INNOVATIONSSTIFTUNG
BAYERISCHE KOMMUNE

Einsatzbereiche für elektronische Signaturen, multifunktionale Chipkarten und den neuen Personalausweis in bayerischen Kommunen

Prof. Dr. Rainer Thome

Dipl.-Vw. Jürgen Scherer M.A.

Stand: Juli 2012

Impressum

Herausgeber

Innovationsstiftung Bayerische Kommune

http://www.bay-innovationsstiftung.de

Postadresse

c/o Anstalt für Kommunale Datenverarbeitung in Bayern (AKDB)

Hansastraße 16

80686 München

Inhaltsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

AFS-HKR	Anforderungen an den Einsatz fortgeschrittener Signaturen im Haushalts-, Kassen-und Rechnungswesen der Bayerischen Kommunen
AKDB	Anstalt für Kommunale Datenverarbeitung in Bayern
AZR	Ausländerzentralregister
BayDSG	Bayerisches Datenschutzgesetz
BayVwVfG	Bayerisches Verwaltungsverfahrensgesetz
DESTATIS	Statistisches Bundesamt Deutschland
DKK	Dienste- und kartenspezifisches Kennzeichen
DMS	Dokumentenmanagement-System
DTA	Datenträgeraustauschverfahren
eANV	Elektronisches Abfallnachweisverfahren
eFES	„Erweiterte“ fortgeschrittene elektronische Signatur
eID	Elektronische Identität
ePR	Elektronisches Personenstandsregister
ES	Einfache elektronische Signatur
eSig	Elektronische Signaturen
FES	Fortgeschrittene elektronische Signatur
GEZ	Gebühreneinzugszentrale
HKR	Haushalts-, Kassen- und Rechnungswesen
KBA	Kraftfahrt-Bundesamt
KommHV	Verordnung über das Haushalts-, Kassen- und Rechnungswesen der Gemeinden, der Landkreise und der Bezirke
KommHV-Doppik	Verordnung über das Haushalts-, Kassen- und Rechnungswesen der Gemeinden, der Landkreise und der Bezirke nach den Grundsätzen der doppelten kommunalen Buchführung
LfStaD	Landesamt für Statistik und Datenverarbeitung

MFC	Multifunktionale Chipkarte
MFD	Multifunktionaler Dienstausweis
nPA	Neuer Personalausweis
QES	Qualifizierte elektronische Signatur
SigG	Signaturgesetz
SSO	Single-Sign-On
VOB	Vergabe- und Vertragsordnung für Bauleistungen
VOL	Vergabe- und Vertragsordnung für Leistungen
VPS	Virtuelle Poststelle
ZEPR	Zentrales elektronisches Personenstandsregister

1 Prozessunterstützung in bayerischen Kommunalverwaltungen

Die öffentliche Kommunalverwaltung steht vor einer Vielzahl aktueller Herausforderungen wie Bürgerfreundlichkeit, Bürokratieabbau, Verwaltungsmodernisierung, Angebot von Verwaltungsdienstleistungen über das Internet, aber auch Sicherheit in der Informationstechnologie und demographischer Wandel.

1.1 Medienbruchfreiheit als Baustein der modernen Verwaltung

Um diese Herausforderungen bewältigen zu können und zugleich den Weg in Richtung moderne Verwaltung zu beschreiten, müssen in erster Linie die Verwaltungsprozesse vereinfacht und beschleunigt werden. Um die Ziele Vereinfachung und Beschleunigung zu erreichen, sind zum einen organisatorische Änderungen erforderlich, andererseits ist aber auch die Verringerung der derzeit noch vielfach bestehenden „Medienbrüche“ ein entscheidender Baustein einer modernen Verwaltung. Unter einem Medienbruch wird der Übergang von einem schriftlichen in ein elektronisches Medium bzw. umgekehrt verstanden. In der Praxis also etwa das Eintippen von Daten in ein elektronisches System oder der Ausdruck von Daten auf Papier. Während die Datenverarbeitung innerhalb der bestehenden Fachverfahren (aber nicht immer zwischen diesen) der Verwaltung automatisiert auf elektronischem Wege abläuft, führen gerade die Übergänge, die nicht elektronisch stattfinden, zu hohen, grundsätzlich vermeidbaren Aufwänden und stellen auch eine prinzipielle Fehlerquelle dar. An die zunehmend elektronisch durchgeführte Verwaltungsarbeit mit möglichst wenigen Medienbrüchen werden daher hohe Erwartungen geknüpft, die gerade auch qualitative Verbesserungen umfassen. Hierzu zählen insbesondere:

- Plausibilitätsprüfungen und Richtlinien

  Bei durchgängig elektronischen Abläufen können in die Software implementierte Plausibilitätsprüfungen verwendet werden, um Falscheingaben und fehlende Informationen rechtzeitig zu erkennen. Auch Berechtigungen und Richtlinien wie z. B. die Bearbeitung durch mehrere Mitarbeiter in bestimmter Reihenfolge kann elektronisch hinterlegt und protokolliert werden.

- Bessere Nachprüfbarkeit

  Die Nachprüfbarkeit der Arbeitsschritte verbessert sich und die vorgenommenen Änderungen lassen sich besser nachvollziehen. Dies kann insbesondere im Bereich der Vergabe und der Anordnungen wichtig sein.

- Aktueller Bearbeitungsstand

  Der aktuelle Bearbeitungsstand ist jederzeit einsehbar, und es kann nachvollzogen werden, in welchem Status sich ein Prozess befindet.

- Automatische Erinnerungen und Benachrichtigungen

  Automatische Erinnerungen via E-Mail können Mitarbeiter an ablaufende Fristen (z. B. Skonto) erinnern. Auch lässt sich ein entsprechender Workflow hinterlegen. Durch diesen werden anhand bestimmter Regeln Mitarbeiter benachrichtigt und/oder das Dokument wird ihnen zur Weiterbearbeitung zugestellt.

- Höhere Datenqualität

  Durch die medienbruchfreie Übertragung der Daten kann sich die Datenqualität erhöhen. Fehleingaben (Tippfehler, Zahlendreher), schlecht gescannte Dokumente und unleserliche handschriftliche Zeichen werden vermieden.

- Einfacheres Suchen und Finden

  Liegen alle Dokumente und Arbeitsergebnisse in elektronischer Form vor, können sie anhand recherchierbarer Kriterien schneller gesucht und gefunden werden.

- Zuverlässige Weitergabe von Dokumenten

  Werden alle Dokumente elektronisch versendet, können sie nicht mehr auf dem Postweg verloren gehen. Etwaige Irrläufer werden zudem schneller gefunden werden, da es aufgrund der automatischen Protokollierung leichter nachvollziehbar ist, wohin sie gesendet wurden.

- Kostensenkung beim Drucken, Versenden und Scannen

  Durch die Medienbruchfreiheit und den Verzicht auf Papier lassen sich Druck- und Portokosten einsparen. Die Kosten für die Archivierung sinken ebenfalls, da deutlich weniger Raum für die Lagerung der Papierakten erforderlich ist.

- Beschleunigung der Abläufe

  Ein wesentlicher Aspekt ist die Beschleunigung der Abläufe. So ist die Bearbeitung von Anordnungen deutlich schneller, da die langwierigen Transportzeiten via (Haus-)Post entfallen.

Vor diesem Hintergrund ist im Auftrag der Innovationsstiftung Bayerische Kommune untersucht worden, inwiefern

- elektronische Signaturen (eSig),

- multifunktionale Chipkarten/Dienstausweise (MFC/MFD) und
- der neue Personalausweis (nPA)

dazu beitragen können, die Kommunen bei der Erfüllung ihrer Aufgaben zu unterstützen. Der Fokus liegt dabei darauf, wie diese Technologien verwaltungsinterne Prozesse insbesondere hinsichtlich der Medienbruchfreiheit verbessern können.

Das Ziel der vorliegenden Untersuchung ist es, die Einsatzfelder von elektronischen Signaturen, multifunktionalen Chipkarten/Dienstausweisen und neuem Personalausweis aufzuzeigen sowie die resultierenden Möglichkeiten zur Prozessunterstützung zu erläutern. Die jeweiligen Technologien werden hinsichtlich ihrer Eignung für die unterschiedlichen Anwendungsgebiete bewertet. Zudem werden Empfehlungen für die Kommunen gegeben, ob und unter welchen Umständen sich die Beschaffung und der Einsatz dieser Technologien lohnen.

1.2 Vorgehen und Begriffsabgrenzung

- Datenerhebung

  Zur Ermittlung der Einsatzbereiche und der Verbreitung der Technologien wurde ein Fragebogen entworfen und an 75 bayerische Kommunen in den sieben Regierungsbezirken versandt. Dafür wurden in jedem Bezirk Kommunen nach unterschiedlicher Größe und unterschiedlicher Körperschaftsart (Gemeinde, Stadt, kreisfreie Stadt, Landkreis sowie die jeweilige Bezirksverwaltung) ausgewählt, die nach telefonischer Vorabinformation den Fragebogen zugesandt bekamen. Einige Gemeinden sind auch telefonisch oder persönlich vor Ort befragt worden. Ansprechpartner waren entweder die Amtsleiter oder die IT-Verantwortlichen. Die Rücklaufquote lag bei 32 Prozent. Die Stadt Regensburg hatte sich freundlicherweise dazu bereit erklärt, für die Untersuchung als Partnerkommune zur Verfügung zu stehen und gab detaillierte Einblicke in Verfahrensabläufe und praktische Problemstellungen.

  Hinsichtlich der Thematik der multifunktionalen Chipkarten (MFC) gibt es bislang nur wenige Erfahrungen seitens der Kommunen. Daher wurde ein weiterer, speziell auf diesen Bereich zugeschnittener Fragebogen erstellt und an diejenigen bayerischen Kommunen versandt, die sich bereits aktiv mit diesem Thema auseinandersetzen. Alle sieben angeschriebenen Kommunen beantworteten die Fragen schriftlich oder telefonisch.

  Spezialfragen zum Thema fortgeschrittene elektronische Signatur hat das Bayerische Landesamt für

Statistik und Datenverarbeitung (LfStaD) beantwortet. Zu Fragen bezüglich der qualifizierten elektronischen Signatur sowie der dazugehörigen Zertifikate haben Mitarbeiter der Trustcenter D-Trust, Telesec und S-Trust umfassend Auskunft gegeben. Im Rahmen verschiedener Tagungen und Workshops zum neuen Personalausweis und zu Chipkarten wurden weitere Informationen gewonnen.

- Untersuchte Bereiche

  Eine generelle Eingrenzung auf bestimmte Bereiche in den Kommunen ist nicht erfolgt. Da die Fragen meist von der Amtsleitung oder von Mitarbeitern der IT-Abteilung beantwortet wurden, konnte bezüglich der eingesetzten und geplanten Technologien (multifunktionale Chipkarten, Signaturen) ein Überblick über die gesamte Verwaltung gewonnen werden. Hinsichtlich der Fragen zu Kommunikationspartnern in der Verwaltung lag der Fokus auf den allgemeinen Bürgerdiensten. Gezielte Befragungen wurden zudem in den Bereichen Finanzen (Kasse, Buchhaltung), Bauaufsicht und Sozialamt durchgeführt.

- Eignung und Praxisrelevanz

  Bei der Gegenüberstellung wurde darauf geachtet, welche Technologien sich grundsätzlich für die identifizierten Einsatzbereiche eignen. Dabei wurde berücksichtigt, dass für die Realisierung neben den technischen auch organisatorische und rechtliche Voraussetzungen erfüllt sein müssen.

  Aber nicht alles, was technisch, organisatorisch und juristisch möglich bzw. geeignet ist, hat auch praktische Relevanz. Diese ergibt sich aus mehreren Faktoren. Erstens spielen die Kosten der Technologien eine wesentliche Rolle. Zweitens sind Synergieeffekte, Kompatibilität und Wiederverwendung bzw. Kombination mit vorhandenen Komponenten ein starkes Argument für oder gegen eine bestimmte Lösung. Und schließlich ist auch die Akzeptanz bei Mitarbeitern und Bürgern ein für die Praxis ganz entscheidendes Element.

- Einteilung der Kommunengrößen

  Die vom Statistischen Bundesamt Deutschland (DESTATIS) verwendete Größeneinteilung der Kommunen nach Einwohnerzahlen ist für die vorliegende Untersuchung nicht unmittelbar anwendbar. Da der Fokus hier auf den internen Anwendungsbereichen liegt, ist die Anzahl der in einer Verwaltung tätigen Mitarbeiter mit PC-Arbeitsplatz die ausschlaggebende Größe.

  In dieser Untersuchung werden drei Größenklassen verwendet:

  - Kleine Kommunen: bis zu 25 Mitarbeiter,

- mittlere Kommunen: 25 bis 100 Mitarbeiter und
- große Kommunen: über 100 Mitarbeiter.

Hierbei wird nicht unterschieden, ob es sich dabei um Vollzeit- oder Teilzeitkräfte handelt. Dies ist dadurch begründet, dass viele der benötigten Komponenten personalisiert werden müssen und sich daher nicht wie bei anderen Aufgaben (z. B. von mehreren Teilzeitkräften verwendeter PC) gemeinsam nutzen lassen. Unter Mitarbeiter werden im Folgenden alle Angestellten und Beamten der Kernverwaltung einer Kommune aufgefasst, die für ihre Tätigkeit einen PC benötigen. Die Eingrenzung auf die Kernverwaltung erfolgt deshalb, um „Verzerrungen" z. B. durch Schulpersonal, das nicht in allen Kommunen vorhanden ist, zu vermeiden. Die Einschränkung auf PC-Nutzung ergibt sich aus der Tatsache, dass wesentliche Anwendungsbereiche mit der Computernutzung in Verbindung stehen.

Auf die Besonderheiten der jeweiligen Körperschaft (Gemeinde, Stadt, Landkreis, Bezirk) wird bei Bedarf hingewiesen.

1.3 Aufbau der Untersuchung und Lesepfade

Dieses Dokument ist modular aufgebaut, um verschiedenen Zielgruppen mit unterschiedlichem Informationsbedarf gerecht zu werden. Die einzelnen Bestandteile sind voneinander unabhängig und können in beliebiger Reihenfolge gelesen werden. Dies führt jedoch dazu, dass in den einzelnen Unterabschnitten Wiederholungen auftreten.

1 **Vorgehen und Aufbau**

Im ersten Kapitel werden Vorgehensweise und Aufbau der Studie beschrieben.

2 **Einsatzbereiche von elektronischen Signaturen, multifunktionalen Chipkarten und neuem Personalausweis**

Die unterschiedlichen Einsatzbereiche werden in diesem Kapitel ausführlich erläutert. Ausgehend von der Darstellung der aktuellen Situation werden für die Zukunft mögliche Anwendungsfälle (unter Einsatz der oben genannten Technologien), deren Funktionsweise sowie die jeweiligen Voraussetzungen aufgezeigt.

3 **Beschreibung der Technologien und Zuordnung zu den Anwendungsbereichen**

In drei Unterkapiteln werden die verschiedenen Technologien in ihren Grundlagen beschrieben. Anschließend werden sie den jeweils geeigneten Einsatzbereichen gegenübergestellt. Es folgt ei-

ne Beschreibung der Potenziale und, soweit möglich, der Kostenfaktoren. Anschließend werden die Technologien bewertet und Empfehlungen für die Kommunen ausgesprochen.

4 Zusammenfassung der Ergebnisse für den schnellen Überblick

Hier finden sich alle wichtigen Informationen in knapper Form.

Anhang Leitfäden für die Implementierung (Zusatzdokumente)

Im Anhang finden sich Informationen, Vorgehensweisen und Hilfestellungen für die Einführung der oben genannten Technologien. Folgende Leitfäden wurden erstellt:

- Leitfaden zur Implementierung multifunktionaler Chipkarten/Dienstausweise in bayerischen Kommunen
- Leitfaden zur Beschaffung fortgeschrittener und erweiterter fortgeschrittener elektronischer Signaturen in bayerischen Kommunen
- Leitfaden zur Beschaffung qualifizierter elektronischer Signaturen in bayerischen. Kommunen
- Leitfaden zur Implementierung der elektronischen Identitätsfunktion (eID-Funktion) des neuen Personalausweises (nPA) in bayerischen Kommunen

Nicht für alle Ansprüche ist es erforderlich, sämtliche Kapitel zu lesen. Daher können die folgenden Lesepfade verwendet werden:

- *Schneller Überblick*: Inhaltsübersicht und Ergebnisse
  Kapitel 1 + 4

- *Fokus Einsatzbereiche*: Inhaltsübersicht und Einsatzbereiche
  Kapitel 1 + 2

- *Fokus Einsatzbereiche und Technologien*: Inhaltsübersicht, Einsatzbereiche und Technologien
  Kapitel 1 + 2 + 3

- *Fokus Technologien*: Inhaltsübersicht und Technologien
  Kapitel 1 + 3

- *Umfassender Überblick*: Studie ohne Implementierungsleitfäden

Kapitel 1 - 4

- *Umsetzung*: Implementierungsleitfäden (Zusatzdokumente)
  Anhang

Aus Gründen der Lesbarkeit wurde im Text nur die männliche Form gewählt. Die Angaben beziehen sich jedoch selbstverständlich auf Angehörige beider Geschlechter.

2 Einsatzbereiche für elektronische Signaturen, multifunktionale Chipkarten und den neuen Personalausweis

In den nachfolgenden Abschnitten werden die möglichen Einsatzbereiche für elektronische Signaturen, multifunktionale Chipkarten und den neuen Personalausweis beschrieben. Für deren dauerhaft erfolgreiche und Kosten sparende Nutzung ist es von entscheidender Bedeutung, dass von vornherein über die mehrfache Nutzung dieser Lösungen in den verschiedenen Aufgabenbereichen nachgedacht und dazu ein Anforderungskatalog aufgestellt wird. Eine sukzessive Einführung dieser Identifikationslösungen ist zwar möglich und aus Kosten- sowie Realisierungsgründen wahrscheinlich auch der richtige Weg, er kann aber nur dann erfolgreich beschritten werden, wenn zuvor ein Gesamtmodell für die jeweilige kommunale Informationsverarbeitung erstellt wird. Das bedeutet, dass alle möglichen Anwendungsbereiche darauf überprüft werden, ob sie in der gegebenen Situation sinnvoll genutzt werden können. Ist dies der Fall, so muss die Gesamtlösung ihren Einsatz auch berücksichtigen und damit aufwandsarm ermöglichen. Ansonsten entstünden unnötig hohe Entwicklungs- und noch schlimmer Betriebskosten, die in Zukunft auf Dauer anfallen würden.

Nicht alle Anwendungsbereiche sind in allen Kommunen vorhanden oder gleichermaßen relevant. Daher erfolgt die Beschreibung der Einsatzbereiche in alphabetischer Reihenfolge.

Der Aufbau der Abschnitte folgt dabei im Wesentlichen immer dem gleichen Schema:

Zunächst wird kurz die aktuelle Situation beschrieben, wobei nur ausgewählte Szenarien gezeigt werden.

Anschließend folgt ein Ausblick auf die zukünftige Situation, wie sie mit einer der oben genannten Technologien realisiert werden kann.

Daran schließen sich eine Beschreibung der Funktionsweise der zukünftigen Abläufe und die dafür erforderlichen Voraussetzungen an.

Für die nachfolgend genannten Anwendungsbereiche gilt, dass im konkreten Fall immer geprüft werden muss, ob und inwieweit der Personalrat und/oder der Datenschutzbeauftragte einzubeziehen sind. Bei sämtlichen Anschaffungen muss ebenfalls geprüft werden, ob Ausschreibungen bzw. Vergleichsangebote erforderlich sind.

2.1 Dienstausweis

Mitarbeiter einer Kommune können mit Dienstausweisen ausgestattet werden. Ob solche Ausweise verwendet werden, kann dabei jede Kommune selbst entscheiden. In der Regel werden Dienstausweise jedoch

nur für Mitarbeiter mit Außenkontakt ausgestellt.

2.1.1 Aktuelle Situation

Derzeit bestehen die Dienstausweise aus Papier oder Kunststoff. Sie enthalten meist ein Lichtbild, Vor- und Zuname, die Beschäftigungsbehörde mit Anschrift und die Unterschrift des Ausweisinhabers. Sie dienen als Sichtausweis und haben darüber hinaus keine weitere Funktion.

2.1.2 Zukünftige Situation

Die Mitarbeiter können künftig mit einem multifunktionalen Dienstausweis ausgestattet werden, auf dessen Außenhülle Identifikationsdaten wie Lichtbild, Name, Vorname, Beschäftigungsbehörde usw. aufgebracht sind. Zusätzlich sind diese Daten auch in elektronischer Form auf dem Ausweis gespeichert. Der Dienstausweis vereint neben der Funktion „Sichtausweis“ zusätzlich zahlreiche weitere Funktionalitäten, für die bislang eigenständige Systeme erforderlich waren bzw. keine Lösungen bestanden. Die Ausstattung kann je nach Kommune etwa die Zugangsfunktion zum Gebäude oder zu bestimmten Räumen auch die Zeiterfassung, die Anmeldung am PC, die Verschlüsselung von E-Mails, das sichere Drucken am Computer oder die bargeldlose Bezahlung in der Kantine oder am Kaffeeautomat erfassen. Die Mitarbeiter tragen, soweit erforderlich, auch innerhalb der Dienststelle sichtbar ihren Ausweis und sind somit für Verwaltungskunden und -mitarbeiter (vor allem in größeren Kommunen relevant) eindeutig als der Dienststelle zugehörig identifizierbar.

2.1.3 Funktionsweise

Der multifunktionale Dienstausweis unterscheidet sich in seiner Funktionsweise als reiner Sichtausweis nicht von einem Papier- oder Plastikkartenausweis. Neben dem Aufdruck der Daten kann aber auch eine Speicherung der Daten auf dem Chip erfolgen.

2.1.4 Voraussetzungen

Voraussetzung ist das Vorhandensein multifunktionaler Chipkarten. Im Rahmen der Ausstellung eines Ausweises bei dem u. a. der kontaktlose und der kontaktbehaftete Chip beschrieben werden, können auch die entsprechenden Daten in elektronischer Form und als Aufdruck auf den Ausweis übertragen werden.

Die Mitarbeiter sind mit entsprechenden Chipkarten auszurüsten. Die Karten müssen an zentraler Stelle

ausgegeben und wieder eingesammelt werden können (z. B. beim Ausscheiden eines Mitarbeiters oder bei Praktikanten).

2.1.5 Kurzbewertung

Das **Erfordernis** des Dienstausweises obliegt jeder Kommune selbst.

Der **Einsatz elektronischer Lösungen** (hier der multifunktionale Dienstausweis) findet sich nur in wenigen Kommunen.

Die **Anzahl der Betroffenen** umfasst in der Regel nur die Mitarbeiter mit Außenkontakt einer Kommune. Es können aber alle Mitarbeiter damit ausgestattet werden.

Der **Hauptvorteil** ist die erhöhte Sicherheit durch die Identifikation der Mitarbeiter innerhalb und außerhalb der Behörden.

2.2 Drucken vertraulicher Dokumente (Follow-Me-Printing)

Der Ausdruck von Dokumenten an Ausgabegeräten kann so geregelt werden, dass die Ausgabe erst dann beginnt, wenn sich der betreffende Mitarbeiter tatsächlich am Ausgabegerät befindet.

Der Begriff „Follow-Me Printing“ ist ursprünglich registriertes Markenzeichen des Unternehmens Ringdale, wird mittlerweile aber synonym zur produktneutralen Bezeichnung dieser Vorgehensweise, „Pull-Printing“, verwendet.

2.2.1 Aktuelle Situation

In Kommunen sind nicht alle Arbeitsplätze der Mitarbeiter mit einem eigenen Drucker, Fax oder Kopierer ausgestattet. Häufig stehen die Geräte in einem Gang innerhalb der Behörde, um den Mitarbeitern der anliegenden Büros einen zentralen Zugriff zu ermöglichen. Aus Sicht des Datenschutzes und der Datensicherheit ist dies bedenklich. Denn wenn ein Mitarbeiter ein Dokument ausdruckt oder ein Fax erhält, ist er meist nicht sofort am Ausgabegerät, um es entgegen zu nehmen. Zudem ist der Drucker für viele Personen zugänglich. Dies ermöglicht es Unbefugten, vertrauliche Daten einzusehen und unter Umständen sogar zu entwenden.

2.2.2 Zukünftige Situation

Die Mitarbeiter können mit einer Chipkarte ausgestattet werden. Nach Absenden des Druckauftrages geht der Mitarbeiter zum Drucker oder Kombigerät Chipkartenleser, das ihn anhand seiner Karte identifizieren kann. Der Mitarbeiter hält die Karte vor das Lesegerät und der Druck des Dokumentes wird gestartet. Falls mehrere Ausgabegeräte vorhanden sind, kann der Mitarbeiter auch ein anderes auswählen, sollte das von ihm bevorzugte gerade durch einen Druck- oder Kopiervorgang belegt sein. Die Dokumente werden immer an dem Ausgabegerät gedruckt, das der Mitarbeiter mit seiner Chipkarte aktiviert.

Eine alternative Strategie wäre die Anschaffung von Arbeitsplatzdruckern, da hier nicht nur die Datenschutzproblematik gelöst würde, sondern auch Prozessunterbrechungen vermieden werden könnten.

2.2.3 Funktionsweise

Um das Follow-Me-Printing zu ermöglichen, wird eine spezielle Software installiert, die Ausgabegeräte werden mit Lesegeräten bestückt oder sind bereits damit ausgestattet. Erteilt der Mitarbeiter an seinem Arbeitsplatz den Druckauftrag, ist dieser mit der Kartenkennung verknüpft. Das System erkennt somit, welcher Mitarbeiter welchen Druckauftrag gestartet hat. Allerdings wird der Druckauftrag nicht sofort ausgeführt, sondern zunächst zwischengespeichert. Mit Hilfe der Kennung auf dem Chip wird der Druckvorgang gestartet, sobald der Mitarbeiter seine Chipkarte in oder an einen Kartenleser eines Ausgabegerätes führt. Dies erzwingt einerseits das untätige Warten bis der Ausdruck erfolgt ist, andererseits können mehrere einzelne Ausdrucke in einem „Gang zum Drucker“ zusammengefasst werden..

2.2.4 Voraussetzungen

Folgende Rahmenbedingungen sind notwendig, um das Follow-Me-Printing zu ermöglichen:

- Chipkarte

  Die Mitarbeiter sind mit entsprechenden Chipkarten auszurüsten. Die Karten müssen an zentraler Stelle ausgegeben und wieder eingesammelt werden können (z. B. beim Ausscheiden eines Mitarbeiters oder bei Praktikanten).

- Geeignete Hardware mit Lesegerät

  Die Drucker und Kombigeräte müssen für diese Art des Druckens geeignet und mit Lesegeräten ausgestattet sein.

- Software

Neben der Hardware ist auch die entsprechende Software erforderlich, die sowohl die Kartenleser bedienen und die Druckvorgänge steuern kann.

- Berücksichtigung aller bestehenden und geplanten Komponenten

  Bei der Anschaffung müssen bereits vorhandene oder geplante Komponenten wie Zeiterfassung, Bezahlung in der Kantine, Zugangskontrolle, Signaturen, Single-Sign-On usw. berücksichtigt werden.

2.2.5 Kurzbewertung

Das **Erfordernis** des Druckens vertraulicher Dokumente ist in allen Kommunen gegeben.

Der **Einsatz elektronischer Lösungen** (Follow-Me-Printing) findet sich nur in wenigen Kommunen.

Die **Anzahl der Betroffenen** umfasst fast alle Mitarbeiter einer Kommune.

Die **Hauptvorteile** sind die erhöhte Datensicherheit und der erhöhte Datenschutz.

2.3 Elektronischer Anordnungs-Signatur-Workflow

Der elektronische Anordnungs-Signatur-Workflow ermöglicht das vollständige elektronische Erstellen, Bearbeiten und Prüfen von Anordnungen.

2.3.1 Aktuelle Situation

Anordnungen (Einzahlungsanordnung, Auszahlungsanordnung, Stundungsanordnung u. a.) werden in den Kommunalverwaltungen noch papierbasiert abgewickelt. In der Regel ist eine sachliche und rechnerische Prüfung eigenhändig zu unterzeichnen. Anschließend muss der Anordnungsbefugte die Anordnung handschriftlich unterzeichnen (rechtliche Grundlage hierfür sind die KommHV und KommHV-Doppik). Dieser Ablauf wird nachfolgend am Beispiel einer Auszahlungsanordnung skizziert.

Nach Eingang einer Rechnung muss die sachliche und rechnerische Richtigkeit durch einen befugten Mitarbeiter festgestellt und mit seiner Unterschrift bestätigt werden. Dazu erstellt der Mitarbeiter in der Finanzsoftware eine Anordnung, druckt diese aus und unterzeichnet sie handschriftlich. Beide Dokumente (Anordnung und Rechnung) werden an den Anordnungsbefugten weitergeleitet. Dieser prüft die Anordnung, die Rechnung (zahlungsbegründende Unterlage) und die haushaltsmäßigen Voraussetzungen.

Anschließend wird die gedruckte Anordnung vom anordnungsbefugten Mitarbeiter unterzeichnet (hand-

schriftlich) und erhält im Finanzverfahren die Freigabe. Die gedruckte Anordnung und die zahlungsbegründenden Unterlagen werden an die Kasse weitergegeben.

In der Kasse werden die Berechtigungen und die Unterschriften auf der Anordnung und eventuell auf der zahlungsbegründenden Unterlage geprüft.

Die Kasse erstellt im Finanzverfahren die Sollstellung. Damit wird die Anordnung in das Sach- und Zeitbuch eingetragen. Anschließend wird die Zahlung ausgeführt, d. h. die Überweisung per Datenträgeraustauschverfahren (DTA) an den Empfänger veranlasst. Der papiergebundene Workflow wird mit der Ablage im Belegarchiv oder mit dem Scannen der Dokumente und der Speicherung im elektronischen Archiv abgeschlossen.

Die Prüfung der sachlichen und rechnerischen Richtigkeit kann je nach Fall in räumlich getrennten Ämtern oder Fachabteilungen erforderlich sein. Dies tritt z. B. bei Schulen, Bauverwaltung usw. häufiger auf. Die Konsequenz sind lange Transportzeiten der Anordnungen und Rechnungen zwischen den Ämtern, insbesondere wenn die Fachabteilungen räumlich weit entfernt sind. Da in mittleren und größeren Kommunen der Bereich der Anordnungen einen größeren Teil der Mitarbeiter betrifft, wobei die Mehrzahl hier mit der sachlich-rechnerischen Prüfung befasst ist, verursacht der papiergebundene Ablauf einen erheblichen und kostspieligen zeitlichen Aufwand.

2.3.2 Zukünftige Situation

Die Prozesse von der sachlichen und rechnerischen Prüfung bis zur Anweisung durch die Kasse sind in elektronischer Form abgebildet und werden somit deutlich beschleunigt. Basis ist ein sogenannter Anordnungs-Signatur-Workflow, in dem die Berechtigungen und Befugnisse für die betreffenden Mitarbeiter hinterlegt sind. Die zukünftige Vorgehensweise unterscheidet sich im Wesentlichen dadurch, dass die Unterschriften elektronisch geleistet werden. Somit wird der weitere Ablauf nach Eingang der Rechnung komplett elektronisch durchgeführt. Das Ausdrucken, Unterschreiben und erneute Einscannen sowie der Postversand entfallen. Nach Durchlauf des Workflows werden die Dokumente (z. B. Rechnungen) und die Anordnung im Dokumentenmanagement-System gespeichert.

2.3.3 Funktionsweise

Die handschriftliche Unterschrift erfordert zwangsweise den papierbasierten Ablauf. Der elektronische Anordnungs-Signatur-Workflow basiert darauf, dass die beteiligten Mitarbeiter über eine qualifizierte elektronische Signatur (QES) verfügen. Alternativ ist als Erleichterung für bayerische Kommunen auch der Ein-

satz einer erweiterten fortgeschrittenen elektronischen Signatur (eFES) möglich, die die QES für diesen speziellen Einsatzzweck ersetzen kann. Rechtliche Grundlagen hierfür sind § 87 Nr. 12 KommHV-Kameralistik und § 98 Nr. 21 KommHV-Doppik sowie die „Anforderungen an den Einsatz fortgeschrittener Signaturen im Haushalts-, Kassen-und Rechnungswesen der Bayerischen Kommunen (AFS-HKR) und die „Begründung zur AFS-HKR". Im Finanzverfahren bzw. in den Modulen, in denen der elektronische Workflow möglich ist, werden die jeweiligen Befugnisse der Mitarbeiter hinterlegt. Auch Vertretungsregelungen bei Urlaub und Krankheit können hier definiert werden.

Durch die Anmeldung im Workflow bzw. im Finanzverfahren ist der Mitarbeiter dem System bekannt. Somit können sowohl bei Feststellung der sachlichen und/oder rechnerischen Richtigkeit als auch bei der Anordnung stets die Befugnisse des jeweils signierenden Mitarbeiters abgeglichen werden.

Da es im Finanzbereich deutlich komplexere Sachverhalte abzubilden gilt, als den vorgestellten einfachen Standardfall, kann der Ablauf anhand bestimmter Kriterien auch anders festgelegt werden, so dass z. B. zusätzliche Personen einbezogen werden können. Diese Regelungen lassen sich ebenfalls hinterlegen.

2.3.4 Voraussetzungen

Folgende Voraussetzungen sind für eine elektronische Form der Abwicklung essentiell:

- eFES oder QES

  Es muss eine entsprechende elektronische Signatur(landschaft) vorhanden sein. Hier hat der Verordnungsgeber in Bayern für die öffentliche Verwaltung mit der „erweiterten" fortgeschrittenen Signatur eine Erleichterung geschaffen, d. h. dass alternativ zur qualifizierten elektronischen Signatur auch die „erweiterte" fortgeschrittene Signatur verwendet werden kann.

- Lesegeräte

  Die Arbeitsplätze müssen bei Verwendung von Chipkarten mit Lesegeräten (mind. Klasse 2) oder speziellen Tastaturen mit integriertem Kartenleser ausgestattet werden.

- Finanzsoftware

  Über eine Finanzsoftware verfügen alle Kommunen. Diese muss dazu geeignet sein, den Anordnungsvorgang komplett elektronisch zu unterstützen. Hierfür müssen gegebenenfalls eine andere Software oder die benötigten Module beschafft werden.

- Änderungen in der Poststelle

  In der Poststelle können Änderungen im Arbeitsablauf erforderlich sein, wenn bereits dort einge-

hende Rechnungen digitalisiert werden. Hierfür ist in jedem Fall ein Scanner nötig. Je nachdem wie die gescannten Rechnungen weitergeleitet werden, sind entsprechende Softwarekomponenten erforderlich.

- Dokumentenmanagement-System (DMS)

  Die Verwendung eines DMS setzt die Beschaffung eines passenden Systems voraus bzw. die Anpassung eines bestehenden hinsichtlich der neuen Anforderungen.

- Archivsystem

  Zur revisionssicheren Aufbewahrung der Anordnungen und Rechnungen muss – sofern noch nicht vorhanden – ein revisionssicheres Archivsystem eingerichtet werden.

- Organisatorische Änderungen

  Vor der Festlegung der Arbeitsabläufe im Finanzprogramm bzw. Workflow sind die bestehenden papiergebundenen Abläufe zu analysieren. Dabei sollte auch die Vielfalt der Ablaufvarianten reduziert werden. Ebenfalls muss überlegt werden, ob sich die Abläufe in den unterschiedlichen Abteilungen angleichen oder sogar vereinheitlichen lassen, soweit dies rechtlich möglich ist. Beide Maßnahmen verringern den Wartungs- und Pflegeaufwand des Systems und beschleunigen häufig auch den Gesamtablauf.

- Berücksichtigung aller bestehenden und geplanten Komponenten

  Bei der Anschaffung müssen bereits vorhandene oder geplante Komponenten wie Zeiterfassung, Bezahlung in der Kantine, Zugangskontrolle, Signaturen, Single-Sign-On usw. berücksichtigt werden.

2.3.5 Kurzbewertung

Das **Erfordernis** der Anordnungserstellung ist in allen Kommunen gegeben.

Der **Einsatz elektronischer Lösungen** findet sich bislang nur in wenigen Kommunen.

Die **Anzahl der Betroffenen** umfasst einen größeren Teil der Mitarbeiter einer Kommune.

Die **Hauptvorteile** sind die beschleunigte Abwicklung (Medienbruchfreiheit) und die jederzeitige Nachvollziehbarkeit.

2.4 Elektronischer Vergabeprozess (eVergabe)

Der elektronische Vergabeprozess nach der Vergabe- und Vertragsordnung für Leistungen (VOL), der Vergabe- und Vertragsordnung für Bauleistungen (VOB) und der Vergabeordnung für freiberufliche Leistungen (VOF) kann bislang nur von wenigen am Markt etablierten Lösungen vollelektronisch durchgeführt werden. Im Weiteren soll unter einer elektronischen Vergabe (eVergabe) der durchgängig IT-gestützte sowie medienbruchfrei implementierte Prozess einer Auftragsvergabe verstanden werden. Von einer eVergabe kann somit dann gesprochen werden, wenn

- die Vergabeunterlagen von der Verwaltung elektronisch bereitgestellt,
- die Bekanntmachung durch die Verwaltung auf einer elektronischen Plattform durchgeführt,
- die Angebote der Bieter mittels eines elektronischen Werkzeugs übermittelt (und ggf. signiert) sowie
- die Angebotsauswertung und die Zuschlagsübermittelung mittels einer Software elektronisch unterstützt werden.

Grundsätzlich basieren die heute am Markt verfügbaren Lösungen für die elektronische Vergabe auf einer Client-Server-Anwendung oder vereinzelt auf einer webbasierten Architektur. Unabhängig für welche Alternative sich eine Kommune entscheidet, sollte der Betrieb bei einem externen Dienstleister erfolgen, um personelle Ressourcen zu sparen und Kostenvorteile zu erzielen.

Aufgrund der Komplexität und auch aufgrund der rechtlichen Möglichkeiten bei der Verfahrensausprägung wird an dieser Stelle auf eine detaillierte Verfahrensbeschreibung (die sich zudem noch in nationale und EU-weite Verfahren untergliedert) verzichtet. Es werden nachfolgend nur einige zentrale Prozessschritte innerhalb des Vergabeprozesses beschrieben.

Nach § 13 (1) VOL/A und §13 (1) VOB/A legt der Auftraggeber fest, in welcher Form die Angebote einzureichen sind. Dies kann auch die Unterzeichnung mit einer fortgeschrittenen elektronischen Signatur (FES) beinhalten. Weder die Verwendung der FES oder der QES ist innerhalb der Verwaltung bei einem Vergabeprozess vorgeschrieben. Die nachfolgenden Ausführungen beziehen sich daher auf die freiwillige Verwendung der FES bzw. einer QES innerhalb der Behörde (im Vergabeprozess), um die Beweiskraft und die Nachvollziehbarkeit zu verbessern.

2.4.1 Aktuelle Situation

Aktuell wird der Großteil der Vergaben im kommunalen Umfeld noch auf klassische Weise durchgeführt, d. h. grundlegend papierbasiert und mit entsprechenden Veröffentlichungen in den Printmedien. Der ein-

deutige politische Wille ist jedoch die elektronische Vergabe, und so kann eine steigende Tendenz zu dieser Art der Vergabe festgestellt werden.

2.4.2 Zukünftige Situation

Bereits bei der Bereitstellung der Ausschreibungsunterlagen können alle erforderlichen Dokumente sowie dort, wo fachlich sinnvoll, auch die E-Mail-Kommunikation mit der FES bzw. einer QES signiert werden.

Ein für die Vergabe berechtigter Mitarbeiter meldet sich mit Benutzernamen und Passwort am Vergabesystem an. Aufgrund seiner dort hinterlegten Benutzerrolle sind die für seine Aufgaben benötigten Berechtigungen im System hinterlegt. Die Systemanmeldung sowie alle Einstellungen und Eingaben, die der Mitarbeiter innerhalb des Vergabesystems durchführt, werden vom System protokolliert und, sofern relevant, in den Vergabevermerk übernommen.

Bei einer Vergabe tritt häufig der Fall ein, dass Bieter Fragen zu den Angaben in den Ausschreibungsunterlagen haben. Diese Fragen können an die Verwaltung gerichtet werden, die die Antworten dann an alle Bieter bzw. Anforderer der Ausschreibungsunterlagen senden. Bei Verwendung einer eVergabe-Lösung werden diese Antworten in der Regel via E-Mail versendet oder als Nachricht in einem nicht-öffentlichen Bereich auf einer eVergabe-Plattform eingestellt und im Vergabevermerk eingetragen. Auch von Seiten der öffentlichen Auftraggeber können noch weitere Informationen an die Bieter weitergegeben werden. Alle für die Vergabe relevanten Dokumente und E-Mails können, um einen möglichst hohen Beweiswert zu erhalten, von dem zuständigen Mitarbeiter innerhalb der eVergabe-Lösung der Verwaltung mit der QES oder FES signiert werden. Dies ist im Ergebnis auch wesentlich einfacher und schneller als eine händische oder nicht-integrierte Vorgehensweise.

Nach Beendigung der Ausschreibungen werden die elektronisch eingegangenen Angebote am Submissions- bzw. Angebotsöffnungstermin geöffnet, geprüft und anschließend ausgewertet. Diejenigen, die den Zuschlag nicht erhalten sowie der bzw. die Bestbieter, werden über die geplante Zuschlagserteilung bzw. über den Zuschlag gemäß der Verfahrensregeln elektronisch informiert.

Auch dieser Aufgabenbereich unterstreicht eindringlich, dass es für den wirklich sinnvollen und Kosten sparenden Einsatz von Informationsverarbeitungslösungen entscheidend ist, alle miteinander in Beziehung stehenden Aufgaben in integrierte Lösungen mit einzubeziehen. So kann ein Verfahren zur Bearbeitung von Ausschreibungen, in das sowieso alle mit dem Vorgang verbundenen Daten einzugeben sind, weit mehr, als nur den operativen Ablauf zu unterstützen. Die komplizierten und durchaus öfter fortgeschriebenen Vorschriften sind für Mitarbeiter von kleineren Kommunen, in denen die verschiedenen Arten und Volumina

von Projekten nicht so oft vorkommen, nur schwer zu erinnern. Eine E-Vergabelösung kann und sollte daher in der Lage sein, die ihm bereitgestellten Informationen gegen die Regeln der Ausschreibung zu prüfen und den zuständigen Mitarbeitern Hinweise auf die korrekte Vorgehensweise zu geben.

2.4.3 Funktionsweise

Das Signieren mit FES bzw. QES ist in der Regel in das Vergabeverfahren integriert, so dass seitens des Behördenmitarbeiters nur das Einstecken der Karte und die Eingabe des Passwortes nötig sind.

2.4.4 Voraussetzungen

- Chipkarten mit FES / QES

  Die Mitarbeiter sind mit entsprechenden Chipkarten auszurüsten. Die Karten müssen an zentraler Stelle ausgegeben und wieder eingesammelt werden können (z. B. beim Ausscheiden eines Mitarbeiters).

- Lesegeräte

  Die Arbeitsplätze müssen bei Verwendung von Chipkarten mit Lesegeräten (bei QES mit Klasse 2) oder speziellen Tastaturen mit integriertem Kartenleser ausgestattet werden.

- Vergabesoftware
  Die Verwaltung muss über eine entsprechende Vergabesoftware verfügen.

2.4.5 Kurzbewertung

Das **Erfordernis** der Vergabe ist in allen Kommunen gegeben.

Der **Einsatz elektronischer Lösungen** (vollständig elektronischer Vergabeprozesse) findet sich nur in sehr wenigen Kommunen.

Die **Anzahl der Betroffenen** umfasst prozentual nur sehr wenige Mitarbeiter einer Kommune.

Die **Hauptvorteile** sind die beschleunigte Abwicklung (Medienbruchfreiheit) und die erhöhte Sicherheit beim Vergabeverfahren.

2.5 Elektronischer Versand personenbezogener Daten (per E-Mail)

In Kommunen werden sehr häufig personenbezogene Daten verarbeitet. Sie dürfen laut Art. 1 BayDSG von öffentlichen Verwaltungsinstitutionen nur erhoben, verarbeitet und genutzt werden, wenn die Persönlichkeitsrechte der Bürger nicht beeinträchtigt werden. Diese Daten sind besonders zu behandeln.

2.5.1 Aktuelle Situation

Das elektronische Versenden von Daten innerhalb der Kommunen ist in der Regel unproblematisch, da der Datenverkehr innerhalb des geschützten Netzes verläuft. Auch der regelmäßige Datenaustausch, der direkt via Fachverfahren durchgeführt wird (z. B. Übertragung der Daten bei Zuzug eines Bürgers an die Wegzugsgemeinde) ist unkritisch. Er ist verschlüsselt und erfolgt über besondere Übermittlungsprotokolle (z. B. OSCI).

Darüber hinaus gibt es allerdings noch weitere Kommunikationswege und -partner.

- Kommunikation mit Behörden und Institutionen

  Kommunen haben in unterschiedlicher Häufigkeit Kontakt zu anderen öffentlichen Einrichtungen, wie etwa staatlichen Behörden, anderen Kommunen oder sonstigen Institutionen wie z. B. Schulen, Krankenhäuser, psychiatrische Einrichtungen usw. Der Bayerische Landesbeauftragte für den Datenschutz empfiehlt, E-Mail-Kommunikation von personenbezogenen Daten stets verschlüsselt durchzuführen (vgl. Orientierungshilfe: Datensicherheit beim Betrieb eines Intranets am Beispiel eines Landkreis-Behördennetzes, Punkt 3.13, www.datenschutz-bayern.de). Die E-Mail-Übertragung soll also ausdrücklich auch innerhalb geschlossener Netze wie des Bayerischen Behördennetzes oder Kommunaler Behördennetze verschlüsselt erfolgen. Gleiches gilt selbstverständlich auch für Daten, die an die Kirchensteuerämter, die Gebühreneinzugszentrale (GEZ) oder andere Institutionen aufgrund gesetzlicher Pflichten übermittelt werden. Je nach Kommune gibt es hier bereits unterschiedliche Übertragungswege.

  Dennoch kommt es in der Praxis auch vor, dass personenbezogene Daten ungeschützt, d. h. unverschlüsselt per E-Mail versendet werden. Das Ausdrucken und das Versenden per Post ist eine häufig verwendete Methode, um personenbezogene Daten auszutauschen. Aber auch der Versand von Daten auf USB-Sticks, CD-ROMs oder Disketten ist üblich.

- Kommunikation mit Bürgern und Unternehmen

  Häufig handelt es sich bei der E-Mail-Kommunikation mit Bürgern um Nachfragen zum aktuellen

Bearbeitungsstand eines Vorganges, um das Senden von gescannten Unterlagen oder um zusätzliche Informationen, die die Behörde vom Bürger für die Bearbeitung eines Vorganges benötigt. Hierbei werden sehr oft personenbezogene Daten ohne die erforderliche Verschlüsselung ausgetauscht, obwohl dies datenschutzrechtlich untersagt ist. Die Hauptursache hierfür ist das fehlende Problembewusstsein seitens der Kommunikationspartner. Daneben gibt es auch Hürden in der Technik und der Handhabung. Bei der verschlüsselten E-Mail-Kommunikation benötigen z. B. beide Partner entsprechende Verschlüsselungsmechanismen, die zudem kompatibel sein müssen. Dies ist in der Regel weder bei den Bürgern noch bei den Kommunen der Fall.

- Dateiverschlüsselung (für alle potenziellen Empfänger)

  Neben den Möglichkeiten der Verschlüsselung von E-Mails können Daten auch mit anderen Programmen verschlüsselt werden. Hierfür ist beim Absender und Empfänger eine spezielle Software nötig. Mit diesen Programmen werden die Daten verschlüsselt und können dann entweder als E-Mail-Anhang oder auf einem Datenträger ausgetauscht werden. Dem Empfänger muss jedoch der Schlüssel zum Dechiffrieren der Daten bekannt sein bzw. mitgeteilt werden. Diese Vorgehensweise kann dann als „Notlösung“ angewendet werden, wenn der Empfänger oder Absender keine in das E-Mail-Programm integrierte Verschlüsselung hat.

2.5.2 Zukünftige Situation

Zukünftig werden personenbezogene Daten stets verschlüsselt, bevor sie per E-Mail an die jeweiligen Kommunikationspartner gesendet werden. Alle Teilnehmer verfügen über die notwendige Verschlüsselungstechnik. Dabei ist zu berücksichtigen, dass nicht jegliche Art (personenbezogener) Daten via E-Mail versendet werden kann. Dies gilt z. B. nicht für Papierdokumente, die im Original vorliegen müssen, oder umfangreiche Daten wie ganze Aktenordner. Letzteres wird erst dann möglich sein, wenn auch die Akten elektronisch geführt werden. Bei der Kommunikation mit Bürgern können von den Behörden auch spezielle Internet-Portale (Bürgerservice-Portale) verwendet werden. Diese bieten nicht nur die Möglichkeit der Online-Antragstellung, sondern erlauben über eine verschlüsselte Verbindung auch anderweitigen elektronischen Nachrichtenaustausch wie z. B. Nachfragen, Nachreichen von digitalisierten Unterlagen o. Ä.

2.5.3 Funktionsweise

Um den Versand personenbezogener Daten auf elektronischem Wege bzw. über E-Mail zu ermöglichen, sind folgende Varianten möglich:

- E-Mail-Verschlüsselung allgemein

  Die technische Funktionsweise bei der Verschlüsselung wie auch bei der Signatur ist eine komplizierte Berechnung, die hier nicht weiter ausgeführt wird. Sowohl der Versender einer verschlüsselten E-Mail wie auch der Empfänger müssen über die geeigneten Techniken und Schlüssel verfügen.

  Um die Sicherheit zu erhöhen, können für die Verschlüsselung Chipkarten verwendet werden. Zum Ver- und Entschlüsseln muss in diesem Fall die Chipkarte in ein Lesegerät gesteckt werden. Die eigentliche Verschlüsselungssoftware lässt sich in das E-Mail-Programm integrieren. Soll nun eine E-Mail an einen bestimmten Empfänger gesendet werden, wird dieser aus dem Adressbuch des E-Mail-Programms ausgewählt. Die Verschlüsselung selbst erfolgt anschließend automatisch. Ebenso einfach ist das Entschlüsseln von E-Mails oder Dokumenten. Der Empfänger gibt bei Erhalt einer verschlüsselten E-Mail sein Passwort ein. Danach wird die Nachricht automatisch entschlüsselt und ist lesbar.

- Zukünftige Verschlüsselung zwischen Behörden

  Derzeit ist eine Initiative des Bayerischen CIO und den bayerischen kommunalen Spitzenverbänden zur sicheren elektronischen Kommunikation in Vorbereitung. Ziel ist es, alle Kommunen und staatlichen Stellen in Bayern mit einem softwarebasierten Verschlüsselungszertifikat auszustatten. Die Verschlüsselung ist hierbei aber nicht personalisiert, sondern funktionsorientiert (Funktionszertifikat). Das bedeutet, dass jede Kommune und staatliche Stelle in Bayern ein Zertifikat der Bayerischen Verwaltungs-PKI für ein bestimmtes, aber nicht personalisiertes E-Mail-Konto (z. B. „poststelle@xyz.de“) erhält. Der Austausch der verschlüsselten E-Mails erfolgt dann über dieses Benutzerkonto. Nach dem Entschlüsseln wird die E-Mail dann intern an den entsprechenden Mitarbeiter weitergeleitet.

- Virtuelle Poststelle

  Die virtuelle Poststelle bietet eine Möglichkeit, an zentraler Stelle die Ver- und Entschlüsselung des E-Mail-Verkehrs für die Behördenmitarbeiter zu erledigen. Werden E-Mails auf diese Weise verschlüsselt und verschickt, ist dies für die Behördenmitarbeiter komfortabler und auch einfacher. Über die virtuelle Poststelle läuft der gesamte interne und externe E-Mail-Verkehr. Soll eine Nachricht verschlüsselt und/oder signiert werden, muss dies nur beim Versenden der E-Mail angegeben werden. Diese Vorgehensweise ist sehr komfortabel, weil auf den Rechnern der Mitarbeiter nichts installiert werden muss und die Zertifikate für die Verschlüsselung und Entschlüsselung zentral gespeichert werden. Jedoch bringt die Einführung einer virtuellen Poststelle einen großen technischen und auch finanziellen Aufwand mit sich und ist nicht zuletzt deshalb im kommunalen Bereich kaum

verbreitet.

- Bürgerservice-Portal

  Verfügt die Kommune über ein Bürgerservice-Portal, haben die Verwaltungskunden die Möglichkeit, dort ein Benutzerkonto zu erstellen. Nach der Anmeldung können von den Bürgern Dokumente hochgeladen oder Nachrichten an die Mitarbeiter bzw. Antragsbearbeiter in der Kommune gesendet werden. Auf Seiten des Bürgers ist dafür nur ein Internetbrowser erforderlich. Hat ein Sachbearbeiter Informationen für einen Bürger, so kann er sie in dessen Benutzerkonto hinterlegen. Bei der nächsten Anmeldung am Portal (oder bereits vorab via E-Mail) wird der Bürger darüber informiert, dass neue Nachrichten für ihn bereitstehen. Somit kann die gesamte Kommunikation verschlüsselt durchgeführt werden, ohne dass auf Seiten der Kommunikationsteilnehmer zusätzliche Aufwände entstehen.

- De-Mail und/oder E-Postbrief

  Weitere Möglichkeiten, vertrauliche Daten mit Bürgern oder anderen Kommunikationspartnern auszutauschen, könnten zukünftig die beiden Dienste De-Mail und E-Postbrief bieten.
  De-Mail
  Die Konzeption von De-Mail ist auf staatlicher Seite erfolgt, der Betrieb wird hingegen von privaten Anbietern durchgeführt werden. Bislang ist De-Mail aber noch nicht im Wirkbetrieb. Der Vorteil dieser Lösung besteht darin, dass die Daten sicher (d. h. verschlüsselt) übertragen werden. Für das Versenden und Empfangen ist ein spezielles Benutzerkonto mit einer besonderen De-Mail-Adresse nötig. Um ein solches Benutzerkonto zu eröffnen, ist eine Identifikation des Teilnehmers zwingend erforderlich. E-Mails von einem De-Mail-Konto können nur an ein anderes De-Mail-Konto gesendet werden. Beim Versenden können Versand- bzw. Empfangsbestätigungen angefordert werden, so dass hier prinzipiell eine elektronische Alternative zum postalischen Einschreiben besteht. Die Kosten für die Nutzung des De-Mail-Dienstes sind derzeit noch nicht bekannt. Der Vorteil von De-Mail liegt darin, dass mit dem Versenden der E-Mail sowohl die Vertraulichkeit und Unverändertheit (Integrität) des Inhaltes wie auch die Identität des Senders bzw. Empfängers sichergestellt sind. Für Behörden und größere Firmen werden Lösungen angeboten, die De-Mail in das vorhandene E-Mail-System integrieren.
  E-Postbrief

  Der E-Postbrief der Deutschen Post AG basiert auf einem ähnlichen Konzept wie De-Mail. Auch hier benötigt der Benutzer ein spezielles E-Mail-Konto, für das er sich identifizieren muss, bevor er E-Mails versenden und empfangen kann. Wie auch bei De-Mail gibt es die Möglichkeit, Versand-

und Empfangsbestätigungen anzufordern. Der E-Postbrief hat jedoch eine Eigenschaft, die ihn von De-Mail abhebt. E-Postbriefe werden auf Wunsch des Versenders auch ausgedruckt, kuvertiert und auf herkömmliche Weise zugestellt. Nachrichten können daher im sogenannten Hybrid-Verfahren versendet werden. Für die Inhaber eines E-Postbrief-Kontos erfolgt die Zustellung elektronisch, für alle anderen erfolgt sie auf Papier. Für den Versender hat dies den Vorteil, dass er nur einen „Kanal", nämlich den Versand via E-Postbrief bedienen muss. Den Rest erledigt die Deutsche Post AG als Diensteanbieter.

Für beide Verfahren bestehen hinsichtlich des Einsatzes in der öffentlichen Verwaltung noch unbeantwortete Fragen hinsichtlich Datenschutz, Zugangseröffnung, Praktikabilität und der rechtlichen Anerkennung. Das für 2012 geplante E-Government-Gesetz des Bundes wird für eine Reihe dieser Fragen weitergehende Klärung bringen.

2.5.4 Voraussetzungen

Die Voraussetzungen sind davon abhängig, welche der oben genannten Alternativen zum Versand personenbezogener Daten gewählt wird.

- E-Mail-Verschlüsselung zwischen Behörden

  Für die Verschlüsselung von E-Mails sind entsprechende Schlüssel (und Zertifikate) notwendig, die vom LfStaD für die öffentliche Verwaltung kostenlos ausgestellt werden. Zudem werden die geeigneten Softwareerweiterungen, sogenannte Plug-Ins, für die E-Mail-Programme an den Arbeitsplätzen der Mitarbeiter benötigt. Um die Verschlüsselung anwenden zu können, müssen die Benutzer geschult werden. Da rechtsverbindliche E-Mails oftmals über einen längeren Zeitraum aufbewahrt werden sollen, ist zudem eine Speicherung in einem Dokumentenmanagement-System mit ggf. anschließender längerfristiger Ablage in einem Archivsystem erforderlich. Die Speicherung sollte dabei jedoch unverschlüsselt erfolgen, da eine Entschlüsselung über lange Zeiträume hinweg mit dem privaten Schlüssel des jeweiligen Benutzers in der Praxis nicht sichergestellt werden kann.

- Chipkarte

  Um die Sicherheit zu erhöhen, können die für die Verschlüsselung erforderlichen Schlüssel und Zertifikate auch auf Chipkarten gespeichert werden. Die Mitarbeiter sind mit entsprechenden Chipkarten auszurüsten. Die Karten müssen von einer zentralen Stelle verwaltet, ausgegeben und wieder eingesammelt werden können (z. B. beim Ausscheiden eines Mitarbeiters oder bei Praktikanten).

- Lesegeräte

Die Arbeitsplätze müssen bei Verwendung von Chipkarten mit Lesegeräten oder speziellen Tastaturen mit integriertem Kartenleser ausgestattet werden.

- Virtuelle Poststelle (VPS)

  Für den Einsatz der virtuellen Poststelle sind je nach Ausprägung größere technische Maßnahmen erforderlich.

- Verschlüsselungsprogramme

  Für das sporadische Verschlüsseln oder das Versenden an Empfänger ohne E-Mail-Verschlüsselung, können auch spezielle Verschlüsselungsprogramme verwendet werden. Diese sind einfach in der Handhabung und bieten einen guten Schutz. Schwachpunkt hierbei ist aber, dass der Schlüssel über einen sicheren Kanal, also entweder persönlich, via Telefon oder Post übertragen werden muss.

- De-Mail und/oder E-Postbrief

  Hinsichtlich De-Mail lassen sich noch keine Aussagen über den Aufwand organisatorischer und technischer Maßnahmen treffen.

  Bei Verwendung des E-Postbriefes benötigt die Kommune ein oder mehrere entsprechende Konten für den Empfang und Versand der E-Postbriefe. Um die Zugangseröffnung seitens der Empfänger sicher zu stellen, muss deren Einwilligung explizit erfolgen.

- Vorgaben durch staatliche Stellen

  Eine Vielzahl personenbezogener Daten wird zwischen Kommunen und staatlichen Stellen ausgetauscht. Eine gegenseitige Verständigung über ein bayernweit einheitliches Verschlüsselungsformat und einen Kommunikationsweg ist für eine praxistaugliche Lösung unabdingbar. Die dargestellte Lösung (siehe „Zukünftige Verschlüsselung zwischen Behörden“) kann hierzu die erforderlichen Voraussetzungen schaffen.

- Berücksichtigung aller bestehenden und geplanten Komponenten

  Bei der Anschaffung müssen bereits vorhandene oder geplante Komponenten wie Zeiterfassung, Bezahlung in der Kantine, Zugangskontrolle, Signaturen, Single-Sign-On usw. berücksichtigt werden.

2.5.5 Kurzbewertung

Das **Erfordernis** des Versands personenbezogener Daten ist in allen Kommunen gegeben.

Der **Einsatz elektronischer Lösungen** (zur Verschlüsselung) findet sich nur in wenigen Kommunen.

Die **Anzahl der Betroffenen** umfasst nahezu alle Mitarbeiter einer Kommune.

Die **Hauptvorteile** sind die beschleunigte Abwicklung (Medienbruchfreiheit) und der erhöhte Datenschutz.

2.6 Elektronisches Abfallnachweisverfahren (eANV)

Gemäß der Verordnung über die Nachweisführung bei der Entsorgung von Abfällen (Nachweisverordnung -NachwV) muss seit 01.04.2010 die Nachweisführung für alle am Prozess der Entsorgung gefährlicher Abfälle beteiligten Stellen (Abfallerzeuger, Entsorger, Abfallbeförderer und die zuständigen Behörden) elektronisch durchgeführt werden. Bis zu diesem Datum wurde der elektronische Abfallbegleitschein auf Papier mit mehreren Durchschlägen geführt. Durch die elektronische Bearbeitung müssen alle an diesem Verfahren beteiligten Stellen mit einer qualifizierten elektronischen Signatur (QES) ausgestattet sein. Der bisherige Papieraufwand entfiel dadurch und der Ablauf erfolgt seitdem medienbruchfrei. Die Kommunen können hierbei als Abfallerzeuger, Abfallbeförderer wie auch als öffentlich-rechtlicher Entsorgungsträger betroffen sein.

2.6.1 Funktionsweise

Zur Teilnahme am eANV müssen sich alle Beteiligten bei der Zentralen Koordinierungsstelle (ZKS) anmelden. Sie fungiert als technische Datendrehscheibe und nimmt alle Nachweisdaten bundesweit entgegen. Den Teilnehmern wird dabei ein elektronisches Postfach eingerichtet, mit dem sie auch Mitteilungen empfangen können. Alternativ kann die elektronische Abwicklung auch über einen Dienstleister erfolgen. Die Bestätigung der Zulässigkeit des Entsorgungsweges wird seitens der Behörde, die ebenfalls an die ZKS angeschlossen ist, mit der QES erteilt. Auch bei der Kontrolle über den Verbleib gefährlicher Abfälle, bei der Transport und Entsorgung dokumentiert werden, wird mit der QES eines Behördenmitarbeiters quittiert.

2.6.2 Voraussetzungen

- Chipkarten mit QES

  Die Mitarbeiter sind mit entsprechenden Chipkarten auszurüsten. Die Karten müssen an zentraler

Stelle ausgegeben und wieder eingesammelt werden können (z. B. beim Ausscheiden eines Mitarbeiters).

- Lesegeräte

  Die Arbeitsplätze müssen bei Verwendung von Chipkarten mit Lesegeräten (Klasse 2) oder speziellen Tastaturen mit integriertem Kartenleser ausgestattet werden.

- Software

  Für die Teilnahme am eANV muss eine entsprechende Software beschafft werden.

2.6.3 Kurzbewertung

Das **Erfordernis** des Abfallnachweises ist in allen Kommunen gegeben, die als Abfallentsorger, Abfallbeförderer oder öffentlich-rechtlicher Entsorgungsträger auftreten und nicht unter eine Ausnahmeregelung fallen.

Der **Einsatz elektronischer Lösungen** ist verpflichtend und findet sich in allen Kommunen, die den Abfallnachweis bearbeiten müssen und keine Ausnahmegenehmigung haben.

Die **Anzahl der Betroffenen** umfasst nur sehr wenige Mitarbeiter einer Kommune.

Die **Hauptvorteile** sind die Integration, die beschleunigte Abwicklung (Medienbruchfreiheit) und die reduzierten Vorgangskosten.

2.7 Elektronisches Personenstandsregister (ePR)

Ab 01.01.2014 wird das elektronische Personenstandsregister die bisherigen Personenstandsbücher ablösen.

2.7.1 Aktuelle Situation

Standesbeamte beurkunden derzeit mit Siegel und eigenhändiger Unterschrift. Registereinträge werden ebenfalls noch handschriftlich geführt. Durch die papiergebundene Form und das Erfordernis, dass Registereinträge durch den Standesbeamten ergänzt werden können, war die elektronische Registerführung bis 2009 nicht zulässig.

2.7.2 Zukünftige Situation

Zukünftig wird das elektronische Personenstandsregister vollständig elektronisch geführt. Die QES ersetzt dabei die eigenhändige Unterschrift der Standesbeamten. In Bayern wird bis Mitte 2013 ein zentrales elektronisches Personenstandsregister (ZEPR) eingerichtet und bei der AKDB betrieben.

2.7.3 Funktionsweise

Die Funktionsweise des ePR und die Mechanismen zur revisionssicheren Speicherung sind aufgrund der detaillierten Vorgaben im Personenstandsrecht sehr komplex. Sie werden an dieser Stelle nicht detailliert erläutert. Relevant hierbei ist, dass die bisherige eigenhändige Unterschrift der Standesbeamten bei Registereinträgen zukünftig durch eine QES ersetzt werden wird.

Durch das ZEPR können Standesämter auch auf die Registereinträge der anderen angeschlossenen Standesämter lesend zuzugreifen. Für die Bürger hat dies den Vorteil, dass sie die Personenstandsurkunden zukünftig auch bei den örtlichen Standesämtern erhalten können und nicht lediglich bei den Behörden, bei denen der Personenstandsfall beurkundet wurde.

2.7.4 Voraussetzungen

- Chipkarten mit QES

  Die Mitarbeiter sind mit entsprechenden Chipkarten auszurüsten. Die Karten müssen an zentraler Stelle ausgegeben und wieder eingesammelt werden können (z. B. beim Ausscheiden eines Mitarbeiters).

- Lesegeräte

  Die Arbeitsplätze müssen durch die Verwendung von Chipkarten (mit QES) mit Lesegeräten (mind. Klasse 2) oder speziellen Tastaturen mit integriertem Kartenleser ausgestattet werden.

- Fachverfahren und ZEPR

  Die erforderlichen Fachverfahren für das Standesamt müssen auf die neuen Anforderungen angepasst werden. Das ZEPR für Bayern muss aufgebaut und wird bis Mitte 2013 bei der AKDB in Betrieb genommen werden.

2.7.5 Kurzbewertung

Das **Erfordernis** der Führung von (zukünftig elektronischen) Personenstandsregistern ist in allen Kommu-

nen mit einem Standesamt gegeben.

Der **Einsatz elektronischer Lösungen (ePR)** findet sich (derzeit) in keiner Kommune.

Die **Anzahl der Betroffenen** umfasst prozentual nur sehr wenige Mitarbeiter einer Kommune.

Der **Hauptvorteil** ist die beschleunigte Abwicklung (Medienbruchfreiheit).

2.8 Interne Antragstellung und Datenabruf

Innerhalb von Kommunen müssen die Mitarbeiter verschiedenste Anträge ausfüllen und von den Vorgesetzten oder zuständigen Stellen genehmigen lassen (z. B. Beschaffung von Büromaterial, Dienstreiseanträge usw.). Daneben erhalten die Mitarbeiter auch persönliche Informationen und Nachweise (wie z. B. Gehaltsabrechnungen).

2.8.1 Aktuelle Situation

Bei den meisten Anträgen, die intern von Mitarbeitern gestellt werden, herrscht Formfreiheit, so dass das Schriftformerfordernis nicht gegeben ist. In der Regel genügt die Anmeldung am Fachverfahren mit Benutzername und Passwort, damit der Anwender authentifiziert ist und seinen Antrag elektronisch stellen kann. Nach der Anmeldung gibt der Mitarbeiter die erforderlichen Daten in eine Bildschirmmaske ein und bestätigt die Eingabe. Sofern erforderlich, wird der Antrag vom Adressaten ebenfalls elektronisch innerhalb des Fachverfahrens bearbeitet und ggf. genehmigt.

In der Praxis wird bei internen Anträgen häufig die Papierform verwendet, obwohl aus rechtlichen Gründen keine Schriftform vorgegeben ist. Die Formulare werden entweder am Rechner oder handschriftlich ausgefüllt und dann vom Antragsteller auf Papier unterschrieben. Anschließend werden sie per Post oder Hauspost zugestellt oder persönlich beim Empfänger abgegeben. Dieser prüft den Antrag und etwaige Unterlagen, genehmigt den Antrag (mit seiner Unterschrift), lehnt ihn ab (ebenfalls mit seiner Unterschrift) oder verlangt noch ergänzende Informationen. Nach Abschluss der Antragsbearbeitung wird der Antrag ggf. aufbewahrt.

Die Mitarbeiter erhalten auch persönliche Informationen, die in Zusammenhang mit ihrem Beschäftigungsverhältnis stehen. Dies können z. B. Gehaltsnachweise sein, die in der Regel postalisch zugesendet werden.

2.8.2 Zukünftige Situation

Interne Anträge, die eine Unterschrift erfordern, können elektronisch unterzeichnet und versendet werden. Hierfür wird das Antragsformular elektronisch bereitgestellt, vom Antragsteller elektronisch aufgefüllt und mit der qualifizierten elektronischen Signatur (QES) unterzeichnet. In den zahlreichen Fällen, in denen kein Schriftformerfordernis gegeben ist, können andere Vorgehensweisen verwendet werden, um sicherzustellen, dass nur die befugte Person den Antrag stellt bzw. die benötigten Informationen erhält. Hierfür bietet sich die Zwei-Faktor-Authentisierung mit Hilfe einer Chipkarte und einem Passwort an, was die Sicherheit im Vergleich zur Anmeldung mit Benutzername und Passwort deutlich erhöht.

Gehaltsnachweise und anderweitige Informationen, die ein erhöhtes Schutzbedürfnis haben, können von den Mitarbeitern zukünftig online angesehen und ausgedruckt werden. Als Authentisierung kann dabei die sichere Anmeldung am PC/Fachverfahren mittels einer Chipkarte (z. B. multifunktionale Chipkarte) oder auch eID-Funktion des nPA verwendet werden.

2.8.3 Funktionsweise

Mit Schriftformerfordernis

Nach dem Ausfüllen des Antrags führt der Mitarbeiter seine Chipkarte mit der QES in das Lesegerät und gibt seine PIN ein. Die QES wird von der Karte gelesen und das Dokument unterzeichnet. Anschließend kann das signierte Dokument via E-Mail oder innerhalb eines Fachverfahrens versendet werden. Der Empfänger öffnet das Dokument, die Gültigkeit der QES wird automatisch überprüft. Nach der Bearbeitung des Falles wird die Genehmigung oder Ablehnung elektronisch erstellt (ggf. innerhalb eines Fachverfahrens), mit einer QES unterzeichnet und an den Absender zurückgesendet.

Ohne Schriftformerfordernis

Der Mitarbeiter meldet sich mit Chipkarte und PIN am PC an und öffnet das entsprechende Fachverfahren oder den erforderlichen Online-Antrag. Nach dem Ausfüllen bestätigt der Anwender die Richtigkeit der Daten und sendet den Auftrag ab. Der für die Antragsbearbeitung zuständige Mitarbeiter erhält eine elektronische Nachricht über den Eingang des Antrages. Die Antragsbearbeitung erfolgt innerhalb des Fachverfahrens und der Antragsteller kann auf demselben Weg über das Ergebnis informiert werden. Sinnvoll ist ein solches Vorgehen etwa für Verfahren mit besonders hohen Sicherheitsanforderungen.

Datenabruf

Zum Abrufen sensibler Daten kann das gleiche Verfahren wie für die Antragstellung ohne Schriftformerfordernis verwendet werden. Nach der Anmeldung mit Chipkarte und PIN ist der Zugriff auf die ge-

wünschten Daten möglich. Sinnvoll erscheint dies ebenfalls für Anwendungen mit hohen Sicherheitsanforderungen, etwa dem Abruf einer elektronischen Gehaltsabrechnung.

Alternativ könnte auch die eID-Funktion hierfür verwendet werden. Dazu öffnet der Mitarbeiter zunächst das entsprechende Programm. An der erforderlichen Stelle im Authentisierungsprozess legt der Mitarbeiter den neuen Personalausweis auf ein entsprechendes Lesegerät und bestätigt das Auslesen der Daten mit seiner PIN. Anschließend hat er Zugriff auf die gewünschten Daten.

2.8.4 Voraussetzungen

- Chipkarten (mit QES für Anträge mit Schriftformerfordernis) zur Anmeldung am PC.

  Die Mitarbeiter sind mit entsprechenden Chipkarten auszurüsten. Die Karten müssen an zentraler Stelle ausgegeben und eingesammelt werden können (z. B. beim Ausscheiden eines Mitarbeiters oder bei Praktikanten).

- Lesegeräte

  Die Arbeitsplätze müssen bei Verwendung von Chipkarten mit Lesegeräten (mind. Klasse 2) oder speziellen Tastaturen mit integriertem Kartenleser ausgestattet werden.

- Elektronische Anträge/Fachverfahren

  Die Anträge müssen in elektronischer Form bzw. innerhalb der Fachverfahren vorhanden sein.

- nPA mit aktivierter eID-Funktion

  Für die Verwendung der eID-Funktion muss der Mitarbeiter über einen nPA mit freigeschalteter eID-Funktion verfügen.

- eID-Infrastruktur

  Die Kommune oder der Diensteanbieter muss bei Verwendung der eID-Funktion auch die dafür benötigten eID-Komponenten (Zertifikate, eID-Service) beschaffen bzw. bereitstellen.

2.8.5 Kurzbewertung

Das **Erfordernis** der internen Antragstellung ist in allen Kommunen gegeben.

Der **Einsatz elektronischer Lösungen** findet sich in den meisten Kommunen, die QES wird hierzu in nahezu keiner Behörde verwendet.

Die **Anzahl der Betroffenen** umfasst alle Mitarbeiter einer Kommune.

Die **Hauptvorteile** sind die beschleunigte Abwicklung (Medienbruchfreiheit) und die Rechtssicherheit.

2.9 Kantine und Verpflegungsautomaten

Die Bezahlung in Kantine, Cafeteria und/oder an Verpflegungsautomaten erfolgt häufig noch mit Bargeld oder Essensmarken. Hier kann für die Mitarbeiter eine bargeldlose Bezahlung realisiert werden.

2.9.1 Aktuelle Situation

Die Bezahlung in Kantinen kann über verschiedene Bezahlsysteme organisiert sein. Diese sind Barzahlung, (mit Bargeld erworbene) Essensmarken, EC-Geldkartenfunktion, Plastikkarte mit Magnetstreifen oder die Verwendung von Chipkarten oder Schlüsselanhängern mit integriertem Chip. Die Bezahlung bei den letztgenannten Verfahren erfolgt entweder durch Aufladen und Abbuchen auf bzw. von einer Karte oder die Beträge werden monatlich summiert vom Gehalt abgezogen. Gemeinsam ist allen, dass die Abrechnung seitens der Kommune (bzw. dem Betreiber der Kantine) weniger aufwändig ist, wenn kein Bargeld verwendet wird. Für die Mitarbeiter ist es ebenfalls einfacher, wenn sie nicht immer Bargeld zur Hand haben müssen. Auch bei Verpflegungsautomaten mit Süßigkeiten, Kaltgetränken oder Kaffee ist zumeist die Bezahlung mit Bargeld oder Wertmarken üblich. Hier entstehen durch die Barzahlung ebenso Aufwände.

2.9.2 Zukünftige Situation

Zukünftig können die Mitarbeiter in der Kantine und an den Automaten bargeldlos mit einer Chipkarte bezahlen. Dazu führen sie an der Kasse oder Essensausgabe die Karte an einem Lesegerät vorbei. Die Beträge werden über den Monat hinweg summiert und vom Gehalt abgezogen oder in Rechnung gestellt. Am Ende des Monats erhält jeder Mitarbeiter elektronisch einen Auszug über seine Ausgaben für Kantine und Automaten. Alternativ ließe sich die Karte auch (prepaid) über einen Aufladeautomaten laden. An der Kasse würde dann der jeweilige Geldbetrag abgebucht werden. Für die Kommune oder den Kantinenbetreiber entfallen in jedem Fall der Verkauf von Essens- oder Wertmarken und die umständliche sowie aufwändige Handhabung von Barkassen.

2.9.3 Funktionsweise

Für die Bezahlung können abhängig vom vorhandenen oder zu beschaffenden System unterschiedliche

Verfahren zum Einsatz kommen. Mit seiner Karte kann ein Mitarbeiter in der Kantine identifiziert werden. Dabei ist es lediglich notwendig, dass eine eindeutige Kennung ausgelesen wird, die dem Mitarbeiter zugewiesen ist. Die Zuordnung wird innerhalb der Software durchgeführt. Diese Software ist mit der Buchhaltung verbunden, so dass die Beträge aus der Kantine direkt vom Gehalt abgezogen und an den Betreiber der Kantine oder das entsprechende Konto der Kommune überwiesen werden können. Bei Automaten kann die Verwendung einer direkten Anbindung an die Buchhaltung zu aufwändig sein. Hier gibt es die Alternative, dass die Daten der Automaten zunächst nur gesammelt und dann einmal pro Monat ausgelesen und in die Buchhaltungssoftware zur weiteren Verarbeitung überspielt werden.

2.9.4 Voraussetzungen

- Infrastruktur in der Kantine

  Für die bargeldlose Bezahlung in der Kantine muss dort die erforderliche Infrastruktur vorhanden sein oder geschaffen werden. Dazu gehören primär die geeigneten Lesegeräte und ggf. deren Anbindung an das Datennetz.

- Geeignete Automaten

  Soll auch an Automaten mit Chipkarten bezahlt werden können, müssen diese dafür ausgerüstet sein oder nachgerüstet werden.

- Chipkarten

  Die Mitarbeiter sind mit entsprechenden Chipkarten auszurüsten. Die Karten müssen an zentraler Stelle verwaltet, ausgegeben und wieder eingesammelt werden können (z. B. beim Ausscheiden eines Mitarbeiters oder bei Praktikanten).

- Software

  Passend zu den Chipkarten muss eine spezielle Software angeschafft werden, mit der die Karte ausgelesen oder die Beträge abgebucht werden können.

- Schnittstellen

  Bei der Anschaffung der Software ist darauf zu achten, dass die nötigen Schnittstellen zur Buchhaltungssoftware vorhanden sind oder geschaffen werden können. Diese Schnittstellen müssen sowohl die strukturellen Anforderungen an das Format der Daten erfüllen, als auch die inhaltliche Interpretation der Informationen semantisch korrekt zulassen. Wäre dies nicht möglich, müssten die summierten Beträge jeweils entweder halbautomatisch oder im schlimmsten Fall sogar manuell in

die Buchhaltung übernommen werden. Alternativ könnten den Mitarbeitern auch Rechnungen ausgestellt werden, was aber wiederum mit zusätzlichem hohen Aufwand und weiteren Schritten (Mahnungen bei Nichtbezahlung usw.) verbunden wäre. Hier wird beispielhaft deutlich, dass die Einführung einer Ergänzungstechnologie bezüglich ihrer Anbindung an bestehende organisatorische Lösungen intensiv prüft werden muss, weil sonst auf Dauer nicht vertretbare Kosten verursacht werden.

- Berücksichtigung aller bestehender und geplanter Komponenten

  Bei der Anschaffung sollten im Sinne der genannten semantischen Integration die bereits vorhandene und auch die geplanten Komponenten wie Zeiterfassung, Single-Sign-On (SSO), Zugangskontrolle, Signaturen usw. berücksichtigt werden. Ohne den Entwurf eines Gesamtkonzeptes für die Informationsverarbeitung ist das jedoch kaum möglich.

2.9.5 Kurzbewertung

Das **Erfordernis** von Kantine und Verpflegungsautomaten ist nur in wenigen Kommunen gegeben.

Der **Einsatz elektronischer Lösungen** zur bargeldlosen Bezahlung findet sich nur in wenigen Kommunen.

Die **Anzahl der Betroffenen** umfasst grundsätzlich alle Mitarbeiter einer Kommune. Abweichungen können bei besonderen örtlichen Gegebenheiten auftreten (z. B. viele Außenstellen).

Die **Hauptvorteile** sind die vereinfachte Abrechnung und die erhöhte Mitarbeiterzufriedenheit.

2.10 Online-Antragstellung für Bürger und Unternehmen

Unter den derzeit bestehenden Möglichkeiten, sich gegenüber einer Behörde zu identifizieren und Anträge online zu stellen, ist der neue Personalausweis (nPA) zwar noch die Ausnahme, aber unter dem Gesichtspunkt der Sicherheit und der Verbindlichkeit die vielversprechendste Variante. Für die Online-Antragstellung werden daher in den nachfolgenden Abschnitten speziell die Funktionen des nPA berücksichtigt.

2.10.1 Aktuelle Situation

Bei der Antragstellung ist das persönliche Erscheinen der Bürger bei der Behörde noch vorherrschend. Dies hat seine Ursachen in der notwendigen Identifikation der Antragsteller, dem Schriftformerfordernis, dem

Beifügen von Originalunterlagen, dem persönlichen Aushändigen von Unterlagen an den Antragsteller und der Bezahlung von Gebühren. Teilweise können Formulare bereits heute online ausgefüllt und abgeschickt werden. Der Antragsteller muss in vielen Fällen aber dennoch zusätzlich zur Identifikation und/oder Unterschriftsabgabe persönlich erscheinen, sofern dies gesetzlich vorgeschrieben ist oder von der Kommune verlangt wird. Erschwert wird die Online-Antragstellung auch deshalb, weil es keinen umfassenden und allgemeingültigen Katalog gibt, aus dem ersichtlich wird, für welche Anträge überhaupt das Schriftformerfordernis notwendig ist. In der kommunalen Praxis ist nahezu jeder Papierantrag mit einem Unterschriftsfeld für den Antragsteller versehen, ganz gleich, ob die eigenhändige Unterschrift explizit vorgeschrieben ist oder nicht.

2.10.2 Zukünftige Situation

Künftig verfügt ein größerer Teil der Bürger über einen nPA mit aktivierter elektronischer Identitätsfunktion (eID-Funktion). Die Antragstellung kann daher vollständig via Internet auch für diejenigen Anträge erfolgen, für die bisher eine Identifikation, d. h. das persönliche Erscheinen erforderlich war. Daten und Dokumente (auch vertraulicher Art) können zwischen Verwaltung, Bürgern und Unternehmen elektronisch ausgetauscht werden. Die im elektronischen Antrag übermittelten Daten werden direkt in die Fachverfahren übernommen und dort weiterverarbeitet. Originalunterlagen müssen nur noch in Ausnahmefällen beigefügt werden. Bezahlt werden kann ebenfalls über das Internet via Lastschrift oder E-Payment. Aufgrund der dafür fälligen Gebühren und der negativen Werbung ist nicht zu erwarten, dass die qualifizierte elektronische Signatur (QES) eine substanziell größere Verbreitung als heute finden wird. Auch die Möglichkeit, sie auf den nPA zu übertragen, wird dies nicht ändern.. Es ist daher erforderlich, dass das neue E-Government-Gesetz dieser Tatsache Rechnung trägt und das Schriftformerfordernis bzw. das Erfordernis der QES zugunsten anderer Verfahren reduziert. Großes Potenzial bietet hierfür Der seit Frühjahr 2012 vorliegende Referentenentwurf des eGovernment-Gesetzes bietet mit der DE-Mail bzw. der eID-Funktion des nPA zwei mögliche Alternativen..

Für Unternehmen ist die Situation identisch, sofern es sich um Einzelunternehmer handelt oder die Mitarbeiter bereit sind, ihren Personalausweis auch dienstlich zu verwenden. Jedoch muss hier zunächst sichergestellt werden, dass eine Person auch im Namen eines Unternehmens handeln darf bzw. dort beschäftigt ist. Für den Kfz-Bereich können alleine mit Hilfe von eID-Funktion und QES keine wesentlichen Verbesserungen erreicht werden, da derzeit noch Papierdokumente erforderlich sind. Bis zum Einsatz der vollelektronischen Zulassung wäre aber denkbar, dass für diese Gruppen ein spezieller Zugriff auf die Zulassungssoftware eingerichtet wird, für den die Anmeldung mittels eID-erforderlich ist. Die nötigen Unterlagen

könnten dabei auf dem Postweg versendet werden. Im Rahmen des Deutschland-Online Vorhabens „Kfz-Wesen“ ist zudem die An-, Um und Abmeldung über das Internet geplant.

2.10.3 Funktionsweise

Eine neue und sehr sichere Möglichkeit zur Identifikation des Bürgers über das Internet bietet die eID-Funktion des nPA. Ferner lässt sich damit auch ein Teil der auf dem Ausweis gespeicherten Daten für die Antragsbearbeitung direkt auslesen. Die eID-Funktion kann für die Antragstellung in zwei unterschiedlichen Verfahrensweisen verwendet werden:

- Anmeldung an einem Bürgerservice-Portal

  Verfügt eine Kommune über ein Bürgerservice-Portal, können sich die Bürger dort mit der eID-Funktion registrieren und ein Benutzerkonto einrichten. Nach der Anmeldung mit dem Ausweis und einer PIN sind sie identifiziert und können Anträge ausfüllen und weitere Funktionen eines solchen Portals nutzen. Im Portal kann der Benutzer etwa seine Adressdaten, Geburtstag usw. hinterlegen. Diese Daten müssen dann bei einem weiteren Antrag nicht noch mal eingegeben werden. Bei der erneuten Anmeldung wird nur noch die Pseudonymfunktion (Dienste- und kartenspezifisches Kennzeichen) zur Identifikation des Nutzers ausgelesen. Weitere Daten werden dabei nicht übertragen.

- Ausfüllen von Anträgen

  Auch ohne Bürgerservice-Portal können Anträge mit der eID-Funktion gestellt werden. Dazu füllt er den betreffenden Antrag (z. B. spezielles PDF-Formular) aus, wobei ein Teil der erforderlichen Daten direkt aus dem Ausweis übernommen wird. Will der Anwender zu einem späteren Zeitpunkt einen weiteren Antrag ausfüllen und absenden, beginnt die Prozedur von neuem. Im Gegensatz zur Portallösung können die Bürger keine eigenen Daten hinterlegen oder zusätzliche Funktionen in Anspruch nehmen.

Dem Erfordernis der Schriftform kann bei beiden oben genannten Verfahren nachgekommen werden, sofern eine QES auf den nPA aufgebracht wurde.

2.10.4 Voraussetzungen

Nachfolgend werden die notwendigen Voraussetzungen sowohl technischer als auch organisatorischer Art für eine Online-Antragstellung benannt und beschrieben.

- Bürger, Unternehmen – Aktivierte eID-Funktion

  Auf Bürgerseite bzw. auf Unternehmensseite ist es erforderlich, dass die eID-Funktion des nPA aktiviert ist.

- Bürger, Unternehmen – Qualifizierte elektronische Signatur (QES)

  Um Anträge elektronisch unterzeichnen zu können, ist auf Seite der Bürger und Unternehmen eine QES und ein entsprechendes Lesegerät erforderlich. Nutzer des nPA, die eine QES nachladen möchten, müssen dafür ein Lesegerät der Kategorie K (Komfort) verwenden.

  Derzeit laufen Tests mit einer sogenannten Ad-hoc-Signatur für den nPA, die eine Unterschrift nur für einen kurzen Zeitraum und nur für bestimmte Transaktionen ermöglicht, dafür aber innerhalb weniger Minuten geladen werden kann und außerdem deutlich günstiger in der Anschaffung sein soll.

- Bürger, Unternehmen – Software zum Auslesen der Ausweisdaten (AusweisApp)

  Um die Daten aus dem nPA auszulesen und die Zertifikate der Diensteanbieter überprüfen zu können, ist seitens der Bürger und Unternehmen noch eine spezielle (kostenlose) Software erforderlich (z. B. AusweisApp).

- Kommune, Unternehmen – Online-Anträge/Bürgerservice-Portal

  Um die eID-Funktion und/oder die QES seitens der Bürger und Unternehmen einzubinden, ist eine spezielle technische Infrastruktur erforderlich. Möglich sind hierbei Bürgerservice-Portale und spezielle PDF-Formulare, die mit den erforderlichen Funktionen zur Verwendung mit dem nPA nachgerüstet oder neu beschafft werden.

- Kommune – eID-Infrastruktur

  Um die eID-Funktion nutzen zu können, sind verschiedene technische Aspekte zu berücksichtigen. Zum einen sind entsprechende Zertifikate erforderlich, die von der Kommune oder dem Softwarehersteller bereitgestellt werden. Zum anderen ist ein eID-Servicebetrieb erforderlich, der als Dienstleistung in Anspruch genommen werden sollte. Der eID-Service wird vom LfStaD kostenlos als Infrastrukturkomponente zur Verfügung gestellt.

- Kommune – Auswahl geeigneter Prozesse

  Die Auswahl geeigneter Prozesse für die Nutzung der eID-Funktion ist entscheidend für die Akzeptanz beim Bürger und auch innerhalb der Behörde.

- Kommune – Organisatorische Anpassungen

  Für die Nutzung der eID-Funktion und evtl. der QES sind organisatorische Anpassungen erforderlich. Z. B. müssen Abläufe neu gestaltet werden, wenn Bürger bspw. nicht bei der Antragstellung vor Ort vorsprechen, sondern die Anträge online an die Mitarbeiter versenden.

- Kommune – Folgeaktivitäten und Gesamtkonzept

  Die Online-Antragstellung darf nicht als isolierter Schritt betrachtet werden, sondern es müssen auch nachgelagerte Tätigkeiten und Funktionen berücksichtigt werden. Bei einem komplett elektronischen Antragseingang ist z. B. die Aufbewahrung in Papierform nicht mehr erforderlich. Jedoch muss hierfür ein geeignetes Dokumentenmanagement-System bereitstehen und für diese Aufgabe angepasst werden.

- Kommune – Integration in Fachverfahren

  Damit auch die Kommune aus der Online-Antragstellung größtmöglichen Nutzen ziehen kann, ist eine medienbruchfreie und weitgehend automatische Übertragung der Daten vom PC des Benutzers bis in das Fachverfahren von Vorteil. Welche Fachverfahren über entsprechende Schnittstellen verfügen und für welche Anträge bzw. Verwaltungsvorgänge eine vollständige Integration möglich ist, muss mit dem jeweiligen Fachverfahrenshersteller geklärt werden. Bisher ist die automatische Übernahme von Daten in das Fachverfahren nur in einigen Fällen möglich, so dass nicht alle Potenziale realisiert werden können, die eine Online-Antragstellung bietet.

- Schriftformerfordernis

  Für viele Anträge ist die Unterschrift des Antragstellers gesetzlich nicht erforderlich, wird aber bei fast allen Anträgen verlangt. Dies kann darin begründet sein, dass es im Ortsrecht oder in Formularen der jeweiligen Kommune so festgelegt wurde oder „etwas Schriftliches“ vom Antragsteller verlangt wird, das seine Willenserklärung eindeutig dokumentiert. Es bleibt zunächst abzuwarten, welche Änderungen das E-Government-Gesetz in dieser Hinsicht bringen wird. Unabhängig davon muss es das Ziel sein, die eigenhändige Unterschrift bzw. die QES nur dann zu verlangen, wenn es unumgänglich und gesetzlich vorgeschrieben ist.

- Bezahlfunktion

  Viele Anträge sind für die Antragsteller kostenpflichtig. Der Nachweis der Bezahlung erfolgt in der Regel durch einen Beleg bei Barzahlung, eine Quittung bei Überweisung oder mittels Lastschriftverfahren. Um daher nicht nur den Prozess der Antragstellung, sondern den Gesamtablauf zu beschleunigen, muss sich die Kommune überlegen, wie auch die Bezahlung der anfallenden Kosten

elektronisch durchgeführt werden kann (z. B. E-Payment, Kreditkarten, Einzugsermächtigung usw.).

- Bürger, Unternehmen – Kosten

  Für den Ausweisinhaber entstehen außer für die Anschaffung des nPA (derzeit 28,80 €) noch weitere Kosten. Für ein einfaches Lesegerät (Basisleser Kategorie B), das für die Nutzung der eID-Funktion ausreicht, fallen ca. 30 € (ohne Förderung, Stand: September 2011) an. Soll der Ausweis um die QES erweitert werden, fallen noch für diese Signatur Kosten und ca. weitere 120 € (ohne Förderung, Stand: September 2011) für ein Komfortlesegerät (Kategorie K) an (die Preise gelten für die Kartenleser der Firma REINER Kartengeräte GmbH und Co. KG, Stand November 2011).

- Kommune – Kosten

  Die Kosten für eine Kommune bemessen sich daran, welche Infrastruktur vorhanden ist. Nicht im Aufwand zu unterschätzen sind organisatorische Änderungen bzw. die damit einhergehenden Prozessuntersuchungen sowie deren Auswahl und Anpassung.

  Die zum Auslesen der Daten aus dem nPA erforderlichen Berechtigungszertifikate, sind z. B. im Bürgerservice-Portal der AKDB integriert. Dies beinhaltet auch die Nutzung des eID-Services.

  Wird eine andere Lösung präferiert, müssen diese Zertifikate von der Kommune selbst beantragt und beschafft werden.

2.10.5 Kurzbewertung

Das **Erfordernis** der Antragstellung für Bürger und Unternehmen ist in allen Kommunen gegeben.

Der **Einsatz elektronischer Lösungen** findet sich nur in wenigen Kommunen.

Die **Anzahl der Betroffenen** umfasst grundsätzlich alle Verwaltungskunden einer Kommune.

Die **Hauptvorteile** sind die beschleunigte Abwicklung (Medienbruchfreiheit) und erhöhter Bürgerservice.

2.11 Sichere Anmeldung am PC

Die vorherrschende, nur bedingt sichere Vorgehensweise zur Anmeldung am PC durch Verwendung von Benutzername und Passwort kann für die Mitarbeiter durch weitaus sicherere Verfahren ersetzt werden.

2.11.1 Aktuelle Situation

Für die Anmeldung am Arbeitsplatzrechner ist die Verwendung von Benutzerkennung (Login) und Passwort das am weitesten verbreitete Verfahren. Passwörter werden im Normalfall so gewählt, dass sie vom Benutzer leicht zu merken sind. Es gibt zwar Vorgaben, wie z. B. eine Mindestanzahl an Zeichen oder die Kombination aus Ziffern und Buchstaben sowie Groß- und Kleinschreibung. Dennoch sind personengenerierte Passwörter grundsätzlich unsicherer, als zufallsgenerierte vom Rechner. Zur Erhöhung der Sicherheit müssen die Passwörter daher in regelmäßigen Abständen verändert werden, was häufig dazu führt, dass die Passwörter nur geringfügig geändert oder aufgeschrieben und in der Nähe des PCs aufbewahrt werden.

Das Problem besteht einerseits darin, dass sich Unbefugte am Rechner anmelden und unberechtigt Daten einsehen oder verändern können. Zum anderen lässt sich evtl. nicht mehr nachvollziehen, welcher Mitarbeiter welchen Sachverhalt bearbeitet hat. Denn die Authentifizierung am Rechner oder an einem Fachverfahren dient auch als Nachweis, wer welche Vorgänge bearbeitet oder selbst intern Anträge gestellt hat. Daher sind „Unbefugte“ in diesem Sinn auch Mitarbeiter, die Login und Passwort ihrer Kollegen kennen, weil sie diese z. B. im Rahmen einer Urlaubs- oder Krankheitsvertretung erhalten haben.

2.11.2 Zukünftige Situation

Die Anmeldung kann künftig durch eine sogenannte Zwei-Faktor-Authentisierung durchgeführt werden. Dabei erhält jeder Anwender eine Chipkarte und eine geheime PIN. Zur Anmeldung am Rechner wird die Karte in ein Lesegerät eingeführt, das mit dem Rechner verbunden ist. Anschließend gibt der Anwender die PIN ein. Neben dem Schlüssel ist auch noch ein sogenanntes Authentifizierungszertifikat hinterlegt, das die Echtheit des Schlüssels beweist. Die erhöhte Sicherheit entsteht dadurch, dass für eine Anmeldung immer sowohl die Chipkarte mit dem gültigen Schlüssel und Zertifikat wie auch die korrekte PIN verfügbar sein müssen (Zwei-Faktor-Authentisierung). Das System kann auch so konfiguriert werden, dass der Rechner automatisch gesperrt wird, wenn die Karte aus dem Lesegerät entfernt wird (z. B. wenn der Mitarbeiter zum Drucker oder in die Pause geht). Während sich also beim herkömmlichen Verfahren ein Unbefugter anmelden kann, wenn er Login und Passwort (welches häufig leicht zu erraten ist) des „Opfers“ kennt, benötigt er im hier dargestellten Szenario immer sowohl die Karte wie auch die PIN. Dies trägt erheblich zur Erhöhung des Sicherheitsniveaus auch gegenüber Hilfspersonal (Reinigung, Handwerker, Servicetechniker, IT-Berater etc.) bei.

2.11.3 Funktionsweise

Wesentlich für die sichere Anmeldung in der beschriebenen Weise sind Schlüssel und Authentifizierungszertifikat (Login-Zertifikat), die auf die Karte aufgebracht werden. Für das Auslesen der Schlüssel und die Prüfung der Zertifikate wird eine spezielle Software (Middleware) installiert. Die Karte wird in einen Kartenleser gesteckt. Das Betriebssystem liest in Verbindung mit der Middleware den Schlüssel und das Zertifikat aus. Über eine Online-Verbindung wird jedes Mal die Gültigkeit des Zertifikates abgefragt und anschließend die Richtigkeit der PIN geprüft. Sind alle Angaben korrekt, ist der Anmeldevorgang abgeschlossen und der Anwender kann mit dem PC arbeiten. Durch die Zertifikatsprüfung am Anfang kann der Anmeldevorgang jedoch geringfügig länger dauern.

Falls der Mitarbeiter die Karte vergisst, kann ihm auch eine Ersatzkarte ausgestellt werden oder der Anmeldevorgang ausnahmsweise ohne Karte, aber mit einer speziellen Benutzerkennung und einem Einmal-Passwort erlaubt werden. Bei Verlust der Karte oder Ausscheiden des Mitarbeiters wird die Karte eingezogen und/oder das Login-Zertifikat gesperrt und somit der Zugriff des Mitarbeiters unterbunden.

2.11.4 Voraussetzungen

- Chipkarten

  Die Mitarbeiter sind mit entsprechenden Chipkarten auszurüsten. Die Karten müssen an zentraler Stelle ausgegeben und eingesammelt werden können (z. B. beim Ausscheiden eines Mitarbeiters oder bei Praktikanten).

- Lesegeräte

  Die Arbeitsplätze müssen bei Verwendung von Chipkarten mit Lesegeräten oder speziellen Tastaturen mit integriertem Kartenleser ausgestattet werden.

- Middleware für Chipkarten

  Für das Auslesen der Schlüssel und Zertifikate von den Chipkarten ist eine spezielle Software (Middleware) erforderlich. Diese steuert den Kartenleser und wird für die Zertifikatsprüfung benötigt.

- Zertifikate und Schlüssel

  Für den Nachweis der Echtheit der Karten müssen diese mit Zertifikaten und Schlüsseln ausgestattet werden. Hier ist zu prüfen, welche Institution die Zertifikate und Schlüssel auf den Chip überträgt und wo dies durchgeführt wird. Diese Schlüssel und Zertifikate können über Trustcenter, das LfStaD oder auch direkt von einem MS-Windows-Server erzeugt werden. Im kommunalen Umfeld

sind aufgrund der weiten Verbreitung von MS-Windows meist diese Zertifikate im Einsatz. Sie können entweder in der Kommune selbst (kostenlos) oder von einem Dienstleister erzeugt werden. Die Prüfung der Zertifikate bei der Anmeldung des Benutzers am PC erfolgt dann ebenfalls durch einen MS-Windows-Server entweder in der Komme oder beim Dienstleister.

- Berücksichtigung aller bestehenden und geplanten Komponenten

  Schon bei der Konzeption zur Einführung einer solchen Komponente sollten bereits vorhandene oder weitere geplante Komponenten wie Zeiterfassung, SSO, Bezahlung in der Kantine, Zutrittskontrolle, Signaturen usw. berücksichtigt werden, um spätere Inkompatibilitäten zu vermeiden.

2.11.5 Kurzbewertung

Das **Erfordernis** der Anmeldung am PC ist in allen Kommunen gegeben.

Der **Einsatz elektronischer Lösungen** mit Chipkarten findet sich (flächendeckend) in keiner Kommune.

Die **Anzahl der Betroffenen** umfasst grundsätzlich alle Mitarbeiter einer Kommune mit PC-Zugang.

Die **Hauptvorteile** sind die erhöhte Mitarbeiterzufriedenheit und die erhöhte Sicherheit.

2.12 Single-Sign-On (SSO)

Single-Sign-On ermöglicht es den Mitarbeitern mit nur einer einzigen Anmeldung am PC eine Vielzahl an Programmen zu verwenden, ohne sich für jedes separat mit Benutzernamen und Passwort anmelden zu müssen.

2.12.1 Aktuelle Situation

Die Anmeldung am PC betrifft in erster Linie die Mitarbeiter, aber auch die IT-Administration, die für die Sicherheit der PC-Arbeitsplätze und der gesamten IT-Infrastruktur verantwortlich sind. Die nachfolgende Beschreibung erfolgt daher jeweils aus Sicht der Mitarbeiter bzw. der IT-Administration.

- Mitarbeitersicht

  Die Mitarbeiter in Behörden melden sich mit einem Benutzernamen und Passwort am PC an. Zur Nutzung von Fachverfahren, Internetportalen (z. B. für das Kraftfahrtbundesamt, für Sozialversicherungsmeldungen usw.) sind separate Anmeldedaten nötig. Für die Mitarbeiter kann es eine Belastung sein, sich einerseits viele Passwörter merken zu müssen und andererseits zu wissen, dass der

Schutz dennoch nicht sehr hoch ist. Auch führt das Zurücksetzten vergessener Passwörter durch die IT-Abteilung oft zu unerwünschten Arbeitsunterbrechungen.

- Administrationssicht

Sicherheitsaspekte

Um die Sicherheit zu erhöhen, müssen die Passwörter in regelmäßigen Abständen geändert werden. Ebenfalls aus Sicherheitsgründen müssen bzw. sollten für alle verwendeten Fachverfahren unterschiedliche Passwörter verwendet werden. Diese beiden Sicherheitsvorkehrungen bewirken aber nicht selten, dass gerade dadurch das Sicherheitsniveau sinkt. Denn durch die hohe Änderungsfrequenz werden erstens nicht für alle Applikationen auch unterschiedliche Passwörter verwendet. Zweitens werden die Passwörter häufig auf Papier oder im Rechner notiert. Drittens werden vergleichsweise einfache Passwörter verwendet bzw. mit einer laufenden Nummer versehen, damit sie leichter zu merken sind. Das Sicherheitsniveau wird in vielen Fällen auch dadurch gesenkt, dass Kollegen die Zugangskennung für bspw. Urlaubs- oder Krankheitsvertretungen erhalten.

Vergessene Passwörter

Durch die Anzahl an Passwörtern und deren häufigen Wechsel vergessen Mitarbeiter oft ein oder auch mehrere Passwörter (häufig nach dem Urlaub). In diesem Fall muss die IT-Abteilung oder ein für diese Fälle geschulter Mitarbeiter um Hilfe gebeten werden. Das Passwort der Anwendung wird dann zurückgesetzt, der Mitarbeiter vergibt ein neues Passwort und kann weiterarbeiten. Wurde bei einer Portalanwendung das Passwort vergessen, muss entweder der Support des Portalbetreibers informiert werden oder es stehen Funktionen zur Verfügung, mit denen der Mitarbeiter sich selbst ein neues Passwort vergeben kann.

Praktikanten und Wechsler

Innerhalb der Fachbereiche arbeiten zeitlich begrenzt oftmals Praktikanten oder Hospitanten aus anderen Fachabteilungen. Für diese Mitarbeiter beantragen die Leiter der Fachdienststellen die entsprechenden Zugangsberechtigungen (Rollen mit Benutzernamen und Passwörtern) für Fachverfahren und Portale. Nach Beendigung ihrer Tätigkeit wird häufig vergessen, an die IT-Abteilung die Beendigung der Tätigkeit und somit auch den Entzug der Berechtigungen zu melden. In manchen Fällen ist auch gar nicht mehr bekannt, für welche Programme überhaupt Berechtigungen erteilt wurden. Dies gilt auch für Mitarbeiter, die die Abteilung wechseln oder die Behörde verlassen. Dadurch ergeben sich verschiedene negative Aspekte. Es entstehen z. B. „Karteileichen“ in Form von Benutzerkonten und Berechtigungen, von denen in der IT-Abteilung nicht bekannt ist, ob sie

noch aktuell sind und benötigt werden. Gravierender ist aber, dass Mitarbeiter nach dem Verlassen der Abteilung u. U. immer noch Zugriff auf alle oder einige Programme haben.

2.12.2 Zukünftige Situation

Die nachfolgend beschriebene Version des SSO ist eine Erweiterung des sicheren Anmeldens am PC. Die Erweiterung bezieht sich darauf, dass die Verwendung einer Chipkarte und PIN neben der Anmeldung am PC auch die Anmeldung an die verschiedenen Programme einschließt.

Verbesserungen ergeben sich sowohl für die Mitarbeiter wie auch für die IT-Administration.

- Mitarbeitersicht

  In Zukunft verfügt jeder Mitarbeiter über eine Chipkarte. Diese wird in ein Lesegerät gesteckt, das in die Tastatur integriert ist oder separat daneben steht. Der Mitarbeiter muss bei der Anmeldung am PC nur noch eine PIN eingeben und kann alle Fachverfahren und Portale, die für seine Tätigkeit erforderlich sind, ohne weitere Eingabe eines Benutzernamens oder Passwortes verwenden. Verlässt ein Mitarbeiter den Arbeitsplatz weil er bspw. in die Pause geht, entnimmt er seine Chipkarte aus dem Lesegerät, sein PC ist dadurch automatisch gesperrt.

- Administrationssicht

  Sicherheitsaspekte

  Durch die Zwei-Faktor-Authentisierung erhöht sich das Sicherheitsniveau deutlich. Das missbräuchliche Verwenden eines Benutzerkontos (mit oder ohne Zustimmung des Kontoinhabers) ist dadurch nicht mehr möglich, es sei denn, Karte und PIN stehen dem Unbefugten zur Verfügung.

  Keine (vergessenen) Passwörter

  Die Chipkarten werden von einer Abteilung (Personal, IT oder Organisation) an die Mitarbeiter vergeben. In der SSO-Software sind die Programme, die die jeweiligen Mitarbeiter benötigen mit der Karte „verknüpft“. Die Mitarbeiter benötigen daher nur noch eine einzige PIN, was deutlich einfacher zu merken ist, als eine Reihe von Passwörtern. Dies wiederum führt dazu, dass die PIN seltener vergessen wird, was auch weniger Aufwand für die IT-Abteilung bedeutet.

  Praktikanten und Wechsler

  Praktikanten können ebenfalls diese Karten erhalten und haben dann die erforderlichen Berechtigungen. Nach Beendigung des Praktikums geben sie ihre Karte zurück und haben damit auch keinerlei Zugriff mehr auf die Systeme. Wird vergessen, die Karte zurückzugeben, so ist lediglich die

Chipkarte zu sperren und der Zugriff auf alle damit verbundenen Applikationen ist ebenfalls gesperrt. Auch eine Befristung der Chipkarten ist von vornherein möglich.

2.12.3 Funktionsweise

Für das hier beschriebene Single-Sign-On gibt es mehrere technische Realisierungsmöglichkeiten, wobei die folgende Vorgehensweise allgemein gebräuchlich ist: In der SSO-Software sind die Benutzerrollen und die dafür nötigen unterschiedlichen Benutzernamen und Passwörter für die verschiedenen Anwendungen hinterlegt. Die Anmeldung am PC erfolgt mittels Chipkarte und PIN. Auf dem Chip selbst befinden sich ein Schlüssel und ein Zertifikat, das die Echtheit der Karte nachweist. Eine installierte Middleware prüft nach Einstecken der Chipkarte die Echtheit des Schlüssels/Zertifikates und stellt nach Eingabe des richtigen Passwortes die Verbindung zur Software mit den gespeicherten Passwörtern her. Startet der Anwender ein Fachverfahren, erkennt die SSO-Software dieses Programm und überträgt den dazugehörigen Benutzernamen und das Passwort für diese Applikation. Für jede Anwendung gibt es eine individuelle Kombination aus Benutzernamen und Passwort, die dem Anwender aber nicht bekannt ist. Je nach Vorgabe ändert die SSO-Software in regelmäßigen Abständen automatisch die Passwörter für die einzelnen Anwendungen.

2.12.4 Voraussetzungen

Das Single-Sign-On unter Einsatz von Chipkarten ist an die folgenden Voraussetzungen gebunden:

- Chipkarten

  Die Mitarbeiter sind mit entsprechenden Chipkarten auszurüsten. Die Karten müssen an zentraler Stelle ausgegeben und wieder eingesammelt werden können (z. B. beim Ausscheiden eines Mitarbeiters oder bei Praktikanten).

- Lesegeräte

  Die Arbeitsplätze müssen bei Verwendung von Chipkarten mit Lesegeräten oder speziellen Tastaturen mit integriertem Kartenleser ausgestattet werden.

- SSO-Software

  Passend zu den Chipkarten ist eine spezielle Software anzuschaffen, innerhalb derer die Rollen den Kombinationen aus Benutzernamen und Passwörtern zugeordnet werden können. Auch ein entsprechendes Sperrmanagement muss hinterlegt werden.

- Middleware für Chipkarten

Für das Auslesen der Schlüssel und Zertifikate von den Chips ist eine spezielle Software (Middleware) erforderlich. Diese steuert den Kartenleser und wird für die Zertifikatsprüfung benötigt.

- Zertifikate und Schlüssel

  Für den Nachweis der Echtheit der Karten müssen diese mit Zertifikaten und Schlüsseln ausgestattet werden. Hier ist zu prüfen, welche Institution die Zertifikate und Schlüssel auf den Chip überträgt und wo dies durchgeführt wird. Diese Schlüssel und Zertifikate können über Trustcenter, das LfStaD oder auch direkt von einem MS-Windows-Server erzeugt werden. Im kommunalen Umfeld sind aufgrund der weiten Verbreitung von MS-Windows meist diese Zertifikate im Einsatz. Sie können entweder in der Kommune selbst (kostenlos) oder von einem Dienstleister erzeugt werden. Die Prüfung der Zertifikate bei der Anmeldung des Benutzers am PC erfolgt dann ebenfalls durch einen MS-Windows-Server entweder in der Kommune oder beim Dienstleister.

- Organisatorische Vorbereitungen

  Die Verwendung von SSO erfordert einige organisatorische Veränderungen, die vorbereitet und durchgeführt werden müssen. Neben der Ausgabe der Karten und dem Aufspielen der Zertifikate sind auch Vorgehensweisen bei Verlust, Vergessen der Karten, Entzug und Erweiterung von Berechtigungen usw. zu regeln.

- Schnittstellen

  Single-Sign-On kann nur dann korrekt funktionieren, wenn die zu bedienenden Programme dies auch unterstützen. Hierfür gibt es unterschiedliche Technologien und Verfahren. Es ist daher mit den Herstellern oder Betreibern der Anwendungsverfahren zu klären, inwieweit deren Produkte für SSO geeignet sind.

- Berücksichtigung aller bestehenden und geplanten Komponenten

  Bei der Anschaffung sollten bereits vorhandene oder geplante Komponenten wie Zeiterfassung, Bezahlung in der Kantine, Zugangskontrolle, Signaturen usw. berücksichtigt werden.

2.12.5 Kurzbewertung

Das **Erfordernis** der Anmeldung an Fachverfahren und anderen Programmen ist in allen Kommunen gegeben.

Der **Einsatz elektronischer Lösungen** mit Chipkarten findet sich (flächendeckend) in keiner Kommune.

Die **Anzahl der Betroffenen** umfasst grundsätzlich alle Mitarbeiter einer Kommune.

Die **Hauptvorteile** sind die erhöhte Sicherheit und die erhöhte Mitarbeiterzufriedenheit.

2.13 Zeiterfassung

Durch die elektronische Zeiterfassung lassen sich die Arbeitszeiten der Mitarbeiter exakt ermitteln und automatisch auswerten. Hierbei können unterschiedliche Arbeitszeitmodelle, Urlaub, Feiertage usw. berücksichtigt werden.

2.13.1 Aktuelle Situation

Für die Zeiterfassung der Mitarbeiter gibt es unterschiedliche Vorgehensweisen. Die Arten der Zeiterfassung reichen vom Führen einer Excel-Liste durch die Mitarbeiter, über eine spezielle Software, die auch die Urlaube und Krankheitstage verwalten kann, bis zu Zeiterfassungssystemen mit Chipkarten oder anderen Hardwaretoken (z. B. Schlüsselanhänger) mit kontaktlosen Chips. In allen größeren Kommunen sind bereits chipbasierte Zeiterfassungssysteme im Einsatz.

2.13.2 Zukünftige Situation

Zukünftig sind Mitarbeiter mit einer Chipkarte ausgestattet. Beim Betreten der Dienststelle wird ihre Ankunftszeit und bei Verlassen die Endzeit festgehalten. Die Mitarbeiter haben stets Zugriff und Einblick in ihr Zeitkonto. Bei Dienstreisen werden die Zeiten am PC nachgetragen. Die unterschiedlichen Arbeitszeitmodelle sind in der Zeiterfassung hinterlegt, so dass auch Überstunden und Zuschläge automatisch errechnet werden.

2.13.3 Funktionsweise

Die Mitarbeiter halten ihre Chipkarte vor den Kartenleser. Das Lesegerät übernimmt das eindeutige Kennzeichen und überträgt es in die zugehörige Software. Diese kann automatisch die Arbeitszeiten, Überstunden, Zuschläge usw. errechnen oder die erfassten Daten an die Lohn- und Gehaltssoftware weiterleiten. Teilweise sind Zeiterfassungssysteme auch in die Zugangskontrollsysteme integriert. Für Dienstreisen oder sonstige Aufenthalte außer Haus können die Zeiten auch direkt am PC in das System eingegeben werden. Die Mitarbeiter selbst haben Zugriff auf ihre Arbeitszeitkonten und können jederzeit ihren aktuellen Stand, Urlaubs- und Fehlzeiten einsehen. Für die Zeiterfassung müssen nicht alle Lesegeräte (Terminals) mit der zugehörigen Software verbunden sein. Dies kann oft aufgrund der baulichen Situation oder der räumlichen

Entfernung zu teuer oder gar nicht realisierbar sein. Für diese Fälle gibt es spezielle Offline-Terminals. Hält ein Mitarbeiter die Karte vor das Terminal, wird die Zeitbuchung im Terminal gespeichert und kann später mit Hilfe eines PCs oder USB-Sticks ausgelesen und in das Hauptsystem übertragen werden. Bei anderen Verfahren werden die Daten nach der Buchung am Offline-Terminal auch unmittelbar auf die Karte geschrieben. Bei der nächsten Verwendung an einem Online-Terminal wird die Karte dann ausgelesen und die Buchung „nachgetragen".

2.13.4 Voraussetzungen

Zur Unterstützung der Zeiterfassung sind folgende Voraussetzungen notwendig:

- Chipkarten

  Die Mitarbeiter sind mit entsprechenden Chipkarten auszurüsten. Die Karten müssen an zentraler Stelle ausgegeben und wieder eingesammelt werden können (z. B. beim Ausscheiden eines Mitarbeiters oder bei Praktikanten).

- Lesegeräte

  Für die chipgestützte Zeiterfassung mit Chipkarten sind an den Eingängen oder an zentralen Stellen Kartenleser nötig. Bei vielen Eingängen oder einer dezentralen Infrastruktur mit mehreren Gebäuden müssen entsprechend viele Lesegeräte installiert werden.

- Management der Hard- und Software

  Die Mitarbeiter sind mit den erforderlichen Karten auszustatten, hierfür ist die Ausgabe zu organisieren. Schnittstellen zum System der Personalverwaltung (Stammdaten, Urlaubsanspruch usw.) und/oder zu anderen Systemen mit relevanten Daten müssen gepflegt werden. In größeren Kommunen gibt es häufig mehrere Arbeitszeitmodelle für unterschiedliche Bereiche. Diese sind ebenfalls im System zu hinterlegen. Schließlich müssen auch die Vorgehensweisen bei Verlust oder Vergessen der Chipkarte geregelt sein. Eine weitere Option ist das Hinterlegen von Genehmigungsabläufen z. B. für das Nachtragen von Arbeitszeiten.

- Software

  Die dazugehörige Software kann an die Software für die Personalverwaltung angebunden werden und verfügt somit über die Mitarbeiterdaten wie z. B. Urlaub, Krankheitstage usw. Diese Software sollte zudem so ausgelegt sein, dass Zeiten außer Haus ebenfalls am PC eingetragen werden können.

- Schnittstellen zu bestehenden Systemen

  Die Software für die Zeiterfassung übernimmt Aufgaben, die bisher mit anderen Softwarelösungen durchgeführt wurden und benötigt Daten aus anderen Fachverfahren. Es muss daher geprüft werden, inwieweit Schnittstellen mit bestehenden Lohn- und Gehaltsprogrammen vorhanden sind. Falls der Datenaustausch nicht möglich ist, ist zu überlegen, ob Aufgaben zukünftig mit der Software der Zeiterfassung und nicht mehr mit den bestehenden Systemen durchgeführt werden.

- Berücksichtigung aller bestehenden und geplanten Komponenten

  Schon bei der Konzeption zur Einführung einer solchen Komponente sollten bereits vorhandene oder weitere geplante Komponenten wie Single-Sign-On, Bezahlung in der Kantine, Zutrittskontrolle, Signaturen usw. berücksichtigt werden, um spätere Inkompatibilitäten zu vermeiden. Nur so ist der geplante Aufbau einer integrierten Lösung zu erreichen.

2.13.5 Kurzbewertung

Das **Erfordernis** der Zeiterfassung ist in Kommunen mit Gleitzeitregelung gegeben.

Der **Einsatz elektronischer Lösungen** findet sich in vielen Kommunen.

Die **Anzahl der Betroffenen** umfasst grundsätzlich alle Mitarbeiter einer Kommune.

Die **Hauptvorteile** sind die vereinfachte Abwicklung und die erhöhte Mitarbeiterzufriedenheit.

2.14 Zutrittskontrolle

Mit einer elektronischen Zutrittskontrolle für die Mitarbeiter kann exakt gesteuert werden, wer wann und wo für den Zugang zu Räumen oder Gebäudeteilen berechtigt ist. Die Zutritte lassen sich zudem auch protokollieren und somit nachprüfen.

2.14.1 Aktuelle Situation

Zugangskontrollen zu Gebäuden, Gebäudeteilen, einzelnen (Besprechungs-) Räumen, Tiefgaragen oder Parkplätzen sind in vielen Kommunen schon mit elektronischen Hilfsmitteln geregelt. Meist sind es Chipkarten oder Schlüsselanhänger mit einem Chip, die drahtlos die Informationen zum Lesegerät übertragen. Vereinzelt kommen auch noch Karten mit Magnetstreifen zum Einsatz. Bei der Verwendung von elektronischen Zugangskontrollen sind nicht immer alle Räume einbezogen. Oft werden nur Serverraum, Archiv

usw. mit einer solchen Technologie ausgestattet, weil hier neben dem Schutzaspekt auch noch die Information relevant sein kann, wer wann den Raum betreten hat. Vor allem in kleineren Kommunen erfolgt die Zutrittskontrolle noch mit Türschlüsseln für den Haupteingang und für die einzelnen Räumlichkeiten. Die Handhabung von Türschlüsseln ist in einer Verwaltung mit vielen Mitarbeitern sehr aufwändig. Wenn ein Mitarbeiter die Abteilung wechselt, hat er auch andere Befugnisse und benötigt gegebenenfalls auch andere Türschlüssel. Praktikanten können nicht immer mit einem eigenen Türschlüssel ausgestattet werden. Geht ein Türschlüssel verloren, müssen dieser und die zugehörigen Schließzylinder ausgetauscht werden.

2.14.2 Zukünftige Situation

Alle Mitarbeiter können zukünftig mit einer Chipkarte zum Öffnen von Türen ausgestattet werden. Realisierbar sind Lösungen, die nur den Zutritt zu Gebäuden regeln bis hin zu vollständigen Schließsystemen für alle Diensträume. Mit Hilfe des Zutrittskontrollsystems kann, je nach Ausprägung der Installation, für jeden Mitarbeiter exakt eingegrenzt werden, welche Räume er zu welchen Zeiten betreten darf. So kann z. B. festgelegt werden, dass zu den normalen Öffnungszeiten die Türen für jedermann offen sind. Außerhalb der Öffnungszeiten haben nur noch die Mitarbeiter und am Wochenende oder an Feiertagen lediglich die Amtsleiter, die IT-Administratoren und die Hausverwaltung Zutritt. Es lassen sich zudem noch weitere Sicherheitsvorkehrungen wie die zwingend notwendige Eingabe einer PIN außerhalb der Öffnungs- oder Dienstzeiten treffen. Zugangskontrollsysteme können auch mit einer Zeiterfassung gekoppelt werden.

2.14.3 Funktionsweise

Bei den Zugangskontrollsystemen gibt es verschiedene Möglichkeiten, die auch kombinierbar sind.

- Online-Systeme

  Sie gleichen die Berechtigungen, die ein Ausweisinhaber hat, unmittelbar online ab, wenn die Ausweisdaten der Chipkarte vom Lesegerät im Türöffner erfasst werden. Änderungen an den Berechtigungen werden über eine spezielle Software vorgenommen und sind sofort nach dem Eintrag in den elektronischen Schließplan wirksam.

- Offline-Systeme

  Diese Variante kann dann verwendet werden, wenn die Verkabelung für Online-Systeme zu aufwändig ist. Ein Offline-System enthält selbst einen Speicher innerhalb des Türöffners, in dem die berechtigten Ausweise und evtl. noch weitere Daten (z. B. Öffnungszeiten für Alle, Sperrzeiten für Alle usw.) hinterlegt sind. Offline-Systeme agieren autonom und müssen bei Änderungen einzeln

aktualisiert werden.

- Aktiv-Systeme

  In den meisten Fällen liefern die Lesegeräte für den Identifikationsvorgang ein elektrisches Feld, das ausreicht, um die Kennung von der Karte zu lesen. In bestimmten Situationen kann es jedoch erforderlich sein dass der Chipträger, den der Mitarbeiter mit sich führt, selbst seine Kennung an das Lesegerät überträgt. Hierfür muss der Chipträger mit einer Stromversorgung ausgestattet werden. In diesem Szenario kann eine einfache Chipkarte nicht verwendet werden, da sie nicht mit einer Batterie ausgestattet werden kann.

Die Kombination von Online- und Offline- sowie Aktiv-Systemen ist ebenfalls möglich. Es lassen sich z. B. innerhalb der Gebäude, in denen die Verkabelung bereits vorhanden ist, Online-Systeme verwenden, an den Ausgängen, die weiter entfernt sind, werden Offline-Systeme eingesetzt.

Daneben gibt es noch die Möglichkeit, die Zugangsberechtigungen auf die Karte selbst zu schreiben. Ein Terminal für die Zutrittskontrolle ist mit speziellen Funktionen ausgestattet, wodurch die aktuellen Zugangsberechtigungen auf den Chip geschrieben werden können. Der Gültigkeitszeitraum der Berechtigungen lässt sich dabei beliebig definieren. So kann er für Mitarbeiter auf die Dauer von einem Tag gesetzt werden. Für Handwerker oder andere Dienstleister können bestimmte Zeiträume festgelegt werden. Verliert ein Mitarbeiter seinen Ausweis, der mit einer bestimmten Berechtigungsdauer versehen ist, so kann ein Unbefugter ihn nach Ablauf dieser Frist nicht verwenden.

2.14.4 Voraussetzungen

Folgende Punkte müssen für eine effiziente Umsetzung des Konzeptes erfüllt sein:

- Türöffner

  Für die Verwendung von Zutrittskontrollen müssen geeignete Türen und Türöffner (Schließzylinder) vorhanden sein. Sie müssen beschafft und nachgerüstet werden.

- Lesegeräte

  Türen, die mit der Zutrittskontrolle gesteuert werden, müssen mit entsprechenden Online- oder Offline-Lesegeräten ausgestattet sein.

- Verkabelung

  Insbesondere bei Online-Systemen muss eine ausreichende Verkabelung zur Verfügung stehen. Ist dies nicht der Fall, können bauliche Maßnahmen erforderlich werden.

- Chipkarten oder Schlüsselanhänger

  Karten oder Schlüsselanhänger sind die meist verbreiteten Hardware-Medien für die Zugangskontrollen. Hier muss je nach Anwendungszweck das richtige Medium ausgewählt und beschafft werden. Die Karten oder Schlüsselanhänger müssen an zentraler Stelle ausgegeben und wieder eingesammelt werden können (z. B. beim Ausscheiden eines Mitarbeiters oder bei Praktikanten).

- Software

  Für die Türen und/oder zum Beschreiben der Karten ist eine entsprechende Steuersoftware erforderlich.

- Organisatorische Maßnahmen

  Bei Verwendung einer Zugangskontrolle muss zunächst geplant und überlegt werden, welche Bereiche damit ausgestattet werden sollen. Zudem müssen die elektronischen Schließpläne erstellt und dauerhaft gepflegt werden. Auch die Ausgabe der Karten oder Schlüsselanhänger und die Mechanismen bei Verlust müssen überdacht und realisiert werden.

- Berücksichtigung aller bestehenden und geplanten Komponenten

  Schon bei der Konzeption zur Einführung einer solchen Komponente sollten bereits vorhandene oder weitere geplante Anwendungen wie Single-Sign-On, Bezahlung in der Kantine, Zeiterfassung, Signaturen usw. berücksichtigt werden, um spätere Inkompatibilitäten zu vermeiden.

2.14.5 Kurzbewertung

Das **Erfordernis** der Zutrittskontrolle ist in allen Kommunen gegeben.

Der **Einsatz elektronischer Lösungen** findet sich in vielen Kommunen.

Die **Anzahl der Betroffenen** umfasst grundsätzlich alle Mitarbeiter einer Kommune.

Die **Hauptvorteile** sind die vereinfachte Abwicklung, die erhöhte Sicherheit und Kostenvorteile bei Kartenverlust im Vergleich zum Schlüsselverlust (Austausch der Schlüssel und Schließzylinder).

2.15 DOI-Karten/Zertifikate

Neben den detailliert beschriebenen Einsatzbereichen gibt es noch einige spezielle Signatur- und Verschlüsselungskarten (DOI-Karten, vormals X-Safe-Karten) aus dem Vorhaben Deutschland Online Infrastruktur (DOI) des Aktionsplanes von Deutschland Online. Sie werden für das verschlüsselte Übertragen und Sig-

nieren von Daten aus den Bereichen Ausländerwesen und Meldewesen verwendet. Dabei handelt es sich um Chipkarten mit fortgeschrittener elektronischer Signatur (FES). Laut Entscheidung des Bundesinnenministeriums dürfen für diese Zwecke ausschließlich DOI-Karten (und bis zum Ablauf der Gültigkeitsdauer auch noch X-Safe-Karten) verwendet werden. Für die verschlüsselte Kommunikation mit dem Ausländerzentralregister ist ein DOI-Softwarezertifikat erforderlich. Auch hierfür können keine alternativen Zertifikate verwendet werden. DOI-Karten und -Zertifikate werden derzeit vom Unternehmen Telesec (Trustcenter von T-Systems) erstellt. Aus technischen und organisatorischen Gründen dürfen für diese Anwendungsbereiche nur die genannten Chipkarten (DOI, X-Safe) verwendet werden.

2.16 Zwischenergebnis

Nicht alle der oben genannten Anwendungsbereiche betreffen alle Kommunen gleichermaßen. Teilweise ist hier aber nicht die Größe oder die Art der Körperschaft entscheidend, sondern die örtlichen Gegebenheiten (z. B. Vorhandensein einer Kantine). Die Einsatzbereiche decken dabei unterschiedliche Anforderungen ab. Bei einigen steht der Datenschutz im Vordergrund, vielfach liegt das Hauptaugenmerk aber auf der Sicherheit und insbesondere der medienbruchfreien und damit beschleunigten Durchführung von Verwaltungsvorgängen. In einigen Bereichen wie Zeiterfassung und Zutrittskontrolle sind heute schon vielerorts elektronische Verfahren im Einsatz. Andere wiederum, wie das sichere Anmelden am PC oder Single-Sign-On stehen noch am Anfang. Nicht alle Einsatzbereiche werden zudem als gleichermaßen wichtig erachtet. So findet der vollelektronische Vergabeprozess unter Verwendung der QES kaum Beachtung, während z. B. die sichere Anmeldung am PC und der Anordnungs-Signatur-Workflow zumindest bei mittleren und großen Kommunen auf reges Interesse stoßen.

Es kann festgehalten werden, dass

- in den oben genannten Bereichen und Prozessen große Verbesserungspotenziale unter Verwendung von MFC, nPA oder ggf. QES vorhanden sind,
- die meisten Verbesserungen freiwillig erfolgen, da mit Ausnahme von ePR und ANV keine Verpflichtung bestehen,
- die meisten Mitarbeiter einer Behörde von mehreren der identifizierten Einsatzbereiche betroffen sind und
- zusätzliche Potenziale entstehen, wenn Synergieeffekte durch die Verwendung einer Technologie für verschiedene Anwendungsbereiche realisiert werden können.

3 Zuordnung der Technologien zu den Einsatzbereichen

In diesem Kapitel werden die Technologien der elektronischen Signatur, der multifunktionalen Chipkarte und des neuen Personalausweises in ihren Grundfunktionen beschrieben. Anschließend werden sie tabellarisch den Einsatzbereichen gegenübergestellt. Daraufhin werden die Kostenfaktoren und die Potenziale aufgezeigt. Jeder Abschnitt schließt mit einer Bewertung und Empfehlungen für die Kommunen.

3.1 Elektronische Signaturen

Es gibt mehrere Arten elektronischer Signaturen, die sich durch unterschiedliche Komplexität in der Erzeugung, in der Handhabung und in den Verwendungsmöglichkeiten unterscheiden.

3.1.1 (Einfache) Elektronische Signatur (ES)

Die einfache elektronische Signatur (§ 2 Nr. 1 SigG) ist hinsichtlich ihrer Ausprägung nicht scharf abgegrenzt. Sie kann eine Signaturzeile in einer E-Mail („Mit freundlichen Grüßen Ihr Max Mustermann“) oder auch eine eingescannte Unterschrift auf einem elektronischen Dokument sein. Da grundsätzlich auch Unbefugte diese Signatur fälschen können, hat sie nur geringe Beweiskraft, weshalb sie im weiteren Verlauf nicht weiter berücksichtigt wird.

3.1.2 Fortgeschrittene elektronische Signatur (FES)

Die fortgeschrittene elektronische Signatur (§ 2 Nr. 2 SigG) ist technisch aufwändiger aber auch sicherer als die einfache elektronische Signatur. Mit der FES lässt sich feststellen, ob ein mit ihr unterschriebenes Dokument (z. B. eine E-Mail-Nachricht) während des Versands verändert wurde. Jede Signatur besteht aus einem Signaturschlüssel und einem Zertifikat, das den Namen des Signaturinhabers, die Gültigkeitsdauer und noch weitere Informationen enthält. Da Signaturschlüssel (und Zertifikate) für fortgeschrittene elektronische Signaturen in der Regel aber nur als Softwaredatei gespeichert werden, können sie leichter „gestohlen“ und missbräuchlich verwendet werden. Die FES hat deshalb nur geringe Beweiskraft und ist kein Ersatz für die eigenhändige Unterschrift (einzige Ausnahme in Bayern ist die eFES). Eine FES kann für Personen, für Abteilungen oder eine ganze Behörde ausgestellt werden. Die FES ist für bayerische Kommunen kostenlos vom LfStaD im Rahmen der Bayerischen Verwaltungs-PKI erhältlich. Sie hat eine Gültigkeitsdauer von maximal drei Jahren. Der Freistaat Bayern und die kommunalen Spitzenverbände Bayerns realisieren derzeit ein Projekt zur sicheren elektronischen Kommunikation zwischen Behörden. Bei den staatlichen und

allen kommunalen Behörden sollen zumindest bei den Poststellen (Funktionsadresse poststelle@behörde.de) die fortgeschrittenen Zertifikate der Verwaltungs-PKI (Bayern-PKI) für die Signatur und Verschlüsselung zum Einsatz kommen.

3.1.3 „Erweiterte“ fortgeschrittene elektronische Signatur (eFES)

Unter einer erweiterten fortgeschrittenen elektronischen Signatur wird eine FES verstanden, die auf einer sicheren Signaturerstellungseinheit (z. B. Chipkarte) gespeichert ist und weitere „ergänzende Merkmale aufweist“. Der Zusatz „erweitert“ ist keine offizielle oder technische Bezeichnung, sondern wird in dieser Untersuchung zur Abgrenzung von der FES verwendet. Die ergänzenden Merkmale sind in den „Anforderungen an den Einsatz fortgeschrittener Signaturen im Haushalts-, Kassen-und Rechnungswesen der Bayerischen Kommunen (AFS-HKR)“ mit Stand vom 10.08.2010 und der „Begründung zur AFS-HKR“ ebenfalls mit Stand vom 10.08.2010 beschrieben. Die eFES kann unter bestimmten Bedingungen für den Bereich von Haushalts-, Kassen- und Rechnungswesen (HKR) in bayerischen Kommunen zur elektronischen Unterzeichnung von Anordnungen verwendet werden.

Für die eFES sind ein Signaturschlüssel, ein Zertifikat (FES) und eine Chipkarte erforderlich. Die Karten selbst werden von speziellen Herstellern gefertigt und geliefert. Anschließend werden die Signaturschlüssel und Zertifikate auf die Karten aufgebracht. Dies kann prinzipiell von jeder Kommune selbst durchgeführt werden, wenn sie einen entsprechenden Kartendrucker beschafft und die organisatorischen Voraussetzungen für dessen Sicherung sowie die Verwaltung der ausgegebenen Karten schafft. Somit wird sie eine produzierende RA (Registration Authority) für die Bayerische Verwaltungs-PKI. Dies lohnt sich aufgrund der Kosten aber nur für Kommunen mit einem Bedarf von mehreren hundert Karten. Wirtschaftlicher ist die Beauftragung eines Dienstleisters, mit dem ein Vertrag über den Bezug entsprechender Karten geschlossen wird. Zu den notwendigen Vertragsinhalten gehören nicht nur die Preise, sondern auch Vereinbarungen über die sichere Verfahrensabwicklung und die Möglichkeit, in Notfällen auch ganz schnell an einzelne Ersatzkarten zu kommen. Zum Beispiel bietet die AKDB/Living Data GmbH einen solchen Dienst als RA für die Bayerische Verwaltungs-PKI an. Dem grundsätzlichen Nachteil des Zeitverzugs bei der „Fremdproduktion“ stehen aber ganz handfeste Vorteile gegenüber, zumal der erwähnte Zeitverzug je nach Abstimmung mit dem Dienstleister auch gar nicht wirklich spürbar in Erscheinung treten muss. Bei der Eigenproduktion kann eine neue Karte theoretisch in wenigen Minuten erstellt werden, wenn das Gerät betriebsbereit und ein verantwortlicher eingewiesener Mitarbeiter zur Verfügung steht. Das bedeutet, es muss eine Vertretung organisiert werden und die Maschine muss so gewartet werden, dass sie stets genutzt werden kann, denn die Eigenproduktion kennt kein zweites Verfahren, das im Notfall eingesetzt werden könnte.

Die eFES hat eine Gültigkeit von drei Jahren danach muss die Signatur erneuert werden, indem ein aktueller Signaturschlüssel und ein neues Zertifikat auf dieselbe Karte geschrieben werden.

Im Unterschied zu den DOI/X-Safe-Karten, auf die ebenfalls eine FES aufgebracht ist, darf die eFES nur für Personen und nicht für Gruppen oder Abteilungen ausgestellt werden.

3.1.4 Qualifizierte elektronische Signatur (QES)

Ist die Schriftform erforderlich, kann allein die QES nach § 3a BayVwVfG die eigenhändige Unterschrift ersetzen. Vorschriften zur QES finden sich in § 2 Nr. 3 SigG (Stand: 28.12.2009) sowie in der Signaturverordnung (Stand: 23.11.2010). Die QES muss immer mit einer sicheren Signaturerstellungseinheit (z. B. Chipkarte) erstellt werden. Neben dem Signaturschlüssel ist auch ein Zertifikat aufgebracht. Qualifizierte elektronische Signaturen dürfen in Deutschland nur von Trustcentern ausgestellt werden, die bestimmte Voraussetzungen erfüllen.

Um eine QES zu erhalten, muss sich der Antragsteller entweder via PostIdent-Verfahren oder bei einer Registrierungsstelle identifizieren. Dies kann je nach Trustcenter bei der Post, der Sparkasse oder auch der IHK erfolgen. Teilweise wird von Dienstleistern auch angeboten, die Antragstellung mit der erforderlichen Identifizierung vor Ort in der Kommune durchzuführen. Für die QES des nPA soll dies zukünftig mit der eID-Funktion des neuen Personalausweises möglich sein. Von der Bestellung bis zur Auslieferung können einige Wochen vergehen. Die QES ist aufgrund ihrer aufwändigeren technischen Erzeugung und den gesetzlichen Anforderungen, die die Trustcenter erfüllen müssen, deutlich teurer als die eFES.

Je nach Aussteller hat die QES eine Gültigkeit von einem bis zu fünf Jahren. Nach Ablauf der Gültigkeit muss eine neue Karte mit Signaturschlüssel und Zertifikat beschafft werden. Für eFES und QES gilt, dass die Signatur und damit die Sicherung nur dann geprüft werden können, wenn auf Seiten der Empfänger die entsprechende Software vorhanden ist. Der signierte Inhalt selbst ist jedoch auch ohne diese Software lesbar.

3.1.5 Einsatzbereiche für elektronische Signaturen

Bei den Einsatzbereichen für elektronische Signaturen wird unterschieden, ob eine erweiterte fortgeschrittene elektronische Signatur (eFES) oder eine qualifizierte elektronische Signatur (QES) verwendet wird. Eine ausführliche Beschreibung der Einsatzbereiche ist in Kapitel 2 zu finden.

In den nachstehenden Tabellen werden die Eignung und die Praxisrelevanz von eFES und QES gegenübergestellt.

Tabelle 1: Einsatzbereiche und Eignung elektronischer Signaturen (behördenintern)

Technologie/ Einsatzbereich	Eignung	
	Erweiterte fortgeschrittene elektronische Signatur (eFES)	Qualifizierte elektronische Signatur (QES)
Elektronischer Anordnungs-Signatur-Workflow	++	++
Elektronischer Vergabeprozess (eVergabe)	–	++
Elektronisches Abfallnachweisverfahren (eANV)	–	++
Elektronisches Personenstandsregister (ePR)	–	++
Interne Antragstellung	+(1)	++

- nicht möglich, + geeignet, ++ sehr gut geeignet

(1) Die eFES kann zwar das Schriftformerfordernis nicht erfüllen, aber dennoch die Beweiskraft deutlich erhöhen, insbesondere in Verbindung mit einer Zwei-Faktor-Authentisierung.

Tabelle 2: Einsatzbereiche und Praxisrelevanz elektronischer Signaturen (behördenintern)

Technologie/ Einsatzbereich	Praxisrelevanz	
	Erweiterte fortgeschrittene elektronische Signatur (eFES)	Qualifizierte elektronische Signatur (QES)
Elektronischer Anordnungs-Signatur-Workflow	Ja	Nein
Elektronischer Vergabeprozess (eVergabe)	Nein	Nein
Elektronisches Abfallnachweisverfahren (eANV)	Nein	Ja
Elektronisches Personenstandsregister (ePR)	Nein	Ja
Interne Antragstellung	Nein	Nein

3.1.6 Kostenfaktoren

Sofern in den nachfolgenden Punkten konkrete Summen genannt werden, handelt es sich um Informationen von Herstellern oder Kommunen, die diese Technik bereits eingeführt haben. Eine übertragbare Kostenschätzung kann an dieser Stelle nicht gegeben werden, da die finanziellen Aufwände sehr stark von den individuellen Voraussetzungen in der jeweiligen Kommune determiniert sind. Daher werden lediglich die Bereiche genannt, in denen mit zusätzlichen Kosten zu rechnen ist.

- Kosten für Anwendungssoftware

  Kosten können für die Anwendungssoftware z. B. für Zusatzmodule, Workflow-, Scan- und Speicherlösungen anfallen. Diese Kosten sind in starkem Maße davon abhängig, welche Komponenten bereits mit welcher Lizenzierung im Einsatz sind und ob aufgrund fehlender Kompatibilität Zusatzaufwendungen notwendig sind.

- Kosten für eFES

Die Kosten für die Karten und das Aufbringen der Schlüssel und Signaturen (sowie Zertifikate) hängen sehr stark von der Stückzahl ab. Die Preise für Karten mit Signaturen liegen bei ca. 25 Euro pro Stück.

- Kosten für QES

  Qualifizierte elektronische Signaturkarten kosten je nach Trustcenter zwischen 100 und 120 Euro, bezogen auf eine Gültigkeit von zwei Jahren. Für den Anordnungs-Signatur-Workflow können sogenannte Massensignaturen erforderlich sein. Damit lassen sich mehrere Signaturen mit nur einer PIN-Eingabe erstellen. Der Preis für diese Variante liegt etwas über dem für „herkömmliche" Signaturen.

- Kosten für Kartendrucker

  Für die meisten Kommunen wird es sich nicht lohnen, Karten für die eigene Verwaltung zu produzieren. Die gesamten Betriebskosten für die normale Kartenproduktion müssen kalkuliert und um den Aufwand für die Bereitstellung von Karten in Sonder- bzw. Notfällen ergänzt werden. Die Preise für die Geräte selbst liegen je nach Ausstattung zwischen 4.000 und 6.000 Euro.

- Kosten für Kartensoftware

  Um die Signaturen aus den Karten auslesen zu können, muss eine spezielle Software (Middleware) beschafft werden. Der Preis hierfür liegt bei unter 10 Euro pro Arbeitsplatz.

- Kosten für Lesegeräte

  Zusätzlich zu den Karten müssen ggf. neue Lesegeräte (oder Tastaturen mit integrierten Lesegeräten) beschafft werden. Die Kosten sind abhängig von der Anforderung (Klasse 1 oder 2, integrierte Tastatur).

- Kosten für Dienstleistungen

  Daneben können noch Kosten für Beratung und weitere Dienstleistungen anfallen.

- Kartenmanagement

  Beschaffung, Ausgabe, Einzug und Beschriftung von Karten verursachen ebenfalls Aufwände und damit letztendlich Kosten, die berücksichtigt werden müssen.

3.1.7 Potenziale von elektronischen Signaturen

In den oben genannten Einsatzbereichen ist die eigenhändige Unterschrift ein Hauptgrund dafür, dass noch

papierbasiert gearbeitet wird. Die Potenziale elektronischer Signaturen liegen vor allem in der Vermeidung bzw. Reduzierung von Medienbrüchen, was dazu führt, dass die Abläufe (durchgehend) elektronisch durchführbar sind. Die vergleichsweise hohe technische Sicherheit dieser Karten kann dazu beitragen, Bedenken hinsichtlich rechtlicher und praktischer Aspekte zu beseitigen. Die QES erhöht dabei die Rechtssicherheit und Beweiskraft, da stets unabstreitbar nachvollziehbar ist, wer wann ein Dokument unterzeichnet bzw. bearbeitet hat.

3.1.8 Bewertung

Nachfolgend werden die wesentlichen Aspekte der untersuchten Signaturen kurz bewertet.

- Anzahl der Mitarbeiter

  Die eFES ist zu deutlich geringeren Kosten als die QES erhältlich. Dieser Kostenunterschied ist vor allem in größeren Kommunen ausschlaggebend, in denen für den Anordnungs-Signatur-Workflow ein größerer Teil der Belegschaft eingebunden sein kann. Die Anzahl der mit einer Signatur ausgestatteten Mitarbeiter ist aber noch in weiterer Hinsicht relevant. Erstens sinken die Kosten pro Karte mit steigender Stückzahl und zweitens erhöht sich der positive Gesamteffekt umso stärker, je mehr Mitarbeiter daran beteiligt sind.

- Beschaffungsvorgang

  Der Beschaffungs- und Produktionsvorgang der eFES ist organisatorisch einfacher und vor allem kürzer als bei der QES. Für die Produktion bis zur Auslieferung der Karte werden nur wenige Tage benötigt, vorausgesetzt Kartenrohlinge und Signaturen liegen vor. Verfügt die Kommune über einen eigenen Kartendrucker, dauert die Erstellung einer neuen Karte samt dem Aufbringen der Signatur (Schlüssel und Zertifikat) nur wenige Minuten. Hingegen muss die QES mit deutlich größerem Aufwand bei einem Trustcenter bestellt und der entsprechende Mitarbeiter zudem bei einer Registrierungsstelle oder via PostIdent-Verfahren identifiziert werden.

- eFES oder QES?

  Die QES umfasst den größten Einsatzbereich auf dem Gebiet der elektronischen Signaturen. Aber abseits der Pflichtanwendungen hat sie bislang keine Praxisrelevanz erlangt. Daher bleibt der Einsatz der QES auf die Bereiche beschränkt, in denen sie gesetzlich benötigt wird. Für den Anordnungs-Signatur-Workflow ist die deutlich günstigere eFES ausreichend.

- Wirtschaftlichkeit von eFES und QES

Die Kosten für eFES und insbesondere QES sind nicht unerheblich. Neben den Karten und Signaturen fallen noch Kosten für Lesegeräte und weitere Komponenten an wie etwa bei Fachverfahren, DMS oder Workflowsystemen. Demgegenüber stehen die Einsparungen einer weitgehend medienbruchfreien Verwaltung.

Finanzielle Auswirkungen machen sich z. B. unmittelbar durch sinkende Druck-, Versand- und Archivierungskosten bemerkbar. Aber viele positive Effekte können monetär nicht exakt bestimmt werden, weil sie sich innerhalb der Kommunen nicht unmittelbar finanziell auswirken. Der Anordnungs-Signatur-Workflow verkürzt z. B. die Durchlaufzeiten erheblich und beschleunigt die Abarbeitung der Vorgänge. Er vereinfacht zudem die Fallbearbeitung für die Mitarbeiter. Auch beim Suchen und Finden von Anordnungen oder sonstigen Dokumenten, die in elektronischer Form vorliegen ergeben sich erhebliche zeitliche Einsparungen.

3.1.9 Empfehlung

Die Verwendung von elektronischen Signaturen in den genannten Anwendungsbereichen erhöht die Medienbruchfreiheit und ermöglicht damit eine weitere Digitalisierung und somit auch Beschleunigung der Prozessabläufe. Ihr Einsatz ist in jedem Fall zu empfehlen. Hinsichtlich Signaturart und Bezugsquelle muss es aber, je nach Kommunengröße, unterschiedliche Empfehlungen geben.

- Mittlere und große Kommunen

  Entscheiden sich mittlere und große Kommunen für den Anordnungs-Signatur-Workflow, ist die eFES in jedem Fall der QES vorzuziehen. Sie ist nicht nur deutlich günstiger, sondern bietet auch hinsichtlich der Beschaffungszeit große Vorteile. Die eigene Erstellung (d. h. Aufbringung der Zertifikate und Schlüssel auf die Karte) der Signaturkarten lohnt sich kaum. Diese Aufgaben sollten auf externe Dienstleister, Shared Service Center oder andere spezialisierte Einrichtungen übertragen werden. Dies ist erforderlich um Kostenvorteile zu nutzen und die IT-Abteilungen der Kommunen von diesen nicht wertschöpfenden Tätigkeiten zu entlasten. Verwaltungen, die nicht selbst Karten produzieren, können die eFES derzeit entweder bei kartenproduzierenden Kommunen (einige Landratsämter) oder der AKDB/LivingData GmbH beziehen. Für die Pflichtbereiche, wie z. B. das elektronische Abfallnachweisverfahren oder das elektronische Personenstandsregister, muss eine Kommune hingegen qualifizierte elektronische Signaturen für die in diesen Bereichen beschäftigten Mitarbeiter beschaffen.

- Kleinere Kommunen

  Auch hier gilt, dass für die Pflichtbereiche in jedem Fall die QES beschafft werden muss. Sind in einer Kommune nur zwei oder drei Mitarbeiter mit Anordnungen befasst und soll ein Anordnungs-Signatur-Workflow installiert werden, kann auch die Beschaffung einer QES für diesen Anwendungsbereich erwogen werden. Vorteil hierbei ist, dass alle Mitarbeiter mit der gleichen Signaturart (sowohl für Pflicht- wie auch für freiwillige Bereiche) arbeiten und sich so gegenseitig unterstützen können. Ferner ist nur ein Ansprechpartner für Fragen und Hilfestellungen erforderlich. Außerdem werden keine unterschiedlichen Middleware-Lösungen benötigt, die zu Inkompatibilitäten führen können. Die Wiederbeschaffungszeit bei Verlust ist bei der QES zwar länger, aber bei Fremdbezug der eFES dauert auch dies einige Tage, so dass ohnehin eine Übergangslösung gefunden werden muss. Entscheidet sich eine kleine Kommune für die Verwendung der eFES, sollte sie diese – soweit möglich – als Komplettpaket inklusive Installation, Wartung und Support von einem externen Dienstleister beziehen.

3.1.10 Zwischenergebnis

Die QES kann zwar mehr Einsatzbereiche als die eFES abdecken, ist aber derzeit wesentlich teurer in der Anschaffung und langwieriger in der Beschaffung. Die QES muss in einigen Pflichtbereichen (eANV, ePR) verwendet werden, jedoch betrifft dies nur wenige Mitarbeiter in einer Kommune. In den elektronischen Anordnungs-Signatur-Workflow hingegen kann ein größerer Teil der Mitarbeiter eingebunden sein. Der Workflow ist sowohl mit der QES als auch mit der eFES durchführbar.

3.2 Multifunktionale Chipkarte (MFC) und multifunktionaler Dienstausweis (MFD)

Multifunktionale Chipkarten sind Karten (Smart Cards, Mikroprozessorkarten), die für mehrere Anwendungsbereiche wie z. B. Zeiterfassung, Zutrittskontrolle, Signatur, sichere Anmeldung am PC usw. verwendet werden können. Solche Karten sind in vielen Unternehmen bereits im Einsatz. In einigen Kommunen befinden sie sich in der Test- oder Einführungsphase. Im Produktivbetrieb sind diese Karten bislang nur in wenigen bayerischen Kommunen. Wenn die multifunktionale Chipkarte so ausgestattet ist, dass sie zusätzlich als Dienstausweis verwendet werden kann, d. h. mit Lichtbild, Unterschrift, Dienststelle des Karteninhabers usw., wird sie multifunktionaler Dienstausweis genannt. MFC werden im Scheckkartenformat ausgestellt (ID-1 Format). Im kommunalen Umfeld werden sogenannte Hybridkarten verwendet, die sowohl

einen kontaktlosen als auch einen kontaktbehafteten Chip enthalten.

3.2.1 Ausstattung

Die Ausstattung einer multifunktionalen Chipkarte ist innerhalb bestimmter Grenzen frei wählbar, aber nicht alle möglichen Ausprägungen lassen sich heute schon parallel auf der Karte implementieren. Nachfolgend werden die unterschiedlichen Ausstattungsmerkmale kurz beschrieben.

- Sichtausweis

  Die (Chip-)Karte kann als Sichtausweis bzw. als Dienstausweis verwendet werden, wenn die dafür erforderlichen Merkmale aufgebracht werden.

- Kontaktloser Chip

  Kontaktlose Chips benötigen keinen direkten physischen Kontakt zu einem Lesegerät. Die Daten werden via Funk zum Lesegerät gesendet, was den Vorteil hat, dass die Karte nur kurz vor ein Lesegerät an dem entsprechenden Anwendungssystem gehalten werden muss.

  Das umständliche Einstecken in einen Kartenschlitz ist dabei nicht nötig. Auf dem Chip lassen sich eine Reihe von Programmen und Daten speichern wie beispielsweise die Kennung für die Zeiterfassung und Zutrittskontrolle (zumindest bei neueren Systemen)

- Kontaktbehafteter Chip

  In der behördlichen Praxis werden auf dem kontaktbehafteten Chip folgende Daten und Anwendungen gespeichert:

  - Authentisierungsschlüssel und -zertifikat z. B. für die sichere Anmeldung am PC,
  - Schlüssel und Zertifikat für die Verschlüsselung sowie
  - Signaturschlüssel und Zertifikat für die eFES.

3.2.2 Beschaffung

Wenn die MFC auch für die Zutrittskontrolle und die Zeiterfassung verwendet werden soll, ist aus technischen Gründen die Reihenfolge zu beachten, in der die Daten auf die Karten aufgebracht werden. Zuerst werden die erforderlichen Daten für die Zutrittskontrollsysteme/Zeiterfassungssysteme aufgespielt. Dies übernehmen die Hersteller dieser Systeme in der Regel selbst. Erst danach können weitere Funktionen wie z. B. Verschlüsselung oder eFES hinzugefügt werden. Hier gelten die gleichen Bedingungen wie bei der

Beschaffung der eFES (siehe Abschnitt 3.1.2 Fortgeschrittene elektronische Signatur (FES)). Für MFC bietet z. B. die AKDB/Living Data GmbH ein Komplettpaket, das Installation, Betrieb, Wartung und Support beinhaltet.

3.2.3 Gültigkeitsdauer und Erneuerung

Die Gültigkeit von MFC ist grundsätzlich nicht beschränkt. Für den Fall, dass sich Schlüssel, und Zertifikate für die Signatur, die Verschlüsselung oder zum sicheren Anmelden am PC auf der Karte befinden, müssen diese Komponenten nach Ablauf der Gültigkeit (in der Regel drei Jahre) erneuert werden, indem aktuelle Schlüssel und Zertifikate auf den Kartenchip übertragen werden.

3.2.4 Einsatzbereiche

Eine ausführliche Beschreibung der Einsatzbereiche ist in Kapitel 2 zu finden.

Technisch ist es zwar möglich, multifunktionale Chipkarten mit einer qualifizierten elektronischen Signatur (QES) auszustatten, aber dies bringt einige Nachteile mit sich. Der Beschaffungsvorgang einer QES ist im Vergleich zur eFES deutlich aufwändiger, langwieriger und teurer. Zudem muss die Karte nach Ablauf der Gültigkeit der Signatur ausgetauscht werden, was einen erhöhten organisatorischen und Aufwand und auch Kosten verursacht. Daher wird bei der folgenden Zuordnung die QES in Kombination mit der MFC nicht weiter berücksichtigt.

In den nachstehenden Tabellen werden die Eignung und die Praxisrelevanz von MFC gegenübergestellt.

Tabelle 3: Einsatzbereiche und Eignung von multifunktionalen Chipkarten (behördenintern)

Technologie/ Einsatzbereich	Eignung multifunktionaler Chipkarten (MFC)
Dienstausweis	++
Drucken vertraulicher Dokumente (Follow-Me-Printing)	++
Elektronischer Anordnungs-Signatur-Workflow (mit eFES)	++
Elektronischer Versand personenbezogener Daten	++
Interne Antragstellung und Datenabruf	+(1)
Kantine und Verpflegungsautomaten	++
QES (für ePR, eANV eVergabe usw.)	o(2)
Sichere Anmeldung am PC	++
Single-Sign-On	++
Zeiterfassung	++
Zutrittskontrolle	++

- nicht möglich, o nicht praktiziert + geeignet, ++ sehr gut geeignet

(1) Aufgrund des hohen Sicherheitsniveaus bei der sicheren Anmeldung am PC mit einer MFC bewirkt diese sichere Authentisierung auch eine verbesserte Sicherheitslage bei internen Anträgen ohne Schriftformerfordernis

(2) Wird derzeit aufgrund organisatorischer Schwierigkeiten nicht auf MFC verwendet.

Tabelle 4: Einsatzbereiche und Praxisrelevanz von multifunktionalen Chipkarten (behördenintern)

Technologie/ Einsatzbereich	Praxisrelevanz multifunktionaler Chipkarten (MFC)
Dienstausweis	Ja (1)
Drucken vertraulicher Dokumente (Follow-Me-Printing)	Ja, aber nicht überall erforderlich
Elektronischer Anordnungs-Signatur-Workflow (mit eFES)	Ja
Elektronischer Versand personenbezogener Daten	Eingeschränkt (2)
Interne Antragstellung und Datenabruf	Eingeschränkt (3)
Kantine und Verpflegungsautomaten	Ja, aber nicht überall vorhanden
QES (für ePR, eANV eVergabe usw.)	Ja
Sichere Anmeldung am PC	Ja
Single-Sign-On	Ja
Zeiterfassung	Ja

(1) Wird in Kombination z. B. mit der Zutrittskontrolle kritisch gesehen. Daher können in diesen Fällen zusätzliche Sicherheitsmechanismen wie PIN-Abfrage, zeitliche Befristung des Zutritts u. ä. ergriffen werden.

(2) Auch der Kommunikationspartner muss zur Ver-/Entschlüsselung in der Lage sein, was derzeit nur selten gegeben ist.

(3) Aufgrund des hohen Sicherheitsniveaus bei der sicheren Anmeldung am PC mit einer MFC bewirkt diese sichere Authentisierung auch eine verbesserte Sicherheitslage bei internen Anträgen ohne Schriftformerfordernis. Derzeit aber noch geringe Verbreitung und nur wenige Anwendungsfälle.

3.2.5 Mögliche Einschränkungen und Lösungen

Die Funktionen, die für die verschiedenen Einsatzbereiche erforderlich sind, basieren auf unterschiedlichen Bestandteilen der MFC. Dies kann bei der Einführung der MFC in den Kommunen aufgrund der Vielzahl unterschiedlicher Anwendungen und Hersteller von Hard- und Software zunächst zu Komplikationen führen. Diese müssen dann jeweils im Einzelfall betrachtet und gelöst werden.

Als problematisch kann es angesehen werden, wenn die MFC sowohl als Sichtausweis als auch für die elektronische Zutrittskontrolle verwendet wird. Auf der Karte sind in der Verwendung als Sichtausweis Name und Dienstelle vermerkt. Dadurch weiß der „Finder" zu welcher Behörde dieser Ausweis Zugang gestattet. Wird ein Verlust oder Diebstahl rechtzeitig bemerkt, kann die Karte binnen kürzester Zeit gesperrt werden. Bis dahin aber gewährt der Ausweis Zugang zu den behördlichen Räumlichkeiten. Auch hierfür können Lösungsmöglichkeiten gefunden werden. Diese können sein:

- Zugangskontrolle gilt nur für die Gebäudeeingänge (Außenhaut)

  Wenn der Zugang mit der Karte nur für die Gebäude, nicht aber für die darin liegenden Räumlichkeiten möglich ist, verringert dies das Gefahrenpotenzial, da zu den regulären Arbeitszeiten ohnehin häufig Parteiverkehr stattfindet und somit Personen auch ohne Kontrollen Zutritt erhalten.

- Zugangskontrolle ist zeitgesteuert

  Ist die Zugangskontrolle zeitgesteuert, so dass das Gebäude außerhalb der Öffnungszeiten nicht oder nur von bestimmten Personengruppen (Amtsleitung, IT-Mitarbeiter, Hausverwaltung) betreten werden kann, verringert dies das Risiko des unbefugten Betretens.

- Zugangserlaubnis ist zeitlich begrenzt

  Einen etwas höheren Schutz bieten Zugangskontrollen, die den Chip des Ausweises mit einer Gültigkeitsdauer versehen. Ist diese bspw. nur für einen Tag ausgestellt, muss der Inhaber innerhalb dieser Zeit ein bestimmtes Terminal aufsuchen und die Gültigkeitsdauer erneut verlängern. Dies funktioniert im Regelbetrieb ohne Probleme. Wird das Ablaufdatum nicht innerhalb der Gültigkeitsdauer verlängert, muss die Karte von einem Mitarbeiter erneut freigeschaltet werden.

- Zugangskontrolle ist zusätzlich PIN-gesichert

  Die höchste Sicherheit gibt eine PIN, die beim Zugang mit der Karte ergänzend eingegeben werden muss. Mit dieser Vorgehensweise erhält ein Unbefugter (ohne Kenntnis der PIN), selbst wenn er im Besitz einer noch nicht gesperrten Karte ist, keinen Zutritt.

3.2.6 Kostenfaktoren

Für die Entscheidung, ob eine MFC eingeführt werden soll, sind neben der grundsätzlichen Eignung für bestimmte Einsatzbereiche insbesondere die Kosten zu berücksichtigen. Sie können hier nicht pauschal beziffert werden, da in den Kommunen unterschiedliche Szenarien sowie Ausgangssituationen anzutreffen sind und die Kartenpreise bei den unterschiedlichen Herstellern variieren. Die folgenden Punkte geben da-

her die zu berücksichtigenden Faktoren wieder, die im Einzelfall monetär oder mit anderen Ressourcen bewertet werden müssen.

- Kosten für Karten

  Für die Beschaffung der Karten sowie das Aufbringen der Schlüssel und Signaturen fallen Kosten an. Die Kartenpreise hängen dabei sehr stark von der Stückzahl ab. Die Preise für Karten mit Signaturen liegen bei ca. 25 Euro.

- Kosten für Kartenproduktion in Ausnahmefällen

  Für die Kartenproduktion in Sonderfällen (dringender Bedarf, Verlust) müssen mit dem jeweiligen Hersteller Lösungen für die Sofortherstellung und Lieferung vereinbart werden. Dies verursacht zusätzlichen Aufwand und damit weitere Kosten.

- Kosten für Kartensoftware

  Um die Signaturen aus den Karten auslesen zu können, muss eine spezielle Software (Middleware) beschafft werden. Der Preis hierfür liegt bei unter 10 Euro pro Arbeitsplatz.

- Kosten für Lesegeräte

  Zusätzlich zu den Karten müssen ggf. neue Lesegeräte beschafft werden. Die Kosten sind abhängig von der Anforderung (Klasse 1 oder 2, integrierte Tastatur) und liegen zwischen 20-30 Euro pro Stück.

- Externer Beratungsaufwand

  Vor der Entscheidung, ob die MFC tatsächlich eingeführt wird, sollten in jedem Fall Beratungsleistungen eines Anbieters von MFC in Anspruch genommen werden oder Kommunen, die dies Technik bereits im Einsatz haben, befragt werden. Der Beratungsaufwand ist abhängig von dem bereits vorhandenen Wissen in der Kommune, etwaigen Kompatibilitätsproblemen und der Anzahl der zu integrierenden Anwendungsbereiche. Auch müssen entsprechende Anfragen an die Hersteller der vorhanden Hard- und Software gerichtet werden.

- Installationsaufwand

  Für die Einrichtung der Hardware und Software fällt zusätzlicher Aufwand an. Die Installation kann entweder durch ein externes Unternehmen oder von der eigenen IT-Abteilung durchgeführt werden.

- Softwareanpassungen

Unter Umständen sind Schnittstellen anzupassen oder zu erstellen. Auch kann das Auswechseln einer Software erforderlich werden. Diese Anpassungen müssen nicht unmittelbar mit der MFC selbst in Verbindung stehen, sondern können auch erforderlich sein, wenn im Rahmen der MFC-Einführung z. B. Softwareapplikationen wie DMS eingebunden werden.

- Bauliche Maßnahmen

  Bauliche Maßnahmen können insbesondere bei Zutrittskontrolle und Zeiterfassung nötig werden. Dabei beeinflussen sich die Hardware der auszuwählenden Lösung und die baulichen Gegebenheiten wechselseitig; diese Alternativen müssen verglichen und bewertet werden.

- Kartenmanagement

  Beschaffung, Ausgabe, Einziehen und Beschreiben von Karten verursachen Aufwand, der einkalkuliert werden muss.

- Organisatorische Aufwendungen

  Bereits vor der Einführung einer MFC sind organisatorische Abstimmungen erforderlich. Diese bemessen sich im Umfang zunächst danach, wie viele Einsatzbereiche (zu Beginn) abgedeckt werden sollen. Anschließend ist zu überlegen, ob bisherige Abläufe nicht im Zuge der Einführung von MFC geändert werden können bzw. müssen.

3.2.7 Potenziale von multifunktionalen Chipkarten

Inwieweit die Potenziale der MFC ausgeschöpft werden ist abhängig davon, wie viele Einsatzbereiche in welchem Umfang integriert werden können.

- Medienbruchfreiheit

  Die Verwendung von elektronischen Signaturen auf Basis von MFC führt dazu, dass Medienbrüche vermieden bzw. reduziert werden können und die Abläufe (durchgehend) elektronisch durchführbar sind. Die vergleichsweise hohe technische Sicherheit dieser Karten kann dazu beitragen, Bedenken hinsichtlich rechtlicher und praktischer Aspekte zu beseitigen.

- Vereinfachung der IT-Administration

  Die Verwendung von MFC vereinfacht auch Aufgaben der IT-Administration. Zum einen werden die Mitarbeiter z. B. durch den Einsatz von SSO (Single-Sign-On) von Aufgaben wie das Zurücksetzen von Passworten entlastet. Zum anderen bewirkt die Verwendung von nur einer MFC pro Mitarbeiter eine Reduzierung des administrativen Aufwandes im Vergleich zu mehreren Techniken

wie Signaturkarte, Karte für sicheres Anmelden am PC, Schlüsselanhängern usw.

- Erhöhung der Mitarbeiterzufriedenheit

  Der Einsatz der MFC führt zu einer Erhöhung der Mitarbeiterzufriedenheit. Dies gilt z. B. beim Einsatzbereich SSO, bei dem sich die Mitarbeiter nur noch eine PIN merken müssen. Aber auch der elektronische Anordnungsworkflow führt zu mehr Zufriedenheit, weil bspw. umständliche Arbeitsschritte entfallen und die Abarbeitung schneller erledigt werden kann. Ebenfalls einfacher für die Mitarbeiter werden das bargeldlose Bezahlen in der Kantine und an Automaten, die Zutrittskontrolle und die Zeiterfassung.

- Erhöhung der Sicherheit und des Datenschutz

  Sehr großes Potenzial gibt es bei der Verbesserung der Sicherheit in unterschiedlichen Bereichen. So kann die Gebäudesicherheit und Raumüberwachung sensitiver Bereiche (z. B. Serverräume) durch Zutrittskontrollen deutlich verbessert werden. Durch die sichere Anmeldung am PC durch SSO erhöht sich die Sicherheit am Arbeitsplatz gegen unbefugten Zugriff von intern und extern.

3.2.8 Bewertung

- Kompatibilität

  Die vorhandene Hard- und Software ist nicht immer auf Anhieb kompatibel zu den technischen Anforderungen der MFC. Daher müssen an verschiedenen Stellen Anpassungen vorgenommen oder Komponenten ausgetauscht werden.

- Anzahl der Mitarbeiter

  Die Anzahl der Mitarbeiter determiniert einerseits die entstehenden Anschaffungs- und Wartungskosten, andererseits beeinflusst sie auch den Gesamteffekt, den die Verwendung der MFC mit sich bringen kann. Die Stückkosten für die Karten und die dazugehörige Software sinken mit steigender Abnahmezahl und die positiven Auswirkungen erhöhen sich umso stärker, je mehr Mitarbeiter mit der MFC ausgestattet sind. Daher ist es auf den ersten Blick für größere Kommunen vorteilhafter, die MFC einzusetzen. In Bezug auf Sicherheits- und Datenschutzaspekte ist die Anzahl der Mitarbeiter jedoch nicht relevant. Daher bringt der Einsatz von MFC in Kommunen aller Größen und kommunalen Ebenen eine Verbesserung der Prozesse mit sich.

- Anwendungsbereiche

  Die Art und Anzahl der Anwendungsbereiche entscheidet auch darüber, wie wirtschaftlich oder

auch sinnvoll der Einsatz der MFC ist. Die Rentabilität ist grundsätzlich umso höher, je mehr Einsatzbereiche abgedeckt werden können. Aber der Einsatz ist auch dann sinnvoll, wenn z. B. nur die Sicherheit erhöht werden soll, indem sicheres Anmelden am PC, SSO und Zugangskontrolle mit der MFC realisiert werden.

- Betrieb der MFC-Infrastruktur

  Abhängig von der verwendeten Technologie muss auch entsprechendes Know-how für die Installation, den laufenden Betrieb und den Support für die Mitarbeiter aufgebaut werden. Dies erfordert entweder entsprechende Kapazitäten bei den Behördenmitarbeitern und deren laufende Fort- und Weiterbildung mit der Bindung wichtiger personeller Ressourcen. Oder der Betrieb wird langfristig mit einem externen Dienstleister zu günstigen Konditionen vereinbart. Unter Betrieb wird dabei die Produktion der Karten inklusive des Aufbringens von Signaturschlüsseln, Schlüsseln für die Verschlüsselung von E-Mails (oder Dokumenten) sowie die zugehörigen Zertifikate verstanden. Die Aufgaben und Funktionen der CA (Certification Authority), die z. B. für das sichere Anmelden am PC erforderlich ist, lässt sich ebenfalls nach außen vergeben. Allerdings muss dabei auf die Reaktionsfähigkeit und -zeit der Dienstleister geachtet werden. Für Kommunen, die über das erforderliche Wissen nicht verfügen oder nicht in der Lage sind, die nötigen personellen Ressourcen bereitzustellen, können auch entsprechende Lösungen komplett von externen Dienstleistern beschafft werden.

- Wirtschaftlichkeit

  In vielen größeren Kommunen gibt es bereits individuelle Lösungen für einen Teil der genannten Einsatzbereiche. Hier ist aus technischer Sicht zu überprüfen, inwieweit die bestehenden Komponenten bei Einführung der MFC weiterverwendbar sind oder abgelöst werden müssen.

  Positive finanzielle Auswirkungen machen sich z. B. unmittelbar durch sinkende Druck-, Versand- und Archivierungskosten bemerkbar. Aber viele Effekte können monetär nicht exakt bestimmt werden, weil sie sich innerhalb der Kommunen nicht unmittelbar finanziell auswirken, wie beispielsweise verringerte Transportzeiten von Dokumenten.

  Investitionen in MFC sind auch als Investitionen in die Sicherheit und in den Datenschutz aufzufassen. Denn es muss berücksichtigt werden, welcher Schaden an Reputation und in finanzieller Art entstehen kann, wenn sensible und personenbezogene Daten an die Öffentlichkeit gelangen oder Daten durch Unbefugte manipuliert oder gelöscht werden.

  Der entscheidende Gesichtspunkt ist jedoch von der Konkurrenz zwischen Investitionskosten und niedrigen Betriebskosten einerseits und höheren laufenden Betriebskosten ohne Investition ande-

rerseits bestimmt. Ökonomisch ist der Übergang zur neuen Lösung mit Investition immer dann sinnvoll, wenn die laufenden Einsparungen den Investitionsaufwand übersteigen. Dazu muss eine korrekte Berechnung im Einzelfall aufgestellt werden. Wahrscheinlich wird jedoch der Einsatz von MFC deutlich besser bewertet, weil viele Nutzenfaktoren damit verbunden sind, die sich gleichzeitig auf Dauer positiv auswirken. Dieser langfristige Aspekt ist ein entscheidendes Kriterium.

3.2.9 Empfehlung

- Große und mittlere Kommunen

  Mittlere und vor allem große Kommunen haben in der Regel die „kritische Masse“ an Anwendungsbereichen und Mitarbeiterzahl, die den Implementierungsaufwand und die Anschaffungskosten für MFC rechtfertigen. Die Einführung von MFC in Kommunen ist ein umfangreiches und komplexes Vorhaben. Aufgrund fehlender Standards und der großen Kombinationsvielfalt vorhandener Anwendungen kann keine pauschale Aussage getroffen werden, welche Komponenten reibungslos miteinander interagieren. Daher ist mit Herstellern und Lieferanten zunächst zu prüfen, inwieweit sich deren Produkte in die erforderliche Struktur einbinden lassen. Es wird außerdem empfohlen, einen auf dieses Gebiet spezialisierten Dienstleister frühzeitig einzubeziehen und auch auf die Erfahrungen in anderen Kommunen zurückzugreifen.

  Es ist davon abzuraten, die erforderliche Infrastruktur (oder einen Teil davon) selbst zu betreiben, auch wenn die Reaktionszeiten bei Fremdbetrieb im Störfall, z. B. hinsichtlich der Ausstellung von Ersatzkarten bei Verlust, länger erscheinen, als bei einem Betrieb durch eine eigene Abteilung. Der Betrieb einer MFC-Infrastruktur innerhalb der Kommune ist aber ein Fremdkörper, weil diese Aufgabe so wenig in die behördlichen Aufgaben passt, wie ein Schlüsseldienst oder die Reparatur von Hardware.

  Auf Dauer können Externe den Betrieb und die Dienstleistungen auch zu besseren Konditionen und in einer höheren Servicequalität anbieten. Zudem können sie das erforderliche Wissen dauerhaft und auf dem aktuellen Stand bereitstellen. Dies entlastet die Kommunen von diesen Aufgaben und hilft ihnen, sich auf ihre Kernaufgaben zu fokussieren. Die langfristige Strategie für eine Kommune sollte daher stets sein, derartige Leistungen von externen Partnern zu beziehen und Verfügbarkeit, Reaktionszeit usw. durch Service Level Agreements sicherzustellen.

- Kleine Kommunen

  Grundsätzlich gilt, dass sich die MFC umso eher lohnt, je mehr Mitarbeiter und Einsatzbereiche

einbezogen werden können. Gerade in kleineren Kommunen ist die Mitarbeiterzahl jedoch geringer und auch die Anzahl möglicher Anwendungsbereiche kleiner. Dennoch kann es auch hier erforderlich oder erwünscht sein, das Sicherheitsniveau z. B. durch sicheres Anmelden am PC zu erhöhen und auch noch andere Anwendungsbereiche abzudecken. In diesem Fall empfiehlt es sich, ein Komplettpaket von einem Dienstleister zu beziehen, das auch Beratung, Installation, Betrieb, Wartung und Support beinhaltet. Dabei ist zu beachten, dass bei Verlust oder Diebstahl einer Karte Zeit bis zum Ersatz vergehen kann, die mit Übergangslösungen überbrückt werden muss, bis ein Ersatzexemplar ausgestellt ist. Es wäre sicher vorteilhaft, wenn sich Kommunen in der gleichen Region zu einem gemeinsamen Vorgehen entschließen könnten, da sie dann mit ihrer gebündelten Nachfrage die Konditionen für die Dienstleistung besser bestimmen können.

3.2.10 Zwischenergebnis

Multifunktionale Chipkarten decken mit ihrem Funktionsumfang eine ganze Reihe von Anwendungsbereichen ab und tragen somit erheblich zur Verbesserung der Prozesse bei. Dabei werden je nach Einsatzgebiet unterschiedliche Anforderungen wie Datenschutz, Datensicherheit, Beschleunigung der Abläufe usw. ganz oder in Teilen erfüllt. Ohne die MFC sind zukünftig Karten für Signaturen, Kantine, Drucker, Zeiterfassung, Zugangskontrolle, Anmeldung am PC usw. erforderlich. Mit MFC wird die Verwaltung für die Karten und auch die Handhabung für die Mitarbeiter deutlich vereinfacht.

Die Einführung von MFC ist jedoch kein ganz einfaches Vorhaben. Die MFC ist für alle Kommunengrößen und kommunalen Körperschaftsgruppen geeignet. Zum Betrieb der Infrastruktur sollte ein externer Dienstleister mit der Aufgabe betraut werden. Ideal wäre eine gegenseitige Abstimmung der Kommunen über eine gemeinsame Vorgehensweise.

3.3 Neuer Personalausweis (nPA)

Hauptfunktion des neuen Personalausweises (nPA), der seit 01.11.2010 ausgeben wird, ist der Nachweis der Identität eines Bürgers durch einen Lichtbildausweis. Um den Anforderungen an die Sicherheitslage, aber auch den neuen Kommunikationsmöglichkeiten gerecht zu werden, wurde er mit zusätzlichen Funktionen ausgestattet.

Der elektronische Personalausweis wird im Scheckkartenformat (ID1-Format) ausgegeben. Er hat nur einen kontaktlosen Chip, mit dem alle nachfolgend genannten elektronischen Funktionen realisiert werden können. Von den Funktionen des nPA werden im weiteren Verlauf lediglich der elektronische Identitätsnach-

weis (eID-Funktion) und die qualifizierte elektronischer Signatur (QES) berücksichtigt.

3.3.1 Ausstattung

- eID-Funktion

  Die eID-Funktion dient dazu, den Ausweisinhaber in der elektronischen Kommunikation zweifelsfrei zu identifizieren. Diese Funktion ist das elektronische Pendant zum Vorzeigen des Personalausweises in der nicht-elektronischen Welt. Dazu können bei der Online-Kommunikation oder beim elektronischen Geschäftsverkehr wahlweise Name, Vorname, Anschrift, Geburtstag, Geburtsort usw. ausgelesen werden. Hinzu kommen die beiden Sonderfunktionen der Alters- und Wohnortverifikation. So kann z. B. geprüft werden, ob der Ausweisinhaber ein bestimmtes Mindestalter hat oder zu einer definierten Altersgruppe gehört. Bei der Wohnortverifikation wird einem Diensteanbieter lediglich bestätigt, ob der Ausweisinhaber in einem bestimmten Ort wohnt oder ob dies nicht der Fall ist. Der tatsächliche Wohnort wird dabei nicht bekannt gegeben.

  Ein Kommunikationspartner erhält somit den Nachweis, dass die Person auch diejenige ist, die sie zu sein vorgibt. Obgleich die Identifikation der Kommunikationspartner häufig ausreicht, um Rechtsgeschäfte zu tätigen, darf die eID-Funktion nicht mit einer elektronischen Unterschrift verwechselt werden. Ist die Schriftform erforderlich, so muss im elektronischen Medium zwingend die qualifizierte elektronische Signatur verwendet werden.

- Qualifizierte elektronische Signatur (QES)

  Anders als die eID, die von staatlicher Seite auf den nPA aufgebracht wird, gibt es für die QES nur kommerzielle Anbieter. Der Ausweisinhaber kann sich die QES nach Erhalt des Ausweises mit aktivierter eID-Funktion kostenpflichtig nachladen. Wie lange diese Signatur gültig ist, steht noch nicht fest und ist abhängig vom ausstellenden Trustcenter. Derzeit sind auch sogenannte Ad-hoc-Signaturen im Test. Sie haben voraussichtlich eine Gültigkeit von nur wenigen Tagen und sind auch nur für bestimmte Rechtsgeschäfte zugelassen. Dafür werden sie aber erheblich preiswerter sein.

3.3.2 Beschaffung

Der nPA wird bei der zuständigen Meldebehörde beantragt. Die eID-Funktion ist für Personen ab 16 Jahren standardmäßig aktiviert. Die QES ist derzeit noch nicht erhältlich, soll aber ab Frühjahr 2012 nachladbar sein. Die QES wird via AusweisApp über das Internet nachgeladen werden können, sofern vorher die Identifikation mit der eID-Funktion durchgeführt wurde. Nach Ablauf der Gültigkeit kann auf gleichem Wege

eine neue QES nachgeladen werden.

3.3.3 Gültigkeitsdauer und Erneuerung

Der nPA hat eine Gültigkeit von sechs Jahren für Personen bis zu 24 Jahren. Für Personen über 24 Jahre ist der Ausweis zehn Jahre lang gültig, Anschließend wird ein neuer Ausweis benötigt. Die eID-Funktion ist über die gesamte Laufzeit verfügbar. Die Gültigkeitsdauer der QES hängt vom Trustcenter ab. Nach Ablauf der Gültigkeit kann eine neue QES auf den Ausweis geladen werden. Die Gültigkeit der QES kann die Gültigkeitsdauer des nPA nicht überdauern.

3.3.4 Einsatzbereiche für die QES

Für den dienstlichen Einsatz einer auf dem Personalausweis aufgebrachten Signatur gilt das oben zur QES Gesagte. Besonderheiten ergeben sich vor allem daraus, dass die QES in der Regel als dienstliche Signatur erkennbar ist und der nPA (anders als eine dienstliche Signaturkarte) nicht wieder entzogen werden kann, Bei einem Verwaltungsakt, der aufgrund der Schriftform mit der QES unterzeichnet wird, muss gemäß § 37 Abs. 3 BayVwVfG immer die erlassende Behörde erkennbar sein. Dies wird dadurch erreicht, dass der Behördenname im Hauptzertifikat gespeichert wird. Allerdings sind mit einer solchen QES in der Regel ausschließlich Unterschriften für den dienstlichen Gebrauch erlaubt. Scheidet ein Mitarbeiter aus oder wechselt er die Abteilung, wird ihm üblicherweise die Karte entzogen. Zusätzlich wird die Karte bzw. das für die Unterschrift nötige Zertifikat gesperrt, so dass zukünftige Unterschriften auf keinen Fall mehr gültig sind.

Bei der QES für den nPA ist zunächst kein dienstlicher Zusammenhang herstellbar, da der nPA für den persönlichen Gebrauch vorgesehen ist. Auch das Einziehen des Ausweises nach Verlassen der Behörde greift hier nicht. Es gibt jedoch die Möglichkeit, ein zusätzliches dienstliches Zertifikat (Attributzertifikat) mit der QES zu verknüpfen. Dann kann ein Mitarbeiter auswählen, ob er als Privatperson signiert, ohne dass der dienstliche Bezug hergestellt wird, oder ob er als Behördenmitarbeiter signiert, wobei dann die Informationen über die Dienststelle mit einbezogen werden. Verlässt der Mitarbeiter die Behörde, wird das zusätzliche dienstliche Zertifikat gesperrt und der Signaturinhaber kann nur noch privat unterzeichnen. Wechselt er in eine andere Abteilung mit anderen Befugnissen, kann ein neues Zertifikat ausgestellt und das alte gesperrt werden. Somit könnte zumindest aus technischer Sicht sichergestellt werden, dass ein Mitarbeiter mit der QES seines Personalausweises auch dienstlich unterschreiben kann.

Aus praktischer Sicht spricht gegen den Einsatz der QES auf dem nPA für den dienstlichen Gebrauch vor allem, dass die Mitarbeiter nicht verpflichtet werden können, sich einen nPA ausstellen zu lassen oder diesen

für dienstliche Zwecke zu verwenden. Daher wären die möglichen Einsatzbereiche rein theoretische Betrachtungen und werden hier nicht weiter verfolgt.

3.3.5 Einsatzbereiche für die eID-Funktion

Das Konzept der eID-Funktion sieht vor, dass sich sowohl der Ausweisinhaber als auch der Diensteanbieter identifizieren müssen. Dies bedeutet in den nachfolgenden Fällen, dass bei jeder Anwendung der nPA und jeweils auch das Zertifikat des Diensteanbieters überprüft werden. Dies geschieht in der Regel online. Das Einbeziehen von Automaten, z. B. zur Warenausgabe, ist derzeit noch in der Entwicklungsphase.

Für das Auslesen jeglicher Daten, auch des dienste- und kartenspezifischen Kennzeichens (DKK, Pseudonym) ist stets die Eingabe der sechsstelligen PIN nötig. Für alle Anwendungsbereiche gilt, dass eine Internetverbindung bestehen muss. In den Anwendertests zum nPA wurden einige Einsatzbereiche wie Zeiterfassung, Zutrittskontrolle usw. getestet. Jedoch wurde seitens der Hersteller dieser Systeme die Entwicklung von mit dem nPA nutzbaren Lösungen nicht weiter fortgesetzt.

Aufgrund der vergleichsweise umständlichen Handhabung, der fehlenden Software und der Tatsache, dass die Mitarbeiter nicht verpflichtet werden können, den nPA für dienstliche Zwecke zu nutzen, wird die derzeitige Praxisrelevanz für die interne Nutzung als sehr gering eingeschätzt. Bis auf die interne Antragstellung und den Datenabruf wird der nPA für interne Einsatzbereiche daher nicht weiter betrachtet.

Mit der eID-Funktion kann jedoch die Antragstellung seitens der Bürger sehr gut realisiert werden.

In den nachstehenden Tabellen wird der nPA den Anwendungsbereichen gegenübergestellt und hinsichtlich seiner praktischen Bedeutung bewertet.

Tabelle 5: Einsatzbereiche und Eignung des neuen Personalausweises

Technologie/Einsatzbereich	Eignung
Interne Antragstellung und Datenabruf (eID-Funktion)	+(1)
Online-Antragstellung durch Bürger und Unternehmen (eID-Funktion)	++(2)
Online-Antragstellung durch Bürger und Unternehmen (QES)	o (3,4)

\- nicht möglich, o nicht praktiziert, + geeignet, ++ sehr gut geeignet

(1) Sofern eine starke Authentisierung der Mitarbeiter erforderlich ist, könnte die eID-Funktion auf freiwilliger Basis hierfür verwendet werden.

(2) Für alle Bürger und für Unternehmen bei denen die Mitarbeiter mittels der eID-Funktion Anträge stellen dürfen (z. B. Anmeldung an einem Portal als Login-Ersatz) oder bei Einzelunternehmern bzw. Freiberuflern.

(3) Grundsätzlich möglich, hat aber nur sehr geringe Verbreitung.

(4) Nur wenn Mitarbeiter einverstanden sind oder bei Einzelunternehmern bzw. Freiberuflern.

Tabelle 6: Einsatzbereiche und Praxisrelevanz des neuen Personalausweises

Technologie/Einsatzbereich	Praxisrelevanz
Interne Antragstellung und Datenabruf (eID-Funktion)	Nein(1)
Online-Antragstellung durch Bürger und Unternehmen (eID-Funktion)	Ja
Online-Antragstellung durch Bürger und Unternehmen (QES)	Eingeschränkt (2)

- nicht möglich, o nicht praktiziert, + geeignet, ++ sehr gut geeignet

(1) Die Verwendung der eID-Funktion für interne Anträge liegt derzeit nur als Prototyp vor.

(2) Aufgrund der voraussichtlich geringen Verbreitung evtl. nur für bestimmte Zielgruppen relevant.

3.3.6 Mögliche Einschränkungen und Hindernisse

- Derzeit noch keine QES erhältlich

  Voraussichtlich wird die QES im Frühjahr 2012 auf den nPA nachladbar sein und steht dann grundsätzlich für die oben genannten Funktionen zur Verfügung.

- Geringe Verbreitung der eID-Funktion

  Der nPA hat derzeit nur eine sehr geringe Verbreitung. Stand Dezember 2011 waren etwas mehr als acht Millionen Ausweise im Umlauf. Allerdings ist die Zahl der freigeschalteten eID-Funktionen deutlich geringer. Vom einzig derzeit zertifizierten Lesegerät sind erst ca. 600.000 Stück im Umlauf (Stand Dezember 2011).

3.3.7 Kostenfaktoren

- Kosten für Zertifikate

  Sollen die Bürger Anträge mit ihren eID-Funktionen ausfüllen oder sich an Bürgerservice-Portalen anmelden können, sind seitens der Kommunen sogenannte Berechtigungszertifikate erforderlich, um die Daten aus den Ausweisen auslesen zu können. Die Zertifikate gliedern sich in die Berechtigung selbst, die von der Vergabestelle für Berechtigungszertifikate erteilt werden, und in technische Zertifikate, die auf dem eID-Server installiert werden.

  - Berechtigungszertifikate

    Für Kommunen fallen hier keine Kosten an.

- Technische Zertifikate

  Die Kosten hierfür können variieren. Wird z. B. das Bürgerservice-Portal der AKDB verwendet, fallen keinen weiteren Kosten an. Eine Kommune kann jedoch die technischen Zertifikate auch selbst beschaffen. Der genaue Preis hierfür ist noch nicht bekannt, dürfte in Bayern aber deutlich unter. 2.000-2.500 Euro pro Jahr liegen. Die genauen Preise müssen hierbei vom ausstellenden Trustcenter erfragt werden.

- Installationsaufwand

  Für die Hardware und die Software fällt jeweils auch ein entsprechender Aufwand. Die Installation kann entweder durch ein externes Unternehmen oder von der eigenen IT-Abteilung durchgeführt werden.

- Softwareanpassungen

  Unter Umständen müssen erst Schnittstellen oder Fachverfahren angepasst oder erstellt werden.

- Organisatorische Aufwände

  Bereits vor der Einführung der nPA-Nutzung (eID-Funktion und QES) zur Antragstellung für die Bürger sind organisatorische Abstimmungen erforderlich. Diese bemessen sich im Umfang zunächst danach, wie viele Einsatzbereiche (zu Beginn) abgedeckt werden sollen. Anschließend ist zu überlegen, ob bisherige Abläufe nicht im Zuge der Einführung geändert werden können oder müssen.

- Keine Kosten für eID-Server bzw. eID-Service

  Für die Nutzung des eID-Service zum Auslesen der eID-Daten von Bürgern fallen für die Kommunen in Bayern keine Kosten an. Hierfür wird der eID-Service über das LfStaD als kostenlose Infrastrukturkomponente zur Verfügung gestellt.

3.3.8 Potenziale des neuen Personalausweises

- (Teilweiser) Ersatz der Schriftform

  Im Rahmen des im Frühjahr 2012 als Referentenentwurf vorliegenden eGovernment-Gesetzes des Bundes ist die eID-Funktion des neuen Personalausweises in zahlreichen Fällen als Alternative zur händischen Unterschrift bzw. QES vorgesehen.

- Medienbruchfreiheit

Die Online-Erfassung der Daten führt dazu, dass Medienbrüche vermieden bzw. reduziert werden können und die Abläufe (durchgehend) elektronisch durchführbar sind.

- Modernes Image

  Ein verstärktes Online-Angebot verbessert das Image einer Behörde.

- Erhöhung der Bürgerzufriedenheit

  Die Möglichkeit, mehr Dienste online durchzuführen, erhöht die Bürgerzufriedenheit, da sich diese dadurch zumindest einen Teil der Wege zu den Behörden sparen können.

3.3.9 Bewertung

- Behördeninterner Einsatz

  Zukünftig könnten Mitarbeiter eventuell die eID-Funktion auf freiwilliger Basis für bestimmte Anwendungsbereiche nutzen. Jedoch müssen auch für diesen Fall zur eID-Funktion alternative Möglichkeiten vorhanden sein.

- Online-Anträge für Bürgerseite und Unternehmen

  Prozessauswahl

  Die eID-Funktion eignet sich sehr gut für die elektronische Antragstellung seitens der Bürger. Die Kommune muss hierfür aber auch die geeigneten Prozesse bereitstellen. Zu Beginn sollten Anträge ausgewählt werden, die eine hohe Fallzahl und eine geringe Komplexität aufweisen. Daneben sind auch Aspekte wie Bürgerfreundlichkeit, Mitarbeiterfreundlichkeit, Kosteneinsparungen usw. von Bedeutung, die von der jeweiligen Verwaltungsspitze unterschiedlich gewichtet werden können.

  Prüfung des Schriftformerfordernis'

  Die QES ist zwar zukünftig auf dem nPA möglich, aber es kann nicht davon ausgegangen werden, dass sie weite Verbreitung finden wird. Der Gesetzgeber beabsichtigt daher, neben der QES weitere Alternativen als Ersatz der Schriftform anzuerkennen. Der derzeit vorliegende Entwurf des E-Government-Gesetzes des Bundes liefert mit einer weitgehenden rechtlichen Anerkennung von eID-Funktion und DE-Mail hierzu wichtige Impulse. Für Kommunen bedeutet dies, sich zunächst möglichst auf solche Vorgänge zu konzentrieren, bei denen von den geplanten Erleichterungen Gebrauch gemacht werden kann.

QES für Zielgruppen

Die geringe Verbreitung der QES macht sie für die Antragstellung aus Sicht der Kommunen lediglich für bestimmte Zielgruppen, wie z. B. KFZ-Händler, Autohäuser (KFZ-Zulassung) oder andere Berufsgruppen, interessant, die häufig mit der Verwaltung zu tun haben.

Integration in Fachverfahren

Damit die Kommunen größtmöglichen Nutzen haben, müssen die Daten medienbruchfrei in die Fachverfahren übertragen werden können. Bei der Auswahl von Fachverfahrenskomponenten ist daher großer Wert darauf zu legen, dass die entsprechenden Daten automatisiert übernommen werden können.

Weitere Komponenten

Um Verbesserungen in der Prozessabwicklung zu erreichen, reicht die aktivierte eID-Funktion seitens der Bürger oder Unternehmen nicht aus. Es müssen mehrere Komponenten, technischer und auch organisatorischer Art, zusammenspielen. Die eID-Funktion ist bei der Online-Abwicklung von Prozessen somit nur ein Baustein, der beispielsweise durch Bezahlfunktionen, dem Wegfall von Unterschriften, Akzeptieren elektronischer Dokumente statt Originalvorlagen usw. begleitet sein muss.

Alternativen zur eID

Bislang verfügen nur ca. 10 Prozent der Bürger über einen nPA, wovon nur weniger als die Hälfte die eID-Funktion aktiviert haben. Daher sollte bei der Online-Antragstellung auch immer eine Alternative zur Verwendung der eID-Funktion angeboten werden (z. B. Online-Konto, bei dem man sich schriftlich anmelden muss).

Wirtschaftlichkeit

Durch die Bereitstellung des eID-Services als kostenlose Infrastrukturkomponente fällt zwar ein erheblicher Kostenblock weg, aber zunächst entstehen zumindest für die organisatorischen Veränderungen und internen Abstimmungen Kosten und zeitliche Aufwände. Inwieweit diesen Kosten auch Erträge gegenüber stehen, ist von mehreren Faktoren abhängig. Dazu gehört z. B. die Anzahl der Anträge, die via Internet gestellt werden. Auch die Integrationstiefe, der Grad der Medienbruchfreiheit und die Automatisierungsfähigkeit von Prozessen beeinflussen die Wirtschaftlichkeit.

Bislang kann nur ein Bruchteil der vorhandenen Anträge von den Bürgern online vollständig ausgefüllt werden. Durch den Wegfall des Schriftformerfordernis und der Verbreitung von Bürger-

Service-Portalen wird sich diese Quote jedoch erhöhen und somit auch die Wirtschaftlichkeit verbessern.

3.3.10 Empfehlung

- Interne Nutzung der QES Kommunen (alle Kommunengrößen)

  Für Kommunen stellt der nPA keine Alternative dar. Die Funktionen für den internen Bereich (Zutrittskontrolle, Zeiterfassung etc.) können derzeit nicht realisiert werden. Für Mitarbeiter, die eine QES benötigen, muss eine „herkömmliche" QES für den dienstlichen Gebrauch beschafft werden. Für die anderen Einsatzbereiche aus der oben stehenden Übersicht kann sich je nach Art und Umfang die MFC lohnen.

- eID-Funktion für Bürger und Unternehmen (alle Kommunengrößen)

  Der allgemeine Trend in Wirtschaft und öffentlicher Verwaltung geht in Richtung Online-Abwicklung von Prozessen. Daher wird es zukünftig für Kommunen aller Art und Größe erforderlich sein, das vorhandene Online-Angebot auszuweiten und für die Bürger einfacher und bequemer zu machen. Dazu gehört auch, den Bürgern die Möglichkeit zu geben, die eID-Funktion ihres nPA für die Antragstellung zu verwenden.

  Für das Angebot von Online-Diensten ist auf lange Sicht eine Portallösung die geeignetste und auch wirtschaftlichste Lösung. Landkreise, Städte und Gemeinden haben in großen Bereichen deckungsgleiche Aufgaben und sogar identische Antragsformulare. Dafür bieten sich standardisierte Produkte, wie z. B. Portale an, die bereits über die erforderlichen Funktionen und Komponenten wie ePayment, Nutzung der eID-Funktion, Anbindung an Formularserver usw., verfügen. Für die jeweilige Behörde kann dann Aussehen und Funktionsumfang angepasst werden. Somit stehen Kommunen aller Größen grundsätzlich alle Funktionen zur Verfügung, die sich je nach Anforderung auch nachträglich zu- oder abschalten lassen. Die Portallösungen sollten bei einem externen Dienstleister betrieben werden, da sich hierdurch weitere Kostenvorteile ergeben, wenn die Applikation für mehrere Kommunen verwendet wird. Zudem können hier Verfügbarkeit und Ausfallsicherheit, die insbesondere bei kundenbezogenen Lösungen eine große Rolle spielen, in höherem Maß gewährleistet werden.

3.3.11 Zwischenergebnis

Der nPA ist in seiner derzeitigen Ausprägung für den kommuneninternen Einsatz nicht geeignet. Hierfür sind die anderen vorgestellten Technologien, je nach Anwendungsbereich, die deutlich bessere Wahl. Bezüglich der Online-Antragstellung für Bürger und teilweise auch für Unternehmen bietet insbesondere die eID-Funktion des Ausweises aber große Potenziale, vorausgesetzt die erforderlichen (Portal-)Lösungen auf Seiten der Kommunen werden dafür bereitgestellt.

4 Zusammenfassung

In diesem Kapitel werden die Technologien und deren Einsatzbereiche noch einmal gesamthaft tabellarisch gegenübergestellt. Anschließend folgt eine Zusammenstellung der wesentlichen Ergebnisse der Untersuchung.

4.1 Übersicht Technologien und Einsatzbereiche

In den beiden nachfolgenden Tabellen werden die Eignung und die Praxisrelevanz aller identifizierten Einsatzbereiche und Technologien gegenübergestellt.

Tabelle 7: Einsatzbereiche und Eignung insgesamt

Technologie / Einsatzbereich	Eignung				
	nPA		MFC/MFD (mit eFES)	Signaturen	
	eID	QES		eFES	QES
Online-Antragstellung durch Bürger und Unternehmen	++(5)	o (2,6)	–	–	o(2)
Behördenintern					
Dienstausweis	–	–	++	–	–
Drucken vertraulicher Dokumente (Follow-Me-Printing)	–	–	++	–	–
Elektronischer Anordnungs-Signatur-Workflow	–	–	++	++	++
Elektronischer Vergabeprozess (eVergabe)	–	–	o(1)	–	++
Elektronischer Versand personenbezogener Daten	–	–	++(4)	–	–
Elektronisches Abfallnachweisverfahren (eANV)	–	–	o (1)	–	++
Elektronisches Personenstandsregister (ePR)	–	–	o(1)	–	++
Interne Antragstellung und Datenabruf	+(7)	–	+(3)	–	++
Kantine und Verpflegungsautomaten	–	–	++	–	–
Sicheres Anmelden am PC	–	–	++	–	–
SSO	–	–	++	–	–
Zeiterfassung	–	–	++	–	–
Zutrittskontrolle	–	–	++	–	–

- nicht möglich, o nicht praktiziert, + geeignet, ++ sehr gut geeignet

(1) Hierfür wäre die QES erforderlich, diese wird aufgrund technischer und organisatorischer Schwierigkeiten derzeit nicht auf den MFC aufgebracht.

(2) Grundsätzlich möglich, hat aber nur sehr geringe Verbreitung.

(3) Aufgrund des hohen Sicherheitsniveaus bei der sicheren Anmeldung am PC mit einer MFC bewirkt diese sichere Authentisierung auch eine verbesserte Sicherheitslage bei internen Anträgen ohne Schriftformerfordernis.

(4) Mit einem Schlüssel und einem entsprechenden Zertifikat vom LfStaD können E-Mails innerhalb von bayerischen Behörden verschlüsselt versendet werden, sofern die Kommunikationsteilnehmer über die erforderliche Infrastruktur verfügen.

(5) Nur für Unternehmen bei denen die Mitarbeiter mittels der eID-Funktion Anträge stellen dürfen (z. B. Anmeldung an einem Portal als Login-Ersatz) oder bei Einzelunternehmern bzw. Freiberuflern.

(6) Nur wenn Mitarbeiter einverstanden sind oder bei Einzelunternehmern bzw. Freiberuflern.

(7) Sofern eine starke Authentisierung der Mitarbeiter erforderlich ist, könnte die eID-Funktion auf freiwilliger Basis hierfür verwendet werden.

Tabelle 8: Einsatzbereiche und Praxisrelevanz insgesamt

Technologie / Einsatzbereich	Praxisrelevanz				
	nPA		MFC/MFD (mit eFES)	Signaturen	
	eID	QES		eFES	QES
Online-Antragstellung durch Bürger und Unternehmen	Ja[3]	Nein	Nein	Nein	Nein
Behördenintern					
Dienstausweis	Nein	Nein	Ja [2]	Nein	Nein
Drucken vertraulicher Dokumente (Follow-Me-Printing)	Nein	Nein	Ja, aber nicht überall erforderlich.	Nein	Nein
Elektronischer Anordnungs-Signatur-Workflow	Nein	Nein	Ja	Ja	Nein
Elektronischer Vergabeprozess (eVergabe)	Nein	Nein	Nein	Nein	Nein
Elektronischer Versand personenbezogener Daten	Nein	Nein	Eingeschränkt [1]	Nein	Nein
Elektronisches Abfallnachweisverfahren (eANV)	Nein	Nein	Nein	Nein	Ja
Elektronisches Personenstandsregister (ePR)	Nein	Nein	Nein	Nein	Ja
Interne Antragstellung und Datenabruf	Nein[4]	Nein	Eingeschränkt [5]	Nein	Nein
Kantine und Verpflegungsautomaten	Nein	Nein	Ja	Nein	Nein
Sicheres Anmelden am PC	Nein	Nein	Ja	Nein	Nein
SSO	Nein	Nein	Ja	Nein	Nein
Zeiterfassung	Nein	Nein	Ja	Nein	Nein
Zutrittskontrolle	Nein	Nein	Ja	Nein	Nein

(1) Auch der Kommunikationspartner muss zur Ver-/Entschlüsselung in der Lage sein, was derzeit unwahrscheinlich ist.

(2) Wird in Kombination z. B. mit der Zutrittskontrolle kritisch gesehen. Daher können in diesen Fällen zusätzliche Sicherheitsmechanismen wie PIN-Abfrage, zeitliche Befristung des Zutritts u. ä. ergriffen werden. .

(3) Nur für Privatpersonen, Einzelunternehmer oder Freiberufler.

(4) Die Verwendung der eID-Funktion für interne Anträge liegt derzeit nur als Prototyp vor.

(5) Aufgrund des hohen Sicherheitsniveaus bei der sicheren Anmeldung am PC mit einer MFC bewirkt diese sichere Authentisierung auch eine verbesserte Sicherheitslage bei internen Anträgen ohne Schriftformerfordernis. Derzeit aber noch geringe Verbreitung und nur wenige Anwendungsfälle.

4.2 Zusammenfassung der Untersuchungsergebnisse

Die nachfolgenden Aspekte beziehen alle Kommunengrößen und Körperschaftsgruppen mit ein.

- Überschneidung der Funktionen

  Die beschriebenen Technologien überschneiden sich zum Teil in ihren Funktionen. So kann die erweiterte fortgeschrittene elektronische Signatur als eigenständige Kartenlösung eingesetzt werden, sie kann aber auch Bestandteil einer multifunktionalen Chipkarte sein. Eine MFC lässt sich allerdings auch ohne eFES verwenden, dann jedoch ohne die Möglichkeit der Signatur. Die qualifizierte elektronische Signatur ist ebenfalls als eigenständige Kartenlösung erhältlich.

- Ersatz bestehender elektronischer Lösungen

  Für einige der Anwendungsbereiche wie z. B. die Zeiterfassung und Zutrittskontrolle existieren bereits elektronische Lösungen, meist in Form eines Schlüsselanhängers mit integriertem Kontaktloschip. Diese bisherigen Technologien können z. B. durch MFC ersetzt werden.

- Größter Funktionsumfang mit MFC

  Das größte Einsatzpotenzial für die hier untersuchten Anwendungsbereiche böte unter den genannten Technologien die multifunktionale Chipkarte, wenn sie mit einer QES ausgestattet wären. Bislang ist es aus organisatorischen, technischen und auch finanziellen Gründen schwierig, MFC mit solchen Signaturen auszurüsten. Einen etwas geringeren Funktionsumfang bieten diese Karten daher, wenn sie mit einer eFES versehen sind. Dies bedeutet allerdings, dass für einige Anwendungsfälle zusätzlich Karten mit einer QES beschafft werden müssen.

- Finanzielle Aspekte nicht allein ausschlaggebend

  Bei der Anschaffung einer eFES, QES oder MFC sind finanzielle Einsparungen immer nur ein Kriterium von mehreren. Denn Aspekte wie Mitarbeiterzufriedenheit, Bürgerservice, vor allem aber

Datenschutz und Sicherheit lassen sich nicht monetär messen, sind aber dennoch von entscheidender Bedeutung. Hier muss beispielsweise kalkuliert werden, wie hoch die Kosten und der Imageschaden wären, wenn Daten durch Unbefugte gelöscht oder manipuliert würden oder sensible und personenbezogene Daten gestohlen und an die Öffentlichkeit gelangen würden.

- Hemmschuh Schriftformerfordernis

  In einigen Bereichen ist das Schriftformerfordernis der Hauptgrund für die papierbasierte Abwicklung. Da sich die QES weder im privaten noch im öffentlichen Bereich durchgesetzt hat, ist der Gesetzgeber gefragt, etwa im Rahmen des geplanten E-Government-Gesetzes Einschränkungen oder Alternativen zur Erfüllung eines Schriftformerfordernises zuzulassen. Wo dies nicht möglich ist, müssen innerhalb der Kommunen QES eingesetzt werden, um dennoch einen medienbruchfreien Ablauf zu ermöglichen.

  eFES, QES oder MFC

  Die eFES kann nur wenige Einsatzbereiche abdecken, darunter aber den sehr wichtigen Anordnungs-Signatur-Workflow. Die MFC hingegen hat den größten Funktionsumfang und kann dadurch auch die meisten Anwendungsbereiche abdecken. Zwar sind nicht in jeder Kommune alle beschriebenen Anwendungsbereiche vorhanden, so dass das Potenzial von MFC nicht überall voll ausgeschöpft werden kann. Aber hinsichtlich Medienbrüchen, Datensicherheit und Datenschutz gibt es in jeder Kommune Anforderungen und in den meisten auch Defizite. Daher sind einige der Einsatzbereiche in jeder Kommune gegeben. Grundsätzlich sollte die Lösung so gewählt werden, dass eine spätere Ausweitung der Funktionalitäten auf die jeweils in der Kommune vorhandenen Anwendungsbereiche nicht verhindert wird.

  Sofern keine Alternativen zur Erfüllung der Schriftform geschaffen werden und es im Gegenzug möglich bzw. organisatorisch und finanziell attraktiv ist, MFC mit einer QES auszustatten, könnte auch dieser Weg gewählt werden. Durch eine QES vergrößert sich dann der potentielle Funktionsumfang und die durchgängige Medienbruchfreiheit von Prozessen wird noch weiter erhöht.

- Notwendige Verbesserungen bei Integration und Standardisierung

  Seitens der Hersteller von Hard- und Softwarekomponenten – dies schließt auch die Fachverfahrenshersteller ein – sind noch einige Herausforderungen hinsichtlich Medienbruchfreiheit, Kompatibilität, Integration und Standardisierung zu bewältigen, damit die Kommunen hiervon in vollem Umfang profitieren können. Eine technische Lösung, die alle vorliegend untersuchten Anforderungen vollständig erfüllt und wirtschaftlich zu beschaffen ist, gibt es noch nicht.

  Ähnliches gilt auch für den Einsatz von Bürgerservice-Portalen. Die am Markt verfügbaren Lösun-

gen stehen noch am Anfang der Entwicklung, soweit es um die umfassende Abwicklung der Verwaltungskommunikation geht. Auch gibt es noch große Verbesserungspotenziale hinsichtlich Standardisierung, Anpassbarkeit und Interaktion wie Integration, wenn es etwa darum geht, dass die Fachverfahren unterschiedlicher Hersteller in ein Bürgerportal eingebunden werden.

- Externe Dienstleister

  Insbesondere kleinere Kommunen sind nicht in der Lage, die nötigen Infrastrukturen und Softwareapplikationen für eFES, MFC und Bürgerserviceportale selbst zu betreiben und zu betreuen. Um trotzdem von den Prozessverbesserungen durch die beschriebenen Technologien zu profitieren, sollten sie sich dringend an spezialisierte Dienstleister wenden. Aber auch für größere Kommunen sollte es grundsätzlich Strategie sein, komplexe und anspruchsvolle IT-Aufgaben hinsichtlich eFES, MFC und Bürgerservice-Portalen an externe Spezialisten zu vergeben. Für die Kommunen ist es gegenwärtig noch schwierig, Betrieb und Support von Hard- und Software auszulagern. Es ist jedoch absehbar, dass kompatible Produkte als Serviceleistungen angeboten werden und damit ausgereifte wie standardisierte Vorgehensweisen und Service-Modelle zum Betrieb durch externe Dienstleister Shared Service Center oder andere zentrale Einrichtungen Verbreitung finden.

5 Glossar

Ad hoc Signatur

Bei der Ad hoc Signatur handelt es sich um eine qualifizierte elektronische Signatur, die kurzfristig bei Bedarf auf den nPA geladen, dann aber nur einmalig für einen bestimmten Zweck verwendet werden kann. Der Vorteil dieser Lösung liegt in der vergleichsweise einfachen Beschaffung sowie dem günstigeren Preis gegenüber der regulären QES. Diese Signaturform befindet sich derzeit in der Testphase.

AusweisApp

Die AusweisApp ist eine kostenlose Software des Bundes und läuft auf dem PC des Ausweisinhabers. Sie übernimmt die Kommunikation zwischen dem Ausweis-Chip des neuen Personalausweises und dem eID-Server des Diensteanbieters.

Authentisierung

Bei der Authentisierung stellt eine Person eine Behauptung zu ihrer Identität auf. Dazu legt sie einen bestimmten Nachweis vor, der bestätigt, dass sie tatsächlich diejenige ist, für die sie sich ausgibt. Setzt ein Ausweisinhaber bspw. seinen nPA im Internet als elektronischen Identitätsnachweis ein, spricht man von einer Authentisierung.

Authentifizierung

Bei der Authentifizierung überprüft ein Kommunikationspartner die Identität seines Gegenübers anhand des Nachweises, den dieser im Rahmen der Authentisierung erbracht hat.

Benutzerrolle

Benutzerrollen werden verwendet, um unterschiedliche Berechtigungen, Eigenschaften oder Aufgaben von Personen bei der Nutzung einer Software abzubilden.

Berechtigungszertifikat

Um auf die elektronische Identitätsfunktion des nPA zugreifen zu können, muss ein Diensteanbieter über ein sogenanntes Berechtigungszertifikat verfügen. Dieses weist seine Identität sowie die Berechtigung zum Zugriff auf bestimmte Datenfelder des Ausweises nach. Derartige Zertifikate müssen bei der Vergabestelle für Berechtigungszertifikate beantragt und von einem privaten Berechtigungszertifikatsanbieter bezogen werden.

Chipkartenlesegerät

Das Kartenlesegerät bildet die Verbindung zum PC und ermöglicht den Zugriff auf die Anwendungen und Daten der Chipkarte. Es werden unterschiedliche Sicherheitsklassen unterschieden. Zur sicheren PIN-Eingabe benötigt der Kartenleser ein eigenes PIN-Pad (ab Klasse 2). Nur Kartenleser ab Klasse 2 können für die QES eingesetzt werden. Für die Nutzung der eID-Funktion und des nPA sind andere Kartenleser erforderlich. Für die Nutzung der eID-Funktion können Leser der Kategorie B (Basis) und S (Standard) verwendet werden. Für die Nutzung der QES mit dem nPA ist ein Leser der Kategorie K (Komfort) nötig.

eFES

Siehe Elektronische Signatur, „erweiterte" fortgeschrittene.

eGovernment

Integration aller digitalisierbaren Informationsaufgaben in Behörden, mit den Bürgern und den Unternehmen.

eID

Siehe Elektronische Identitätsfunktion.

eID-Server

Der eID-Server bildet die Schnittstelle zwischen dem Diensteanbieter und dem Ausweisinhaber. Die elektronische Kommunikation sowie das Abrufen bestimmter Ausweisdaten erfolgt über diese Schnittstelle. Der eID-Server kann vom Diensteanbieter selbst oder von einem Dienstleister betrieben werden.

eID-Service

Im Rahmen eines eID-Services übernimmt der eID-Server eines Dienstleisters gegen eine bestimmte Transaktionsgebühr die Kommunikation sowie das Abrufen der Ausweisdaten. In Bayern wird dieser Dienst vom LfStaD kostenlos zur Verfügung gestellt.

Elektronische Identitätsfunktion (eID)

Der neue Personalausweis besitzt eine sogenannte eID-Funktion, mit deren Hilfe sich der Ausweisinhaber in der virtuellen Welt eindeutig gegenüber Dritten identifizieren kann. Im Sinne der gegenseitigen Authentifizierung muss auch der Diensteanbieter seine Identität sowie seine Berechtigung zum Zugriff auf die Ausweisdaten über ein Berechtigungszertifikat nachweisen.

Elektronisch Signatur, einfache (ES)

Das SigG definiert unterschiedliche Arten elektronischer Signaturen. Die einfachste Form sind allgemein nach § 2 SigG „Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit

ihnen verknüpft sind und die zur Authentifizierung dienen“. Sowohl die gescannte Unterschrift, als auch eine einfache Namensangabe unter einer E-Mail fallen in diese Kategorie. Einfache elektronische Signaturen haben keinerlei Beweiskraft vor Gericht.

Elektronische Signatur, fortgeschrittene (FES)

Eine FES sichert die Unverfälschtheit der signierten Daten und ermöglicht die Identifizierung des Signaturerstellers. Technisch gesehen kann sie auf unterschiedliche Weise (Softwarezertifikat oder auf Hardwaretoken) realisiert werden. Sie bietet zwar ein höheres Schutzniveau als die einfache elektronische Signatur, ist aber dennoch nicht zum rechtswirksamen Unterzeichnen elektronischer Dokumente geeignet. Bei der FES ist stets die Vertrauenswürdigkeit der ausstellenden Institution sehr wichtig. Die FES der Bayerischen Verwaltungs-PKI hat daher einen sehr hohen Stellenwert hinsichtlich Beweiskraft und Vertrauenswürdigkeit.

Elektronische Signatur, „erweiterte“ fortgeschrittene (eFES)

Eine „erweitere“ FES erfüllt viele Kriterien der qualifizierten elektronischen Signatur. So ist sie bspw. auf einer Signaturkarte gespeichert. Sie hat hinsichtlich Beweiskraft und Vertrauenswürdigkeit einen noch höheren Stellenwert als die FES. In bayerischen Kommunen kann die eFES im Bereich des HKR zur elektronischen Unterzeichnung von Anordnungen verwendet werden.

Elektronische Signatur, qualifizierte (QES)

Die QES bildet die höchste Sicherheitsstufe elektronischer Signaturen. Nur eine QES ist per Gesetz der eigenhändigen Unterschrift gleichgestellt.

Elektronisches Zertifikat

Zertifikate sind elektronische Bescheinigungen, die im Rahmen der Signaturprüfung einen öffentlichen Schlüssel sicher einer bestimmten Person zuordnen und deren Identität bestätigen. Sie werden von sogenannten Trustcentern ausgestellt.

Erweiterte fortgeschrittene elektronische Signatur (eFES)

Siehe Elektronische Signatur, „erweiterte“ fortgeschrittene.

ES

Siehe Elektronisch Signatur, einfache.

FES

Siehe Elektronische Signatur, fortgeschrittene.

Follow-Me-Printing

Unter „Follow-Me-Printing“ versteht man das sichere Drucken von Dokumenten. Der Mitarbeiter sendet dabei wie gehabt einen Druckbefehl an den Drucker. Die Dokumente werden aber erst ausgegeben, wenn der Mitarbeiter sich tatsächlich am Drucker befindet und sich bspw. mithilfe seiner MFC am Drucker authentisiert hat.

Fortgeschrittene elektronische Signatur (FES)

Siehe Elektronische Signatur, fortgeschrittene.

Integrität

Integrität bezeichnet die Unverfälschtheit elektronischer Daten. Integritätsgesicherte Daten ermöglichen es, nachträgliche Veränderungen während der Übertragung oder während der Speicherung zu erkennen.

Integration

Integration ist für ein System der betrieblichen Informationsverarbeitung einmalige Erfassung und dauerhafte Speicherung aller Informationen bei ihrer Entstehung, die Ableitung neuer Informationen durch semantische Verknüpfung und Darstellung sowie die Bereitstellung von Informationen und Daten zur aufgabenbezogenen Verwendung.

Medienbruch

Ein Medienbruch liegt vor, wenn Informationen von einem Medium auf ein anderes übertragen werden müssen (bspw. von der Papierform auf die elektronische Form). Um eine möglichst hohe Effizienz der Prozesse zu gewährleisten, sollte die Anzahl der Medienbrüche minimiert werden.

MFC

Siehe Multifunktionale Chipkarte.

MFD

Siehe Multifunktionaler Dienstausweis.

Middleware

Als Middleware bezeichnet man eine Software, die über entsprechende Schnittstellen zwischen inkompatiblen Anwendungen vermittelt.

Multifunktionale Chipkarte (MFC)

MFC sind Smartcards in Scheckkartenformat, deren integrierter Chip unterschiedliche Anwendungen ermöglicht, wie bspw. Verschlüsselung, SSO, Zeiterfassung, Zugangskontrollen sowie Bezahlfunktion. Über ein Kartenlesegerät erfolgt der Zugriff auf die Anwendungen und Daten.

Multifunktionaler Dienstausweis (MFD)

MFD sind Smartcards, die einerseits als MFC für unterschiedliche Anwendungen eingesetzt werden, dem Inhaber daneben aber auch als Sichtausweis dienen, also das Lichtbild, die Unterschrift, Dienststelle o. Ä. des Ausweisinhabers tragen.

nPA

Siehe Neuer Personalausweis.

Neuer Personalausweis (nPA)

Der nPA ist ein scheckkartengroßes hoheitliches Ausweisdokument mit integriertem Funkchip, das einen Identitätsnachweis auch virtuell und zudem das rechtsverbindliche Unterschreiben elektronischer Dokumente ermöglicht.

QES

Siehe Elektronische Signatur, qualifizierte.

Qualifizierte elektronische Signatur (QES)

Siehe Elektronische Signatur, qualifizierte.

Single-Sign-On (SSO)

SSO ermöglicht es, dass ein Mitarbeiter nach einmaliger Anmeldung am PC auf eine Vielzahl unterschiedlicher Anwendungen und Daten zugreifen kann, ohne dafür wiederum spezielle Anmeldedaten verwenden zu müssen.

Trustcenter

Als Trustcenter oder auch Zertifizierungsstelle bezeichnet man eine vertrauenswürdige Instanz, die einer Person einen bestimmten öffentlichen Schlüssel zuweist und deren Identität bestätigt. Nur Trustcenter können qualifizierte Zertifikate zum Erzeugen einer QES ausstellen.

Verbindlichkeit

Die Verbindlichkeit stellt einen wesentlichen Aspekt elektronischer Kommunikation dar. Sie beinhaltet die Authentizität der Kommunikationsteilnehmer sowie die Nichtabstreitbarkeit der Inhalte. Die Verbindlichkeit kann mithilfe einer elektronischen Signatur gesichert werden.

Vertraulichkeit

Vertrauliche Daten müssen über geeignete Maßnahmen vor unberechtigtem Zugriff geschützt werden.

Zertifizierungsstelle

Siehe Trustcenter.