Nutzung des offenen OCRA-Algorithmus zur Transaktionsabsicherung mit LinOTP beim Online-Banking: QR-TAN.

Cornelius Kölbel
cornelius.koelbel@lsexperts.de
http://www.lsexperts.de

Chemnitzer Linuxtage 2013 (März 2013)

Zusammenfassung

Mit dem im RFC 6287 spezifizierten OATH Challenge Response Algorithm (OCRA) steht ein Challenge-Response Algorithmus offen und frei zur Verfügung. Der Algorithmus wurde federführend von der Initiative for Open Authentication spezifiziert und erlaubt mittels eines Challenge-Response-Verfahrens sowohl das Authentisieren als auch das Signieren einer Nachricht. Das modulare Authentisierungsbackend LinOTP nutzt diesen Algorithmus um ein robustes TAN-Verfahren für Online-Banken zu implementieren. Dabei sind die entstehenden TANs kryptografisch unverwechselbar an die Transaktionen gebunden.

LinOTP[1] ist ein modulares Authentisierungsbackend, das sehr unterschiedliche Tokentypen unterstützen und auch zahlreiche Benutzerdatenbanken wie LDAP, SQL oder Flatfile gleichzeitig anbinden kann. LinOTP setzt

[1] http://www.linotp.org

auf Opensource-Komponenten auf und steht zu weiten Teilen selber unter freien Lizenzen. Offene und gut dokumentierte Schnittstellen ermöglichen die leichte Integration in heterogene Infrastrukturen und die Einbindung in bestehende Workflows. LinOTP verwendet bevorzugt Einmalpasswörter[2] zur Authentisierung. Diese können auf unterschiedliche Art und Weise erzeugt und ebenso unterschiedlich von LinOTP verifiziert werden.

In diesem Vortrag wird vorgestellt, wie dank der modularen Erweiterbarkeit im Bereich der Tokentypen LinOTP verwendet wurde, um für Online-Banken ein zusätzliches TAN-Verfahren zu etablieren. Hierzu wurde der offene OATH Challenge Response Algorithm[3] implementiert. Die Transaktionsdaten (also bspw. der Überweisungsbetrag, die Kontonummer des Empfängers und weiterer Text) werden kryptographisch an die Challenge-Daten gebunden. Mit einer App, die für iOS und Android zur Verfügung steht, wird dieses Datenpaket mit Hilfe eines QR-Codes eingelesen. Der verwendetet QR-Code gibt dem Verfahren seinen Namen: QR-TAN. In der App wird die kryptografische Unversehrtheit der empfangenen Daten sichergestellt und aus der Challenge der entsprechende OTP-Wert berechnet. Dieser kann nun als TAN an das Bank-Portal übergeben werden. Die eingegebene TAN wird von dem Authentisierungsbackend LinOTP gegen die Challenge verifiziert.

Mit LinOTP und QR-TAN steht nun ein zeitgemäßes und sicheres Verfahren zur Verfügung, das gegenüber herkömmlichen iTAN- oder mTAN-Verfahren auch in den Bereichen Nutzerfreundlichkeit und Kosteneffizienz punkten kann.

Dieser Vortrag soll zum Einen die Flexibilität von LinOTP aufzeigen, wodurch dieses Verfahren schnell implementiert werden konnte, und zum Anderen auch die kryptografisch interessanten Hintergründe beleuchten.

[2] OTP = One time password
[3] http://tools.ietf.org/rfc/rfc6287.txt