



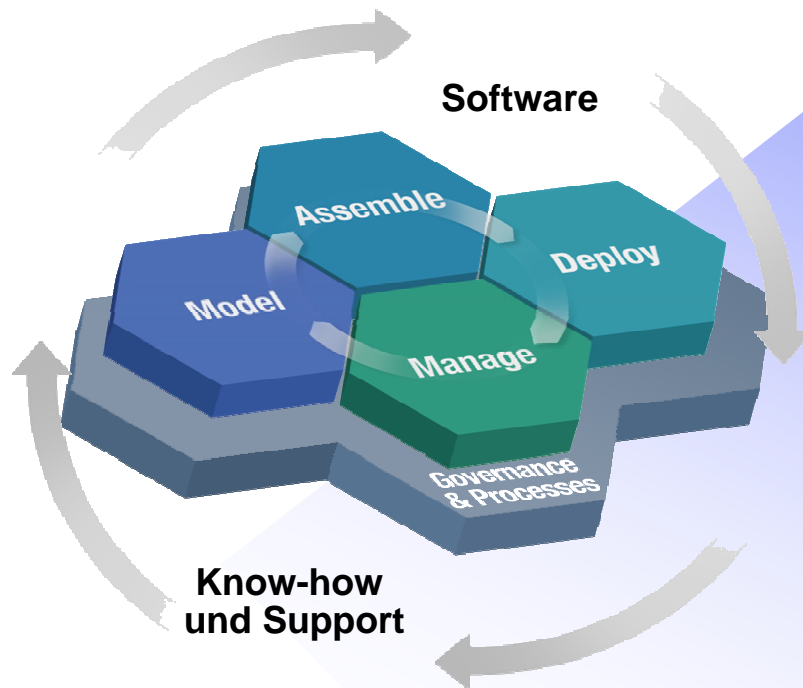
IBM Software Partner Academy Program

Telefonkonferenz am 08.05.09

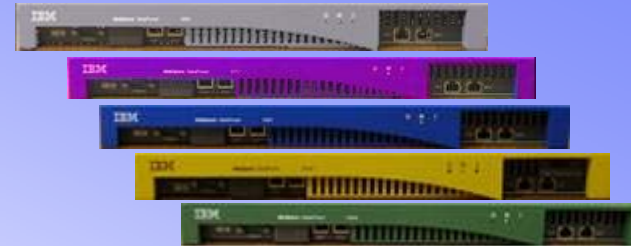
DataPower SOA-Appliances

Dr. Thorsten Harth, IBM DataPower Technical Sales

Überblick DataPower Produktfamilie



Eine SOA-Appliance ...



Mehrwert für Kunden durch hohe SOA-Performance und Sicherheit

- Vereinfacht SOA durch spezialisierte Geräte
- Beschleunigt SOA durch hohen XML-Durchsatz
- Absicherung von SOA/XML-Implementierung

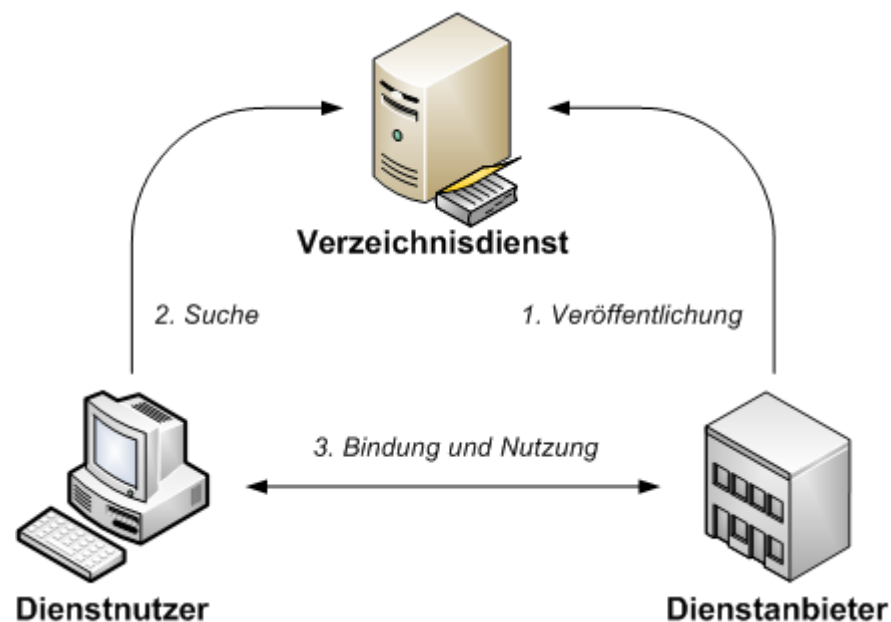
WebSphere DataPower SOA-Appliances definieren die SOA-Landschaft neu, durch **spezialisierte, benutzerorientierte und dedizierte Geräte** und die Kombination aus **verbesselter Performance** und **sehr hoher Sicherheit**.

Serviceorientierung - Recap

- Keine „point-to-point“ Verbindung
- Ein Dienst, der mit Hilfe von XML auf der Basis von Internet-Netzwerkprotokollen erbracht wird.
 - Zusammenfinden
 - Binden
 - Datenaustausch
- Methoden, die über ein Netzwerk auf entfernten Rechnern zur Verfügung stehen.
- Enterprise Service Bus

Architektur - Recap

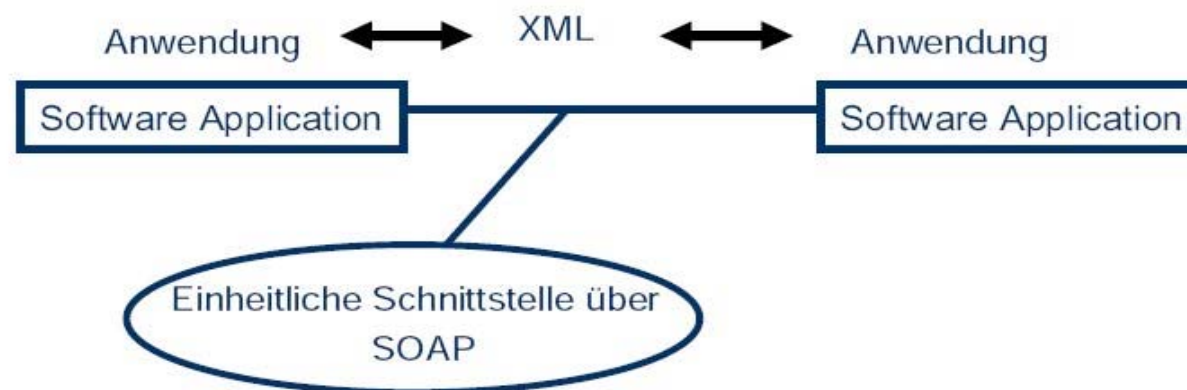
- Web Services im engeren technischen Sinn meint automatisierte Kommunikation zwischen Applikationen übers Intra-/Internet. Es werden also nicht HTML-Seiten zu einem Webbrowser geschickt, die von einem Menschen betrachtet werden, sondern Programme tauschen Daten und starten auf entfernten Rechnern Funktionen



SOAP (Simple Object Access Protocol)
WSDL (Web Services Definition Language)
WSSR (Web Services Registry and Repository)
XML (Extensible Markup Language)

Nachrichten über SOAP

- Die wichtigsten Vorteile von SOAP sind: allgemein akzeptierte Standardisierung, Plattformunabhängigkeit, Offenheit, Robustheit und Skalierbarkeit
- Die gravierendsten Nachteile sind: geringere Performance durch Verwendung von XML und neuartige Sicherheitsaspekte



Nachrichten über SOAP - ESB

Führt folgende Aufgaben aus:

- **ROUTING** messages between services
- **CONVERTING** transport protocols between requestor and service
- **TRANSFORMING** message formats between requestor and service
- **DISTRIBUTING** business events to and from disparate sources



Die Verschlüsselung zwischen Anwendungen ist doch befriedigend gelöst?



Der Enterprise Service Bus als Teil einer SOA hat bestimmte Aufgaben zu erfüllen: Mapping, Routing, Enrichment ... (1/3)



Servicenehmer



Verschlüsselte
Nachricht

Servicegeber

ESB

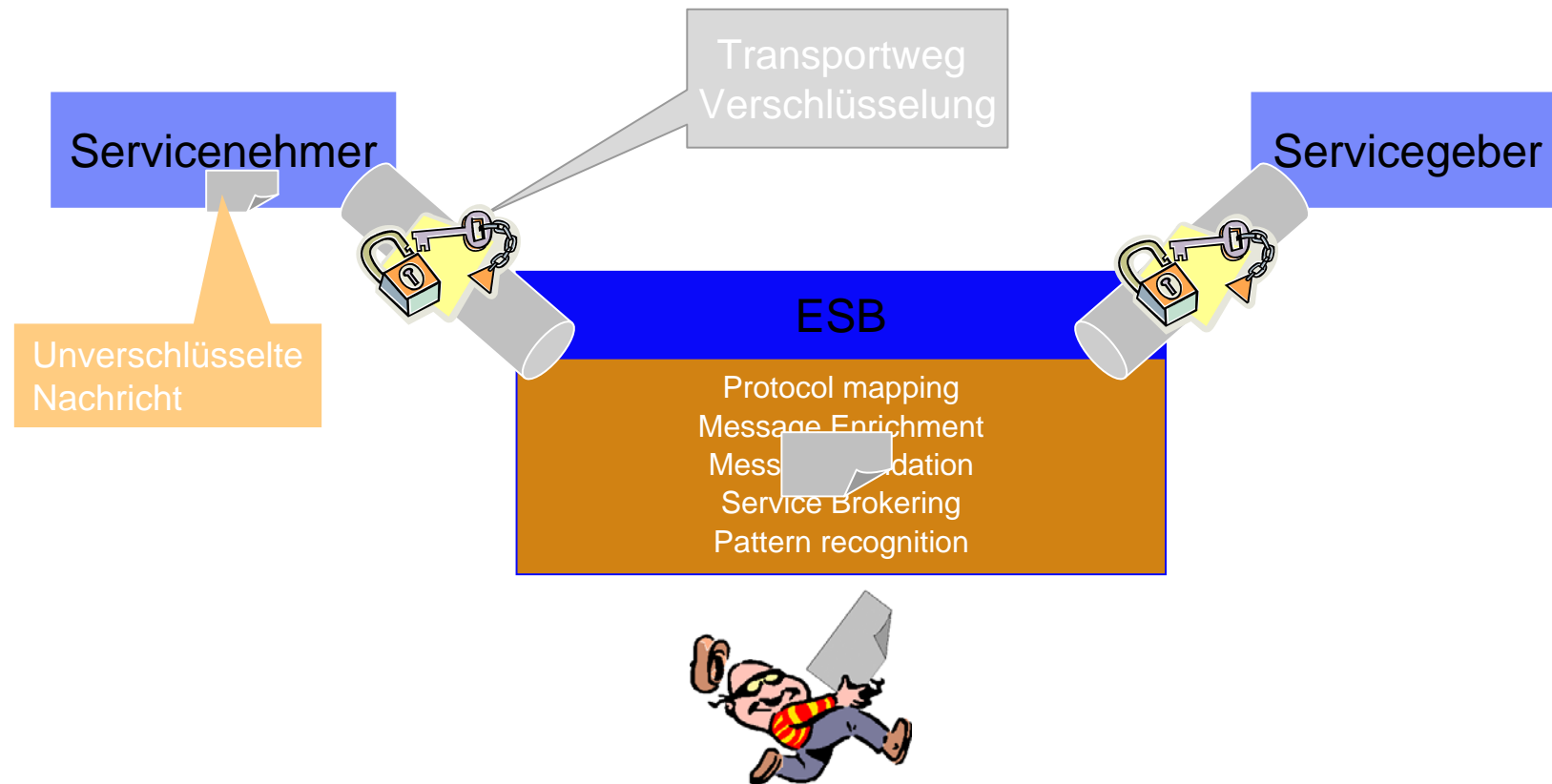


- Protocol mapping
- Message Enrichment
- Message Validation
- Service Brokering
- Pattern recognition



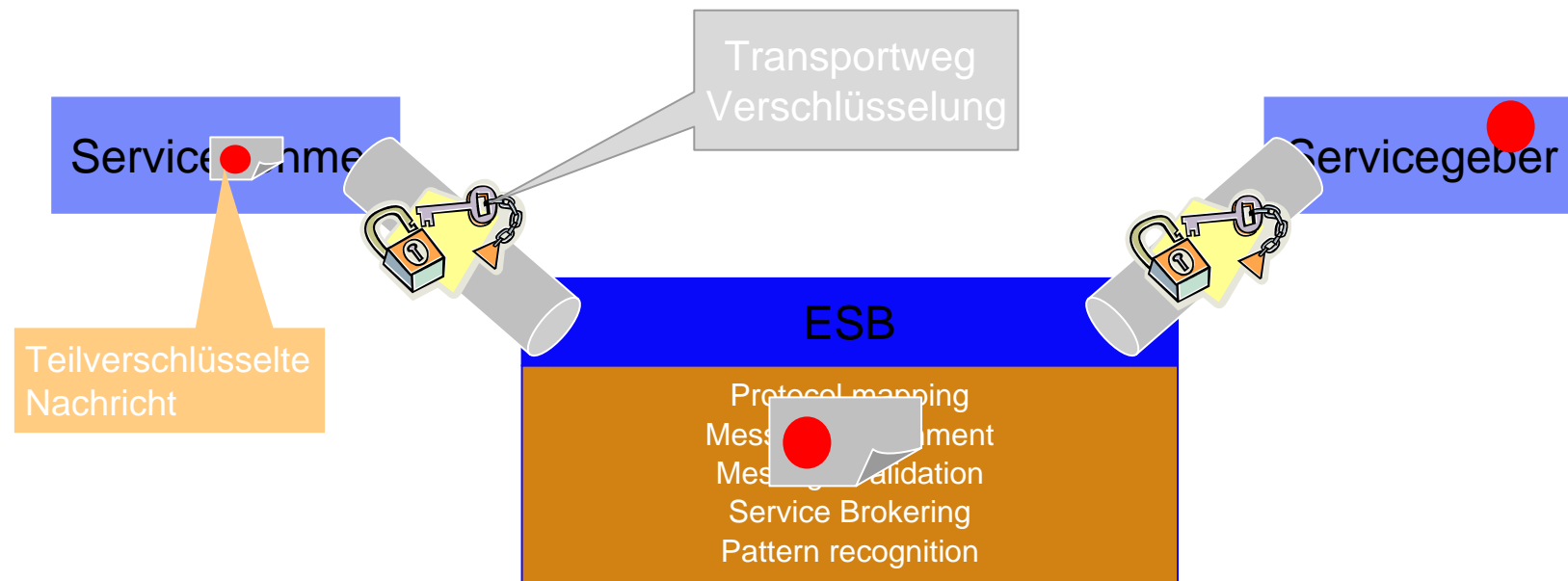
End-to-End verschlüsselte Daten können von einem ESB nicht verarbeitet werden.

Der Enterprise Service Bus als Teil einer SOA hat bestimmte Aufgaben zu erfüllen: Mapping, Routing, Enrichment ... (2/3)



➤ Teilstreckenverschlüsselung ist möglich, aber nicht geheim.

Der Enterprise Service Bus als Teil einer SOA hat bestimmte Aufgaben zu erfüllen: Mapping, Routing, Enrichment... (3/3)



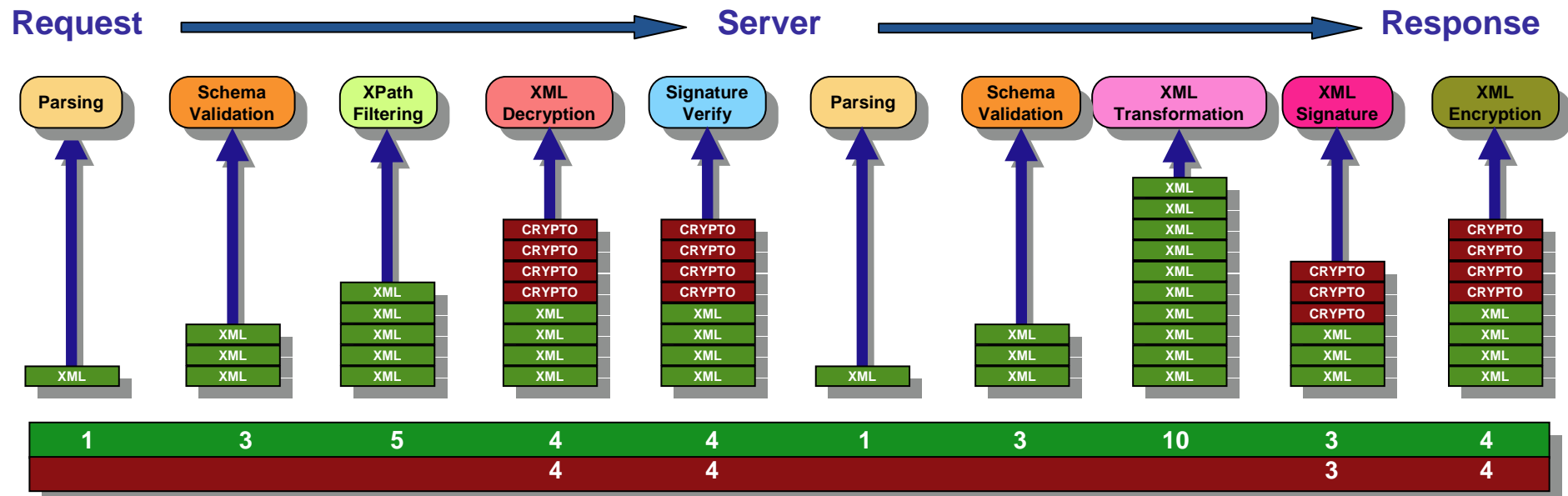
➤ Teilverschlüsselung der Nachricht löst das Vertraulichkeitsproblem.

Neben der Vertraulichkeit existieren jedoch noch weitere Anforderungen an die Sicherheit von Service-Aufrufen.

- **Vertraulichkeit**
Niemand außer Berechtigten erhält Einsicht in die Transaktionsdaten.
- **Berechtigung**
Nur die zum Aufruf eines Services berechtigten Teilnehmer werden für diese zugelassen (Natürliche Personen oder weitere Services).
- **Datenkonsistenz**
Die Konsistenz bzw. Unveränderlichkeit der Transaktionsdaten muss sichergestellt werden.
- **Glaubwürdigkeit**
Der Verfasser der Daten muss zweifelsfrei identifiziert werden können.
- **Verbindlichkeit**
Es muss nachweisbar sein, dass der Verfasser der Ursprung der Transaktionsdaten ist.

SOA ist XML Verarbeitung

Round-trip Security Processing Requirements



- XML Performance ist der “key enabler” für umfassende SOA Sicherheit
 - ▶ XML ist der Schlüssel für formatübergreifende Daten-Validierung auf Nachrichtenebene
 - ▶ Alle Security Funktionen beruhen auf einem signifikanten Anteil von XML Bearbeitung
 - ▶ Schlechte Performance der Sicherungsfunktionen veranlasst Kunden of diese Sicherheitsfunktionen abzuschalten und damit Risiken zu erhöhen
 - ▶ Sicherheit darf nicht einer unzureichenden Leistungsfähigkeit der verarbeitenden System geopfert werden

Gründe für eine SOA-Appliance

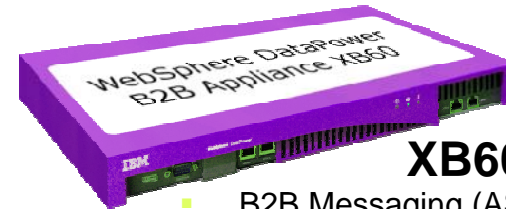
- **Gehärtete, spezialisierte Hardware** für die Integration, Absicherung und Beschleunigung von SOA
- **Viele Funktionen in einem einzelnen Gerät**
- **Strikte Sicherheitszertifizierungen erfordern eine Hardware**
 - Beispiel: FIPS Level 3 HSM, Common Criteria
- **Höhere Leistung durch Hardwarebeschleunigung**
 - Folge: Ausführung von mehr Sicherheitsprüfungen bei besserer Systemleistung
- **Anforderungen von verschiedenen Gruppen werden abgedeckt**
 - z.B.: IT-Architekten, Netzwerkbetrieb, Sicherheit, Identitätsmanagement, Web-Services-Entwickler
- **Vereinfachte Implementierung, vereinfachtes Systemmanagement**
 - Folge: Geringerer Bedarf an SOA-Know-how vor Ort und schnellere Nutzung der SOA-Vorteile

WebSphere DataPower SOA Appliance Product Line



XM70

- High volume, low latency messaging
- Enhanced QoS and performance
- Simplified, configuration-driven approach to LLM
- Publish/subscribe messaging
- High Availability



XB60

- B2B Messaging (AS2/AS3)
- Trading Partner Profile Management
- B2B Transaction Viewer
- Unparalleled performance
- Simplified management and configuration



XA35

- Offload XML processing
- No more hand-optimizing XML
- Lowers development costs



XS40

- Enhanced Security Capabilities
- Centralized Policy Enforcement
- Fine-grained authorization
- Rich authentication

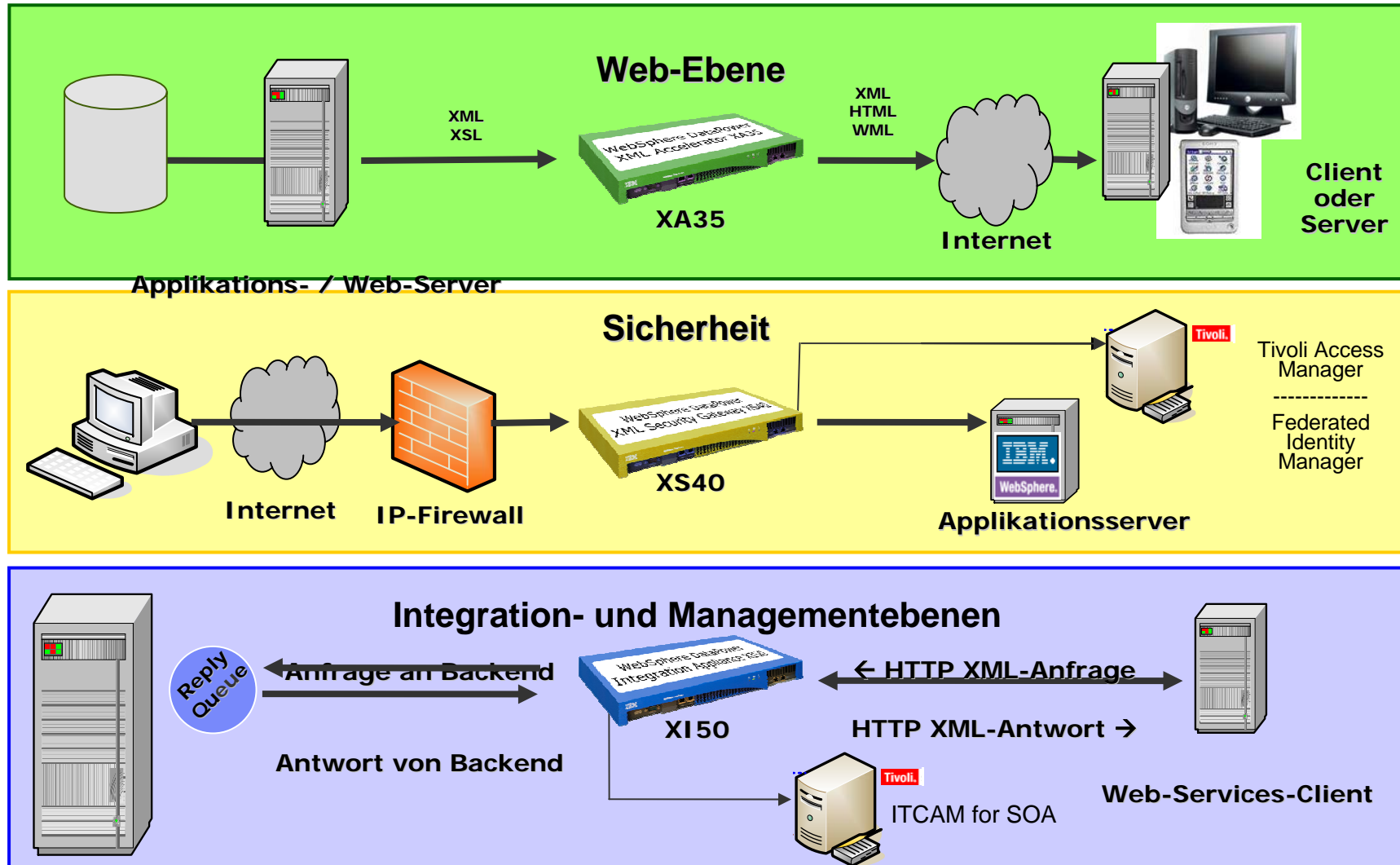


XI50

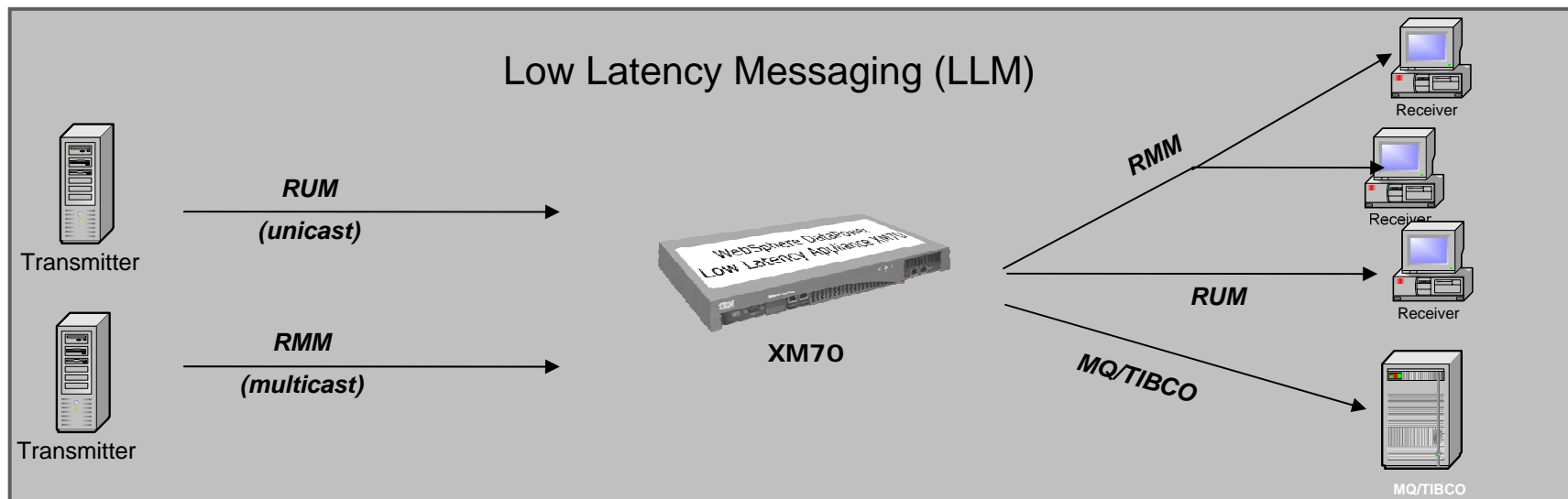
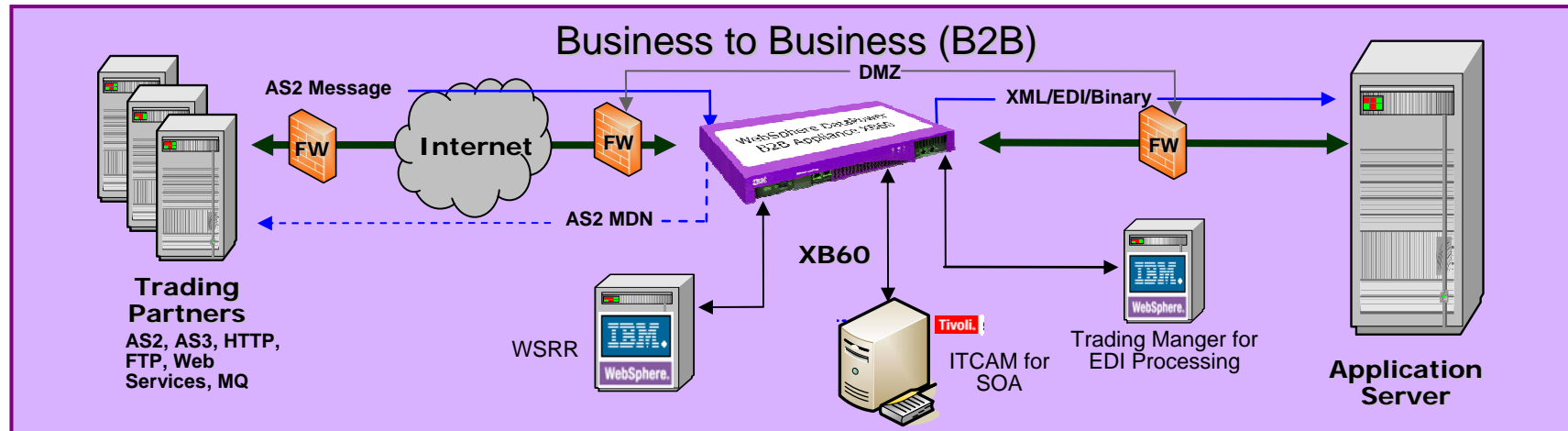
- Hardware ESB
- “Any-to-Any” conversion at wire-speed
- Bridges multiple protocols
- Integrated message-level security



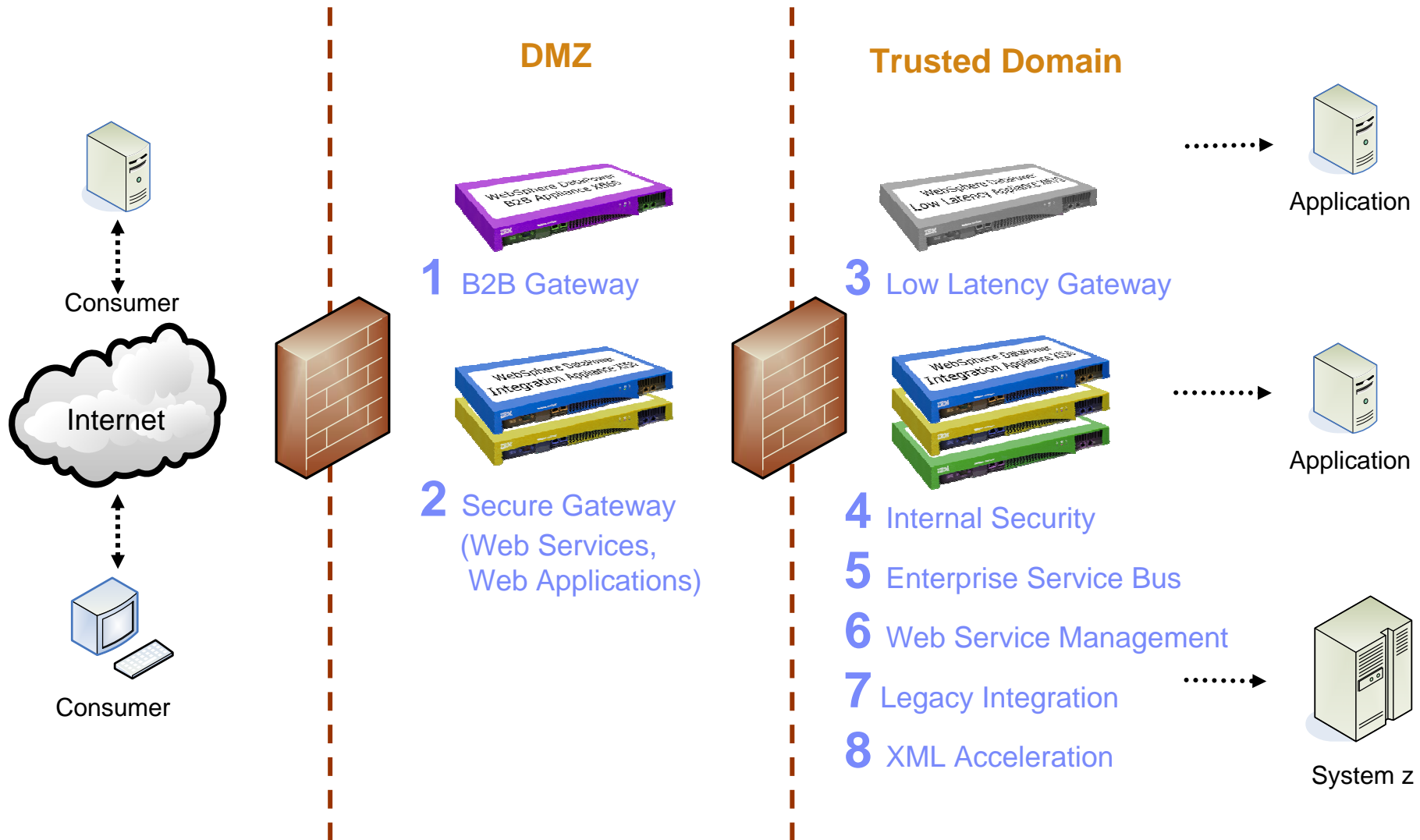
Einsatzmöglichkeiten von IBM SOA-Appliances 1/2



Einsatzmöglichkeiten von IBM SOA-Appliances 2/2



WebSphere DataPower SOA Appliance Basic Use Cases



XML Security Gateway XS40

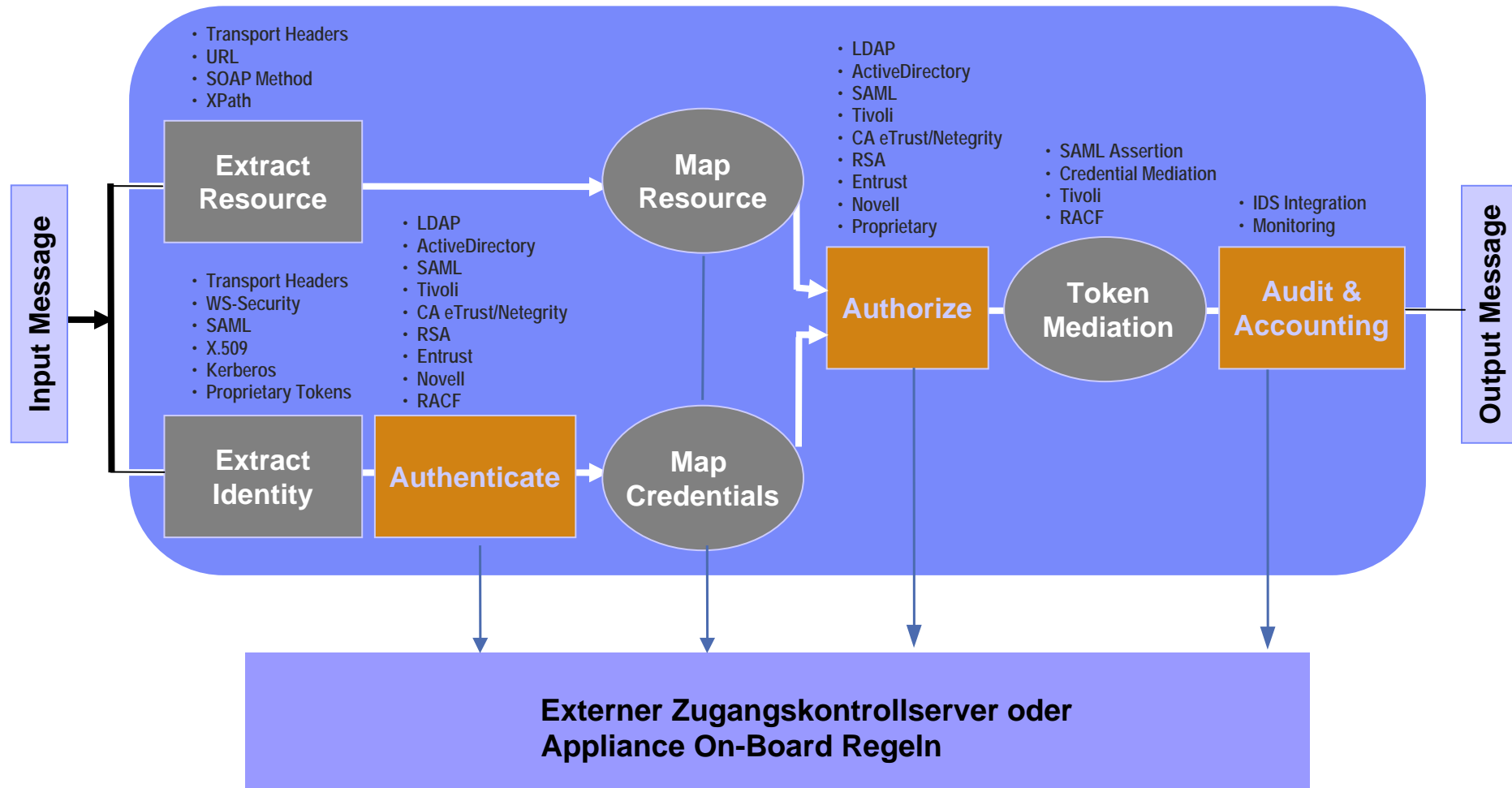


**Benutzerfreundliche Appliance
für mehr SOA-Sicherheit**

- **XML/SOAP-Firewall** - Filter für beliebige Inhalte, Metadaten oder Netzwerkparameter
- **Datenvalidierung** - Prüfung ein- / ausgehender XML und SOAP Dokumente mit "wirespeed"
- **Feldspezifische Sicherheit** - WS-Security, Verschlüsselung und Digitale Signatur für einzelne XML Elemente, Nachweisbarkeit
- **Zugriffssteuerung/AAA für XML-Web-Services** - SAML, LDAP, RADIUS usw.
- **MultiStep** - ausgefeilte mehrphasen Pipeline
- **Web-Services-Management** - Service Level Management, Service Virtualisierung, Richtlinien-Management
- **Flexibilität der Transportschicht** - HTTP, HTTPS, SSL
- **Einfache Konfiguration und Verwaltung** - WebGUI, CLI, IDE und Eclipse Konfigurations-Plug-in, um ein weites Spektrum Organisatorischen Anforderungen abzudecken (Architekten, Entwickler, Netzwerkbetrieb, Sicherheit)

AAA-Framework – Diagramm

Authentifizierung, Authorisierung, Audit



XML Integration Appliance XI50



Middleware-Appliance zur
Anwendungsintegration

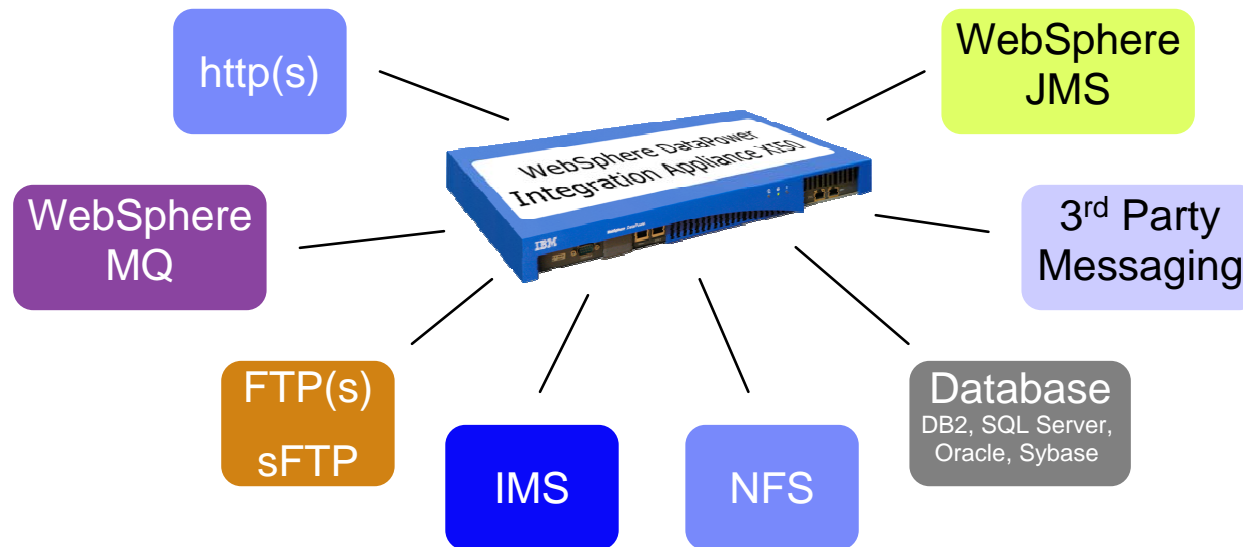
- **„Any-to-Any“-Konvertierungseengine DataGlue**
- **Inhaltsbasiertes Nachrichtenrouting**
- **Protokoll Brücke (HTTP, MQ, JMS, FTP usw.)**
- **XML/SOAP-Firewall** - Filter für beibiege Inhalte, Metadaten oder Netzwerkparameter
- **Datenvalidierung** - Prüfung ein- / ausgehender XML und SOAP Dokumente mit “wirespeed”
- **Feldspezifische Sicherheit** - WS-Security, Verschlüsselung und Digitale Signatur für einzelne XML Elemente, Nachweisbarkeit
- **Zugriffssteuerung/AAA für XML-Web-Services** - SAML, LDAP, RADIUS usw.
- **MultiStep** - ausgefeilte mehrphasen Pipeline
- **Web-Services-Management** - Service Level Management, Service Virtualisierung, Richtlinien-Management
- **Flexibilität der Transportschicht** - HTTP, HTTPS, SSL, MQ, JMS, Tibco EMS
- **Einfache Konfiguration und Verwaltung** – Web-GUI, CLI, IDE und Eclipse Plug-in’s, um ein weites Spektrum Organisatorischen Anforderungen abzudecken (Architekten, Entwickler, Netzwerkbetrieb, Sicherheit)

Protocol Mediation

Independently bridge inbound and outbound protocols

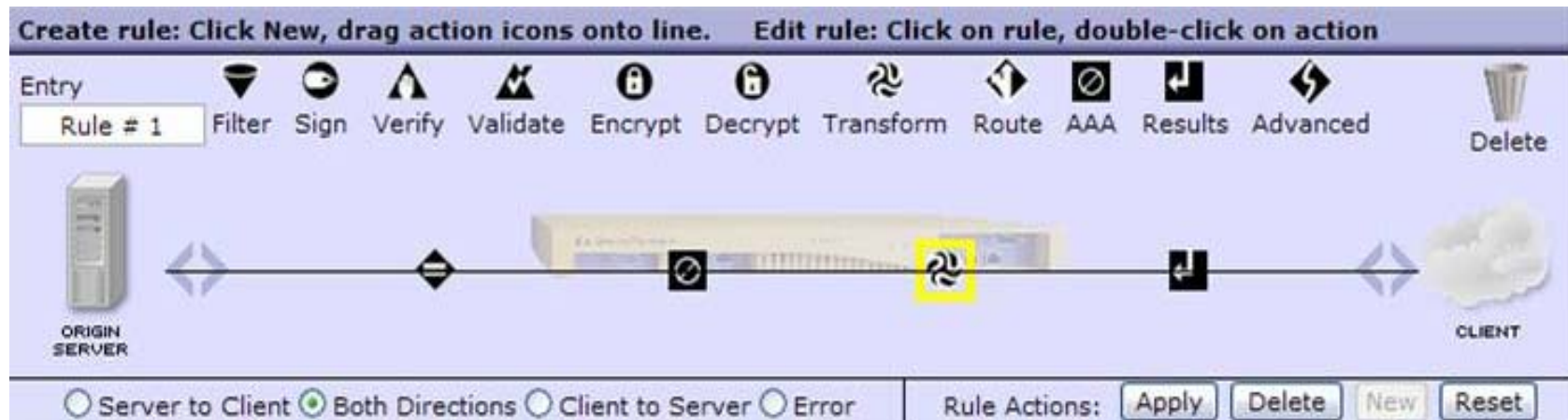


- First-class support for message and transport protocol bridging
- Protocol mediation with simple configuration:
 - HTTP ↔ MQ ↔ WebSphere JMS ↔ FTP ↔ Tibco EMS
- Request-response and sync-async matching
- Configurable for fully guaranteed, once-and-only-once delivery



Mehrfach für Benutzerfreundlichkeit ausgezeichnetes WebGUI:

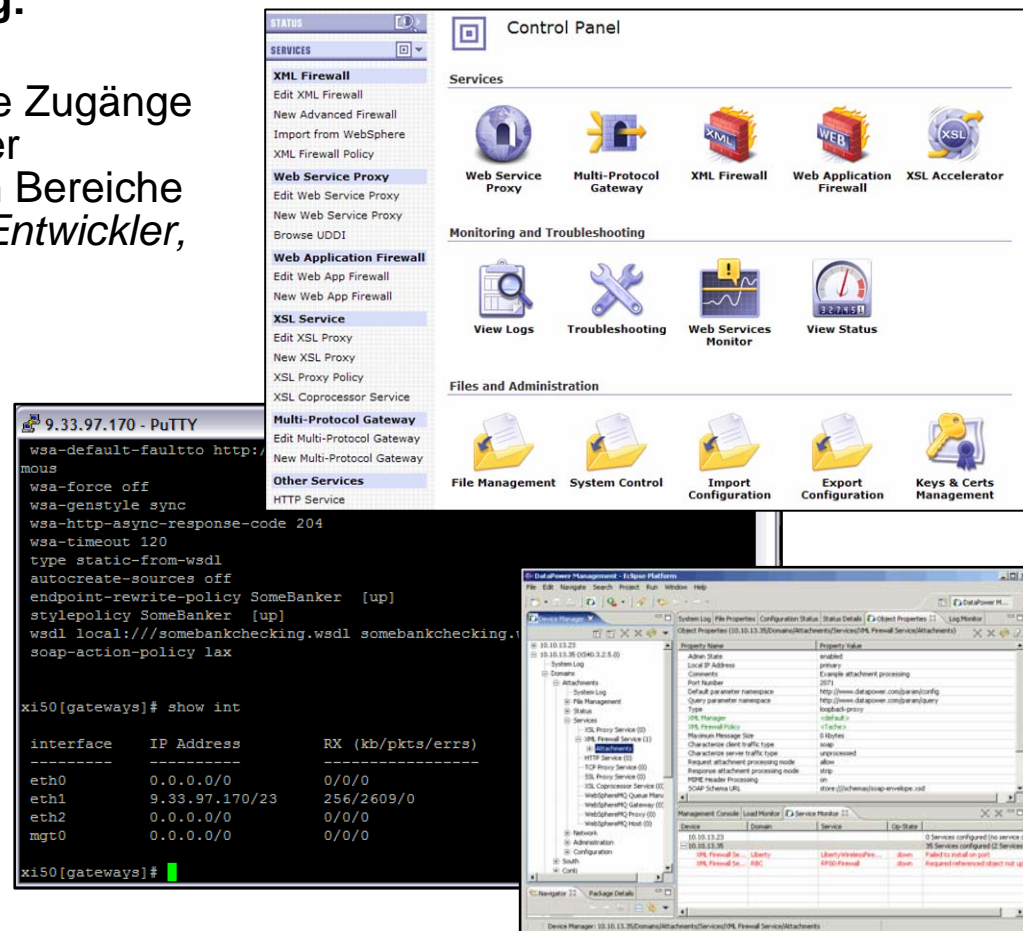
- WSDL-basierte Erstellung von Richtlinien (Policies)
- Hierarchische Service-Levels bei WSDL; Service-, Port-, Operation-Level
- Drag-and-drop Richtlinien Konfiguration ermöglicht einfaches und flexibles Verketteten von benötigten Operationen
- Konfiguration und Installation innerhalb weniger Minuten



Einfache Konfiguration der Appliance für komplexe Funktionalitäten

Passt in alle vorhandenen Umgebung:

- Die Konfiguration über verschiedene Zugänge berücksichtigt die Anforderungen der unterschiedlichen organisatorischen Bereiche eines Unternehmens (*Architekten, Entwickler, Netzwerkbetrieb, Sicherheit*)
- Vollständige Konfiguration über GUI-, CLI-Schnittstelle oder SOMA
- IDE-Integration/Eclipse-Plug-in
- XPath/XML-Konfigurationsdateien
- SNMP
- SOAP-Managementschnittstelle



SOA-Appliance im Betrieb

- **Sehr flexible Protokollierung / Logging**
- **Rollenbasiertes Management**
- **Management von Konfigurationen und Richtlinien (Policies)** – Deployment, Backups, Darstellung von Änderungen bzw. Zurücksetzung auf vorherigen Stand, Anwendungsdomänen ermöglichen viele virtuelle Einheiten
- **Separates, gesichertes Audit-Protokoll**
- **Hilfestellungen bei der Fehlerbehebung**
- **Sicherheit** – Gerätesicherheit, Schlüssel- und Zertifikatsmanagement, HSM-Option, Sicherheitsprüfung, Firmware-Upgrade mit nur einem Image

The running configuration of the device has been modified. To apply the changes to the startup configuration, click the 'save config' button.

Troubleshooting Enabled (The performance of the device may be impacted!)

Active Services

Refresh Status Show All Domains

local IP	local port	type	name
0.0.0.0	5550	XML Management Interface	xml-mgmt
0.0.0.0	9090	Web Management Service	web-mgmt

Create a user account

What kind of user account do you want to create?

Select one of the following:

Developer (configuring services in a domain)

Domain Account Type

Backup User (domain backup)

Guest (read-only in domain)

Or select an existing user group:

User Group (none) + ...

Back Next Cancel

Export Configuration

Create a backup of the entire system

Create a backup of one or more application domains

Export

Export configuration and files from the current domain

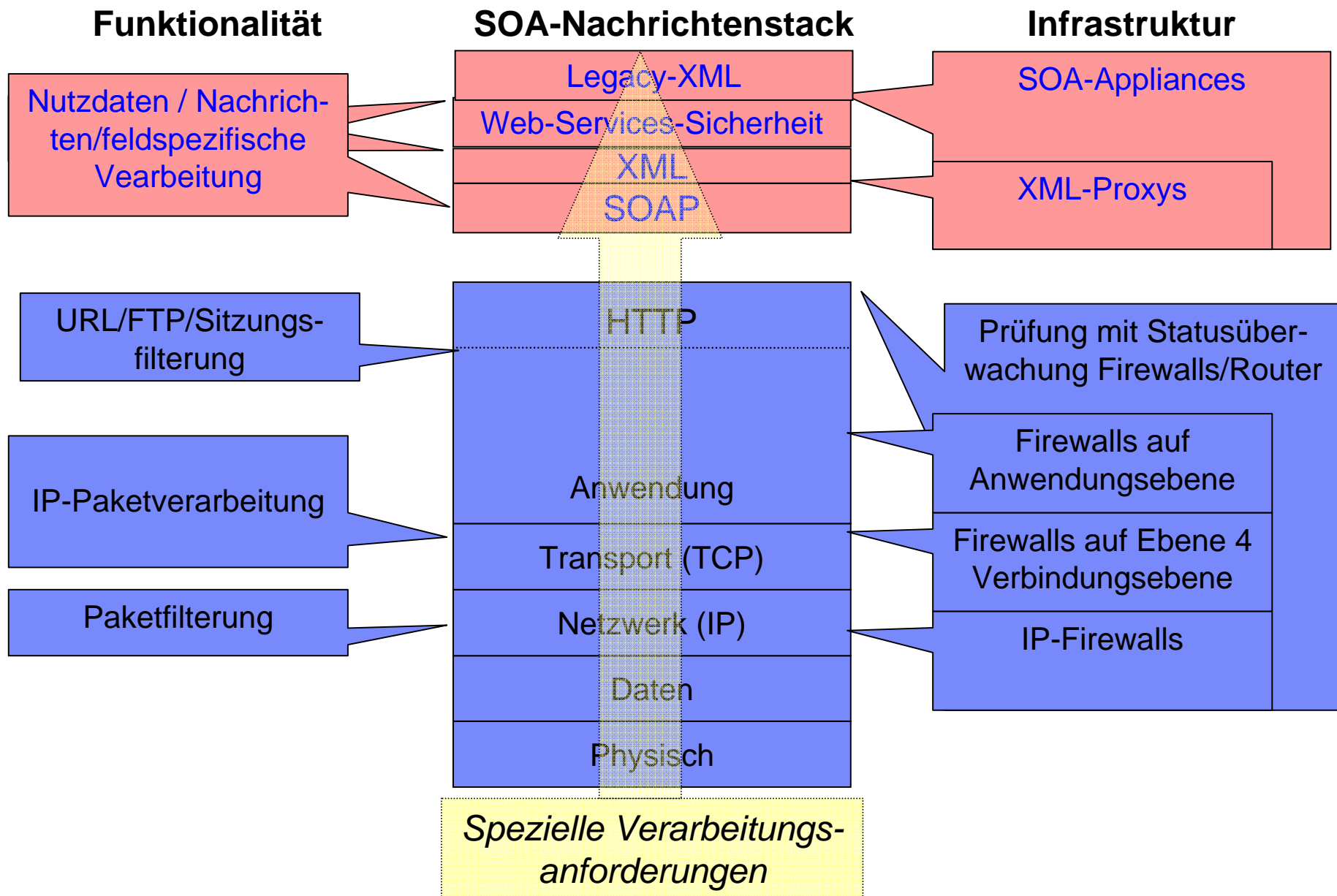
Copy or move configuration and files between domains

Next Cancel

Protocol Headers:

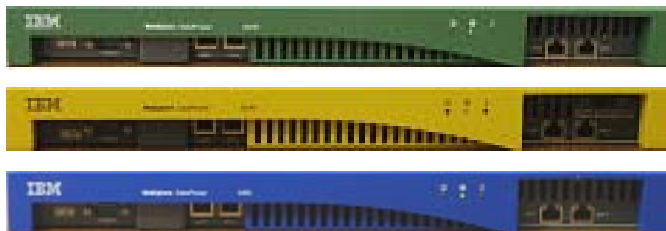
name	value
User-Agent	curl/7.15.0 (586-pc-mingw32msvc) libcurl/7.15.0 OpenSSL/0.9.7e zlib/1.2.2
Host	10.10.13.35:2049
Content-Length	3270
Content-Type	application/x-www-form-urlencoded
Via	1.1 SchemaFilter
Warning	199 Debug mode means sensitive data might be visible
X-Client-IP	10.10.100.229

Zusammenfassung



IBM SOA-Appliances – Zusammenfassung

- Gehärtet, spezialisiert für die Integration, Absicherung und Beschleunigung von SOA
- Viele Funktionen in einem einzelnen Gerät
- Tiefe Integration in IBM Software und Software anderer Anbieter
- Hohe Sicherheitszertifizierungen verlangen zuverlässige Hardware
- Hohe Performance durch Hardwarebeschleunigung
- Einfache Inbetriebnahme, benutzerfreundliches Systemmanagement



Mehrwert für Kunden durch hohe SOA-Performance und Sicherheit

- **Vereinfachung** von SOA durch spezialisierte Geräte
- **Beschleunigung** durch hohen XML-Durchsatz
- **Absicherung** von SOA/XML-Implementierung

Informationen im Internet unter <http://www.ibm.com/software/integration/datapower/>



IBM Software Partner Academy Program

Noch Fragen?

Kontaktieren Sie Thorsten Harth

IBM DataPower Technical Sales
+49 160 9011 8872
thorsten.harth@de.ibm.com