



Thesepapier des Arbeitskreises „Datenschutz und IT-Sicherheit“ der Gesellschaft für Informatik zur

Gestaltung von Identitätsmanagementsystemen

Identitätsmanagementsysteme (IdM-Systeme) befassen sich mit der Verwaltung von Benutzermerkmalen, die nicht nur Identifizier, sondern auch weitere Attribute umfassen. Ein Beispiel ist der neue elektronische Personalausweis, der Identifizierung und Authentifizierung auch im Internet unterstützt. Im Zuge der Suche nach datenschutzfreundlichen Methoden zu Identifizierung und Authentifizierung im Internet finden neue IdM-Systeme Verbreitung. Sie müssen den Benutzer dabei unterstützen, im jeweiligen Anwendungskontext nur die relevanten Attribute zu offenbaren und ggf. zu belegen.

Die Technik des kryptographisch gesicherten Identitätsmanagements, wie sie in den EU-Projekten PRIME und PrimeLife prototypisch vorgeschlagen wird, unterstützt verbindliches Handeln bei gleichzeitigem Schutz der Privatsphäre. Gleichzeitig wird es möglich, ausgewählte Attribute der eigenen Identität, etwa die Tatsache der Volljährigkeit, von dritter Seite bestätigt und ansonsten anonym zu präsentieren.

Damit kann diese Form des Identitätsmanagements grundsätzlich auch für den neuen elektronischen Personalausweis eingesetzt werden. Dies hätte folgende Vorteile:

- Vertrauensrelevante Eigenschaften der eigenen Person können anonym oder in Verbindung mit einem selbstgewählten Pseudonym nachgewiesen werden. Nicht erforderliche Information muss nicht präsentiert werden, etwa im Kontext nicht relevante Eigenschaften.
- Jede Person kann sich in mehreren Teilidentitäten mit verschiedenen personenbezogenen Attributen präsentieren, ohne dabei alle Identitätsinformationen preisgeben zu müssen.
- Nutzer können dadurch im Umgang mit Diensten ausgewählte Identitätsinformationen zielgerichtet einsetzen. Dies fordert und fördert eine „digitale Selbstständigkeit“ der Nutzer.
- Insbesondere besteht damit technisch kein Hinderungsgrund mehr, gemäß § 13 Abs. 6 Telemediengesetz Telemedien und ihre Bezahlung anonym oder unter Pseudonym anzubieten.

Die Realisierung dieser Vorteile hängt von einer Reihe von Bedingungen ab:

- Die Bedienbarkeit der Systeme muss so einfach und intuitiv sein, dass Nutzer tatsächlich in der Lage sind, sie im Alltag einzusetzen.
- Dienstanbieter müssen sich darauf einstellen, Geschäftsvorgänge auch mit weniger umfassenden aber gleichwohl hinreichenden Informationen abzuwickeln und dazu Policies und Abwicklungsprozesse zu entwickeln.



- Die technischen Systeme, die diese Verlässlichkeit und Privatheit mehreren Parteien anbieten, müssen in ihrer Funktionsweise für alle Beteiligten transparent sein, d.h. die Technik muss von unabhängigen Dritten jederzeit vollständig nachprüfbar sein.
- Standardisierung sollte in diesem Zusammenhang auf eine Vereinheitlichung der Benutzungsschnittstellen hinwirken.
- Die zugrunde liegende Technik sollte im Interesse von Nutzerunabhängigkeit und Verlässlichkeit auf Redundanz ausgerichtet werden. Entsprechende Schnittstellen sind zu standardisieren.
- Die Gesetzgebung muss die elektronische Erhebung personenbezogener Daten an die Möglichkeit einer verbindlichen Zustimmung binden und deren ebenfalls elektronisch signierten Widerruf ermöglichen.

Kontakt:

Gesellschaft für Informatik e.V. (GI)

Ahrstraße 45

53175 Bonn

Telefon: 0228 302145

www.gi.de

gs@gi.de