Cheatsheet zum sicheren Login für UCI, Chat und Adressbuch

In diesem Cheatsheet werden in einer kurzen Übersicht die Informationen zur UCI-Schnittstelle der Version 6.4.2.19 der STARFACE aufgeführt.

Ein neuer Server mit Secure Login unterstützt die REST-Methode GET über http und https

https://<host address>/ucp-free/info/serverinformations
http://<host address>/ucp-free/info/serverinformations

Die Antwort kommt als Json mit dem Header

Content-Type: application/json
Date: Fri, 19 May 2017 09:03:58 GMT
Server: Apache-Coyote/1.1
Transfer-Encoding: chunked

und den Daten:

{"version":"6.4.3.1","activeDirectory":false}

Daraus kann ein Client ableiten:

• Wenn die Antwort kommt, handelt es sich um einen Server, welcher das neue Secure Login unterstützt.

- Der Boolean Parameter "activeDirectory" gibt an, ob die Active Directory Authentisierung eingeschaltet ist. Dies muss für die UCI und XMPP Authentisierung berücksichtigt werden.

• Wenn der REST-API Aufruf "serverinformations" mit einem 404 - Not Found fehlschlägt, geht der Client davon aus, dass es sich um einen älteren Server handelt und meldet sich mit TLS aber ansonsten unverschlüsselt an.

• Wenn der REST-API Aufruf "serverinformations" mit einem beliebigen anderen Fehlercode fehlschlägt, verwendet der Client die Secure Login Methode. Der Client geht davon aus, dass es sich um einen neuen Server mit umgestellten http / https-Ports handelt.

- Wenn die eingegebene Login ID aussieht wie eine STARFACE Login ID (also nur Ziffern), meldet sich der Client mit Secure Login an.
- Sieht die User ID wie ein AD-Benutzername aus (alphanumerisch), meldet sich der Client mit Secure Active Directory Login an.
- Nun kann es Kunden geben, deren AD Benutzernamen nur aus Ziffern bestehen. Für diesen Sonderfall unterstützt der Client die Eingabe von AD-Benutzernamen in der Form Domainname\UserName oder UserName@FQDN. Der Client verwendet dann aus der Eingabe den UserName und führt ein Secure Active Directory Login aus.

Für die REST-Authentisierung fragt der Client mit der Methode https://<host address>:443/rest/login die Login-Parameter ab. Parameter LoginType == "ActiveDirectory" bedeutet: Active Directoy Authensierung für REST verwenden, andernfalls wird die Staraface-Authentisierung angewendet. Im Paramter Nonce gibt der Server den Nonce für die Secret-Berechnung vor.

Secure Login mit Starface Authentisierung:

UCI Nonce ist zur Zeit noch fix: *
UCI und XMPP Secret:

SHA512(LoginId + Nonce + SHA512(Password).ToLower()).ToLower()

REST Secret (Nonce kommt vom Server):

LoginId + ":" + SHA512(LoginId + Nonce + SHA512(Password).ToLower()).ToLower()

Secure Login mit Active Directory Authentisierung:

UCI und XMPP Secret:

Password

REST Secret (Nonce kommt vom Server):

Base64Encode(LoginId + Nonce + Password)

Legacy Login mit Starface Authentisierung:

UCI und XMPP Secret:

Password

REST Secret (Nonce kommt vom Server):

SHA1(LoginId + Nonce + Password).ToLower()

Legacy Login mit Active Directory Authentisierung:

UCI und XMPP Secret:

Password

REST Secret (Nonce kommt vom Server):

Base64Encode(LoginId + Nonce + Password)