OpenID trifft elektronischen Personalausweis

Sichere Authentisierung im Internet

OpenID ist ein offener, dezentraler und URL-basierter Standard für Single Sign-On im Internet. Sein Protokoll ist mit dem neuen elektronischen Personalausweis (nPA) kombinierbar, der in Deutschland seit November 2010 ausgegeben wird. Dadurch entstehen Mehrwerte sowohl für Anwender als auch für Dienstanbieter. Ein nPA-basierter OpenID-Provider ist eine einfache Möglichkeit, sehr schnell die sichere Authentisierung des neuen Personalausweises zu nutzen, ohne eine komplett neue Infrastruktur aufbauen zu müssen. Der folgende Beitrag stellt das Konzept eines OpenID-Providers mit nPA-Unterstützung vor und erläutert, welche Voraussetzungen auf Seiten der Anwender und Dienstanbieter zu erfüllen sind.

Heutzutage müssen sich Anwender von IT-Systemen sowohl im Privat- als auch im Unternehmensumfeld immer mehr Zugangsdaten merken. Im Privatumfeld entspringt dies der Tatsache, dass sich IT-Anwendungen mehr und mehr in das Internet verlagern. Bei nahezu jedem Internetdienst findet erst die sogenannte Authentisierung (oft auch: Login) statt, bevor der Internetdienst genutzt werden kann. Die Authentisierung besteht aus der Behauptung (Login-Name) und dem anschließenden Beweis (Passwort) einer Identität. Dies führt zu Problemen, wenn ein Anwender für die Vielzahl an Internetdiensten zu kurze oder zu einfache Passwörter wählt, der Bequemlichkeit halber das gleiche Passwort für verschiedene Internetdienste verwendet oder Passwörter aufschreibt und den Zettel an den Monitor oder unter die Tastatur klebt.

Auch im Unternehmensumfeld muss sich ein Mitarbeiter um das Thema kümmern. Administratorenseitig findet es hier als Identity Management statt. Durch die personenbezogene Nutzung von Diensten führt ein Mitarbeiter oft mehrmals täglich verschiedene Logins beziehungsweise Authentisierungen durch. Es existieren unterschiedliche Herangehensweisen als Abhilfe für die beschriebene Problematik. Im Folgenden geht es um die Idee des Web Single Sign-On (Web-SSO) sowie um die sogenannte starke Authentisierung.

Single Sign-On (SSO) im Internet

Bei der Technologie Single Sign-On (SSO, etwa „Einmalanmeldung") besitzt der Anwender nur noch einen Identifikator (Benutzernamen) und ein stark gewähltes Passwort. Der große Nutzen von SSO ist die einmalige Anmeldung beim Identitätenverwalter (ID-Provider) und die anschließende Nutzung aller angeschlossenen Internetdienste (vgl. Abbildung 1). Die Zugangsdaten eines Anwenders müssen nicht mehr an vielen Punkten im Internet, bei verschiedenen Internetdiensten, hinterlegt werden, sondern nur noch an einer zentralen und vertrauenswürdigen Stelle – bei dem Identitätenverwalter.

Das OpenID-Protokoll

OpenID ist ein offener Standard für Single Sign-On im Internet. Der Mechanismus agiert dezentral und URL-basiert. Das bedeutet, dass ein Anwender sowohl seine Identität als auch seinen Identitätenverwalter frei wählen kann. Die Identifizierung eines Anwenders erfolgt grundsätzlich über den Beweis des „Besitzes" einer URL, der sogenannten OpenID-Identität, zum Beispiel https://openid.internet-sicherheit.de/JohnDoe. Vor der eigentlichen Nutzung des OpenID-Protokolls muss sich ein Anwender eine OpenID-Identität erstellen. Hierfür sind grundsätzlich vier Schritte notwendig:

1. Wahl des OpenID-Providers: Der Anwender wählt einen vertrauenswürdigen OpenID-Provider (OP), der fortan für die Bestätigung der digitalen Identität zuständig ist. Dieser repräsentiert den Identitätenverwalter im SSO-Gesamtbild (siehe Bild 1).

2. Wahl des Identifikators: Der Anwender wählt eine URL, die eigentliche OpenID-Identität. Diese URL repräsentiert die digitale Identität des Anwenders und wird den Internetdiensten anstelle eines Benutzernamens präsentiert. Ein Anwender hat fortan nicht mehr viele verschiedene Be-

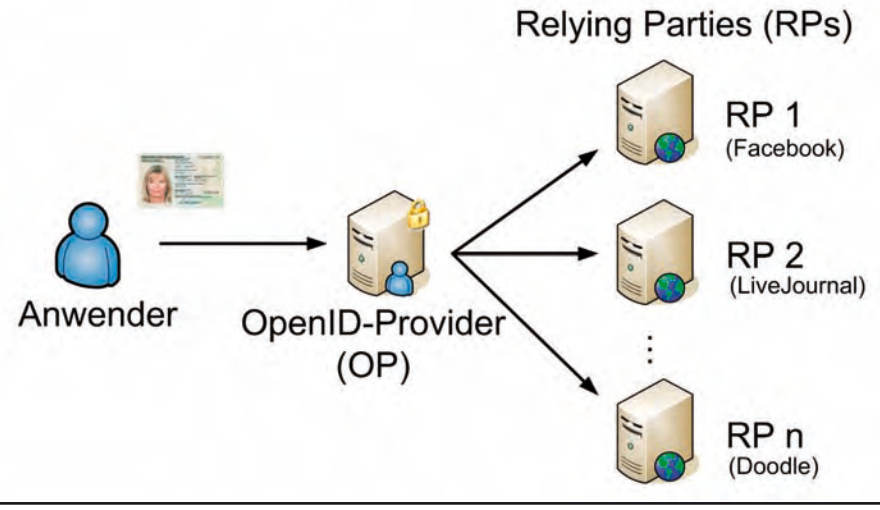

Bild 1: Wahl des OpenID-Providers: Der Anwender wählt einen vertrauenswürdigen OpenID-Provider (OP), der fortan für die Bestätigung der digitalen Identität zuständig ist.

nutzernamen, sondern nur noch einen Identifikator: die OpenID-Identität.

3. Eingabe persönlicher Informationen: Wenn gewünscht, kann der Anwender Informationen wie etwa Vor- und Zuname oder E-Mail-Adresse bei dem OP hinterlegen. Da die Eingabe der Informationen dem Anwender freigestellt ist, kann dieser zum Beispiel lediglich ein Pseudonym hinterlegen oder ein vollständiges Profil. Mittels des OpenID-Protokolls kann ein Internetdienst nicht nur die Authentisierung des Anwenders anfragen, sondern optional auch weitere Informationen. Diese gibt der Anwender in jedem Fall gesondert frei.

4. Festlegung der Zugangsdaten: Bei der Registrierung der OpenID-Identität hinterlegt der Anwender seine Zugangsdaten. Für gewöhnlich ist dies zurzeit eine Kombination aus Benutzername und Passwort. Hierüber wird der Anwender vom OP wieder erkannt.

Nachdem ein Anwender einmalig eine OpenID-Identität angelegt hat, können sämtliche OpenID-unterstützenden Internetdienste genutzt werden. Dies kann im Grunde ebenfalls in vier Schritte eingeteilt werden:

1. Aufruf der Login-Seite: Der Anwender möchte einen OpenID-fähigen Internetdienst nutzen und ruft die entsprechende Webseite mit dem Login-Formular auf.

2. Behauptung der Identität: Statt wie gewohnt eine Benutzername-Passwort-Kombination einzugeben, übermittelt der Anwender lediglich die OpenID-Identität. Der Anwender behauptet seine digitale Identität darüber, dass er den Besitz einer URL, der OpenID-Identität, vorgibt.

3. Beweis der behaupteten Identität: Der Internetdienst führt den Beweis der behaupteten Identität nicht selbst durch, sondern leitet den Anwender zu dem entsprechenden OpenID-Provider weiter. Der Anwender meldet sich dort, sofern noch nicht geschehen, an. Wenn der Login, das heißt die Authentisierung, beim OP erfolgreich verlief, so hat der Anwender den Besitz der OpenID-Identität und somit auch die eigene digitale Identität bewiesen. Dieses Ergebnis teilt der OP dem Internetdienst mit und leitet den Anwender zurück.

4. Nutzung des Internetdienstes: Wenn die Antwort des OpenID-Providers positiv ausfällt, so kann der Internetdienst die Identität des Anwenders als bestätigt ansehen und die Nutzung freigeben. Die Bestätigung der Identität wurde faktisch ausgelagert.

Vor- und Nachteile der Auslagerung der Authentisierung

Die Auslagerung der Authentisierung seitens der Internetdienste hin zu dem OpenID-Provider bringt mehrere Vorteile, aber auch verschiedene Gefahren. Ein Vorteil ist die Zentralisierung der Authentisierung. Der Anwender kann sich die Instanz für den Beweis der Identität bewusst aussuchen und diese besser sichern. Die Zugangsdaten sind nicht mehr bei vielen Internetdiensten verteilt, sondern liegen nur noch bei dem eingesetzten OP. Für die Internetdienste, die OpenID einsetzen, ergibt sich der Vorteil, dass verschiedene Methoden zur Authentisierung angeboten beziehungsweise genutzt werden können. Ein Internetdienst kann beispielsweise das Login mittels Benutzername und Passwort anbieten, aber indirekt auch sämtliche Methoden, die der OP des Anwenders anbietet. Der Internetdienst lagert die Authentisierung des Anwenders aus.

Nachteilig an OpenID beziehungsweise an SSO im Generellen ist der Single Point of Failure. Ein Angreifer kann mittels eines DoS-Angriffs den zentralen OpenID-Provider lahmlegen und somit die Loginversuche des Anwenders erschweren oder temporär unmöglich gestalten. Schließlich ist OpenID hochgradig anfällig gegenüber Phishing. Kopiert ein Angreifer die Login-Seite und „phisht" so das Passwort eines Anwenders, kann er diese Identität missbrauchen. Eine Maßnahme gegen die Hauptkritik von OpenID – Phishing – ist der Einsatz einer Multi-Faktor-Authentisierung wie etwa die eID-Funktion des neuen Personalausweises.

Kombination mit der eID-Funktion des neuen Personalausweises (nPA)

Am 1. November 2010 wurde in Deutschland der neue Personalausweis (nPA) eingeführt. Das grundsätzliche Ziel ist die Ausweitung der herkömmlichen Nutzung des Personalausweises auf die elektronische Welt und damit die Ermöglichung einer sicheren und auch rechtsverbindlichen Kommunikation im Internet. Der nPA ist mit einem kontaktlosen Chip (RF-Chip) ausgestattet, der über Funk verschlüsselt mit einem RF-Lesegerät kommuniziert.

Grundsätzlich besitzt der neue Personalausweis drei Funktionalitäten: Die Funktion des ePasses (als hoheitliche Anwendung), die Online-Authentisierung (oder eID-Funktion) sowie die qualifizierte elektronische Signatur (für die Bestätigung von Transaktionen). Relevant für die Verbindung mit OpenID ist die Online-Authentisierung des nPAs. Hierbei handelt es sich um die Identitätsfeststellung beziehungsweise authentische Übertragung von Attributen.

In der Spezifikation des Personalausweises wurde zudem der Anwendungsfall des Wiedererkennens eines bereits registrierten Anwenders bedacht. Da die Verwendung der Seriennummer des Personalausweises rechtlich nicht zulässig ist, wird stattdessen die sogenannte sektorspezifische Identifikation, ein Pseudonym, genutzt. Dieses Pseudonym hat zwei besondere Eigenschaften: Zum einen kann ein Anwender von einem Internetdienst wieder erkannt werden, ohne genau zu wissen, wer diese Person ist. Andererseits ist das Pseudonym nur zwischen dem Personalausweis der Person und dem auslesenden Internetdienst gültig (eben sektorspezifisch). Es ist nicht möglich, das Pseudonym über Dienstgrenzen hinweg zu vergleichen und somit Rückschlüsse auf die entsprechende Person zu erhalten.

Genau diese Vorteile der sektorspezifischen Identifikation können mit dem OpenID-Protokoll kombiniert werden. Wenn ein Anwender eine OpenID-Identität erstellt, so wird statt eines Passworts das mittels nPA berechnete Pseudonym bei dem OpenID-Provider hinterlegt. Bei einem erneuten Besuch des OPs, beispielsweise zwecks Login, kann der Besitzer der OpenID-Identität wiedererkannt werden, ohne jedoch zu wissen, welche Person es tatsächlich ist. Es wird lediglich das Pseudonym aus dem Personalausweis ausgelesen (genauer gesagt: berechnet). (Siehe Bild 2.)

Voraussetzungen zum Einsatz eines nPA-basierten OPs

Die Integration beziehungsweise Nutzung eines OpenID-Providers mit nPA-Unterstützung ist einfach. Für einen Anwender än-

dert sich nur die Form der eigentlichen Authentisierung. Der Anwender muss nach wie vor beweisen, dass er tatsächlich im Besitz einer OpenID-Identität ist. Hierfür wird anstelle eines Passwortes eine auf dem nPA basierende starke Authentisierung – Besitz (nPA) und Wissen (geheime PIN) – durchgeführt. Das mittels nPA berechnete Pseudonym verlässt den OpenID-Provider nie. Die Prinzipien der Datensparsamkeit und Datenvermeidung werden eingehalten.

Dienstanbieter müssen zur Nutzung von OpenID eine entsprechende Schnittstelle in die Anwendung integrieren. Es existieren Bibliotheken für verschiedene Programmiersprachen, sodass die OpenID-Schnittstelle schnell realisiert werden kann. Für einen Dienstanbieter kommen keine zusätzlichen Kosten auf, da neben der integrierten Schnittstelle keine weiteren Voraussetzungen zu erfüllen sind. Ein OpenID-Provider mit nPA-Unterstützung ermöglicht nicht nur die Auslagerung der Authentisierung, sondern durch die Proxy-Funktionalität auch die indirekte Nutzung der eID-Funktion des nPAs.

Generelle Vorteile eines nPA-basierten OPs

Der Einsatz eines nPA-basierten OpenID-Providers hat mehrere Vorteile. Durch die eID-Funktion wird zum einen die Authentisierung des Anwenders sicherer gestaltet. Der Anwender ist durch die Verwendung des nPAs nicht mehr in der Lage, schwache Passwörter (zu kurz, einfach zu erraten etc.) zu wählen, die von einem Angreifer leicht „geknackt" werden können. Zum anderen ist das größte Problem von OpenID beim Einsatz von Passwörtern – Phishing – nicht mehr gegeben. Durch die Multi-Faktor-Authentisierung wird einerseits kein Geheimnis mehr über das Internet versendet. Andererseits findet durch die eID-Funktion eine Authentisierung des OPs statt. Nur ein OP im Besitz eines gültigen Berechtigungszertifikats kann Informationen – in diesem Falle das Pseudonym – aus dem nPA auslesen beziehungsweise berechnen.

Ein weiterer, genereller Vorteil ist die Zentralisierung, einerseits eingesetzt bei der digitalen Identität des Anwenders. Der Beweis der Identität, die Authentisierung, findet nur noch an einer Stelle im Internet statt (bei dem OP) und kann somit bewusster gewählt werden. Andererseits können, sofern es der Anwender wünscht, Informationen zentral gespeichert werden. Ein Anwender kann E-Mail-Adresse, Geburtsdatum und dergleichen bei dem OP hinterlegen und auf Wunsch an Internetdienste übermitteln lassen. So wird sichergestellt, dass die persönlichen Informationen nicht mehr redundant, veraltet und verteilt im Internet vorliegen. Außerdem werden die Zugangsberechtigungen zentralisiert. Ein Anwender muss nicht mehr jedem Internetdienst einzeln die Zugangsberechtigungen wie zum Beispiel Benutzername und Passwort anvertrauen, sondern nur noch einer zentralen Instanz. Die Sicherung der Zugangsberechtigung und somit der digitalen Identität kann konzentriert werden.

Nutzen und Vorteile für Anwender ...

Durch den Einsatz eines nPA-basierten OpenID-Providers wird dem Anwender eine Infrastruktur für Web-SSO kombiniert mit einer Multi-Faktor-Authentisierung zur Verfügung gestellt. Da der bereits vorhandene nPA genutzt wird, sind keine zusätzlichen SmartCards oder Lesegeräte notwendig. Durch das Berechtigungszertifikat des OPs kann der Anwender diesen eindeutig verifizieren.

Durch die weite Verbreitung von OpenID kann der Personalausweis auch leicht im privaten Bereich eingesetzt werden. Private Webseiten, die mittels Frameworks wie Drupal, Joomla, TYPO3, WordPress und dergleichen erstellt wurden, können über Plug-ins OpenID-fähig gestaltet werden. Einem Anwender stehen nicht mehr nur die von der Software angebotenen Authentisierungsmethoden zur Verfügung, sondern zusätzlich die des eingesetzten OPs. Die Administration privater Webseiten oder Blogs kann folglich leicht mit Multi-Faktor-Authentisierung abgesichert werden, wenn diese vom OP angeboten wird. Wenn der OP garantiert, dass die Login-Informationen nicht gespeichert und für eine Profilbildung analysiert werden, kann die Privatsphäre des Anwenders einfacher geschützt werden.

... und für Dienstanbieter

Wie bereits beschrieben, bewirkt das „Outsourcing" der Authentisierung, dass einem Anwender nicht nur die Authentisierungsmethoden der Software, sondern auch die

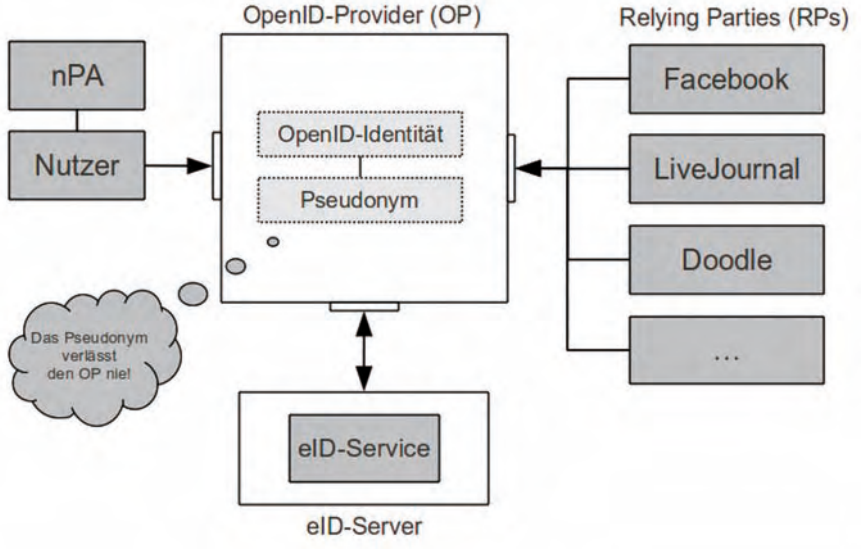

Bild 2: Das Bild zeigt das Konzept und die Schnittstellen eines OpenID-Providers mit Unterstützung des neuen Personalausweises. Im linken Bereich der Abbildung ist der Anwender dargestellt, der im Besitz eines nPAs ist. In der Mitte ist ein nPA-basierter OP abgebildet, der eine erstellte OpenID-Identität an das mittels Personalausweis ausgelesene Pseudonym knüpft. Hierüber wird der Anwender wiedererkannt. Im rechten Bereich der Abbildung sind verschiedene Internetdienste des Anwenders zu sehen, die alle eine OpenID-Schnittstelle implementiert haben. Im unteren Bereich ist ein sogenannter eID-Server eingezeichnet, der für die Kommunikation mit dem Personalausweis notwendig ist. Der OP benötigt ein von der Bundesregierung ausgestelltes Berechtigungszertifikat, womit Informationen aus einem nPA ausgelesen werden dürfen. In diesem konkreten Fall ist die einzige ausgelesene beziehungsweise berechnete Information das Pseudonym.

des eingesetzten OpenID-Providers zur Verfügung stehen. Dies ist auch ein Vorteil für einen Dienstanbieter, da dieser sich nicht um die Zugangsberechtigungen des Anwenders kümmern muss. Er vertraut, ebenso wie der Anwender, der Aussage des eingesetzten OPs. Zusätzlich bringt ein nPA-basierter OpenID-Provider eine gewisse „Internationalisierung" der eID-Funktion. Grundsätzlich ist der Einsatz des nPA für Anwendungen deutscher Dienstanbieter vorgesehen. Dienstanbieter, die über kein gültiges Berechtigungszertifikat verfügen, können den nPA beispielsweise für die Authentisierung nicht einsetzen.

Ein Dienstanbieter muss lediglich eine OpenID-Schnittstelle implementieren, um die Proxy-Funktionalität eines OPs mit nPA-Unterstützung nutzen zu können. Fortan können sich Anwender, die im Besitz eines deutschen nPAs sind, mithilfe des OpenID-Providers beim entsprechenden (internationalen) Internetdienst anmelden. Der Dienstanbieter kann keine Informationen aus dem nPA auslesen (auch nicht das Pseudonym), sondern nutzt die eID-Funktion indirekt über den OP. Ein Anwender kann folglich eine starke Authentisierung auch bei Dienstanbietern verwenden, die nicht über die nötigen finanziellen oder organisatorischen Ressourcen für den Einsatz der eID-Funktion verfügen.

Fazit und Ausblick

Im Internet besteht die Notwendigkeit, die Identität einer Person möglichst sicher zu beweisen. Offene Standards für Web-SSO wie etwa OpenID bieten eine einfache Möglichkeit. Die Schwächen des OpenID-Protokolls können durch die Verwendung der eID-Funktion des neuen Personalausweises kompensiert werden. Die größte Gefahr bei OpenID – Phishing – wird ausgeschlossen. Außerdem kann durch die Proxy-Funktionalität eines solchen OPs die Verwendung des nPAs ausgeweitet, quasi internationalisiert werden. Der OpenID-Provider des Instituts für Internet-Sicherheit wird einer der ersten seiner Art sein, der die Kombination von OpenID mit dem neuen Personalausweis anbietet. Da derzeit nahezu alle OPs lediglich eine Authentisierung mittels Benutzername und Passwort anbieten, wird ein OpenID-Provider mit nPA-Unterstützung eine willkommene und zudem sichere Alternative darstellen. Der Wechsel eines Anwenders zu einem anderen OP ist durch die dezentrale Architektur von OpenID ohne Probleme möglich. ■

Prof. Dr. (TU NN) Norbert Pohlmann,
Informatikprofessor für Verteilte Systeme und Informationssicherheit sowie Leiter des Institut für Internet-Sicherheit an der Fachhochschule Gelsenkirchen (www.internet-sicherheit.de)

B.Sc. Sebastian Feld,
wissenschaftlicher Mitarbeiter des Instituts für Internet-Sicherheit im Forschungsschwerpunkt Identity Management