E-ConsentPro

HTTPS-Verbindung einrichten

Zielsetzung des Dokuments

Dieses Dokument soll Sie bei der Entscheidung unterstützen, ob HTTPS eingesetzt werden sollte oder nicht. Es erläutert zudem, welche Zertifikate für welchen Einsatzzweck genutzt werden können und welche Anpassungen gegebenenfalls nötig sind.

Wir setzen beim Einsatz von Zertifikaten voraus, dass Sie als IT-Administrator

- selbstständig auf die Laufzeiten von Zertifikaten achten und sich rechtzeitig um den nötigen Ersatz kümmern,
- Zertifikate selbstständig in Ihrer Umgebung verwalten und auf allen Geräten installieren, die Zugriff auf die Anwendung erhalten sollen.

Weshalb HTTPS?

Für eine sichere und datenschutzkonforme Kommunikation zwischen Server und Clients wird grundsätzlich die Kommunikation über eine HTTPS-Verbindung empfohlen.

Um diese Sicherheit auch für den digitalen Prozess der Patientenaufklärung zu gewährleisten, unterstützt E-ConsentPro die Kommunikation über eine HTTPS-Verbindung unter Verwendung von TLS 1.0–1.2.

Im Folgenden wird erklärt, wie Sie eine sichere Verbindung zwischen dem E-ConsentPro Server und den Client-Geräten einrichten können. Das Dokument erklärt nur die Einrichtung für das Produkt E-ConsentPro WebClient, das auf einem Apache Tomcat Server basiert.

Erläuterung aus Sicht des Datenschutz

Verbindungen im Internet sollten grundsätzlich verschlüsselt übertragen werden. Besonderes Augenmerk sollten Sie darauf richten, wenn Sie personenbezogene Daten wie Patientendaten in E-ConsentPro eingeben und standortübergreifend in Ihrem Netzwerk oder über das Internet versenden.

Thieme Compliance

Unterstützte Verfahren

In **E-ConsentPro Classic** (ohne digitalen Workflow) können Sie eine verschlüsselte Übertragung wie folgt umsetzen:

- Mit dem von Thieme Compliance zur Verfügung gestellten Zertifikat.
- Mit einem von einer öffentlichen, autorisierten Zertifizierungsstelle wie VeriSign erworbenen Zertifikat.
- Mit einem selbstsignierten Zertifikat. Vor der eigenverantwortlichen Umsetzung empfehlen wir Ihnen, sich mit dieser Lösung technisch auseinanderzusetzen und entsprechende Ressourcen einzuplanen.

In **E-ConsentPro mobile** (inklusive mobiler Workflow) können Sie eine verschlüsselte Übertragung wie folgt umsetzen:

- Mit dem von Thieme Compliance zur Verfügung gestellten Zertifikat.
- Mit einem von einer öffentlichen, autorisierten Zertifizierungsstelle wie VeriSign erworbenen Zertifikat.

Hinweis: Aufgrund des Einsatzes der Apps (iOS und Android) kann kein selbstsigniertes Zertifikat verwendet werden. Durch die hohen Sicherheitsanforderungen und fest eingebetteten Vertrauensstellen müssen die Zertifikate von einer autorisierten Zertifizierungsstelle wie VeriSign ausgestellt sein.

Entscheidungshilfe – wann HTTPS verwenden?

Wir empfehlen HTTPS für Kunden, die Patientendaten über nicht zusätzlich gesicherte, standortübergreifende Installationen übertragen.

Bedenken Sie vor der Entscheidung, dass die Verwendung von HTTPS einen Mehraufwand erfordert. Sie müssen eine regelmäßige Kontrolle und Aktualisierung von Zertifikaten einplanen, da diese ab Erstellung ein Verfallsdatum enthalten.

Falls Sie HTTPS verwenden wollen, müssen Sie im Vorfeld klären, welches Zertifikat in Ihrem Netzwerk installiert werden kann. Stellen Sie sicher, dass am Installationsort eine feste IP-Adresse zugewiesen wurde.

Notwendige Schritte für HTTPS

Um HTTPS verwenden zu können, führen Sie nach einer Update- oder Komplettinstallation die folgenden Schritte aus.

Hinweis:

- Verwenden Sie für den URL-Aufruf via HTTPS den Hostnamen oder die IP-Adresse, die Sie während der Installation angegeben haben.
- Für Nutzer von E-ConsentPro mobile mit Android-Geräten: Nutzen Sie ausschließlich die IP-Adresse. Ein Aufruf der Apps unter Android ist mit Hostnamen nicht möglich.

Schritt 1 – Zertifikat an den Anwender-PCs importieren:

Um das Zertifikat in Ihrem Netzwerk zu verteilen, nutzen Sie Ihre übliche Vorgehensweise.

Für einen Test mit dem von Thieme Compliance angeforderten Zertifikat können Sie beispielsweise wie folgt vorgehen:

Importieren Sie die Zertifikatsdatei `cacert.pem`, die Sie von Thieme Compliance per E-Mail erhalten, in den Browser.

- **Internet Explorer**: Der Internet Explorer verwenden die Zertifikatsverwaltung von Windows. Importieren Sie das Zertifikat daher in die Windows-Zertifikatsverwaltung (Systemsteuerung oder im Internet Explorer **Extras** > **Internetoptionen** > **Inhalte** > **Zertifikate** > **Vertrauenswürdige Stammzertifizierungsstellen** > **Importieren**).
- **Firefox**: Firefox verwendet nicht die Zertifikatsverwaltung von Windows, sondern nutzt einen eigenen Zertifikatspeicher. Importieren Sie das Zertifikat daher in den Zertifikate-Manager von Firefox (**Menü** > **Einstellungen** > **Erweitert** > **Zertifikate** > **Zertifikate anzeigen** > **Importieren**).

Schritt 2 – Firewall-Regeln hinzufügen:

Für eine HTTPS-Verbindung auf den E-Consent Pro-Server müssen Sie eine eingehende Regel für den Port in der Firewall konfigurieren:

Windows Firewall > **Eingehende Regeln** > **Neue Regel** > **„Regeltyp“**: **Port > TCP**, **„Bestimmte lokale Ports“**: **8445** > **Verbindung zulassen** > **„Wann wird diese Regel angewendet?“: Domäne > „Name“ / „Beschreibung“**

Hinweis:

- Tragen Sie statt 8445 den von Ihnen bei der Installation angegebenen Port ein.
- Wenn Sie neben HTTPS- auch HTTP-Verbindungen zulassen wollen, müssen Sie beide eingehende Regeln konfigurieren und aktivieren.

Schritt 3 – Verbindung in den Apps ändern:

Passen Sie die Verbindung der Apps „Anamnese mobil“ und „Aufklärung mobil“ zum Server an:

1. Stellen Sie das mobile Endgerät wie folgt ein:
    - **iOS**: Aktivieren Sie in den Einstellungen der App die Option **E-ConsentPro Server** – **Beim nächsten Start konfigurieren**.
    - **Android**: Leeren Sie den Cache.
2. Öffnen Sie die App und speichern Sie die neue URL.
3. Wenn Sie die App anschließend erneut öffnen, verbindet sie sich wieder automatisch mit dem E-ConsentPro-Server, ohne die URL abzufragen.

Schritt 4 – KIS-Aufruf anpassen:

Informationen über die Anpassung im Krankenhaus-Informationssystem (KIS) finden Sie in Ihrem KIS-Handbuch oder erhalten Sie vom Hersteller der KIS-Software.

Anhang: Ein von einer offiziellen Zertifizierungsstelle erworbenes Zertifikat einbinden

Vorgehensweise:

1. Beschaffen Sie für den E-ConsentPro-Server ein SSL-/TLS-Zertifikat, das von einer offiziellen Zertifizierungsstelle ausgestellt ist.
2. Installieren Sie OpenSSL und gegebenenfalls nötige Zusatzkomponenten, um einen Keystore zu generieren.
3. Generieren Sie ein Zertifikat anhand des nachfolgenden Beispiels. Erstellen Sie einen Keystore mit OpenSSL. Verwenden Sie hierzu das bereits vorhandene Zertifikat sowie einen privaten Schlüssel:

```
openssl pkcs12 -export -name tomcat -in example.com.crt
-inkey example.com.key.pem -out ecp.keystore.p12

Enter Export Password: MYPASSWORD

Verifying - Enter Export Password: MYPASSWORD
```

Informationen zu den Parametern:

- `example.com.crt`

  Geben Sie Ihr SSL-/TLS-Zertifikat an.

- `example.com.key.pem`

  Geben Sie Ihren privaten Schlüssel an.

- `ecp.keystore.p12`

  Keystore-Datei.

- `MYPASSWORD`

  Geben Sie Ihr eigenes Passwort an. Das Passwort dient zum Schutz des Keystore.

4. Falls Sie E-ConsentPro **nicht** mit der Option HTTPS installiert hatten, führen Sie das Installationsprogramm (ab Version 2.6) aus.

   Wenn Sie das Installationsprogramm ausführen, werden die relevanten Konfigurationsdateien (`adapter.ini`, `config.ini` und `server.xml`) automatisch für HTTPS konfiguriert.

5. Stoppen Sie den Dienst **E-ConsentPro** in der Windows Diensteverwaltung.

6. Passen Sie die Konfiguration des E-ConsentPro Servers (Apache Tomcat) wie folgt an:

    a) Ersetzen Sie die Keystore-Datei im Ordner `C:\E-ConsentPro\tomcat\conf\ecp.keystore.p12` durch Ihre eigene.

    b) Öffnen Sie im Ordner `C:\E-ConsentPro\tomcat\conf` die Datei `server.xml`.

    c) Passen Sie die Datei `server.xml` an Ihr eigenes Zertifikat an und fügen Sie die SSL-Verbindungsparameter hinzu.

```
<Connector protocol="org.apache.coyote.http11.Http11NioProtocol"
port="443"
SSLEnabled="true"
maxThreads="200"
scheme="https"
secure="true"
keystoreFile="${catalina.home}/conf/ecp.keystore.p12"
keystorePass="MYPASSWORD"
keyAlias="tomcat"
keystoreType="PKCS12"
clientAuth="false"
URIEncoding="UTF-8"
useServerCipherSuitesOrder="true"
ciphers="TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384,
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384,
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256, 4
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA,
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA,
TLS_DHE_DSS_WITH_AES_256_CBC_SHA,
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256,
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA,
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA,
TLS_ECDHE_ECDSA_WITH_RC4_128_SHA,
TLS_ECDH_ECDSA_WITH_RC4_128_SHA,
TLS_ECDH_RSA_WITH_RC4_128_SHA,
```

```
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
TLS_RSA_WITH_AES_256_GCM_SHA384,
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384,
TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384,
TLS_DHE_DSS_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
TLS_RSA_WITH_AES_128_GCM_SHA256,
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256,
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256,
TLS_DHE_DSS_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA,
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA,
TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA,
TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA,
TLS_EMPTY_RENEGOTIATION_INFO_SCSVF
"/>
```

Achtung:

- Stellen Sie sicher, dass `keystorePass` ihr Keystore-Passwort enthält.
- Falls Sie das `URlEncoding` zuvor geändert hatten, passen Sie den benötigten Wert wieder an, siehe `server.xml.bak`.

7. Starten Sie den Dienst **E-ConsentPro** in der Windows Diensteverwaltung neu, damit die Änderungen wirksam werden.

06/2018

Thieme Compliance GmbH
Am Weichselgarten 30a · 91058 Erlangen
www.thieme-compliance.de

Tel.: +49 9131 93406-40
Fax: +49 9131 93406-70
E-Mail: support@thieme-compliance.de

Thieme Compliance