Einsatz von Javaimplementierungen zur XML-Signatur und –Verschlüsselung in einem Projekt der Automobilindustrie

Prof. Mario Jeckle

Fachhochschule Furtwangen
mario@jeckle.de
http://www.jeckle.de

XML Signatur Workshop, Ilmenau, 2003-04-04

Inhaltsübersicht

- **Anwendungsfall**: XML Digitale Signatur und XML Verschlüsselung für Web Services
  - Besonderheiten und Herausforderungen
  - Standards und Umsetzungen
- **Projekthintergrund**: B2B Web Services zur Integration verteilter Engineeringpartner in der Automobilindustrie
  - Softwarearchitektur
  - Heterogenitätsaspekte
- **Lessons Learned**:
  - Standards
  - Verfügbare Implementierungen
  - Interoperabilitätsaspekte

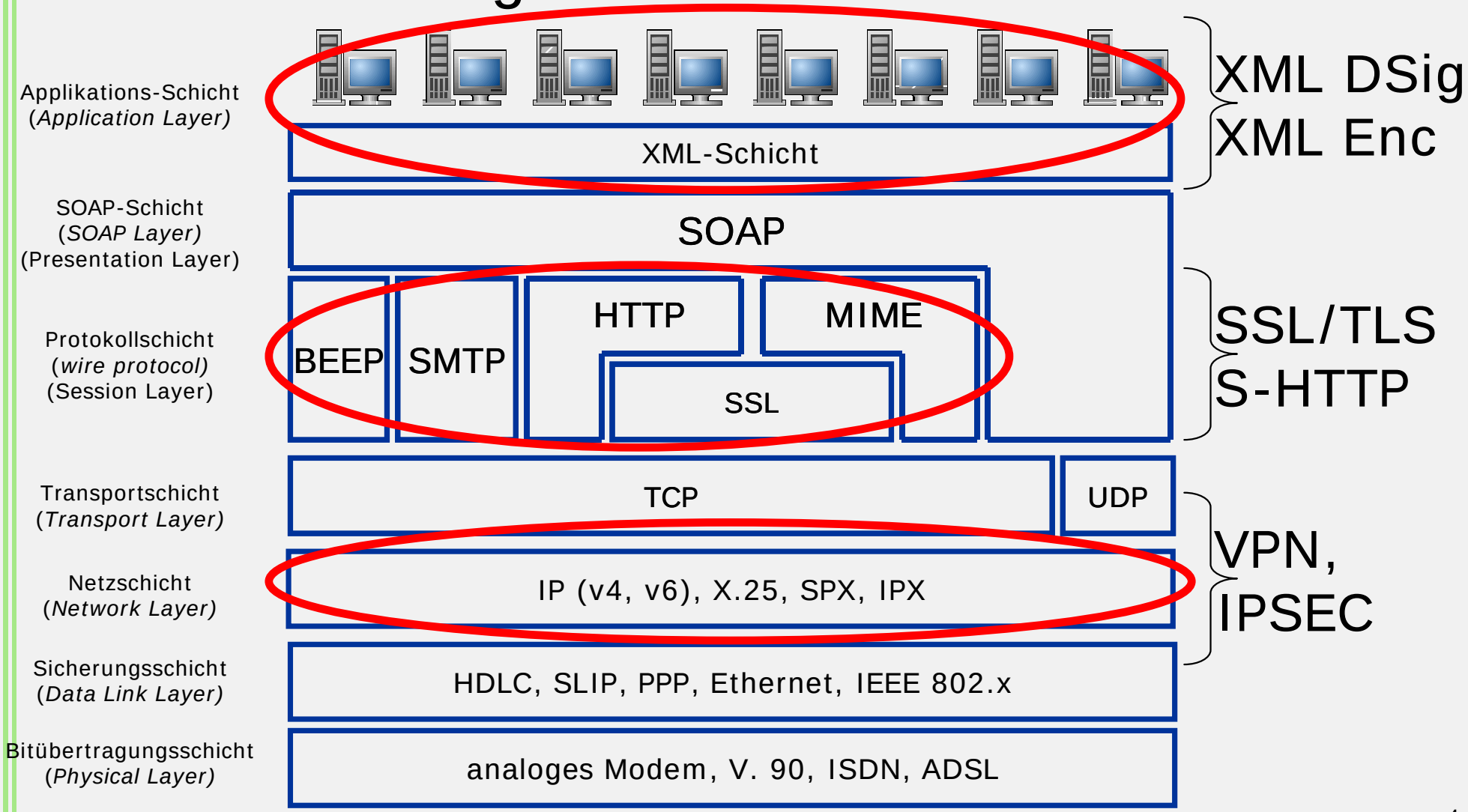
Der Anwendungsfall

XML Digitale Signatur und Verschlüsselung für Web Services

- Ziel:
  - „Sichere“ Kommunikation über unsichere Verbindungen
  - Sicherstellung der Berechtigung
  - … darauf aufbauend: Vertraulichkeit
- Technische Randbedingungen:
  - Einsatz von XML
  - Einsatz von Web Services (SOAP)
  - Kommunikation via HTTP bzw. WLAN

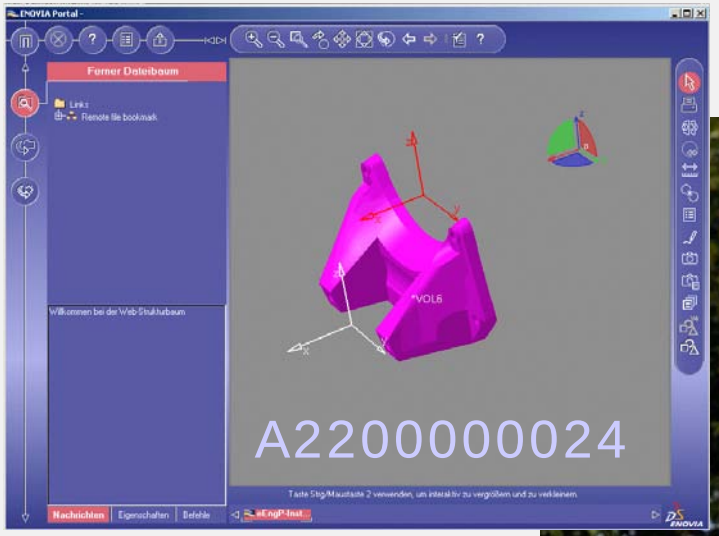
Der Anwendungsfall

XML Digitale Signatur und Verschlüsselung für Web Services



Projekthintergrund

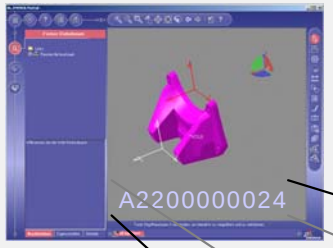
Sicherung von Web Services zum Zugriff auf Entwicklungsinformation



Motorlagerung

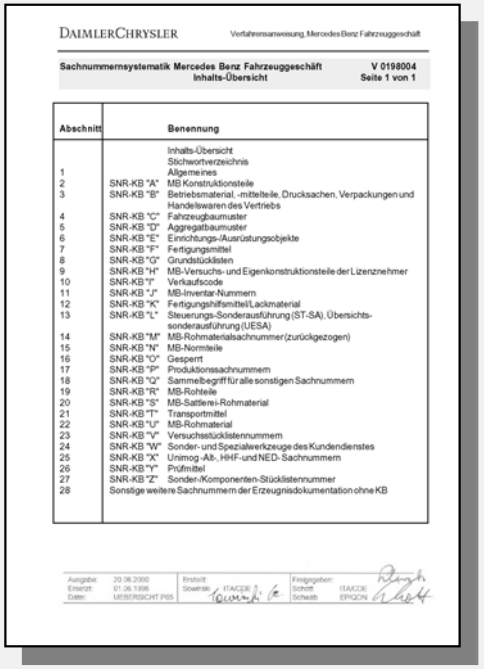
Projekthintergrund

Sicherung von Web Services zum Zugriff auf Entwicklungsinformation



A2200000024

- Hauptgruppe
- Abwandlung
- Konstruktionsuntergruppe
- Kennzeichen für Anordnung
- Typzahl (Baureihe)
- Sachnummernkennbuchstabe (Serienteil)



DAIMLERCHRYSLER Verfahrensanweisung, Mercedes Benz Fahrzeuggeschäft

Sachnummernsystematik Mercedes Benz Fahrzeuggeschäft V 0198004
Inhalts-Übersicht Seite 1 von 1

Abschnitt		Benennung
		Inhalts-Übersicht
		Stichwortverzeichnis
1		Allgemeines
2	SNR-KB "A"	MB Konstruktionsteile
3	SNR-KB "B"	Betriebsmaterial, -mittelteile, Drucksachen, Verpackungen und Handelswaren des Vertriebs
4	SNR-KB "C"	Fahrzeugbaumuster
5	SNR-KB "D"	Aggregatbaumuster
6	SNR-KB "E"	Einrichtungs-/Ausrüstungsobjekte
7	SNR-KB "F"	Fertigungsmittel
8	SNR-KB "G"	Grundstücklisten
9	SNR-KB "H"	MB-Versuchs- und Eigenkonstruktionsteile der Lizenznehmer
10	SNR-KB "I"	Verkaufscode
11	SNR-KB "J"	MB-Inventar-Nummern
12	SNR-KB "K"	Fertigungshilfsmittel/Lackmaterial
13	SNR-KB "L"	Steuerungs-Sonderausführung (ST-SA), Übersichts-sonderausführung (UESA)
14	SNR-KB "M"	MB-Rohmaterialsachnummer (zurückgezogen)
15	SNR-KB "N"	MB-Normteile
16	SNR-KB "O"	Gesperrt
17	SNR-KB "P"	Produktionssachnummern
18	SNR-KB "Q"	Sammelbegriff für alle sonstigen Sachnummern
19	SNR-KB "R"	MB-Rohteile
20	SNR-KB "S"	MB-Sattlerei-Rohmaterial
21	SNR-KB "T"	Transportmittel
22	SNR-KB "U"	MB-Rohmaterial
23	SNR-KB "V"	Versuchsstücklistennummern
24	SNR-KB "W"	Sonder- und Spezialwerkzeuge des Kundendienstes
25	SNR-KB "X"	Unimog -Alt-, HHF- und NED-Sachnummern
26	SNR-KB "Y"	Prüfmittel
27	SNR-KB "Z"	Sonder-/Komponenten-Stücklistennummer
28		Sonstige weitere Sachnummern der Erzeugnisdokumentation ohne KB

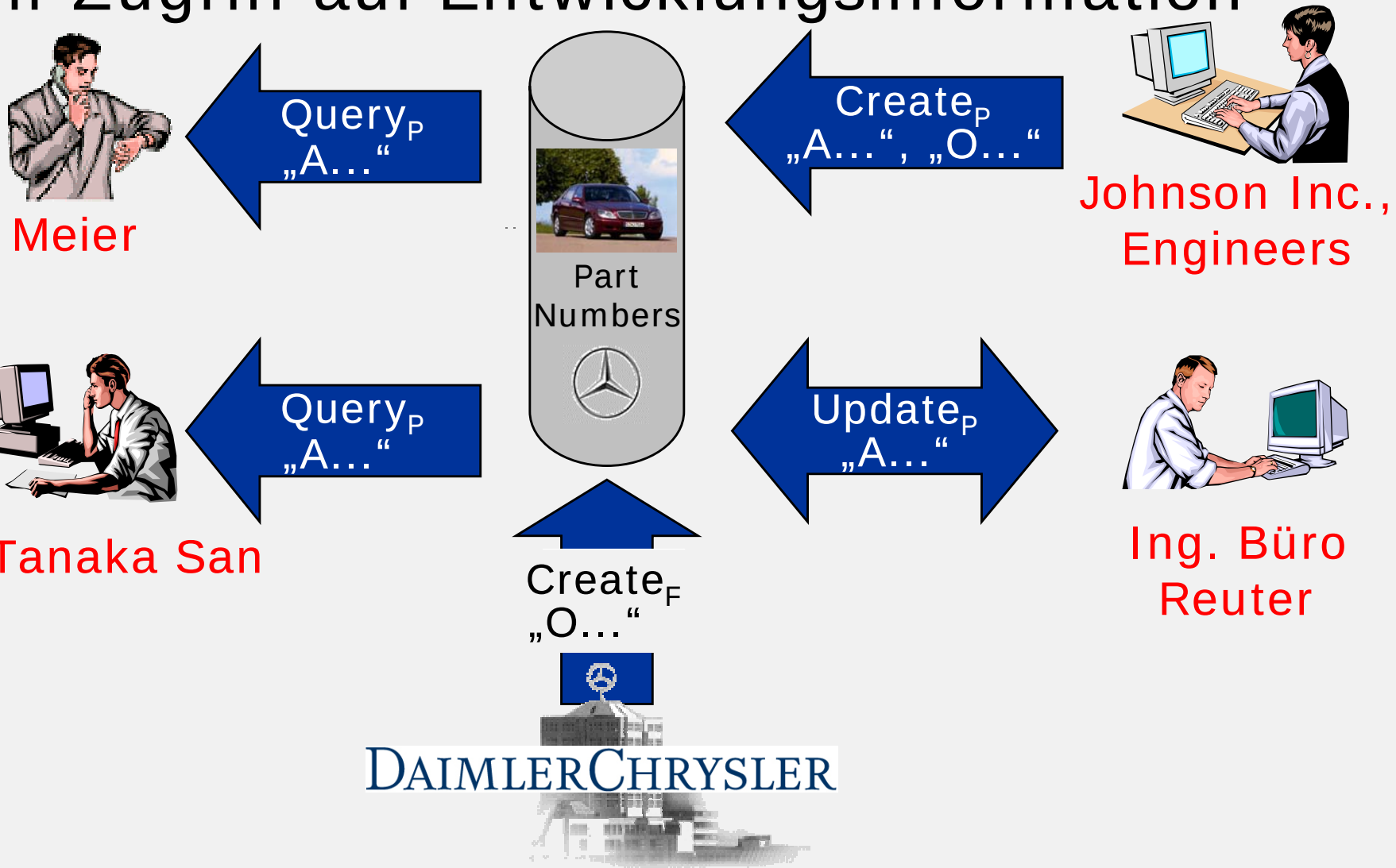
Projekthintergrund

Zugriff auf Sachnummerninformation

- Relevanz des Anwendungsfalles:
  Sachnummern(-information) durchzieht alle Prozesse.
- Sicherheitsrelevanz:
  Anfrage auf „sprechende“ Sachnummern stellt implizit eine Anfragesprache für produktive und (noch) nichtproduktive Teile dar.
- Benutzerkreis:
  Geschlossene Benutzergruppe gebildet durch Entwicklungspartnern und DaimlerChrysler.
- Technik:
  Standardbasiertheit notwendig.

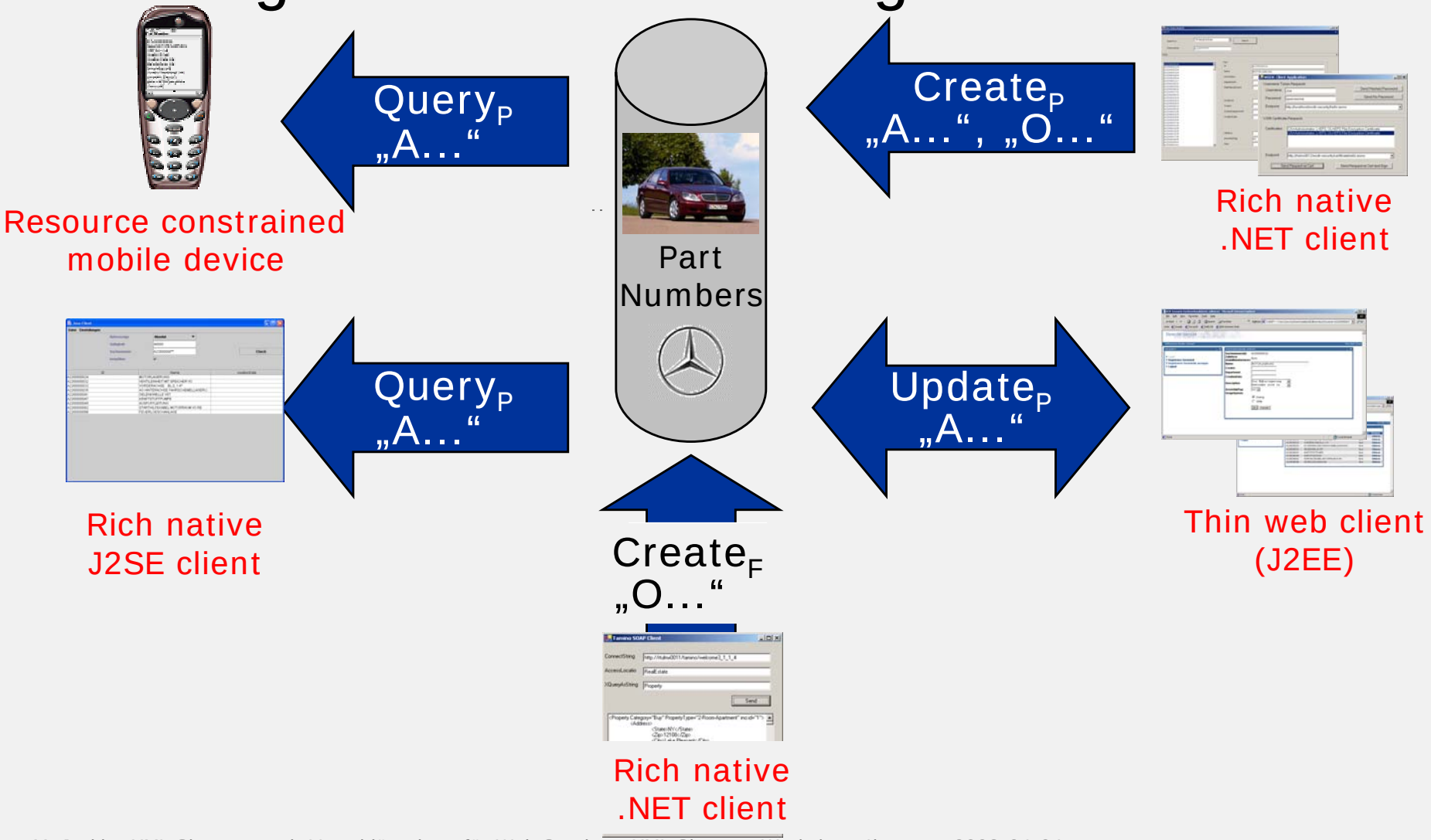
Projekthintergrund

Sicherung von Web Services zum Zugriff auf Entwicklungsinformation



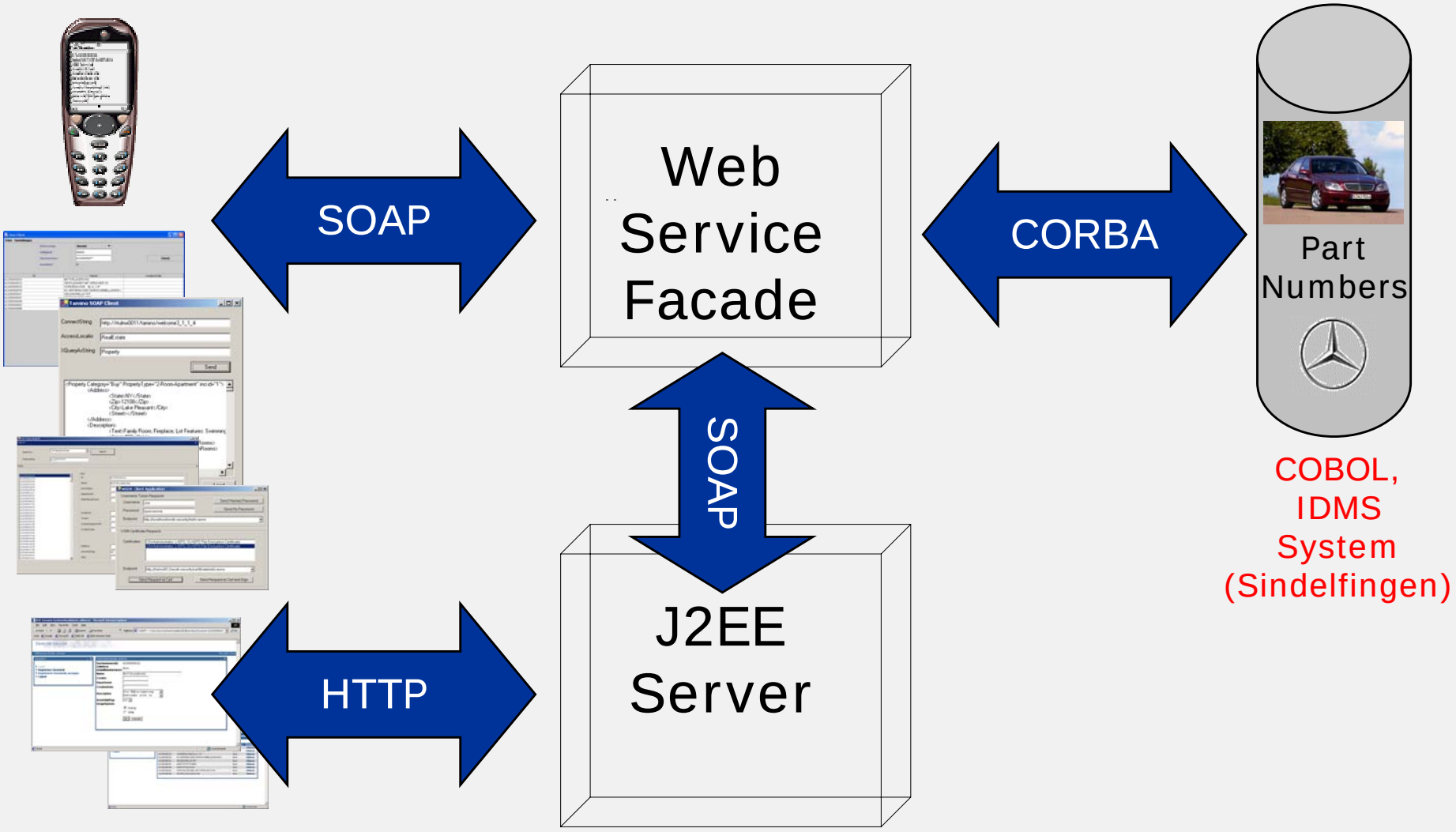
Projekthintergrund

Sicherung von Web Services zum Zugriff auf Entwicklungsinformation



Projekthintergrund

Sicherung von Web Services zum Zugriff auf Entwicklungsinformation



Projekthintergrund

Angestrebte Ziele

- Authentisierung und Autorisierung aller Anfragen auf Basis digitaler Signaturen.
- Verschlüsselung der Antworten.

- Plattformunabhängigkeit.
- Zukunftsfähigkeit (hinsichtlich Skalier- und Adaptierbarkeit)
- Standard-basiertheit.
- Integration in bestehende Systemlandschaft.

- Anwendung:
  - Zunächst: B2B-Umfeld
  - Später: B2C-Umfeld

Projekthintergrund

Eingesetzte Technik

- J2SE: SUN JDK v1.4+
- J2EE: SUN JDK v1.3
- J2ME: SUN JDK v1.4
- kXML, kSOAP
- .NET: Visual Studio .NET Release incl. SP 2
- Apache Web Server 1.3.x
- Jakarta Tomcat Servlet Engine 4.0.3
- AXIS beta3+
- IBMs XML Security Suite 2002-04-22
- SSL: openssl/mod_ssl
- W3C Note: *SOAP Security Extensions: Digital Signature*
- Kommunikation: HTTP, IEEE802.11b, (CORBA)
- Signatur: http://www.w3.org/2000/09/xmldsig#dsa-sha1
- Verschlüsselung: urn:rsadsi-com:rsa-1.5

Projekthintergrund

Eingesetzte Technik

- SOAP
  - RPC-style Kommunikation über HTTP (d.h. synchrones Request-Response-Schema)
  - Keine aktiven Inhalte (Java Script o.ä.)
  - Nachrichtenformate durch XML-Schema und WSDL beschrieben
  - Kein direkter Systemzugriff (Interpretation durch Web Service Endpunkt)

Projekthintergrund

Eingesetzte Standards

- *XML Signature Syntax and Processing* (W3C Recommendation)
- *XML Encryption Syntax and Processing* (W3C Recommendation)
- Anfänglich: *SOAP Security Extensions: Digital Signature* (W3C Note)
- Später: *Web Service Security* (OASIS)

- SOAP v1.1, 1.2 WDs
- XML v1.0. 2nd ed.
- WSDL v1.1
- XML-Schema v1.0

Lessons Learned

- WEP (IEEE 802.11b) kaum ausreichend
- SOAP-Toolkit unterstütz(t)en XML-Signaturen nicht (vollständig)
- Transportsicherung (SSL/TLS) kaum sinnvoll
- XSS4J kaum praktisch einsetzbar
- API-Instabilität in .NET
- Interoperabilitätsprobleme Java -- .NET
- Anwenderakzeptanz und -toleranz
- Standards nutzen – Standards setzen

Lessons Learned

SOAP Toolkits

- Manuelle Codemodifikationen notwendig zur korrekten Unterstützung von XML DSig. (Serialisierungsproblem für XML-Attribute eines Wurzelelements).
- Race condition in AXIS Client Bibliothek. (Exceptions auf Mehrprozessormaschinen).
- Unterschiedliche Interpretationen der gegenwärtig verfügbaren SOAP-Spezifikation.

Lessons Learned

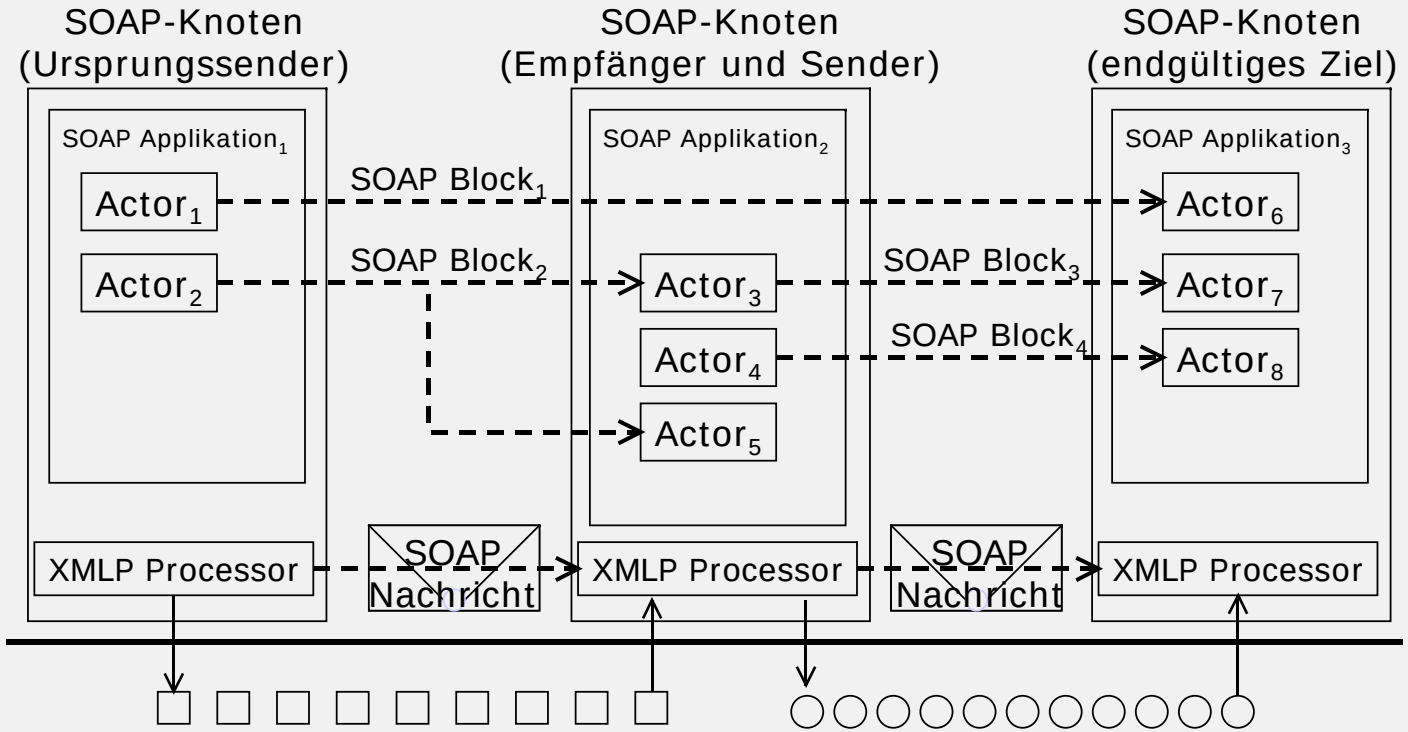
Transportsicherung (SSL/TLS) kaum sinnvoll

- Client-seitige Ablage der empfangenen Zertifikate im Unternehmensumfeld kaum effizient und sicher handhabbar.
  - Wer akzeptiert Zertifikate?
  - Auf wen wirkt sich diese Akzeptanz aus?
  - SSL ist inhärent für längerfristige Kommunikations-beziehungen konzipiert

Lessons Learned

Transportsicherung (SSL/TLS) kaum sinnvoll

- SSL/TLS für Ende-zu-Ende-Sicherung nicht einsetzbar, wenn aktive SOAP-Zwischenknoten (*SOAP Intermediäre)* benutzt werden sollen.



Lessons Learned

XSS4J kaum praktisch einsetzbar

- (Massive) Geschwindigkeitsprobleme.
- (damals) keine Alternativen.
- Keine Umsetzung für J2ME.
- IBM favorisiert inzwischen *Web Service Toolkit* als Nachfolgelösung.

Lessons Learned

.NET-Erfahrungen

- Bestehende API instabil und durch Service Pack geändert.
- Anfänglich keine Interoperabilität mit Java erzielbar.

Lessons Learned

Anwenderakzeptanz und -toleranz

- Sicherheit wird gefordert und ihr Vorhandensein generell begrüßt.
- Realisierte Lösung erfordert Identifikation durch tastaturbasierte Paßworteingabe.
- Manuelle Authentisierung und Autorisierung jedes entfernten Funktionsaufrufs nicht praktikabel.
- Sinnvollerweise Kopplung an Systemlogin (*single-sign-on*).

Lessons Learned

Standards nutzen – Standards setzen

- Standard-basiertheit unbedingt sinnvoll.
- Plattformübergreifende Standards ermöglichen Einsatz der Technik überhaupt erst.
- Implementierungen noch in Kinderschuhen und daher mit Kinderkrankheiten behaftet.
- Konkrete Einsatzkonfiguration des Standards nicht standardisiert ausdrückbar.
  => Erschwert Kontrahtierung signifikant.
  XML DSig Profile könnte Lösung sein.

XML DSig Profile

- Inhalt:
  - Genutze Algorithmen per QName.
  - Verwendete Transformationen.
  - ...
- Anwendung:
  - Sinnvollerweise Ablage in UDDI, gemeinsam mit WSDL-formulierter Schnittstellenbeschreibung des Dienstes.
  - Ermöglicht gesicherten Erstkontakt.

W3C's Web Service Architecture Stack Diagram