RUHR-UNIVERSITÄT BOCHUM

AMTLICHE BEKANNTMACHUNGEN

DER
RUHR-UNIVERSITÄT BOCHUM

Nr. 606 30. Mai 2005

Dienstvereinbarung über Einführung und Einsatz einer Bedienstetenchipkarte

vom 29. April 2005

→ UNIVERSITÄTSSTRASSE 150 · D-44801 BOCHUM, GERMANY

Dienstvereinbarung
über Einführung und Einsatz
einer Bedienstetenchipkarte
vom 29. April 2005

zwischen dem

Personalrat
der Ruhr-Universität Bochum
vertreten durch den Vorsitzenden

und der

Ruhr-Universität Bochum
vertreten durch den Kanzler

sowie zwischen dem

Personalrat
der Medizinischen Einrichtungen
der Ruhr-Universität Bochum
vertreten durch den Vorsitzenden

und der

Ruhr-Universität Bochum
vertreten durch den Kanzler

sowie zwischen dem

Personalrat
der wissenschaftlich/künstlerisch Beschäftigten
der Ruhr-Universität Bochum
vertreten durch den Vorsitzenden

und der

Ruhr-Universität Bochum
vertreten durch den Rektor

sowie zwischen dem

Hauptpersonalrat der wissenschaftlich/künstlerisch Beschäftigten beim
Ministerium für Wissenschaft und Forschung
des Landes Nordrhein-Westfalen

als Personalrat
der wissenschaftlich Beschäftigten
der Medizinischen Einrichtungen
der Ruhr-Universität Bochum
vertreten durch den Vorsitzenden

und der

Ruhr-Universität Bochum
vertreten durch den Rektor

wird gemäß § 6 der Rahmendienstvereinbarung über Planung, Einführung, Betrieb und Erweiterung/Änderung von Systemen der Informationstechnik (IT-Rahmen-DV) vom 26.5.04 und § 70 Personalvertretungsgesetz für das Land Nordrhein - Westfalen (Landespersonalvertretungsgesetz - LPVG -) folgende Einzeldienstvereinbarung abgeschlossen:

§ 1
Geltungsbereich

Diese Dienstvereinbarung gilt für den Einsatz von Bedienstetenchipkarten für Beschäftigte der Ruhr-Universität Bochum im Sinne der §§ 5 und 110 LPVG NW sowie für den Betrieb der dazu notwendigen Verwaltungssoftware. Die Ruhr-Universität Bochum wird die Regelungen dieser Dienstvereinbarung auch für die Beschäftigten anwenden, die nicht von Personalräten vertreten werden.

§ 2
Begriffsbestimmungen

(1) Unter Verarbeitung wird gem. DSG NW die Erhebung (das Beschaffen von Daten), Speicherung, Veränderung, Übermittlung (das Bekanntgeben gespeicherter Daten an einen Dritten), Sperrung (das Verhindern der weiteren Verarbeitung), Löschung (das Unkenntlichmachen der gespeicherten Daten) sowie Nutzung von Personaldaten verstanden.

(2) Eine Digitale Signatur ist ein mit einem privaten Signaturschlüssel erzeugtes Siegel zu digitalen Daten, das mit Hilfe eines zugehörigen öffentlichen Schlüssels, der mit einem Signaturschlüssel-Zertifikat einer Zertifizierungsstelle versehen ist, den Inhaber des Signaturschlüssels und die Unverfälschtheit der Daten erkennen lässt.

(3) Authentifizierung ist die Feststellung der Identität einer Person mit Hilfe der Digitalen Signatur.

§ 3
Zweckbestimmungen

(1) Anfallende Daten im Sinne dieser Dienstvereinbarung dürfen gem. § 3 der IT-Rahmen-DV nur für die vereinbarten Zwecke verarbeitet werden.

(2) Der Zweck der Bedienstetenchipkarte ist der Einsatz

a) als Bedienstetenausweis mit folgenden optischen Merkmalen: Lichtbild, Name, Vorname, Titel, eindeutige Nummer (RUB-ID)

b) zur Authentifizierung und Digitalen Signatur bei als sicherheitskritisch eingestuften IT-Systemen und Dokumenten. In der Anlage 1 werden die dafür auf der Karte gespeicherten Daten aufgeführt. Die Einstufung eines IT-Systems als sicherheitskritisch wird in der jeweiligen Dienstvereinbarung vorgenommen, die nach § 6 Abs. 2 der Rahmen-DV für jedes System vor Nutzung abzuschließen ist.

   Die Nutzung der Bedienstetenchipkarte für weitere Zwecke wird im gemeinsamen IT-Auschuss mit dem Ziel der Einigung verhandelt und bedarf der Zustimmung durch die Personalräte. Dies gilt auch für Nutzungen, die den Bediensteten auf freiwilliger Basis angeboten werden. Die Möglichkeit einer anonymen Nutzung ist der Authentifizierung und der Digitalen Signatur jeweils vorzuziehen.

(3) Die zum Betrieb der Bedienstetenchipkarte gespeicherten Daten der Beschäftigten werden nur verwendet zum Zweck der eindeutigen Authentifizierung beim Zugang zu sicherheitskritischen IT-Systemen und beim Einsatz der Digitalen Signatur im Sinne des SigG und der entsprechenden SigV. Die RUB-ID dient auch der Identifizierung in anderen DV-Systemen.

(4) Die bei der Nutzung der Bedienstetenchipkarte anfallenden Daten dürfen nicht zu Zwecken einer Verhaltens- oder Leistungskontrolle oder zu Zwecken einer Ermittlung von Grundlagen für dienstliche Beurteilungen, Disziplinarmaßnahmen oder als Grundlage für die Feststellung des Gesundheitszustandes verarbeitet werden. Konkrete Regelungen für den Umfang und den weiteren Umgang mit diesen Daten werden unter Beachtung des Grundsatzes der Datensparsamkeit in den gesonderten Dienstvereinbarungen vorgenommenen, die nach § 6 Abs. 2 der Rahmen-DV für jedes System vor Nutzung abzuschließen sind.

§ 4
Systemdokumentation

(1) Beim Zugang zu als sicherheitskritisch eingestuften IT-Systemen und Dokumenten gemäß §3(2)(b) dieser Dienstvereinbarung erfolgt die Identifikation des Authentifizierungsschlüssel-Inhabers über Besitz (Bedienstetenchipkarte) und Wissen (PIN). Die Erzeugung der Authentifizierungsschlüssel erfolgt auf der Bedienstetenchipkarte selbst. Für die Erzeugung und Anwendung der Authentifizierungsschlüssel gilt die Signaturverordnung sinngemäß, die eingesetzten Algorithmen und zugehörigen Parameter müssen nach SigV geeignet sein.

(2) Die Identifikation des Karteninhabers/der Karteninhaberin bei Anwendung des Signaturschlüssels für die Digitale Signatur erfolgt über Besitz (Bedienstetenchipkarte) und Wissen (PIN). Die Erzeugung der Signaturschlüssel erfolgt auf der Bedienstetenchipkarte. Für die Funktion der Digitalen Signatur muß die Bedienstetenchipkarte die technischen Anforderungen des Signaturgesetzes SigG und der Signaturverordnung SigV erfüllen.

(3) Die Signierfunktion der Bedienstetenchipkarte darf nur im Innenverhältnis der Ruhr-Universität Bochum angewandt werden und die Signierfunktion ist auf dienstliche Zwecke beschränkt.

(4) In den Anlagen zu dieser Dienstvereinbarung werden Software und technischer Umfang des DV-Systems, Regelungen zum Datenschutz und zur Datensicherung, Festlegungen von Datenfeldern, Standardauswertungen und Zugriffsberechtigungen beschrieben. Die Anlagen sind Bestandteil dieser Dienstvereinbarung und konkretisieren sie.

Im Einzelnen sind folgende Anlagen beigefügt:

Anlage 1 Technische Dokumentation der Bedienstetenchipkarte

Anlage 2 Richtlinien für die Ausstellung und den Betrieb der Bedienstetenchipkarte

Anlage 3 Antrag auf Erstellung einer Bedienstetenchipkarte

Anlage 4 Verpflichtungserklärung und Merkblatt

Anlage 5 Liste der Zugriffsberechtigten zur Verwaltungssoftware

Anlage 6 Ergebnis der Vorabkontrolle des behördliche Datenschutzbeauftragten (bDSB)

§ 5
Generierung und Ausgabe der Bedienstetenchipkarte

(1) Zuständig für die Generierung der Bedienstetenchipkarte ist das „Dezernat für Informations- und Kommunikationsdienste, Studierendenservice“ (Certification Authority / CA). Zuständig für die Datenerfassung und die Ausgabe der Bedienstetenchipkarte ist das „Dezernat für Personalangelegenheiten“ (Registration Authority /RA). (vgl. Anlage 2)

(2) Die Generierung der Karte erfolgt offline. Es erfolgt keine Verknüpfung der vom Personaldezernat eingesetzten Personaldatensoftware mit der zur Generierung der Bedienstetenchipkarte eingesetzten Software. Nach Erstellung der Bedienstetenchipkarte werden die zur Erstellung erforderlichen Daten gelöscht.

(3) Die Karte wird nur persönlich auf Antrag ausgegeben. Die Karte ist kostenlos. Der Verlust der Bedienstetenchipkarte ist unverzüglich dem Personaldezernat anzuzeigen.

§ 6
Rechte und Pflichten der Beschäftigten

(1) Jede/r Beschäftigte ist berechtigt, eine Bedienstetenchipkarte zu erhalten. Die Ausgabe der Karte erfolgt auf freiwilliger Basis unter schriftlicher Einwilligung des/der Beschäftigten. Die Karte ist nicht übertragbar.

(2) Jede/r Beschäftigte erhält auf Wunsch schriftliche Informationen über alle auf der Bedienstetenchipkarte und in der Verwaltungssoftware zu ihrer/seiner Person aktuell gespeicherten Daten. Dazu werden alle genutzten Datenfelder mit ihrem aktuellen Inhalt, dem Verwendungszweck jedes Datenfeldes und die vorgesehene Speicherdauer angegeben. Die Dienststelle stellt ein System bereit, das das Auslesen der Daten und Datenfelder auf der Bedienstetenchipkarte an jedem entsprechend ausgestatteten PC ermöglicht.

(3) Personelle Maßnahmen, die auf Informationen beruhen, die unter Verletzung dieser Dienstvereinbarung gewonnen wurden, sind unwirksam und unverzüglich rückgängig zu machen.

(4) Für die Funktion als Bedienstetenausweis können Mitarbeiter/Mitarbeiterinnen alternativ zur Bedienstetenchipkarte eine Karte ohne Chip erhalten.

§ 7
Aus- und Weiterbildung

(1) Die Beschäftigten, die mit der Bedienstetenchipkarte arbeiten, werden ausreichend unterrichtet. Schulungen zu den Funktionen der Bedienstetenchipkarte werden im Rahmen des Weiterbildungsprogramms der RUB angeboten.

(2) Mitglieder der Personalräte sind berechtigt, zur Wahrnehmung ihrer Aufgaben aus dieser Vereinbarung an Weiterbildungsveranstaltungen zu den hier geregelten Themen teilzunehmen. Die Kosten trägt die Dienststelle.

§ 8
Rechte der Personalräte

(1) Die Personalräte und der behördliche Datenschutzbeauftragte (bDSB) haben das Recht, die Einhaltung dieser Dienstvereinbarung zu überprüfen und Stichproben zu machen. Zu diesem Zweck ist ihnen der erforderliche Zugang zu allen Stellen zu gewähren, an denen Daten im Zusammenhang mit der Nutzung der Bedienstetenchipkarte erhoben, verarbeitet und/oder genutzt werden.

(2) Die Personalräte können auf allen Ebenen des Systems (Betriebssysteme, Datenbanksysteme, Kommunikationssysteme, Protokolle) die vereinbarte Verwendung und die Einhaltung des Datenschutzes kontrollieren. Dazu können sie auch in alle vom System gespeicherten Daten und Protokolle Einblick nehmen. Alle zum System gehörenden Handbücher und Systemunterlagen einschließlich der Vorabkontrolle sind ihnen auf Wunsch in der aktuellen Version zeitweise zu überlassen.

(3) Die Personalräte haben das Recht, alle Personen, die mit der Verarbeitung und Nutzung von Daten des Systems beschäftigt sind, bezüglich der rechtmäßigen, vereinbarten Verwendung zu befragen. Diese sind gegenüber den Personalräten zur wahrheitsgemäßen Auskunft berechtigt und verpflichtet. Auf Verlangen haben sie Funktionen auf der Ebene der Betriebssysteme und Datenbankanwendungen zu Prüfzwecken durchzuführen. Auf Wunsch werden für die Personalräte Ausdrucke erzeugt.

§ 9
Datenschutz

(1) Die Dienststelle stellt sicher, dass die organisatorischen und technischen Maßnahmen zur Umsetzung der im Landesdatenschutzgesetz geforderten Ziele getroffen werden.

(2) Der Kreis der zugriffsberechtigten Personen für die Verwaltungssoftware wird unter Beachtung der Zweckbestimmung festgelegt und in Anlage 5 dokumentiert. Veränderungen werden den Personalräten mitgeteilt.

§ 10
Schlussbestimmungen

Diese Vereinbarung tritt am Tage ihrer Unterzeichnung in Kraft. Sie kann von jeder Seite mit sechsmonatiger Frist gekündigt werden. In diesem Fall wirkt sie bis zum Abschluss einer neuen Vereinbarung insgesamt nach.

Sollte sich ein Teil der Vereinbarung als unwirksam herausstellen, gelten die anderen Teile weiterhin.

Bochum, den 29.04.2005

für die Dienststelle:

Ruhr-Universität Bochum	**Ruhr-Universität Bochum**
Der Rektor	**Der Kanzler**
Prof. Dr.-Ing. G. Wagner	**G. Möller**

für die Personalräte:

für den Personalrat	**für den Personalrat der Medizinischen Einrichtungen**
Der Vorsitzende	**Der Vorsitzende**
für den Personalrat der wissenschaftlich/ künstlerisch Beschäftigten	**Hauptpersonalrat der wissenschaftlich/ künstlerisch Beschäftigten beim Ministerium für Wissenschaft und Forschung des Landes Nordrhein-Westfalen**
	für den Personalrat der wissenschaftlichen Beschäftigten der Medizinischen Einrichtungen
Der Vorsitzende	**Der Vorsitzende**

Protokollnotiz zur
Dienstvereinbarung über Einführung und Einsatz
einer Bedienstetenchipkarte

Bei Bruch des Sicherheitssystems der Bedienstetenchipkarte bzw. bei Versagen der Sicherheitsmaßnahmen im Zuge der Verwendung der Bedienstetenchipkarte entstehen der/dem Beschäftigten keinerlei Nachteile. Das bezieht sich auf die Bedienstetenchipkarte selbst, die für den Betrieb dazu notwendigen Verwaltungssoftware und die durch Nutzung der Bedienstetenchipkarte generierten Verwaltungsvorgänge.

Im Zweifelsfall obliegt es der Dienststelle, den Beweis zu führen, ob der/die Beschäftigte vorsätzlich oder grobfahrlässig gehandelt hat.

Wenn die/der Beschäftigte befürchtet, dass die Sicherheitsmaßnahmen versagt haben bzw. ein Bruch des Sicherheitssystems vorliegt, ist die Bedienstetenchipkarte unverzüglich zu sperren (siehe Anlage 2 der Dienstvereinbarung).

Anlage 1: Technische Dokumentation der Bedienstetenchipkarte

1. Daten der Bedienstetenchipkarte

1.1 Daten zur Antragstellung

Folgende Daten werden für die Antragstellung benötigt:

- Anrede
- Titel *(im strengen Sinne)*
- Vorname
- zweiter Vorname *(opt.)*
- Nachname
- Geburtsdatum
- Institution
- Entweder: Gebäude, Ebene, Raum *alternativ Anschrift*: Strasse PLZ Ort
  Oder: RZ loginID
- Telefon dienstlich
- Foto

1.2 Daten zur Kartenproduktion

Folgende Daten werden zur **Kartenproduktion** benötigt:

- RUB-ID *(eindeutige Kundennummer)*
- Titel
- Nachname
- Vorname
- Foto
- PIN

Folgende Daten werden nach der Kartenproduktion gelöscht:

- Foto
- PIN

1.3 Daten auf der Kartenoberfläche

Folgende Daten werden auf die **Kartenoberfläche** gedruckt:

- RUB-ID
- Titel *durch Inhaber wählbar*
- Nachname
- Vorname
- Zweiter Vorname *(wenn durch Inhaber gewünscht)*
- Foto der Mitarbeiterin bzw. des Mitarbeiters

1.4 Daten auf dem Chip

Frei auslesbar sind die folgenden Karten-Daten:

- Kartenseriennummer
- Herausgeber
- Kartentyp

Neben den Schlüsseldaten werden folgende personenbezogene Daten auf dem **Chip** gespeichert:

- RUB-ID
- Titel *(wenn durch Inhaber/Inhaberin gewünscht)*
- Nachname
- Vorname
- zweiter Vorname *(wenn durch Inhaber/Inhaberin gewünscht)*

Diese Daten sind Bestandteil des Zertifikats, das auf dem Chip gespeichert ist.

Das **Zertifikat** besteht aus der Signatur einer Zeichenkette in festgelegtem Format. Diese Zeichenkette enthält folgende Einträge:

- Version des Zertifikats
- Seriennummer des Zertifikats
- Informationen über den Algorithmus des Zertifikats
- Herausgeber
- Gültigkeit
- Empfänger
- Informationen über den Algorithmus des Öffentlichen Schlüssels (Empfänger)
- Öffentlicher Schlüssel des Empfängers

z.B.:

Version 10
Seriennummer des Zertifikats 004000017C0901659D9C793F
Information über den Algorithmus des Zertifikats Algorithmus: RSAWITHSHA1 Padding: PKCS#1 Schlüssellänge: 2048
Herausgeber Land: DE Organisation: RUHR-UNIVERSITAET BOCHUM Abteilung: DEZERNAT6 Seriennummer: 6 gebräuchlicher Name : RUHR-UNIVERSITAET BOCHUM
Gültigkeit: gültig von: 20030930170917 gültig bis: 20530930170917 Zeitzone: GMT+1:00
Empfänger Land: DE Organisationsname : RUHR-UNIVERSITAET BOCHUM Abteilung: Seriennummer: 108803911810 Titel: Prof. Dr. gebräuchlicher Name: Testname,Testvorname
Information über den Algorithmus des Öffentlichen Schlüssel des Empfängers Algorithmus: RSAWITHSHA1 Padding: PKCS#1 Schlüssellänge: 1024
Öffentlicher Schlüssel des Empfängers Modulus: B0D7FF477A842FA4CC9F232D20DE3A2D02E9B4035B7499232B67C9DBD1D96218749877C08FA11A70675FE3EB6947B9 916983A026FAB3FDB5071B1091718BEBB5A16108E77CFD44090563CBCB7AE4A75CE7BAFB2ACE96150B3FE6EAEFAFB F47EAC1F1B4E455D0F70675F02D7AE09524D158E2A076D623638E22886E2EB5DFF7B7 Exponent: 010001

Die für Bedienstete der Ruhr-Universität Bochum ausgestellten Zertifikate können für *fortgeschrittene Signaturen* im Sinne des Signaturgesetzes (SigG) innerhalb der Ruhr-Universität verwendet werden.

1.5 Daten in der Verwaltungssoftware

Folgende Daten werden in der **Verwaltungssoftware** gespeichert:
Kontaktdaten:

- Anrede
- Titel *(im strengen Sinne)*
- Vorname
- zweiter Vorname *(wenn durch Inhaber/Inhaberin gewünscht)*
- Nachname
- Geburtsdatum
- Institution
- Entweder: Gebäude, Ebene, Raum *alternativ Anschrift*: Strasse, PLZ, Ort
  Oder: RZ loginID
- Telefon

Zur Verwaltung von kryptographischen Schlüsseln ist eine spezielle Infrastruktur erforderlich. Diese wird als *Public Key Infrastructure* (PKI) bezeichnet. Eine PKI stellt jene Informationen zur Verfügung, die aktuelle Informationen über den Gültigkeitszustand eines Zertifikats geben.

Die PKI der Ruhr-Universität ist nur für an der RUB ausgestellte Chipkarten zu nutzen. In der PKI sind alle öffentlichen Daten, die zur Chipkarte gehören, hinterlegt. Dazu gehören auch Sperrinformationen, die bei jedem Versuch der Authentifizierung überprüft werden.

Daten für den **Betrieb der PKI**:

Für das **Zertifikat**:

CERTSERIALNR	Seriennummer des Zertifikats
CARDSN	Seriennummer der Karte
SUBJECTID	RUB-ID
SUBJECTNAME	Nachname
SUBJECTFIRSTNAME	Vorname
CAKEYVERSION	Versionsnummer des RUB CA-Zertifikates
CERTIFICATE	Persönliches Zertifikat
CERTVERSION	Versionsnummer des persönlichen Zertifikates
CERTALGO	Algorithmus der Zertifikatserstellung
CERTPADDING	Verfahrensvorschrift zur Zertifikatserstellung
CERTKEYLENGTH	Schlüssellänge des Zertifikates
ISSUERCOUNTRYNAME	Land des Ausstellers (DE)
ISSUERORGNAME	Organisation des Austeller (RUB)
ISSUERORGUNIT	Abteilung unterhalb der Organisation
ISSUERSERIALNR	Eindeutige Nummer des Austellers
ISSUERCOMMONNAME	Wie ISSUERORGNAME
VALIDSINCE	Gültig ab
VALIDUNTIL	Gültig bis
VALIDTIMEZONE	Zeitzone
SUBJECTCOUNTRYNAME	Land des Inhabers
SUBJECTORGNAME	Organisation des Inhabers
SUBJECTORGUNIT	Abteilung unterhalb der Organisation
SUBJECTTITLE	Titel
SUBJECTCOMMONNAME	Wie SUBJECTORGNAME
PKALGO	Algorithmus zur Erstellung des privaten Schlüssels
PKPADDING	Verfahrensvorschrift zur Schlüsselerzeugung
PKKEYLENGTH	Länge des privaten Schlüssels
SUBJECTPKMOD	Ergibt mit SUBJECTPKEXP den öffentlichen Schlüssel
SUBJECTPKEXP	s.o.
LOCKDATE	Sperrdatum

Für die **Karte**:

CARDSN	Seriennummer der Karte
TIMESTAMP	Erstellungszeitpunkt
CARDDELIVERYNR	Liefernummer der Karte
PRODUKTIONSPLATZID	Nummer des Produktionsplatzes
LOCKDATE	Sperrdatum
SUBJECTID	RUB-ID
SUBJECTNAME	Name
SUBJECTFIRSTNAME	Vorname
PRODCODE	Produktionscode
PRINTREASON	Grund der Erstellung (Erstausstellung, Chip defekt, Sonstiges)
CHIPTYPE_ID	Typ des Chips
CARDPURPOSE_ID	Verwendungszweck (Mitarbeiter, Studierender)

2. Erstellung der Bedienstetenchipkarte

Gemäß den in Anlage 2 dargestellten Richtlinien zur Ausstellung von Bedienstetenchipkarten wird ein technisches Sicherheitskonzept umgesetzt, das in der folgenden Graphik dargestellt ist:

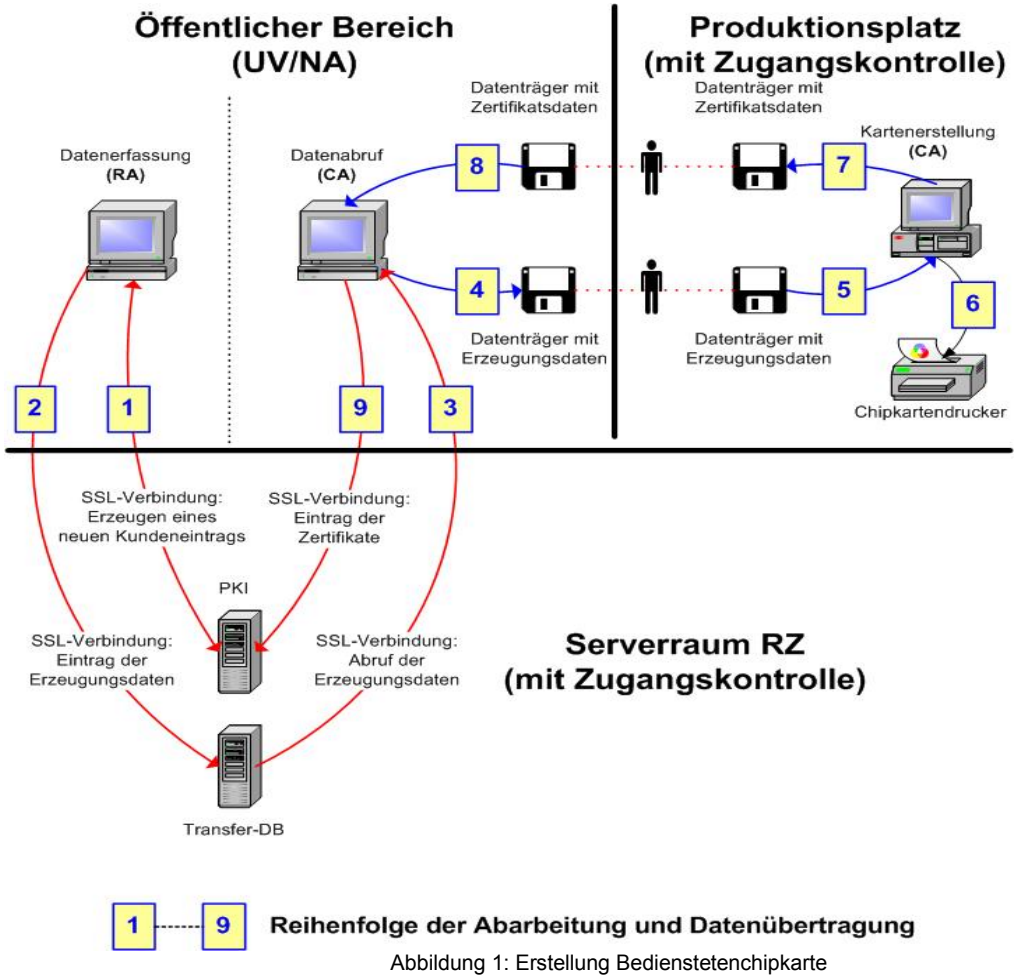

Abbildung 1: Erstellung Bedienstetenchipkarte

3. Betrieb der Bedienstetenchipkarte

Für den Betrieb der Bedienstetenchipkarte sind spezielle Software-Komponenten erforderlich, die sich zum einen auf die Administrations- und Prüfkomponente beziehen, zum anderen auf die Signierfunktion der Bedienstetenchipkarte.

3.1 Administrations- und Prüfkomponente

Die Administrations- und Prüfkomponente dient der Überprüfung der korrekten Funktion sowie dem Setzen einer neuen PIN nach dreimaliger Falscheingabe. Diese Komponente wird in gleicher Form auch bei den Studierendenkarten eingesetzt und enthält deshalb auch Anzeigemöglichkeiten für Felder, welche auf den Bedienstetenkarten nicht vorhanden sind.

Es gibt zwei Ansichten: eine für die frei zugänglichen Daten *(Abbildung 2)* und eine für die PIN-geschützten Daten des Zertifikats *(Abbildung 3)*.

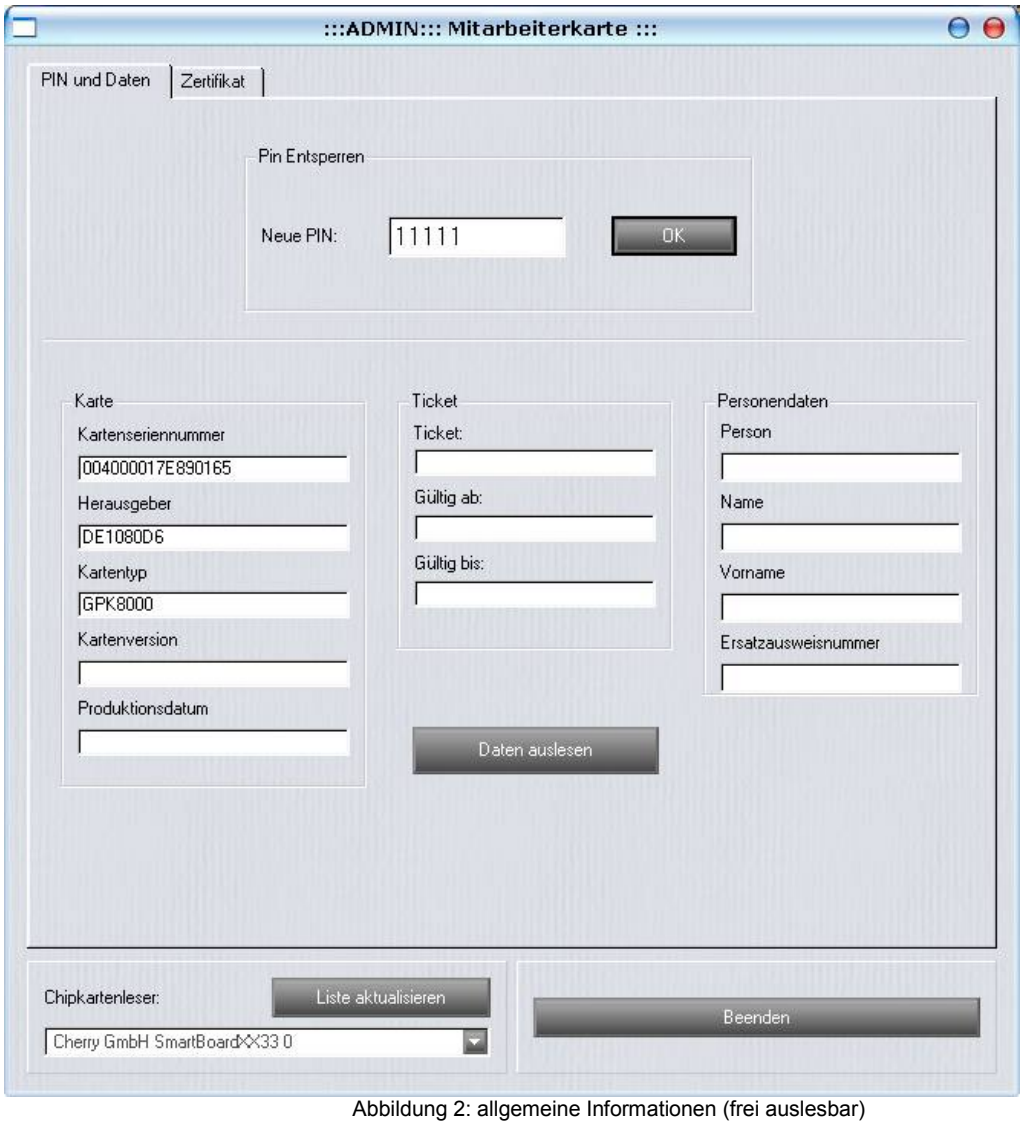

Abbildung 2: allgemeine Informationen (frei auslesbar)

Beim Setzen einer neuen PIN wird diese im Klartext angezeigt. Die auf der Abbildung leeren Felder sind auf der Bedienstetenkarte nicht vorhanden.

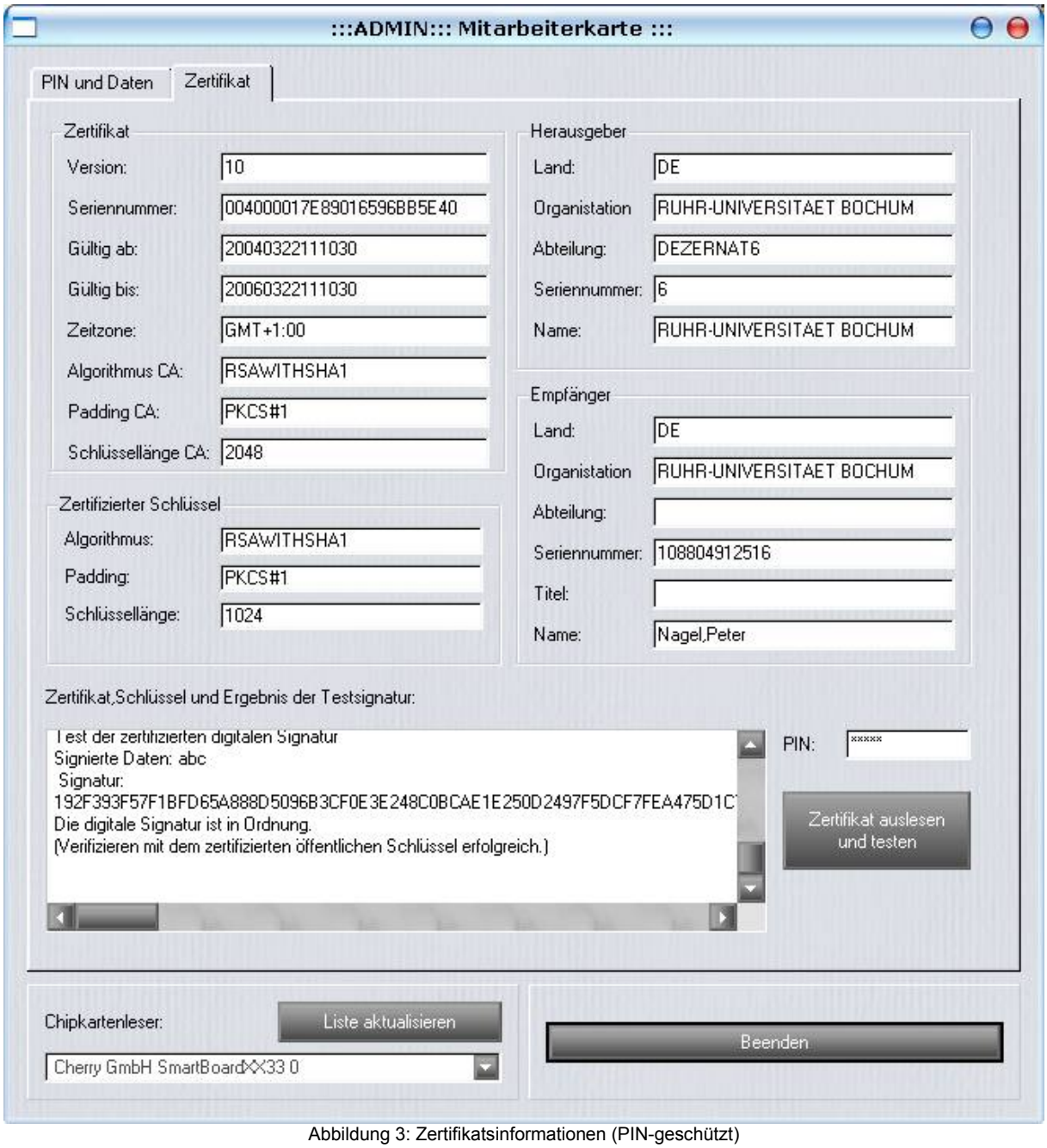

Abbildung 3: Zertifikatsinformationen (PIN-geschützt)

Um die Zertifikatsdaten auszulesen und die Gültigkeit des Zertifikats sowie die Signaturfunktion zu testen, muss der Inhaber die PIN verdeckt eingeben.

3.2 Signierfunktion der Bedienstetenchipkarte

Im Folgenden werden die Sicherheitseigenschaften der Signierfunktion und die Grundlagen der Digitalen Signatur dargestellt.

3.2.1 Sicherheitseigenschaften

Für die Signierfunktion erfüllen die Bedienstetenchipkarten die folgenden Sicherheitsanforderungen:

Der Signierschlüssel wird auf dem Chip erzeugt, so dass der private Schlüssel niemals auslesbar ist und nur vom Chipkarten-Betriebssystem benutzt werden kann.
Die digitale Signatur wird auf dem Chip durchgeführt und ist durch eine fünfstellige PIN geschützt. Diese PIN wird bei der Erstausstellung zufällig bestimmt, muss aber anschließend vom Inhaber unverzüglich geändert werden. Wird die PIN dreimal hintereinander falsch eingegeben, wird die Karte gesperrt.
Der Kryptoprozessor des Chips ist in der Lage, die jeweils aktuell als sicher erachteten Krypto-Algorithmen selbständig durchzuführen.

3.2.2 Digitale Signatur

Grundlage der digitalen Signatur ist ein asymmetrisches Verschlüsselungsverfahren. Bei der Erstellung jeder Chipkarte werden zwei Schlüssel generiert. Ein so genannter privater Schlüssel und ein öffentlicher Schlüssel. Der private Schlüssel wird von dem auf der Chipkarte vorhandenen Prozessor selbst generiert und verlässt diese niemals. Der öffentliche Schlüssel wird in die PKI transferiert und steht dort potenziell jedem zur Überprüfung zur Verfügung. Wird etwas mit dem einen Schlüssel verschlüsselt, so kann es nur mit dem dazugehörigen anderen Schlüssel wieder sichtbar gemacht werden.

Bei der digitalen Signatur macht man sich das zunutze. Zunächst wird durch ein mathematisches Verfahren ein so genannter Hash-Wert berechnet, der den Fingerabdruck eines zu signierenden Dokumentes darstellt. Die verwendeten Verfahren stellen sicher, dass Änderungen am Dokument zu nicht vorhersagbaren Änderungen des Hash-Wertes führen. Deshalb ist es praktisch unmöglich, zu einem vorgegebenen Hash-Wert ein beliebiges sinnvolles Dokument zu erzeugen. Eine Änderung eines bestehenden Dokuments ohne Änderung des Hash-Wertes ist deshalb ausgeschlossen.

Dieser Hash-Wert wird dann zusammen mit Daten über den Benutzer sowie den Zeitpunkt der Signatur mit dem privaten Schlüssel der Chipkarte des Benutzers verschlüsselt. Das Ergebnis ist die digitale Signatur. Will man nun diese digitale Signatur auf ihre Echtheit hin überprüfen, benötigt man zunächst wieder das Dokument sowie die Daten über den (angeblichen) Unterzeichner und den Zeitpunkt der Signatur. Über das Dokument wird wiederum mit gleichen Verfahren der Hash-Wert gebildet. Jetzt wird mit dem öffentlichen Schlüssel des Benutzers, der sich in der PKI befindet, die digitale Signatur entschlüsselt. Stimmt das Ergebnis mit dem ermittelten Hash-Wert sowie den weiteren Daten überein, so ist die digitale Signatur gültig. Unterscheiden sich die Hash-Werte oder andere Rahmendaten, so ist keine Verifizierung möglich.

Die jeweilige Anwendung, die eine digitale Signatur nutzen will, ist dafür verantwortlich, alle notwendigen Daten (Dokument, Benutzer, Datum, Signatur) in geeigneter Form zu speichern.

3.2.3 Authentifizierung und Digitale Signatur

Die Bedienstetenchipkarte bietet auf Grund ihrer Krypto-Fähigkeit eine Möglichkeit der sicheren Authentifizierung. Eine solche Identitätsprüfung läuft folgendermaßen ab:

Der Klientenrechner nimmt Verbindung mit dem Authentifizierungsserver auf und teilt ihm mit, dass sich jemand authentifizieren möchte. Dazu schickt er dem Server ein Identifikations-Merkmal: die RUB-ID.
Der Server erzeugt einen zufälligen Wert und schickt ihn dem Klienten.
Der Klient lässt diesen Zufallswert von der Karte digital signieren. Damit dies möglich ist, muss der Benutzer seine PIN eingeben.
Die erzeugte Signatur wird an den Server zurückgeschickt.
Der Server prüft mit Hilfe des öffentlichen Schlüssels der entsprechenden RUB-ID die Korrektheit der Signatur. Den öffentlichen Schlüssel bekommt er aus der PKI, der Schlüsselverwaltung.
Jetzt gibt der Server das Ergebnis der Prüfung (gültig/ungültig) zurück.

Anlage 2: Richtlinien für die Ausstellung und den Betrieb der Bedienstetenchipkarte

1. Richtlinien für die Ausstellung von Bedienstetenchipkarten an der RUB

Für die Ausstellung von Bedienstetenchipkarten wird eine organisatorische Hierarchie gebildet. Zertifikate werden ausschließlich von der *Certification Authority* (CA) der Ruhr-Universität Bochum ausgestellt. Diese CA wird durch das Dezernat für Information und Kommunikation, Studierendenservice (Dezernat 6) betrieben. Getrennt von der CA arbeitet eine *Registration Authority* (RA), die durch das Dezernat für Personalangelegenheiten (Dezernat 3) betrieben wird.
Zur Verwaltung von kryptographischen Schlüsseln ist eine spezielle Infrastruktur erforderlich. Diese wird als *Public Key Infrastructure* (PKI) bezeichnet und ermöglicht nach dem derzeitigen Stand der Technik, dass die Authentifizierung, Identifizierung, Vertraulichkeit und Glaubhaftmachung von elektronischen Daten sichergestellt wird. Eine PKI stellt unter anderem jene Informationen zur Verfügung, die aktuelle Informationen über den Gültigkeitszustand eines Zertifikats geben. Diese PKI wird vom Rechenzentrum der RUB betrieben.

1.1 Aufgaben der Registration Authority (RA)

Aufgaben der RA sind:

- Entgegennahme der Anträge für eine Bedienstetenchipkarte mit Lichtbild für den Ausweisdruck.
- Die Identitätsüberprüfung der Antragsteller (durch Personalausweis, sofern nicht persönlich bekannt).
- Die Prüfung, ob es sich um Bedienstete der RUB handelt (der Zertifizierungswunsch also zulässig ist).
- Die Erzeugung der Zertifizierungsaufträge an die CA und die sichere Ablage der Daten in der Transfer-Datenbank.
- Die Entgegennahme der erstellten Bedienstetenausweise und Aushändigung an die Antragsteller, zusammen mit der zugehörigen PIN, die im verschlossenen Umschlag übergeben wird. Der Empfang und die Kenntnisnahme der zugehörigen Informationen muss durch eigenhändige Unterschrift bestätigt werden.
- Entsperrung der PIN nach Falscheingabe.

1.2 Aufgaben der Certification Authority (CA)

Die CA hat die Aufgabe, anhand der Zertifizierungsaufträge,

- die Bedienstetenausweise auf sichere Weise im Offline-Verfahren zu erstellen,
- die zugehörigen Informationen und Briefe mit der Erst-PIN zu erstellen,
- den erzeugten öffentlichen Schlüssel mit den zugehörigen Zertifikatsdaten in die PKI der Ruhr-Universität Bochum einzupflegen.

Da die Sicherheit der CA essentiell für die Sicherheit und Vertrauenswürdigkeit der Signaturen ist, gelten folgende Anforderungen:

- Die CA besteht aus einem Rechner mit Chipkarten-Drucksystem und separatem Kartenlesegerät, welcher keine physikalische Verbindung zu Datennetzwerken gleich welcher Art besitzt. Dieser Arbeitsplatz befindet sich in einem nicht frei zugänglichen Raum.
- Auf diesem Rechner ist außer dem Betriebssystem nur die zum Betrieb der CA notwendige Software installiert.
- Die Zertifikatsanträge gelangen in Form von Dateien auf einem externen Datenträger auf den CA-Rechner. Diese enthalten ausschließlich die für die Zertifikatserstellung notwendigen Daten sowie jeweils ein Bild für den Kartenaufdruck.
- Nach Erstellung einer Bedienstetenchipkarte werden die PKI-Daten ebenfalls in eine Datei geschrieben, um anschließend in die PKI-Datenbank eingelesen zu werden. Diese Datei gelangt über einen externen Datenträger zum PKI-Rechner.
- Die Daten auf dem externen Datenträger sind nach Nutzung zu löschen, beim Umgang mit dem externen Datenträger ist die Datensicherheit zu gewährleisten.
- Der CA-Schlüssel wurde auf einer abgezählten Menge von SmartCards (Masterkarten) gespeichert, die ebenfalls mit einer fünfstelligen PIN versehen sind. Dieser Schlüssel wurde auf einem isolierten Rechner mit neuem Betriebssystem erstellt. Die Masterkarten werden in einem Tresor der CA aufbewahrt und nur zum Zweck der Zertifikats-/Chipkartenerstellung entnommen, die PIN für die Masterkarten wird an einem davon getrennten verschlossenen Ort aufbewahrt.

1.3 Übergabe der Bedienstetenchipkarte an den Empfänger durch die RA

Nach Erstellen der Chipkarte kann diese zusammen mit dem verschlossenen PIN-Brief in der RA abgeholt werden und zwar ausschließlich persönlich von dem/der Antragsteller/in.

Des weiteren wird das Merkblatt (siehe Anlage 4) ausgehändigt, welches die Bedeutung der Bedienstetenchipkarte und damit verbunden die Grundzüge von Public-Key-Verfahren erläutert.

Darüber hinaus werden dem Antragsteller/der Antragstellerin alle mit der Nutzung seiner/ihrer RUB-eMail-Adresse erforderlichen Informationen überreicht.

Dabei ist der Empfang sowie die Kenntnisnahme der Verhaltensregeln durch Unterschrift zu bestätigen:

- Die Karte ist nicht übertragbar.
- Die Karte ist sorgfältig zu behandeln.
- Die ausgegebene PIN muss unverzüglich auf einen selbst gewählten Wert geändert werden.
- Die jeweilige PIN darf an niemanden weitergegeben werden.
- Die RA ist umgehend zu informieren, wenn eine Karte verloren oder gefunden wurde.
- Alle Verpflichtungen, die mit der Nutzung der RUB-eMail-Adresse verbunden sind, sind einzuhalten.

2. Richtlinien für den Betrieb von Bedienstetenchipkarten an der RUB

2.1 Gültigkeit der Zertifikate

Die Benutzer-Zertifikate haben eine Gültigkeit von 50 Jahren ausgehend vom Ausstellungsdatum; das CA-Zertifikat hat eine Gültigkeitsdauer von 100 Jahren.
Wenn der Master-Schlüssel aus sicherheitstechnischen Gründen gesperrt werden muss, verlieren auch die damit ausgestellten Zertifikate ihre Gültigkeit.

Zwischenzeitlich ausgeschiedene Bedienstete können ihr Zertifikat nicht erneuern lassen.
Mit Ausscheiden eines Bediensteten aus der RUB wird sein Zertifikat gesperrt. Die Bedienstetenchipkarte ist zurückzugeben.

2.2 Sperrung von Zertifikaten

Die Benutzer haben das Recht, jederzeit ihr bestehendes Zertifikat bei der Ausgabestelle (RA) sperren zu lassen und ein neues Zertifikat zu beantragen. Die Ausgabestelle muss sich durch geeignete Maßnahmen davon überzeugen, dass der Sperrwunsch vom Zertifikatsinhaber selbst stammt bzw. autorisiert ist. Bei Kartenverlust ist der Benutzer verpflichtet, dies umgehend der Ausgabestelle mitzuteilen und die Sperrung des Zertifikats zu veranlassen. Dies ist auch über die Leitwarte der Ruhr-Universität, die immer erreichbar ist, möglich.

Bei der Sperrung werden die Karte und das darauf befindliche Zertifikat in der PKI als gesperrt vermerkt (mit Sperrdatum und -zeit). Wird die Karte nach einer Verlustmeldung wiedergefunden, kann, falls noch keine neue Chipkarte ausgestellt wurde, ein neues Zertifikat auf diese Karte aufgebracht werden. Hierzu muss die Karte bei der RA abgegeben werden, die diese zum Aufbringen eines neuen Zertifikats an die CA weiterleitet, dabei ist der Ablauf wie bei der Erstausstellung organisiert.

Die Reaktivierung eines gesperrten Zertifikats ist in keinem Fall möglich.

2.3 Sperrung einer Bedienstetenchipkarte

Wird die PIN dreimal hintereinander falsch eingegeben, ist der Zugriff auf die Karte gesperrt, nicht aber das Zertifikat. In diesem Fall kann die Karte von der RA durch Setzen einer neuen PIN wieder entsperrt werden. Dazu muss sich der/die Inhaber/in der Karte mittels seines/ ihres Personalausweises ausweisen. Die ausgegebene PIN ist unverzüglich auf einen selbst gewählten Wert zu ändern.

2.4 Missbrauch

Bei Verstoß gegen die Verpflichtungen gemäß Anlage 4 (Missbrauch) wird durch die RA in der Verwaltungssoftware der Dienst gesperrt, bei dem der Missbrauch bekannt wurde. Darüber hinaus muss die PIN neu gesetzt werden und ein neues Zertifikat generiert werden.

Anlage 3: Antrag auf Erstellung einer Bedienstetenchipkarte

Antrag auf Erstellung einer Bedienstetenchipkarte

Ruhr-Universität Bochum

Dezernat für Personalangelegenheiten (Dez. 3)
UV 2 / 271

44780 Bochum

Anrede: _____
Titel (optional): _____
Nachname: _____
Vorname: _____
2. Vorname (optional): _____
Geburtsdatum: _____

(Lichtbild)

Ich beantrage die Erstellung einer Bedienstetenchipkarte als Bedienstetenausweis und zur Authentifizierung und Signierung bei sicherheitskritischen IT-Systemen.

Informationen im Zusammenhang mit der Bedienstetenchipkarte können entweder per Post oder per eMail zugesandt werden.

☒ Ich wünsche, über meine persönliche RUB-eMail-Adresse informiert zu werden.

- ☐ Ich besitze noch keine persönliche Zugriffsidentifikation („RUB-LoginID“) des Rechenzentrums der RUB. Es wird eine RUB-LoginID für mich erzeugt. Diese RUB-LoginID sowie das Erstpasswort werden mir bei Abholung der Chipkarte zusammen mit den Nutzungsbestimmungen des Rechenzentrums ausgehändigt.
- ☒ Meine persönliche Zugriffsidentifikation des Rechenzentrums der RUB („RUB-LoginID“)lautet: _____

☐ Ich wünsche, über meine folgende Dienstanschrift informiert zu werden:

Institut: _____

Gebäude: _____
Etage: _____
Raum: _____
Telefon (intern): _____

oder

Straße: _____
PLZ Ort: _____
Telefon: _____

Mit der Speicherung der oben genannten personenbezogenen Daten in der vom Rechenzentrum gepflegten Kundendatenbank sowie der für den Einsatz meiner Bediensteten-Chipkarte erforderlichen Bereitstellung des öffentlichen Schlüssels und des Zertifikats in der vom Rechenzentrum dafür betriebenen Public Key Infrastructure (PKI) bin ich einverstanden.

Mir wird zugesichert, dass oben genannte personenbezogene Daten nur zu Zulassungs- und/oder Benachrichtigungszwecken benutzt und spätestens 3 Monate nach meinem Ausscheiden gelöscht werden. Meine Zertifikatsdaten und öffentlichen Schlüssel werden gemäß den Regelungen des Signatur-Gesetzes archiviert.

Mein Lichtbild wird digitalisiert nur zum Zweck der Chipkarten-Erstellung genutzt und anschließend gelöscht. Es wird mir bei Aushändigung meiner Bediensteten-Chipkarte wieder zurückgegeben.

Mir ist bekannt, dass die Ausgabe und die Nutzung dieser Bedienstetenchipkarte gemäß § 29a Datenschutzgesetz NRW freiwillig ist und mit meinem Einverständnis erfolgt. Die Bedienstetenchipkarte ist nicht übertragbar, ein Verlust der Karte ist unverzüglich bei der Ausgabestelle zu melden.

_____ _____
Datum Unterschrift

Anlage 4-Verpflichtungserklärung und Merkblatt

Verpflichtung

Ich, _____
Vorname Zuname

erkläre, dass ich bei der Benutzung der Bedienstetenchipkarte folgende Regeln anerkenne und sie einhalten werde:

- Die Bedienstetenchipkarte darf nicht an andere übertragen werden.
- Die Bedienstetenchipkarte ist sorgfältig zu behandeln und zweckgemäß einzusetzen.
- Die ausgegebene PIN ist unverzüglich auf einen selbst gewählten Wert zu ändern.
- Die jeweilige PIN darf an niemanden weitergegeben werden.
- Es ist umgehend die Ausgabestelle beim Dezernat für Personalangelegenheiten zu informieren, wenn eine Bedienstetenchipkarte verloren oder gefunden wurde. Dies ist auch über die Leitwarte der Ruhr-Universität möglich.
- Beim Ausscheiden aus dem Dienst der RUB muss die Bedienstetenchipkarte zurückgeben werden.

Das Merkblatt zur Bedienstetenchipkarte habe ich zur Kenntnis genommen. Auf meine Rechte nach § 5 sowie §§ 18, 29a des Datenschutzgesetzes NRW bin ich hingewiesen worden.

_____ _____
Datum Unterschrift

Merkblatt „Die Bedienstetenchipkarte der RUB“

Sie haben heute eine neue Bedienstetenchipkarte erhalten, die auch die Funktion eines Bedienstetenausweises hat. Diese zeigt Ihr Bild, Ihren Namen und eine eindeutige Nummer. Darüber hinaus enthält sie einen Chip mit einem Prozessor, welcher in der Lage ist, selbständig komplexe Verschlüsselungsverfahren durchzuführen. Mit dem Chip ist es möglich, Ihre Bedienstetenchipkarte für digitale Signaturen, das heißt „elektronische Unterschriften“ zu benutzen.

Öffentlicher Schlüssel, Privater Schlüssel, Zertifikat

Es gibt zwei grundsätzlich verschiedene Verfahren zur Verschlüsselung von Daten: symmetrische und asymmetrische Verfahren. Beim symmetrischen Verfahren exisitert nur ein Schlüssel, mit dem die Daten sowohl verschlüsselt als auch entschlüsselt werden. Beim asymmetrischen Verfahren existieren zwei verschiedene, aber zusammengehörende Schlüssel. Daten, welche mit einem der beiden Schlüssel verschlüsselt wurden, lassen sich nur mit dem anderen Schlüssel wieder entschlüsseln. Daraus resultieren die sogenannten „Public Key“-Verfahren. Einer der beiden Schlüssel bleibt geheim und steht nur dem Besitzer zur Verfügung („privater Schlüssel“), der zweite wird öffentlich gemacht und steht allen Interessierten zur Verfügung („öffentlicher Schlüssel“). Daten, die mit einem öffentlichen Schlüssel verschlüsselt werden, lassen sich nur mit dem zugehörenden privaten Schlüssel des Besitzers wieder entschlüsseln. Daten, die mit einem privaten Schlüssel verschlüsselt werden, sind nur mit dem passenden öffentlichen Schlüssel zu entschlüsseln. So läßt sich sichergestellen, dass die Daten vom Besitzer des privaten Schlüssels stammen und nicht verändert wurden.
Dieser Mechanismus ist die Grundlage der digitalen Signatur. Bei der Erstellung jeder Chipkarte werden diese zwei Schlüssel (privat und öffentlich) von dem auf der Chipkarte vorhandenen Prozessor generiert. Der private Schlüssel kann nicht ausgelesen werden und steht ausschließlich auf der Chipkarte für Ver-/Entschlüsselungen zur Verfügung. Der öffentliche Schlüssel wird in den zentralen, öffentlichen Verzeichnisdienst der RUB transferiert. Dabei muss aber gewährleistet werden, dass der Schlüssel echt ist. Dies erreicht man dadurch, dass der öffentliche Schlüssel von der RUB als Aussteller der Karte mit dem gleichen mathematischen Verfahren signiert wird und damit ein sogenanntes Zertifikat ausgestellt wird. Dieses Zertifikat wird neben dem öffentlichen Schlüssel in der Public Key Infrastructure (PKI) der RUB abgelegt.

Digitale Signatur

Die Verschlüsselung eines kompletten Dokuments mit Hilfe der Chipkarte würde sehr lange dauern. Deshalb wird zur Absicherung von größeren Datenmengen ein anderer Weg gegangen: die digitale Signatur. Hierfür wird zunächst ein Hash-Wert (eine Art Prüfsumme oder Fingerabdruck des Dokuments) ermittelt. Die Besonderheit dieses Hash-Werts liegt darin, dass es nicht möglich ist, zu einem vorgegebenen Hash-Wert ein beliebiges sinnvolles Dokument zu erzeugen. Es ist deshalb praktisch unmöglich, innerhalb eines Dokuments Veränderungen so vorzunehmen, dass sich der Hash-Wert nicht ändert. Deshalb ist ein Dokument durch seinen Hash-Wert zweifelsfrei zu identifizieren.
Dieser Hash-Wert wird nun zusammen mit einigen Rahmendaten (z.B. Datum der Signatur, Name des Signierenden sowie einige technisch notwendige Daten) mit dem privaten Schlüssel der Chipkarte des Benutzers verschlüsselt. Das Ergebnis ist die digitale Signatur.
Will man nun diese digitale Signatur auf ihre Echtheit hin überprüfen, benötigt man zunächst wieder das Dokument. Über dieses Dokument wird wiederum mit dem gleichen Verfahren der Hash-Wert gebildet. Jetzt wird mit dem öffentlichen Schlüssel des Benutzers, der sich in der PKI befindet, die digitale Signatur entschlüsselt. Stimmt das Ergebnis mit dem ermittelten Hash-Wert überein, so ist die digitale Signatur gültig. Unterscheiden sich die Hash-Werte, so ist die digitale Signatur ungültig.

Sichere Authentifizierung

Zur sicheren Authentifizierung wird der Mechanismus der digitalen Signatur verwendet, das Verfahren nennt sich „Challenge-Response-Verfahren“. Vereinfacht dargestellt läuft es so ab: die Applikation, welche sich von der (angeblichen) Identität eines Benutzers überzeugen möchte, sendet dem Klientenprogramm einen Zufallswert („Challenge“). Der Klient lässt diesen Wert von der Chipkarte verschlüsseln und sendet das Ergebnis zurück („Response“). Die Applikation entschlüsselt diese Antwort mit dem öffentlichen Schlüssel des (angeblichen) Benutzers und prüft, ob der von ihr geschickte Zufallswert herauskommt. Falls ja, wurde der Benutzer eindeutig identifiziert und damit authentifiziert.

Umgang mit der Bedienstetenchipkarte

Ihre Bediensten- Chipkarte ist nicht übertragbar. Zur Benutzung der Karte ist eine fünfstellige PIN erforderlich, die Ihnen bei der Kartenausgabe ausgehändigt wurde. Die Erst-PIN müssen Sie unverzüglich ändern. Weitere Änderungen der PIN sind jederzeit selbstständig möglich. Bei Ausscheiden aus dem Dienst der RUB ist die Karte bei der Ausgabestelle wieder zurückzugeben.
Hinweis: Sollten Daten mit einem öffentlichen Schlüssel verschlüsselt werden, ist das zugehörige Originaldokument gesondert aufzubewahren, da bei Verlust der Bedienstetenchipkarte die Daten nicht wiederhergestellt werden können.

Verlust der Bediensteten-Chipkarte

Einen Verlust der Karte müssen Sie unverzüglich bei der Ausgabestelle melden, damit Missbrauch verhindert werden kann.
Dies ist auch über die Leitwarte der RUB möglich. Die Karte und das darauf befindliche Zertifikat werden gesperrt. Im Regelfall erhalten Sie unverzüglich eine neue Bedienstetenchipkarte.
Wenn vor Ausgabe einer neuen Karte die alte wiedergefunden wird, wird ein neues Zertifikat aufgebracht.

Dienstvereinbarung zur Bediensteten-Chipkarte

Die Dienstvereinbarung zur Bediensteten-Chipkarte finden Sie im Intranet der RUB unter
www.rub.de/Bedienstetenchipkarte
Dort finden Sie auch die Information, wie Sie einsehen können, welche personenbezogenen bzw. –beziehbaren Daten über Sie im Zusammenhang mit der Nutzung der Bedienstetenchipkarte gespeichert sind. Bitte beachten Sie, dass nach Rückgabe Ihrer Bedienstetenchipkarte diese Daten nicht alle sofort gelöscht werden können. Ihre Zertifikatsdaten werden weiterhin vorgehalten, damit es möglich ist, früher von Ihnen ausgestellte digitale Signaturen zu überprüfen. Die Speicherung Ihrer Zertifikatsdaten entspricht der maximalen Gültigkeitsdauer des Zertifikats von 50 Jahren ab Datum der Ausstellung.

Ihre Kontakt-Adresse

Informationen, die für Sie im Zusammenhang mit der Nutzung der Bedienstetenchipkarte wichtig sind, werden Ihnen über Ihre RUB-eMail-Adresse oder, falls Sie es auf Ihrem Antrag entsprechend vermerkt haben, per Post an Ihre Dienstanschrift gesendet.

Ausgabestelle

Dezernat für Personalangelegenheiten, Sachgebiet 3.1, UV 2 / 271,Tel.: 25676

Leitwarte

Tel: 23333

Auszug aus dem Datenschutzgesetz NRW:

§ 5
Rechte der betroffenen Person

Jeder hat nach Maßgabe dieses Gesetzes ein Recht auf

1. Auskunft, Einsichtnahme (§ 18),
2. Widerspruch aus besonderem Grund (§ 4 Abs. 5),
3. Unterrichtung (§§ 12 Abs. 2, 13 Abs. 2 Satz 2, 16 Abs. 1 Satz 2 und 3),
4. Berichtigung, Sperrung oder Löschung (§ 19),
5. Schadensersatz (§ 20),
6. Anrufung des Landesbeauftragten für Datenschutz und Informationsfreiheit (§ 25 Abs. 1),
7. Auskunft aus dem beim zuständigen behördlichen Datenschutzbeauftragten geführten Verfahrensverzeichnis (§ 8).

Diese Rechte können auch durch die Einwilligung der betroffenen Person nicht ausgeschlossen oder beschränkt werden.

§ 18
Auskunft, Einsichtnahme

(1) Der betroffenen Person ist von der verantwortlichen Stelle auf Antrag Auskunft zu erteilen über

1. die zu ihrer Person verarbeiteten Daten,
2. den Zweck und die Rechtsgrundlage der Verarbeitung,
3. die Herkunft der Daten und die Empfänger von Übermittlungen sowie
4. die allgemeinen technischen Bedingungen der automatisierten Verarbeitung der zur eigenen Person verarbeiteten Daten.

Dies gilt nicht für personenbezogene Daten, die ausschließlich zu Zwecken der Datensicherung oder der Datenschutzkontrolle gespeichert sind.

(2) Auskunft oder Einsichtnahme sind zu gewähren, soweit die betroffene Person Angaben macht, die das Auffinden der Daten mit angemessenem Aufwand ermöglichen. Auskunftserteilungen und Einsichtnahme sind gebührenfrei, die Erstattung von Auslagen kann verlangt werden.

(3) Die Verpflichtung zur Auskunftserteilung oder zur Gewährung der Einsichtnahme entfällt, soweit

a. dies die ordnungsgemäße Erfüllung der Aufgaben der verantwortlichen Stelle erheblich gefährden würde,
b. dies die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde,
c. die personenbezogenen Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder wegen der berechtigten Interessen einer dritten Person geheimgehalten werden müssen.

(4) Einer Begründung für die Auskunftsverweigerung bedarf es nur dann nicht, wenn durch die Mitteilung der Gründe der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. In diesem Fall sind die wesentlichen Gründe für die Entscheidung aufzuzeichnen.

(5) Bezieht sich die Auskunftserteilung oder die Einsichtnahme auf die Herkunft personenbezogener Daten von Behörden des Verfassungsschutzes, der Staatsanwaltschaft und der Polizei, von Landesfinanzbehörden, soweit diese personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung speichern, sowie von den in § 19 Abs. 3 Bundesdatenschutzgesetz genannten Behörden, ist sie nur mit Zustimmung dieser Stellen zulässig. Gleiches gilt für die Übermittlung personenbezogener Daten an diese Behörden. Für die Versagung der Zustimmung gelten, soweit dieses Gesetz auf die genannten Behörden Anwendung findet, die Absätze 3 und 4 entsprechend.

(6) Werden Auskunft oder Einsichtnahme nicht gewährt, ist die betroffene Person darauf hinzuweisen, dass sie sich an den Landesbeauftragten für Datenschutz und Informationsfreiheit wenden kann.

§ 29 a
Mobile personenbezogene Datenverarbeitungssysteme

(1) Informationstechnische Systeme zum Einsatz in automatisierten Verfahren, die an die Betroffenen ausgegeben werden und die über eine von der ausgebenden Stelle oder Dritten bereitgestellte Schnittstelle Daten automatisiert austauschen können (mobile Datenverarbeitungssysteme, z. B. Chipkarten), dürfen nur mit Einwilligung der betroffenen Person nach ihrer vorherigen umfassenden Aufklärung eingesetzt werden.

(2) Für die Betroffenen muss jederzeit erkennbar sein,

1. ob und durch wen Datenverarbeitungsvorgänge auf dem mobilen Datenverarbeitungssystem oder durch dieses veranlasst stattfinden,
2. welche personenbezogenen Daten der betroffenen Person verarbeitet werden und
3. welcher Verarbeitungsvorgang im Einzelnen abläuft oder angestoßen wird.

Den Betroffenen müssen die Informationen nach Nummer 2 und 3 auf ihren Wunsch auch schriftlich in Papierform mitgeteilt werden.

(3) Die Betroffenen sind bei der Ausgabe des mobilen Datenverarbeitungssystems über die ihnen nach § 5 zustehenden Rechte aufzuklären. Sofern zur Wahrnehmung der Informationsrechte besondere Geräte oder Einrichtungen erforderlich sind, hat die ausgebende Stelle dafür Sorge zu tragen, dass diese in angemessenem Umfang zur Verfügung stehen.

Anlage 5: Liste der Zugriffsberechtigten zur Verwaltungssoftware

Zugriff zu dem Verwaltungsprogramm der RA haben Mitarbeiter des *Dezernats für Personalangelegenheiten*.

Zugriff zu dem Verwaltungsprogramm der CA haben Mitarbeiter des *Dezernats für Information und Kommunikation, Studierendenservice.*

Die Namen dieser Mitarbeiter sind den Personalräten bekannt. Wenn sich eine Zuständigkeit ändert, wird den Personalräten eine aktualisierte Version der Anlage 5 zur Mitbestimmung vorgelegt.

Anlage 6: Ergebnis der Vorabkontrolle des bDSB

Begründetes Ergebnis der Vorabkontrolle
nach §8 DSG NW:
Bediensteten-Chipkarte

1. Systemeigenschaften

Bei der Bediensteten-Chipkarte handelt es sich um eine Krypto-Chipkarte, die

- eine sichere Authentifizierung,
- die Sicherstellung von Vertraulichkeit und
- die Glaubhaftmachung von signierten elektronischen Daten ermöglicht.

Die Chipkarte dient in erster Linie der Sicherung des Zugangs zu und der Verarbeitung in sicherheitskritischen Anwendungen in der RUB, wie der Verarbeitung von Personaldaten (HIS-SVA GX) oder Studierendendaten (VSPL).
Als weitere Funktion dient die Karte als Bedienstetenausweis. Für die Anwendung der Chipkarte wird eine Infrastruktur für die Erstellung und Ausgabe, die Prüfung der Zertifikate und Korrektur der Daten bereitgestellt, die Teil des Verfahrens *Chipkarte* ist.

Die Verarbeitung der Daten erfolgt in vier Bereichen:

- Bei der Ausgabe der Chipkarte in der Personalabteilung (RA) werden Anträge gestellt und Daten in ein Verwaltungssystem für die Ausgabe der Chipkarte eingetragen. Es werden solche Daten verarbeitet, die man benötigt, um den Antragsteller zu erreichen bzw. zu informieren.
- Bei der Erzeugung der Chipkarte werden Zertifikate generiert und gemeinsam mit Daten zur Identifizierung und Überprüfung abgespeichert sowie die Chipkarte bedruckt und eine Benachrichtigung bzgl. der PIN erzeugt.
- Bei der Anwendung der Karte wird das öffentliche Zertifikat zur Authentifizierung eines Nutzers oder zur Signierung von Daten bzw. zur Prüfung von Signaturen abgefragt.
- Die Karte sperrt sich selbst, wenn eine PIN mehrfach falsch eingegeben wird. Die öffentlichen Zertifikate können gesperrt werden, womit der Zugang zu den gesicherten Anwendungen verhindert wird.

2. Rechtmäßigkeit der Datenverarbeitung

Die wesentliche Grundlage der Verarbeitung der Datenverarbeitung für und mit der Chipkarte basiert auf der Freiwilligkeit der Ausgabe der Karte, die nach §29a (1) DSG NW für mobile Datenträger gefordert ist. Daraus ist auch eine Zustimmung für die Verarbeitung der Daten nach §4 (1) DSG NW gewährleistet. Der ebenfalls notwendigen Aufklärung der Betroffenen (§ 29a (1) DSG NW) wird entsprochen.
Für die Doppelfunktion der Karte als Karte für Sicherungsfunktionen und als Bedienstetenausweis ist es erforderlich, eine Alternative für den Bedienstetenausweis anzubieten, die zu keinen Nachteilen bei den Betroffenen führt. Eine entsprechende Regelung ist vorgesehen.
Für die Anwendung der Karte im Rahmen von weiteren Verfahren ist es laut DSG NW erforderlich alternative Bearbeitungswege anzubieten, die ohne Anwendung einer Chipkarte auskommen, damit kein Zwang entsteht, der die Freiwilligkeit der Ausgabe der Karte aufhebt. Auf diesen Aspekt ist in den entsprechenden Vorabkontrollen der Verfahren zu achten.

Bei der Anwendung der Bediensteten-Chipkarte werden Personaldaten nach §29 DSG NW verarbeitet. Eine Dienstvereinbarung zur Chipkarte regelt hierzu näheres.
Datenarten, bei denen die Erforderlichkeit fraglich ist finden sich in Form von:

- *Geschlecht und Titel*: Ist als freiwillige Angabe anzusehen und wird für die persönliche Ansprache benutzt.
- *Geburtsdatum* : Wird für einige Fälle verwendet, um eindeutige Identifikation zu ermöglichen. Ebenfalls wird das Datum bei der Kontaktaufnahme zur Sperrung der Karte relevant.
- *Foto*: Wird zwischenzeitlich dazu verwendet, um ein Foto auf die Chipkarte für den Bedienstetenausweis aufbringen zu können. Das Foto wird anschließend gelöscht.

Die Ausgabe der Karte erfolgt auf freiwilliger Basis. Um den Anforderungen des §29a gerecht zu werden ist deshalb bei den Anwendungssystemen, in denen die Chipkarte eingesetzt werden soll, darauf zu achten, dass die Freiwilligkeit der Ausgabe der Karte gewährleistet ist.

3. Erforderlichkeit der Daten und Beachtung des Minimalisierungsgebotes

Die in dem Verfahren zu Verarbeitung vorgesehenen personenbezogenen Daten sind für die korrekte und vor allem sichere Durchführung erforderlich. Im Wesentlichen dienen die Daten den Zwecken der Korrespondenz, der eindeutigen Identifizierung des Inhabers, der Durchführung der Authentifizierung und Signierung sowie der Erzeugung von Redundanz für die Erhöhung der Sicherheit und Überprüfungszwecke.

4. Wahrung der Rechte der Betroffenen

§5 DSG NW benennt folgende Rechte von Betroffenen, die im Verfahren Chipkarte selbst sicherzustellen sind:

- **Auskunft-/Einsichtnahme**: Für die Einsichtnahme der für die Chipkarte gespeicherten Daten sind einerseits Terminals geplant, an denen die Daten eingesehen werden können und andererseits wird Software bereitgestellt, mit der die Daten am Arbeitsplatz eingesehen werden können.
- **Unterrichtung:** Der Unterrichtungspflicht der Betroffenen wird in geeigneter Weise nachgekommen (die dazu verwendeten Informationsmaterialien finden sich als Anhang der Dienstvereinbarung zur Bedienstetenchipkarte).
- **Berichtigung, Sperrung oder Löschung und Widerruf der Einwilligung:** Sperrung von Daten findet insbesondere für das Zertifikat statt. Der Sperrung der anderen Datenarten ist auf organisatorischem Wege nachzukommen. Berichtigung und Löschung sind für diese Datenarten ebenfalls möglich. Als problematisch stellt sich hier das Zertifikat dar.

Löschung von Zertifikatsdaten

Die Überprüfung von Signaturen macht eine dauerhafte Speicherung eines oder mehrerer (z.B. bei Kartenverlust) öffentlicher Zertifikate zu einer Person notwendig. Ohne diese Zertifikate sind Signaturen nicht mehr nachprüfbar und alle gespeicherten Signaturen werden ungültig.
Die Löschung wäre nur dann möglich, wenn keine gespeicherte Signatur mit dem Schlüssel generiert wurde, also die Karte praktisch nur zur Autorisierung eingesetzt wurde. Da auf Protokolle bei der Anwendung der Zertifikate verzichtet werden soll, muss man davon ausgehen, dass alle ausgegebenen Zertifikate für diesen Zweck eingesetzt wurden.
Zur Erfüllung der Aufgaben ist es erforderlich, auch längerfristig eine entsprechende Überprüfung der Unterschrift/Signatur zu ermöglichen. Dies macht die dauerhafte Speicherung der Zertifikate notwendig, wie es beispielsweise auch in der Signaturverordnung für Zertifikatsherausgeber verlangt ist. Die Antragsteller sind darauf hinzuweisen, dass eine Löschung der Zertifikatsdaten wegen der nachträglichen Überprüfung von Signaturen nicht möglich ist, auch wenn sie die Einwilligung zurückziehen.

5. Risikoeinschätzung

Bei der Risikoeinschätzung ist zu prüfen, ob es durch menschliches oder technisches Versagen möglich ist, die im Chipkarten-Verfahren verarbeiteten personenbezogenen Daten zum Nachteil der Betroffenen zu nutzen oder zu manipulieren. Hier ist es zunächst von Vorteil, dass keine sensiblen Daten nach §2 DSG NW verarbeitet werden.
Eine Besonderheit des hier zu beurteilenden Verfahrens besteht darin, dass es den Zugang zu anderen Verfahren (hier Anwendungen genannt) steuert, in denen wiederum personenbezogene Daten verarbeitet werden – etwa von Studierenden. Das Risiko für diese Betroffenen ist jedoch im Rahmen dieser Vorabkontrolle nicht zu analysieren, sondern bei der Betrachtung der Anwendungen. Allerdings können die Inhaber von Chipkarten, deren Risiko es hier zu betrachten gilt, indirekt betroffen sein: Wenn Daten in den Anwendungssystemen so gefälscht werden könnten, dass ein Chipkarten-Inhaber als Verursacher gälte, ohne dass er das Gegenteil beweisen könnte, so wäre das für ihn ein erheblicher Nachteil, der möglichst weitgehend abgewendet werden muss.

Weitere Details der an dieser Stelle vorhandenen Risikoanalyse können aus Sicherheitsgründen nicht veröffentlicht werden.

6. Zusammenfassung

Für die Verarbeitung der Daten im Rahmen der Bedienstetenchipkarte ist eine ausreichende Rechtsgrundlage beschrieben. Die Hauptgrundlage ist die Freiwilligkeit/Einwilligung nach den §§4 (1) und 29a DSG NW. In Teilen ist für die Begründung der Verarbeitung bei der Chipkarte die Anwendung in sicherheitskritischen Systemen relevant.

Die beschriebenen Sicherheitsmaßnahmen wirken den beschriebenen Risiken ausreichend entgegen.

Es gibt ausreichend Ansätze, um die Sicherheitsmaßnahmen beim Erkennen zusätzlicher Gefahren zu erweitern. Dies gilt insbesondere mit Hinblick auf den praktischen Betrieb, bei dem große Mengen von Daten bearbeitet werden müssen. Hier können sich weitere Anforderungen und Probleme ergeben, die zum jetzigen Zeitpunkt schwer vorherzusehen sind. Aufgrund der zentralen Bedeutung der Chipkarte für die Sicherungsmaßnahmen im Rahmen anderer Verfahren, ist eine regelmäßige Prüfung der Umsetzung und eventuell eine kontinuierliche Verbesserung der Sicherheitsmaßnahmen sinnvoll.