Haushalten) zu 6,2% aus kurzfristigen, zu 28,2% aus mittelfristigen und zu 65,5% aus langfristigen Mitteln zusammen. Letztere haben sich im Berichtsjahr von 761,7 Millionen Euro auf 1102,8 Millionen Euro und die mittelfristigen Kredite von 369,5 Millionen Euro auf 475,0 Millionen Euro erhöht. Kurzfristige Kredite wurden vom Freistaat erstmals wieder seit Ende 1998 nachgefragt.

Im Jahr 2001 tilgte der Freistaat 1503,0 Millionen Euro Schulden, 13,2 Millionen Euro (0,9%) weniger als im Jahr davor. Von den Rückzahlungen wurden 80,0% oder 1202,5 Millionen Euro zur Tilgung von direkten Darlehen, 16,8% oder 253,1 Millionen Euro zum Abbau von Wertpapierschulden in Form von Landesobligationen und Landesschatzanweisungen und 47,4 Millionen Euro zur Verminderung der Schulden beim Bund verwendet. Die Schuldentilgungen beim Bund waren um 51,7 Millionen Euro niedriger als im Vorjahr.

Neben den aufgenommenen Krediten und Schuldentilgungen beeinflussen sonstige Schuldenzu- und Schuldenabgänge, die dem Staat weder Haushaltsmittel zuführen noch entziehen, die Höhe der Nettoneuverschuldung. Im Bereich der Kreditmarktverschuldung hielten sich die sonstigen Schuldenzu- und -abgänge mit jeweils 102,7 Millionen Euro die Waage. Bei diesen Posten handelte es sich lediglich um Umbuchungen von Abtretungen. Die bereits bestehenden Schuldscheindarlehen wurden auf diesem Weg buchmäßig von den bisherigen Kreditgebern auf die neuen Gläubiger übertragen, an der Verschuldungshöhe des Freistaats veränderte sich dadurch nichts. Im Bereich der Schulden bei öffentlichen Haushalten ergab sich jedoch eine Verschuldungsminderung. Bei den vom Bund für den Wohnungsbau bereitgestellten Mitteln verbuchte der Freistaat 53,3 Millionen Euro sonstige Schuldenabgänge. Dieser Betrag setzt sich zusammen aus rund 2 Millionen Euro Bundesanteil aus Rückflußausfällen bei Wohnungsbaudarlehen und aus Umwandlungen von Darlehen für den Wohnungsbau in Zuschüsse in Höhe von 51,3 Millionen Euro. 2000 lagen diese Zuschüsse bei 35,5 Millionen Euro.

Zinsaufwand weiter gesunken

Für die aufgenommenen Kredite hatte der Freistaat im Jahr 2001 973,4 Millionen Euro Zinsen zu leisten. Nachdem 1996 die Zinsaufwendungen mit 925,0 Millionen Euro auf den niedrigsten Stand seit 1984 abgebaut werden konnten, stiegen sie bis Ende 1998 auf 1063,7 Millionen Euro. 1999 sind die Aufwendungen für Zinsen geringfügig um 2,3 Millionen Euro, im Jahr 2000 um 41,5 Millionen Euro und im Berichtszeitraum um 4,6% oder um weitere 46,5 Millionen Euro gesunken. Der gesamte Schuldendienst (Tilgungen einschließlich Zinsen) belief sich 2001 auf 2476,4 Millionen Euro und war damit um 59,8 Millionen Euro niedriger als im Vorjahr. Gemessen an der fundierten Verschuldung zum 31. 12. 2000 in Höhe von 20303,0 Millionen Euro betrug 2001 der Schuldendienst unverändert 12,2%.

Dipl.-Volksw. Helmut Zaska

---

1) Artikel 104c Absatz 2 des Vertrages zur Gründung der Europäischen Gemeinschaft.
2) Falls die Wertpapierschulden unverzinsliche Schatzanweisungen oder Finanzierungsschätze enthalten, ist noch die Differenz zwischen ihren Nominalwerten und ihren abgezinsten Werten zu berücksichtigen. In der Schuldenstatistik werden diese Wertpapiere nur mit dem abgezinsten Betrag erfaßt. Nach dem Maastricht-Vertrag sind entsprechend dem Europäischen System Volkswirtschaftlicher Gesamtrechnungen alle Schulden zum Nominalwert nachzuweisen.
3) Kreditmarktschulden hier immer einschließlich der Vorkriegsauslandsschulden in Höhe von 689576,80 Euro.
4) Saldo aus Schuldenaufnahmen, Tilgungen und sonstigen Schuldenzu- und -abgängen.
5) Bei allen Verschuldungszahlen je Einwohner wurde der jeweilige Schuldenstand zum 31. Dezember auf die Bevölkerungszahlen vom 30. Juni bezogen.
6) Sondervermögen gemäß Artikel 81 der Verfassung des Freistaats.

Public Key Infrastruktur im Freistaat Bayern

An dieser Stelle wurde bereits in einer früheren Ausgabe (vgl. „E-Mail-Sicherheit im Bayerischen Behördennetz“, Bayern in Zahlen 7/1999) über die Sicherheitsanforderungen im Behördennetz, die Struktur und Aufgaben einer Public Key Infrastruktur (PKI), sowie die laufenden Pilotversuche berichtet.

Dieser Artikel informiert über den aktuellen Stand der PKI, die das Landesamt für Statistik und Datenverarbeitung für die staatlichen und kommunalen Behörden im Freistaat Bayern aufgebaut hat.

Die Kommunikation in offenen und damit unsicheren Netzen erfordert gewisse Sicherheitsmaßnahmen, die sich aus den 4 Grundanforderungen

- Authentizität
- Nicht-Abstreitbarkeit
- Nachrichtenintegrität
- Vertraulichkeit

ergeben:

Authentizität bedeutet die sichere Bestimmung des Ursprungs einer Nachricht. Der Ursprung kann z.B. eine Person, Institution oder auch ein Rechner sein. Das Versenden von Nachrichten unter falschem Namen kann dadurch aufgedeckt werden.

Nicht-Abstreitbarkeit des Ursprungs unterbindet die Möglichkeit, daß der Absender seine Urheberschaft an einer Nachricht abstreiten kann.

Nachrichtenintegrität bezeichnet die Unversehrtheit oder Echtheit der Nachricht. Es muß sichergestellt werden, daß der Empfänger informiert ist, wenn die Nachricht auf dem Übertragungsweg verändert wurde.

Vertraulichkeit heißt, daß unberechtigte Dritte die

Nachricht nicht einsehen können. Dies kann sich auf den bloßen Übertragungsweg beschränken, kann aber beim Versand von E-Mail bis zur sicheren Aufbewahrung im Postkorb des Empfängers ausgebaut werden (Ende-zu-Ende-Sicherheit).

Die ersten drei Sicherheitsanforderungen können durch digitale Signatur (elektronische Unterschrift) erfüllt werden, für die Forderung nach Vertraulichkeit ist Verschlüsselung notwendig. In Abhängigkeit von den technischen Verfahren sind unterschiedliche Ansätze (vgl. Schaubild 1) zur Realisierung der Sicherheitsanforderungen möglich:

Der **Sichere Kanal** dient zur Absicherung von Transaktionen und wird vorwiegend im Bereich WebServer und Webbrowser eingesetzt. Das bekannteste Sicherungsverfahren in diesem Bereich ist das Protokoll SSL, das nahezu bei allen Angeboten und Formularen im Web, bei denen persönliche Daten (z.B. Personalien, Kreditkartennummern) über das Internet gehen, eingesetzt wird.

Der **Sichere Transport** wird vor allem zur Absicherung von elektronischen Nachrichten (E-Mails) eingesetzt. Das zugrundeliegende Verfahren garantiert dabei eine echte Ende-zu-Ende-Sicherheit.

Der **Sichere Container** ist ähnlich wie der Sichere Transport, dabei aber unabhängig vom Transportweg bzw. Transportprotokoll. Das Verfahren wird eingesetzt, um Datenträger, z.B. Festplatten von Laptops gegen fremde Zugriffe zu schützen.

Alle drei Ansätze basieren auf kryptographischen Verfahren, die elektronische Ausweise, sogenannte Zertifikate, zur Identifikation der Nutzer und zur Definition der Vertrauensstellung einsetzen. Die logische und organisatorische Struktur einer PKI definiert dabei die Regeln zur Beantragung und Verwaltung der Zertifikate. Im Rahmen der eingesetzten Software werden die technischen Prozesse festgelegt, die für die Erzeugung und Verteilung der Zertifikate verantwortlich sind.

Ein kurzer Rückblick:

Im Rahmen des Projektes *Bayerische Sicherheitslösung für Dienste in offenen Kommunikationsnetzen (BASILIKA)* wurden bereits im Jahr 1996 die ersten Untersuchungen und Vorstudien zum Thema Sicherheit vorgenommen. Im Herbst 1997 erfolgten dann die ersten Tests und Pilotversuche. Zum Einsatz kamen (Zusatz-)Produkte europäischer Hersteller, da nach der damaligen US-amerikanischen Rechtslage kryptographische Software-Produkte mit starken Verschlüsselungstechniken nicht exportiert werden durften.

Die Ergebnisse bei einer größeren Anzahl von Benutzern zeigten allerdings, daß die Produkte in technischer Hinsicht (Installation, Stabilität, Bedienkomfort) noch nicht ausgereift waren. Ferner wurde deutlich, daß vor einer flächendeckenden Einführung eine Vielzahl von organisatorischen Regelungen einschließlich einer Sicherheitsrichtlinie zu erstellen und unter den Beteiligten abzustimmen war. Eine flächendeckende Einführung konnte deshalb zum damaligen Zeitpunkt nicht verantwortet werden.

Mit dem Wegfall der Export-Einschränkung seitens der USA war Ende 1999 der Zeitpunkt für eine Neuorientierung gekommen, da nun auch die aktuellen kryptographischen Produkte der Firma Microsoft bei der Auswahl und der Durchführung der Tests berücksichtigt werden konnten.

Aufgrund der Ergebnisse einer Machbarkeitsstudie zum Einsatz von Produkten der Fa. Microsoft im Bereich der PKI und der Sicheren E-Mail und der Verabschiedung des Rahmenkonzeptes zur Einführung von Windows 2000 und Active Directory in der staatlichen Verwaltung wurde im September 2000 folgender Auftrag definiert:

Realisierung einer PKI für die Abwicklung sicherer E-Mail in der öffentlichen Verwaltung in Bayern mit modernen Standardkomponenten

In einem ersten Schritt wurde zunächst die aktuelle Ausgangslage analysiert:

- Die staatlichen Behörden umfassen ca. 2200 Dienststellen mit ca. 190000 Mitarbeitern, rund die Hälfte dieser Behörden ist am Bayerischen Behördennetz (BYBN) angeschlossen.
- Es ist bei einer flächendeckenden Ausstattung von ei-

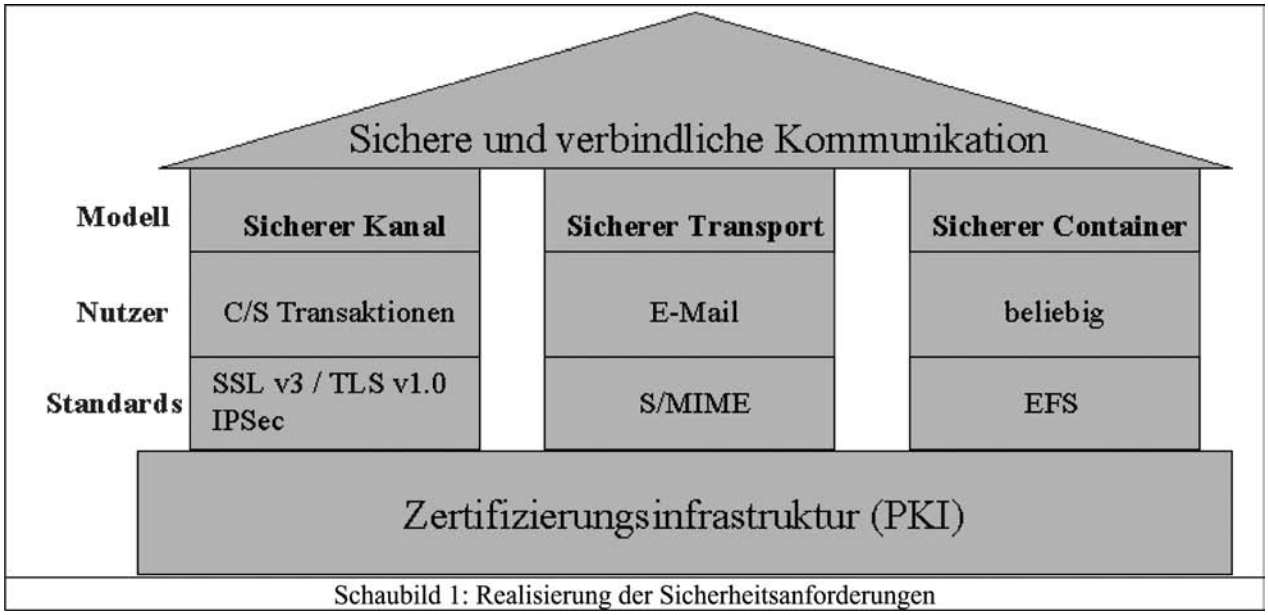

Schaubild 1: Realisierung der Sicherheitsanforderungen

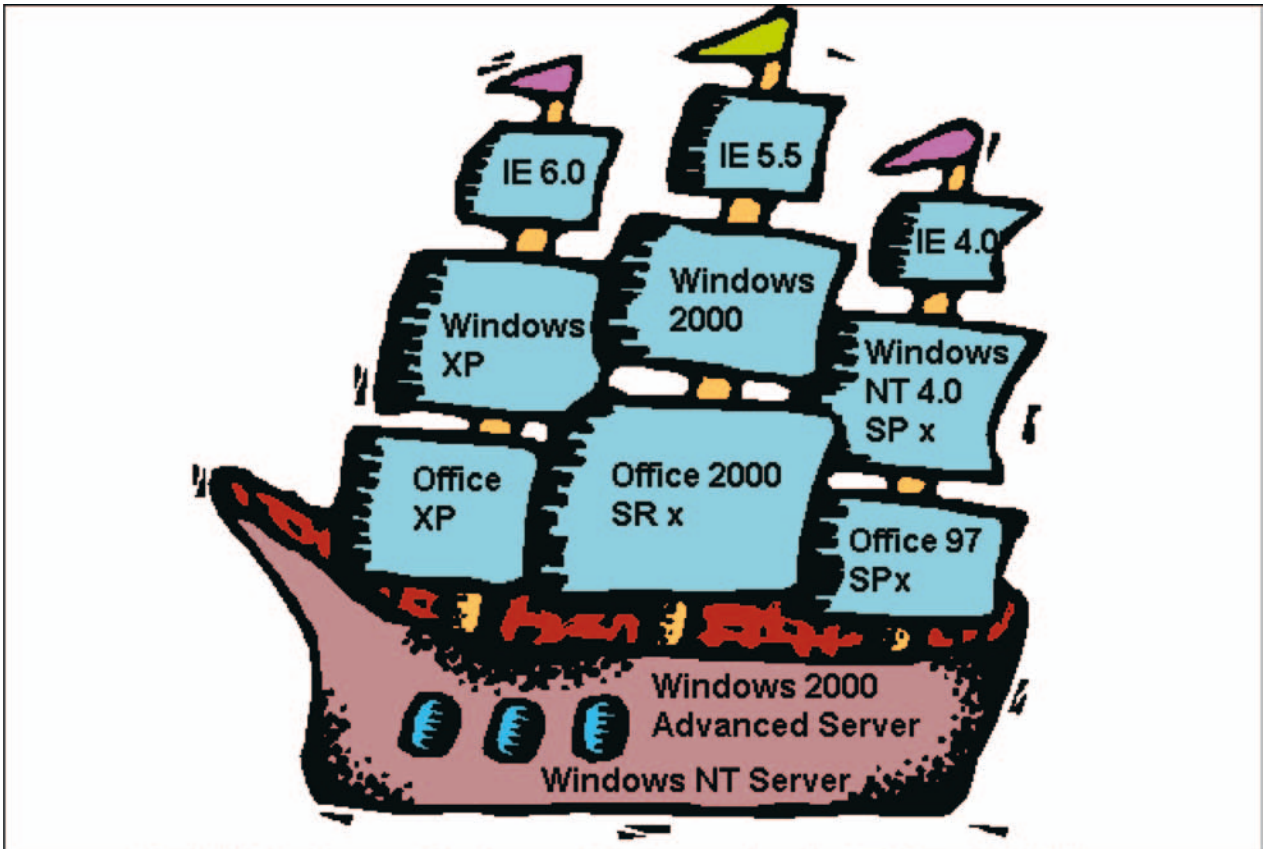

Schaubild 2: Spektrum an Plattformen und Softwareversionen im Umfeld von MS-Windows

nem Bedarf von ca. 60 000 Zertifikaten auszugehen. Die Mitarbeiter besitzen dabei unterschiedliches Know-How und sind unterschiedlichen Komfort in Bezug auf die Bedienung der Software gewohnt.

- Die in den Behörden eingesetzten Plattformen und Softwareversionen sind sehr heterogen und umfassen allein in der Windows Welt ein breites Spektrum (Schaubild 2). Ferner wird in den Behörden unterschiedliche Zusatzsoftware (z.B. FaxServer in Kombination mit dem E-Mail-System) eingesetzt.
- Die Umstellung der einzelnen Geschäftsbereiche (Ministerien mit ihren nachgeordneten Behörden) auf das Betriebssystem Windows 2000 und damit der Beitritt zum Windows 2000-Verbund der Bayerischen Verwaltung (Bündnis-Forest) erstreckt sich auf einen langen, mehrjährigen Zeitraum.
- Die einzelnen Geschäftsbereiche verfolgen unterschiedliche Sicherheitsphilosophien (z.B. Abschottung des Netzes des Geschäftsbereiches gegenüber dem Bayerischen Behördennetz).

In enger Zusammenarbeit mit den Geschäftsbereichen wurden daraufhin konkrete Ziele für die Realisierung definiert und Rahmenbedingungen für den künftigen Einsatz festgelegt:

Für die Erstellung der Zertifikate kommt eine gemeinsame Hierarchie von Zertifizierungsstellen zum Einsatz (Schaubild 3), die von allen Teilnehmern des Bündnis-Forest genutzt werden soll. Die zentralen Komponenten hierfür sowie die Kapazitäten zur Administration stellt das Landesamt für Statistik und Datenverarbeitung den Teilnehmern der PKI kostenfrei zur Verfügung. Selbstverständlich kann die Dienstleistung der Zertifizierungsstellen auch von anderen Behörden innerhalb und außerhalb des BYBN in Anspruch genommen werden.

Ferner muss die bayerische PKI so aufgebaut werden, daß sie sich in gerade entstehende länderübergreifende Verwaltungsstrukturen (Verwaltungs-PKI) einbinden läßt. Nur so ist eine sichere Kommunikation auch mit Bundesbehörden und den Dienststellen anderer Bundesländer dauerhaft möglich.

Schließlich muß die Nutzung der sicheren E-Mail (insbesondere die Verteilung, Verwaltung und Prüfung der Zertifikate) weitgehend automatisiert werden, so daß im Regelfall der Nutzer nur je einen Knopf für die Verschlüsselung und die elektronische Signatur betätigen muß.

In einer Zwischenphase wurden dann die erforderlichen Schritte grob geplant und in einen technischen und organisatorischen Bereich unterteilt (Schaubild 4).

Technische Komponenten

In Zusammenarbeit mit den Beratern der Firma Microsoft wurden die technischen Fragen in bezug auf die PKI untersucht. Im Vordergrund standen dabei folgende Kernfragen:

- Welche Komponenten können/müssen zentral für alle Behörden zur Verfügung gestellt werden?

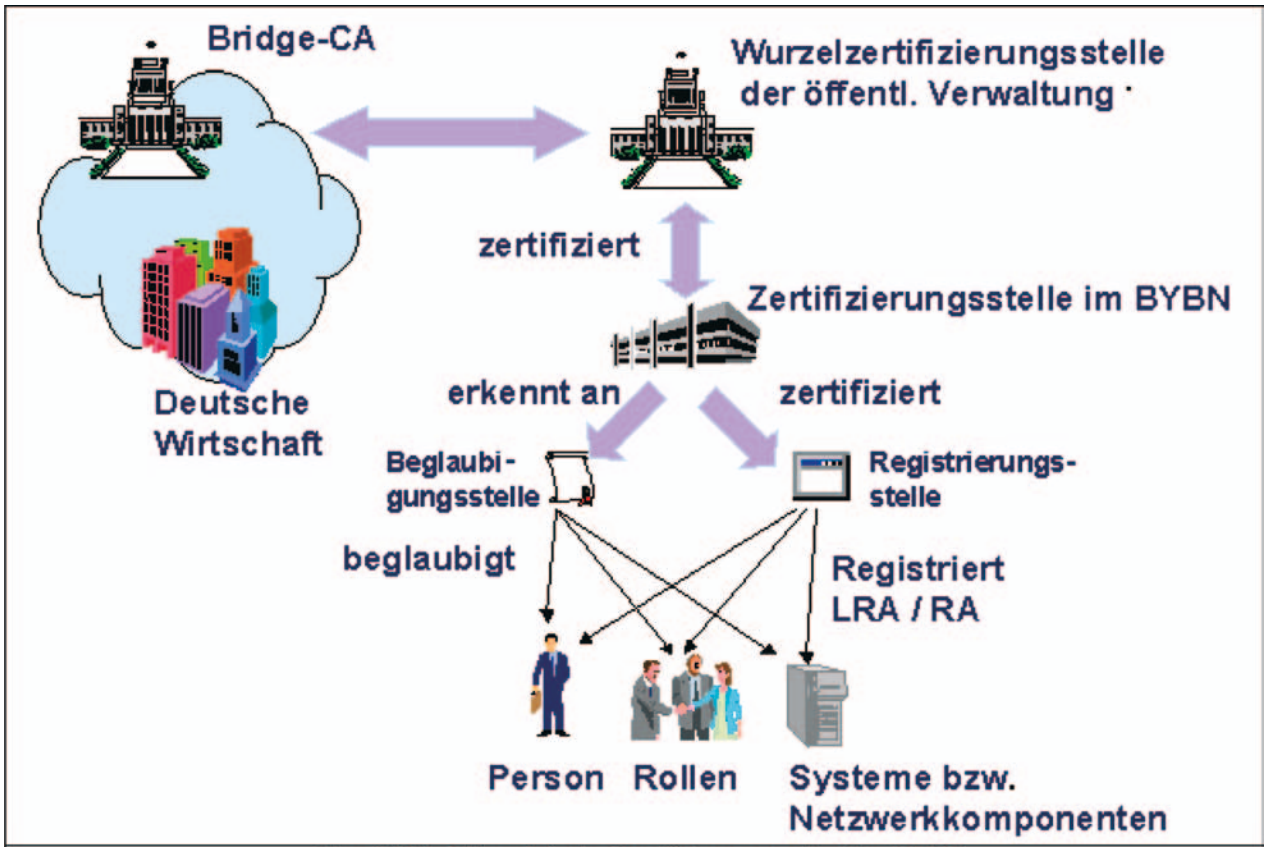

Schaubild 3: Hierarchie der Zertifizierungsstellen im BYBN

- Wie können sich die Komponenten in die bisherige Architektur des Bayerischen Behördennetzes einfügen?
- Welche Hard- und Software ist für den Betrieb der PKI erforderlich?

Gleichzeitig wurden die Vorgaben für die Arbeitsplätze definiert, an denen die PKI künftig eingesetzt werden soll. Dazu wurde festgelegt, die bereits in Microsoft Outlook 2000 bzw. Microsoft Outlook XP implementierte Funktionalität für Sichere E-Mail zu nutzen und auf Produkte von Drittherstellern zu verzichten. Die Arbeitsplätze sollten so konfiguriert werden, daß die erforderlichen Funktionen zur Verschlüsselung und Signatur, sowie zur Verwaltung der Zertifikate automatisch und zuverlässig ablaufen können. Da in der staatlichen Verwaltung zum damaligen Zeitpunkt Microsoft Outlook 97 das am häufigsten eingesetzte E-Mail-Produkt war, wurde ferner eine Installations- und Konfigurationsroutine für den Update auf Microsoft Outlook 2000 erstellt. Diese erleichtert die Einführung der sicheren E-Mail in den einzelnen Geschäftsbereichen und ist auch für die Installation im Rahmen von Systemen zur Softwareverteilung geeignet.

Ausführliche Tests der zentral zu betreibenden Komponenten sowie der E-Mail-Clients in unserem Testlabor folgten. Dabei mußten zahlreiche technische Probleme, einschließlich fehlerhafter Software, gelöst werden. Bei der Auswahl der Testszenarien wurde Wert auf eine praxisnahe Nachbildung der Rahmenbedingungen des Bayerischen Behördennetzes und der entstehenden länderübergreifenden Strukturen gelegt.

Organisationsmodell

Parallel zur technischen Realisierung wurden die organisatorischen Aufgaben in Angriff genommen.

Mit der Formulierung einer Sicherheitsrichtlinie (Policy) wurde die Struktur und das Sicherheitsniveau der PKI festgelegt:

- Definition der Teilnehmer an der PKI (u.a. Zertifizierungsstellen, Nutzer)
- Definition der erforderlichen Geschäftsprozesse zur Verwaltung von Zertifikaten
- Festlegung technischer Rahmenbedingungen (z.B. Schlüssellängen, Zertifikatsformate)
- Regeln zur Vergabe der Namen

Zur praktischen Umsetzung der Sicherheitsrichtlinie wurde ein Konzept erstellt, das die Einrichtung von Registrierungs- und Beglaubigungsstellen[1)] in den einzelnen Behörden vorsieht. Entsprechend der festgelegten Geschäftsprozesse sollen die Anträge von Mitarbeitern entgegengenommen, deren Identität geprüft und die für die Ausfertigung von Zertifikaten erforderlichen Informationen auf vertraulichem Wege an die Zertifizierungsstelle übermittelt werden.

Länderübergreifende Strukturen (Verwaltungs-PKI)

Noch während der technischen Realisierung und der Erarbeitung des Organisationsmodelles zeigte sich, daß auch beim Bund und in anderen Bundesländern ähnliche Anstrengungen unternommen wurden. Da auch die vielfältigen Kommunikationsbeziehungen zwischen den

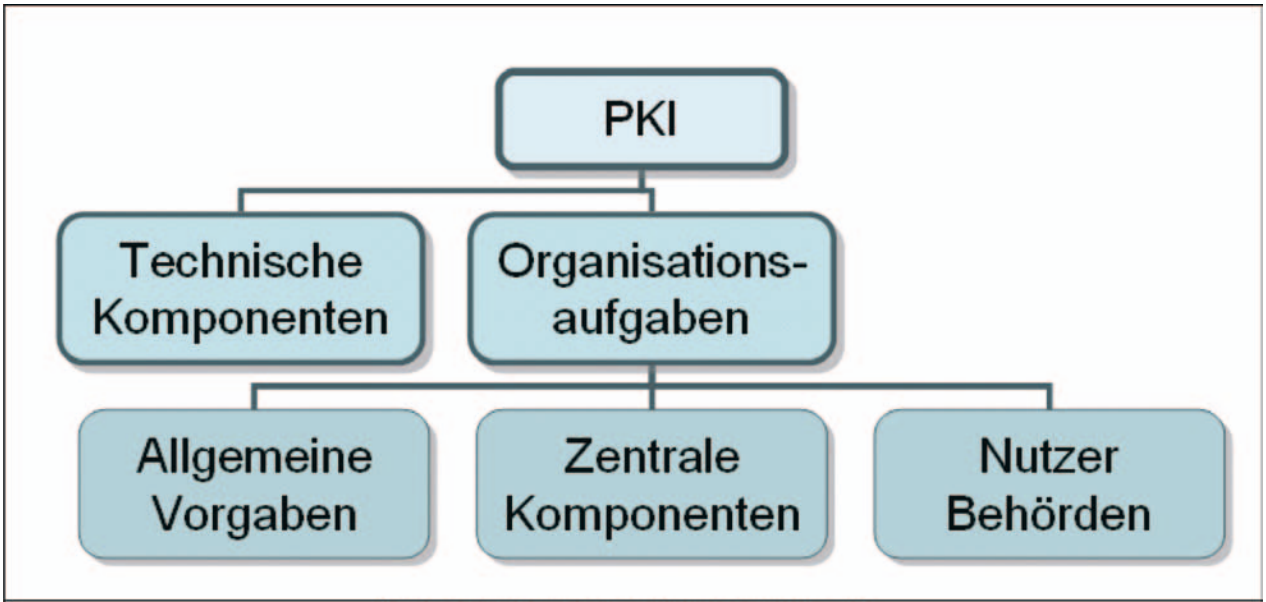

Schaubild 4: Schritte zur Realisierung der PKI

Ländern und dem Bund den eingangs beschriebenen Grundanforderungen genügen müssen, wurde eine Zusammenfassung und Standardisierung der einzelnen PKIen beschlossen. Die Wurzel dieser PKI wird vom Bundesamt für Sicherheit in der Informationstechnik im Auftrag des Bundesinnenministeriums betrieben und ersetzt bilaterale, technische und organisatorische Absprachen zwischen den Ländern und dem Bund. Die bayerische PKI ist dieser Verwaltungs-PKI im Juli 2001 als erstes Bundesland beigetreten und hat damit seine Rolle als Vorreiter im Bereich der PKI unter Beweis gestellt.

Konzept zur Nutzung der elektronischen Signatur in der Verwaltung

Im Auftrag der Staatsregierung wurde im Frühjahr 2002 ein Konzept zur Nutzung der elektronischen Signatur in der bayerischen Verwaltung erstellt. Darin ist vorgesehen, die bayerische staatliche Verwaltung bis zum Jahr 2005 flächendeckend mit Zertifikaten und den erforderlichen Sicherheitskomponenten auszurüsten, um eine gesicherte und vertrauliche Kommunikation zwischen den einzelnen Behörden zu ermöglichen.

Für die Kommunikation des Bürgers mit der Verwaltung sollen im Bereich der Erstellung elektronischer Bescheide gemäß dem deutschen Signaturgesetz qualifizierte Zertifikate zum Einsatz kommen.

Aktueller Stand

Derzeit ist in den einzelnen Behörden die Installation der E-Mail-Clients und die Verteilung der Zertifikate in vollem Gange. Im Landesamt für Statistik und Datenverarbeitung wurden bisher zwei Abteilungen (150 Mitarbeiter) mit den Komponenten zur sicheren E-Mail ausgerüstet. In den Ministerien und der Staatskanzlei erfolgte die Ausstattung von Mitarbeitern im Bereich Ministerratsangelegenheiten, so daß derzeit insgesamt ca. 500 Zertifikate im Einsatz sind.

Parallel zur Einführung von MS-Exchange 2000 als aktuellem Server für den E-Mail-Verkehr wurde ein Konzept zur Nutzung des Schlüssel- und Zertifikatsverwaltungsserver (KMS 2000) als Komponente des MS-Exchange 2000 erstellt. Dadurch ist eine sichere und weitgehend automatisierte Verteilung von Zertifikaten an die Inhaber eines Postfaches möglich. Noch im Januar 2003 wird im Staatsministerium der Finanzen der erste KMS 2000 seinen Betrieb aufnehmen und dort die flächendeckende Einführung der Sicheren E-Mail unterstützen.

Künftige Entwicklungen

Auch für das Jahr 2003 sind zahlreiche Aktivitäten im Umfeld der bayerischen PKI geplant:

- Für das Frühjahr 2003 ist von der Fa. Microsoft die Nachfolgeversion von Windows 2000 Server unter dem Namen .NET angekündigt. In ihr werden neue und verbesserte Funktionen für den praktischen Betrieb der PKI enthalten sein. Untersuchungen im Landesamt für Statistik und Datenverarbeitung sollen den Einsatz dieser Nachfolgeversion vorbereiten und die Einführung in den Behörden begleiten.
- Neben der Standardmethode zur Speicherung von Zertifikaten und Schlüssel auf der Festplatte des PCs wird von einzelnen Behörden vermehrt der Einsatz von Chipkarten gefordert. Auch hier sollen detaillierte Untersuchungen einen flächendeckenden Einsatz entsprechend der vorgegebenen Rahmenbedingungen vorbereiten.
- Neben Produkten der Fa. Microsoft werden in einigen Bereichen der Staatsverwaltung auch die E-Mail-Clients anderer Hersteller eingesetzt. Ziel wird es sein, auch diese Produkte in die PKI einzubinden und so für den Einsatz sicherer E-Mail vorzubereiten. Hauptaugenmerk wird dabei auch auf Produkten aus dem Bereich der Open-Source-Systeme (OSS) liegen, welche das individuelle Anpassen der Programme erlauben und deren Einsatz lizenzkostenfrei ist.
- Entsprechend den eingangs vorgestellten Ansatzpunkten sollen die Einsatzmöglichkeiten der von der PKI verwalteten Zertifikate ausgeweitet werden. Vorrangig ist hier der Bereich Sichere Transaktionen zu

nennen, der in vielen webbasierenden Verfahren der Verwaltung zum Einsatz kommen wird.

Im Hinblick auf die Problematik mit Viren und aktiven Inhalten (Makros in Dokumenten und Formularen) wird aber auch die Signatur von ausführbaren Programmen und Skripten (CodeSignatur) einen wichtigen Einsatzbereich der PKI darstellen. Nur so kann die Unversehrtheit und Herkunft des auszuführenden Programmes zweifelsfrei festgestellt werden. Die technische Plattform zur Realisierung dieser Anforderungen wird das Arbeitsplatz-Betriebssystem Windows XP bilden, das automatische Prüfungen in diesem Bereich anbietet. Windows XP steht kurz vor der Einführung in der bayerischen Verwaltung.

Dipl.-Informatiker (Univ.) Rudolf Zenkert

---

[1] Während Beglaubigungsstellen auf dem Antrag die Identität des Mitarbeiters bestätigen und ihn anschließend per Post an die Zertifizierungsstelle senden, nutzen Registrierungsstellen ein Programm zur elektronischen Übermittlung der erforderlichen Informationen.

Glossar

Active Directory	Im Rahmen von Windows 2000 eingesetztes Verzeichnis für den automatisierten Abruf von Systeminformationen (Benutzer, Rechte, Konfigurationen)
Bridge-CA	Initiative der Deutschen Bank und der Dt. Telekom zur gegenseitigen Anerkennung von PKI-Strukturen / Zertifikaten ohne explizite Cross-Zertifizierung.
BS	*Beglaubigungsstelle,* Stelle (i.d.R. die Personalstelle oder kleinere Dienststellen), die den Antrag eines Teilnehmers auf ein Zertifikat entgegennimmt, vor Ort die Identität des Teilnehmers feststellt und den Wunsch auf Schlüsselerzeugung und Zertifizierung an die Endstellen-CA weiterleitet.
BYBN	*Bayerisches Behördennetz,* geschlossenes Netz auf TCP/IP-Basis für die staatlichen und kommunalen Behörden Bayerns
CA	*Certification Authority*, Zertifizierungsinstanz, Zertifizierungsstelle. Stellt Zertifikate (sichere Zuordnung von öffentlichem Schlüssel und Teilnehmer) aus.
Bündnis Forest	Domänen-Konzept für den Einsatz von Windows 2000 im Bereich des BYBN
EFS	*Enrcypted File System,* Methode zur Online-Verschlüsselung von Datenträgern, insbesondere Festplatten
FaxServer	Komponente zum Versand und Empfang von Fax über das E-Mail-System
IE	*Internet Explorer*, Browser der Fa. Microsoft zur Darstellung von Informationen aus dem Internet
IP	*Internet Protocol*, Protokoll zur Datenübertragung im Inter- und Intranet. (Ebene 3 des OSI-Schichtenmodells)
IPSec	Ein von der *IP Security* Working Group der Internet Engineering Task Force (IETF) für IPv4 und IPv6 spezifiziertes einheitliches IP Security Protokoll.
KMS	*Key management Server,* Komponente des E-Mail-Servers Exchange der Fa. Microsoft zur automatisierten Verteilung von Schlüsseln und Zertifikaten an die Inhaber eines Postfaches
LRA	*Local Registration Authority*, Stelle, die den Antrag eines Teilnehmers auf ein Zertifikat entgegennimmt, vor Ort die Identität des Teilnehmers feststellt und im Gegensatz zur RA lokal Schlüssel erzeugt.
PKI	*Public Key Infrastruktur*, organisatorische und technische Einheit, deren Teilnehmer von einer gemeinsamen CA zertifiziert werden.
RA	*Registration Authority*, Stelle, die den Antrag eines Teilnehmers auf ein Zertifikat entgegennimmt, vor Ort die Identität des Teilnehmers feststellt und den Wunsch auf Schlüsselerzeugung und Zertifizierung an die CA weiterleitet.
S/MIME	*Secure Multipurpose Internet Mail Extension*, standardisierte Security-Hülle für E-Mails mit Anhängen (Attachments).
SSL	*Secure Socket Layer,* von der Firma Netscape entwickeltes Protokoll zur Transportsicherung einer Client-Server-Kommunikation (Ebene 3 des OSI-Schichtenmodells)
TCP	*Transmission Control Protocol,* Protokoll zur Datenübertragung im Inter- und Intranet. (Ebene 4 des OSI-Schichtenmodells)
TLS	*Transport Layer Security,* im Entstehen begriffener Internet-Standard mit denselben Funktionalitäten wie SSL.
Trustcenter	Sammelbegriff für mehrere technische CAs (Root-CA und untergeordnete CAs), die sich unter einer organisatorischen Einheit (z.B. BYBN) befinden.