocol (SSL client certificates) .
    - If you don't use https, an error message will be delivered in the trace and 403 forbidden by role shows up.

Roland Trauner trauner@us.ibm.com

SSL Client Authentication

Web Server enablement

- **More Remarks:**
  - Browser Action:
    - When *SSLClientAuth=on* then the server requests a client certificate the first time the server will be accessed through SSL (https).
    - This requires a certificate grant action at the browser at the first time.

```
>> THE SITE .... requested client authentication
>> Here is the site's certificate
>> Select your certificate
```

    - The browser then keeps the status and issues the certificate every time it will be asked.
    - If one decided not to grant the certificate the first time, it is also denied every subseqent time.
    - This is configurable through browser parameters.

Roland Trauner trauner@us.ibm.com

SSL Client Authentication

Web Server enablement

- **More Remarks:**
  - DGW's vv trace shows the user certificate:

```
HTHandle.... Beginning SKREAD
HTSession... SSL server handshake complete
Client certificate data:
   Common Name = Roland Trauner
   Locality = Internet
   Organization = VeriSign, Inc.
   Organizational Unit = VeriSign Class 1 CA -
Individual Subscriber
   Issuer Locality = Internet
   Issuer Organization = VeriSign, Inc.
   Issuer Organizational Unit = VeriSign Class 1 CA -
Individual Subscriber
Keep-Alive.. Starting HTTPD 1.1 loop.
```


Roland Trauner trauner@us.ibm.com

SSL Client Authentication

Web Server enablement

- **Protection based on client certificates**
  - Possible since ICSS 2.2
  - Authentication process ran under the user ID defined by the UserID directive. The user ID was either a generic user ID *(PUBLIC)* or a user specified user ID *(%%CLIENT%%)*.
  - DGW 4.6.1 invented *%%CERTIF%%* and enabled the use of client certificates to set up the user ID the process should run under.
  - *%%CERTIF%%* forces RACF to compate the certificate with the certificate stored in the **CERTDATA** segment of the **DIGTCERT** RACF class.
    - RACF APAR OW26930 describes the details or look at SYS1.SAMPLIB(IRR26930 and IRR31933)

Roland Trauner trauner@us.ibm.com

SSL Client Authentication

RACF Digital Certificate Support

- **Enable RACF to handle certificates**
  - Enable the RACF DIGTCERT class
    - SETR CLASSACT(DIGTCERT) RACLIST(DIGTCERT)
  - Allow individual users to register a certificate with their own RACF user ID
    - RDEFINE FACILITY IRR.DIGTCERT UACC(NONE)
    - PERMIT IRR.DIGTCERT CLASS(FACILITY) ID(*) ACC(READ)
    - SETR RACLIST(FACILITY) REFRESH

Roland Trauner trauner@us.ibm.com

SSL Client Authentication

RACF Digital Certificate Support

- **Register a certificate using RACDCERT**
  - Obtain a client certificate from a CA in PKCS7 format.
  - Upload the certificate to an OS/390 PS dataset (FTP, binary)
    - DSORG=PS, RECFM=VB, LRECL=4096, BLKSIZE=27998
  - Register the certificate using the RACDCERT TSO command
    - RACDCERT ID(TRAUNER) ADD('TRAUNER.CERT.P7C') TRUST
- **Use %%CERTIF%%**
  - Define UserID %%CERTIF%% and SSLClientAuth local
    - The referring userid is now set when a registered certificate is presented.
    - If no certificate or no valid certificate is presented, %%CERTIF%% acts like %%CLIENT%% and asks for user ID and password.

Roland Trauner trauner@us.ibm.com

- See SG24-5158 Ready for e-business: OS/390 Security Server Enhancements

SSL Client Authentication

RACF Digital Certificate Support

- **RACF AutoRegistration Web Application**
  - Instead of registering the certificates in TSO, the RACF AutoRegistration Web Application can be used.
  - Is is shipped as a PTF since OS/390 R5 or can be obtained via FTP from: ftp://www.redbooks.ibm.com/redbooks/SG245158
  - It contains three html pages and one REXX registration clist
  - Enables to register user certificates with OS/390 through the web interface
    - requires a browser and DGW 4.6.1 or higher running on OS/390 R5 or higher

Roland Trauner trauner@us.ibm.com