Paper (2017) - Sicherheitsarchitektur
Roland Portmann, dipl. Ing. ETH

Identity Management bei Dialog G6

Die Sicherheitsarchitektur im Wandel

Aktuell findet in den IT-Umgebungen von Organisationen ein grösserer Anpassungsprozess statt, welchem verschiedene Ursachen zugrunde liegen können:

- Die Anzahl der den Mitarbeitern zur Verfügung stehenden Applikationen steigt. Damit wird es immer schwieriger die Mitarbeiter ausreichend zu schulen, so dass die Applikationen selbsterklärend sein müssen.
- Viele Mitarbeiter arbeiten gleichzeitig für mehrere Arbeitgeber und wollen nicht ständig das IT-Gerät wechseln.
- Mindestens ein Teil der Mitarbeiter will mit eigenen IT-Geräten arbeiten können (z.B. Home-Office). Es müssen daher BYOD-Konzepte (Bring Your Own Device) implementiert werden.
- Der Einsatz von Cloud-Services (Dropbox, Office 365, Streaming-Plattformen, Social Netzworks) nimmt auch im öffentlichen Bereich rasant zu.
- Es wird immer schwieriger die Grenzen einer öffentlichen Organisation festzulegen. Zunehmend kann selbst der Bürger über eGovernment-Applikationen auf seine Daten zugreifen.

Moderne Web-Applikationen adressieren die obigen Rahmenbedingungen. Daher ist aktuell bei vielen Organisationen ein starker Trend hin zu dieser zukunftsträchtigen Architektur festzustellen.

Single-Sign-On für erleichtertes Arbeiten und höhere Sicherheit

Bei den meisten Geschäftsaktionen muss sich ein Benutzer zuerst anmelden, so dass die Applikation festlegen kann, mit welchen Berechtigungen der Benutzer innerhalb der Applikation arbeiten darf. Der recht restriktive Datenschutz in der Schweiz verlangt zudem, dass der Zugriff auf Daten (lesend oder verändernd) möglichst stark eingeschränkt wird. Bei älteren Applikationen erschien beim Start eine Anmeldemaske, wo man seinen Benutzernamen und das Passwort angegeben musste. Neuere Applikationen benutzen die Identität, die man beim Anmelden an den Rechner eingeben muss. Mit diesem Single-Sign-On-Verfahren wurde das Arbeiten erleichtert und die Sicherheit erhöht, da der Benutzer sich nur einmal anmelden muss und zudem auch starke Authentisierungsverfahren (z.B. Anmeldung mittels Smartcards) zur Verfügung stehen. Im Hintergrund wurden die Identitäten mit einem «Active Directory» verwaltet. Das Active Directory übernimmt dabei die Funktion eines «Identity Providers».

Federated Identity Management: Eine Anmeldung in verschiedenen Umgebungen

Bereits vor ungefähr 10 Jahren kam man auf die Idee, dass es möglich sein müsste, dass eine Applikation mit mehreren Identity-Providern aus unterschiedlichen Organisationen zusammenarbeiten kann. Man entwickelte die Protokolle des «federated Identity Managements». Auf Hochschul-Ebene etablierte sich das Protokoll Sibboleth. Mit Hilfe dieses Protokolls können heute Hochschulangehörige Europaweit auf Applikationen anderer Hochschulen zugreifen. Im industriellen Bereich etablierten sich die weiterentwickelten Protokolle SAML 2 und Open ID Connect. Diese Protokolle sind insbesondere für Web-Applikationen geeignet. Microsoft arbeitet primär mit dem SAML 2-Protokoll (Office 365, Azure-Cloud-Services). Im Social Media Umfeld (Facebook, Google usw.) setzte man mehr auf Open ID Connect (resp. OAuth 2.0). Dank dieser Protokolle kann man sich auf mehreren Services mit dem gleichen Account (z.B. Facebook-Account) anmelden. Zudem muss man sich für den Zugriff auf mehrere Services nur ein einziges Mal anmelden (Single-Sign On).

Das Funktionsprinzip der verschiedenen Federation-Protokolle ist im Wesentlichen gleich:

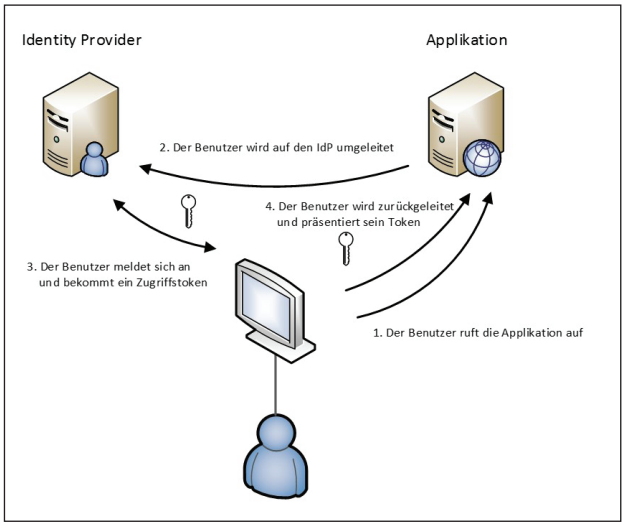
1. Ein Benutzer ruft mit dem Browser auf seinem Rechner die Webseite der Applikation auf.
2. Die Applikation stellt fest, dass sich der Benutzer noch nicht angemeldet hat und leitet den Browser auf die Webseite des Identity-Providers weiter (redirekt).
3. Der Benutzer meldet sich auf der Webseite des Identity-Providers an und bekommt ein Zugriffstoken. Das Zugriffstoken enthält die Identität des Benutzers und kann zusätzlich Berechtigungsinformationen (Authorisierung) enthalten.
4. Der Benutzer wird auf die Webseite der Applikation

zurückgeleitet (redirekt) und präsentiert sein Zugriffstoken.

5. Die Applikation überprüft das Token und gewährt dem Benutzer Zugriff auf die Applikation.

Bereits heute gibt es viele Identity Provider:

- Das Active Directory von Microsoft kann mit dem Dienst ADFS erweitert werden und unterstützt dann die Protokolle SAML 2.0 und Open ID Connect.
- Facebook, Google und weitere Dienste können als Identity Provider verwendet werden.
- Swisscom bietet mit Mobile ID einen Identity Provider an.
- Post und SBB bieten die SwissID an. Dies ist im Wesentlichen ein Identity Provider Dienst.
- Der von Dialog eingesetzte Dienst «Identity Server» übernimmt die Funktion eines Identity Providers und kann gleichzeitig die Dienste von weiteren Identity Providers verwenden.



Grafik 1: Funktionsprinzip eines Federation-Protokolls

Die Firma Dialog setzt bei Ihrer neusten Produktegeneration Dialog G6 den «Identity Server» ein. Dieses Produkt hat sich als Open-Source-Projekt breit etabliert und bietet eine vollständige Implementation der Protokoll-Suite OAuth 2.0 und Open ID Connect. Dieses Produkt erlaubt es, selbst Identitäten zu verwalten. Es hat eine eigene Benutzerdatenbank. Zudem erlaubt die Konfiguration des Identity-Servers die Einbindung von weiteren Identity Providern wie beispielsweise «Microsoft Active Directory», «Mobile ID von Swisscom» oder «Facebook». Neben der Verwaltung von Identitätsinformationen bietet «Identity Server» weitere Funktionen wie Session-Management, Validierungsservices für Token usw. an, die eine professionelle Web-Applikationsentwicklung vereinfachen.

Die gewählte Architektur der neuen Version von Dialog G6 hat für den Anwender grosse Vorteile:

- Der Benutzer meldet sich nur zu Beginn des Arbeitstages am «Active Directory» an und kann danach ohne neue Anmeldung direkt auf die Applikation Dialog G6 zugreifen.
- Das Authentisierungsverfahren wird vom Active Directory vorgegeben. So gelten beispielsweise die AD-Passwort-Richtlinien oder man könnte eine Mehrfaktor-Authentisierung bzw. eine biometrische Authentisierung vorsehen.
- Man kann weitere «Identity Provider» konfigurieren. So ist es beispielsweise möglich zusätzlich auch Swisscom Mobile ID als Identity Provider zu verwenden. So kann man auch ohne AD-Account mit der Applikation sicher arbeiten.
- Es wäre denkbar, dass ein Benutzer mehrere digitale Identitäten hat und damit auch unterschiedliche Zugriffsberechtigungen auf Dialog G6 hat. So kann man beispielsweise konfigurieren, dass ein Benutzer von seinem Home-Arbeitsplatz andere Berechtigungen hat, als am Büroarbeitsplatz.
- Es können auch Benutzer mit Dialog G6 arbeiten, die nicht im Active Directory erfasst sind, da Benutzer direkt im «Identity Server» konfiguriert werden können.
- Mit einer Deaktivierung eines Accounts auf dem Active Directory verliert ein Benutzer die Zugriffsberechtigungen an Dialog G6.

Die neue Software Dialog G6 besitzt eine sehr moderne Sicherheitsarchitektur und stellt sicher, dass auch zukünftige Anforderungen im Umfeld der Benutzerverwaltung elegant und effizient konfiguriert werden können.

Über den Autor: Roland Portmann dipl. Ing. ETH war bis 2016 hauptamtlich Dozent für Informationssicherheit an der Hochschule Luzern. Seine Erfahrungen beruhen auf seiner nebenamtlichen Tätigkeit als Berater für Informationssicherheit für diverse Security Firmen und Zertifizierungsorganisationen in verschiedenen Branchen, auch im öffentlichen Bereich.