Fraunhofer FOKUS

FRAUNHOFER-INSTITUT FÜR OFFENE KOMMUNIKATIONSSYSTEME FOKUS

VERTRAUENSWÜRDIGE DIGITALE IDENTITÄT: BAUSTEIN FÜR ÖFFENTLICHE IT

Ansprechpartner

Jens Fromm
Leiter Kompetenzzentrum
Öffentliche IT
Tel. +49 (0)30 3463-7173
Fax +49 (0)30 3463-99-7173
jens.fromm@fokus.fraunhofer.de

Fraunhofer FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin

www.fokus.fraunhofer.de
www.oeffentliche-it.de

Kompetenzzentrum Öffentliche IT

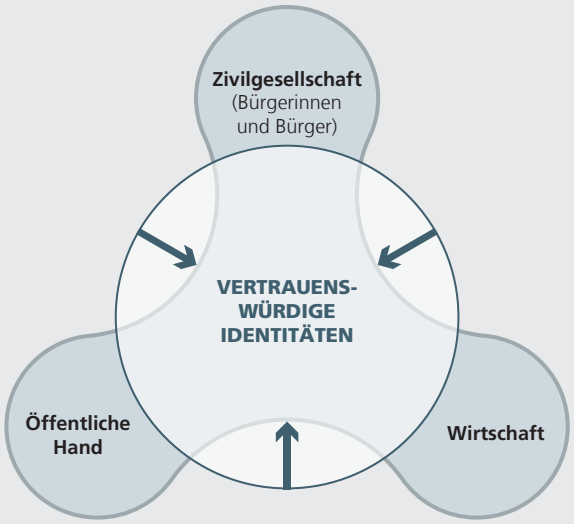
GEFÖRDERT VOM
Bundesministerium des Innern

Öffentliche IT funktioniert nur, wenn sie vertrauenswürdig ist. Dieses Vertrauen zu schaffen und es zu erhalten, ist nicht nur eine große Herausforderung, sondern auch eine dauerhafte Aufgabe, die regelmäßige gesellschaftliche Debatten erfordert. Digitale Identitäten bilden einen entscheidenden Vertrauensanker zur Erkennung von Entitäten, wie beispielsweise Personen, Organisationen, Dienste oder Objekte, im digitalen Raum.

Digitale Identitäten

Die Durchdringung aller Lebensbereiche mit Informationstechnologien nimmt stetig zu. Viele Bereiche des öffentlichen Lebens wären bereits heute ohne den Einsatz von IT kaum noch denkbar – sei es bei der Energieversorgung, der Kommunikation oder auch der organisationsübergreifenden Zusammenarbeit. Dem Staat fällt dabei eine immer komplexere Rolle hinsichtlich der Daseinsvorsorge zu. Insbesondere für die elektronische Kommunikation und Identifikation bildet der Faktor Vertrauen eine wichtige Grundlage. In der realen Lebenswelt können persönliche Begegnungen eine Basis der Vertrauensbildung darstellen. Analogen Mechanismen bedarf es auch in der digitalen Welt, insbesondere, da es hier einfacher ist, eine scheinbare Vertrauenswürdigkeit vorzuspiegeln.

Digitale Identitäten sind ein Mechanismus zur Etablierung von Vertrauen und damit ein elementarer Baustein für öffentliche IT. Sie dienen der Identifikation oder Genehmigung von Aktionen im Internet, wie beispielsweise dem Kauf von Produkten, der Autorisierung von Finanztransaktionen oder auch dem Nachweis von Zugangsvoraussetzungen wie etwa einer Altersbestätigung. Da elektronische Kommunikation zwangsläufig immer über eine technische Infrastruktur erfolgt, sind Mechanismen der Vertrauensbildung bereits bei der Konzeption der Ihr zugrunde liegenden Systeme miteinzubeziehen.



Vertrauenswürdige Identitäten ermöglichen eine verlässliche Kommunikation zwischen den unterschiedlichen Subsystemen öffentlicher IT.

Sicher und vertrauenswürdig

Immer dann, wenn Personen, Organisationen, Objekte oder Dienste im öffentlichen Raum miteinander kommunizieren, werden Mechanismen für sichere und vertrauenswürdige Identitäten benötigt. Sicher und vertrauenswürdig bedeutet in diesem Fall nicht die vollständige Offenlegung eigener Daten, sondern lediglich die Sicherstellung ihrer Authentizität. Bei Personen ist der Grad der Anonymität häufig Gegenstand gesellschaftlicher Debatten. So wie es heute in der analogen Welt Orte der Privatheit gibt, muss es diese auch im digitalen Raum geben. Anonymität und Pseudonymität müssen als legitime Konzepte gesellschaftlich etabliert und fundiert werden.

Vertrauenswürdige Kommunikation heißt auch, dass sich Kommunikationspartner fair und in angemessener Art und Weise identifizieren. Geht es darum, sensible Daten preiszugeben, muss die Identifikation auf Gegenseitigkeit beruhen. Als Vorbild kann hier die Online-Ausweisfunktion des neuen Personalausweises dienen.

Digitale Identitäten werden heute häufig von privatwirtschaftlichen Unternehmen vergeben. Gerade im Bereich der elektronischen Verwaltung bedarf es jedoch zumeist verlässlicher Identitäten, die im Optimalfall von staatlicher Seite bestätigt sind. Die Ausgabe digitaler Identitäten kann also nicht allein globalen IT-Unternehmen überlassen werden. Mechanismen zur Etablierung vertrauenswürdiger Kommunikation sollten außerdem von anderen marktwirtschaftlichen Interessen getrennt werden.

Herausforderungen

Heutige Verfahren wiegen die Nutzer allzu oft in falscher Sicherheit. Falsche oder nicht vertrauenswürdige Nachweise werden von den Nutzern häufig ignoriert oder nicht verstanden. Herkömmliche technische Mechanismen zur Identifikation und Authentisierung, wie Benutzername und Passwort stoßen zunehmend an ihre Grenzen. Der Bedarf nach alternativen Verfahren führt bereits zu zahlreichen neuen Entwicklungen sowohl aus dem privatwirtschaftlichen als auch dem staatlichen Bereich.

Eine weitere Herausforderung öffentlicher IT-Systeme ist deren Interoperabilität, also die Fähigkeit mit anderen Systemen zusammenzuarbeiten. Obwohl es auch für digitale Identitäten bereits technische Standards gibt, zeigt sich, dass gerade das Identitätsmanagement in vielen Bereichen noch eine Individuallösung ist. Dabei stellt sich heraus, dass weniger die technischen als vielmehr unterschiedliche rechtliche Rahmenbedingungen die größere Herausforderung darstellen.

Trend: Vernetzte Objekte

Mit der steigenden Automatisierung und Vernetzung öffentlicher IT rücken auch digitale Identitäten von Objekten zunehmend in den Mittelpunkt. Dieser Trend wird häufig unter dem Stichwort Internet der Dinge zusammengefasst. Objekte interagieren dabei mit einer Reihe unterschiedlicher Kommunikationspartner.

Die Absicherung dieser Kommunikation ist ein zentrales Thema. Neben technischen Fragestellungen sind dabei insbesondere auch rechtliche Aspekte zu erörtern.

Die Vernetzung von Objekten hat bereits die Endanwender erreicht. Viele Hersteller setzen auf diesen Trend und erstellen Produkte zur Heimautomatisierung, die über Smartphones oder das Internet gesteuert werden können. Im Bereich der öffentlichen Infrastruktur steht vor allem das Verkehrswesen vor großen Veränderungen. Unter dem Stichwort »Car2X-Kommunikation« wird intensiv an sicheren Kommunikationsmechanismen zwischen Fahrzeugen oder Fahrzeugen und anderen Systemen geforscht. Derartige Systeme sind bereits sehr weit entwickelt, wie man etwa beim eCall-System (emergency call) – einem automatischen Notrufsystem für Fahrzeuge innerhalb der EU – sehen kann.

Das Internet der Dinge bietet ein hohes Innovationspotenzial für die Zukunft. Der Bedarf an sicheren Identitätslösungen für Objekte wird daher weiter steigen. Hierbei sind auch gesellschaftliche Debatten zu führen um Nutzen, Sicherheit und Da-tenschutz miteinander in Einklang zu bringen.

Im Sinne öffentlicher IT müssen dabei interoperable, sichere Lösungen für digitale Identitäten gefunden und weiterentwickelt werden. Hier sind Forschung, Wirtschaft und Verwaltung in gleicher Weise gefordert.