



bw-trust

Gestaltung einer Public-Key-Infrastruktur für den Bedarf einer Großstadt

KoopA ADV - 44. Erfahrungsaustausch
in Dresden vom 26.-27. März 2007

Referent: Gunnar Wolf, Landeshauptstadt Stuttgart

Agenda



- ❖ Ausgangslage - Vorgeschichte
- ❖ Projektstatus
- ❖ Grobkonzept
- ❖ Projektpartner
- ❖ Zeitplanung
- ❖ Policy und Practise Statement
(Zertifizierungsrichtlinie)

Ausgangslage



❖ Die öffentliche Verwaltung

- benötigt nur wenig qualifizierte Signatur-Zertifikate
 - **Sie sind personengebunden, nicht funktions-/gruppenorientiert**
 - **Unterliegen der privaten Verfügungsgewalt**
 - **In die Rechtsbeziehung Trustcenter ⇔ Privatmann kann schlecht eingegriffen werden**
- benötigt vorwiegend Verschlüsselungs- und Authentifizierungs-Zertifikate
 - **Sicherung der elektronischen Kommunikation**
 - **Zulassung der Benutzer für Systeme und Verfahren**
- benötigt die Verfügungsgewalt über die den Mitarbeitern überlassenen Zertifikate
 - **Entziehung bei Ausscheiden des MA**
 - **Wiederherstellung verschlüsselter Nachrichten/Dateien**
 - **Behördenname sollte Bestandteil des Zertifikats sein**

❖ Aus denselben Gründen hat der Bund die Verwaltungs-PKI geschaffen, in die sich Länder und Kommunen eingliedern können



Anwendungsfälle



- eMail-Verschlüsselung und -Signatur
- Festplatten- und Dateiverschlüsselung
- Verschlüsselung des Netzverkehrs
- SmartCard-Logon an der Domäne
- Datenaustausch über OSCl
- Transaktionsverschlüsselung (TLS)
- Clientauthentifizierung (SSL)
- WLAN-Authentifizierung (EAP)
- Signatur im PDF-Dokument
- Datei-Signatur
- Signatur in Verwaltungsprozessen
- Zeitstempel

Vorgeschichte



- ❖ 2002-2004 Pilotprojekt eVAS
(elektronische Verschlüsselung Authentifizierung Signatur)
 - Eigene PKI-Lösung (Pilotinstallation)
 - Einsatz von Zertifikaten auf Smartcard und als Soft-PSE
 - Unterstützung von drei produktiven verwaltungsinternen Verfahren
- ❖ 2005 Europaweite Ausschreibung einer PKI-Nachfolgelösung für die Pilotinstallation
- ❖ 2006 Beschränkte Ausschreibung und Vergabe

Projektstatus



- ❖ Ausschreibung
Mai 2006 ✓
- ❖ Vergabeentscheidung
Nov. 2006 ✓
- ❖ Vertragsverhandlungen
Dez./Jan. 2007 ✓
- ❖ Vertragsunterzeichnung ✓
am 30.01.2007 in Berlin



Unser Partner für die Technik:



Grobkonzept



- ❖ Trägerschaft
- ❖ Certification Authorities
- ❖ Verfahren / Prozesse
- ❖ Token und Schlüsselmaterial
- ❖ Verzeichnisdienst / CRL
- ❖ PIN-Briefe / Freischaltung

Trägerschaft



❖ Die bw-trust CA ist eine Einrichtung der Landeshauptstadt Stuttgart zur Beglaubigung von Identitäten in der öffentlichen Verwaltung Baden-Württembergs mittels elektronischer Zertifikate

❖ Partner in der Gestaltung der CA sind

- der Kommunale DV-Verbund Baden-Württemberg (dvv) und
- die Stuttgarter Straßenbahnen AG (SSB)



Arbeitsgrundlagen



- ❖ D-TRUST stellt das Certificate Management System und den Verzeichnisdienst
- ❖ bw-trust betreibt zunächst eine Registration Authority über eine Online-RA für
 - die Standard-Signaturkarte von D-TRUST
 - die auf eigener Policy basierenden Zertifikate der Basic-CA und der V-CA
- ❖ Weitere Online-RA's der bw-trust CA sind möglich, aber noch nicht geplant

Certification Authorities



In der OnlineRA werden folgende CAs benutzt:

❖ D-TRUST Qualifizierte CA

- Qualifiziertes Signaturzertifikat nach SigG auf Standard-Signaturkarte

❖ D-TRUST Fortgeschrittene Card-CA

- Verschlüsselungs- und Authentifizierungszertifikat auf Standard-Signaturkarte

❖ bw-trust Basic-CA

- Fortgeschrittene Signatur-, Verschlüsselungs- und Authentifizierungszertifikate auf Chipkarte und als Soft-PSE (PKCS#12-Datei)

❖ bw-trust V-CA (voraussichtlich in 2008)

- Zertifikate unter der Verwaltungs-PKI des Bundes

Prozesse



- ❖ Beantragung einer bw-trust Chipkarte oder einer Soft-PSE (PKCS#12-Datei)
 - nach Identitätsprüfung in der RA für Einzelfälle
 - nach Identitätsprüfung in dezentralen **ID-Punkten** durch Übermittlung von Listen in Dateiform
- ❖ Beantragung einer Standard-Signaturkarte der D-TRUST mit Identifizierung anhand von Ausweisen in der RA
- ❖ Beantragung einer Standard-Signaturkarte über eine Webanwendung mit nachträglicher Identifizierung per Post-Ident-Verfahren (erst ab 2008)

Organisationsschema



Technischer Dienstleister -
Hosting der ASP-Lösung
„Certificate Manager“

D-TRUST

13.03.2007

Organisatorischer
Überblick

Autor: Gunnar Wolf

Verantwortlicher Diensteanbieter -
Produktbildung, Zertifikatsrichtlinien,
Auftraggeber für den techn. Dienstleister

bw-trust CA

OnlineRA
(Stammzelle)

Weitere OnlineRAs
sind möglich
aber noch nicht
geplant

Identifizierungs-
stellen

ID-Punkt DVV
(OfflineRA)

ID-Punkt SSB
(OfflineRA)

ID-Punkt ...
(OfflineRA)

ID-Punkt
(OfflineRA)

2007-03-25

bw-trust CA

Token und Schlüssel



❖ Chipkarten

- Signaturgesetzkonforme Smartcards mit Siemens CardOS 4.3b
- Schlüssellänge 2048 Bit

❖ Standard-Signaturkarte D-TRUST

- 2 Zertifikate – kein key recovery

❖ bw-trust ID-Card

- 2 Zertifikate – key recovery für Verschl.-Zertifikate
- +Windows-Logon-Zertifikat

❖ bw-trust Soft-PSE (PKCS#12- und DER-Datei)

- Je Zertifikat eine Datei .p12 und .der

ID-Card



bw-trust CA

ID-Card



o= Landeshauptstadt Stuttgart

ou= *Haupt- und Personalamt*

cn= **Gunnar Wolf**

SN: 47114722

Gültig bis 31.03.2009

bw-trust Basic-CA

PIN-Briefe



❖ Sowohl für Smartcard-basierende Zertifikate als auch für PKCS#12-basierende Zertifikate

➤ PIN-Briefe für den Inhaber

- per Secure-Printer direkt in der Online-RA
- per Secure-Printer und Post-Versand an den ID-Punkt

❖ Freischaltung öffentlicher Zertifikate für den Verzeichnisdienst

➤ Signatur rechtlich überprüfbar nach SigG

Schritte zur Nutzung



- ❖ Der bw-trust CA können sich alle öffentlichen Verwaltungen (incl. Mehrheitsgesellschaften) in Baden-Württemberg bedienen
- ❖ Verwaltung stellt Mitarbeiter für einen ID-Punkt zur Verfügung
 - Zertifikate für die vertrauliche und verbindliche Kommunikation mit der RA
 - Schulung und Einweisung der Mitarbeiter
- ❖ Verwaltung anerkennt die Zertifizierungsrichtlinie der bw-trust CA

Zeitplanung



- ❖ Grobkonzept abgenommen Ende Jan.07
- ❖ Entwurf Feinkonzept Anf. Feb.07
- ❖ Fertigstellung Feinkonzept Mitte März 07
- ❖ Endgültige Preiskalkulation Ende März 07
- ❖ Aufsetzen der Profile Anf. April 07
- ❖ Rohfassung des CPS Ende
März 07
- ❖ Schulung RA-Mitarbeiter Mitte April 07
- ❖ Test der RA Ende April 07
- ❖ Zulassung von ID-Punkten ab Mai 07

Zertifizierungsrichtlinie



- ❖ Zertifizierungsrichtlinie der bw-trust CA
 - Enthält sowohl Certification Policy (CP) als auch Certificate Practise Statements (CPS)
- ❖ Kernfragen:
 - Qualität der Identitätsprüfung
 - Prozessabläufe
 - Sicherheitsmaßnahmen
- ❖ Abstimmungsgremium ist die AG bw-trust CA (LHS, dvv, SSB)

Identitätsprüfung



❖ Personen

- Anhand von Personalausweis o. Reisepass

❖ Gruppen (= z.B. Posteingangsstellen)

- Erklärung des organisatorischen Leiters

❖ Rechner

- Ripe-Handle des Admin-c / Erklärung des org. Leiters
- Pers. Erscheinen des Admin-c in dem ID-Punkt

❖ ID-Punkt

- Benennung der Mitarbeiter d. Verwaltung
- Pers. Erscheinen in der RA mit Ausweisen

Prozessabläufe



- ❖ Identifikation durch besonders autorisierte dezentrale Stellen (ID-Punkt)
- ❖ Übermittlung der Zertifikatsanträge in Listenform an die bw-trust CA
- ❖ Ausstellung der Zertifikate auf SmartCard oder in Dateiform + PIN-Brief
- ❖ Rückübermittlung an den ID-Punkt

Zertifikatsprüfung und -erneuerung



- ❖ Öffentlicher Verzeichnisdienst
 - Per LDAP (für jeden ID-Punkt)
- ❖ Mail-Benachrichtigung für Personenzertifikate vor Ablauf der Gültigkeit
- ❖ Antragsberechtigt ist nur der ID-Punkt

Fragen?



Vielen Dank für Ihre Aufmerksamkeit



bw-trust



Beglaubigte Identitäten
für die öffentliche Verwaltung