Terravis - Hinweise zur Implementierung der SSL-Verbindung

Version: 1.0
Datum: 19.04.2013
Autoren: Claude Eisenhut

Verzeichnis:

Einführung

Das folgende Dokument gibt Hinweise zur Implementierung der 2way-SSL Verbindung zwischen Teilenehmer-System (Bank oder Grundbuch) und Terravis. Es geht um die Maschine-zu-Maschine Verbindung. Die Authentisierung des einzelnen Benutzers im Terravis-Portal ist nicht Gegenstand des vorliegenden Dokumentes.
Massgebend ist aber das Dokument "Sicherheitsleitfaden für die Integration in Terravis".

Kontaktpersonen

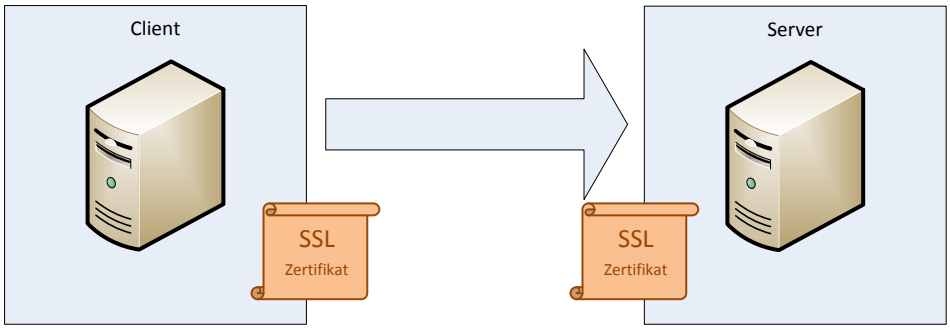
Für den Austausch der Zertifikate:
Christoph Widmer, christoph.widmer@six-group.com

Für technische Unterstützung:
Die für den Teilnehmer technische Ansprechsperson (Daniel Lübke, Christian Scheidegger oder Claude Eisenhut).
Für Unterstützung benötigen wir die Log-Datei des fehlgeschlagenen SSL-Verbindungsaufbaus inkl. Zeitangaben (s. Abschnitt Fehlersuche) und ein Dump des Keystores und des Truststores.

Allgemeines

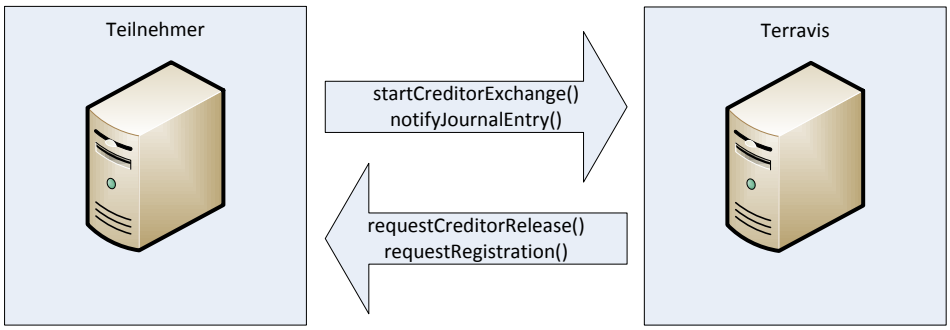
2way-SSL

Bei einer 2way-SSL Verbindung haben beide beteiligten Systeme (Client und Server) ein Zertifikat (Bei einer einfachen SSL Verbindung hat nur der Server ein Zertifikat).



Eine 2way-SSL Verbindung verschlüsselt die Kommunikation und erlaubt dem Server den Client zu authentisieren und erlaubt umgekehrt auch dem Client den Server zu authentisieren.
Das Zertifikat des Teilnehmer-Systems wird wie folgt verwendet:

1. Client-Zertifikat, wobei Terravis als Server und das Teilnehmer-System als Client agiert.
2. Server-Zertifikat, wobei Terravis als Client und das Teilnehmer-System als Server agiert.

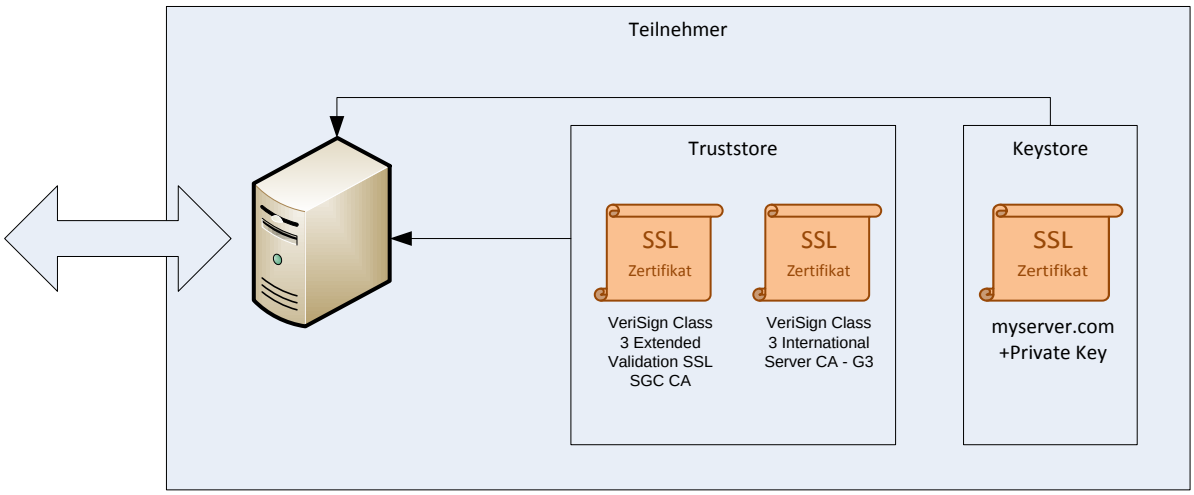


Zertifikate

Public-Key-Zertifikate sind ein Element einer PKI (Public-Key-Infrastructure). Jedes digitale Zertifikat - ganz gleich ob personen- oder organisationsbezogen - ist mit einem öffentlichen Schlüssel (public key) verknüpft, dem ein privater Schlüssel (private key) zugeordnet ist. Diesen privaten Schlüssel besitzt nur der Zertifikatsinhaber. Das Zertifikat, das den öffentlichen Schlüssel enthält, kann hingegen jedem zugänglich gemacht werden, der mit dem Inhaber eines Zertifikats sicher kommunizieren möchte. Jedes Zertifikat ist nur bis zu einem bestimmten Ablaufdatum gültig, und muss danach erneuert werden.
Die Zuordnung des öffentlichen Schlüssels mit einer Person oder Organisation, wird von einer Zertifizierungsstelle (CA, Certificate Authority) beglaubigt, indem sie das Zertifikat mit ihrer eigenen digitalen Unterschrift versieht.
Im Kontext von Terravis werden verschiedene Arten von Zertifikaten verwendet:

- Zertifikat für eine rechtsgültige Unterschrift (SuisseId QC)
- Zertifikat für Login im Terravis-Portal (SuisseId IAC)
- Zertifikat für Integration via Web-Service (SSL-Zertifikate)

Es gibt verschiedene Arten von SSL-Zertifikaten. Diese unterscheiden sich dadurch, welche Art von Prüfung der Zertifikatsherausgeber vornimmt (z.B. ob die Firma, die das Zertifikat beantragt, im Handelsregister eingetragen ist).
Ein wichtiges Element eines SSL-Zertifikats ist der CN (Common Namen) des Zertifikatinhabers. Dieser muss bei einem SSL-Zertifikat der Domain-Name des Systems sein (z.B. für https://test.terravis.ch ist der CN "test.terravis.ch").
Die privaten Schlüssel und zugehörigen Zertifikate werden typischerweise in einem Keystore gespeichert.
Die Zertifikate der Kommunikationspartner oder der Zertifikatausgabestellen denen man vertraut werden typischerweise in einem Truststore gespeichert.

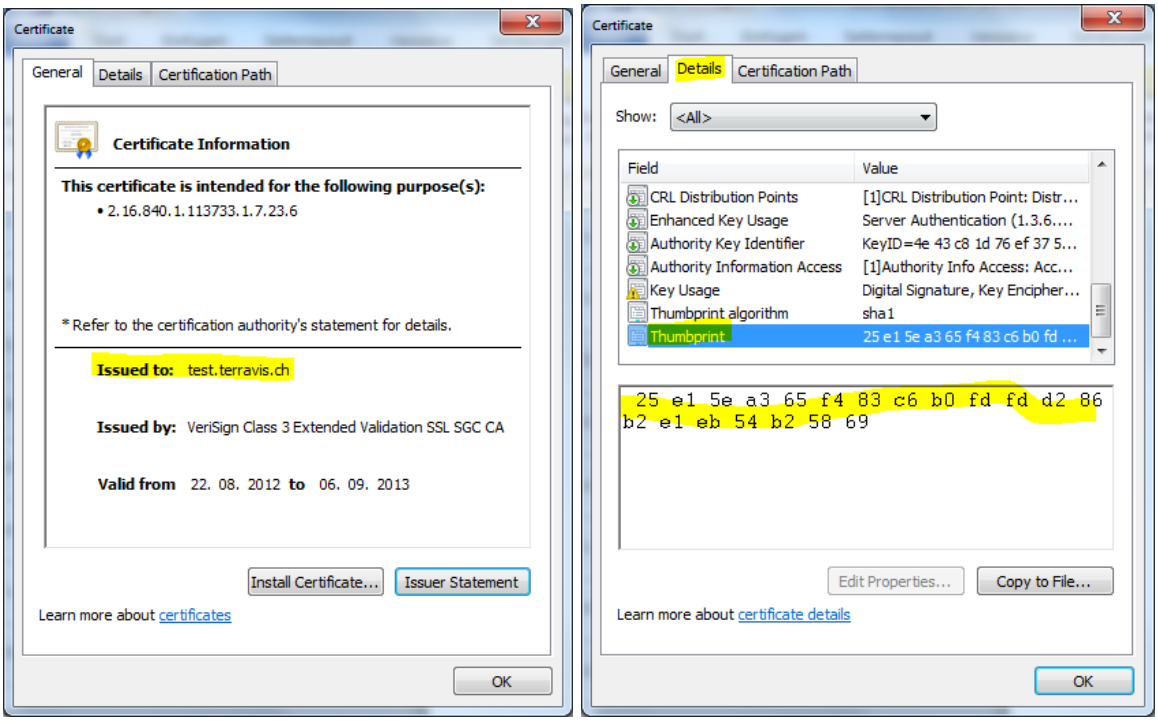


Austausch der Zertifikate

Nach dem Austausch der Zertifikate, müssen diese verifiziert werden. Um das Zertifikat zu verifizieren, muss der folgende Wert telefonisch verglichen werden[1]:

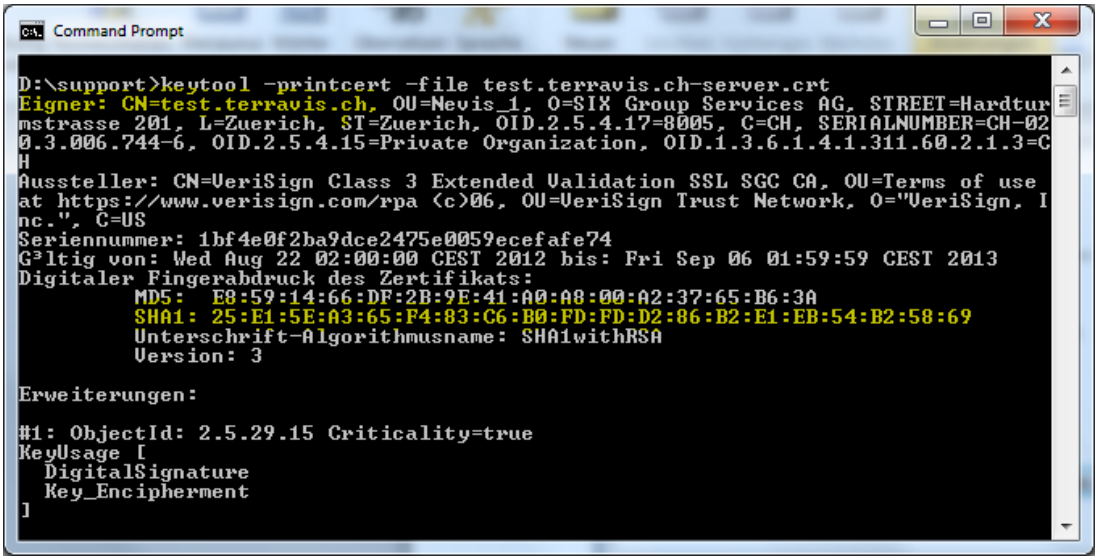
- CN des Inhabers
- Fingerprint/Hash des Zertifikats

Unter Windows können Zertifikate (Dateien mit der Endung .crt oder .cer) mit dem Explorer geöffnet/angesehen werden.



[1] Kontaktperson am Anfang des Dokumentes

Auf der Kommandozeile kann das Zertifikat mit keytool angesehen werden (Teil der JAVA-Umgebung oder openssl):



Hinweise zum Zertifikat des Teilnehmers

Es werden keine self-signed Zertifikate akzeptiert.
Es werden alle bekannten Zertifikat-Herausgeber akzeptiert wie z.B. VeriSign, Thawte, GoDaddy, SuisseSign, QuoVadis. Die genaue Liste der akzeptierten Herausgeber (CA) kann bei Terravis bezogen werden. Zu beachten ist, insbesondere bei Zertifikatsketten (certificate chain), dass das Zertifikat der letzten Herausgeber-Stelle in der Kette massgebend ist (z.B. "VeriSign Class 3 International Server CA - G3"), und nicht ein davor liegendes ("VeriSign Class 3 Public Primary Certification Authority - G5") und auch nicht die Firma ("VeriSign").
Es werden alle Arten von SSL-Zertifikaten akzeptiert (z.B. Domainvalidiert oder EV).
Als CN des Zertifikats muss der Domain-Name des Teilnehmer-Systems verwendet werden (z.B. für https://test.terravis.ch ist der CN "test.terravis.ch").

Hinweise zum Zertifikat von Terravis

Für von Terravis ausgehende Verbindungen verwendet Terravis ein Zertifikat mit dem CN "test.terravis.six-group.com". Das Zertifikat des Herausgebers hat als CN "VeriSign Class 3 International Server CA - G3"[2].
Für eingehende Verbidungen verwendet Terravis ein Zertifikat mit dem CN "test.terravis.ch". Das Zertifikat des Herausgebers hat als CN "VeriSign Class 3 Extended Validation SSL SGC CA".
Obwohl beides VeriSign Zertifikate sind, ist das Herausgeber-Zertifikat nicht identisch. Es muss darum das jeweils richtige in den jeweiligen Truststore des Teilnehmers aufgenommen werden.

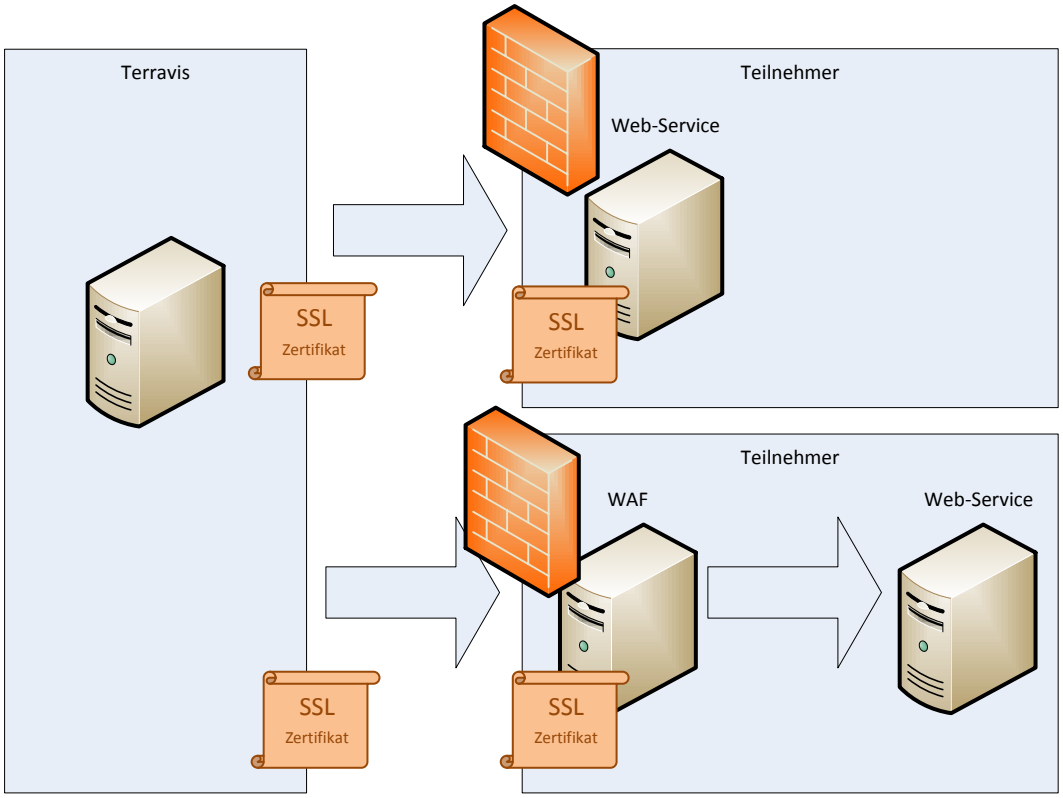
[2] https://www.verisign.com/support/roots.html

Implementierung beim Teilnehmer

Es muss definiert werden, wo die SSL-Verbindung beim Teilnehmer terminiert wird. Das ist in der Regel abhängig von den Vorgaben im jeweiligen Unternehmen bzw. Kanton. Grob kann man zwei Varianten unterscheiden:

- beim Web-Service
- bei einem vorgelagerten System (Web Application Firewall (WAF)[3])

In beiden Fällen muss darauf geachtet werden, dass allfällig vorgelagerte Netzwerk-Firewalls (Hard- und Software) die Verbindung zulassen.



Im Fall des Einsatzes eines vorgelagerten Systems (WAF), ist die sichere Verbindung zwischen WAF und Web-Services in der Verantwortung des Teilnehmers.

Hinweise zur Implementierung mit JAVA

Für die Implementierung mit JAVA muss mindestens JAVA Version 6 Update 22 verwendet werden.

Um bei fehlerhaftem SSL-Verbindungsaufbau weitere Informationen im Log zu erhalten, kann die Option `-Djavax.net.debug=all` benutzt werden. Um bei fehlerhaftem SSL-Verbindungsaufbau Hilfestellung durch Terravis zu erhalten, sind dies Log-Informationen bereitzuhalten.
Um den Inhalt eines Zertifikates anzuzeigen, kann der folgende Befehl verwendet werden:

```
keytool -printcert -file mycertificate.crt
```

[3] https://www.owasp.org/index.php/Category:OWASP_Best_Practices:_Use_of_Web_Application_Firewalls

Um den Inhalt eines Keystores oder Truststores anzuzeigen, kann der folgende Befehl verwendet werden:

```
keytool -v -list -keystore mystore.jks
```

Um ein Zertifikat inkl. Private-Key zu exportieren, kann der folgende Befehl verwendet werden:

```
keytool -srcalias mycertalias -importkeystore -srckeystore
existing-store.jks -destkeystore export.p12 -deststoretype PKCS12
```

Fehlersuche

Als erstes sollte geprüft werden, ob die Verbindung zum Zielsystem grundsätzlich hergestellt werden kann (ob also z.B. alle Firewalls die entsprechende Verbindung zu lassen). Das kann z.B. mit telnet geprüft werden (443 ist der Standardport für das https Protokoll):

```
telnet -p 443 test.terravis.ch
```

Die Verbindung wird durch den Server sofort wieder geschlossen. Falls die Verbindung nicht geöffnet werden kann, sieht man eine Fehlermeldung.
Dann sollten die Zertifikate geprüft werden (CN des Inhabers, CN des Herausgeber, Fingerprint/Hash des Zertifikats, Gültig-von, Gültig-bis). Unter Windows können Zertifikate (Dateien mit der Endung .crt oder .cer) mit dem Explorer geöffnet/angesehen werden (auf der Kommandozeile mit keytool oder openssl).

```
openssl x509 -text -in cert.crt
```

Dann sollte der Inhalt des Keystores geprüft werden. Ist darin das eigene Zertifikat inkl. Private-Key vorhanden?
Dann sollte der Inhalt des Truststores geprüft werden. Sind darin alle Zertifikate der Herausgeber der Zertifikate von Terravis vorhanden?
Dann sollte für den SSL-Verbindungsaufbau ein Log erstellt und geprüft werden. Die Log-Datei kann mit openssl erstellt werden:

```
openssl s_client -msg -connect test.terravis.ch:443 -cert
cert.pem
```

(Das kann i.d.R. auch durch eine entsprechende Einstellung beim Starten des Web-Services erreicht werden (JAVA: `-Djavax.net.debug=all`).)
Um das PKCS12-Dateiformat in das PEM-Format umzuwandeln, kann das folgende Kommando verwendet werden.

```
openssl pkcs12 -in ix.ehi.ch.p12 -out ix.ehi.ch.pem
```