ARTIKEL 29-DATENSCHUTZGRUPPE

10054/03/DE
WP 68

Arbeitspapier zu Online-Authentifizierungsdiensten

Angenommen am 29. Januar 2003

Die Gruppe ist gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzt worden. Sie ist ein unabhängiges europäisches Beratungsgremium in Datenschutzfragen. Ihre Aufgaben sind in Artikel 30 der Richtlinie 95/46/EG sowie in Artikel 14 der Richtlinie 97/66/EG festgelegt.

Die Sekretariatsgeschäfte werden wahrgenommen von: Europäische Kommission, GD Binnenmarkt, Direktion E (Dienstleistungen, Geistiges und Gewerbliches Eigentum, Media und Datenschutz), B-1049 Brüssel, Belgien, Büro C100-6/136.
Website: www.europa.eu.int/comm/privacy

DIE GRUPPE FÜR DEN SCHUTZ VON PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN

eingesetzt nach Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 [1],

gestützt auf Artikel 29 und 30 Absatz 1 Buchstabe a) und Absatz 3 dieser Richtlinie,

gestützt auf die Geschäftsordnung, insbesondere Artikel 12 und 14,

HAT DAS VORLIEGENDE ARBEITSDOKUMENT ANGENOMMEN:

1. EINLEITUNG: ZUNAHME DER ONLINE-AUTHENTIFIZIERUNGSDIENSTE

Die zunehmende Nutzung von Online-Authentifizierungsdiensten hat die Internetlandschaft[2] verändert. Immer mehr Websites schlagen Benutzern vor oder verlangen von ihnen, dass sie sich registrieren lassen, z. B. weil sie vertrauliche Informationen anbieten, weil sie die Möglichkeit bieten, die Vorzugseinstellungen der Benutzer zu registrieren, weil sie kostenpflichtige Dienstleistungen erbringen oder die Lieferung von Waren Gegenstand ihrer Dienstleistungen ist. Bei all diesen Websites müssen sich die Benutzer in irgendeiner Form identifizieren, was oft über eine E-Mail-Adresse erfolgt, und ihre Authentizität bestätigen - häufig per Passwort.

Die Verwendung der Kombination aus „Benutzername“ und „Passwort“ kann für den Dienstanbieter eine nicht zu unterschätzende Herausforderung darstellen:

- Benutzer neigen dazu, ihr Passwort zu vergessen. Immer mehr Anrufe oder Mails an den Support betreffen vergessene Passwörter. Die Kosten für die erneute Einrichtung von Passwörtern wird zusehends zu einer Belastung für die Betreiber der Websites.
- Immer mehr Benutzer verwenden verschiedene Zugriffsmethoden auf das Internet, erwarten jedoch den gleichen Service von den Dienstanbietern. Die Zugriffsmethoden unterscheiden sich zwar auch in technischer Hinsicht (Zugang vom PC, über WAP usw.), besonders problematisch ist jedoch der Zugriff auf das Internet von verschiedenen Personalcomputern aus - in Internetcafés oder öffentlichen Bibliotheken. Die Benutzer müssen sich also eine Vielzahl von Kennwörtern merken.
- Außerdem haben manche Benutzer keine Lust, immer wieder ihre Benutzernamen und Passwörter einzugeben, weil sie das Gefühl haben, bei ihrem Surferlebnis gestört zu werden. Da die Benutzer sich beim Surfen so wenig wie möglich anstrengen möchten, geben sie nur kurze und somit unsichere Passwörter ein und verwenden diese gleich auf mehreren Websites.

Eine Lösung der drei oben genannten Probleme setzt voraus, dass der Benutzer jemand anderem einen Teil seiner Authentifizierung überlässt. Es gibt derzeit vier Möglichkeiten:

- Die Passwortverwaltung wird vom Browser des Benutzer-PCs übernommen, wie z. B. beim Passwort Manager von Mozilla.
- Die Passwortverwaltung wird an einen Proxy-Server im Internet delegiert, der möglicherweise vom Internet-Dienstanbieter (ISP) bereitgestellt wird.

1 ABl. L 281 vom 23.11.1995, S. 31, siehe: http://europa.eu.int/comm/internal_market/en/dataprot/index.htm

2 Die Datenschutzgruppe wies bereits in vorangegangenen Dokumenten darauf hin, dass die Grundsätze der Richtlinie auch für Online-Aktivitäten gelten. Siehe auch: WP 37, Arbeitsdokument - Privatsphäre im Internet - Ein integrierter EU-Ansatz zum Online-Datenschutz, angenommen am 2. Juli 2002.

- Die Authentifizierung erfolgt von dritter Seite durch ein spezielles Authentifizierungsprotokoll. Ein Beispiel hierfür ist .NET Passport von Microsoft.
- Die Authentifizierung wird von einem Vertragspartner innerhalb eines „Circle of Trust“ durchgeführt. Dazu wird ein spezielles Protokoll verwendet, wie z. B. Liberty Alliance.

Diese Möglichkeiten werden in den folgenden Abschnitten genauer unter die Lupe genommen.

1. Ein Passwort-Manager auf dem PC

Ein in den Internet-Browser integrierter Passwort-Manager löst das Problem nur teilweise. Er nimmt dem Benutzer zwar die Arbeit ab, sein Passwort einzugeben, und vermindert so das Risiko, dass das Passwort verloren geht. Es löst jedoch nicht das Zugangsproblem von Benutzern, die von verschiedenen PCs aus auf die Dienste zugreifen.

Aus der Sicht des Datenschutzes stellt sich die Situation relativ einfach dar: Sämtliche Software läuft auf dem PC des Benutzers und unter dessen Aufsicht. Die persönlichen Daten werden von keiner externen Firma kontrolliert. Der Benutzer wird lediglich gefragt, ob er damit einverstanden ist, dass seine Daten in die Datenbank des Passwort-Managers aufgenommen werden. Der Passwort-Manager gibt das Passwort ein, überträgt es jedoch nicht von selbst. Auf diese Weise wird sichergestellt, dass nichts ohne Einwilligung des Benutzers geschieht. Sicherheitstechnisch müssen geeignete Maßnahmen ergriffen werden, damit die gespeicherten Daten vor Angriffen geschützt sind.

2. Verwendung eines Proxy-Servers

Anstatt den Passwort-Manager des Benutzeragenten (d. h. des Browsers) zu verwenden, kann die gleiche Funktionalität auch in einen Proxy-Server im Internet integriert werden. Dies ist mit den eher bekannten „Anonymizing Proxies“ (Anonymizer) vergleichbar. Ein Proxy-Server kann viele Benutzer bedienen und setzt deshalb die Registrierung von Passwörtern jeweils pro Benutzer und pro Zielseite voraus. Die Registrierung muss von den Benutzern für vertrauenswürdig erklärt worden sein. Dies geschieht ganz explizit, denn der Benutzer muss vor der Nutzung eines bestimmten Proxys eine bewusste Entscheidung treffen (es gibt keine Standarddienste). Der Benutzer muss sich beim Proxy anmelden, wenn er seine Passwörter benutzen möchte. Ist er einmal angemeldet, genießt er die gleichen Vorteile wie beim im Browser integrierten Passwort-Manager. Der besondere Vorteil beim Proxy ist, dass er von verschiedenen PCs und/oder anderen Geräten aufgerufen werden kann.

Die Proxys sollten Benutzerdaten niemals ohne Einwilligung des Benutzers weitergeben. Tun sie es dennoch, verlieren sie das Vertrauen ihrer Kunden und somit die Grundlage für ihre Existenz. In der Regel wird zwischen Proxy-Betreiber und Kunde ein Vertrag abgeschlossen. Der Dienst finanziert sich wahrscheinlich nicht aus Werbung, sondern aus anderen Quellen, möglicherweise zusammen mit den Dienstleistungen eines ISP.

3. Online-Authentifizierungsdienste mit speziellen Protokollen

Keine der oben genannten Lösungen erfordert das Aufrufen der Website des Dienstanbieters. Eine andere Möglichkeit für die Authentifizierung besteht darin, ein spezielles Authentifizierungsprotokoll zu verwenden. Die grundlegende Architektur für diese Protokolle ist immer gleich. Es gibt drei Beteiligte: einen Endanwender, einen Dienstanbieter und einen Anbieter der Authentifizierungsdienste. Bevor der Endanwender die Leistungen des Dienstanbieters nutzen kann, muss er seine Identität vom Authentifizierungsanbieter überprüfen lassen. Der Dienstanbieter vertraut dem Authentifizierungsdienst und akzeptiert die Anmeldung des Benutzers.

Die Architektur von .NET Passport baut auf einem einzigen, von Microsoft betriebenen Authentifizierungsserver auf. Der Passport enthält einige Identifizierungs- und Authentifizierungsinformationen sowie bestimmte Profildaten. In der Zukunft werden diese beiden Datensätze wahrscheinlich zunehmend voneinander getrennt werden. Ein Benutzer, der sich bei Passport angemeldet hat, besitzt eine eindeutige Kennung (Passport User ID - PUID). Wenn sich der Benutzer bei einem Dienstanbieter einloggen möchte, weist er den Passport-Server an, die PUID in einer Form zu übergeben, die vom Dienstanbieter gelesen werden kann, was derzeit in symmetrisch verschlüsselter Form geschieht.

Die Liberty Alliance wendet ein föderatives Modell an, d. h. der Benutzer kann sein Konto bei zwei Dienstanbietern verwenden. Wurde ein Konto auf diese Weise angelegt, akzeptiert ein Dienstanbieter die Übermittlung der Daten des anderen Dienstanbieters, der als Authentifizierungsdienst fungiert.

Die Datenschutzgruppe ist sich der raschen Zunahme von Online-Authentifizierungsdiensten bewusst und hat deshalb vor einigen Monaten beschlossen, die Auswirkungen des Einsatzes dieser Systeme auf den Datenschutz zu untersuchen[3]. Die Datenschutzgruppe weiß um die Bedeutung sicherer Authentifizierungsmechanismen, wenn es darum geht, die Sicherheit und insbesondere die Integrität vieler elektronischer Transaktionen (insbesondere Online-Zahlungen) zu gewährleisten, und möchte deshalb betonen, dass bei der Entwicklung dieser Dienste die Prinzipien des Datenschutzes erfüllt werden müssen, die in der europäischen Datenschutzrichtlinie[4] und in den nationalen Gesetzen zur Umsetzung dieser Richtlinie festgeschrieben sind.

2. FALLSTUDIE 1: .NET PASSPORT VON MICROSOFT

.NET Passport ist derzeit eine Initiative von beachtlicher Bedeutung in diesem Bereich. Folglich hat sich die Datenschutzgruppe im Frühjahr 2002 zunächst mit diesem System befasst[5]. Nach einer ersten Analyse ist die Datenschutzgruppe der Auffassung, dass Microsoft zwar einige datenschutzrelevante Maßnahmen eingeführt hat, eine Reihe der Merkmale des .NET Passport-Systems aber juristische Probleme aufwirft und daher weiterer Überlegungen bedarf.

In den folgenden Monaten nahm die Datenschutzgruppe Gespräche mit Microsoft auf, um die Arbeitsweise des Systems besser zu verstehen, die verschiedenen akuten Probleme zu besprechen und insbesondere zu beurteilen, ob die europäischen Datenschutzregeln eingehalten werden, und ggf. Bereiche des Systems zu benennen, die einer Änderung bedürfen. Nach diesem sehr offenen und fruchtbaren Dialog sicherte Microsoft zu, Änderungen am System vorzunehmen und besonders die Seite des Datenschutzes zu verbessern.

Die Bereitschaft, alle mit der Datenschutzgruppe erörterten Maßnahmen umzusetzen, dokumentierte Microsoft in mehreren Schreiben an den Vorsitzenden der Gruppe, Professor

---

[3] Siehe WP 60, Arbeitsdokument - Erste Orientierungen der Artikel 29 Datenschutzgruppe zu Online-Authentifizierungsdiensten, angenommen am 2. Juli 2002.

[4] ABl. L 281 vom 23/11/1995, S. 31; siehe: http://europa.eu.int/comm/internal_market/de/dataprot/index.htm

[5] Siehe WP 60, Arbeitsdokument - Erste Orientierungen der Artikel 29 Datenschutzgruppe zu Online-Authentifizierungsdiensten, angenommen am 2. Juli 2002.

Rodotà[6], sowie in einem Zeitplan, der die Fristen für die Abwicklung der einzelnen Vorhaben festlegt. Die unterschiedliche Art der Maßnahmen rechtfertigt längere und kürzere Umsetzungsfristen. Einige vereinbarten Maßnahmen, z. B. die Überarbeitung des Wortlauts der Datenschutzerklärung zu .NET Passport (.NET Passport Privacy Statement) und die Bereitstellung zusätzlicher Informationen auf den Registrierungsseiten, sind nicht kompliziert und können rasch umgesetzt werden. Andere, z. B. der neue, nachstehend dargelegte Informationsfluss, verursachen beträchtlichen Programmieraufwand für .NET Passport und sind somit zeitaufwändiger.

Die Datenschutzgruppe hat den von Microsoft vorgelegten Zeitplan, um sich mit den Belangen der Datenschutzgruppe auseinandersetzen zu können, zur Kenntnis genommen. Dieser Zeitplan umfasst drei Kategorien von Zeitrahmen: erste Kategorie (0-4 Monate), zweite Kategorie (4-8 Monate) und dritte Kategorie (8-18 Monate). Der Zeitrahmen ist hinter der jeweiligen Maßnahme in Klammern angegeben. Einige der erörterten Maßnahmen sind in der Zwischenzeit bereits umgesetzt worden und werden im nachfolgenden Wortlaut entsprechend gekennzeichnet.

2.1. Kurzbeschreibung des .NET Passport-Systems von Microsoft

.NET Passport ist ein internetbasierter Authentifizierungsdienst, der eine einmalige Anmeldung (Single Sign-On) bei mehreren Partner-Sites ermöglicht, damit der Benutzer Zeit spart und seine Daten beim Surfen durch das Internet nicht wiederholt eingeben muss. Es handelt sich nicht um einen Dienst zur Autorisierung oder Identifikation von Benutzern, sondern um einen reinen Authentifizierungsdienst, der die Benutzer durch Prüfung der übermittelten Anmeldedaten eindeutig und sicher authentifiziert.[7] Der Dienst wurde 1999 eingerichtet und erhielt im Sommer 2000 den neuen Namen .NET Passport. Heute gibt es weltweit mehr als 250 Millionen Konten (wobei ein Benutzer mehrere Konten haben kann, was der Fall ist, wenn er mehrere Hotmail-Konten hat). Mehr als 40 Millionen Konten gehören in der EU ansässigen Personen.

Es gibt mehrere Wege zu einer Passport-Registrierung:
- über die Adresse www.passport.net;
- über eine Partner-Site;
- über die Einrichtung eines Hotmail-Kontos.

Ungefähr 87 % der Benutzer lassen sich über eine Partner-Site oder Hotmail, d. h. nicht direkt über die Microsoft-Site, registrieren. Ungefähr 120 Millionen Konten gehören Hotmail-Kontoinhabern und eine nicht unerhebliche Zahl von Benutzern lässt sich über Window Messenger registrieren. Hotmail ist ein E-Mail-Dienst, der weltweit genutzt und vollständig von der Firma Microsoft oder von anderen Unternehmen verwaltet wird, die von Microsoft kontrolliert werden.

Personenbezogene Daten werden derzeit über drei vordefinierte Informationsblöcke erhoben.

1. Mindestinformationen: Benutzername (E-Mail-Adresse) und Passwort.
2. Anmeldedaten: geheime Frage und Antwort, Telefonnummer und PIN, Sicherheitsschlüssel und drei zusätzliche Fragen und Antworten. Diese werden dann

[6] Siehe WP 60, Arbeitsdokument - Erste Orientierungen der Artikel 29 Datenschutzgruppe zu Online-Authentifizierungsdiensten, angenommen am 2. Juli 2002.

[7] Es sei darauf hingewiesen, dass neben der Datenschutz-Richtlinie auch andere Richtlinien wie die über den elektronischen Geschäftsverkehr oder die elektronische Signatur auf diese Dienste Anwendung finden können.

erforderlich, wenn der Benutzer sein Passwort vergessen hat. Diese Daten gehören nicht zum Profil und werden nicht an andere Sites übermittelt.

3. Maximale Profilinformationen: die oben genannten Daten plus Vorname, Nachname, Zeitzone, Geschlecht, Geburtsdatum, Beruf und Adresse. Die beteiligten Sites können die Daten direkt abrufen und zusätzliche Informationen verarbeiten. Momentan nehmen 69 externe (d. h. nicht zu Microsoft gehörige) Websites an .NET Passport teil, 22 davon sind EWR-Sites.

2.2. Juristische Probleme und Ergebnisse des Dialogs mit Microsoft

In seinem Papier von Juli 2002 verwies die Datenschutzgruppe auf eine Reihe von Problemen, die einer Klärung bedurften. In den folgenden Abschnitten wird jedes dieser Probleme genau untersucht, und es werden die Ergebnisse des Dialogs mit Microsoft zu jedem einzelnen Thema dargelegt.

Es sollte noch allgemein darauf hingewiesen werden, dass Microsoft außer den speziellen Maßnahmen, die in den folgenden Abschnitten beschrieben werden, eine Änderung des Datenflusses von .NET Passport zugesagt hat. Im Wesentlichen wird der Dienst dahingehend modifiziert, dass die Erstellung eines .NET Passport-Kontos getrennt von der Speicherung persönlicher Daten im Passport-Profil erfolgt. Der geänderte Datenfluss dürfte sich positiv auf einen gerechten Umgang bei der Erfassung und Verarbeitung von persönlichen Daten der Benutzer auswirken. Dies wird weiter unten bei der Frage der Verhältnismäßigkeit ausführlicher erläutert. Die Datenschutzgruppe hat diese Tatsache erfreut zur Kenntnis genommen.

2.2.1. Information der Benutzer zum Zeitpunkt der Datenerhebung, Weiterverarbeitung der Daten oder Übermittlung an Dritte, möglicherweise in einem Drittland

Bei der Untersuchung der Arbeitsweise von .NET Passport stieß die Datenschutzgruppe zuallererst auf das Problem, klare und transparente Informationen über dieses System zu finden. Das verfügbare Informationsmaterial war zum Teil unpräzise und konnte keine Aufklärung zu den wesentlichen Datenschutzfragen bieten (Identität des für die Verarbeitung Verantwortlichen, Zweck der Verarbeitung, Rechte der Betroffenen, Empfänger der Daten, Aspekte, die zwecks fairer Verarbeitung unbedingt geklärt werden müssen); manchmal erhielt das Material sogar widersprüchliche Angaben.
Zwei Fragen, die die Datenschutzgruppe besonderes beunruhigten, war die mangelhafte Information darüber, dass persönliche Daten direkt in ein Drittland übermittelt werden und dass eine Verbindung zwischen Hotmail und Passport besteht.

In der Zwischenzeit hat sich Microsoft verpflichtet, die folgenden Maßnahmen einzuleiten, um diese Bedenken der Datenschutzgruppe auszuräumen:

- Microsoft wird, wie von der Artikel 29-Datenschutzgruppe in seiner Empfehlung 2/2001[8] empfohlen, ein leicht zugängliches und benutzerfreundliches Dialogfeld einrichten, das die nach Artikel 10 der Richtlinie vorgeschriebenen Informationen enthält. Für die Benutzer, die angeben, in einem Land der Europäischen Union wohnhaft zu sein, wird auf der Registrierungsseite direkt neben dem Eingabefeld für das Land ein Link zu diesem Dialogfeld angezeigt. Wenn die Benutzer auf diesen Link klicken, wird das

[8] Empfehlung 2/2001 zu einigen Mindestanforderungen für die Online-Erhebung personenbezogener Daten in der Europäischen Union, angenommen am 17. Mai 2001, WP 43.

Dialogfeld in einem Fenster daneben angezeigt. Diese Funktion wird spätestens ab April 2003 zur Verfügung stehen.

- Die Benutzer werden entsprechend informiert, wenn sie sich auf einer Partner-Site des Landes registrieren, aus dem die Site stammt (8-18 Monate); außerdem können sie über einen Link im Dialogfeld zur Seite der Europäischen Kommission gelangen, auf der die Länder aufgelistet sind, deren Datenschutzgesetze den EU-Standards entsprechen (4 - 8 Monate).
- Über dieses Dialogfeld wird Microsoft die Benutzer aus EU-Staaten darüber informieren, wie lange die Protokolldaten gespeichert bleiben (derzeit höchstens 90 Tage) (0 - 4 Monate).
- Die Benutzer werden ganz am Anfang darüber informiert, wie sie ein .NET Passport-Konto anlegen können, ohne ihre tatsächliche E-Mail-Adresse verwenden zu müssen. Die Datenschutzgruppe hat eine solche Funktion schon mehrmals empfohlen. Gleichzeitig werden die Benutzer über die Einschränkungen für Pseudonym-Konten informiert, damit sie eine fundierte Entscheidung treffen können (8 - 18 Monate).
- Microsoft hat sich verpflichtet, alle Sprachfassungen der Datenschutzerklärung zu .NET Passport (.NET Passport Privacy Statement) gleichzeitig zu aktualisieren, es sei denn, Erwägungen vor Ort würden eine unverzügliche Änderung einer bestimmten Sprachfassung erfordern. In diesen voraussichtlich sehr seltenen Fällen wird Microsoft in den Datenschutzerklärungen der anderen Sprachen darauf hinweisen, dass diese bald aktualisiert werden (kurzfristig).
- Microsoft hat sich verpflichtet, eine Reihe von Maßnahmen bezüglich der Information von Hotmail-Benutzern zu ergreifen, um sicherzustellen, dass diesen Benutzern bei der Hotmail-Registrierung auch mitgeteilt wird, dass sie gleichzeitig ein Passport-Konto erhalten (bereits umgesetzt); ferner dass die Benutzer bei der Hotmail-Registrierung erfahren, dass sie für den Zugriff auf Hotmail ein Passport-Konto benötigen und dieses Konto nicht schließen können, ohne damit auch ihr Hotmail-Konto zu schließen (0 - 4 Monate).

2.2.2. Wert und Qualität der Zustimmung der Betroffenen

Nach der ersten Analyse des Systems ergaben sich für die Datenschutzgruppe einige Fragen bezüglich der Gültigkeit und Qualität der Einwilligung der Benutzer als gesetzliche Grundlage für die Verarbeitung von Daten gemäß Artikel 2 Buchstabe h der Richtlinie[9]. Mit anderen Worten: Die Datenschutzgruppe war nicht davon überzeugt, dass die Einwilligung der Benutzer ausreichend fundiert, freiwillig und spezifisch erfolgt, insbesondere bei Benutzern, die sich über Hotmail registrieren, sowie bei der Übermittlung personenbezogener Daten an Partner-Sites.

Wie oben erwähnt hat sich Microsoft verpflichtet, umfassende Maßnahmen zu ergreifen, um den Benutzern umfassende Informationen zur Verfügung zu stellen. Was die Entscheidung der Benutzer betrifft, persönliche Daten an Passport übermitteln zu lassen oder nicht, erlaubt ihnen der neue Datenfluss, persönliche Daten an eine Partner-Site zu übergeben, ohne diese in ihrem Passport-Profil zu speichern, und ein pseudonymes Passport-Konto ohne zusätzliche persönliche Daten anzulegen (8 - 18 Monate).

Die verbesserte Information von Hotmail-Benutzern umfasst auch weitere Maßnahmen, mit denen die Benutzer darauf hingewiesen werden, dass sie mit der Registrierung ihrer Hotmail-Konten auch ihre Zustimmung erteilen, dass Hotmail ihre Profildaten verwendet, um ihnen

[9] Die Einwilligung eines Benutzers ist ein freiwilliger, spezifischer und fundierter Ausdruck seines Wunsches, durch den er sich mit der Verarbeitung seiner persönlichen Daten einverstanden erklärt.

gezielte Werbemitteilungen zuzusenden (0 - 4 Monate). Es wird ihnen auf der Registrierungsseite von Hotmail explizit mitgeteilt, dass sie mit der Einwilligung in die allgemeinen Nutzungsbedingungen von Hotmail auch damit einverstanden sind, Werbung von Hotmail zu erhalten. Wie bei allen Partner-Sites wird Benutzern, die sich auf der Homepage von Hotmail für .NET Passport registrieren, die Möglichkeit eingeräumt werden, ihre persönlichen Daten nur an Hotmail zu geben und sie nicht in ihr .NET Passport-Profil aufnehmen zu lassen (8 - 18 Monate).

Die Datenschutzgruppe hat mit Microsoft auch die Möglichkeit erörtert, inwieweit die Hotmail-Benutzer eine gezielte Werbung durch Hotmail ablehnen können (Opt-Out). Microsoft hat dazu erklärt, dass ein Benutzer nach der Registrierung eines Hotmail-Kontos kostenlos ablehnen kann, gezielte Werbung zu erhalten, womit jedoch sein Hotmail-Konto geschlossen würde. Ein Benutzer kann also nicht ein kostenloses Hotmail-Konto führen, ohne diese Art von Werbung zu erhalten, weil es nur aufgrund der Einnahmen aus dieser gezielten Werbung möglich sei, die Hotmail-Konten kostenlos anzubieten. Wenn die Werbetreibenden sich nicht sicher sein könnten, dass sie mit ihrer Werbung die Benutzer auch erreichten, würden sie viel weniger für die Plazierung von Werbung zahlen und diese Einnahmequelle, die das kostenlose Hotmail-Angebot ermögliche, würde versiegen.

Die Datenschutzgruppe ist nach wie vor der Auffassung, dass noch nicht geklärt ist, ob diese Vorgehensweise im Einklang mit den EU-Rechtsvorschriften steht. Sie ist der Ansicht, dass diese Frage mit einem anderen Thema im Zusammenhang steht, nämlich mit der Praxis mehrerer Unternehmen, die Bereitstellung ihrer Dienstleistungen an die Auflage zu knüpfen, dass die Benutzer der Verwendung ihrer Daten zu Werbezwecken zustimmen, ohne dass sie dies ablehnen könnten. Dieses Thema hat nichts mit der konkreten Frage der Online-Authentifizierungsdienste zu tun, die Gegenstand dieses Arbeitspapiers ist; es wird später in einem breiteren Kontext behandelt.

Was die Einwilligung der Benutzer gegenüber Partner-Sites anbelangt, werden die Benutzer mit dem neuen Registrierungsvorgang ein Passport-Konto nur mit Benutzername und Passwort erhalten, da die Erstellung von Passport-Konten von der Entscheidung der Benutzer getrennt wird, den Partner-Sites persönliche Daten mitzuteilen oder im Profil zu speichern (8 - 10 Monate). Die Benutzer werden darauf hingewiesen werden, dass sie sich auf der Passport-Website für ein Passport-Konto registrieren können, indem sie lediglich Benutzername und Passwort angeben, dass sie bei der Anmeldung über eine Partner-Site jedoch eventuell speziell für diese Site zusätzliche Informationen bereitstellen müssen (diese Informationen werden in 4 - 8 Monaten in das Dialogfeld aufgenommen). Es wird eine neue Funktion eingerichtet, mit der die Benutzer für jede Site darüber entscheiden können, ob sie ihre Profildaten mitteilen möchten oder nicht. Das Benutzerprofil wird neu konfiguriert, damit die Benutzer nur die gewünschten Felder ausfüllen und andere leer lassen können (8 - 18 Monate).

Der neue Datenfluss wird es Benutzern ebenfalls ermöglichen, bei jeder Registrierung auf einer Partner-Site die Profildaten zu ändern, zu ergänzen sowie darüber zu entscheiden, ob diese Änderungen im Passport-Profil gespeichert werden sollen oder nicht, und welche Daten an die Site übermittelt werden sollen (8 - 18 Monate).

2.2.3. Verhältnismäßigkeit und Qualität der von .NET Passport erhobenen, gespeicherten und an Partner-Sites übermittelten Daten

Die Datenschutzgruppe hatte Bedenken bezüglich der Menge der von Passport erhobenen Daten, insbesondere der Profildaten. Dies gilt auch für die Tatsache, dass nach Anlegen eines

.NET Passport-Kontos - sofern der Benutzer die Freigabefelder ausgewählt hat - die gespeicherten Daten an alle Partner-Sites, die der Benutzer besucht und bei denen er sich anmeldet, übermittelt werden, unabhängig davon, ob dies für die betreffende Site überhaupt erforderlich ist. Bei der ersten Analyse des Systems hatte der Benutzer nicht die Möglichkeit, lediglich die Übermittlung eines Teils seiner Daten zu veranlassen, da alle Profildaten als Ganzes behandelt wurden.

Der neue, von Microsoft zu implementierende Datenfluss wird die Einrichtung eines .NET Passport-Kontos klar von der Entscheidung des Benutzers abgrenzen, persönliche Daten für die Partner-Site und .NET Passport mitzuteilen oder nicht. Die Benutzer werden selbst entscheiden können (Opt-In), ob die Informationen, die sie der Partner-Site mitteilen, in ihrem .NET Passport-Profil gespeichert werden sollen. Wenn ein Benutzer, dessen Daten in seinem .NET Passport-Profil gespeichert sind, eine Partner-Site besucht, wird er in der Lage sein, diese Daten feldweise zu ändern oder zu löschen, bevor er sie der Partner-Site mitteilt. Der Benutzer wird auch angeben können, ob diese geänderten oder gelöschten Daten in sein .NET Passport-Profil übernommen werden sollen oder nicht (8 - 18 Monate).

Mit diesen Änderungen und der Tatsache, dass der Benutzer darüber bestimmen kann, ob seine tatsächliche E-Mail-Adresse in bestimmten Fällen verwendet werden soll, werden, sobald sie einmal implementiert sind, die Bedenken der Datenschutzgruppe ausgeräumt werden, auch wenn die Datenschutzgruppe diesen Punkt weiter beobachten will, und zwar insbesondere unter Berücksichtigung der Tatsache, dass Microsoft dabei die Rolle zufällt, personenbezogene Daten und andere aufschlussreiche Informationen, die vom Benutzer freigegeben wurden, zu verarbeiten.

2.2.4. Datenschutzregeln der Partner-Sites von .NET Passport

Ein weiterer Kritikpunkt der Datenschutzgruppe bezog sich auf die Tatsache, dass bei den Partner-Sites nicht klar angegeben wird, bis zu welchem Grad der Schutz der Daten sichergestellt ist.

Bei den Gesprächen mit der Datenschutzgruppe stellte Microsoft klar, dass das Unternehmen keinen Einfluss auf die Datenschutzpraktiken der Partner-Sites hat. Durch den Kontakt mit diesen Sites würde Microsoft seinen Partnern jedoch eine Reihe von Schutzmechanismen vorschreiben; so seien die Partner beispielsweise verpflichtet, den Branchenstandards entsprechende Datenschutzregeln an prominenter Stelle auf den Sites und leicht zugänglich zu veröffentlichen, angemessene Sicherheitsmaßnahmen zu treffen, geltende Gesetze einzuhalten und keine Daten ohne Einwilligung der Benutzer für Dienste zu verwenden, die über die Bereitstellung der vereinbarten Dienste hinausgehen.

Microsoft hat sich verpflichtet, zusätzliche Schritte einzuleiten:

- Microsoft wird in seiner Datenschutzerklärung klar formulieren, dass Microsoft auf die Datenschutzregelungen der Partner-Sites keinen Einfluss hat (0 - 4 Monate).
- Microsoft wird die Partner-Sites zur Teilnahme an TRUSTe, BBBOnLine oder ähnlichen Diensten motivieren (0 - 4 Monate).
- Die Partner-Sites werden die Möglichkeit erhalten, sowohl auf der Seite, auf der die persönlichen Daten erhoben werden, als auch - in detaillierter Form - über einen Link von dieser Seite, die Benutzer darüber aufzuklären, wofür die Daten verwendet, wer die Empfänger sind und wie lange sie gespeichert werden (8 - 18 Monate). Die Datenschutzgruppe empfiehlt Microsoft, die Partner-Sites so schnell wie möglich über

ihre Empfehlungen für bestimmte Mindestanforderungen bei der Online-Erhebung personenbezogener Daten in der Europäischen Union zu informieren.[10]

Es sollte auf jeden Fall klar gestellt werden, dass, abgesehen von der Rolle, die Microsoft innerhalb des .NET Passport-Systems spielt, alle Partner-Sites als für die Verarbeitung Verantwortliche anzusehen sind, soweit es ihre eigenen Verarbeitungsoperationen betrifft. Sie tragen damit selbst die Verantwortung für die Einhaltung der Datenschutzgesetze.

2.2.5. Notwendigkeit und Voraussetzungen für die Nutzung eindeutiger Kennungen

Seit sich die Datenschutzgruppe mit dem Passport-System befasst, hat sie Bedenken dagegen, dass .NET Passport jedem Benutzer eine eindeutige Kennung - die PUID - zuteilt.

Die eindeutige Passport-Kennung (kurz „PUID“) wird bei der Registrierung erzeugt und bleibt während der gesamten Lebensdauer des Kontos bestehen. Sie umfasst 64 Bit und besteht aus zwei Teilen: 16 Bit zur Identifikation der Datenquelle, aus der sie generiert wurde, sowie 48 Bit zur Identifikation eines bestimmten Kontos. Die wichtigste Voraussetzung bei der Erzeugung einer PUID ist die Eindeutigkeit dieser Kennung. Die PUID basiert nicht auf Daten, die vom Kontoinhaber übermittelt wurden, und es gibt keine Informationen über den Kontoinhaber, die von der PUID abgeleitet werden können. Die PUID wird primär als Index für site-spezifische Datenspeicher verwendet. Eine PUID allein erlaubt keine Anmeldung und keinen Zugang zu den Profildaten eines Benutzers. Nur ein korrekt gebildetes Authentifizierungsticket (das die PUID enthält), das mit dem der Partner-Site zugewiesenen Schlüssel verschlüsselt wurde, kann als Token für die Sitzung verwendet werden. Ein Benutzer kann mehr als eine PUID haben, da jedem Passport-Konto eine PUID zugewiesen wird und ein Benutzer mehrere Passport-Konten besitzen darf.

Die Datenschutzgruppe war hauptsächlich darüber besorgt, dass die Verwendung von PUIDs die Partner-Sites in die Lage versetzen würde, Informationen über .NET Passport-Benutzer auszutauschen und Benutzerprofile zu erstellen. Die Verträge zwischen Microsoft und den Partner-Sites untersagen zwar den Verkauf von PUID-Einträgen an Dritte oder die Verlinkung von Seiten ohne Zustimmung der Benutzer, ferner sehen sie strenge Einschränkungen für die Nutzung der PUID vor, dennoch bleibt immer ein Risiko, wenn die technischen Möglichkeiten gegeben sind. Eine weitere Frage, die von der Datenschutzgruppe angesprochen wurde, war die Möglichkeit der Benutzer, auf ihre eigene PUID zuzugreifen.

Den zweiten Punkt betreffend hat Microsoft sich verpflichtet, den Benutzern auf Anfrage Zugriff auf ihre PUIDs zu gewähren (8 - 18 Monate). Die Datenschutzgruppe möchte dabei auf die übermäßige Verzögerung bei der Ausübung der Zugriffsrechte auf die PUID hinweisen. Auch wenn der Zugang nicht online erfolgt, sollten sie umgehend auf andere Art und Weise in die Lage versetzt werden, ihr Recht auszuüben.

Die Nutzung einer eindeutigen Kennung wurde von Microsoft und den Mitgliedern der Internet-Taskforce ausgiebig erörtert. Microsoft versteht die Bedenken der Arbeitsgruppe und hat sich bereit erklärt, nach alternativen Identifikationsstrukturen für .NET Passport zu suchen.

[10] Empfehlung 2/2001 zu einigen Mindestanforderungen für die Online-Erhebung personenbezogener Daten in der Europäischen Union, angenommen am 17. Mai 2001, WP 43.

Es wurde mit Microsoft vereinbart, die Diskussion über diesen Punkt weiterzuführen, um nach einer geeigneten Alternative zu suchen.

2.2.6. Wahrung der Rechte der Benutzer

Die Datenschutzgruppe zeigte sich besorgt über die Probleme im Zusammenhang mit den Rechten der Benutzer, insbesondere bei dem Versuch, sich von Passport abzumelden.

In seinen Gesprächen mit der Datenschutzgruppe gab Microsoft zu, dass es in der Vergangenheit Schwierigkeiten gegeben habe, und sicherte zu, eine Reihe von Maßnahmen zu ergreifen, um den Benutzern die Ausübung ihrer Rechte zu erleichtern. Hierzu zählen:

- Bereitstellung einer übersichtlichen, verständlichen Zusammenfassung der gemäß Artikel 10 der Richtlinie vorgeschriebenen Informationen in einem Dialogfeld, einschließlich Informationen über die Rechte der Betroffenen (spätestens April 2003).
- Information der Benutzer in der Datenschutzerklärung und im Begrüßungsmail, dass sie direkte Anfragen an passpriv@microsoft.com senden können (bereits umgesetzt bzw. 0 - 4 Monate).
- Beantwortung von Anfragen von Passport-Benutzern in der Sprache des jeweiligen Kunden, sofern Passport in dieser Sprache angeboten wird (0 - 4 Monate).

Seit September 2002 können die Benutzer ihr .NET Passport-Konto einfach schließen, indem sie passport.net aufrufen und auf den Link „Mitgliederservice“ klicken. Der Benutzer wird dann durch die einzelnen Schritte zum Schließen seines Passport-Kontos geführt. Bei Konten, die auf passport.net erstellt wurden, läuft dieser Vorgang vollautomatisch ab. Der Benutzer gelangt auf eine Seite, auf der die Folgen der Kontoschließung erläutert werden und auf der sich eine Schaltfläche zum Schließen des Kontos befindet. Bei Konten, die auf Hotmail angelegt wurden, geht der Benutzer ähnlich vor: Er wird zunächst auf die Homepage von Hotmail weitergeleitet, auf der sich die Seite zum Schließen des Kontos befindet.

2.2.7. Sicherheitsrisiken bei diesen Aktionen

Die Datenschutzgruppe überprüfte auch etwaige Sicherheitsrisiken des Systems, insbesondere im Zusammenhang mit der Konzentration der Daten auf zwei großen Datenbanken. Dies ist besonders brisant, da Microsoft ein beliebtes Angriffsziel für Hacker darstellt.

Die Datenschutzgruppe hat zur Kenntnis genommen, dass Microsoft ein Informationssicherheitsprogramm (Information Security Program) im Rahmen des übereinstimmenden Antrags (Consent Order) der US-Handelsbehörde aus dem Jahre 2002 in Angriff genommen hat. Die wichtigsten Auflagen dieses Programms sind:

- Einrichtung geeigneter administrativer, technischer und physischer Schutzfunktionen, einschließlich überarbeiteter Sicherheitsregelungen basierend auf ISO 17799. Die Standardverfahren werden für jede größere Gruppe so geändert, dass sie dem Informationssicherheitsprogramm entsprechen. Diese Verfahren werden den technologischen und geschäftlichen Entwicklungen nach Bedarf angepasst.
- Ernennung mindestens eines Mitarbeiters, der die Koordination und Verantwortung für das Informationssicherheitsprogramm übernimmt. Interessenvertreter aller beteiligten Gruppen werden bei der Ausarbeitung und Umsetzung der Standardverfahren des Informationssicherheitsprogramms helfen.

Es werden mehrere Programme formalisiert und gleichzeitig mit der Implementierung des überarbeiteten Programms dokumentiert. Zu diesen Programmen gehören:

- Sicherheitstraining für Teams, die mit dem Betrieb und der Anwendungsentwicklung beschäftigt sind;
- Reaktionsverfahren bei Zwischenfällen und Eskalation;
- Aufbau eines Überwachungsteams für Sicherheitsfragen auf Abteilungsebene.

2.3. Schlussfolgerung

Die Datenschutzgruppe begrüßt die bedeutenden Schritte, die Microsoft bereits unternommen hat bzw. in den nächsten Monaten noch unternehmen wird, und mit denen das Unternehmen dafür sorgen will, dass das .NET Passport-System den Bestimmungen der europäischen Datenschutzrichtlinie gerecht wird. Es muss nicht betont werden, dass die Datenschutzgruppe die Weiterentwicklung des Systems in den nächsten Monaten genau verfolgen und dabei prüfen wird, wie die von Microsoft angekündigten Maßnahmen umgesetzt werden.

Die Datenschutzgruppe nimmt auch die von den NROs geäußerte Besorgnis über die Einrichtung eines zentralen Systems zur Speicherung personenbezogener Daten zur Kenntnis. Die Datenschutzgruppe wird diesen Punkt auch im Hinblick auf die Sicherheitsaspekte weiterhin überwachen.

Da sich der .NET Passport -Dienst in ständigem Wandel befindet, seine Architektur sich deshalb möglicherweise verändern wird und die Notwendigkeit besteht, die Überlegungen zu einigen der oben genannten Probleme zu vertiefen (insbesondere hinsichtlich der PUID), wird die Datenschutzgruppe deshalb die künftige Entwicklung des Systems weiter verfolgen und nötigenfalls den Dialog mit Microsoft wieder aufnehmen. Microsoft hat sich damit einverstanden erklärt, die Datenschutzgruppe über die betreffend das.NET Passport-System unternommenen Schritte zu unterrichten.

3. FALLSTUDIE 2: DAS LIBERTY ALLIANCE-PROJEKT

3.1. Kurze Beschreibung des Systems

Das Projekt Liberty Alliance wurde im Dezember 2001 ins Leben gerufen und umfasst inzwischen mehr als 100 Unternehmen, gemeinnützige Organisationen und Regierungen weltweit, die sich auf Vertragsbasis zu dieser Gruppe zusammengeschlossen haben. Die Liberty Alliance ist keine Rechtssubjekt, sondern ein Ad-hoc-Projekt, an dem verschiedene Unternehmen gemäß den Bedingungen der Projektvereinbarung teilnehmen. Die Aufgabe der Liberty Alliance ist die Entwicklung von Standards für eine offene und föderative Netzwerkidentität mittels offener technischer Spezifikationen. Vereinfachte Registrierung und föderative Netzwerkidentität (ein System zur Bindung mehrerer Konten für einen Benutzer) sind die Schlüsselelemente des Systems. Single Sign-On bietet dem Benutzer die Möglichkeit, sich einmal in einer Sitzung über einen „Identitätsanbieter“ (Identity Provider) zu authentifizieren und danach innerhalb einer vertrauenswürdigen Domäne (Trust Domain) zu verschiedenen Dienstanbietern zu navigieren, ohne sich erneut authentifizieren zu müssen.

Das System funktioniert innerhalb vertrauenswürdiger Domänen oder so genannter „Circles of Trust“, d. h. einem Verbund sich gegenseitig vertrauender Dienst- und Identitätsanbieter, deren Geschäftsbeziehungen auf die Architektur und die Betriebsbedingungen der Liberty Alliance setzen und mit denen geschäftliche Transaktionen in einer sicheren und scheinbar nahtlosen Umgebung abgewickelt werden können.

Die Liberty Alliance-Spezifikationen befinden sich noch in einer frühen Entwicklungsphase und sind bislang kaum implementiert worden[11]. Es wird erwartet, dass diese Spezifikationen in der Zukunft von Technologieunternehmen implementiert werden, um Techniken bereitzustellen, die gemäß den Liberty Alliance-Spezifikationen zugelassen sind.

3.2. Analyse der derzeitigen Situation

- Das Protokoll in seiner heutigen Form ermöglicht die Erfüllung der Anforderungen der Richtlinie. Die Datenschutzgruppe möchte betonen, dass die Liberty Alliance die Verantwortung für die technische Entwicklung des Projekts trägt. Es sollte sichergestellt werden, dass die Spezifikationen und das Protokoll die nutzenden Unternehmen in die Lage versetzt, die Richtlinie zu erfüllen. Darüber hinaus gelten alle beteiligten Unternehmen als für die Verarbeitung der Daten Verantwortliche, wenn sie eine gemäß Liberty zugelassene Site betreiben; sie tragen in diesem Zusammenhang ferner die Verantwortung für die Einhaltung der geltenden Datenschutzgesetze.

- Das Liberty Alliance-Protokoll ist bezüglich des Datenschutzes „neutral“; d. h. es ermöglicht die Erfüllung der Richtlinie, setzt sie jedoch nicht voraus; es werden auch keine Maßnahmen dahingehend ergriffen. Die Datenschutzgruppe möchte die Liberty Alliance darin bestärken, Empfehlungen und Leitlinien auszuarbeiten, die die Unternehmen motivieren sollen, die Spezifikationen im Sinne des Datenschutzes oder gar zu seiner weiteren Verbesserung umzusetzen. Das System kann auch spezielle Funktionen enthalten, die auf die Besonderheiten der europäischen Gesetzgebung auf diesem Gebiet abstellen. Dies könnte besonders wichtig für die Identitätsanbieter sein, die riesige Datenmengen über die Benutzer besitzen werden.

- Der Datenschutzgruppe ist aufgefallen, dass viele an der Liberty Alliance beteiligte Unternehmen aus den USA stammen; es ist zu erwarten, dass die Anwendung der Spezifikationen in der Praxis dazu führen wird, dass eine ganze Menge persönlicher Daten von Europa in die USA übermittelt werden. Die Datenschutzgruppe empfiehlt den US-Unternehmen, die am Liberty Alliance-Projekt teilnehmen, die persönlichen Daten, die an sie übermittelt werden, angemessen zu schützen.

- Angesichts der Tatsache, dass das Liberty Alliance-Projekt noch nicht so weit fortgeschritten ist und noch nicht in die Praxis umgesetzt wurde, ist es schwierig, die Vor- und Nachteile der Nutzung paarweiser Identitäten vorauszusehen. Die Datenschutzgruppe möchte jedoch an dieser Stelle deutlich machen, dass das System paarweiser IDs zwar den Vorteil hat, dass keine eindeutige ID für den Benutzer erstellt wird, dass andererseits aber diese Frage aus Sicht des Datenschutzes weiter untersucht werden muss, insbesondere was die technischen Möglichkeiten von Sites anbelangt, die personenbezogene Daten von Benutzern ohne deren Einwilligung miteinander teilen könnten.

Auch wenn paarweise IDs weniger strenge Anforderungen als generelle an die Authentifizierung zu stellen scheinen, sind die technischen Möglichkeiten von Sites, sich miteinander zu teilen, weiterhin ein Thema, das zu Besorgnis Anlass gibt.

[11] Sun One ist besitzt die „Liberty-Zulassung“.

3.3. Einige Erwägungen zu möglichen Problemen in der Zukunft

Momentan gleichen die Spezifikationen der Liberty Alliance eher einem Prototyp, der kaum in der Praxis angewendet wurde und in der Zukunft sicherlich noch mehrmals geändert werden muss.

Die Datenschutzgruppe möchte deshalb diese Entwicklung in der Zukunft weiter verfolgen, um sicherzustellen, dass die Anforderungen der Richtlinie berücksichtigt werden. In diesem Zusammenhang sollten insbesondere die Nutzung von Cookies, die Möglichkeit der Benutzer, ihre Kennung aktiv zu aktualisieren[12], die automatisierte Föderation[13], die Rolle der Identitätsanbieter, die Arbeitsweise der „Circles of Trust“[14] und die Verträge geprüft werden, die zwischen den Unternehmen geschlossen werden, die eine föderative Identitätsverwaltung nutzen.

Die Datenschutzgruppe möchte die Liberty Alliance auffordern, die in Fallstudie 1 genannten Probleme und die Ergebnisse der Gespräche mit Microsoft bei der Erörterung seiner Spezifikationen zu berücksichtigen. Wenn sich die Liberty Alliance mit Fragen der „Opaque handles“ und paarweisen Identitäten befasst, sollten alle im Zusammenhang mit der PUID angesprochenen Probleme bedacht werden.

4. VERGLEICH DER DERZEITIGEN ONLINE-AUTHENTIFIZIERUNGSSYSTEME

Mozilla Password Manager	**Authentifizierung durch Proxy**	**Microsoft Passport**	**Liberty Alliance**
Kein externer Identity Provider	Externer Identity Provider wird vom Benutzer gewählt.	Microsoft arbeitet mit externem Identity Provider.	Externer Identity Provider wird vom Dienstanbieter gewählt (gegenseitige Verträge).
Zugang nur über eigenen PC	Zugang über die vom Authentifizierungsan-bieter bereitgestellten Kanäle	Zugang über verschiedene Geräte möglich, momentan v. a. PC-ähnliche Geräte	Zugang über verschiedene Geräte möglich, auch Mobiltelefone
Derzeit verfügbar und weit verbreitet	Nur begrenzt verfügbar	Derzeit verfügbar; wird von allen Microsoft-Diensten genutzt	Umsetzung noch in Anfangsphase

[12] “Opaque handles” werden für die Bindung mehrer lokaler Konten innerhalb einer vertrauenswürdigen Domäne benutzt. Sie werden jeweils von zwei Anbietern innerhalb einer vertrauenswürdigen Domäne anerkannt. Eine „Kennung“ ist eine willkürliche Zeichenfolge, die jeder Anbieter seinen Daten über den Benutzer zuordnet.

[13] Das Projekt Liberty Alliance wendet für die Einrichtung und Schließung von Konten durch die Benutzer ein föderatives Modell an.

[14] Ein gemäß Liberty zugelassenes System, das für die Vertragspartner Identitätsinformationen erstellt, bewahrt und verwaltet und Vertragspartner bei anderen Dienstanbietern innerhalb eines „Circle of Trust“ authentifiziert.

Benutzer-ID und Passwort pro Site	Benutzer-ID und Passwort pro Site	Eine Benutzer-ID und ein Passwort	Benutzer-ID und Passwort pro Site
Benutzer wird durch Benutzer-ID und Passwort identifiziert.	Benutzer wird durch Benutzer-ID und Passwort identifiziert.	Eine eindeutige ID für einen Benutzer (PUID)	Verschiedene Kennungen pro Site-Paar
Kein Vertrag notwendig	Vertrag zwischen Benutzer und Anbieter	Vertrag zwischen Microsoft und Dienstanbieter	Vertrag zwischen allen Sites innerhalb des Circle of Trust
-	Das Authentifizierungs-protokoll setzt voraus, dass dem Proxy-Anbieter bekannt ist, welche Sites mit Authentifizierung besucht werden (Speichern von Kombination aus Benutzername/ Passwort pro Site).	Microsoft verwendet eine eindeutige PUID pro Benutzer.	Eindeutige Kennung pro Benutzer pro föderativem Site-Paar. Authentifizierungs-anbieter muss nur die Sites kennen, die die ID verwenden.
Durch die Verwendung verschiedener Benutzer-IDs kann der Benutzer verhindern, dass die Dienstanbieter Daten kombinieren.	Durch die Verwendung verschiedener Benutzer-IDs kann der Benutzer verhindern, dass die Dienstanbieter Daten kombinieren.	Eindeutige PUID identifiziert den Benutzer. Vertragsvereinbarun-gen verhindern, dass Dienstanbieter Daten kombinieren.	Benutzerdaten können nur nach Paar-Sites kombiniert werden. Sites legen ihre eigenen Verträge untereinander fest.
Nur Dienstanbieter hat die Kontrolle über die Daten.	Dienstanbieter und Proxy-Anbieter haben Kontrolle über die Daten.	Dienstanbieter, die eine Authentifizierungs-anfrage bearbeiten, und Microsoft haben Kontrolle über die Daten.	Dienstanbieter innerhalb eines Circle of Trust haben in dem Moment Kontrolle über die Daten, in dem Benutzer ihre Site besuchen.
Keine Datenübermittlung zwischen Anbietern.	Authentifizierungs-daten werden zwischen Anbietern übermittelt.	Authentifizierungs- und manchmal auch Profildaten werden zwischen Anbietern übermittelt.	Authentifizierungs-daten werden zwischen Anbietern übermittelt.
Benutzer steuert sämtliche Kommunikation.	Einwilligung des Benutzers erforderlich	Einwilligung des Benutzers erforderlich (gefordert durch Plattform und Verträge von Microsoft)	In der Regel ist zweimal pro Föderation eine Einwilligung des Benutzers erforderlich, automatische Föderation ist jedoch möglich.

Authentifizierungs-protokoll erfordert keine Cookies.	Authentifizierungs-protokoll erfordert keine Cookies.	Derzeitige Version verwendet Cookies.	Derzeitige Version verwendet Cookies.

5. SCHLUSSFOLGERUNG

Die Arbeitsgruppe betont, dass die Schlussfolgerungen, die aus den beiden Fallstudien gezogen wurden, für alle Online-Authentifizierungssysteme gelten, wenn es um Datenschutzfragen geht. Bei der Auswahl der beiden Fallstudien wurde die aktuelle Entwicklung des Marktes von Online-Authentifizierungsdiensten berücksichtigt - alle ähnlichen Dienste sollten jedoch dieselben datenschutzrelevanten Überlegungen anstellen, die sich wie folgt zusammenfassen lassen:

- Wer Online-Authentifizierungssysteme konzipiert oder tatsächlich umsetzt (Authentifizierungsanbieter), ist für die datenschutzrelevanten Aspekte verantwortlich, wenngleich auf unterschiedlichen Ebenen. Websites, die diese Technologien einsetzen (Dienstanbieter), tragen ihrerseits Verantwortung in dem Prozess. Die verschiedenen Akteure sollten klare Vertragsvereinbarungen treffen, in denen die Pflichten der jeweiligen Partei ausdrücklich aufgeführt sind.
- Es sollte alles darangesetzt werden, dass Online-Authentifizierungssysteme anonym oder pseudonym genutzt werden können. Sofern dies den vollen Funktionsumfang einschränken würde, sollte ein System so aufgebaut sein, dass ein Minimum an Informationen für die Authentifizierung des Benutzers ausreicht und der Benutzer völlig frei darüber entscheiden kann, zusätzliche Informationen (beispielsweise Profildaten) bereitzustellen. Diese Möglichkeit sollte sowohl beim Authentifizierungsanbieter als auch bei den Dienstanbietern (den Sites, die das System nutzen) bestehen.
- Es ist unabdingbar, die Benutzer angemessen über die datenschutzrechtlichen Hintergründe eines Systems zu informieren (Identität des für die Verarbeitung Verantwortlichen, Zweck, erhobene Daten, Empfänger usw.). Diese Informationen sollten leicht zugänglich und benutzerfreundlich angeboten werden, vorzugsweise im Anmeldeformular oder in einem sich automatisch öffnenden Dialogfeld, das auf dem Bildschirm des Benutzers erscheint, und in allen Sprachen, in denen der Dienst angeboten wird.
- Falls persönliche Daten in Drittländer übermittelt werden, sollten Authentifizierungsanbieter mit Dienstanbietern zusammenzuarbeiten, die alle erforderlichen Schutzmaßnahmen ausschöpfen[15] oder den Schutz der persönlichen Daten der Systembenutzer durch entsprechende Sicherheitsvorkehrungen gewährleisten, sei es auf vertraglicher Basis oder durch verbindliche Unternehmensgrundsätze. Das sollte die allgemeine Regel sein. Falls in spezifischen Fällen die Übermittlung auf Grund der Einwilligung erfolgt, sollten dem Benutzer ausreichende Informationen und Auswahlmöglichkeiten angeboten werden, so dass er seine Zustimmung zu der Übermittlung von Fall zu Fall erteilen oder verweigern kann.
- Die Verwendung von Kennungen jeglicher Form birgt Datenschutzrisiken. Allen möglichen Alternativen sollte in vollem Umfang Rechnung getragen werden. Wenn Benutzerkennungen unumgänglich sind, sollte erwogen werden, den Benutzern die Möglichkeit einzuräumen, die Kennungen zu aktualisieren.

[15] Diese Möglichkeit besteht z. B. in den Vereinigten Staaten bei Unternehmen, die die „Safe Harbor"-Kriterien erfüllen und dazu bewegt werden sollten, sich diesem System anzuschließen.

- Die Verwendung einer Software-Architektur, die die Zentralisierung von personenbezogenen Daten der Internet-Benutzer auf ein Mindestmaß beschränkt, sollte als Maßnahme gewürdigt und gefördert werden, um die Fehlertoleranz-Eigenschaften des Authentifizierungssystems zu vergrößern und die Entstehung von umfangreichen Datenbanken zu verhindern, die einem einzigen Unternehmen oder einem kleinen Kreis von Unternehmen oder Organisationen gehören und von diesen verwaltet werden.
- Die Benutzer sollten die Möglichkeit haben, ihre Rechte auf einfache Weise wahrzunehmen (dies schließt das Recht zur Ablehnung (Opt-Out) ein) und auf Löschung ihrer Daten zu bestehen, wenn sie ein Online-Authentifizierungssystem nicht mehr benutzen wollen. Sie sollten ferner angemessen darüber informiert werden, wie sie bei Anfragen oder Beschwerden zu verfahren haben.
- Die Sicherheit spielt eine Schlüsselrolle in diesem Zusammenhang. Es sollten organisatorische und technische Maßnahmen ergriffen werden, die dem jeweiligen Risiko angemessen sind.

Angesichts des stetigen Wandels von .NET Passport, Liberty Alliance und ähnlicher Authentifizierungsdienste wird die Datenschutzgruppe zukünftige Entwicklungen in diesem Bereich weiter verfolgen, **insbesondere um sicherzustellen, dass die von Microsoft eingegangenen Verpflichtungen in dem vorgeschlagenen**, in Kapitel 2 dieses Papiers aufgeführten **Zeitrahmen erfüllt werden**.

Brüssel, den 29. Januar 2003
Für die Datenschutzgruppe
*Der Vorsitzende*Stefano RODOTA