



Der neue  
Personalausweis

# Methoden und Tools zur effizienten Integration in Anwendungen und Geschäftsprozesse

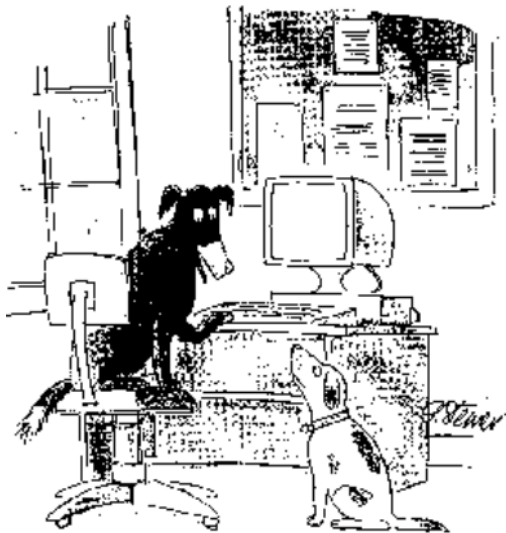


smarter together

04.03.2010  
Marc Albrecht  
[marc.albrecht@de.ibm.com](mailto:marc.albrecht@de.ibm.com)

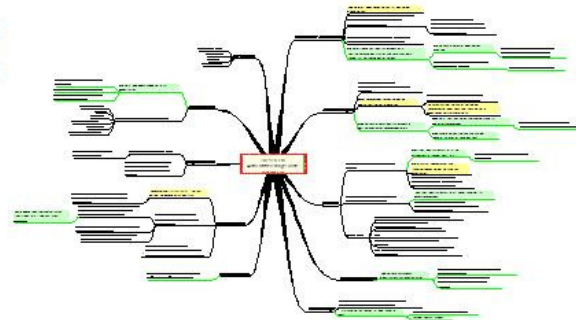
# 199x / 200x / 201x von der Vision über die Diskussionen zur Realisierung – der neue Personalausweis

Thesensammlung „digitale Authentifizierung“  
– Authentifizierungskarte – Bürgerkarte –  
„Online-Perso“

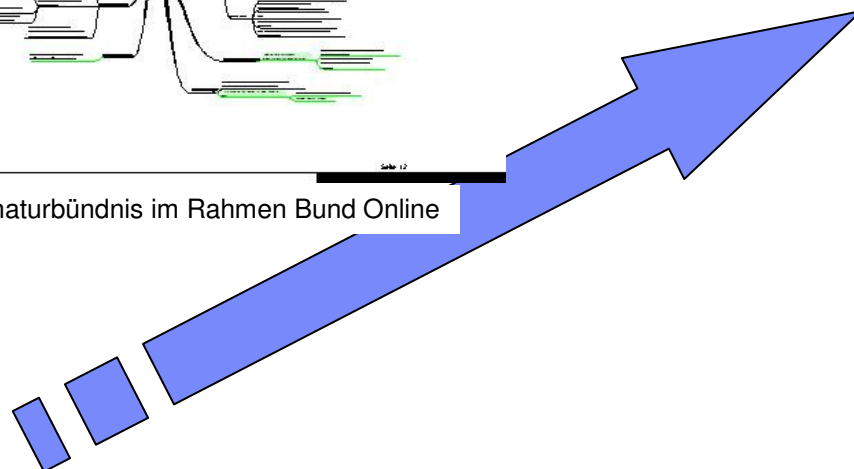


*On the internet, nobody  
knows you're a dog*

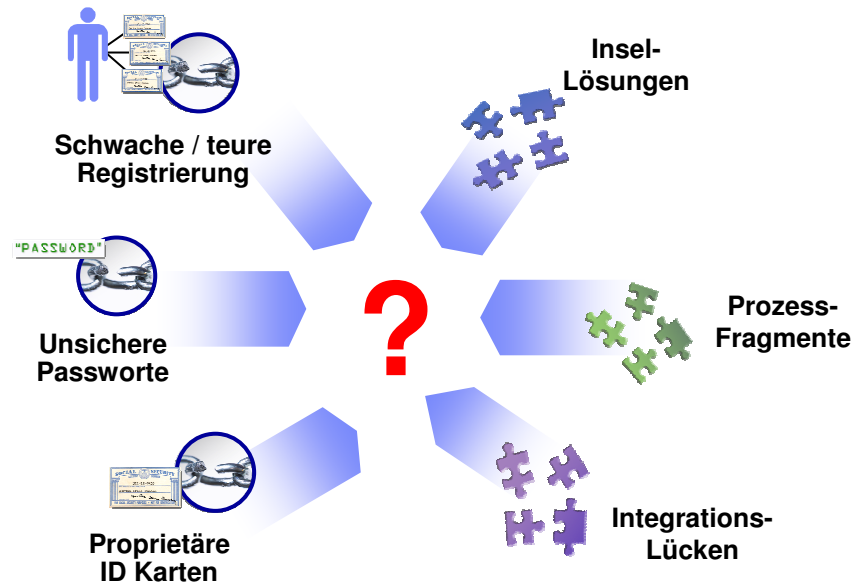
New Yorker, 5-Jul-1993



BMI, Signaturbündnis im Rahmen Bund Online



Identitäts- und Accessmanagement besteht heute oft aus fragmentierten Einzelprozessen und Lösungen und verursacht hohe Kosten für Unternehmen und Behörden

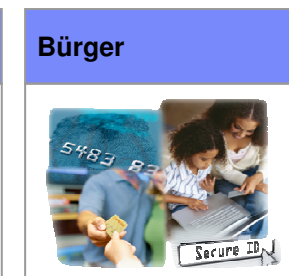


„Das erinnert mich daran, dass ich noch Ordnung in das Identitätsmanagement meiner Firma bringen muss.“

## Der neue Personalausweis liefert eine Infrastruktur für ein staatlich gestütztes Identitätsmanagement in eBusiness und eGovernment

- Der nPA ist ein RFID und Biometrie-gestütztes, elektronisches Reisedokument
- Der nPA bietet eine zentrale Authentifizierungsinfrastruktur, die jeder Bürger ab 16 Jahren nutzen kann
- Der nPA ermöglicht eine starke Authentisierung zwischen Nutzern und Betreibern von eBusiness- und eGovernment Diensten
- Inhaber können den nPA als „**Internet-Ausweis**“ nutzen (eID)
- Der nPA bietet zusätzlich eine Signaturfunktion
- Der nPA bietet ein höheres Sicherheitsniveau als heutige Standardverfahren (z.B. User-ID/Passwort oder PIN/TAN).

Der neue Personalausweis liefert neue Chancen, fordert aber auch ein Umdenken im Identitätsmanagement vieler Behörden und Firmen

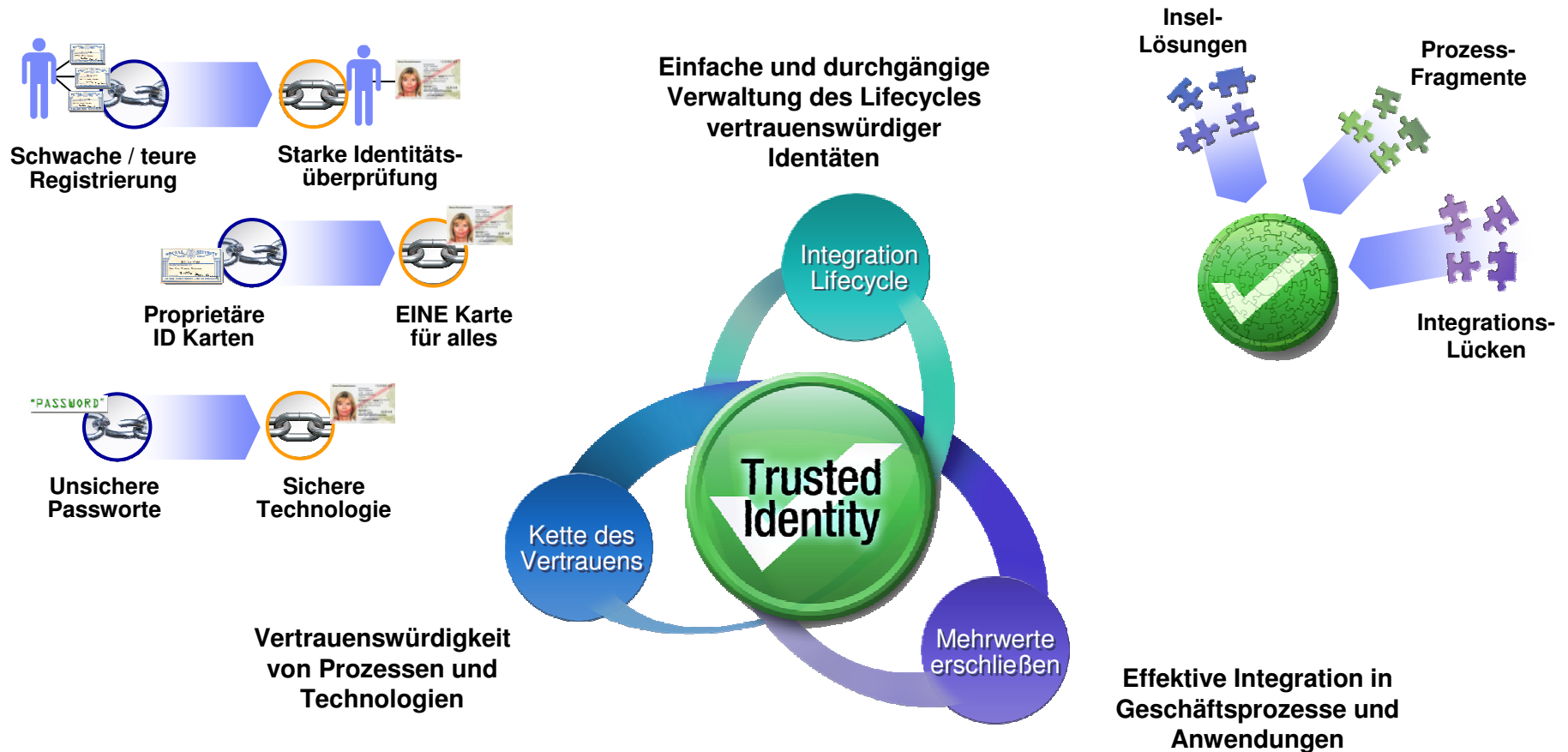


## Für einen potentiellen Diensteanbieter stellen sich unterschiedliche Fragen und Herausforderungen bei der Einführung des neuen Personalausweises

- Welche Geschäftsprozesse eignen sich für die Nutzung des nPA?
- Wie wird der nPA sicher in die bestehende Fachverfahren integriert?
- Wie schaffe ich eine nahtlose und effektive Integration in meine bestehende IT Infrastruktur?
- Wie kann ich einen Parallelbetrieb unterschiedlicher Authentifizierungsverfahren realisieren?
- Wie kann ich einfach, schnell und sicher weitere Dienste und Fachverfahren anbinden?
- Wie können zusätzliche Sicherheitsanforderungen umgesetzt werden?
  - Übergreifendes Identitätsmanagement
  - Integration in Autorisierungsmodelle (Rollen und Berechtigungen)
  - Nachvollziehbarkeit / Nachweisbarkeit / Berichtswesen
  - Einhaltung von Sicherheitsstandards- und Richtlinien
  - Sicheres Transaktions- & Sessionmanagement
  - Single Sign-On / Off



Es ist das Ziel der IBM innovative Methoden und Tools für ein integriertes und effektives Identitätsmanagement auf Basis des neuen Personalausweises zu entwickeln



## Die IBM ist Teilnehmer des erweiterten Anwendertests und integriert den neuen Personalausweis in seine Lösungen für ein integriertes Identitäts- und Accessmanagement

- Umfangreiche Beratungsservices zur Integration des neuen Personalausweises in eBusiness und eGovernment
- Integration des neuen Personalausweises in die Tivoli Identity und Accessmanagement Produkte
- Integration des neuen Personalausweises in die WebSphere Applikations- und Portalserver
- Enge Zusammenarbeit mit bremen online services (bos) bei der Entwicklung eines eID-Servers auf Basis der Governikus® Produktreihe
- Nutzung offener Standards wie SAML, OSCI, XML, SOAP, Common PKI, ITIL

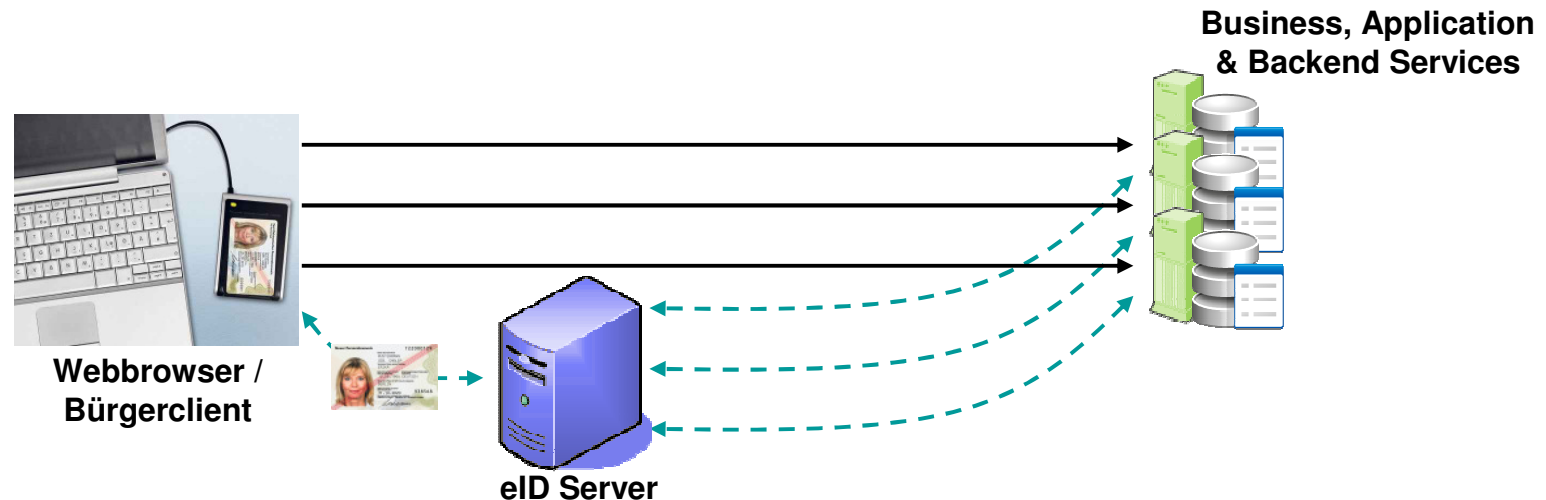


**Tivoli.**

**WebSphere.**

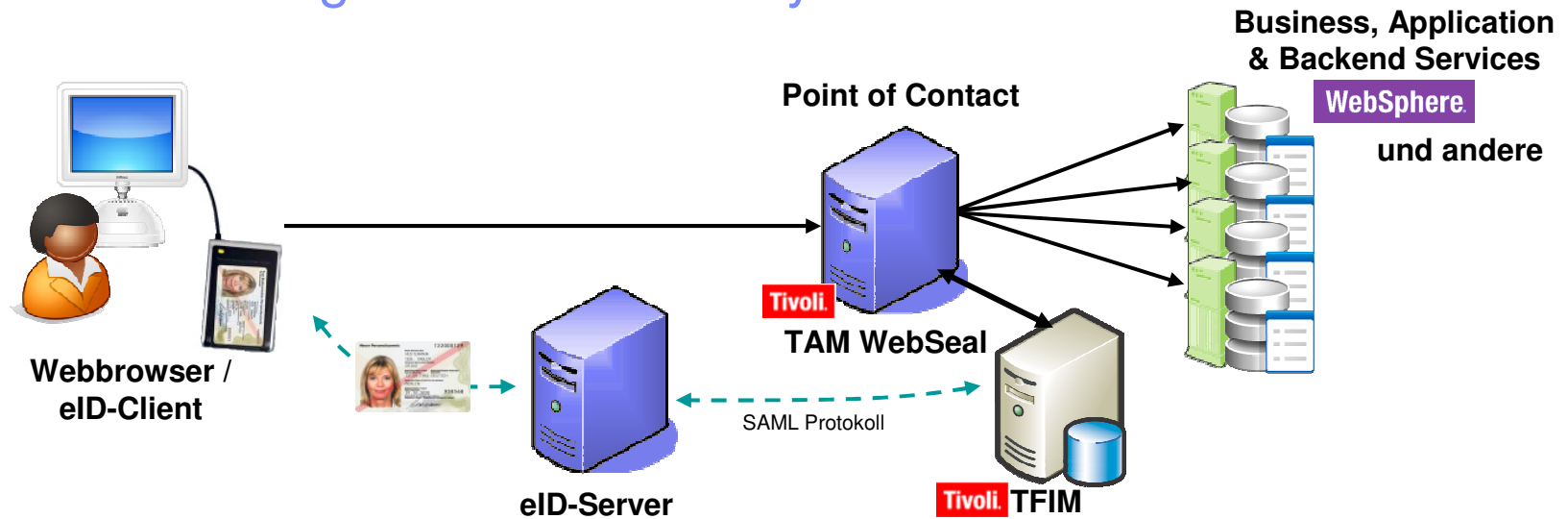


## Es gibt unterschiedliche Integrationsmodelle für die Einbindung des nPA in bestehende und neue Anwendungen



- Eine direkte Integration in die Web-Applikationen ist möglich, aber nicht die beste Lösung
  - Relativ hoher Entwicklungs- & Integrationsaufwand
  - Eigene Implementierung der nPA / SAML Schnittstellen notwendig
  - Keine zentrale Administration der Authentifizierung und Zugriffsberechtigungen
  - Schwierigere Umsetzung zonierter Sicherheitsarchitekturen

## Integration des nPA in ein zentrales Access Management für multiple Anwendungen und Backendsysteme



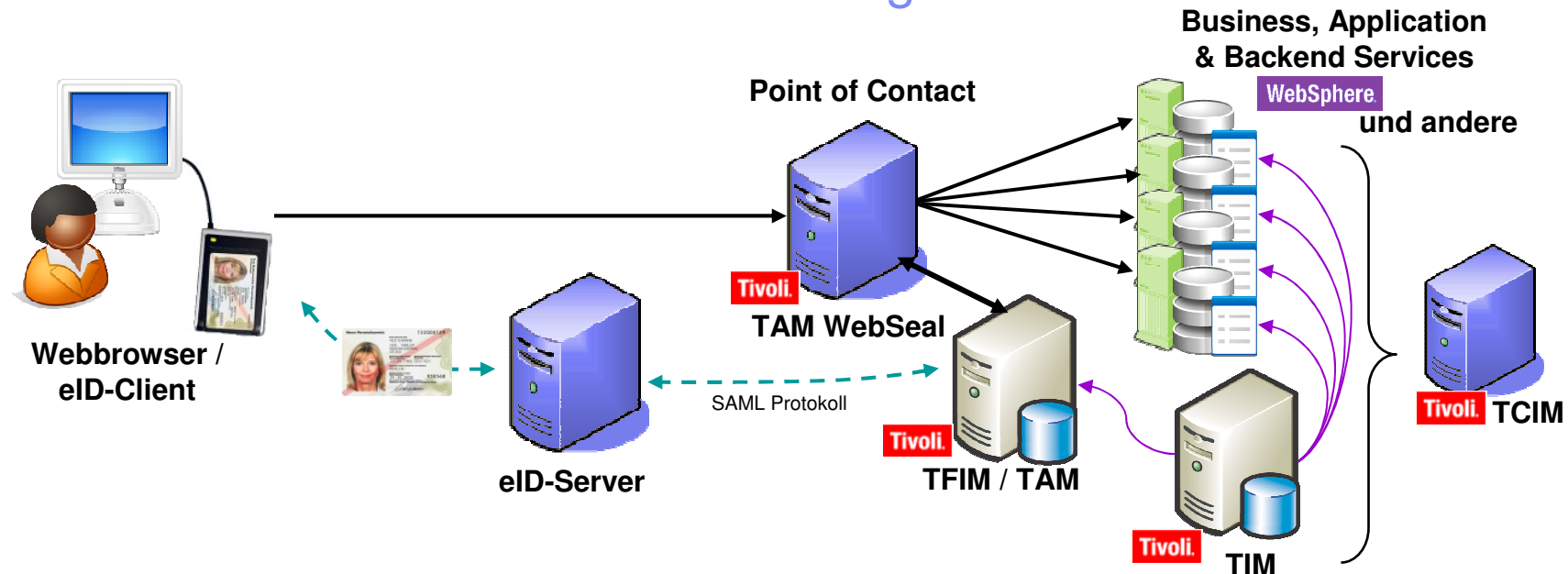
### Tivoli Federated Identity Manager (TFIM)

- SAML basierte Kommunikation mit eID Server/Bürgerclient
- Fertige Schnittstellen zu bestehenden Web-Servern, Proxies und Applikations-Servern
- Unterstützung unterschiedlicher Authentifizierungsverfahren

### Tivoli Access Manager (TAM)

- Verwendung des Tivoli Access Managers als „Single Point of Contact“
- Web Single Sign-On und Session Management
- Zentrale Authentifizierung und Autorisierung durch den TAMeB (vom BSI nach CC EAL3 zertifiziert)
- Zentrale Verwaltung der Zugriffsberechtigung für alle Server und alle Anwendungen

## Zusätzliche Lösungsbausteine für ein zentralisiertes, integriertes und automatisiertes Sicherheitsmanagement



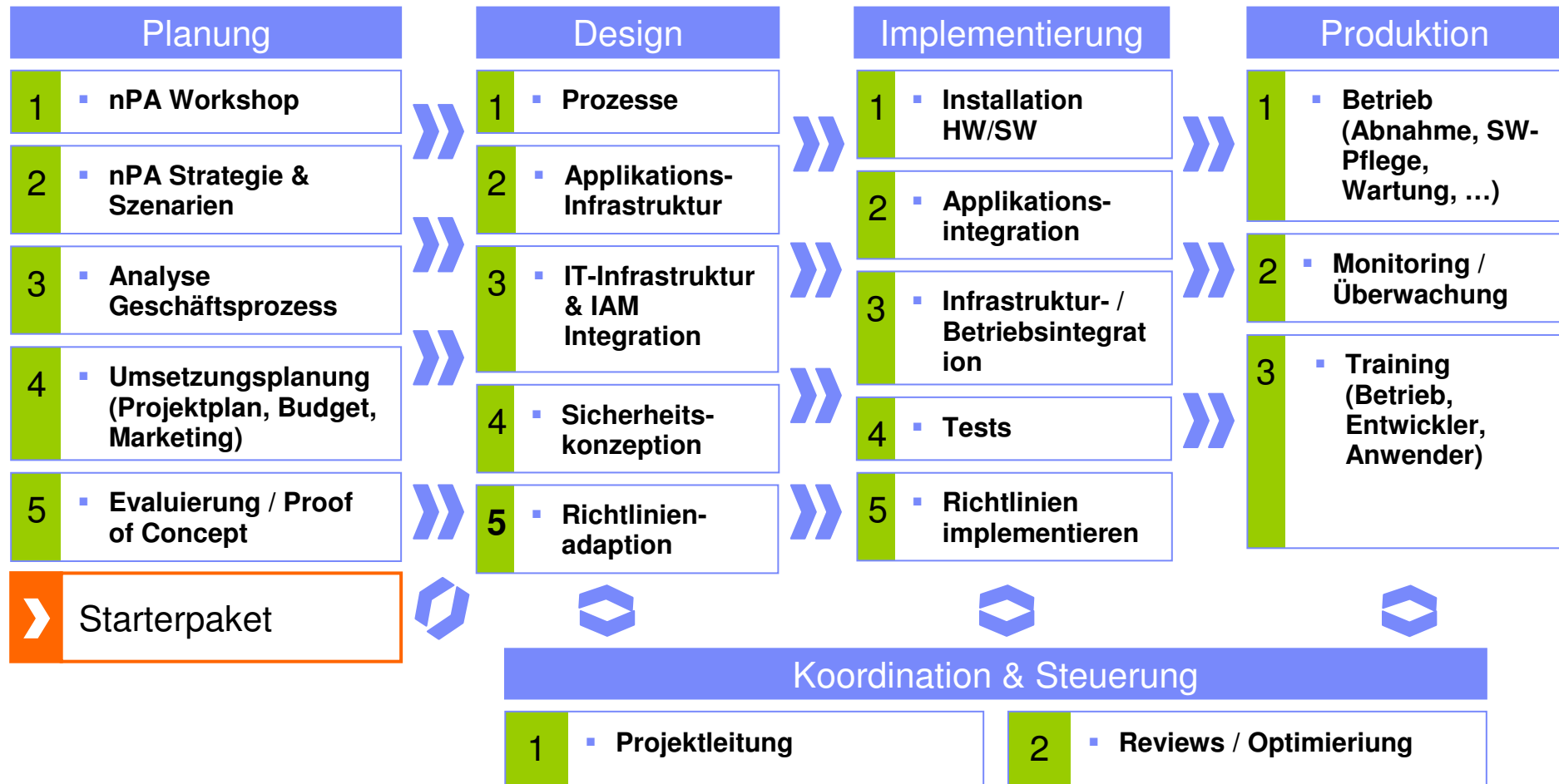
### Tivoli Identity Manager (TIM)

- Zentrales Identitätsmanagement für alle beteiligten Komponenten
- Workflow gesteuerte Genehmigungsprozesse
- Erweiterte Benutzermanagement Funktionen und Provisionierung

### Tivoli Compliance Insight Manager






- Zentrales Log-Management und Kontrolle aller Aktivitäten
- Privileged User Monitoring and Auditing (PUMA)
- Nachweisbarkeit und Nachvollziehbarkeit aller Benutzeraktivitäten

Neben der technischen Integration haben wir modulare Beratungs- und Servicepakete entwickelt, die eine effektive und nachhaltige Umsetzung von nPA Projekten erlauben



## Der neue Personalausweis kann sich zu einem zentralen Baustein für ein „Smarter Security Management“ in Deutschland entwickeln

Kritische Erfolgsfaktoren sind:

- Breite Annahme von Bürgern, Wirtschaft und Verwaltung 
- Einfache Integration in Geschäftsprozesse und Anwendungen ohne größere Änderung der IT-Anwendungen und Systeme 
- Effiziente Integration in ein unternehmens-/behördenweites Identity und Access Management 
- Erweiterung der sinnvollen Anwendungsszenarien durch Anpassung von Rechtsvorschriften an die Bedürfnisse von eBusiness und eGovernment 
- Sicherheits- und Datenschutzdiskussion auf Grundlage von Fakten und fair bewerteten Risiken 

## Vielen Dank! Haben Sie Fragen?

Wir zeigen die Integration des neuen Personalausweises live auf der CeBIT –  
kommen Sie einfach vorbei.

- IBM Hauptstand Halle 2 – Demopunkt 12 (Smarter Security Zone)
  - ShowCase **nPA-Integration**
  - Beratungsleistungen rund um den nPA
  - Integration des nPA in die IBM Tivoli Produkte
- IBM Public Sektor Stand Halle 9 – Demopunkt 7
  - ShowCase **eSAFE**
  - Anwendungsszenarien für den nPA
  - Integration des nPA in die IBM Tivoli Produkte

Marc Albrecht



**Senior Managing Consultant**

IBM Deutschland  
Beim Strohause 17  
20097 Hamburg

Mobil: 49-172-7350851  
Mail: [marc.albrecht@de.ibm.com](mailto:marc.albrecht@de.ibm.com)

