ORH-Bericht 2006 TNr. 19
Verzeichnisdienst und elektronische Signatur in der Verwaltung

Jahresbericht des ORH

Die Verwaltung hat Ministerratsbeschlüsse und entsprechende Handlungszwänge zum Aufbau der Basiskomponenten Zentraler Verzeichnisdienst und elektronische Signatur initiiert, ohne zuvor den Bedarf und die Wirtschaftlichkeit zu untersuchen. Die elektronische Signatur ist kaum im praktischen Einsatz.

Beschluss des Landtags
vom 17. April 2007
(Drs. 15/7950 Nr. 2 d)

Die Staatsregierung wird gem. Art. 114 Abs. 3 und 4 der Bayerischen Haushaltsordnung ersucht, beim Aufbau eines zentralen Verzeichnisdienstes und bei der Einführung der elektronischen Signatur den Bedarf und die Wirtschaftlichkeit unter Berücksichtigung der Feststellungen des ORH zu prüfen und dem Landtag über die Ergebnisse bis zum 30.11.2008 zu berichten. Hinsichtlich der elektronischen Signatur ist bis zum 30.11.2007 zu berichten.

Stellungnahme des Staatsministeriums des Innern
vom 15. April 2009
(Gz. IZ7-1074.9-12)

Das Staatsministerium stellt im Wesentlichen die technischen Grundlagen und den aktuellen Sachstand dar:

Zentraler Verzeichnisdienst:

Ein Verzeichnisdienst stelle in einem Computernetz notwendige Informationen in einer festgelegten Art über Objekte zur Verfügung, die über dieses Netz miteinander verbunden werden. Der Vorteil eines zentralen Verzeichnisdienstes sei, dass Daten wie etwa bei einer Benutzerkennung (Namen des Benutzers und Rechnername) nur einmal an einer zentralen Stelle zur Verfügung gestellt würden und damit eindeutig seien. Typische Anwendungsgebiete seien die Verwaltung von Adressbüchern, Ressourcen und Benutzern sowie die Authentisierung.

Man verfolge die Implementierung eines integrierenden zentralen Verzeichnisdienstes in der Funktion eines Identity-Management-Systems. Dieses sei als Infrastrukturkomponente notwendig. Die Nutzer sollen sich nur mit einer Kennung für die zugelassenen Anwendungen anmelden kön-

nen. Der zentrale Verzeichnisdienst bestehe im Wesentlichen aus dem Active Directory von Microsoft. Dieses verwalte alle Nutzerkonten wie Kennungen, E-Mail-Adressen, Telefonnummern. Parallel dazu gäbe es VIVA. Dieses umfasse alle Personaldaten der staatlichen Beschäftigten. VIVA decke sich damit teilweise mit dem Active Directory.

Derzeit werde ein Abgleich dieser beiden Verzeichnisse geprüft.

Die noch ausstehende Beschaffung einer konkreten Software für das Identity Managementsystem hänge von bestimmten Funktionalitäten ab. Dabei würden die Kriterien der Wirtschaftlichkeit und Sparsamkeit berücksichtigt. Der Schwerpunkt liege derzeit auf der vordringlichen Ertüchtigung des Active Directory.

Elektronische Signatur:

Die Einführung der elektronischen Signatur, Verschlüsselung und Authentisierung setze eine Infrastrukturkomponente voraus, die digitale Ausweise in Form von software- und hardwarebasierten Zertifikaten ausstellen, verteilen und prüfen könne. Diese Komponente werde als Public Key Infrastructure (PKI) bezeichnet. Die von einer PKI ausgestellten Zertifikate würden zur Absicherung der computergestützten Kommunikation verwendet. Eine Wirtschaftlichkeitsbetrachtung habe ergeben, dass der Aufbau einer verwaltungseigenen PKI kostengünstiger sei als die Beschaffung von Zertifikaten über externe Anbieter.

Im Oktober 2005 sei eine neue bayerische Verwaltungs-PKI entwickelt worden. Diese sei bis auf eine Komponente, die derzeit getestet werde, seit Anfang 2007 in Betrieb. Diese neue Lösung habe bereits wenige Monate nach Inbetriebnahme vielfältige Anwendungsfelder für die Zertifikate erschlossen. Die Anzahl der Zertifikate sei seitdem stark gestiegen und habe im Februar 2009 mehr als 14.000 betragen.

Wegen der Bedeutung der Verwaltungs-PKI für die sichere Nutzung der Informations- und Kommunikationstechnik (IuK) sei die Darstellung ihrer Wirtschaftlichkeit nach der klassischen Kapitalwertmethode problematisch.

Anmerkung des ORH

Eine Verwaltungs-PKI und als deren Grundlage ein zentraler Verzeichnisdienst sind unabdingbare Infrastrukturanwendungen für eine sichere elektronische Kommunikation und Zusammenarbeit sowohl innerhalb der Verwaltung als auch mit der Öffentlichkeit.

Bei der Ausschreibung im Oktober 2005 ging die Verwaltung noch davon aus, dass die PKI anfänglich für 30.000 Mitarbeiter Zertifikate ausstellen und verwalten werde, langfristig dann für 100.000 Mitarbeiter. Der ORH kritisierte bereits damals die Annahme eines derartig flächendeckenden Bedarfs. Die nunmehr berichtete Anzahl aktuell ausgestellter Zertifikate von lediglich etwas über 14.000 bestätigt diese Bedenken. Hinzu kommt, dass ursprünglich allein für das Integrierte Haushalts- und Kassenverfahren (IHV) 20.000 Zertifikate erstellt werden sollten. Nunmehr werden für das IHV doch keine Zertifikate benötigt.

Der Aufbau des zentralen Verzeichnisdienstes geht zudem schleppend voran. Erschwert durch die Ressorthoheit müssen mühsam Probleme in der Implementierung des Verzeichnisdienstes Active Directory der Firma Microsoft beseitigt werden. Das bindet Ressourcen, die für den Aufbau des zentralen Verzeichnisdienstes fehlen.

Beschluss des Ausschusses für Staatshaushalt und Finanzfragen
vom 28. Mai 2009

Kenntnisnahme.

Dem Landtag ist bis 30.11.2011 zu berichten.

Stellungnahme des Staatsministeriums des Innern
vom 2. Januar 2012
(IZ4-1074.6-12)

Das Staatsministerium stellt die technischen Grundlagen und den aktuellen Sachstand dar.

Verwaltungs-PKI:

Der Einsatz einer Verwaltungs-PKI im Eigenbetrieb sei ein unverzichtbarer Bestandteil einer sicheren und modernen IuK-Technik.

Die 2005 im Rahmen einer europaweiten Ausschreibung beschaffte Lösung sei zunächst ohne die Komponente zur automatischen Verteilung der Zertifikate (Auto Enrollment) in Betrieb genommen worden. Dies sei zwischenzeitlich nachgeholt worden.

Die möglichen und bereits implementierten Anwendungsbereiche der PKI seien sehr vielfältig. Eine Reihe weiterer Anwendungen der PKI seien geplant.

Der erwartete Bedarf an Zertifikaten habe im Jahre 2006 bei 30.000 Zertifikaten gelegen. Im Oktober 2011 seien 29.500 Zertifikate im Einsatz gewesen.

Die Kosten für den Betrieb der PKI im Landesamt für Statistik und Datenverarbeitung seien bei der aktuellen Zahl der Zertifikate genauso hoch wie bei einem externen Bezug.

Zentraler Verzeichnisdienst:

Die Basiskomponente Zentraler Verzeichnisdienst (ZVD) diene der Integration dezentraler Verzeichnisse und hätte ursprünglich als ein zentrales, übergeordnetes Verzeichnis aufgebaut werden sollen.

Der ZVD sei auf Anregung der IT-Stabsstelle in ein technisches und in ein organisatorisches Verzeichnis aufgeteilt worden.

- Als *technisches Verzeichnis* komme das Active Directory zum Einsatz, das in größeren Microsoft-Umgebungen zwingend erforderlich sei. Der Betrieb der technischen Komponenten werde derzeit von den beiden Rechenzentren sukzessive übernommen.
- Der *organisatorische Verzeichnisdienst* (OVD) werde parallel dazu benötigt und sei insbesondere für Fachanwendungen relevant. Er solle zukünftig die organisationsrelevanten Daten aller staatlichen Mitarbeiter enthalten.

Das ursprünglich mit der Basiskomponente ZVD verbundene Ziel werde künftig mit dem technischen und dem organisatorischen Verzeichnisdienst erreicht.

Anmerkung des ORH

Verwaltungs-PKI:

Die dargestellten möglichen, tatsächlichen und geplanten Anwendungen sind vielfältig, jedoch beschränkt sich die bisherige Zahl der Zertifikate auf 29.500. Ob der Bedarf auf 100.000 steigen wird und die Investitionen gerechtfertigt waren, bleibt weiterhin offen.

Zentraler Verzeichnisdienst:

Ein zentraler Verzeichnisdienst ist unerlässlich für die Umsetzung der Ziele der IuK-Landesstrategie.

Die Aufteilung des ZVD in eine technische (Active Directory) und in eine organisatorische (OVD) Komponente liefert nur neue Wortschöpfungen.

Der OVD befindet sich seit Jahren in der Planung. Über eine konkrete Implementierung ist bislang nichts bekannt.

Als flächendeckend einheitliche technische Basis gibt es derzeit nur den Active Directory. Er ist das technische Fundament für die gesamte IuK-Landschaft der Staatsverwaltung.
Aufgrund vorhandener Prüfungserkenntnisse bestehen jedoch erhebliche Zweifel an seiner Stabilität und Sicherheit. Dies ist vor allem darauf zurückzuführen, dass sich die Betriebsverantwortung für die Domänenverwaltung derzeit nicht in einer Hand befindet, sondern sich auf zahlreiche einzelne Behörden erstreckt. Ein Totalzusammenbruch mit Auswirkungen auf nahezu alle PC-Arbeitsplätze in der Staatsverwaltung hätte fatale Folgen.

Das ursprüngliche Ziel des ZVD wurde nach 10 Jahren noch nicht erreicht.

Beschluss des Ausschusses für Staatshaushalt und Finanzfragen
vom 31. Januar 2012

Die Staatsregierung wird ersucht,

- die Stabilität und Sicherheit der technischen Verzeichnisdienste als technisches Fundament schnellstmöglich herbeizuführen. Dies erfordert insbesondere die Verlagerung der Betriebsverantwortung für die Domänenverwaltung ausschließlich in die Hand des federführenden RZ-Süd.
- ein schlüssiges Gesamtkonzept für das Zusammenwirken der unterschiedlichen Verzeichnis- und Zertifikatsdienste zu erstellen. Für die interne und externe Kommunikation sollte eine einheitliche Lösung unter Verwendung vorhandener Strukturen zum Einsatz kommen. Der Aufbau und Betrieb paralleler Systeme ist zu vermeiden.

  Dem Landtag ist bis 30.11.2012 zu berichten.

Stellungnahme des Staatsministeriums des Innern, für Bau und Verkehr
vom 10. Dezember 2013
(IZ4-0924-1-72-4)

Das Innenministerium berichtet, dass bei den Verzeichnis- und Zertifikatsdiensten in den letzten beiden Jahren wesentliche Fortschritte erzielt worden seien. Allerdings hätten sich aufgrund der Komplexität der Themenbereiche noch nicht alle Problemstellungen erledigen lassen.

Zertifikatsdienst:

Das Innenministerium erläutert die Ziele und Funktionsweise einer Publik-Key-Infrastruktur (PKI) im Allgemeinen, die Hintergründe für die Schaffung der Bayern-PKI sowie die Bedeutung sicherer Verschlüsselungsverfahren für die Datensicherheit. Die Bayerische Verwaltungs-PKI („Bayern-PKI“) sei nach Beschluss des Ministerrats als landeseigene PKI für verwaltungseigene Zwecke geschaffen worden. Sie sei universell einsetzbar und könne Zertifikate für Personen, Gruppen, Funktionen und Maschinen erstellen.

Die wichtigsten Anwendungsbereiche der PKI lägen in der E-Mail-Verschlüsselung, der Leitungsverschlüsselung im Bayerischen Behördennetz sowie der Authentifizierung an zentralen Portalen (z. B. Portal der Bayerischen Schulen, Härtefallkommission, Melderegister oder die sog. „Erreichbarkeitsplattform“).

Das Innenministerium berichtet von einer gestiegenen Nachfrage nach Zertifikaten, d. h. einem Zuwachs von über 80 % in zwei Jahren (von weniger als 30.000 auf über 54.000) sowie von einem Kostenvorteil des Eigenbetriebs gegenüber dem Bezug der Zertifikate durch einen Fremdanbieter. Es räumt ein, dass mit dem vom Finanzministerium entwickelten AUTHEGA neben der Bayern-PKI eine weitere PKI-Lösung existiere, die ebenfalls zur Produktion von Zertifikaten eingesetzt werde. Die Bayern-PKI und AUTHEGA seien für verschiedene Aufgabenstellungen entwickelt worden und unterschieden sich in der Art der Anwendung. Im Rahmen einer Machbarkeitsstudie seien die Möglichkeiten zur Zusammenführung der beiden Lösungen untersucht worden. Im Ergebnis habe eine echte Zusammenführung eine Reihe gravierender Nachteile, wie z. B. Migrations- und Anpassungsaufwände. Eine konkrete Quantifizierung dieser Aufwände liege jedoch bis-

her nicht vor.

Zentraler Verzeichnisdienst:

Das Innenministerium fasst die Unterscheidung zwischen einem technischen und einem organisatorischen Verzeichnisdienst zusammen.

Als technischer Verzeichnisdienst komme zwischenzeitlich das Active Directory (AD) flächendeckend zum Einsatz. Das zentrale ressortübergreifende AD („AD-Bündnis-Forest“) sei die Grundlage für das Funktionieren von über 5.700 Servern und über 65.000 Clients sowie über 100.000 Nutzer, die hierüber verwaltet würden. Daraus resultierten eine besondere Bedeutung dieses Verzeichnisdienstes sowie erhöhte Anforderungen an die Stabilität und Sicherheit. Ohne ein funktionierendes AD könnten sich die Nutzer nicht mehr am Arbeitsplatz-PC anmelden. Fehler bei der Administration eines der über 380 dezentralen Verzeichnisdienstservers („Domainencontroller“) wirkten sich nicht nur lokal aus; da sich die Domainencontroller laufend untereinander abglichen, könnten örtliche Fehler zu schweren Betriebsstörungen im gesamten Verbund führen. Um dieses Risiko zu vermindern, soll insbesondere die bisher dezentrale Betriebsverantwortung an ein zentrales Rechenzentrum verlagert werden. Dieser Prozess solle bis Mitte 2014 abgeschlossen sein. Bis dahin sollten sich sämtliche Domänen-Controller in zentraler Betriebsverantwortung befinden. Ein kürzlicher Test durch den Hersteller, der Firma Microsoft, habe aber schon jetzt einen ausgezeichneten Zustand ergeben.

Das Innenministerium weist schließlich darauf hin, dass als organisatorischer Verzeichnisdienst inzwischen der sog. „Behördenwegweiser“ benannt worden sei, einem Web-Angebot, welches die Bürger über die Behörden und deren Aufgaben informiere.

Anmerkung des ORH

Bei der Bayern-PKI und AUTHEGA handelt es sich um zwei PKI-Lösungen, die parallel und unabhängig voneinander entstanden sind. Auch wenn sie für verschiedene Aufgabenbereiche entwickelt wurden, decken sie dennoch stark überlappende Funktionalitäten ab. Dass die Zusammenführung parallel entwickelter Verfahren Auf-

wände verursacht, liegt in der Natur der Sache: Es wurden ähnliche Funktionalitäten realisiert, auf der Basis unterschiedlicher Plattformen und mit unterschiedlichen externen Dienstleistern.

Der favorisierte „Mischbetrieb“ bedeutet letztendlich, dass man die Parallelentwicklung als gegeben hinnimmt und die beiden Verfahren dauerhaft nebeneinander betreibt. Auf lange Sicht führt dies jedoch dazu, dass alle im Kontext solcher Systeme anfallenden Aufwände zweifach entstehen werden. Der ORH bezweifelt, dass dies langfristig sinnvoll und wirtschaftlich ist. Jedenfalls sollte die zentrale strategische Steuerung des IuK-Einsatzes durch das Finanzministerium künftig solche Parallelentwicklungen verhindern.

Der technische Verzeichnisdienst, das Active Directory, stellt eine Plattform für nahezu alle Einsatzgebiete der IuK in der Verwaltung dar. Daraus entstehen hohe Anforderungen an die Stabilität und Sicherheit, die sich nur erreichen lassen, wenn die Betriebsverantwortung komplett in zentraler Hand liegt. Dieses Ziel wurde bisher noch nicht vollständig erreicht. Das Staatsministerium stellt dies jedoch für Mitte 2014 in Aussicht. Dabei kommt es entscheidend darauf an, dass sich die zentrale Betriebsverantwortung wirklich auf das gesamte AD erstreckt, einschließlich der Domänen der nachgeordneten Behörden.

Beschluss des Ausschusses für Staatshaushalt und Finanzfragen
vom 11. Februar 2014

Die Staatsregierung wird gemäß Artikel 114 Absätze 3 und 4 der Bayerischen Haushaltsordnung ersucht,

- hinsichtlich des Zertifikatsdienstes eine Zusammenführung von Bayern-PKI und AUTHEGA zu prüfen und dabei auch langfristige Aufwände zu betrachten,
- hinsichtlich des Verzeichnisdienstes die zentrale Betriebsverantwortung wie angekündigt auch tatsächlich bei sämtlichen Teilen des Active Directory bis Mitte 2014 zu erreichen.

Dem Landtag ist bis 30.11.2014 abschließend zu berichten.

Stellungnahme des Staatsministeriums der Finanzen, für Landesentwicklung und Heimat
vom 4. Dezember 2014
(77/LB-C 0001-4/127)

Das nunmehr zuständige Finanzministerium teilt mit, dass die beiden staatlichen Registrierungs- und Authentifizierungsdienste „Bayern-PKI“ und „AUTHEGA“ unterschiedliche Zielsetzungen, Zielgruppen und Einsatzumgebungen hätten. Es handele sich nicht um konkurrierende, sondern um sich wechselseitig ergänzende Dienste, deren Zusammenführung aus fachlichen sowie wirtschaftlichen Gründen ausscheide.

Die Bayern-PKI diene zur Absicherung des staatlichen Handelns durch personalisierte Zertifikatsausstellung und Begrenzung der Zertifikate auf Verwaltungsmitarbeiter und Gerät (Server, Router) des Freistaates und der Kommunen. Bei AUTHEGA stehe dagegen die Nutzung der Zertifikate durch Bürger und Mitarbeiter an privaten Endgeräten im Vordergrund. Die AUTHEGA-Zertifikate ermöglichten einen generischen Dienst für unterschiedliche webbasierte Fachanwendungen und Portale im eGovernment wie etwa derzeit Mitarbeiter-Mitteilungs-Service, Kurtaxverfahren der Staatsbäder, Bürgerzugang zur Erreichbarkeitsplattform zum Einheitlichen Ansprechpartner.

Die Weiterentwicklung eines der beiden Dienste, um die Aufgaben des jeweils anderen Systems erfüllen zu können, sei nur unter sehr hohem Entwicklungsaufwand und unter Missachtung der für die jeweiligen Systeme gültigen Rahmenbedingungen möglich.

Zur zentralen Betriebsverantwortung des Active Directory berichtet das Finanzministerium von der Prüfung durch den ORH, der sich im Herbst 2014 abschließend erfreut über die erreichten Fortschritte bei der betrieblichen Konsolidierung geäußert habe. Das IT-Dienstleistungszentrum (ehemals Rechenzentrum Süd) rechne mit dem Abschluss dieser Arbeiten im ersten Quartal 2015.

Anmerkung des ORH

Die Staatsregierung hat die beiden Aufträge aus dem letzten Beschluss des Ausschusses für Staatshaushalt und Finanzfragen vom 11.02.2014 umgesetzt. Sie hat geprüft, ob eine Zusammenführung der beiden Zertifikatsdienste von Bayern-PKI und AUTHEGA möglich und wirtschaftlich ist und diese Fragen verneint. Die Begründungen erscheinen plausibel. Während die Bayern-PKI die

IT-Sicherheit im „Innern“ des staatlichen IT-Betriebs - also innerhalb des bayerischen Behördennetzes - erhöht, zielt AUTHEGA auf die Absicherung von Kommunikationsbeziehungen nach außen: eGovernment-Angebote für Bürger und Unternehmen können damit sicherer im Internet offeriert werden. Ob sich die Parallelität der beiden Zertifikatsdienste hätte vermeiden lassen, wenn die Verwaltung diese beiden Anwendungsbereiche schon bei der anfänglichen Konzeption eines Zertifikatssystems berücksichtigt hätte, kann dahinstehen.

Hinsichtlich der Konsolidierung der Betriebsverantwortung beim Active Directory kann der ORH aufgrund seiner Prüfung wesentliche Fortschritte bestätigen. Die Staatsregierung hat den Abschluss der Arbeit für das erste Quartal 2015 in Aussicht gestellt.

Beschluss des Ausschusses für Staatshaushalt und Finanzfragen
vom 4. März 2015

Kenntnisnahme.