Anwenderdokumentation

eGO-MAIL
FÜR
BÜRGER

Autoren	Petra Carl Tanja Scheib
Layout	Martin Weinberg
Version des Dokuments	1.0
Stand	16.01.2007

Inhaltsverzeichnis

RECHTLICHE INFORMATIONEN UND WEITERE HINWEISE

eGo-Mail basiert auf der von der Firma bos KG entwickelten Client-Anwendung Govello. Als Grundlage für diese Anwenderdokumentation wurden Ausschnitte aus dem aktuellen Nutzerhandbuch der Firma bos KG zur Client-Anwendung Govello übernommen. Wir möchten Sie bitten, die nachfolgend aufgeführten rechtlichen Hinweise der Firma bos zu beachten.

Sofern in dem vorliegenden Produkt für Personen ausschließlich die männliche Form benutzt wird, geschieht dies nur aus Gründen der besseren Lesbarkeit und hat keinen diskriminierenden Hintergrund.

Der Begriff „Kommunen“ wird hier als Oberbegriff für alle kommunalen Körperschaften, wie Städte, Gemeinden, Kreise oder Zweckverbände mit eigenen Selbstverwaltungsaufgaben, verwendet.

Obwohl diese Produktdokumentation nach bestem Wissen und mit größter Sorgfalt erstellt wurde, können Fehler und Ungenauigkeiten nicht vollständig ausgeschlossen werden. Eine juristische Verantwortung oder Haftung für eventuell verbliebene fehlerhafte Angaben und deren Folgen wird nicht übernommen. Die in dieser Produktdokumentation enthaltenen Angaben spiegeln den aktuellen Entwicklungsstand wieder. Künftige Auflagen können zusätzliche Informationen enthalten.

Wenn Ihnen in diesem Dokument Fehler auffallen oder wenn Sie Verbesserungsvorschläge haben, schicken Sie diese bitte per E-Mail an: petra.carl@saarbruecken.de oder an tanja.scheib@saarbruecken.de

1 VORWORT

eGo-Mail ist eine Anwendung, die eine sichere und vertrauliche Kommunikation und Datenübertragung über das Transport–Medium Internet ermöglicht. Genutzt werden zur Datenübertragung das sichere Transportprotokoll OSCI und die Middleware Governikus.

Betreiber von eGo-Mail ist der Zweckverband Elektronische Verwaltung für saarländische Kommunen (eGo-Saar, URL: http://www.ego-saar.de). Der eGo-Saar ist ein freiwilliger Zweckverband, dem –bis auf die Stadt Bexbach- alle saarländischen Städte und Gemeinden, die Kreise, der Stadtverband, der Landkreistag, der Entsorgungsverband Saar und andere kommunale Dienstleister angehören. Der eGo-Saar hat es sich zum Ziel gesetzt, die Verwaltungsmodernisierung unter Nutzung von IT-gesteuerten Verfahren für und mit den saarländischen Kommunen, auch in Zeiten knapper finanzieller Ressourcen, kostengünstig umzusetzen.

Durch die in dieser Form einmalige interkommunale Zusammenarbeit und die tatkräftige Unterstützung der Firma bos KG, sowie dem internen Dienstleister der Landeshauptstadt Saarbrücken, dem Informations- und Kommunikationsinstitut (kurz IKS), wurde es möglich, mit eGo-Mail die Anforderungen des § 3a des saarländischen Verwaltungsverfahrensgesetzes zu erfüllen und einen Zugang zur rechtsverbindlichen elektronischen Kommunikation mit den entsprechenden Kommunen zu eröffnen. eGo-Mail ergänzt hierdurch als zentraler Posteingang die Zugangsmöglichkeit zu den kommunalen Dienstleistungen, wenn die Schriftform erforderlich ist und demgemäß die qualifizierte Signatur eingesetzt werden muss.

Insbesondere für gewerbliche Nutzergruppen (z.Bsp. Rechtsanwälte, Notare, Architekten), die kontinuierlich Verwaltungskontakte und eine hohe Anzahl von Transaktionen verzeichnen, bietet eGo-Mail zukünftig ein zielgruppenorientiertes Applikationsangebot, das zur Optimierung der Arbeitsabläufe und zur Verkürzung der Bearbeitungszeiten führen wird.

Wir wünschen Ihnen viel Erfolg bei der Nutzung von eGo-Mail!

Haftungsausschluss:

Der Betreiber eGo-Saar schließt jegliche Haftungsansprüche für die Installation und Nutzung von eGo-Mail aus.

2 ÜBER DIESE ANWENDERDOKUMENTATION

Diese Anwenderdokumentation soll Sie in die Lage versetzen mit den unterschiedlichen Funktionen von eGo-Mail sinnvoll umzugehen, bzw. Ihnen bei Fragen oder Problemen unterstützend zur Seite stehen.

eGo-Mail ist ein komfortables Kommunikationstool auf Basis der Intermediär-Software Governikus. eGo-Mail bietet Behörden, sowie deren Kunden, die Möglichkeit einer sicheren und rechtsverbindlichen Kommunikation über das Internet. Eine starke Verschlüsselung sorgt für die Vertraulichkeit. Eingesetzt werden hierfür elektronische Signaturen, das Übertragungsprotokoll OSCI und die entsprechenden Verschlüsselungstechnologien.

2.1 Elektronische Signaturen

Eine elektronische Signatur ist ein elektronisches Siegel, das die Integrität (Unverfälschtheit) eines Dokumentes nach dem Willen des Verfassers bestätigt. Bei der qualifizierten Signatur wird jedem Inhaber einer Signaturkarte je ein Schlüsselpaar, bestehend aus einem privaten und einem öffentlichen Schlüssel, zugewiesen.

Bei der Signaturbildung wird durch den Unterzeichner eines Dokumentes der private Schlüssel zur Signierung verwendet. Der öffentliche Schlüssel wird dem Empfänger mitgesandt und verifiziert beim Empfänger die Gültigkeit des Dokumentes. Dies geschieht über einen Hashwert (komprimierter Fingerabdruck der Datei).

Für die Sicherstellung der Vertraulichkeit wird ein zweites Schlüsselpaar benötigt. Zur Verschlüsselung des Dokumentes wird der öffentliche Schlüssel des Empfängers benötigt.

Der Empfänger entschlüsselt dann mit seinem privaten Schlüssel die übermittelten Informationen. eGo-Mail nutzt zur Ver- und Entschlüsselung standardmäßig Softwarezertifikate.

2.2 Datenübermittlung per OSCI

OSCI (Online Services Computer Interface) ist der Standard für die sichere Datenübermittlung in Deutschland. eGo-Mail überträgt die Daten in Form von OSCI-Nachrichten. Durch die Trennung von Sende- und Inhaltsdaten und den Einsatz von Verschlüsselungstechniken wird gewährleistet, dass auch bei der Prüfung der Signatur und der Zertifikate, durch den von IKS betriebenen Intermediär Governikus, die Vertraulichkeit der Kommunikation gewahrt bleibt. Hierdurch wird auch den Anforderungen des Datenschutzes Rechnung getragen.

Durch Protokollierungs- und Quittungsmechanismen wird das "elektronische Einschreiben mit Rückschein" realisiert.

2.3 Zertifikatsverwaltung

Zum Verschlüsseln von OSCI-Nachrichten benutzt eGo-Mail Schlüssel deren bestätigende Zertifikate gleichzeitig zur Adressierung der Nachrichten verwendet werden. Um mit eGo-Mail nach der Installation auch adressiert werden zu können, müssen Sie sich über einen Registrierungsdienst anmelden. Dies geschieht, indem die in einer Visitenkarte einzugebenden Daten verschlüsselt an einen Registrierungsserver übertragen werden. Mit diesem Vorgang werden Sie in einem zentralen Adressbuch registriert und können so später als Empfänger von Nachrichten ausgewählt werden

2.4 Kommunikationsablauf

Die Daten werden in Form von Nachrichten zwischen Bürgern und Behörden ausgetauscht. Dabei können Bürger und Behörden sowohl Absender als auch Empfänger von Nachrichten sein.

Die zu einer Nachricht gehörenden Daten werden nach ihrer Erfassung oder Übernahme innerhalb von eGo-Mail

- visualisiert,
- von den Absendern elektronisch signiert und dann

- von eGo-Mail im OSCI-Format an einen so genannten Intermediär (auch OSCI Manager genannt) gesendet.

2.5 Intermediär (Governikus)

Zur Übertragung von OSCI-Nachrichten wird immer ein Intermediär benötigt. Im Auftrag des eGo-Saar wird der für eGo-Mail genutzte Intermediär, von IKS betrieben.

Der Intermediär:

- prüft die Signatur und die Zertifikate,
- erstellt darüber ein Prüfprotokoll und
- hält die Nachricht im Postfach des Empfängers zum Abruf bereit.
- Die Nachricht kann, wiederum im OSCI-Format, über eGo-Mail abgeholt werden.

Nach diesem Schema läuft die Kommunikation zwischen Kommunikationspartnern grundsätzlich immer ab.

3 SYSTEMANFORDERUNGEN

Um die Anwendung nutzen zu können, sind folgende Systemanforderungen erforderlich:

- Für die Nutzung von eGo-Mail benötigen Sie einen PC und einen hinreichend schnellen Internetanschluss, beispielsweise DSL, da beim Start von eGo-Mail und der Übermittlung von umfangreicheren Nachrichten größere Datenmengen übertragen werden. eGo-Mail setzt die Darstellbarkeit von mindestens 256 Farben voraus; die Bildschirmauflösung sollte 1024 x 768 Pixel nicht unterschreiten.
- Die Betriebssysteme unter denen die Anwendung funktioniert, finden Sie unter der Internetadresse http://www.ego-saar.de (für Bürger –Homepage der Kommune).
- Da die Anwendung ohne Signaturkarten nicht genutzt werden kann, benötigen Sie ein Chipkarten-Lesegerät, das an den PC angeschlossen wird. Eine Liste der aktuell unterstützten Lesegeräte finden Sie unter der Internetadresse http://www.ego-saar.de (für Bürger –Homepage der Kommune).
- Zur Ausführung der Anwendung ist eine Java Runtime Environment (JRE) ab Version 1.4.2_04 unbedingt erforderlich. Im Allgemeinen wird die JRE als Bestandteil eines der genannten Browser automatisch und ohne Ihr Zutun mitinstalliert. Sollte die JRE auf dem gewünschten Rechner dennoch nicht existieren, besteht die Möglichkeit, das aktuell für die Nutzung von eGo-Mail empfohlene Softwarepaket vom USB-Stick (für Bürger – Homepage der Kommune) auf Ihren Rechner herunter zu laden, siehe dazu auch das Kapitel "Installation und Start von eGo-Mail".
- Um die Anwendung aufzurufen benötigen Sie das Programm Java Web Start (JWS). Wenn Sie die JRE installieren, wird JWS automatisch mitinstalliert.

Während der Installation am Arbeitsplatzcomputer sind bestimmte Nutzerrechte erforderlich:

- Zur Installation von Java Runtime Environment / Java Web Start sowie zur ersten Installation von eGo-Mail benötigen Sie, als späterer Nutzer, lokale Administratorrechte für Ihren Arbeitsplatzcomputer, weil dabei Änderungen an den so genannten Java-Policies vorgenommen werden. .
- Für später erforderliche Updates werden dagegen nur die normalen Rechte eines Standardbenutzers benötigt. Bitte sprechen Sie für die Erstinstallation gegebenenfalls Ihren Systemadministrator an.

4 INSTALLATION UND START DER ANWENDUNG eGO-MAIL

Dieses Kapitel beschreibt die Schritte zur Installation und erstmalige Inbetriebnahme von eGo-Mail.

4.1 Installation

4.1.1 Java Runtime Enviroment (JRE)

Die Java Laufzeitumgebung (JRE) wird aus zwei Gründen benötigt.

1. eGo-Mail ist eine in Java erstellte Anwendung, die eine JRE zur Ausführung benötigt
2. Zusammen mit der JRE wird automatisch auch Java Web Start installiert.

eGo-Mail wird anfangs mit Java Web Start installiert und danach immer über Java Web Start gestartet. Java Web Start verbindet sich vor jedem Start von eGo-Mail mit dem Server, auf dem die eGo-Mail Installationsdateien abgelegt sind. Auf diesem Server findet eine Überprüfung auf Aktualität statt. Ist eine der eGo-Mail Komponenten auf dem Server aktueller als auf Ihrem Rechner, wird diese vor dem Start von eGo-Mail aktualisiert. Damit ist sichergestellt, dass Sie eGo-Mail immer in der aktuellsten Version starten.

Hinweis: Wenn Sie nicht wissen, welche Version der JRE oder ob überhaupt eine JRE auf Ihrem Rechner installiert ist, gehen Sie wie folgt vor.

- Für MS Windows Anwender: Öffnen Sie über "Start" -> "Programme" -> "Zubehör" ein Eingabeaufforderungsfenster (DOS Prompt). Geben Sie dort diesen Befehl ein: `java –version` Es wird entweder die Version Ihrer JRE ausgegeben oder, wenn noch kein JRE installiert wurde, die Ausgabe "`Befehl konnte nicht gefunden werden`".
- Für Linux Anwender: Öffnen Sie eine Shell und geben Sie dort diesen Befehl ein: `java –version` Es wird entweder die Version Ihrer JRE

ausgegeben oder, wenn noch kein JRE installiert wurde, die Ausgabe "`Command not found`".

Laden Sie die gewünschte Version auf Ihren Rechner herunter und starten Sie die Installation durch Doppelklick auf die Datei.

Lesen und akzeptieren Sie die Lizenzbestimmungen und folgen Sie danach den Anweisungen des Installationsassistenten.

Mit der Installation einer passenden JRE auf Ihrem Computer haben Sie die notwendigen Voraussetzungen geschaffen, um eGo-Mail zu starten. Bitte beachten Sie, dass hierzu eine Internetverbindung bestehen muss.

Es erscheint das folgende Fenster:

Abbildung 3: Java Runtime lädt eGo-Mail

4.1.2 Java Web Start (JWS)

eGo-Mail wird immer mit Java Web Start (JWS) installiert und danach auch immer mit JWS gestartet. JWS ermittelt fehlende bzw. aktuellere Module und startet nach kurzer Zeit den Download-Vorgang vom Server. Je nach benötigter Datenmenge, verfügbarer Netzanbindung und Auslastung des Servers kann der Download unter Umständen mehrere Minuten in Anspruch nehmen.

Der Download-Umfang hängt davon ab, ob Sie eGo-Mail erstmalig herunterladen oder ob eine Aktualisierung stattfindet. Ersteres wird - je nach Netzanbindung - einige Zeit in Anspruch nehmen, da eGo-Mail komplett geladen wird. Beim Starten einer bereits installierten eGo-Mail Anwendung ist der Aufwand dagegen sehr viel geringer, da nur die aktualisierten Dateien geladen werden.

Dieser Aktualisierungs-Download erfolgt entweder bei bestehender Online-Verbindung beim Start der Anwendung oder beim nachträglichen Herstellen einer

Online-Verbindung, beispielsweise beim Senden und Empfangen der Nachrichten.

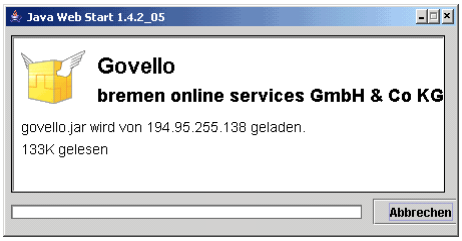

Abbildung 4 Java Web Start

Sobald der Download erfolgreich beendet wurde, erscheint eine Meldung, mit der JWS den unbeschränkten Zugriff auf den lokalen Rechner und das Netzwerk fordert. In dieser Sicherheitswarnung der SUN Microsystems Inc. wird das Zertifikat genannt, mit dem die gerade herunter geladenen Module signiert wurden, sowie das Trust Center, das die Authentizität dieses Zertifikats garantiert.

Klicken Sie auf den Button “Installieren“ (in anderen JRE Versionen kann dieser Button mit "Ausführen" bezeichnet sein) um den Programmstart fertig zu stellen. Die Sicherheitswarnung von SUN Microsystems Inc. erscheint nur beim ersten Download der Anwendung. Die eGo-Mail Programmoberfläche wird angezeigt

Beim ersten Start von eGo-Mail erscheint nun das Fenster "Unlimited Strength Java Cryptography Extension Policy Files", das in Englisch über die Java-Lizenzbedingungen informiert. Bitte lesen Sie die Erklärung und stimmen Sie dieser zu.

4.2 Die Anwendung eGo-Mail starten

Nach dem Download der Dateien und der Anzeige der verschiedenen Meldungen während der Installation befinden Sie sich nun in der eigentlichen eGo-Mail Anwendung. Zur Begrüßung wird vor der eigentlichen Anwendungsoberfläche von eGo-Mail ein Startbild eingeblendet. Dieses Bild wird auch bei jedem folgenden Aufruf von eGo-Mail am Anfang erscheinen.

Abbildung 5 Startbild eGo-Mail

Beim ersten Aufruf von eGo-Mail erscheint ein Fenster mit zwei Funktionen: Zum einen informiert es Sie über die bei eGo-Mail geltenden Lizenzbedingungen, zum anderen dient es dazu, Ihren zukünftigen Speicherort des Nachrichtenordners für die auf OSCI basierende Kommunikation dauerhaft festzulegen.

4.2.1 eGo-Mail Lizenzerklärung

Bitte lesen Sie sich zunächst die Lizenzbedingungen aufmerksam durch. Stimmen Sie den Bedingungen zu, wenn Sie eGo-Mail benutzen wollen.

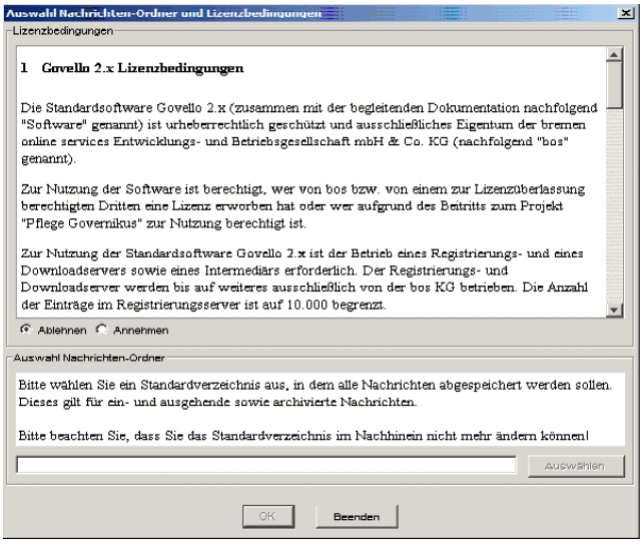

Abbildung 6: Lizenzbedingungen und Auswahl des Speicherortes

4.2.2 Auswahl des Speicherortes für den Nachrichtenordner

Im nächsten Schritt wird der Nachrichtenordner festgelegt.

Achtung: Sie können dieses Verzeichnis nur beim ersten Start der Anwendung definieren und im Nachhinein nicht mehr ohne weiteres ändern.

Wir empfehlen Ihnen, den Standard-Nachrichtenordner für eGo-Mail auf einer hohen Ebene im Verzeichnissystem auf Ihrer Festplatte anzulegen, also zum

Beispiel: c:\eGo-Mail. Die Anwendung legt in diesem Verzeichnis einen Ordner "osci_governikus" an und speichert in einem Unterordner alle Nachrichten und deren Anhänge.

Wenn Sie Ihre Vorüberlegungen abgeschlossen haben, klicken Sie bitte auf den Button "Auswählen".

Verwenden Sie die sich jetzt öffnende Verzeichnisauswahl-Box, um das Arbeitsverzeichnis für Ihr neues Postfach festzulegen. Navigieren Sie zum gewünschten Verzeichnis und legen Sie es mit dem "Auswählen" Button fest.

Nach der Festlegung des Nachrichtenordners wird das Verzeichnisauswahlfenster ausgeblendet und Sie sehen wieder das zuvor geöffnete Fenster und Auswahl des Nachrichtenordners. Bitte kontrollieren Sie, ob der ausgewählte Nachrichtenordner korrekt ist und klicken Sie auf den OK-Button. Die Einrichtung (Eröffnung) Ihres eGo-Mail Postfaches wird im Kapitel „Handhabung des Postfaches“ erläutert.

4.2.3 Datenschutzerklärung

Bitte lesen Sie sich zunächst die Datenschutzerklärung aufmerksam durch. Stimmen Sie den Bedingungen zu, wenn Sie eGo-Mail benutzen wollen.

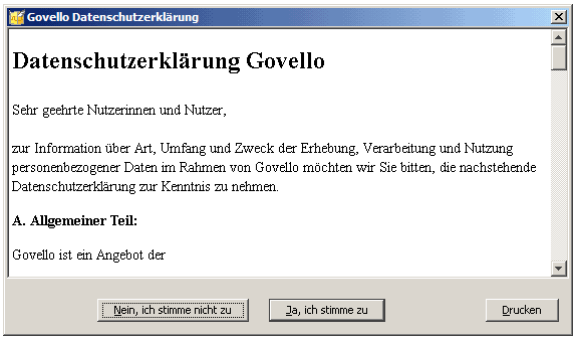

Abbildung 7: Datenschutzerklärung Govello

5 VISITENKARTE UND GRUNDEINSTELLUNGEN

5.1 Registerblatt Visitenkarte

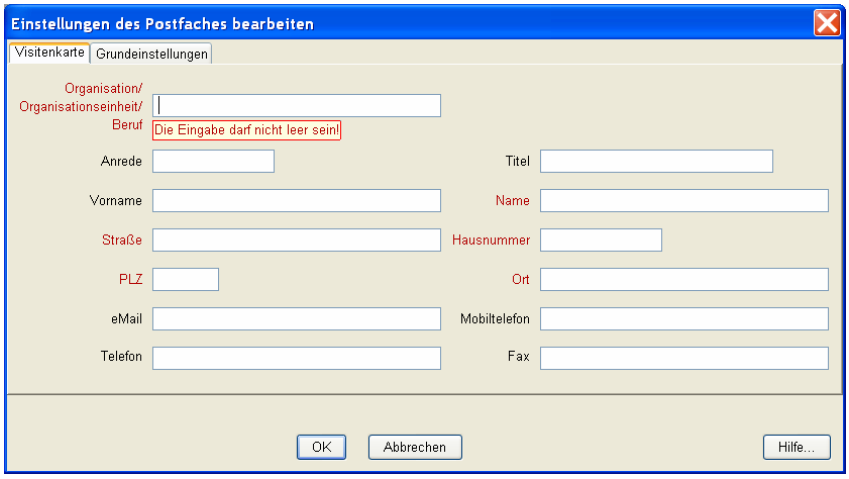

Abbildung 8: Registerblatt Visitenkarte

Nach Ihrer Zustimmung und beim ersten Start wird Ihnen der Visitenkartendialog angezeigt. Geben Sie bitte Ihre Kontaktdaten ein. Alle rot gekennzeichneten Felder sind Pflichtfelder. Je nach Client können die Pflichtfelder unterschiedlich vorkonfiguriert sein. Die Visitenkarte wird immer mit den Nachrichten an den Empfänger übersandt.

5.2 Registerblatt Grundeinstellungen

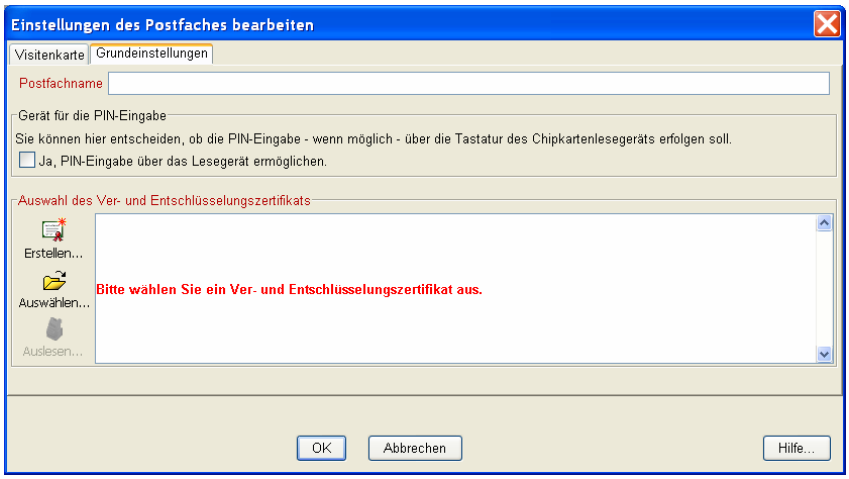

Abbildung 9: Registerblatt Grundeinstellungen

In dem zweiten Registerblatt „Grundeinstellungen“ werden der Name Ihres Postfachs und das dazu gehörende Verschlüsselungszertifikat festgelegt. Bei Nutzung einer Signaturkarte können Sie optional die PIN für das Zertifikat über den Kartenleser eingeben. Sie benötigen dazu ein sog. Klasse 2- oder Klasse 3-Lesegerät, das mit einer eigenen Tastatur ausgestattet ist und bei dem die Anwendung eine PIN-Eingabe über die Tastatur unterstützt wird.

Zur Authentifizierung bei der Anmeldung von eGo-Mail und zur Ver- und Entschlüsselung wird ein Zertifikat benötigt. Sofern kein Zertifikat vorhanden ist, können Sie sich über den Button „Erstellen“ ein Software-Zertifikat erstellen. Diese Zertifikat können Sie allerdings nicht zum signieren von Nachrichten nutzen.

Sofern Sie ein bereits bestehendes Softwarezertifikat nutzen möchten, bestätigen Sie den Button „Auswählen“ .Es öffnet sich der Datei-Explorer, Sie können das gewünschte Zertifikat auswählen und durch Anklicken des „Öffnen“-Buttons in das Registerblatt Grundeinstellung übernehmen.

Bei Verwendung einer Signaturkarte können Sie über den Button „Auslesen“ auch das Verschlüsselungszertifikat der Signaturkarte auslesen. Der Kartenleser wird, sofern dieser unterstützt wird, automatisch erkannt. Bitte beachten Sie hierbei, dass bei Verlust der Karte ein Zugriff auf das Postfach nicht mehr

möglich ist und somit keine Nachrichten empfangen bzw. versendet werden können. Wir empfehlen Ihnen aus diesem Grund zur Ver- und Entschlüsselung ein fortgeschrittenes Softwarezertifikat zu nutzen.

5.2.1 Erstellen eines Zertifikats

Sie haben die Möglichkeit sich über den Button „Erstellen“ ein Software-Zertifikat zu erstellen. Die Felder „Name“, „Organisation“ und „Organisationseinheit“ werden hierbei aus der ausgefüllten Visitenkarte übernommen.

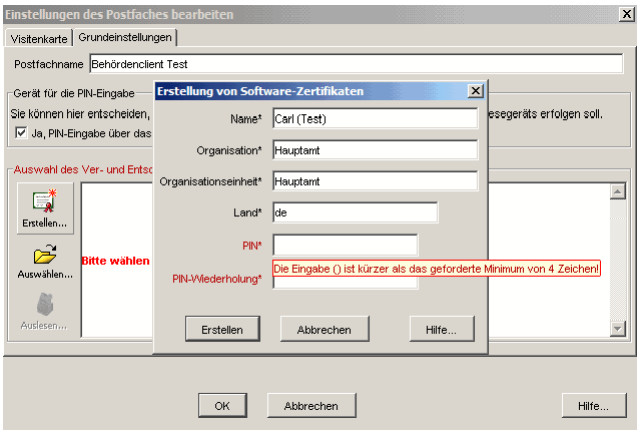

Abbildung 10: Vergabe einer PIN

Klicken Sie auf den Button „Erstellen“ öffnet sich der Datei-Explorer. Hier können Sie einen Namen für das Zertifikat angeben und das Verzeichnis, in dem das Zertifikat abgespeichert werden soll.

Bevor das Zertifikat angezeigt wird, werden Sie erneut zur Eingabe der PIN aufgefordert. Nach Eingabe der PIN wird das erzeugte Zertifikat an den Registrierungsserver (OSCI-Manager) bei bos gesandt.

Danach gelangen Sie sofort in Ihr Postfach. Sie können nun Nachrichten erstellen, versenden und empfangen.

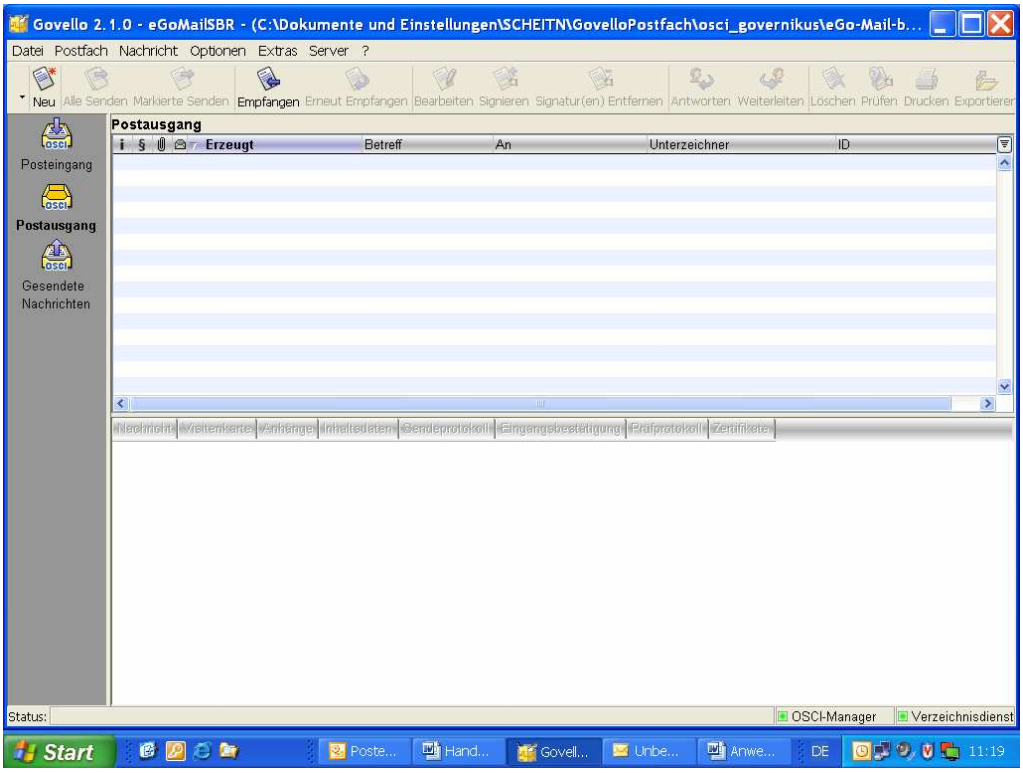

Abbildung 11: Hauptverwaltungsfenster

Das Postfach kann über den Menüpunkt „ Datei“ oder das „ x “ geschlossen werden. Wenn sich im Postausgang noch Nachrichten befinden, werden sie bei der Abmeldung darauf hingewiesen.

6 HANDHABUNG DES POSTFACHS

6.1 Postfach öffnen

Ein bereits bestehendes Postfach kann nur geöffnet werden, wenn Sie die PIN für das Verschlüsselungszertifikat eingeben. Drücken Sie hierzu den Button „Öffnen“.

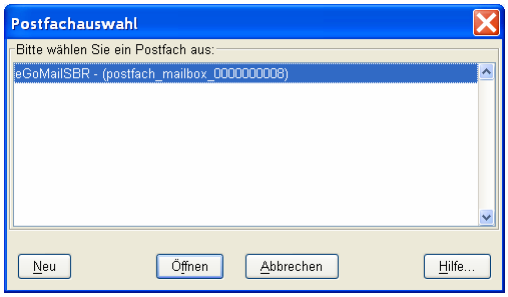

Abbildung 12: Anmeldefenster

Anschließend erscheint ein Fenster, in dem Sie Ihre PIN für das mit dem Postfach verknüpfte Verschlüsselungszertifikat eingeben können. Nach Eingabe der korrekten PIN öffnet sich das Verwaltungsfenster des Postfachs. Sie können nun wieder Nachrichten empfangen, erstellen und versenden.

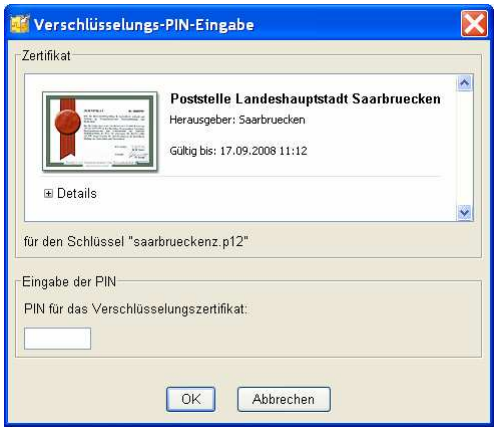

Abbildung 13: Eingabe der PIN

6.1.1 Weiteres Postfach eröffnen

Über den Button „Neu“ im Anmeldefenster kann ein weiteres Postfach eingerichtet werden.

6.2 Postfach bearbeiten

Im Verwaltungsfenster finden Sie den Menüpunkt „Postfach“. Unter „Bearbeiten“ öffnet sich das Einstellungsfenster für das geöffnete Postfach. In diesem können Sie alle spezifischen Parameter eines Postfachs ändern. Dies sind z.B. Ihre persönlichen Daten (Visitenkarte) sowie der Postfachname und das zugehörige Zertifikat. Ebenso können Sie für die unterstützten Lesegeräte eine andere Art der PIN-Eingabe auswählen (Tastatur des Kartenlesegeräts oder Tastatur des PCs).

6.3 Postfach schließen

Durch Auswahl der Option "Schließen" im Menüpunkt "Postfach" wird ein geöffnetes Postfach geschlossen.

6.4 Postfach löschen

Durch Auswahl der Option "Löschen" im Menüpunkt "Postfach" kann ein Postfach gelöscht werden. Bitte beachten Sie Zum Löschen des Postfachs gehen Sie wie folgt vor:

- Holen Sie ggf. noch für Ihr Postfach vorhandene Nachrichten ab bzw. versenden Sie noch im Postausgang befindliche Nachrichten.
- Schließen Sie das Postfach über den Menüpunkt „Postfach“ – „Schließen“.
- Wählen Sie im Menüpunkt „Postfach“ die Option „Löschen“.
- Markieren Sie das Postfach das gelöscht werden soll und geben Sie die Verschlüsselungs-PIN des zugehörigen Zertifikats ein.
- Das Postfach wurde gelöscht.

7 ANWENDUNGSOBERFLÄCHE

Wer mit E-Mail Programmen bereits vertraut ist, wird die Grundzüge der Anwendung schnell verstehen. Die Anwendungsoberfläche besteht im Wesentlichen aus einem Nachrichtenbereich, in dem gesendete und empfangene Nachrichten dargestellt werden. Weitere Dialogfenster öffnen sich entsprechend der Nutzreaktivität bei Bedarf. So gibt es zum Beispiel einen Anmeldefenster beim ersten Aufruf der Anwendung, ein Fenster zur Erstellung neuer Nachrichten, ein Fenster zur Festlegung der individuellen Postfacheinstellungen usw.

Die wesentlichen Bestandteile des Verwaltungsfensters sind:

- Die Funktionsliste: Über die Buttons in der Funktionsleiste können Nachrichten erstellt und bearbeitet werden. Auf die gleichen Funktionen zum Erstellen und Bearbeiten von Nachrichten kann unter dem Menüpunkt "Nachrichten" zugegriffen werden.
- Die Postkorbleiste: Die Postkorbleiste befindet sich am linken Rand der Anwenderoberfläche und ermöglicht die Auswahl von "Posteingang", "Postausgang" und "Gesendete Nachrichten". Der von Ihnen aktuell ausgewählte Postkorb wird in der Postkorbleiste in Fettdruck angezeigt und als Beschriftung über dem Nachrichtenbereich angezeigt.
- Der Nachrichtenbereich: Im Nachrichtenbereich des Verwaltungsfensters werden die wichtigsten Daten zu den erstellten, gesendeten und empfangenen Nachrichten angezeigt. Je nach Postkorb werden verschiedene Informationen für den Nutzer bereitgestellt.
- Die Registerblätter: Die acht Registerblätter zeigen alle Informationen, die die Anwendung zu einer Nachricht speichert. Markieren Sie dazu im Nachrichtenbereich im oberen Teil des Verwaltungsfensters die gewünschte Nachricht und klicken Sie dann in der unteren Fensterhälfte auf die Reiter der Registerblätter. Bitte beachten Sie, dass je nachdem welcher Postkorb gerade aktiv ist, nur bestimmte Registerblätter anwählbar sind.

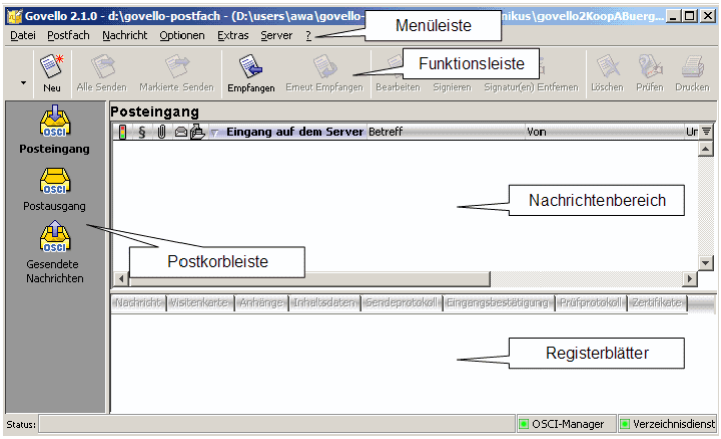

Abbildung 14: Anwendungsoberfläche

7.1 Die Postkorbleiste

7.1.1 Posteingang

Klicken Sie auf den Button "Posteingang", um alle empfangenen Nachrichten anzuzeigen. Im Nachrichtenbereich des Verwaltungsfensters werden die Spalten "Status", "Eingang auf dem Server", "Betreff“, "Von", "Unterzeichner" und "ID“ angezeigt. Bei den Registerblättern im unteren Bereich sind "Nachricht", "Visitenkarte", "Anhänge", "Inhaltsdaten", "Prüfprotokoll" und "Zertifikate" aktiviert

7.1.2 Postausgang

Klicken Sie auf den Button "Postausgang", um alle zum Senden bereitstehenden Nachrichten anzuzeigen. Im Nachrichtenbereich des Verwaltungsfensters werden die Spalten "Status", "Erzeugt", "Betreff", "An", "Unterzeichner" und "ID" angezeigt. Bei den Registerblättern im unteren Bereich sind "Nachricht", "Anhänge", "Inhaltsdaten" und "Zertifikate" aktiviert.

7.1.3 Gesendete Nachrichten

Klicken Sie auf den Button "Gesendete Nachrichten", um alle bereits gesendeten Nachrichten anzuzeigen. Im Nachrichtenbereich des Verwaltungsdialogs werden

die Spalten "Status", "Eingang auf dem Server", "Betreff", "An", "Unterzeichner" und "ID" angezeigt. Bei den Registerblättern im unteren Bereich sind "Nachricht", "Visitenkarte", "Anhänge", "Inhaltsdaten", "Sendeprotokoll", "Eingangsbestätigung" und "Zertifikate" aktiviert.

7.2 Der Nachrichtenbereich

7.2.1 Ampel

In dieser Spalte wird für eingegangene Nachrichten das Ergebnis der Signatur- und Signaturzertifikatsprüfung in Kurzform dargestellt. Die Haken in den Zeilen haben folgende Bedeutung:

- Grüner Haken: sämtliche durchgeführten Prüfungen haben ein positives Ergebnis geliefert.
- Gelbes Dreieck mit rotem Ausrufezeichen: mindestens eine der Prüfungen konnte nicht durchgeführt werden.
- Rotes Kreuz: mindestens eine der durchgeführten Prüfungen hat ein negatives Ergebnis geliefert.

Bitte klicken Sie auf das Registerblatt "Prüfprotokoll", um sich die Ergebnisse im Detail anzusehen.

7.2.2 Signaturniveau

Die Spalte Signaturniveau wird durch ein Paragraphensymbol dargestellt. Es zeigt an mit welchem Signaturniveau die Nachricht signiert wurde (Posteingang) bzw. signiert werden muss (Postausgang). eGo-Mail kann nur mit einer qualifizierten Signatur genutzt werden. Insofern wird hier ein (Q) für ein qualifiziertes Signaturniveau angezeigt.

7.2.3 Anhänge (Heftklammer)

Die Spalte zeigt an, ob mit der Nachricht Anhänge mitgeführt werden.

7.2.4 gelesen / ungelesen

Diese Spalte zeigt an, ob eine Nachricht gelesen wurde oder ungelesen im "Posteingang", "Postausgang" oder "Gesendete Ordner" abgelegt wurde. Sie können erkennen, dass Sie eine Nachricht noch nicht gelesen haben, wenn diese im Fettdruck dargestellt wird.

7.2.5 Information (i)

Diese Spalte wird nur im Postausgang angezeigt und informiert den Nutzer über den Status der Nachricht:

- Nachricht wird gerade versendet.
- Die Nachricht muss noch mindestens mit dem im Spalte "Signaturniveau" geforderten Signaturniveau signiert werden Haken: sämtliche durchgeführten Prüfungen haben ein positives Ergebnis geliefert.
- Die Nachricht wird gerade bearbeitet.

7.2.6 Eingang auf dem Server (Ende des Empfangsvorgangs)

Die Spalte "Eingang auf dem Server" erscheint nur, wenn der "Posteingang" oder "Gesendete Nachrichten" ausgewählt wurde. Hier werden Eingangsdatum und Eingangsuhrzeit der Nachricht wiedergegeben.

Bitte beachten Sie, dass es sich hier um den Zeitpunkt handelt, zu dem die Nachricht vollständig beim Intermediär (Governikus) eingegangen ist und nicht um den Zeitpunkt des Nachrichtenempfangs durch eGo-Mail. Dieselbe Zeitangabe findet sich auch im Prüfprotokoll zu der eingegangenen Nachricht sowie im Sendeprotokoll, das der Absender dieser Nachricht beim Versand vom Intermediär erhalten hat.

Für die Wahrung von Fristen ist der Eingang auf dem Intermediär maßgebend.

7.2.7 Erzeugt

Die Spalte "Erzeugt" erscheint nur im Ordner „Postausgang“. Hier wird der Zeitpunkt dokumentiert, in dem die Nachricht verfasst und gespeichert worden ist.

7.2.8 Betreff

In der Spalte "Betreff" wird der Inhalt der Betreffszeile der Nachricht angezeigt

7.2.9 "Von" bzw. "An"

Angezeigt wird im "Posteingang" die Spalte "von" (Name des Absenders der Nachricht), im "Postausgang" die Spalte "An“ und im "Gesendete Nachrichten" die Spalte "an" (Name des Nachrichtenempfängers). Durch Klick auf den Spaltennamen wird die gesamte Tabelle aufsteigend bzw. wieder absteigend nach Namen und Vornamen sortiert.

7.2.10 Unterzeichner

Diese Spalte erscheint im "Posteingang", "Postausgang" oder "Gesendete Nachrichten" und stellt den Namen der Person dar, die die Nachricht unterzeichnet hat. Ist eine Nachricht unterzeichnet, wird dies zusätzlich durch die Statuszeile "Signatur" symbolisch angezeigt. Durch Klick auf den Spaltennamen wird die gesamte Tabelle aufsteigend bzw. wieder absteigend sortiert.

7.2.11 ID

Diese Spalte gibt es in allen Postkörben. Hierin werden die vom Intermediär vergebenen eindeutigen Identifikationsnummern der zugehörigen Nachrichten dargestellt. Standardmäßig sind die Nachrichten absteigend nach dem Datum sortiert, d.h. die neueste Nachricht findet sich an erster Stelle. Durch Klick auf den Spaltennamen "ID" wird die gesamte Tabelle aufsteigend bzw. wieder absteigend nach der ID sortiert

7.3 Die Registerblätter

Im Folgenden Abschnitt wird dargestellt, welche Informationen die Registerblätter Nachricht, Visitenkarte, Anhänge, Inhaltsdaten, Sendeprotokoll, Eingangsbestätigung, Prüfprotokoll und Zertifikate für Sie bereitstellen und von welchem Postkorb aus die unterschiedlichen Registerblätter anwählbar sind.

Tabelle 1: Registerblätter

Registerblatt	**Bereitgestellte Informationen:**	**Anwählbar…**
Nachricht	Hier wird der Inhalt der Nachricht genau so dargestellt, wie er im Nachrichtenfenster ausgefüllt wurde. Damit haben Sender und Empfänger innerhalb von eGo-Mail die Gewähr, die Inhalte in derselben Weise angezeigt zu bekommen.	…in jedem Postkorb
Visitenkarte	Hier sehen Sie die Visitenkarte der markierten Nachricht, d.h. Informationen zum Empfänger bzw. Absender.	… in "Posteingang" und Gesendete Nachrichten
Anhänge	Das Registerblatt zeigt die Dateinamen der Anhänge einer erstellten, versendeten oder empfangenen Nachricht. Mit einem Doppelklick können die Anhänge geöffnet werden.	…in jedem Postkorb
Inhaltsdaten	In diesem Registerblatt werden die Dateien angezeigt, die über die Funktion "Signieren" signiert werden. Es handelt sich hierbei um den "eigentlichen" Inhalt der Nachricht.	…im Postkorb "Postausgang"
Sendeprotokoll	Das Registerblatt stellt das Sendeprotokoll dar. Die darin enthaltenen Angaben wurden während des Sendevorgangs vom Intermediär an den Absender zurückgeschickt und enthalten u.a. den genauen Zeitpunkt des Nachrichteneingangs beim Intermediär sowie das Ergebnis der Prüfung des Signaturzertifikats.	…im Postkorb "Gesendete Nachrichten"

Registerblatt	**Bereitgestellte Informationen:**	**Anwählbar…**
Eingangsbe-stätigung	Hier sehen Sie die Angaben, die während des Sendevorgangs vom Intermediär an den Absender zurückgeschickt wurden. Enthalten ist u.a. den genauen Zeitpunkt des Nachrichteneingangs beim Intermediär.	…im Postkorb "Gesendete Nachrichten"
Prüfprotokoll	Dieses Registerblatt stellt das Prüfprotokoll dar. Dieses wurde zusammen mit der eigentlichen Nachricht empfangen und enthält das Ergebnis der Signatur- und Signaturzertifikatsprüfung durch den Intermediär.	…im Postkorb "Posteingang"
Zertifikate	Hier sehen Sie eine Übersicht der mit der Nachricht empfangenen oder gesendeten Zertifikate. Hinweis: Über die rechte Maus-Taste kann jedes Zertifikat, nachdem es markiert wurde, online nachträglich hinsichtlich des Status bei der zugrunde liegenden ZDA verifiziert werden.	…in jedem Postkorb

8 NUTZERSPEZIFISCHE EINSTELLUNG IM POSTFACH

Zur effektiven Nutzung des Postfaches stehen verschiedene Funktionen zur Verfügung, mit denen Sie Ihre eGo-Mail Anwendung entsprechend Ihres persönlichen Bedarfs konfigurieren können. Diese Funktionen können über die Menüpunkte "Optionen" und "Extras" aufgerufen werden und werden im Folgenden kurz beschrieben.

8.1 Allgemeine Funktionen des Menüs "Optionen"

8.1.1 E-Mailbenachrichtigung

Bei Auswahl dieser Option öffnet sich ein Fenster in dem festgelegt werden kann, ob eine Benachrichtigung per E-Mail stattfinden soll, wenn eine Nachricht (auf dem Intermediär) eingegangen ist. Durch Aktivierung der Check-Box und der Eintragung einer korrekten E-Mailadresse in das Eingabefeld wird die Funktion aktiviert. Sollen mehrere Empfänger benachrichtigt werden, muss eine E-Mailsammeladresse eingerichtet und hier eingegeben werden.

8.1.2 Automatisiertes Empfangen

Bei Auswahl dieser Option öffnet sich das Fenster "Automatisiertes Empfangen". In diesem Fenster besteht die Möglichkeit ein Intervall (in Minuten) anzugeben, in dem die Nachrichten, die im Postfach auf dem Intermediär liegen, automatisch abgeholt werden sollen.

Die Nachrichten und Anhänge selbst bleiben im Archivordner gespeichert. Der Zeitraum muss mindestens 30 Tage betragen.

8.2 Allgemeine Funktionen des Menüs "Extras"

8.2.1 Lesegerät suchen

Diese Funktion ermöglicht Ihnen das erneute Suchen des an dem PC angeschlossenen Kartenlesers. Diese Option sollten Sie immer dann auswählen, wenn die Anwendung den Kartenleser nicht ansprechen/finden kann. Dies ist zum Beispiel der Fall, wenn Sie eine Nachricht signieren möchten und das Signatur-PIN-Eingabe-Fenster nicht erscheint. Sollten Sie diese Funktion nutzen, müssen Sie anschließend die Anwendung neu starten.

8.2.2 Adressbuch

Bei Auswahl dieser Option öffnet sich das Fenster "Adressbuch". Dieses Fenster dient dazu, aus den gespeicherten Visitenkarten einen Empfänger auszuwählen. Im Adressbuch finden Sie alle Personen und Institutionen, mit denen ein Nachrichtenaustausch mit eGo-Mail möglich ist. Das Adressbuch bietet die Möglichkeit, über die obere Fensterhälfte Empfänger nach Name, Organisation oder Ort zu suchen. Die Suchergebnisse werden in der unteren Fensterhälfte als gefundene Adressen dargestellt. Wenn Sie keine Sucheinschränkungen aktiviert haben, zeigt Ihnen das Adressbuch alle Einträge an.

8.2.3 Zertifikat Erzeugen

Bei Auswahl dieser Option öffnet sich das Fenster "Zertifikat Erzeugen". Diese Funktion steht zur Verfügung um sich ein neues Zertifikat zu erzeugen.

9 INFORMATIONEN ZUM POSTFACH

Informationen über das Postfach sind abrufbar unter den Menüpunkten "Server" und "?".

9.1 Menüpunkt Server

Bei Aufruf des Menüpunkts "Server" können Sie zwischen Informationen zum Intermediär, zum Verzeichnisdienst und zum Verifikationsserver wählen.

9.1.1 OSCI Manager (Intermediär)

Bei Auswahl dieser Option werden Informationen über den Intermediär der Anwendung dargestellt:

- URL: Nennt die Internetadresse (URL), unter der der Intermediär betrieben wird.
- CA Zertifikat: Zeigt das CA-Zertifikat des öffentlichen Schlüssel des Intermediärs.

9.1.2 Verzeichnisdienst

Bei Auswahl dieser Option werden Informationen über den Verzeichnisdienst der Anwendung dargestellt:

- Benutzer ID: Nennt die eindeutige ID unter der das ausgewählte Postfach beim Verzeichnisdienst registriert ist
- ZDA Zertifikat: Nennt die Internetadresse (URL) unter der der Verzeichnisdienst betrieben wird.

9.1.3 Verifikationsserver

Bei Auswahl dieser Option wird die Internetadresse (URL) des Verifikationsserver angezeigt.

9.2 Hilfe (?)

Mit Auswahl dieser Option starten Sie die Hilfefunktion, hier erhalten Sie weitere Informationen zu diesem Fenster oder zur gesamten Anwendung.

10 NACHRICHTEN ERSTELLEN UND VERARBEITEN

Für das Erstellen einer neuen Nachricht klicken Sie bitte im Verwaltungsfenster auf den Button Neu oder wählen Sie den Menüpunkt „Nachricht“ – „Neu“. Es öffnet sich das Nachrichtenfenster

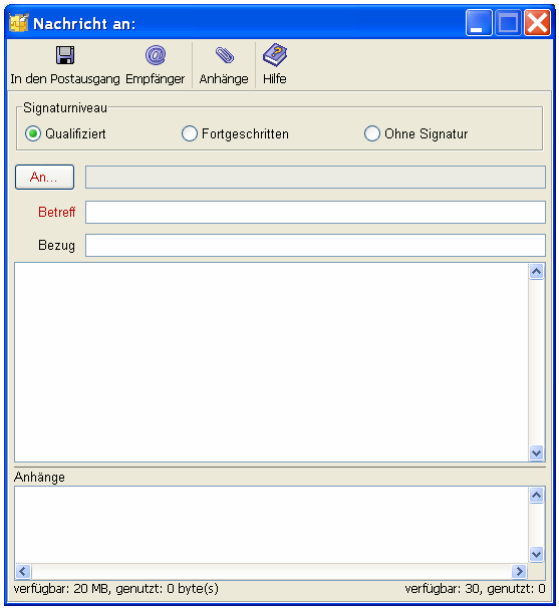

Abbildung 15: Nachrichtenfenster

10.1 Nachrichten erstellen

10.1.1 Empfänger auswählen

Im Nachrichtenfenster können Sie neue Nachrichten erstellen, Anhänge einfügen und im Postausgang speichern. Über die Befehle in der Menüleiste können Sie die fertig erstellte Nachricht im Postausgang zwischenspeichern, den Empfänger festlegen, Anhänge anfügen oder die Hilfe aufrufen. Das Signaturniveau ist auf qualifiziert festgelegt.

Über „An“ gelangen Sie zum Adressbuch.

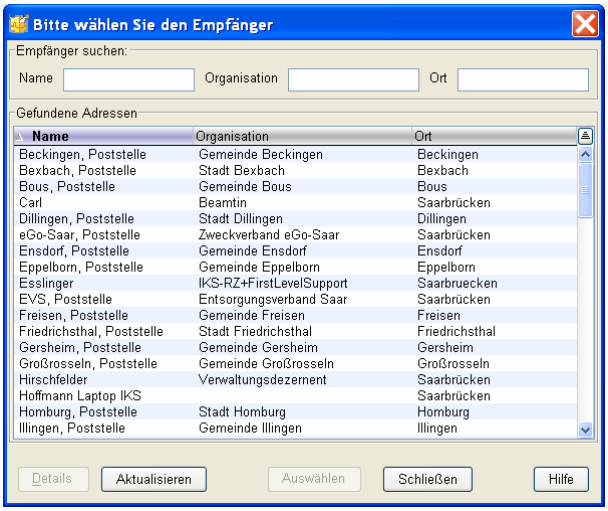

Abbildung 16: Adressbuch

Das Fenster „Adressbuch“ dient dazu einen Empfänger auszuwählen. Im Adressbuch werden Ihnen alle Behörden angezeigt, mit denen Sie über eGo-Mail kommunizieren können. In der oberen Fensterhälfte besteht die Möglichkeit einen Empfänger nach Name, Organisation oder Ort zu suchen. Die Suchergebnisse werden in der unteren Fensterhälfte als „Gefundene Adressen“ dargestellt. Ohne Sucheinschränkung werden hier alle gespeicherten Adressen aufgelistet.

Über die Auswahl des Buttons „Details“ erhalten Sie nähere Informationen zur zugehörigen Visitenkarte und zum Zertifikat des ausgewählten Adressaten.

Mit Hilfe des „Aktualisieren“ –Buttons besteht die Möglichkeit, das gesamte Adressbuch erneut von Verzeichnisdienst zu laden und den aktuellen Stand der möglichen Adressaten zu erhalten.

Markieren Sie den von Ihnen gewünschten Empfänger:

Nach Betätigen der Funktion „Auswählen“ gelangen Sie wieder ins Nachrichtenfenster.

10.1.2 Nachrichten verfassen und speichern

Über eGo-Mail können Sie nur dann Nachrichten versenden, wenn Sie die Nachricht mir einer qualifizierten Signatur versehen. Hierzu benötigen Sie eine gültige Signaturkarte, die mindestens der qualifizierten Signatur entspricht und einen Chipkartenleser.

Der „ Betreff“ im Nachrichtenfenster ist als Pflichtfeld gekennzeichnet. Hierdurch wird gewährleistet, dass immer ein eindeutiger Bezug zwischen der Nachricht und den einzelnen Protokollen hergestellt werden kann.

Für die eigentliche Nachricht steht Ihnen ein Freifeld zur Verfügung.

Ihre fertig erstellte Nachricht können Sie über das Disketten-Symbol in den Postausgang verschieben und dort zwischenspeichern

10.1.3 Anhänge versenden

Wenn Sie Dateianhänge versenden möchten, klicken Sie auf das Symbol in der Menüleiste. Es öffnet sich der Explorer und Sie können die gewünschten Anhänge aus Ihrem Dateisystem auswählen. Bitte beachten Sie hierbei, dass nicht alle Dateiformate zugelassen sind. Sie können insgesamt bis zu 30 Anhänge mit einer Nachricht versenden. Die Größe der Anhänge darf insgesamt 20 MB nicht überschreiten.

10.2 Nachricht verarbeiten

Im Postkorb „Postausgang“ stehen Ihnen folgende Möglichkeiten zur Verfügung die Nachricht zu bearbeiten und zu versenden:

10.2.1 Bearbeiten

Über diesen Button können Nachrichten, die sich im Postausgang befinden und noch nicht signiert wurden, erneut aufgerufen und bearbeitet werden. Sollen bereits signierte Nachrichtenerneut bearbeitet werden, müssen vorher alle Signaturen mit dem „Signatur-Entfernen“ - Button entfernt werden.

10.2.2 Signieren

Durch Auswahl der Funktion öffnet sich ein Anzeigefenster, das Sie zur Eingabe der PIN über den angeschlossenen Kartenleser auffordert. Nach Eingabe der PIN ist die Nachricht signiert. Bitte beachten Sie, dass die Nachricht vorab markiert

werden muss. Sollte der Kartenleser nicht angesprochen werden, können Sie über den Menüpunkt „Extras“ – „Lesegerät suchen“ ein erneutes Ansprechen des Kartenlesers veranlassen. Sollten Sie diese Funktion nutzen, müssen Sie anschließend die Anwendung neu starten. Bitte beachten Sie, dass jede Nachricht einzeln signiert werden muss.

10.2.3 Markierte Senden

Durch Auswahl der Option werden nur die im Postausgang markierten Nachrichten versendet.

10.2.4 Alle Senden

Durch Auswahl der Option werden alle Nachrichten im Postausgang versendet. Nach dem Versenden werden die Nachrichten sowie die zugehörigen Sendeprotokolle und Übermittlungsbelege im Postkorb „ Gesendete Nachrichten“ abgelegt. Die Nutzung der Funktionen „Markierte/Alle Senden“ setzt voraus, dass sich im Postausgang Nachrichten befinden, diese einzeln signiert wurden und eine aktive Internetverbindung besteht.

Die Funktionen Bearbeiten, „Signieren“, „Signatur Entfernen“, „Markierte Senden“ und „Alle Senden“ finden Sie auch unter dem Menüpunkt „Nachricht“.

11 POSTEINGÄNGE VERARBEITEN

11.1 Nachrichten empfangen

Durch Auswahl der Option „Empfangen“ werden alle beim Intermediär vorgehaltenen Nachrichten für das aktive Postfach abgerufen und in den Posteingang übertragen. Voraussetzung für diese Funktion ist eine aktive Internetverbindung.

Hinweis: Durch Auswahl der Funktion automatisiertes Empfangen werden eingehende Nachrichten automatisch im Posteingang abgelegt. Durch Hinterlegung einer E-Mailadresse im Fenster E-Mailbenachrichtigung werden Sie zudem über eingehende Nachrichten per Mail informiert.

Durch Auswahl der Option „Erneut Empfangen“ kann eine Nachricht wiederholt vom Server angefordert werden. Hierfür muss die Nachricht, die erneut empfangen werden soll, im Posteingang markiert werden. Diese Funktion kann dann zum Tragen kommen, wenn z.Bsp. die Prüfung über den „Prüfen“ - Button nicht erfolgreich war.

11.2 Signatur erneut prüfen

Wurde eine Nachricht übermittelt, deren Status auf dem Prüfprotokoll nicht eindeutig oder nicht ok ist, haben Sie folgende Möglichkeiten zur erneuten Prüfung:

- Über die rechte Mausetaste kann jedes Zertifikat, nachdem es im Reiter "Zertifikate" markiert wurde, online nachträglich hinsichtlich des Status beim zugrunde liegenden Trustcenter verifiziert werden. Bitte beachten Sie, dass eine bestehende Internetverbindung zwingende Voraussetzung für diese Option ist. Das Prüfergebnis wird angezeigt und kann abgespeichert und ausgedruckt werden. Eine nachträgliche Änderung der Prüfergebnisse in dem zur Nachricht zugehörigen Reiter "Prüfprotokoll" erfolgt nicht. Der Prüfzeitpunkt ist vorgesteuert. Sie können ihn wie

nachfolgend beschrieben ändern. Löschen Sie die Markierung in der Check-Box, danach können Sie über „Auswählen“ ein Datum und die Uhrzeit auswählen. Durch Auswahl des Buttons „Prüfen“ können Sie eine Signaturprüfung der im Verwaltungsfenster markierten Nachricht durchführen. Das Ergebnis wird in dem Fenster "Händische Signaturprüfung" dargestellt. Diese Menüfunktion hat dieselbe Funktion wie der Button "Prüfen" in der Buttonleiste des Verwaltungsfensters.

Die Funktionen Bearbeiten, „Empfangen“, und „Prüfen“ finden Sie auch unter dem Menüpunkt „Nachricht“.

12 GEMEINSAME FUNKTIONEN DER ORDNER POSTEINGANG UND GESENDETE OBJEKTE

12.1 Drucken

Durch Auswahl dieser Funktion können Sie eine vorher markierte Nachricht ausdrucken. Es öffnet sich ein Fenster, in dem Sie auswählen können, ob die Registerblätter, die Nachricht oder die Visitenkarte ausgedruckt werden sollen. Nach Anklicken des Buttons "OK" öffnet sich das Fenster zur Auswahl der Druckeroptionen, durch Anklicken des Buttons "Abbrechen" wird der Vorgang beendet. Durch Anklicken des Buttons "Hilfe" kann die Hilfe zur Druckoption oder anderen Funktionen der Anwendung aufgerufen werden.

12.2 Löschen

Durch Auswahl dieser Funktion können Sie vorher markierte Nachrichten löschen. Bevor Sie eine Nachricht endgültig löschen, müssen Sie den Löschvorgang im sich daraufhin öffnenden Fenster durch Anklicken des Button "Ja" bestätigen. Soll die die Nachricht nicht gelöscht werden, können Sie den Vorgang abbrechen, indem Sie auf den Button "Nein" klicken.

12.3 Senden an E-Mail-Empfänger

Wenn Sie eine Nachricht markiert haben, können Sie über das Kontextmenü diese Funktion aufrufen. Die Nachricht wird dann an Ihr E-Mail-Programm übergeben und kann an einen beliebigen Empfänger versandt werden.

13 PROTOKOLLE

Beim Empfang oder beim Versand von Nachrichten werden verschiedene Protokolle erzeugt. Die zu einer Nachricht gehörenden Protokolle werden auf den entsprechenden Registerblättern im unteren Bereich der Anwendungsoberfläche dargestellt, sofern die Nachricht im Nachrichtenbereich zuvor ausgewählt wurde. Bitte beachten Sie, dass je nachdem, welcher Postkorb gerade aktiv ist, nur bestimmte Registerblätter auswählbar sind. Im Folgenden werden die drei möglichen Protokolle kurz beschrieben.

13.1 Sendeprotokoll

Dieses Registerblatt ist nur im Postkorb "Gesendete Nachrichten" anwählbar. Das Sendeprotokoll enthält Angaben zum Absender und Unterzeichner, Informationen zum verwendeten Zertifikat sowie eine Aufzählung der mit der Nachricht übermittelten Anlagen.

13.2 Eingangsbestätigung.

Dieses Registerblatt ist nur im Postkorb "Gesendete Nachrichten" anwählbar. Die darin enthaltenen Angaben wurden während des Sendevorgangs vom Intermediär an den Absender zurückgeschickt und enthalten u. a. den genauen Zeitpunkt des Nachrichteneingangs beim Intermediär.

13.3 Prüfprotokoll

Dieses Registerblatt ist nur im Postkorb "Posteingang" anwählbar. Dieses wurde zusammen mit der eigentlichen Nachricht empfangen und enthält das Ergebnis der Signatur- und Signaturzertifikatsprüfung durch den Intermediär.

13.3.1 Arten von Prüfungen

Der Intermediär kann verschiedene Prüfungen durchführen, um dem Empfänger einer elektronisch signierten Nachricht eine Handlungsgrundlage zur weiteren Verarbeitung der Nachricht zu geben. Je nach Signaturniveau und Zertifizierungsdiensteanbieter werden alle oder einige dieser Prüfungen durchgeführt. Grundsätzlich ist zwischen einer Signaturprüfung einerseits und der Prüfung des für die Signatur verwendeten Zertifikats andererseits zu unterscheiden. Die Signaturprüfung findet stets lokal (d.h. auf dem Rechner des Empfängers) statt. Zertifikatsprüfungen erfolgen online, sofern das betreffende Trustcenter für diesen Zertifikatstyp eine Onlineprüfung anbietet.

13.3.1.1 KRYPTOGRAPHISCHE SIGNATURPRÜFUNG.

Bei der Erzeugung einer elektronischen Signatur wird der Hashwert (eine Art "Fingerabdruck") eines Dokuments von einem Signaturschlüsselinhaber signiert, d.h. mit bestimmten Daten verknüpft. Bei der Prüfung einer Signatur verfährt der Intermediär daher folgendermaßen: Zunächst wird der Hashwert des Dokuments neu berechnet; dieser wird anschließend mit dem vom Signaturschlüsselinhaber signierten Hashwert verglichen. Stimmen beide überein, so kann mit Sicherheit davon ausgegangen werden, dass das signierte Dokument nicht verändert wurde: die Integrität des Dokuments ist gewährleistet.

13.3.1.2 ZERTIFIKATSPRÜFUNG.

Die Prüfung des Signaturzertifikats wird durchgeführt um festzustellen, ob die Identität der unterschreibenden Person dem Herausgeber (= Trustcenter) bekannt ist und ob das Zertifikat nicht gesperrt wurde. Hier geht es also um die Prüfung der Authentizität der unterschreibenden Person. Dafür werden folgende Einzelprüfungen durchgeführt:

- Ist die Signatur des Herausgebers des Signaturzertifikats mathematisch korrekt?
- Ist das Herausgeberzertifikat gültig?

- Hat die unterzeichnende Person innerhalb des Gültigkeitszeitraumes ihres Signaturzertifikats signiert?
- Ist dem Trustcenter das verwendete Signaturzertifikat bekannt und ist es nicht gesperrt?

Für die Prüfung werden folgende Onlineprüfungen über das Trustcenter vom Intermediär unterstützt:

- OCSP-Prüfung: Bei der OCSP-Prüfung meldet das Trustcenter den Status des Zertifikats (gültig und nicht gesperrt, unbekannt oder gesperrt) zurück. Den Status "gesperrt" erhält ein Zertifikat z.B. dann, wenn der Inhaber seine Signaturkarte wegen Verlusts o.ä. hat sperren lassen.
- Bei der CRL-Prüfung wird geprüft, ob sich das Zertifikat in der aktuellen Sperrliste des Herausgebers befindet. In der Sperrliste wird ein Zertifikat z.B. dann geführt, wenn der Inhaber seine Signaturkarte wegen Verlusts o. ä. hat sperren lassen.
- Bei der LDAP-Prüfung wird geprüft, ob das Zertifikat beim Herausgeber bekannt ist.

Den Anforderungen des Signaturgesetzes an die Prüfung qualifizierter Zertifikate genügen lediglich die OCSP-Prüfung und die kombinierte CRL- und LDAP-Prüfung.

13.3.2 Abschnitte im Prüfprotokoll

Das Prüfprotokoll enthält die folgenden verschieden Abschnitte:

- Prüfergebnisse
- Nachrichteninhalt
- Einzelprüfergebnisse der Signaturen und Zertifikate
- Informationen über die unterzeichnende(n) Person(en)
- Prüfergebnisse im Detail und
- Anmerkungen.

13.3.2.1 PRÜFERGEBNISSE

Dies ist der wichtigste Abschnitt des Prüfprotokolls, denn er enthält die Zusammenfassung der Ergebnisse aller durchgeführten Prüfungen.

- Betreff: Der Betreff wird so angezeigt wie vom Autor bzw. Sender der Nachricht eingegeben. (in Realisierungsphase)
- Nachrichtenkennzeichen: Das Nachrichtenkennzeichen wird vom Intermediär vergeben und dient Ihnen auch im Nachhinein zur eindeutigen Bezugnahme auf die betreffende Nachricht.
- Eingang auf dem Server: Der Eingang auf dem Server bezeichnet den Zeitpunkt, zu dem der Eingang der Nachricht auf dem Server abgeschlossen wurde. Bei Nachrichten an die Behörde, welche eine bestimmte Fristenanforderung gestellt hat, kann hierüber der fristgerechte Eingang kontrolliert werden. Aus dem Eintrag geht hervor, ob es sich um die Serverzeit des Intermediärs oder einen Zeitstempel eines entsprechend akkreditierten Dienstleisters handelt.
- Prüfergebnis: Hier wird Ihnen der Status der Nachricht angezeigt. Folgende Ergebnisse sind möglich:
    - Status OK: Alle Prüfungen ergaben "gültig". Die Weiterverarbeitung ist bedenkenlos möglich.
    - Status nicht eindeutig: Mindestens eine Prüfung konnte nicht abschließend durchgeführt werden. Bitte prüfen Sie als Empfänger die Angaben im Abschnitt "Prüfergebnisse im Detail".
    - Status nicht OK: Mindestens eine Prüfung hatte das Ergebnis "ungültig" zur Folge. Damit ist die Nachricht nicht rechtsverbindlich.

13.3.2.2 NACHRICHTENINHALT

Hier wird der gesamte Nachrichteninhalt nach Abschnitten gegliedert dargestellt. Zu jedem Abschnitt, der eine Signatur enthält, wird zusätzlich der Name des

Inhabers des Signaturzertifikats (z.Bsp. "signiert durch Max Mustermann") angezeigt. Sollte ein Nachrichtenabschnitt mehrfach signiert worden sein, so wird zu jeder Signatur der Name des Inhabers des Signaturzertifikats angezeigt.

13.3.2.3 Einzelprüfergebnisse der Signaturen und Zertifikate

Hier befindet sich zu jeder in der Nachricht enthaltenen Signatur ein Gesamtergebnis (Ergebnis der kryptographischen Signaturprüfung kombiniert mit der Zertifikatsprüfung).

13.3.2.4 Informationen über die unterzeichnende Person

Diesem Abschnitt können Sie alle vorhandenen Informationen über den oder die Unterzeichner der Nachricht entnehmen.

13.3.2.5 Prüfergebnisse im Detail

Hier werden Ihnen alle Prüfergebnisse aufgeführt. Insbesondere, wenn der Gesamtstatus der Nachricht "nicht eindeutig" oder "nicht o. k." ist, finden sich hier hilfreiche weiterführende Informationen, die nach jeder in der Nachricht enthaltenen Signatur gegliedert sind:

- Kryptographische Signaturprüfung: Mögliche Zustände sind "gültig" oder "ungültig". Der Status "ungültig" zeigt an, dass die Nachricht mit hoher Wahrscheinlichkeit von einem unbefugten Dritten verändert wurde.
- Prüfzeitpunkt: Der Prüfzeitpunkt ist der Zeitpunkt der Signaturerstellung durch den Unterzeichnenden (vorgeschrieben für die Prüfung qualifizierte Signaturzertifikate). Kann der Zeitpunkt nicht ermittelt werden, wird Hilfsweise die Systemzeit des Servers, der die Prüfung durchführt, verwendet.
- Zeitpunkt der Anbringung der Signatur: Dies ist der Zeitpunkt der Signaturerstellung durch den Unterzeichnenden

- Durchgeführtes Prüfverfahren: Die lokalen Prüfungen werden immer durchgeführt. Anschließend erfolgt die Onlineprüfung des Signaturzertifikats, falls das betreffende Trustcenter für diesen Zertifikatstyp eine Onlineprüfung anbietet. Folgende Prüfverfahren werden vom Intermediär unterstützt:
    - Bei der OCSP-Prüfung meldet das Trustcenter den Status des Zertifikats (gültig und nicht gesperrt, unbekannt oder gesperrt) zurück.
    - Bei der CRL-Prüfung wird geprüft, ob sich das Zertifikat in der aktuellen Sperrliste des Herausgebers befindet.
    - Bei der LDAP-Prüfung wird geprüft, ob das Zertifikat beim Herausgeber bekannt ist.
- Gültigkeitsmodell: Hier wird aufgeführt, nach welchem Gültigkeitsmodell das Zertifikat überprüft wurde. Mögliche Gültigkeitsmodelle neben dem Gültigkeitsmodell nach ISIS-MTT sind Schalen- oder Kettenmodell.
- Signaturzertifikat der unterzeichnenden Person: Hier wird der Status des Zertifikats gemäß dem durchgeführten Prüfverfahren (s. o.) aufgeführt. Mögliche Ergebnisse sind:
    - OK: Das Zertifikat ist dem Herausgeber bekannt und gültig.
    - Widerrufen: Das Zertifikat wurde widerrufen.
    - Prüfung konnte nicht abschließend durchgeführt werden:
    - Die Prüfung hat kein eindeutiges Ergebnis gebracht. Mögliche Gründe sind die Nichterreichbarkeit des Herausgebers, Netzwerkverbindungen etc.

GLOSSAR

Akkreditierung

Der Begriff Akkreditierung wird in verschiedenen Bereichen benutzt, um den Umstand zu beschreiben, dass eine allgemein anerkannte Instanz einer anderen Instanz das Erfüllen einer besonderen (nützlichen) Eigenschaft bescheinigt.

asymmetrische Verschlüsselung

Kommen zur Steuerung von Ver- und Entschlüsselung unterschiedliche Schlüssel zum Einsatz, so spricht man von asymmetrischer Verschlüsselung (auch Public Key Verfahren genannt). Mit einem geeigneten Verfahren wird ein Paar asymmetrischer Schlüssel (Private Key / privater Schlüssel, Public Key / öffentlicher Schlüssel) generiert. Die besondere Eigenschaft dieser Schlüssel ist es, dass mit dem einen Schlüssel entschlüsselt werden kann, was mit dem anderen Schlüssel verschlüsselt wurde. Nur die Schlüssel aus dem generierten Paar gestatten im Zusammenspiel die Ver- und Entschlüsselung.

Einer der Schlüssel aus dem Paar verbleibt beim Absender einer Nachricht (privater Schlüssel), der andere wird dem Empfänger zur Verfügung gestellt (öffentlicher Schlüssel). Diese Schritte werden von jedem Kommunikationsteilnehmer vollzogen, so dass alle am Ende über ein Unikat ihres privaten Schlüssels und über Kopien der öffentlichen Schlüssel der anderen verfügen.

Authentizität

Unter Authentizität wird die Echtheit von Informationen und Daten verstanden. Im Falle der digitalen Verschlüsselung heißt dies, dass der Absender eindeutig identifiziert werden kann. Authentizität ist eine der zentralen Sicherheitsanforderungen neben Verfügbarkeit, Integrität, Vertraulichkeit und Nichtabstreitbarkeit, welche für sichere Interaktionen erfüllt sein müssen.

Autorisierung

Autorisierung ist die Einräumung von Rechten gegenüber Dritten. Es beantwortet die Frage, wer wozu berechtigt ist. In der Informationstechnologie bezeichnet sie die Zuweisung und Überprüfung von Zugriffsrechten auf Daten und Diensten an Systemnutzer. Die Autorisierung erfolgt meist nach einer erfolgreichen Authentifizierung.

Die zwei häufigsten Spezialfälle sind:

der erlaubte Zugriff auf so genannte Ressourcen (z.B. auf Verzeichnisse oder Dateien) in einem Computernetzwerk.

die Erlaubnis zur Installation oder Benutzung von technisch geschützten Computerprogrammen (Software).

Behörde

Eine Behörde ist eine relativ selbständige Dienststelle im Verwaltungsaufbau des Staates und öffentlicher Körperschaften mit der Befugnis, die Verwaltungsaufgaben des Behördenträgers (Bund, Land, Gemeinde) im Rahmen ihrer Zuständigkeit selbständig nach außen wahrzunehmen. Alle Behörden des Bundes und der Länder sind nach Artikel 35 Grundgesetz (GG) zu gegenseitiger Rechts- und Amtshilfe verpflichtet.

Certification Authority (CA)

Eine Certification Authority (CA) ist eine vertrauenswürdige Institution, die öffentliche Schlüssel beglaubigt, also digitale Zertifikate ausstellt. Dazu werden die darin enthaltenen Informationen, insbesondere die Identität des Schlüsselinhabers, überprüft.

CRL

CRL steht für Certificate Revocation List, siehe Zertifikatsperrliste.

Elektronische (digitale) Signatur

Die elektronische Signatur kann als das elektronische Äquivalent zur eigenhändigen Unterschrift angesehen werden.

Fachverfahren

Behörden erbringen Dienstleistungen gegenüber Bürgern, Firmen oder anderen Behörden. Für die Unterstützung dieser Dienstleistungen bieten Hersteller fachspezifische Programme an, so genannte Fachverfahren.

Integrität

Unter Integrität wird die Unversehrtheit von Informationen und Daten verstanden. Im Falle der digitalen Verschlüsselung heißt dies, dass die Daten beim Übertragungsvorgang nicht verändert wurden.

Integrität ist eine der zentralen Sicherheitsanforderungen neben Verfügbarkeit, Authentizität, Vertraulichkeit und Nichtabstreitbarkeit, welche für sichere Interaktionen erfüllt sein müssen.

Intermediär

Intermediär, zwischen zwei Dingen befindlich, in der Mitte liegend; vermittelnd.

In OSCI-Transport kommunizieren zwei Kommunikationspartner (so genannte OSCI-Benutzer, wobei hier Computersysteme bzw. Softwarekomponenten und nicht menschliche Benutzer gemeint sind) niemals direkt, sondern stets über eine Vermittlungsstelle, den so genannten OSCI-Intermediär. Hauptaufgabe dieses Intermediärs ist es, als Vermittlungsstelle, die beiden Kommunikationspartner jeweils getrennt bekannt ist und der sie jeweils einzeln direkt vertrauen, eine indirekte Vertrauensbeziehung zwischen den sich nicht notwendigerweise gegenseitig bekannten Kommunikationspartnern herzustellen.

Der Intermediär ist gemäß Spezifikation eine Rolle, die systemtechnisch auf unterschiedliche Weise umgesetzt werden kann. Die Rolle kann zum Beispiel übernommen werden von einem dem Fachverfahren direkt vorgeschalteten Intermediärs-Modul, von einem freistehenden Intermediärs-Server innerhalb der Kommune oder von einem Intermediärs-Server, der von einem Drittanbieter betrieben wird.

Zu den technischen Aufgaben des Intermediärs gehören insbesondere die Zertifikatsprüfung, die Aufbewahrung von Laufzetteln sowie zahlreiche andere Prüfungen, die die korrekte Durchführung des Protokolls sichern.

Geht eine Nachricht beim Intermediär ein, so gilt sie als rechtsverbindlich zugestellt.

LDAP

LDAP ist die Abkürzung von Lightweight Directory Access Protocol, einem Netzwerkprotokoll, das für den Zugriff (Abfrage und Modifikation) auf Informationssammlungen entwickelt wurde. In solchen Informationssammlungen bzw. Verzeichnissen werden Daten zentral gespeichert, so muss nicht ein ganzes Netzwerk nach Daten durchsucht werden. Das LDAP ist in einer Baumstruktur organisiert.

Nichtabstreitbarkeit

Unter Nichtabstreitbarkeit wird die Gewährleistung verstanden, dass der Versand und der Empfang von Daten und Informationen nicht in Abrede gestellt werden kann. Nichtabstreitbarkeit ist eine der zentralen Sicherheitsanforderungen neben Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit, welche für sichere Interaktionen erfüllt sein müssen.

OCSP

Das Online Certificate Status Protocol (OCSP) ist ein Internet-Protokoll, das es Clients ermöglicht, den Status von X.509-Zertifikaten abzufragen.

OSCI

OSCI (engl. für Online Services Computer Interface) ist der Name eines Protokollstandards für die deutsche Kommunalwirtschaft: Er steht für eine Menge von Protokollen, deren gemeinsames Merkmal die besondere Eignung für das E-Government ist. Die sichere und vertrauliche Übertragung digital signierter Dokumente über das Internet. Dies ist beschrieben in OSCI-Transport.

Die Standardisierung von Inhaltsdaten, damit strukturierte Dokumente medienbruchfrei und effizient verarbeitet werden können. Hier gibt es mehrere Projekte, z.B. das Datenaustauschformat OSCI-XMeld für Geschäftsvorfälle des Meldewesens.

OSCI-Empfänger

Der Empfänger kennzeichnet die Rolle innerhalb einer OSCI-Transport-Kommunikation, die eine Nachricht vom Sender (über den Intermediär) entgegen nimmt. Für die technische Abwicklung ist der Rolle ein Softwaresystem (i.d.R. ein Server) zugeordnet. Dieses System kann das Meldefachverfahren, die Implementierung der Clearingstelle oder ein vorverarbeitendes Schnittstellensystem sein – je nach gewählter Lösungsarchitektur.

OSCI-Transport

Ein Protokollstandard zur vertraulichen und sicheren Übermittlung von Nachrichten in einer auf das deutsche Signaturgesetz abgestimmten Sicherheitsumgebung. OSCI ist vor allem in Hinblick auf Kommunikationsanforderungen im E-Government zugeschnitten. OSCI-Transport ist im Rahmen der Initiative BundOnline 2005 als obligatorischer Standard festgelegt.

OSCI-Transport Nachrichten haben einen zweistufigen “Sicherheitscontainer”. Dadurch ist es möglich, Inhalts- und Nutzungsdaten streng voneinander zu trennen und kryptografisch unterschiedlich zu behandeln. Die Inhaltsdaten werden vom Autor einer OSCI-Transport-Nachricht so verschlüsselt, dass nur der berechtigte Leser sie dechiffrieren kann. Die Nutzungsdaten werden vom Intermediär für die Zwecke der Nachrichtenvermittlung und die Erbringung der Mehrwertdienste benötigt, sie werden deshalb für den Intermediär verschlüsselt. Ein Angreifer kann wegen dieser Verschlüsselungen weder die Nutzungs-, noch die Inhaltsdaten einsehen.

Jeder Sicherheitscontainer (für Nutzdaten und Inhaltsdaten) erlaubt die digitale Signatur und die Verschlüsselung des jeweiligen Inhalts. Dadurch sind Vertraulichkeit, Integrität und Authentizität der Nachrichten gewährleistet.

Provider

Provider sind Institutionen, die zur Realisierung von Onlinediensten notwendige Infrastruktursysteme betreiben.

Register

Ein Verzeichnis (oder Register) ist eine übersichtliche, meist nach bestimmten Strukturen gegliederte, Listen-Anordnung von Informationen. Beispiele sind das Inhaltsverzeichnis, das Handelsregister, der Kataster, das Schiffsregister, die Telefonverzeichnisse und andere Arten von alphabetischen Verzeichnissen und Listen.

Vertraulichkeit

Unter Vertraulichkeit wird die Gewährleistung verstanden, dass ausschließlich Berechtigte auf Daten und Informationen zugreifen können und dass außerdem nur Berechtigte das Wissen darüber besitzen, ob Nachrichten etc. ausgetauscht wurden.

Vertraulichkeit ist eine der zentralen Sicherheitsanforderungen neben Verfügbarkeit, Integrität, Authentizität und Nichtabstreitbarkeit, welche für sichere Interaktionen erfüllt sein müssen.

XML

Die Extensible Markup Language (engl. für „erweiterbare Auszeichnungs-Sprache“), abgekürzt XML, ist ein Standard zur Erstellung maschinen- und menschen-lesbarer Dokumente in Form einer Baumstruktur, der vom World Wide Web Consortium (W3C) definiert wird. XML definiert dabei die Regeln für den Aufbau solcher Dokumente. Für einen konkreten Anwendungsfall ("XML-Anwendung") müssen die Details der jeweiligen Dokumente spezifiziert werden. Dies betrifft insbesondere die Festlegung der Strukturelemente und ihre Anordnung innerhalb des Dokumentenbaums.

Zeitstempel

Elektronische Bescheinigung einer (vertrauenswürdigen) Stelle, dass bestimmte elektronische Daten zu einem bestimmten Zeitpunkt vorgelegen haben. Es ist dabei im Allgemeinen. nicht erforderlich, dass diese Stelle den Inhalt der Daten zur Kenntnis nimmt.

Zertifikat

Digitale Zertifikate können als Pendant eines Ausweises betrachtet werden und bestätigen die Zugehörigkeit eines kryptografischen Schlüssels zu einer Person / Firma / Institution (z.B. bei der Verschlüsselung von Dateien oder E-Mails), einer Maschine (z.B. bei der SSL-Verschlüsselung). Dadurch können Authentizität, Vertraulichkeit und Integrität von Daten gegenüber Dritten garantiert werden.

Ein Zertifikat enthält Informationen über den Namen des Inhabers, dessen öffentlichen Schlüssel, eine Seriennummer, eine Gültigkeitsdauer und den Namen der Zertifizierungsstelle. Diese Daten sind in der Regel mit dem privaten Schlüssel der Zertifizierungsstelle signiert und können somit mit dem öffentlichen Schlüssel der Zertifizierungsstelle überprüft werden. Zertifikate für Schlüssel, die nicht mehr sicher sind, können über eine so genannte Certificate Revocation List (Zertifikatssperrliste) gesperrt werden.

ERROR: syntaxerror
OFFENDING COMMAND: --nostringval--

STACK:

/Title
()
/Subject
(D:20070116143420)
/ModDate
()
/Keywords
(PDFCreator Version 0.8.0)
/Creator
(D:20070116143420)
/CreationDate
(carlapt)
/Author
-mark-