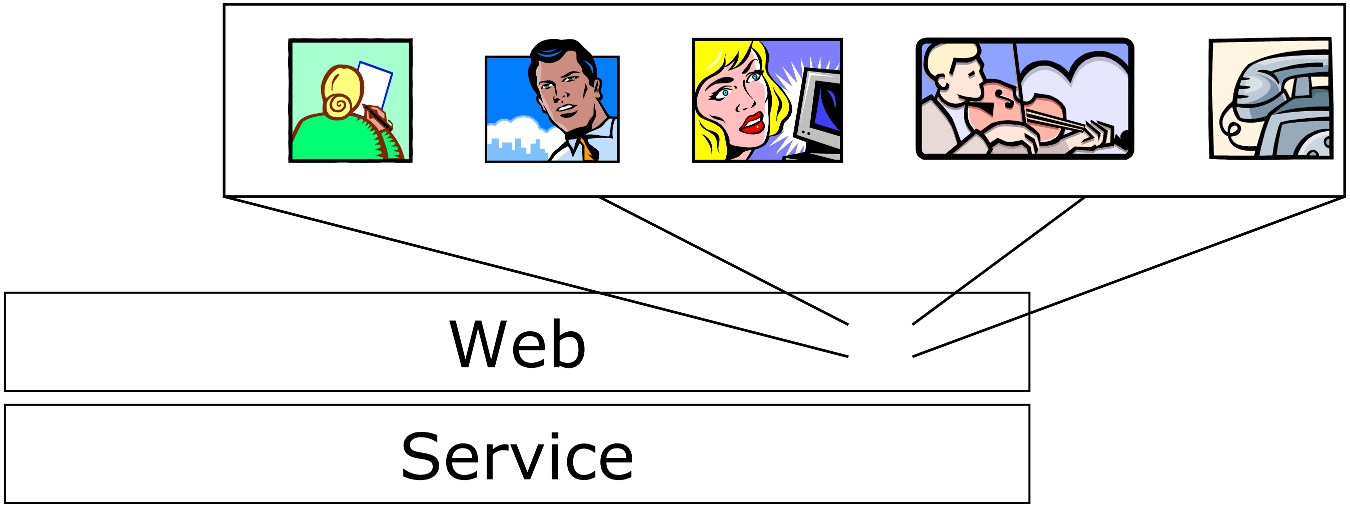
DaimlerChrysler

A Signing Proxy for Web Services Security

Dr. Ingo Melzer
RIC/ED

What is a Web Service?

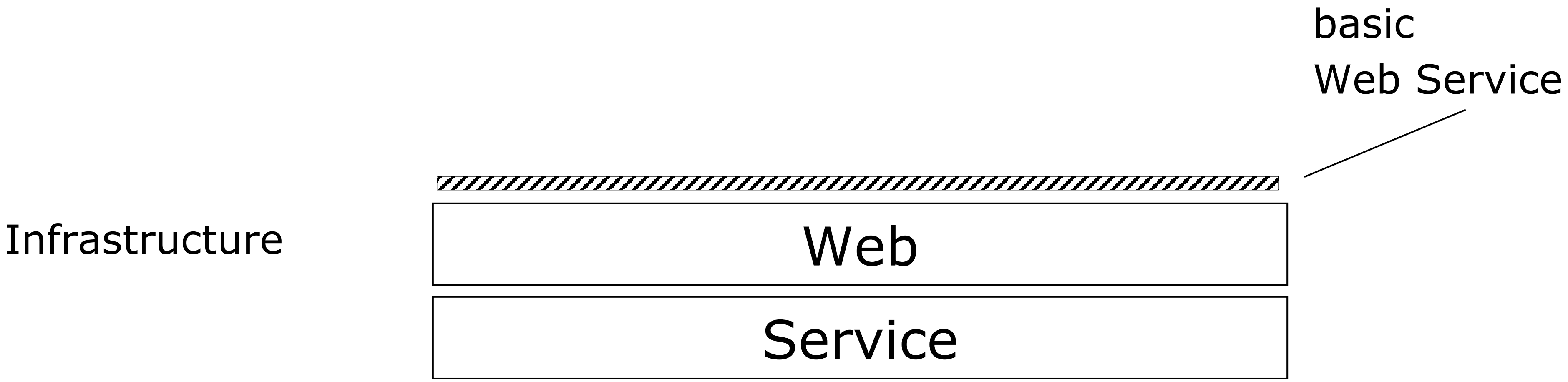
Infrastructure



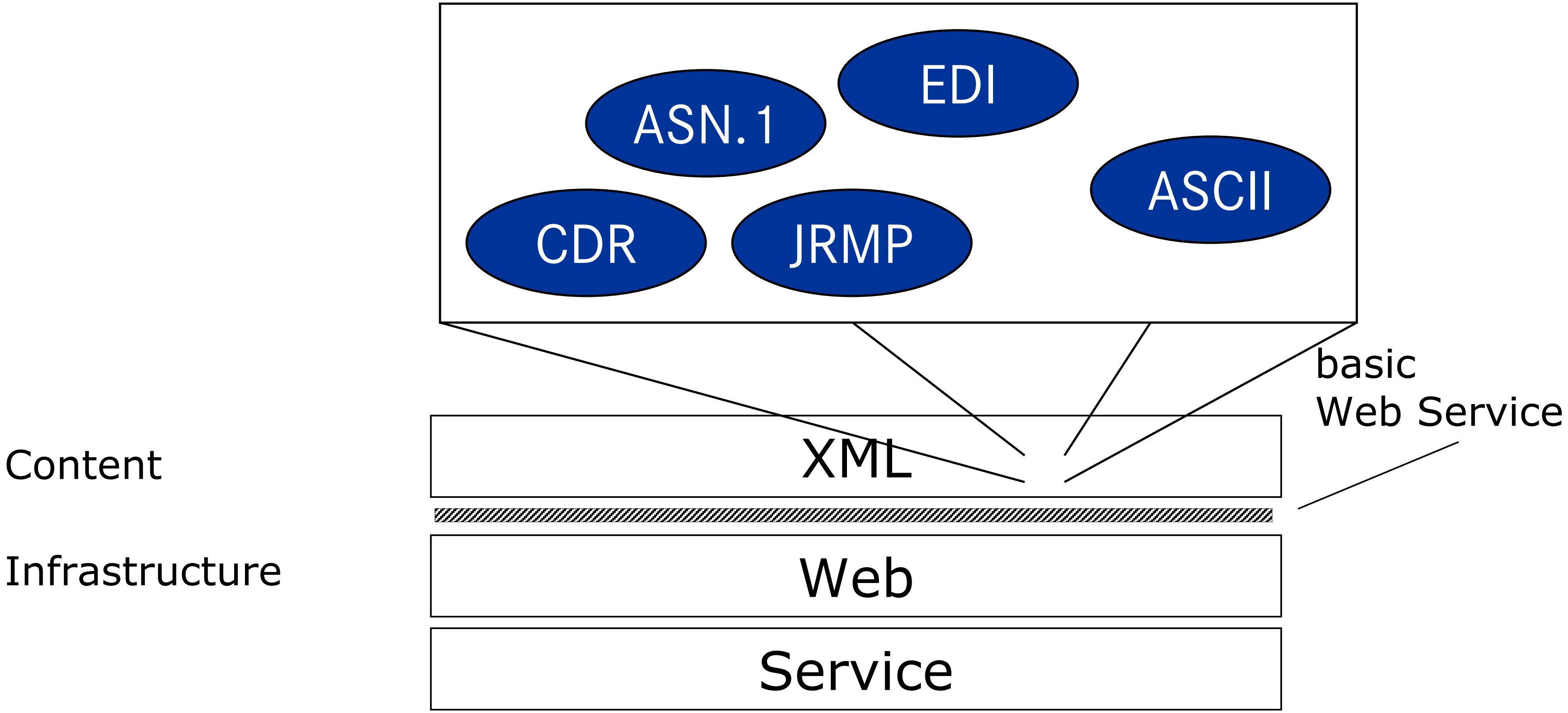
Web

Service

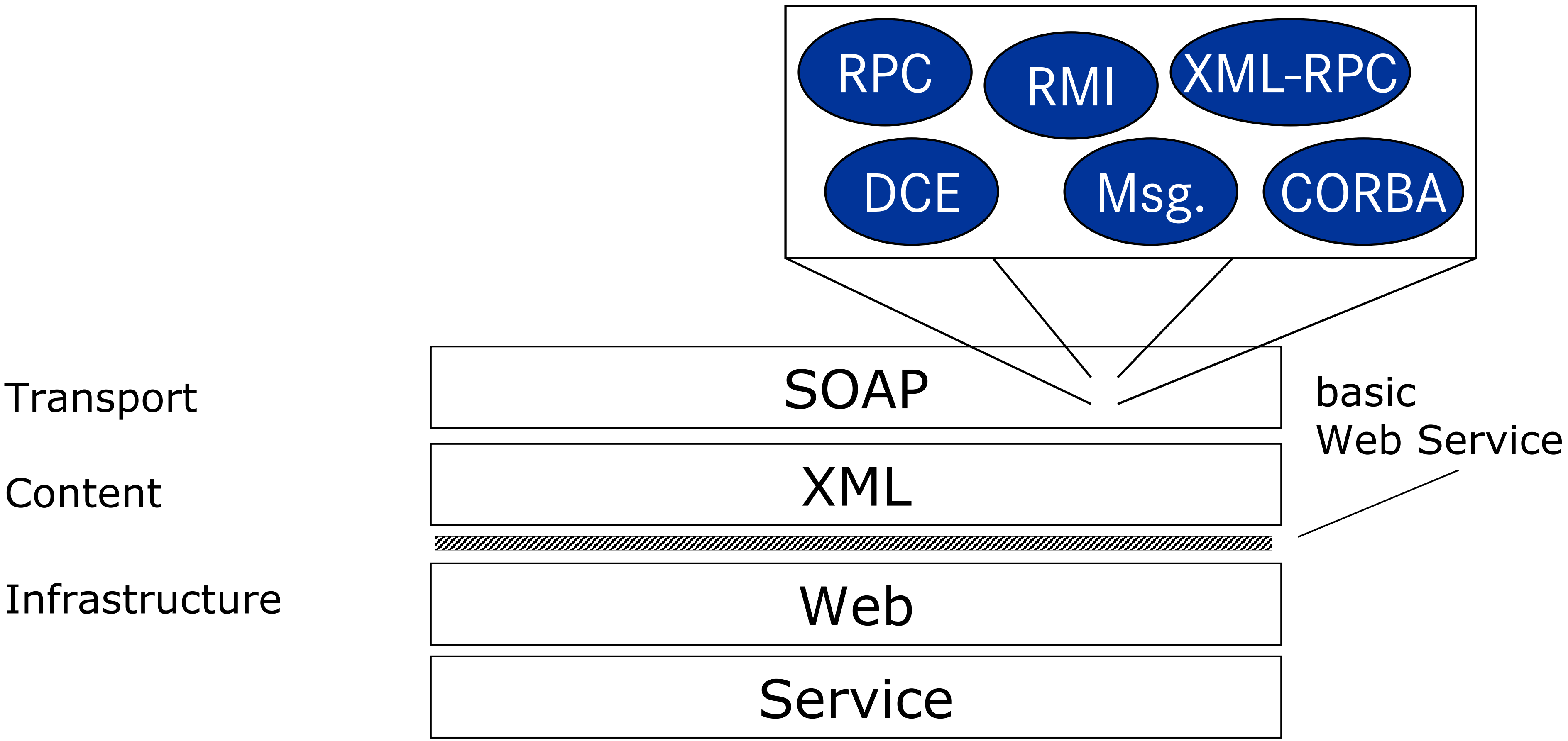
What is a Web Service?



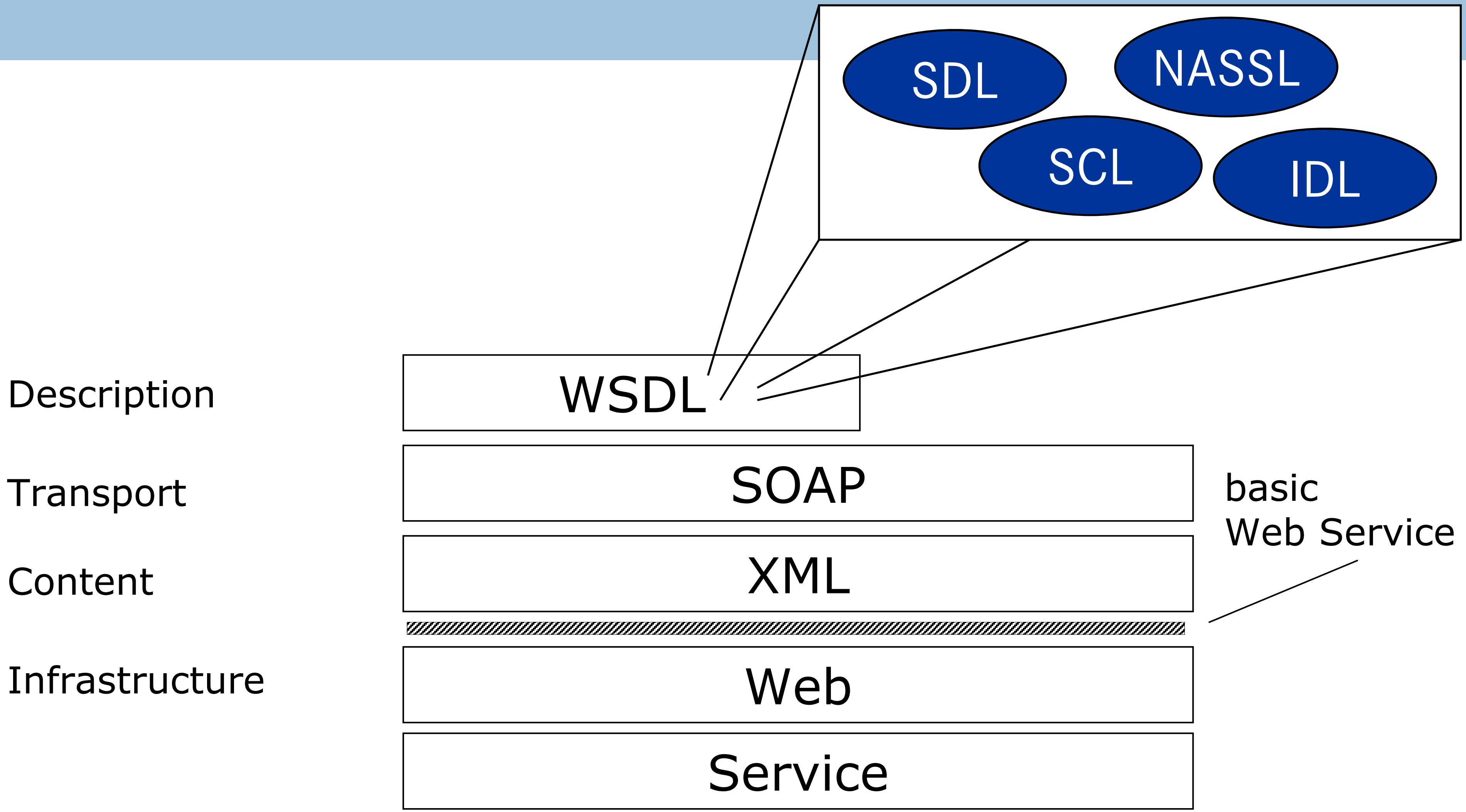
What is a Web Service?



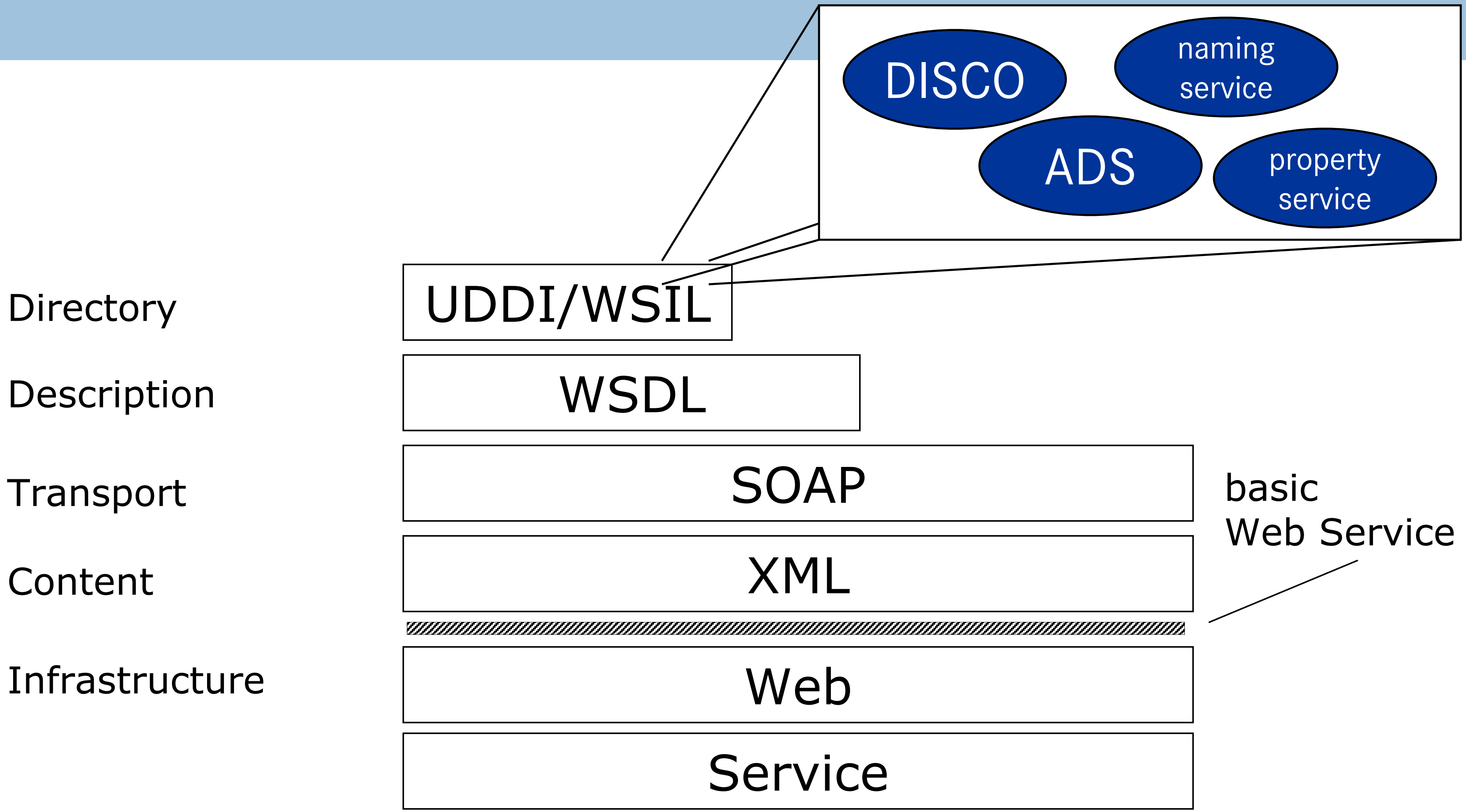
What is a Web Service?



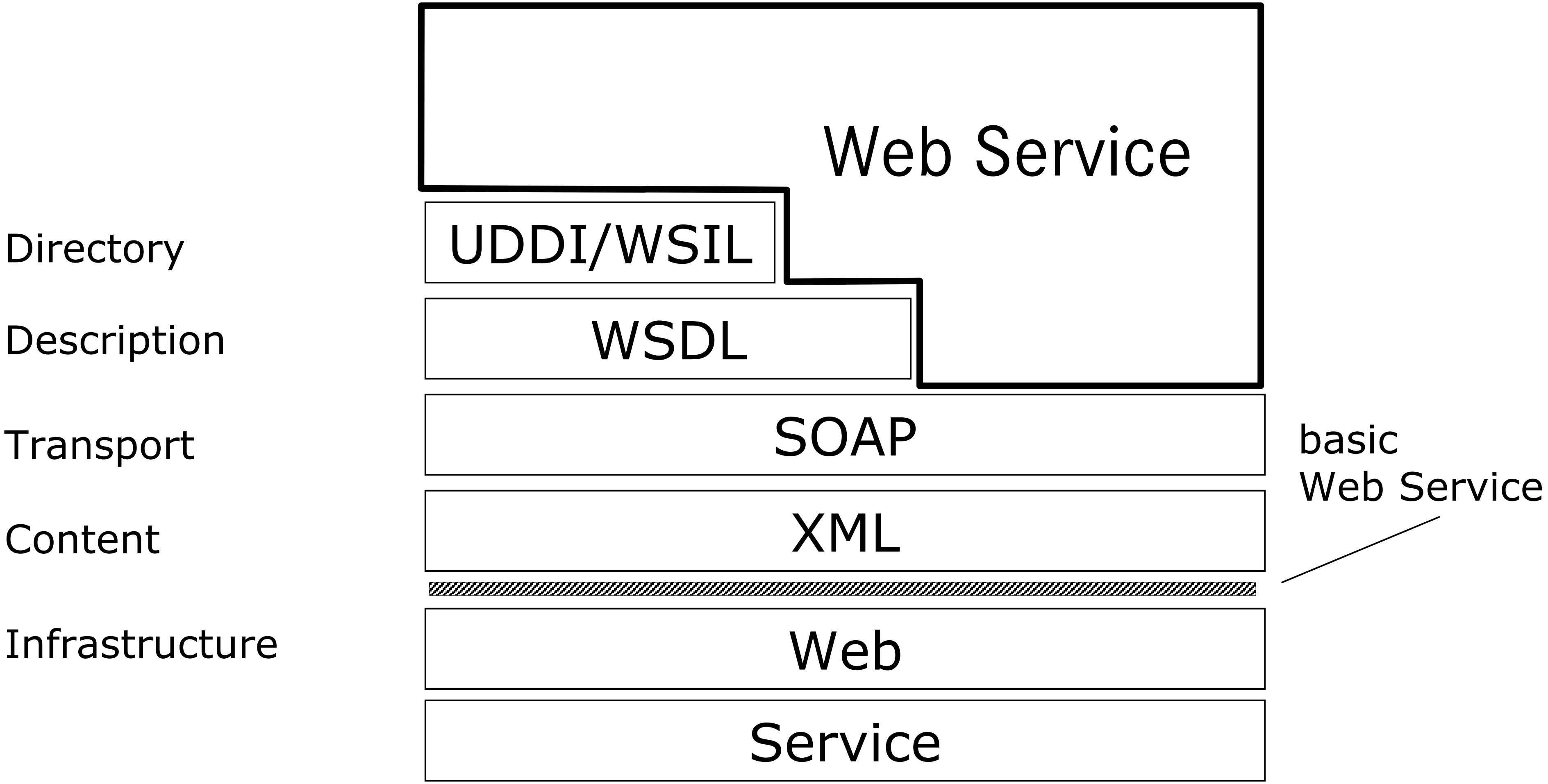
What is a Web Service?



What is a Web Service?



What is a Web Service?



Web Service

Directory — UDDI/WSIL

Description — WSDL

Transport — SOAP

Content — XML

basic Web Service

Infrastructure — Web Service

Properties of Web Services

- Web Services allow collaboration of different systems
- Integration of existing systems
- Facade for set of similar systems
- Web Services offer two styles: RPC and messaging
- Protocol of Web Services: SOAP (XML-based)
- SOAP mainly used over HTTP(S)
- Most of the time: Computer to computer communication
- Easy access of otherwise hidden systems → Security issue!

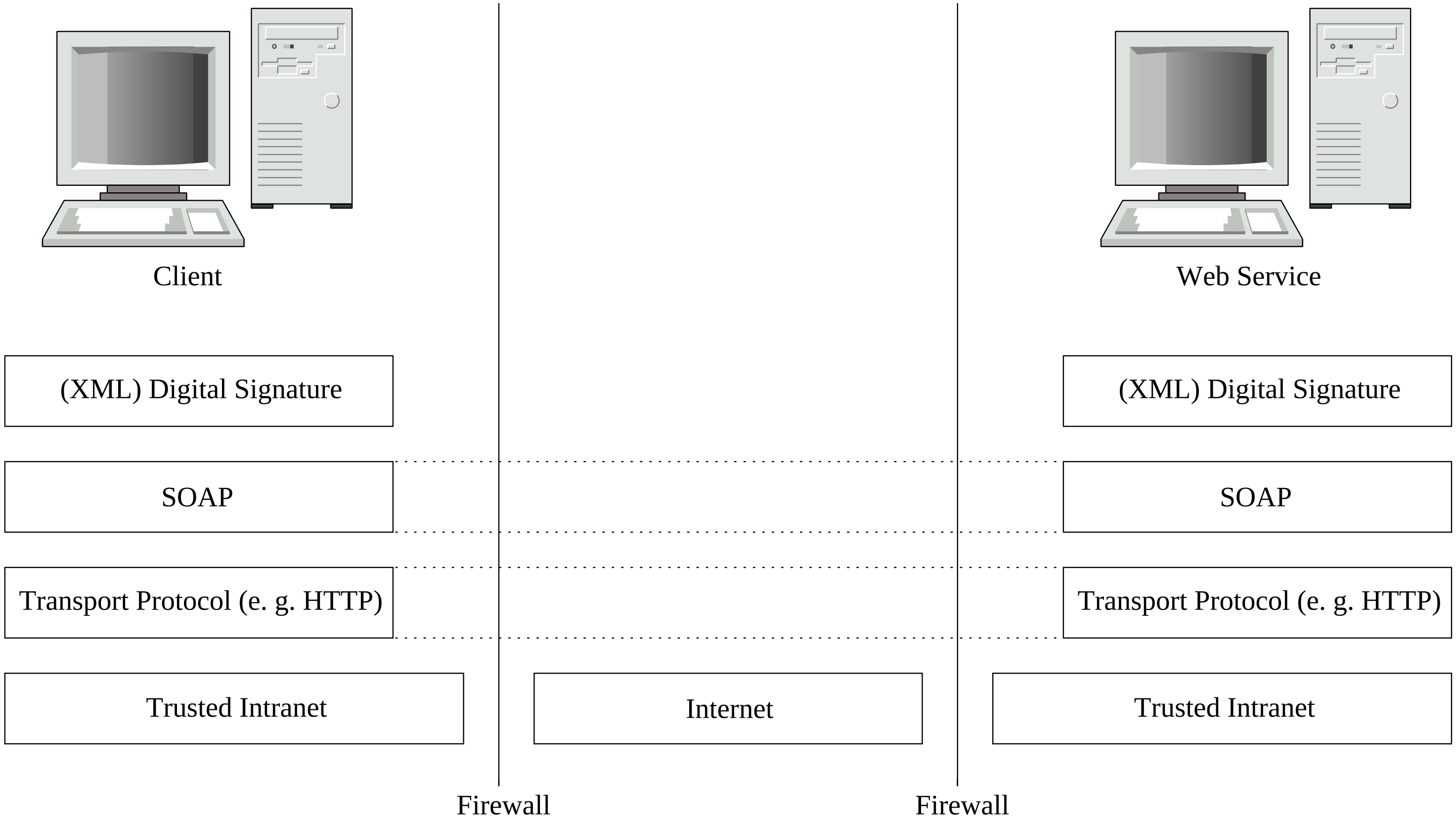
Definition: Web Services

A Web Service is a piece of server-side software that provides a certain functionality (as a black box) and is accessible through Internet protocols using XML/SOAP messages with a described and published interface (typically by means of WSDL).

Those interface descriptions should be registered in a (global) registry such as UDDI.

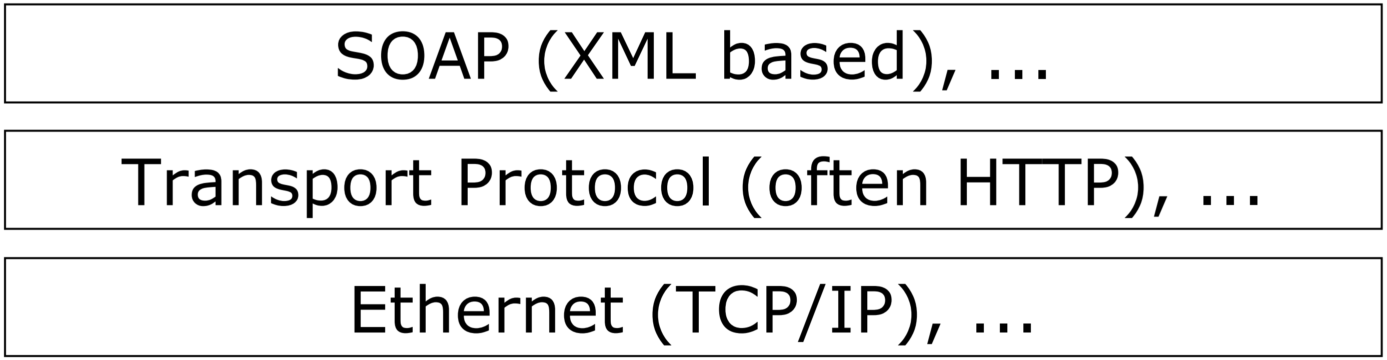
Common Web Services Scenario

- Client calls Web Service over the Internet



Web Services Architecture

- Web Services Protocol: SOAP (XML based)
- SOAP usually over other protocol
- SOAP does not deal with security (and does not have to)



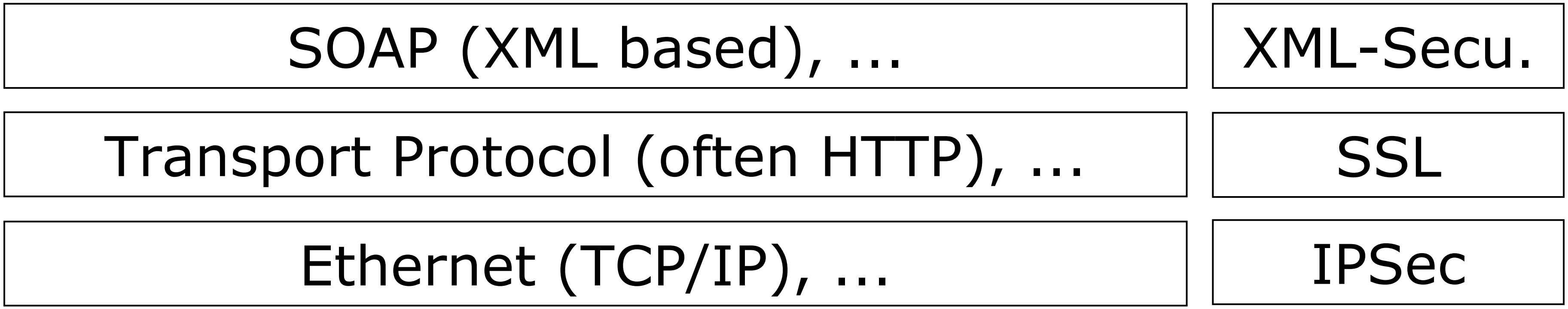
SOAP (XML based), ...

Transport Protocol (often HTTP), ...

Ethernet (TCP/IP), ...

Web Services Architecture + Security

- Security can be added at each layer
- No layer completely suitable for securing all services
- XML-layer important for flexibility (intermediaries)
- XML-Signature, XML-Encryption, WS-Security, SAML



SOAP (XML based), ...	XML-Secu.
Transport Protocol (often HTTP), ...	SSL
Ethernet (TCP/IP), ...	IPSec

Why SSL (HTTPS) often does not help:

- SSL is only for point to point connections
- Only usable for a few protocols (mainly HTTP)
- Only transport of **whole** document is encrypted
- Header information no longer readable
  - Routing information
  - Intermediaries
- Calling a set of Web Services?
- Asynchronous call of Web Services not possible
- Data unprotected upon reaching the server
- Authentication of origin lost if more than one service is involved

Needs and Wishes

- Security at XML level, e. g. to keep only parts of the message readable
- Transparent for users → impossible to forget it
- Centralized control → single point of administration
- Easy integration into existing systems
- Usable even with external partners → no proprietary solutions
- Open Standards like XML-Signature, WS-Security, …
- Interoperability
- Framework for exchange and adaptation of security technologies at any time

XML-Signature (Existing Technology)

- RFC 3275: Digitally sign document and represent in XML
- Result is (still) an XML document
- XPath to locate and identify parts to be signed
- Multiple signatures can added to one document

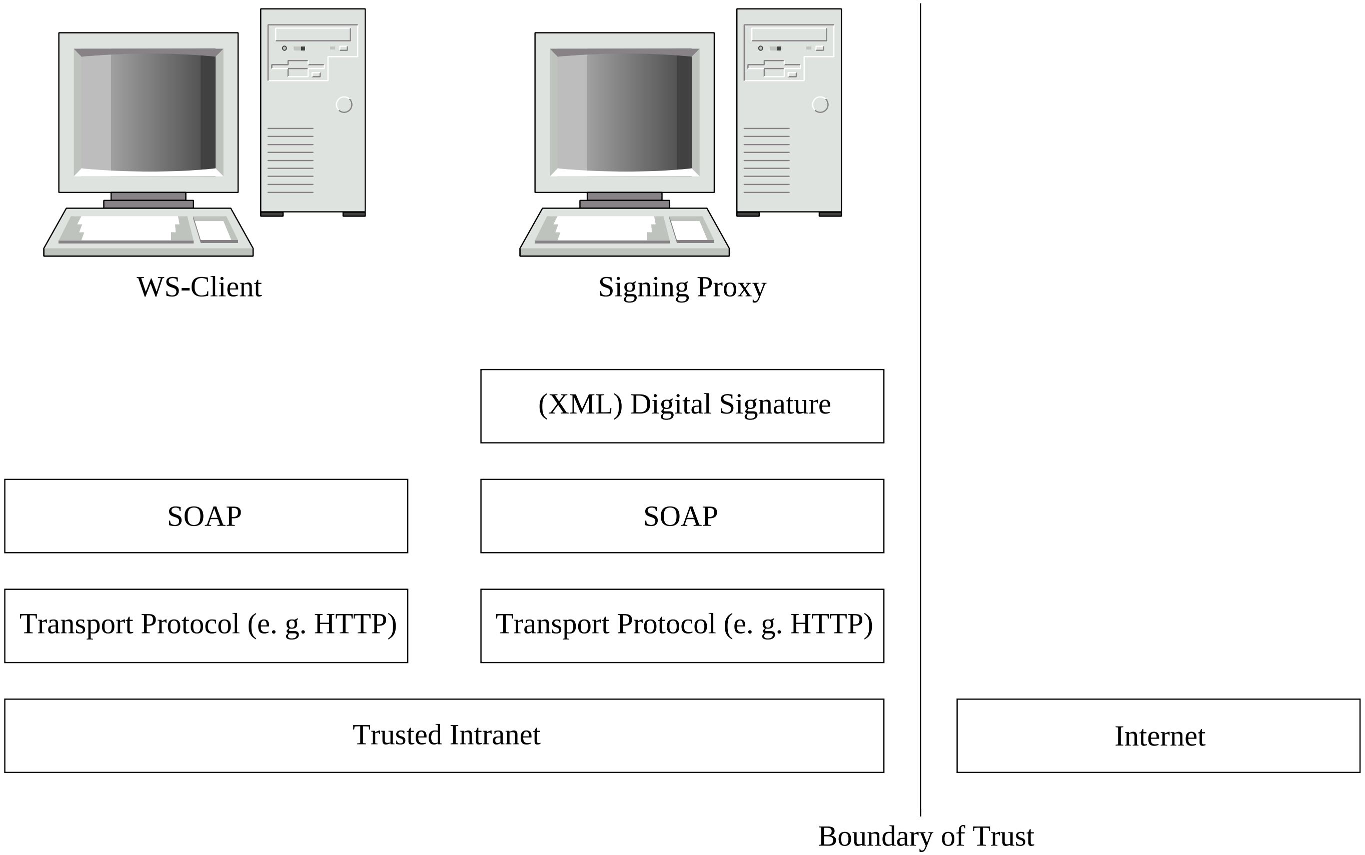
1. Choose parts of documents to sign
2. Calculate digest (or hash sum) of each part (after canonization)
3. Build <SignedInfo> element (contains digest, used algorithms, XPath)
4. Calculate digest of SignedInfo and sign it → <SignatureValue>
5. SignedInfo, SignatureValue, KeyInfo are added to document in <Signature>

Needs and Wishes not solved at once by XML Signature

- ■ Security at XML level, e. g. to keep only parts of the message readable
- ➢ Transparent for users → impossible to forget it
- ➢ Centralized control → single point of administration
- ➢ Easy integration into existing systems
- ■ Usable even with external partners → no proprietary solutions
- ■ Open Standards like XML-Signature, WS-Security, …
- ■ Interoperability
- ■ Framework for exchange and adaptation of security technologies at any time

Adding Security Transparently

- Proxy transparently adds XML-Signature



WS-Client

Signing Proxy

(XML) Digital Signature

SOAP

SOAP

Transport Protocol (e. g. HTTP)

Transport Protocol (e. g. HTTP)

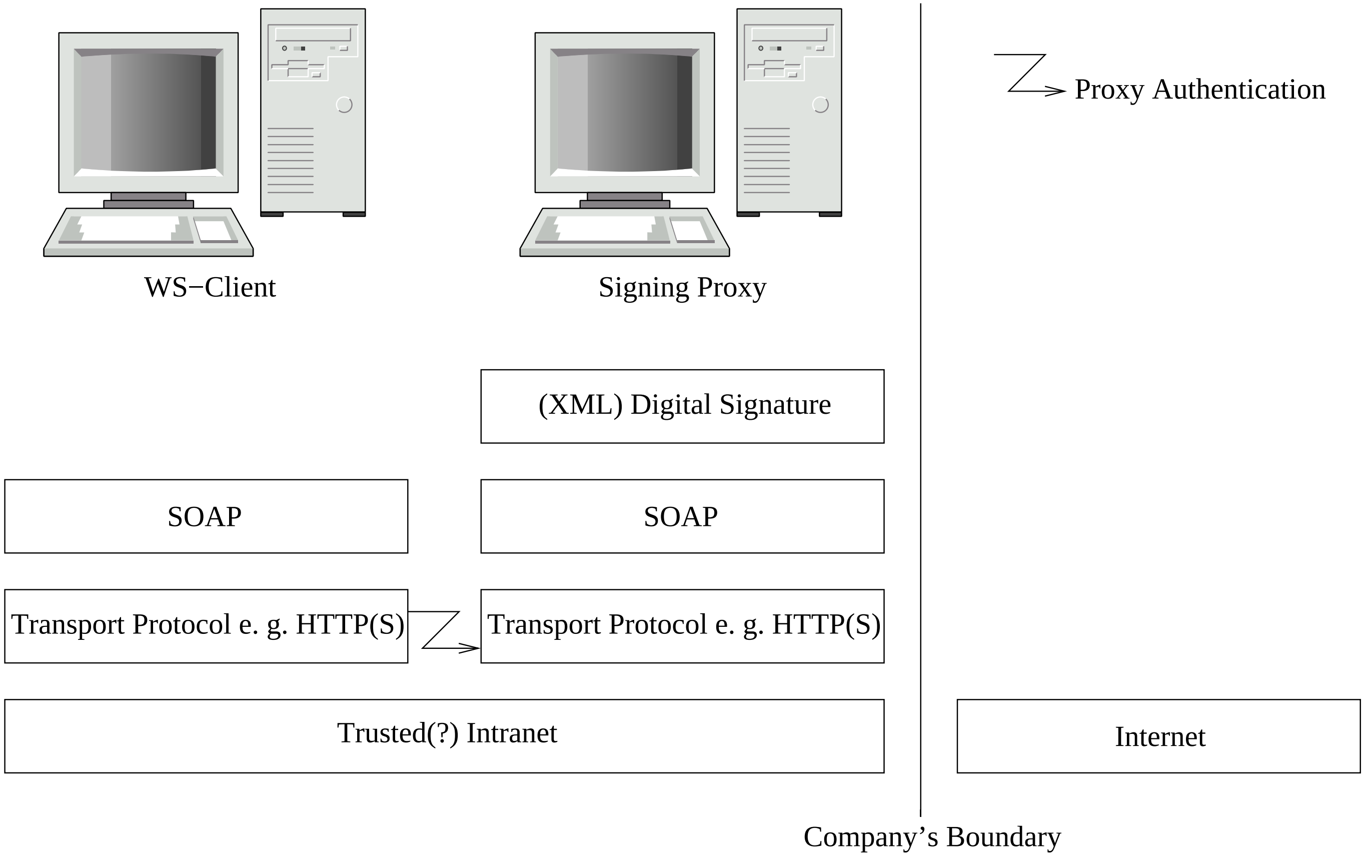
Trusted Intranet

Internet

Boundary of Trust

Adding Security Transparently II

- Proxy authentication for personal XML-Signature



Encryption for B2B Environment
Static Set of Partners

- In a B2B environment, it is possible to keep a list of partners
- Therefore encryption can be done in this way:

1. Determine Partner for outgoing message (e. g. domain of URL)
2. Get public key of partner (database, PKI, …)
3. Encrypt e. g. body of message using the key and XML-Encryption

- Firewall of receiver can use its private key for decryption
- Information for a more precise encryption possible with header expansions
- This job could also be done by an intermediary

Requirements for Bigger Encryption Scenario

- Public Key of receiver needed for encryption.
  Possible Solutions:
  - PKI or public key servers (like for pgp)
  - Expansion for WSDL (where are the public keys)
- Standard for SOAP header expansion to specify part to be encrypted
- Further spreading of XML encryption
- Signature can be ignored, encryption cannot

It does not help if receiver cannot decrypt message

Status

- Two papers accepted:

1. Ingo Melzer, Mario Jeckle:
   Using Corporate Firewalls for Web Services Trust,
   ICWS-Europe'03, Erfurt, Germany, September 23 to 25, 2003, to appear
2. Ingo Melzer, Mario Jeckle:
   A Signing Proxy for Web Services Security,
   Berliner XML-Tage 2003, Berlin, Germany, October 13 to 15, 2003, to appear

- Ongoing Master Theses with University of Ulm (Prof. Dr. Schweiggert) and the University of Applied Sciences Furtwangen (Prof. Jeckle)
- Demonstrator for proof of concept
- T. b. d.: More on encryption including concept for bigger scenario

Summary I

- SOAP does not deal with security (and does not have to)
- No secure Web Services available yet
- HTTP is no longer static (or dumb?) → Firewalls have to be able to process SOAP, but
- Today’s firewall software for Web Services not sufficient
- Other XML-based standards suitable for this job:
  XML-Signature, XML-Encryption, SAML, WS-Security, …
- Idea: Signing Proxy to transparently add signatures
- Improvement for firewall to check signatures not very difficult

Summary II (Signing Proxy)

- Signing Proxy offers single point of administration
- WS developers have to deal much less with security
- Can be part of security infrastructure
- Offer a service (just like a PKI)
- Signing Proxy fits perfectly into Service Oriented Architecture
- Encryption easily added in B2B environment

Nevertheless: Security for Web Services has to be improved