Zusammenfassung

Dieser Beitrag ist entstanden bei der Voruntersuchung zur Erstellung der Requirement-Spezifikationen für ein IT-Projekt, bei dem die EID-Funktion des neuen deutschen Personalausweises (nPA) zur elektronischen Identitätsprüfung eingesetzt werden sollte.

Zielsetzung dieses Projektes war es u.a. auch, die Schwachstellen gängiger techn. Implementierung zu untersuchen und die Vorteile einer Online-Identitätsprüfung mit dem nPA dagegen zu stellen.

Das erste Projektziel „Technische Integration des nPA in Online- und Internet-Anwendungen“ wurde erreicht und der Nachweis der Funktionsfähigkeit in unterschiedlichen System- und Netzwerk-Konfigurationen mit ganz verschiedenen Interface-Konstellationen wurde erbracht.

Das nächste Projektziel, nämlich eine breitere Akzeptanz für den Einsatz dieser Lösung in kommerziellen eCommerce- und eGovernment zu finden, ist trotz intensiver Bemühungen noch lange nicht erreicht. Der Artikel versucht, hier die Ursachen und Hintergründe zu beleuchten.

EIDENT bezeichnet sowohl ein Konzept als auch eine Implementierung von IT-Lösungen, mit dem Ziel, die Identitätsprüfung in elektronischen Systemen sicherer und anwendungsfreundlicher zu gestalten und dabei eine sehr hohe Zuverlässigkeit der Identitätsprüfung zu garantieren.

Identitätsprüfung in elektronischen Systemen

Missbrauch als Grundproblem in elektronischen Systemen

Missbrauch in elektronisch und internet-basierten Verkaufs- und Service-Systemen wie E-Commerce, E-Payment, E-Banking, E-Government ist ein ernstes Problem, Tendenz steigend. Zahlreiche mehr weniger erfolgreiche sicherheitstechnische Maßnahmen werden eingesetzt, um negative Auswirkungen gering zu halten. Anbieter und Betreiber investieren hohe Summen in die Sicherheit von Netzwerken, Infrastruktur und die sichere Übertragung und Speicherung von Daten. Benutzer werden gezwungen sich immer ausgefeiltere Passwörter und „persönliche" Mermale auszudenken und zu merken ohne ausreichende Kontrolle darüber wie die Betreiber die Daten letztendlich verwenden. Im kommerziellen Bereich sind Schäden „kalkulierbar", d.h. trotz bekannter Sicherheitslücken kalkulieren die Betreiber mögliche Schäden ein, wenn das Beseitigen der Lücken einen zu hohen Aufwand bedeutet, Beispiele dafür gibt es genügend. Die Kosten werden letztendlich wieder auf alle Nutzer umgelegt.

Spannender wird die Sache, wenn der Betreiber oder Benutzer mit juristischen Konsequenzen rechnen muss. Das Risiko ist hier relativ ungleich verteilt, denn ein schwarzes (Benutzer-) Schaf mit Betrugsambitionen kann im Netz relativ einfach identifiziert und rechtlich belangt werden, was im umgekehrten Fall wesentlich schwieriger wird, sofern der Anbieter z.B. im Ausland sitzt oder über eine ausgefuchste Rechtsabteilung verfügt.

Am spannensten wird es, wenn es durch Missbrauch zu Schäden kommt, die sich unmittelbar auf das Image von Produkten oder die Marke eines Anbieterauswirkt. Dann besteht die Gefahr, dass das Vetrauen von Kunden nachhaltig Schaden erleidet und dann wird es für den Anbieter auch nicht mehr so einfach kalkulierbar.

Fazit: Verfolgt man die Statistiken kommt man schnell zu dem Schluss, dass die These „Alle tun nur das Nötigste" Kojunktur hat, wobei eine unmittelbare Zunahme der Anstrengungen in Abh. des jeweiligen Risikos „kommerzieller Schaden", rechliche Konsequenzen, Vertrauens- oder Imageverlust festzustellen ist. Und man kann weiterhin feststellen, dass Online-Anwendungen in der Praxis zunehmen, und sicherheitstechnisch auch „irgendwie" funktionieren, jedoch gegen ausreichend hohem Einsatz von krimineller Energie nur ungenügenden Schutz bieten. Der E-User ist i.allgem. nach kurzer Zeit im Netz bestens bekannt, der Widerruf nicht einfach.

Technische Verfahren zur Identitätsprüfung

Sicherheit ist objektiv betrachtet immer „relativ", d.h. man muss sich immer die Frage stellen, ob die definierte Sicherheit für den Anwendungsfall ausreichend ist.

Die Identitätsprüfung bei der Registrierung oder Erstanmeldung eines Benutzers an einem elektronischen Anwendungsystem ist ein zentraler Sicherheitsaspekt. Die meisten Systeme basieren auf der sog. zweistufigen Authentifizierung, d.h. dem Prinzip der Trennung von Wissen und Besitz, wobei „Besitz" in diesem Fall bedeutet Email-Adresse, Kreditkarte, Ausweis, Pass, Personalausweis, oder ein biometrisches Merkmal wie Fingerabdruck, Augenfarbe. „Wissen" bedeutet dann ein „persönliches Geheimnis" wie Passwort oder Pin. Nach diesem Prinzip arbeiten i.w. auch die meisten Login-Systeme, d.h. die Übergänge zwischen Identitätsprüfung und Login sind fliessend.

Die üblichen techn. Verfahren kennt jeder Benutzer durch seine Registrierung an einer Web-Anwendung im Internet oder einer Smartphone-App (M-App):

- Eingabe von mehr oder weniger vielen persönlichen Daten
- Eingabe von Benutzer-ID / Passwort
- Email-Adresse mit Bestätigung der Email-Registrierung
- Bestätigung von Datenschutzregelungen, AGBs, Haftungsregelungen
- bei hohen Sicherheitsanforderungen zusätzlich Erfassung und Auswertung biometrischer Merkmale wie Fingerprint oder Foto
- Eingabe von Zahlungsinformationen für Paypal, Kreditkarte, Lastschrift, Vorauskasse
- Vorlage eines amtl. Dokument wie Pass oder Personalausweis mit ggf. persönlichem Erscheinen des Kunden in einer Zeigstelle des Anbieters oder einer Service-Stelle wie z.B. bei Postident oder bei Behörden

Der Identitätsnachweis von Anbietern gegenüber den Kunden ist relativ bescheiden:

- Anbieter-Name, Logo, usw.
- Impressum
- Präsentation der Webseite bzw. der M-App auf dem Display
- ein Echtheitsnachweis der Anbieter-Session fehlt i.d.R., also der Nachweis darüber, dass der Nutzer auch tatsächlich mit dem (echten) Anbieter kommuniziert

Einsatz neuer Technologien zur Identitätsprüfung in elektronischen Systemen

Die im Folgenden genannten Technologien und Verfahren zur Identitätsprüfung in elektronischen Systemen sind unter der Bezeichnung ***EIDENT*** (-Verfahren) zusammengefasst, wobei der Begriff unmittelbar für Elektronische Identitätsprüfung steht.

Zielsetzungen EIDENT

EIDENT hat das Ziel, die Identitätsprüfung in elektronischen Systemen sicherer und anwendungsfreundlicher zu gestalten und dabei eine sehr hohe Zuverlässigkeit der Identitätsprüfung zu garantieren. Die Identitätsprüfung kann ohne Medienbruch und ohne zeitliche Einschränkungen quasi jederzeit „Online" erfolgen. Dazu setzt EIDENT ausschließlich auf elektronische Verfahren, die i.d.R. in bereits vorhandene Registrierungsprozesse von E-Anwendungen eingebunden werden können.

EIDENT favorisiert die sog. starke Authentisierung, d.h. den Nachweis der Identität eines Benutzers, eines Gerätes oder des Betreibers einer IT-Anwendung durch Besitz und Wissen.
Das kann ein Benutzer z.B. auf verschiedenen Wegen erreichen:

- Nachweis der Kenntnis einer Information, er weiß etwas, zum Beispiel ein Passwort;
- Verwendung eines Besitztums, er hat etwas, zum Beispiel einen Schlüssel oder einen nPA
- Gegenwart des Benutzers selbst, er ist etwas, zum Beispiel in Form eines biometrischen Merkmals.

Die Wahl der Authentisierungsmethoden führt je nach Anwendungsgebiet zu verschiedenen Vor- und Nachteilen bei der praktischen Nutzung durch den Benutzer im Alltag und dem Sicherheitsbedarf der Beteiligten.

Der Schwerpunkt von EIDENT liegt in der Nutzung von amtl. Dokumenten wie Personalausweis oder Pass, die persönliche Daten enthalten, die elektronisch lesbar, aufgedruckt, aufgelasert, oder in einem intergrierten Chip gespeichert sind. Bei einem amtl. Dokument ist die Prämisse Trennung von Wissen und Besitz qausi von Amtswegen immer gegeben, so dass eine Identitätsprüfung über dieses Medium eine nahezu 100% hohe Sicherheit und Zuverlässigkeit garantieren kann.

Im Folgenden wird kurz auf verschiedene Verfahren und Methoden eingegangen.

Standard-Verfahren

In marktgängigen Lösungen hat sich die Registrierung mittels Email-Adresse und Passwort etabliert ggf. noch erweitert durch Hochladen eines Fotos, eine persönliche Registrierungs-Smart Card oder einen Stick. Der Anbieter sichert sich i.d.R. gegen eine Haftung im Schadensfall ab, indem er den Benutzer eine entsprechende Datenschutz- und/oder AGB-Erklärung anklicken lässt.

z.B. mit mobiler **Bilderfassung (relativ neu)**

- manuelle Online-Erfassung der Benutzerdaten sowie Online-Bilderfassung des Benutzerkonterfeis, z.B. durch Abfotografiern von vorgezeigtem Pass oder Personalausweis per Web-Kamera oder Smartphone Kamera
  Speicherung und Verknüpfung der digitalisierten Fotos mit dem User-Account

Visuelle Kontrolle des Benutzer-Fotos gegen das Ausweis-Foto in einem entsprechend techn. ausgerüsteten Call-Center

Über die Beurteilung der Sicherheit dieser Verfahren kann man Tausende Beiträge Googlen. U.E. ist diese Art der Authentisierung, also der Nachweis der Identität eines Benutzers häufig nur mittels Email-Adresse und Passwort als sehr schwaches Verfahren einzustufen, und von jedem (durchschnittlichen) Hacker oder Web-Programmierer leicht zu mißbrauchen. Die Anbieter selbst identifizieren sich i.d.R. über ihren Internet-Auftritt, mit Impressum, aber ansonsten ohne weitere Authentifizierung-Nachweise. Damit sind dann beide Seiten autorisiert, d.h. sie können miteinander Geschäfte tätigen, der Anbieter fordert den Benutzer zur Übermittlung persönlicher Daten auf, Konto- und Zahlungsdaten werden ausgetauscht usw.

EIDENT-Techologien

Das Produkt EIDENT kann in unterschiedlichen Konfigurationen und unter Nutzung verschiedener Technologien zum Einsatz kommen.

Grundlage des Verfahrens:

- Der Benutzer einer eCommerce- oder eGovernment-Anwendung startet einen Online-Registrierungsvorgang am jeweiligen Provider-System.
- Dazu gibt er im ersten Schritt seine persönlichen Daten in eine Online-Erfassungsmaske ein. Diese Daten werden vom Provider in einem sicheren Kontext zwischengespeichert und unterliegen dem Datenschutz. Der Provider teilt dann dem Benutzer einen eindeutigen Registrierungscode mit.
- Mit dem Registrierungscode als Zugangscode startet der Benutzer dann den Elektronischen Authentisierung-Prozess mit EIDENT. Dabei liest EIDENT wiederum Personendaten aus dem elektronischen Speicher von amtlichen Dokumenten aus, die der Provider dann mit den zuvor erfassten Benutzerdaten abgegleicht. Eine Übereinstimmung bestätigt die Autorisierung des Benutzers für den jeweiligen Anwendungsfall.
- In Deutschland verwendet EIDENT die für Nicht-Hoheitliche Authentisierung-Zwecke erlaubten EID-Funktion des nPA (nPA im ec-Kartenformat mit kontaktlosem Chip [1]), in Ländern außerhalb Deutschlands entsprechende amtliche Dokumente mit elektronisch lesbaren Daten (Beispiele E-ID Card Macao, Kombi E-ID Card Nigeria, Bürgerkarte Österreich und Bürgerausweise in den Baltischen Staaten).

Beurteilung der EIDENT-Technologie:

- Die elektronische Identitätsprüfung mittels nPA ist das sicherste und zuverlässigte Verfahren. Der nPA kann nicht manipuliert werden. Da der nPA ein amtl. Dokument ist, ist Weitergabe des nPA und der persönlichen PIN eine Ordnungswidrigkeit.
- Im Gegensatz dazu ist die Registrierung mittels (elektronischem) Foto weniger sicher, da fehleranfälliger und zudem manipulierbar. Das Prinzip Trennung von Besitz und Wissen ist im Remote Verfahren nicht eindeutig nachweisbar.
- Im Authentisierung-Prozessablauf mit EIDENT treten außerhalb der sicheren Umgebung des Anbieter-Systems an keiner Stelle zu keinem Zeitpunkt Personendaten im Klartext auf.

[1] Anstelle des nPA kann auch der sog. elektronischen Aufenthaltstitel eAT benutzt werden

- Beim Einsatz von EIDENT mit dem nPA ist zusätzlich auch die Autorisierung des Anbieters sichergestellt , zB. durch elektronische Prüfung der Berechtigungszertifikate des Anbieters sowie Darstellung von Provider-Informationen während der Authentisierung-Session nach vorgeschriebenen Regeln und Inhalten des BSI.

Voraussetzungen und Einschränkungen:

- Den elektronischen Personalausweis mit maschinell lesbaren Personendaten aus dem integrierten Chip zur Anwendung für kommerzielle Anwendungen gibt es derzeit nur in Deutschland (nPA).
- Der nPA muss freigeschaltet sein, d.h. der Inhaber muss bei der Beantragung die sog. EID-Funktion frei schalten lassen (das ist die Standardkonfektionierung)
- Der Inhaber muss eine 6-stellige persönlichen PIN einstellen (bei Beantragung erhält er vom Amt die sog. 5-st. Transport PIN schriftlich mitgeteilt, die muss er ändern).

Verfügbarkeit von EID und EIDENT

BMI-App
Das Bundesinnenministerium stellt für die Nutzung von EID mit dem nPA die sog. AusweisApp und seit Ende 2014 eine verbesserte AusweisApp2 (für Windows und Mac) zur Verfügung. Bei der neuen AusweisApp2 wurden Installation, Handling, Speicherbedarf und Performance gegenüber der alten Version verbessert. Die AusweisApp wird in den Web-Client des Anbieters eingebunden und über entsprechende Browser-Interfaces angesprochen.

EIDENT-App
Die EIDENT-App beinhaltet als Basiskomponente ebenfalls einen EIDENT-Client, der den sicheren Zugriff auf den nPA ermöglicht. Zusätzlich sind im Kern des Client alle Web-Interfaces integriert, die die Online-Kommunikation mit den weiteren Partnern der elektronischen Identitaätsprüfung implementieren (zum Web-Server Anbieter, EID-Serviceprovider, Web-Client). Der EIDENT-Client ist in Java programmiert, kann somit auf allen Java-fähigen Systemen laufen und zur Nutzung der eID-Funktion des nPA optimiert (Speicher, Code). Vom Sicherheitsaspekt aus betrachtet, ist der Client vollständig gekapselt, d.h. es gibt keine Zugriffsmöglichkeiten außer über die verfügbaren Interfaces (Java-Calls oder IP-Calls), so dass sich ein absolut sicherer Kontext herstellen lässt (z.B. auf öffentlich zugänglichen POS-Terminals, Bürger-Terminals und Geldausgabeautomaten).
Ansonsten entspricht die EIDENT-App der eCard-Strategie des BSI (siehe BSI Technische Richtlinie TR-03127), d.h. der nPA bzw. der eAT werden im Sinne eines „nichthoheitlichen/ausländischen Authentisierungsterminal“ eingesetzt.

Ausblick
Derzeit verwendet die EIDENT-App für den Zugriff auf den nPA noch einen (kontaktlosen) Chipkartenleser mit herkömmlichem Geräteanschluss am PC oder einem POS-Terminal. Die Erweiterung der EIDENT-App als mobile App zur Nutzung im Smartphone ist in Vorbereitung und erhöht die Akzeptanz für zahlreiche Anwendungsfälle. Weiterhin möglich wäre der Einsatz der EIDENT-App zur qualifizierten elektronischen Signatur (QES) an einem Signaturterminal.

EIDENT-Anwendungsfälle

Anwendungsfall: elektronische Identitätsprüfung bei Online-Bank-Kontoanmeldung

Gemäß Geldwäschegesetz ist die Identitätsprüfung für neue Kunden vorgeschrieben.
Beim herkömmlichen Verfahren erfolgt die Identitätsprüfung durch persönliches Erscheinen des Kunden bei der Bank oder über das postident-Verfahren mit Bestätigung der Kundenindetität in einer Postfiliale. Mit der EIDENT-App identifiziert sich der Kunde stattdessen elektronisch mit seinem nPA/eAT und persönlicher PIN an einem POS-Terminal der Bank (z.B. Geldausgabeautomaten) oder im Home-Banking an seinem PC.

Vorteile für den Kunden:
- Kein persönliches Erscheinen erforderlich
- Keine zeitliche Beschränkung durch Öffnungszeiten
- Nutzung an einem Automaten der Bank, nach Freischaltung steht das Online-Konto sofort zur Verfügung
- Optional Nutzung der EIDENT-App beim Home-Banking am PC, falls der Kunde die Installation des EIDENT-Client und eines kommerziellen Kartenlesers an seinem PC durchführt. Durch ein besonderes Merkmal der EID-Funktion des nPA kann optional auch eine Instituts-bezogene Kurzkennung generiert und im nPA-Chip gespeichert werden. Dies ermöglicht z.B. eine Quick-Anmeldung des Kunden beim Online-Banking.

Vorteile für die Bank:
- Anerkanntes Verfahren nach dem Prinzip der starken, sog. zweistufigen Authentifizierung, durch Trennung von Wissen und Besitz
- Vereinfachtes elektronisches Verfahren ohne Medienbruch
- Erhebliche Kosteneinsparung (60 -70 %)
- Marketing-Effekte

Die beschriebene EIDENT-App wurde von der meco GmbH für die Firma NCR zum Einsatz auf den Plattformen Geldausgabeautomat und Selbstbedienungsterminal realisiert.

Weiterer ähnlicher Anwendungsfall: elektronische Identitätsprüfung für den Vertragsabschluss bei der Online-Policierung

Prozessablauf ähnlich Online-Banking, Kontakte zu interessierten Kunden bestehen.

EIDENT-App in E-Government Anwendungen (Ausblick)

Status

Im Zusammenhang mit der E-Government Initiative des Bundes-Innenministerium sind Behörden dazu aufgefordert mit De-Mail und der EID-Funktion des Personalausweises deutlich mehr Dienstleistungen in höherer Qualität und ohne Medienbruch auch Online anzubieten. Die Initiative führt aus, dass durch eine konsequente elektronische Abwicklung zahlreicher Verwaltungsprozess, die Behörden ihre eigenen Kosten senken können und gleichzeitig für den Bürger eine spürbare Vereinfachung und Beschleunigung nach sich zieht. Siehe dazu auch folgende Links.

Beiträge zu E-Government-Initiative:

http://www.bmi.bund.de/DE/Themen/IT-Netzpolitik/E-Government/E-Government-Initiative/e-government-initiative_node.html;jsessionid=4A3842058F8C1F79BEEB502A8BF6F574.2_cid287

Laufende Vorhaben (inclusive Bayern):
http://www.personalausweisportal.de/DE/Verwaltung/E-Government-Initiative/Alle-Vorhaben/Alle-Vorhaben_node.html

E- und Open-Government der Landeshauptstadt München:

http://www.personalausweisportal.de/DE/Verwaltung/E-Government-Initiative/Alle-Vorhaben/Alle-Vorhaben_node.html#doc4185108bodyText3

http://www.personalausweisportal.de/SharedDocs/Downloads/DE/Ergebnisdokumente/Landeshauptstadt_M%C3%BCnchen_Kommunikationskonzept.html?nn=3043802

https://joinup.ec.europa.eu/community/nifo/news/nifo-renews-egovernment-data-collection-34-factsheets

Akzeptanz von EID und De-Mail

Das Hauptziel von De-Mail ist es, Nachrichten und Dokumente über das Internet vertraulich, sicher und nachweisbar zu versenden und zu empfangen und damit ein elektronisches Pendant zur heutigen Briefpost zu etablieren. Damit sollen Bürger, Wirtschaft und Verwaltung kostengünstig, zuverlässig und vertraulich elektronisch miteinander kommunizieren können. De-Mail setzen bereits viele Behörden ein.

Im Gegensatz dazu ist die Nutzung der eID Funktion des nPA noch wenig verbreitet. Einzelne Städte und größere Gemeinden (siehe Beispiel München), setzen/oder setzten die Initiative bereits um, indem sie die elektronische Identitätsprüfung mittels AusweisApp in ihre individuellen E-Goverment Anwendungen integrieren, teilweis geschieht dies auch auf Länderebene.

EIDENT-Service im Rahmen der E-Government Initiative

Im Gegensatz zu *De-Mail* ist die Nutzung der eID Funktion des nPA noch wenig verbreitet. Einzelne Städte und größere Gemeinden (siehe Beispiel München), setzen/oder setzten die Initiative bereits um, indem sie die elektronische Identitätsprüfung mittels AusweisApp in ihre individuellen E-Goverment Anwendungen integrieren, teilweis geschieht dies auch auf Länderebene.

Mit einem zentralen EIDENT-Service könnte die elektronische Identitätsprüfung mit dem nPA in individuellen E-Government Anwendungen für die staatliche Administration in Städten, Gemeinden und Behörden allgemein zur Verfügung gestellt werden.

Vorteile:

- Die Integration der elektronischen Identitätsprüfung mit dem nPA/eAT in so gut wie jede E-Government Anwendung ist problemlos möglich. Anstelle der Einbindung der AusweisApp in einzelne individuelle E-Government Anwendungen, wird die Identitätsprüfung als Web-Service aufgerufen, die Anwendung selbst erhält dann nur noch das Ergebnis gemeldet (Identität OK / nicht OK, ggf. zusätzlich verschlüsselt die Personendaten)
- Investitions- und Betriebskosten des EIDENT-Serviceprovider können auf alle Anwender umgelegt werden, beispielsweise durch ein Lizenzmodell und oder günstige Transaktionsgebühren, d.h. staatliche Investitionskosten sind niedrig
- Vereinheitlichung und quasi Standardisierung der eGovernment-Prozesse, Interfaces und Funktionalität
- Einheitliches Erscheinungsbild gegenüber den Benutzern (Bürger, Firmen, Behörden untereinander, etc.), damit Erhöhung der Akzeptanz

Voraussetzungen an die *EIDENT-App für E-Government:*

Aus technisch/organisatorischer Sicht ist die Beantragung eines einheitlichen Berechtigungszertifikats zur Nutzung der Online-Ausweisfunktion (eID-Funktion) des nPA als EIDENT-Service erforderlich

- Zuständig dafür ist die Vergabestelle für Berechtigungszertifikate (VfB) des Bundesverwaltungsamtes. I.d.R. muss jeder Anbieter eines solchen Dienstes eine extra Erlaubnis beantragen. Da es sich in diesem Anwendungsfall um staatliche Stellen handelt sollte es eigentlich keine Probleme geben ein allgemein gültiges Zertifikat für den Service zu erhalten
- Beauftragung eines (externen) EID-Service Providers, der das laut BSI vorgeschriebene HSM-Modul sowie die techn. Zertifikate bereitstellt, z.B. EID-Service der T-Systems oder der Bundsdruckerei.
- Schaffung einer PKI-Infrastruktur zur Nutzung des Service im Netz (Backend-Server, Transaktions-Server, Netzwerkverbindungen, Verschlüsselungdienste, Multichannel-Nutzer-Interfaces wie Browser, Smartphone, Tablet)
- Bereitstellung Personal für einen 7/24 Stunden Betrieb

Vertriebliche Maßnahmen:

- Zuordnung der Aufgaben und Verantwortlichkeiten, Businessplan
- Finden von Interessenten/Kunden im Behördenbereich

Ausblick

Zur absolut sicheren Identitätsprüfung eines Kunden oder Nutzer eines elektronisch unterstützten Verkaufs- oder Service-Angebotes bei der der zweifelsfreie Identitätsnachweis von zentraler Bedeutung ist, ist auch heute noch die Vorlage eines entprechenden amtlichen Dokumentes i.allg. zwingend erforderlich. In herkömmlichen Verfahren muss der Kunde persönlich in einer Zeigstelle oder Niederlassung des Anbieters oder einer damit beauftragten Service-Stelle erscheinen (wie z.B. bei Postident) und seinen Personalausweis, Pass oder ein entsprechendes amtl. Dokument vorlegen.

EIDENT ist eine Softwarelösung, die an geeigneter Stelle in neue oder vorhandene IT-gestützte Verfahren eingebaut wird und die Identitätsprüfung elektronisch durchführt, so dass das persönliche Erscheinen entfällt und somit auch die damit verbundenen Einschränkungen wir Öffnungszeiten, Wartezeiten oder vorheriges Anmelden.

Eine wesentliche Erhöhung der Akzeptanz der elektronischen Nutzung des nPA würde sich sicherlich durch Migration der EIDENT-App auf mobile Plattformen (Smartphones) ergeben.