Wolf Müller, Jens-Peter Redlich, Mathias Jeschke

Auth²(nPA)

Starke Authentifizierung mit nPA für jedermann

Für viele heutige IT-Dienste wäre eine stärkere Authentifizierung als die mit Nutzername und Passwort wünschenswert. Insbesondere für sicherheitskritische Prozesse, wie das Zurücksetzen von Passwörtern, sind bestehende Lösungen oft unbefriedigend. Der neue Personalausweis (nPA) stellt mit seiner eID-Funktion die Möglichkeit für eine starke Authentisierung bereit. Jedoch stehen dem erreichbaren Sicherheitsgewinn nicht unerhebliche Kosten gegenüber, die pro Dienstanbieter aufgebracht werden müssen, um die eID-Funktion zu nutzen. Wir zeigen mit dem Konzept Auth²(nPA), wie eine Zweifaktorauthentisierung mit dem nPA von mehreren Einrichtungen gemeinsam genutzt werden kann. Um für diesen Dienst ein Berechtigungszertifikat zu erhalten, realisiert das Auth²(nPA)-Konzept ein vergleichbar hohes Datenschutzniveau wie die generische eID-Lösung mit getrennten Dienstanbietern.

Dr. Wolf Müller

Wissenschaftlicher Mitarbeiter am Institut für Informatik der Humboldt-Universität zu Berlin
E-Mail: wolfm@informatik.hu-berlin.de

Prof. Jens-Peter Redlich

Professor für Systemarchitektur am Institut für Informatik der Humboldt-Universität zu Berlin
E-Mail: jpr@informatik.hu-berlin.de

Mathias Jeschke

Diplomstudent am Institut für Informatik der Humboldt-Universität zu Berlin
E-Mail: jeschke@informatik.hu-berlin.de

1 Nachweis digitaler Identitäten – ein Verfahrensvergleich

Unser tägliches Leben ist zunehmend geprägt von der Nutzung von IT-Systemen und Diensten. Um Zugang zu diesen zu erlangen, authentisiert sich ein Nutzer gegenüber dem Dienst[1], den er verwenden möchte. In der Regel verwendet der Nutzer dazu einen Identifikator (wie beispielsweise eine Benutzerkennung), der eine Behauptung darstellt, um welche Person oder welches Subjekt es sich handelt. Im zweiten Schritt wird dann im Zuge der Authentisierung ein Nachweis dieser Behauptung gegenüber dem IT-System durch den Nutzer angetreten. Dieser Nachweis kann auf drei unterschiedliche Arten erbracht werden: durch *Wissen*, durch *Besitz* oder durch *Sein* (also mittels *biometrischer* Verfahren). Die unterschiedlichen Verfahren haben verschiedene Stärken und Schwächen.

Wissensbasierte Verfahren gestatten eine enge Bindung an eine Person und sind ohne hohe Kosten umsetzbar. Allerdings können sich Menschen oft nur wenige und in ihrer Komplexität unzureichende Passworte zuverlässig merken. Passworte unzureichender Länge und Entropie sind automatisiert angreifbar, wenn keine systemseitigen Vorkehrungen[2] getroffen werden. Eine willentliche oder auch ungewollte Weitergabe des Wissens kann nicht sicher ausgeschlossen werden. Ein Geheimnis kann während der Eingabe an einem IT-System oder durch „Social Engineering" ausgespäht werden.

Biometrische Authentifizierungsverfahren haben in jüngster Vergangenheit eine rapide Entwicklung genommen. Trotz zusätzlicher Kosten für geeignete Infrastruktur (Sensoren zur Merkmalerfassung, Einrichtungen zur sicheren Speicherung der Referenzdatensätze) und gewissen verfahrensimmanenten Fehlerraten gewinnen diese Verfahren zunehmend an Verbreitung. Die besondere Stärke dieser Verfahren liegt in der extrem engen Bindung des Authentifikators an die jeweilige Person. Dies stellt aber zugleich in bestimmten Anwendungsszenarios eine Schwäche dar: Die Erfassung biometrischer Merkmale eröffnet prinzipiell

1 Sinnvoll ist es auch, dass das IT-System sich seinerseits vorher gegenüber dem Nutzer authentisiert.

2 Eine Einschränkung des Zugangs oder zeitliche Verzögerung nach mehreren Fehlversuchen sind denkbar.

die Möglichkeit zur Profilbildung und Schutzziele wie Anonymität oder Pseudonymität lassen sich nur sehr schwer realisieren.

Besitzbasierte Verfahren verwenden ein Hardwaretoken (USB-Token, Smartcard, RSA-SecureID), um sich gegenüber einem IT-System zu authentisieren. Ähnlich wie bei Haustürschlüsseln, ist je nach Aufwand mit besitzbasierten Verfahren ein sehr hohes Sicherheitsniveau erreichbar. Insbesondere stellen höherwertige Lösungen sicher, dass solch ein Token nicht kopiert werden kann. Somit ist zur Authentifizierung immer der Besitz oder exakter der Zugriff auf solch ein Token notwendig. Wie aber bei einem Hausschlüssel auch ist nach Konstruktion keine Bindung an eine Person gegeben – wer den Token oder den Schlüssel hat, kann das IT-System nutzen oder die Tür öffnen.

Um eine starke Authentifizierung zu erreichen, werden mehrere dieser Verfahren in geeigneter Weise kombiniert, sodass die Stärken summiert und die Schwächen möglichst eliminiert werden. Man spricht dann von einer Zwei- bzw. einer Mehrfaktorauthentifizierung. Aus unserem täglichen Leben kennen wir die übliche Zweifaktorauthentifizierung am Geldautomaten mit der EC-Karte (Besitz) und der zugehörigen PIN (Wissen). Durch die Verwendung einer EC-Karte mit Chip (im Gegensatz zum Magnetstreifen) wird erreicht, dass die Karte nicht kopiert werden kann. Die PIN realisiert die Bindung an den legitimen Besitzer (da hoffentlich nur *er* die PIN kennt). Obwohl die PIN nur aus vier Stellen besteht, kann diese nicht einfach ausprobiert werden, da drei aufeinanderfolgende Fehlversuche zu einer Sperrung der Karte führen würden. Dieses System realisiert eine sehr starke Authentifizierungsform. Allerdings verursacht es auch nicht zu vernachlässigende Kosten durch Ausgabe der Karten und Installation der zugehörigen Infrastruktur, die jedoch aufgrund der zu schützenden Werte gerechtfertigt sind.

2 Der neue Personalausweis

2.1 Funktion

Am 1. November 2010 wurde in Deutschland mit dem neuen Personalausweis (nPA) ein modernes elektronisches Identitätsdokument eingeführt. Es gestattet neben der hoheitlichen Nutzung über die ePass-Funktion (beispielsweise bei einer Grenz- oder Polizeikontrolle) mit der eID-Funktion auch ausdrücklich die optionale nicht-hoheitliche Verwendung zum elektronischen Identitätsnachweis. Ebenfalls optional ist das Nachladen eines Zertifikats für die sichere Erstellung einer qualifizierten elektronischen Signatur und die Nutzung der eSign-Funktion.

Mit der eID-Funktion erhält jeder Bundesbürger, der dies wünscht, ohne Aufpreis Zugang zu einem Token (dem nPA) mit sehr starker Zweifaktorauthentisierung (Besitz des nPA und Kenntnis der zugehörigen eID-PIN). Mit dem nPA kann er wählbare Teile seiner Identität über das Internet gegenüber berechtigten Dienstanbietern beweisen.

2.2 Datenschutz

Die gesetzlichen Vorgaben für die Entwicklung des nPA und der zugehörigen Infrastruktur sind bezüglich seiner eID-Funktion auf ein sehr hohes Niveau an Datensicherheit, Datenschutz, Transparenz und Kontrolle durch den Nutzer und die Möglichkeit zur pseudonymen und anonymen Verwendung ausgerichtet. Diese Schutzziele finden in dem Protokoll zur gegenseitigen Zugriffskontrolle zwischen Ausweis und dem Dienstanbieter „Extended Access Control"–Protokoll (EAC Version 2), welches in der Technischen Richtlinie TR-03110 beschrieben wird [Bun10a], ihren Ausdruck. So sind insbesondere die Zugriffsmöglichkeiten auf Daten oder Funktionen des nPA durch ein Terminal feingranular durch Berechtigungszertifikate regelbar.

Berechtigunszertifikate legen fest, auf welche Anwendung (ePass, eID, eSign) und auf welche Datengruppen und Funktionen innerhalb dieser Anwendung ein Terminal höchstens zugreifen darf. Die Ausstellung dieser Zertifikate durch die Vergabestelle für Berechtigungszertifikate (VfB) erfolgt im Interesse der Bürger recht restriktiv. Ein Dienst muss die Erforderlichkeit der aus dem nPA gewünschten Daten für seinen Geschäftszweck darlegen und verschiedene Voraussetzungen bezüglich Datenschutz und Datensicherheit nachweisen. Ein Berechtigungszertifikat wird insbesondere nicht gewährt, wenn „der Zweck der Datenerhebung ausschließlich in der Auslesung oder Bereitstellung personenbezogener Daten aus dem Personalausweis für den Ausweisinhaber oder Dritte besteht".[3]

Der Ablauf des Zugriffs auf den nPA, hier für den Fall der eID-Funktion beschrieben, erfolgt in mehreren Schritten. Dem Benutzer wird zuerst angezeigt, welcher Dienstanbieter welche Daten oder Funktionen aus der eID-Anwendung verwenden möchte. Der Nutzer kann gegebenenfalls hier weitere Einschränkungen vornehmen. An den Chip des nPA wird die resultierende Zusage (Anwendung: eID, die folgenden Daten, durch genau diesen Dienstanbieter) exakt diesen Protokolllauf durchzuführen (als effektiver CHAT in [Bun10a] codiert) übergeben, und durch die Eingabe der eID-PIN durch den Benutzer autorisiert. Der Chip des nPA kümmert sich dann um alles Weitere, also das Einhalten der gegebenen Zusage. Es wird zuerst ein kryptografisch sicherer Kanal, authentisiert durch die eID-PIN, etabliert, der die drahtlose Kommunikation zwischen Lesegerät und nPA absichert (PACE in [Bun10a]). Nun muss der Dienstanbieter (durch Vorlage des Berechtigungszertifikats) den Nachweis antreten, dass er mindestens über die (im effektiven CHAT) versprochenen Berechtigungen verfügt. Und er muss (durch Beantwortung einer Challenge mit dem zum Berechtigungszertifikat gehörigen privaten Schlüssel) nachweisen, dass er selbst der zugesagte legitime Zertifikatsinhaber ist. Die vorgelegten Zertifikate werden von dem Chip des nPA auf das Penibelste kryptografisch geprüft. Wenn hier zweifelsfrei alles korrekt ist, ist die Terminalauthentisierung (TA) erfolgreich.

Wenn ein Terminal oder ein Angreifer nicht über ein gültiges Berechtigungszertifikat (und den zugehörigen privaten Schlüssel) verfügt, ist es ihm nicht möglich irgendwelche Daten aus dem nPA zu erhalten, die einem konkreten Ausweis zuzuordnen sind. Der Benutzer ist nicht identifizierbar. Erst im Anschluss an die Terminalauthentisierung macht der nPA-Chip relevante Angaben über sich selbst.

Im Zuge der sich anschließenden Chipauthentisierung (CA) weist der Chip des nPA nach, dass der Dienst mit einem validen neuen Personalausweis spricht. Im Anschluss wird zum Ende der „Extended Access Control" ein neuer sicherer Kanal zwischen dem Chip des nPA und

3 Verordnung über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisverordnung vom 1. November 2010), PAuswV, Kapitel 8, §29.

dem Dienstanbieter (genauer dem eID-Server oder eID-Service) etabliert. Nach erfolgreich abgeschlossener Chipauthentisierung kann der Dienstanbieter sicher sein, dass die über diesen Kanal vom nPA-Chip gesendeten Daten (oder Antworten auf Funktionsaufrufe) authentisch sind.

Die deutsche eID-Lösung verzichtet hier bewusst auf das Signieren der Datengruppen, um möglichst exakt den bisherigen Ablauf „Jemand zeigt seinen Ausweis vor" in der digitalen Welt nachzubilden. Insbesondere kann sich der digital Auslesende nur zum Zeitpunkt des „Vorzeigens" von der Richtigkeit der Angaben überzeugen, dieses Wissen jedoch nicht später an einen Dritten beweiskräftig weitergeben. Der Auslesende kann nicht (und soll auch nicht) einmal gegenüber Dritten beweisen, dass überhaupt ein Auslesevorgang stattgefunden hat. Ein Berechtigungszertifikat kann in diesem Bild dann als Schablone verstanden werden, die über den Personalausweis gelegt wird, die nur für die bewilligten Datenfelder überhaupt durchsichtig ist. Der Nutzer konnte ja weitere Felder abwählen, was in unserem Bild dem Abdecken durch die Schablone noch sichtbarer Bereiche auf dem Ausweis entspräche, die er nicht preisgeben möchte.

Der nPA-Chip stellt beim Auslesevorgang sicher, dass durch diesen sicheren Kanal ausschließlich die im effektiven CHAT angekündigten, durch den Nutzer bestätigten und durch das Berechtigungszertifikat auch zulässigen Daten und Funktionen genutzt werden können.

Neben weitgehend statischen Datengruppen[4] ähnlich wie bereits auf dem Ausweis aufgedruckt, stellt die eID-Anwendung noch vier Funktionen bereit: die Altersverifikation, die Wohnortabfrage *Community-ID Verification*, das sektorspezifische Sperrmerkmal und die sektorspezifische Kennung.

2.3 Anonyme oder pseudonyme eID-Anwendung

Die vier genannten Funktionen erweitern das Potenzial der eID-Funktion auf anonyme und pseudonyme Anwendungsfälle. So ist es möglich, die Fragen: „Ist der Besitzer älter als x Jahre?" oder „Wohnt er in der Gemeinde y?" einem Dienst zweifelsfrei zu beantworten, ohne Hinweise auf die Identität des Nutzers preiszugeben. Hier ist Anonymität das angestrebte Ziel, ein Nutzer soll nicht (wieder-)erkannt werden.

In anderen Szenarien (z. B. Onlineabstimmungen oder pseudonymes Login) ist es wünschenswert, den Nutzer nicht zu identifizieren, ihn jedoch bei erneuter Dienstnutzung wiederzuerkennen. Der Dienst soll nicht herausfinden können, wer der Nutzer ist, aber der Nutzer soll mit dem nPA in der Lage sein zu beweisen, dass er ohne Zweifel der gleiche ist wie beim letzten Mal. Verbindet sich der gleiche nPA mit dem gleichen Dienst, so ist das die berechnete Pseudonym identisch. Um ein Zusammenführen von Nutzungsprofilen (engl. Tracking) in dieser Nutzungsart zwischen verschiedenen Dienstanbietern zu verhindern, wurden Terminalsektoren eingeführt. Diese Terminalsektoren stellen sicher, dass das für den gleichen nPA berechnete Pseudonym, das dienste- und kartenspezifische Kennzeichen, bei Nutzung unterschiedlicher Dienste (mit verschiedenen Terminalsektoren) nicht korrelierte Werte annimmt. Die Reichweite des Psydonyms wird auf den jeweiligen Dienst begrenzt, daher der Name *Restricted Identification (rID)*. Die rID ist für ein Paar (nPA, Dienst) konstant, ändert sich einer der Teilnehmer, so ändert sich auch die rID. Technisch erfolgt die Ermittlung des Sperrmerkmals von Ausweisen ähnlich der rID-Funktion, allerdings mit unabhängigem Schlüsselmaterial. Wird ein Ausweis gesperrt, werden für jeden Sektor individuelle Sperrlisten erzeugt, die dann mit dem durch den nPA zwingend übermittelten Sperrmerkmal abgeglichen werden. Das Sperrmerkmal, das verplichtend bei der Verwendung der eID-Funktion ausgewertet werden muss, ist somit polymorph und lässt kein Profiling über Sektorgrenzen hinweg zu.[5]

3 Auth²(nPA)

3.1 Motivation

Will man einen Dienst für eine starke Authentisierung mit Besitz und Wissen in Deutschland realisieren, so bietet sich mit der eID-Funktion des neuen Personalausweises eine sehr interessante Möglichkeit. Der nPA ist kryptografisch stark, kompatible Lesegeräte sind oft ohnehin vorhanden und werden bereits für andere Anwendungen genutzt. Die nötige Software für den Endanwender (z. B. AusweisApp) wird gepflegt und weiterentwickelt. Für den nPA gibt bereits ein etabliertes System zum Sperrmanagement für verlorene oder gestohlene Ausweise.

Pro Nutzer sind folglich nur geringe Investitionskosten nötig. In der Regel wird zukünftig der deutsche Bürger über den nPA als Hardwaretoken ohnedies verfügen, sodass er nur, wenn noch nicht geschehen, die eID-Funktion beim Bürgeramt aktivieren lassen muss.

Damit werden nun ausdrücklich Szenarios wirtschaftlich umsetzbar, in denen die Authentifizierung eines Nutzers weniger häufig, aber insgesamt für eine sehr große Nutzeranzahl (was viele Token notwendig macht) erforderlich ist.

So treten Aufgaben wie das Neusetzen vergessener Passworte, beantragen zusätzlicher Rechte oder Ressourcen an IT-Systemen (z. B. WLAN-Zertifikate) in der Regel pro Nutzer nicht wöchentlich auf. Jedoch ist für diese Aufgaben eine sichere Authentifizierung des Nutzers unbedingt wünschenswert.

Je größer die Summe (durch die große Nutzerzahl) aus individuellen Nutzungen wird, um so mehr rentieren sich die jährlichen Kosten für die zentral benötigte Infrastruktur (im Wesentlichen der Betrieb des eID-Service und das erforderliche Berechtigungszertifikat).

Das in den folgenden Abschnitten Abschnitt erläuterete Auth²(nPA)-Konzept ermöglicht einen geteilten Authentifizierungsdienst für Nutzer an vielen Einrichtungen gleichzeitig, auf Grundlage einer einzigen eID-Service-Instanz. Die strikte Trennung der Informationen zwischen den Einrichtungen, dem Nutzer und dem einrichtungsübergreifendem Dienst, stellt die Basis für einen erfolgreichen Antrag auf ein Berechtigungszertifikat für den Auth²(nPA)-Dienst dar.

3.2 Komponenten

An dem Authentisierungsdienst sind drei Parteien und eine Anonymisierungskomponente (siehe Abbildung 1) beteiligt:

- Mit einer *Einrichtung (**E**)* bezeichnen wir eine Organisation oder Institution, die für ihre Nutzer oder Mitglieder

4 DG1–DG9, DG17, DG18 siehe TR-03127 S.11 [Bun10b].

5 Das vom nPA erhaltene Sperrmerkmal darf nicht gespeichert werden, sondern ist nur für den Abgleich mit den Sperrlisten gedacht. Wird gegen diese Policy (was natürlich verboten ist) verstoßen, so kann (rein technisch) die anonyme Nutzung (z. B. Altersverifikation) in eine pseudonyme überführt werden.

gewisse IT-Dienste erbringt. Jede Einrichtung verwaltet ihre Nutzer und deren Zugang zu Ressourcen autark.

- Ein *Nutzer (**N**)* kann Accounts an einer oder auch mehreren Einrichtungen haben oder eröffnen. Der Nutzer verfügt über einen nPA mit freigeschalteter eID-Funktion und die nötige Hard- und Software (Computer, geeigneter Leser, Browser, AusweisApp).
- Mit dem *Dienstanbieter (**D**)* sei hier ein IT-Dienst gemeint, der den Auth²(nPA)-Dienst für mehrere Einrichtungen erbringt. Er verfügt für diesen Zweck nach Beantragung beim Bundesverwaltungsamt über ein Berechtigungszertifikat für die karten-und dienstespezifische Kennung und hat Zugang zum zugehörigen privaten Schlüssel. Der Dienstanbieter sei in der Lage die eID-Funktionalität bezüglich rID des neuen Personalausweises zu nutzen.[6] Insbesondere ist er also auch ein Dienstanbieter im Kontext des nPA.
- Ein anonymisierender *Proxy[7] (**P**)* wird für Datenschutz auf Verbindungsebene zwischen Einrichtung und Dienst benötigt.

3.3 Anforderungen und Lösungsidee

Die Kernaufgabe von Auth²(nPA) ist es, eine starke Zweifaktorauthentisierung mit der rID des nPA für mehrere Einrichtungen unter Benutzung nur eines Dienstanbieters zu ermöglichen. Da in unserem Konzept gerade nur ein Berechtigungszertifikat nötig ist, ist keine Trennung in Terminalsektoren gegeben. Jedoch ist das Konzept derart konstruiert, dass das Tracking von Nutzern verschiedener Einrichtungen dennoch wirksam verhindert wird. Dies wird durch eine Beschränkung des Wissens der drei beteiligten Parteien (Nutzer, Einrichtung und Dienstanbieter) auf das absolut notwendige Minimum für eine sichere Authentisierung des Nutzers erreicht. Der Dienstanbieter und die Einrichtung besitzen jeweils nur Teilgeheimnisse. Der Nutzer kennt seine Einrichtung, seinen Loginnamen dort und die PIN des nPA. Mit diesem Wissen kann er mithilfe der rID, die mit der eID-Funktion seines nPA ermittelt wird, die beiden richtigen Geheimnisteile referenzieren, die zur Authentisierung nötig sind.

Um eine erfolgreiche Authentisierung eines Nutzers zu bewerkstelligen, müssen also alle drei Parteien aktiv zusammenarbeiten. Der Nutzer startet den Authentisierungsvorgang an einer Einrichtung, indem er eine Behauptung über seine Identität (Loginname) angibt, die bewiesen werden soll. Die Einrichtung betrachtet den Nachweis als erbracht, wenn der Nutzer mithilfe der Einrichtung, des nPA und dem Dienstanbieter es schafft, das in der Einrichtung für seinen Account hinterlegte Referenzergebnis erneut authentisch und frisch berechnen zu lassen.

Für die Berechnung, die im Dienstanbieter ausgeführt wird, sind zwei Teilgeheimnisse $G_{1,2}$ nötig. Das Teilgeheimnis G_1(E,N) wird für jeden Nutzer bei der Initialisierung individuell und zufällig in der Einrichtung erstellt und für das Nutzerkonto dort gespeichert. Das zweite Teilgeheimnis G_2(rID) wird beim Dienstanbieter einmal bei Initialisierung für den Nutzer (authentisiert durch die rID des nPA) zufällig gewählt und wird für diese rID dort abgespeichert. Das beim Dienstanbieter unter einer rID gespeicherte Geheimnis G_2(rID), lässt keinen Rückschluss zu, ob oder wie viele Konten ein Nutzer N an irgendeiner Einrichtung E hat.

Startet der Nutzer N die Authentisierung, so übergibt die Einrichtung ihren Geheimnisteil G_1(N, E) verschlüsselt für den Dienstanbieter dem Nutzer, der diesen mit der Authentisierungsanfrage an den Dienstanbieter weiterreicht. Der Dienstanbieter führt mit dem Nutzer dann die Authentisierung mit dem nPA und der rID durch, und gelangt im Erfolgsfall an das zweite Teilgeheimnis G_2(rID). Damit kann das Referenzergebnis $R = R(G_1,G_2)$ berechnet werden, welches für die Einrichtung verschlüsselt frisch bereitgestellt wird. Zur Berechnung von R sollte eine geeignete kryptografische Funktion und[8] verwendet werden, um zu verhindern, dass aus dem bereitgestellten Referenzergebnis ein Rückschluss auf eines der beiden Teilgeheimnisse gezogen werden kann. Stimmt dieses Ergebnis mit dem bei der Einrichtung für den Nutzer gespeicherten Referenzergebnis überein, so war die Authentisierung erfolgreich.

Hiermit sind die wichtigsten Anforderungen sowie die Grundidee für den Auth²(nPA)-Dienst skizziert.

Es müssen bei der konkreten Umsetzung jedoch noch weitere Anforderungen beachtet werden, die jedoch mit Standardtechniken[9] umsetzbar sind und daher hier nicht ausführlich erläutert werden sollen:

- Vertraulichkeit und Authentizität der Kommunikation zwischen Nutzer und Einrichtung bzw. Dienstanbieter,
- Authentisierung der gestellten Anfragen an den Dienstanbieter,
- Signierung und Verschlüsselung des Referenzergebnisses,
- Kontrolle und Sorgfalt beim Informationsfluss von Einrichtung über Nutzer an den Dienstanbieter.
- Frische der Kommunikation und Bindung der Sitzungen aneinander,
- Verwendung adäquater kryptografischer Verfahren und Schlüssellängen[10] [Bun08].

Im folgenden Abschnitt wird die Essenz der in Abbildung 1 dargestellten Kommunikationsschritte angegeben.

3.4 Kommunikation

1. **N** initiiert starke Authentisierung und gibt **login** an **E** bekannt.
2. Einrichtung generiert Anfrage an Auth²(nPA)-Dienst. Darin sind $\mathbf{G_1}$ für das entsprechende **login** und kryptografisches Material und für vertrauliche anonyme Abholung des durch **D** frisch berechneten Ergebnisses enthalten. Diese Anfrage ist authentisiert und für **D** verschlüsselt und wird an **N** zusammen mit einer Weiterleitung gesendet.
3. **N** leitet Anfrage an **D** weiter.
4. Nachweis der **rID** von **N** mit der eID-Funktion des nPA gegenüber **D**.
5. Durch **P** anonymisierte Abfrage des von **D** aus $\mathbf{G_1}$ und $\mathbf{G_2}$ berechneten Ergebnisses **R'**.
6. Auslieferung des von **D** frisch berechneten und signierten Ergebnis **R'**, verschlüsselt mit einem Schlüssel, den **E** in ❷ gewählt hat.

6 Dies kann auch durch Miete eines eID-Servers oder Nutzung eines eID-Service realisiert sein.

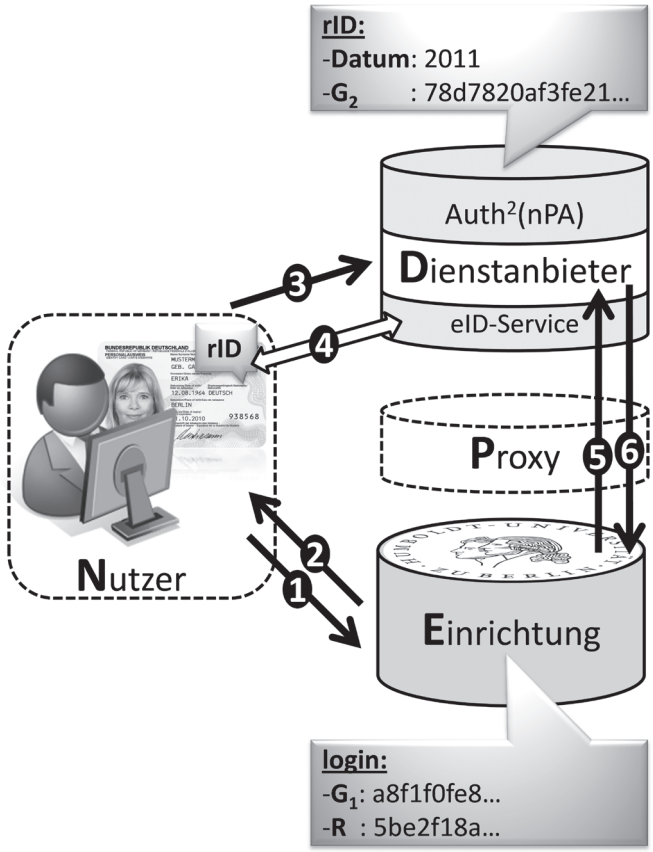
7 Als zentraler vertrauenswürdiger Dienst oder dezentral durch Nutzung eines Tor-Netzwerks (https://www.torproject.org/) realisierbar.

8 z. B. HMAC mit G_1 als Nachricht und G_2 als Schlüssel [KBC97].

9 SSL/TLS mit PKI, MAC, Signaturverfahren wie RSA oder DSA, AES, standardisierte Formularübermittlung und Vermeidung von Referer-URLs, Verwendung von Nonces und Sessionkeys.

10 Vorschlag: SHA-512, G_1: 512 Bit, G_2: 2048 Bit.

Abbildung 1 | Komponenten und ihre Kommunikation in Auth²(nPA).



3.5 Prozesse

Für die Umsetzung des Auth²(nPA)-Diensts werden folgende sieben wesentliche Prozesse benötigt.

- Vertragsschluss.
  Mit dem Vertragsschluss wird die rechtliche Grundlage zwischen dem Dienstbetreiber und der jeweiligen Einrichtung geschaffen. Hierbei werden unter anderem Verpflichtungen zur Einhaltung des Datenschutzes und entsprechende Nutzungsgebühren vereinbart.[11]
- Initialisierung des Zugangskontos der Einrichtung.
  Ein Zugangskonto wird, auf Grundlage des genannten Vertrags, mit der entsprechenden Identität der Einrichtung erstellt und verknüpft (Name, Anschrift, Ansprechpartner, Kontaktdaten, Loginname / Zugangskennwort oder Public-Key bzw. Zertifikat). Mittels dieses Zugangskontos ruft die Einrichtung das benötigte Schlüsselmaterial für die Authentisierung[12] der Anfragen an den Auth²(nPA)-Dienst in den zu vereinbarenden Zeitintervallen ab.
- Schlüsselerneuerung.
  Die über zwei verschiedene Nutzer einer Einrichtung gestellten Anfragen an den Dienstanbieter sollen nicht zugeordnet werden können. Deshalb wäre erkennbar einrichtungsindividuelles Schlüsselmaterial an dieser Stelle problematisch. Jedoch ist die Nutzung eines gemeinsamen symmetrischen Schlüssels für alle Einrichtungen für einen relativ kurzen Zeitraum (z. B. 24 Stunden) möglich, aber auch entsprechende Gruppenschlüssel wären denkbar. Die Schlüsselerneuerung für die Authentisierung der Anfragen sollte unabhängig von der tatsächlichen Dienstnutzung regelmäßig geschehen, sodass zwischen Schlüsselaktualisierung durch eine Einrichtung und Nutzerauthentisierung mit dem Auth²(nPA)-Dienst keine unmittelbare zeitliche Korrelation sichtbar wird. Dies ist leicht automatisiert zu bewerkstelligen.
- Neuer rID-Eintrag.
  Wird im Zuge des elektronischen Identitätsnachweis durch einen nPA eine in der Auth²(nPA)-Datenbank noch nicht als Schlüssel vorhandene rID übertragen, wird ein neuer Eintrag in dieser mit dem rID als Schlüssel erstellt. Unter diesem Schlüssel werden zwei Werte, das Erstellungsdatum (Jahr)[13] und das Geheimnis G_2 (ein hinreichend langer zufälliger Wert[14]) abgespeichert. Ist der Eintrag für die neue rID einmal erstellt, so bleibt er im Laufe seines etwas länger als 10 Jahren langen Lebens unverändert und wird lediglich gelesen.
- Nutzerinitialisierung an einer Einrichtung.
  Soll ein Account an einer Einrichtung für die Nutzung des Auth²(nPA)-Diensts freigeschaltet werden, so müssen bereits alle drei Parteien mitwirken, um ein Referenzergebnis zu berechnen und für spätere Authentisierungen in der Einrichtung zu hinterlegen. Die Einrichtung erweitert die Accountdaten des Nutzers um zwei weitere Felder (für G_1 und R).[15] Es wird ein zufälliges Geheimnis für den Nutzer durch die Einrichtung erzeugt und in dem Feld G_1 gespeichert. Anschließend werden die Schritte ❷ bis ❻ in Abbildung 1 abgearbeitet. Das im letzten Schritt erhaltene Ergebnis R' wird der Einrichtung im Feld R als Referenz gespeichert und bildet die Grundlage für die Authentisierung dieses Nutzers an dieser Einrichtung.
- Nutzerauthentisierung.
  Zur Authentisierung eines Nutzers werden die Schritte ❶ bis ❻ in Abbildung 1 durchlaufen. Das im letzten Schritt erhaltene Ergebnis R' wird mit dem in der Einrichtung für diesen Nutzer gespeicherten Referenzergebnis R verglichen. Die Authentisierung ist nur dann erfolgreich, wenn R = R' gilt.
- Löschung.
  Ein explizites Löschen eines durch eine rID referenzierten Nutzereintrags in der Datenbank des Auth²(nPA)-Dienstes ist

11 Aus Datenschutzgründen ist ein pauschales Vergütungsmodell hier sicherlich naheliegend.

12 Nachweis, dass Einrichtung berechtigt ist, diesen Dienst zu nutzen.

13 Es empfiehlt sich, nur die Jahreszahl zu speichern, da eine genauere Angabe Seiteninformation offenlegen würde.

14 Hier sollte an die Laufzeit von 10 Jahren gedacht werden, sodass wir derzeit 2048 Bit vorschlagen.

15 Diese Felder können mit in einem bereits existierenden LDAP-Verzeichnis abgelegt werden.

nicht nötig. Ist der Datensatz älter als 10 Jahre (Erstellungsdatum in Datenbank), so kann er getrost automatisch aus der Datenbank entfernt werden, da kein gültiger Ausweis[16] mehr zu dieser rID existieren kann. Wird ein nPA wegen Diebstahl oder Verlust gesperrt, so muss ebenfalls keine explizite Löschung für den zugehörigen rID-Eintrag erfolgen, da dieser nPA nun auf der sektorspezifischen Sperrliste des Auth²(nPA)-Dienstanbieters steht und somit der Zugriff auf die rID mit der eID-Funktion verwehrt wird. Scheidet ein Nutzer aus einer Einrichtung aus, so sperrt diese seinen lokalen Account. Aktionen auf dem Auth²(nPA)-Dienst sind hierzu nicht erforderlich. Insbesondere wird der zu dem Nutzer gehörende rID-Eintrag nicht gelöscht, da der Nutzer das Teilgeheimnis G_2 ggf. noch in anderen Einrichtungen nutzt. Ähnlich verhält es sich, sollte eine Einrichtung ihren Vertrag mit dem Dienstanbieter beenden. Dies bedeutet lediglich, dass die Einrichtung kein neues Schlüsselmaterial mehr bekommt und somit keine weiteren Auth²(nPA)-Authentisierungsanfragen stellen kann. Die rID-Einträge im Auth²(nPA)-Dienst bleiben davon unberührt.

16 Gültigkeitsdauer des nPA ist maximal 10 Jahre.

4 Fazit

Mit dem Auth²(nPA)-Dienst gelingt es, das Potenzial des neuen Personalausweises als starker Zweifaktorauthentifikator für Anwendungsfälle mit vielen Nutzern aber seltener bis mittlerer Nutzung pro Individuum wirtschaftlich zu erschließen. Der einrichtungsübergreifende Dienstanbieter muss insbesondere keine personenbezogenen Daten in seiner Datenbank, sondern lediglich pro rID die Jahreszahl der ersten Nutzung und einen zufälligen Bytestring, speichern. Eine Profilbildung oder die Zusammenführung von Daten über Nutzerdaten an einer oder mehreren Einrichtungen wird effektiv verhindert, sodass ein Berechtigungszertifikat für den Auth²(nPA)-Dienst erfolgreich beantragt werden kann.

Wir hoffen, dass zukünftig auch auf diese Weise, der nPA als starkes Authentifizierungstoken intensiv genutzt wird.

Literatur

[Bun08] Bundesamt für Sicherheit in der Informationstechnik: *Technische Richtlinie TR-02102*. 1.0, 6 2008

[Bun10a] Bundesamt für Sicherheit in der Informationstechnik: *Technical Guideline TR-03110*. 2.05, 10 2010

[Bun10b] Bundesamt für Sicherheit in der Informationstechnik: *Technische Richtlinie TR-03127*. 1.13, 10 2010

[KBC97] Krawczyk, H. ; Bellare, M. ; Canetti, R.: *HMAC: Keyed-Hashing for Message Authentication*. RFC 2104 (Informational), Februar 1997 (Request for Comments). – Updated by RFC 6151