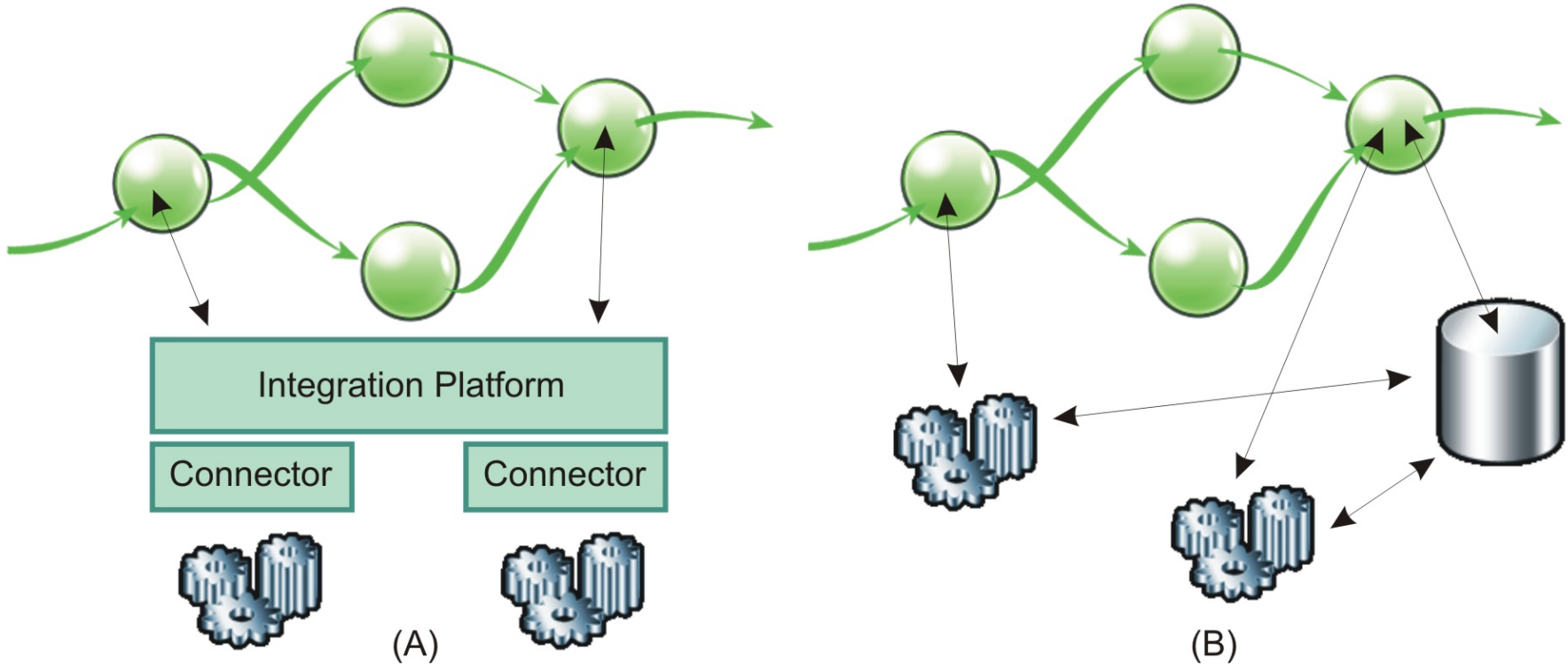




Identität und Autorisierung als Grundlage für sichere Web-Services

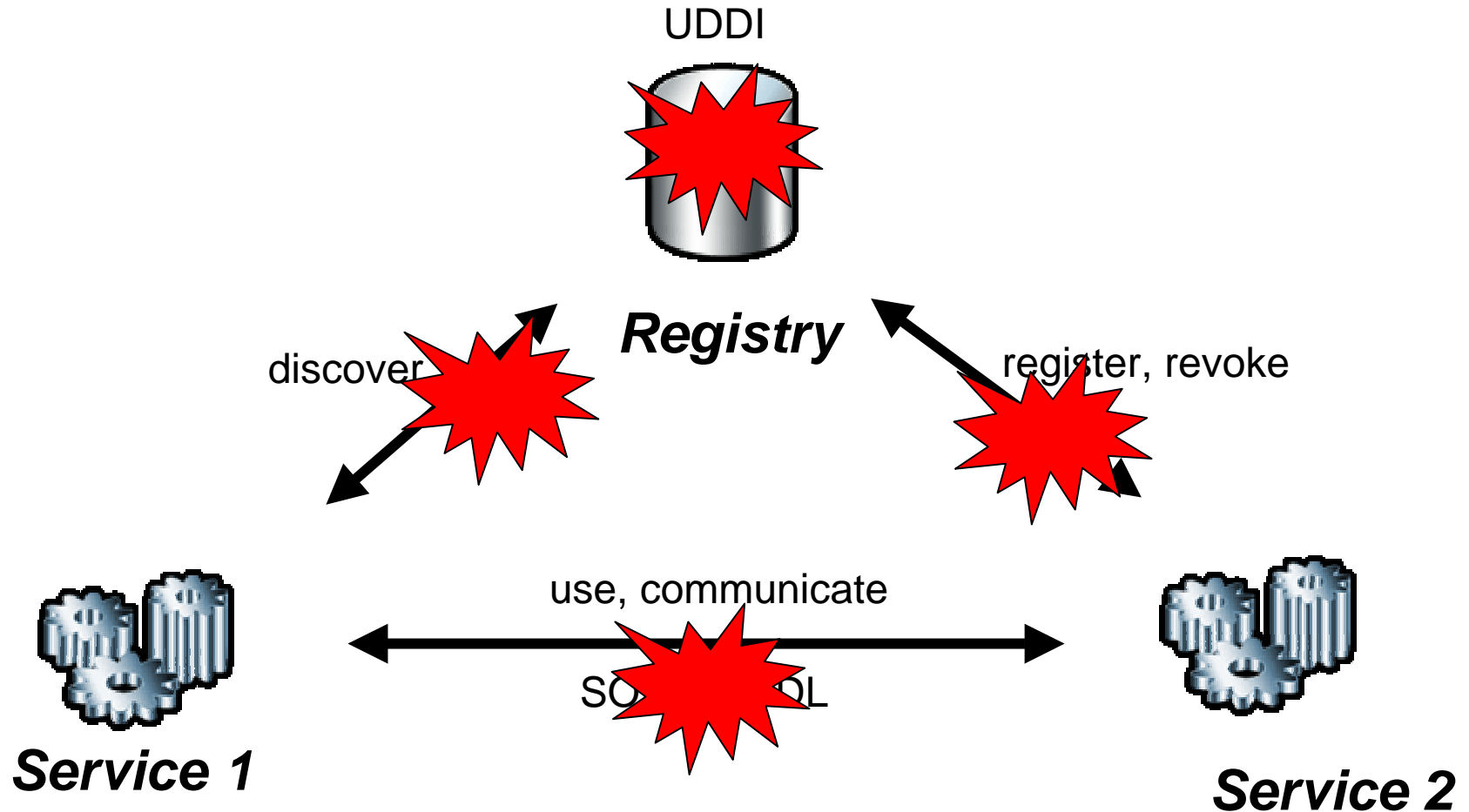
Dr. Hannes P. Lubich
IT Security Strategist

The Web Services “Temptation”

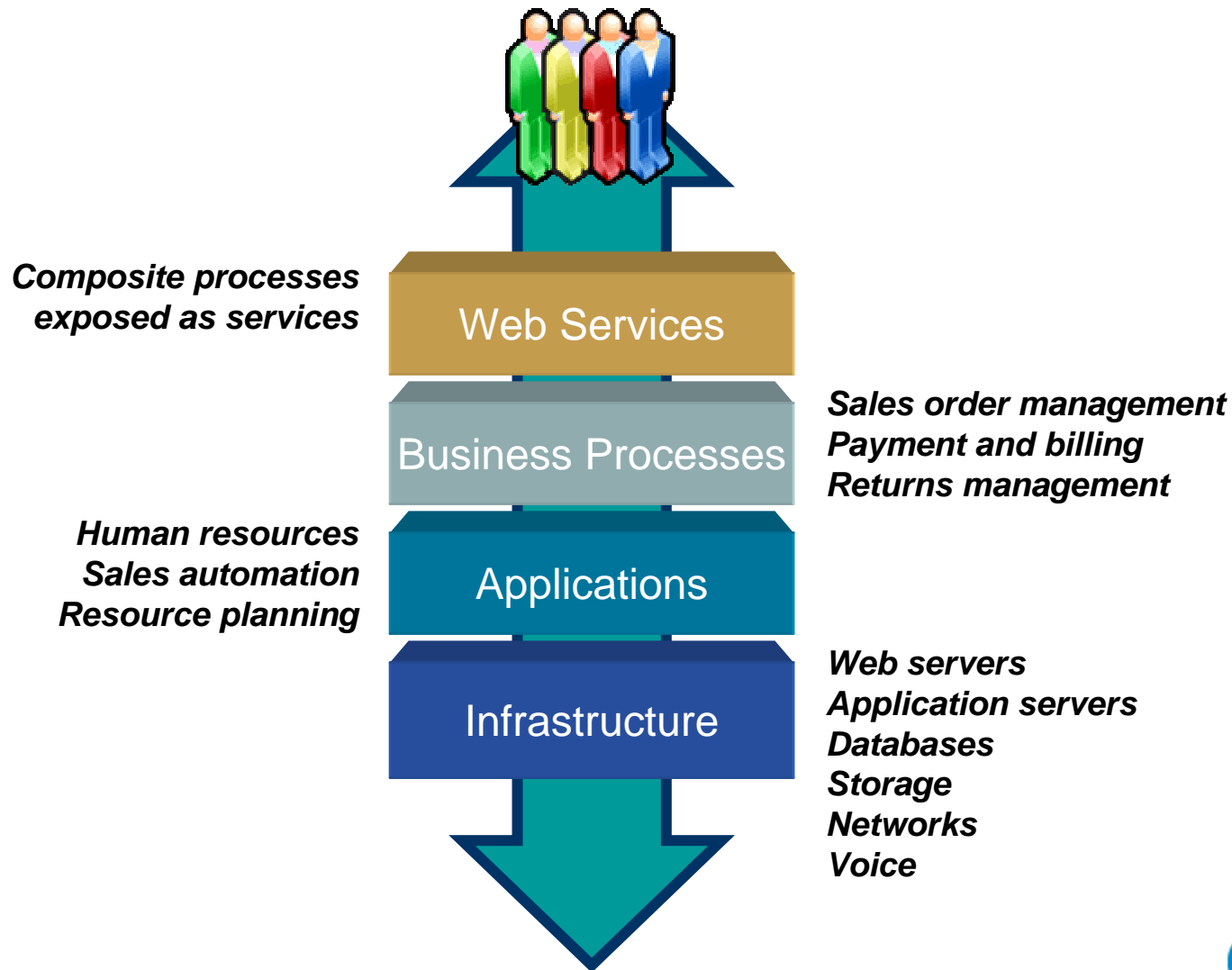


- For every \$1 spent on software \$3 to \$5 is spent on integration
- 70% of IT budgets is spent on integration
- Web services replace expensive top down integration with a bottom up grass roots effort

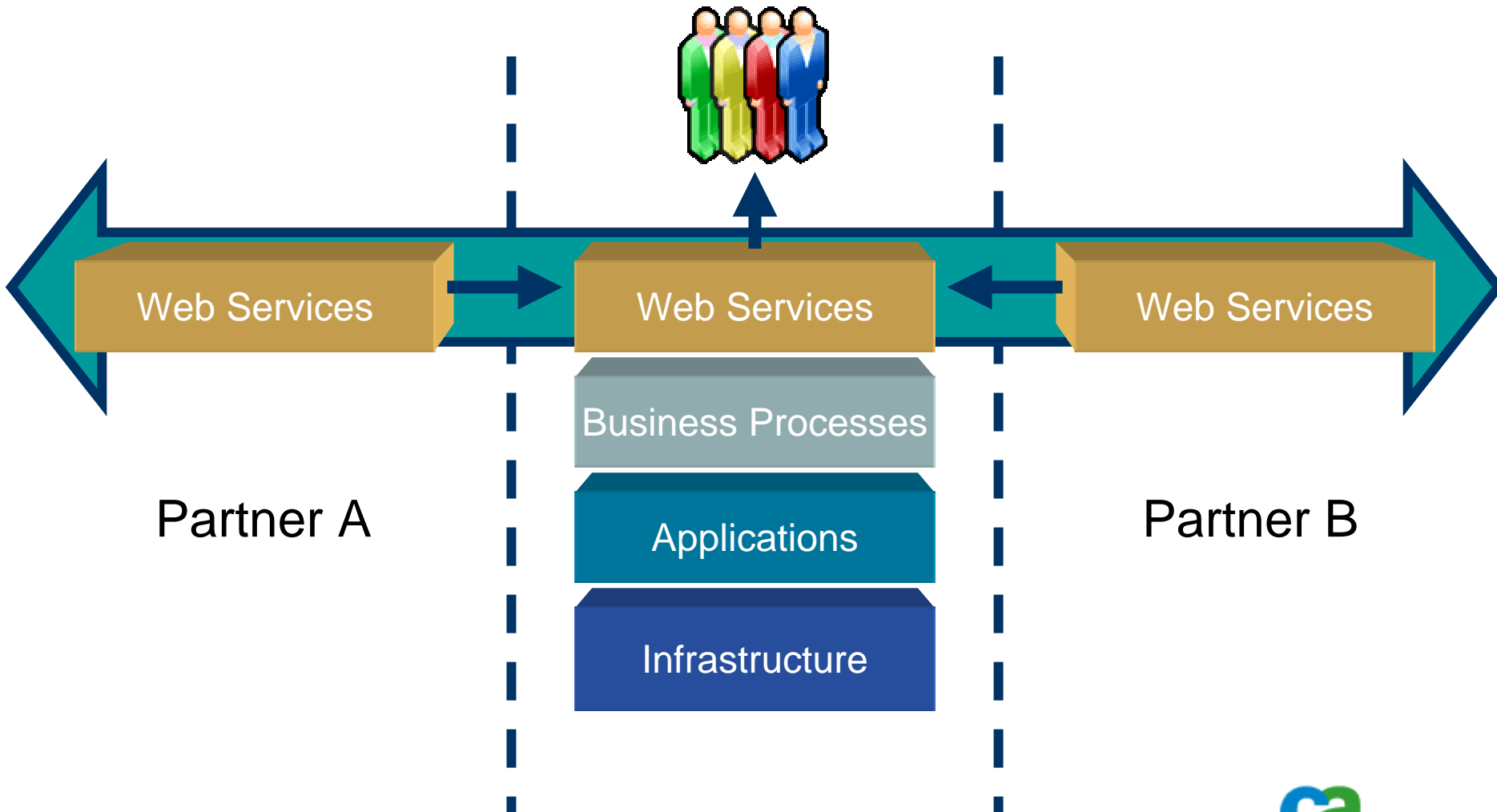
Service-Oriented Architecture: Weak Spots



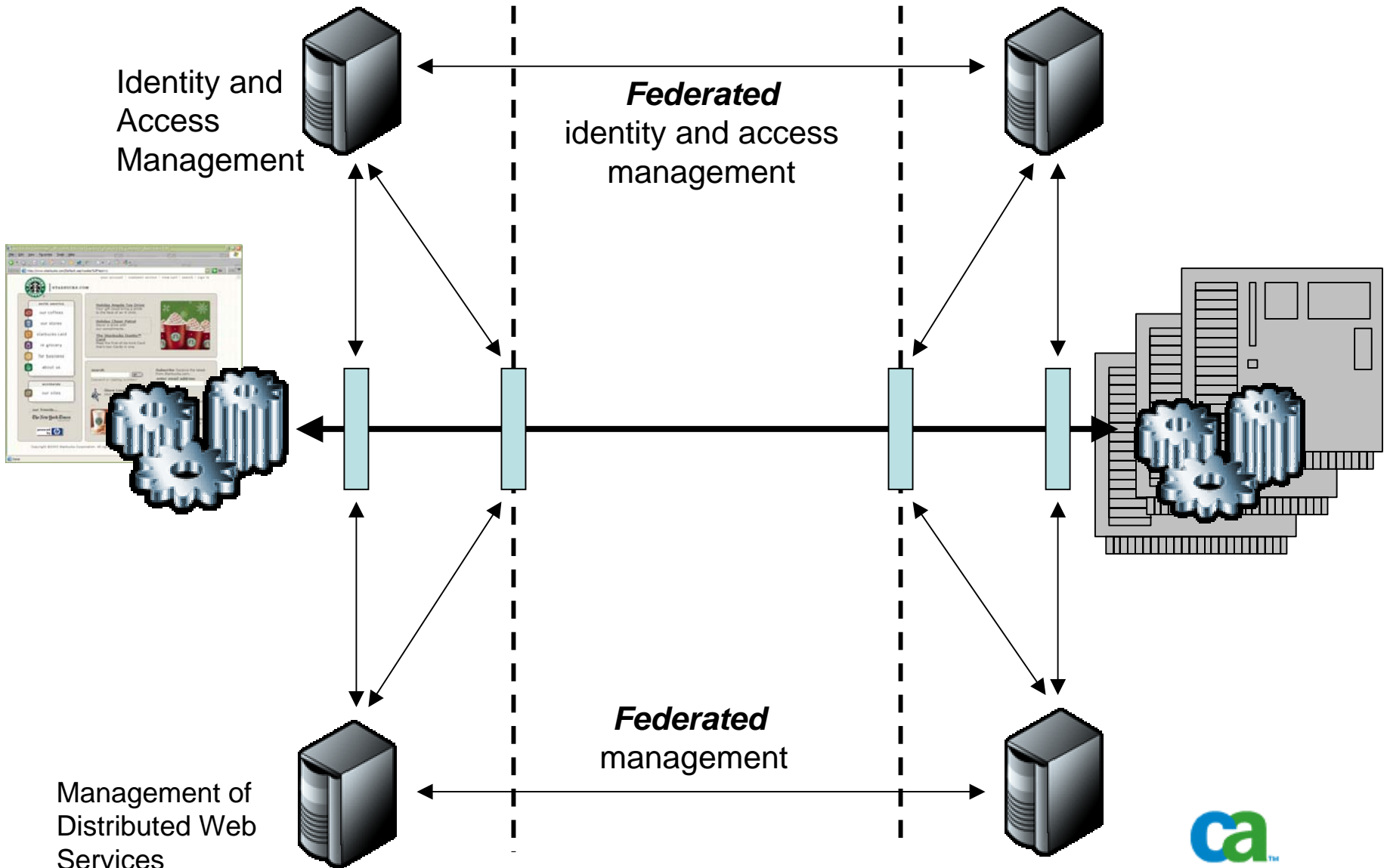
Traditional Web Services Security Model: Security layers built on top of each other



Intermediary Web Services Security Model: Additional end to end web services security



Managing and Securing Web Services



Security Requirements for Web Services

- CIAO: Confidentiality, Integrity, Availability, Obligation
- Strong identification, authentication and authorization chain
 - Between users and applications, as well as between applications
- Monitoring, event management/correlation, and auditability
- Transparent and acceptable cost/risk versus benefit ratio
- Clearly defined change / configuration management
- Scalability, also in federated environments
- Usage of standards and best practices



Web Services Security Standards

- **XML Signature** ensures integrity of XML information inside a SOAP message.
- **XML Encryption** ensures confidentiality of XML information transfers.
- **WS-Security*** defines a carrier of identity and other security-related information in interactions with a Web service (IBM, Microsoft).
- **Security Assertion Markup Language (SAML)** helps to assert statements and conditions against a security authority and policies that it manages. SAML can be used in interactions between security authorities.
- **XML Key Management (XKMS)** describes how to obtain keys, certificates, tokens, and others, from a security authority and from Web services themselves.
- **eXtensible Access Control Markup Language (XACML)** expresses and exchanges policy definitions in XML. It can be used to reconcile policies in a federation scenario.
- **Service Provisioning Markup Language (SPML)** helps to interface a security agent or a platform itself to allow control and configuration of security.

Further information: <http://www.oasis-open.org/committees/>
<http://www.projectliberty.org/>



Key Standards & Specifications

SAML – Security Assertion Markup Language

- An open framework for sharing security information on the Internet through XML documents
- Designed to address the following
 - Limitations of web browser cookies
 - SAML provides a standard way to transfer “cookies” across multiple Internet domains
 - Proprietary web single sign-on (SSO)
 - SAML provides a standard way to implement SSO within a single domain or across multiple domains
- Standard managed by OASIS
 - SAML 1.0, 1.1, & 2.0
 - CA key long-time contributor
- Protocol & ticket together enable federation
 - Cross-domain/cross-company SSO



Key Standards & Specifications

The Liberty Alliance Project

- Liberty includes three phases
 - *Phase 1: Identity Federation Framework (ID-FF)*
 - Federated network identity services including single sign-on/out, opt-in account linking, privacy
 - *Phase 2: Identity Web Services Federation (ID-WSF)*
 - Framework for interoperable federated network identity services including identity data service definition, identity service discovery and invocation, attribute sharing, interaction, security profiles
 - *Phase 3: Identity Services Interface Specification (ID-SIS)*
 - Interoperable identity services providing implementation of ID-WSF definitions in specific web services, e.g., personal profile, employee profile, etc.



Key Standards & Specifications

WS-* Key Specifications – Microsoft & IBM

- WS-Trust

- Defines the protocol used for security token acquisition or challenges to a requestor to ensure the validity of a security token

- WS-SecureConversation

- Extends WS-Security by:

- Defining the creation and sharing of security contexts between communicating parties using security context tokens (SCT)
- Specifying how derived keys (used for signing and encrypting messages associated with the security context) are computed and passed



Key Standards & Specifications

WS-* Key Specifications – Microsoft & IBM

■ WS-Policy

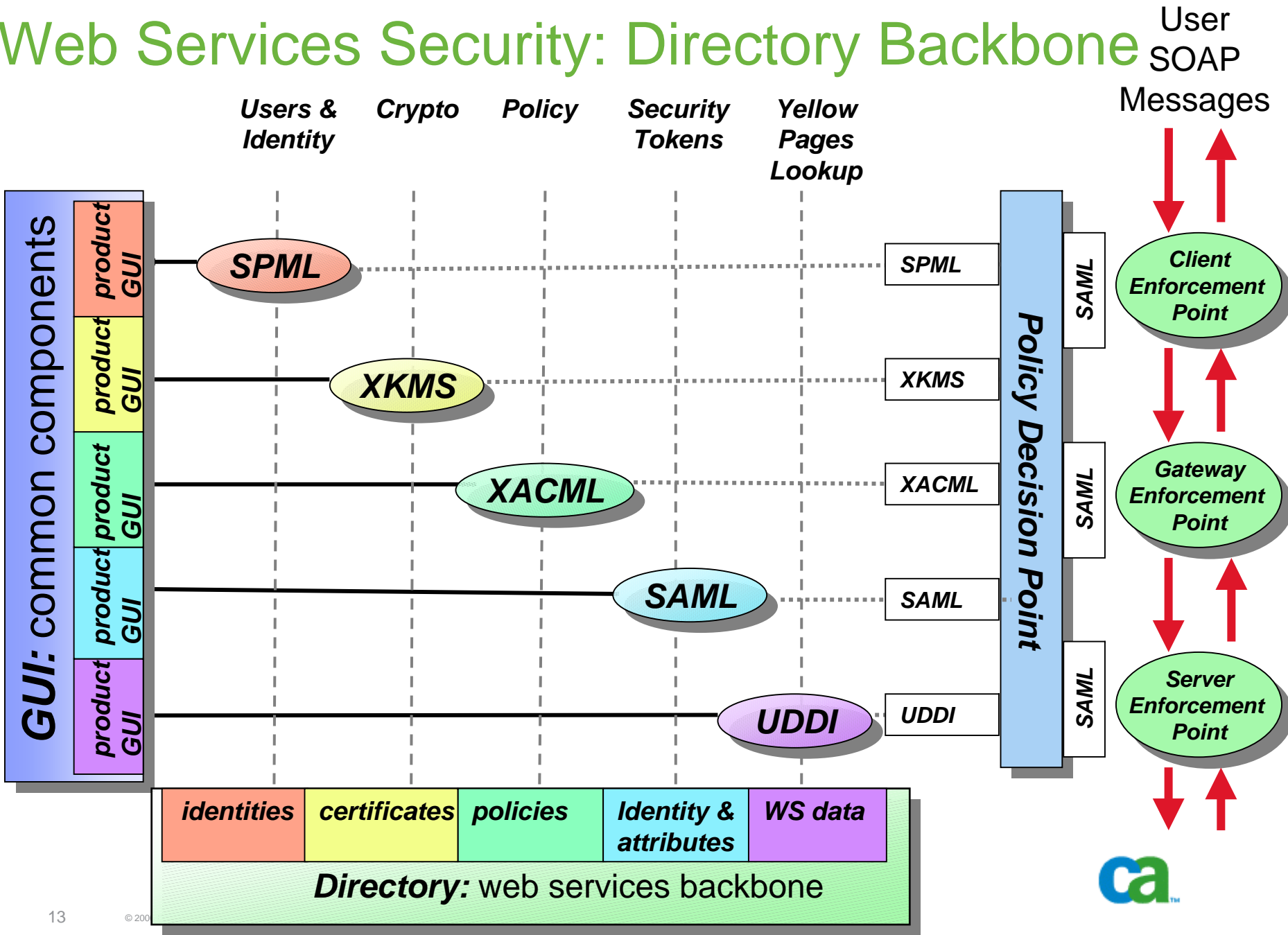
- Expresses the capabilities and requirements of entities used in web services environments
- A policy is expressed as policy assertions
- A policy assertion represents a capability or a requirement (Policy assertions are defined in the WS-PolicyAssertions specification)
- WS-Policy expressions are associated with various web services components using the Web Services Policy Attachment specification (WS-PolicyAttachment)

■ WS-Federation

- Relies on the models defined in WS-Security, WS-Trust, and WS-Policy
- Enables brokering of trust and security token exchange, support for privacy by hiding identity and attribute information, and federated sign-out
- Competes with Liberty's ID-WSF

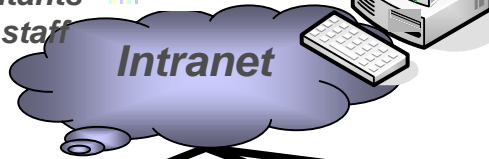
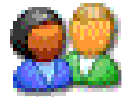


Web Services Security: Directory Backbone

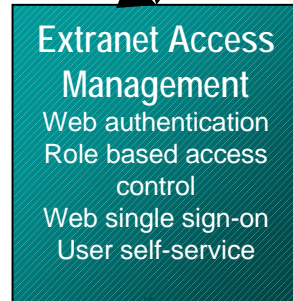
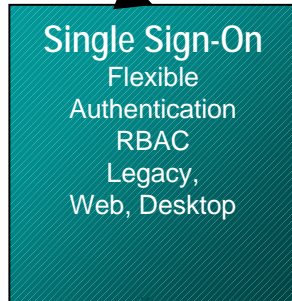
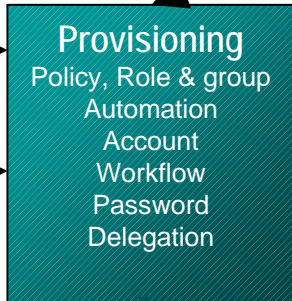
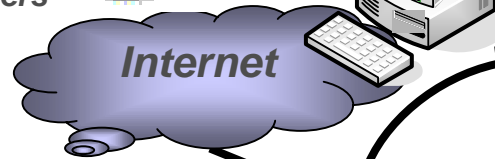
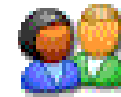


Security Building Blocks and Interfaces

Employees
Partners
Consultants
Temp. staff



Clients
Partners
Suppliers



Summary

Communication End User – Web Application

- ONE centralized user administration and provisioning environment for MANY Web applications
- Reduction of administrative user handling overhead by automation
- „Closing the gap“ to existing PKI or SSO environments (who am I?)
- “Secure enough” primary identification and authentication process (what am I allowed to do?)
- Standardized application and middleware interfaces

Communication Web Application - Web Application

- Centralized access control for transactions between applications in federated environments
- Confidentiality of information through strong encryption mechanisms
- Integrity of data being transferred and processed through digital signatures
- End to end availability of applications through service levels and monitoring
- Obligation of transactions through stringent record keeping and auditing

