HTTPS-Verbindung einrichten 2.8

E-ConsentPro, E-ConsentPro mobile, E-DocumentPro

Zielsetzung des Dokuments

Dieses Dokument soll IT-Administratoren bei der Entscheidung unterstützen, ob E-ConsentPro mit einer Verbindung über HTTPS konfiguriert werden sollte oder nicht. Es erläutert, welche Zertifikate genutzt werden können und welche Anpassungen 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.

Erläuterung aus Sicht des Datenschutzes

Verbindungen im Internet sollten grundsätzlich verschlüsselt hergestellt 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.

Empfehlung: Wann und weshalb HTTPS?

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

E-ConsentPro unterstützt die Kommunikation über eine HTTPS-Verbindung unter Verwendung von TLS 1.0–1.2.

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.

Wenn 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.

Im Folgenden wird erklärt, wie Sie eine sichere Verbindung zwischen dem E-ConsentPro Server und den Client-Geräten einrichten können.

Das Dokument erklärt die Einrichtung für das Produkt E-ConsentPro WebClient, das auf einem Apache Tomcat Server basiert, unabhängig von der genutzten Ausprägung (E-ConsentPro, E-ConsentPro mobile, E-DocumentPro).

Thieme Compliance

Mögliche Verfahren

In **E-ConsentPro** (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. Hierbei sind manuelle Anpassungen nötig.
- Mit einem selbstsignierten Zertifikat.
  Vor der **eigenverantwortlichen Umsetzung** empfehlen wir Ihnen, sich mit dieser Lösung technisch auseinanderzusetzen und entsprechende Ressourcen einzuplanen.
  Ein selbstsigniertes Zertifikat kann ähnlich eingebettet werden wie Zertifikate offizieller Zertifizierungsstellen. Diese Methode wird jedoch von uns nicht getestet und von unserem Support nicht unterstützt.

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.

Achtung: Aufgrund des Einsatzes von Apps 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.

Notwendige Schritte für HTTPS

Allgemeine Hinweise

Um HTTPS einzusetzen, sollten Sie bei der Installation von E-ConsentPro entscheiden, ob der Aufruf der Anwendung per IP-Adresse oder Rechnernamen stattfinden soll. Dies wird vom Setup abgefragt (vorbelegt ist die IP-Adresse des Installationsservers) und für die Erstellung der Zertifikatsdatei verwendet. Damit ist auch festgelegt, wie ein Fremdaufruf über die Schnittstelle mit HTTPS erfolgen muss.

Um HTTPS verwenden zu können, führen Sie nach einer Neuinstallation bzw. einem Update 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 auf den Anwender-PCs importieren:

Um das Zertifikat in Ihrem Netzwerk zu verteilen, nutzen Sie die übliche Vorgehensweise für Ihr Netzwerk, z. B. den Rollout über einen Zertifikatsserver. Eine Anleitung für einen Schnelltest finden Sie im Anhang.

Schritt 2 – Firewall-Regeln hinzufügen:

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

Schritt 3 – Verbindung in den Apps ändern:

Passen Sie die Verbindung der Apps „Anamnese mobil“ und „Aufklärung mobil“ zum Server an. Sollten Sie die App „E-DocumentPro“ einsetzen, müssen Sie auch dort die Verbindung anpassen.

1. Stellen Sie das Tablet wie folgt ein:
    - **iOS**: Aktivieren Sie in den Einstellungen der jeweiligen App die Option **E-ConsentPro (EDP) 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 – Aufruf anpassen:

Informationen über die Anpassung im Patientenverwaltungssystem finden Sie im Handbuch zum Patientenverwaltungssystem oder erhalten Sie vom Hersteller der Patientenverwaltungssoftware.

Anhang

Schnelltest HTTPS

Für einen Schnelltest mit dem von Thieme Compliance angeforderten Zertifikat können Sie beispielsweise wie folgt vorgehen.

1. Importieren Sie die Zertifikatsdatei `cacert.pem`, die Sie von Thieme Compliance per E-Mail erhalten, in den Browser.
    - Der **Internet Explorer** verwendet die Zertifikatsverwaltung von Windows. Importieren Sie das Zertifikat deshalb in die Windows-Zertifikatsverwaltung. Wählen Sie dazu im Internet Explorer **Extras** > **Internetoptionen** > **Inhalte** > **Zertifikate** > **Vertrauenswürdige Stammzertifizierungsstellen** > **Importieren**.
    - **Firefox** verwendet nicht die Zertifikatsverwaltung von Windows, sondern einen eigenen Zertifikatspeicher. Importieren Sie das Zertifikat daher in den Zertifikate-Manager von Firefox (**Menü** > **Einstellungen** > **Datenschutz und Sicherheit** > **Zertifikate** > **Zertifikate anzeigen** > **Zertifizierungsstellen** > **Importieren**). Wählen Sie **Dieser CA vertrauen, um Websites zu identifizieren**.
2. Empfehlung: Starten Sie nach Änderungen den Browser neu.

Ein von einer offiziellen Zertifizierungsstelle erworbenes Zertifikat einbinden

Falls Sie unser bereitgestelltes Zertifikat nicht nutzen, gehen wir davon aus, dass Sie Erfahrung im Umgang mit selbst erworbenen Zertifikaten haben und diese selbstständig implementieren und pflegen können.

Beispielhafte 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) über die bestehende Installation nochmals aus und passen die Einstellungen darüber an.

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

FAQ

E-ConsentPro zeigt eine Warnung an, dass das Zertifikat demnächst abläuft oder abgelaufen ist.

Hinweis: Das Onlineupdate der Software ist nicht in der Lage Zertifikate zu generieren.

- Bei Betrieb mit dem von Thieme Compliance zur Verfügung gestellten Zertifikat:

  Nutzen Sie zur Erneuerung das Installationsprogramm. Dieses muss dieselbe oder eine höhere Version haben wie Ihre aktuelle E-ConsentPro-Installation.

  Achten Sie bei der vorgeschlagenen IP-Adresse darauf, ob diese Ihrem bisherigen Aufruf entspricht.

- Mit einem von einer öffentlichen, autorisierten Zertifizierungsstelle wie VeriSign erworbenen Zertifikat:

  Aktualisieren Sie den Keystore gegebenenfalls mit Hilfe eines neu beschafften Zertifikats wie im Kapitel *Ein von einer offiziellen Zertifizierungsstelle erworbenes Zertifikat einbinden auf Seite 4* beschrieben.

- Mit einem selbst erstellten Zertifikat:

  Diese Methode kann ähnlich eingebettet werden wie Zertifikate offizieller Zertifizierungsstellen, wird aber von uns nicht getestet und nicht supportet.

Umstellung einer bestehenden Installation von HTTP auf HTTPS

Nutzen Sie zur Umstellung auf HTTPS das Installationsprogramm. Dieses muss dieselbe oder eine höhere Version haben wie Ihre aktuelle E-ConsentPro-Installation.

Das Onlineupdate der Software ist nicht in der Lage Zertifikate zu generieren.

Für den Einsatz eines erworbenen oder eigenen Zertifikats nutzen Sie die Anleitung im Kapitel *Ein von einer offiziellen Zertifizierungsstelle erworbenes Zertifikat einbinden* auf Seite 4.

Zugriff für HTTP gesperrt, E-ConsentPro funktioniert nicht mehr

Eine generelle Sperre des Ports verhindert, dass E-ConsentPro am Server Routinen z. B. über `localhost` ausführen kann, die für den Einsatz der Software erforderlich sind. Sperren Sie den Port nur für eingehende Anfragen.

Was muss ich beim Serverwechsel beachten?

Wenn Sie anhand der Umzugsanleitung vorgehen, können Sie ein neues Zertifikat erstellen lassen. Achten Sie darauf, dass der Aufruf für Schnittstellen dann angepasst werden muss.

Stand: Oktober 2019

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

Tel.: +49 9131 93406-40
Fax: +49 9131 93406-74
E-Mail: support@thieme-compliance.de

Thieme Compliance