Sichere Webanwendungen mit dem neuen Personalausweis

Olaf Heimburger
Oracle Deutschland B.V. & Co. KG
Berlin

Schlüsselworte:

Fusion Middleware, Security, Web Anwendungen, neuer Personalausweis, OID, OIF, OAM

Einleitung

Heutige Anforderungen an Datensicherheit werden immer komplexer und wichtiger. Diese Funktionalität darf aber nicht nur den Entwicklern überantwortet werden, sondern muss auch im produktiven Einsatz den aktuellen Bedürfnissen angepasst werden können.

Um die Sicherheit bei allen Beteiligten (Anwendern, Anbietern, Behörden, etc.) zu erhöhen, werden bei vielen Anwendungsumgebungen die etablierten Mechanismen wie die Angabe von Anwendername und Kennwort durch zusätzliche Technologien ergänzt oder sogar ersetzt. In der Regel bedeutet dies einen erheblichen Aufwand an zusätzlicher Hard- und Software sowie eines vertrauenswürdigen Verteilungsvorganges.

Mit der Einführung des neuen Personalausweises im Oktober 2010 wurde eine bundesweite Infrastruktur geschaffen, die es quasi jedem Anbieter erlaubt, diese Infrastruktur einzusetzen und seinen Anwendungen und Anwendern zusätzliche Sicherheit zu bieten.

Einfach und Sicher

Es vergeht nahezu kein Tag an dem keine Meldung über Sicherheitslücken und deren Ausnutzung durch Unbefugte die breite Öffentlichkeit erreicht. Trotzdem werden selbst bei hochsensiblen Anwendungen mit mehreren Millionen Nutzern immer noch archaische Mittel wie die Angabe von Anwendername und Kennwort zur Anwenderauthentifizierung und –autorisierung verwendet.

Der meistgenannte Grund hierfür ist die einfache Nutzung von nahezu jedem Ort und mit nahezu jedem Endgerät. Diese Methoden erfüllen immer das Kriterium „Einfach“ aber selten das Kriterium „Sicher“. Einfach ist hier nicht nur die Anwendbarkeit, sondern auch der Schutz vor missbräuchlicher Nutzung. Programme zum Knacken von Kennworten sind Legion und häufig bei einfachen Kennworten erfolgreich.

Damit ein Zugangsschutz auch als „Sicher“ eingestuft werden kann, muss der Zugriff auf die Authentifizierungsinformation durch Manipulation (Raten, Ausspähen oder Stehlen) vermieden werden. Es ist sowohl im Sinne des Anwenders als auch des Anbieters diese Information ohne Manipulation zu erhalten und an die Anwendung zu übermitteln.

Auf der anderen Seite darf die Integration in bestehende Anwendungen nicht zu aufwändig oder zu kompliziert sein.

Zielarchitektur

Die Architektur einer solchen Lösung darf nicht von der bisherigen Anwendungsarchitektur abweichen. Sie muss einfach zu Integrieren und zu Pflegen sein und im besten Fall nicht auf das Einsatzgebiet „neuer Personalausweis“ beschränkt sein. Wird die Anwendung über die Landesgrenzen beliebt, sind andere Mechanismen erforderlich und zu verwenden.

Anwender

Eine zeitgemässe Anwendung erlaubt entsprechend der verwendeten Endgeräte oder der geografischen Position des Anwenders unterschiedliche Zugangsmethoden. Es kann aber auch nicht davon ausgegangen werden, dass der Anwender immer und überall über einen vertrauenswürdigen, nicht manipulierten Kartenleser verfügt. Für diese Fälle müssen alternative aber adäquat sichere Methoden berücksichtigt werden, damit dem Anwender die versprochene Sicherheit gewährleistet werden kann.

Auf jeden Fall muss der Anwender in der Lage sein die Anwendung mit möglichst wenig eigenem Aufwand verwenden zu können. Verfügt seine Umgebung die technischen Voraussetzungen für einen Kartenleser sind diese zu nutzen, in allen anderen Fällen sind Alternativen einzusetzen.

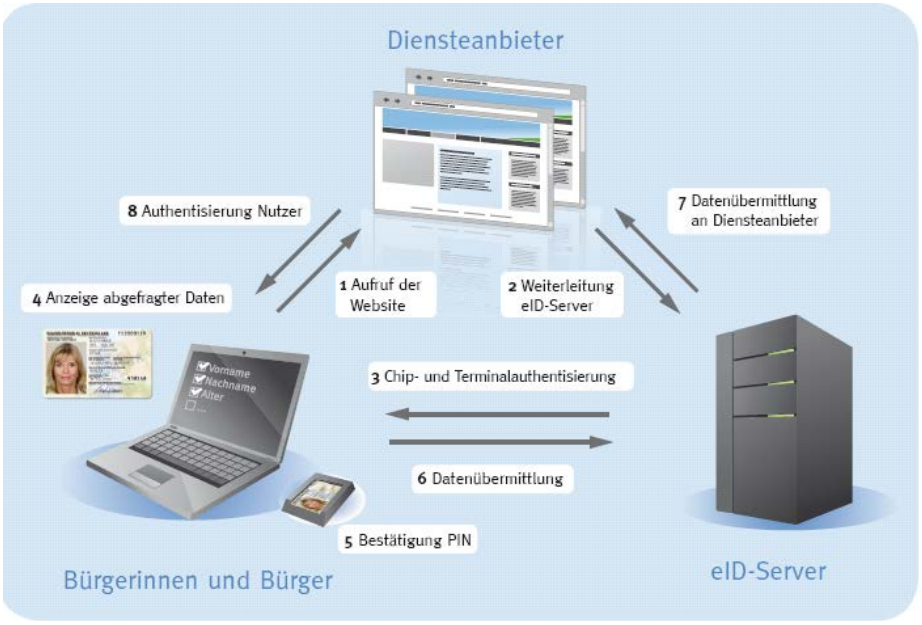
Anwendung

Sicherheitsverfahren und -mechanismen sind immer ganzheitlich im Unternehmenskontext zu betrachten. Verfügen verschiedene Anwendungen über unterschiedliche Sicherheitstechnologie führt dies sehr schnell zu einer unübersehbaren Menge von Fehlerquellen die schnell nicht mehr zu bewältigen sind.

Aus diesem Grund wird eine einheitliche Technologiebasis für alle Anwendungen empfohlen, die im Idealfall transparent für die Anwendung und die Entwicklung eingesetzt werden kann. Diese kann bei Bedarf an die Herausforderungen angepasst werden und die Verfügbarkeit erheblich verbessern.

Übersetzt in unseren Fall heisst dies, dass die Anwendungsentwickler nicht wissen müssen wie der Anwender sich anmelden wird, sondern lediglich auf das Vorhandensein der benötigten Daten vertrauen müssen.

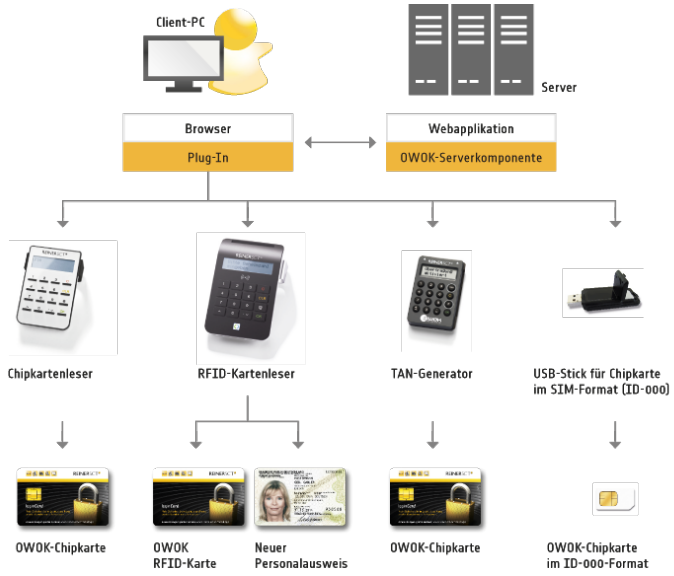
Ablauf Neuer Personalausweis



(Quelle: BMI)

Architektur Anwendung

Das häufig eingesetzte OWOK (One Web One Key) Toolkit von Reiner SCT kann für die Realisierung der Anbindung an die Anwendung verwendet werden. Reiner SCT skizziert den Einsatz des OWOK Toolkits wie folgt:



(Quelle: Reiner SCT)

Implementierung

Bei der Implementierung der Architektur gilt die Prämisse „Konfiguration vor Codierung“. Alles was konfiguriert werden kann, reduziert die Entwicklungszeit und beschleunigt die Verfügbarkeit der gewünschten Funktionalität.

Bevor eine Anwendung die Zugangsinformation des neuen Personalausweis nutzen kann, müssen die passenden Voraussetzungen für die Hardware und Software geschaffen werden.

Hardware

Um das Manipulationspotential zu reduzieren wird ein autonomer Kartenleser mit eigenem Eingabefeld für die PIN empfohlen. Preiswertere Lösungen fragen die PIN über Software-Dialoge ab und sind lohnenswerte Angriffsziele für Key- oder Mouselogger.

Die Empfehlung für den autonomen Kartenleser stellt auf den ersten Blick eine nicht zu unterschätzende Hürde für den potentiellen Anwender dar, da dieser die Anschaffungskosten scheuen wird. Sobald aber mehr Anwendungen die gleichen Möglichkeiten nutzen rentiert sich die einmalige Anschaffung. Bei einem Mehrprotokollgerät werden auch weitere Kartentypen (z.B. Geldkarte oder Gesundheitskarte) unterstützt, womit der Anwendungskreis erheblich erweitert wird.

Software

Natürlich müssen die Zugangsinformationen vom Personalausweis über den Kartenleser zu der Anwendung gelangen. Die dafür notwendige Software wird in der Regel vom Hersteller des Kartenlesers zur Verfügung gestellt und kann zentral auf dem Anwendungsserver an die Anwender ausgeliefert werden.

Das Ergebnis

Natürlich sind Worte nur leere Hülsen wenn die beschriebenen Ansätze nicht nachgeweisen werden können. Der Nachweis, gerne auch mit einem Personalausweis aus dem Publikum, erfolgt während des Vortrages.

Kontaktadresse:

Olaf Heimburger
Oracle Deutschland B.V. & Co. KG
Schloßstr. 2
D-13507 Berlin

Telefon:	+49 (0) 30 435 795-160
Fax:	+49 (0) 30 435 795-419
E-Mail	olaf.heimburger@oracle.com
Internet:	blogs.oracle.com/olaf