

Anwender Authentifizierung für E-Commerce

SAVERNOVA Software Development Kit ersetzt das statische Passwort-Login auf Ihren Webseiten durch eine sichere „One-Time-Password“ Methode. An der bestehenden Umgebung müssen nur wenige Änderungen vorgenommen werden. Die Implementierung kann mit einem minimalen Zeitaufwand realisiert werden.

Installation der Authentifizierungs Web Applikation oder Webdienstes

Die Applikation kann entweder auf demselben Webserver installiert werden wie die Kundenapplikation (es ist nicht notwendig den Kommunikationskanal zu sichern, da die gesamte Kommunikation lokal auf dem Server stattfindet), oder auf einem anderen Netzwerk-Server wie SSL, HTTPS oder VPN. Ansonsten sollte die Kommunikation verschlüsselt oder über einen anderen geschützten Kanal stattfinden. Diese Web Applikation / Webdienst generiert die Startpunkte und kontrolliert die „One-Time-Passwords“ der Anwender. Als Kommunikations-Protokoll wird XML-RPC verwendet. Dieses einfache „Remote Procedure Call“ Protokoll benützt XML-Code und HTTP zur Uebertragung. XML-RPC wird von den wichtigsten Programmiersprachen und Plattformen unterstützt (PHP, Java, ASP.NET, ...). Falls notwendig, kann die gesamte Kommunikation auch per HTTP Protokoll durchgeführt werden.

Definition des Anwender Anmeldevorgangs

Der Anmeldevorgang muss angepasst, beziehungsweise ausgeweitet werden. Die Kartenaktivierung wird in den Anmeldevorgang integriert, indem entweder der aktuelle Passwortvorgang ersetzt, oder durch SAVERNOVA verstärkt wird. Der Kartenaktivierungsvorgang ist vereinfacht, da die SAVERNOVA Passwortkarte automatisch zugewiesen werden kann (in diesem Fall ist einzig die Lesemethode und deren Bestätigung notwendig). Falls eine manuelle Zuweisung der Karten bestimmt worden ist (z.B. um den Anwendern zu ermöglichen, ihre eigene Karte zu importieren und diese somit auf verschiedenen Webseiten zu benutzen), wären zusätzliche Schritte zum Kartenimport notwendig.

Anwender Anmeldevorgang

Die Login Web-Seite mit SAVERNOVA Web Applikation / Webdienst verlangt gewisse Anpassungen, um den OTP Startpunkt und, falls notwendig, die SAVERNOVA „Card-on-Screen“ anzeigen zu können.

SAVERNOVA SDK

Welche Datenbank soll benutzt werden:

Die SAVERNOVA Karten, Anwender-Lesemethoden und weitere Informationen können entweder in der aktuellen Datenbank integriert, oder in einer separaten speziell dafür bestimmten Datenbank gespeichert werden. Je nach Bedürfnissen kann die Datenbank wie folgt strukturiert sein:

tbISAVERNOVA_SECURITY_GROUPS

- SG_ID (PK)
- SG_name
- SG_logins
- SG_password_age
- SG_password_times
- SG_show_card
- SG_use_secure_code
- SG_secure_code_position

tbISAVERNOVA_USERS

- USR_ID (PK)
- SG_ID (FK)
- USR_reading_method

tbISAVERNOVA_CARDS

- CRD_ID (PK)
- USR_ID (FK)
- CRD_content
- CRD_secure_code
- CRD_flags
- CRD_status
- CRD_imported
- CRD_assigned
- CRD_activated
- CRD_expired
- CRD_starting_positions

tbISAVERNOVA_SESSIONS

- session_ID
- USR_ID
- CRD_ID
- CRD_starting_position

Beispiel:

Gehen wir davon aus, dass auf der Webseite Login und Passwort für den Authentifizierungsvorgang benötigt werden. Das Web-Login-Formular login.html (login.php, login.aspx, ...) besteht aus zwei Feldern und Textboxen – Login und Passwort. Dieses Web-Formular wird an den Customer-Server zurückgesandt, wo das serverseitige Skript (login.pgp, login.aspx, I11) die Parameter des Web-Formulars mit den Angaben in der Datenbank vergleicht. Ist das Passwort korrekt erhält der Anwender Zugang zum geschützten Inhalt, oder seinem Kundenkonto. Wenn nicht, wird der Zugang verweigert.

Notwendige Anpassungen:

Der Anmeldevorgang wird in zwei Schritte aufgeteilt. Im ersten Schritt gibt der Anwender nur sein Login Name ein. Dieser wird zusammen mit der Session ID zum serverseitigen Code gesandt (identisch wie beim Web-Login-Formular oder im Zusammenhang mit der Anwendung der AJAX Technologie). Daraufhin wird eine XML-RPC Anfrage generiert und an den SAVERNOVA Web Applikation / Webdienst gesandt (neu). SAVERNOVA Applikation / Webdienst generiert einen neuen OTP Startpunkt und sendet diesen an den serverseitigen Code der Kunden Web Applikation.

In einem weiteren Schritt wird diese Information dem Anwender zugänglich gemacht (Startpunkt, „Card-on-Screen“, Secure Code, etc.). Der Anwender schreibt sein „One-Time-Password“ (OTP) in das für das Passwort vorgesehene Feld. Dieses OTP wird dem serverseitigen Kunden Code weitergeleitet. Eine neue XML-RPC Anfrage wird erstellt und an SAVERNOVA Applikation / Webdienst gesandt, wo das OTP mit der Datenbank verglichen wird. Eine entsprechende OK/Fehler Meldung geht automatisch zurück an die Kunden Web Applikation, welche in Übereinstimmung mit dieser Meldung gleich wie vorher weiterfährt und dem Anwender den Zugang verweigert oder erlaubt.

Minimale Investition für maximale Sicherheit**Kontakt**

Savernova Ltd
info@savernova.com

Vor Implementierung von SAVERNOVA:

```
login.html (simplified)
...
<form action="login.php" method="post">
  Login: <input id="login" name="login" type="text" />
  Password: <input id="password"
             name="password" type="password" />
</form>
...

login.php (simplified)
<?php
...
$login = $_POST("login");
$password = $_POST("password");

if (check_password($login, $password))
  access OK
else
  access denied
...
?>
```

Nach Implementierung von SAVERNOVA:

```
login.html (simplified)
...
<form action="login.php" method="post">
  <div id="step1">
    Login: <input id="login" type="text" />
  </div>
  <div id="step2">
    Starting position: <div id="starting_position"></div>
    Password: <input id="password" type="password" />
  </div>
</form>
...

login.php (simplified)
<?php
...
//step2
$password = $_POST("password");
if (XMLRPC->CheckPassword(sessionID, $password))
  access OK
else
  access denied
...
?>
```