Die Beschäftigten der Bundesagentur für Arbeit wurden mit digitalen Dienstausweisen ausgestattet

Britta Heuberger*), Dagmar Lück-Schneider°)

*) Zentrale/IT 2
Bundesagentur für Arbeit
Regensburger Straße 104
90478 Nürnberg
britta.heuberger@arbeitsagentur.de

°) Fachbereich 3
Hochschule für Wirtschaft und Recht
Alt Friedrichsfelde 60
10315 Berlin
dagmar.lueck-schneider@hwr-berlin.de

Abstract: Die Bundesagentur für Arbeit (BA), größter Dienstleister am deutschen Arbeitsmarkt hat im Jahr 2008 ihre informationstechnologische Sicherheitsinfrastruktur ausgebaut. Damit wurde nicht nur das Sicherheitsniveau für etliche interne Prozesse erhöht, es wurden zugleich die technischen und rechtlichen Voraussetzungen für behördenübergreifende Vertragsgestaltungen geschaffen.
Die Beschäftigten erhielten in diesem Zusammenhang eine multifunktionale Dienstkarte. Neben drei Zertifikaten, die der Anmeldung an Systemen, der Verschlüsselung von Dokumenten und einer elektronischen Signatur dienen, umfasst sie auch Funktionen für Zeiterfassung und Zutrittskontrolle.
Der Beitrag beschreibt neben technologischen Grundlagen, welche neuen Infrastrukturmaßnahmen in der BA aufgebaut wurden, wesentliche Schritte des Projektvorgehens sowie einzelne Hintergründe getroffener Entscheidungen. Ferner wird darauf eingegangen, welche Prozesse hiervon bereits jetzt oder aber künftig profitieren werden.

1 Einleitung

Bereits im Jahr 2002 startete die Bundesagentur für Arbeit (BA), größter Dienstleister am deutschen Arbeitsmarkt, ein Projekt zur Einführung einer signaturgesetzkonformen „public key Infrastruktur“ (PKI). Eine solche Infrastruktur basiert auf privaten (geheimen) und öffentlichen Schlüsseln und setzt die Voraussetzungen für die Wahrung von Integrität, Authentizität und Vertraulichkeit. Ihre Errichtung erfordert eine Reihe recht aufwändiger Maßnahmen.

Die BA musste umfassende organisatorische und technologische Voraussetzungen schaffen. Als eine unter wenigen deutschen Einrichtungen verfügt sie hierfür inzwischen über ein eigenes *Trustcenter*. Dieses bildet einen hochverfügbaren und besonders gesi-

cherten physikalischen Rechenzentrumsbereich. Im ersten Halbjahr 2010 wird die Betriebsanzeige bei der Bundesnetzagentur (Deutschland) erfolgen.

Für die Entscheidung, ein eigenes Trustcenter aufzubauen sprach, die Anforderung vom damaligen Projekt „JobCard“, dass jeder Mitarbeiter einer abrufenden Stelle den Abruf bei der Zentralen Speicherstelle qualifiziert elektronisch signieren muss. In der BA wären davon ca. 40000 Mitarbeiter betroffen. Bei dieser Menge rechnete sich der Aufbau einer BA-eigenen signaturgesetzkonformen PKI.

Die BA hat ihre Beschäftigten im Jahr 2008 mit digitalen Dienstkarten (dDk) ausgestattet, die Funktionen zur Zeiterfassung, Zutrittskontrolle, zum Verschlüsseln und Signieren von Daten sowie zur Authentisierung gegenüber IT-Systemen bereitstellt.

Die Fertigstellung fällt dabei in eine Zeit, in der der Fokus im E-Government zunehmend auf durchgehend digitale Prozessketten gerichtet wird und liefert hierfür der BA technologische Voraussetzungen. Ferner trägt die PKI steigenden Ansprüchen an Datenschutz und Datensicherheit Rechnung.

2 Grundlagen

Sicherheitsinfrastruktur
Eine sichere Verschlüsselung über öffentliche und geheime Schlüssel in Rechnernetzen erfordert nicht nur das Vorhandensein entsprechender Verschlüsselungsverfahren, sondern vor allem auch besondere Vorkehrungen zur Generierung und Verteilung der öffentlichen und privaten Schlüssel. Deshalb spricht man auch von der Errichtung einer *Infrastruktur*.

Konzept der Datenverschlüsselung

Verschlüsselungsverfahren basieren auf den in Computern verwendeten Binärdarstellungen erfasster Zeichen, die prinzipiell als Vertreter natürlicher Zahlen interpretiert werden können und auf denen somit Rechenoperationen durchführbar sind. Mit privaten und öffentlichen Schlüsseln lassen sich derartige Rechenoperationen eindeutig festlegen.

Ein vorliegendes Zeichen kann nun mit Hilfe des privaten Schlüssels in eine andere Binärdarstellung umgerechnet werden und ist so verschlüsselt. Lässt man dann eine weitere Berechnung mit dem dazugehörigen öffentlichen Schlüssel durchführen, erhält man die Binärdarstellung des Ursprungszeichens zurück. Das gleiche gilt im Übrigen auch, wenn man zunächst den öffentlichen und anschließend den privaten Schlüssel anwendet.

Solche, auf zwei verschiedenen Schlüsseln beruhende Verschlüsselungen, werden auch *asymmetrisch* genannt. Das bei der BA konkret zum Einsatz kommende asymmetrische Verschlüsselungsverfahren ist das RSA-Verfahren, das nach den drei Mathematikern Rivest, Shamir und Adlemann benannt ist.

Sicherheit der Datenverschlüsselung

Für die in der BA zum Einsatz kommenden Schlüssel gelten Mindestgrößen. Dies soll Angriffe abwehren, die auf dem Versuch der Berechnung des geheimen Schlüssels ba-

sieren. Da derartige Berechnungen einzig und allein aufgrund des hierfür zu hohen Rechenaufwandes scheitern, ist die Haltbarkeit der Schlüssel wegen möglicher technologischer Weiterentwicklungen grundsätzlich begrenzt. Die Schlüssellänge, welche für die asymmetrische Verschlüsselung bei der digitalen Dienstkarte eingesetzt werden, beträgt 2048 bit. Nach der letzten Veröffentlichung über geeignete Algorithmen gilt diese Schlüssellänge bis ins Jahr 2015 als sicher.

Allerdings gibt es weitere Angriffsmöglichkeiten (vgl. [Ky96], S. 174). Hierzu zählen das Verfälschen öffentlicher Schlüssel oder auch das Klartext-Raten. Das Klartextraten kann beim Abfangen von Nachrichten eingesetzt werden, die ausschließlich einen bestimmten Empfänger erreichen sollen und deshalb mit dessen öffentlichem Schlüssel verschlüsselt wurden. In diesem Fall kann die vorliegende Codierung mit einer weiteren verglichen werden, die durch die Verschlüsselung eines geratenen Textes mit demselben öffentlichen Schlüssel gebildet wird. Das Raten wird so lange durchgeführt, bis man eine Übereinstimmung erzielt. Anschließend ist der Angreifer im Besitz der tatsächlichen Nachricht oder in der Lage, diese zu verfälschen.

Zertifizierungsstelle der Bundesagentur

Von eminenter Bedeutung ist, dass man Sicherheit darüber hat, dass der vorliegende öffentliche Schlüssel tatsächlich unverfälscht ist und auch wirklich zu der angegebenen Person gehört. In diesem Zusammenhang kommt dem Trustcenter – der zentralen Zertifizierungsinstanz – eine bedeutende Rolle zu. Es hat nicht nur die Aufgabe, die notwendigen Schlüsselpaare zu erzeugen, es muss auch die öffentlichen Schlüssel in einem Verzeichnisdienst publizieren. Eine wesentliche Grundlage hierfür sind *Zertifikate.* Diese sind mit behördlich ausgestellten, fälschungssicheren Ausweisdokumenten vergleichbar, welche spezifische Kennzahlen mit einer konkreten Person verknüpfen und damit einem bestimmten Zweck dienen, etwa der Identifikation. So verknüpft auch das Zertifikat einen speziellen öffentlichen Schlüssel mit einem Zertifikatsinhaber und definiert den Zweck, für den der Schlüssel zugelassen ist. Jedes Zertifikat kann über den Verzeichnisdienst des Trustcenters elektronisch abgefragt werden. Die interne Zertifizierungsstelle muss umfassende gesetzliche Bestimmungen einhalten und höchstmöglichen Schutz der zur Signierung der Zertifikate eingesetzten privaten Schlüssel und der erhobenen Antragsdaten gewährleisten.

Auf die Fälschungssicherheit der lediglich elektronisch lesbaren Zertifikate wird weiter unten noch eingegangen.

Persönliche digitale Dienstkarte

Die Beschäftigten der BA erhalten ihre persönlichen, geheimen Schlüssel und die Zertifikate über die dDks, deren Erstellung und Verteilung an hohe organisatorische Auflagen gebunden ist, damit sie keiner falschen Person zugeordnet werden können. Die dDk selbst ist durch eine PIN zusätzlich geschützt und der geheime Schlüssel lässt sich nicht einmal durch die besitzende Person auslesen. Auch die auf den Schlüsseln basierenden Berechnungsverfahren sind auf den dDks gespeichert.

In einem ersten Rollout wurden ca 80.000 an Computerarbeitsplätzen arbeitende Beschäftigte ausgestattet . Das hierfür eigens initiierte Projekt sah folgende Schritte vor:

- eine bundesweite Einrichtung von sogenannten Lokalen Registrierungsstellen (LRA) in ausgewählten Dienststellen der BA,
- die Erstellung eines gut koordinierten Zeitplans, wann in welchen LRAs Registrierungen und Kartenausgaben statt fanden,
- eine Schulung des Personals, das in den LRAs eingesetzt wurde.

3 Einsatzfelder

Prinzipiell kann man mit Hilfe der beschriebenen Verschlüsselung zugleich eine unversehrte Datenübertragung und die Authentizität der sendenden Person organisieren. Dazu muss lediglich der gesamte Text zeichenweise mit dem geheimen Schlüssel verschlüsselt abgeschickt werden. Auf Empfangsseite würde mit dem öffentlichen Schlüssel alles entschlüsselt. *In der Praxis wird aber anders verfahren*. Oft ist das mit einem ausgesprochen hohen Rechenaufwand verbundene Ver- und Entschlüsseln der insgesamt übertragenen Daten nämlich gar nicht erforderlich.

So wird, wenn lediglich die Unversehrtheit des Textes und die Authentizität der sendenden Person sichergestellt werden soll – also eine Verschlüsselung nicht zwingend ist –, wie folgt vorgegangen: Aus der als Zahlenfolge interpretierbaren Zeichenfolge des zu übertragenen Textes wird eine Prüfzahl gebildet. Nur diese wird mit dem geheimen Schlüssel der absendenden Person codiert. Text, codierte Prüfzahl und das Zertifikat für den passenden öffentlichen Schlüssel werden dann gemeinsam verschickt. Auf der Empfangsseite wird die codierte Prüfzahl entschlüsselt und mit einer erneut aus dem Text berechneten verglichen. Bei Gleichheit ist der Text vertrauenswürdig, da das Zertifikat die korrekte Personengebundenheit des öffentlichen Schlüssels sichert. Ein auf diese Weise elektronisch signiertes ausgetauschtes Dokument ist besser gegen Verfälschungen geschützt als ein handschriftlich gezeichnetes Dokument.

Selbstverständlich kann eine Textverschlüsselung zusätzlich erfolgen. Weil die asymmetrische Verschlüsselung jedoch mit sehr hohem Rechenaufwand verbunden ist und eine Textverschlüsselung das Klartext-Raten erleichtern würde, wird hierzu weniger rechenintensiv *symmetrisch* verschlüsselt (vgl. [FHW01], S. 93). Dabei nutzen sendende wie empfangende Person gleiche, allerdings stets neu generierte und anderen gegenüber geheime Schlüssel. Das Verfahren ist genauso sicher, *da der generierte Schlüssel asymmetrisch ausgetauscht wird*.

Zertifikatstypen

Da Zertifikate zweckgebunden ausgestellt werden, erhalten die BA-Beschäftigten für die verschiedenen Vorgänge drei Zertifikate mit unterschiedlichen Schlüsselpaaren (Authentisierungs-, Verschlüsselungs- und Signaturzertifikat).

Zur Authentisierung an Computersystemen wird ein mit dem geheimen Schlüssel codierter Zugangscode übertragen und mit dem öffentlichen Schlüssel des Authentisierungszertifikat geprüft.

Die Fälschungssicherheit der Zertifikate beruht nun darauf, dass auch das Trustcenter für jeden der verschiedenen Zertifikatstypen ein Schlüsselpaar unterhält. Jedes durch das

Trustcenter der BA verteilte Zertifikat ist ein mit dem entsprechenden geheimen Schlüssel des Trustcenters signiertes Dokument. Auf den dDks der Beschäftigten sind zu deren schnellen Lesbarkeit die entsprechenden öffentlichen Schlüssel der Zertifizierungsinstanz zusätzlich mit aufgebracht.

4 Weitreichende neue Handlungsspielräume

Bereits realisierte Anwendungen

Gegenwärtig werden die bereits verteilten dDks für Zutritt und Zeiterfassung sowie zur Anmeldung an den Computersystemen genutzt.

Schriftverkehr

Zwischen Schlüsselinhabern können zukünftig E-Mails signiert und auch verschlüsselt ausgetauscht werden. Mit der Betriebsanzeige des Trustcenters werden Dokumente, die mit der dDk signiert wurden, nach deutschem Signaturgesetz rechtsverbindlich sein. Sie stellen damit eine juristisch akzeptierte Alternative zu herkömmlich schriftlich unterzeichneten Dokumenten dar.[1]

Ferner ist die BA dabei, Schriftverkehr und Aktenhaltung *vollständig* auf elektronische Basis umzustellen. Der Digitalisierung folgen die Archivierung der zuvor zu signierenden Dokumente sowie die informationstechnologische prozessbezogene an keinen bestimmten Standort oder Sachbearbeiter gebundene Bereitstellung derselben. Die Einsparung immenser Mengen an Archivflächen ist ein positiver Nebeneffekt.

Maschinenzertifikate

Das Trustcenter eröffnet der BA auch die eigene Erstellung von Maschinenzertifikaten. Diese können dazu eingesetzt werden, dass bestimmte Software ausschließlich auf mit Zertifikaten versehenen Rechnern genutzt werden kann. Ebenso lässt sich die Kommunikation zwischen Hardwarekomponenten auf diese Weise absichern.

Arbeitgebernachweise über Entgeltzahlungen

Auch für das seit 1.1.2010 angelaufene Verfahren Elena könnte die neu aufgebaute PKI der BA noch eine wesentliche Rolle. übernehmen. So hat das Bundeskabinett beschlossen, dass Arbeitgebernachweise über Entgeltzahlungen, die Personen bei Beantragung von Leistungen, etwa von Arbeitslosengeld I[2], von Bundeserziehungsgeld und Wohngeld vorlegen müssen, bis Ende 2011 elektronisch erfolgen sollen.

Dazu sind von Arbeitgeberseite monatlich Einkommensdaten in signierter und verschlüsselter Form an die Deutsche Rentenversicherung Bund (DRVS) zu senden. Für Personen, die entsprechende Leistungen beantragen, ist vorgesehen, die Antragsabwicklung durch elektronische Geschäftsprozesse zu automatisieren und zu beschleunigen. Für

[1] Ausnahmen sind ausdrücklich im Gesetz benannt.
[2] Arbeitslosengeld I ist von der Höhe des letzten Einkommens abhängig. Um es zu erhalten, muss u. a. eine Anwartschaftszeit aus sozialversicherungspflichtigen Entgeltverhältnissen erfüllt sein.

die Zugriffe auf die Datensätze der Antragstellenden sind elektronische Signaturen zur Autorisierung notwendig.

Mobile Arbeitsplätze

Zertifikate können auch der Erzielung eines höheren Sicherheitsstandards bei der Nutzung von mobilen Arbeitsplätzen dienen. Neben der generell üblichen Authentisierung des Zugriffs auf diese Geräte, werden in der BA auf solchen Geräten Daten grundsätzlich verschlüsselt abgelegt, damit bei einem möglichen Verlust Missbrauchsmöglichkeiten weiter reduziert werden. Analoges gilt für Speichersticks. Bislang wird hierfür aber die PKI nicht herangezogen.

5 Ausblick

Darüber hinaus ist damit zu rechnen, dass mit weiter zunehmender Internetnutzung eine medienbruchfreie Prozessabwicklung in den nächsten Jahren in Europa und weltweit immer mehr an Bedeutung gewinnen wird. Das gilt für die behördeninterne Zusammenarbeit genauso wie für Geschäfts- und Kundenbeziehungen mit Unternehmen wie auch mit Bürgern. Auch letztere werden künftig zunehmend über digitale Zertifikate verfügen. In diese Richtung zielen in Deutschland Möglichkeiten auf Gesundheitskarten und Personalausweisen.

Literaturverzeichnis

[BA08] Spezifische Informationen zur Bundesagentur für Arbeit basieren auf Auskünften des Zertifizierungsdiensts der BA sowie der Unterlage: PKI – dDk. Workshop für Multiplikatoren. Unterrichtsmaterialien des IT-Systemhaus der BA. Nürnberg, 2008

[FHW01] Fuhrberg, K.; Häger, D.; Wolf, S.: Internet Sicherheit. Browser, Firewalls und Verschlüsselung. Carl Hanser: München, Wien, 2001.

[Ky96] Kyas, O.: Sicherheit im Internet. Risikoanalyse – Strategien – Firewalls. Datacom, Bergheim, 1996.

[LÜ09] Lück-Schneider, D. (2009). Ausbau der Sicherheitsinfrastruktur der Bundesagentur für Arbeit in Deutschland. eGov Präsenz 1/2009 (Online-Zeitschrift), S. 79-81.