eID

Digitales Ich ausweisen

[08.01.2019] Durch technologischen Fortschritt und gesetzliche Vorgaben wachsen die Anforderungen im Umgang mit digitalen Identitäten. Auch steigt mit der zunehmenden Heterogenität von eIDs die Bedeutung von Identitätsmanagement-Systemen und ihrer interoperablen Gestaltung.

Wir verfügen im Netz – anders als in der analogen Welt – nicht nur über eine, sondern über eine Vielzahl von Identitäten, die sich je nach Bedarf und Anforderung unterscheiden und an die meist persönliche Daten gekoppelt sind. Da Identitätsdiebstähle immer mehr zunehmen, sind nicht nur, aber vor allem, im E-Government und im E-Banking sichere elektronische Identitäten (eID) mit unterschiedlichen Merkmalen auf unterschiedlichen Vertrauenslevels unerlässlich. Die Bundesregierung hat vor einigen Jahren die rechtliche Grundlage für sichere Identitäten im Netz geschaffen und mit der Online-Ausweisfunktion des Personalausweises – beziehungsweise des elektronischen Aufenthaltstitels für Nicht-EU-Bürger – eine eID an ein hoheitliches Dokument gekoppelt. Seit November 2010 werden diese beiden Dokumente mit einer verwendbaren eID ausgegeben und die entsprechenden Infrastrukturen bereitgestellt. In anderen EU-Mitgliedstaaten sind parallel dazu ebenfalls eID-Infrastrukturen entstanden. Darüber hinaus hat die Europäische Kommission mit einer Verordnung für elektronische Identitäten, Authentifizierung und Signaturen den gesetzlichen Rahmen für den Umgang mit sicheren Identitäten sowie deren gegenseitige Anerkennung innerhalb Europas geschaffen. Der deutsche Personalausweis wurde als erstes eID-System im Zuge der eIDAS-Verordnung notifiziert, weitere Mitgliedstaaten befinden sich in der Notifizierung.

Nur drei Klicks

Außerhalb der politischen Arena sind ebenfalls eID-Infrastrukturen entstanden, die unseren Alltag durchziehen. In den unterschiedlichen Segmenten treffen wir auf verschiedene Identitätstoken mit einem oder mehreren Faktoren zur Sicherung des Zugangs zu den eIDs. Zu nennen wären hier beispielsweise das Online-Banking und Identitätsplattformen wie Verimi oder NetID. Die Komplexität der verschiedenen Verfahren stellt dabei nicht nur eine Herausforderung für jeden einzelnen dar, sondern auch für die Anbieter von Online-Dienstleistungen und -Prozessen. Identitätsmanagement-Systeme sind heutzutage ein wichtiger Bestandteil von IT-Infrastrukturen. Die Bedeutung dieser Systeme und ihrer interoperablen Gestaltung wird mit der zunehmenden Heterogenität von eIDs weiter zunehmen. Und damit steigt auch der Bedarf an einer Vergleichbarkeit dieser Verfahren im Hinblick auf Verlässlichkeit, Vertrauensniveau und Nutzerfreundlichkeit.
In seiner Sitzung am 14. Dezember 2016 hat das Bundeskabinett neue Maßnahmen zur Beflügelung des E-Governments in Deutschland beschlossen. Bund, Länder und Kommunen werden verpflichtet, alle geeigneten Verwaltungsdienstleistungen innerhalb von fünf Jahren als Online-Fachverfahren anzubieten. Um die Suche nach Dienstleistungen und den dafür zuständigen Anbietern zu erleichtern, wird das Ziel verfolgt, dass jeder Dienst mit drei Klicks aus jedem Verwaltungsportal heraus erreichbar sein soll. Aus diesem Grund sollen die Verwaltungsportale aller Administrationsebenen zu einem Portalverbund zusammengeschlossen werden.

Zentrales Anmeldesystem

Die Nutzung der meisten Dienstleistungen ist personalisiert, etwa wenn ein Bürger einen Termin beim Amt reservieren oder ein Unternehmen seine Dienstleistungen einer Kommune in Rechnung stellen möchte. Die entscheidende Voraussetzung für den Ausbau von Online-Fachverfahren ist also, dass Bürger und Unternehmen sich im Internet gegenüber einem Verwaltungsdienstleister schnell, benutzerfreundlich und sicher identifizieren können. Zum Zweck der Authentisierung werden aktuell von allen Bundesländern und vom Bund Nutzer- beziehungsweise Servicekonten eingerichtet. Dabei handelt es sich um Identitätsmanagement-Systeme, die gegenüber den Service-Providern die Rolle des Identity Provider (IdP) einnehmen, also gewissermaßen als zentrales Anmeldesystem zwischen Nutzern und Anbietern von Dienstleistungen fungieren. Dem Nutzer bieten die Konten Web-Oberflächen zur Administration seines Accounts. Nutzerkonten werden dabei zunächst nur für natürliche Personen eingeführt. Dadurch können Bürger E-Government-Dienstleistungen unter Verwendung einer einzigen elektronischen Identität abrufen. In einer weiteren Ausbaustufe werden auch Nutzerkonten für Organisationen eingeführt. Dazu werden Rollen für Vertreterregelungen definiert, sodass natürliche Personen im Auftrag eines Unternehmens E-Government-Leistungen in Anspruch nehmen können.

Föderiertes Identitätsmanagement-System

Eine besondere Herausforderung bei der Etablierung der Nutzerkonten ergibt sich aus der föderalen Struktur der Bundesrepublik. Jedes Bundesland und auch der Bund werden eigene Instanzen eines Nutzerkontos installieren. Jedes Fachverfahren delegiert die Nutzerauthentifizierung an das Konto desjenigen Bundeslandes, dem das Fachverfahren zugeordnet ist. Bundesweit sollen jedoch alle Fachverfahren unabhängig davon, wo der Bürger oder das Unternehmen sein Nutzerkonto angelegt hat, nutzbar sein. Um dies zu realisieren, muss ein Mechanismus der Identitätsweitergabe (Identity Propagation) von einem Nutzerkonto zu einem anderen entwickelt werden. Alle Nutzerkonten müssen interoperabel für Fachverfahren und Nutzer einsetzbar sein und bilden damit zusammen ein föderiertes Identitätsmanagement-System. Betrachtet man nun die unterschiedlichen Vertrauensniveaus, die sich auch aus der eIDAS-Verordnung ergeben – normal, substanziell und hoch –, sind aktuell die Niveaus normal (Benutzername und Passwort) sowie hoch (Online-Ausweisfunktion) verfügbar. Die eID-Funktion des Personalausweises hat neben der hohen Vertrauensstellung den Vorteil, dass sie schriftformersetzende Qualität hat, also mit einer qualifizierten elektronischen Signatur gleichgesetzt werden kann. Für die meisten Verwaltungsvorgänge ist allerdings gar keine hohe Authentisierung notwendig und auch nur rund zehn Prozent aller Vorgänge bedürfen der Schriftform und sind somit klassische Anwendungsszenarien für die Online-Ausweisfunktion. Die Verwendung von Benutzername und Passwort ist an den meisten Stellen jedoch auch kein ausreichend sicherer Zugang, um vertrauensvolles Verwaltungshandeln auszulösen. Hier erscheint es zielführend, weitere vorhandene und etablierte Authentisierungstoken in Betracht zu ziehen. Mit dem Log-in am Servicekonto über die ELSTER-ID, ein Bankkonto oder auch andere Identitätsplattformen, wie Verimi (sofern der Account dort mit einem entsprechenden Niveau angelegt wurde), könnte beispielsweise ein substanzielles Niveau erreicht werden. Synergieeffekte zu nutzen, ist angesichts der rasanten Entwicklungen rund um elektronische Identitäten nicht nur sinnvoll, sondern notwendig, nicht zuletzt, um die Akzeptanz bei den Nutzern zu erhöhen, ohne auf eine entsprechende Vertrauensstellung und Datenqualität verzichten zu müssen. Google- und Facebook-Log-ins, so bequem sie sein mögen, sind aus Datenschutzgründen im E-Government kein Mittel der Wahl.

Integraler und interoperabler Ansatz

Das Unternehmen Governikus beschäftigt sich seit vielen Jahren mit der Komplexität elektronischer Identitäten. Die in der Anwendung Governikus des IT-Planungsrats enthaltenen Produkte und

Komponenten verfolgen dabei einen integralen und interoperablen Ansatz, mit denen sich föderale Szenarien realisieren lassen und die darüber hinaus als Authentisierungsbroker die Verwendung weiterer Identitätstoken, wie ELSTER, Online-Banking oder Verimi, ermöglichen.

()

Dieser Beitrag ist in der Ausgabe Januar 2019 von Kommune21 im Schwerpunkt Digitale Identität erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: Digitale Identität, Governikus, Identitätsmanagement, Portalverbund