



Projekt: Zentrale Speicherung von Arbeitnehmerdaten unter Einsatz der elektronischen Signaturkarte

Präsentation Signaturbündnis – 12. Januar 2004

Agenda



- **Vorstellung Projekt JobCard**
- **Problemstellung – etwas mehr Technik**
- **Schnittstellen**



Ziele der Veranstaltung

Im Auftrag des BMWA müssen wir

- **Das Verfahren JobCard auf den bekannten Rahmenbedingungen aufbauen !**
 - **Signaturgesetzkonforme Lösung mit qualifizierter Signatur**
 - **Kopplung mit Signaturbündnis**
 - **Anwendung der Standards und Normen**
 - **Basis für weitgehend offene Umsetzung durch die freie Marktwirtschaft**
 - **Integration statt Konfrontation**

Was das BMWA nicht will und wir nicht dürfen

- **Proprietäre Lösungen**
- **Schaffung von Monopolen**
- **Unseren vorgegeben Projekt- und Terminplan überschreiten**
- **Daher: Keinen Zeitverlust durch Arbeiten ohne klare Zielvorgabe**



Projekt: Zentrale Speicherung von Arbeitnehmerdaten unter Einsatz der elektronischen Signaturkarte

Eine kurze Einführung

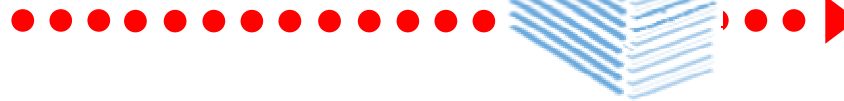


Bescheinigungen

60 Mio. Bescheinigungen pro Jahr



ca. 99% Papier

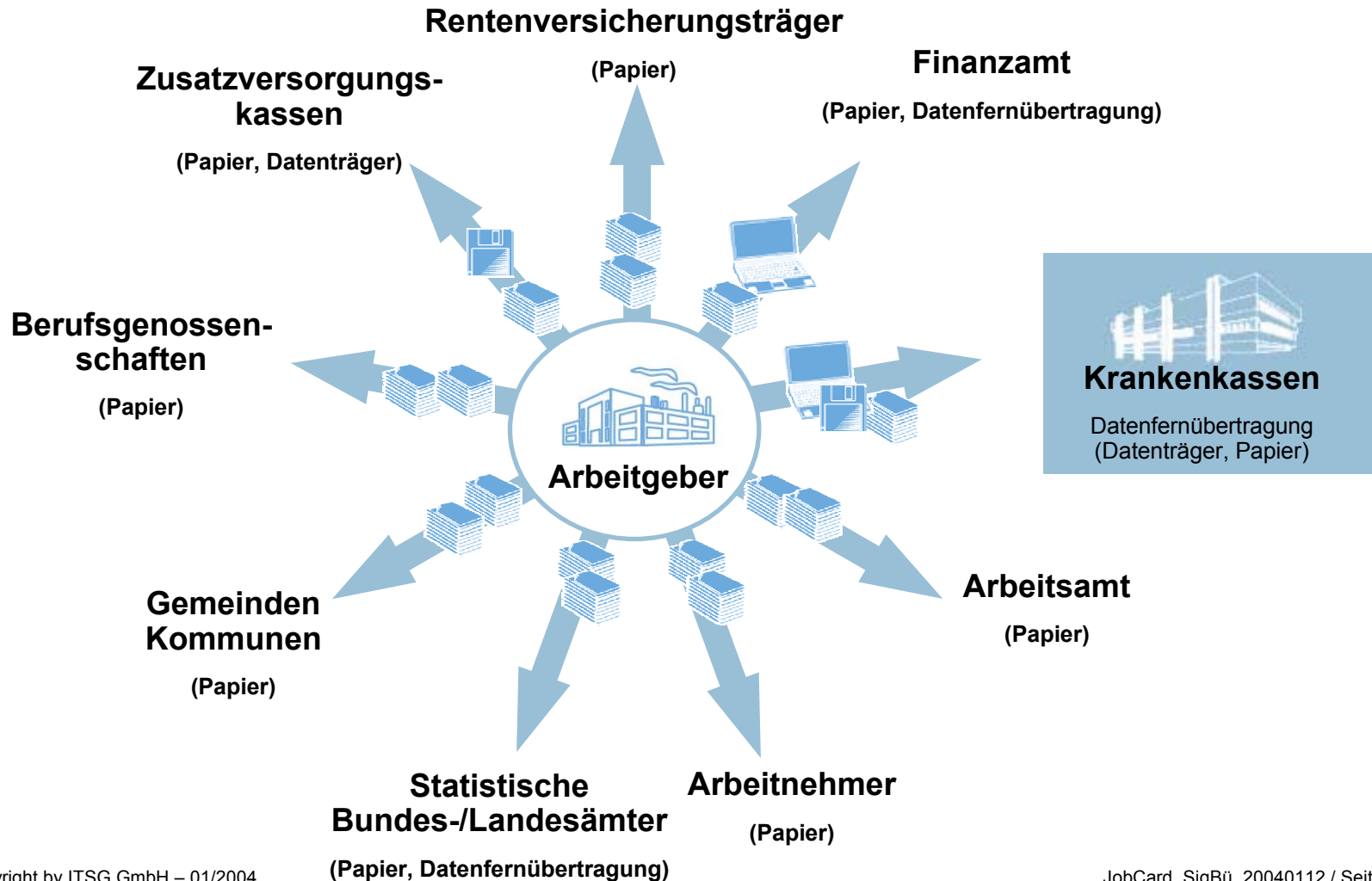


Geschätztes Rationalisierungspotential auf Arbeitgeberseite

- ca. 100.000 Arbeitstage pro Jahr für die Ausstellung von Papierbescheinigungen
- Rechnerische Entlastung: ca. 500 Mio. € pro Jahr



Aktuelles Verfahren





Datenaustausch

120 Mio. Beitragsnachweise pro Jahr

113 Mio. Sozialversicherungsmeldungen pro Jahr



2/3 Daten



1/3 Papier



**01.01.2006
Gesetzliche
Neuregelung**



Projektauftrag

- **Zentrale Annahmestelle für das Bescheinigungswesen**
- **Am Beispiel der Arbeitsbescheinigung nach § 312 SGB III**
- **Geschützter Abruf der Daten unter Einsatz der Signaturkarte**

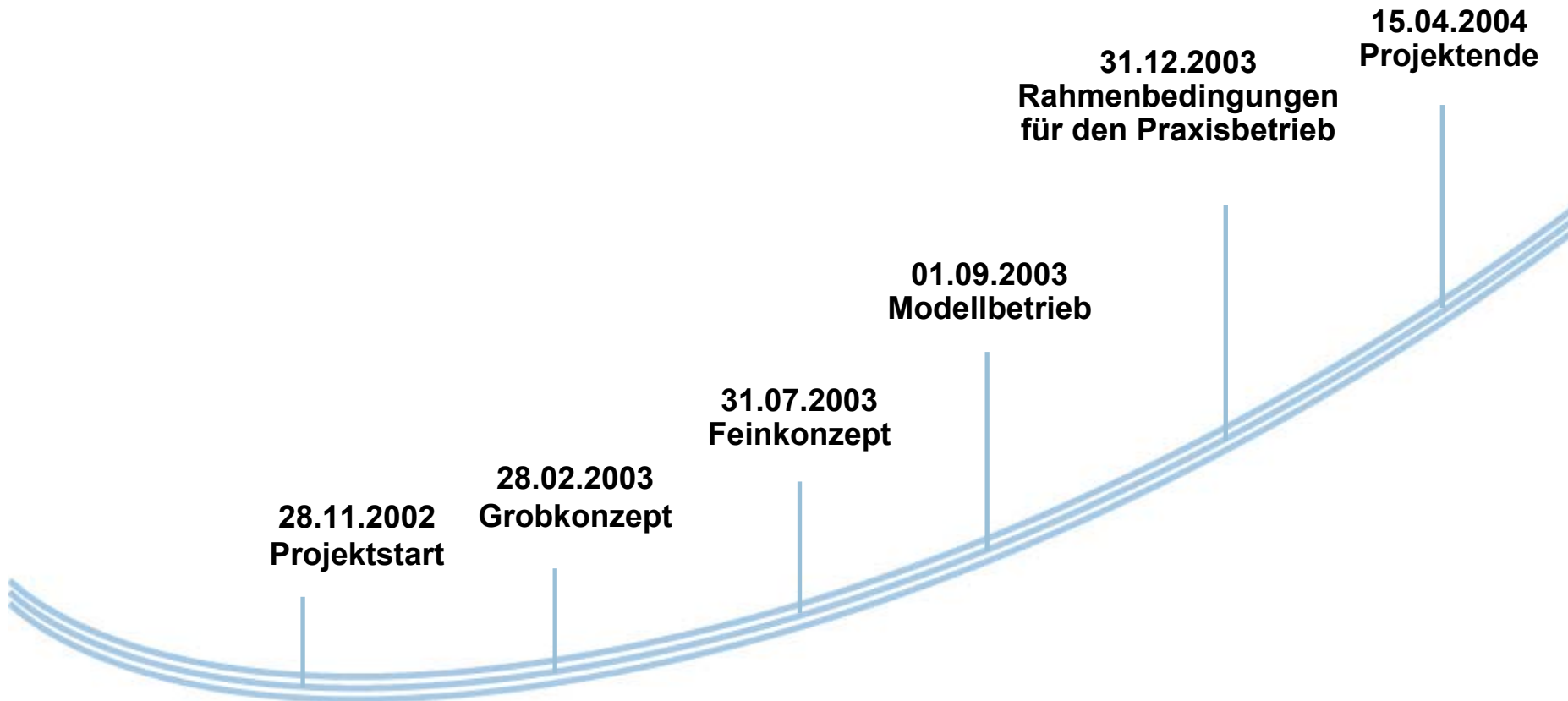


Projektergebnis

- **Organisatorische und technische Richtlinien für den Praxisbetrieb**
- **Modellhafte Erprobung mit Arbeitgebern und Arbeitsämtern**
- **Nachweis für die Machbarkeit**
- **Berücksichtigung der Datenschutzaspekte**
- **Formulierung der gesetzlichen Grundlage**
- **Betreibermodell**

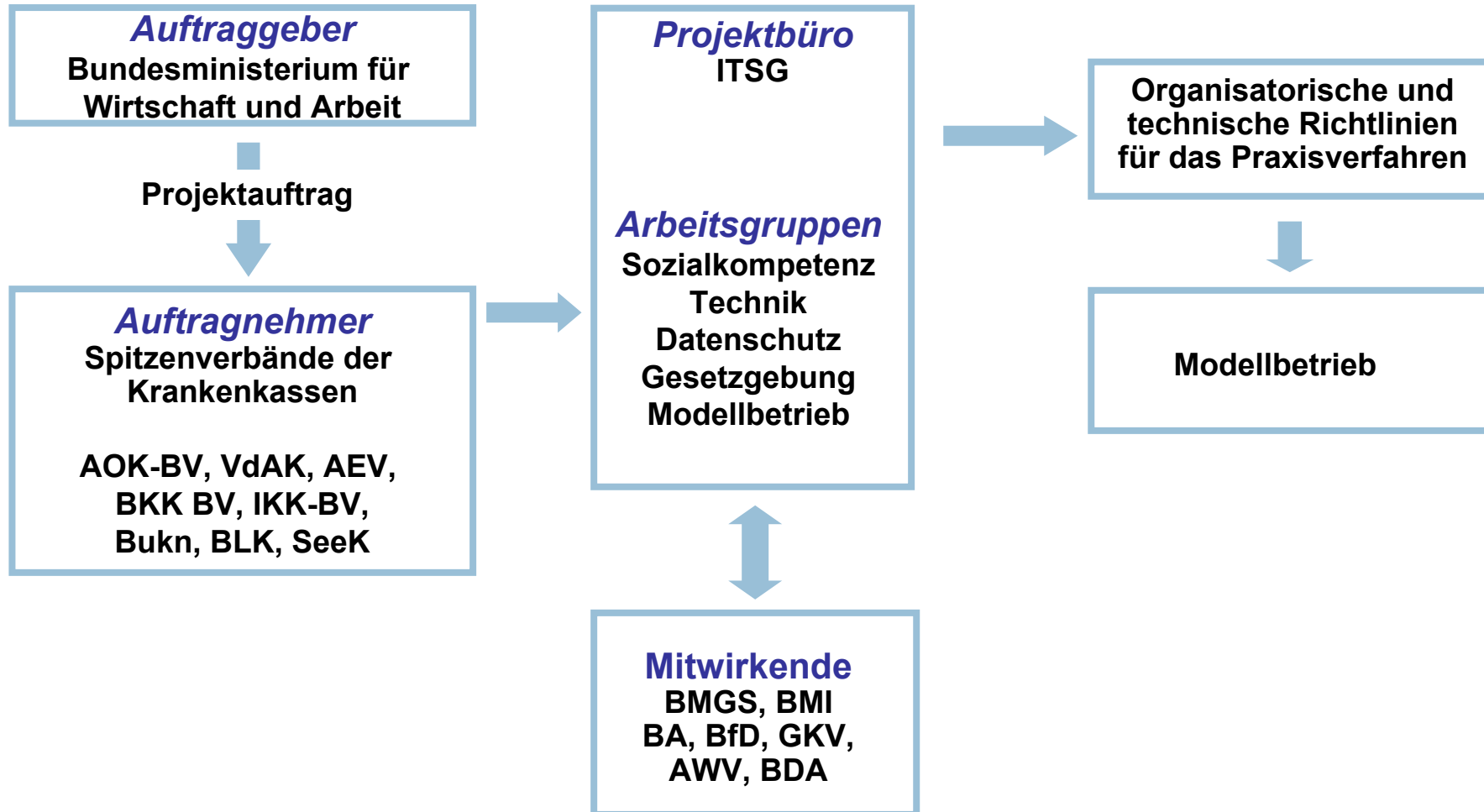


Projektplan



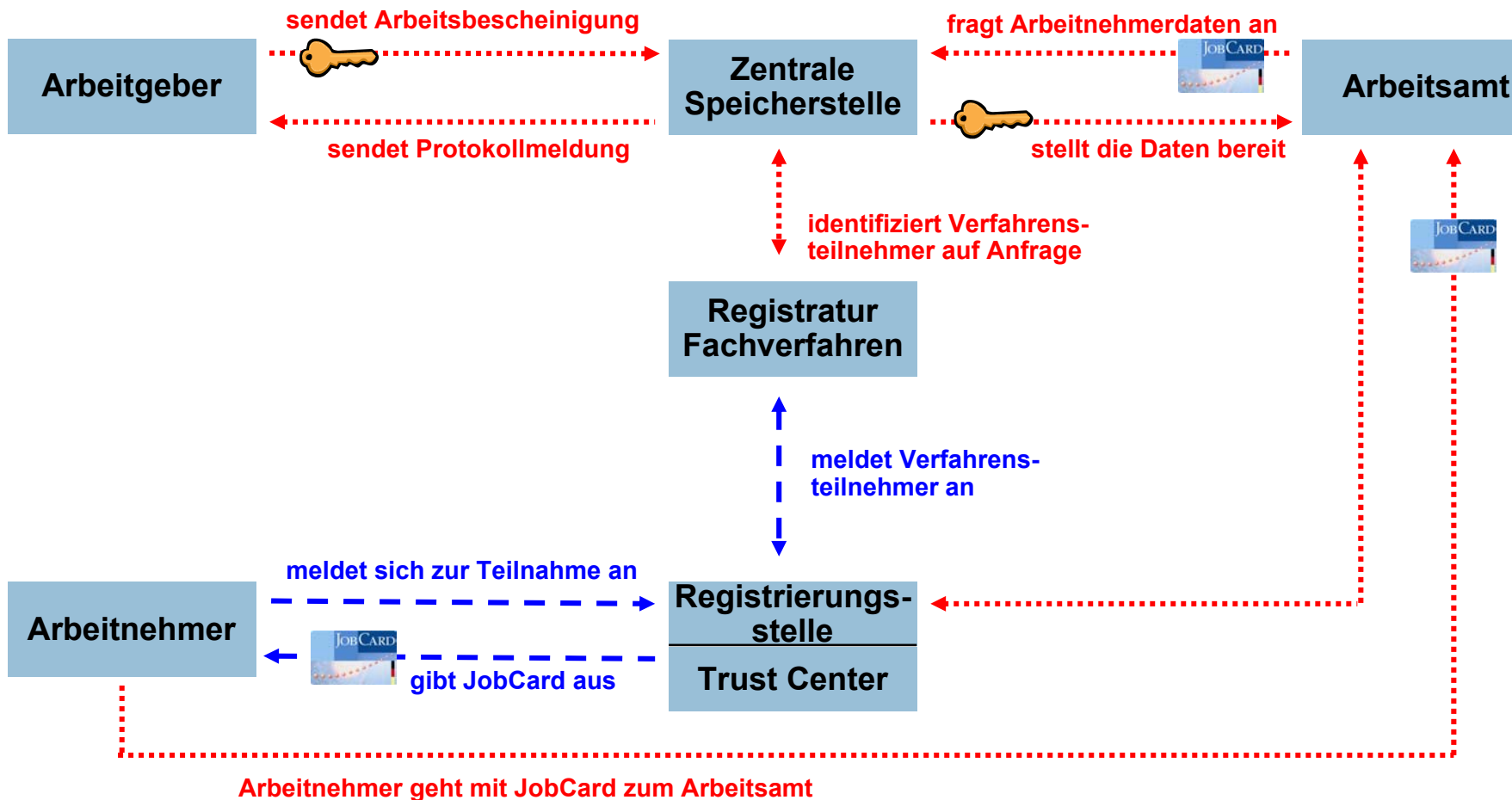


Projektbeteiligte



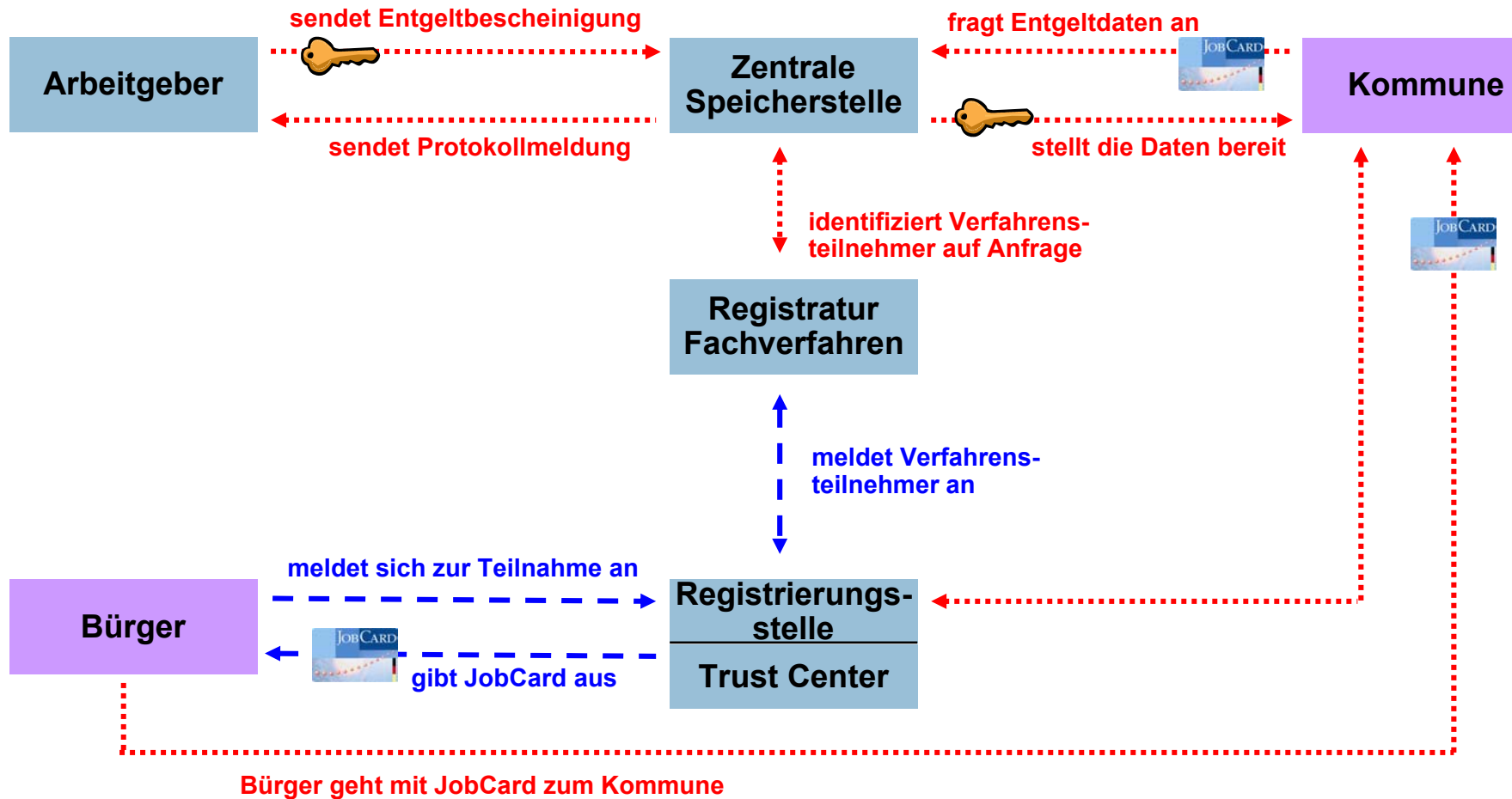


Funktionaler Ablauf



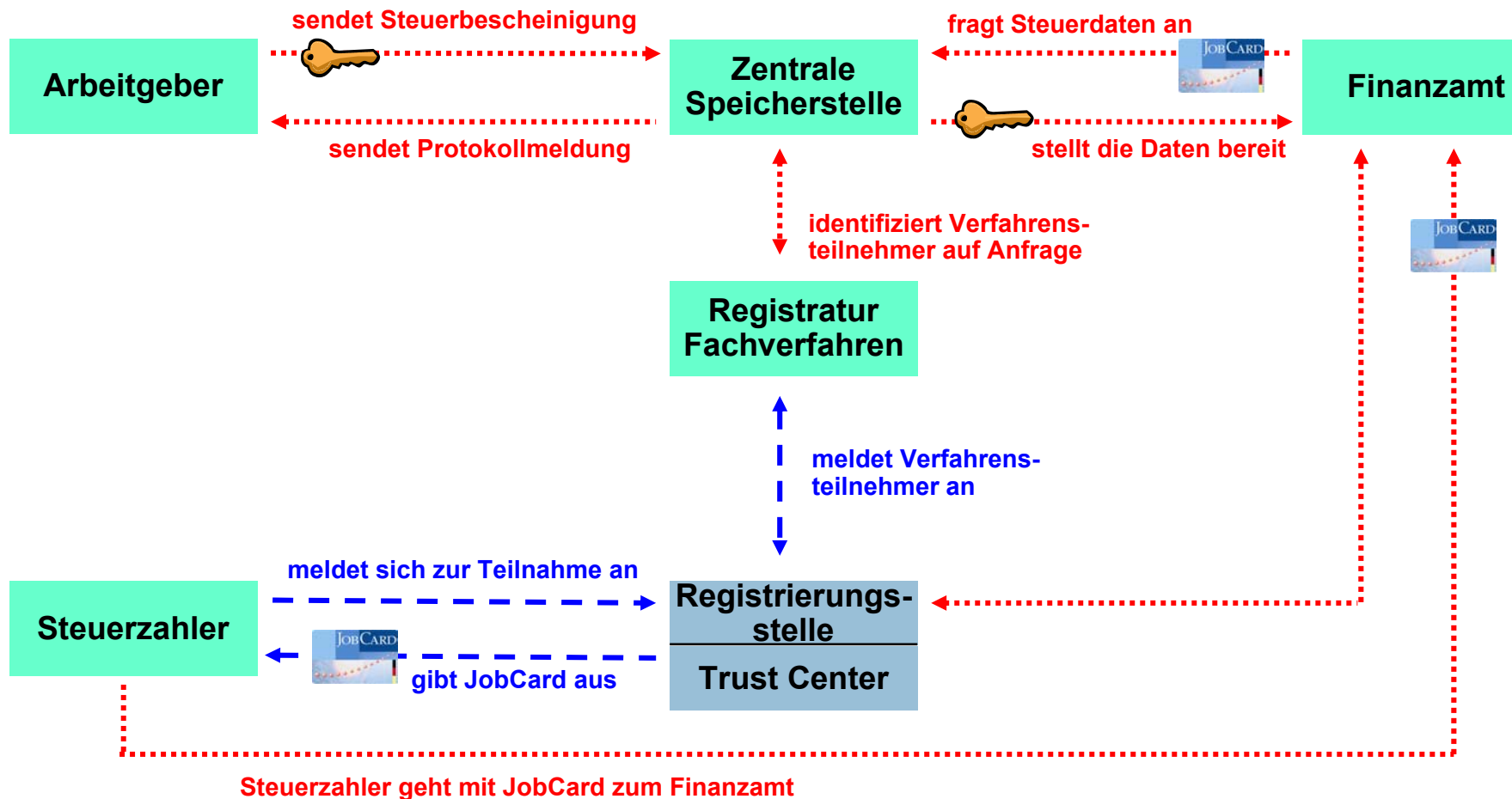


Variante x



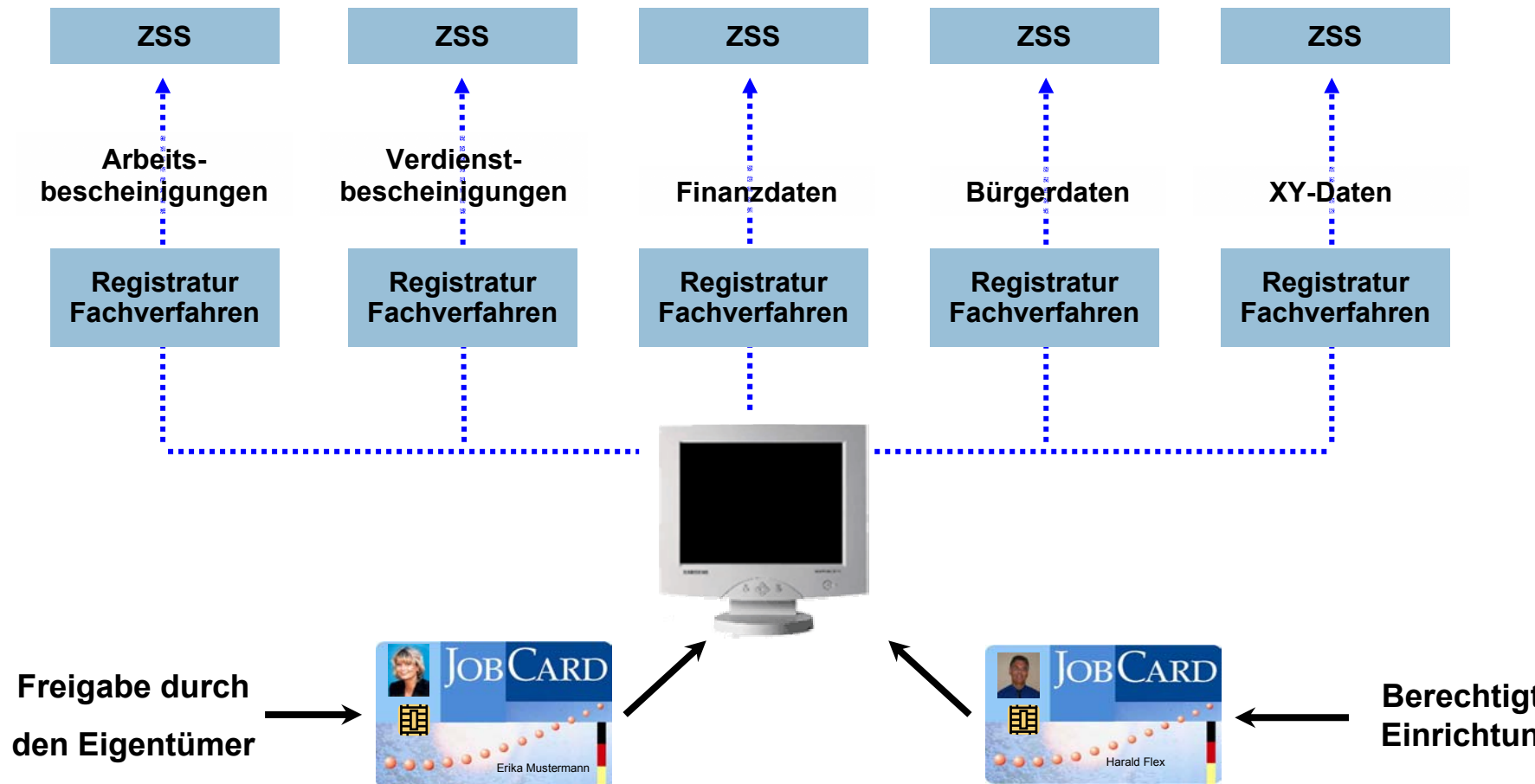


Variante y



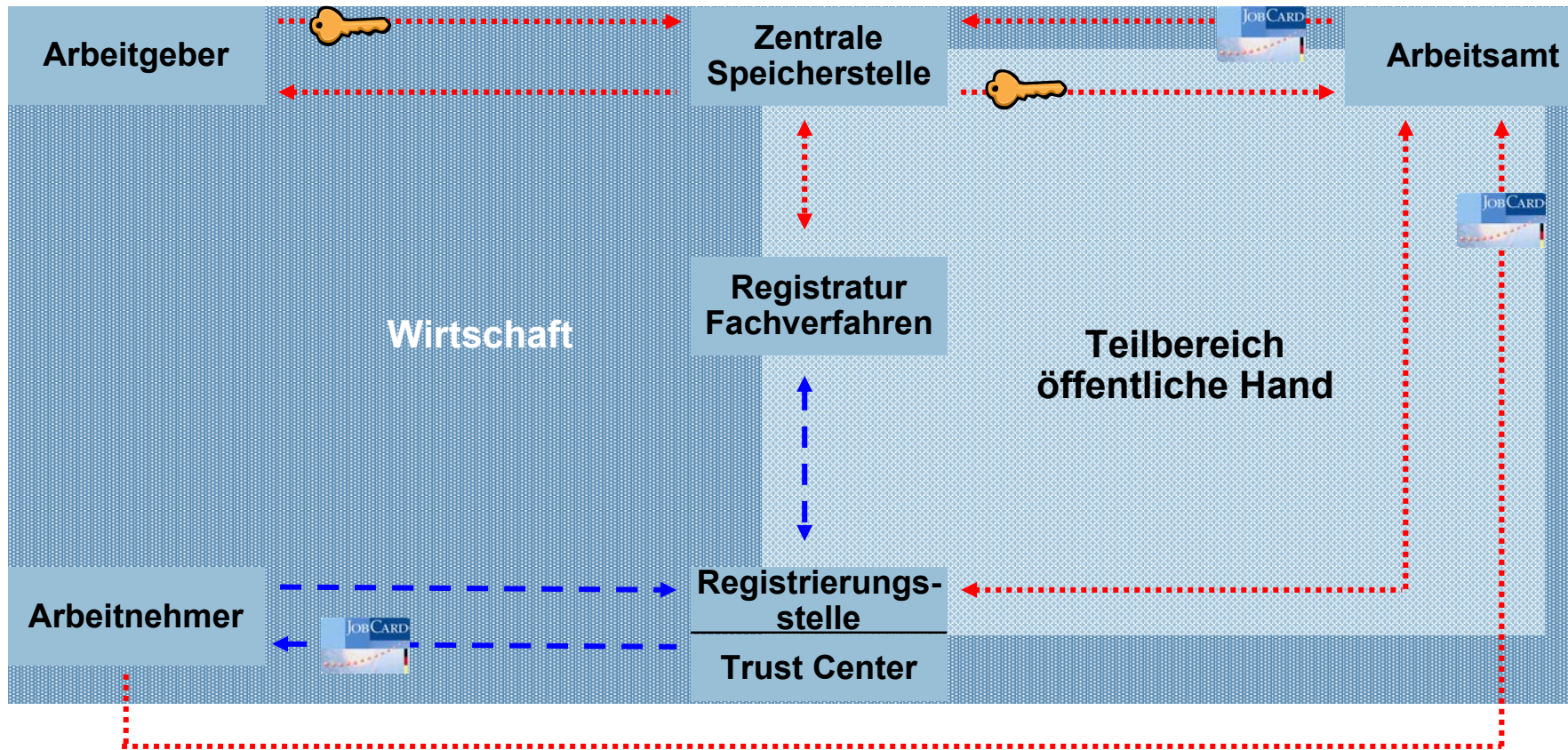


Multifunktionaler Einsatz





Betreiberkonzept





Modellbetrieb ab September 2003

Arbeitsämter

- **Arbeitsamt Helmstedt**
- **Arbeitsamt Bamberg**
- **Arbeitsamt Offenbach**

Arbeitgeber

- **Volkswagen AG, Wolfsburg (Software-Ersteller: SAP)**
- **Deutsche Lufthansa AG (Software-Ersteller: ITSG und SAP)**
- **Steuerberater Krause & Gleu, Rodgau (Software-Ersteller: Datev)**
- **Datev als Rechenzentrum für diverse Arbeitgeber (Software-Ersteller: Datev)**
- **Stadtverwaltung Frankfurt (Software-Ersteller: P&I)**
- **Arbeitsamt Mainz (vertreten durch BA)**

Testverfahren

- **50 komplexe Testszenarien mit 1.500 Testfällen für fiktive Arbeitnehmer**



Die JobCard ist realisierbar !

Nachweis

- Organisatorische und technische Umsetzung
- Entkopplung der Signaturkarte von der Teilnahme am Fachverfahren
- Keine Speicherung von Daten auf der JobCard
- Modellbetrieb ab Herbst 2003

Zukunftsweisend

- Akzeptanz im praktischen Einsatz durch Multifunktionalität der Signaturkarte

Realisierbar

- Eine Karte für eine Vielzahl von Fachverfahren

Empfehlung

- Festlegung des Betreiberkonzeptes
- Klärung der Finanzierung
- Verabschiedung der gesetzlichen Grundlage



To Do - Arbeitsgruppen

Arbeitsgruppe Normierung

- Prüfung der Standards und Normen (Signaturgesetz, Signaturlösung, ISIS-MT etc.)
- Aufdecken der noch endgültig festzulegenden oder offenen Punkte
- Festschreibung der Richtlinien für JobCard ohne Interpretationsspielräume
- Nächster Termin: 19.11.2003 mit den Institutionen und Wirtschaftsunternehmen

Arbeitsgruppe Finanzierung

- Ausarbeitung eines Finanzierungskonzeptes für alle Funktionseinheiten
- Geschäftsplan für nutznutzerbezogenes Umlageverfahren Kartengebühr
- Nächster Termin: 02.12.2003 mit diversen Wirtschaftsunternehmen

Arbeitsgruppe Gesetzgebung

- Formulierung der gesetzlichen Änderungen



JobCard – Stufe 2

Beauftragung und Projektstart am 27.10.2003

Vorarbeit durch AWW – Multifunktionale Verdienstbescheinigung

Projektplan

- **Einrichtung Projektbüro und Arbeitsgruppen bis 31.12.2003**
- **Grobkonzept bis 30.06.2004**
- **Anpassung der Organisation und Technik für Modellbetrieb bis 31.10.2004**
- **Feinkonzept und gesetzliche Rahmenbedingungen bis 31.12.2004**
- **Ende Modellbetrieb bis 30.06.2005**



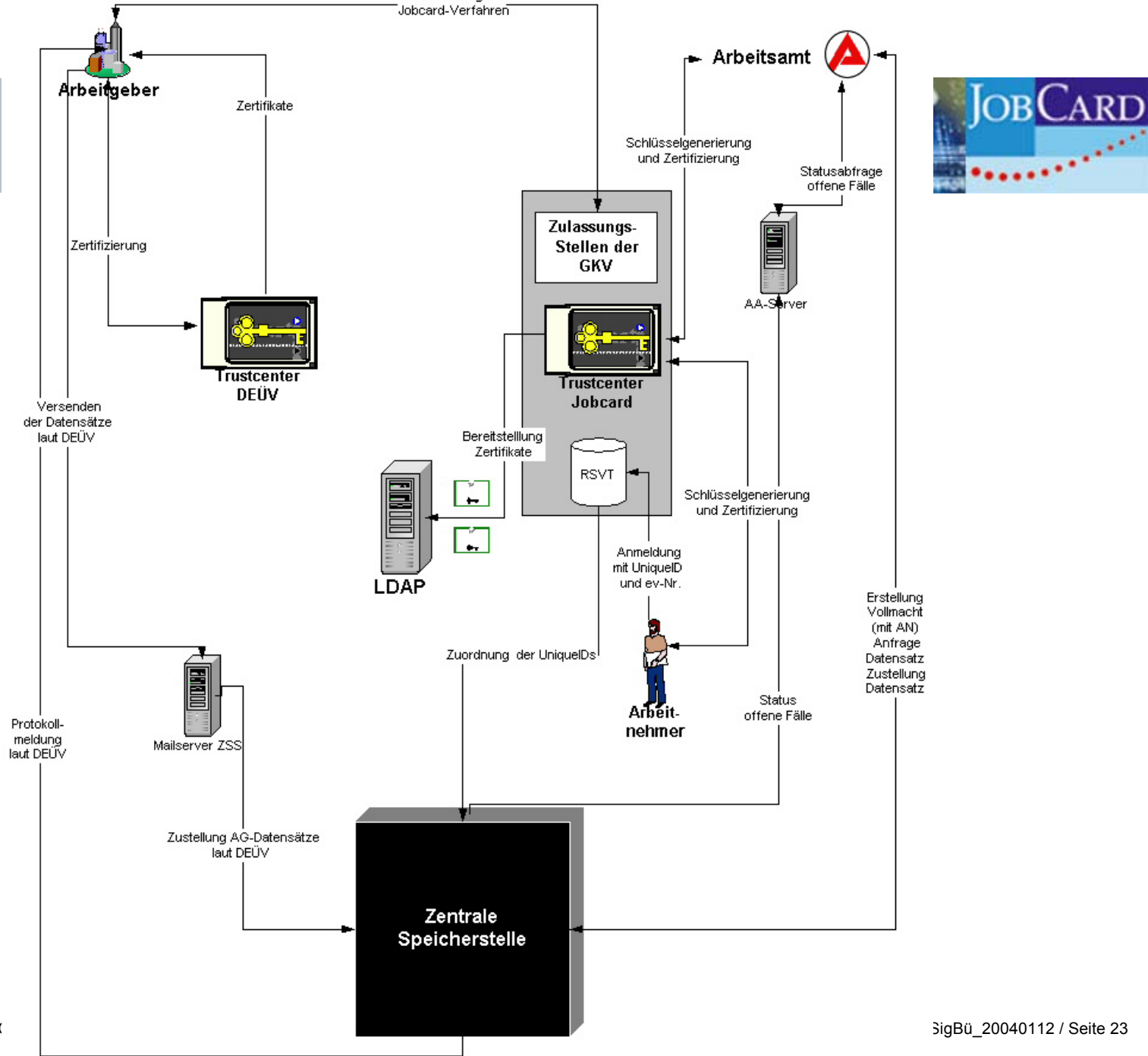
Projekt: Zentrale Speicherung von Arbeitnehmerdaten unter Einsatz der elektronischen Signaturkarte

Aufgaben der Arbeitsgruppe Normierung



Technik – etwas genauer

- **Das Modell JobCard I ist implementiert und läuft in der Erprobung**
- **Der Auftrag für JobCard II ist erteilt – multifunktionaler Datensatz**
- **Sehr enger Terminplan**
- **Das bringt eine Reihe von Problemen mit sich...**
- **Zunächst ein Blick auf das Modell**





Fragestellungen

- **Wie kann größtmögliche Interoperabilität erreicht werden?**
- **Wie kann der enge Zeitrahmen eingehalten werden?**
- **Wie kann die Karte für mehr als eine Anwendung verwendet werden?**



Am Verfahren Beteiligte

- **Zentrale Speicherstelle**
- **Arbeitgeber**
- **Arbeitnehmer**
- **Behörde**
- **Zertifizierungsdiensteanbieter (ZDA)**
- **Registrierungsstelle der ZDA**
- **Verzeichnisdienst der ZDA**
- **DEÜV-Trustcenter**
- **Registratur Fachverfahren**
- **Verzeichnisdienst DEÜV**
- **Zeitstempeldienst**



Externe Schnittstellen

- Arbeitgeber – ZSS
- Arbeitgeber – Trustcenter DEÜV
- Arbeitgeber – Verzeichnisdienst DEÜV
- ZSS – Behörde
- ZSS – Arbeitnehmer
- ZSS– Verzeichnisdienst DEÜV
- ZSS– Verzeichnisdienst ZDA
- ZSS– Trustcenter DEÜV
- ZSS– Registratur Fachverfahren
- ZSS- Zeitstempeldienst
- Behörde – Arbeitnehmer
- Behörde - Verzeichnisdienst ZDA
- Behörde – Zeitstempeldienst
- Behörde – Registrierungsstelle ZDA
- Arbeitnehmer – Registrierungsstelle ZDA
- Arbeitnehmer – Registratur Fachverfahren
- Registratur Fachverfahren – ZDA



Arbeitgeber (und Leistungserbringer)

- **DEÜV-Standard als Grundlage**
 - **Security-Schnittstelle im Gesundheitswesen**
 - **Technischen Richtlinien**
- **Übertragung von zwei Dateien per E-Mail**
 - **Verschlüsselte Nutzdatendatei**
 - **Auftragssatz**
- **Rückmeldung per E-Mail**
- **Dezentrale Softwareschlüsselerzeugung**
- **Eigenes Trustcenter**
- **Etabliertes Verfahren zur Verschlüsselung mit ca. 20.000 aktive Teilnehmer**



Zentrale Speicherstelle

- **Mit der Behörde**
 - **Berechtigungen**
 - **Vollmachten**
 - **Benachrichtigungen**
 - **Abfrage**
- **Mit dem Arbeitnehmer**
 - **BDSG §19**
- **Mit dem DEÜV-Verfahren**
 - **Zentrale Speicherstelle ist eine normale Annahmestelle**
- **Mit dem Verzeichnisdienst ZDA**
 - **Zugriffe LDAP**
 - **Zugriffe OCSP**
- **Mit der Registratur Fachverfahren**
 - **UniquelD – RV-Nummer**
 - **UniquelD-Historie**



Behörde

- **Mit dem Arbeitnehmer**
 - **Smartcard-Schnittstelle**
- **Mit dem Verzeichnisdienst ZDA**
 - **Als Option**
- **Mit dem Zeitstempeldienst**
 - **Für die Signaturerstellung**
- **Mitarbeiter in der Behörde werden wie normale Arbeitnehmer behandelt**



Arbeitnehmer

- **Mit der Registrierung ZDA**
 - **Bekannte Prozesse**
- **Mit der Registratur Fachverfahren**
 - **Wird im Detail in JobCard II definiert**



Registratur Fachverfahren

- **Mit der Registrierung ZDA**
 - **Wird in JobCard II definiert**



Orientierung an Standards

Folgende Standards wurden gesichtet

- **ISIS-MTT**
- **OSCI**
- **PKCS#7, 10, 11, 12, 15**
- **PEM**
- **Sowie diverse, sich daraus ergebende Standards**



Public Key Infrastruktur für JobCard

DEÜV-Infrastruktur – ist exakt definiert und muss nicht weiter behandelt werden

Genauer betrachtet werden muss die JobCard-Infrastruktur einschließlich

- **Zertifikate**
- **Sperrlisten**
- **LDAP**
- **OCSP**
- **Time Stamping Service**
- **Gültigkeitsmodell**



Zertifikate

- **X.509v3**
- **Keine überflüssigen bzw. optionalen Felder**
- **Als einzige Zertifikatserweiterung ist die KeyUsage gefordert**
- **Alle anderen Erweiterungen müssen non-critical sein**
- **Keine Cross-Zertifizierung**
- **Keine Attribut-Zertifikate für JobCard erforderlich**



Sperrlisten

- **Orientierung an ISIS-MTT**
- **Delta-CRLs erlaubt**
- **Keine weiteren Attribute**
- **Keine indirekte Erstellung zugelassen**



LDAP

- Ein nicht-personalisiertes Suchkriterium wird benötigt (UniqueID). Für die Zuordnung UniqueID <-> Zertifikat gibt es keine Zugriffsbeschränkungen.
- Standardmäßiger Aufbau des LDAP DN: „cn=<UniqueID>, ou=<Untergruppe1>, ..., ou=>Untergruppe n>, dc=<Trustcenter-Bezeichnung>, dc=DE“
- Innerhalb des LDAP Users wird in dem Feld „CN“ der Name des Benutzers gespeichert. Weitere Felder dürfen bei Bedarf gefüllt werden. Felder mit personalisierten Daten (auch das Feld „CN“) sind nur autorisierten Usern über eine SSL-Verbindung zugänglich.
- Schreibrecht haben nur bestimmte autorisierte Benutzer, die über eine SSL-Verbindung auf den LDAP-Server zugreifen müssen.
- Die aktuelle CRL liegt direkt im Root-Pfad und ist im Leserecht nicht beschränkt.



OCSP

- **Orientierung an ISIS-MTT**
- **Keine Unterstützung von optionalen Feldern**
 - **Z.B. kein Sperrgrund**
- **Aber: Bei OCSP-Antwort muss Signatur vorhanden sein (signature aus ISIS-MTT SiG-Profil)**



TSS

- **Orientierung an RFC 3161**
- **TimeStampResp nur im Sekundenbereich zugelassen**
- **Verzicht auf optionale Felder**
- **Transport des Timestamp per http**



Gültigkeitsmodell

- **Orientierung am ISIS-MTT, SigG-Profil**
- **Schalenmodell**
- **Falls CA-Zertifikat gesperrt wird, gelten alle Zertifikate der CA, die bis dahin ausgestellt wurden, weiter**
- **Ausnahme: Sperrung wegen Kompromittierung?**
 - **Dann: Sperrung aller User-Zertifikate, Sperrung CA-Zertifikat**
 - **Übergangsfrist?**



Schlüsselmedien

- **DEÜV-Verfahren: Keine Aussage, bisher zu 100% Softwareschlüssel**
- **Zentrale Speicherstelle-Schlüssel: Sonderfall**
- **Arbeitnehmer-, Sachbearbeiter-Schlüssel: Smartcard**



Signaturkarte

- **Physikalische Ausprägung wird hier nicht definiert**
- **Logische Aufteilung in zwei Bereiche**
 - **Schlüsselbereich**
 - **Datenbereich**
- **Schlüsselbereich**
 - **Drei private und öffentliche Schlüssel**
 - **Drei Zertifikate mit dem jeweiligen KeyUsage-Attribut**
- **Datenbereich**
 - **Beschreibung des Zugriffs**
 - **Keine weiteren Vorgaben**
- **Beschreibung aus der PKCS #11-Sicht**



Benutzung der Signaturkarte

- **Jeweils Beschreibung in PKCS #11 Syntax, wie die Karte bzw. die Schlüssel darauf verwendet werden**
 - **Signatur**
 - **Authentisierung**
 - **Entschlüsselung**

- **Verwendung der Objekte im Datenbereich**



Algorithmen

- **SHA-1**
- **(DES-CBC)**
- **TripleDES-CBC**
- **RSA**



Kommunikation Behörde – ZSS

- **Standards, die in Frage kommen**
 - OSCI
 - ISIS-MTT
 - Evtl. weitere
- **Im Moment Vor- und Nachteile noch nicht genau klar**
- **Ziel: Möglichst offene und interoperable Standards zu verwenden**



Sonstiges

- **Fragen? Anregungen?**