Sutol Czech Lotus User Group

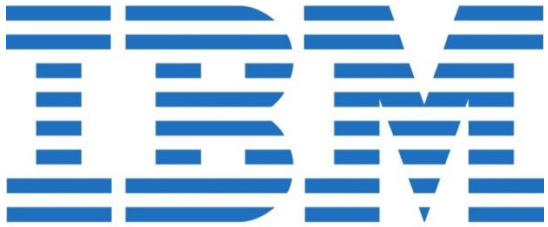
Howto: Secure your IBM Traveler for 2017

Aleš Lichtenberg – KAISER DATA

SUTOL Conference2016

November 10-11, Prague

Thanks to our sponsors!



IMPORTANT

You must

ensure that your

IBM Verse Mobile and Traveler connections are secure and compliant with these requirements by

January 1, 2017

Mandatory requirements

- Mobile apps must connect only using HTTPS and not the unsecure HTTP protocol
- The server certificate must not be expired or invalid
- The leaf certificate hashing algorithm must be Secure Hash Algorithm 2 (SHA-2) with a digest length of at least 256 (SHA-256 or greater).

Mandatory requirements

- The negotiated Transport Layer Security version must be TLS 1.2. Since devices running Android prior to version 4.1 do not support TLS 1.2, they can no longer be supported

- The server certificate common name (CN)or a name from the server certificate's Subject Alternate Name (SAN) list must match the host name of the server with which the client is connecting

Mandatory requirements

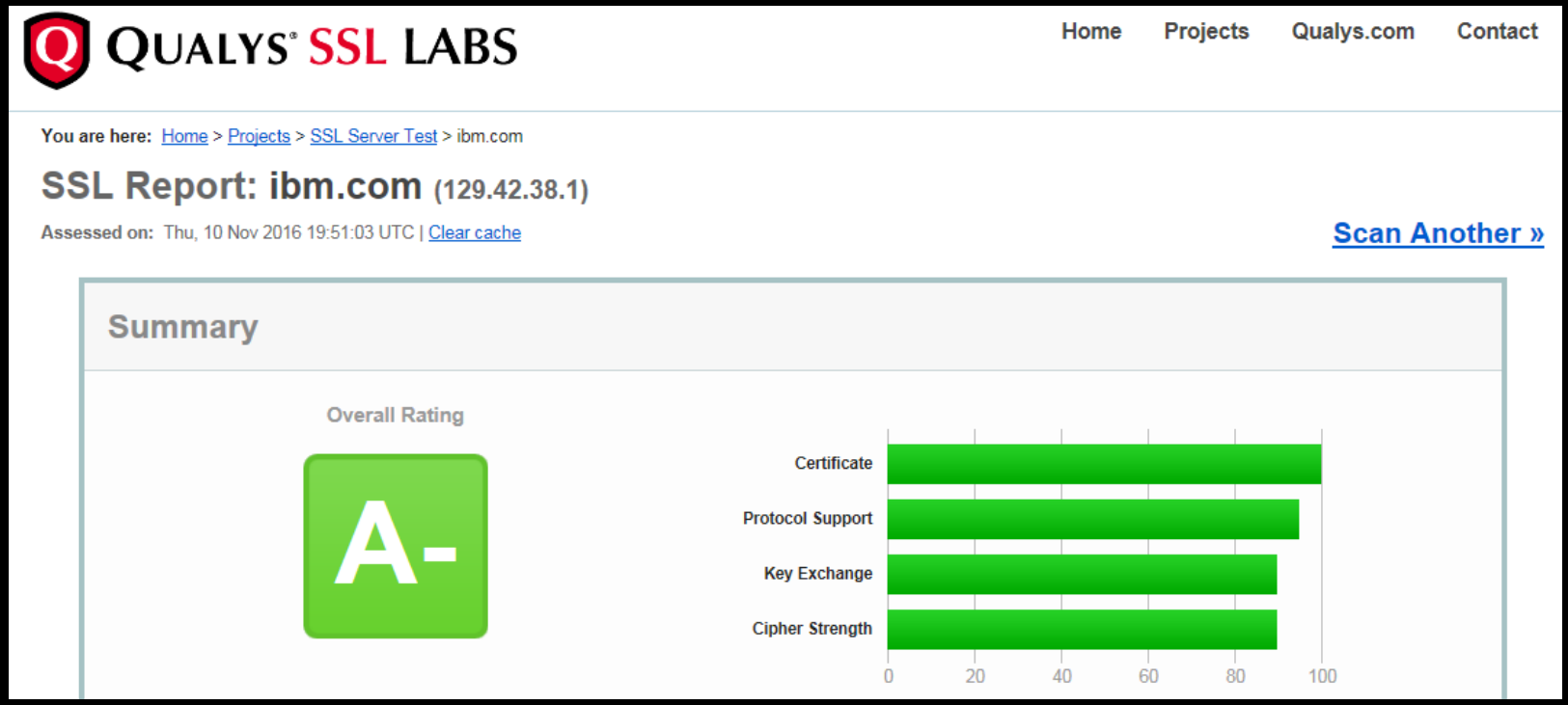
- The server certificate must be trusted and either issued by a certificate authority (CA) whose root certificate is incorporated into the device operating system or is a trusted root CA that has been installed by the user or a system administrator on the device

- The negotiated TLS connections cipher suite must support forward secrecy

HOWTO

Test your server

- https://www.ssllabs.com/



Howto…

- Creating Self-signed SHA-2 4096 SSL Certificates for Domino using OpenSSL
- **Create a Self-Signed Certificate**
- Create a new keyring file using kyrtool
- Configuration Domino server

Creating SHA-2 4096 SSL Certificates for Domino

- Running Domino 9.0.1 Fix Pack 5 or later
- **Download** the latest version of OpenSSL (**http://tinyurl.com/qccn8fc**)
  - you install it in C: \ OpenSSL example
- **Download** the kyrtool and copy the executable to your Notes program directory (**http://tinyurl.com/horaxb2**)

Generating a keyring file with a self-signed SHA-2 cert using OpenSSL and kyrtool

- Generate an RSA keypair

openssl genrsa -out server.key 4096

```
.+.....+.
OpenSSL> genrsa -out server.key 4096
Loading 'screen' into random state - done
Generating RSA private key, 4096 bit long modulus
.....................++
.................++
e is 65537 (0x10001)
OpenSSL> _
```

Generate a Certificate Signing Request (CSR)

openssl req -new -sha256 -key server.key -out server.csr

```
OpenSSL> req -new -sha256 -key server.key -out server.csr
Loading 'screen' into random state - done
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:CZ
State or Province Name (full name) [Some-State]:Czech republic
Locality Name (eg, city) []:Prague
Organization Name (eg, company) [Internet Widgits Pty Ltd]:SUTOL
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:traveler.sutol.cz
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
OpenSSL> _
```

Create a Self-Signed Certificate

openssl x509 -req -days 3650 -sha256 -in server.csr -signkey server.key -out server.pem

```
Signature ok
subject=/C=CZ/ST=Czech republic/L=Prague/O=SUTOL/CN=traveler.sutol.cz
Getting Private key
```

Create a new keyring file

kyrtool =c:\lotus\notes\notes.ini create -k c:\lotus\notes\data\keyring_traveler.kyr -p password

```
C:\Lotus\Notes>kyrtool =c:\lotus\notes\notes.ini create -k c:\lotus\notes\data\k
eyring_traveler.kyr -p password

Keyfile c:\lotus\notes\data\keyring_traveler.kyr created successfully
```

Import the RSA keypair and self-signed certificate into the new keyring file

- **Concatenate server.key and server.pem into a single file:** [C:\Openssl] cat server.txt

```
-----BEGIN RSA PRIVATE KEY-----
MIIJKAIBAAKCAgEAr9uZYZ1BrraxW1AdM1ecexiD2uaPxNKjS2p2p9pygUc/vU2d
rrqjj3tAybdkNEFcwQLY/eIZcEowHmhH0b9Ut5EOsMMxkB4vUHg6gWmse64wr2qx
[Many lines removed]
7Rw9zpLxTJmbd3iWW3+ZVHhpudYZrDE8NbaaiGMbfyfQBnSH1XbDHSveTxLOY3fo
+d91ePMThdnmme6b1v8X4sCuDKrFjoV5Veo4Qq8I+099hu3tTRq2zGpNPsg=
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIEyjCCArICCQDa3d9OQUIsWzANBgkqhkiG9w0BAQsFADAnMSUwIwYDVQQDDBx1
bHRyYXZpb2xldC5zd2cudXNtYS5pYm0uY29tMB4XDTE0MTAwODE4MzQ0N1oXDTI0
[Many lines removed]
qddsfWubEwoMYKevnV8u9EFp7f0RONGqp93iU9O5jYPdrcB+RryT7bwErDTQKjua
ZAcuoKnUrnXiGIiq/dkXg2Umaf9Quewz0ow7BrCW
-----END CERTIFICATE-----
```

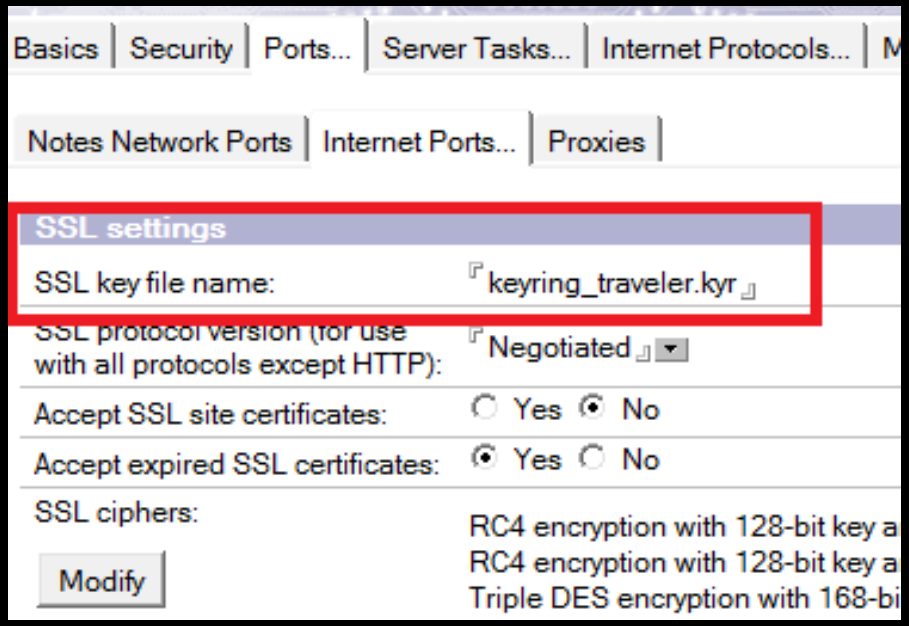
Import the keypair and self-signed certificate

kyrtool =c:\lotus\notes\notes.ini import all -k c:\lotus\notes\data\keyring_traveler.kyr -i c:\OpenSSL\server.txt

```
Using keyring path 'c:\lotus\notes\data\keyring_traveler.kyr'
Successfully read 4096 bit RSA private key
SECIssUpdateKeyringPrivateKey succeeded
SECIssUpdateKeyringLeafCert succeeded
```

Configuration Domino server

- Copy over your new keyring file to Data directory (keyring_traveler.kyr and keyring_traveler.sth)
- Settings: Server documents\Ports\Internet Ports
- Restart http task



THANK YOU ....

Aleš Lichtenberg

KAISER DATA s.r.o.
www.kaiser.cz
a.lichtenberg@kaiser.cz