BENUTZERDOKUMENTATION (ALEPHINO 5.0)

Verschlüsselung mit Alephino

Autor: Frank Bieber

Inhalt

Verschlüsselung in Alephino

Mit dem Wirksamwerden der Datenschutz-Grundverordnung (DSGVO / GDPR) in der Europäischen Union erhob sich die Notwendigkeit umfassender Maßnahmen zum Schutz personenbezogener Daten in Alephino. Wesentliche Maßnahme hierzu ist die Verschlüsselung der Kommunikation sowohl zwischen GUI-Clients und dem Alephino-Server als auch der browserbasierten Dienste OPAC und Web Services. Sofern Alephino-Datenbank (Server) und dessen Anwendungen nicht ausschließlich im lokalen Netzwerk betrieben werden, die Dienste also im öffentlichen Internet erreichbar sind, ist Verschlüsselung empfehlenswert.

1) Verschlüsselung des Alephino C/S Protokolls

Mit dem Encryption Service Pack für Alephino stehen zwei Methoden zur Verschlüsselung der Kommunikation zwischen GUI-Clients und Server zur Verfügung. Die entsprechenden Fähigkeiten sind zugleich in die seit Ende des Jahres 2018 verfügbaren Installationspakete integriert. Es ist zu beachten, daß Alephino Server und Z39.50 Gateway aus Sicht der Clients Server darstellen, die dasselbe Protokoll bedienen. Damit Clients beide Dienste zugleich nutzen können, muß die Verschlüsselung stets identisch konfiguriert sein.

a) **„Ex Libris“**
Diese Methode wurde von Ex Libris entwickelt und kommt in Aleph und Alephino bereits zur Verschlüsselung von Kennworten der Mitarbeiterkonten zum Einsatz. Nunmehr ist derselbe Algorithmus auch zur Verschlüsselung der Kommunikation verfügbar.

a. **Konfiguration der Server**
Dateien : etc/alephino.cfg und etc/zgate.cfg
Parameterblock : (Communication)
Parameter : Encryption = 1

b. **Konfiguration des GUI**
Datei : alephcom/tab/alephcom.ini
Parameterblock : [Main]
Parameter : Encryption = 1

b) **DES**
Diese Methode verwendet den Algorithmus des Data Encryption Standard und arbeitet mit einem symmetrischen Schlüssel, der Client und Server gleichermaßen bekannt sein muß.

a. **Konfiguration der Server**
Dateien : etc/alephino.cfg und etc/zgate.cfg
Parameterblock : (Communication)
Parameter 1 : Encryption = 2
Parameter 2 : DESKey = ../etc/des_key.dat (Pfadname der Schlüsseldatei)

Datei : etc/des_key.dat
Inhalt : Beliebige Zeichenfolge (Ziffern, Buchstaben), wobei nur 7

Zeichen (56 Bit) relevant sind.

b. **Konfiguration des GUI**

Datei : alephcom/tab/alephcom.ini
Parameterblock : [Main]
Parameter : Encryption = 2

Datei : alephcom/tab/des_key.dat
Inhalt : Beliebige Zeichenfolge (Ziffern, Buchstaben), wobei nur 7 Zeichen (56 Bit) relevant sind.

2) Ausnahmen

Alle Komponenten von Alephino kommunizieren mittels desselben Client/Server Protokolls. Ein Alephino-Datenbankserver bedient nicht nur die GUI-Clients, sondern auch die webbasierten Bestandteile des Systems, wie den OPAC und das Service-Modul, sowie die Server für Z39.50 und Self-Check (SIP2). Mit Ausnahme des GUI findet die Kommunikation zwischen Server und Clients ausschließlich auf lokaler (localhost) oder der Ebene des Intranet bzw. VPN statt. Ein Z39.50- oder Self-Check-Server wird unwahrscheinlich auf einer anderen Maschine als dessen zugeordneter Alephino-Server betrieben, und falls doch, diese schon gar nicht über öffentliche IP-Adressen miteinander verbunden sein.

Somit benötigen die internen Server-Server Kommunikationsstrecken keine Verschlüsselung und besitzen die Fähigkeit dazu bislang auch nicht. Damit nun ein mit Verschlüsselung betriebener Alephino-Datenbankserver auch solche internen Komponenten weiterhin bedienen kann, ***müssen*** für diese Ausnahmen von der Verschlüsselung definiert werden. Dies geschieht über die Festlegung von IP-Adressen bzw. Adressbereichen.

Konfiguration des Servers

Datei	: etc/alephino.cfg	
Parameterblock	: (IpfilterUNENCRYPTED)	
Parameter 1	: Allowed = 127.0.0.1	(localhost)
Parameter 2	: Allowed = 192.168.*.*	(local network)
…		
Parameter n	: Allowed = 10.180.*.*	(VPN)

Selbstverständlich kann dieses Prinzip auch auf GUI-Clients angewendet werden, sofern diese ausschließlich im lokalen Netzwerk mit ihrem Server kommunizieren, mithin keine Gefahr des Abhörens des Nachrichtenaustausches besteht.

Achtung: Nicht korrespondierende Konfiguration der Verschlüsselungsmethoden auf Server- und Clientseite führt stets zum Versagen der Programme. Dagegen gibt es leider keine Sicherung, da weder die verwendete Methode noch der Schlüssel (verständlicherweise) offen ausgetauscht werden dürfen. Wurde der Server mit einer unpassenden Methode adressiert, antwortet dieser zunächst nicht mehr und muß neu gestartet werden!

3) Verschlüsselung des OPAC und des Service-Moduls

Zur Sicherung gegen das Abhören des browserbasierter Nachrichtenaustausches kommt das Protokoll HTTPS anstelle des unverschlüsselten HTTP zum Einsatz. Die hierzu notwendige Konfiguration der asymmetrischen Verschlüsselung mit SSL/TLS ist spezifisch für den verwendetem Webserver, hat also strenggenommen nichts mit Alephino zu tun, so daß Kontrolltabellen oder Webseiten in Alephino nicht geändert werden müssen.

Nachfolgend eine beispielhafte Konfiguration, wie diese für den am häufigsten genutzten Webserver Apache gilt. Voraussetzung ist, daß der Webserver SSL unterstützt und es keine Konflikte mit auf demselben Server betriebenen Diensten hinsichtlich der verwendeten Ports gibt. Somit geht das Beispiel davon aus, daß ein dedizierter Server für Alephino genutzt wird.

```
#
# Basic SSL configuration
#
LoadModule ssl_module /usr/lib/apache2/modules/mod_ssl.so

<IfModule mod_ssl.c>

SSLRandomSeed startup builtin
SSLRandomSeed startup file:/dev/urandom 512
SSLRandomSeed connect builtin
SSLRandomSeed connect file:/dev/urandom 512

AddType application/x-x509-ca-cert .crt
AddType application/x-pkcs7-crl    .crl

SSLPassPhraseDialog  exec:/usr/share/apache2/ask-for-passphrase

SSLSessionCache         shmcb:${APACHE_RUN_DIR}/ssl_scache(512000)
SSLSessionCacheTimeout  300

SSLCipherSuite HIGH:!aNULL

SSLProtocol all -SSLv3

</IfModule>
```

```
#
# ExLibris(D) GmbH
# Settings for Alephino 5.0
#

# Ports for Alephino services
Listen 80
<IfModule mod_ssl.c>
  Listen 443
</IfModule>

# Allow access to Alephino directories
<Directory  "/home/exlibris/alephino_50">
Require all granted
Options -Indexes
</Directory>

# Alephino Administration
<IfModule mod_ssl.c>
<VirtualHost *:443>
SSLEngine on
SSLCertificateFile "/home/exlibris/alephino_50/etc/server.cer"
SSLCertificateKeyFile "/home/exlibris/alephino_50/etc/server.key"
SSLCertificateChainFile  "/home/exlibris/alephino_50/etc/trustchain.cer"

AddDefaultCharset UTF-8
AddType application/x-Research-Info-Systems .ris
DocumentRoot "/home/exlibris/alephino_50"
Alias /german "/home/exlibris/alephino_50/htdoc/aliadm_ger"
Alias /wjhk.jupload.jar "/home/exlibris/alephino_50/bin/wjhk.jupload.jar"
Alias /download "/home/exlibris/alephino_50/temp"
Alias /pix "/home/exlibris/alephino_50/htdoc"
Alias /repository "/home/exlibris/alephino_50/data/objects"
ScriptAlias /alipac "/home/exlibris/alephino_50/bin/alipac"
ScriptAlias /alix "/home/exlibris/alephino_50/bin/alix"
ScriptAlias /aliadm "/home/exlibris/alephino_50/bin/aliadm"
ScriptAlias /aliadz "/home/exlibris/alephino_50/bin/aliadz"
ScriptAlias /upload "/home/exlibris/alephino_50/bin/upload"
ScriptAlias /cgistart "/home/exlibris/alephino_50/bin/cgistart"
ErrorLog "|/usr/sbin/rotatelogs /home/exlibris/alephino_50/weblog/https_error.%Y-%m-%d-%H_%M 10M"
TransferLog "|/usr/sbin/rotatelogs /home/exlibris/alephino_50/weblog/https_access.%Y-%m-%d-%H_%M 10M"
RedirectMatch “^/$” “/alipac”

# Authentication
<Location "/aliadm">
AuthType Basic
AuthName "Alephino Administration"
AuthUserFile "/home/exlibris/alephino_50/etc/passwords"
Require user alephino
</Location>

</VirtualHost>
</IfModule>

# Alephino OPAC
<VirtualHost *:80>
ServerName alephino.meinebibliothek.de
DocumentRoot "/home/exlibris/alephino_50"
Redirect permanent / https://alephino.meinebibliothek.de/
</VirtualHost>
```

Zur Erläuterung:

- Privater Schlüssel und SSL-Zertifikat. Ein solches kann entweder von einer CA ausgestellt oder selbstsigniert sein. In ersterem Falle ist die sog. Vertrauenskette, also die Liste der Zertifikate des Ausstellers mit anzugeben.
- Für den Aufruf des OPAC genügt die Angabe des Servernamens in der Adresszeile des Browsers.
- Da das Service-Modul unbeschränkten Zugriff auf die Alephino-Datenbank ermöglicht, sollte diese vorteilhaft durch eine zusätzliche Passwortabfrage geschützt werden. Im Beispiel ist das Passwort des Benutzers „alephino“ mittels „htpasswd“ zu erzeugen bzw. zu ändern.
- Zugriffe auf den OPAC mittels unverschlüsseltem HTTP werden hiermit automatisch auf HTTPS umgeleitet.