Sicherheitsaspekte im X.500 und im Projekt AMBIX

Vortrag für den Workshop
„Sicherheit in vernetzten Systemen“
am 4. und 5. März 1997 in Hamburg

Karl-Peter Gietz, DFN-Projekt AMBIX,
Zentrum für Datenverarbeitung, Universität Tübingen

Inhaltsverzeichnis

1 Security im X.500

1.1 Einführung in X.500

Das X.500-Verzeichnis ist eine von internationalen Standardisierungsgremien genormte weltweit verteilte und weltweit zugängliche Datenbank. Es hat bisher zwei Versionen dieses Standards gegeben, nach dem Erscheinungsjahren 88er bzw. 93er Standard genannt. Ein 97er Standard ist in der Planungsphase. Der folgendende Vortrag bezieht sich, soweit nicht anders angegeben, auf den aktuellen, den 93er Standard.

1.1.1 Aufbau und Struktur

X.500 hat ein Client/Server-Konzept. Die Daten werden von Servern, sogenannten *Directory System Agents* (DSAs), lokal vorgehalten und verwaltet. Mit *Directory User Agents* (DUAs) können über eigene Protokolle Daten gesucht, angezeigt, aber auch verändert und gelöscht werden. Mittlerweile wird eines der DUA-DSA-Protokolle, das *Lightweight Directory Access Protokoll* (LDAP) von allen wichtigen Softwareproduzenten in die WWW-Browser als Schnittstelle zu Directory-Informationen eingebaut.

Alle DSAs innerhalb des X.500-Verzeichnisses sind für einen festgelegten Bereich im hierarchischen *Directory Information Tree* (DIT) zuständig und kommunzieren miteinander über spezielle Protokolle. Ein DIT-Bereich hat also einen sog. Master-DSA, kann aber von beliebig vielen weiteren DSAs als Kopie vorgehalten werden. Ein solches mirroring wird Replikation genannt. Unabhängig von der Replikation können von jedem DSA aus die Daten der anderen DSAs abgefragt werden.

Der DIT ist somit eine virtuelle hierarchische Datenstruktur, die ausgehend von einer *root* über Länderknoten und Organisationen, die wiederum hierarchisch strukturiert sein können, Knoten für beliebige weitere Einträge zur Verfügung stellt.

Die Struktur der Einträge ähnelt bis zu einem gewissen Grad der einer herkömmlichen Datenbank, wobei jedoch eine andere Terminologie verwendet wird. Demnach entspricht dem Datensatz der Eintrag, der einen Knoten im DIT darstellt. Felder werden im X.500 Attribute genannt, die einer genau bestimmbaren Attributsyntax unterliegen und einen oder mehrere Attributwerte haben können. Bestimmte Attributwerte bilden den *Relative Distinguished Name* (RDN) eines Eintrags, der zusammen mit den RDNs der hierarchisch im Baum weiter oben angesiedelten Einträge den *Distinguished Name* (DN) des Eintrags ergibt. Es ist möglich eine Gruppe von Attributen, sogenannte *Attribute sets* zu bilden. Jeder Eintrag gehört zu mindestens einer sogenannten Objektklasse, wie z.B. *„country“*, *„organization“*, *„organizationalUnit“ oder „person“*. Durch die Objektklasse werden eine Reihe von Attributen zur Verfügung gestellt, in denen die Informationen gespeichert werden können. So beinhaltet die Objektklasse *„person“* z.B. die Attribute *„commonName“*, und dem Attributgruppe *„telecommunicationAttributeSet“* etc.

X.500 ist eine objektorientierte Datenbank. Alle auftretenen Elemente (Eintrag, Attribut, Attributsyntax, Attributwert) werden als Objekte verwaltet. Mit Objektklassen werden Einträgen definiert, indem Attributgruppen zusammengefaßt werden und festgelegt wird, welche Attribute obligatorisch sind und welche optional. Objektklassen können Eigenschaften (Attributwerte bzw. Zugriffsrechte) vererben. Ein weiteres Mittel bestimmte Attributwerte einem ganzen Teilbereich von Einträgen zur Verfügung zu stellen, sind die Kollektivattribute (*Collective Attributes*).

1.1.2 Verantwortlichkeiten der Verwaltung

Die Verantwortung für die Daten einzelner Bereiche des DIT, den gesamten Bereich eines DSA oder Aufteilungen davon, sogenannten *Administrativ Areas* (AA), wird im X.500 genau festgelegt. Hierbei werden vier Administrationsfunktionen unterschieden:

- *Naming Administration*: Hier werden Regeln festgelegt über den Inhalt von namensrelevanten Attributen, also Namenskonventionen, Regeln zur Vermeidung von Doppelnamen etc.
- *Subschema Administration*: Hier wird festgelegt, welche Information in der AA abgelegt werden kann und welche Attribute zur Bildung der DNs verwendet werden.
- *Security Administration*: Hier werden alle Zugriffsrechte definiert.
- *Collective Attribute Administration*: Hier werden die Inhalte der bereits erwähnten *Collective Attributes* festgelegt.

Für alle diese Funktionen können *Policies* erstellt und Personen als verantwortlich bestimmt werden.

1.1.3 Zugriffsmöglichkeiten auf das X.500

Nach der Bereitstellung eines WWW-X.500-Gateway setzts sich das WWW zunehmend als einziger Benutzerzugang zum X.500 durch. Der X.500-Zugriff ist hierbei über die LDAP-Schnittstelle realisiert. Dieses Gateway befindet sich in einer zweisträngigen ständigen Weiterentwicklung, Web500gw an der TU-Chemnitz und das davon abgeleitete TWEB an der Universität Tübingen. Letztere Implementierung legt besonderen Wert auf Konfigurierbarkeit aller wichtigen Komponenten:

- Technische Konfigurierung (Zuordnung LDAPDaemon/DSA, Gateway Basisport, etc.)
- Gestalterische Konfigurierung (Darstellung der Attribute, selektive Ausgabe, sprachspezifische Texte, etc.)
- Politische Konfigurierung (Zugriffskontrolle, Modify-Zugriff, Listenbeschränkgungen, Erklärungstexte, etc.)

Um zu erreichen, daß die Daten im jeweils hierfür konfigurierten Gateway dargestellt werden („*Corporate Identity*"), wurde der Mechanismus des Gateway-Switching eingeführt, mit dem diesbezügliche Information zu einem HTML-Link auf ein anderes Gateway aufbereitet wird (vgl. weiter unten, Abschnitt 2.3.2).

1.2 Zugriffskontrollen im X.500

In der Definition von X.500 waren von vorneherein einige securityrelevante Features enthalten über die es im Folgenden gehen soll.

Beim Zugriff auf die Daten kann für einzelne Einträge oder für beliebige Bereiche des DIT genau bestimmt werden, wer was machen darf. Genauere Angaben bezüglich der Zugriffskontrolle wurden erst im 93er Standard gemacht, im 88er Standard gibt es nur proprietäre Lösungen in den Einzelimplementierungen.

Der 93er Standard definiert das sog. *Basic Access Control Scheme*, wo alle Belange der Zugriffsbeschränkung behandelt werden. Schützbare Elemente („*Protected Items*") sind: Einträge, Attribute, Attributwerte und DNs. Diese können einzeln aufgezählt oder in folgenden vordefinierten Gruppen angesprochen werden:

- Gruppe von Einträgen innerhalb der gleichen AA
- alle Attribute eines Eintrags
- alle Werte eines Attributs

Es kann genau definiert werden, welcher Vorgang erlaubt bzw. nicht erlaubt sein soll: lesen, auflisten, vergleichen, filtern, hinzufügen, ändern, löschen, umbenennen, an anderen Ort im DIT exportieren, an neuen Ort importieren, Rückgabe eines DN und Rückgabe einer Fehlermeldung, die die Existenz eines Eintrags verrät (vgl. Tabelle 1)

Solche Rechte können an einzelne Benutzer(innen), an verschieden zusammfaßbare Gruppen oder an Alle vergeben werden. Die Vergabe solcher Rechte kann von der Art der Benutzer-Authentifizierung abhängig gemacht werden.

Bei der Auswertung der Rechte gelten folgende Grundregeln:

- Es wird kein Zugriffsrecht durch Voreinstellung vergeben.
- Ein spezielles Zugriffsrecht (z.B. auf ein Attributtyp) beinhaltet kein allgemeineres (z.B. auf den Eintrag).
- Ein Zugriffsrecht auf einen Eintrag beinhaltet kein Zugriffsrecht auf die darin enthaltenen Attributtypen und -werte. Die zwei Ausnahmen dieser Grundregel sind Löschung und Umbennenung, obwohl im letzteren Fall das Attribut, das für den RDN zuständig ist, geändert wird.
- Es finden keine Überprüfungen nach unlogischen Kombinationen von Zugriffsrechten statt.

Tabelle 1: *Zugriffsrechte im Basic Access Controll Scheme* (n.v. = nicht vorhanden

Recht	Wirkung bei Eintrag (= E)	bei Attributtyp (= AT)	bei Attributwert (= AW)
Read	erlaubt Lesezugriff für Operationen, die den Namen des E betreffen; ist notwendige aber nicht ausreichende Voraussetzung für Lesezugriffe auf AT bzw. AW	erlaubt Lesezugriff für Operationen die AT einschließen; ist notwendige aber nicht ausreichende Voraussetzung für Lesezugriffe auf AW	erlaubt den Lesezugriff auf einzelne AW
Browse	erlaubt Auflist- und Suchoperationen, die den Namen des E betreffen	n.v.	n.v.
Compare	n.v.	erlaubt nach Vorhandensein eines ATs zu vergleichen; Read-Recht für E ist Voraussetzung	erlaubt Inhalt eines AWs zu vergleichen; Voraussetzungen: Read-Recht für E und Compare-recht für AT
FilterMatch	n.v.	erlaubt einen AT bei der Evaluierung eines Suchfilters zu verwenden; Browse-Recht für E ist Voraussetzung	erlaubt einen AW bei der Evaluierung eines Suchfilters zu verwenden; FilterMatch-Recht auf AT und Browse-Recht für E sind Voraussetzung
Add	erlaubt einen neuen E anzulegen, jedoch ohne AT bzw. AW; Add-Recht für obligatorische AT muß gegeben sein	erlaubt Hinzufügung eines ATs zu einen E; Add-Recht für mindestens einen AW muß gegeben sein, genauso wie Add- bzw. Modify-Recht auf E	erlaubt Hinzufügung eines AWs; falls AT noch nicht existiert, ist Add-Recht für AT Voraussetzung
Modify	erlaubt Veränderungen am E	n.v.	n.v.
Remove	erlaubt Löschung eines E; keinerlei sonstige Rechte sind hierfür vonnöten!	erlaubt Löschung eines AT; Remove-Recht für alle AW und Modify-Recht für E sind Voraussetzungen	erlaubt Löschung eines AW; wenn letzter AW gelöscht wird, ist Remove-Recht für AT Voraussetzung
Rename	erlaubt Umbennenung (= Änderung des RDNs) eines Es; keinerlei Rechte bezüglich AT und AW sind hierfür vonnöten; keinerlei Rechte auf untergeordnete Es, die hierdurch ihren DN ändern, sind vonnöten!	n.v.	n.v.
Export	erlaubt den E an eine andere Stelle im DIT umzusetzen; Voraussetzung ist Import-Recht für den neuen Übergeordneten E; keinerlei Rechte bezüglich AT und AW sind hierfür vonnöten; keinerlei Rechte auf untergeordnete E, die hierdurch ihren DN ändern sind vonnöten!	n.v.	n.v.
Import	erlaubt die Einfügung eines E an dieser Stelle im DIT	n.v.	n.v.
ReturnDN	erlaubt den DN eines E als Ergebnis einer Operation zurückzugeben	n.v.	n.v.
Disclose on Error	erlaubt eine Fehlermeldung als Ergebnis einer Operation zurückzugeben, die das Vorhandensein eines E verrät	n.v.	n.v.

Konflikte zwischen verschiedenen Rechten, können dadurch geregelt werden, daß jedes definierte Zugriffsrecht eine Gewichtung („*precedence*") erhält.

1.3 X.509 - Authentifizierungsmechanismen

Für die Umsetzung der Zugriffsrechte, aber auch für viele anderen sicherheitsrelevante Transaktionen, ist die Authentifizierung der Benutzer(innen), bzw. der DUAs und der DSAs wichtige Voraussetzung. Hierzu werden im X.500 eine ganze Reihe von Mechanismen unterstützt. Diese sind im Standard X.509 definiert. X.500 und X.509 sind zwei aufeinander abgestimmte und voneinander abhängige Konzepte.

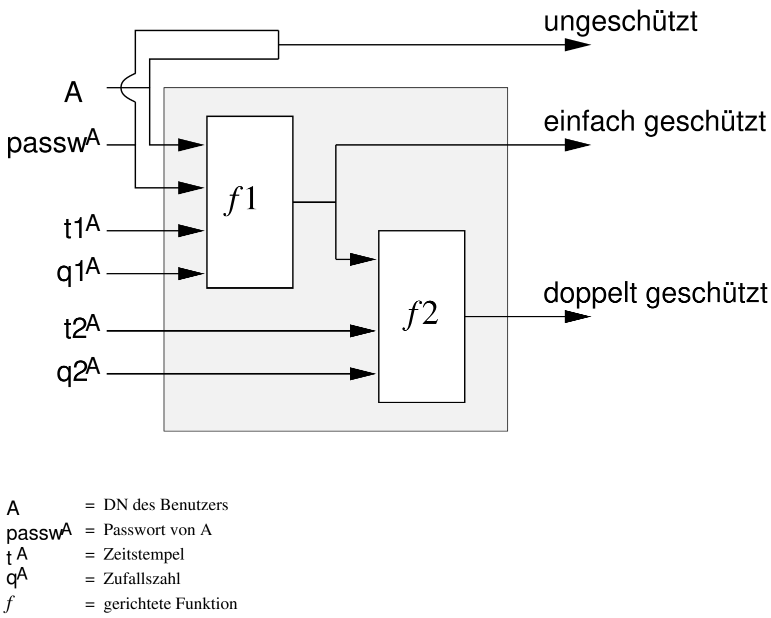

Abbildung 1: *Einfache Authentifizierung*

1.3.1 Einfache Authentifizierung

Die einfache Authentifizierung, *simple bind* genannt, besteht darin, daß ein(e) Benutzer(in) sich mittels eines in seinem X.500-Eintrag gespeicherten Paßworts als Besitzer(in) dieses Eintrags authentifiziert. Da die Paßwortvergabe keinerlei Restriktionen unterliegt, und da das Paßwort unverschlüsselt über das Netz geht, ist diese Methode sehr unsicher.

Diese Authentifizierung kann jedoch geschützt werden, indem das Paßwort, zusammen mit einer Zufallszahl und/oder einem Zeitstempel versehen und durch eine oder zwei gerichtete Funktionen *(one-way functions)* verschlüsselt, übertragen wird. Man spricht hierbei von *protected simple bind* (vgl. Abbildung 1).

Mit der einfachen Authentifizierung können sich sowohl Benutzer(innen) über einen DUA bei einem DSA authentifizieren, als auch ein DSA bei einem anderen DSA.

1.3.2 Strenge Authentifizierung mittels *Public Keys*

Neben der einfachen Authentifizierung wird in X.509 noch eine strenge Authentifizierung (*strong bind*) definiert, die ein Kryptosystem mit öffentlichen Schlüsseln voraussetzt (*public-key cryptosystem*, PKCS). Dieses Kryptosystem, das auch asymmetrisch genannt wird, basiert auf einem Schlüsselpaar für jede(n) Benutzer(in) (hier X genannt), einem geheimen, privaten Schlüssel (Xs), der zur Entschlüsselung verwendet wird, und einem öffentlichen Schlüssel (Xp), der zur Verschlüsselung dient. Xp wird aus Xs errechnet, aber Xs kann nicht aus Xp erschlossen werden. Hierzu wurden spezielle Algorithmen entwickelt, von denen der bekannteste und in X.509 empfohlene der RSA-Algorithmus ist, dessen Namen sich aus den Anfangsbuchstaben der Nachnamen der Autoren (Rivest, Shamir, Adleman) zusammensetzt. Eine Entschlüsselung kann mit folgender Formel abgebildet werden, wobei D für die Daten steht: D = Xs[Xp[D]]

Dieser Authentifizierungsmechanismus wird heute auch für Anwendungen außerhalb von X.500 verwendet, z.B. bei E-Mail im *„Privacy enhancement for Internet Electronic Mail"* (PEM), beim Dokument-Austausch im *„Office Document Interchange Format"* (ODIF), beim elektronischen Datenaustausch im kommerziellen Bereich, *Electronic Data Interchange* (EDI), für das eine ganze Reihe von Standards definiert worden sind.

Voraussetzung für alle Kommunikation mit strenger Authentifizierung ist, daß der öffentliche Schlüssel Xp jederzeit öffentlich zugänglich ist. Diese Voraussetzung wird durch die Ablage von Xp im X.500-Directory erfüllt. Somit kommt dem X.500 für alle diese Anwendungen eine wichtige Rolle zu.

Mit der asymmetrischen Authentifizierung können auch sogenannte elektronische Signaturen erstellt werden, mit denen man sowohl den Inhalt einer Nachricht als auch die Benutzer-Identität bestätigen kann. Die kleinste Änderung an einem so signierten Dokument wird durch eine Überprüfung bemerkt.

Für strenge Authentifizierung ist die Sicherstellung der Zugehörigkeit eines öffentlichen Schlüssels zu einer Person erforderlich. Eine solche Identität kann von sog. Zertifizierungsinstanzen (*certificate authority, CA)* überprüft werden. Nach der Überprüfung der Identität signiert eine CA den öffentlichen Benutzer-Schlüssel und erstellt somit ein Zertifikat. CAs sind hierarchisch organisiert und die jeweils untere CA wird von einer übergeordneten CA wiederum zertifiziert, wodurch eine sichere Hierarchie des Vertrauens aufgebaut wird. Teilbereiche dieser Hierarchie sind einer *Policy Certification Authority* (PCA) untergeordnet, die für diese die *Security Policy* definiert. Eine weitere Aufgabe von CAs ist die Veröffentlichung von zurückgezogenen Zertifikaten in Form von *certificate revocation list*s (CRLs). Auch diese müssen jederzeit öffentlich zugänglich sein, auch hierfür kann das X.500 genutzt werden.

Eine weitere Voraussetzung für die Identifizierung einer Person ist die Sicherstellung der Eindeutigkeit der Person. Dies wird durch den DN des zur Person gehörigen Eintrags erreicht. Die Eindeutigkeit des DNs ist aber nur gewährleistet, wenn alle DNs im X.500-Directory wirklich eingetragen sind, da es im Directory keine zwei

Einträge mit dem gleichen DN geben kann.

In X.509 sind alle Attribute zur Verwaltung von öffentlichen Schlüsseln, Zertifikaten und CAs definiert, so daß sowohl Schlüssel, Zertifikate und CRLs, als auch die CA-Hierachie im X.500 abgebildet werden können. Der Standard definiert darüberhinaus mehrere Verfahren der strengen Authentifizierung: Ein-Weg-, Zwei-Weg- und Drei-Weg-Verfahren, auf die hier jedoch nicht näher eingegangen werden soll.

Mit SecuDE hat die GMD ein Packet von Programmierschnittstelle, Libraryroutinen und Hilfswerkzeugen zur Verfügung getellt, mit der man Sicherheitsfunktionalität auf der Basis von X.509 in eigene Programme einbauen kann.

2 Security im Projekt AMBIX

2.1 Das DFN-Projekt AMBIX

AMBIX, „(A)ufnahme von (M)ail-(B)enutzern (i)n das (X).500“, ist ins Leben gerufen worden, um DFN-Mitgliedsorganisationen die Möglichkeit zu bieten, datenschutzkonform und einheitlich kommunikationsrelevante Personendaten von E-Mail-Benutzer(inne)n im X.500 zu veröffentlichen und aktuell zu halten, ohne selbst einen DSA betreiben zu müssen.

Basierend auf einer datenschutzrechtlichen Expertise wurde als Kompromiß zwischen den Interessen der Organisationen an einem Mitarbeiterverzeichnis und den Interessen der Betroffenen auf Hoheit über ihre personenbezogenen Daten ein Minimalset von Daten konzipiert, den die Organisationen an das Projekt liefern. Dieser Set besteht aus: Name, akademischer Titel, Organisationszugehörigkeit, dienstliche Telefon- und Faxnummern, sowie die E-Mail-Adresse. Als eine Ausweitung dieses Sets kommen, nach Absprache mit dem Berliner Datenschutzbeauftragten folgende freiwillige Angaben hinzu: URL, Arbeitsgebiet und v.a. öffentliche Schlüssel für asymmetrische Krypto-Verfahren. Die Betroffenen werden von AMBIX über die Datenübermittlung und über ihre Rechte der Löschung oder Veränderung der Daten informiert. Erst nach Ablauf einer Widerspruchsfrist von 6 Wochen nach dieser Informierung werden die Daten im X.500 veröffentlicht. Dieses Vorgehen setzt eine Datenhaltung außerhalb des X.500-Verzeichnis, sowie automatisierte Schnittstellen zu Organisationsdatenlieferungen und Benutzerinteraktion voraus. Diese wurden realisiert durch eine Client-Server-Implementation mit Kommunikation über *Remote Procedure Calls* (RPC). Zusätzlich zu der Datenlieferung durch Organisationen wurde eine Selbsteintragsmöglichkeit via WWW implementiert (vgl. Abbildung 2).

Das hier beschriebene Vorgehen beinhaltet eine Reihe von Sicherheitsproblemen, die im Folgenden behandelt werden sollen.

2.2 Datenschutzrechtliche Grundlage

Da es sich bei der Datensammlung um personenbezogene Daten handelt, ist es von größter Wichtigkeit, diese Daten vor unberechtigtem Zugriff zu schützen. Im Zeitalter von Internetwerbung kommt hierbei der E-Mail-Adresse eine besondere Be-

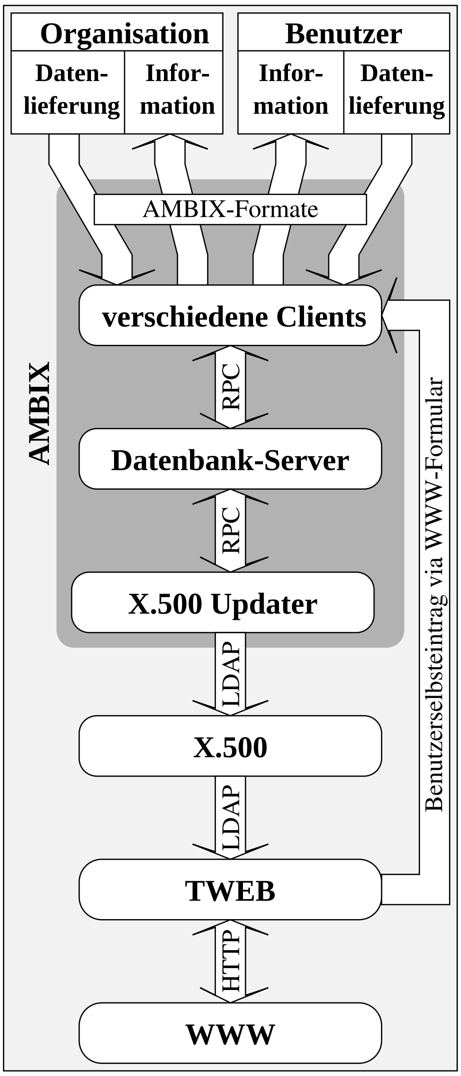

Abbildung 2: *AMBIX als Brücke zwischen Organisationen und X.500*

deutung zu, wegen der Gefahr massenhafter unerwünschter Werbe-E-Mails. In den USA ist eine solche Praxis leider Gang und Gäbe, obwohl sie per Gesetz verboten ist. Auch in Deutschland, gibt es mittlerweile E-Mail-Werbung-treibende Firmen. Es gibt zwar keine speziellen Gesetze für diesen Fall, die allgemeine Datenschutzgesetzgebung deckt ihn aber ab. Desweiteren gibt es ein BGH-Urteil zur Frage einer wettbewerbswidrigen Belästigung durch Werbung im Btx-Mitteilungsdienst (BGH, Urteil vom 3. 2. 1988 - I ZR 222/85), so daß man auch für Deutschland sagen kann, daß solche Werbungen illegal sind. Im Interesse der Benutzer(innen) muß das Projekt in jedem Fall besonderen Augenmerk darauf legen, daß die im Verzeichnis gespeicherten E-Mail-Adressen nicht in Massen an kommerzielle Firmen gelangen können, die sie zu eben diesen Zwecken mißbrauchen könnten.

Die schon erwähnte Datenschutzexpertiese schreibt vor, daß die Personendaten nur an Länder ausgegeben werden, in denen eine der deutschen Datenschutzgesetzgebung adäquate Rechtslage vorherrscht. Die ebenfalls vom Projekt gesammelten Organisationsstrukturdaten unterliegen jedoch keinerelei Zugriffsbeschränkungen.

2.3 Implementierung der Zugriffsbeschränkungen

Aus der beschriebenen datenschutzrechtlichen Lage ergibt sich für das Projekt die Notwendigkeit, Zugriffe auf die Daten nur kontrolliert zuzulassen. Es gibt eine ganze Reihe von Ebenen auf denen die Daten geschützt werden müssen, wobei der Benutzer-Authentifizierung eine große Bedeutung zukommt.

2.3.1 Zugriff von anderen DSAs bzw. DUAs

Da die Authentifizierung im X.500 nur über vorhandene Einträge im Verzeichnis möglich ist, im Augenblick aber nicht vorausgesetzt werden kann, daß jeder potenzielle Nutzer des E-Mail-Verzeichnisses einen Eintrag im X.500 hat, können die erforderlichen Zugriffsbeschränkungen nicht unmittelbar mit Hilfe der im Abschnitt 1.3 beschriebenen Authentifizierungsmechanismen des X.509 implementiert werden. Die Zugriffsrechte beim AMBIX-DSA werden mit diesen Mechanismen so gesetzt, daß Personendaten grundsätzlich nur an das AMBIX-TWEB weitergegeben werden, das sich mit *protected simple bind* beim DSA authentifiziert und selbst eigene Zugriffsbeschränkungen durchsetzt. Organisationsstrukturdaten werden auch an andere DSAs und DUAs weitergegeben. Für die geplante Veröffentlichung von *Public keys* werden zusätzlich Dienste eingerichtet, durch die solche Schlüssel ohne Zugriffsbeschränkungen recherchierbar gemacht werden.

2.3.2 Zugriff über das AMBIX WWW-X.500-Gateway

Das bereits erwähnte TWEB wurde unter anderem weiterentwickelt, um im Gateway die für AMBIX geforderten Zugriffsbeschränkungen umzusetzen. Das Gateway gibt nur Daten an Rechner weiter, die im *Domain Name Service* eingetragen sind und deren Toplevel-Domain einem datenschutztreibenden Land entspricht. Dies schließt von vorneherein die kommerziellen Toplevel-Domains, wie z.B.: „.com“ und „.net“ aus.

Zusätzlich zu den Möglichkeiten des *Robot Exclusion Protocoll* (REP) registriert das AMBIX-Gateway regelmäßige und häufige Zugriffe von einer Domain oder einem Einzelrechner, die auf einen nicht REP-konformen Roboter schließen lassen, kann diese automatisch kurzfristig sperren und stellt darüberhinaus die Möglichkeit bereit, solche Rechner dauerhaft durch entsprechende Eintragungen in der Konfigurationsdatei vom Zugriff auf die Daten zu sperren.

Alle diese Sicherheitsmechanismen sind so nur im projekteigenen Gateway konfiguriert. Andere Gateways dürfen also auch, wie andere DSAs keine Personendaten vom AMBIX-DSA erhalten. Unter anderem aus diesem Grund wurde in Deutschland über die DSA-DSA-Kommunikation eine Schicht Gateway-Gateway-Kommunikation gesetzt: das schon erwähnte Gateway-Switching. Ein Gateway erhält - statisch aus Einträgen in der Konfigurationsdatei, oder dynamisch über Einträge im X.500 das Wissen, welches Gateway für den jeweiligen X.500-Bereich zuständig ist, und wählt automatisch die URL und den Port dieses Gateways an, wenn Benutzer(innen) sich diesen Bereich anzeigen lassen möchten. Ein Gateway, das dieses Feature beherrscht, wird also automatisch auf das AMBIX-Gateway umschalten, wenn Benutzer(innen) den AMBIX-Datenbestand einsehen möchten (vgl. Abbildung 3).

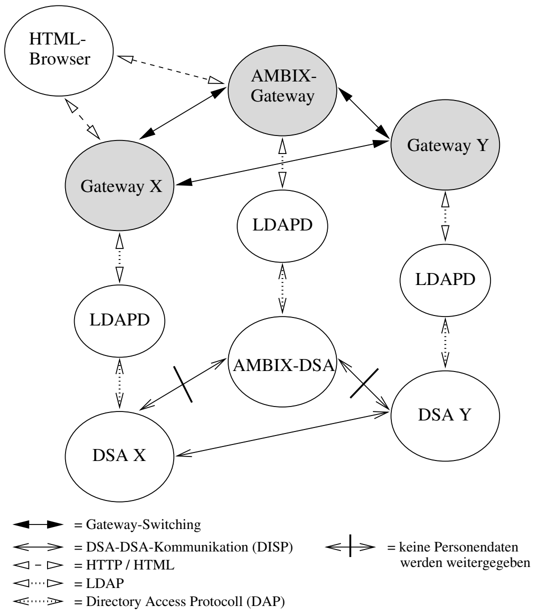

Abbildung 3: *Gateway-Switching*

2.3.3 Angriffe auf die AMBIX-Rechner

Natürlich muß auch die Möglichkeit in Betracht gezogen werden, daß jemand versucht, die Daten unberechtigt abzuhorchen.

Von vorneherein wurde die RPC-Schnittstelle der projekteigenen Client/Server Kommunikation als möglicher Angriffspunkt gesehen, zumal auf der verwendeten Plattform (HP-UX) kein Secure-RPC zur Verfügung steht. Deshalb wurden an dieser Stelle Sicherheitsmaßnahmen eingebaut. Jeder Clientrequest muß sich über ein vom Server generierten Handle authentifizieren, durch einen Zeitstempel hat ein solcher Handle nur eine beschränkte Gültigkeit. Eine weitere Absicherung der Schnittstelle durch Verschlüsselungsverfahren ist in Vorbereitung.

Mittlerweile ist die Systemadministration um einige Security-Features erweitert worden. Folgende Sicherheitstools werden auf den AMBIX-Rechnern (sowohl Server als auch Arbeitsplatz-PCs) eingesetzt:

- TCP-Wrapper zur Zugriffskontrolle und Überwachung auf TCP-Ebene: telnet, rlogin, remsh, rexecd, etc.
- Secure Shell, um ein sicheres *remote login* mit Authentifizierung über RSA-Verschlüsselungstechnik und eine ebenso sichere Tunnelung der X.11-Verbidung zu erreichen.

- Portmapper zur Zugriffskontrolle und Überwachung auf Port-Ebene: alle RPC-Dienste.
- Logsurfer mit dem alle sicherheitsrelevanten Logfiles automatisch ausgewertet werden können.

2.4 Authentifizierung von Datenlieferungen

Um sicherzustellen, daß die von den Organisationen und den Benutzer(inne)n gelieferten Daten authentisch sind, wurden in allen Eingabedatenformaten des Projekts Mechanismen der Authentifizierung implementiert.

2.4.1 Organisationslieferungen

Für jede Organisation wurde mindestens ein(e) Administrator(in) bei AMBIX registriert. An die registrierten Administrator(inn)en wurde ein Paßwort geschickt, mit dem sie ihre Datenlieferungen authentifizieren müssen. Diese Paßwort ist zusammen mit der E-Mail-Adresse im X.500 in einem DS-Manager-Eintrag abgelegt. Der Client, der die Organisationsdaten verarbeitet, überprüft mithilfe dieses X.500-Eintrags E-Mail-Adresse und Paßwort, die im Header der Datei angegebenen werden müssen. Für die Zukunft ist eine zusätzliche Verifizierung sowie die Verschlüsselung der Daten via *Public-Key*-Verfahren geplant.

2.4.2 Benutzerinteraktion

Jede(r) gemeldete Benutzer(in) erhält an die registierte E-Mail-Adresse ein Daten-Änderungs-Formular zugeschickt, in dem ein mit einer komplexeren Prüfsumme versehene Personenidentifikationsnummer eingetragen ist. Diese dient als Authentifizierung und ist Vorbedingung für das Akzeptieren von Datenänderungen. Darüberhinaus werden die Datenänderungen auf formale Kriterien hin überprüft. Um zu verhindern, daß jemand mit dem Formular eines Anderen seine Daten eintragen und somit die Daten des Anderen löschen kann, ist es nur über den/die Administrator(in) möglich, gleichzeitig Vor- und Nachname zu ändern. Auch die Kommunikation über das Datenänderungsformular soll in Zukunft durch *Public-Key*-Verfahren noch sicherer gemacht werden, die jedoch die Einrichtung einer entsprechenden, weiter unten noch zu behandelnden Infrastruktur voraussetzt.

Ein Schwachpunkt im System ist die Selbsteintragsmöglichkeit, da die so eingetragenen Daten vor der Eintragung ins X.500 vom Projekt nur formal überprüft werden können. Zusätzlich werden die Selbsteinträgerdaten den zuständigen Administrator(inn)en zur inhaltlichen Überprüfung zugeschickt. Letzlich wird hiermit jedoch nur die Verantwortung für die Korrektheit der Daten auf die Administrator(inn)en übertragen, das Projekt hat keinerlei Gewißheit darüber, ob die Daten wirklich überprüft werden. Nur von einem Teil der Organisationen kommt eine Rückmeldung auf diese Selbsteinträgerlisten. An dieser Stelle ist zu betonen, daß die Selbsteintragsmöglichkeit erst konzipiert wurde, als sich herausgestellt hatte, daß nur ein Teil der Organisationen zu einer aktiven Benutzerdatenlieferung bereit war.

Immerhin wird in jedem Fall verhindert, daß benutzerinduzierte Datenänderungen bzw. Neueinträge von jemanden gemacht werden, der nicht Besitzer der angegebenen E-Mail-Adresse ist, da jeder Vollzug einer Datenänderung an diese E-Mail-Adresse gemeldet wird, und vom Besitzer wieder rückgängig gemacht werden kann. Wenn eine solche Überprüfungs-E-Mail mit einer Fehlermeldung zurückkommt, aus der man die Funktionsunfähigkeit der Adresse schließen kann (z.B. „*user unknown*“), wird diese Adresse automatisch aus dem Verzeichnis gelöscht. Handelt es sich hierbei um die einzige E-Mail-Adresse eines Eintrags, wird der gesamte Eintrag gelöscht.

Nicht verhindert werden kann, daß jemand unter dem Namen eines Anderen einen Eintrag mit seiner eigenen E-Mail-Adresse anlegt, um so zu versuchen, E-Mails, die an diesen Anderen gerichtet sind, abzuhören. Sobald jedoch ein korrekter Eintrag einer Person im Verzeichnis existiert, kann eine solche Manipulation nicht mehr ohne Kenntnis der als Paßwort fungierenden Personenidentifizierungsnummer gemacht werden. Dies ist, neben den offensichtlichen Vorteilen in Bezug auf Vollständigkeit des Verzeichnisses, ein weiteres Argument für Datenlieferungen von den Benutzerverwaltungen der Organisationen.

2.5 *Public-Key*-Verwaltung

Neben den bisher gesammelten Daten erschließt sich durch den zunehmenden Einsatz von Kryptoverfahren und dem damit verbundenen gesicherter Datenaustausch ein weiteres wichtiges Betätigungsfeld für das Projekt AMBIX für seine Aufgabe, kommunikationsrelevante Daten zur Verfügung zu stellen. Wie bereits dargelegt, kommt dem X.500 als zugrundeliegender Infrastruktur bei der Bereitstellung der öffentlichen Schlüssel, ihrer Zertifikate und der Zertifikat-Rückruf-Listen eine entscheidende Bedeutung zu. Diesen Dienst will AMBIX für die von dem Projekt verwalteten Organisationen ebenfalls zur Verfügung stellen.

In Zusammenarbeit mit dem DFN-PCA-Projekt an der Universität Hamburg soll eine Kommunikationsstruktur mit einzelnen von der PCA zertifizierten CAs aufgebaut werden. Diese CAs sollen, vergleichbar mit dem bereits entwickelten Verfahren der Benutzerdatenlieferung durch Organisationen, zertifizierte *Public Keys* an AMBIX weiterleiten, damit sie vom Projekt im X.500 veröffentlicht werden. Hierfür wurden folgende Regeln aufgestellt:

- Durch CAs zertifizierte Schlüssel werden grundsätzlich nur von den CAs bzw. der DFN-PCA an AMBIX geliefert.
- Zertifikate werden generell nur von solchen CAs angenommen, die sich in der Zertifizierungshierarchie unterhalb der DFN-PCA befinden.
- Benutzer(innen) und Organisationsadministrator(inn)en (OAs) dürfen eigene, unzertifizierte (bzw. selbst-zertifizierte) Schlüssel ins X.500 eintragen.

- CAs und OAs dürfen nur Einträge löschen, die kein gültiges Benutzer-Zertifikat oder einer CA mehr enthalten. Einmal veröffentlichte CA-Zertifikate dürfen frühestens nach Ablauf der Gültigkeitsdauer aus dem X.500 entfernt werden, auch wenn ein Zertifikat zwischenzeitlich widerrufen wurde.

- Benutzer(innen) dürfen nach wie vor jederzeit ihren eigenen Eintrag löschen lassen, auch wenn dieser ein noch gültiges Zertifikat enthält.

- Ändert sich der DN eines eingetragenen Benutzers, ist der zuständige OA zu benachrichtigen.

Durch die sich im Entwurfstadium befindliche Verordnung zur digitalen Signatur (Signaturverordnung - SigV) kann sich eventuell die CA-Hierarchie ändern, da dort unterhalb einer CA bisher keine weitere CA vorgesehen ist.

Es sollen nicht nur Schlüssel, die nach X.509 erstellt und zertifiziert worden sind, aufgenommen werden, sondern auch PGP-Schlüssel, da dieses Verfahren augenblicklich das am weitesten verbreitetste ist. Darüberhinaus sollen zukünftige Entwicklungen mit berücksichtigt werden. Bei PGP-Schlüssel und -Zertifikaten gibt es noch keine standardisierte Möglichkeit der Ablage im X.500. Allerdings ist es wegen der offenen Konzeption von X.500 leicht möglich, hierfür eigene Attribute zu definieren. Zum gegenwärtigen Zeitpunkt soll aber zunächst abgewartet werden, ob sich hierfür nicht ein internationaler Standard durchsetzt. Dieses Abwarten ist deshalb unkritisch, da es für PGP-Schlüssel ein eigenes Veröffentlichungssystem neben X.500 gibt: die PGP-Keyserver.

Da nach dem aktuellen SigV-Entwurf Zertifikate über einen Zeitraum von mindestens 15 Jahren nach Ausstellung überprüfbar sein müssen, wird von AMBIX für abgelaufene Zertifikate ein eigener X.500-Datenbestand aufgebaut und entsprechende Recherche-Tools zur Verfügung gestellt, sofern sich hierfür ein Bedarf abzeichnet. Die Implementierung dieses „historischen DSA" hat allerdings zunächst keine hohe Priorität, sondern ist eher als ein gegebenenfalls zusätzlich anzubietender Service zu betrachten. Nur Zertifikate, deren reguläre Gültigkeitsdauer abgelaufen ist - nicht aber via CRLs zurückgezogene Zertifikate - sollen in diesem historischen DSA abgelegt und aus dem aktuellen Datenbestand gelöscht werden. Da gerade über die Gültigkeit und Gültigkeitsdauer beim Entwurf der erwähnten SigV noch diskutiert wird, bleibt abzuwarten, ob es eines solchen Dienstes überhaupt bedarf.

3 Abkürzungsverzeichnis

AA	*Administrativ Areas*
AMBIX	Aufnahme von Mail-Benutzern in das X.500
AT	Attributtyp
AW	Attributwert
CA	*certificate authority*
CRL	*certificate revocation list*
DIT	*Directory Information Tree*
DFN	Deutsches Forschungsnetz
DN	*Distinguished Name*
DSA	*Directory System Agents*
DUA	*Directory User Agents*
E	Eintrag
EDI	*Electronic Data Interchange*
GMD	Gesellschaft für Mathematik und Datenverarbeitung
LDAP	*Lightweight Directory Access Protokoll*
OA	Organisationsadministrator(in)
ODIF	*'Office Document Interchange Format*
PCA	*Policy Certification Authority*
PEM	*Privacy enhancement for Internet Electronic Mail*
PKCS	*public-key cryptosystem*
RDN	*Relative Distinguished Name*
RPC	*Remote Procedure Calls*
REP	*Robot Exclusion Protocoll*
SigV	Verordnung zur digitalen Signatur (Signaturverordnung)

4 Literaturverzeichnis

- [Gietz et al. 1996] X.500 für alle - Das DFN–Projekt AMBIX / Gietz. K.-P.; Schneider, R.; Spanier, K. - In: DFN Mitteilungen, Heft 42, November 1996

- [Kossakowski 1994] Sicherheit im Deutschen Forschungsnetz / Kossakowski, K.-P. - In: Workshop „Sicherheit in vernetzten Systemen" DFN-Bericht Nr. 75, 1994

- [NADF 1993] Directory Security - Mechanisms and Practicality / North American Directory Forum (NADF), DF-479/SD-11, 1993

- [Schneider 1992] SecuDE - Overview, Version 4.0 / Schneider, Wofgang. - Darmstadt: Gesellschaft für Mathematik und datenverarbeitung (GMD), 1992

- [Schneider o.j.] PASSWORD - Ein EG-Projekt zur pilotmäßigen Erprobung von Authentisierungsdiensten / Schneider, Wolfgang.- Gesellschaft für Mathematik und Datenverarbeitung (GMD), o.j.

- [Waugh 1994] X.500 and the 1993 Standard - Technical Report TR-SA-94-03 / Waugh, Andrew. - CSIRO Division of Information Technology, 1994

- [Steedman 1993] X.500 - The Directory Standard and its Application / Steedman, Douglas. - Twickenham: Technology Appraisals LTd, 1993

- [X.500 (1993)] The Directory: Overview of Concepts, Models, and Services - Recommendation X.500 ISO/IEC 9594-1 / Information Technology; Open Systems Interconnection. - 1993

- [X.501 (1993)] The Directory: Modells - Recommendation X.501 ISO/IEC 9594-2 / Information Technology; Open Systems Interconnection. - 1993

- [X.509 (1993)] The Directory: Authentication Framework - Recommendation X.509 ISO/IEC 9594-8 / Information Technology; Open Systems Interconnection. - 1993

- [X.511 (1993)] The Directory: Abstract Service Definition - Recommendation X.511 ISO/IEC 9594-3 / Information Technology; Open Systems Interconnection. - 1993