Microsoft® Forefront™

Microsoft Identity & Access Plattform

Jörg Schanko
Technologieberater Forschung & Lehre
Microsoft Deutschland GmbH
joergsc@microsoft.com

Extending into the Cloud

Traditional Datacenter

Virtualized Datacenter

Private Cloud

- Management Costs Decrease Significantly
- Scale-out Development Expense

Public Cloud

- Capacity on Demand
- Global Reach

Herausforderung

- Identity & Access Management
  - Wie und wo verwalte ich Benutzer?
  - Wo lege ich Berechtigungen fest?
  - Wie implementiere ich ein *einheitliches* System in einer *heterogenen* Umgebung?
  - ???


Bali, Indonesien

Weiß' dich aus, dann stelle ich einen aus.

Ich benötige einen Reisepaß

Ich vertraue der BRD. Mit einem offiziellen Reisepaß bekommst Du ein Visum

Ich möchte einreisen. Was benötige ich?

Ich vertraue nur meiner eigenen Regierung. Frag' die!

Ich möchte einreisen. Was benötige ich?


Berlin


EUROPÄISCHE UNION
BUNDESREPUBLIK DEUTSCHLAND
REISEPASS

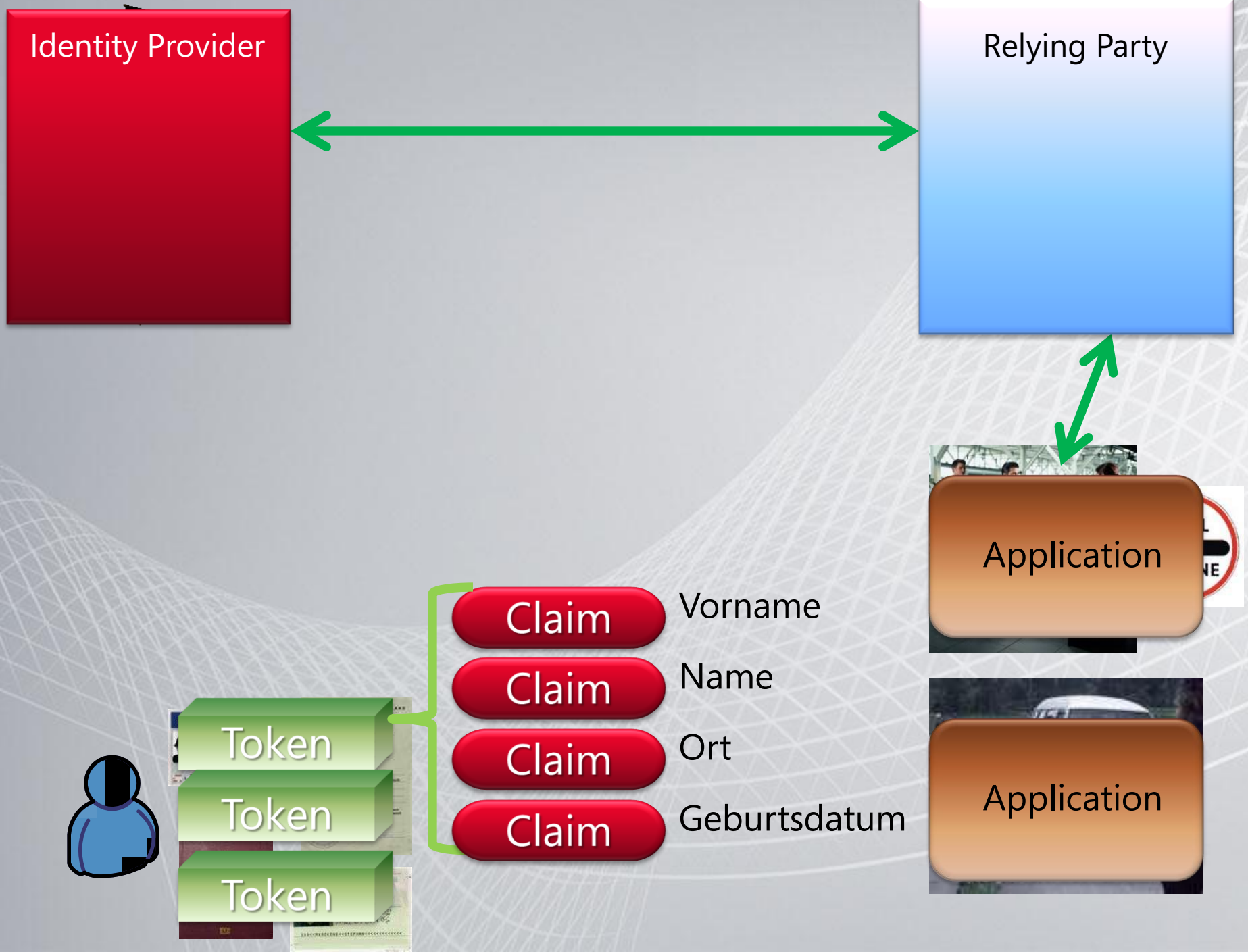

EUROPÄISCHE UNION
BUNDESREPUBLIK DEUTSCHLAND
REISEPASS


ZOLL
DOUANE

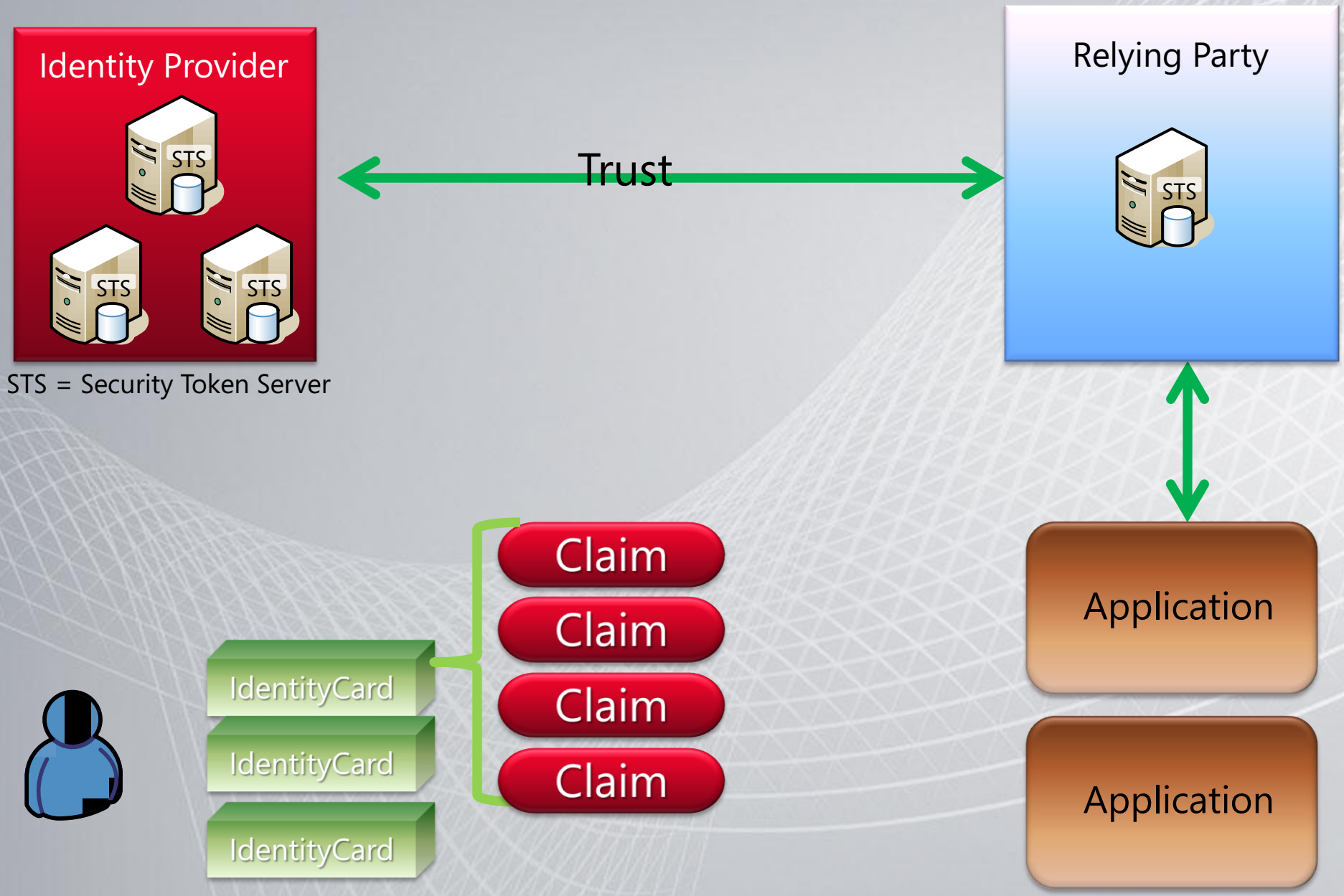

Berlin


ZOLL
DOUANE

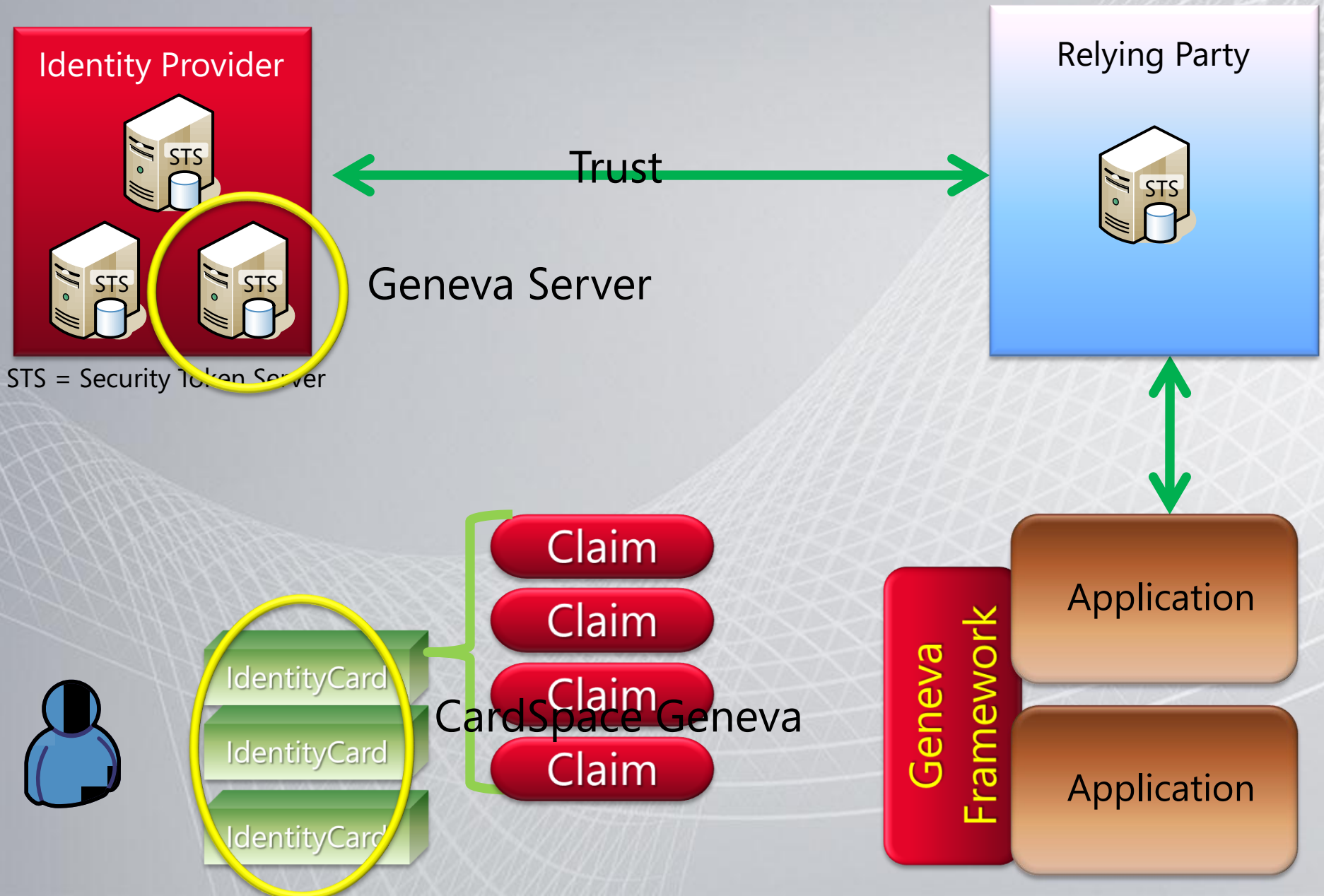

EUROPÄISCHE UNION
BUNDESREPUBLIK
DEUTSCHLAND
REISEPASS


Identity Provider
Relying Party
Application
Application
Token
Token
Token
Claim
Claim
Claim
Claim
Vorname
Name
Ort
Geburtsdatum

Claim-based Authentication



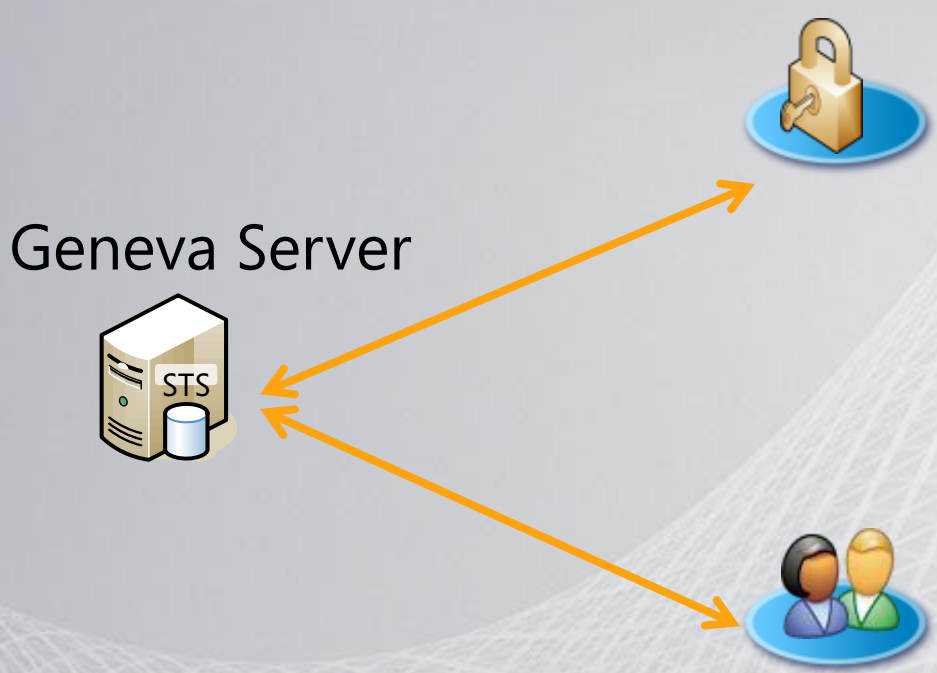
„Geneva"


Identity Provider
STS
STS
STS
Trust
Relying Party
STS
Geneva Server
STS = Security Token Server
Claim
Claim
Claim
Claim
IdentityCard
IdentityCard
IdentityCard
CardSpace Geneva
Geneva Framework
Application
Application

Geneva Server

- Security Token Server zur Ausgabe und Umwandlung von Claims und Token
- Weiterentwicklung von ADFS 1.0
- Unterstützt WS-Federation und SAML 2.0
- Aktive und passive Clients
- Einrichten und Verwalten von Vertrauensstellungen (Trusts)
- Automatische Erneuerung von Zertifikaten
- Getrennte Speicher für Konten und Attribute möglich

Geneva Server



Account Provider
- Active Directory
- LDAP (AD LDS)
- …

Attribute Provider
- Active Directory
- AD LDS
- SQL Server
- …

CardSpace Geneva

- Benutzerbezogener Speicher für Identitätskarten
  - Identitätskarte=XML-Datei, die eine Verbindung zu einem STS repräsentiert
- Ermöglicht dem Benutzer visuelle oder automatische Auswahl des passenden STS zu einer Anwendung
- Kann vom STS befüllt werden
- InformationCards können mit PIN geschützt werden
- Unterstützung von „roaming“ Benutzern

Geneva Framework

- Unterstützt Entwickler bei der Erstellung von „Claims-aware“ Anwendungen
  - Verifizierung von Token
  - Extrahierung der Claims aus einem Token
  - Umgang mit Claims (Type, Value, Issuer,…)
- Erlaubt das Erstellen eigener STSe
  - Geneva Server basiert auf Geneva Framework

Identity and Access Management

Create

- Provision user
- Provision credentials
- Provision resources

Retire

- De-provision identities
- Revoke credentials
- De-provision resources

Policy Management

- Policy authoring
- Policy enforcement
- Approvals and notifications
- Audit trails

Credential Management

- Identity validation
- Smart Card/Certificates Issuance
- Access Entitlements established
- Integrated Workflow

Update

- Role changes
- Password and PIN reset
- Resource requests

Forefront Identity Manger - Feature areas

Policy Management

- SharePoint-based console for policy authoring, enforcement & auditing
- Extensible WS– * APIs and Windows Workflow Foundation workflows
- Heterogeneous identity synchronization and consistency

Credential Management

- Heterogeneous certificate management with 3rd party CAs
- Management of multiple credential types, including One Time Passwords
- Self-service password reset integrated with Windows logon

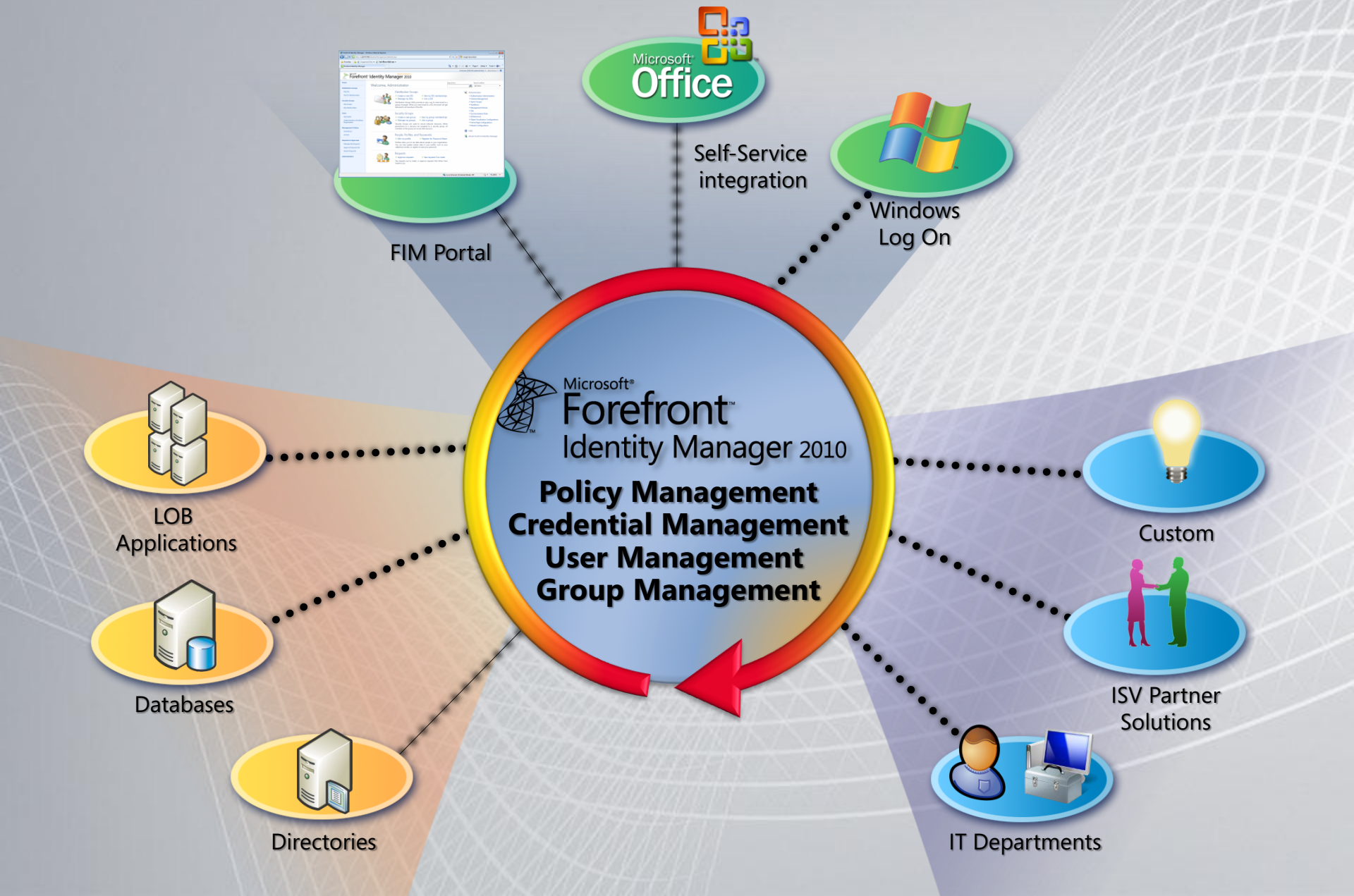
User Management

- Integrated provisioning of identities, credentials, and resources
- Automated, codeless user provisioning and de-provisioning
- Self-service profile management

Group Management

- Rich Office-based self-service group management tools
- Offline approvals through Office
- Automated group and distribution list updates

Forefront Identity Manager in Action



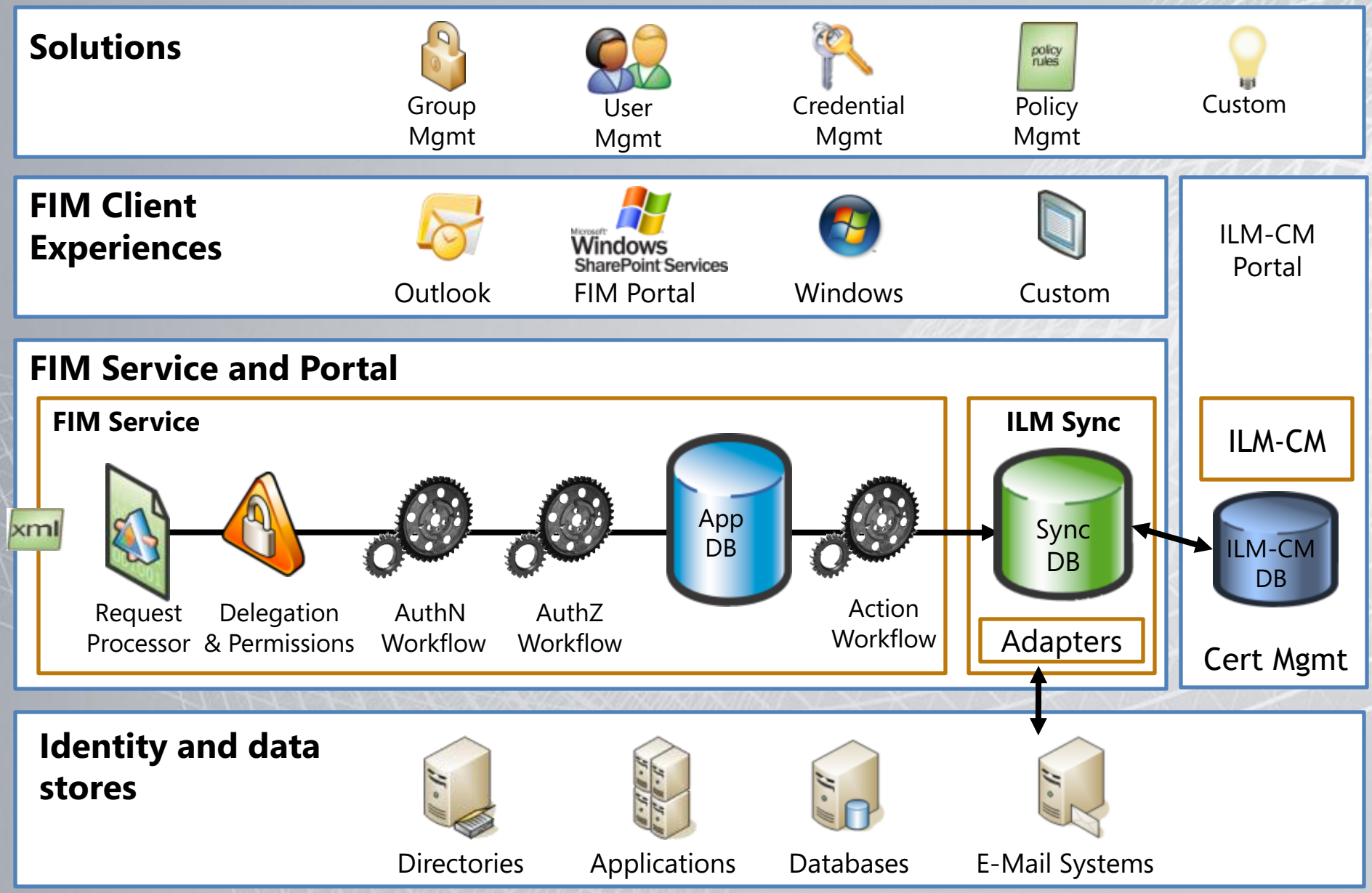
Customizable Identity Portal

SharePoint-based Identity Portal for Management and Self Service

How you extend it

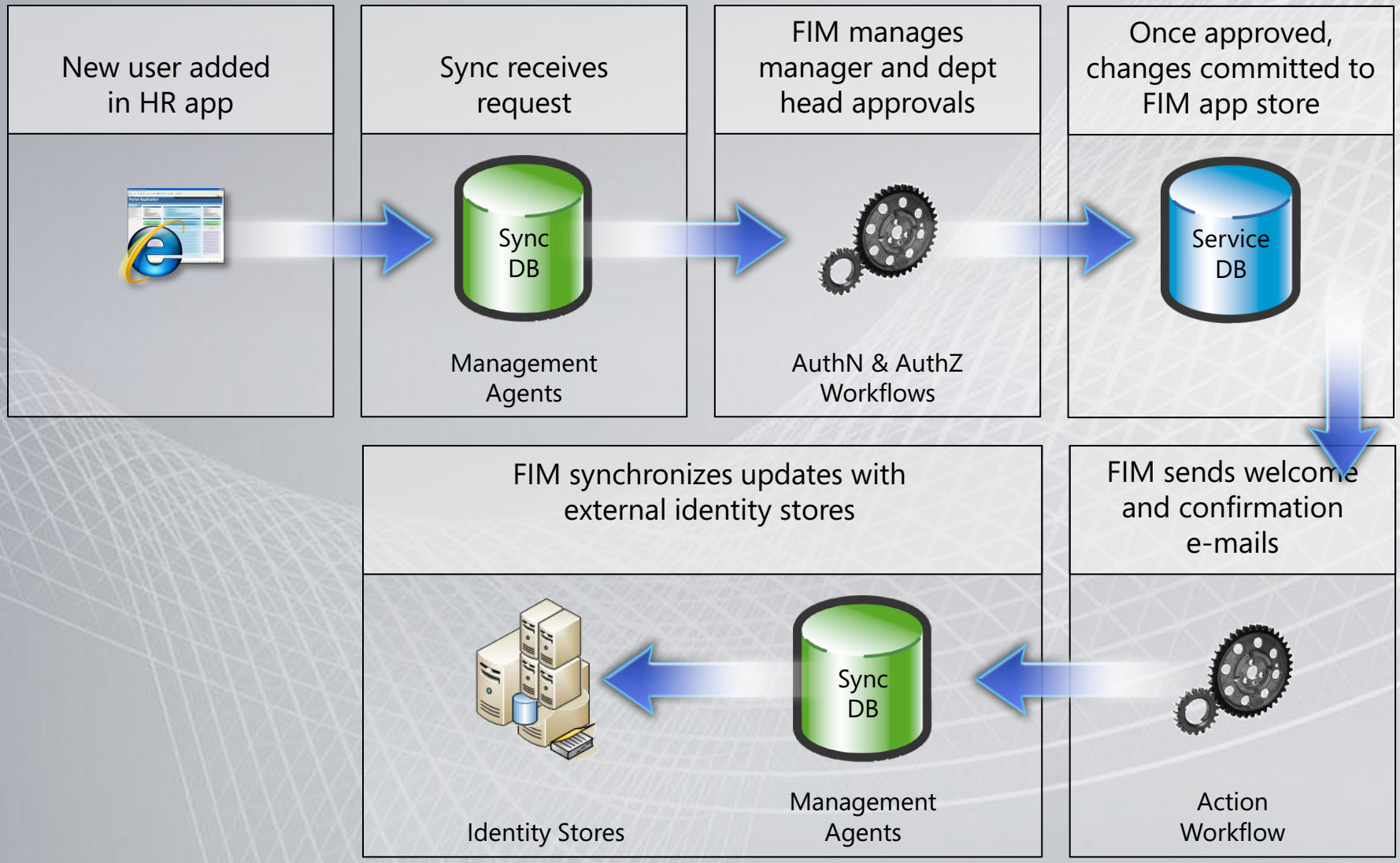
- Add your own portal pages or web parts
- Build new custom solutions
- Expose new attributes to manage by extending FIM schema
- Choose SharePoint theme to customize look and feel

Forefront Identity Manager 2010 Architecture



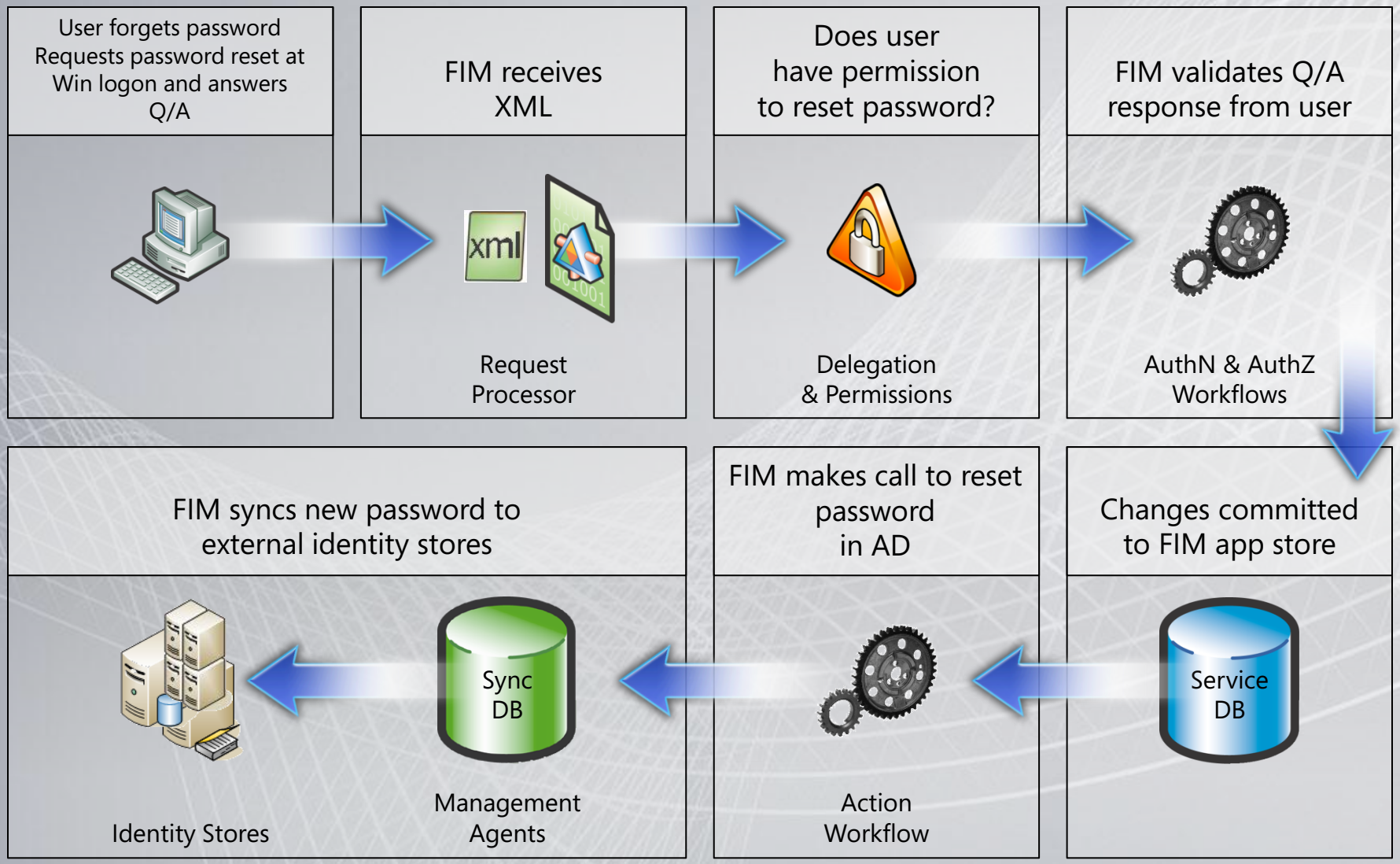
FIM 2010 In Action

HR-driven provisioning a of new employee



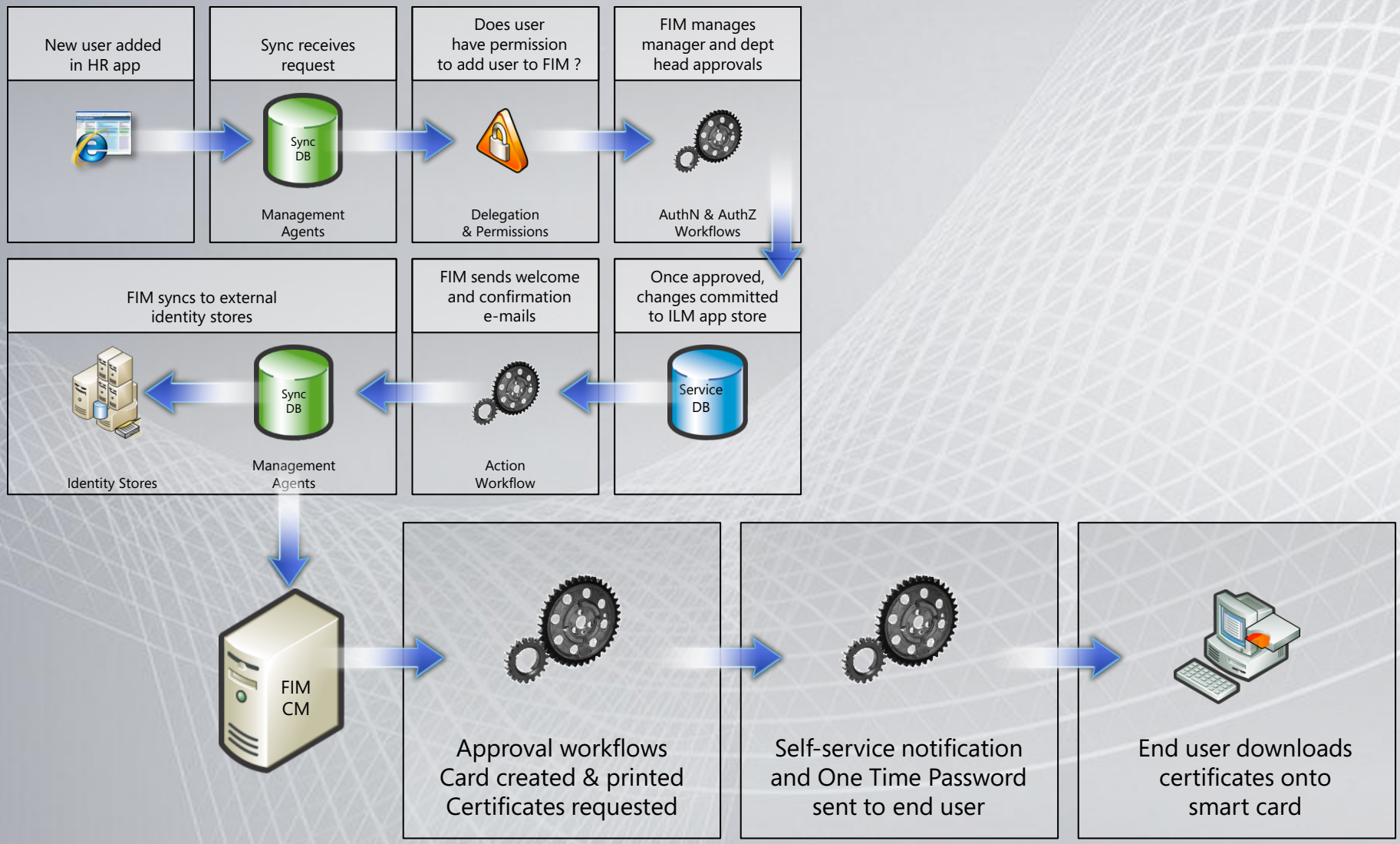
FIM 2010 In Action

Self-service password management



FIM 2010 In Action

Self-service smart card provisioning



Management Agents

- Active Directory
- ADAM
- iPlanet
- SQL
- Oracle
- DSML 2.0
- LDAP Directory Interchange Format (LDIF)
- Delimited Text
- Fixed-Width Text
- Attribute-Value Pair Text
- NT4
- Exchange 5.5
- Lotus Notes
- Novell eDirectory
- IBM DB2
- IBM Directory Manager
- SAP
- OpenLDAP
- Management Agent SDK (für eigene Erweiterungen)

Webcast

- **"Geneva" Server and Framework Overview (Level 300)**
- Tuesday, November 04, 2008 7:00 PM Pacific Time (US & Canada)

- https://msevents.microsoft.com/CUI/WebCastEventDetails.aspx?EventID=1032394338&EventCategory=5&culture=en-US&CountryCode=US

Hilfreiche Links

- Geneva
  - https://connect.microsoft.com/site/sitehome.aspx?SiteID=642
  - www.microsoft.com/geneva
- FIM 2010
  - http://www.microsoft.com/forefront/en/us/identity-manager.aspx