

Bayerische Verwaltungs-PKI

Public Key Infrastructure



Anwendungsgebiete

- Sichere E-Mail zwischen Behörden
- Windows LogOn mit Smartcard
- SSL/TLS (https://)
- USW.

Allgemeines



Sinn und Zweck einer PKI

Die zentrale Fragen zur Sicherheit in der Informationstechnologie:

> **Vertraulichkeit**

Wie stelle ich sicher, dass nur befugte Nutzer Zugriff auf bestimmte Daten erhalten?

> **Integrität**

Wie stelle ich sicher, dass Daten nicht unbefugt verändert werden?

> **Authentizität**

Wie stelle ich sicher, dass ein Nutzer tatsächlich die Person ist, die er vorgibt zu sein?

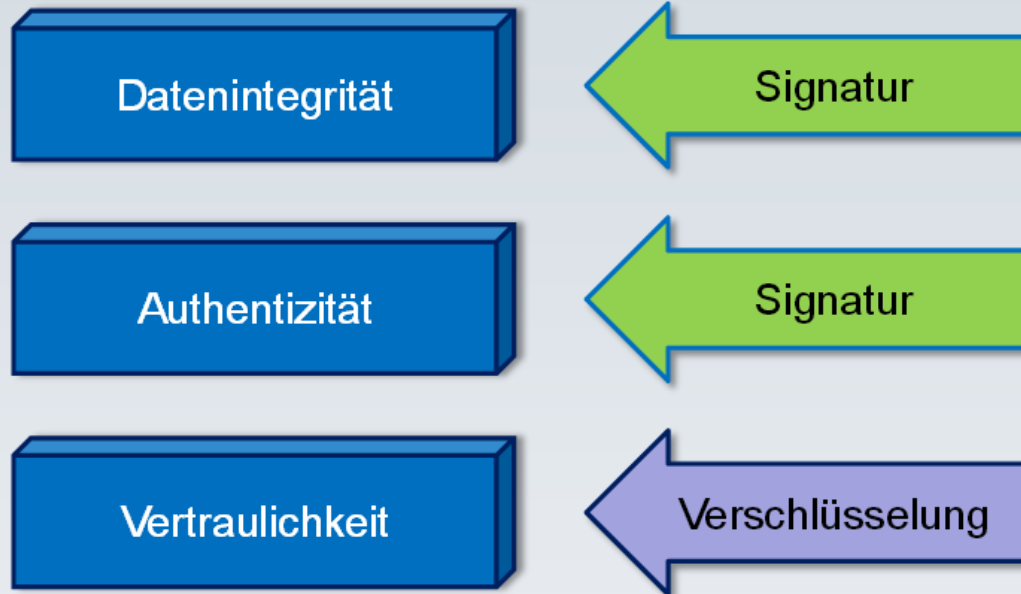
> **Verbindlichkeit**

Wie stelle ich sicher, dass eine elektronische Kommunikation oder ein elektronischer Prozess tatsächlich stattgefunden hat bzw. nicht abgestritten werden kann?

**Eine Public Key Infrastruktur ist eine Möglichkeit,
diese Sicherheiten in der IT zu gewährleisten!**

Allgemeines

Was ist „sichere elektronische Kommunikation“?



Von der sicheren elektronischen Kommunikation ist die Schriftformerfüllung zu unterscheiden!

Allgemeines



<Grundlagen PKI – Begriffsbestimmungen (1)>

> Asymmetrische Kryptographie

Einsatz eines **Schlüsselpaars** als Basis für kryptographische Verfahren, bestehend aus einem öffentlichen Schlüssel (**Public Key**) und einem privaten Schlüssel (**Private Key**)

> Public Key

Nicht geheimer bzw. **öffentlicher Schlüssel** eines asymmetrischen Schlüsselpaars, der zur **Verschlüsselung** von Daten oder zur **Prüfung einer elektronischen Signatur** benutzt wird.

> Private Key

Geheimer Schlüssel eines asymmetrischen Schlüsselpaars, der zur **Entschlüsselung** von Daten oder zur **Erzeugung einer elektronischen Signatur** benutzt wird.

Allgemeines



Grundlagen PKI – Verschlüsselung

Private Key (S) und Public Key (S')

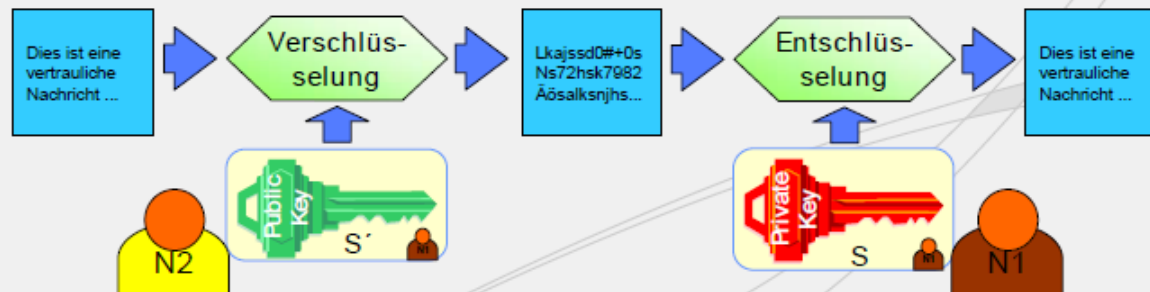
Der Nutzer N1 verfügt über ein Schlüsselpaar S (geheim) und S' (öffentlich).

Verschlüsselung:

Ein Nutzer N2 verschlüsselt die Information mit dem öffentlichen Schlüssel S' und versendet die verschlüsselte Information an Nutzer N1.

Entschlüsselung:

Nutzer N1 entschlüsselt die verschlüsselte Information durch Anwendung seines privaten Schlüssels S und erhält als Ergebnis die ursprüngliche Information.



23.11.2008

6

Zentrales Postfach



Verwaltungsservice
Bayern



[BEHÖRDEN](#) | [LEISTUNGEN](#) | [LEBENSLAGEN](#) | [ONLINE-SERVICES](#)

Suchbegriff eingeben



Startseite > Behörden > Landratsämter > Neustadt a.d.Aisch-Bad Windsheim

Behörden

- Allgemeine Suche
- Hierarchische Übersicht
- Alphabetische Übersicht
- Kartensuche

LOKALISIERUNG

Bitte auswählen, damit ggf. weitere Informationen angezeigt werden.

PLZ / Ort

Wählen

Landratsamt Neustadt a.d.Aisch-Bad Windsheim

Hausanschrift Konrad-Adenauer-Str. 1
91413 Neustadt a.d.Aisch

Postanschrift Postfach 1520
91405 Neustadt a.d.Aisch

Telefon +49 (0)9161 92-0
Telefax +49 (0)9161 92-106

Webseite <http://www.kreis-nea.de>

E-Mail poststelle@kreis-nea.de

Landrat Walter Schneider

Einwohnerzahl 97.536 (Stand: 30. September 2013)



ZUR BEHÖRDE

- Gebäude, Öffnungszeiten
- Ansprechpartner
- Organigramm

ZUM LANDKREIS

- Gemeinden
- Städtische und

Landratsamt Neustadt a. d. Aisch - Bad Windsheim

Bad Windsheim	info@bad-windsheim.de	Marktbergel	rathaus@marktbergel.de
Baudenbach	gemeinde@baudenbach.de	Münchsteinach	gemeinde@muenchsteinach.de
Burgbernheim	info@burgbernheim.de	Neuhof a.d.Zenn	markt.neuhof@vg-neuhof.de
Burghaslach	gemeinde@burghaslach.de	Neustadt a.d.Aisch	info@neustadt-aisch.de
Dachsbach	dachsbach@vg-uehlfeld.de	Oberickelsheim	gemeinde@oberickelsheim.de
Diespeck	gemeinde@diespeck.de	Obernzenn	info@obernzenn.de
Dietersheim	gemeinde@dietersheim.de	Oberscheinfeld	info@oberscheinfeld.de
Emskirchen	info@emskirchen.de	Scheinfeld	info@scheinfeld.de
Ergersheim	gemeinde@ergersheim.de	Simmershofen	info@simmershofen.de
Gallmersgarten	gallmersgarten@gmx.de	Sugenheim	info@sugenheim.de
Gerhardshofen	gerhardshofen@vg-uehlfeld.de	Trautskirchen	info@trautskirchen.de
Gollhofen	gemeinde@gollhofen.de	Uehlfeld	info@vg-uehlfeld.de
Gutenstetten	gemeinde@gutenstetten.de	Uffenheim	info@uffenheim.de
Hagenbüchach	info@hagenbuechach.de	Weigenheim	gemeinde@weigenheim.de
Hemmersheim	verwaltungsgemeinschaft@uffenheim.de	Wilhelmsdorf	info@wilhelmsdorf.de
Illesheim	info@illesheim.de		
Ippesheim	info@ippesheim.de	VG Burgbernheim	info@burgbernheim.de
Ipsheim	info@ipsheim.de	VG Diespeck	verwaltungsgemeinschaft@vg-diespeck.de
Langenfeld	buergermeister@langenfeld-mfr.de	VG Hagenbüchach-Wilh.	info@wilhelmsdorf.de
Markt Bibart	kanzlei-marktbibart@t-online.de	VG Neuhof a.d.Zenn	info@vg-neuhof.de
Markt Erlbach	info@markt-erlbach.de	VG Scheinfeld	info@vgem.scheinfeld.de
Markt Nordheim	gemeinde@markt-nordheim.de	VG Uehlfeld	info@vg-uehlfeld.de
Markt Taschendorf	info@markttaschendorf.de	VG Uffenheim	verwaltungsgemeinschaft@uffenheim.de

VG oder Gemeinde

- Beispiel: Es gibt 1 VG-Postfach und 5 Gde-Postfächer
- für alle Postfächer ist dieselbe Person verantwortlich (gleiches Dienstgebäude, gleiche Telefonnr.)
→ nur die VG-Funktionsstelle anlegen
- alle Postfächer werden von unterschiedlichen Personen gelesen (Sekretärinnen der Bürgermeister)
→ alle Funktionsstellen anlegen
- Die Verwaltungsgemeinschaften sollten mir mitteilen, wie es bei ihnen organisiert ist.

Reihenfolge

- Registrierungsformulare
- Identifizierung (Ausweiskopie)
- LRA beantragt Zertifikate
- Zertifikate installieren
- Outlook-Einstellungen anpassen
- Funktionstest mit poststelle@kreis-nea.de

Registrierung



Teilnehmer-
Registrierung

Frank Härtlein
frank.haertlein@beispielheim.de
09161 999-99
Gemeinde Beispielheim
Frank Härtlein
Broller, 1. Bgm.



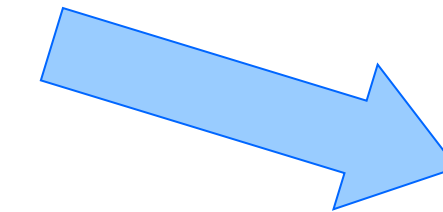
Funktionsstellen-
Registrierung

Poststelle
poststelle@beispielheim.de
Verantwortlicher:
Frank Härtlein
frank.haertlein@beispielheim.de
09161 999-99
Gemeinde Beispielheim
Frank Härtlein
Broller, 1. Bgm.

Registrierung



Formulare



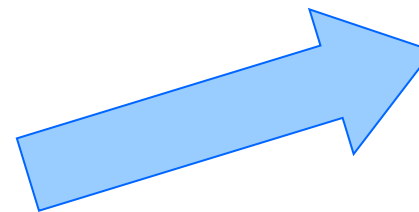
Mail/Post/persönlich
abgeben



Landratsamt
Zimmer A 110
(ggüb. Büro des Landrats)
Herr Härtlein / Herr Krug



Personalausweis



FSt.-Verantwortlicher
muss persönlich erscheinen

Registrierung

Im Landratsamt:

- Anlegen der Behörde im System (Gemeinde Beispielheim)
- Anlegen der Funktionsstelle (poststelle@beispielheim.de)
- Anlegen des/der Verantwortlichen
- Diese Person bekommt vom Landratsamt einen Registrierungsbrief
- Beantragung der Zertifikate

In den Gemeinden

- Per E-Mail bekommen Sie zwei Dateien:



enc_Poststelle.p12

Encryption = Verschlüsselung




sig_Poststelle.p12

Signature

- Diese Dateien gut aufheben!

In den Gemeinden

Bayerisches Landesamt für
Statistik und Datenverarbeitung 
Rechenzentrum Süd

Trustcenter der Bayerischen Verwaltung
Persönlich und vertraulich

Paula Post
Gemeinde Posthausen

Hauptstraße 1
98765 Posthausen

Ihre Zeichen Unsere Zeichen Telefon 089 2119-4924 E-Mail: München,
Ihre Nachricht vom Nachricht vom Telefax 089 2119-14924 trustcenter@lstad.bayern.de 03.12.2012
Teilnehmernummer: 0000049

Transport-PIN für Ihre Funktionsstellen-Zertifikate

Sehr geehrte Frau Post,
Ihre Registrierungsstelle hat für Sie ein Funktionsstellen-Zertifikat beantragt.
Dieses wurden Ihnen bereits per E-Mail zugesendet.
Anbei finden Sie die zum Installieren notwendige Transport-PIN:

Funktionsstellenbezeichnung: Posthausen, Poststelle
Zertifikatstyp: ENCRYPTION (key encipherment; data encipherment)

Zertifikats-Serienr.: 4abd
Transport-PIN: P7W3Q6YAFJ

Bitte beachten Sie auch unsere Informationen auf <https://www.pki.bayern.de>.
Für weitere **Fragen** wenden Sie sich bitte an **Ihre Registrierungsstelle**.

Dieses Schreiben wurde automatisch generiert und trägt daher keine Unterschrift.

Bayerisches Landesamt für Statistik und Datenverarbeitung
St.-Martin-Str. 47
81541 München
Telefon 089 2119-0
Telefax 089 2119-3410 allgemein
E-Mail: poststelle@statistik.bayern.de
Internet: www.statistik.bayern.de
Bankverbindung: Staatsbank Bayern,
Buchungstelle München, Bayer. Landesbank
BLZ 700 500 00
Konto-Nr. 24 092

Österreichische Verkehrsmittel: S-Bahn S3 u. S7 Haltestelle St.-Martin-Str.

Per Post bekommen
Sie zwei Transport-PINs
(ENCRYPTION +
SIGNATURE)

Diese PINs gut aufheben!

In den Gemeinden

Beschreibungen zur Installation bei Ihnen finden Sie unter

www.pki.bayern.de

→ Bay. VerwaltungsPKI → Teilnehmer → Dokumente

Dokumente für Teilnehmer der Bay. Verwaltungs-PKI

Es gibt im Verwaltungsumfeld eine Vielzahl von Systemumgebungen und -kombinationen. Zudem stellt jede dieser Kombination eigene Anforderungen an die Schritte zur Konfiguration für den Einsatz sowie bei der Verwendung von Zertifikaten. Dies fängt in der Regel schon bei unterschiedlichen Oberflächen und Menüstrukturen an, und setzt sich im Umgang mit der jeweiligen Anwendung fort.

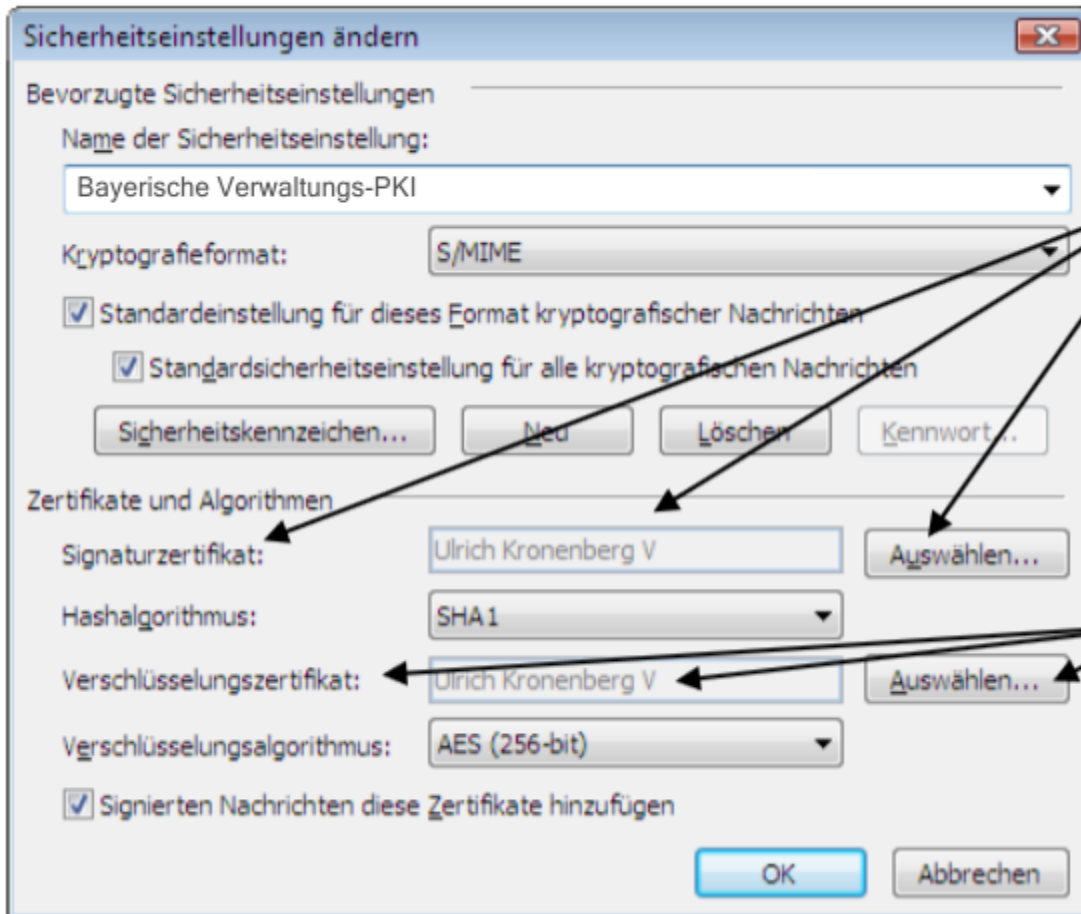
Daher steht an dieser Stelle ein modulares Handbuch zur Verfügung, aus welchem die jeweils für die vor Ort eingesetzte Umgebung einschlägigen Teilbereiche selbst zusammengestellt werden können:

	Windows XP	Windows Vista	Windows 7	Mozilla	Thunderbird
Zertifikatsimport Sichere E-Mail	PDF	PDF	PDF	PDF	PDF
Zertifikatsimport SSL-Authentifizierung	PDF	-	-	PDF	-

	Outlook 2000	Outlook XP	Outlook 2003	Outlook 2007	Outlook 2010	Thunderbird	Lotus Notes
Konfiguration	PDF	PDF	PDF	PDF	PDF	PDF	PDF
Verwendung	PDF	PDF	PDF	PDF	PDF	PDF	-

Installation

- Zertifikatsdateien installieren (weiter – weiter – Sicherheitsstufe „Hoch“ – fertigstellen)
- Eigenes Passwort zum Verschlüsseln/Entschlüsseln und Signieren angeben
- Zertifikate in Outlook hinzufügen:
 - Outlook 2007: Menü Extras → Vertrauensstellungscenter → E-Mail-Sicherheit → Einstellungen
 - Outlook 2013: Datei → Optionen → Trust Center → Einstellungen für das Trust Center → E-Mail-Sicherheit → Einstellungen

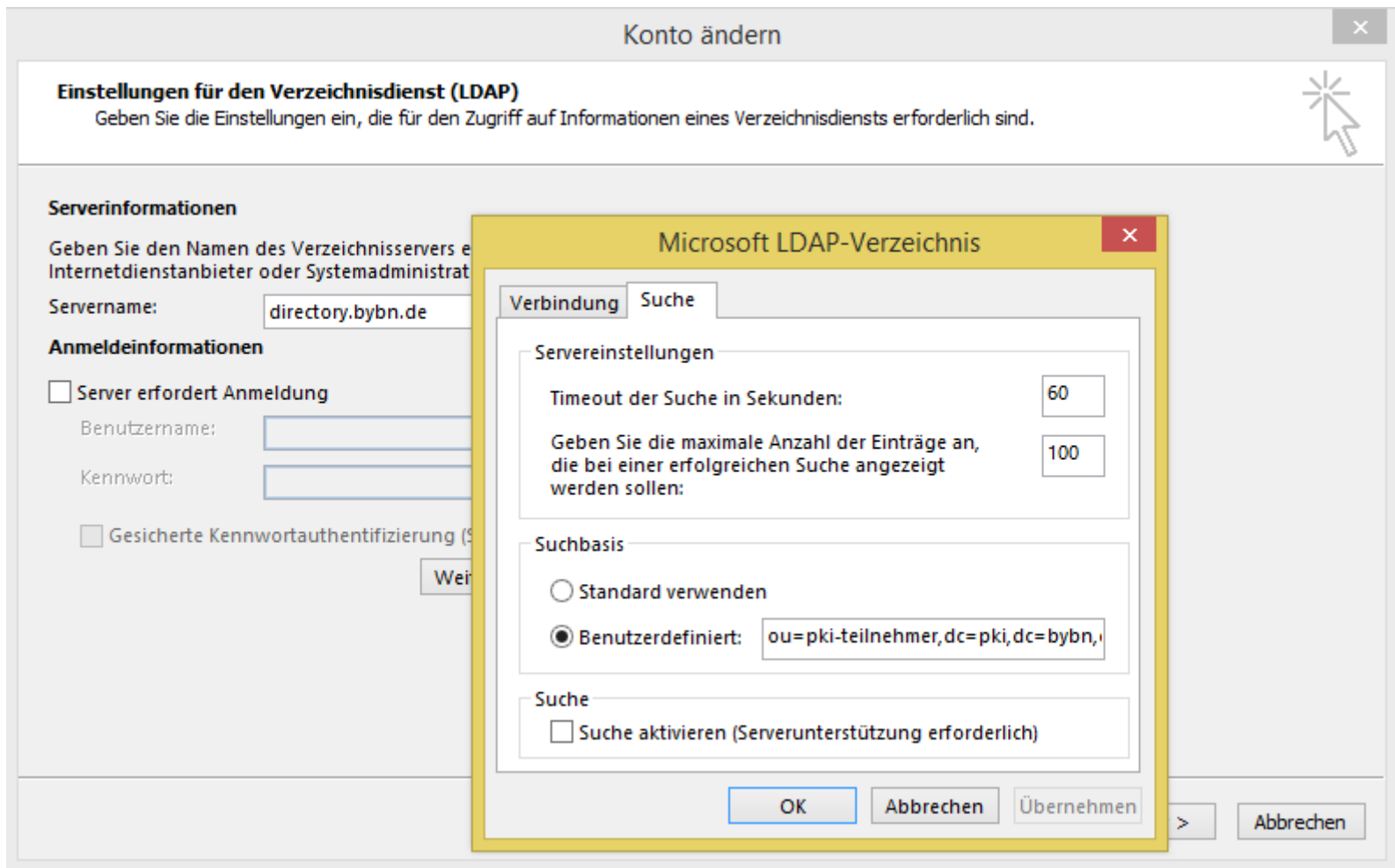


Hier wird das Signaturzertifikat ausgewählt.

Hier wird das Verschlüsselungszertifikat ausgewählt.

Adressbuch hinzufügen

- Outlook 2007: Menü Extras → Kontoeinstellungen → Adressbücher → Neu...
- Outlook 2013: Menü Datei → Kontoeinstellungen → Adressbücher → Neu...
- Verzeichnistyp: Internetverzeichnisdienst (LDAP)



Adressbuch hinzufügen

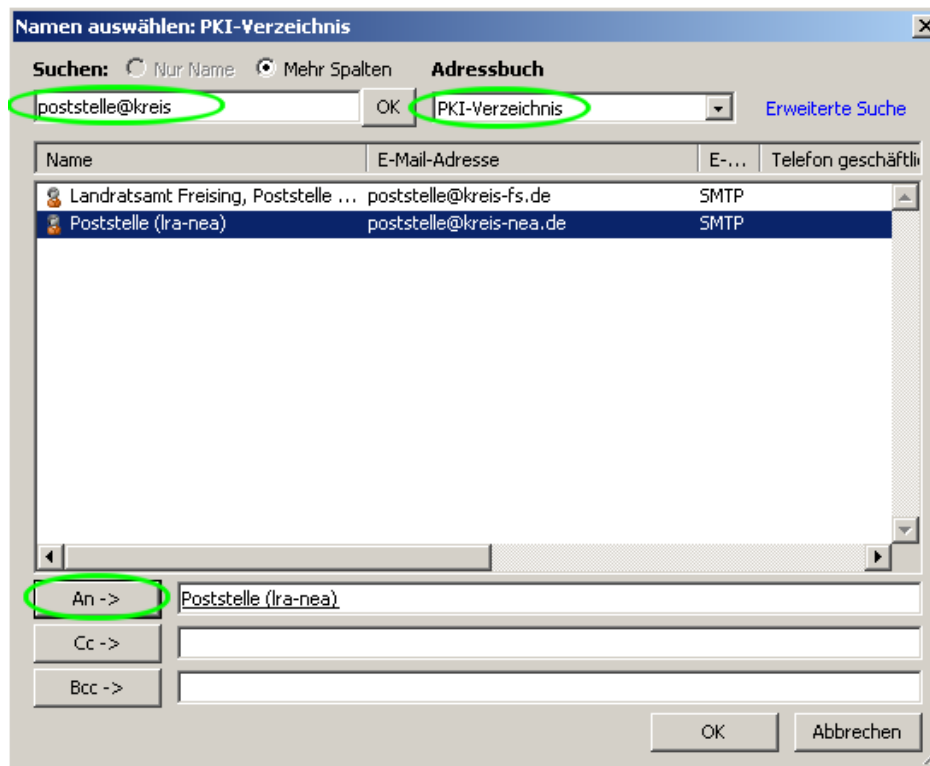
- Servername:
 - `directory.bybn.de` (mit Behördennetz)
 - `directory.bayern.de` (ohne Behördennetz)
- Anzeigename: `PKI-Verzeichnis`

- Suche/Suchbasis:

`ou=pki-teilnehmer, dc=pki, dc=bybn, dc=de`
(mit Behördennetz)

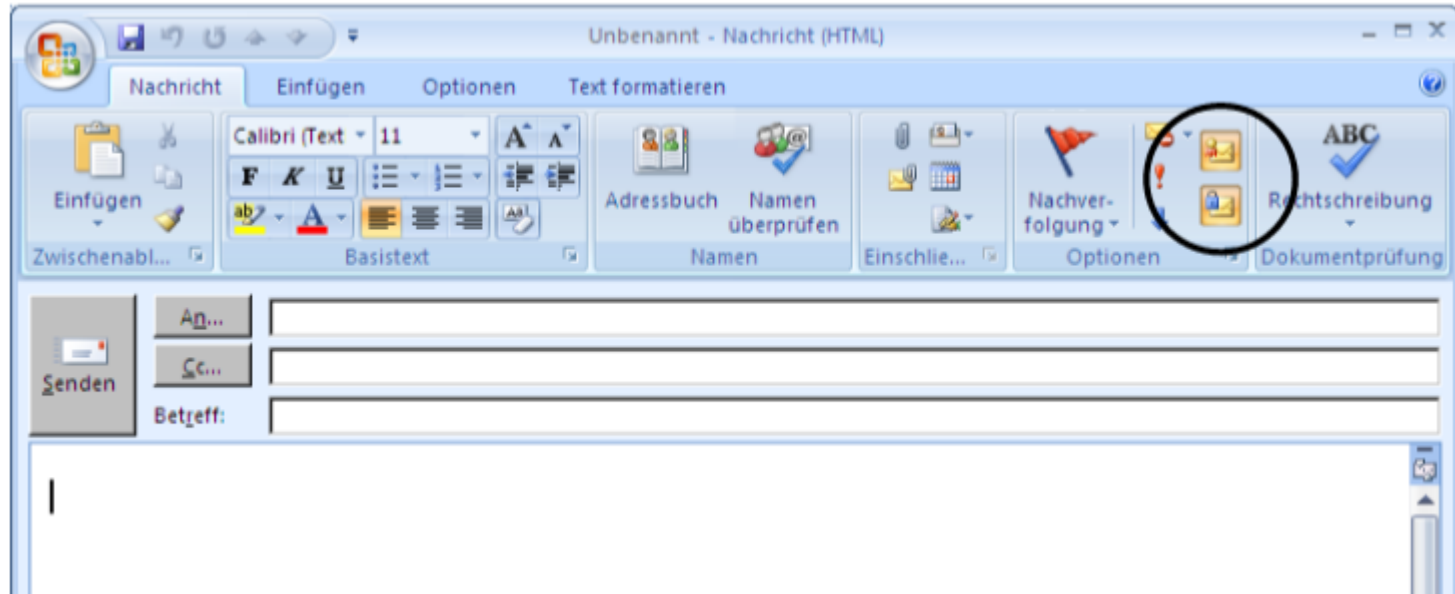
`ou=pki-teilnehmer, dc=pki, dc=bayern, dc=de`
(ohne Behördennetz)

Funktionstest



Empfänger aus PKI-Verzeichnis aussuchen

Funktionstest



Verschlüsselung und Signatur einschalten

Unbenannt - Nachricht (Rich-Text) ? [Icons] - [X]

DATEI NACHRICHT EINFÜGEN **OPTIONEN** TEXT FORMATIEREN ÜBERPRÜFEN LivingData

Designs [Icons] Seitenfarbe [Icons] Bcc Von Berechtigung Abstimmungsschaltfl. verwenden [Icons] Übermittlungsbestät. anfordern Lesebestät. anfordern Verlauf Gesendetes Element speichern unter [Icons] Übermittlung verzögern Direkte Antworten auf [Icons] Weitere Optionen [Icons]

Von [Dropdown] poststelle@kreis-nea.de

An... [Text Input]

Cc... [Text Input]

Betreff [Text Input]

Senden [Icon]

Mit freundlichen Grüßen

Frank Härtlein

Landratsamt
Neustadt a.d.Aisch-Bad Windsheim
- Hauptverwaltung -
Konrad-Adenauer-Straße 1
91413 Neustadt a.d.Aisch
Tel.: 09161 92-110
Fax: 09161 92-8110
E-Mail: frank.haertlein@kreis-nea.de
Internet: <http://www.kreis-nea.de/>

Funktionstest



Passwortabfrage

Sonstiges

- Für jede Funktionsstelle genau ein/e Verantwortliche/r
- Zertifikatsdateien können auf mehreren Rechnern installiert und von mehreren Benutzern genutzt werden
- Bei der Installation gibt jeder Benutzer ein eigenes Passwort an
- Das Passwort wird zum Verschlüsseln/Entschlüsseln/Signieren abgefragt
- Ohne Zertifikat oder ohne Passwort können verschlüsselte E-Mails nicht gelesen werden!
- Wenn Sie eine Behörde erstmals verschlüsselt anschreiben, immer über das PKI-Verzeichnis!

Weitere Informationen

- Registrierungsformulare haben Sie bereits erhalten
- Diese Präsentation, Formulare und Links unter www.kreis-nea.de/pki
- Ansprechpartner:
Frank Härtlein
frank.haertlein@kreis-nea.de
Tel. 09161 92-110
Zimmer A 110