FH Gelsenkirchen
Fachbereich Informatik

Institut für Internet-Sicherheit - if(is)

Studie

Zwischenbericht: „Restrisiken beim Einsatz der AusweisApp auf dem Bürger-PC zur Online-Authentisierung mit Penetration-Test“

Oktober 2010

M.Sc. Christian J. Dietrich

M.Sc. Christian Rossow

Prof. Dr. (TU NN) **Norbert Pohlmann**

Institut für Internet-Sicherheit – if(is)
Fachhochschule Gelsenkirchen

Neidenburger Str. 43
45877 Gelsenkirchen

https://www.internet-sicherheit.de

1 Potential der eID-Funktion

Wenn man sich heutzutage als Internetnutzer gegenüber einer Webseite authentisiert, dann kommt dabei meist ein Mittel zum Einsatz: die Kombination von Benutzername und Passwort. Ein Kunde muss auf diese Weise seine Identität gegenüber einem Diensteanbieter beweisen. Nur, wenn ein Kunde die richtige Kombination aus Benutzername und Passwort vorweisen kann, wird der Prozess fortgesetzt. Das Beispiel zeigt, dass es sich um eine einseitige Authentisierung handelt, nämlich vom Benutzer gegenüber dem Diensteanbieter. In der Gegenrichtung ist es üblich, dass der Diensteanbieter ein SSL-Zertifikat einsetzt. Auf diese Weise kann der Diensteanbieter zumindest die Echtheit der Webseiten-Domain beweisen.

Die Schwachstellen der bisherigen Authentisierung im Internet liegen dabei in erster Linie beim Benutzer. Häufig werden Passwörter mit unzureichender Stärke verwendet, wie beispielsweise kontextsensitive Begriffe (der Vorname des Lebenspartners oder des Haustieres etc.). Ferner werden mitunter für verschiedene Dienste das gleiche Passwort verwendet. Passwörter werden teilweise im Klartext (z.B. in E-Mails) über das Internet übertragen. Darüber hinaus gibt es Abhängigkeiten von Passwörtern. So kann beispielsweise der Bruch des E-Mail-Konto-Passworts dazu führen, mit Hilfe von Passwort-Reset-Funktionen anderer Dienste, jegliche Identitäten des Benutzers bei weiteren Diensteanbietern zu brechen.

Aber auch die Authentifizierung des Diensteanbieters durch den Benutzer wird in der Praxis nicht immer in genügendem Maße durchgeführt. So baut ein Großteil an Phishing-Angriffen darauf, dass der Benutzer eben gerade nicht erkennt, dass er seine Daten einem vorgetäuschten Diensteanbieter preisgibt. In der Praxis bedeutet dies, dass der Benutzer beispielsweise nicht prüft, ob der Diensteanbieter SSL nutzt, ein gültiges SSL-Zertifikat aufweist und die Identität eindeutig ist.

Die eID-Funktion des elektronischen Personalausweises greift an dieser Stelle und leistet einen wichtigen Beitrag, um diese Schwachstellen zu entschärfen. Bei der eID-Funktion handelt es sich um eine sichere gegenseitige Authentisierung. Ein entscheidender Vorteil gegenüber der herkömmlichen Authentisierung mit Passwörtern ist die Tatsache, dass sich die eID-Funktion auf Besitz (der Personalausweis) und Wissen (die geheime PIN) abstützt und damit eine Zweifaktor-Authentisierung darstellt. Darüber hinaus garantiert das sog. Berechtigungszertifikat durch das Bundesverwaltungsamt, dass bereits im Vorfeld geprüft wurde, welche Daten ein Diensteanbieter aus dem nPA auslesen darf. Ferner sorgt, im Gegensatz zum oben dargestellten Beispiel, der Personalausweis für die Überprüfung der Gültigkeit des Berechtigungszertifikats. Zusätzlich wird dem Benutzer das Berechtigungszertifikat angezeigt, und er kann auf die Freigabe einzelner Merkmale Einfluss nehmen. Diese

Überprüfung ist damit in der Praxis, im Vergleich zur optionalen manuellen Prüfung eines SSL-Zertifikats, deutlich sicherer. Zudem werden die ausgelesenen Daten zu keiner Zeit im Klartext, sondern jederzeit verschlüsselt und signiert über das Internet übermittelt.

2 Aufgabenstellung dieser Studie

Trotz der, gegenüber Passwort-Authentisierung vergleichsweise erhöhten Sicherheit durch den Einsatz der eID-Funktion, bestehen Risiken, die Einfluss auf die Sicherheit der Online-Authentisierung haben. Zur Klärung dieser Restrisiken beauftragte das Bundesministerium des Innern diese Studie, die das Institut für Internet-Sicherheit - if(is) in vier Monaten mit einem Arbeitsaufwand von insgesamt 150 Personentagen durchgeführt hat. Vorkenntnisse im Bereich des elektronischen Personalausweises sind im Institut für Internet-Sicherheit, insbesondere durch eine vorhergehende Studie mit einer Beispiel-Implementierung der eID-Funktion, vorhanden.

Im Rahmen dieser Studie wurden dem Institut für Internet-Sicherheit die Komponenten des nPA-Anwendungstests mit Stand von November 2009 zur Verfügung gestellt. Im Detail lagen den Autoren dieser Studie die AusweisApp (Bürgerclient) in Version 1.0.0 beta und das Kartenlesegerät SCM SDI010 vor. Der Zugang zu einem eID-Server sowie zu einem beispielhaften Diensteanbieter in Form eines Webshops wurde freundlicherweise vom Fraunhofer FOKUS zur Verfügung gestellt.

Im Rahmen des Penetration Tests dieser Studie hat das if(is) die Rolle des Angreifers eingenommen. Dabei hatten die Autoren Zugriff auf sehr viele Informationen. Die Ergebnisse der Studie wurden dem Auftraggeber im März 2010 präsentiert.

Die Studie enthält insgesamt 11 Empfehlungen. 7 Empfehlungen sind bis heute umgesetzt worden, haben zu Änderungen in der Spezifikation und den Implementierungen geführt oder wurden nach intensiver Diskussion als nicht risiko-relevant eingestuft. Im folgenden Kapitel werden die verbliebenen 4 Risiken dargestellt, die im Rahmen dieser Studie des Instituts für Internet-Sicherheit identifiziert wurden und heute berücksichtigt werden sollten.

3 Restrisiken beim Einsatz der eID-Funktion

3.1 Risikobetrachtung: Lesegeräte

Die Kommunikation zwischen Bürger-PC und nPA erfolgt über ein nPA-kompatibles Lesegerät. Das BSI zertifiziert Lesegeräte (nach BSI TR-03119) in drei unterschiedlichen Kategorien: Basisleser, Standardleser und Komfortleser. Die folgende Tabelle veranschaulicht die wesentlichen Unterschiede der Lesegerätklassen:

Merkmal	Basisleser	Standardleser	Komfortleser
Kontaktlose Schnittstelle	X	X	X
Kontaktbehaftete Schnittstelle	O	O	X
Pinpad	O	X	X
Zweizeiliges Display	O	O	X
Qualifizierte Signatur	-	-	X

Tabelle 1: Unterscheidung Lesegeräte-Klassen; X = obligatorisch, O = optional

Das Sicherheitslevel der drei verschiedenen Lesegerät-Typen unterscheidet sich im Rahmen der eID-Funktion deutlich. Ein Restrisiko beim Einsatz des nPA ist der Basisleser, bei dem die Eingabe der PIN mangels Pinpad über die Tastatur am potentiell nicht vertrauenswürdigen Bürger-PC vorgenommen wird. Ist ein Bürger-PC mit spezialisierter Schadsoftware (Malware) befallen, so kann diese, mittels Keylogging, die PIN eines nPA während der Eingabe mitlesen. Bei Standard- und Komfortlesern ist ein Mitlesen am PC nicht möglich, da die PIN direkt am Pinpad des Lesegeräts eingegeben wird.

Ist die PIN im Besitz eines potentiellen Angreifers, so kann dieser die Identität des betroffenen Benutzers auch per entferntem Zugriff mit Hilfe der eingeschleusten Malware missbrauchen. Wird vom Benutzer ein Basisleser eingesetzt und ist der nPA auf das Basislesegerät aufgelegt, so kann ein Angriff automatisiert durchgeführt werden. In einem solchen Szenario böte die Authentisierung mittels eID-Funktion keinen Mehrwert gegenüber der herkömmlichen Passwort-Authentisierung. Bei der Nutzung der eID-Funktion entfällt zudem die Vielfalt der Authentisierungsgeheimnisse (z.B. verschiedene Logins, Passwörter), so dass ein Angreifer im schlimmsten Fall die Identität des betroffenen Benutzers bei jedem Diensteanbieter mit eID-Funktion missbräuchlich erstellen oder verwenden könnte. Dies muss insbesondere Diensteanbietern bewusst sein, da diese die Vertrauenswürdigkeit der Nutzer-PCs nicht verifizieren können.

Standard- und Komfortleser bieten einen höheren Schutz vor einem Identitätsmissbrauch. Bei beiden Lesegerätklassen wird zum einen das Mitlesen der PIN unterbunden. Zum anderen erfordert eine Online-Authentisierung im Kontext der eID-Funktion immer die tatsächliche Eingabe der PIN am Lesegerät und somit ein aktives Mitwirken des Benutzers. Der Angriffsversuch scheitert, wenn der Benutzer selbst keine Authentisierung initiiert hat und folglich die Eingabe der PIN verweigert. Ein Komfortleser bietet einen darüber hinaus gehenden Schutz dadurch, dass im Display des Lesegeräts zusätzlich die Gegenstelle der Authentisierung sowie die Berechtigungen vertrauenswürdig angezeigt werden kann.

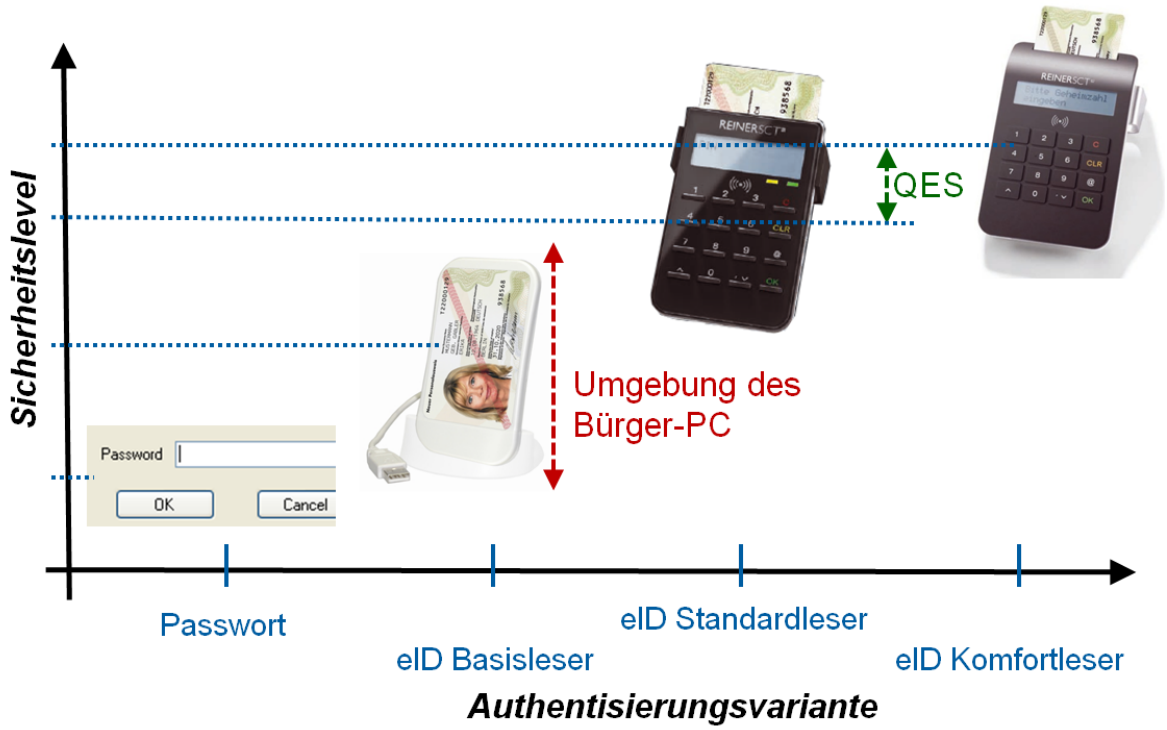

Abbildung 1: Sicherheitslevel abhängig von der eingesetzten Authentisierungsvariante und dem Lesegerät

In Abbildung 1 ist zu sehen, dass die Vertrauenswürdigkeit des Bürger-PCs großen Einfluss auf den zu erzielenden Sicherheitslevel beim Einsatz des Basislesers hat.

Risikobetrachtung

Die Wahl der Lesegerätklasse durch den Benutzer ist neben der Integrität des Bürger-PCs ein zentrales Standbein der Sicherheit der eID-Funktion. Basisleser weisen ein höheres Restrisiko als Standard- oder Komfortleser auf.

Zur Benutzung eines Basislesers kann grundsätzlich nur dann geraten werden, wenn die dauerhafte Vertrauenswürdigkeit des Bürger-PCs gewährleistet werden kann. Für einen Großteil der Benutzer ist diese Voraussetzung jedoch heute noch nicht erfüllt. Daher

sollte mindestens ein Standardleser oder besser noch ein Komfortleser eingesetzt werden.

3.2 Awareness

Ein vorbildliches Verhalten des Benutzers erhöht – wie bei der Passwort-Authentisierung auch – die Sicherheit der eID-Funktion. Somit ist es dringend notwendig, den Benutzer durch gezielte Awareness-Strategien auf verschiedene Aspekte aufmerksam zu machen.

Benutzern der eID-Funktion muss zum einen verständlich sein, welche Ziele die eID-Funktion hat und für welche Zwecke sie eingesetzt werden kann. Die eID-Funktion muss in erster Linie als ein Ersatz bei herkömmlichen Login- oder Registrierungsvorgängen im Web verstanden werden. Weitergehende Funktionalitäten, z.B. die Absicherung einer Transaktion, wie etwa die abschließende Bestätigung im Rahmen eines Bestellprozesses in einem Online-Shop, sind Gegenstand der qualifizierten elektronischen Signatur und werden nicht im Kontext dieser Sicherheitsbetrachtung behandelt. Ein Wissen über diesen elementaren Unterschied zwischen der eID-Funktion und der Signaturfunktion ist für den Benutzer und insbesondere für den Diensteanbieter von großer Wichtigkeit!

Darüber hinaus spielt die Integrität des Bürger-PCs eine große Rolle, insbesondere bei der Verwendung eines Basislesers. Der Benutzer sollte dazu aufgefordert werden, die Vertrauenswürdigkeit seines PCs beispielsweise mit Hilfe gängiger Antiviren-Software, Firewall und automatischen Updates des Betriebssystems zu prüfen und sicherzustellen. Hilfreich ist an dieser Stelle möglicherweise auch ein Hinweis auf das Anti-Botnet-Beratungszentrum des eco – Verband der deutschen Internetwirtschaft e.V., das unter der Webseite www.botfrei.de Informationen zum Schutz vor Bots zur Verfügung stellt. Ferner ist in diesem Kontext die Aufklärung des Benutzers über die Wahl eines sicheren Lesegeräts, wie beispielsweise Standardleser oder Komfortleser, unabdingbar.

Risikobetrachtung

Nicht zuletzt muss sich der Benutzer mit der eID-Funktion vertraut machen und gewisse Vorsichtsmaßnahmen ergreifen. So muss für den Benutzer die Vorgehensweise beim Sperren des nPA klar und einfach sein, um die eID-Funktion im Falle eines Missbrauchs zügig deaktivieren zu können. Zudem sollte der Benutzer den nPA nur während einer Online-Authentisierung auf das Lesegerät legen und ihn danach entfernen, um das Zeitfenster eines potentiellen Missbrauchs zu minimieren.

Derartige Hinweise zum Umgang mit dem Personalausweis sind auf dem Webportal www.personalausweisportal.de abrufbar.

3.3 Tracking

Aus datenschutzrechtlichen Gründen sollte es durch den Einsatz des nPA keinem Beteiligten ermöglicht werden, ohne Einwilligung und Wissen des Benutzers ein Profil über sein Authentisierungsverhalten zu erstellen. Diese Anforderung wird inbesondere dann kritisch, wenn die Authentisierung nicht ohnehin personeneindeutige Merkmale hervorbringt, wie es beispielsweise bei der Altersverifikation der Fall ist. Beim Tracking muss zwischen dem anbieterübergreifenden und dem anbieterspezifischen Tracking unterschieden werden.

Ziel des anbieterspezifischen Trackings ist es, einen Benutzer trotz Verwendung von uneindeutigen Merkmalen bei wiederholter Authentisierung wiederzuerkennen. Diese Wiedererkennung ist bei der eID-Funktion seitens des eID-Servers technisch möglich, wenn das, im Rahmen der Sperrlistenprüfung verwendete, für einen nPA eindeutige Merkmal vom eID-Server (unrechtmäßig) abgespeichert wird. So kann beispielsweise ein eID-Server, der im Rahmen der eID-Funktion lediglich die Volljährigkeit eines Benutzers prüft, den dabei verwendeten nPA in zwei unabhängigen Authentisierungen wiedererkennen. Dieses Risiko ist jedoch dadurch begrenzt, dass eID-Server das im Rahmen der Sperrlistenprüfung verwendete eindeutige Merkmal nicht speichern oder anderweitig verarbeiten dürfen. An dieser Stelle sei darauf hingewiesen, dass die Sperrlistenprüfung für eine verlässliche Online-Authentisierung unabdingbar ist.

Beim anbieterübergreifenden Tracking zielen mehrere Diensteanbieter darauf ab, anonyme Benutzerprofile untereinander zu vergleichen und diese auf eine einzige Identität des Benutzers zu reduzieren. Konkret bedeutet dies, dass mehrere Anbieter durch vereintes Wissen darauf schließen wollen, ob ein und der selbe Benutzer gleichzeitig Nutzer mehrerer Dienstleistungen ist. Die Nutzung der eID-Funktion verhindert ein solches Tracking dadurch, dass anonymisierte Daten diensteanbieterspezifisch erstellt werden und somit ein Vergleich über mehrere Diensteanbieter hinweg misslingt. So wird beispielsweise die so genannte Restricted Identification, eine anonyme Identifikation eines Benutzers/nPAs, spezifisch je Diensteanbieter erstellt. Dies erlaubt zwar die gewünschte Wiedererkennung des Benutzers bei ein und dem selben Diensteanbieter, verhindert jedoch erfolgreich das anbieterübergreifende Tracking.

Risikobetrachtung

Zusammenfassend kann festgehalten werden, dass ein anbieterübergreifendes Tracking im Kontext des nPA nicht möglich ist. Das anbieterspezifische Tracking ist zwar technisch möglich, verstößt jedoch gegen geltendes Recht.
Es stellt insbesondere dann ein Risiko dar, wenn durch personenbezogene Daten nicht ohnehin eine eindeutige Identität des Benutzers gebildet werden kann. Jedoch ist das anbieterspezifische Tracking im Kontext des nPA zum einen rechtlich untersagt, zum anderen stellen bestehende Tracking-Methoden ebenfalls Möglichkeiten zur Profilbildung dar. Dennoch sollte sich der Benutzer darüber bewusst sein, dass ein nPA vom eID-Server wiedererkannt werden kann, auch wenn keine personeneindeutigen Merkmale übermittelt werden (z.B. Altersverifikation). Das gesetzliche Verbot des Trackings muss hinsichtlich der Einhaltung überprüft werden!

3.4 Sicherheit des Kommunikationsmodells

Die Sicherheit des Kommunikationsmodells wurde im Rahmen dieser Studie untersucht, und es wurden bis auf eine Ausnahme in einer frühen Version der Spezifikation keine konzeptionellen Schwachstellen gefunden. Im Folgenden wird diese sowie eine weitere potentielle Schwachstelle beschrieben, die durch eine fehlerhafte Implementierung der damaligen Komponenten entstanden ist.

Das Kommunikationsprotokoll ist so gestaltet, dass es Angreifern weder ermöglicht wird, Authentisierungsergebnisse einzusehen, noch sie zu modifizieren. Die einzige konzeptionelle Schwachstelle des Kommunikationsmodells zum damaligen Untersuchungszeitpunkt betrifft das Session-Hijacking. Schafft es ein Angreifer, sich als Man-in-the-Middle zwischen Diensteanbieter und Benutzer zu bringen, so kann er zwar die Ergebnisse der Authentisierung nicht mitverfolgen, kann aber möglicherweise die vom Diensteanbieter erstellte Session nach erfolgreicher Authentisierung übernehmen und missbrauchen. Schwachstelle bei diesem Angriff ist das Unterlassen einer optionalen manuellen Verifikation der Identität des Diensteanbieters (z.B. anhand des SSL-Zertifikats). Um dieses Problem zu beseitigen, sollte die AusweisApp im Browser des Bürger-PCs die Gegenstelle mit einer im Berechtigungszertifikat hinterlegten Identität (z.B. Hash des SSL-Zertifikats) abgleichen. Somit wird die bisher optionale Prüfung des SSL-Zertifikats durch den Browser bzw. Benutzer durch eine automatische Prüfung in der AusweisApp ersetzt. Auf diese Weise werden Man-in-the-Middle-Angriffe und das einhergehende Session-Hijacking verhindert. Darüber hinaus werden durch diese Vorgehensweise Phishing-Angriffe, wie sie bei der Passwort-Authentisierung möglich sind, verhindert. Die entsprechenden Änderungen sind bereits in die Spezifikation (BSI

TR-03110, TR-03112 und TR-03127) übernommen und die Schwachstelle ist somit beseitigt.

Eine weitere gefundene Schwachstelle wurde aufgrund einer fehlerhaften Implementierung des damaligen eID-Servers in der Kommunikation mit dem Diensteanbieter aufgedeckt. Generell stehen für die Kommunikation zwischen dem eID-Server und dem Diensteanbieter nach BSI TR-03130 zwei verschiedene Alternativen für die Integration eines eID-Servers zur Verfügung. Der wesentliche Unterschied der Alternativen liegt in der Art und Weise, wie der eID-Server dem Diensteanbieter das Authentisierungsergebnis mitteilt. Jedoch unabhängig davon, ob das Authentisierungsergebnis direkt zwischen eID-Server und Diensteanbieter übermittelt wird, oder aber einen Umweg über den Bürger-PC nimmt, müssen die übermittelten Daten vom eID-Server signiert und so verschlüsselt werden, dass nur der Diensteanbieter selbst das Authentisierungsergebnis lesen kann. In der im Rahmen dieser Studie zur Verfügung gestellten Version war es möglich, die personenbezogenen Daten, die vom eID-Server aus dem nPA ausgelesen wurden, bei der Übergabe an den Diensteanbieter auf dem Bürger-PS zu manipulieren. Der Grund hierfür lag in einer bis zum derzeitigen Zeitpunkt unerkannten Abweichung der Implementierung von der Spezifikation. Eine Möglichkeit, derartige Schwachstellen zu vermeiden, liegt in der Zertifizierung von Implementierungen der Kommunikation zwischen dem eID-Server und dem Dienstanbieter.

Risikobetrachtung

Zusammenfassend kann festgehalten werden, dass die aktuelle Spezifikation des Kommunikationsmodells für die eID-Funktion keine Schwachstellen aufweist. Es ist notwendig, dass Implementierungen auf die Einhaltung der sicheren Konzepte genau geprüft werden.

4 Fazit

Zusammenfassend lässt sich feststellen, dass die eID-Funktion im Vergleich zur herkömmlichen Authentisierung mit Passwörtern ein höheres Sicherheitsniveau aufweist.

Der Grad des Sicherheit-Zuwachses ist dabei unmittelbar von der Vertrauenswürdigkeit des Bürger-PCs, der Aufklärung des Benutzers und der Wahl des Lesegeräts abhängig. Die Benutzer müssen Kompetenz entwickeln, um ihren Computer (PC, Notebook, Smartphone, …) sicher einzurichten, unabhängig vom neuen Personalausweis!

Da deshalb die Vertrauenswürdigkeit von vielen[1] PCs in Deutschland faktisch nicht sichergestellt ist, kann abschließend nur der Einsatz eines höherwertigen Lesegeräts (Standardleser, Komfortleser) empfohlen werden. Bei der Nutzung eines höherwertigen Lesegeräts bietet die eID-Funktion einen deutlich höheren Grad an Sicherheit, verglichen mit herkömmlichen Authentisierungsmethoden.

1 Über den genauen Anteil an infizierten PCs in Deutschland gibt es unterschiedliche Einschätzungen.