



■ Web Identitäten

Begriffsbestimmungen
und Einführung in das Thema

Oktober 2005

■ Impressum

Herausgeber:

BITKOM

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10
10117 Berlin-Mitte

Tel.: 030/27 576 – 0

Fax: 030/27 576 – 400

bitkom@bitkom.org

www.bitkom.org

Redaktion:

Klaus-Dieter Wolfenstetter (Deutsche Telekom AG),
k.wolfenstetter@telekom.de,
Dr. Sandra Schulz (BITKOM e.V)

Verantwortliches BITKOM-Gremium: Fachausschuss Identitäten- und Rollen-Management

Redaktionsassistentz:

Leila Ambrosio

Stand:

Oktober 2005, Finale Version

Die Inhalte dieses Leitfadens sind sorgfältig recherchiert. Sie spiegeln die Auffassung im BITKOM zum Zeitpunkt der Veröffentlichung wider. Die vorliegende Publikation erhebt jedoch keinen Anspruch auf Vollständigkeit. Wir übernehmen trotz größtmöglicher Sorgfalt keine Haftung für den Inhalt.

Der Leitfaden kann unter www.bitkom.org/publikationen kostenlos bezogen werden. Alle Rechte, auch der auszugsweisen Vervielfältigung, liegen beim BITKOM.

Ansprechpartner:

Dr. Sandra Schulz, BITKOM e.V.

Tel: +49 (0)30 / 27576 – 242

E-Mail: s.schulz@bitkom.org

Klaus-Dieter Wolfenstetter, Deutsche Telekom AG

Tel: +49(0)30 / 8353 - 58419

E-Mail: k.wolfenstetter@telekom.de

Inhaltsverzeichnis

1	Zusammenfassung.....	4
2	Einleitung	5
3	Definition und Zweck von WebIDs	6
3.1	Identität und digitale Identität	6
3.2	Profil.....	7
3.3	WebID und ihre Anwendungseigenschaften	8
4	Anwendungsszenarien für WebIDs.....	11
5	Generierung, Aufbewahrung und Sicherheit von WebIDs	19
6	Wirtschaftliche und rechtliche Rahmenbedingungen	21
6.1	Wirtschaftliche Rahmenbedingungen	21
6.2	Rechtliche Rahmenbedingungen.....	22
Anhang	24

1 Zusammenfassung

Wir alle bewegen uns heute wie selbstverständlich nicht nur in der realen, sondern auch in der virtuellen Welt des so genannten „Cyberspace“. Dabei ist für immer mehr Menschen das Internet zu einem festen Bestandteil ihres Lebens geworden.

Es entwickelt sich damit mehr und mehr zu einem sozioökonomischen Raum, in dem die Nutzer einen Teil ihrer Arbeits- und Freizeit verbringen. Einerseits herrscht immer noch eine, wenn auch oftmals vermeintliche Anonymität und Isolation des einzelnen Nutzers vor. Andererseits hat ein Nutzer verschiedene **Identitäten**, wenn er sich im Internet bewegt: In Chatrooms wird er unter einem selbst gewählten Anonym agieren, beim Online-Shopping verkauft er sein Buch unter einem Pseudonym und beim eBanking ist er unter dem zugewiesenen Benutzernamen aktiv. Diese vielen Identitäten müssen durch den Nutzer gehandhabt werden. Die verschiedenen Identitäten eines Nutzers sind im Internet als eine **Web Identität** (WebID) abbildbar. Die Definitionen zu den wichtigsten Begriffen wie Identität, Profil, Attribut, WebID sind in der Guideline festgelegt.

Um den verschiedenen **Rollen** eines Nutzers im Internet gerecht zu werden, unterscheidet man bei Web Identitäten zwei grundlegende Eigenschaften: Die **Einfachheit des Rückschlusses** von einer WebID auf den Nutzer (offen, pseudonym, anonym) und den **Grad der Rechtssicherheit** der WebID (allgemein, rechtssicher). Möchte der Nutzer nur eine einfache Stadtplanauskunft, so reicht ihm und dem Dienstanbieter eine allgemeine anonyme Identität. Unterschreibt der Nutzer seine Steuererklärung online, so ist seine WebID offen und rechtssicher. Abhängig von der Dienstleistung ergeben sich damit unterschiedliche Anforderungen an die Sicherheit einer WebID. Vergleicht man verschiedene Speichermedien wie Gedächtnis, Papier, Festplatte so haben mobile, geschützte Speichermedien wie Chipkarte oder USB-Token für den Nutzer als auch für den Diensteanbieter die meisten Vorteile. In der Guideline sind einige **Szenarien** mit unterschiedlichen Sicherheitsanforderungen beschrieben.

Setzt sich die Nutzung von sicheren, mobilen Speichermedien für die WebID durch, so ergeben sich zukünftig weitere neue **Geschäftsmodelle**. Auch bei der Verwaltung und Nutzung von WebIDs wird es in Zukunft neue Arten von Geschäftsfeldern geben. Vertrauenswürdige, sichere Single-Sign-On-Lösungen über mehrere Webdienste oder auch die Freigabe auf seine bei einem zentralen Dienstleister gespeicherten Attribute für einen neuen Webdienst durch den Nutzer sind denkbar bzw. schon realisiert.

Die Wirtschaftlichkeit hängt insbesondere von der Einfachheit der Handhabung, vom Erreichen der Skaleneffekte und der Universalität der Anwendbarkeit ab.

2 Einleitung

Ziel des Dokuments

Ziel des Papiers ist es, in das Thema Web Identitäten einzuführen, Begriffe zu definieren und wichtige Aspekte zu diskutieren. Grundlage ist hierbei die gängige Praxis. Außerdem werden an Hand von Szenarien Anforderungen, Lösungsansätze und Anwendungen aufgezeigt, welche im Internet im Umgang mit digitalen Identitäten bestehen. Das Papier soll Anregung für neue Geschäftsmodelle geben.

An wen richtet sich dieses Papier?

Dieses Papier richtet sich an Vertreter aus Politik, Behörden und Wirtschaft sowie dem Bürger (Nutzer/Endverbraucher).

Welche Themen werden behandelt?

Behandelt werden Art und Einsatz von digitalen Identitäten im Internet sowie der Umgang mit ihnen. Insbesondere wird auf die spezielle digitale Identitätsart Web Identitäten eingegangen.

Struktur des Dokuments

- 1 Zusammenfassung
- 2 Einleitung
- 3 Definition und Zweck von WebIDs
- 4 Anwendungsszenarien für WebIDs
- 5 Genierung, Aufbewahrung und Sicherheit von WebIDs
- 6 Wirtschaftliche und rechtliche Rahmenbedingungen
- 7 Anhang

Abgrenzung von anderen Dokumenten zu diesem Thema

Das Papier soll keine neuen technischen Standards oder Normen definieren.

3 Definition und Zweck von WebIDs

3.1 Identität und digitale Identität

Eine **Identität** ist eine in ihrem Verwendungskontext eindeutige, wiedererkennbare Beschreibung einer natürlichen oder juristischen Person oder eines Objektes z. B. Personengruppe, Unternehmen, Rechner, Programm, Datei.

Eine Identität setzt sich zusammen aus:

- **Attributen** zur Charakterisierung der Person / des Objektes sowie
- einem in seinem Gültigkeitsbereich eindeutigen **Identitätsbezeichner** (z. B. Personalnummer im Unternehmen, Rechner-Nummer)

Beispiele für die Attribute einer Personen-Identität (siehe Abbildung 1):

- Persönliche Merkmale (Name, Geburtsort, Adresse usw.)
- Körperliche Merkmale (Alter, Größe usw.)
- Fähigkeiten/persönliche Vorlieben (Interessen, Hobbys usw.)

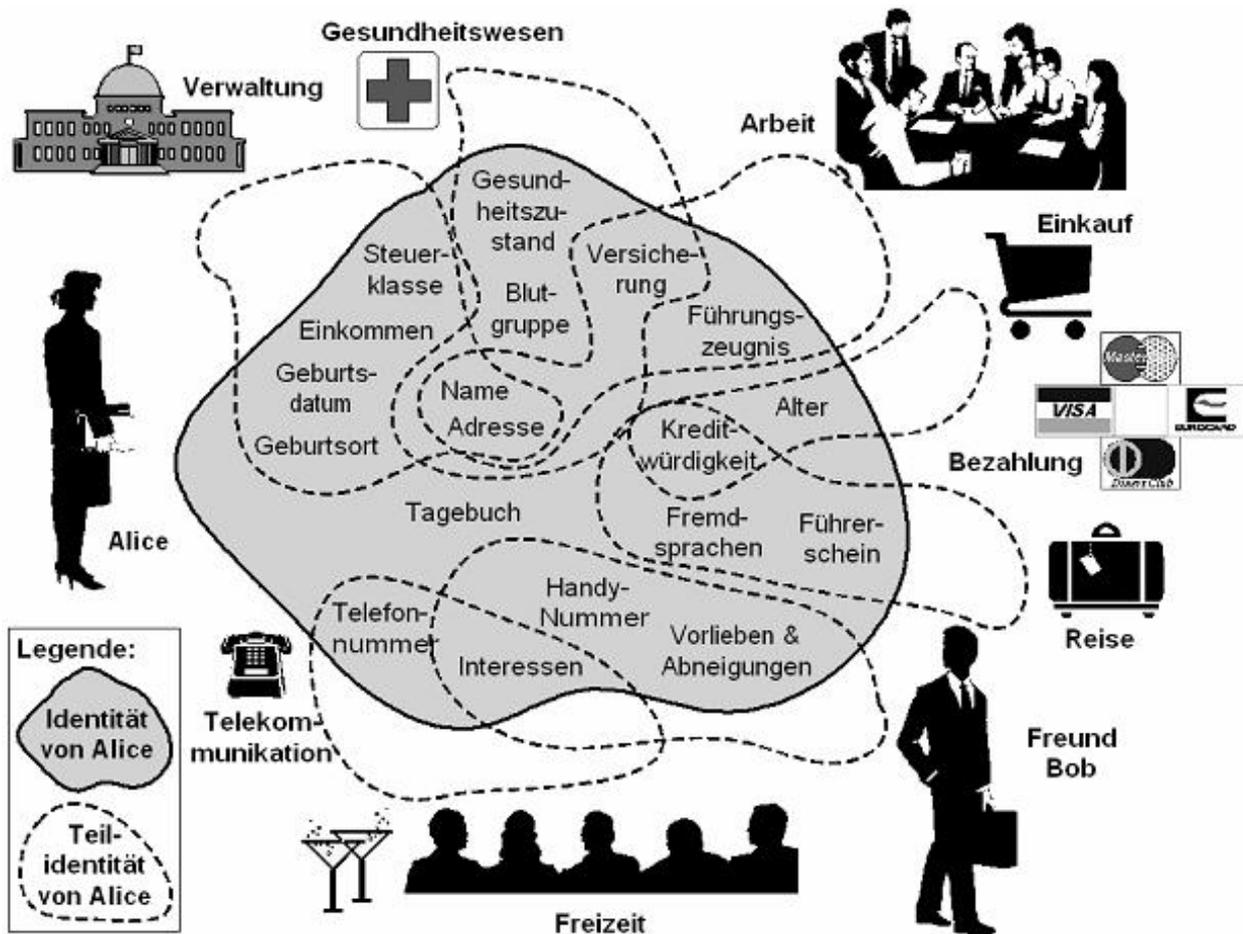


Abbildung 1: Darstellung von WebID-Profilen für verschiedene Anwendungen
Quelle: Marit Hansen, ULD Schleswig-Holstein

Eine **digitale Identität** ist eine Identität, die von einem Rechner verstanden und verarbeitet werden kann. Die digitale Identität entsteht, indem Attribute einer natürlichen Person oder eines Objektes in einem Rechner in elektronischer Form sicher registriert werden. Man spricht daher auch vom Identitäts-Lieferanten (engl. Identity Provider, kurz IdP).

Eine **Netzwerk-Identität** ist eine digitale Identität, die innerhalb eines elektronischen Netzwerks, z. B. von einem Unternehmen, verstanden wird.

Eine **föderierte Identität** ist eine Netzwerk-Identität, die in mehreren Netzwerken verstanden wird. Sie setzt eine zuvor in einem diesem Netzwerk registrierte Netzwerk-Identität voraus.

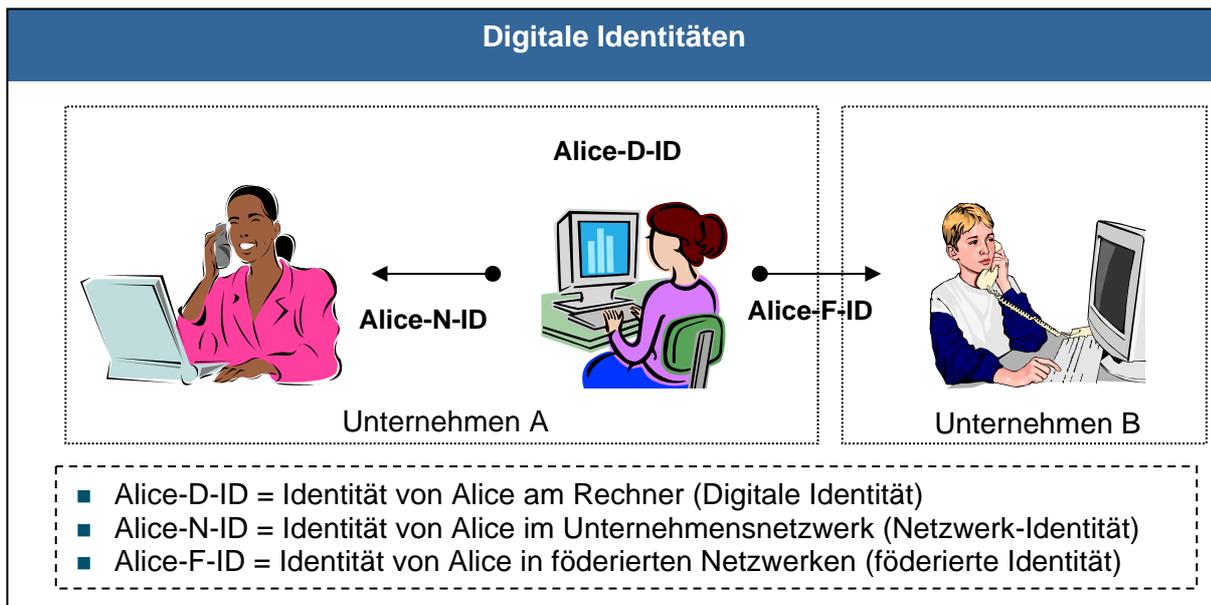


Abbildung 2: Digitale Identitäten

In der Abbildung 2 sind die drei Identitäten dargestellt: Alice arbeitet im Unternehmen A. Ihre digitale Identität am Rechner ist Alice-D-ID. Kommuniziert sie über den Rechner mit anderen Personen im Unternehmen, so wird dafür ihre Netzwerk-Identität Alice-N-ID genutzt. Kommuniziert sie mit Bob vom Unternehmen B, so wird ihre föderierte Identität Alice-F-ID verwendet.

Die Identitäten werden vom System (System-Management) verwaltet und untereinander referenziert. Alice meldet sich nur mit ihrer digitalen Identität am Rechner an, diese ergibt sich in der Regel aus dem Benutzernamen und dem Passwort.

3.2 Profil

Als (elektronisches) **Profil** bezeichnet man die bei der Registrierung einer digitalen Identität anzugebenden Attribute, welche zur Erlangung einer bestimmten Dienstleistung im Internet erforderlich sind. Je nach Diensteanbieter bzw. erwünschter Online-Dienstleistung ist ein Profil mehr oder weniger umfangreich.

Das Profil eines Kunden wird i. d. R. vom Dienstleister um zusätzliche, für die Geschäftsprozesse erforderlichen Attribute erweitert, z. B. Bankverbindung, Telefonnummern, Lieferadresse, Interessen des Kunden. In der Abbildung 3 ist dies schematisch dargestellt: Im Rahmen eines Registrierungsprozess z. B. bei einem Online-Buchshop gibt der Kunde zunächst seine E-Mail-Adresse sowie ein Passwort ein. Ein Profil mit Basisattributen wird angelegt. Kauft er später ein Buch, so wird seine Bankverbindung und seine Lieferadresse verlangt und dann im erweiterten Profil gespeichert.

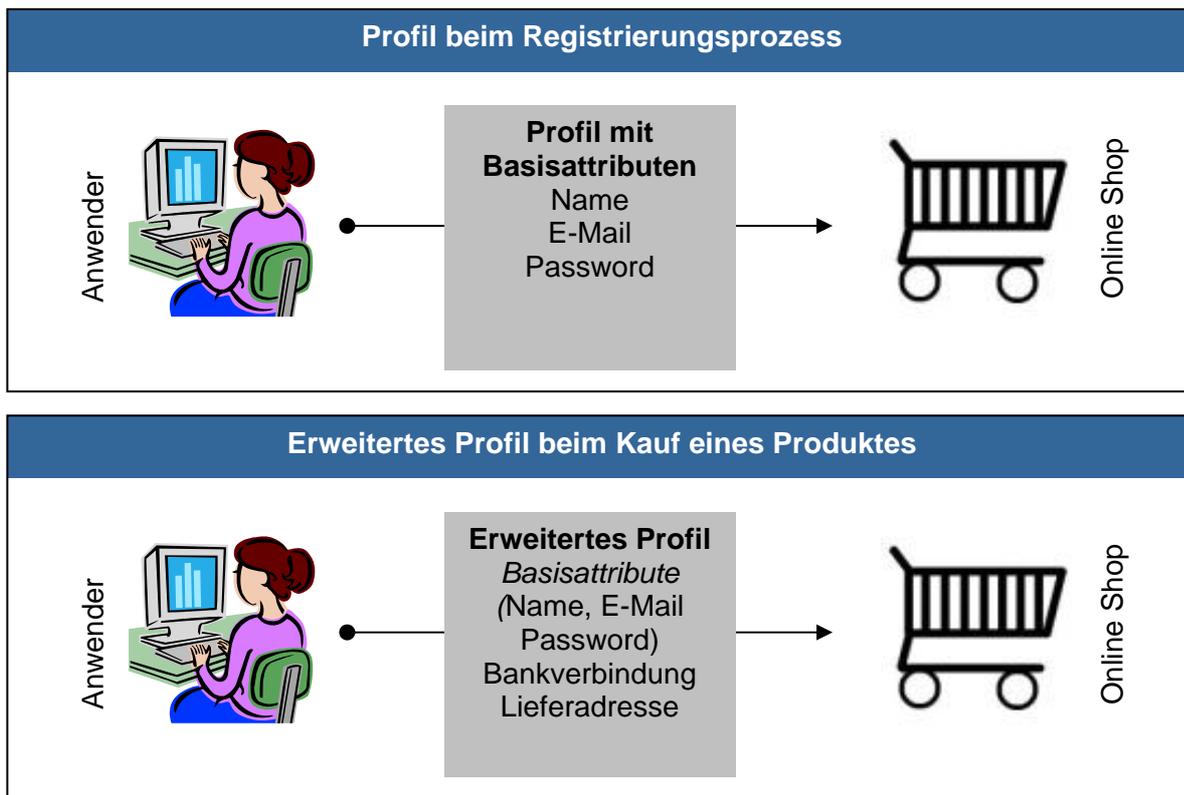


Abbildung 3: Profile

3.3 WebID und ihre Anwendungseigenschaften

Eine **WebID** ist eine Netzwerk-Identität oder föderierte Identität und ermöglicht die Nutzung von Dienstleistungen und Informationen im Internet. Sie bezieht sich in der Regel auf Personen, doch sind auch Anwendungen mit Bezug auf Objekte von Rechnern usw. denkbar.

Die registrierende Stelle (z. B. Behörde, Bank, Unternehmen) kennt die Identität des Identitätsbezeichners. Die Stelle definiert den Umfang der personenbezogenen Attribute, die ein Nutzer ihrer Dienste angeben muss. Für kostenlose Dienste kann ein Unternehmen bei der Registrierung einer WebID auf das Erfassen von personenbezogenen Attributen und deren Überprüfung verzichten. Gegenüber Dritten, etwa an Geschäftspartner der registrierenden Stelle, werden je nach Situation entweder nur der Identitätsbezeichner oder bestimmte Attribute der Identität offen gelegt.

In Online-Transaktionen unterscheiden sich also WebIDs gegenüber Transaktionspartnern vor allem dadurch,

- welche Attribute bei der Registrierung einer WebID erfasst wurden,
- welche Attribute einem Transaktionspartner mitgeteilt werden.

Beides zusammen definiert für die registrierende Stelle bzw. den Transaktionspartner die **Einfachheit des Rückschlusses** von einer WebID bzw. ihrem Identitätsbezeichner auf die handelnde Person oder Gruppe:

- Offene¹ Identitäten: Rückschluss auf die natürliche Person ist direkt möglich, da hinreichend viele persönliche Attribute erfasst bzw. mitgeteilt wurden;

¹ „Offen“ in Analoge zu offenen Benutzergruppen.

- Pseudonyme Identitäten: Rückbeziehung auf die natürliche Person ist für Transaktionspartner über die registrierende Stelle möglich;
- Anonyme Identitäten: Rückbeziehung auf die natürliche Person ist auch für die registrierende Stelle nicht möglich;

Zu beachten ist, dass hinter einem pseudonymen Identitätsbezeichner (z. B. X345) durchaus personenbezogene Attribute stehen können. Solche pseudonymen WebIDs sind aus drei Gründen verbreitet:

1. Geschäftsinteresse der Unternehmen, die eine Kunden-Identität registriert haben:
Ein Unternehmen ist in der Regel daran interessiert, Kundendaten für sich zu behalten und gegenüber Wettbewerbern zu verbergen.
2. Bereitschaft eines Kunden, personenbezogene Attribute zu liefern:
Anbieter von Onlinediensten machen die Erfahrung, dass der Kunde wesentlich mehr Details über seine persönlichen Verhältnisse preiszugeben bereit ist, wenn er darauf vertrauen kann, dass seine Daten hinter einem pseudonymen Identitätsbezeichner verborgen bleiben.
3. Datenschutz:
Eine Person beansprucht zumindest den gesetzlich geregelten Schutz personenbezogener Daten vor unerlaubter Verwendung und unerwünschter Verbreitung.

Wegen dieser Vorteile wird in vielen Fällen in Kauf genommen, dass pseudonyme WebIDs im Streitfall zu einem Mehraufwand bei Feststellung der dahinter verborgenen Person führen. Letztlich entscheidet allerdings der Anwendungsfall oder wie beim Online-Banking gesetzliche Regelungen, ob eine Offene WebID erforderlich ist.

Zum Schutz vor unbefugter Nutzung ist die WebID häufig durch eine 2-Faktoren-Authentisierung gesichert. Das heißt, der Nutzer muss im Besitz eines Tokens oder einer Karte sein (Besitzkomponente) und ein geheimes Passwort kennen (Wissenskomponente). Dadurch kann der Transaktionspartner feststellen, ob die handelnde Person diejenige ist, die sie vorgibt zu sein (Authentisierung).

WebIDs unterscheiden sich insbesondere auch nach dem **Grad der Rechtssicherheit** der nach ihrer Authentisierung durchgeführten Transaktionen:

- Für **rechtssichere** WebIDs ist deren Verwendung in Online-Transaktionen und damit verbundene Rechtsfolgen im Internet durch Gesetz geregelt.
- Bei **allgemeinen** WebIDs sind keine speziellen gesetzlichen Regelungen vorhanden; damit durchgeführte Transaktionen können jedoch auch rechtskräftig sein (Bsp.: Online-Erwerb einer Ware mittels einer nur durch Passwort geschützten WebID). Der juristische Laie kann allerdings bei allgemeinen WebIDs meist nicht erkennen, ob Transaktionen mit allgemeinen WebIDs rechtskräftig sind.

So ergeben sich verschiedene Typen von WebIDs, die nun näher betrachtet werden. In der Tabelle 1 werden für diese verschiedenen Nutzungsformen bzw. Verwendungszwecke gezeigt, welche Typen von Web-Identitäten einsetzbar sind.

Nutzungsformen – Verwendungszweck (Auswahl)	Typ			
	Allgemeine WebIDs		Rechtssichere WebIDs	
	Anonyme WebID	Offene -/ Pseudonyme WebID	Anonyme WebID	Offene -/ Pseudonyme WebID
1. Rechtsgeschäfte (national – international z. B. Kaufvertrag, Notarielle Dokumente etc.)				X
2. Verbindliche Transaktionen zwischen Wirtschaft und Wirtschaft, z. B. Einkauf eines Unternehmens				X
3. Verbindliche Transaktion zwischen Wirtschaft und Nutzer, z. B. Einkauf im Internet		X		X
4. Unverbindliche Transaktion zwischen Wirtschaft und Nutzer, z. B. Werbung, kostenlose Informationsmöglichkeiten	X	X		
5. Verbindliche Transaktionen zwischen öffentliche Verwaltung und Wirtschaft z. B. Ausstellung einer Baugenehmigung				X
6. Transaktion zwischen öffentliche Verwaltung und Bürger, z. B. Ausstellung eines Führerscheins		X		X
7. Verbindliche Transaktionen zwischen Nutzer und Nutzer, z. B. Ebay		X		X
8. Unverbindliche Transaktion zwischen Nutzer und Nutzer, z. B. Nutzung von Chatrooms, Newsgroups	X	X		
9. Verbindliche Transaktionen zwischen öffentliche Verwaltung und Nutzer, z. B. E-Voting ²			X	

Tabelle 1: Nutzungsform für die verschiedenen Typen von WebID

Neben dem Umfang des Profils und den beiden anwendungsbezogenen Eigenschaften (Rückschluss bzw. Rechtssicherheit) unterscheiden sich WebIDs noch durch eine Reihe weiterer (technischer) Eigenschaften, siehe dazu Tabelle 3 im Anhang.

² Für den Registrierungsprozess wird eine offene Identität benötigt. Für den Wahlvorgang selbst eine anonyme Identität.

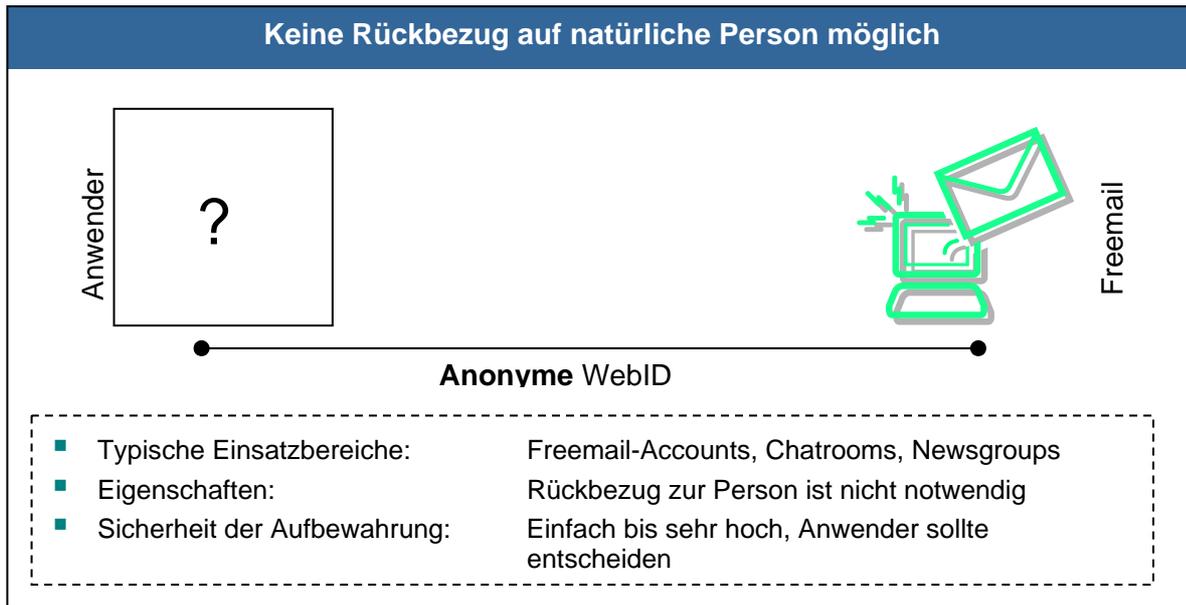
4 Anwendungsszenarien für WebIDs

WebIDs unterscheiden sich je nach Anwendungsszenario in ihren Eigenschaften. So stellt der Zugriff auf kostenfreie verfügbare Online-Informationen relativ niedrige Anforderungen an die Eigenschaften der WebID. Manche e-Business / m-Business Anwendungen und Services wären aber ohne hinreichend sichere WebIDs nicht möglich. Durch die Sicherheit für den Nutzer als auch Dienstleister ergeben sich (neue) Geschäftsmodelle. Dadurch haben WebIDs auch eine Business-Enabler-Funktion:

- Erwerb von kostenpflichtigen Waren sei es zwischen Firmen (B2B), zwischen einem Kunden und einem Unternehmen (B2C) oder zwischen mehreren Endkunden (C2C).
- Erwerb von kostenpflichtigen digitalen Informationen wie Musik, Nachrichten, Filmen. Dies wird ermöglicht durch DRM (Digitales Rechte Management), das neben der Identität des Kunden Identitäten für Endgeräte, Medienobjekte und Rechteinhaber benötigt.
- Rechtsgeschäfte, z.B. Transfer und Abschluss von Verträgen über das Internet, nicht nur zwischen Unternehmen, bzw. zwischen Kunden und Unternehmen, sondern auch zwischen Bürgern und staatlicher Verwaltung (e-Government).
- One-to-One Marketing, d.h. individualisiertes Ansprechen des Kunden.
- Authentisierungsdienste und Ausstellen von WebIDs.

In den folgenden Szenarien ist anhand von Beispielen dargestellt, welche möglichen Vorteile die Speicherung der WebID auf einem **sicheren, mobilen** Medium bringt.

- Szenario 1: Nutzung von Portalen im Internet (Anonyme WebID)



Die WebID wird von einem Portalbetreiber, z. B. einem Freemailanbieter oder einem Reiseplan- oder Stadtplanservice online vergeben. Normalerweise ist der Zugang durch den Identitätsbezeichner und Passwort geregelt.

Wenn der Nutzer diese auf einem mobilen Medium speichert, ergeben sich Vorteile für den Nutzer als auch für den Dienstanbieter.

Vorteile für den Nutzer:

- Erhöhung der Bequemlichkeit: Zum Anmelden und Nutzen des Service im Internet braucht der Anwender nur noch sein mobiles sicheres Speichermedium, in dem seine "WebID" gespeichert ist an dem PC, an dem er gerade ist, zu verbinden.
- Erhöhung der Sicherheit: Im Gegensatz zur direkten Eingabe von Benutzername und Passwort, kann die WebID nicht unbefugt mitgelesen werden. Es müsste das Medium, auf dem die WebID gespeichert ist und eine eventuelle zusätzliche PIN, die die WebID freigibt, gestohlen werden.

Vorteile für den Portalbetreiber: In diesem Szenario steht nicht die Rechtssicherheit sondern der praktische Schutz im Vordergrund. Der Portalbetreiber hat allerdings auch die Sicherheit, dass die WebID nicht kopiert werden kann. Für oben beschriebene Anwendungen, die die Rechtssicherheit der Zuordnung zu einer bestimmten natürlichen Person nicht benötigen, ist die anonyme WebID völlig ausreichend.

▪ Szenario 2: Einkaufen im Internet (Allgemeine offene WebIDs)

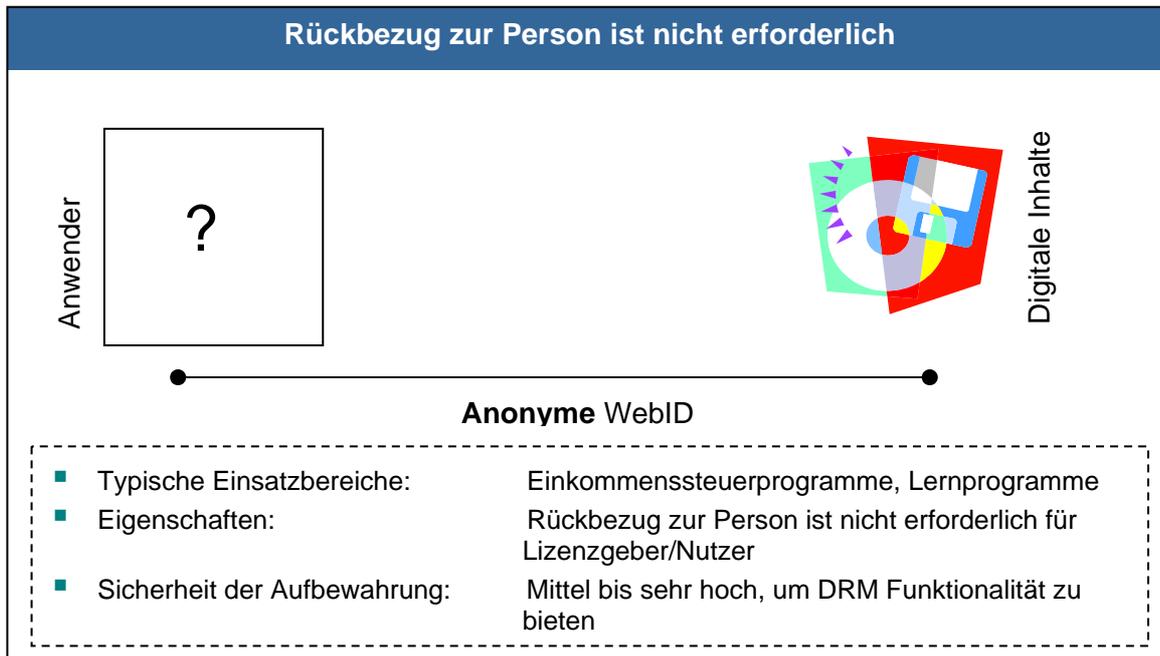


Die WebID wird vom Online-Shop online vergeben. In der Regel enthält diese Kreditkarteninformation und Lieferadresse.

Vorteile für den Nutzer: Durch die Verwendung einer sicher gespeicherten WebID ergibt sich wieder höhere Bequemlichkeit und höhere Sicherheit.

Vorteile für den Shopbetreiber: Er erhält Eindeutigkeit und Nichtweitergabemöglichkeit mit direkter Zuordnung zur Person. Des Weiteren werden weitere Merkmale wie Zahlungshistorie gespeichert.

- Szenario 3: Lizenzierung von digitalem Content und Software (Anonyme WebID)



Heutige Situation: Lizenzen über die Nutzung von Online Zeitungen, Studien, Software usw. werden mit folgenden vertraglichen Vereinbarungen vergeben:

- Ungeschützt
- Aktivierung, d.h. Bindung an ein Endgerät, an dem die digitalen Inhalte oder die Software nutzbar sein sollen
- Verwendung von Schutzmodulen (sog. Dongles³)

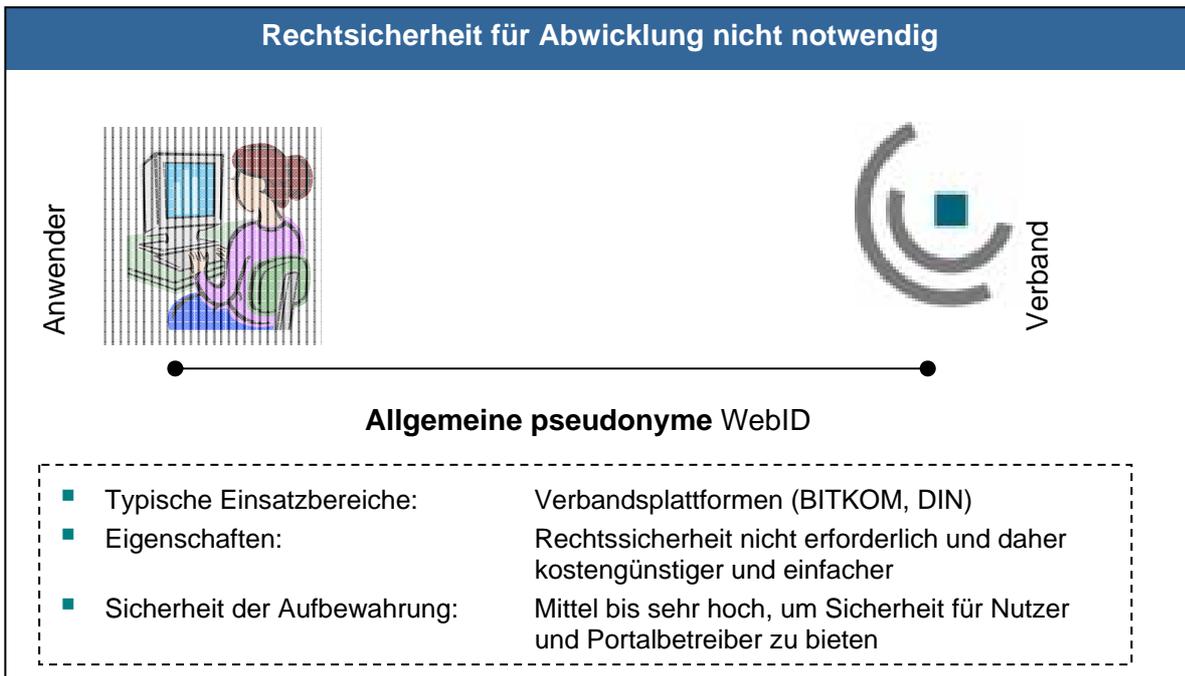
Möglichkeit mit WebID: Der digitale Content oder die Software wird an die WebID gebunden und ist nur nutzbar, wenn die WebID verfügbar ist. Dies setzt eine sichere Speicherung der WebID voraus. Wenn der Speicher der WebID viele IDs speichern kann und mobil ist, bringt dies erheblichen Nutzen für den Anwender.

Vorteil für den Lizenzgeber: Ein technisches Verfahren verhindert die Mehrfachnutzung von digitalen Inhalten und Software und vermeidet damit Piraterie und Raubkopien.

Vorteil für den Anwender: Die Anonymität bleibt gewahrt, da der Anbieter die WebID anonym vergeben kann. Die Mobilität ist sichergestellt, da keine Gerätebindung seiner digitalen Inhalte oder Software vorliegt.

³ nur bei hochpreisigen Produkten

- Szenario 4 : Portale geschlossener Benutzergruppen (Allgemeine pseudonymisierte WebID)

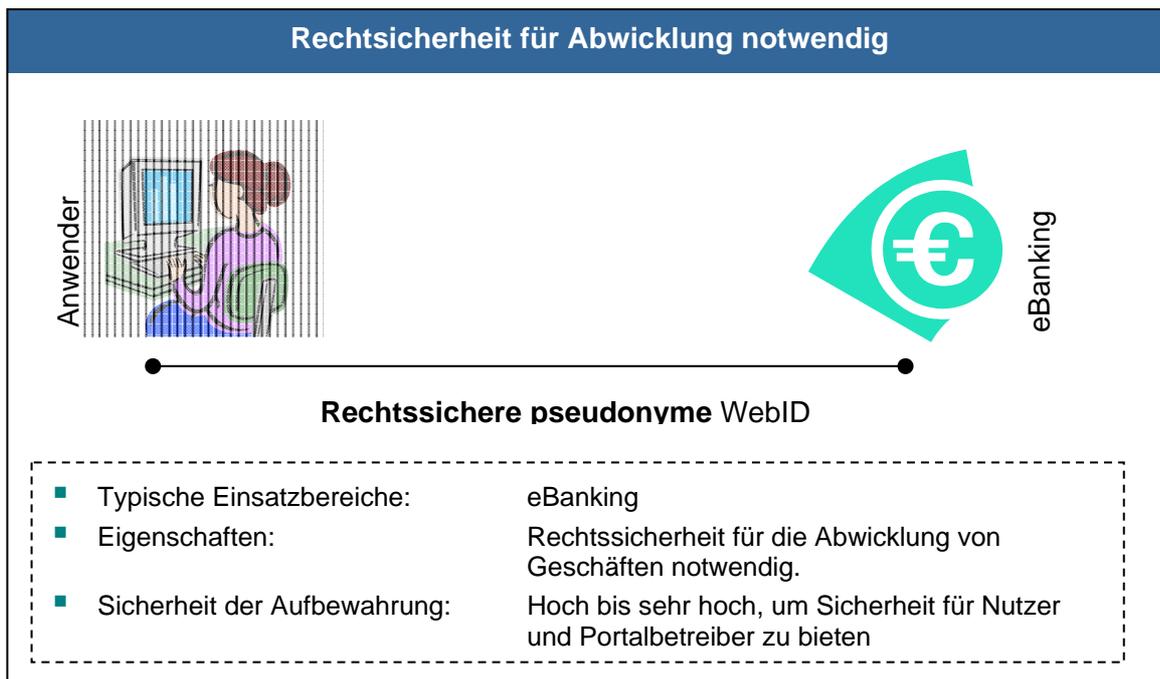


Die WebID wird vom Portalbetreiber online vergeben. Durch die Verwendung einer sicheren gespeicherten WebID ergibt sich wieder höhere Bequemlichkeit und höhere Sicherheit.

Beispiel: Zugang zu MyBITKOM (Mitgliederbereich des BITKOM)

Heute erfolgt der Login über Benutzername und Passwort um Zugang zu internen Papieren und Protokollen, Anmeldung zu Veranstaltungen zu gewähren. Mit einer vom BITKOM-Portal vergebenen WebID könnte der Benutzer sich bequem, ohne sich Login-Daten merken zu müssen, anmelden. Nach einmaliger Zuweisung der WebID hätte man auch einen Missbrauchsschutz und könnte diese WebID auch für Abstimmungen, Wahlen und andere Anwendungen verwenden, bei denen Merkmale einer digitalen Signatur benötigt werden.

▪ Szenario 5: Finanztransaktion (Rechtssichere pseudonymisierte WebID)



Heutige Situation bei Online Banken: Teilweise mehrere lange feste Zugangskennungen und TAN-Listen für Transaktionen

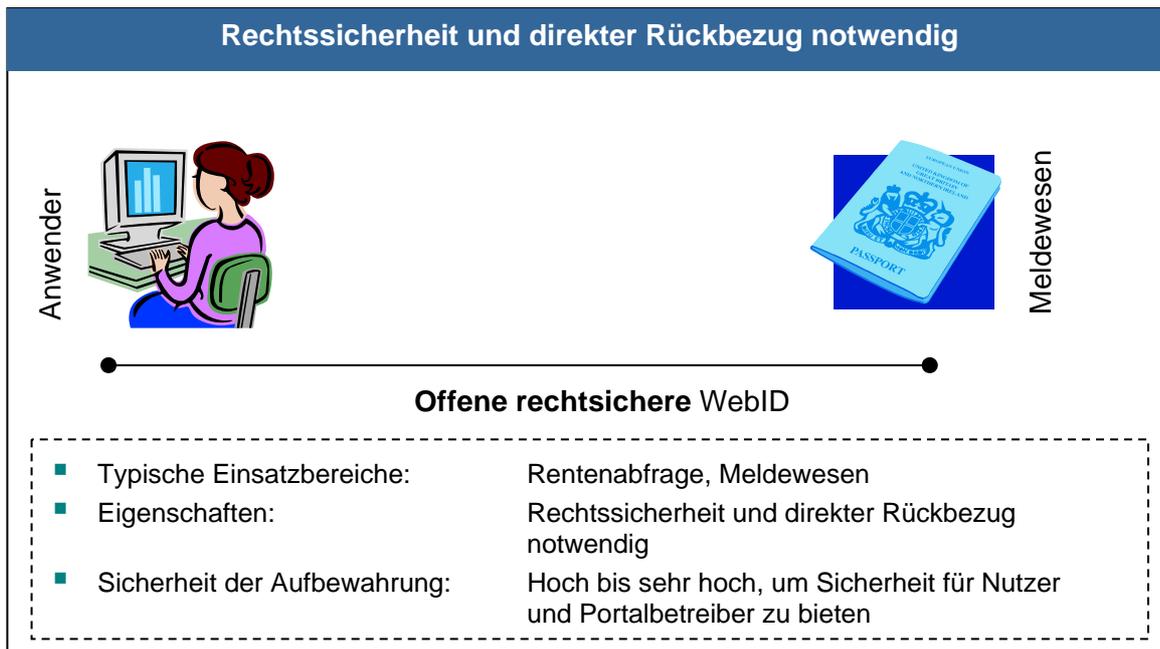
Alternativen mit WebID:

- Ausgabe oder Aktivierung eines Tokens oder einer Karte durch die Bank
- Nutzung von elektronisch generierten oder kommunizierten Einmalpasswörtern

Vorteil für Kunde: Sicherheit, Missbrauchsschutz und Komfort, Mobilität, da er alle Zugangsdaten bei sich haben kann.

Vorteil für Bank: Sicherheit und nur einmaligen Aufwand bei der Zuweisung der WebID. Kostenersparnis durch Verzicht auf TAN Briefe und Versand. TANs könnten optional in einer WebID gespeichert werden, wenn das TAN-Prinzip übertragen werden sollte.

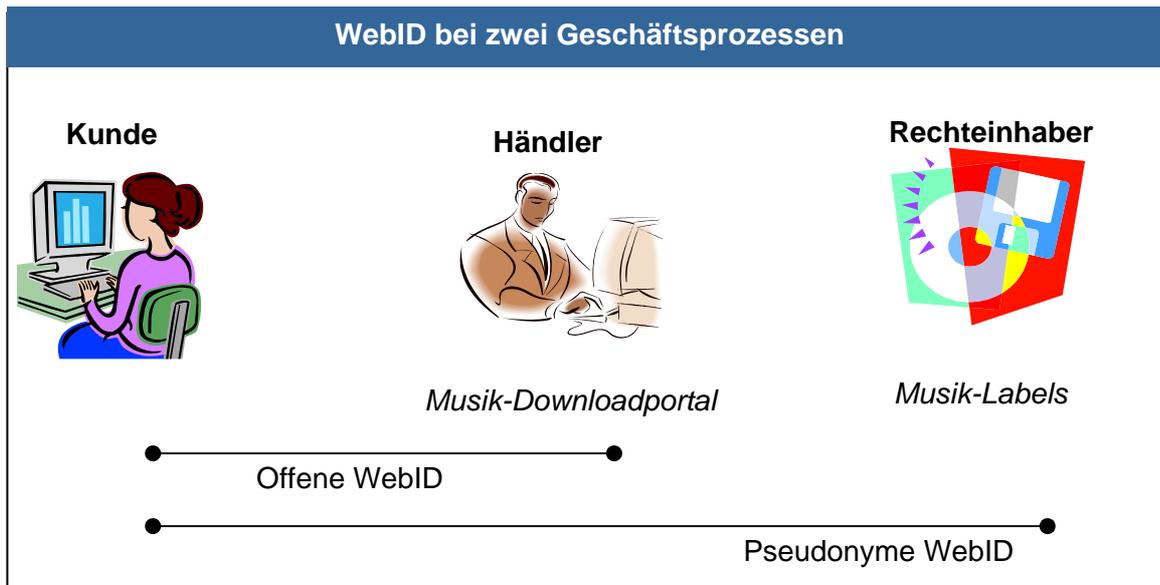
▪ Szenario 6: eGovernment (Rechtssichere Offene WebID)



Im eGovernment sind viele Leistungen und Informationen anonym abruf- und nutzbar (z. B. Stadtplan, Veranstaltungen, Adressen von Ämtern, Öffnungszeiten öffentlicher Gebäude). Es gibt aber auch Leistungen, für die die eindeutige Identifikation der handelnden Person z. B. eine „rechtsverbindliche“ Unterschrift bei der Beantragung oder dem Abruf von Leistungen notwendig ist. Hierzu gehören z. B. das An- und Ummelden einer Person, das Stellen eines Bauantrags, das Abrufen von kostenpflichtigen Leistungen auf Rechnung und das Abrufen spezieller, personenbezogener Auskünfte. In diesen Fällen wird eine eindeutige Identifikation bzw. die Leistung einer rechtsverbindlichen Unterschrift verlangt. Die dabei jeweils anzugebenden persönlichen Daten sind in einschlägigen Gesetzen, Verordnungen und Verfahrensvorschriften festgelegt: Es dürfen nur die für den jeweiligen Zweck notwendigen Daten erhoben und nicht mit anderen kommunalen oder staatlichen Anwendungen abgeglichen werden. Auch für das Löschen der Daten nach Ende der Nutzung gibt es entsprechende Gesetze und Vorschriften. Laut Drittem Gesetz zur Änderung verwaltungsverfahrenrechtlicher Vorschriften vom 21.8.2002 ist die Signierung mit einem Pseudonym, das die Identifizierung der Person des Signaturschlüsselinhabers nicht ermöglicht, nicht zulässig.

▪ Szenario 7: Zwei Geschäftsprozesse (Offene WebID, Pseudonyme WebID)

Die bisherigen Szenarien sind heutige, typische Einsatzbereiche von WebIDs. Die folgende Abbildung stellt den Zusammenhang von zwei Geschäftsprozessen dar. Auf den ersten Blick ein ungewöhnlich aber zukünftig durchaus vorstellbarer Geschäftsprozess. Hier wäre z. B. eine Anwendung aus dem DRM-Bereich denkbar: Der Kunde registriert sich bei einem Musik-Downloadportal mit einer offenen WebID, um Musikstücke runterzuladen. Die Musikstücke werden von den Musik-Labels über den Händler dem Kunden gegen Bezahlung zur Verfügung gestellt. Der Kunde erscheint hierbei gegenüber dem Musik-Label nur als pseudonyme Identität, gegenüber dem Händler offen.



5 Generierung, Aufbewahrung und Sicherheit von WebIDs

Entsprechend der Vielfalt möglicher WebIDs gibt es auch viele Möglichkeiten, diese zu erzeugen, verwalten und nutzen. Hier spielt die Qualität im Hinblick auf Zuverlässigkeit und Sicherheit der erhobenen und genutzten Daten eine wichtige Rolle.

Beispielsweise erstellt der Nutzer seine Attributsdaten selbst und übergibt die im jeweiligen Kontext zu nutzenden Daten (Profil) an eine Anwendung. Der Nutzer erlaubt auch die möglichen Wege der Kopplung dieser Daten zu weiteren Anwendungen.

Umgekehrt fordern Anwendungsanbieter und Unternehmen im Allgemeinen ein spezifisches Profil vom Nutzer an. Bei mehrfacher Nutzung dieses Profils wird dann der Einfachheit halber die Authentizität des Nutzers durch Eingabe von Identitätsdaten und Passwort bestätigt.

Es gibt auch neue Konzepte die einen zentralen ID-Provider beinhalten. Hier werden die Attributsdaten vom Nutzer erstellt und an *einen* Dienstleister übergeben. Dieser Dienstleister legt das Gesamt-Profil des Nutzers mit dem Identitätsbezeichner und allen Attributen an und gibt nach Weisung des Nutzers Teilmengen dieser Daten an die jeweiligen Anwendungsanbieter. Änderungen von Attributen können nach Vorgabe des Nutzers automatisch erfolgen (z.B. bei Adressänderung).

Sicher werden auch hier und da Identitätsdaten von Nutzern unkontrolliert und von den Nutzern nicht autorisiert an Dritte weitergegeben und für weitere Anwendungszwecke genutzt.

Hierzu noch einige allgemeine Anmerkungen: Wenn der Austausch von Profilen zwischen Anwendungen funktionieren soll, müssen die Attribute in standardisierter Form vorliegen. Ist darüber hinaus eine Bestätigung der Identitätsdaten oder eines oder mehrerer Attribute notwendig, gibt es mehrere Wege:

- Die Gültigkeit der Daten wird online von der die Identität registrierenden Stelle (z. B. Meldebehörde, Post, Kammer) bestätigt. Diese hat eine hochwertige Identitätsüberprüfung bei der Registrierung durchgeführt. Hierfür ist eine entsprechende Infrastruktur aufzubauen.
- Die Gültigkeit der Daten wird von einer zentralen Stelle (einem sog. Akquirer) bestätigt. Hierfür ist eine entsprechende Infrastruktur aufzubauen.
- Die Gültigkeit der Daten wird über eine Kopplung vertrauenswürdiger Quellen bestätigt (z. B. Bank an Internet-Shop). Hierfür ist eine entsprechende Infrastruktur aufzubauen.
- Die Gültigkeit von Attributen wird über eine eindeutige und nicht auflösbare Kopplung an die Basisdaten (z. B. Attributszertifikate gemäß SigG) gewährleistet. Die Gültigkeit der Basisdaten und/oder der Attributsdaten wird von der ausgehenden Stelle bestätigt. Hierfür ist eine entsprechende Infrastruktur aufzubauen.
- Die Daten sind nur in der jeweiligen Anwendung gültig und werden dort bestätigt (z. B. Name und Passwort).

Die Anforderungen an die Sicherheit und an die Aufbewahrung von WebIDs sind je nach Anwendung unterschiedlich. Internet Browser und andere Softwarepakete bieten Speichermöglichkeiten für längere Listen solcher WebIDs an. Stellt die Anwendung erhöhte Sicherheitsanforderungen an die WebID sind solche Systeme nicht ausreichend. Typischerweise ist dies bei Transaktionen im Bankenbereich, im Gesundheitsbereich, im militärischen Bereich, im Handel und vor allem im rechtsverbindlichen Bereich der Fall.

Diese Transaktionssysteme haben Sicherheitsanforderungen, die über reines *Wissen* (z. B. von Username und Passwort bzw. PIN/TAN) hinausgehen, und daher das *Besitzen* eines fälschungssicheren Mediums (Ausweis, USB-Token oder ähnlichem) verlangen. Durch dieses Medium sind solche WebIDs mobil, geräteunabhängig aber dennoch fest einer Person zugeordnet. Wenn solche fälschungssichere Medien gleichzeitig leicht an das Internet anzubinden und zu verwenden sind, bieten sie die Chance, die Rolle echter Business Enabler wahrzunehmen.

Fälschungssicherheit bedeutet, dass sichere WebID lokal nicht auf Festplatten oder nur im Gedächtnis des Nutzers aufbewahrt werden sollten. Solche Speichermedien sind unsicher (siehe Tabelle 2). Sichere Speichermedien sind z. B. Chipkarten, gesicherte USB-Token oder gesicherte Flashcards.

Speichermedium	Nutzungsdauer	Mobilität	Sicherheitslevel	Bequemlichkeit
Papier	Mittel	Mittel	Niedrig	Hoch
Unverschlüsselt auf Festplatte	Hoch	Niedrig	Niedrig	Mittel
Verschlüsselt auf Festplatte	Hoch	Niedrig	Mittel	Mittel
Mobiles, nicht geschütztes Speichermedium	Hoch	Hoch	Niedrig	Hoch
Mobiles, geschütztes Speichermedium z. B. USB-Token, Chipkarten	Hoch	Hoch	Hoch	Hoch

Tabelle 2: Vergleich Sicherheit von WebID auf verschiedenen Speichermedien

Die Mobilität und Sicherheit gegen Fälschung und Missbrauch von Hardwarelösungen ist am besten dadurch gewährleistet, dass Daten, Schlüssel u. ä. in speziell abgesicherten Bereichen gespeichert sind. Insbesondere stellt die Chiptechnologie dabei sicher, dass wertvolle Daten erfolgreich vor Angriffen bewahrt werden. Dabei wird die Sicherheit doppelt garantiert: Im Softwarebereich durch sichere Kryptoalgorithmen (DES; AES, elliptische Kurven) und im Hardwarebereich durch eine Kombination von Silizium- und verwandten Technologien gegen das direkte Erspähen der Schlüssel. Bei USB-Token besteht zur Erhöhung der Zugriffssicherheit auch die Möglichkeit für biometrische Zugangssicherung.

6 Wirtschaftliche und rechtliche Rahmenbedingungen

6.1 Wirtschaftliche Rahmenbedingungen

Einleitend lassen sich zwei grundsätzlich notwendige Erfolgsfaktoren für die Wirtschaftlichkeit von *sicheren* WebIDs nennen: (1) Erreichen einer hohen Economy-of-Scale und (2) Gewährleistung niedriger Grenzkosten. Nur hohe Stückzahlen garantieren mit einer großen Verbreitung ausreichende Skaleneffekte und damit auch niedrige Stückkosten. Dies gilt insbesondere für WebIDs, die hohen Sicherheitsansprüchen genügen, beispielsweise WebIDs auf Smartcards. Erst bei hohen Stückzahlen rechnen sich die hohen Investitionen in Entwicklung und Infrastruktur. Niedrige Grenzkosten lassen sich beispielsweise erzielen, wenn WebIDs, die bereits als Identifikationsmittel für einen Service eingesetzt werden, auch für weitere Services genutzt werden. Diese Wirtschaftlichkeitsüberlegungen sind im Sinne eines Single-Sign-On bzw. bei der Föderation von Identitäten relevant. Grenzkosten lassen sich ebenfalls senken, wenn die Prozesse für die Registrierung und Herausgabe eines konventionellen Identifikationsmediums relativ leicht in die digitale Welt übertragen werden können (Beispiel Personalausweis – zukünftige elektronische Identitätskarte).

Je höher die an eine WebID gestellten Sicherheitsanforderungen sind, umso größer wird auch der Investitionsbedarf für die benötigte technische und organisatorische Infrastruktur. Besonders deutlich wird dies bei der elektronischen Signatur: Zwar gibt es seit 1997 ein Signaturgesetz in Deutschland. Aber die Infrastruktur für die Benutzung der Signatur in Form von evaluierten Smartcards, Kartenlesegeräten und Signaturanwendungssoftware hat in der Fläche keine Verbreitung erfahren. Die Marktbedeutung der Signatur ist deshalb auch alles andere als signifikant.

Anders verhält es sich mit WebID für geringeren Schutzbedarf: Logon auf einer Website mit Accountname und Passwort ist heute weit verbreitet und akzeptiert. Ebenso E-Banking mit Authentifizierung über PIN/TAN-Listen.

Eine wesentliche Ursache der nach wie vor relativ gering ausgeprägten Akzeptanz sicherer WebID ist die Tatsache, dass deren Nutzen in der Regel nicht bei der Partei anfällt, die in die Beschaffung der WebID und der dafür erforderlichen Technologie investiert. Erfolg und Misserfolg einer sicheren WebID sind somit unmittelbar abhängig vom darunter liegenden Geschäftsmodell. Warum sollte ein Bürger sich schließlich eine Signaturkarte beschaffen, wenn er durchschnittlich nur 2 – 3mal jährlich mit einer Verwaltungsbehörde kommuniziert? Den Nutzen effektiver Online-Prozesse hätte unmittelbar erst einmal nur die Verwaltung. Oder warum sollte der Kunde eines Web Shops in ein Zertifikat von einem akkreditierten Trustcenter investieren, wenn der Einsatz des Zertifikats zur seiner sicheren Authentifizierung primär im Interesse des Shops liegt, den Vertragsschluss und Abnahme- und Bezahlungsverpflichtung des Bestellers beweisen zu können?

Solange sich keine kreativen Geschäftsmodelle durchsetzen, die einen weithin sichtbaren Nutzen für Anwender generieren, werden sich WebIDs auf hohem Sicherheitsniveau schwer tun.

Dennoch ist es im Zeitalter der elektronischen Kommunikation unverzichtbar, Kommunikationsbeziehungen und Transaktionen über potentiell unsichere Netze mit Hilfe von WebIDs, die der jeweiligen Situation unter Sicherheitsgesichtspunkten angemessenen sind, abzusichern.

D.h. WebIDs sind inzwischen zum Business Enabler geworden. Sie ermöglichen in großem Umfang täglich zahlreiche e-Business-Transaktionen, etwa zum Einkauf von Waren im Internet, die ohne hinreichend sichere WebID keinen e-Business-Umsatz generiert hätten.

Welche Formen von WebID und welche Arten von Kundenanmeldungen verwendet werden, hängt zum einen davon ab, wie ausgeprägt das Sicherheitsbedürfnis und –bewusstsein der handelnden Akteure ist. Zum anderen aber auch von der Antwort auf die Frage, ob sich der Einsatz von WebID auf einem bestimmten Sicherheitsniveau auch betriebswirtschaftlich rechnet. Hier stellt sich die Frage nach dem Return of Invest in WebID. Um diesen nach betriebswirtschaftlich einigermaßen nachvollziehbar rechnen zu können, ist grundsätzlich eine Befassung mit dem Thema Risikomanagement erforderlich. Nur wer seine Risiken kennt und die Folgen ihrer Realisierung kalkuliert, kann Investitionen in WebID auch betriebswirtschaftlich sauber begründen. Dabei geht es dann um Fragen wie Restrisikobewertung, Rückstellungen für Risiken oder Versicherungsschutz. Die Diskussion dazu ist aber noch im Fluss, mit viel Phantasie sind gerade im Rahmen von Risikomanagementstrategien sehr viele unterschiedliche Varianten denkbar.

6.2 Rechtliche Rahmenbedingungen

Die wesentlichen rechtlichen Rahmenbedingungen die im Umgang mit WebID beachtet werden müssen sind (1) die Einhaltung von **Datenschutzbestimmungen** sowie (2) die Klärung von **Haftungsfragen**. Während die Wahrung des Persönlichkeitsschutzes bzw. Eingriffe in diesen Schutz bei einer eventuellen Strafverfolgung weitestgehend gesetzlich vorgegeben sind, so müssen für die Regelung der Haftung beim Gebrauch von WebID meist erst noch vertragliche Grundlagen geschaffen werden.

Haftung

Werden WebID (für *juristische* Personen) von einem Online-Dienstanbieter selbst herausgegeben, so sind die Verantwortlichkeiten und die Haftung bei ordnungsgemäßem bzw. missbräuchlichem Umgang in der Regel in den Allgemeinen Geschäftsbedingungen oder in Online-Verträgen geregelt.

Beispiel: Hat ein e-Banking Kunde einer Online-Bank beispielsweise nachweislich unbeabsichtigt Einsicht in das Konto eines anderen Kunden bekommen, liegt die Verantwortung dafür sicher bei der Bank. Dies sollte in einem Audit offen gelegt werden können. Gelangt allerdings eine Liste mit PIN/TAN-Codes in fremde Hände oder wurde sie unbemerkt kopiert, und kommt es als Folge dessen zu ungewollten Transaktionen, so wird der Bank schwerlich ein Fehler und somit die Haftung zuzuweisen zu sein, da für sie nachweislich eine ordnungsgemäße Anmeldung stattgefunden hat.

Komplexer sind die Verantwortungen und die Regelung der Haftung, wenn mehrere Parteien involviert sind: Träger und Benutzer der WebID, Anbieter von Online-Diensten, Herausgeber von WebID, Stellen, die Zugehörigkeit von WebID zu ihren Trägern zertifizieren, Vertragspartner in einer Föderation. Doch auch hier können entsprechende vertragliche Regelungen getroffen werden (Beispiele: Certificate Practice Statement von Trust Centern, Identity Federation). Das Internet und seine Benutzer haben sich bei der Regelung des Gebrauchs von WebID insbesondere auch durch den stetigen Kampf gegen Fälschung und Missbrauch als überaus lern- und anpassungsfähig erwiesen.

Datenschutz

WebID haben die Tendenz, im Spannungsfeld zwischen dem allgemeinen Persönlichkeitsrecht des einzelnen Individuums und anderen Interessen wie z. B. der Werbewirtschaft oder der staatlichen Strafverfolgung zu stehen. WebID machen Kommunikationsvorgänge und Transaktionen im Internet wesentlich besser auf natürliche Personen beziehbar, sofern sie es leicht machen, auf die durch sie repräsentierten Personen zu schließen. Sie sind deshalb datenschutzrechtlich besonders relevant.

Wichtig ist, dass der Anwender einer WebID grundsätzlich selbst darüber entscheiden können muss, wann und wem er seine personenbezogenen Informationen offenbart (soweit nicht an-

ders lautende gesetzliche Regelungen existieren, die zur Offenbarung verpflichten). Wenn erforderlich, muss einem Einverständnis zur Offenbarung persönlicher Daten grundsätzlich eine geeignete Aufklärung vorausgehen.

In jedem Fall ist auf eine Balance zwischen dem Interesse des einzelnen Individuums und sonstigen Interessen Dritter zu achten. Nur so können WebID ihre segensreiche Funktion zur Absicherung und damit Ermöglichung vertrauenswürdiger Kommunikations- und Transaktionsprozesse über das Internet und sonstige potentiell unsichere Netze erfüllen. Einzelheiten dazu sind in den Datenschutzgesetzen des Bundes und der Länder sowie in vielen bereichsspezifischen datenschutzrechtlichen Regelungen, die den allgemeinen Datenschutzgesetzen vorgehen (z. B. im Multimedia- und Telekommunikationsrecht, öffentlichen Gesundheitswesen oder der Strafrechtspflege).

Anhang

	Typ				
	Allgemeine WebIDs			Rechtssichere WebIDs ⁴	
Eigenschaften und deren mögliche Ausprägung	Offene WebID	Pseudo. WebID	Anon. WebID	Offene WebID	Pseudo. WebID
Für wen gilt die WebID?					
Einzelperson	X	X	X	X	X
Behörde	X			X	
Firma	X	X		X	
Objekt (z. B. Maschine, Software)	X	X	X		
Wer kann für das repräsentierte Subjekt die WebID ausgeben oder ungültig erklären?					
Person/Objekt	X	X	X		
Dienstleistungspartner des Subjekts	X	X	X	X	X
Behörde	X	X		X	X
Wie ist die Verwendung der WebID geschützt?					
Ungeschützt			X		
Passwort oder PIN	X	X			
Hoher Schutz durch Passphrase, one-time-password	X	X		X	X
2-Faktor-Authentizierung (etwa Smart Card & PIN)	X	X		X	X
Anforderung an den Identitätsnachweis des Subjektes bei Ausgabe/Registrierung der WebID					
Hoch: Persönliches Abholen gegen Vorlage von rechtsverbindlichen Dokumenten zum Identitätsnachweis (z. B. Personalausweis)	X	X		X	X
Mittel: Identitätsnachweis auf hohem Sicherheitsniveau unter Mithilfe von autorisierten Dritten (z. B. Zertifikat)	X	X			
Niedrig: Identitätsnachweis auf niedrigem Sicherheitsniveau (z. B. anhand angegebener E-Mail-Adresse)	X	X			
Keine Anforderung: Kein Nachweis bzw. keine Prüfung der Identität notwendig			X		
Integritätsgrad der WebID (Fälschungssicherheit bei Gebrauch der WebID)					
Hoch: Rechtsverbindlicher Identitätsnachweis (mittels Smartcard und digitaler Signatur)	X	X	X	X	X
Mittel: Identitätsnachweis auf hohem Sicherheitsniveau unter Mithilfe von autorisierten Dritten (z. B. Zertifikat)	X	X	X		

⁴ Rechtsichere anonyme WebIDs werden in dieser Tabelle nicht aufgeführt. Es handelt sich hierbei, um einen speziellen Fall handelt, bei dem eine vertrauensvolle dritte Partei eingebunden werden muss. Diese prüft die Identitäten der Personen und deren Berechtigungen und nimmt die Anonymisierung in einem rechtssicheren Rahmen vor.

Niedrig: Identitätsnachweis auf niedrigem Sicherheitsniveau (z. B. Freischaltungs-/Bestätigungslink durch den Nutzer bei korrekt eingegebener Emailadresse)	x	x	x		
Keine Anforderung: Kein Nachweis bzw. keine Prüfung der Identität notwendig			x		
Rechtskraft garantiert und einfach erkennbar	Bedingt	Bedingt	Nein	ja	ja
Eindeutigkeit der WebID (weltweit)	Nein	Nein	Nein	Nein?	Nein?
Multiplizitätsgrad (Wieviele WebIDs je repräsentiertes Subjekt)					
Hoch		x	x		x
Gering	x			x	
Persistenzgrad (Dauerhaftigkeit) der WebID					
Hoch (Jahrzehnte)					
Mittel (Jahre)	x	x		x	x
Niedrig (bis max. 1 Monat)	x	x	x		
Datenschutz (Wie einfach ist es, anhand der des offengelegten Teils der WebID auf die durch die WebID repräsentierte Person / Firma zurückzuschließen)					
Sehr schwer			x		
Mittel bis Schwer		x			x
Einfach	x			x	
Profil, d. h. die benötigte Attribute zur Erlangung der Dienstleistung					
Profil 1 Umgangreiches Profil mit allen Standardattributen (Name, Adresse, BLZ, Kontonr., Telnr., Faxnr., E-Mail-Adresse etc. und zusätzlich allen persönlichen Attributen, siehe z. B. Personalausweis) Alter, Geschlecht, Größe, Gewicht, Augenfarbe, Haarfarbe, Familienstand, Religion usw.				x	x
Profil 2 Profil mit den Standardattributen: Name, Adresse, BLZ, Kontonr., Telnr. Faxnr., E-Mail-Adresse	x	x		x	x
Profil 3: Minimalprofil: E-Mail-Adresse	x	x	x		

Tabelle 3: Eigenschaften von Web Identitäten

Danksagung

Die vorliegende Broschüre entstand im BITKOM-Fachausschuss „Identitäten- und Rollen-Management“ des Kompetenzbereiches Sicherheit.

Wir danken allen Mitgliedern des Fachausschusses für das kontinuierliche Interesse am Thema, die wertvollen Diskussion sowie die zahlreichen Anregungen. Besonderer Dank gilt den federführenden Autoren

- Gerold Hübner (Microsoft Deutschland GmbH)
- Walter Landvogt (Bundesdruckerei GmbH)
- Dr. Michael Marhöfer (Siemens AG)
- Dr. Christoph Schiller (Giesecke & Devrient GmbH)
- Helmut Trautmann (Hewlett-Packard GmbH)
- Christoph Wahlen (Uniquework GmbH)
- Oliver Winzenried (Wibu-Systems AG)
- Klaus Wischniewski (DATEV eG)
- Klaus-Dieter Wolfenstetter (Deutsche Telekom AG) als Leiter des Fachausschusses
- Dr. Frank Zimmermann (Hewlett-Packard GmbH)

sowie den Mitgliedern Torsten Hupe (Bayer Innovation GmbH), Michael Hegenbarth (Bundesdruckerei GmbH), Dirk Schadt (CA Computer Associates GmbH), Dr. Klaus-Dieter Wirth (D-Trust GmbH), Dr. Wolf Osthaus (eBay GmbH), Klaus Matouschek (Hewlett-Packard GmbH), Jürgen Bachinger (Hewlett-Packard GmbH), Rüdiger Kern (IBM Deutschland GmbH), Wolf-Rüdiger Moritz (Infineon Technologies AG), Dr. Detlef Houdeau (Infineon Technologies AG), Michael Lüders (LWP Lüders, Weinbrenner & Partner GmbH), Arno Fiedler (Nimbus Network GbR), Manfred Schäfer (Siemens AG), Hans Wieser (Sun Microsystems GmbH), Andreas Philipp (Utimaco Safeware AG) und den Gästen Dr. Jürgen Elschner (Ident Technology AG), Henning Arendt (@bc - Arendt Business Consulting), Christian Engel (Bundesministerium des Innern), Dr. Harald Ahrens (SignCard GmbH & Co. KG), Ralph Meister (paybox solutions AG), Mike Bergmann (Technische Universität Dresden), Henry Krasemann (Unabhängiges Landeszentrum für Datenschutz) für das außerordentliche Engagement, die diese Guideline erst ermöglichten.

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vertritt 1.300 Unternehmen, davon mehr als 700 Direktmitglieder mit etwa 120 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu zählen insbesondere Geräte-Hersteller, Anbieter von Software, IT-Services, Telekommunikationsdiensten und Content. Der BITKOM setzt sich insbesondere für bessere ordnungsrechtliche Rahmenbedingungen, eine Modernisierung des Bildungssystems und eine innovationsorientierte Wirtschaftspolitik ein.



Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.
Albrechtstraße 10
10117 Berlin-Mitte

Tel.: 030/27 576 - 0
Fax: 030/27 576 - 400

bitkom@bitkom.org
www.bitkom.org
