Identitätsmanagement in Österreich mit MOA-ID 2.0

Thomas Lenz I Bernd Zwattendorfer I Klaus Stranacher I Arne Tauber

abstract

Mit der neuen Version 2.0 von MOA-ID wurde eine umfassende Modularisierung und Erweiterung vorgenommen. Neben vereinfachten Möglichkeiten zur Integration von MOA-ID, wie eine web-basierte Konfiguration, stehen Service Providern nun viele moderne Funktionen eines Identity Providers zur Verfügung. So wurden neue Authentifizierungsprotokolle integriert, Single Sign-On wird unterstützt und die Möglichkeit des Clusterbetriebs geschaffen. Neben der Anmeldung in Vertretung ist nun auch eine Anmeldung ausländischer Personen möglich. Abgerundet werden die neuen Funktionen über ein internes Monitoring und ein zusätzliches Logging für statistische Zwecke.

Die österreichische Bürgerkarte in Form von Chipkarte oder Handy-Signatur ist schon seit Jahren ein wesentlicher Bestandteil im österreichischen E-Government, speziell für die elektronische Kommunikation zwischen Bürgerin bzw. Bürger und Behörde. Neben der Möglichkeit zur Erstellung von elektronischen Signaturen, welche rechtlich handschriftlichen Unterschriften gleichgestellt sind, findet die Bürgerkarte vor allem Einsatz für die sichere und eindeutige Identifizierung und Authentifizierung von Bürgerinnen bzw. Bürgern bei behördlichen oder privatwirtschaftlichen Online-Anwendungen. Um diesen erhöhten Mehrwehrt einer sicheren Identifizierung und Authentifizierung mittels Bürgerkarte auch einfach bei Online-Anwendungen einbinden zu können, bietet das Bundeskanzleramt das Open Source Softwaremodul MOA-ID (Module für Online Applikationen – Identifikation) an. Dieses Modul übernimmt bzw. vereinfacht den Verifikationsprozess bei einer Bürgerkarten-Anmeldung. Weiters stellt es die Identifikations- und Authentifizierungsdaten der jeweiligen Bürgerin bzw. des jeweiligen Bürgers der Online-Anwendung in strukturierter Form zur Verfügung.

Nachdem E-Government zur Effizienzsteigerung von Behördenwegen immer wieder neuen Anforderungen ausgesetzt ist, bedarf es auch entsprechender Anpassungen in einzelnen Modulen wie MOA-ID, um diesen Anforderungen gerecht zu werden. Neue Anforderungen im Identifizierungs- und Authentifizierungsbereich sind beispielsweise eine Authentifizierung in Vertretung mittels elektronischer Vollmachten, die Authentifizierung ausländischer Bürgerinnen und Bürger aufgrund der Dienstleistungsrichtlinie oder neue moderne Authentifizierungsprotokolle, welche zusätzliche Sicherheit bringen. Um diesen neuen Anforderungen im E-Government gerecht zu werden wurde MOA-ID in Bezug auf Sicherheit, Modularität und Vollmachtenunterstützung vollständig überarbeitet.

Die Version 2.0 von MOA-ID (derzeit im Testbetrieb, die öffentliche Release ist für das Quartal 1 2014 geplant[(1)]) unterstützt unterschiedliche Anwendungsfälle, wie z.B. reine Bürgerkartenanmeldung, Authentifizierung in Vertretung mittels elektronischer Vollmachten oder auch die Authentifizierung ausländischer Bürgerinnen und Bürgern. Alle Authentifizierungsvorgänge können von MOA-ID 2.0 auch als Single Sign-On Anmeldung durchgeführt werden, wodurch eine Anmeldung an unterschiedlichen Applikationen nach einmaliger erfolgreicher Authentifizierung ohne erneute Eingabe von Anmeldedaten möglich wird. Eine für Provider von Online-Applikationen interessante Neuerung ist die überarbeitete und vereinfachte Konfiguration, welche die Integration einer Bürgerkarten-Anmeldung in eine bestehende Web-Applikation deutlich vereinfacht. Hierfür wurde MOA-ID 2.0 um ein Konfigurationstool ergänzt, mit dessen Hilfe die MOA-ID Instanz komfortabel über ein HTML Interface verwaltet werden kann. Mit zusätzlichen Funktionen wie ein erweitertes Monitoring der internen Funktionsabläufe oder eine Statistikfunktion für anonymisierte Zugriffsstatistiken bietet MOA-ID 2.0 viele Funktionen eines modernen Identity Providers.

In Abbildung 1 ist die Architektur von MOA-ID 2.0 dargestellt. Ein markanter Unterschied zur vorhergehenden Version ist die Modularität der neuen Version. Alle Hauptkomponenten (Auth Sources, Protocol Adapter, Zusatzmodule) weisen nun ein modernes und modulares Design auf, wodurch die Integration zusätzlicher Authentifizierungsmechanismen oder die Unterstützung neuer Authentifizierungsprotokolle einfach möglich ist.

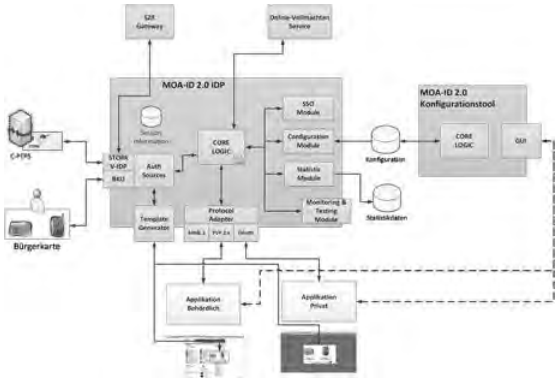

Abb. 1: Modulare Architektur von MOA-ID 2.0

Es müssen nur die dafür vorgesehenen Schnittstellen entsprechend implementiert werden.

Bisher wurde von MOA-ID ausschließlich SAML1[2] als Identitäts- und Authentifizierungsprotokoll unterstützt. Da SAML1 jedoch nicht mehr den aktuellen Sicherheitsanforderungen an einen modernen Identity Provider entspricht, stehen ab der MOA-ID Version 2.0 zusätzliche Authentifizierungsprotokolle zur Verfügung. Diese zusätzlichen Protokolle sind das Portalverbundprotokoll 2.1[3] (PVP2), welches auf SAML2[4] basiert, und OpenID Connect[5], ein leichtgewichtiges Identitätsprotokoll, welches auf dem OAuth2[6]-Standard aufbaut. Die zur Verfügung stehenden Protokolle werden im Laufe der Zeit erweitert. So wird aktuell eine Integration von OpenID[7] analysiert und evaluiert. Die Auswahl an Protokollen soll Betreibern von öffentlichen Applikationen den Umstieg von SAML1 auf aktuellere und sicherere Protokolle erleichtern.

Neben der Identifizierung und Authentifizierung mittels Bürgerkarte oder Handy-Signatur steht ab MOA-ID 2.0 auch eine Anmeldung von Bürgerinnen und Bürgern aus anderen EU Mitgliedsländern über das STORK[8]-Framework zur Verfügung.

Die Architektur in Abbildung 1 zeigt jedoch auch weitere Neuerungen, welche für Betreiber einer MOA-ID Instanz interessant sind. Der Hauptteil der Konfiguration wird ab Version 2.0 in eine Konfigurationsdatenbank ausgelagert, welche über ein mitgeliefertes Konfigurationstool verwaltet werden kann. Dies hat nicht nur den Vorteil, dass die Verwaltung über ein grafisches Interface erfolgt, sondern auch dass im Falle von MOA-ID im Clusterbetrieb allen Instanzen zentral konfiguriert werden können. Für Servicebetreiber, für welche eine hohe Verfügbarkeit wichtig ist, bietet MOA-ID 2.0 ein internes Monitoring- und Testmodul, mit deren Hilfe es möglich ist, den internen Status und die Verfügbarkeit der Anmeldefunktionalität zu prüfen, wobei alle relevanten internen Teile wie z.B. die Kommunikation mit dem Signatur-Prüfservice überprüft werden. Zusätzlich steht ein erweitertes anonymisiertes Logging von Zugriffsdaten oder aufgetretenen Anmeldefehlern zur Verfügung. Hiermit ist Service Providern eine zusätzliche Möglichkeit zur Service- und Auslastungskontrolle zugänglich.

Zusammenfassend unterstützt MOA-ID 2.0 folgende Anwendungsfälle:

- Sichere Identifizierung und Authentifizierung österreichischer Bürgerinnen und Bürger mittels Bürgerkarte oder Handy-Signatur
- Anmeldung in Vertretung von natürlichen oder juristischen Personen
- Sichere Identifizierung und Authentifizierung von Bürgerinnen und Bürger aus anderen EU Mitgliedsländern

Im Vergleich zur Vorgänger-Version von MOA-ID besitzt die Version 2.0 die folgenden Neuerungen bzw. Features:

- Modulares und einfach erweiterbares Design
- Unterstützung unterschiedlicher Identitätsprotokolle wie PVP2 (auf Basis von SAML2) oder OpendID Connect
- Vereinfachter und komfortabler Anmeldeprozess mittels Single Sign-On
- Administrationsfreundliches Web-Interface zur Konfiguration
- Möglichkeit des Clusterbetriebs
- Internes Monitoring- und Testmodul zur Überprüfung des internen Status und der Verfügbarkeit von Services
- Erweiterte Logging-Möglichkeiten für statistische Zwecke
- Einbinden des STORK-Frameworks zur Unterstützung der Anmeldung ausländischer EU Bürgerinnen und Bürger.

literatur

[1] Veröffentlicht unter: https://joinup.ec.europa.eu/software/moa-idspss/description.

[2] P. Hallam-Baker et al.: "Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML)", OASIS Standard, September 2003, http://www.oasis-open.org/committees/download.php/2290/oasis-sstc-saml-1.0.zip.

[3] M. Pellmann et al.: „Portalverbundprotokoll Version 2 S-Profil", AG Integration und Zugänge, August 2013, http://reference.e-government.gv.at/uploads/media/PVP2_S-Profil_2-1-0_20130823.pdf.

[4] S. Cantor et al.: "Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0", OASIS Standard, March 2005, http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf.

[5] OpenID Connect, http://openid.net/connect.

[6] OAuth 2.0, http://oauth.net/2.

[7] B. Fitzpatrick et al: "OpenID Authentication 2.0", OpenID Foundation, Dezember 2007, http://openid.net/specs/openid-authentication-2_0.html.

[8] Secure Identity Across Borders Linked (STORK), https://www.eid-stork.eu/.

DI Thomas LENZ
E-Government Innovationszentrum (EGIZ); thomas.lenz@egiz.gv.at

DI Bernd ZWATTENDORFER
E-Government Innovationszentrum (EGIZ); bernd.zwattendorfer@egiz.gv.at

DI Klaus STRANACHER
E-Government Innovationszentrum (EGIZ); klaus.stranacher@egiz.gv.at

Dr. Arne TAUBER
E-Government Innovationszentrum (EGIZ); arne.tauber@egiz.gv.at