Verteilte Dienstnutzung mit dem neuen Personalausweis *

M. Horsch[1] · J. Braun[1] · A. Wiesmaier[2] · J. Schaaf[3] · C. Baumöller[4]

Technische Universität Darmstadt[1]
{jbraun | horsch}@cdc.informatik.tu-darmstadt.de

AGT Group (R&D) GmbH[2]
awiesmaier@agtinternational.com

Deutsche Telekom AG, Telekom Innovation Laboratories[3]
joachim.schaaf@telekom.de

Telekom Deutschland GmbH[4]
claas.baumoeller@telekom.de

Zusammenfassung

Eine Authentisierung mittels Benutzername und Passwort birgt vielfältige Gefahren, wie beispielsweise das Aufzeichnen durch Schadsoftware. Authentisierungsmechanismen auf Basis von Smartcards wirken durch den Besitzfaktor einem solchen Angriff entgegen, sind aber oftmals nicht einsetzbar, weil es an den passenden Kartenlesern fehlt. Die direkte Verbindung von Lesegeräten zum Nutzersystem ermöglicht dabei neue Angriffe, wenn beispielsweise die PIN über die Tastatur des Nutzersystems eingegeben wird. Wir stellen ein Verfahren vor, das es ermöglicht die Authentisierung gänzlich unabhängig vom Nutzersystem durchzuführen. Dadurch wird das Problem der Verfügbarkeit der Lesegeräte für Smartcards gelöst. Außerdem sind Nutzereingaben nicht weiter durch Schadsoftware auf dem Nutzersystem gefährdet, da diese nur noch auf einem dem Nutzer zugeordneten sicheren Authentisierungsgerät erfasst werden.

1 Einleitung

Eine Authentisierung gegenüber Diensten oder Systemen erfolgt trotz der bekannten Sicherheitsrisiken[1], vorwiegend anhand Benutzernamen und Passwörtern. Dabei birgt eine solche Authentisierung auf Basis von Wissen erhebliche Sicherheitsrisiken in sich. Passwörter lassen sich leicht durch Schadsoftware abgreifen und Nutzer neigen dazu gleiche Zugangsdaten für mehrere Dienste zu verwenden.

Authentisierungsverfahren auf Basis von Besitz und Wissen haben hingegen deutliche Vorteile in Bezug auf die Sicherheit und die Benutzerfreundlichkeit. Für einen flächendeckenden Einsatz mangelt es aber oft an der universellen und flexiblen Einsetzbarkeit. Bei der Verwendung von Smartcards als Besitzkomponente zur Authentisierung fehlt es, beispielsweise unterwegs,

* Das vorliegende Konzept ist ein Ergebnis des Kooperationsprojektes MONA (Mobile Authentisierung mit dem neuen Personalausweis) der Technischen Universität Darmstadt und der Telekom Innovation Laboratories.

[1] http://www.heise.de/security/meldung/Das-Passwort-Die-einzige-Konstante-im-Leben-1030313.html

oft an den passenden Kartenlesern. Aber auch die Sicherheit der verfügbaren Kartenleser, beispielsweise in Internet-Cafés, kann nur schwer überprüft werden.

Mobile Geräte eignen sich durch ihre starke Verbreitung und hohe Bindung an den Besitzer als persönliche Sicherheitsumgebung (Personal Security Environment) und damit als zentrales besitzbasiertes Authentisierungssystem. Ausgestattet mit der passenden Technologie können diese als Schlüssel-Speicher, Signatur-Erstellungseinheit oder Kartenleser fungieren (vgl. [BHWH11, BrHW12] und damit eine deutlich stärkere Authentisierung ermöglichen. Jedoch haben die kleinen Displaygrößen und eine Steuerung per Touchscreen eine andere visuelle und haptische Wahrnehmung zur Folge als klassische Computer, und lassen sich daher für gewisse Dienste nur eingeschränkt nutzen. Dies betrifft insbesondere Dienste mit vielen Multimedia-Inhalten.

Wir stellen ein Verfahren vor, bei dem eine Authentisierung mit einem mobilen Gerät durchgeführt wird (vgl. [BWHB$^+$10, WHBK$^+$11]), die Nutzung der Dienste aber bequem an einem Rechner, Notebook oder Tablet usw. möglich ist. Die strikte Trennung zwischen Systemen zur Authentisierung und zur Dienstnutzung bietet die Möglichkeit jederzeit eine sichere Identifizierung des Nutzers durchzuführen und die Zugangsdaten vor dem Abhören durch Schadsoftware auf dem Dienstnutzungssystem zu schützen. Der Einsatz eines mobilen Gerätes als zentrales Authentisierungssystem bietet den Nutzern einen sicheren Zugriff auf Dienste von beliebigen Computern aus. Diese verteilte Dienstnutzung kann dabei anhand verschiedener Authentisierungsmechanismen und -verfahren erfolgen und gestattet die Umsetzung verschiedener Sicherheitsanforderungen. Im Folgenden betrachten wir beispielhaft den Einsatz des elektronischen Identitätsnachweises (eID-Funktion) des neuen Personalausweises als Authentisierungsmechanismus für die verteilte Dienstnutzung.

Der vorliegende Beitrag fasst in Kapitel 2 die Grundlagen zum neuen Personalausweis zusammen. In Kapitel 3 stellen wir das Verfahren der verteilten Dienstnutzung ausführlich vor und erörtern es in Kapitel 4.

2 Der neue Personalausweis

Der neue Personalausweis (nPA) verfügt über einen Chip zur Speicherung personenbezogener Daten des Ausweisinhabers und ist mit einer kontaktlosen RFID-Schnittstelle gemäß ISO/IEC 14443 [ISO11] ausgestattet. Neben der klassischen Anwendung als hoheitliches Ausweisdokument unterstützt der Ausweis den elektronischen Identitätsnachweis (eID-Funktion) [BSI11b] und das Erstellen von qualifizierten elektronischen Signaturen (eSign-Funktion) [BSI10a]. Diese Funktionen sind jeweils durch eine sechsstellige PIN geschützt [BSI11a].

Die eID-Funktion ermöglicht eine Registrierung und Anmeldung bei Dienstanbietern im Internet. Im Gegensatz zu einer klassischen Authentisierung wird hierbei das Wissen von Benutzername und Passwort durch eine deutlich sicherere Zwei-Faktor-Methode, nämlich den Besitz des Ausweises und das Wissen der PIN, ersetzt. Darüber hinaus können die erforderlichen Daten (z.B. Name, Anschrift) während der Registrierung (z.B. bei einem Online-Shop) direkt vom Ausweis gelesen werden. Die Durchführung eines Authentisierungsvorgangs mit der eID-Funktion erfolgt in der Regel jedoch nicht direkt durch die Dienstanbieter, sondern wird von speziellen eID-Service-Providern [BSI10b] durchgeführt. Für die Nutzung der Funktionen benötigen Bürger neben einem passenden Kartenleser auch eine installierte eID-Applikation wie beispielsweise die AusweisApp [BSI] oder die Open eCard App [HPSW$^+$12].

Das Sicherheitssystem des Ausweises besteht neben physikalischen Eigenschaften auch aus mehreren kryptografischen Sicherheitsprotokollen, die einen unberechtigten Zugriff verhindern [BSI12a]. Das *Password Authenticated Connection Establishment* (PACE) Protokoll führt an-

hand der PIN eine Authentisierung des Benutzers durch und sichert gleichzeitig die kontaktlose Schnittstelle ab. Das *Extended Access Control* (EAC) Protokoll führt eine gegenseitige Authentisierung zwischen dem Ausweis und dem Online-Dienst durch. Dabei muss der Online-Dienst anhand eines Berechtigungszertifikates nachweisen, dass er zum Auslesen des Ausweises berechtigt ist. Ist dies erfolgt, muss der Ausweis seine Echtheit gegenüber dem Dienst nachweisen.

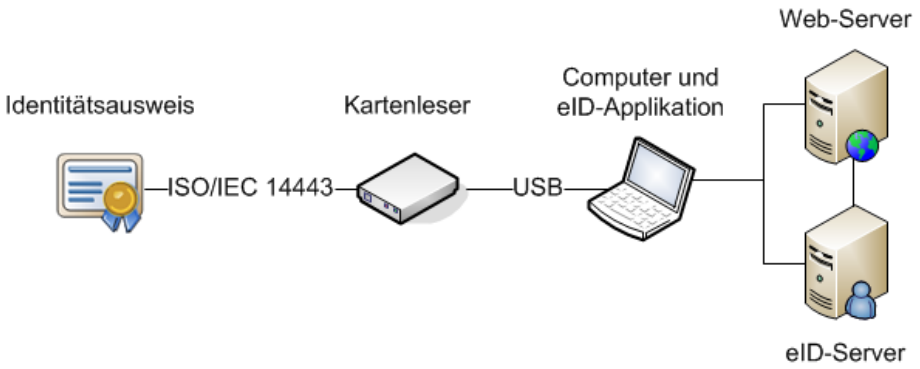

Abb. 1: eID-Infrastruktur

Abbildung 1 zeigt die für die eID-Funktion benötigte Infrastruktur. Auf der Nutzerseite wird der Identitätsausweis, ein Kartenleser und ein Computer mit installierter eID-Applikation benötigt. Die Dienste werden von Web-Servern bereitgestellt, auf die vom Computer aus zugegriffen werden kann. Die eID-Server stellen die benötigte Infrastruktur und Schnittstellen für eine Authentisierung mit dem nPA bereit.

3 Verteilte Dienstnutzung

Im Folgenden stellen wir die verteilte Dienstnutzung vor und zeigen insbesondere, wie die Authentisierung über das Authentisierungssystem ausgelöst wird. Dabei stellen wir zwei unterschiedliche Varianten dar: ein Push-Verfahren, bei dem die Authentisierung von außen ausgelöst wird sowie ein Pull-Verfahren, bei dem der Authentisierungsvorgang von Seiten des Authentisierungssystems angestoßen wird.

Der Prozess der Nutzung von Diensten lässt sich abstrakt in drei Phasen einteilen:

1. Aufruf des Dienstes
2. Nachweis der Berechtigung zur Nutzung des Dienstes
3. Inanspruchnahme des Dienstes

Das vorgestellte Verfahren verteilt die Phasen der Dienstnutzung auf zwei Systeme: Die erste und dritte Phase erfolgt auf einem Nutzungssystem, von dem der Benutzer den Dienst zu Beginn aufruft und abschließend nutzt. Die zweite Phase erfolgt auf einem Authentisierungssystem, auf dem der Benutzer eine Authentisierung durchführt und damit den Nachweis der Berechtigung zur Nutzung des Dienstes erbringt. Nutzungs- und Authentisierungssystem sind dabei physikalisch getrennt, so dass das Nutzungssystem keinen Zugriff auf Eingaben der zweiten Phase wie Zugangsdaten, Passwörter usw. hat, und das Authentisierungssystem umgekehrt keine Kenntnis bezüglich des Dienstes hat. Das heißt, es folgt eine strikte Trennung zwischen diesen Systemen und damit zwischen Dienstnutzung und Authentisierung. Die einzige Schnittstelle zwischen den Systemen ist der Benutzer.

Wie in Abbildung 2 ersichtlich, besteht das Gesamtsystem zur verteilten Dienstnutzung aus

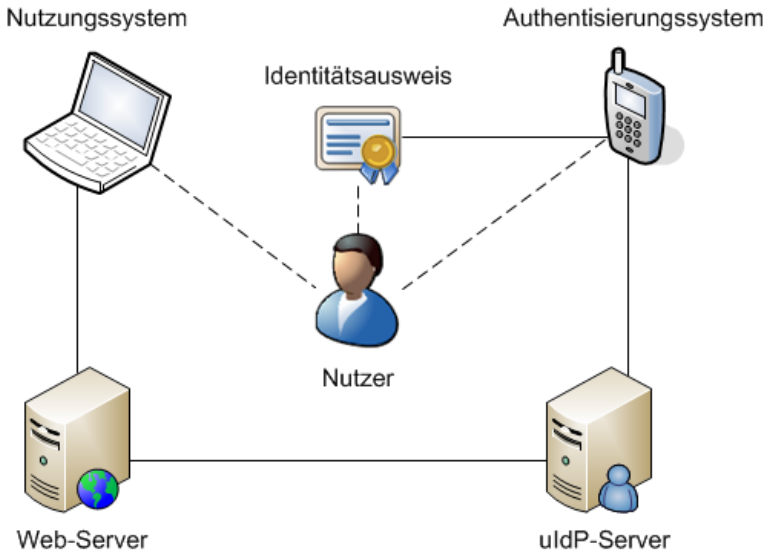

Abb. 2: Verteile Dienstnutzung

mehreren Computer- und Serversystemen. Von dem Nutzungssystem wird auf die von Web-Servern bereitgestellten Dienste zugriffen und die Dienste werden genutzt. Die oftmals notwenige Identifizierung und Authentisierung des Nutzers erfolgt nicht durch die Dienstanbieter direkt, sondern wird von universellen Identitiy-Providern (uIdP) übernommen. Im Fall des Personalausweises fungiert der uIdP-Server als eID-Server gemäß TR-03130 [BSI10b]. Der uIdP-Server kann aber auch verschiedene Authentisierungsmechanismen und -verfahren bereitstellen, um dem geforderten Maß an Authentisierungsstärke und -sicherheit gerecht zu werden (vgl. SkIDentity Projekt [HHRS+11]). Die Authentisierung wird dabei auf einem zweiten, dem Nutzer zugeordneten Computersystem (Authentisierungssystem) durchgeführt. Die Authentisierung kann dabei beispielsweise durch Eingabe eines Benutzernamens und Passworts, in eleganterer Form durch den Nachweis eines Zertifikates, oder bei NFC-fähigen Geräten mit einer Smartcard erfolgen.

Der Ablauf ist dabei wie folgt: Der Nutzer startet auf dem Nutzungssystem beispielsweise einen Web-Browser und öffnet die Webseite des gewünschten Dienstes. Um Zugriff auf das Angebot zu erhalten verlangt der Dienst eine Authentisierung des Nutzers. Diese führt der Nutzer mit Hilfe seines Authentisierungssystems und dem uIdP-Server durch. Nach erfolgreicher Authentisierung bestätigt der uIdP-Server die Anmeldung des Nutzers gegenüber dem Dienst (Web-Server) und der Nutzer erhält Zugriff auf den Dienst.

Ein wesentlicher Punkt der verteilten Dienstnutzung ist die Zuordnung des Authentisierungssystems zum Nutzungssystem bzw. die Verknüpfung der Authentisierung auf dem einen Gerät und der Zugriff auf den Dienst von einem anderen Gerät. Wir stellen dazu in den Kapiteln 3.1 und 3.2 die genannten Push- und Pull-Verfahren vor.

3.1 Push-Verfahren

In den folgenden Abschnitten beschreiben wir das Push-Verfahren. Wir geben zunächst einen Überblick, es folgt eine detaillierte Beschreibung des Ablaufs sowie ein konkretes Beispiel für eine Realisierung mittels nPA und einem NFC-fähigem Mobiltelefon.

3.1.1 Zusammenfassung

Beim Push-Verfahren erfolgt das Auslösen des Authentisierungsvorgangs von außen. Das heißt, der uIdP-Server stößt die Authentisierung auf dem Authentisierungssystem des Benutzers an. Dabei muss der Benutzer beim Zugriff auf einen Dienst einen Identifikator (ID) angeben. Anhand der ID kann der uIdP-Server das Authentisierungssystem ermitteln, d.h. eine Zuordnung zwischen ID und Authentisierungssystem vornehmen. Die ID kann beispielsweise eine E-Mail-Adresse, Mobilfunk-Nummer, IP-Adresse oder ein Benutzername sein.

Zum Auslösen des Authentisierungsvorgangs schickt der uIdP-Server eine Nachricht (SMS, E-Mail, o.ä.) an das Authentisierungssystem. Die eintreffende Nachricht startet auf dem Authentisierungssystem eine eID-Applikation, die dann die Authentisierung des Nutzers vornimmt. Beim Einsatz des Personalausweises muss die Nachricht einen TC TOKEN bzw. eine entsprechende URL zum Erhalt eines TC TOKEN gemäß TR-03112 [BSI12b] zur Aktivierung der eID-Applikation beinhalten.

Das Push-Verfahren hat insbesondere den Vorteil, dass es sehr benutzerfreundlich ist, weil der Authentisierungsvorgang automatisch startet. Das Verfahren erfordert aber ggf. dass der Benutzer bereits beim uIdP-Server registriert ist, damit anhand der ID sein Authentisierungssystem identifiziert werden kann. Die Registrierung beim uIdP-Server hat dabei den Vorteil, dass der Authentisierungsvorgang zusätzlich an ein bestimmtes Gerät gebunden werden kann (beispielsweise über die Rufnummer an das Smartphone, bzw. die SIM Karte des Nutzers). Dies bietet den Sicherheitsgewinn, dass die Authentisierung nur durchgeführt werden kann, wenn zusätzlich Zugriff auf dieses, dem Nutzer zugeordnete Gerät besteht und bspw. die SIM Karte nicht gesperrt ist.

3.1.2 Ablauf des Push-Verfahrens

In Abbildung 3 ist eine Ausführungsform des Push-Verfahrens dargestellt. Im ersten Schritt wird eine Dienst-Anforderung von dem Nutzersystem an den Web-Server gesendet. Dies kann beispielsweise direkt durch den Nutzer erfolgen, etwa durch Eingabe einer URL in einem Web-Browser. Eine andere Möglichkeit ist beispielsweise das Starten eines Programms, welches die Dienste auswählt die über einen Web-Server bezogen werden.

Im nächsten Schritt übermittelt der Nutzer eine ID an den Web-Server. Dies erfolgt beispielsweise durch eine Eingabeaufforderung im Browser oder die ID ist bereits auf dem Nutzersystem gespeichert und wird automatisch übermittelt. Die ID kann beispielsweise eine E-Mail-Adresse, Mobilfunk-Nummer, IP-Adresse oder sonstige URI sein.

Im folgenden Schritt definiert der Web-Server die benötigten Attribute A_1, die für eine Authentisierung oder Identifizierung des Nutzers notwendig sind. Diese Attribute können beispielsweise eine Liste von Identitätsmerkmalen wie Name, Vorname, Anschrift, Alter, Wohnort, Geburtsort, Staatsangehörigkeit, Geschlecht oder sonstige elektronischen Identitäten sein. Sie werden zusammen mit der vorher erhaltenen ID (Nutzerkennung) an den uIdP-Server übermittelt.

Der uIdP-Server bestimmt nun das Authentisierungssystem anhand der ID und sendet im darauffolgenden Schritt eine Nachricht mit weiteren Attributen A_2 an das Authentisierungssystem. Dies kann beispielsweise durch eine SMS, MMS, E-Mail o.ä. erfolgen. Die Attribute A_2 können unter anderem Informationen bezüglich des verwendete uIdP-Servers und Dienstanbieters beinhalten, die für Benutzerinformationen, Authentisierung und Verifizierung notwendig sind. Zusätzlich werden die vom Web-Server definierten Attribute A_1 übermittelt. Durch die Übermittlung wird das Starten der eID-Applikation auf dem Authentisierungssystem ausgelöst. Es ist auch möglich, dass die eID-Applikation bereits gestartet ist und auf einer bestimmten Adresse (z.B. Port, Socket) lauscht und die Nachricht des uIdP-Servers entgegen nimmt.

Anschließend erfolgt eine Authentisierung des Nutzers gegenüber dem Identitätsausweis. Dabei können beispielsweise eine Vielzahl Passwort-basierter Protokolle wie PACE (Password Authenticated Connection Establishment), Encrypted Key Exchange (EKE), SPEKE (Simple Password Exponential Key Exchange), Augmented-Encrypted Key Exchange (A-EKE), Diffie-Hellman Encrypted Key Exchange (DH-EKE), Password Authenticated Key Exchange (PAK) oder Open Key Exchange (OKE) verwendet werden.

Im folgenden Schritt wird eine Verbindung zwischen dem Identitätsausweis und dem uIdP-Server aufgebaut. Das Authentisierungssystem fungiert hierbei als Vermittler und Intermediär.

Dann folgt eine wechselseitige Authentisierung zwischen dem Identitätsausweis und dem uIdP-Server. Die Authentisierung könnte abhängig von der Anwendung jedoch auch einseitig erfolgen. Die Authentisierung kann beispielsweise auf Basis von Zertifikaten und einer Public-Key-Infrastruktur oder mittels eines gemeinsamen Geheimnisses erfolgen.

Nach erfolgreichem Abschluss der Authentisierung erfolgt die Übertragung der erforderlichen Attribute A_3 vom Identitätsausweis zum uIdP-Server, welche als Antwort auf die über die Attribute A_1 definierten Anforderungen zu sehen sind. Diese werden dann vom uIdP-Server an den Web-Server übertragen. Dieser prüft die empfangenen Daten und schaltet ggf. die Dienste zur Nutzung über das Nutzersystem.

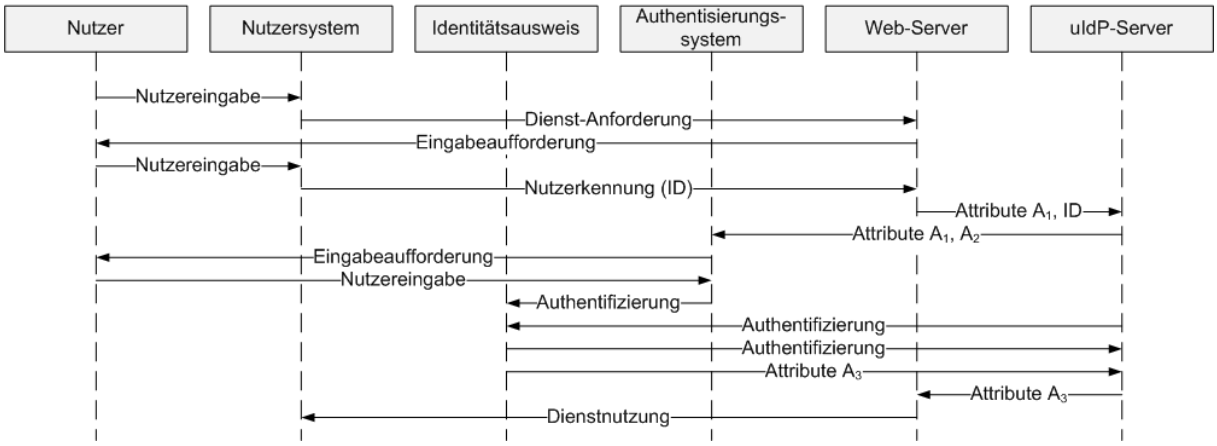

Abb. 3: Ablaufdiagramm Push-Verfahren

3.1.3 Ausführungsbeispiel

In diesem Abschnitt beschreiben wir den Einsatz des Push-Verfahrens im Szenario des neuen Personalausweises und dessen eID-Funktion. Dazu wird ein NFC-fähiges Smartphone als Authentisierungssystem und mobiler Kartenleser, wie in [Hors11] beschrieben, genutzt. Hier erfolgt die Dienstnutzung über einen beliebigen vom Smartphone unabhängigen (nicht vertrauenswürdigen) Computer.

Um eine sichere Authentisierung des Benutzers vorzunehmen, übermittelt der Benutzer dem Dienstanbieter (Web-Server) seine Mobilfunknummer. Hiermit ist der uIdP in der Lage den Mobilfunkanbieter des Benutzers auszuwählen und zu kontaktieren. Der Mobilfunkanbieter sendet dann beispielsweise eine Push SMS/MMS, welche die eID-Applikation auf dem mobilen Endgerät startet und die Authentisierung des Benutzer mittels nPA durchführt. Der Mobilfunkanbieter kann dabei sowohl als uIdP oder nur als reiner Vermittler fungieren.

Das Szenario ist in Abbildung 4 illustriert und der Ablauf wird im Folgenden erläutert:

1. Der Benutzer ruft die Webseite eines Dienstanbieters auf und gibt seine Rufnummer als Identifikator (ID) ein.
2. Der Dienstanbieter sendet entsprechende Informationen zum uIdP. Diese beinhalten unter anderem eine SessionID, die zur Zuordnung benötigt wird und eine Liste mit den erforderlichen Daten, die ausgelesen werden sollen.
3. Der Dienstanbieter kontaktiert den Mobilfunkanbieter und erbittet eine Authentifizierung des Benutzers.
4. Der Mobilfunkanbieter informiert den Kunden bzw. Benutzer z.B. durch eine (Push) SMS über eine gewünschte Authentifizierung und startet ggf. die eID-Applikation auf dem Smartphone. Alternativ kann der Benutzer die Applikation direkt starten und diese erfragt dann bei dem Mobilfunkanbieter die für die Authentisierung benötigten Informationen, welche dieser wiederum in Schritt 2 direkt vom Dienstanbieter mitgeteilt bekommt.
5. Die eID-Applikation baut eine Verbindung zum uIdP-Server (eID-Server) auf, zeigt die Berechtigungen (Zertifikat, Datenschutzerklärung) und erforderlichen Datengruppen an und erfasst die PIN des Ausweisinhabers. Es folgt ein Verbindungsaufbau zwischen nPA und Smartphone und die Durchführung des PACE Protokolls.
6. Nach erfolgreichem Aufbau des PACE Kanals, erfolgt das EAC-Protokoll zwischen nPA und uIdP-Server zur wechselseitigen Authentisierung. Ist dies erfolgreich abgeschlossen besteht ein verschlüsselter Kanal zwischen nPA und uIdP-Server, über den der uIdP-Server die angeforderten Daten ausliest. Die Kommunikation bzw. Datenübertragung zwischen Ausweis und uIdP-Server läuft über die NFC-Schnittstelle und GSM/UMTS Verbindung des Smartphones.
7. Nach erfolgreicher Authentifizierung des Nutzers bestätigt der uIdP dem Dienstanbieter dessen Identität und übergibt ggf. aus dem nPA ausgelesene Daten. Der Anmeldeprozess ist damit abgeschlossen.

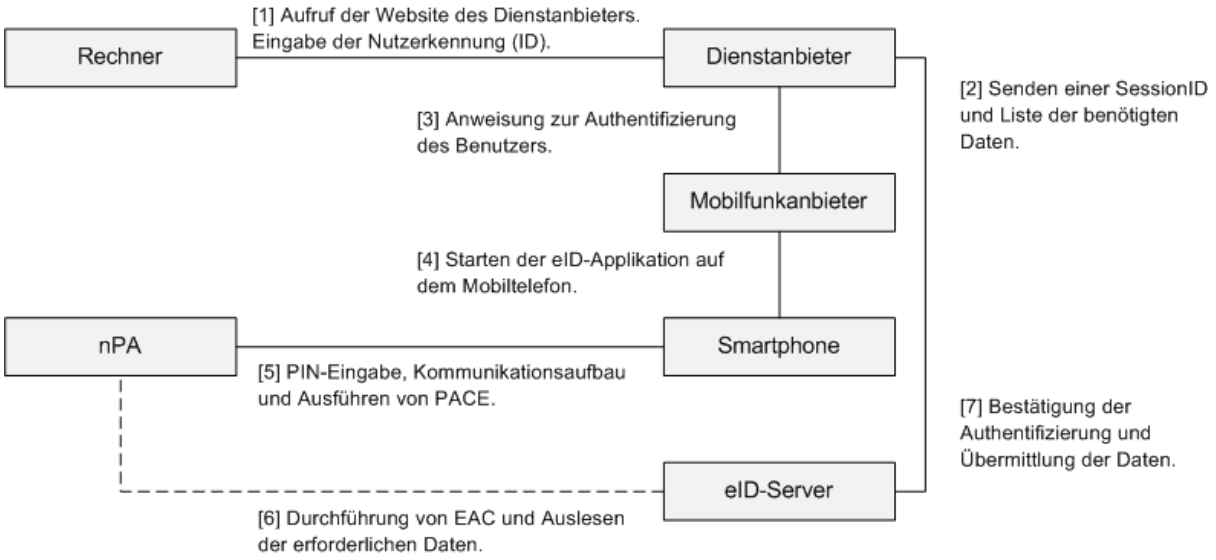

Abb. 4: Push-Verfahren mit nPA und Mobiltelefon

Die Zuordnung zwischen Dienst- und Mobilfunkanbieter bzw. Authentisierungssystems muss durch den Benutzer erfolgen und wird in diesem Setup über die Eingabe der Rufnummer realisiert. Eine andere Möglichkeit wären eine einmalige Vorabanmeldung beim uIdP und die Verwendung eines Pseudonyms als Identifizierungsmerkmal.

Der Vorteil des Einbeziehens des Mobilfunkanbieters ist, dass dieser die Push-Authentisierung als Service anbieten und die entsprechenden Schnittstellen implementieren kann, um als Vermittler zu dienen. Es können dadurch standard eID-Server für die Authentisierung eingesetzt werden, während der Mopbilfunkanbieter die Übermittlung der notwendigen Daten an das entsprechende Mobiltelefon und die Initialisierung des Authentisierungsverfahrens und somit die uIdP-Funktion übernimmt. Darüber hinaus besteht zum Mobilfunkanbieter bereits eine Kundenbindung. Eine Anmeldung bei einem separaten uIdP kann damit entfallen.

3.2 Pull-Verfahren

Ein Nachteil des Push-Verfahrens ist die Eingabe des Identifizierungsmerkmals (ID) des Nutzers auf dem (nicht vertrauenswürdigen) Nutzersystem und dessen Übermittlung an den Dienstanbieter bzw. uIdP-Server. Dadurch ist das Push-Verfahren zur anonymen Dienstnutzung (wie es beispielsweise die Pseudonymfunktion des nPA ermöglicht) nur eingeschränkt geeignet. Dienste können einen Nutzer eindeutig (insbesondere bei Verwendung der Rufnummer als Identifikator) identifizieren. Darüber hinaus könnte ein uIdP, welcher die Authentisierung für viele Dienste durchführt trotz Pseudonymisierung Nutzerprofile erstellen.

In diesem Abschnitt stellen wir das Pull-Verfahren vor, welches dieses Problem löst. Allerdings ist beim Pull Verfahren keine Geräte (bspw. SIM) Bindung möglich und dieser Sicherheitsfaktor entfällt. Nach einer kurzen Zusammenfassung beschreiben wir das Pull-Verfahren detailliert und zeigen die Unterschiede zum Push-Verfahren auf.

3.2.1 Zusammenfassung

Bei dem Pull-Verfahren wird der Authentisierungsvorgang auf dem Authentisierungssystem durch den Benutzer initialisiert. Das heißt, das Authentisierungssystem kontaktiert den uIdP-Server und fordert die Durchführung einer Authentisierung an. Um eine Zuordnung zwischen Authentiserung und Dienstenutzung zu ermöglichen, muss der Dienst auf dem Nutzersystem einen Identifikator (ID) anzeigen, der vom Benutzer auf dem Authentisierungssystem eingegeben werden muss.

Die ID kann dabei z.B. eine Zeichenfolge oder ein Barcode bzw. QR-Code sein, der beispielsweise mit der Kamera des Smartphones (Authentisierungssystem) erfasst wird. Anhand der ID kann die auf dem Authentisierungssystem gestartet eID-Applikation eine Verbindung zum uIdP-Server aufbauen und die Authentisierung des Nutzers durchführen. Im Falle des Personalausweises besteht die ID aus einer URL unter der die eID-Applikation einen TC TOKEN anfordern kann (siehe [BSI12b, Kapitel 3.2]).

Das Pull-Verfahren hat den Vorteil, dass die Initialisierung vom Authentisierungssystem ausgeht und damit der Benutzer beim uIdP-Server nicht bekannt sein muss. Die Authentisierung kann dadurch mit beliebigen uIdP-Servern durchgeführt werden. Dies ermöglicht eine Vorbeugung von Nutzungsprofilen durch Verwendung mehrerer uIdP-Server und eine höhere Ausfallsicherheit.

3.2.2 Ablauf des Pull-Verfahrens

In Abbildung 5 ist das Pull-Verfahren dargestellt. Zunächst wird wieder der Dienst durch den Nutzer angefordert. Anstelle der Eingabe und Übermittlung eines Identifikators durch den Nutzer, wählt der Web-Server eine ID (der insbesondere zufällig gewählt sein kann, beispielsweise eine Session ID) und sendet diesen und ggf. weitere Information die für die Authentisierung benötigt werden an das Nutzersystem. Die ID wird zusammen mit den oben beschriebenen Attributen A_1 an den uIdP-Server übergeben.

Im nächsten Schritt initialisiert der Nutzer den Authentsierungsvorgang durch Starten der eID-Applikation und Eingabe der ID in das Authentisierungssystem. Die ID könnte beispielsweise aus der Adresse (URL) des uIdP-Servers und einer Zahlenkombination bestehen die der Nutzer in einem Browser des Authentisierungssystems eingeben kann. Denkbar ist auch ein Erfassen einen Bildes, Barecodes oder QR-Code (Quick-Response-Code) durch die Kamera des Authentisierungssystems im Falle eines Smartphone oder auch das Aufnehmen eines Audiosignals.

Das Authentisierungssystem kann nun mittels des Identifikators die Anforderung der Attribute A_1 und A_2 (Verifikationsinformationen, angeforderte Authentisierungsdaten, siehe auch Abschnitt 3.1.2) auslösen. Hierin liegt der Hauptunterschied zum Push-Verfahren. Mittels des Identifikators kann der uIdP-Server die Anforderung dem Dienst zuordnen und die entsprechenden Attribute A_2 und A_2 übermitteln. Danach erfolgt die Authentisierung des Nutzers und die Dienstfreischaltung analog zum Push-Verfahren.

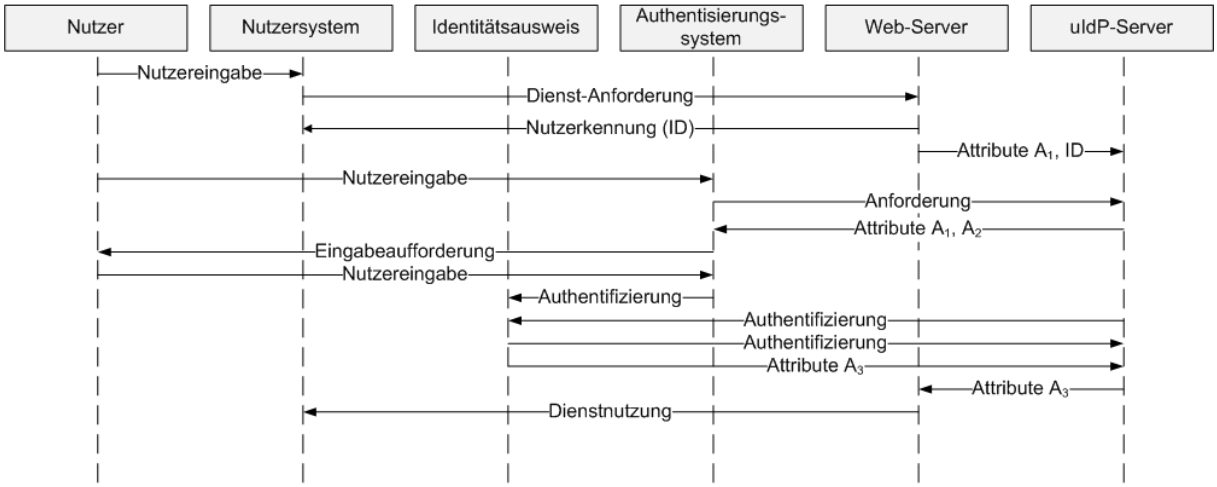

Abb. 5: Ablaufdiagramm Pull-Verfahren

4 Diskussion

Die verteilte Dienstnutzung bietet gegenüber herkömmlichen Authentifizierungsverfahren vielfältige Vorteile. Diese betreffen vor allem die Flexibilität und die Sicherheit. Betrachtet man beispielsweise den Einsatz der eID-Funktion des Personalausweises oder anderer chipkartenbasierter Verfahren mit kontaktlosen Karten, so wird ein spezieller Kartenleser durch den Einsatz eines NFC-fähigen Authentisierungssystems überflüssig. Dabei ersetzt das mobile Gerät jedoch nicht einfach den Kartenleser. Durch die Funktionsweise der verteilten Dienstnutzung wird die Verbindung zum Nutzungssystem obsolet. Dadurch ist eine universelle Einsetzbarkeit gegeben, da proprietäre Schnittstellen und Steckverbindungen oder deren Fehlen, wie das beispielsweise mit USB-Steckplätzen bei einigen Tablet-Computern der Fall ist, irrelevant sind.

Daneben werden sensible Informationen wie Passwörter immer auf einem dem Nutzer gehörenden System eingegeben, was das allgemeine Nutzervertrauen und die Sicherheit steigert. Die Sicherheit des Systems liegt hier unter der Kontrolle des Nutzers, und er muss sich nicht auf die Sicherheitsvorkehrungen anderer, wie beispielsweise bei fremden Arbeitsplatzrechnern, in Internetcafés oder an Hotelrechnern, verlassen.

Der Sicherheitsanker der verteilten Dienstnutzung ist das Authentisierungssystem. Eine Kompromittierung dessen birgt dabei zwar ähnliche Angriffsmöglichkeiten wie eine Kompromittierung bei der normalen Nutzung, jedoch ist beim Push-Verfahren ein lesender Zugriff, wie er

durch Keylogger realisiert wird, nicht ausreichend insofern das Authentisierungssystem beim uIdP-Server registriert ist. Da die Authentisierung in diesem Fall immer über dieses Gerät angefordert wird, muss ein Angreifer zusätzlich die volle Kontrolle über das Gerät haben und beispielsweise Signaltöne unterdrücken und das entsprechende Authentisierungsverfahren einleiten können.

Trotz der wachsenden Anzahl an Angriffen auf Mobiltelefone sind diese auch weiterhin als sicherer zu betrachten als herkömmliche Computer. Betrachtet man beispielsweise Firmenhandys, so ist die Installation von Fremdsoftware oftmals nicht oder nur sehr eingeschränkt gestattet. Daneben ist das Angebot an Software oftmals durch den herstellerspezifischen App-Store beschränkt und unterliegt daher einer gewissen Kontrolle. Darüber hinaus kann durch den Einsatz von *SiMKo* [BSI12c] oder *Mobile Trusted Module* (MTM) [TCG12] Modulen eine Kompromittierung verhindert werden. Zwar ist der Einsatz von MTM-Modulen in mobilen Geräten noch sehr beschränkt, jedoch ist im Vergleich zu normalen Computersystemen hier eine ungleich höhere Kundenakzeptanz und somit leichtere Durchsetzung am Markt zu erwarten. Bei mobilen Geräten ist eine andere Kundenbindung und Besitzverständnis festzustellen. Teilweise entspricht der Erwerb eines mobilen Gerätes bei einigen Mobilfunkanbietern mehr einem Leasing- als einen Kaufvertrag, da das Gerät über die Vertragslaufzeit zu einem festen Entgelt bereitgestellt wird und nach Vertragsende wieder zurückgegeben werden muss. Auch werden Geräte akzeptiert deren Bauart einen Austausch des Akkus nicht gestattet und bei denen sich der Speicher des Gerätes nicht erweitern lässt. Eine Kombination aus MTM geschütztem mobilen Gerät und unserem Verfahren der verteilten Dienstnutzung kann dadurch einen starken Sicherheitsgewinn schaffen, der weit über das Gerät hinaus geht in dem das MTM verbaut ist.

Im Vergleich zu dem etablierten Mobile TAN (mTAN) Verfahren bietet das hier beschriebene Verfahren der verteilten Dienstnutzung universelle Authentisierungsmöglichkeiten wie beispielsweise mit Chipkarten oder Zertifikaten. Des Weiteren schützt das mTAN-Verfahren nur die Bestätigung eines Überweisungsauftrages, die Anmeldung beim Online-Banking Portal erfolgt weiterhin über eine PIN und ist somit Angriffen durch Schadsoftware ausgesetzt. Das Verfahren der verteilten Dienstnutzung sichert bereits die Anmeldung ab, die Bestätigung eines Überweisungsauftrages kann dann über eine mTAN erfolgen.

Zusammenfassend ist festzustellen, dass das Verfahren der verteilten Dienstnutzung durch die Trennung zwischen Dienstnutzung und Authentisierung einen hohen Schutz vor Angriffen durch Schadsoftware auf dem Nutzungssystem bietet. Durch den Einsatz eines mobilen Endgerätes als Authentisierungssystem stehen verschiedene Authentisierungsverfahren universell und allgegenwärtig zur Verfügung.

Literatur

[BHWH11] J. Braun, M. Horsch, A. Wiesmaier, D. Hühnlein: Mobile Authentisierung und Signatur. *In: D-A-CH Security 2011* (2011).

[BrHW12] J. Braun, M. Horsch, A. Wiesmaier: iPIN and mTAN for Secure eID Applications. *In: M. Ryan, B. Smyth, G. Wang (Hrsg.), Information Security Practice and Experience*, Springer Berlin / Heidelberg, *Lecture Notes in Computer Science*, Bd. 7232 (2012), 259–276, .

[BSI] BSI: AusweisApp. `https://www.ausweisapp.bund.de`.

[BSI10a] BSI: Certificate Policy für die eSign-Anwendung des ePA - Elektronische Signaturen mit dem elektronischen Personalausweis. Version 1.01 (2010).

[BSI10b] BSI: Technische Richtlinie eID-Server. Technical Guideline BSI-TR-03130,

Version 1.4.1 (2010), https://www.bsi.bund.de/ContentBSI/Publikationen/TechnischeRichtlinien/tr03130/tr-03130.html.

[BSI11a] BSI: Architektur elektronischer Personalausweis und elektronischer Aufenthaltstitel. Technical Guideline BSI-TR-03127, Version 1.14 (2011), https://www.bsi.bund.de/ContentBSI/Publikationen/TechnischeRichtlinien/tr03127/tr-03127.html.

[BSI11b] BSI: Certificate Policy für die eID-Anwendung des ePA - Elektronischer Identitätsnachweis mit dem elektronischen Personalausweis. Version 1.27 (2011).

[BSI12a] BSI: Advanced Security Mechanisms for Machine Readable Travel Documents. Technical Guideline BSI-TR-03110, Version 2.10, Part 1-3 (2012), https://www.bsi.bund.de/ContentBSI/Publikationen/TechnischeRichtlinien/tr03110/index_htm.html.

[BSI12b] BSI: eCard-API-Framework – Protocols. Technical Guideline BSI-TR-03112-7, Version 1.1.2 (2012), https://www.bsi.bund.de/ContentBSI/Publikationen/TechnischeRichtlinien/tr03112/index_htm.html.

[BSI12c] BSI: SiMKo 2 - eine Lösung für die sichere mobile Kommunikation (2012), https://www.bsi.bund.de/DE/Themen/weitereThemen/MobileSecurity/SiMKo2/simko_node.html.

[BWHB+10] J. Buchmann, A. Wiesmaier, D. Hühnlein, J. Braun, M. Horsch, F. Kiefer, F. Strenzke: Towards a mobile eCard Client. *In: Tagungsband zum 13. KryptoTag* (2010), 4.

[HHRS+11] D. Hühnlein, G. Hornung, H. Roßnagel, J. Schmölz, T. Wich, J. Zibuschka: SkIDentity - Vertrauenswürdige Identitäten für die Cloud. *In: D-A-CH Security 2011* (2011).

[Hors11] M. Horsch: Mobile Authentisierung mit dem neuen Personalausweis (MONA). Master Thesis, TU Darmstadt (2011), http://www-old.cdc.informatik.tu-darmstadt.de/reports/reports/Moritz_Horsch_MONA.master.pdf.

[HPSW+12] D. Hühnlein, D. Petrautzki, J. Schmölz, T. Wich, M. Horsch, T. Wieland, J. Eichholz, A. Wiesmaier, J. Braun, F. Feldmann, S. Potzernheim, J. Schwenk, C. Kahlo, A. Kühne, H. Veit: On the design and implementation of the Open eCard App. *In: Sicherheit 2012* (2012).

[ISO11] ISO/IEC: Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 1-4. International Standard, ISO/IEC 14443 (2008 - 2011).

[TCG12] TCG: TCG Mobile Trusted Module Specification. Version 1.0 (2012), http://www.trustedcomputinggroup.org/resources/mobile_phone_work_group_mobile_trusted_module_specification.

[WHBK+11] A. Wiesmaier, M. Horsch, J. Braun, F. Kiefer, D. Hühnlein, F. Strenzke, J. Buchmann: An efficient mobile PACE implementation. *In: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, ASIACCS '11, ACM, New York, NY, USA (2011), 176–185, .