



Dokumentation

e.sig - Serverbasierte PDF Signatur mit Zustellung

Neue Ziel- und Anwendungsgruppen

Version 1.0, 16. Jänner 2008

DI Thomas Knall – thomas.knall@egiz.gv.at

Zusammenfassung: Im Rahmen des Projekts "E-Government-Anwendungen im Schulbereich" wurde eine Web-Anwendung erstellt, die authentifizierten Benutzern ermöglicht, PDF-Dokumente mit einer serverbasierten Signatur zu versehen, die signierten Dokumente im Anschluss herunterzuladen oder mittels E-Mail bzw. Elektronischer Zustellung zu versenden. Diese Web-Anwendung wird in diesem Dokument in einer generalisierten Version dokumentiert.

Inhaltsverzeichnis:

Abbildungsverzeichnis.....	2
Revision History.....	3
1 Einleitung	4
1.1 Schlüsselwörter	4
1.2 Geschlechtsspezifische Bezeichnungen	4
1.3 Motivation	4
2 Kurzbeschreibung	5
2.1 Systembeschreibung	5
2.2 Voraussetzungen zur Nutzung der Anwendung	10
3 Anwendungsbeschreibung	11
3.1 Authentifizierung	11
3.2 Signatur und Versand von PDF-Dokumenten	13
4 Administration	24
4.1 Allgemeine Informationen	25
4.2 PDF-AS Profile eintragen	27
4.3 MOA-ZS Profile eintragen	29
4.4 Organisation eintragen	30
4.5 Benutzerkonten verwalten	33
5 Deployment.....	36
5.1 Systemanforderungen	36
5.2 Installation	37
5.3 Konfiguration	41
5.4 Neue Organisation registrieren	47
6 Auslieferung	50
6.1 Struktur	50
Anhang	51
Referenzen	60

Abbildungsverzeichnis

Abb. 2.1: Trennung der Signatur-Anwendung von der Administrations-Komponente	5
Abb. 2.2: Systemüberblick.....	6
Abb. 2.3: Datenbank.....	10
Abb. 3.1: Authentisierung mit Bürgerkarte	11
Abb. 3.2: Eingabe des Karten-PINs zum Auslesen der Personenbindung	12
Abb. 3.3: Signatur der Anmeldedaten	12
Abb. 3.4: Startseite der Signatur-Anwendung	13
Abb. 3.5: Hinweis auf fehlende/fehlerhafte Eingaben	14
Abb. 3.6: Auswahl eines Signaturprofils	14
Abb. 3.7: Signatur und Versand mit Elektronischer Zustellung.....	15
Abb. 3.8: Empfänger ist nicht bei einem Zustelldienst registriert	16
Abb. 3.9: Signiertes Dokument erfolgreich an MOA-ZS übergeben	16
Abb. 3.10: MOA-ZS Benachrichtigung über den Status der Zustellung.....	17
Abb. 3.11: Verständigung des Empfängers über eine elektronische Zustellung	17
Abb. 3.12: Zustellnachweis im Falle einer RSa-Zustellung.....	18
Abb. 3.13: Abfrage des Zustellstatus mittels MOA-ZS Proxy.....	19
Abb. 3.14: Zustellstück wurde abgeholt (und gilt damit als zugestellt)	19
Abb. 3.15: Signatur und Versand per E-Mail.....	20
Abb. 3.16: signiertes Dokument per E-Mail versandt.....	21
Abb. 3.17: signiertes Dokument via E-Mail	21
Abb. 3.18: Signatur und Download.....	22
Abb. 3.19: Download eines signierten Dokuments	23
Abb. 4.1: Basic-Authentication	24
Abb. 4.2: Startseite der Administrationskomponente	25
Abb. 4.3: Anzeige der zur Signatur berechtigten Benutzer	26
Abb. 4.4: neues PDF-AS Profil registrieren.....	27
Abb. 4.5: registrierte PDF-AS Profile anzeigen	28
Abb. 4.6: neues MOA-ZS Profil registrieren	29
Abb. 4.7: registrierte MOA-ZS Profile anzeigen	30
Abb. 4.8: neue Organisation registrieren.....	31
Abb. 4.9: registrierte Organisationen anzeigen	32
Abb. 4.10: neuen Benutzer registrieren.....	33
Abb. 4.11: Anzeige der neu registrierten (und noch nicht freigeschalteten) Benutzerkonten	34
Abb. 4.12: Aktivierungs-Mail.....	34
Abb. 5.1: Systemübersicht des vorkonfigurierten Gesamtpakets	38

Revision History

Version	Datum	Autor(en)	
0.1	19.12.2007	T. Knall	erster Entwurf, Struktur des Deliverables
0.2	02.01.2008	T. Knall	Screenshots, Systembeschreibung
0.3	03.01.2008	T. Knall	Anwendungsbeschreibung
0.4	04.01.2008	T. Knall	Anwendungsbeschreibung
0.5	07.01.2008	T. Knall	Administration, Systemanforderungen
0.6	08.01.2008	T. Knall	Deployment, Konfiguration
0.7	09.01.2008	T. Knall	Gesamtpaket, Übersicht
0.8	10.01.2008	T. Knall	Konfiguration, Anhang
0.9	15.01.2008	T. Knall	Datenerhebungsblatt, Überarbeitung
1.0	16.01.2008	T. Knall	finale Überarbeitung

1 Einleitung

1.1 Schlüsselwörter

Dieses Dokument verwendet die Schlüsselwörter MUSS, DARF NICHT, ERFORDERLICH, SOLLTE, SOLLTE NICHT, EMPFOHLEN, DARF und OPTIONAL zur Kategorisierung der Anforderungen. Diese Schlüsselwörter sind analog zu ihren englischsprachigen Entsprechungen MUST, MUST NOT, REQUIRED, SHOULD, SHOULD NOT, RECOMMENDED, MAY und OPTIONAL zu handhaben, deren Interpretation in [KEYWORDS] festgelegt ist.

1.2 Geschlechtsspezifische Bezeichnungen

Alle Personenbezeichnungen, die in diesem Dokument in der männlichen Form verwendet werden, gelten sinngemäß auch für die weibliche Form.

1.3 Motivation

Mit der Komponente PDF-Signatur¹ und der Bürgerkarte² stehen dem Bürger Mittel zu Verfügung, PDF-Dokumente mit einer Signatur zu versehen. Für Unternehmen und Organisationen, die in der Regel zahlreiche Dokumente signieren, erweist sich diese Variante als weniger praktisch, da jede Signatur einzeln über eine Bürgerkarte ausgelöst werden muss. Für diesen Anwendungsfall bietet PDF-AS die Möglichkeit, serverbasierte Signaturen mittels MOA-SS (siehe auch Abschnitt 2.1.3) aufzubringen.

PDF-AS sieht jedoch keine Authentifizierung vor, was die Zuordnung signaturberechtigter Personen zu einzelnen hinterlegten Signaturzertifikaten erschwert. Speziell innerhalb von Organisationen bei denen verschiedene Signaturzertifikate zum Einsatz kommen, ist jedoch eine solche Zuordnung erforderlich.

Darüber hinaus bietet PDF-AS keine Möglichkeit, signierte Dokumente automatisch an bestimmte Empfänger weiterzuleiten, was im Falle von Rechnungen, Zeugnissen, Bestätigungen udgl. häufig nützlich wäre.

Die hier dokumentierte Anwendung "e.sig" erlaubt die Registrierung beliebiger Organisationen (z.B. Behörden oder Schulen), denen ein Sendeprofil³ sowie beliebig viele PDF-AS-Signaturprofile⁴ zugeordnet werden dürfen. Für jede registrierte Organisation können Benutzer eingetragen werden, die – nach erfolgreicher Authentifizierung mittels Bürgerkarte – im Namen ihrer Organisation Signaturen auslösen dürfen. Je nach gewählter Zustell-Art kann das signierte Dokument heruntergeladen werden, oder es wird per E-Mail oder via Elektronischer Zustellung an den angegebenen Empfänger versandt.

¹ siehe http://demo.egiz.gv.at/plain/projekte/signatur_im_e_government/pdf_signatur

² siehe <http://www.buergerkarte.at/>

³ Ein Sendeprofil für eine Elektronische Zustellung umfasst den Namen und die Anschrift einer Organisation. Die Organisation fungiert als Absender des jeweiligen Zustellstücks.

⁴ Ein PDF-AS-Profil umfasst neben dem Layout der Signaturmarke (Schrift, Hintergrund, Bildmarke, Position der Signaturmarke) auch jeweils ein MOA-SS-Profil. Ein MOA-SS-Profil ist direkt mit einem Signaturzertifikat verknüpft.

2 Kurzbeschreibung

Eine serverbasierte PDF-Signatur wurde im Rahmen eines Projekts zur Etablierung von E-Government-Strukturen im Schulbereich implementiert. Im konkreten Fall sollten Schulen die Möglichkeit haben, PDF-Dokumente (z.B. Zeugnisse, Elternbriefe etc.) serverbasiert mit ihren eigenen Signatur-Zertifikaten und eigenen Signatur-Profilen zu signieren und diese den jeweiligen Empfängern per E-Mail oder über eine Elektronische Zustellung zu übermitteln. Gleichzeitig sollte der Aufwand zur Nutzung der Signatur-Anwendung für einzelne Schulen minimiert werden.

Um die Anwendung über den Schulbereich hinaus nutzbar zu gestalten, wurde eine Generalisierung der Anwendung vorgenommen. Diese unterscheidet sich von der Anwendung für den Schulbereich hauptsächlich nur durch die verwendeten Texte.

Der zentralen Signatur-Anwendung ist eine MOA-ID-Authentifizierung mit Bürgerkarte vorgeschaltet. Personen, die zuvor über die Administrations-Komponente registriert und einer Organisation (Schule) zugeordnet wurden, erhalten Zugang zur Anwendung und können im Namen ihrer Organisation PDF-Dokumente signieren und versenden.

2.1 Systembeschreibung

Die Anwendung "e.sig" besteht aus drei Komponenten:

- Der e.sig-Signaturanwendung (jenem Teil, der als "Front-Office" dem Benutzer extern zugänglich ist),
- einem Kern, dem zentrale Aufgaben wie Verwaltung der Konfiguration, Datenbankzugriffe und Kommunikation mit externen Komponenten obliegen,
- sowie einer Administrations-Komponente ("Back-Office").

Die Trennung zwischen Front-Office und Back-Office erfolgte um die Back-Office-Komponente in einem geschützten Bereich (vorzugsweise dem Intranet) betreiben zu können, während das Front-Office innerhalb einer DMZ eingerichtet werden kann (siehe Abb. 2.1).

Warnung: Es muss auf geeignete Weise sichergestellt werden, dass nur berechtigte Benutzer (Administratoren) Zugriff auf die Administrationskomponente haben. Im Auslieferungszustand wird dies durch eine Basic-Authentication (Benutzername/Passwort) sichergestellt (siehe auch Abschnitt 5.3.1).

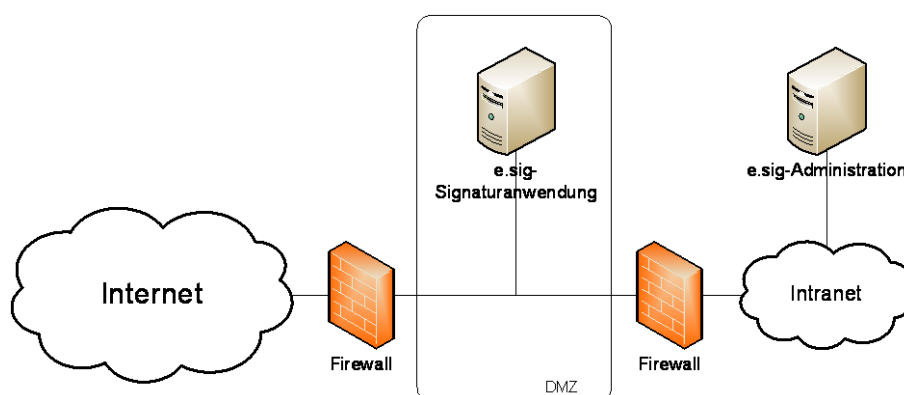


Abb. 2.1: Trennung der Signatur-Anwendung von der Administrations-Komponente

Die Anwendung setzt sich aus den in Abb. 2.2 gezeigten Komponenten zusammen.

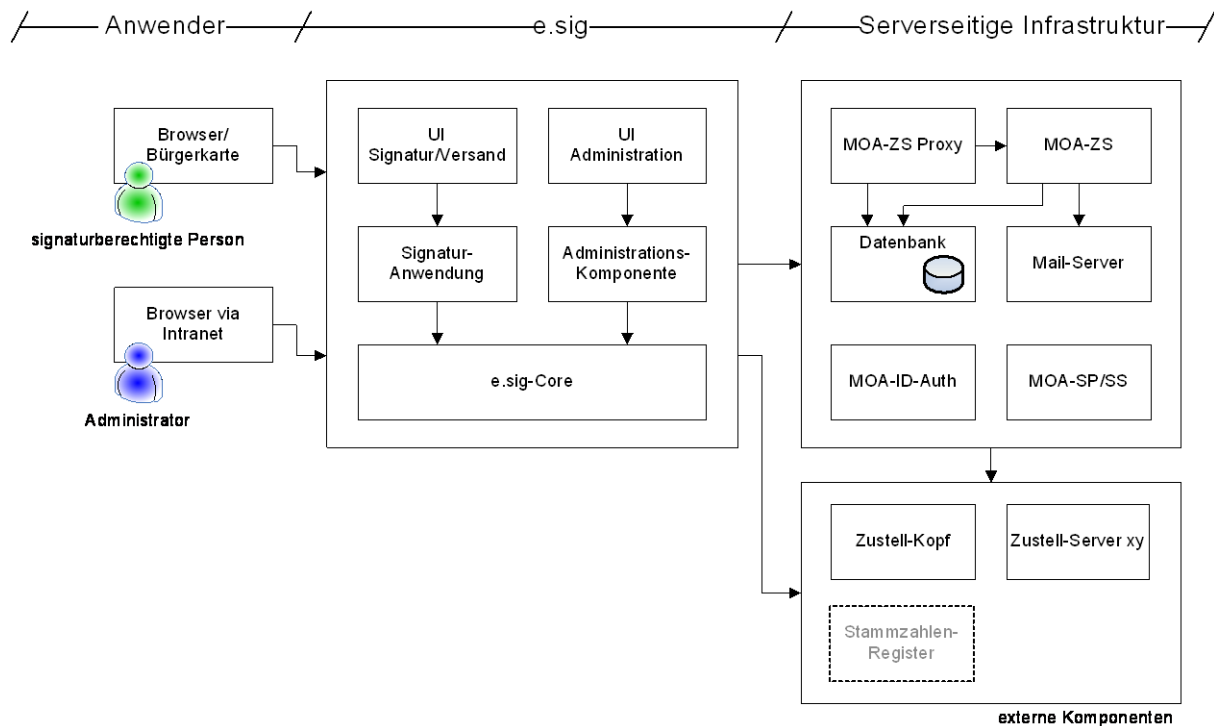


Abb. 2.2: Systemüberblick

Hinweis: Die Systembeschreibung eines vorkonfigurierten Gesamtpakets (siehe auch Abschnitt 5.2.2) ist aus Abb. 5.1 ersichtlich.

2.1.1 Benutzerschnittstellen

UI Signatur/Versand: Über diese (über das Internet erreichbare) Schnittstelle können authentifizierte (und berechnigte) Anwender die ihrer Organisation zugeordneten Signaturprofile benutzen um PDF-Dokumente zu signieren und im Anschluss bei Bedarf mittels Elektronischer Zustellung oder mittels E-Mail versenden.

UI Administration: Die Schnittstelle "Administration" ermöglicht das Eintragen von PDF-AS-Profilen, MOA-ZS-Profilen, Organisationen und Benutzern. Jeder Benutzer muss einer Organisation zugeordnet werden, jeder Organisation können beliebig viele Benutzer sowie beliebige PDF-AS-Profilen und ein MOA-ZS-Profil zugewiesen werden. Nach der Registrierung eines Benutzers wird an diesen automatisch eine Aktivierung-Mail versandt.

2.1.2 Applikation

Die Applikation setzt sich unter anderem aus folgenden Komponenten zusammen:

Signatur-Anwendung: Diese Komponente bietet eine grafische Benutzerschnittstelle für die Authentifikation von Benutzern sowie für den Upload, die Signatur und den Versand von PDF-Dokumenten

Administrations-Komponente: Die Administrations-Komponente beinhaltet eine grafische Benutzerschnittstelle zur Registrierung von Profilen, Organisationen und Benutzern. Die Komponente stellt wiederum nur die Schnittstelle zu Verfügung; die eigentliche Funktionalität wird vom Kern zu Verfügung gestellt.

Anwendungs-Kern: Der Anwendungskern übernimmt Aufgaben wie die Verwaltung der Konfiguration, sämtliche Datenbankzugriffe, die Kommunikation mit PDF-AS, MOA-ZS (bzw. dem MOA-ZS-Proxy) und dem Mail-Server.
Der Kern wird über API-Aufrufe verwendet und bietet demnach keine grafische Benutzerschnittstelle.

Die oben genannten Elemente greifen u.a. auf folgende Frameworks zurück:

Apache Axis⁵: Axis ist eine SOAP-Engine zur Konstruktion von SOAP-basierenden Web-Services. Der Anwendungskern verwendet Axis für die Kommunikation mit MOA-ZS bzw. dem MOA-ZS-Proxy, das Front-Office benutzt es zur Kommunikation mit MOA-ID und PDF-AS verwendet Axis für das Anbringen einer XML-Signatur mit MOA-SS.

Apache Log4J⁶: Log4J ist ein Framework für das Logging von Anwendungsmeldungen.

Apache Struts⁷: Struts ist ein Open-Source-Framework, das für die Präsentationsschicht und die Steuerungsschicht des Front- und Back-Office eingesetzt wird. Es dient hauptsächlich zur Trennung von Darstellung, Geschäftslogik und Datenmodell.

⁵ <http://ws.apache.org/axis/>

⁶ <http://logging.apache.org/log4j/>

⁷ <http://struts.apache.org/>

- Hibernate⁸: Hierbei handelt es sich um ein Persistenz-Framework, das den Zustand von Objekten in einer relationalen Datenbank speichern kann, wobei die eigentliche Datenbankausprägung transparent gehalten wird. Aus Performancegründen werden zusätzlich noch "c3p0"⁹ (ein Connection-Pooling Framework) sowie "ehcache"¹⁰ (ein Caching Framework) eingesetzt.
- IAIK JCE¹¹: Die IAIK-Implementierung eines Providers für die Java Cryptography Extension ermöglicht die Nutzung kryptografischer Funktionen (inkl. Zertifikatsmanagement).
- JConfig¹²: JConfig ist eine Bibliothek, die das Verwalten von Anwendungskonfigurationen erleichtert. Es wird hier in einer modifizierten Form eingesetzt.
- PDF-AS: PDF-AS ist ein Framework, das nach dem E-Government-Gesetz ([EGovG], §§19-21) zum Anbringen von (Amts-)Signaturen auf PDF-Dokumente sowie zur Rekonstruktion von Signaturen aus Papierausdrucken geeignet ist.

2.1.3 Serverseitige Komponenten

Folgende Komponenten sind am Server installiert und werden von den in Abschnitt 2.1.2 erläuterten Komponenten verwendet:

- Datenbank: siehe Abschnitt 2.1.5
- Mail-Server: Über einen SMTP-Zugang wird auf den Mail-Server sowohl von MOA-ZS (zum Versenden von Statusmeldungen) als auch vom Anwendungskern (zum Versenden signierter Dokumente) zurückgegriffen. Der Mail-Server sollte extern nicht erreichbar sein, da dieser ausschließlich von Komponenten am Server verwendet wird.
- MOA-ID¹³: MOA-ID ist die Authentifizierungskomponente von MOA-ID. Diese wird verwendet um Benutzer mittels Bürgerkarte zu authentifizieren.
- MOA-SP/SS: PDF-AS nutzt MOA-SS (Serversignatur) um PDF-Dokumente zu signieren. Hierbei wird auf die hinterlegten Signaturzertifikate zurückgegriffen.
Die Signaturprüfungskomponente (MOA-SP) kommt nicht zum Einsatz.
- MOA-ZS¹⁴: MOA-ZS ist eine Middleware, die Anwendungen den Zugang zur elektronischen Zustellung erleichtert indem sie erforderliche Abfragen und Umrechnungen übernimmt. Anwendungen kommunizieren mit MOA-ZS zum Dokumente elektronisch zuzustellen.

⁸ <http://www.hibernate.org/>

⁹ <http://sourceforge.net/projects/c3p0>

¹⁰ <http://ehcache.sourceforge.net/>

¹¹ <http://jce.iaik.tugraz.at/>

¹² <http://www.jconfig.org/>

¹³ <http://egovlabs.gv.at/projects/moa-idspss>

¹⁴ http://www.cio.gv.at/it-infrastructure/delivery/mzs_final/

MOA-ZS Proxy¹⁵: MOA-ZS bietet zur Verständigung über den Zustellerfolg per se keine direkte synchrone Auskunft an die zustellende Applikation. Grundsätzlich wird die Applikation nur über die erfolgreiche bzw. über eine nicht erfolgte Annahme des Zustellstücks durch MOA-ZS selbst informiert. Das MOA-ZS Proxy Modul hat die Aufgabe, die asynchronen Zustellbestätigungen über ein Webservice anzunehmen und über das MOA-ZS Protokoll an die Applikation weiterzureichen.

2.1.4 Externe Komponenten

Zusätzlich finden folgende unabhängige Komponenten Verwendung:

- Zustell-Kopf:** Wird über die grafische Benutzerschnittstelle für die Signatur (Abschnitt 2.1.1) "Elektronische Zustellung" gewählt, dann erfolgt eine Prüfung der Daten des angegebenen Empfängers über den Zustell-Kopf. Im Fall von fehlerhaften Daten oder Unzustellbarkeit wird dies bereits über die Benutzerschnittstelle angezeigt (siehe Abb. 3.8).
MOA-ZS benutzt ebenfalls den Zustell-Kopf, u.a. um die Zustellbarkeit zu überprüfen.
- Zustell-Server:** MOA-ZS sendet eine Anfrage an den Zustell-Kopf mit den Daten des Empfängers um eine Liste von Zustell-Servern zu erhalten. Anhand verschiedener Kriterien (hinterlegte Zertifikate, Mimetypes, Zufall...) wählt MOA-ZS einen Server aus der Liste für die eigentliche Zustellung aus (siehe [MOA-ZS-TDOK]).
- Stammzahlenregister:** Das Stammzahlenregister wird von MOA-ZS zur Berechnung eines bereichsspezifischen Personenkennzeichens (bPK) für einen für die Zustellung vorgesehen Bereich verwendet. (siehe [MOA-ZS-SPEZ])
Die Signaturanwendung verwendet jedoch anstatt eines bPKs den Vor- und Zunamen, eine E-Mail-Adresse und ggf ein Geburtsdatum zur Adressierung des Empfängers. Aus diesem Grund wird in der vorliegenden Konfiguration auf das Stammzahlenregister nicht zugegriffen.

¹⁵ http://demo.egiz.gv.at/plain/projekte/allgemeine_e_government_infrastruktur/zustellproxy

2.1.5 Datenbank

Als Datenbank wird eine MySQL-Datenbank eingesetzt. Durch das verwendete Persistenz-Framework Hibernate ist es jedoch möglich, die Datenbanksausprägung gegen eine andere (z.B. Oracle) auszutauschen (siehe auch [HBM-DB]).

Abb. 2.3 zeigt die Beziehungen der einzelnen Tabellen der Datenbank.

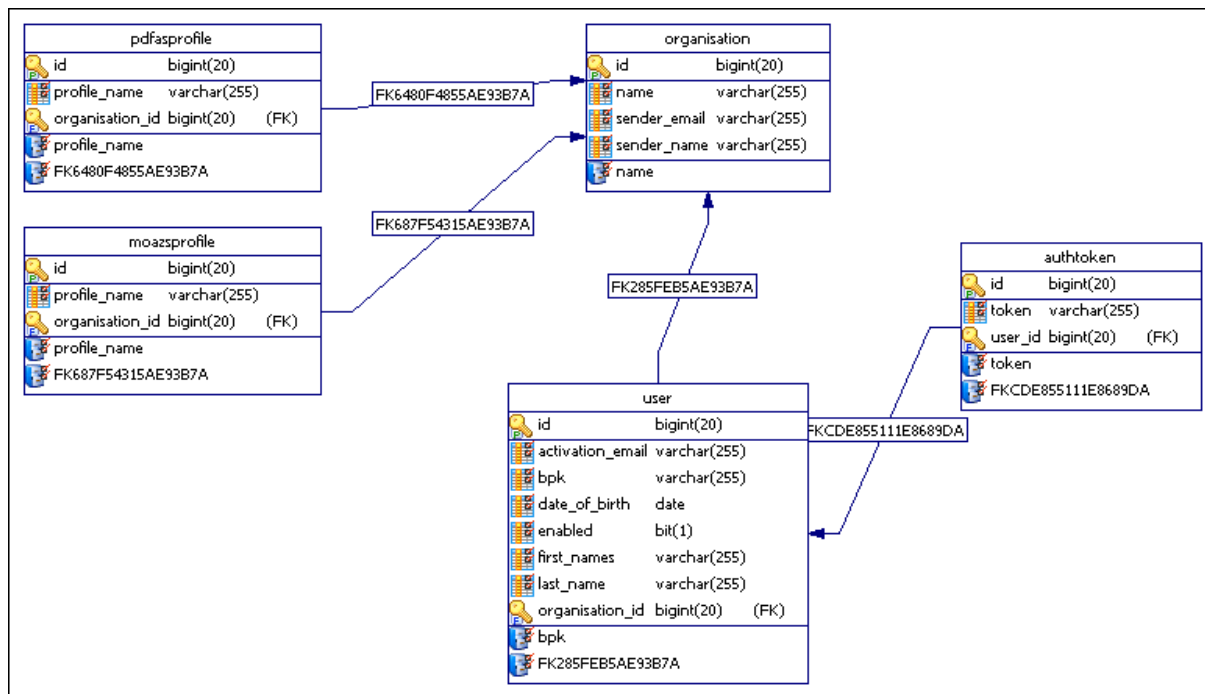


Abb. 2.3: Datenbank

2.2 Voraussetzungen zur Nutzung der Anwendung

Für die Nutzung der Anwendung bestehen clientseitig folgende Voraussetzungen:

- Web-Browser, beispielsweise Internet Explorer 6.0, 7.0 oder Mozilla Firefox 2.0.x¹⁶
- Bürgerkarte
- PC/SC-fähiges Kartenlesegerät
- Bürgerkarten-Software
 Die Kommunikation mit der Bürgerkarte muss mit einer der Security-Layer-Spezifikation ([SL12]) entsprechenden Bürgerkartensoftware erfolgen.
 z.B. ITSolution TrustDesk Basic, Version¹⁷ 2.7.6

¹⁶ <http://www.mozilla.com/firefox/>

¹⁷ <http://www.buergerkarte.at/BKU/>

3 Anwendungsbeschreibung

Die Anwendungsbeschreibung umfasst die Verwendung der grafischen Benutzerschnittstelle zum Signieren und Versenden von PDF-Dokumenten. Die Administration wird im Abschnitt 4 ("Administration") behandelt.

Hinweis: Um die Signatur-Anwendung nutzen zu können muss für den jeweiligen Benutzer ein Benutzerkonto eingerichtet und aktiviert sein (siehe Abschnitt 0).

3.1 Authentifizierung

Der erste Schritt zur Verwendung der Signatur-Anwendung ist eine Authentifizierung mittels Bürgerkarte. Dieser Schritt muss innerhalb einer Sitzung nur einmal durchgeführt werden.

Dazu muss zunächst die Anwendung in einem Web-Browser über ihren Link aufgerufen werden.

beispielsweise <https://behoerde.gv.at/esig/>

Wenden Sie sich an den Administrator falls Sie den Link nicht wissen.

Nach Aufruf des Links zur Signatur-Anwendung wird – falls der Benutzer nicht bereits authentifiziert ist – die in Abb. 3.1 gezeigte Hinweis-Seite dargestellt. Das Symbol in der Mitte der Seite zeigt ob die Bürgerkartenumgebung (siehe Abschnitt 2.2) bereit ist. Stellen Sie sicher, dass die Bürgerkartenumgebung gestartet ist, ansonsten kann die Authentisierung nicht durchgeführt werden.

Starten Sie die Authentisierung durch Klick auf "Authentisierung starten".

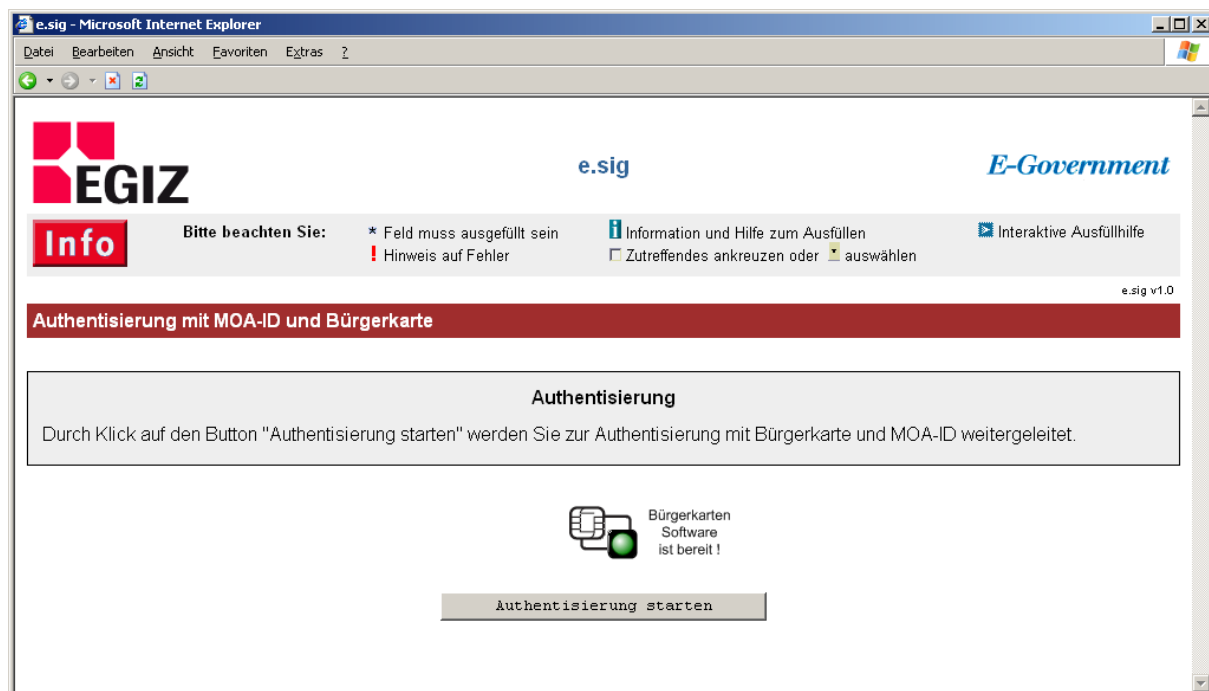


Abb. 3.1: Authentisierung mit Bürgerkarte

Zunächst wird nun die Personenbindung der Bürgerkarte ausgelesen. Hierfür fordert die Bürgerkartenumgebung den Benutzer zur Eingabe des Karten-PINs (im Falle E-Card) bzw. zur Eingabe des Infobox-PINs (im Falle anderer Bürgerkarten) auf.

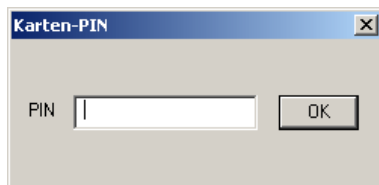


Abb. 3.2: Eingabe des Karten-PINs zum Auslesen der Personenbindung

Nun werden die ausgelesenen Daten in einem Textblock zusammengefasst, den der Benutzer nun im Rahmen der Authentisierung signieren muss. Dazu muss der "6+ stellige Signatur PIN" eingegeben werden (siehe Abb. 3.3).



Abb. 3.3: Signatur der Anmeldedaten

Nach erfolgreicher Authentifizierung wird der Name des Benutzers sowie die Organisation, der er zugeordnet ist im linken oberen Bereich angezeigt (siehe Abb. 3.4). Um die Benutzeroberfläche zum Signieren und Versenden von PDF-Dokumenten aufzurufen, muss auf "Signatur und Versand von PDF-Dokumenten" geklickt werden.

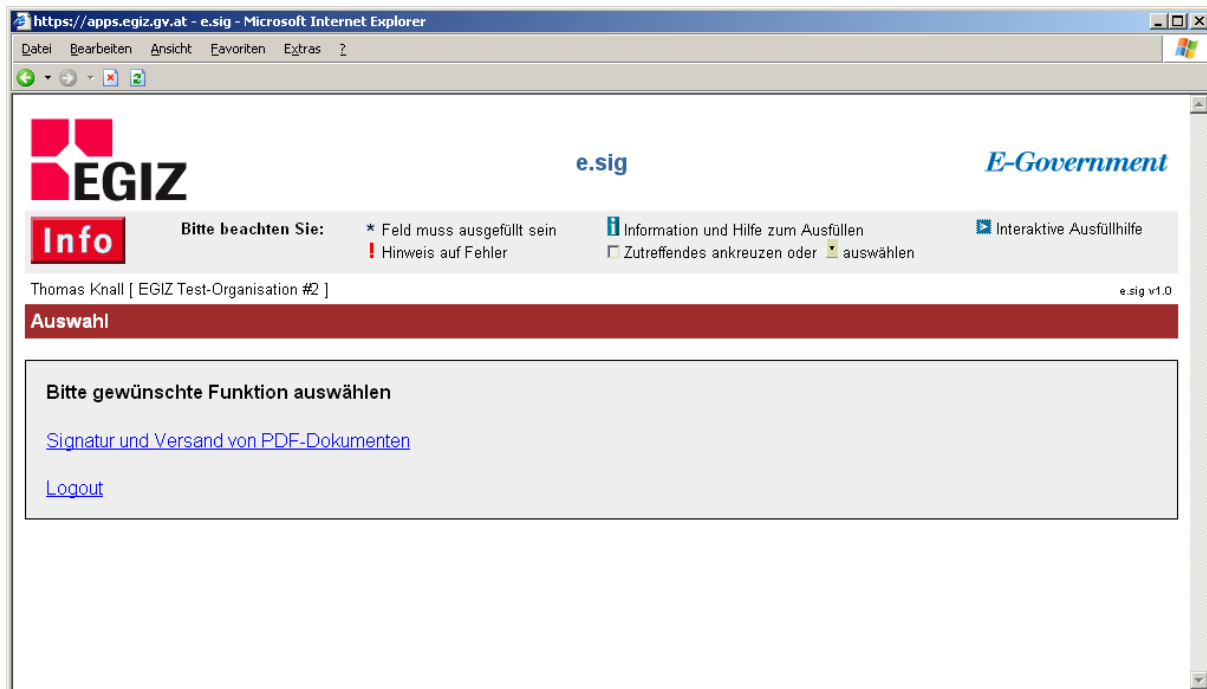


Abb. 3.4: Startseite der Signatur-Anwendung

3.2 Signatur und Versand von PDF-Dokumenten

Der nachfolgende Abschnitt enthält allgemeingültige Informationen zur Benutzeroberfläche für die Signatur und zum Versand von PDF-Dokumenten.

3.2.1 Allgemeine Informationen

Die Benutzeroberfläche unterscheidet sich stark je nach gewählter Art der Zustellung.

Folgende Zustell-Varianten sind möglich:

- via E-Mail
- mit Elektronischer Zustellung (Normal oder mit Zustellnachweis (RSa))
- Download (hier findet keine elektronische Übermittlung des signierten Dokuments statt)

Aus Usability-Gründen bleibt die Wahl der Zustell-Variante inkl. aller individuellen Angaben wie Zustellqualität "RSa" (bei Elektronischer Zustellung), oder Betreff und E-Mail-Text (bei E-Mail-Zustellung) innerhalb einer Sitzung gespeichert, sodass schnell und einfach mehrere Dokumente hintereinander mit gleichen Einstellungen signiert und versandt werden können.

Je nach Art der Zustellung sind einige Felder mit einem Stern * als Pflichtfelder markiert, andere sind optional und müssen nicht ausgefüllt werden.

Werden Pflichtfelder nicht oder Felder fehlerhaft ausgefüllt dann wird dies mit entsprechenden Hinweisen angezeigt (siehe Abb. 3.5).

PDF-Signatur mit elektronischer Zustellung

Folgende Fehler sind aufgetreten

- "Vorname" ist erforderlich
- "E-Mail Adresse" ist keine gültige E-Mail Adresse

Empfänger

Vorname !

Familienname * Mustermann

E-Mail Adresse ! max.mustermann

Abb. 3.5: Hinweis auf fehlende/fehlerhafte Eingaben

Hinweis: Um zu verhindern, dass einzelne (System-)Ressourcen über Gebühr beansprucht werden, wurde eine Beschränkung der Dateigröße der zu verarbeitenden PDF-Dokumente abhängig von der gewählten Zustell-Variante eingeführt. Diese kann über die Konfiguration der Anwendung angepasst werden (siehe Abschnitt 5.3.2). In der Auslieferungsversion wurden folgende Größenbeschränkungen definiert:

- Versand via E-Mail: 6 MB
- Elektronische Zustellung: 1 MB
- Download: 30 MB

Wird versucht, ein Dokument zu verarbeiten, das die konfigurierten Größenbeschränkungen überschreitet, wird eine Fehlermeldung ähnlich wie jene in Abb. 3.5 angezeigt.

3.2.2 Auswahl des PDF-AS Signatur-Profiles

Unabhängig von der Art der Zustellung werden dem Benutzer stets alle seiner Organisation zugeordneten PDF-AS Signatur-Profile über ihren Beschreibungstext¹⁸ in einer Drop-Down-Box angeboten (siehe Abb. 3.6).

Signaturprofil

Profil * Standard-Dokument (englisch)

Abb. 3.6: Auswahl eines Signaturprofils

Ein Signatur-Profil umfasst folgende Elemente:

- Beschreibungstext (z.B. "Standard-Dokument (englisch)");
- Signatur-Zertifikat (über einen MOA-SS Key Identifier)
- Breite und Position der Signaturmarke
- Bildmarke für die Signaturmarke

¹⁸ Der Beschreibungstext wird in der PDF-AS-Konfigurationsdatei für jedes PDF-AS Profil definiert (siehe auch Abschnitt 5.4, Seite 49 bzw. Anhang, Seite 55).

- Text-Bezeichner z.B. ("Signaturwert", "Unterzeichner"...)
- Hinweis auf ein Prüfservice
- Layout der Signaturmarke
 - Schriftart
 - Schriftgröße
 - Hintergrundfarbe
 - Name des Unterzeichners (z.B. "Organisation xy")
 - Schriftausrichtung
 - Rahmenbreite

3.2.3 Versand mit Elektronischer Zustellung

Wird "Elektronische Zustellung" als Zustell-Variante gewählt, wird das in Abb. 3.7 gezeigte Formular dargestellt. Für die Adressierung des Empfängers sind der/die Vorname(n), der Familienname sowie die Email-Adresse mit der der Empfänger bei einem elektronischen Zustelldienst registriert ist, zwingend erforderlich. Wird zusätzlich noch die Zustellqualität "RSa" gewählt, muss darüber hinaus noch das Geburtsdatum des Empfängers angegeben werden.

The screenshot shows a web browser window with the URL <https://apps.egiz.gv.at>. The page header includes the EGIZ logo, the text "e.sig", and "E-Government". Below the header, there is an "Info" section with a "Bitte beachten Sie:" notice. The main content area is titled "PDF-Signatur mit elektronischer Zustellung" and contains a form titled "Signatur und Versand".

The form is divided into several sections:

- Empfänger:** Fields for Vorname * (Max), Familienname * (Mustermann), E-Mail Adresse * (max.mustermann@mustermann.at), and Geburtsdatum * (01.01.1970).
- Zustellung:** A dropdown menu for "Art der Zustellung" set to "Elektronische Zustellung", and a checkbox for "RSa" which is checked. A warning message states: "Hinweis: Für die elektronische Zustellung muss der Empfänger bei einem elektronischen Zustelldienst angemeldet sein."
- Signaturprofil:** A dropdown menu for "Profil" set to "Standard-Dokument (englisch)".
- Auswahl des PDF-Dokuments:** A text input field for "Dokument" and a "Durchsuchen..." button.

At the bottom of the form, there are three buttons: "Signieren und versenden", "Textfelder löschen", and "Abbrechen".

Abb. 3.7: Signatur und Versand mit Elektronischer Zustellung

Bei der Verifizierung der eingegebenen Formulardaten wird im Falle einer Elektronischen Zustellung anhand einer Abfrage an den Zustell-Kopf geprüft, ob der angegebene Empfänger bei einem Zustelldienst registriert ist. Konnte der Empfänger nicht gefunden werden wird die in Abb. 3.8 dargestellte Meldung gezeigt.

The screenshot shows a web interface titled "PDF-Signatur mit elektronischer Zustellung". A red dashed box highlights an error message: "Folgende Fehler sind aufgetreten" followed by a red diamond icon and the text "Die EmpfängerIn ist mit den angegebenen Kontaktdaten NICHT bei einem Elektronischen Zustelldienst registriert." Below this, a form titled "Empfänger" is visible under the heading "Signatur und Versand". The form contains three input fields: "Vorname" with the value "Max", "Familienname" with the value "Mustermann", and "E-Mail Adresse" with the value "max.mustermann@mustermann.at". Each field has a red exclamation mark icon to its left, indicating an error.

Abb. 3.8: Empfänger ist nicht bei einem Zustelldienst registriert

Wurde das Dokument erfolgreich signiert, wird es an MOA-ZS bzw. den MOA-ZS Proxy übergeben woraufhin eine Meldung wie in Abb. 3.9 gezeigt, dargestellt wird.



Abb. 3.9: Signiertes Dokument erfolgreich an MOA-ZS übergeben

Zustellstatus-Meldung über E-Mail

Sobald der Zustellserver das Zustellstück angenommen hat, sendet MOA-ZS eine E-Mail mit dem Zustellstatus (siehe Abb. 3.10) an die für die der jeweiligen Organisation zugeordnete E-Mail-Adresse im MOA-ZS Sendeprofil (siehe auch Seite 52 im Anhang).

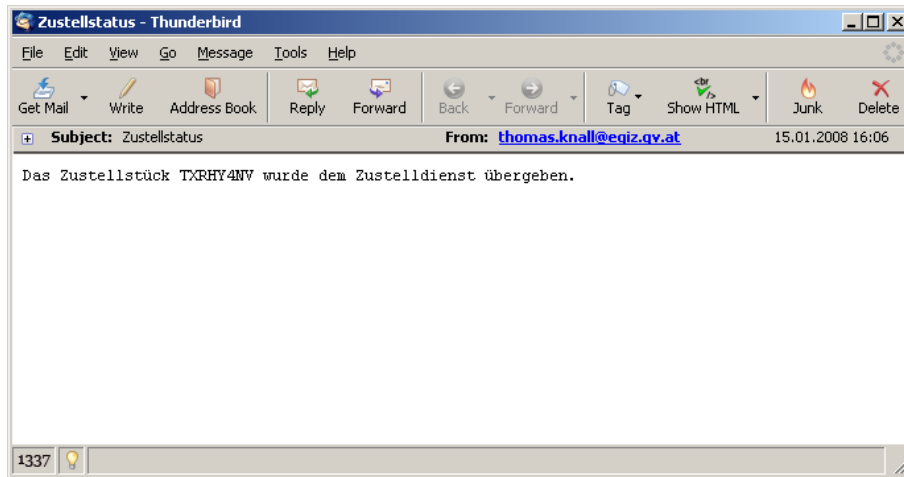


Abb. 3.10: MOA-ZS Benachrichtigung über den Status der Zustellung

Gleichzeitig sendet der Zustellserver eine Zustell-Verständigung an den Empfänger (siehe Abb. 3.11).

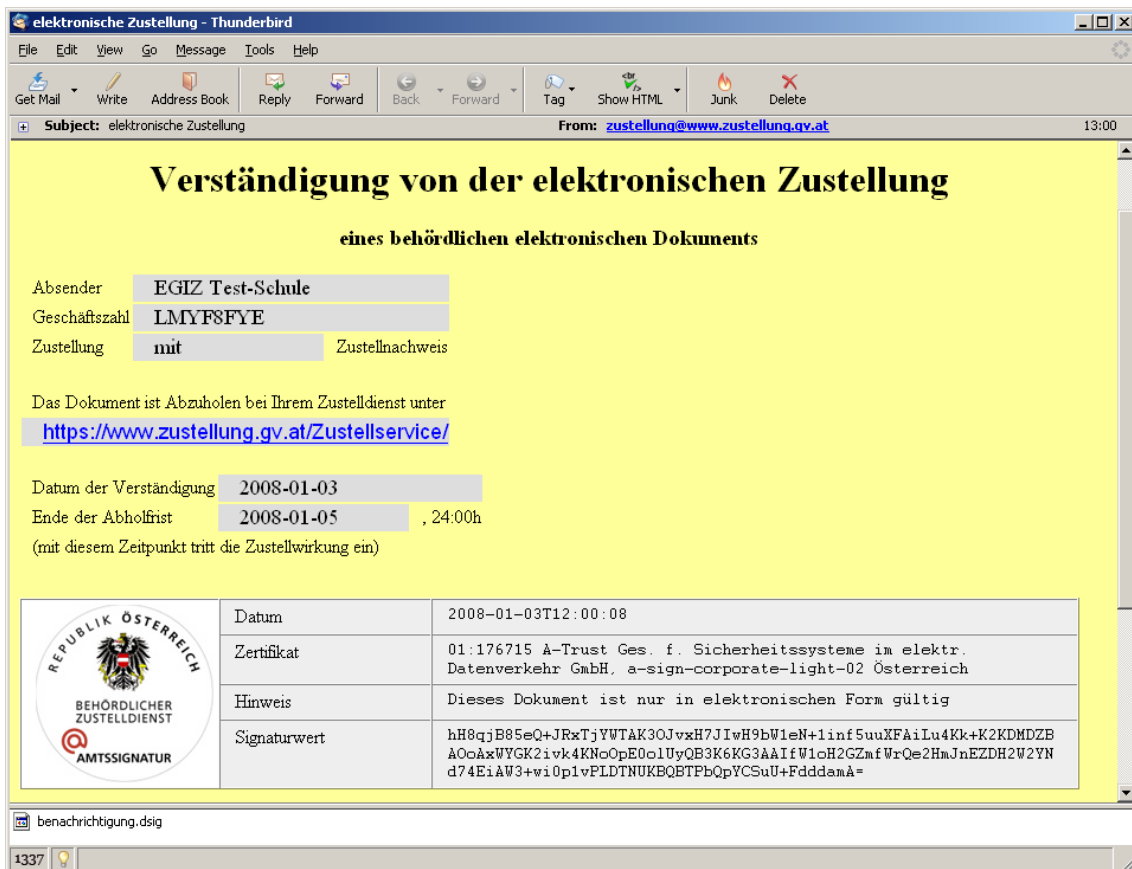


Abb. 3.11: Verständigung des Empfängers über eine elektronische Zustellung

Wurde eine Zustellung mit Zustellnachweis (RSa) gewünscht, dann wird an die der Organisation zugeordneten E-Mail-Adresse der in Abb. 3.12 gezeigte Zustellnachweis übermittelt sobald der Empfänger das Zustellstück abgeholt hat.

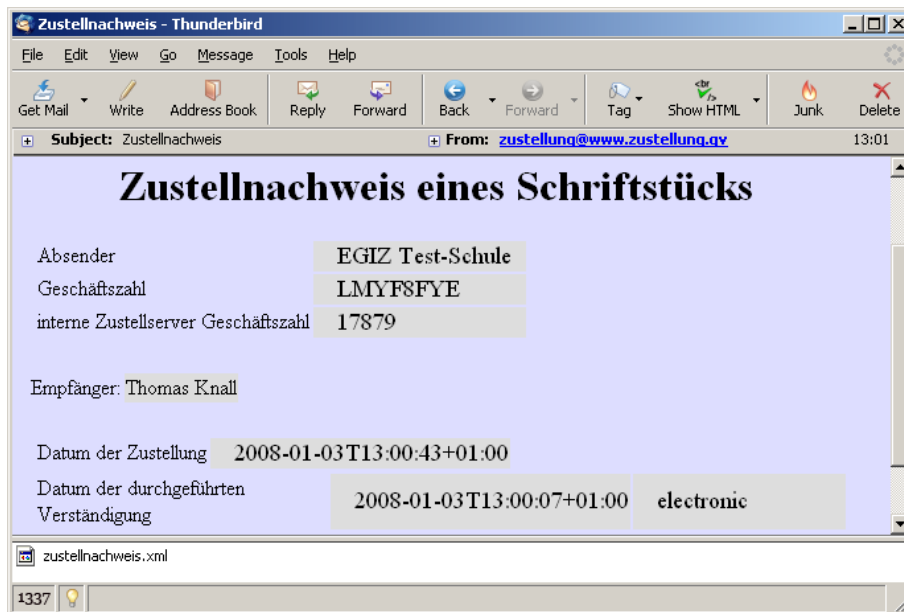


Abb. 3.12: Zustellnachweis im Falle einer RSa-Zustellung

Zustellstatusmeldung über Web-Service

Alternativ zu der Zustellstatus-Benachrichtigung über E-Mail kann MOA-ZS auch so konfiguriert werden, dass der Status über ein Web-Service¹⁹ übermittelt wird (siehe [MOA-ZS-AHB]).

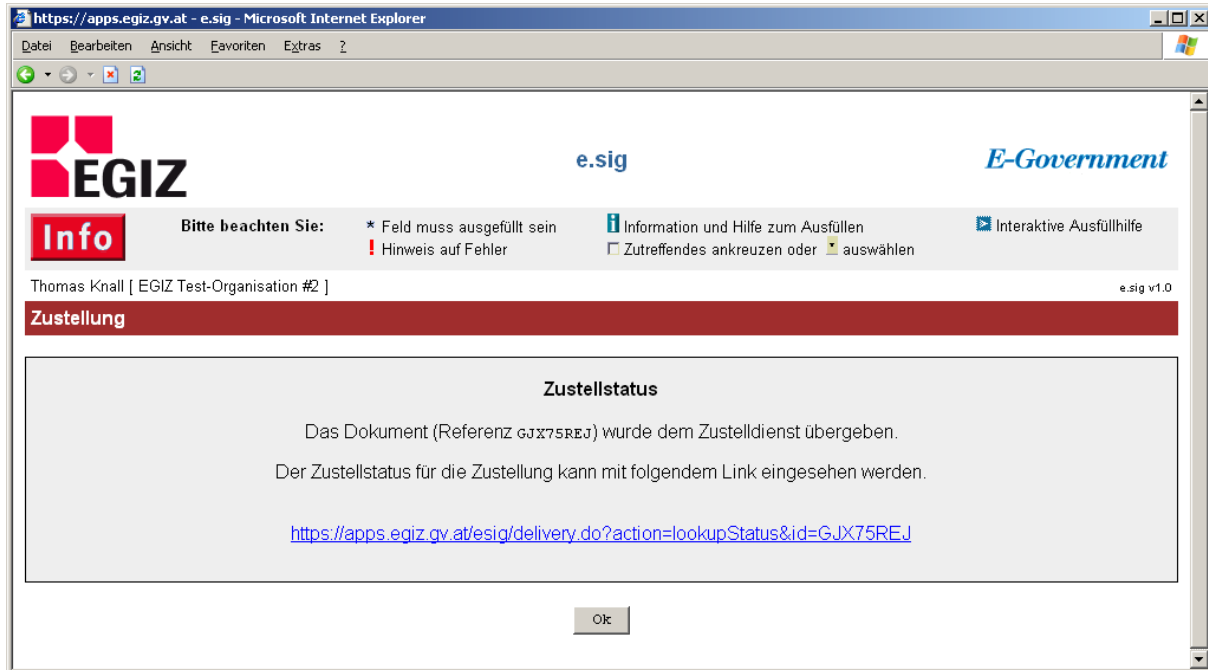


Abb. 3.13: Abfrage des Zustellstatus mittels MOA-ZS Proxy

Durch Anklicken des in Abb. 3.13 gezeigten Links kann jederzeit der Status der Zustellung festgestellt werden (siehe Abb. 3.14).



Abb. 3.14: Zustellstück wurde abgeholt (und gilt damit als zugestellt)

¹⁹ Hierfür muss jedoch das URL-Pattern /services/DeliveryNotification des MOA-ZS Proxy extern erreichbar konfiguriert werden (siehe [MOA-ZS-Proxy]), beispielsweise über einen entsprechenden Eintrag beim Redirector des Web-Servers.

3.2.4 Versand über E-Mail

Bei der Wahl der Zustellart "E-Mail" sieht die Benutzerschnittstelle wie in Abb. 3.15 dargestellt aus. Neu sind hier die Eingabefelder für den Betreff und den Text der E-Mail. Die vorgegebenen Texte sind über die Anwendungskonfiguration (siehe Abschnitt 5.3.2) festgelegt. Werden diese Texte im Formular verändert (um beispielsweise eine dem Anlassfall entsprechende E-Mail zu verwenden) bleiben diese innerhalb der Sitzung gespeichert, sodass das Versenden mehrerer gleichlautender E-Mails erleichtert wird.

The screenshot shows a web browser window with the URL `https://apps.egiz.gv.at - e.sig - Microsoft Internet Explorer`. The page header includes the EGIZ logo, the text "e.sig", and "E-Government". Below the header is an "Info" section with a "Bitte beachten Sie:" notice and several icons for help and interactive assistance. The main content area is titled "PDF-Signatur mit elektronischer Zustellung" and contains a form titled "Signatur und Versand".

The form is divided into several sections:

- Empfänger:** Fields for "Vorname", "Familiennamen", and "E-Mail Adresse *". The email address field contains "max.mustermann@mustermann.at".
- Zustellung:** A dropdown menu for "Art der Zustellung *" is set to "E-Mail". The "Betreff *" field contains "Zustellung eines signierten Dokuments". A text area for "Text" contains "Hiermit übermitteln wir Ihnen ein signiertes Dokument."
- Signaturprofil:** A dropdown menu for "Profil *" is set to "Standard-Dokument (englisch)".
- Auswahl des PDF-Dokuments:** A field for "Dokument *" is empty, with a "Durchsuchen..." button next to it.

At the bottom of the form are three buttons: "Signieren und versenden", "Textfelder löschen", and "Abbrechen".

Abb. 3.15: Signatur und Versand per E-Mail

Nach Absenden des Formulars wird das Dokument signiert und dem Mail-Server übergeben (siehe Abb. 3.16).

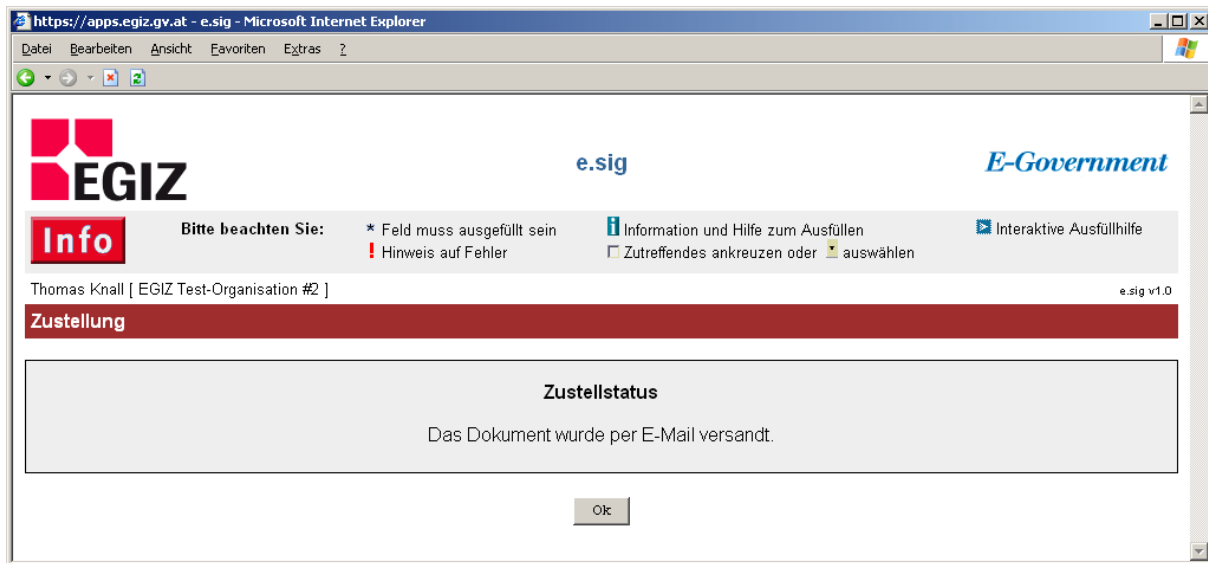


Abb. 3.16: signiertes Dokument per E-Mail versandt

Der Empfänger erhält eine E-Mail mit dem gewählten Betreff und Text sowie mit dem signierten Dokument als Attachment (siehe Abb. 3.17). Als Absender wird nicht die Person, die das Dokument signiert hat genannt, sondern die der Person zugeordnete Organisation.

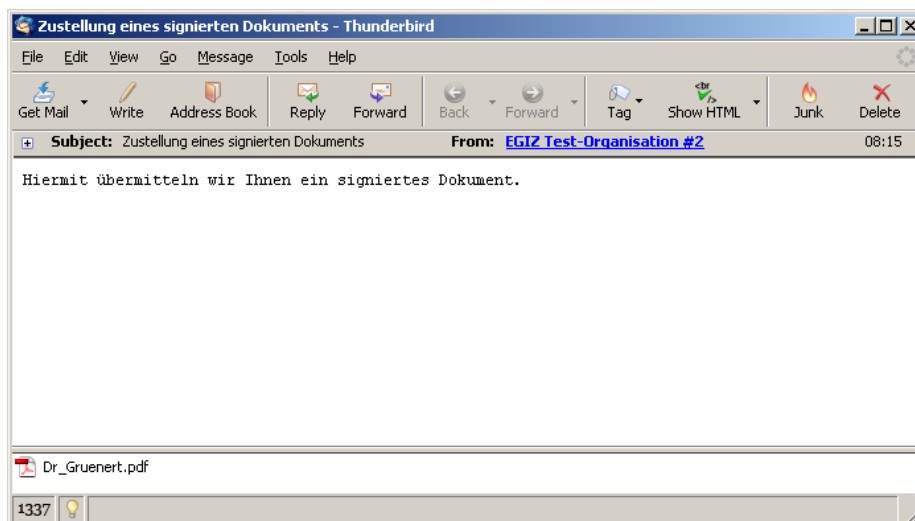


Abb. 3.17: signiertes Dokument via E-Mail

3.2.5 Download signierter Dokumente

Nach Wahl der Zustellart "Download" wird dem Benutzer das in Abb. 3.18 gezeigte Formular präsentiert. Nach Wahl eines Signatur-Profiles kann das Dokument durch Klick auf "Signieren und download" signiert werden.

The screenshot shows a web browser window with the URL <https://apps.egiz.gv.at> and the title "e.sig - Microsoft Internet Explorer". The page header includes the EGIZ logo, the text "e.sig", and "E-Government". Below the header is an "Info" section with a red box containing the text "Bitte beachten Sie:" followed by several instructions: "* Feld muss ausgefüllt sein", "Hinweis auf Fehler", "Information und Hilfe zum Ausfüllen", "Zutreffendes ankreuzen oder auswählen", and "Interaktive Ausfüllhilfe". The user's name "Thomas Knall [EGIZ Test-Organisation #2]" and the version "e.sig v1.0" are displayed. A red banner below the header reads "PDF-Signatur mit elektronischer Zustellung". The main content area is titled "Signatur und Download" and contains three sections: "Zustellung" with a dropdown menu set to "Download", "Signaturprofil" with a dropdown menu set to "Standard-Dokument (englisch)", and "Auswahl des PDF-Dokuments" with a text input field and a "Durchsuchen..." button. At the bottom of the form are three buttons: "Signieren und download", "Textfelder löschen", and "Abbrechen".

Abb. 3.18: Signatur und Download

Der Anwender kann das signierte Dokument über den im darauffolgenden Fenster (Abb. 3.19) gezeigten Link downloaden. Der Link ist an die aktuelle Sitzung gebunden und wird automatisch bei der Rückkehr auf die Startseite verworfen.

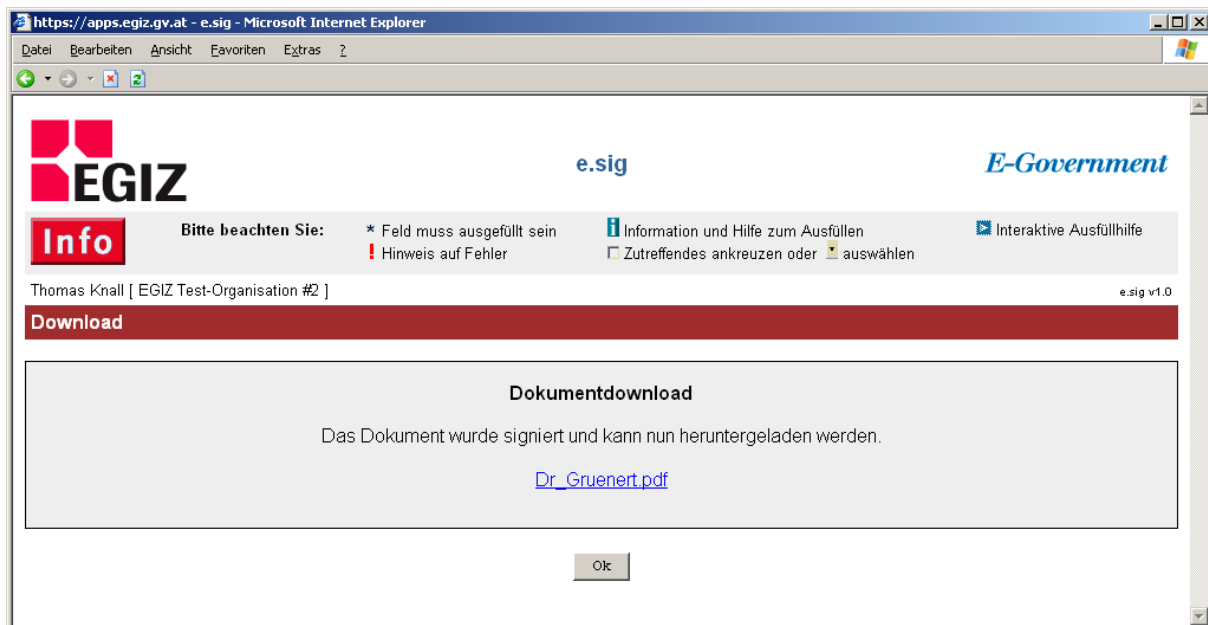


Abb. 3.19: Download eines signierten Dokuments

4 Administration

Die Administrations-Komponente kann über einen Web-Browser aufgerufen werden. Wenden Sie sich an den Administrator falls Sie den Link nicht wissen.

beispielsweise <http://localhost:48080/esig-admin/>

Die Administrations-Komponente sollte aus Sicherheitsgründen nicht über das Internet erreichbar sein oder zumindest mit einer adäquaten Authentifizierung versehen sein. Im Auslieferungszustand wurde der Komponente eine Basic-Authentication (Authentifizierung mit Benutzernamen und Passwort, siehe Abb. 4.1) vorgeschaltet.

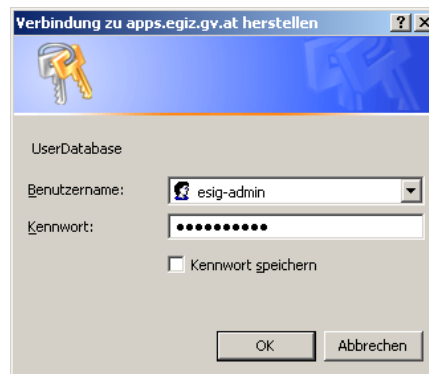


Abb. 4.1: Basic-Authentication

Die Zugangsdaten für die Auslieferungsversion sind:

- Benutzername: esig-admin
- Passwort: esig-admin

Nach Authentifizierung mit Benutzernamen/Passwort wird zunächst die Startseite der Administrations-Komponente dargestellt (siehe Abb. 4.2). Die derzeitige Version sieht als einzigen Menüpunkt die "Administration" vor.

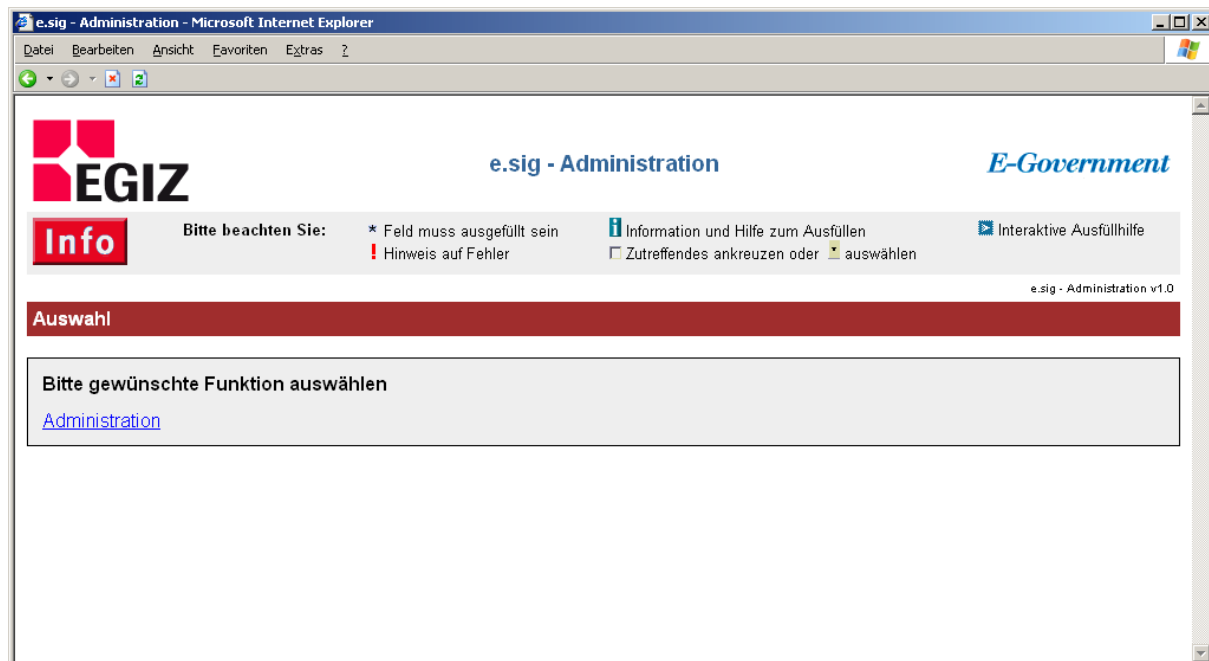


Abb. 4.2: Startseite der Administrationskomponente

4.1 Allgemeine Informationen

Die Administrationsseite gliedert sich in eine Navigationsspalte und einen Inhaltsbereich (siehe auch Abb. 4.3). Die Navigationsspalte ist in einzelne Gruppen unterteilt:

- Organisation:** Dieser Abschnitt umfasst die Verwaltung der Organisationen. Organisationen können angelegt, gelöscht und editiert werden wobei einzelnen Organisationen PDF-AS Profile sowie ein MOA-ZS Profil zugeordnet werden können.
Hinweis: Jedes PDF-AS Profil bzw. jedes MOA-ZS Profil kann Organisationen nur einmal zugeordnet werden. Dies verhindert eine versehentliche Fehlkonfiguration bei der unterschiedliche Organisationen gleiche Signatur- oder Sendeprofile verwenden.
- Benutzerkonten:** Hier können Benutzerkonten angelegt, gelöscht, (de)aktiviert sowie editiert werden. Sobald ein neues Benutzerkonto angelegt wird, wird automatisch eine Aktivierungs-Mail²⁰ versandt. Erst wenn der Empfänger die E-Mail durch Klick auf den enthaltenen Link sowie nachfolgender Authentifizierung mit Bürgerkarte bestätigt ist das Konto freigeschaltet.
Hinweis: Jedem Benutzerkonto MUSS eine (genau eine) Organisation zugeordnet werden. Aus diesem Grund muss vor der Erstellung eines Benutzerkontos zumindest eine Organisation angelegt worden sein.
- PDF-AS:** Diese Gruppe umfasst die Registrierung von PDF-AS Profilen. Profile können eingetragen und gelöscht werden.

²⁰ Mit einer Aktivierungs-Mail wird u.a. die angegebene E-Mail Adresse verifiziert.

MOA-ZS: Äquivalent zu den PDF-AS Profilen können hier MOA-ZS Sendeprofile eingetragen und gelöscht werden.

Bei Aufruf der Administration werden zunächst die aktiven Benutzerkonten angezeigt (siehe Abb. 4.3). Die Liste umfasst all jene Benutzer, die derzeit Serversignaturen auslösen dürfen.

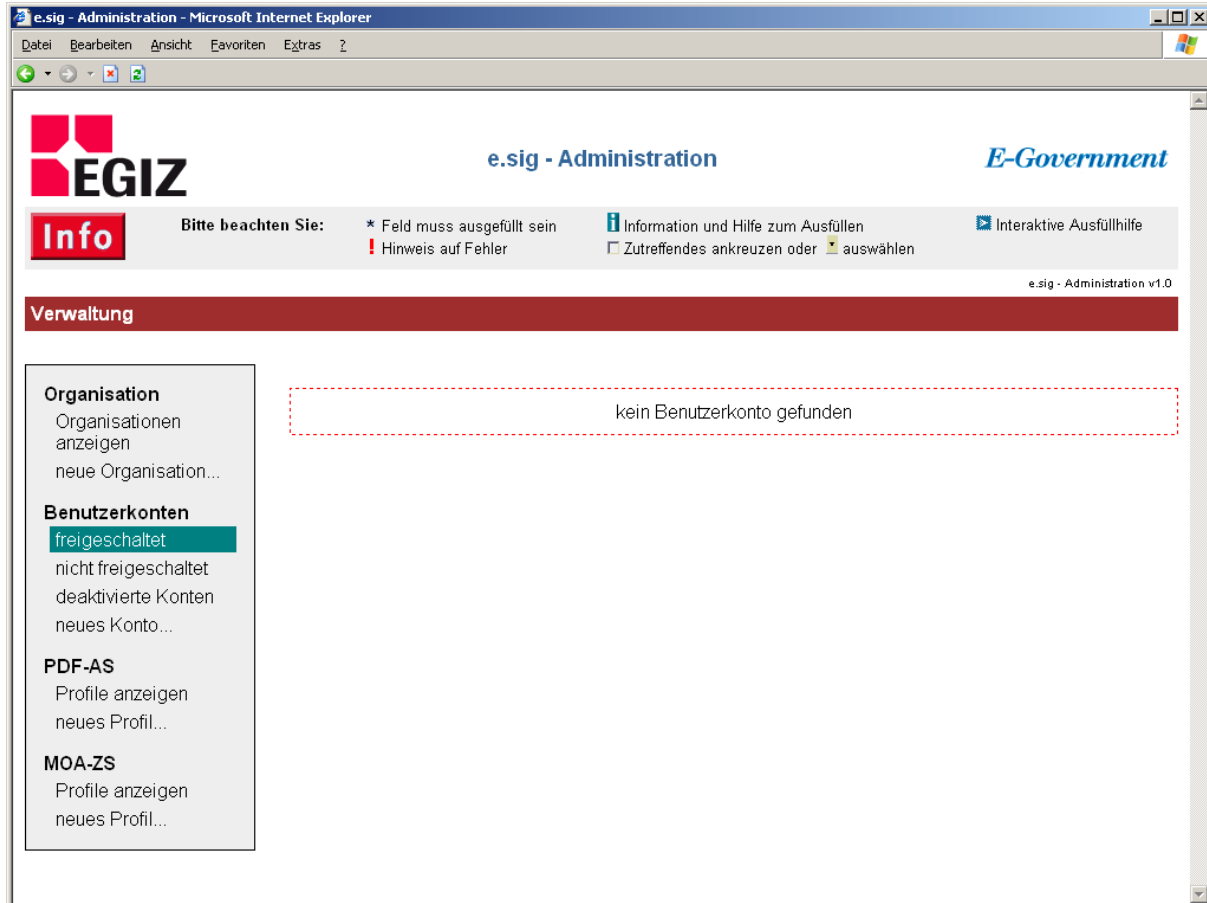


Abb. 4.3: Anzeige der zur Signatur berechtigten Benutzer

Die nächsten Abschnitte beschreiben die notwendigen Schritte zum Registrieren neuer Profile, Organisationen und Benutzer (in chronologischer Reihenfolge).

Hinweis: Um die Erhebung der Daten für neu zu registrierende Organisationen und Benutzer zu erleichtern, kann das im Anhang auf Seite 58 gezeigte Datenerhebungsblatt verwendet werden.

4.2 PDF-AS Profile eintragen

Zum Registrieren neuer Profile muss "neues Profil..." in der Gruppe "PDF-AS" gewählt werden. Im daraufhin dargestellten Formular (Abb. 4.4) ist der Profil-Name einzutragen. Sofern der Name gültig ist (keine Leerzeichen) und nicht bereits vergeben wurde, wird das Profil sofort registriert.

Warnung: Mit dem Eintragen eines PDF-AS Profils wird dieses in der Anwendung nur registriert. Es ist jedoch unbedingt erforderlich, dieses Profil auch in der entsprechenden Konfigurationsdatei für PDF-AS zu konfigurieren (siehe auch Abschnitt 5.4, Seite 48).

The screenshot shows a web browser window with the URL <https://apps.egiz.gv.at>. The page title is "e.sig - Administration" and it features the EGIZ logo and "E-Government" branding. A navigation menu on the left includes "Organisation", "Benutzerkonten", "PDF-AS", and "MOA-ZS". The "PDF-AS" section is active, with "neues Profil..." highlighted. The main content area is titled "PDF-AS Profil registrieren" and contains a form with the following elements:

- Form label: "PDF-AS Profil"
- Input field: "Name des PDF-AS Profils *" with the value "EGIZ1" entered.
- Hint text: "Hinweis: Der hier gewählte Name muss mit dem Profilnamen eines PDF-AS Profils übereinstimmen. Das PDF-AS Profile sind gesondert zu konfigurieren."
- Buttons: "Profil erstellen" and "Formular zurücksetzen".

Additional information on the page includes a "Bitte beachten Sie:" section with instructions on required fields and error handling, and a version indicator "e.sig - Administration v1.0" in the bottom right corner.

Abb. 4.4: neues PDF-AS Profil registrieren

Nach Registrierung des Profils wird automatisch die aktualisierte Liste der eingetragenen PDF-AS Profile angezeigt (Abb. 4.5).

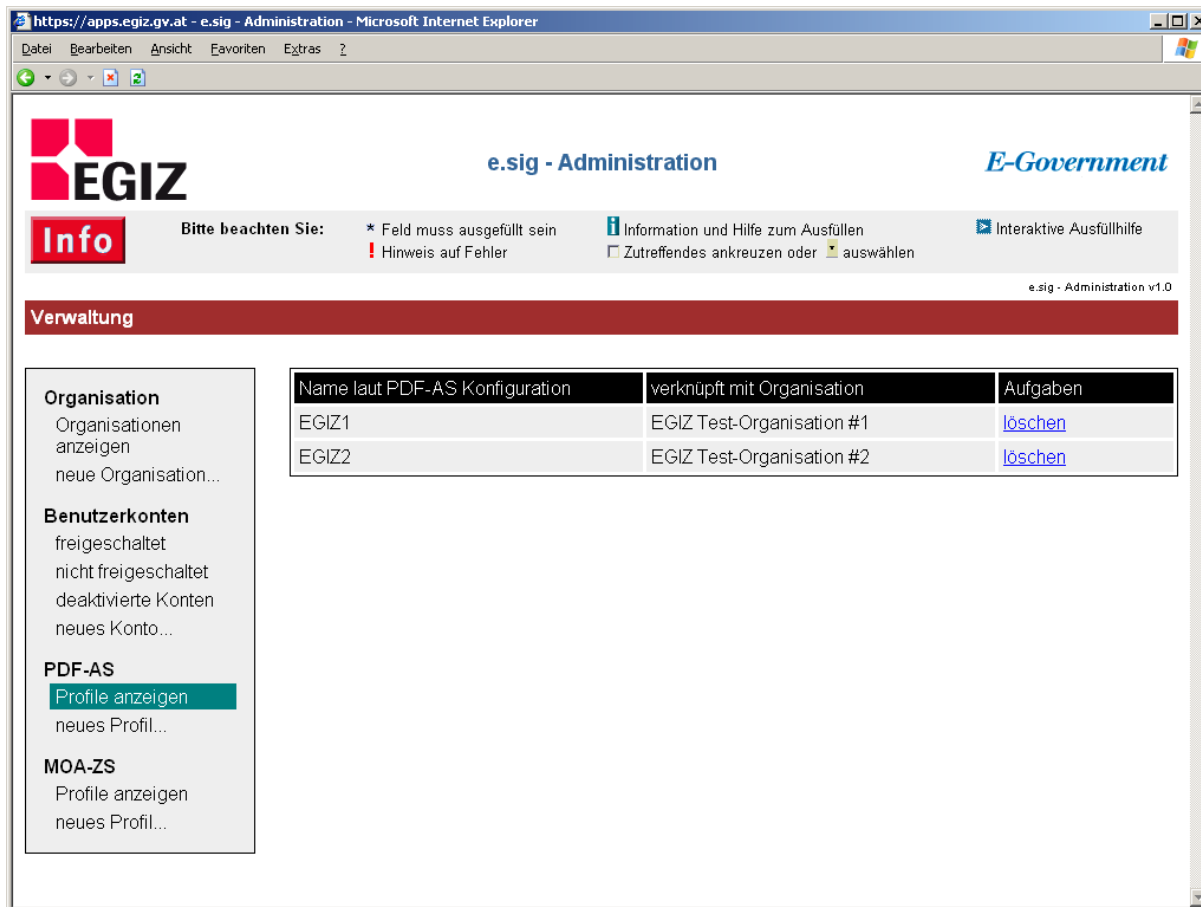


Abb. 4.5: registrierte PDF-AS Profile anzeigen

4.3 MOA-ZS Profile eintragen

Um in weiterer Folge Organisationen und Benutzer eintragen zu können, muss zumindest ein MOA-ZS Profil registriert sein. Dazu ist "neues Profil..." in der Rubrik "MOA-ZS" anzuklicken. Das Registrieren von MOA-ZS Profilen (Formular Abb. 4.6) ist äquivalent zu dem Registrieren von PDF-AS Profilen.

Warnung: Eingetragene MOA-ZS Profile müssen in der entsprechenden MOA-ZS-Konfigurationsdatei ebenfalls eingetragen werden (siehe auch Abschnitt 5.4, Seite 48).

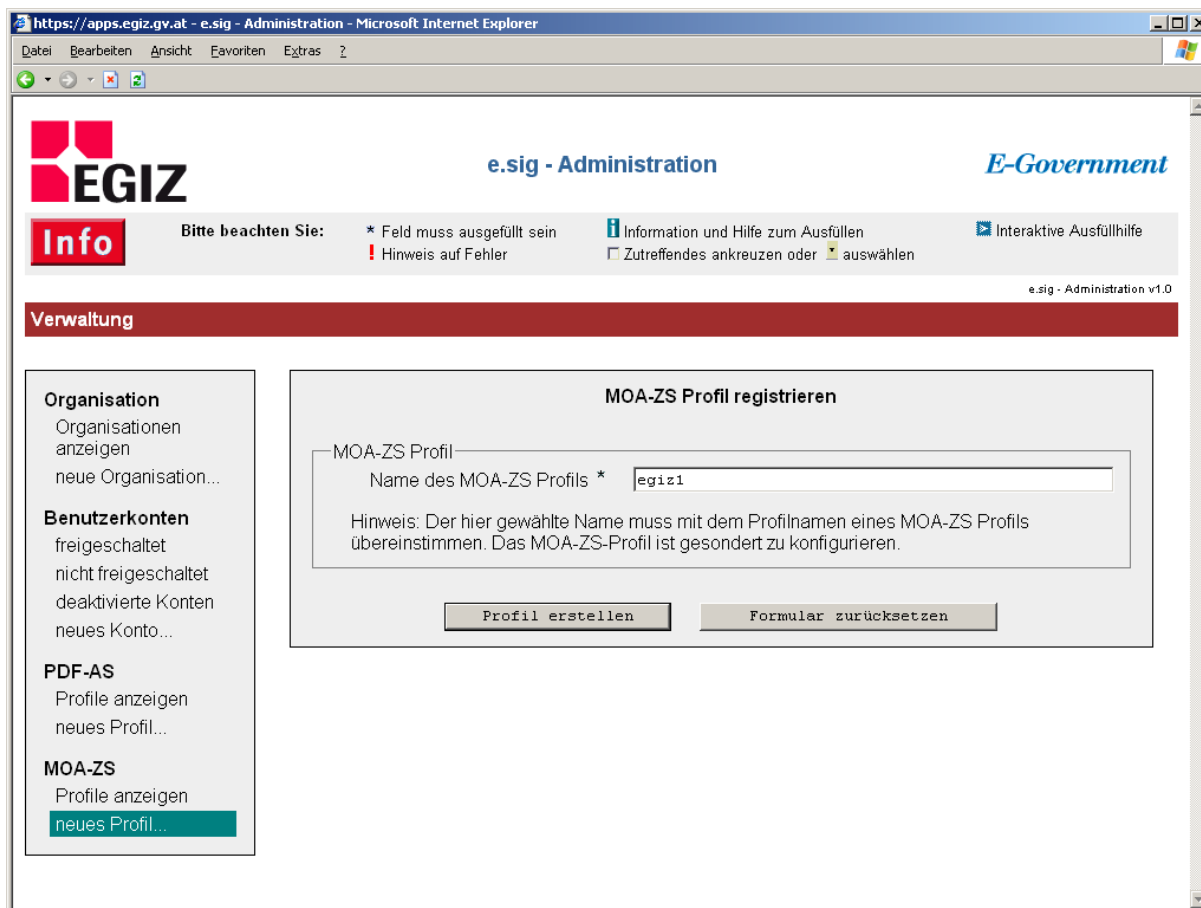


Abb. 4.6: neues MOA-ZS Profil registrieren

Nach der Registrierung neuer MOA-ZS Profile wird automatisch die aktualisierte Ansicht sämtlicher registrierter MOA-ZS Profile angezeigt (Abb. 4.7).

The screenshot shows the 'e.sig - Administration' web interface. At the top, there is a navigation bar with the EGIZ logo, the title 'e.sig - Administration', and the 'E-Government' logo. Below this is an 'Info' section with a red box containing the text 'Bitte beachten Sie:' followed by several instructions: '* Feld muss ausgefüllt sein', 'Hinweis auf Fehler', 'Information und Hilfe zum Ausfüllen', 'Zutreffendes ankreuzen oder auswählen', and 'Interaktive Ausfüllhilfe'. A version number 'e.sig - Administration v1.0' is visible in the bottom right of the header area.

The main content area is titled 'Verwaltung' and features a left-hand navigation menu with categories: 'Organisation' (Organisationen anzeigen, neue Organisation...), 'Benutzerkonten' (freigeschaltet, nicht freigeschaltet, deaktivierte Konten, neues Konto...), 'PDF-AS' (Profile anzeigen, neues Profil...), and 'MOA-ZS' (Profile anzeigen, neues Profil...). The 'MOA-ZS' section is currently selected.

The main content area displays a table of registered MOA-ZS profiles:

Name laut MOA-ZS Konfiguration	verknüpft mit Organisation	Aufgaben
egiz1	EGIZ Test-Organisation #1	löschen
egiz2	EGIZ Test-Organisation #2	löschen

Abb. 4.7: registrierte MOA-ZS Profile anzeigen

4.4 Organisation eintragen

Neue Organisationen können unter der Rubrik "Organisation" durch Klick auf "neue Organisation..." registriert werden.

Hinweis: Um einer Organisation PDF-AS Profile sowie ein MOA-ZS Profil zuweisen zu können, müssen diese zuvor registriert werden (Abschnitte 4.2 und 4.3).

Abb. 4.8 zeigt das Formular zum Registrieren von Organisationen. Zwingend zu tätige Eingaben umfassen den Namen der Organisation, die Absender E-Mail-Adresse sowie das zu verwendende MOA-ZS Profil. Die Absender E-Mail-Adresse sowie der optionale Absender-Name werden als Absender-Daten für die Zustell-Variante "E-Mail" verwendet.

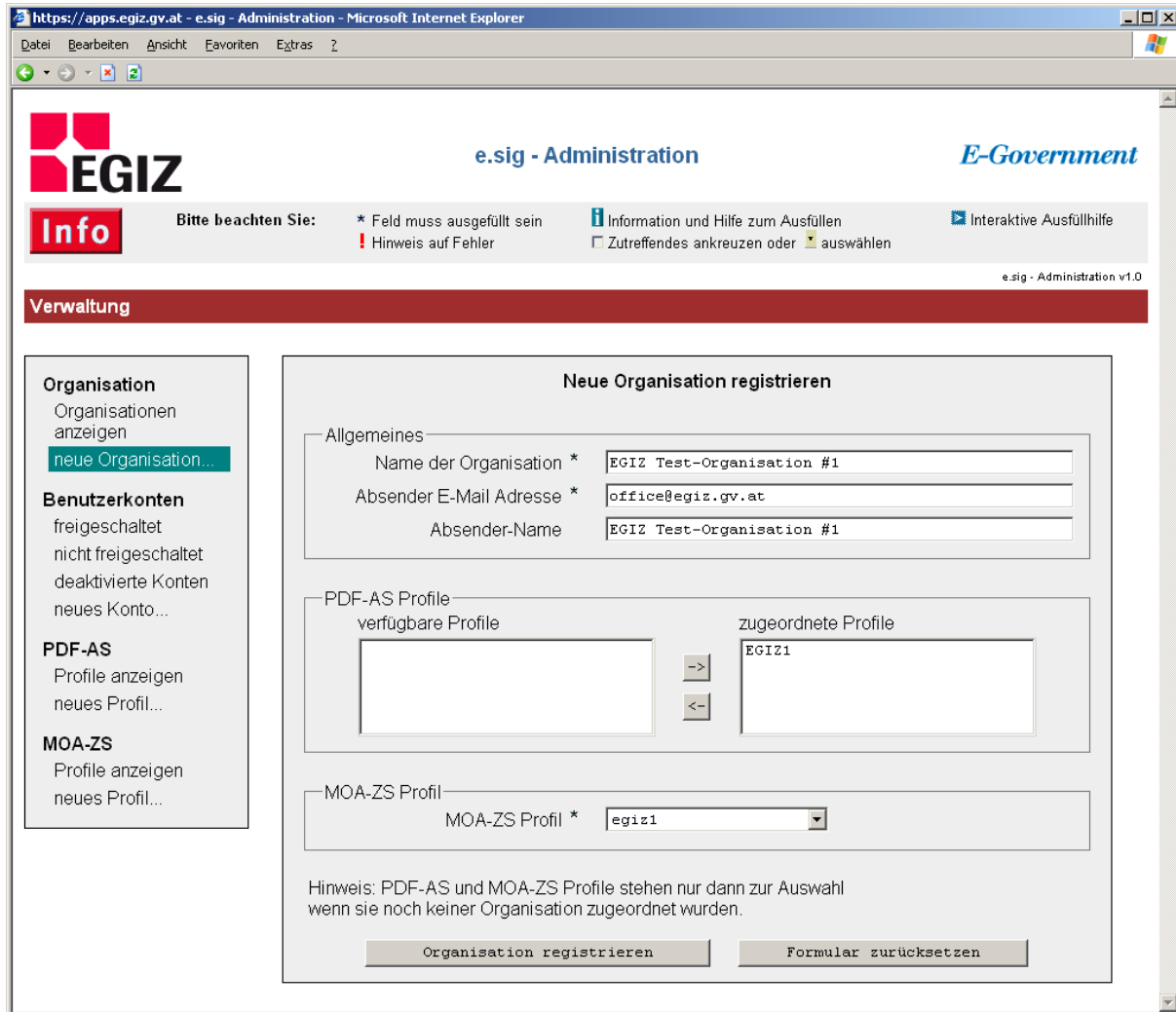


Abb. 4.8: neue Organisation registrieren

Sämtliche verfügbaren (d.h. noch nicht einer Organisation zugewiesenen) PDF-AS Profile sind in der linken Liste (unter "verfügbare Profile") dargestellt. Um ein Profil der aktuell bearbeiteten Organisation zuzuweisen ist dieses von der linken Liste in die rechte Liste zu verschieben. Dies erfolgt in dem das Profil zunächst in der linken Liste markiert wird und dann der Button mit dem nach rechts zeigenden Pfeil angeklickt wird. Auf umgekehrtem Weg können zugeordnete Profile wieder entfernt werden.

Die derzeitige Version der Signatur-Anwendung sieht die Zuordnung genau eines MOA-ZS Profil zu einer Organisation vor, wobei nur jene Profile zur Auswahl stehen, die noch keiner anderen Organisation zugewiesen wurden.

Nach der Registrierung einer Organisation (durch Klick auf "Organisation registrieren") wird eine aktualisierte Liste aktuell registrierter Organisationen angezeigt (Abb. 4.9). Hier sind auch die zugewiesenen PDF-AS Profile, das zugewiesene MOA-ZS Profil sowie die Anzahl der derzeit zugewiesenen Benutzer zu sehen.

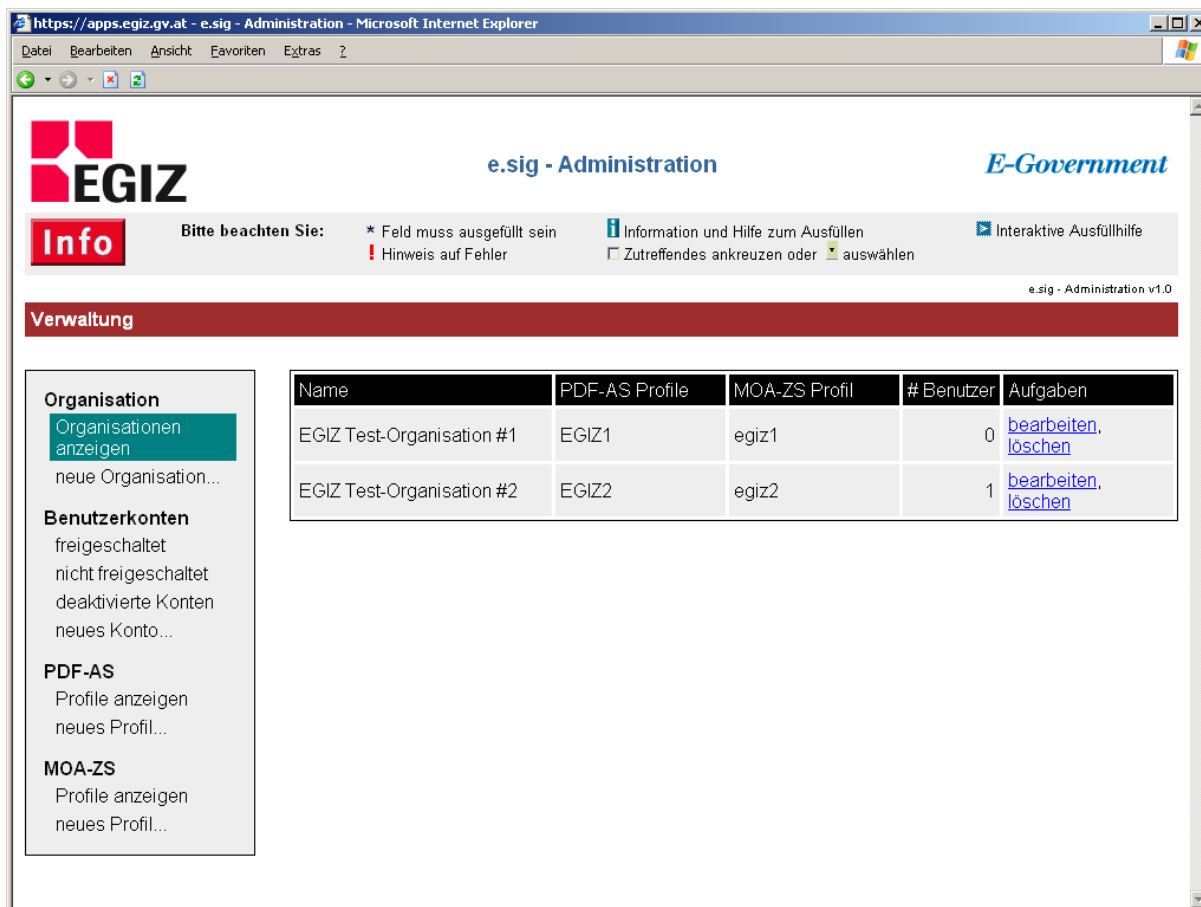


Abb. 4.9: registrierte Organisationen anzeigen

Nachdem nun zumindest eine Organisation verfügbar ist, können nun Benutzerkonten angelegt werden (siehe Abschnitt 4.5.1).

4.5 Benutzerkonten verwalten

Dieser Abschnitt umfasst das Erstellen, Editieren und Löschen von Benutzer-Zugängen.

4.5.1 Neues Benutzerkonto anlegen

Hierfür muss "neues Konto..." unter der Rubrik "Benutzerkonten" gewählt werden woraufhin das in Abb. 4.10 gezeigte Formular dargestellt wird. Sämtliche Felder des Formulars sind Pflichtfelder.

The screenshot shows a web browser window with the URL <https://apps.egiz.gv.at>. The page title is "e.sig - Administration" and it features the EGIZ logo and "E-Government" branding. A navigation menu on the left includes "Organisation", "Benutzerkonten", "PDF-AS", and "MOA-ZS". The "Benutzerkonten" section is active, with "neues Konto..." selected. The main content area is titled "Neues Benutzerkonto erstellen" and contains a form with three sections: "Benutzerdaten laut Bürgerkarte" (with fields for Vorname(n) * Max, Familienname * Mustermann, and Geburtsdatum * 01.01.1970), "Kontaktdaten" (with E-Mail Adresse * max.mustermann@mustermann.at and a note about an activation email), and "Organisation" (with a dropdown menu set to "EGIZ Test-Organisation #1"). At the bottom of the form are buttons for "Konto erstellen" and "Zurücksetzen".

Abb. 4.10: neuen Benutzer registrieren

Hinweis: Besonderes Augenmerk muss auf den Abschnitt "Benutzerdaten laut Bürgerkarte" gelegt werden. Hier müssen sämtliche Vornamen – getrennt durch Leerzeichen – sowie der Familienname und das Geburtsdatum des Bürgers (Benutzers) angegeben werden. Die Angaben müssen exakt mit den Eintragungen auf der Bürgerkarte übereinstimmen, da diese Daten beim Freischaltprozess abgeglichen werden und eine Freischaltung im Falle einer Nicht-Übereinstimmung verweigert wird.

Nach dem Erstellen des Kontos (durch Klick auf "Konto erstellen") wird automatisch eine Aktivierungs-Mail an die angegebene E-Mail Adresse versandt (siehe auch Abschnitt 4.5.2, "Aktivierung eines Benutzerkontos").

Gleichzeitig wird eine aktualisierte Ansicht der derzeit noch nicht freigeschalteten Benutzerkonten angezeigt. Sollte die automatisch versandte Aktivierungsmail beim Empfänger verloren gegangen sein, kann erneut eine Aktivierungsmail durch Klick auf "Aktivierung erneut versenden" verschickt werden.

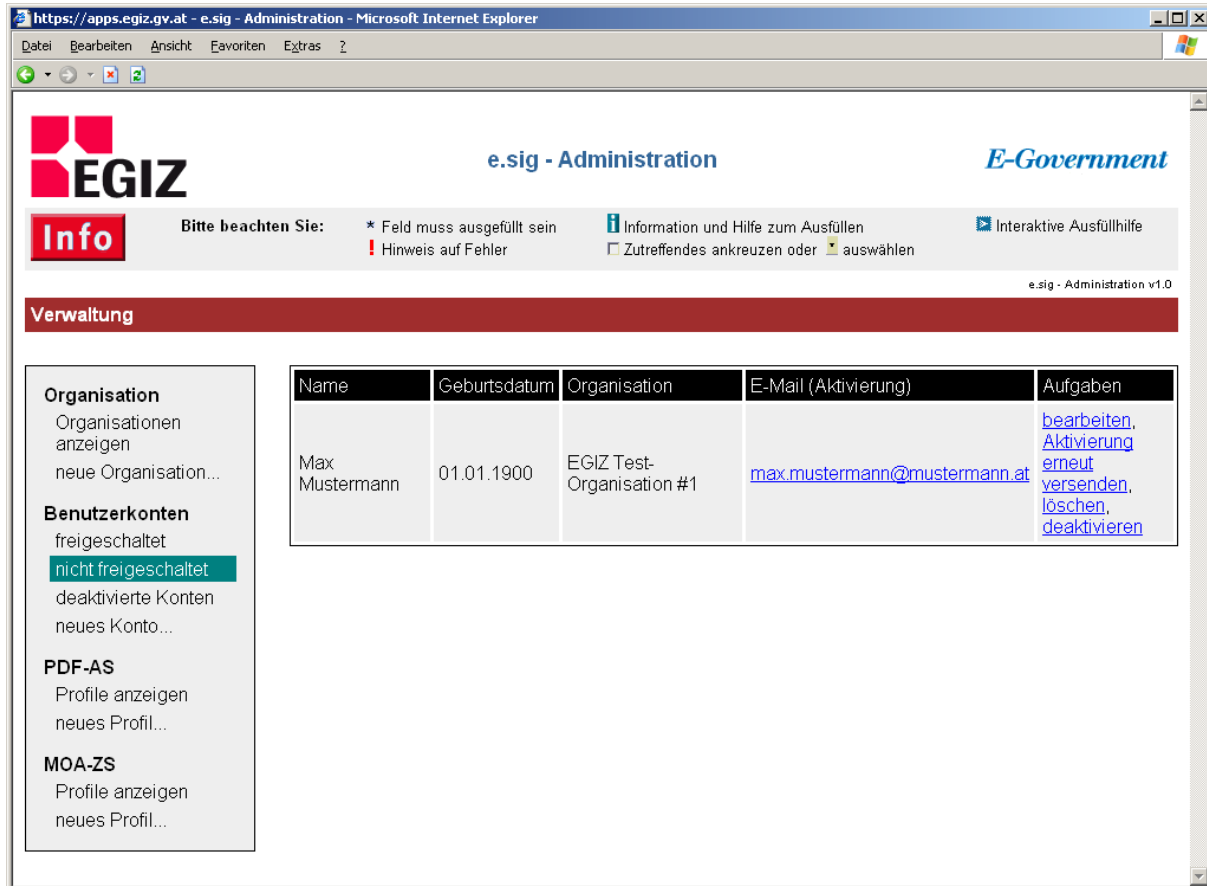


Abb. 4.11: Anzeige der neu registrierten (und noch nicht freigeschalteten) Benutzerkonten

4.5.2 Aktivierung eines Benutzerkontos

Neu registrierte Benutzer erhalten eine Aktivierungs-Mail (wie in Abb. 4.12) in der sie den ersten Link zur Aktivierung ihres Kontos anklicken müssen.

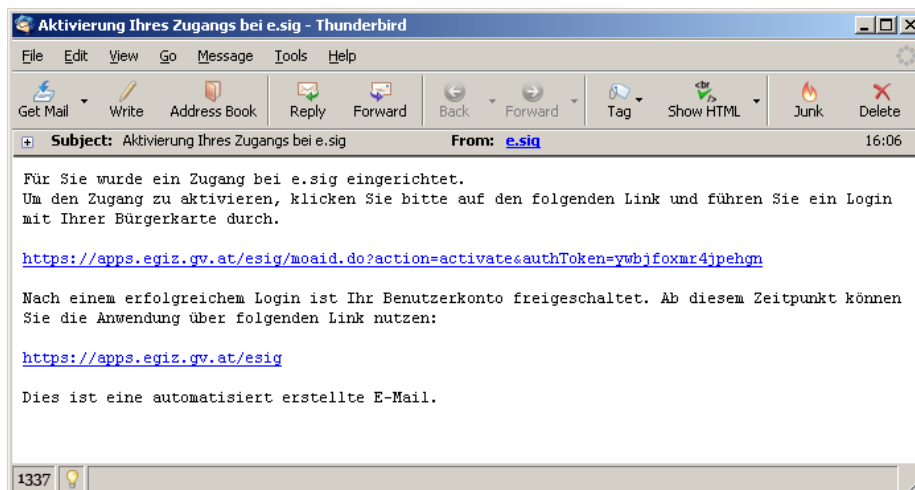


Abb. 4.12: Aktivierungs-Mail

Durch Klick auf den Aktivierungs-Link wird der Anwender zur Authentifizierung (siehe auch Abschnitt 3.1) weitergeleitet. Bei der Authentifizierung werden die bei der Registrierung des Benutzerkontos angegebenen Personendaten mit jenen aus der soeben durchgeführten Authentifizierung verglichen. Sind diese identisch wird das Konto aktiviert und der Benutzer gelangt zur Startseite der Signatur-Anwendung.

5 Deployment

Der Dokumentation des Deployments werden folgende Parameter zu Grunde gelegt:

Parameter

Name	Beschreibung	Beispiel
%INSTALL_DIR%	Verzeichnis in dem die E.SIG-Komponenten (JDK, Tomcat) eingerichtet werden Hinweis: Das Installationsverzeichnis sollte keine Leer- und Sonderzeichen enthalten.	C:\ESIG
%APPS%	Pfad zum Servlet-Container der Signatur-Anwendung bzw. der Administrations-Komponente	%INSTALL_DIR%\apache-tomcat-5.5.25-apps

5.1 Systemanforderungen

Es gelten folgende Anforderungen an die Installationsplattform bzw. an die Client-Komponenten. Die angegebenen Versionen entsprechen der getesteten Umgebung. Um Seiteneffekte zu vermeiden wird empfohlen von den angeführten Versionen nicht abzuweichen.

5.1.1 Server-Komponenten

Die folgenden Komponenten stellen die Anforderungen für die Signatur-Anwendung bzw. für die Administrations-Komponente dar.

- J2SDK Java Standard Development Kit (JDK) v1.5.0_14²¹ inkl. Unlimited Strength Jurisdiction Policy Files 5.0 und IAIK ECC und IAIK JCE Provider²²
- Apache Tomcat v5.5.25²³
- Relationale Datenbank, z.B. MySQL 5.0.21 oder MySQL 5.0.45²⁴

Darüber hinaus bestehen Anforderungen für die in Abschnitt 2.1.3 erläuterten MOA-Komponenten. Es wird empfohlen für jede MOA-Instanz eine eigene Apache Tomcat Instanz einzurichten.

- MOA-ID v1.4.2 oder neuer
 - Apache Tomcat v5.5.25
 - J2SDK Java Standard Development Kit (JDK) v1.5.0_14 inkl. Unlimited Strength Jurisdiction Policy Files 5.0 und IAIK ECC und IAIK JCE Provider
- MOA-SP/SS v1.4.2 oder neuer
 - Apache Tomcat v5.5.25
 - J2SDK Java Standard Development Kit (JDK) v1.5.0_14 inkl. Unlimited Strength Jurisdiction Policy Files 5.0 und IAIK ECC und IAIK JCE Provider

²¹ http://java.sun.com/javase/downloads/index_jdk5.jsp

²² <http://jce.iaik.tugraz.at/>

²³ <http://tomcat.apache.org/>

²⁴ <http://www.mysql.com/>

- MOA-ZS v1.0 / MOA-ZS Proxy v1.0
 - Apache Tomcat v5.0.28
 - J2SDK Java Standard Development Kit (JDK) v1.4.2_16²⁵ inkl. Unlimited Strength Jurisdiction Policy Files 1.4.2, IAIK ECC, IAIK JCE Provider und Bouncycastle-Provider²⁶ für Java 1.4 (build-138)

Hinweis: Die Anwendung nutzt durchgehend plattformunabhängige Komponenten. Getestet wurde jedoch ausschließlich unter Microsoft Windows XP SP2 und Server 2003. Der einwandfreie Betrieb kann unter anderen Betriebssystemen aus diesem Grund nicht zu 100% garantiert werden.

5.1.2 Client-Komponenten

- siehe Abschnitt 2.2, "Voraussetzungen zur Nutzung der Anwendung"

5.2 Installation

Die Installation kann komponentenweise (Abschnitt 5.2.1) – wenn beispielsweise eine Infrastruktur mit MOA-SP/SS, MOA-ID oder MOA-ZS bereits vorhanden ist – oder im Rahmen eines Gesamtpakets (Abschnitt 5.2.2) erfolgen.

5.2.1 Komponentenweise Installation

Die Installation der Anwendung setzt sich aus drei Schritten zusammen:

- Deployment der Signatur-Anwendung (Front-Office)
Das Deployment beschränkt sich auf das Kopieren des Web-Archivs für die Komponente Front-Office (`esig.war`) in das Tomcat-Webapps-Verzeichnis `%APPS%\webapps`.
- Deployment der Administrations-Komponente (Back-Office)
Das Deployment beschränkt sich auf das Kopieren des Web-Archivs für das Back-Office (`esig-admin.war`) in das Tomcat-Webapps-Verzeichnis `%APPS%\webapps`.
- Konfiguration der Web-Anwendung (siehe Abschnitt 5.3)
Hinweis: Front-Office und Back-Office besitzen eine gemeinsame Konfiguration.

Darüber hinaus müssen folgende Installationen getätigt bzw. Konfigurationen angepasst werden. Details zur Konfiguration externer Komponenten (MOA, Mail-Server) entnehmen Sie bitte den angegebenen Dokumentationen.

- Installation einer relationalen Datenbank, vorzugsweise MySQL (siehe Abschnitt 5.1.1)
 - Im Falle von MySQL den Eintrag `"max_allowed_packet=32M"` in die entsprechende MySQL-Konfigurationsdatei unter der Rubrik `"[mysqld]"` einfügen.
 - Anlegen einer Datenbank (z.B. `"esig"`) und eines Benutzers (z.B. `"esig"`) für die Anwendung `"e.sig"`. Die Tabellen werden von der Anwendung automatisch erstellt.
 - Anlegen einer Datenbank für MOA-ZS (z.B. `"moazs"`), eines Benutzers (z.B. `"moazs"`) sowie Initialisieren der Tabellen wie in [MOA-ZS-IHB] erläutert.
 - Anlegen einer Datenbank für MOA-ZS Proxy (z.B. `"zsproxy"`), eines Benutzers (z.B. `"zsproxy"`) sowie Initialisieren der Tabellen wie in [MOA-ZS-Proxy] erläutert.

²⁵ <http://java.sun.com/j2se/1.4.2/download.html>

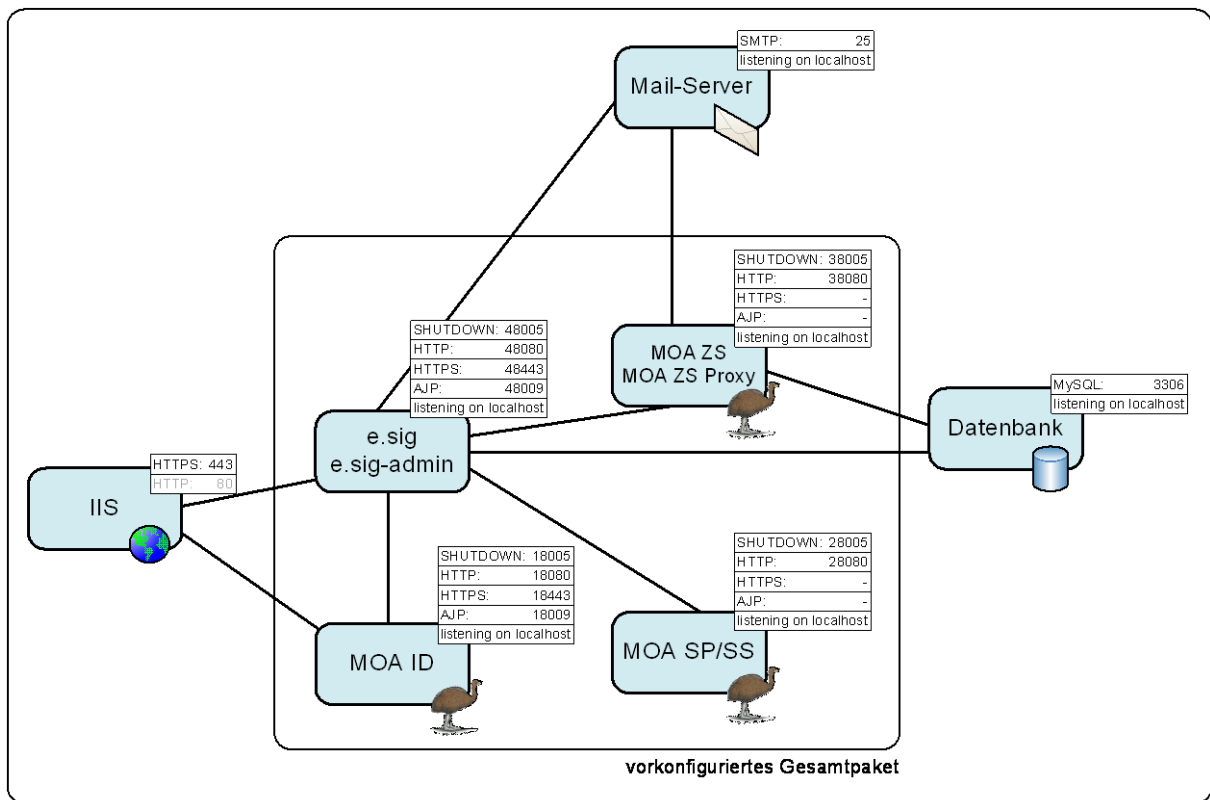
²⁶ http://www.bouncycastle.org/latest_releases.html

- MOA-ID (siehe [MOA-ID-HB])
- MOA-SP/SS (siehe [MOA-SPSS-HB])
- MOA-ZS (siehe [MOA-ZS-IHB], [MOA-ZS-AHB] und [MOA-ZS-BHB])
- Konfiguration des Mail-Servers für den Versand von Mails ohne Authentifizierung

5.2.2 Vorkonfiguriertes Gesamtpaket

Für die Auslieferungsversion der Anwendung wurde ein vorkonfiguriertes Gesamtpaket inkl. MOA-SP/SS, MOA-ID und MOA-ZS zusammengestellt (siehe auch Abschnitt 6.1), das nur noch geringfügig angepasst werden muss um es auf localhost zu betreiben.

Abb. 5.1 zeigt die Konfiguration des vorkonfigurierten Pakets sowie die empfohlene Konfiguration der restlichen Komponenten (Datenbank, IIS, Mail-Server).



Server-Umgebung

Abb. 5.1: Systemübersicht des vorkonfigurierten Gesamtpakets

Der Dokumentation zum vorkonfigurierten Gesamtpaket liegen folgende Parameter zu Grunde.

Parameter

Kurzbezeichnung	Pfad
%APPS%	%INSTALL_DIR%\apache-tomcat-5.5.25-apps
%MOAID%	%INSTALL_DIR%\apache-tomcat-5.5.25-moa-id-auth-1.4.3
%MOASPSS%	%INSTALL_DIR%\apache-tomcat-5.5.25-moa-spss-1.4.3
%MOAZS%	%INSTALL_DIR%\apache-tomcat-5.0.28-moazs-1.0

Daraus ergeben sich für die einzelnen Komponenten folgende Konfigurationsdateien.

Konfigurationsdateien

Komponente	Pfad
MOA-ID	%MOAID%\conf\moa-id\moa-id-config.xml
MOA-SP/SS	%MOASPSS%\conf\moa-spss\moa-spss-config.xml
MOA-ZS	%MOAZS%\webapps\moazs\WEB-INF\classes\moazs_config.xml bzw. falls die Anwendung noch nicht deployed wurde, dann die Datei WEB-INF\classes\moazs_config.xml innerhalb des WebArchivs %MOAZS%\webapps\moazs.war
MOA-ZS Proxy	%MOAZS%\conf\zsproxy\zsproxy_config.xml
PDF-AS	%APPS%\conf\esig\pdf-as\cfg\config.properties
Signatur-Anwendung bzw. Administrations- Komponente	%APPS%\conf\esig\application_config.xml
MOA-ZS Axis	%MOAZS%\webapps\moazs\WEB-INF\server-config.wsdd bzw. falls die Anwendung noch nicht deployed wurde, dann die Datei WEB-INF\server-config.wsdd innerhalb des WebArchivs %MOAZS%\webapps\moazs.war

Vor der Inbetriebnahme des vorkonfigurierten Pakets auf localhost sind folgende Tätigkeiten auszuführen.

- Installieren oder Bereitstellen einer MySQL 5.0.x-Datenbank.
- Im Falle von MySQL den Eintrag "max_allowed_packet=32M" in die entsprechende MySQL-Konfigurationsdatei unter der Rubrik "[mysqld]" einfügen.
- Erstellen einer Datenbank "esig" mit Benutzer "esig" (Passwort: "esig", erlaubten Host auf localhost festlegen).
- Erstellen einer Datenbank "zsproxy" mit Benutzer "zsproxy" (Passwort: "zsproxy", erlaubten Host auf localhost festlegen) sowie Ausführen des SQL Skripts %MOAZS%\scripts\sql\zsproxy_mysql.sql. Den Benutzer "zsproxy" mit allen Rechten für die Datenbank "zsproxy" ausstatten.
- Erstellen einer Datenbank "moazs" mit Benutzer "moazs" (Passwort: "moazs", erlaubten Host auf localhost festlegen) sowie Ausführen des SQL Skripts %MOAZS%\scripts\sql\moazs_mysql.sql. Den Benutzer "moazs" mit allen Rechten für die Datenbank "moazs" ausstatten.
- Ein Client-Zertifikat mit Verwaltungseigenschaft für die Elektronische Zustellung konfigurieren.
 Dazu die MOA-ZS-Konfigurations-Datei Zeile 14 ("`<keystore>`") und Zeile 16 ("`<keystorepw>`") anpassen.
- SMTP-Zugang zum Mail-Server sowie Absender-Mail-Adresse für MOA-ZS eintragen
 Dazu die MOA-ZS-Konfigurations-Datei Zeile 29 ("`<mailhost>`") und Zeile 31 ("`<sender>`") anpassen.
- SMTP-Zugang zum Mail-Server sowie Absender-Mail-Adresse für die Signatur-Anwendung eintragen.
 Dazu die Konfigurations-Datei der Signatur-Anwendung bzw. Administrations-Komponente Zeile 22 ("`<host>`") und Zeile 41 ("`<sender.email>`") anpassen.

- Eventuelles Anpassen sämtlicher Pfade für %INSTALL_DIR%
 - in der MOA-ZS-Konfigurations-Datei
 - in der MOA-ZS Axis Konfigurationsdatei Zeile 5
 - in %MOAZS%\scripts\setVariables.bat Zeile 6
 - in %APPS%\scripts\setVariables.bat Zeile 6
 - in %MOAID%\scripts\setVariables.bat Zeile 6
 - in %MOASPSS%\scripts\setVariables.bat Zeile 6

Wird die Anwendung schließlich für einen bestimmten Server konfiguriert sind zusätzlich folgende Anpassungen erforderlich:

- Server-SSL-Zertifikat in den MOA-ID TrustStore
 %MOAID%\conf\ssl\truststore[pwd=cacerts].jks aufnehmen.
- Redirects für die Signatur-Anwendung sowie für MOA-ID am Web-Server eintragen
 (siehe %INSTALL_DIR%\docs\IIS\config\workers.properties und
 %INSTALL_DIR%\docs\IIS\config\uriworkermap.properties)
- Externe URL der Signatur-Anwendung in der MOA-ID-Konfigurationsdatei Zeile 112
 und 115 anpassen.
- Externe URL der Signatur-Anwendung in die Konfigurationsdatei der Signatur-
 Anwendung bzw. Administrations-Komponente Zeile 5 eintragen.
- Externe URL von MOA-ID in die Konfigurationsdatei der Signatur-Anwendung bzw.
 Administrations-Komponente Zeile 58 eintragen.

Hinweis: Die vier Instanzen von Apache Tomcat können als Windows-Service eingerichtet werden. Hierfür befindet sich innerhalb jedes Apache Tomcat Containers ein Verzeichnis scripts, das folgende Skripte enthält:

installService.bat: Installiert ein Windows-Service über das der jeweilige Tomcat Container gestartet bzw. gestoppt werden kann.

Für die einzelnen Tomcat Instanzen wurden folgende Service-Namen gewählt:

Tomcat	angezeigter Name	Dienstname
%APPS%	ESIG TOMCAT v5.5.25 APPS	esigtomcat5525apps
%MOAID%	ESIG TOMCAT v5.5.25 MOA- ID-AUTH v1.4.3	esigtomcat5525moaidauth143
%MOASPSS%	ESIG TOMCAT v5.5.25 MOA- SPSS v1.4.3	esigtomcat5525moaspss143
%MOAZS%	ESIG TOMCAT v5.0.28 MOA-ZS v1.0	esigtomcat5028moazs10

removeService.bat: Entfernt ein zuvor installiertes Service (nur die Registry-Einträge).

setVariables.bat: Enthält die Umgebungskonfiguration für die jeweilige Tomcat Instanz.

updateService.bat: Werden die Umgebungseinstellungen in der Datei setVariables.bat geändert muss bei einer Installation als Service updateService.bat aufgerufen werden damit diese Einstellungen auch in die Registry übernommen werden.

`startTomcat.bat`: Startet die Tomcat-Instanz aus der Console (z.B. für Test-Zwecke).

`stopTomcat.bat`: Stoppt eine zuvor in der Console gestartete Instanz.

5.3 Konfiguration

Die Konfiguration der Signatur-Anwendung gliedert sich in zwei Teile:

- Konfiguration des Servlet-Containers Apache Tomcat (Abschnitt 5.3.1)
- Konfiguration des Front-Office bzw. des Back-Office (Abschnitt 5.3.2)

Die Konfigurationsdateien für Apache Tomcat, Front/Back-Office sowie für PDF-AS befinden sich im Verzeichnis `%APPS%\conf`.

5.3.1 Apache Tomcat

Die Konfiguration des Servlet-Containers für die Signatur- bzw. Administrationskomponente erfolgt über die Datei `%APPS%\conf\server.xml`. Hier werden die HTTP-, HTTPS-, SHUTDOWN- sowie der AJP-Port für einen Tomcat-Redirector konfiguriert. Weitere Informationen entnehmen Sie bitte der Dokumentation des Servlet-Containers [TOMCAT-DOC].

Die Beispielkonfiguration umfasst unter anderem die Datei `%APPS%\conf\tomcat-users.xml` in der für die Auslieferungsversion Benutzername und Passwort zur Absicherung des Back-Office eingetragen sind. Die Absicherung des Back-Office sollte implizit durch einen vorgeschalteten Web-Server erfolgen. Der Web-Server muss so konfiguriert werden, dass nur Anfragen für das Front-Office über einen AJP-Port an den dahinterliegenden Tomcat Container weitergeleitet werden. Sämtliche Ports der verwendeten Tomcat-Instanzen sollten so konfiguriert werden, dass diese nur auf Anfragen von `localhost` reagieren. Das Back-Office kann dann nur noch direkt vom Server aus aufgerufen werden, wodurch auf die Absicherung via Benutzername/Passwort verzichtet werden kann.

Weitere Informationen entnehmen Sie bitte der Dokumentation Ihres Web-Servers.

Die Signatur-Anwendung und die Administrations-Komponente erwarten ihre gemeinsame Konfiguration unter `%APPS%\conf\esig\application_config.xml`. Der Pfad kann jedoch auch über folgendes System-Property angepasst werden:

System-Property	Beschreibung
<code>esig.configuration</code>	Pfad zur Konfigurationsdatei der Web-Anwendungen, beispielsweise <code>C:\ESIG\apache-tomcat-5.5.25-apps\conf\esig\application_config.xml</code>

5.3.2 Front-Office/Back-Office

Die Konfiguration des Front- und des Back-Office befindet sich – sofern nicht anders konfiguriert – im Ordner %APPS%\conf\esig. Die hier enthaltene Konfigurationsdatei application_config.xml umfasst sämtliche Einstellungen für die beiden Web-Anwendungen.

Wie aus dem folgenden Listing zu entnehmen ist, wurde die Konfiguration in einzelne Kategorien eingeteilt (markierte Werte sind vor Inbetriebnahme der Anwendung anzupassen):

```
<properties>

  <category name="general">
    <frontend.externalurl>
      https://REPLACE_WITH_EXTERNAL_HOST_AND_PORT_OF_FRONTEND/esig
    </frontend.externalurl>
  </category>

  <category name="error">
    <mailto>REPLACE_WITH_ADMIN_URL</mailto>
  </category>

  <category name="delivery">

    <category name="types">
      <email>true</email>
      <moazs>true</moazs>
      <download>true</download>
    </category>

    <category name="email">
      <host>REPLACE_WITH_SMTP_HOST</host>
      <port>25</port>
      <!--
      <username>REPLACE_WITH_SMTP_USERNAME</username>
      <password>REPLACE_WITH_SMTP_PASSWORD</password>
      -->
      <subject>Zustellung eines signierten Dokuments</subject>
      <text>Hiermit übermitteln wir Ihnen ein signiertes Dokument.</text>

    <category name="activation">
      <subject>Aktivierung Ihres Zugangs bei e.sig</subject>
      <!-- allowed substitution tags are
      ${activation.url}, ${frontend.externalurl}, \n
      -->
      <text>
        Für Sie wurde ein Zugang bei e.sig eingerichtet.\n
        Um den Zugang zu aktivieren, klicken Sie bitte auf den folgenden Link und führen Sie
        ein Login mit Ihrer Bürgerkarte durch.\n\n
        ${activation.url}\n\n
        Nach einem erfolgreichem Login ist Ihr Benutzerkonto freigeschaltet. Ab diesem
        Zeitpunkt können Sie die Anwendung über folgenden Link nutzen:\n\n
        ${frontend.externalurl}\n\n
        Dies ist eine automatisiert erstellte E-Mail.
      </text>
      <sender.email>REPLACE_WITH_SENDER_OF_ACTIVATION_EMAIL</sender.email>
      <sender.name>e.sig</sender.name>
    </category>

  </category>

  <category name="moazs">
    <connection.url>
      http://REPLACE_WITH_MOAZS_HOST_AND_PORT/zsproxy/services/DeliveryRequest
    </connection.url>
    <request.url>
      http://REPLACE_WITH_MOAZS_HOST_AND_PORT/zsproxy/services/DeliveryNotificationRequest
    </request.url>
    <ismoazsproxy>true</ismoazsproxy>
    <showlookuplink>>false</showlookuplink>
  </category>

</category>
```

```

<category name="moaid">
  <!-- allowed substitution tags are
    ${scheme}, ${host}, ${port}, ${context}, ${serverurl}, ${baseurl}
  -->
  <connection.url>
    https://REPLACE_WITH_EXTERNAL_MOAID_HOST_AND_PORT/moa-id-auth/
  </connection.url>
  <connection.internal.url>
    http://REPLACE_WITH_INTERNAL_MOAID_HOST_AND_HTTP_PORT/moa-id-auth/
  </connection.internal.url>
  <!-- only needed if internal url (<connection.internal.url>) has not been set
  <keystore.uri>${catalina.base:-.}/conf/ssl-keys/REPLACE_WITH_KEYSTORE.jks</keystore.uri>
  <keystore.type>JKS</keystore.type>
  <keystore.password>REPLACE_WITH_KEYSTORE_PASSWORD</keystore.password>
  <key.password>REPLACE_WITH_KEY_PASSWORD</key.password>
  <truststore.uri>
    ${catalina.base:-.}/conf/ssl-keys/REPLACE_WITH_TRUSTSTORE.jks
  </truststore.uri>
  <truststore.type>JKS</truststore.type>
  <truststore.password>REPLACE_WITH_TRUSTSTORE_PASSWORD</truststore.password>
  -->
</category>

<category name="pdf-as">
  <mode>textual</mode>
  <config.dir>${catalina.base}/conf/esig/pdf-as</config.dir>
</category>

<category name="hibernate">
  <hibernate.connection.driver_class>com.mysql.jdbc.Driver</hibernate.connection.driver_class>
  <hibernate.connection.url>
    jdbc:mysql://REPLACE_WITH_DB_HOST_AND_PORT/REPLACE_WITH_NAME_OF_DATABASE
  </hibernate.connection.url>
  <hibernate.connection.username>REPLACE_WITH_USERNAME</hibernate.connection.username>
  <hibernate.connection.password>REPLACE_WITH_PASSWORD</hibernate.connection.password>
  <hibernate.dialect>org.hibernate.dialect.MySQLDialect</hibernate.dialect>
</category>

<category name="internal">
  <bpk.domain>T1</bpk.domain>
</category>

</properties>
    
```

Kategorie "general"

Schlüssel	Beschreibung
frontend.externalurl	Jene URL unter der die Signatur-Anwendung über das Internet erreichbar ist. Diese URL wird u.a. im Rahmen von Aktivierungs-Mails versandt.

Kategorie "error"

Schlüssel	Beschreibung
mailto	E-Mail-Adresse, die dem Anwender auf einer Fehlerseite zusammen mit der Fehlermeldung als Kontakt-Adresse angezeigt wird. Fehlerseiten werden nur bei abnormem Anwendungsverhalten bzw. intern aufgetretenen Fehlern angezeigt.

Kategorie "delivery"

Diese Kategorie umfasst sämtliche Einstellungen, die Zustellungen betreffen.

Unterkategorie "types"

Schlüssel	Beschreibung
download	Schaltet die Möglichkeit, signierte Dokumente via Download anzubieten ein (<code>true</code>) oder aus (<code>false</code>).
email	Schaltet die Möglichkeit, signierte Dokumente per E-Mail zuzustellen ein (<code>true</code>) oder aus (<code>false</code>).
moazs	Schaltet die Möglichkeit, signierte Dokumente mittels Elektronischer Zustellung zuzustellen ein (<code>true</code>) oder aus (<code>false</code>).

Unterkategorie "email"

Schlüssel	Beschreibung
host	SMTP-Host für den E-Mail Versand
port	Port des SMTP-Hosts (default: 25)
username	Benutzername des Mail-Kontos für den E-Mail Versand. Erlaubt der Server den Versand ohne Authentifizierung wird empfohlen, <code>username</code> und <code>password</code> nicht zu verwenden.
password	Passwort des Mail-Kontos für den E-Mail Versand. Erlaubt der Server den Versand ohne Authentifizierung wird empfohlen, <code>username</code> und <code>password</code> nicht zu verwenden.
payload.maxbytes	Maximale Dateigröße in Bytes von PDF-Dateien, die für den Versand via E-Mail erlaubt ist. (default: 6291456, d.h. 6 MB)
subject	Betreff von E-Mails, die signierte Dokumente enthalten
text	Text von E-Mails, die signierte Dokumente enthalten
xmailer	Bezeichnung der Anwendung, die Mails versendet (default: "e.sig").

Unter-Unterkategorie "activation"

Schlüssel	Beschreibung
sender.email	E-Mail Adresse des Absender-Kontos für automatisiert versandte Aktivierungs-Mails. Hier sollte eine gültige E-Mail Adresse verwendet werden um eventuelle Fehlermeldungen empfangen zu können.
sender.name	Absender-Name des Kontos für automatisiert versandte Aktivierungs-Mails (default: "e.sig")
subject	Betreff von Aktivierungs-Mails, die an potentielle Benutzer automatisiert versandt wird.
text	Text von Aktivierungs-Mails, die an potentielle Benutzer automatisiert versandt werden. Folgende Platzhalter sind hier erlaubt: <code>\${activation.url}</code> Aktivierungs-Link <code>\${frontend.externalurl}</code> .. Link zur Anwendung <code>\n</code> neue Zeile

Unterkategorie "moazs"

Schlüssel	Beschreibung
connection.url	URL zum MOA-ZS (bzw. MOA-ZS Proxy) Web-Service zum Versenden von Dokumenten. MOA-ZS sollte von der Web-Anwendung aus via HTTP erreichbar sein, extern jedoch – sofern Zustellbestätigungen nicht per E-Mail sondern über ein Web-Service entgegengenommen werden sollen – nur über HTTPS.
ismoazsproxy	Da MOA-ZS und MOA-ZS Proxy eine identische Web-Service Schnittstelle besitzen kann unter connection.url sowohl auf das MOA-ZS- als auch auf das MOA-ZS Proxy WebService verwiesen werden. Wurde ein MOA-ZS Proxy angegeben, muss ismoazsproxy auf "true" gesetzt werden, anderenfalls auf "false". Es wird empfohlen, MOA-ZS Proxy zu verwenden.
payload.maxbytes	Maximale Dateigröße in Bytes von PDF-Dateien, die für den Versand mit Elektronischer Zustellung erlaubt ist. (default: 1048576, d.h. 1 MB)
request.url	URL zum MOA-ZS Proxy Web-Service für die Abfrage von Zustellbestätigungen. Dies bedingt jedoch, dass das entsprechende MOA-ZS Sendeprofil so konfiguriert wird, dass Zustellbestätigungen über ein Web-Service und nicht per E-Mail zugestellt werden.
showlookuplink	Wird anstelle einer Zustellstatus-Verständigung per E-Mail die Verständigung über ein Web-Service gewählt UND wurde unter connection.url der MOA-ZS Proxy eingetragen bzw. ismoazsproxy auf "true" gesetzt, dann kann der Zustellstatus jederzeit durch Aufruf eines Links eingesehen werden. Wird showlookuplink auf "true" gesetzt, dann wird dem Anwender dieser Link nach Absenden des signierten Dokuments präsentiert. Ist kein Link erwünscht, ist hier "false" einzutragen.

Unterkategorie "download"

Schlüssel	Beschreibung
payload.maxbytes	Maximale Dateigröße in Bytes von PDF-Dateien, die für den Versand via E Mail erlaubt ist. (default: 6291456, d.h. 6 MB)

Kategorie "moid"

Hier wird die Authentisierungskomponente MOA-ID referenziert. Für einzutragende Werte in dieser Kategorie können folgende Platzhalter verwendet werden:

- `${scheme}`: Schema der Web-Anwendung "e.sig" (z.B. http oder https).
- `${host}`: Host der Web-Anwendung (z.B. behoerde.gv.at oder localhost).
- `${port}`: Port der Web-Anwendung
- `${context}`: Kontext der Web-Anwendung ("esig").
- `${serverurl}`: URL zum Server (z.B. https://behoerde.gv.at).
- `${baseurl}`: URL zur Web-Anwendung (z.B. https://behoerde.gv.at/esig/).

Darüber hinaus werden Java-System-Properties (z.B. `${catalina.base}`) substituiert.

Schlüssel	Beschreibung
<code>connection.url</code>	Externe URL zur MOA-ID-Web-Anwendung. Hier ist jene URL anzugeben, die extern (z.B. über ein Redirect eines Web-Servers) erreichbar ist.
<code>connection.internal.url</code>	Hier ist eine HTTP-URL anzugeben, über die MOA-ID intern erreicht werden kann (z.B. über <code>localhost</code>)

Die folgenden Parameter sind nur dann anzugeben, wenn `connection.internal.url` nicht gesetzt wurde. Über diese Parameter wird dann eine externe SSL-Verbindung zu MOA-ID konfiguriert.

<code>keystore.uri</code>	Pfad zum Keystore für die SSL-Verbindung
<code>keystore.type</code>	Typ des Keystores für die SSL-Verbindung (JKS oder PKCS12)
<code>keystore.password</code>	Passwort des Keystores für die SSL-Verbindung
<code>key.password</code>	Passwort des Schlüssels innerhalb der SSL-Verbindung im Falle von PKCS12)
<code>truststore.uri</code>	Pfad zum Truststore für die SSL-Verbindung
<code>truststore.type</code>	Typ des Truststores für die SSL-Verbindung (JKS oder PKCS12)
<code>truststore.password</code>	Passwort des Truststores für die SSL-Verbindung

Kategorie "pdf-as"

Diese Kategorie konfiguriert die PDF-Signatur-Komponente PDF-AS.

Darüber hinaus werden Java-System-Properties (z.B. `${catalina.base}`) substituiert.

Schlüssel	Beschreibung
<code>config.dir</code>	Pfad zum Konfigurationsverzeichnis von PDF-AS. Hinweis: Hier können auch Java System-Properties (z.B. <code>\${catalina.base}</code>) angegeben werden. Diese werden substituiert.
<code>mode</code>	Signatur-Modus (" <code>textual</code> " um PDF-Dokumente im Text-Modus zu signieren, " <code>binary</code> " um Binärsignaturen anzubringen).

Kategorie "hibernate"

Diese Kategorie umfasst die Konfiguration der Datenbank.

Schlüssel	Beschreibung
<code>hibernate.connection.driver_class</code>	Angabe der Treiber-Klasse für Hibernate. Wird MySQL verwendet sollte der Eintrag <code>com.mysql.jdbc.Driver</code> lauten. <u>Hinweis:</u> Kommt eine andere Datenbank zum Einsatz muss die angegebene Treiber-Klasse über eine datenbankspezifische Bibliothek zu Verfügung gestellt werden (analog zum MySQL-Connector).
<code>hibernate.connection.url</code>	Die Verbindungs-URL zur Datenbank. z.B. <code>jdbc:mysql://localhost:3306/esig</code>
<code>hibernate.connection.username</code>	Der Benutzername zum Zugriff auf die Datenbank.
<code>hibernate.connection.password</code>	Das Passwort zum Zugriff auf die Datenbank.

Schlüssel	Beschreibung
hibernate.dialect	Der Hibernate-spezifische Datenbank-Dialekt. Kommt MySQL zum Einsatz sollte der Eintrag <code>org.hibernate.dialect.MySQLDialect</code> lauten.

Kategorie "internal"

Diese Kategorie beinhaltet interne Einstellungen der Anwendung.

Schlüssel	Beschreibung
allow.twinidentity	Wenn diese Einstellung aktiviert ("true") ist, dann ist es möglich, mehrfach Benutzerkonten unter gleichem Vor- und Zunamen und Geburtsdatum einzurichten. In der Standardkonfiguration ist diese Einstellung deaktiviert ("false").
bpk.domain	Benutzer werden mittels ihres Bereichsspezifischen Personenkennzeichens (bPK) identifiziert. Diese Einstellung legt den Bereich fest, für den MOA-ID das bPK aus der Stammzahl berechnet. Die einzelnen möglichen Bereiche sind in der Bereichsabgrenzungsverordnung ([E-Gov-BerAbgrV]) definiert (z.B. "BF" für den Bildungs- und Forschungsbereich). Der Standard-Wert des Schlüssels <code>bpk.domain</code> wurde auf einen Test-Bereich "T1" festgelegt.

5.4 Neue Organisation registrieren

Die im Abschnitt 4 ("Administration") geschilderten Schritte umfassen die einzelnen Schritte zum Eintragen neuer Organisationen (inkl. Signatur- und Sendeprofile) über die Administrations-Komponente. Zusätzlich müssen jedoch auch die Konfigurationsdateien der Komponenten MOA-SP/SS, MOA-ZS sowie PDF-AS angepasst werden.

MOA-SP/SS

Siehe auch beispielhafte MOA-SP/SS Konfiguration im Anhang auf Seite 53.

- 1.) Signaturschlüssel der Organisation im PKCS#12-Format und das dazugehörige DER-kodierte X.509-Zertifikat in das Keys-Verzeichnis²⁷ von MOA-SP/SS kopieren, vorzugsweise in der Form `"schluesselbezeichnung[pwd=passwort].p12"` bzw. `"schluesselbezeichnung.der"`. Das Zertifikat ist hier zwar nicht explizit erforderlich, es erleichtert jedoch die spätere Zuordnung von Schlüssel zu Zertifikat.
- 2.) Signaturschlüssel in die MOA-SP/SS-Konfigurationsdatei eintragen:
 - a.) `SoftwareKeyModule` eintragen (Identifier wählen, Pfad zum Schlüssel-Container (PKCS12-Datei) und Passwort des Schlüssels eintragen)
 - b.) `KeyGroup` anlegen: Identifier für `KeyGroup` vergeben, den soeben gewählten Identifier des `SoftwareKeyModule` angeben und über `X509IssuerName` und `X509SerialNumber` das Schlüssel-Zertifikat auswählen.
 - c.) Den soeben gewählten Identifier für die `KeyGroup` als `KeyGroupId` in Liste unter `KeyGroupMapping` eintragen.
- 3.) Tomcat für MOA-SP/SS neu starten.

²⁷ Das Keys-Verzeichnis befindet sich normalerweise im MOA-SP/SS Konfigurationsverzeichnis.

MOA-ZS/MOA-ZS Proxy

Siehe auch beispielhafte MOA-ZS Konfiguration im Anhang auf Seite 51.

- 1.) MOA-ZS Konfigurationsdatei öffnen.
- 2.) Unter der Kategorie "SenderProfileIDInfo" (Zeile 140) die auskommentierte Organisation kopieren und alle Einträge die "CHANGEME" lauten entsprechend ändern. Einen Identifier als Kategorie-Namen wählen (sinnvollerweise eine aussagekräftige Bezeichnung ohne Leer- und Sonderzeichen in Kleinschreibung). Dieser Identifier ist der Sendeprofil-Name (siehe auch Abschnitt 4.3). Über diesen Namen wird u.a. auch der Absender bei Elektronischer Zustellung referenziert.
- 3.) Folgende Schlüssel der neuen Unterkategorie anpassen (nicht genannte Schlüssel bitte nicht verändern):
 - a.) <fullname>: Dieser Name scheint bei Zustellbestätigungen auf.
 - b.) <oid>: Beliebigen Identifier wählen.
 - c.) <organization>: Organisationsname (oder "n/a")
 - d.) <postalCode>: Postleitzahl
 - e.) <municipality>: Gemeinde
 - f.) <buildingNumber>: Hausnummer
 - g.) <unit>: Gebäudeeinheit, Stiege... (oder "n/a")
 - h.) <email>: E-Mail-Adresse (Wichtig! An diese E-Mail-Adresse werden Zustell-Protokolle bzw. Zustell-Nachweise übermittelt.)
 - i.) <senderEmail>: Absende-Email Adresse der Behörde
- 4.) MOA-ZS/MOA-ZS Proxy neu starten.

PDF-AS

Siehe auch beispielhafte PDF-AS Konfiguration im Anhang auf Seite 55.

- 1.) Logo der Organisation (im .png, .jpg oder .gif-Format, idealerweise mit etwa 660px x 660px) im Images-Verzeichnis im PDF-AS Konfigurationsverzeichnis²⁸ ablegen.
- 2.) PDF-AS Konfigurationsdatei öffnen.
- 3.) Bestehendes PDF-AS Profil kopieren (z.B. Zeile 217-262).
- 4.) Neuen Profil-Identifier vergeben (z.B. NEUER_IDENTIFIER). Das Profil-Identifier entspricht dem Namen des PDF-AS Profils (siehe auch Abschnitt 4.2). Bitte keine Leer- und Sonderzeichen für den Profil-Identifier verwenden (Underlines "_" sind erlaubt).
Der Profil-Identifier ist der zweite Part jedes profilbezogenen Konfigurationsschlüssels. z.B. sig_obj.EGIZ1.moa.sign.KeyIdentifier=...
- 5.) Folgende Schlüssel anpassen:
 - a.) sig_obj.NEUER_IDENTIFIER.moa.sign.KeyIdentifier: Der in der MOA-SP/SS Konfiguration definierte KeyGroup-Identifier. Dieser referenziert den für die Signatur zu verwendenden Schlüssel.
 - b.) sig_obj.NEUER_IDENTIFIER.value.SIG_LABEL: Das Logo der Organisation angeben. (z.B. ./images/myOrgLogo.png)

²⁸ %APPS%/conf/esig/pdf-as/images

- c.) `sig_obj.NEUER_IDENTIFIER.value.SIG_SUBJECT`: Der Name, der im Signaturblock verwendet werden soll. (z.B. Name der Organisation oder Name des Verantwortlichen). Ein Zeilenumbruch wird mit "`\n`" realisiert.
 - d.) `sig_obj.NEUER_IDENTIFIER.description`: Dieser Schlüssel enthält einen Beschreibungstext zum PDF-AS Profil (z.B. "A4-Hochformat", oder "Rechnungsformular XYZ"...)
- 6.) PDF-Profil aktivieren. Ab Zeile 213 folgende Zeile einfügen.
`sig_obj.types.NEUER_IDENTIFIER=on`
- 7.) Tomcat APPS neu starten.

6 Auslieferung

Die vorliegende Applikation wird zusammen mit den Quelltexten und dieser Dokumentation ausgeliefert.

6.1 Struktur

CATALINA_HOME	Tomcat-Home Verzeichnis ²⁹ .
common	Das common-Verzeichnis der Tomcat-Installation.
lib	Das common/lib-Verzeichnis der Tomcat-Installation ³⁰ .
mysql-connector-java-5.0.5.jar	Der MySQL-Datenbank-Connector.
CATALINA_BASE	Platzhalter für das lokale Tomcat-Installationsverzeichnis.
conf	Das Tomcat-Konfigurationsverzeichnis.
beispiel-konfiguration.zip	Beispielkonfiguration
webapps	Der webapps-Ordner von Tomcat.
e.sig	Generalisierte Signatur-Anwendung
esig.war	Das Back-Office als Web-Archiv.
esig-admin.war	Das Front-Office als Web-Archiv.
e.sig@school	Signaturanwendung für den Schulbereich
esig.war	Das Back-Office als Web-Archiv.
esig-admin.war	Das Front-Office als Web-Archiv.
FULL_PACKAGES	Vorkonfiguriertes Gesamtpaket inkl (MOA-SP/ZS/ID).
esig-complete-package.zip	Generalisierte Anwendung als Gesamtpaket
esig-school-complete-package.zip	Anwendung für den Schulbereich als Gesamtpaket
readme.txt	Anweisungen zum Einrichten der Pakete.
doc	Dokumentationsverzeichnis
esig_dokumentation.pdf	Installations- und Anwendungsdokumentation
source	Sourceverzeichnis
frontend-admin-core-projects.zip	Eclipse/Maven2-Projekt-Ordner
maven2-repository.zip	Maven2-Repository mit den Libraries für das Projekt.

²⁹ In der Praxis wird diese mit CATALINA_BASE übereinstimmen.

³⁰ Hinweis: Ab Tomcat Version 6.x entspricht "common/lib" dem Verzeichnis "lib".

Anhang

Der Anhang enthält Listings beispielhafter Konfigurationsdateien für MOA-ZS, MOA-ZS Proxy, MOA-SP/SS, MOA-ID sowie PDF-AS. Einträge die unter Umständen angepasst werden müssen, sind **gelb markiert**. Längere statische bzw. sicherlich nicht zu verändernde Passagen wurden aus Gründen der Übersichtlichkeit entfernt (gekennzeichnet mit [. . .]).

Erläuterungen zu den einzelnen Konfigurationsdateien entnehmen Sie bitte der jeweiligen Dokumentation (siehe Abschnitt "Referenzen").

Beispielhafte MOA-ZS Konfigurationsdatei

```
<?xml version="1.0"?>
<properties>

  <category name="general">
    <Application.Name>MOA-ZS</Application.Name>
    <!-- URL des Zusekopf -->
    <ZUSEurl>https://zkopf.zustellung.gv.at/zk.php?</ZUSEurl>
    <ZuseContainer>>false</ZuseContainer>
    <QueueID>1</QueueID>
    <!-- ping uri des server (ACHTUNG bei standalone ein 'moazs' aus dem pfad entfernen) -->
    <PingUrl>http://localhost:38080/moazs/moazs/ping</PingUrl>
    <WatchdogSleep>5000</WatchdogSleep>
    <WatchdogLimit>10000</WatchdogLimit>
    <defaultMailBody>
      C:/ESIG/apache-tomcat-5.0.28-moazs-1.0/conf/moa-zs/default-mailbody.txt
    </defaultMailBody>
    <keystore>
      C:/ESIG/apache-tomcat-5.0.28-moazs-1.0/conf/moa-zs/REPLACE_WITH_KEYSTORE.jks
    </keystore>
    <truststore>
      C:/ESIG/apache-tomcat-5.0.28-moazs-1.0/conf/moa-zs/truststore[pw=changeit].jks
    </truststore>
    <keystorepw>REPLACE_WITH_KEYSTORE_PASSWORD</keystorepw>
    <truststorepw>changeit</truststorepw>
    <!-- SUN VM -->
    <sslprovider>com.sun.net.ssl.internal.ssl.Provider</sslprovider>
    <sslpkgs>com.sun.net.ssl.internal.www.protocol</sslpkgs>
    <!-- IBM VM -->
    <!--
      <sslprovider>com.ibm.jsse.IBMJSSEProvider</sslprovider>
      <sslpkgs>com.ibm.net.ssl.internal.www.protocol</sslpkgs>
    -->
    <bereichskennung>urn:publicid:gv.at:cdid+ZU</bereichskennung>
    <bereichskennung_ver>urn:publicid:gv.at:ecdid+ZU</bereichskennung_ver>
    <!-- adresse des mailhost -->
    <mailhost>REPLACE_WITH_SMTP_HOST</mailhost>
    <!-- absenderadresse -->
    <sender>REPLACE_WITH_SENDER_ADDRESS@ABC.XYZ</sender>
    <subject>Zustellstatus</subject>
  </category>

  <category name="clientapp">
    <MaxRetry>5</MaxRetry>
    <RetryTimeout>10</RetryTimeout>
  </category>

  <category name="Hibernate">
    <hibernate.dialect>net.sf.hibernate.dialect.MySQLDialect</hibernate.dialect>
    <hibernate.connection.url>jdbc:mysql://localhost/moazs</hibernate.connection.url>
    <hibernate.connection.charset>utf-8</hibernate.connection.charset>
    <hibernate.connection.driver_class>com.mysql.jdbc.Driver</hibernate.connection.driver_class>
    <hibernate.connection.username>moazs</hibernate.connection.username>
    <hibernate.connection.password>moazs</hibernate.connection.password>
    <hibernate.c3p0.acquire_increment>1</hibernate.c3p0.acquire_increment>
    <hibernate.c3p0.idle_test_period>100</hibernate.c3p0.idle_test_period>
    <hibernate.c3p0.max_size>100</hibernate.c3p0.max_size>
    <hibernate.c3p0.max statements>0</hibernate.c3p0.max statements>
    <hibernate.c3p0.min size>10</hibernate.c3p0.min size>
    <hibernate.c3p0.timeout>100</hibernate.c3p0.timeout>
  </category>
```

```

<category name="Logging">
  <logLevel>WARNING</logLevel>
  <nrOfLogFiles>1</nrOfLogFiles>
  <logFile>C:/ESIG/apache-tomcat-5.0.28-moazs-1.0/logs/moazs.log</logFile>
  <logFileSize>20480</logFileSize>
  <useXML>false</useXML>
</category>

[...]

<category name="moass">
  <!-- adresse des MoaSS webservice -->
  <endpoint>http://localhost:28080/moa-spss/services/SignatureCreation</endpoint>
  <MaxRetry>5</MaxRetry>
  <RetryTimeout>10</RetryTimeout>
</category>

[...]

<category name="SenderProfileIDInfo">

  <!-- ***** EGIS TEST-ORGANISATION 1 ***** -->
  <category name="egiz1">
    <fullName>EGIZ Test-Organisation #1</fullName>
    <oid>EGIZ1</oid>
    <organization>EGIZ</organization>
    <postalCode>8010</postalCode>
    <countryCode>AT</countryCode>
    <municipality>Graz</municipality>
    <streetName>Inffeldgasse</streetName>
    <buildingNumber>16</buildingNumber>
    <unit>a</unit>
    <!--
      <webserviceUrl>
        http://localhost:38080/zsproxy/services/DeliveryNotification
      </webserviceUrl>
    -->
    <email>thomas.knall@egiz.gv.at</email>
    <senderEmail>thomas.knall@egiz.gv.at</senderEmail>
    <emailStylesheet>
      C:/ESIG/apache-tomcat-5.0.28-moazs-1.0/conf/moa-zs/emailstylesheet.xslt
    </emailStylesheet>
    <SkipDeckblatt>yes</SkipDeckblatt>
  </category>

  <!-- ***** EGIS TEST-ORGANISATION 2 ***** -->
  <category name="egiz2">
    <fullName>EGIZ Test-Organisation #2</fullName>
    <oid>EGIZ2</oid>
    <organization>EGIZ</organization>
    <postalCode>8010</postalCode>
    <countryCode>AT</countryCode>
    <municipality>Graz</municipality>
    <streetName>Inffeldgasse</streetName>
    <buildingNumber>16</buildingNumber>
    <unit>a</unit>
    <!--
      <webserviceUrl>
        http://localhost:38080/zsproxy/services/DeliveryNotification
      </webserviceUrl>
    -->
    <email>thomas.knall@egiz.gv.at</email>
    <senderEmail>thomas.knall@egiz.gv.at</senderEmail>
    <emailStylesheet>
      C:/ESIG/apache-tomcat-5.0.28-moazs-1.0/conf/moa-zs/emailstylesheet.xslt
    </emailStylesheet>
    <SkipDeckblatt>yes</SkipDeckblatt>
  </category>

```

```

<!-- ***** EMPTY TEMPLATE ***** -->
<!--
<category name="CHANGEME">
  <fullName>CHANGEME</fullName>
  <oid>CHANGEME</oid>
  <organization>CHANGEME</organization>
  <postalCode>CHANGEME</postalCode>
  <countryCode>AT</countryCode>
  <municipality>CHANGEME</municipality>
  <streetName>CHANGEME</streetName>
  <buildingNumber>CHANGEME</buildingNumber>
  <unit>CHANGEME</unit>
  <email>CHANGEME</email>
  <senderEmail>CHANGEME</senderEmail>
  <emailStylesheet>
    C:/ESIG/apache-tomcat-5.0.28-moazs-1.0/conf/moa-zs/emailstylesheet.xslt
  </emailStylesheet>
  <SkipDeckblatt>yes</SkipDeckblatt>
</category>
-->

</category>

</properties>

```

Beispielhafte MOA-ZS Proxy Konfigurationsdatei

```

<?xml version="1.0" encoding="UTF-8"?>
<properties>

  <category name="general">
    <delete.fetch>>false</delete.fetch>
    <max.backup>0</max.backup>
  </category>

  <category name="moazs">
    <connection.url>http://localhost:38080/moazs/services/DeliveryRequest</connection.url>
    <max.retry>10000</max.retry>
    <retry.timeout>1000</retry.timeout>
  </category>

  <category name="Hibernate">
    <hibernate.dialect>org.hibernate.dialect.MySQLDialect</hibernate.dialect>
    <hibernate.connection.url>jdbc:mysql://localhost/zsproxy</hibernate.connection.url>
    <hibernate.connection.charSet>utf-8</hibernate.connection.charSet>
    <hibernate.connection.driver_class>com.mysql.jdbc.Driver</hibernate.connection.driver_class>
    <hibernate.connection.username>zsproxy</hibernate.connection.username>
    <hibernate.connection.password>zsproxy</hibernate.connection.password>
    <hibernate.c3p0.acquire_increment>1</hibernate.c3p0.acquire_increment>
    <hibernate.c3p0.idle_test_period>100</hibernate.c3p0.idle_test_period>
    <hibernate.c3p0.max_size>100</hibernate.c3p0.max_size>
    <hibernate.c3p0.max_statements>0</hibernate.c3p0.max_statements>
    <hibernate.c3p0.min_size>10</hibernate.c3p0.min_size>
    <hibernate.c3p0.timeout>100</hibernate.c3p0.timeout>
  </category>

</properties>

```

Beispielhafte MOA-SP/SS Konfigurationsdatei

```

<?xml version="1.0" encoding="UTF-8"?>
<!--MOA SPSS 1.4 Configuration File-->
<cfg:MOAConfiguration
  xmlns:cfg=http://reference.e-government.gv.at/namespace/moaconfig/20021122#
  xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">

  <cfg:SignatureCreation>

    <cfg:KeyModules>

      <!-- KeyModule EGIZ Test-Organisation 1 -->
      <cfg:SoftwareKeyModule>
        <cfg:Id>SKM_egiz1</cfg:Id>
        <cfg:FileName>keys/esig/moa-signaturdienst-kunde1[pwd=kunde1].p12</cfg:FileName>
        <cfg>Password>kunde1</cfg>Password>
      </cfg:SoftwareKeyModule>

```

```

<!-- KeyModule EGIZ Test-Organisation 2 -->
<cfg:SoftwareKeyModule>
  <cfg:Id>SKM_egiz2</cfg:Id>
  <cfg:FileName>keys/esig/moa-signaturdienst-allekunden[pwd=allekunden].p12</cfg:FileName>
  <cfg:Password>allekunden</cfg:Password>
</cfg:SoftwareKeyModule>

</cfg:KeyModules>

<!-- KeyGroup EGIZ Test-Organisation 1 -->
<cfg:KeyGroup>
  <cfg:Id>KG_egiz1</cfg:Id>
  <cfg:Key>
    <cfg:KeyModuleId>SKM_egiz1</cfg:KeyModuleId>
    <cfg:KeyCertIssuerSerial>
      <dsig:X509IssuerName>CN=MOA Test CA,OU=EGIZ,O=TU Graz,C=AT</dsig:X509IssuerName>
      <dsig:X509SerialNumber>17</dsig:X509SerialNumber>
    </cfg:KeyCertIssuerSerial>
  </cfg:Key>
</cfg:KeyGroup>

<!-- KeyGroup EGIZ Test-Organisation 2 -->
<cfg:KeyGroup>
  <cfg:Id>KG_egiz2</cfg:Id>
  <cfg:Key>
    <cfg:KeyModuleId>SKM_egiz2</cfg:KeyModuleId>
    <cfg:KeyCertIssuerSerial>
      <dsig:X509IssuerName>CN=MOA Test CA,OU=EGIZ,O=TU Graz,C=AT</dsig:X509IssuerName>
      <dsig:X509SerialNumber>19</dsig:X509SerialNumber>
    </cfg:KeyCertIssuerSerial>
  </cfg:Key>
</cfg:KeyGroup>

<!-- Mapping ohne Client-Authentifizierung -->
<cfg:KeyGroupMapping>

  <!-- KeyGroupId EGIZ Test-Organisation 1 -->
  <cfg:KeyGroupId>KG_egiz1</cfg:KeyGroupId>

  <!-- KeyGroupId EGIZ Test-Organisation 2 -->
  <cfg:KeyGroupId>KG_egiz2</cfg:KeyGroupId>

</cfg:KeyGroupMapping>

<cfg:XMLDSig>
  <cfg:CanonicalizationAlgorithm>
    http://www.w3.org/TR/2001/REC-xml-c14n-20010315
  </cfg:CanonicalizationAlgorithm>
  <cfg:DigestMethodAlgorithm>http://www.w3.org/2000/09/xmldsig#sha1</cfg:DigestMethodAlgorithm>
</cfg:XMLDSig>

</cfg:SignatureCreation>

<cfg:SignatureVerification>

[...]

</cfg:SignatureVerification>

</cfg:MOAConfiguration>

```

Beispielhafte MOA-ID Konfigurationsdatei

```
<?xml version="1.0" encoding="UTF-8"?>
<MOA-IDConfiguration xmlns=http://www.buergerkarte.at/namespaces/moaconfig#
  xmlns:dsig=http://www.w3.org/2000/09/xmldsig#
  xmlns:s110=http://www.buergerkarte.at/namespaces/securitylayer/20020225#
  xmlns:s111="http://www.buergerkarte.at/namespaces/securitylayer/20020831#">

  [...]

  <!-- ESIG -->
  <OnlineApplication type="publicService"
    publicURLPrefix="https://localhost:48443/esig/moaid-login">
    <AuthComponent provideStammzahl="false" provideAUTHBlock="false"
      provideIdentityLink="false" provideCertificate="false">
      <Templates>
        <Template URL="https://localhost:48443/esig/moaid-template.do"/>
      </Templates>
    </AuthComponent>
  </OnlineApplication>

  [...]

</MOA-IDConfiguration>
```

Beispielhafte PDF-AS Konfigurationsdatei

```
[...]

#####
# Signaturdienste

[...]

# MOA Settings
moa.available_for_web=true
moa.available_for_commandline=true

moa.sign.url=http://localhost:28080/moa-spss/services/SignatureCreation
# default Key Identifier (wenn im Signaturprofil kein Key Identifier konfiguriert wird).
moa.sign.KeyIdentifier=KG_egiz1

# default moa enveloping sign template file
moa.sign.request.base64=./templates/default.moa.sign.enveloping.xml
# default moa detached sign template file
moa.sign.request.detached=./templates/default.moa.sign.detached.xml

# MOA Verifying
# Prüf-Einstellungen sind für diese Anwendung egal, da keine Signaturprüfungen vorgesehen sind
moa.verify.url=http://localhost:28080/moa-spss/services/SignatureVerification
moa.verify.TrustProfileID=Test-Signaturdienste

# default moa enveloping verify template files
moa.verify.request.base64=./templates/default.moa.verify.request.enveloping.xml
moa.verify.template.base64=./templates/default.moa.verify.template.enveloping.xml

# default moa detached verify template files
moa.verify.request.detached=./templates/default.moa.verify.request.detached.xml
moa.verify.template.detached=./templates/default.moa.verify.template.detached.xml

#####
# Responsemeldungen der Signaturdienste

[...]

#####
# Anzeige von OID Feldern eines Zertifikats im Prüfergebnis

oid.root=1.2.40.0.10
oid.1_2_40_0_10_1_1_1=Verwaltungseigenschaft
oid.1_2_40_0_10_1_1_2=Dienstleistereigenschaft
```

```
#####  
# Standardfeldlängen der Felder für die Binärsignatur  
  
defaults.phlength.SIG_DATE=50  
defaults.phlength.SIG_NUMBER=50  
defaults.phlength.SIG_ISSUER=250  
defaults.phlength.SIG_VALUE=350  
defaults.phlength.SIG_ID=90  
  
defaults.phlength.SIG_NAME=150  
  
#####  
# LDAP-Mappings  
  
[...]  
  
#####  
# Signatur-Profile  
  
sig_obj.type.default=EGIZ1  
sig_obj.types.EGIZ1=on  
sig_obj.types.EGIZ2=on  
  
#####  
# Signatur Profil (EGIZ Test-Organisation #1)  
sig_obj.EGIZ1.moa.sign.KeyIdentifizier=KG_egiz1  
sig_obj.EGIZ1.value.SIG_LABEL=./images/egiz.png  
sig_obj.EGIZ1.value.SIG_SUBJECT=EGIZ Test-Organisation #1  
sig_obj.EGIZ1.description=Standard-Dokument (deutsch)  
  
sig_obj.EGIZ1.start_text=Signaturwert  
  
sig_obj.EGIZ1.key.SIG_VALUE=Signaturwert  
#sig_obj.EGIZ1.key.SIG_NAME=Unterzeichner  
sig_obj.EGIZ1.key.SIG_SUBJECT=Unterzeichner  
sig_obj.EGIZ1.key.SIG_DATE=Datum/Zeit-UTC  
sig_obj.EGIZ1.key.SIG_ISSUER=Aussteller-Zertifikat  
sig_obj.EGIZ1.key.SIG_NUMBER=Serien-Nr.  
sig_obj.EGIZ1.key.SIG_KZ=Methode  
sig_obj.EGIZ1.key.SIG_ID=Parameter  
sig_obj.EGIZ1.key.SIG_META=Prüfhinweis  
  
sig_obj.EGIZ1.value.SIG_META=Prüfservice: https://demo.a-sit.at/el\_signatur/verification  
  
#----- MAIN TABLE -----  
sig_obj.EGIZ1.table.main.1=SIG_VALUE-cv  
sig_obj.EGIZ1.table.main.2=SIG_LABEL-i|TABLE-info  
sig_obj.EGIZ1.table.main.3=SIG_META-cv  
  
sig_obj.EGIZ1.table.main.ColsWidth=1 5  
sig_obj.EGIZ1.table.main.Style.bgcolor=255 255 255  
sig_obj.EGIZ1.table.main.Style.padding=3  
sig_obj.EGIZ1.table.main.Style.border=0.1  
sig_obj.EGIZ1.table.main.Style.halign=left  
sig_obj.EGIZ1.table.main.Style.valign=middle  
sig_obj.EGIZ1.table.main.Style.font=HELVETICA, 8, NORMAL  
sig_obj.EGIZ1.table.main.Style.valuefont=HELVETICA, 8, NORMAL  
  
#----- INFO TABLE -----  
sig_obj.EGIZ1.table.info.ColsWidth=1 4  
#sig_obj.EGIZ1.table.info.1=SIG_NAME-cv  
sig_obj.EGIZ1.table.info.1=SIG_SUBJECT-cv  
sig_obj.EGIZ1.table.info.2=SIG_DATE-cv  
sig_obj.EGIZ1.table.info.3=SIG_ISSUER-cv  
sig_obj.EGIZ1.table.info.4=SIG_NUMBER-cv  
sig_obj.EGIZ1.table.info.5=SIG_KZ-cv  
sig_obj.EGIZ1.table.info.6=SIG_ID-cv
```

```
#####  
# Signatur Profil (EGIZ Test-Organisation #2)  
sig_obj. EGIZ2.moa.sign.KeyIdentifier=KG_egiz2  
sig_obj. EGIZ2.value.SIG_LABEL=./images/egiz_en.png  
sig_obj. EGIZ2.value.SIG_SUBJECT=EGIZ Test-Organisation #2  
sig_obj. EGIZ2.description=Standard-Dokument (englisch)  
  
sig_obj. EGIZ2.start_text=Signature Value  
  
sig_obj. EGIZ2.key.SIG_VALUE=Signature Value  
#sig_obj. EGIZ2.key.SIG_NAME=Signatory  
sig_obj. EGIZ2.key.SIG_SUBJECT=Signatory  
sig_obj. EGIZ2.key.SIG_DATE=Date/Time-UTC  
sig_obj. EGIZ2.key.SIG_ISSUER=Issuer-Certificate  
sig_obj. EGIZ2.key.SIG_NUMBER=Serial-No.  
sig_obj. EGIZ2.key.SIG_KZ=Method  
sig_obj. EGIZ2.key.SIG_ID=Parameter  
sig_obj. EGIZ2.key.SIG_META=Verification  
  
sig_obj. EGIZ2.value.SIG_META=Service: https://demo.a-sit.at/el\_signatur/verification  
  
#----- MAIN TABLE -----  
sig_obj. EGIZ2.table.main.1=SIG_VALUE-cv  
sig_obj. EGIZ2.table.main.2=SIG_LABEL-i|TABLE-info  
sig_obj. EGIZ2.table.main.3=SIG_META-cv  
  
sig_obj. EGIZ2.table.main.ColsWidth=1 5  
sig_obj. EGIZ2.table.main.Style.bgcolor=255 255 255  
sig_obj. EGIZ2.table.main.Style.padding=3  
sig_obj. EGIZ2.table.main.Style.border=0.1  
sig_obj. EGIZ2.table.main.Style.halign=left  
sig_obj. EGIZ2.table.main.Style.valign=middle  
sig_obj. EGIZ2.table.main.Style.font=HELVETICA, 8, NORMAL  
sig_obj. EGIZ2.table.main.Style.valuefont=HELVETICA, 8, NORMAL  
  
#----- INFO TABLE -----  
sig_obj. EGIZ2.table.info.ColsWidth=1 4  
#sig_obj. EGIZ2.table.info.1=SIG_NAME-cv  
sig_obj. EGIZ2.table.info.1=SIG_SUBJECT-cv  
sig_obj. EGIZ2.table.info.2=SIG_DATE-cv  
sig_obj. EGIZ2.table.info.3=SIG_ISSUER-cv  
sig_obj. EGIZ2.table.info.4=SIG_NUMBER-cv  
sig_obj. EGIZ2.table.info.5=SIG_KZ-cv  
sig_obj. EGIZ2.table.info.6=SIG_ID-cv
```

Erhebungsblatt

Das hier abgebildete Erhebungsblatt erleichtert die Aufnahme neuer Organisationen und Benutzer in das System. Es kann zur Erhebung der erforderlichen Daten verwendet werden.

Angaben zur Organisation

Bezeichnung	Beschreibung	verwendet für	gewünschter Wert
Name	vollständiger Name der Organisation	Elektronische Zustellung	
Absender Name	Name des Absenders bei E-Mail-Zustellung (optional)	E-Mail Zustellung	
Absender E-Mail	E-Mail Adresse des Absenders bei E-Mail-Zustellung	E-Mail Zustellung	
E-Mail für Bestätigungen	An diese Adresse werden Bestätigungen bei Elektronischer Zustellung übermittelt.	Elektronische Zustellung	
Adresse der Organisation	Postleitzahl, Ort, Straße, Hausnummer	Elektronische Zustellung	
Signaturmarke	vorzugsweise 660x660 Pixel; Formate: .png, .jpg, .gif	PDF-Signatur	
Hintergrundfarbe Signaturmarke	RGB-Wert der Hintergrundfarbe der Signaturmarke (derzeit per default RGB: 245 245 240)	PDF-Signatur	

Bezeichnung	Beschreibung	verwendet für	gewünschter Wert
fix definierte Positionen der Signaturmarke + Bezeichnung	Normalerweise wird die Signaturmarke dynamisch an das Ende des Dokuments gesetzt. Wird eine fixe Position (in PDF-Koordinaten) gewünscht, muss diese über (X-Position, Y-Position, sowie optional Seitennummer angegeben werden). Die Breite kann auch angegeben werden. Für jede Angabe wird ein eigenständiges Profil angelegt, das entsprechend bezeichnet werden sollte. z.B.: "Diplomzeugnis": x:642;y:200;w:500;p:2 "Elternbrief": x:300;y:156;p:1 "Mustertext": x:100;y:100;w:450 "Abrechnung": x:150;y:150	PDF-Signatur	
Unterzeichner	Name des Unterzeichners im Signaturblock z.B.: Direktor Max Mustermann MusterOrganisation Musterort	PDF-Signatur	

Angaben für jeden registrierten Benutzer

Bezeichnung	Beschreibung	verwendet für	gewünschter Wert
Vorname(n)	sämtliche Vornamen laut Bürgerkarte	Login mit Bürgerkarte	
Familienname	Nachname laut Bürgerkarte	Login mit Bürgerkarte	
Geburtsdatum	Geburtsdatum (Tag, Monat, Jahr)	Login mit Bürgerkarte	
E-Mail Adresse	An diese E-Mail Adresse wird ein spezieller Link zur Aktivierung eines Kontos versan^dt.		
Organisation	Angabe welcher Organisation der Benutzer zugeordnet werden muss.		

Referenzen

[E-Gov-BerAbgrV]	<i>E-Government-Bereichsabgrenzungsverordnung (E-Gov-BerAbgrV)</i> , 289. Verordnung, ausgegeben am 15.07.2004 abgerufen aus dem World Wide Web a. 10.01.2008 unter http://ris1.bka.gv.at/App/finDBGbl.aspx?name=entwurf&format=pdf&docid=COO_2026_100_2_112317
[EGovG]	<i>E-Government-Gesetz (E-GovG)</i> , BGBl. Nr. 10/2004, ausgegeben am 27.02.2004 abgerufen aus dem World Wide Web am 03.01.2008 unter http://ris1.bka.gv.at/authentic/finDBGbl.aspx?name=entwurf&format=pdf&docid=COO_2026_100_2_30412
[HBM-DB]	<i>Supported Hibernate Databases</i> Hibernate Dokumentation abgerufen aus dem World Wide Web am 31.10.2007 unter http://www.hibernate.org/80.html
[KEYWORDS]	Bradner, S.: RFC 2119: <i>Key words for use in RFCs to Indicate Requirement Levels</i> . IETF Request For Comment, März 1997. Abgerufen aus dem World Wide Web am 20.09.2007 unter http://www.ietf.org/rfc/rfc2119.txt
[MOA-ID-HB]	<i>Module für Online-Applikationen – Identifikation (Handbuch)</i> Version 1.4 abgerufen aus dem World Wide Web am 31.10.2007 unter http://moa-idspss.egovlabs.gv.at/handbook/id/moa_id/moa.htm
[MOA-ID-SPEZ]	R. Schamberger, G. Karlinger und L. Moser: <i>Module für Online-Applikationen – Identifikation (Spezifikation)</i> Version 1.4 vom 02.08.2007 abgerufen aus dem World Wide Web am 31.10.2007 unter http://egovlabs.gv.at/docman/view.php/6/13/MOA_ID_1.4_20070802.pdf
[MOA-SPSS-HB]	<i>Module für Online-Applikationen – Serversignatur und Signaturprüfung (Handbuch)</i> Version 1.4 abgerufen aus dem World Wide Web am 31.10.2007 unter http://moa-idspss.egovlabs.gv.at/handbook/spss/index.html
[MOA-SPSS-SPEZ]	R. Schamberger und L. Moser: <i>Module für Online-Anwendungen (Spezifikation)</i> Version 1.1 vom 30.06.2003 abgerufen aus dem World Wide Web am 31.10.2007 unter http://egovlabs.gv.at/docman/view.php/6/5/MOA-SPSS-1.1_20030630.pdf
[MOA-ZS-AHB]	R. Treutlein und A. Erlacher: <i>Administrationshandbuch zu MOA-ZS</i> Version 0.40 vom 02.11.2004 abgerufen aus dem World Wide Web am 31.10.2007 unter http://www.cio.gv.at/it-infrastructure/delivery/mzs_final/doku.zip

[MOA-ZS-BHB]	A. Heinrich, R. Treutlein und A. Erlacher: <i>Benutzerhandbuch zu MOA-ZS</i> Version 0.4 vom 09.11.2004 abgerufen aus dem World Wide Web am 31.10.2007 unter http://www.cio.gv.at/it-infrastructure/delivery/mzs_final/doku.zip
[MOA-ZS-IHB]	R. Treutlein und A. Erlacher: <i>Installationshandbuch zu MOA-ZS</i> Version 0.51 vom 08.11.2004 abgerufen aus dem World Wide Web am 31.10.2007 unter http://www.cio.gv.at/it-infrastructure/delivery/mzs_final/doku.zip
[MOA-ZS-Proxy]	A. Tauber: Dokumentation Zustellproxy Version 1.0 vom 18.07.2006 abgerufen aus dem World Wide Web am 03.01.2008 unter http://demo.egiz.gv.at/plain/content/download/318/1495/file/Dokumentation.pdf
[MOA-ZS-SPEZ]	L. Naber und M. Liehmann: <i>MOA-ZS – Technische Spezifikation</i> Version 1.0 vom 18.05.2004 abgerufen aus dem World Wide Web am 31.10.2007 unter http://www.cio.gv.at/it-infrastructure/delivery/mzs/mzsspec.pdf
[MOA-ZS-TDOK]	A. Heinrich, N. Gradwohl, R. Treutlein und A. Erlacher: <i>Technische Dokumentation zu MOA-ZS</i> Version 0.4 vom 10.11.2004 abgerufen aus dem World Wide Web am 31.10.2007 unter http://www.cio.gv.at/it-infrastructure/delivery/mzs_final/doku.zip
[PDF-AS]	W. Lackner, W. Prinz: <i>Signatur für elektronische Aktenführung (PDF-Amtssignaturen)</i> Anwenderdokumentation, Version 2.7.1 vom 01.07.2007
[SL12]	A. Hollosi, G. Karlinger: <i>Die österreichische Bürgerkarte, Applikationsschnittstelle Security-Layer</i> Version 1.2.2 vom 01.03.2005 abgerufen aus dem World Wide Web am 03.01.2008 unter http://www.buergerkarte.at/konzept/securitylayer/spezifikation/aktuell/core/Core.html
[TOMCAT-DOC]	The Apache Software Foundation, <i>The Apache Tomcat 5.5 Servlet/JSP Container</i> Dokumentation, abgerufen aus dem World Wide Web am 05.12.2007 unter http://tomcat.apache.org/tomcat-5.5-doc/index.html