# Nastavení HTTPS pro Aleph RESTful API

SUAleph 18-19.4.2018, Zlín
Tomáš Prachař, MZK

# Proč to mám / musím udělat?

Protože GDPR...

Je nutné být v souladu s tímto nařízením a tedy i minimalizovat rizika krádeže dat -> je nutné šifrovat komunikaci např. s CPK.

Za nešifrování komunikace nese zodpovědnost správce osobních údajů - knihovna. CPK dle zpracovatelské smlouvy pouze upozorní na nevhodnost daného zabezpečení.

# Nutné prerekvizity pro úspěšnou implementaci

Rozběhnuté https na Alephu!

Přístup k certifikátům Alephu - nejspíš root?

Odhodlání a 20 minut vašeho času :-)

# Implementace

Návod, podle kterého jsem postupoval - https://knowledge.exlibrisgroup.com/Aleph/Knowledge_Articles/How_to_secure_RESTful_API_(using_Tomcat)_with_https

Je vhodné, aby byl certifikát vydaný důvěryhodnou certifikační autoritou - Man in the Middle při navazování komunikace s CPK -> odchylka v bodě 1. Provedeme export certifikátu pro Aleph a jeho import do JAVA úložiště.

# Export certifikátu - jak na to?

Je třeba zjistit, kde nám ty certifikáty a klíče leží.

V konfiguračním souboru apache:  /exlibris/aleph/u22_1/alephe/apache/conf/httpd.conf hledejte řádky

**SSLCertificateFile** /exlibris/aleph/u/alephe/apache/SSLconf/conf/aleph2016.pem

**SSLCertificateKeyFile**  /exlibris/aleph/u/alephe/apache/SSLconf/conf/aleph2016.key

**SSLCertificateChainFile** /exlibris/aleph/u/alephe/apache/SSLconf/conf/aleph2016-ca.pem

# Export certifikátu - jak na to? 2. díl

Provedeme export:

openssl pkcs12 -export -in aleph2016.pem -inkey aleph2016.key -chain -CAfile aleph2016-ca.pem -name "tomcat" -out tomcat.p12

Heslo pro export musí být stejné jako pro vaše JAVA úložiště klíčů!

Zvolte si něco hodně bezpečného.

# Import certifikátu do JAVA keystore

```
cd $JAVA_HOME/bin/

./keytool -importkeystore -srckeystore
/exlibris/aleph/u/alephe/apache/SSLconf/conf/tomcat.p12 -srcstoretype PKCS12 -alias tomcat

Heslo pro úložiště musí být stejné!
```

# Další nastavení

Body 2, 3 dle návodu Ex Libris - úprava souboru
$aleph_dev/ng/aleph/home/profile/overwrites/thirdparty/tomcat/conf/server.xml.tmpl

Do sekce "SSL HTTP/1.1 Connector"  vložte

```
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"

maxThreads="150" scheme="https" secure="true"

clientAuth="false" sslProtocol="TLS" keystorePass="vase_heslo_k_ulozisti" />
```

# Další nastavení a restart

jbin

./set_globals.sh    - build successful

Proveďte restart Tomcatu: cd /exlibris/aleph/a22_1/ng/aleph/home/system/bin/

./jboss_shutdown

Raději si přes “ps -efl | grep tomcat” ověřte, že je dole

./jboss_startup

# Téměř hotovo

Ověřte, že jede https. Např: `curl -k "https://localhost:8443/rest-dlf/record"`

Nebo na svém webu https://aleph.mzk.cz:8443/rest-dlf/record/

Případné problémy hledat v lozích /exlibris/aleph/a22_1/ng/aleph/home/system/thirdparty/tomcat/logs, zejména server.log

V tuto chvíli jedete jak nezabezpečeně na portu 1891 tak i zabezpečeně na 8443.

# Vsuvka pro knihovny zapojené do CPK

Napište mail na cpk@mzk.cz. Uveďte, že máte nastaveno a pro jistotu číslo portu.

CPK provede otestování a přepnutí rozhraní na zabezpečenou komunikaci (může vyžadovat nějaké dodatečné nastavení na firewallu).

Jakmile dostanete od CPK potvrzující mail (**ne dříve!**), můžete provést vypnutí http.

# Vypnutí http

Do souboru $alephe_root/jboss_conf/main.properties přidejte řádek:

```
api.rest.https=Y
```

Restartujte tomcat.

# Děkuji za pozornost!