ODETTE
SWEDEN

OFTP2 kurs

Odette File Transfer Protocol 2

Peter Nilsson, Business Analyst, Volvo IT
Sten Lindgren, VD Odette Sweden

Fredagen den 18 januari 2013
Tullverket, Luleå

Version 14.2

08.00	**Kommunikationsbehoven inom EDI/B2B och vilka lösningar används** ▪ Applikationsexempel ▪ Typ av integrationsproblem som förekommer ▪ Standarder och begrepp ▪ Användning av OFTP inom olika branscher
	OFTP-protokollet – historiken – vilka är alternativen?
	OSI-stacken
	Krav på infrastruktur för att köra EDI ▪ Vad är Internet? ▪ IP, olika sätt att använda IP ▪ Vilka är begränsningarna? ▪ Risker, hot ▪ Internet som kommunikationskanal för EDI lokalt/globalt ▪ Utmaningar när man kör EDI över Internet ▪ Alternativa datatransporttjänster, ENX, VPN, tjänster under avveckling som ISDN, X.31 …….. ▪ Hur skiljer sig bilden när det gäller datatransporttjänster i Sverige och i andra länder?
10.00	**Paus**

10.15	**Alternativa säkerhetslösningar** **Vad är certifikat?**
	PKI och certifikatsadministration - CA-funktion och hantering av certifikat - Olika parters funktion - PKI - Olika sätt att använda certifikat - Signering, kryptering **TLS och SSL**
11.30	**Lunch**
12.15	**Odettes rekommendationer och tjänster för säkerhetshantering** - Odettes säkerhetspolicy (Odette SCX) - OFTP2 och certifikatshantering - Frågor och svar.

	OFTP2 – innebörd i stort ▪ Nya protokollfunktioner ▪ Interoperabilitetstester ▪ Vilka använder OFTP2?
	Filöverföring enligt OFTP2-protokollet ▪ Sessioner ▪ Kommandon ▪ Partneridentifiering (ICD-koder) ▪ Demo av verklig OFTP2-kommunikation mellan två partners
	Applikations- och kommunikationsavtal
	Frågor och svar
15.15	**Avslutning**

ODETTE SWEDEN

Training course objectives

- Basic understanding of communications services and their usage in B2B Data Exchange (EDI)
- Basic understanding of how to use Internet for EDI and how to build trust between trading partners
- Understanding the OFTP2, information flow, OFTP components etc
- How to identify errors on protocol and network level, including reading of OFTP and communications tracing and logging information
- The understanding of OFTP2 related specifications
- Share implementation experience

ODETTE
SWEDEN

Laget runt

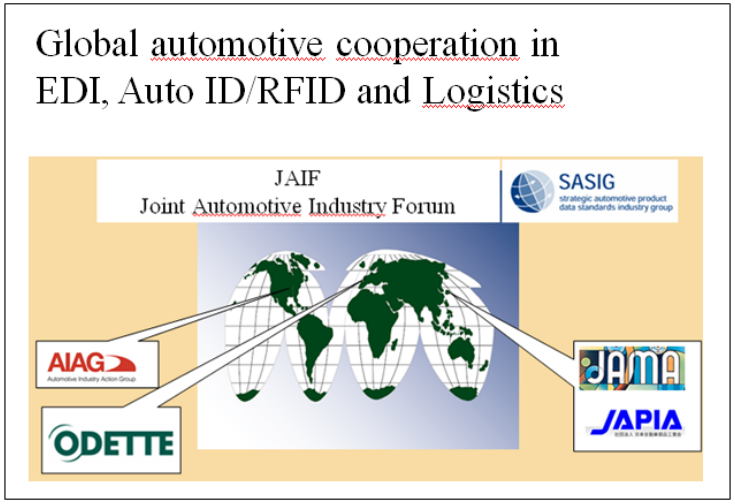
Membership

- National Organisations
- **Germany (VDA)**
- **France (GALIA)**
- **Sweden (Odette Sweden)**
- **Spain (Odette Spain/ANFAC)**
- **Czech Republic (AIA)**
- **United Kingdom (SMMT)**

ODETTE SWEDEN

- Associate National Members
- **Turkey (OSD)**
- **Romania (ACAROM)**
- **Russia, Morocco**
- Associate IT Members
- **Axway, QAD, Microsoft**

- Interest Group Members
- **IVECO & FIAT Auto….**
  (repr. Italian interest group.)



Odette Sweden – for the Nordic countries

SCANIA CV

Volvo Car Corporation

AB VOLVO

The three OEMs are members

Another 41 companies are members through the ”NAF initiative”

Created in 1984
Funded and governed by members
Odette Sweden AB is owned by the Trade Association BIL Sweden
Runs the supplier network NAF

Medlemsläget (44 medlemsföretag)

Nätverk för Affärsutveckling i Försörjningskedjan

AB Volvo	Höganäs AB
ALPS - Sweden	IAC Group Sweden AB
Altiro Consulting AB	Innovative Logistics Umeå AB
Autoliv Sverige AB	Integria Logistics Oy Ltd
Autotube AB	KG KNUTSSON AB
Data Interchange	Kongsberg Automotive AB
DB Schenker	Konstruktions-Bakelit AB
DHL Freight Sweden AB	Leax Group
Edimaster OY	Levi Peterson
Encode AB	Meridion AB
EVRY One Anderstorp AB	Nitator AB
Finnveden Bulten	OGO AB
FLODINS FILTER AB	PipeChain AB
GeBC	Plastal AB
Gestamp HardTech AB	Samhall AB
GKN Driveline Köping AB	Scania CV AB
Gnotec Kinnared	SKF AB
Gnutti Powertrain AB	Thule Sweden AB
Haldex Brake Products AB	TitanX Engine Cooling AB
Heléns Rör AB	Tyringekonsult AB
HellermannTyton AB	Viaduct AB
HT Svarv AB	Volvo Personvagnar AB

ODETTE SWEDEN

Layout proposal – Three label modules

Ship to final name
Ship to final address, Line 1
Line 2
Line 3

Trp serv. – Ship to name
Trp serv. – Ship to address, Line 1
Line 2
Line 3

Sender name
Ship from address, Line 1
Line 2
Line 3

Delivery ref.

Despatch date

Supplier no

Plant/Dock
Logistics ref. 1
Logistics ref. 2

Transport service provider

Transport service

Transport ref. 1

Routing code

Transport ref. 2

Routing code – Bar coded

Part no

Qty **U/M** Traceability ref

Part description

Part revision level

Packaging type

Gross weight

Manufacturer code
Country of Origin
HS code
UN code

(1J) UN 049977473 123456789

ODETTE SWEDEN

ODETTE
SWEDEN

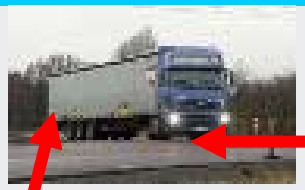
Communications services for B2B Data Exchange (EDI)

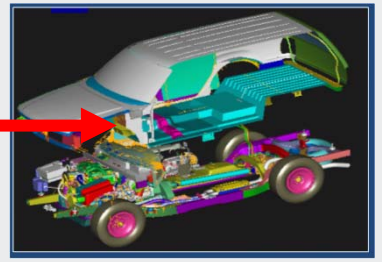
Data Exchange in the automotive industry

Inbound logistics

Component manufacturing

Product development

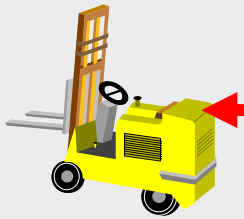



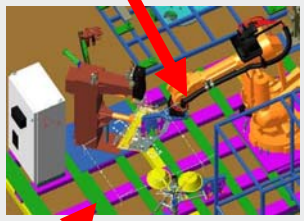



Goods reception

Final Assembly

Sales

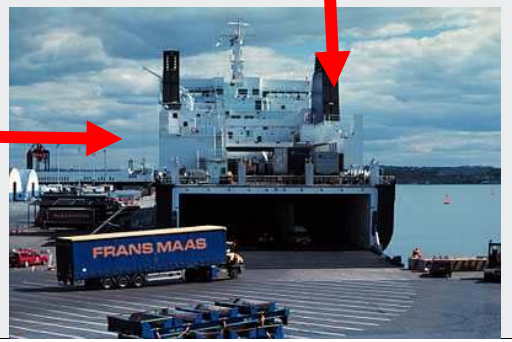



Repair shops

Dealers

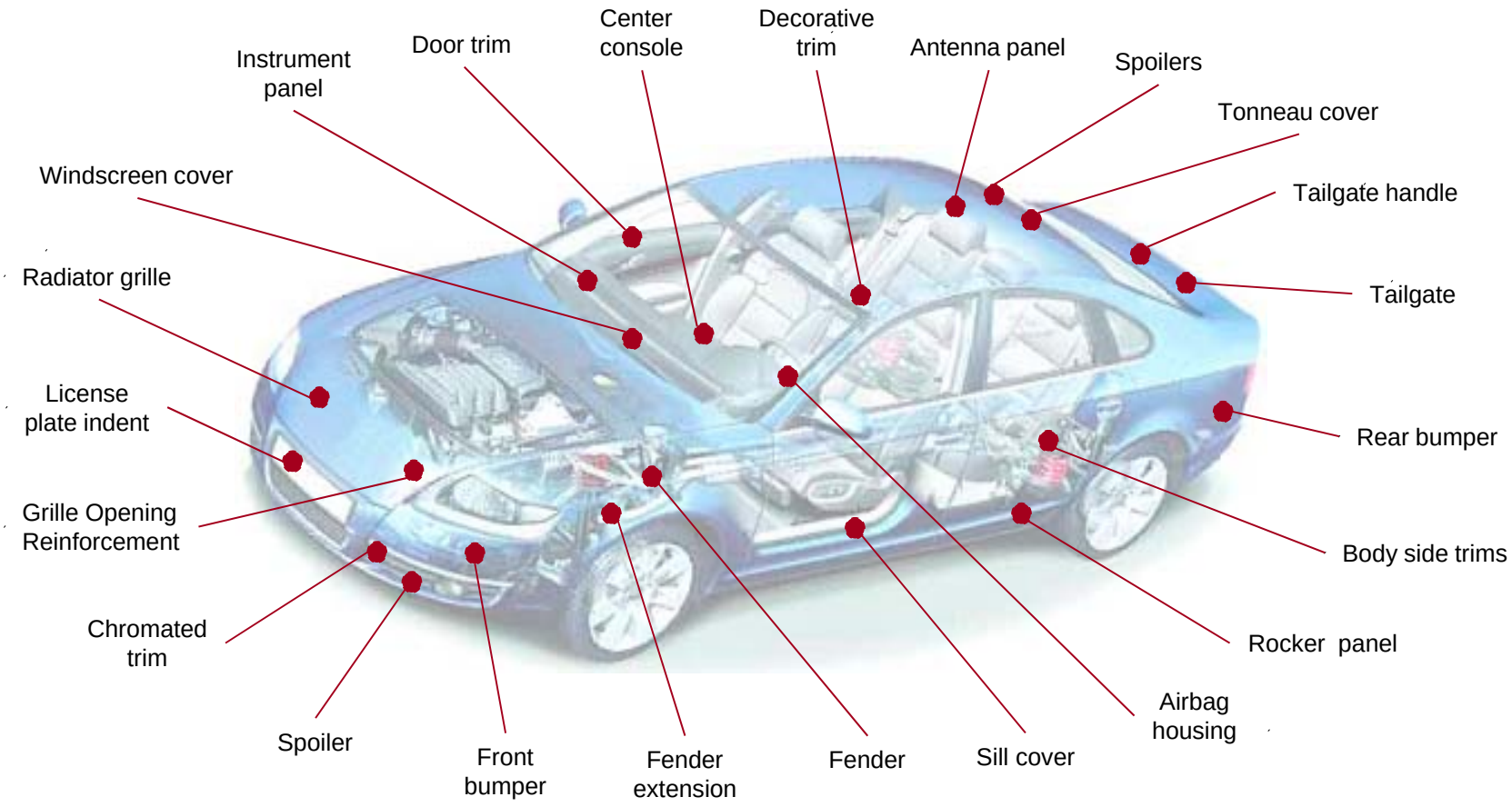
Logistics





EDI supports complex logistics processes

Many parts from a large number of trading partners



EDI supports complex logistics processes

Ordering of individual components/sub-assemblies for sequenced deliveries

ODETTE SWEDEN

ACRONYMS used in the training course (I)

The world of EDI is full of acronyms, some of the most commonly used are:

AIAG	Automotive Industry Action Group	**MITM**	Man-in-the-middle
AS2	Applicability Statement 2	**OEM**	Major (Automotive) Customer
B2B	Business to Business	**OSCAR**	Odette System for Coding And registration
CA	Certification authority	**OSI**	Open Systems Interconnection
DMZ	DeMilitarized Zone	**PKI**	Public Key Infrastructure
ebXML	Electronic Business using eXtensible Markup Language	**SCX**	Odette Security Certificate Exchange project
EDI	Electronic Data Interchange	**SFTP**	SSH File Transfer Protocol
EDIFACT	United Nations EDI standards (EDI For Administration, Commerce and Transport)	**SLA**	Service Level Agreement
ENX	European Network Exchange		

ODETTE SWEDEN

ACRONYMS used in the training course (II)

The world of EDI is full of acronyms, some of the most commonly used are:

ERP	Enterprise Resource Planning	**SMTP**	Simple Mail Transfer Protocol
FTP	File Transfer Protocol	**SSL**	Secure Sockets Layer
GNX	Global Network Exchange	**TCP/IP**	Transmission Control Protocol/Internet Protocol
IETF	Internet Engineering Task Force	**Tier1**	Tier 1 or primary supplier
ISDN	Integrated Services Digital Network	**TSL**	Trust Service Status List
IPSEC	Internet Protocol Security	**VAN**	Value Added Network
JAIF	Joint Automotive Industry Forum	**VPN**	Virtual Private Network
JAMA	Japanese Auto Manufacturers Association	**XML**	EXtensible Mark-Up language
JAPIA	Japanese Auto Parts Industry Association		

ODETTE SWEDEN

European Automotive Industry has experience in e-Business since 1985 (at least)

"Traditional" EDI and web wise, messages, data exchange, labelling

Business information type:

- Product Data Communications
- Procurement
- Supply Chain Logistics
- Invoicing
- After-sales
- Finance
- Transport/Customs

Most messages and other guidelines are global today

Vad gör EDI: Electronic Data Interchange?

EDI paketerar affärsinformationsinnehållet på ett standardiserat sätt så att informationen kan levereras till och från affärssystem

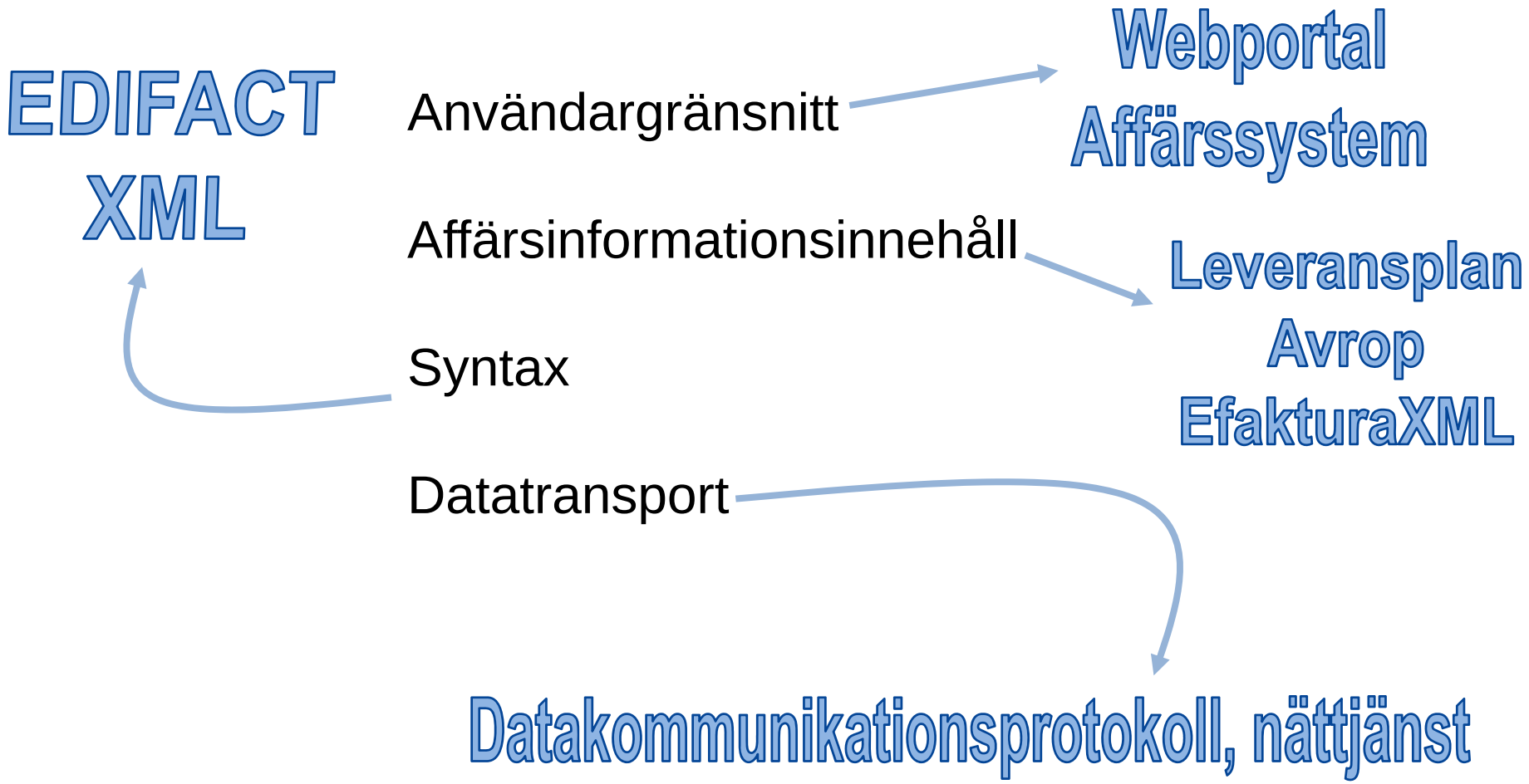
Nytta

- Utan EDI går det inte att hantera de enorma informationsmängder som dagens logistiklösningar förutsätter

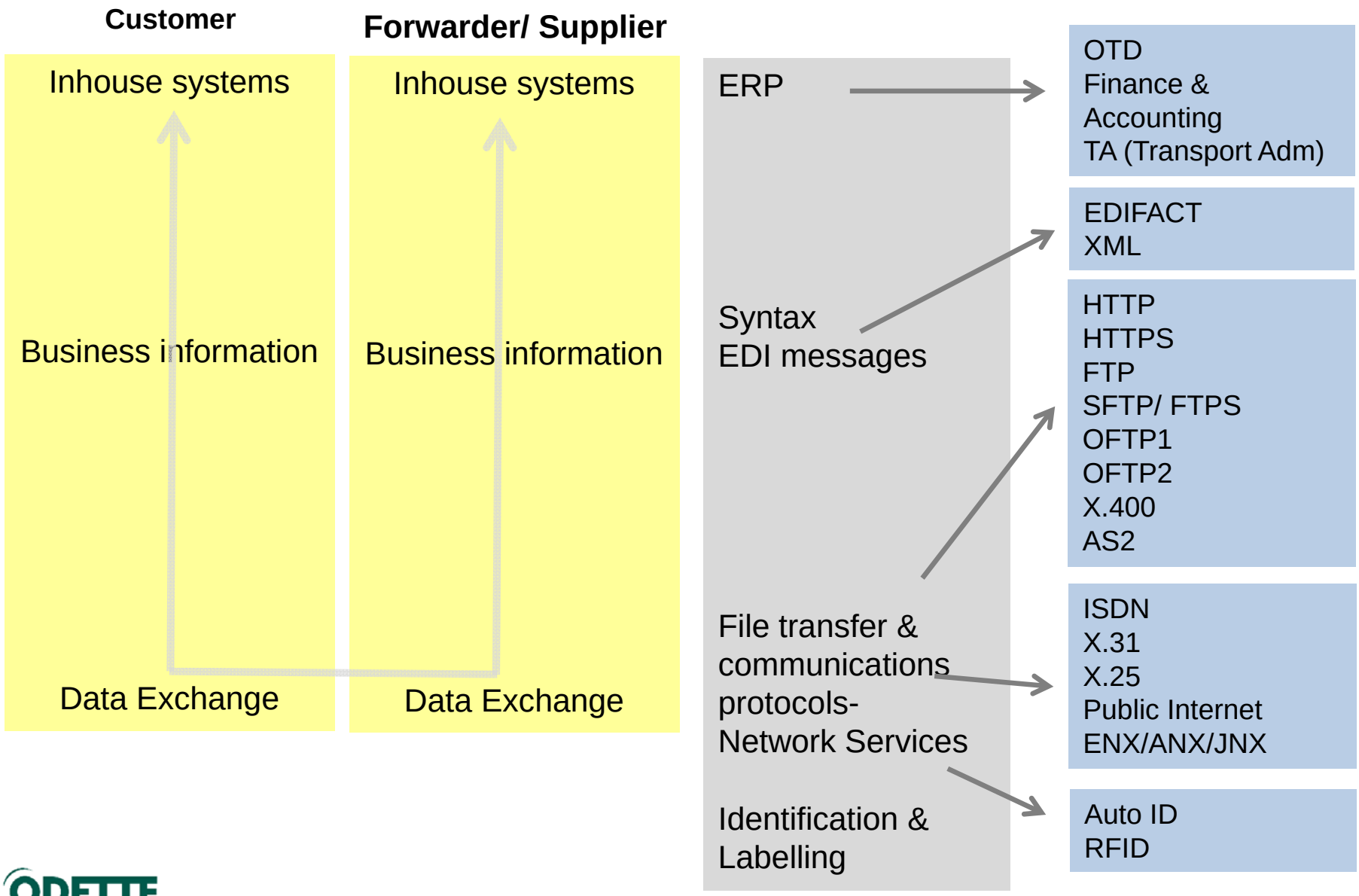
Problem

- Om inte EDI används på ett korrekt sätt begränsas nyttan för en av parterna i informationsutbytet
- Ett stort problem är om ena parten tvingas använda webbportaler
- Ett annat problem är det stora antalet individuella meddelandeprofiler
- Ett tredje problem är rena felaktigheter, dvs då standard inte följs

”e-Business språket”



Bilden i stort: Idag beskriver vi det hela på följande sätt

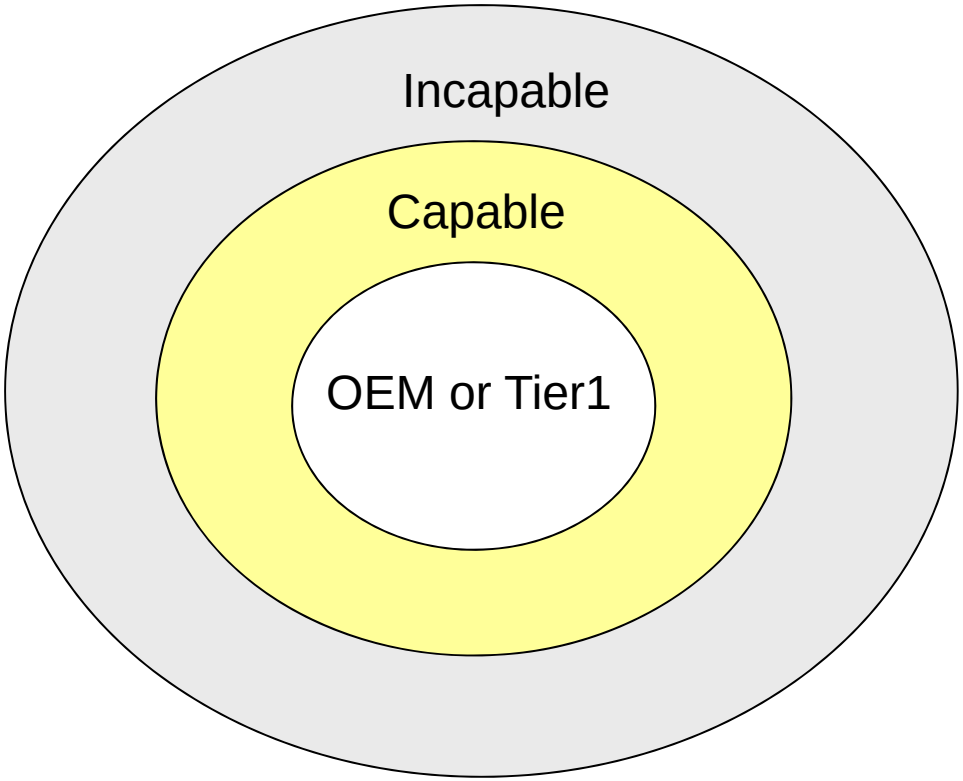


ODETTE SWEDEN

e-Business maturity among trading partners

Capable Trading Partners:
Flexible, standards based B2B gateway
Always ready to connect
Robust trading partner and community management
Examples: Bosch, SKF, ZF, DHL

Challenging Trading Partners:
Connectivity that does not require persistent Internet connections
Minimize security changes required of trading partners
Automated provisioning of End-Points
Support for non-standard and legacy communications
Examples: Medium sized manufacturing companies or forwarders, finance industry



Incapable Trading Partners:
Secure, controlled web-based messaging
Flexible and easy to use data transformation & validation
webEDI solutions
Examples: Emerging markets

Communications services for B2B Data Exchange (EDI)

Challenges

- Handling EDI Capable trading partners
- Handling less EDI capable trading partners
- Handling trading partners in emerging countries
- EDI support for time critical processes
- Managing a large and growing number of EDI relations and growing volumes of information, with all related parameters

Taking advantage of Internet

- Gaining bandwidth and lowering cost
- Without putting the business and it´s information at risk

Examples of the usage of OFTP

Business Sector

Automotive Industry
Other Manufacturing
Customs
Finance
Retail (Often trough VAN: s)
Transports
Engineering Centres

Application fields

Purchasing and Logistics
Suppliers processes
VAN-services
Public services
Banking
Third Party Logistics Services
Product Data CAD/PDM

OFTP– the history

ODETTE SWEDEN

History of OFTP (Odette File Transfer Protocol)

1986 OFTP V1 defined by Odette International

- Mainly used within Europe
- Deployed on secure communication lines (X.25, ISDN, VPN, ENX)
- No encryption

2004 OFTP2 Odette working group started

2007 Odette SCX (Security Certificate Exchange) project group started

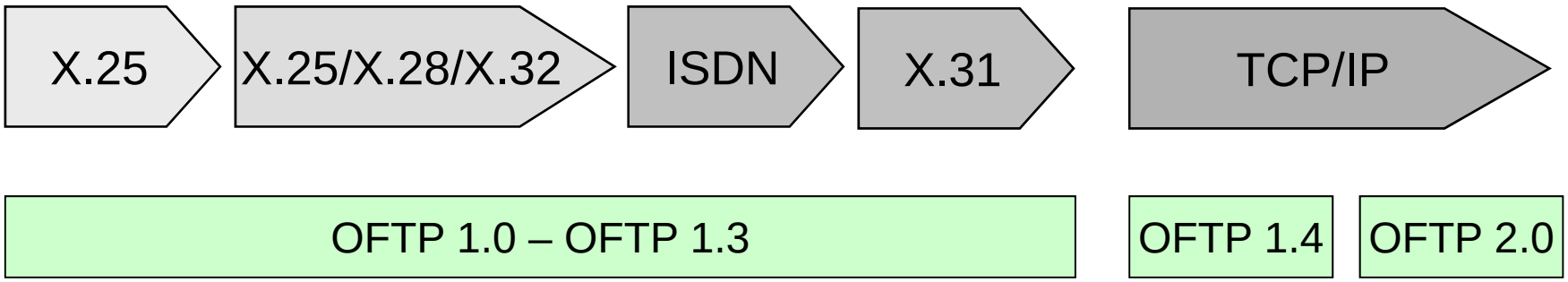
2008 First OFTP2 pilots starting

OFTP in B2B

OFTP is the most commonly used communication alternative for direct B2B communications.

OFTP has been stable since 1986

OFTP has developed in line with the development of communication services:



ODETTE SWEDEN

What is the advantage of using OFTP2?

- With OFTP2 users can take advantage of secure transmission at low cost, high bandwidth and global availability

- OFTP2 was designed to meet high, automotive specific requirements related to mission-critical aspects

- Such requirements include ability to handle large files, restart, technical acknowledgement, confirmation of receipt and non-repudiation

State of the Industry usage of EDI and OFTP

- EDI is widely used in Europe among OEM:s and 1st, 2nd and 3rd Tier suppliers, based on European and/or global automotive recommendations (mainly EDIFACT based)

- The preferred solution is direct data exchange using the OFTP protocol (version 1 or 2).

- OFTP2 is accepted by most actors in the European automotive industry for logistics as well as for engineering data (*BMW, Daimler, Ford, GM Europe, MAN, Peugeot Citroën, Scania, Volvo Group, Volvo Cars, VW Group. ….*)

- There is also some usage outside Europe. One example is VW who established connections in Brazil, US, China, India, Russia

OFTP2 compared to other options

Odette has published a report on File Transfer Alternatives:

- Listed the main aspect to compare
- Investigated specific automotive requirements
- Identified the main alternatives for file transfer

Today´s main alternativs in automotive are:

- OFTP1 /VPN/ENX (decreasing)
- OFTP2 (increasing)
- Web Portals (increasing)
- (AS2)

For the next 10 years probably the main options will be:

- OFTP2
- Web Portals
- Web Services

ODETTE SWEDEN

OFTP2 compared to other options

Web Portals

- Since long seen as a growing problem, could be replaced by EDI based on EDIFACT or XML with OFTP2 or Web Services

Web Services

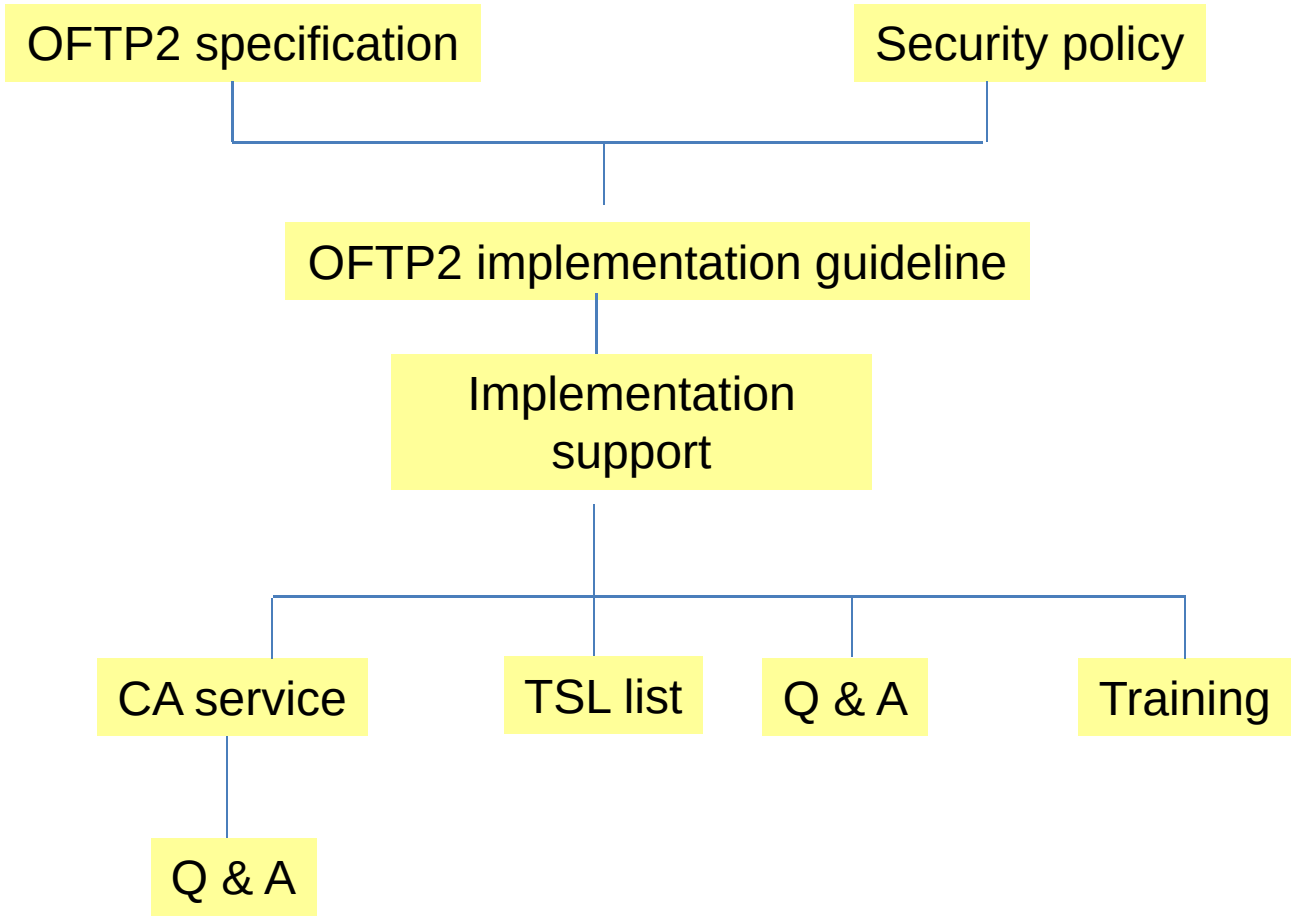
- Suitable for certain applications but not well standardised, only applicable within specifically defined environments
- Could not generally replace OFTP2
- No automated certificate handling

AS2

- Is lacking key functionality needed by the automotive industry
- No automated certificate handling

ODETTE SWEDEN

The role of Odette in OFTP2



ODETTE SWEDEN

ODETTE SWEDEN

Alternative communications protocols

- Secure protocol has been required for some time
- Other protocols have been allowed to creep in
- Suppliers have to meet demands of customers

Protocol	Date
SMTP	1982
X.400	1984
FTP	1985
OFTP	1986
SFTP	2000
AS2	2000
OFTP2	2005

ODETTE SWEDEN

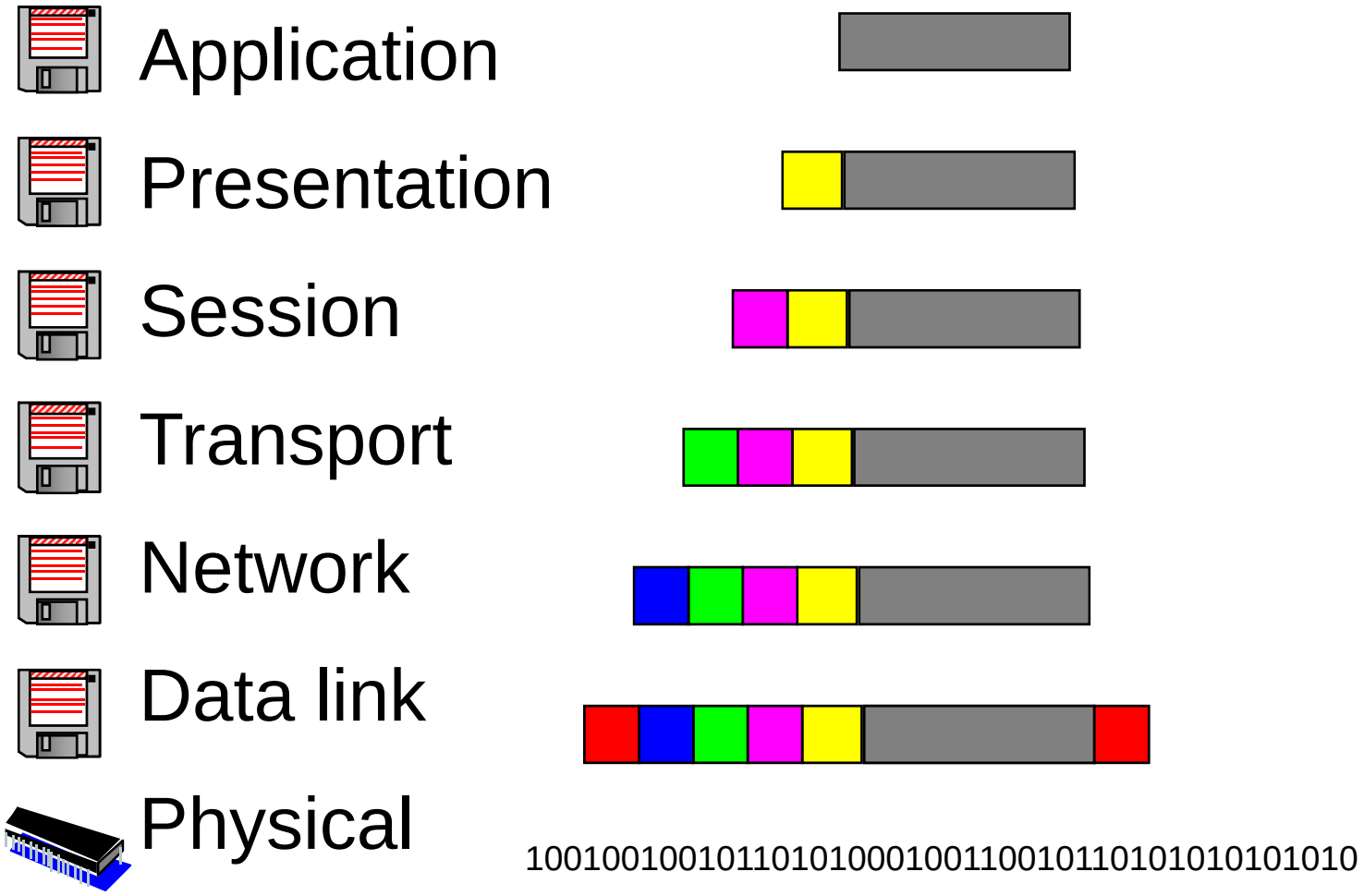
Comparison

	OFTP 2	AS2	SFTP
TCP/IP	Yes	Yes	Yes
X.25	Yes	No	No
ISDN	Yes	No	No
File restart	Yes	No	No
Availability	EU centric	US centric	Global
MITM secure	Yes	No	No
File size and type acceptance	Yes	No	No
Technical Acknowledgement	Yes	No	No
Compression	Yes	No	No

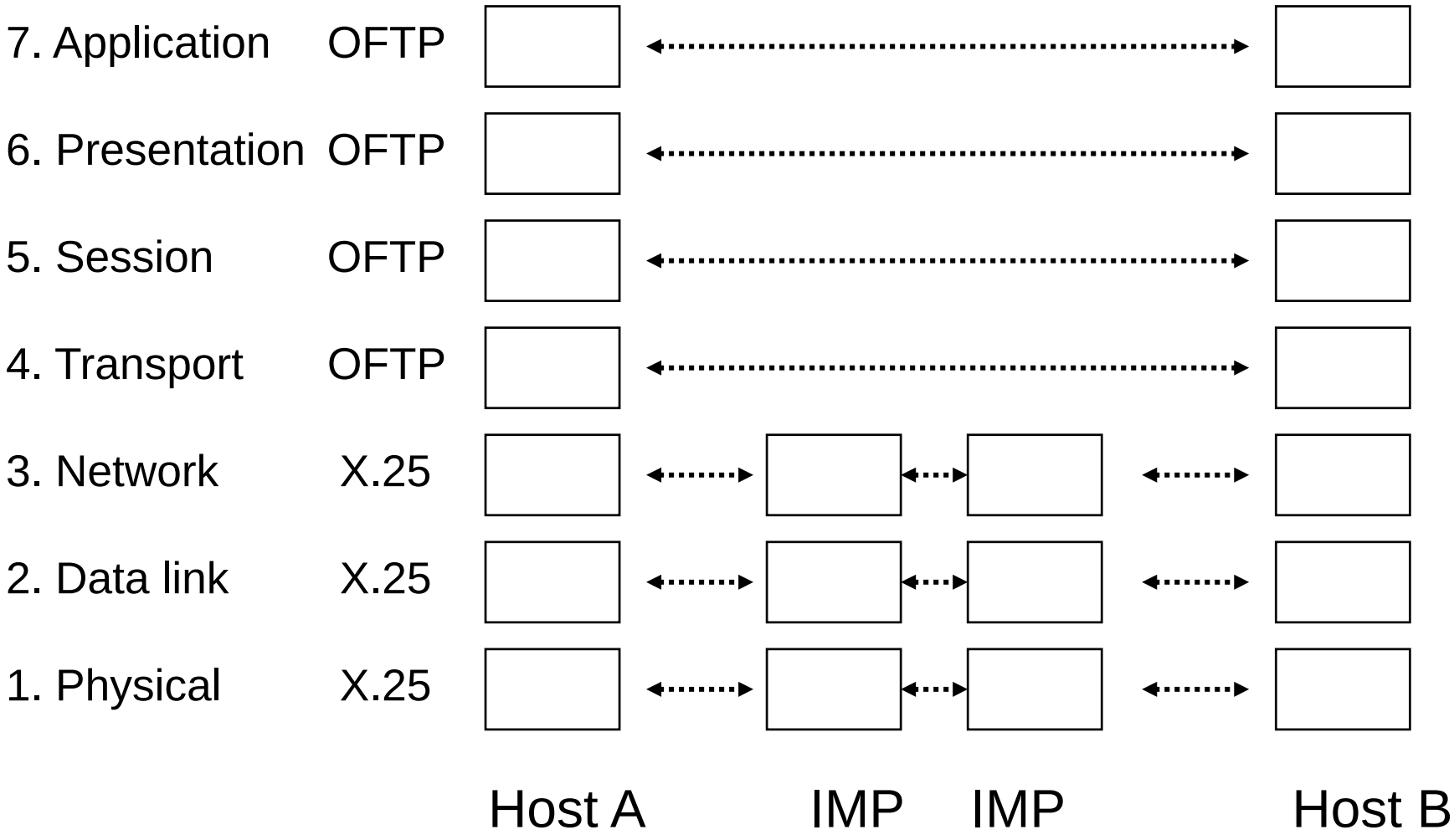
ODETTE
SWEDEN

The OSI model

Open Systems Interconnection



The OSI model (1)



The OSI model (2)

7. Application:
- File transfer
- E-mail
- Virtual terminal

6. Presentation:
- Data representation
- Code conversion
- Encryption
- Compression

5. Session:
- Session start / session end
- Synchronisation, dialogue handling

4. Transport:
- EERP
- NERP
- Multiplexing
- Various service levels

ODETTE SWEDEN

Infrastructure requirements for running EDI

- What is Internet?
- IP, various ways of using IP
- What are the restrictions?
- Risks, threats….
- Internet as a communications channel for EDI locally and globally
- Challenges when running EDI over Internet
- Alternative data transports services: ENX, VPN, older services like ISDN, X.31 ……..
- What is the situation in Sweden compared to other countries when it comes to data transports services?

ODETTE SWEDEN

What is Internet?

Global Communications Network, always available

- The Internet Backbone
- ISP
- Internet protocol – the basis for communications

Examples of how the Internet is used

- Common uses
  - 4.1 E-mail
  - 4.2 The World Wide Web
  - 4.3 Remote access
  - 4.4 Collaboration
  - 4.5 File sharing
  - 4.6 Streaming media
  - 4.7 Voice telephony (VoIP)
- What are the limitations? (Nations, capacity)
  - Coverage
  - Censorship
  - other…
- Risks, threat

ODETTE SWEDEN

Internet Service Provider

Consumers obtain Internet access through an Internet Service Provider (ISP):

- capability to observe Consumer Internet activity
- restricted by legal, ethical, business and/or technical issues
- inspect for business and other purposes

Risks

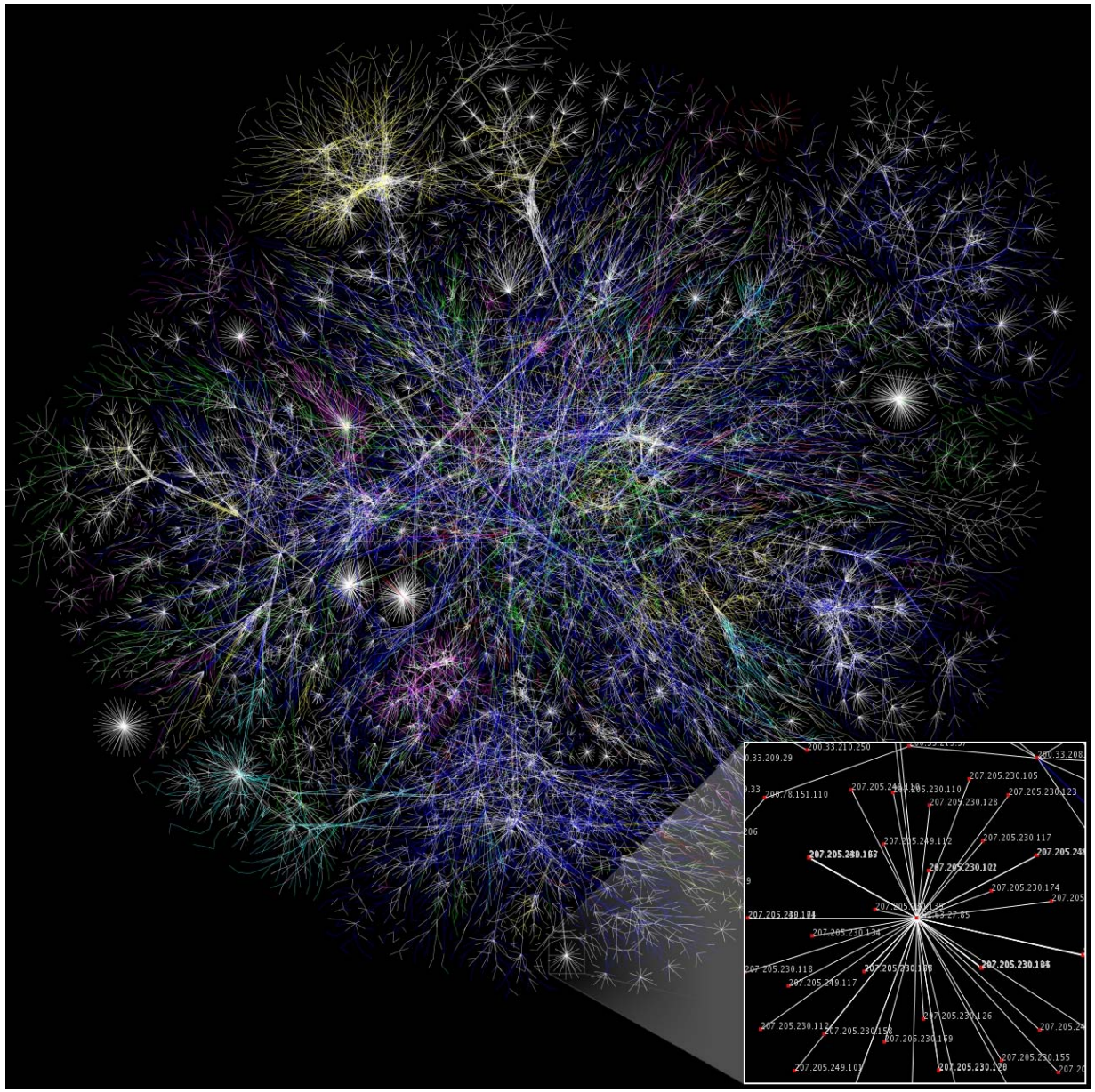
- confidentiality, other actors get access to information about your communication behavior at detailed level and/or access to your information
- Fraud, someone claim an illegitimate identity in order to get access to data and other resources
- ISP share information with other stakeholder such as authorities, communication collaboration partners, business partners…

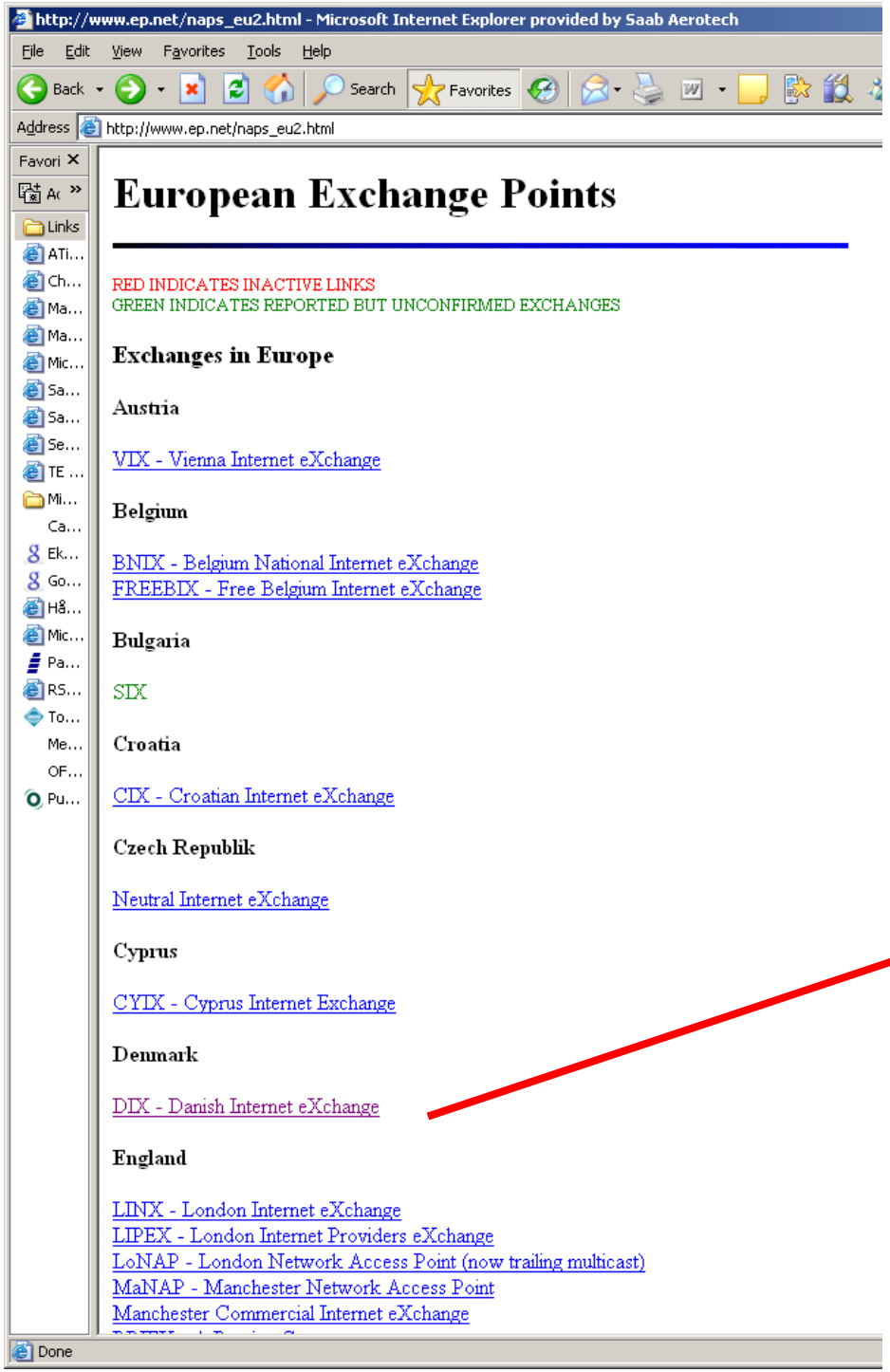
Internet Backbone

http://en.wikipedia.org/wiki/Internet_backbone

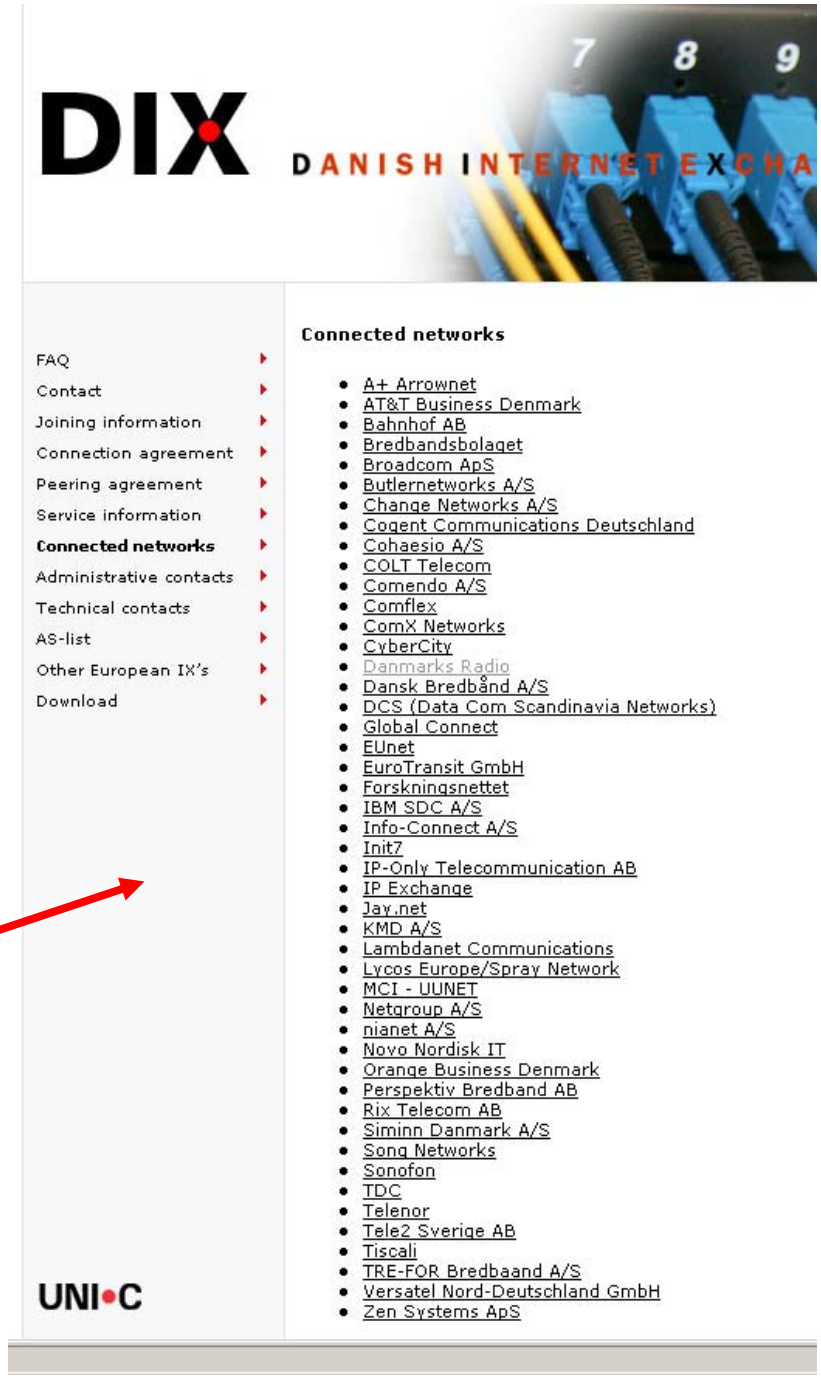
The Internet backbone refers to the main "trunk" connections of the Internet. It is made up of a large collection of interconnected commercial, government, academic and other high-capacity data routes and core routers that carry data across the countries, continents and oceans of the world.

The resilience of the Internet is due to its core architectural feature of storing as little as possible network state in the network elements and rather relying on the endpoints of communication to handle most of the processing to ensure data integrity, reliability, and authentication. In addition, the high level of redundancy of today's network links and sophisticated real-time routing protocols provide alternate paths of communications for load balancing and congestion avoidance.

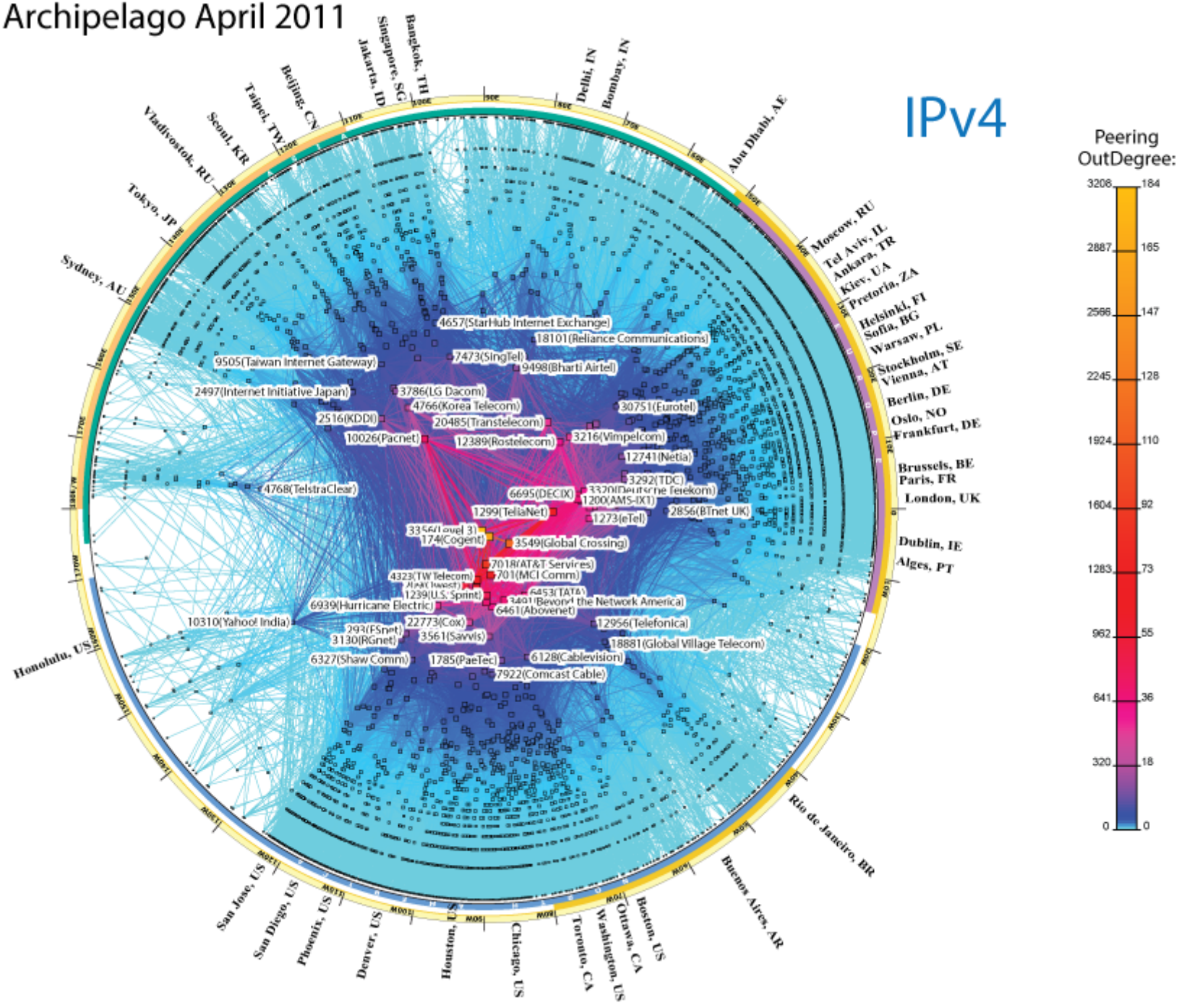




http://www.ep.net/naps_eu2.html

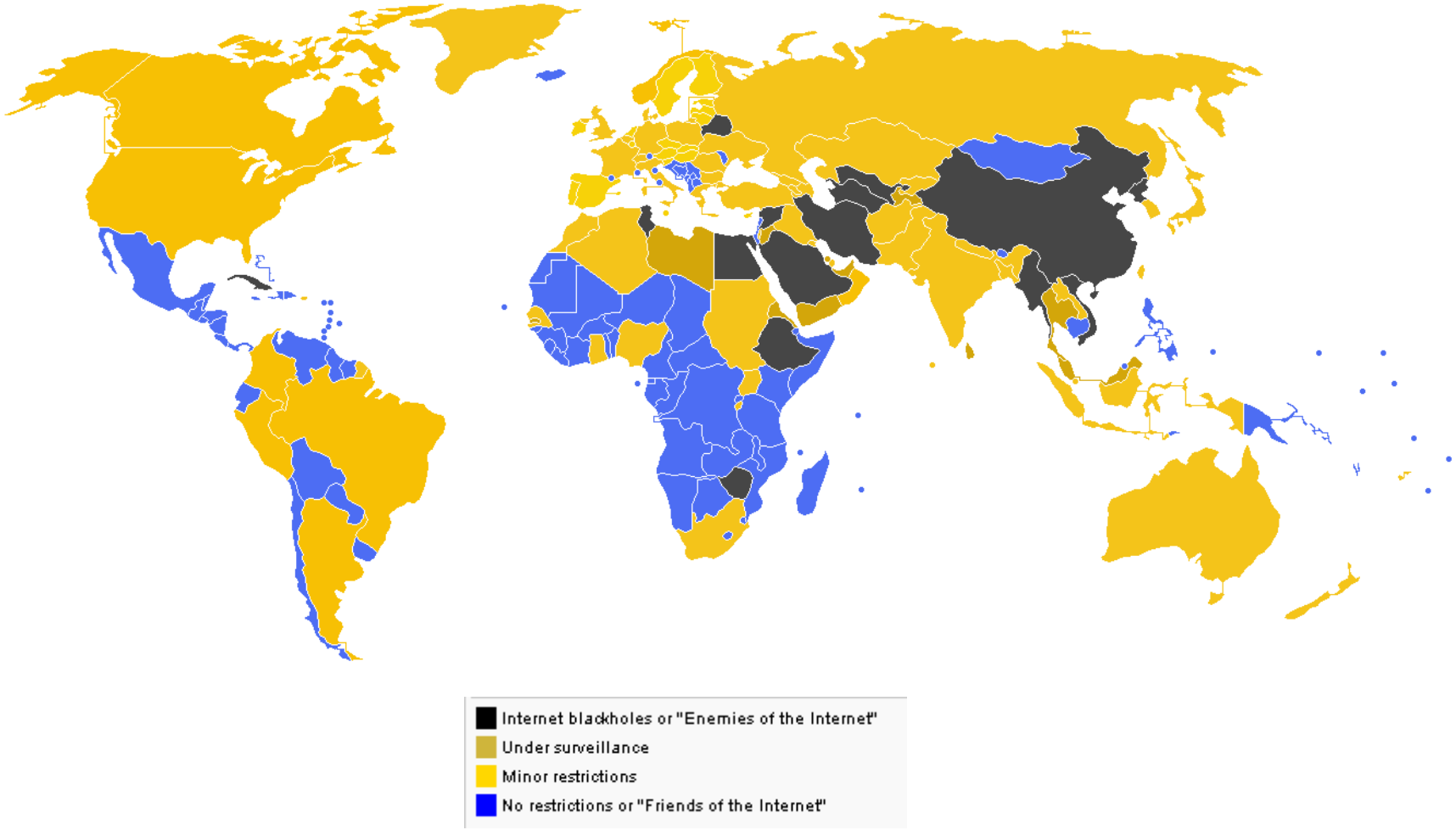


Archipelago April 2011



Internet censorship

December 2008



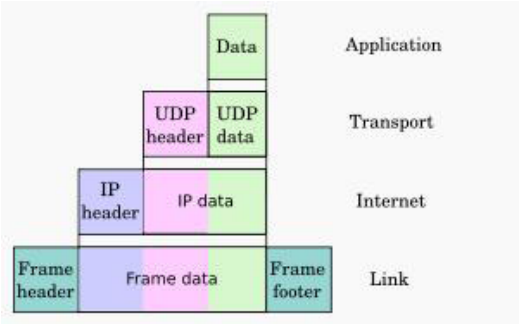
http://en.wikipedia.org/wiki/Internet_censorship

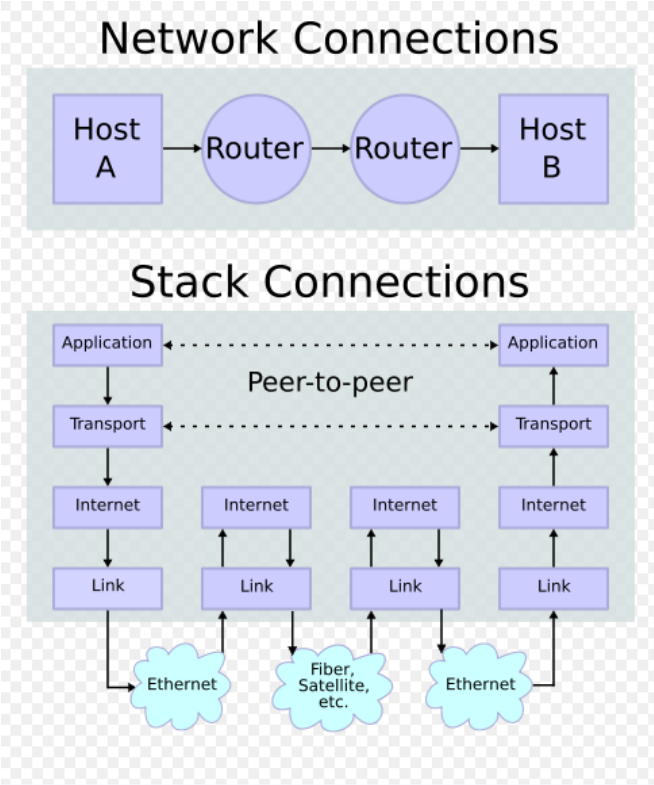
Internet stack and protocols

Encapsulation of application data descending through the protocol stack

The IETF has repeatedly stated that Internet protocol and architecture development is not intended to be OSI-compliant.

Application	DNS, TFTP, TLS/SSL, FTP, Gopher, HTTP, IMAP, IRC, NNTP, POP3, SIP, SMTP, SNMP, SSH, Telnet, Echo, RTP, PNRP, rlogin, ENRP
	Routing protocols like BGP and RIP which run over TCP/UDP, may also be considered part of the Internet Layer.
Transport	TCP, UDP, DCCP, SCTP, IL, RUDP, RSVP
Internet	IP (IPv4, IPv6) ICMP, IGMP, and ICMPv6
	OSPF for IPv4 was initially considered IP layer protocol since it runs per IP-subnet, but has been placed on the Link since RFC 2740.
Link	ARP, RARP, OSPF (IPv4/IPv6), IS-IS, NDP





Challenges related to Networks Services

Networks Services are being closed down in individual countries without any coordination between Service Providers:

- Norway, Denmark and France closed down their X.25 services
- Germany, Belgium, UK , Sweden are keeping their X.25 services based on a new technology
- Sweden is closing down ISDN, or…..? (Telia has changed their policy several times during the last 10 years)

Anyhow the conclusion is that old services like X.25 and ISDN do not meet todays business requirements

Management of security in OFTP2

Odette view on trust and security in open networks (e.g. Internet)

ODETTE SWEDEN

Protect your security on Internet!

- When migrating from ISDN or X.25 Services to Internet we will have to find an acceptable level of security

ODETTE SWEDEN

Today's needs

- More speed, less cost and world wide
- Leave the old networks (X25, ISDN)!
- Go to TCP/IP (Internet, ENX, ...)
- Security: Authentication, Confidentialness, Integrity, Non Repudiation Mandatory over Internet
- Basic components : Keys & Certificates.

SECURITY is based on TRUST

ODETTE SWEDEN

Trust : In which Layer?

Trust at **Network** level:

- Private point to point links
- VPN: Based on IPSEC or SSL
- ENX: A global VPN

Trust at **Software** level:

- Security is inboard, in the application

ODETTE SWEDEN

Trust at Network Level

Security targets:

- Peer **authentication**
- Traffic **protection** against overseer

Advantages:

- Application **transparency** (leased lines or IPSEC)
- ENX: **Delegated management**

Disadvantages:

- ENX: **Cost** & dependency / home made **VPN**
- Leased Lines: **Not flexible**, **Expensive** and finally not that trusty!
- **No file services (**Does not address file content**)**

ODETTE SWEDEN

Trust at Software Level

Security targets:

- Peer **authentication** (not only the site, but the server)
- Traffic **protection** against overseer
- End to end **file services**

Advantages:

- Advanced **file** services features : end to end **encryption**, **signature** and **integrity**, **non repudiation**
- **Same software**: just some configuration items more
- **Low cost** communications (Internet)
- **Autonomy**: no operator and even no IT team dependency

Disadvantages:

- Applications become more **complicated**
- **Internet** connection must be **seriously secured** (DMZ, **Relays**…)

PKI and the handling of certificates

Four basic aspects of security:

- Integrity which guarantees that *data was not altered* during transmission.
- Authenticity which *verifies the identities* of the parties involved in an electronic transmission.
- Non-repudiation of origin which ensures that no party involved in an electronic transaction *can deny their involvement* in the transaction.
- Confidentiality that ensures that only those *who are entitled can access* the transmitted data

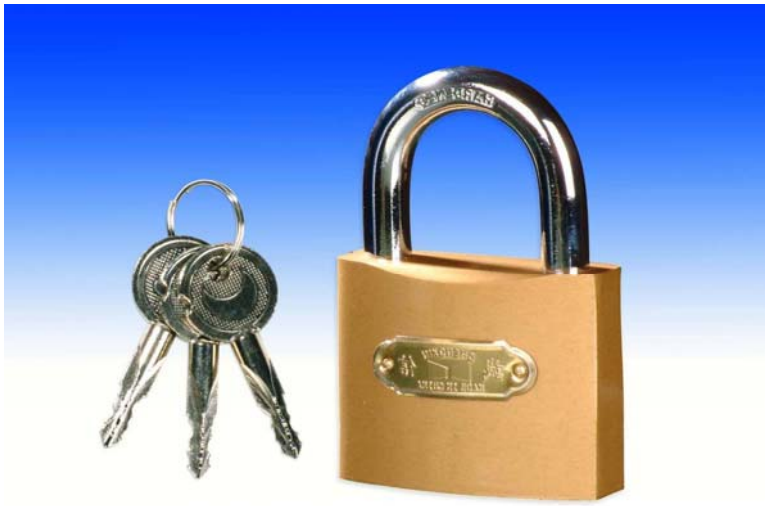
ODETTE
SWEDEN

Introduction to PKI

ODETTE SWEDEN

Public Key Crypto Systems

- Public and private keys
- Speed
- Attacks
- Key length



Public and private key

Symmetric crypto - encrypt and decrypt with same crypto key

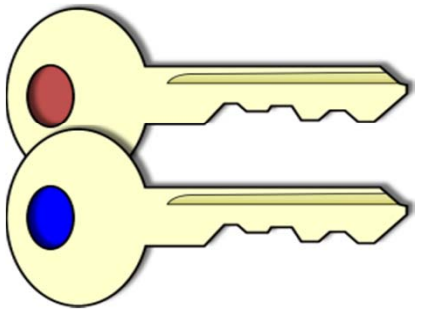
Asymmetric crypto – two different but interdependent keys, encrypt with one and decrypt with the other one, and vice versa

Using Asymmetric crypto for Public and Private Key

- Receive Public Key encrypted messages from many
- Distribute Private Key encrypted messages to many

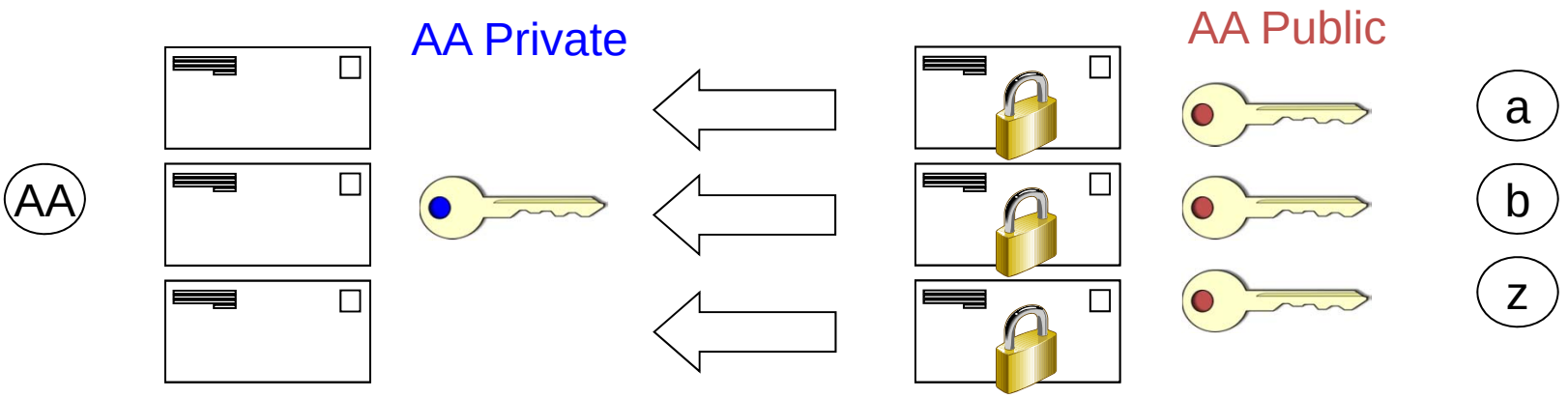
Using Private and Public Key

- Signing
- Protection
- Identification

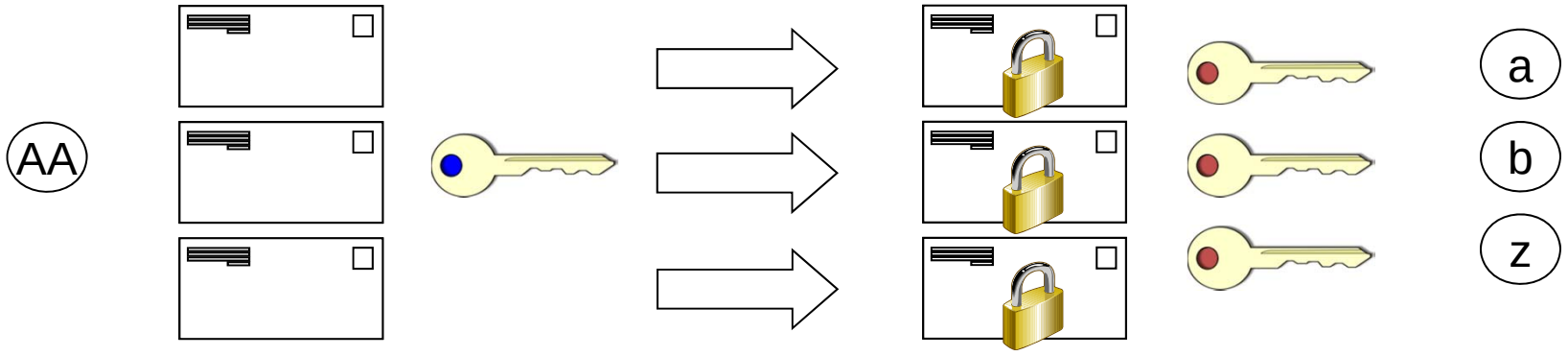


Private and Public key usage, illustration

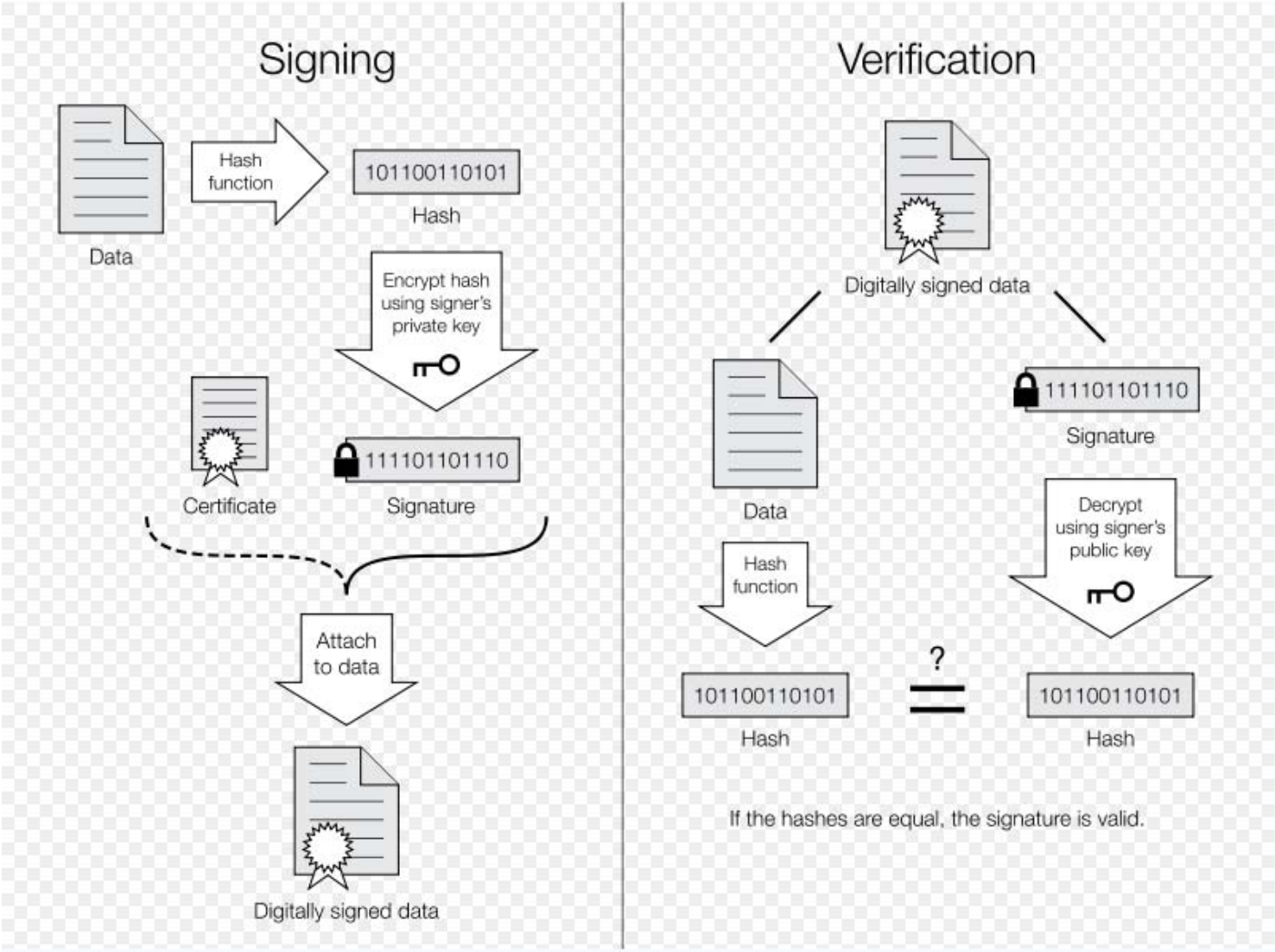
Message to AA encrypted with AA public key



Message from AA encrypted with AA private key



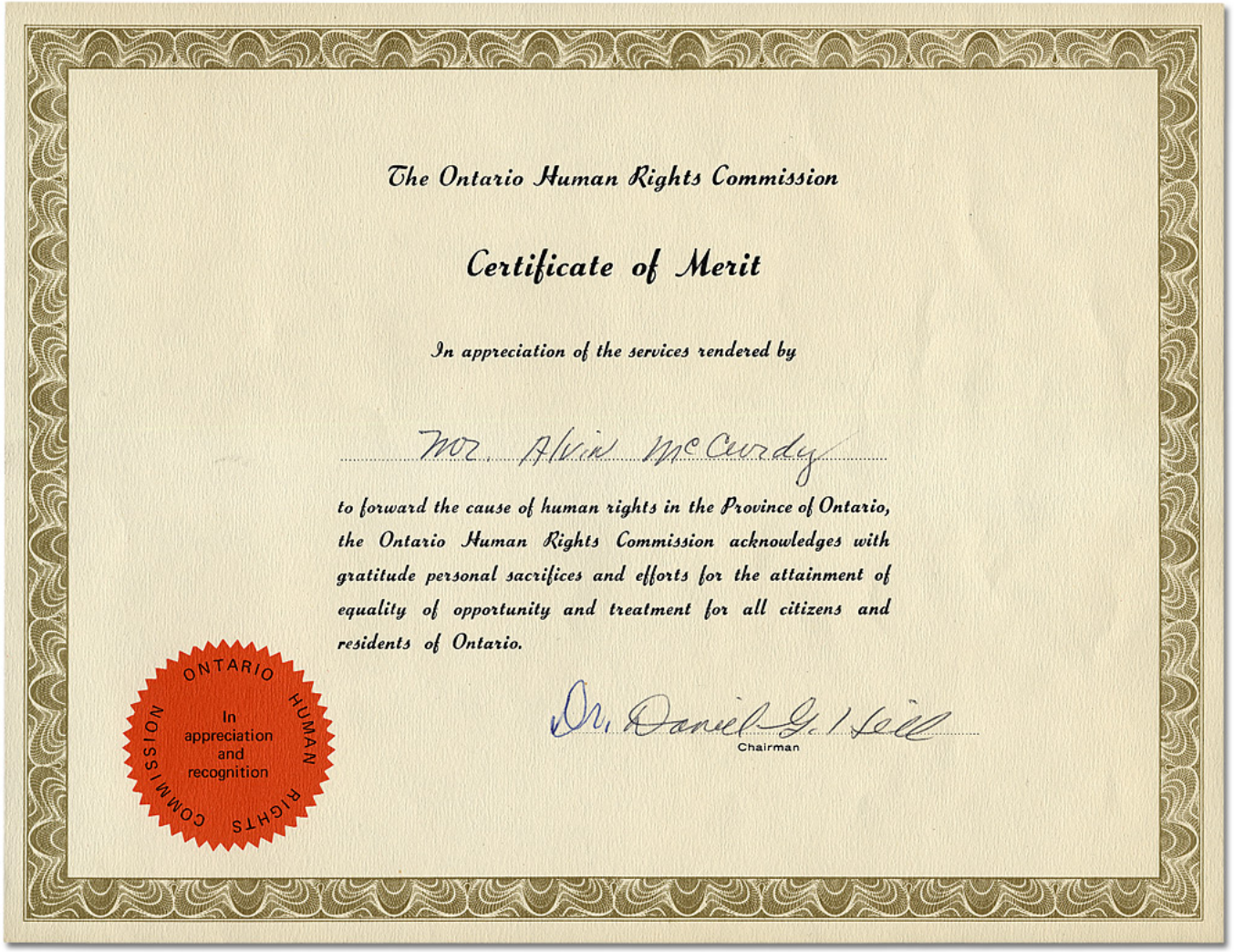
Digital signature, example



http://en.wikipedia.org/wiki/File:Digital_Signature_diagram.svg

ODETTE
SWEDEN

Certificates



The Ontario Human Rights Commission

Certificate of Merit

In appreciation of the services rendered by

Mr. Alvin McCurdy

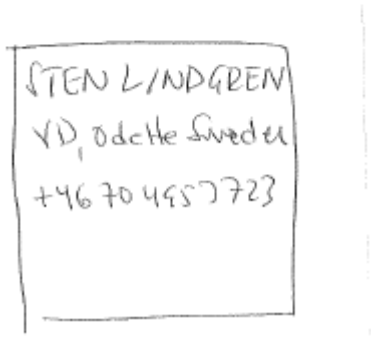
to forward the cause of human rights in the Province of Ontario, the Ontario Human Rights Commission acknowledges with gratitude personal sacrifices and efforts for the attainment of equality of opportunity and treatment for all citizens and residents of Ontario.

ONTARIO HUMAN RIGHTS COMMISSION
In appreciation and recognition

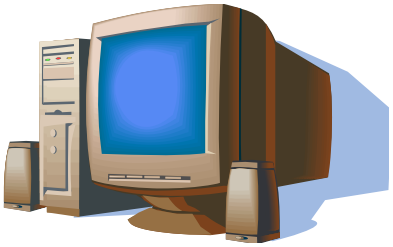
Dr. Daniel G. Hill
Chairman

The Challenge of Trust

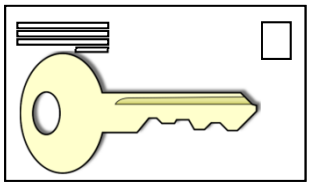
- Technically, (nearly) all certificates implement the same standard technology
- Whether you trust them, depends on the issuing CA and how trustable the CA is
- With hundreds of CA‘s the assessment of trustability of each of them becomes a nightmare



Certificate Authorities



Certificate Signing Request



User sends public key and identifying information

CA creates certificate and signs with CA's private key

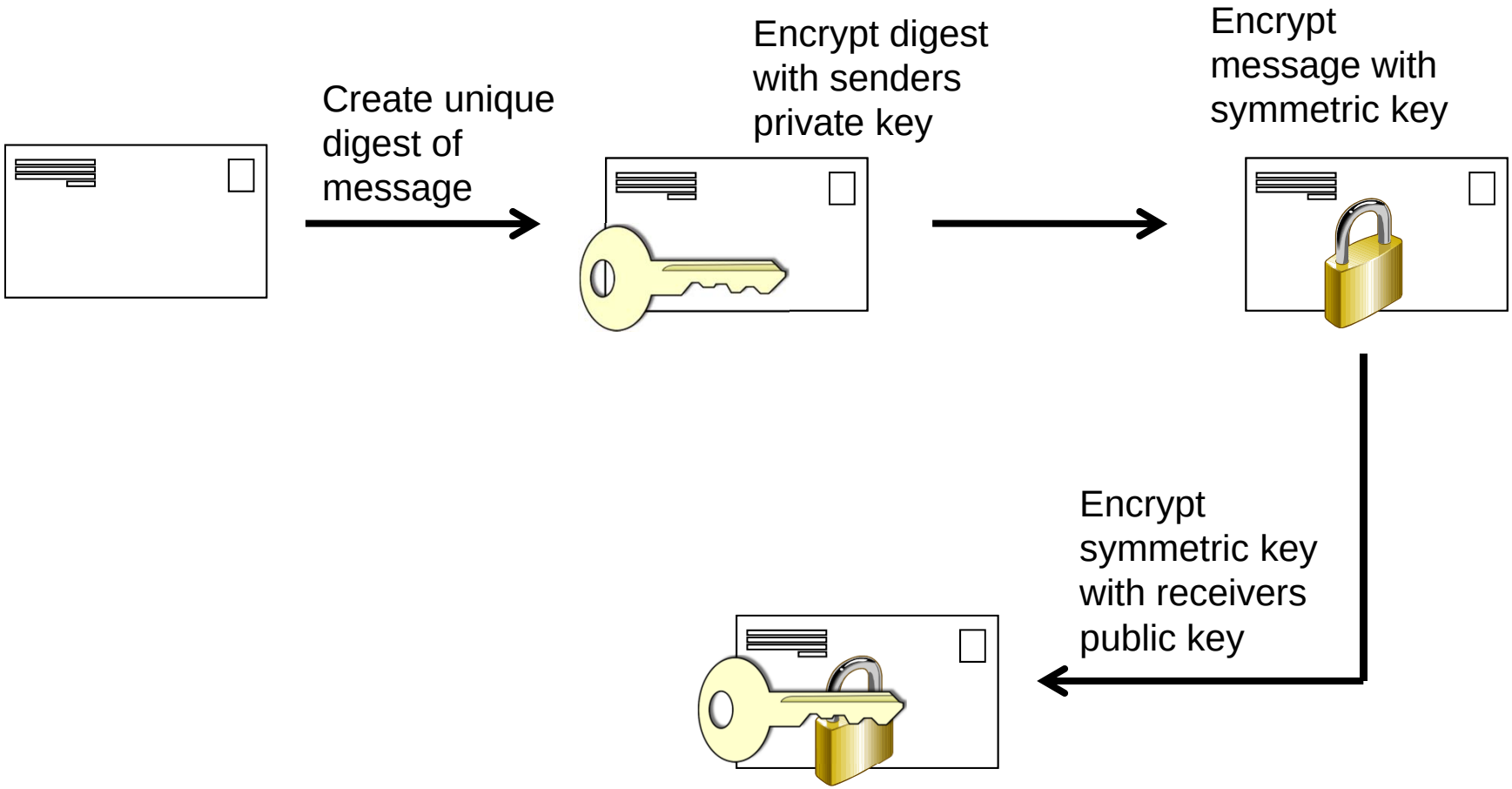
An X.509 certificate typically contains:

- Version
- Serial Number
- Signature
- Issuer name
- the validity time window
- a subject containing the owners identifying details
- statement.the purpose

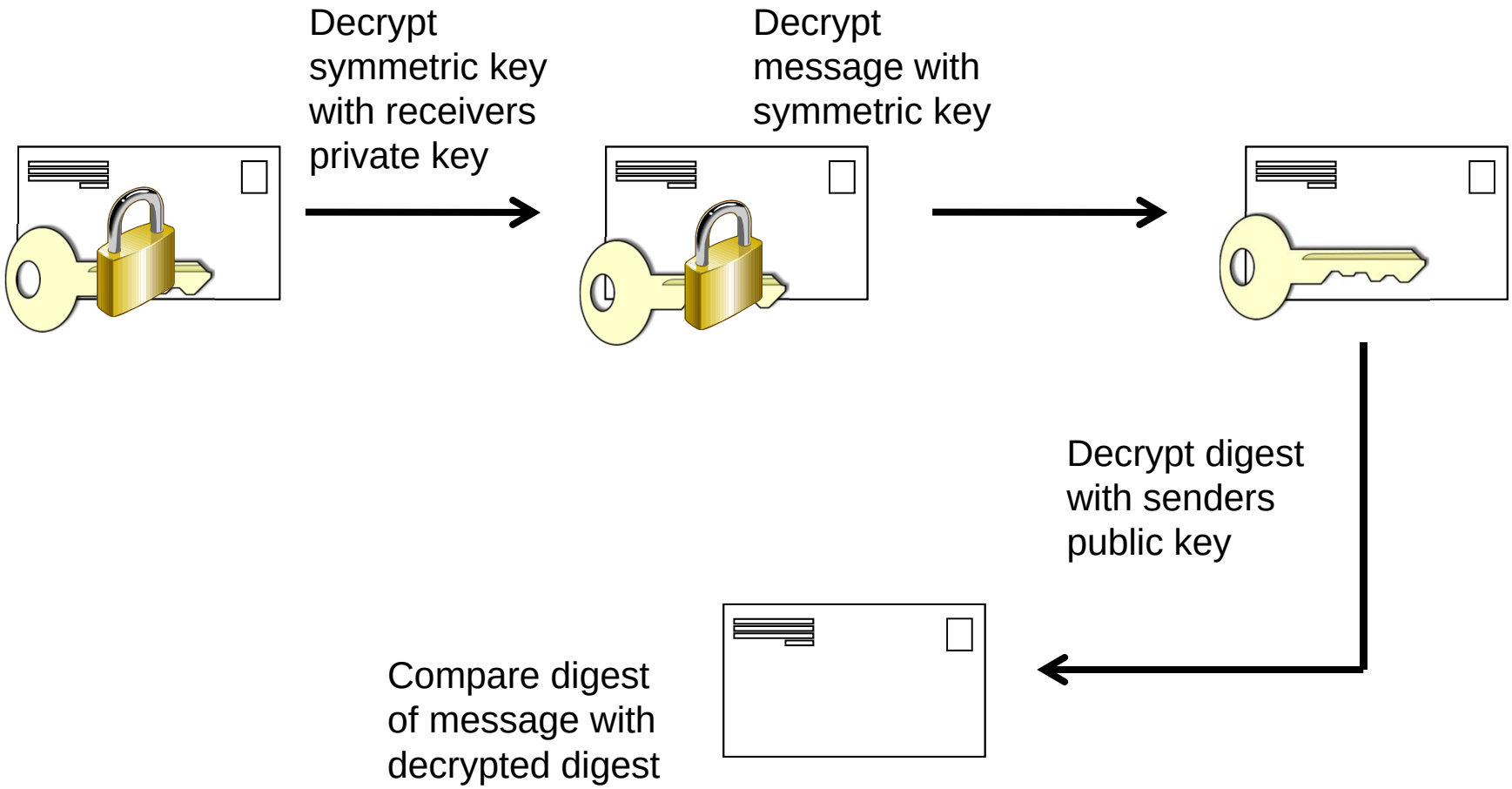
Digital Signatures

- Integrity
- Authenticity
- Non-repudiation of origin

Signing and Sending



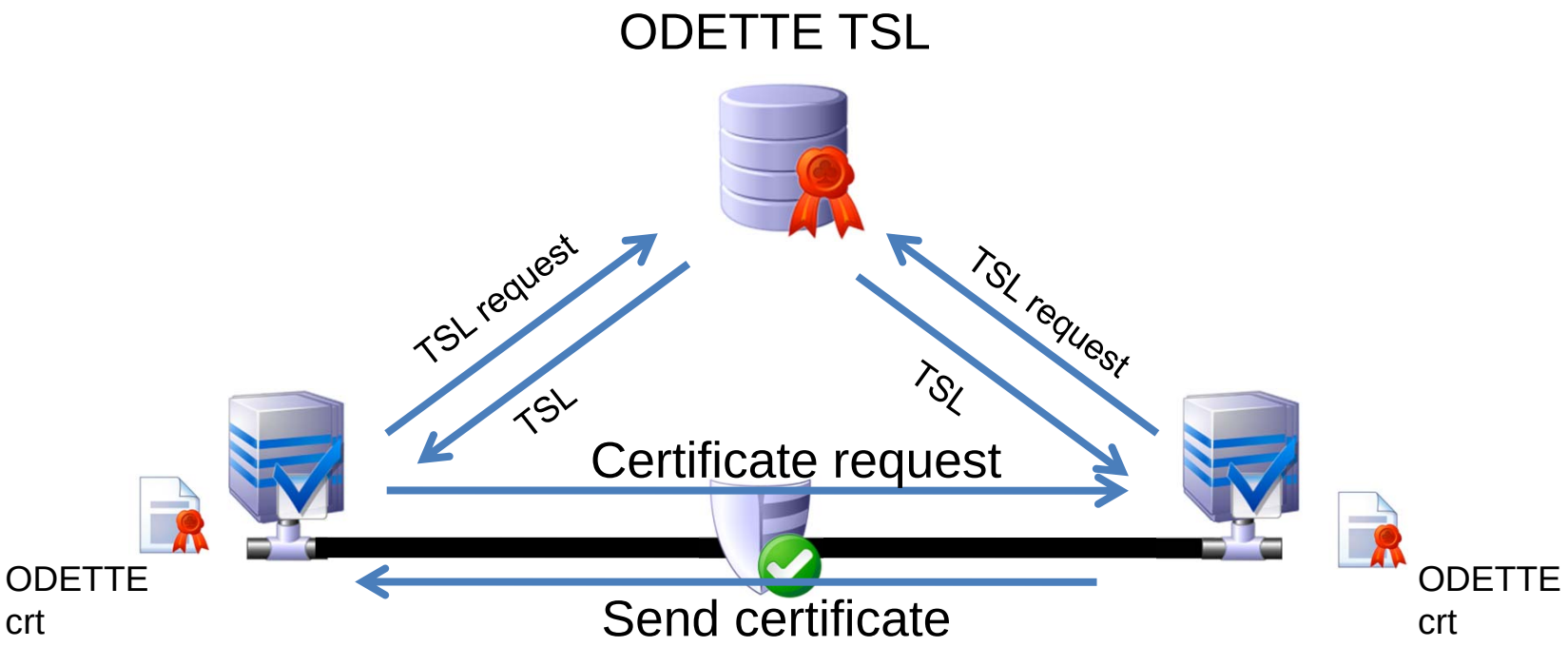
Decrypting and Verifying



ODETTE
SWEDEN

TSL och SSL

Odette – Trust Status signed List –TSL Administration



It needs to underline that this is an automated certificate administration procedure running in real-time. All approved certificates would have to be published as a TSL, else it will not work

ODETTE SWEDEN

The Odette SCX recommendation

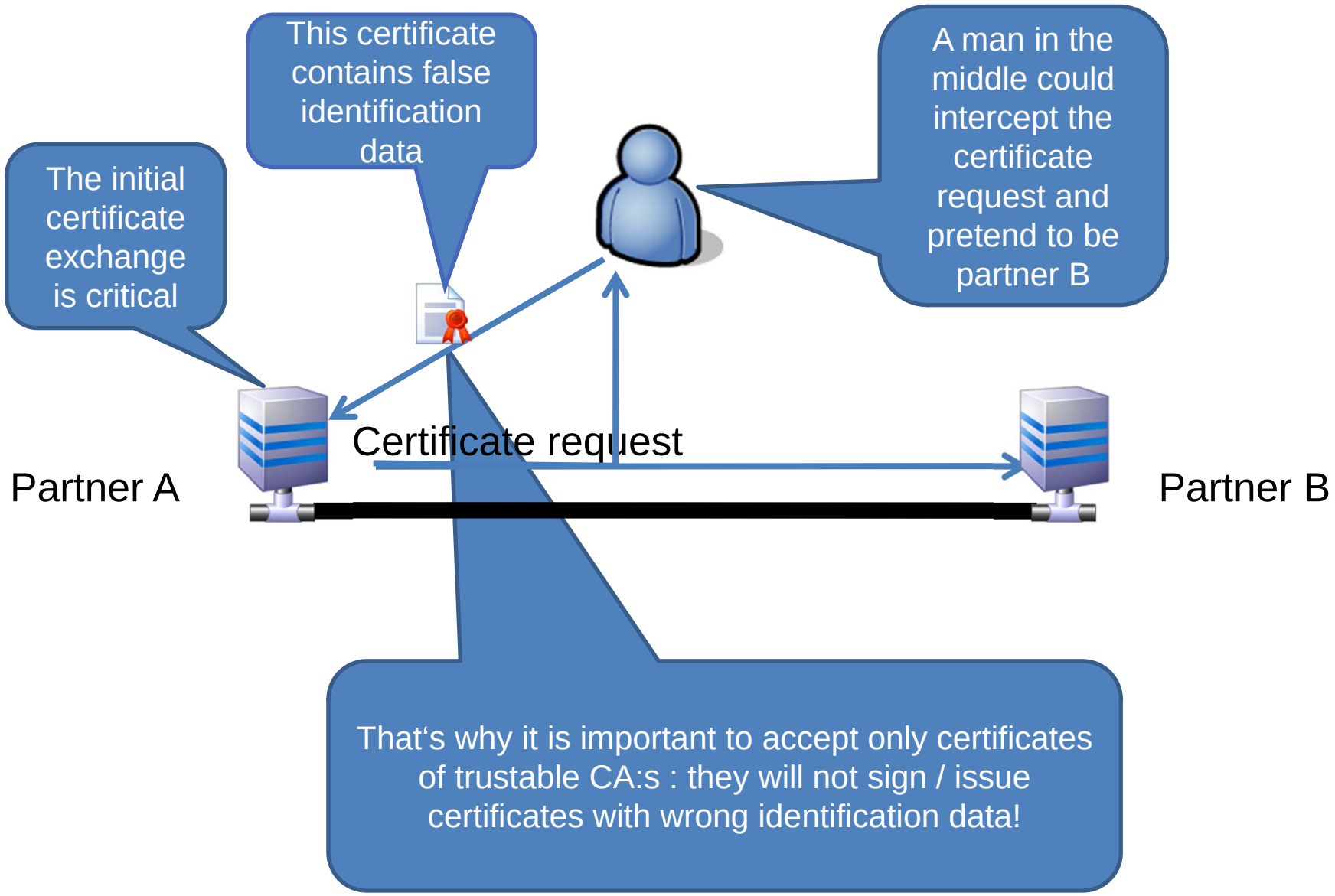
What is a TSL?

Trust Service Status Lists

- An ETSI standard using XML formatting
- Contains the list of the CA:s certificates recognised as “Trusty”, according to an agreed policy.
- The list is signed by a trusted authority (Odette)
- This list is used by the software to trust or reject automatically CA signed certificates

Several lists for different applications will be managed by Odette

TSL helps to prevent Man-in-the-middle Attacks



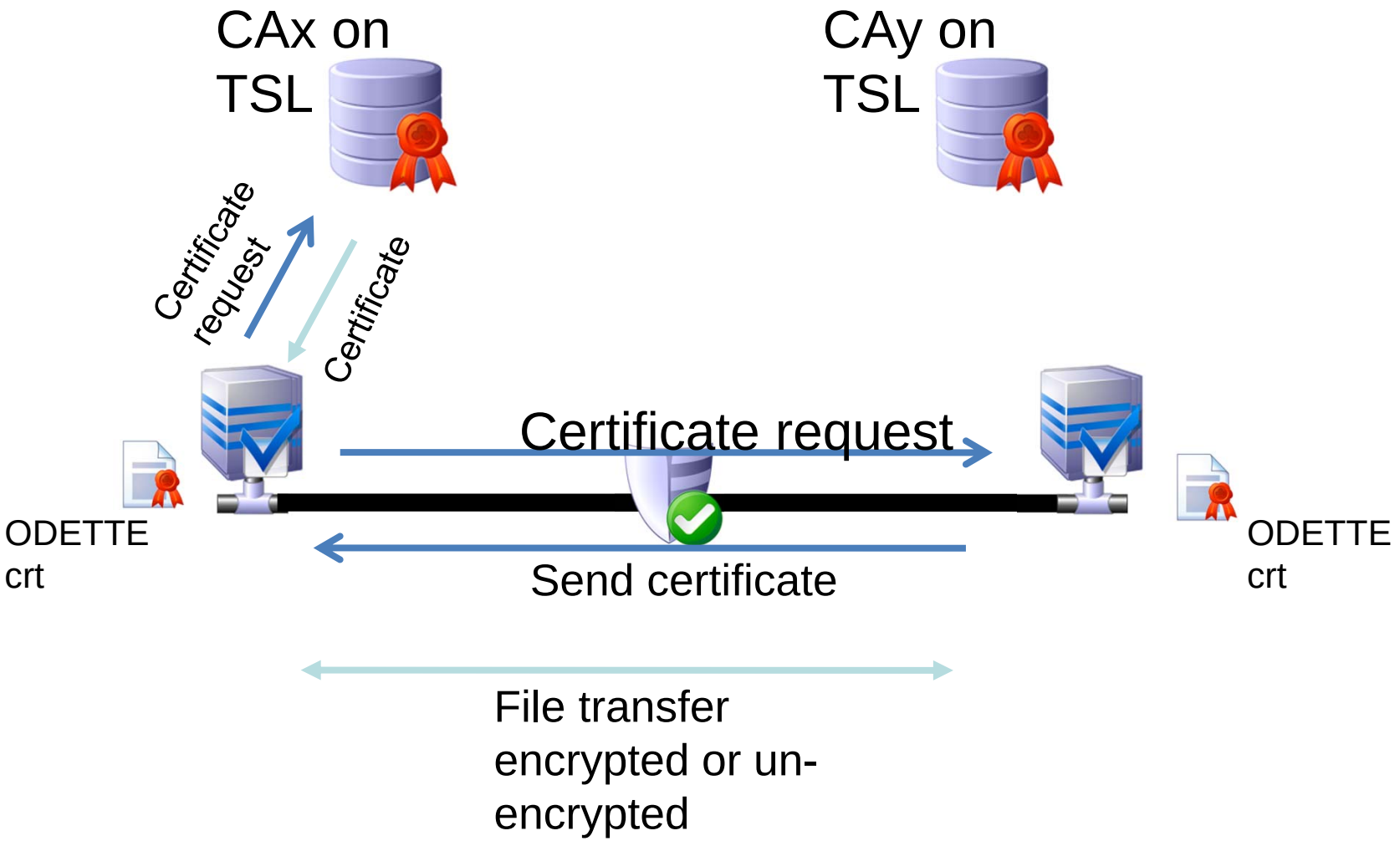
ODETTE SWEDEN

ODETTE
SWEDEN

Odette Recommendations and Services for Security

- Odette Security policy (Odette SCX)
- OFTP2 and handling of certificates
- Odette Services for handling of Security Certificate Exchange
- Ordering, installing and maintaining certificates
- Q & A

OFTP 2 – Certificate administration



Finally – a secure, trusted connection!

ODETTE SWEDEN

Managing Security by Odette SCX working group

- Security Certificate Exchange (SCX) Recommendation has been released
- Security certificates provide proof of identity of the partners, allow encryption / decryption / integrity-check of files and ensure non-repudiation of the data exchange.
- Trust Service Status Lists (TSL) will be established by Odette
- Odette is the trust guardian and provides this service to the automotive industry community
- TSL contains details of the trustable Security Certificate providers (CA:s)
- TSL is being published and updated on Internet and can be accessed by OFTP2 software easily

ODETTE
SWEDEN

Odettes Security Certificate Exchange (Odette SCX)

Secure Communications

Odette File Transfer Protocol Version 2

- Session security
- Secure authentication
- File encryption
- File signing

ODETTE SWEDEN

Security in use

Reduce costs!

- Low cost global network
- Secure use of Internet
- OFTP2

OFTP2 Certificate Policy Version 1.0

Certificate Usage:

OFTP2 application usage for encryption, authentication and integrity.

Certificate Requirements:

Types of certificates

- TLS:
  - One for session authentication and encryption
- OFTP protocol:
  - One for OFTP authentication (challenge encryption),
  - One for EERP signing,
- File security service (CMS):
  - One for file signature,
  - One for file encryption.

The Odette SCX recommendation

Targets for security certificates:

- Allow the **automatic** exchange and management of certificates,
- Use **industry standards**
- Find a solution which can be **implemented quickly** to facilitate introduction of **OFTP2**

ODETTE SWEDEN

Large scale deployment of certificates

Issues of scale:

- Several applications
  - **OFTP2**, e-mail, File encryption and signature, secure access to web server, AS2…
- All of them use **certificates**
- **Hundreds** of partners' certificates
- Signed by **dozen's of CA:s**

- **A mess of various CA:s and certificate in use**

ODETTE SWEDEN

The Challenge of Trust

- Technically, (nearly) all certificates implement the same standard technology
- Whether you trust them, depends on the issuing CA and how trustable the CA is
- With hundreds of CA‘s the assessment of trustability of each of them becomes a nightmare

The Odette SCX recommendation

What's a TSL?

Trust Service Status List

- An ETSI standard using XML syntax
- Contains the list of the issuing CA:s and their certificates, which are recognised as "trustable", according to an agreed policy.
- The list is signed by a trusted authority (Odette)
- This list is used by the software to trust or reject automatically CA signed certificates

Several lists for different applications will be managed by Odette

ODETTE
SWEDEN

TSL Snippet

```
- <TrustServiceProviderList>
  + <TrustServiceProvider>
  - <TrustServiceProvider>
    - <TSPInformation>
      - <TSPName>
          <Name xml:lang="en-GB">Belgacom</Name>
        </TSPName>
      - <TSPTradeName>
          <Name xml:lang="en-GB">Belgacom</Name>
        </TSPTradeName>
      - <TSPAddress>
        - <PostalAddresses>
          - <PostalAddress xml:lang="en-GB">
              <StreetAddress>Boulevard du Roi Albert II, 2</StreetAddress>
              <Locality>Brussels</Locality>
              <PostalCode>1030</PostalCode>
              <CountryName>BE</CountryName>
            </PostalAddress>
          </PostalAddresses>
        - <ElectronicAddress>
            <URI>http://www.belgacom.com</URI>
          </ElectronicAddress>
        </TSPAddress>
      - <TSPInformationURI>
          <URI xml:lang="en-GB">http://www.belgacom.com/ca</URI>
        </TSPInformationURI>
      </TSPInformation>
    + <TSPServices>
```

Current Types of Trust Service-status Lists (TSL)

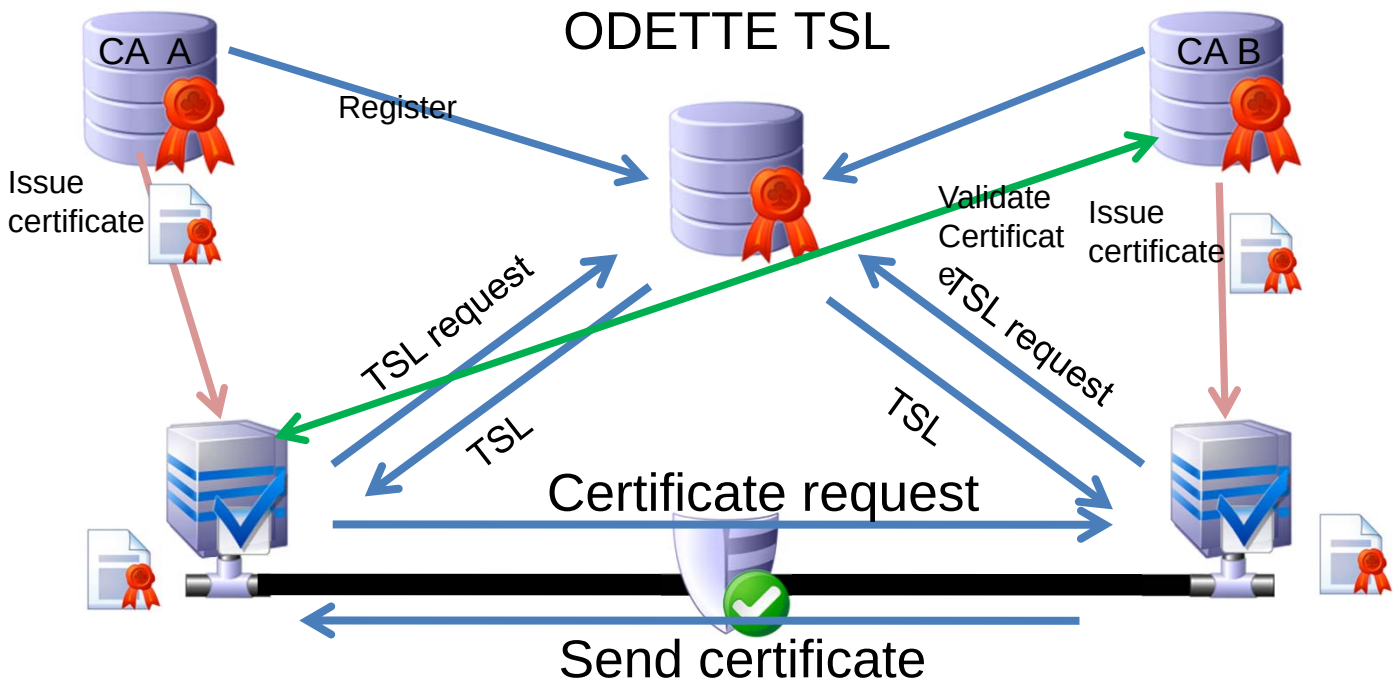
BASIC

- Odette performs an identity check of the CA owner for all CA:s on TSL Basic

OFTP2

- Additional restrictions apply: only CA:s that issue certificates usable for OFTP2 data exchange are listed (i.e. they comply to a certificate policy)
- Pre-requisit: CA:s must be registered on TSL Basic

Odette – Trust Status Service List –TSL Administration



Finally – a secure, trusted connection!

ODETTE SWEDEN

ODETTE
SWEDEN

OFTP2 and the exchange of security certificates

Odette Services

The role of Odette as a Trust Centre

- This function is realised by the Odette community, i.e the Central Office and the National Organisations
- Odette has close links to the industry in our countries and can make sure the system is facilitated and maintained to fit exactly to the needs of the automotive supply chain.
- Odette is a non-profit organisation and provides the service to members free of charge

ODETTE SWEDEN

The role of Odette

- Distribute the certificate policy associated with the TSL to CA organisations
- Collect their commitment
- Build the TSL with the certificates of those who accept the policy
- Verification:
  - The commitment of a CA is made on a volunteer basis, by self-assessment
  - If a CA's policy becomes incompatible with the TSL policy, this CA will finally be discarded.

OFTP2 documents review - SCX recommendations

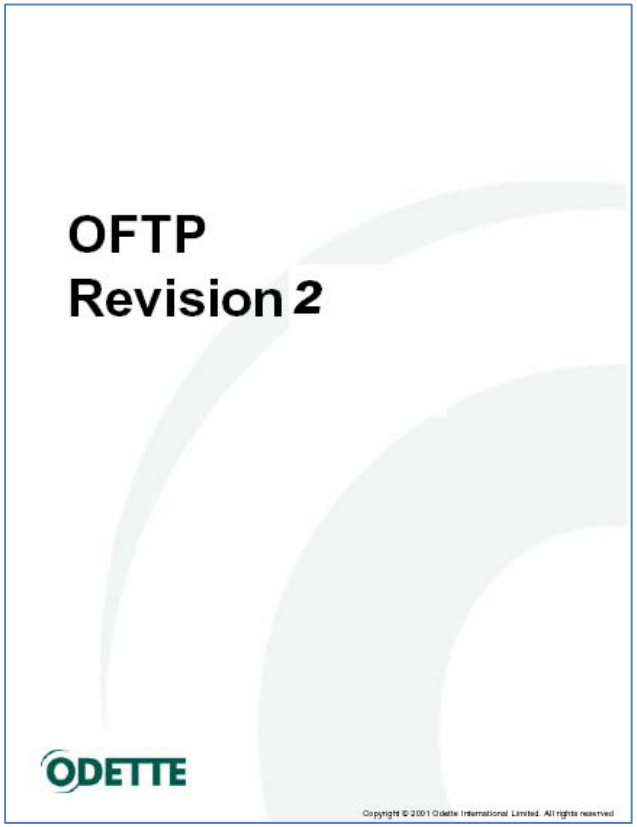
Prerequisites to add a CA to the ODETTE TSL

- Odette must check that the CA exists as a legal entity – e.g. by requiring a copy of the company registration form
- A responsible person of that company must sign a document stating that she/he is responsible for the PKI of that company or branch
- The PKI system belongs to the identified legal entity
- The company adheres to the requirements stated in the policy document
- The company accepts the terms and conditions of the TSL service provided by Odette International

Terms & Conditions exclude claims and warranties for ODETTE and the CA

ODETTE SWEDEN

Overview of OFTP



Start session components

Initiator/Responder

The entity that took initiative to establish the network connection becomes the INITIATOR. The other is called the RESPONDER.

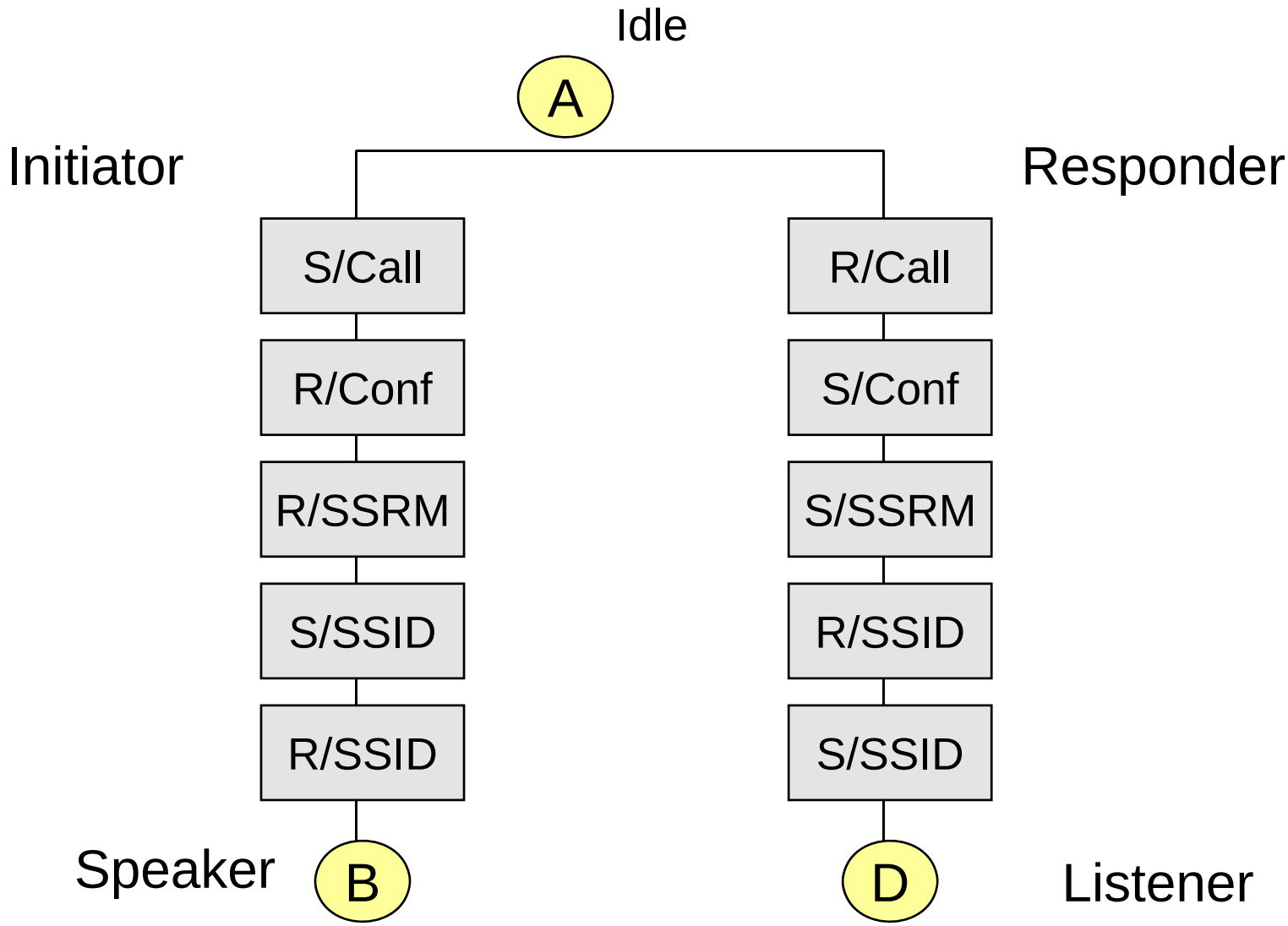
Speaker/Listener

The entity of SPEAKER or LISTENER is the result of the Start Session phase, where the INITIATOR becomes the first SPEAKER or as a result of a change direction request./listener

Protocol

After the Start File phase, data will flow from speaker (sender) to listener (receiver). The speaker has not the right to send data unless he has the permission of the listener. Sending more data than allowed (by the listener) will result in protocol error and leads to an abort.

Initiator and Responder diagram



OFTP commands

Commands and data are not mixed in the DATA EXCHANGE BUFFER.

A command start at the beginning of the buffer.

Command identifier: The command identifier is a single octet (see hereafter).

Parameter(s): There may be as many parameters as needed, but:

- predefined order (sequence as they are specified in the TABLE hereafter)
- positional
- required (no default value)

Initiator:

X SSID Identification Password & Profile

Responder:

I SSRM Ready message
X SSID Identification Password & Profile

ODETTE SWEDEN

Speaker:

F	ESID	End of Session (normal)
H	SFID	Send File Information
T	EFID	End of File Information
E	EERP	End to End Response
N	NERP	Negative End to End Response
R	CD	Change direction
D	DATA	Data

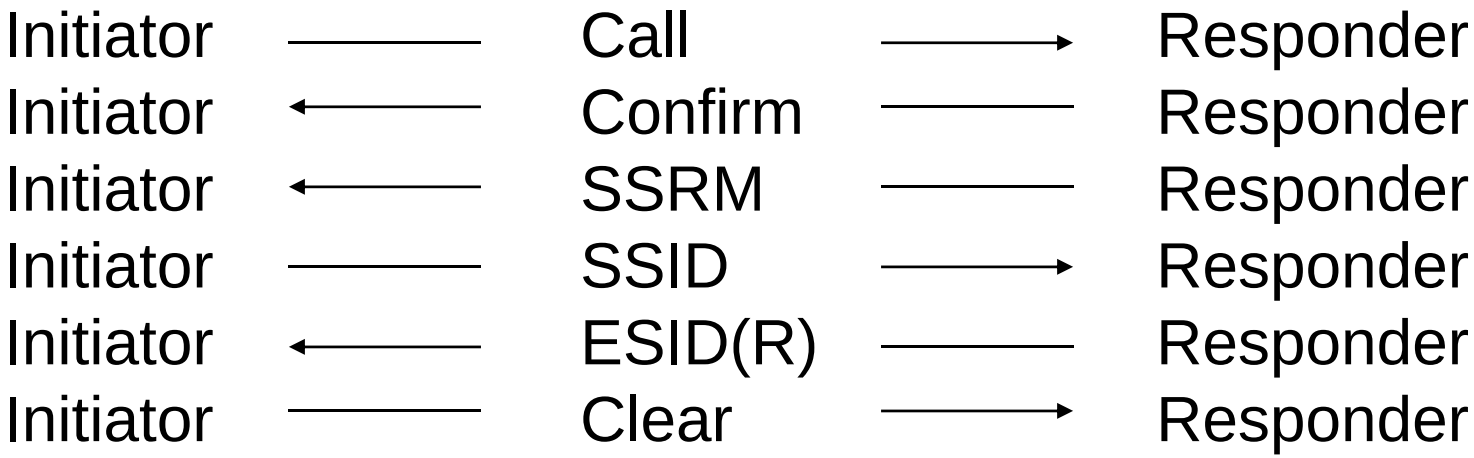
Listener:

F	ESID	End of Session (error)
2	SFPA	Send File Positive Answer
3	SFNA	Send File Negative Answer
4	EFPA	End of File Positive Answer
5	EFNA	End of File Negative Answer
C	CDT	Set Credit
P	RTR	Ready to Receive

Session Control: Start session

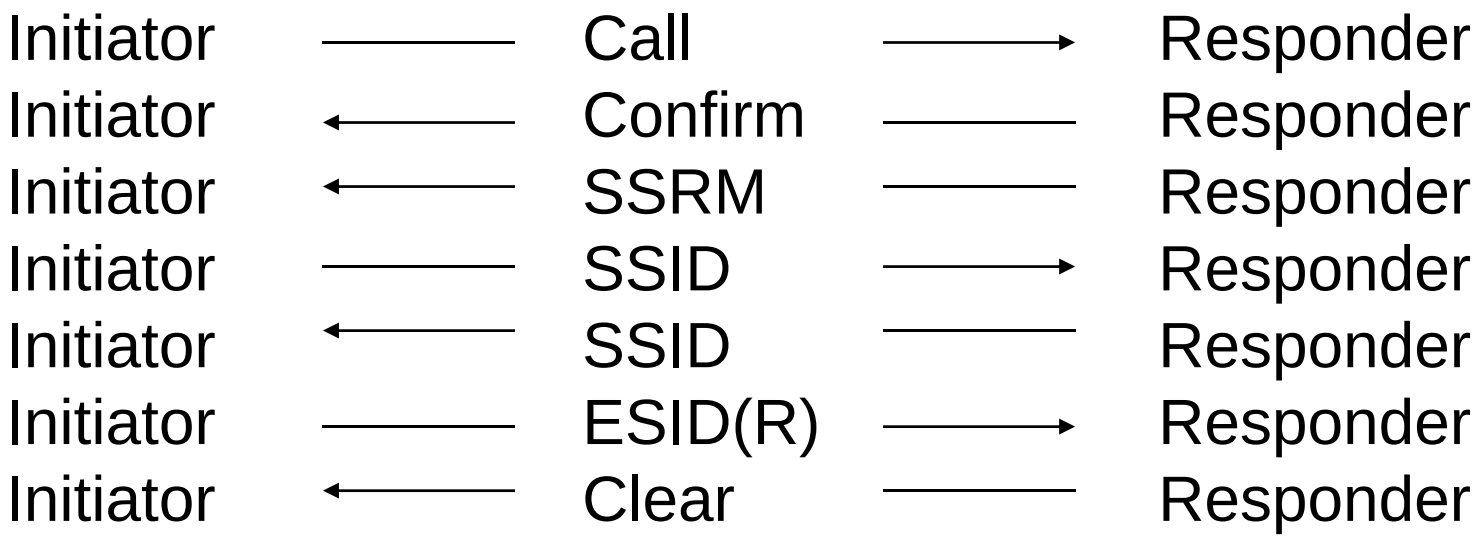
Start session (alt 1):

Start session (alt 2):

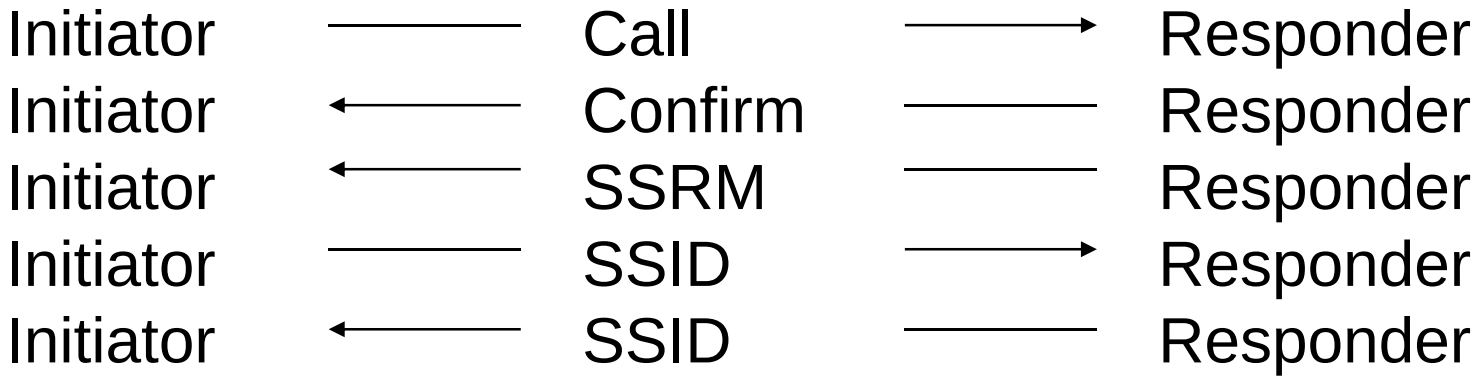


ODETTE SWEDEN

Start session (alt 3):



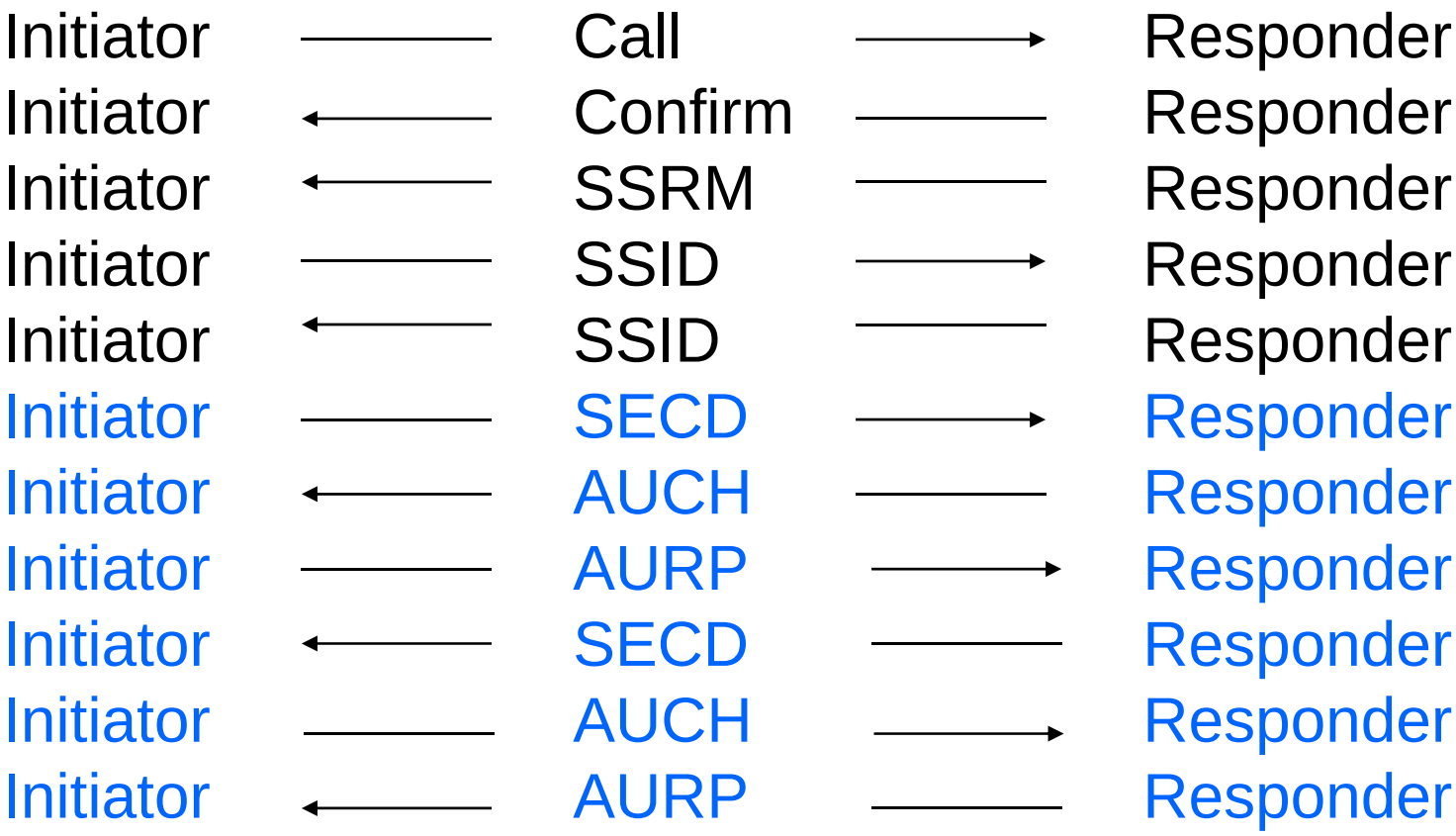
Start session (alt 4 V 1.4):



ODETTE SWEDEN

New

Start session (alt 5 V 2.0):



ODETTE SWEDEN

Session Control: Session established

Initiator remains Speaker
Responder remains Listener

Speaker could send either of the following:

SFID	Send file identification
EERP	End to End response
CD	Change Direction
NERP	Negative end response
AUCH	Authentication Challange
SECD	Security Change Direction
AURP	Authentication Respons

SSRM Ready Message

Command	I
Message	ODETTE FTP READY Carriage Return

SSID Identification & Password

Command	X
Version	Protocol (version) release level (1, 2,4,5)
Code	OFTP code
Password	
Buffer Size	min 128 characters
Snd/Rcv	(S)end only, (R)eceive only, (B)oth
Compression	Y/N
Restart	Y/N
Special logic	Y/N (Not used in V 2.0)
Buffer credit	min 1
Secure Authentication (Y/N)	
User data	
Carriage Return	

OFTP code: Unique identification of an OFTP-system

It identifies in a unique way the Initiator (sender) and the Responder (receiver)

Odette identifier	1	O
ICD	4	International Code Designator, ISO, identifies the coding system
Organisation	14	Organisation Identifier, identifies the owner
Sub-Address	6	Owners system under responsibility of the company

ODETTE SWEDEN

ICD coding scheme

International Code Designator 0001

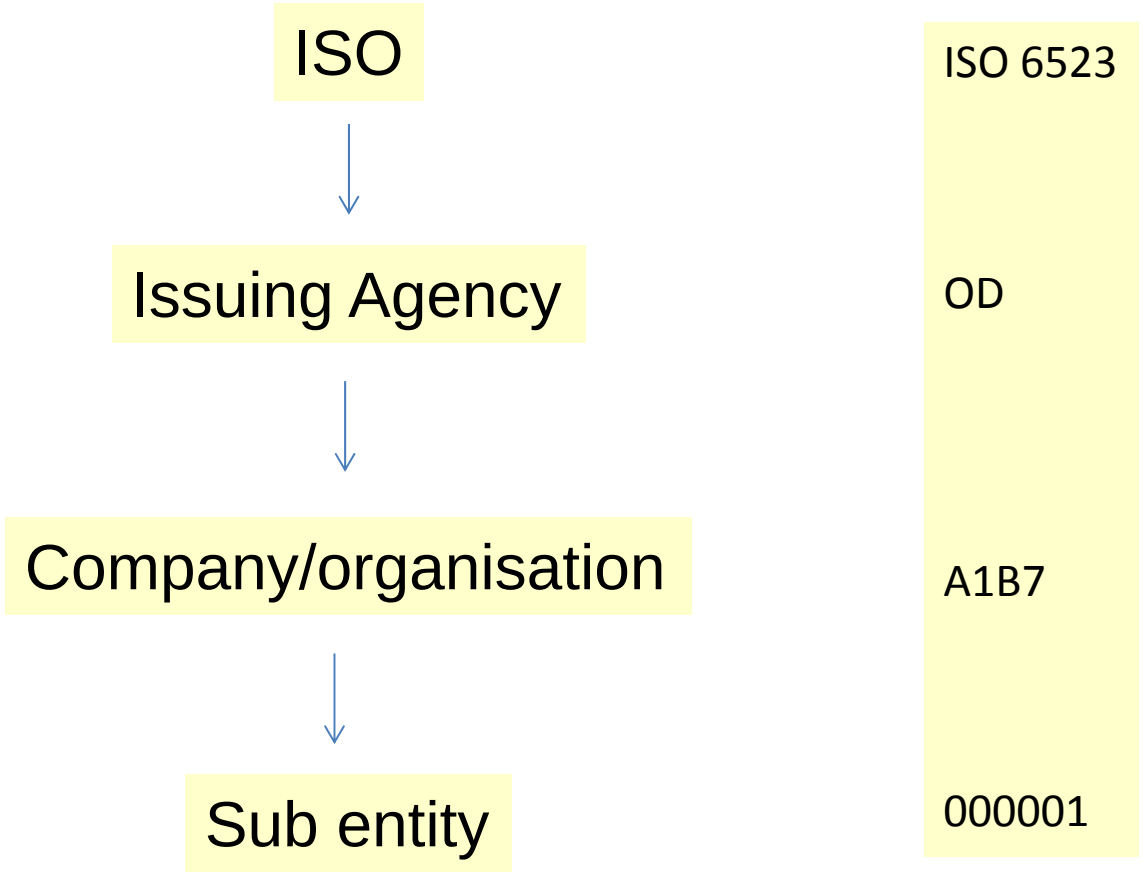
ICD :	0001
Name of Coding System :	(Not Assigned)
Intended Purpose/App. Area	
Issuing Organization :	
Structure of Code :	
Display Requirements :	
Character Repertoire :	
Language(s) Used :	
Supports Org. Parts? :	
Org. Identifier Reuse :	
Orgs Covered by System :	
Notes on Use of Code :	
Alt. Names for Scheme :	
Sponsoring Authority :	
Date of Issue of ICD :	
Additional Comments :	

Registration Authority
c/o RA
British Standards Institution
389 Chiswick High Road
GB-London W4 4AL
United Kingdom
Tel: +44 20 89 96 71 65
Fax: +44 20 89 96 71 98
E-mail: telecoms@bsigroup.com

The codification rules recommended in ODDC020 are based on the ISO standard 6523 : Data Interchange - Structure for the identification of Organisations.

This unique identification of a party codification system is named **ICD** (International code designator) and is allocated by the BSI on behalf of ISO.

ICD coding scheme – basic principles



ODETTE
SWEDEN

International Code Designator 0007

ICD :	**0007**
Name of Coding System :	Organisationsnummer
Intended Purpose/App. Area	
Issuing Organization :	The National Tax Board, (Riksskatteverket, RSV), 171 94 SOLNA, SWEDEN, Tel: 08 981520
Structure of Code :	1) 10 digits. 1st digit = Group number, 2nd - 9th digit = Ordinalnumber1st digit, = Group number, 10th digit = Check digit, 2) Last digit.
Display Requirements :	Single group of 10 digits.
Character Repertoire :	
Language(s) Used :	
Supports Org. Parts? :	
Org. Identifier Reuse :	
Orgs Covered by System :	All persons registered in Sweden for tax purposes.
Notes on Use of Code :	The third digit in the organisation number is never lower than 2 in order to avoid it being confused with personal numbers.
Alt. Names for Scheme :	
Sponsoring Authority :	Organization for Data Exchange by Tele Transmission in Europe: ODETTE
Date of Issue of ICD :	Nov 1986
Additional Comments :	

ICD coding scheme: code examples

0942	Svenskt organisationsnummer
0060	Dun & Bradstreet
0177	Odette International (OSCAR)

OFTP code: Example

O 0942 0000 4203075710 000RVD

0942	Code identifying the Swedish National Tax Board
0000	Non-significant characters
420375710	”Organisationsnummer”, Company registration and VAT nr
000RVD	In-house code
0177	Odette (next slide)

Other European examples:

O001300005560GERMANY
O0931000091823445525155 1
O093200000000341001AND001

The Possible Use of OSCAR Codes

OFTP (25 characters)																									
O	0	1	7	7	0	0	0	0	0	0	0	0	0	0	7	5	1	1	V	E	G	A	0	1
For OFTP (1)	ICD (4)				main OFTP code from Odette register (14)														sub-address (6)					

EDI (variable)																				
	0	1	7	7	0	0	0	0	0	7	5	1	1	V	E	G	A	1		
	ICD (4)				Code from Odette register (9)									sub-address (5)						

PID (19 char)																					
	0	1	7	7	0	0	0	0	0	7	5	1	1	V	E	G	A	1	9		
	ICD (4)				Code from Odette register (9)									sub-address (5)					Origin Code (1)		

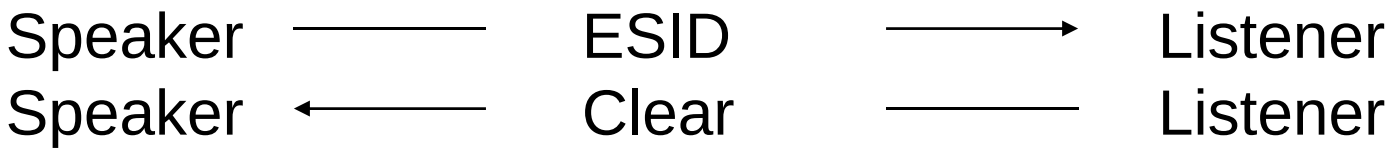
SECD	Security Change Direction
Command	J

AUCH	Authentication Challenge
Command	A
Challenge	A 20 Byte random no uniquely Generated each time an AUCH is sent.

AURP	Authentication Response
Command	S
Signed Challenge	The length of the signed challenge
Signed Challenge	The Challenge from AUCH signed with the Private key encoded into a CMS message.

	After negotiation
Version	Lowest
Buffer size	Lowest
Buffer credit	Lowest
Send/Receive	Could be incompatible
Compression	If one location = N no compressed data
Restart	If one location = N no restart
Secure Authent	No negotiation is allowed

Session termination



ESID End of Session

Command	F
Reason code	Reason code nr
Reason text Length	Max 999
Reason text	UTF-8
	(Carriage Return)

ODETTE SWEDEN

ESID Reason codes

00	Normal termination
01	Command not recognised
02	Protocol violation
03	User code not known
04	Invalid password
05	Local site emergency closedown
06	Command contained invalid data
07	NSDU size error
08	Resources not available
09	Time out
10	Mode or capabilities incompatible
11	**Invalid Challenge response**
12	**Secure Authentication incompatible**
99	Unspecified abort code

File Control

File transfer initiation (alt 1):

Speaker could send either of:

EFID
DATA

File Control

File transfer initiation (alt 2):

Speaker could send anyone of :

SFID (not the same file!)
EERP
CD

SFID Send File

Command	H
Filename	Bilateral agreement
Date	YYMMDD
Timestamp	*See next slide*
User data	Not used
Destination	OFTP code
Origin	OFTP code
File format	F/V/U/T
Max rec. size	Specifies the max record File format = T/U (0)
File size	Amount of space at the origin. for the virtual file
Restart pos	Before compression
Original file size	Before compression max 9,3 PB (9 300 000 000 000 000 byte)
Security Level	00=No security Values 00,01,02,03
Cipher suite	00=No
Compression	0=No , 1 = Comp with ZLIB
File Envelope	0=No , 1 Enveloping using CMS
Signed EERP	N,Y
VFN descr Len	Virtual File description length 0 = no Description
VFN Description	Plain text in UTF-8

ODETTE SWEDEN

Timestamp

This is the time when a file is made available for transmission at the sender's location. The DATE and TIME stamps are assigned by the file originator and have only local significance. They should not be changed by any clearing centre.

REFERENCE: ISO 3307.
The first 2 digits (starting from the left) define the hours.
The 2nd 2 digits represent the minutes.
The 3rd 2 digits define the seconds.
The last 4 digits is a counter (0001-9999), which gives higher resolution.

ODETTE SWEDEN

SFPA Send File Positive

Command	2
Answer count	Restart
	Lower or equal to SFID restart

SFNA Send File Negative

Command	3
Answer reason	As in list of arguments
Retry	Y/N
	Y retry later
	N the file should not be sent
Answer reason	Answer reason text length
Answer reason	Answer reason text

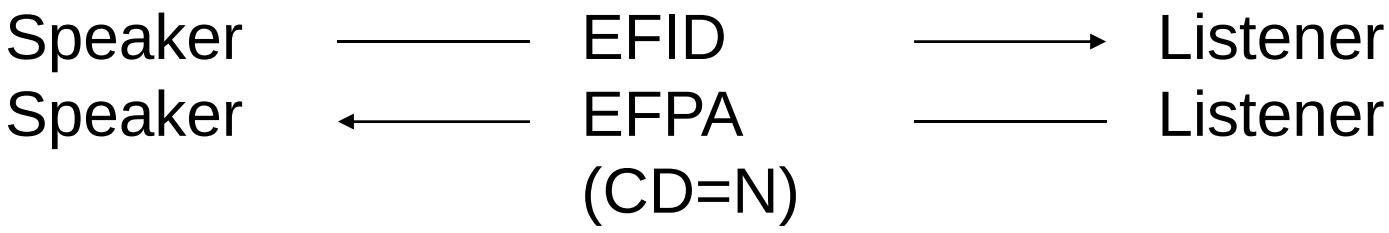
ODETTE SWEDEN

SFNA/EFNA Answer reasons

01	Invalid filename
02	Invalid destination
03	Invalid origin
04	Storage record format not supported
05	Maximum record length not supported
06	File size too big
10	Invalid record count
11	Invalid byte count
12	Access method failure
13	Duplicate file
14	File direction refused
15	Cipher suite not supported
16	Encrypted file not allowed
17	Unencrypted file not allowed
18	Compression not allowed
19	Signed file not allowed
20	Unsigned file not allowed
99	Unspecified reason

File transfer termination

File transfer termination (alt 1):

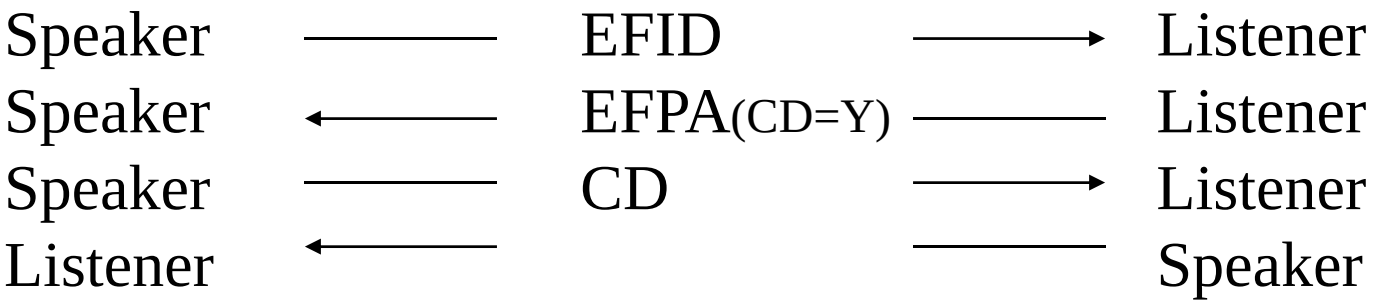


Speaker could send any of:

SFID
NERP
EERP
CD

File transfer termination

File transfer termination (alt 2):



Speaker could send:

SFID
NERP
EERP
CD might not be sent in this alternative!

File transfer termination

File transfer termination (alt 3):

Speaker could send any of:

SFID
NERP
EERP
CD

ODETTE SWEDEN

EFID End of File

Command	T
Record count	F/V or 0
Byte count	F/V/U/T
	Before compression
Unit count	No of octets sent

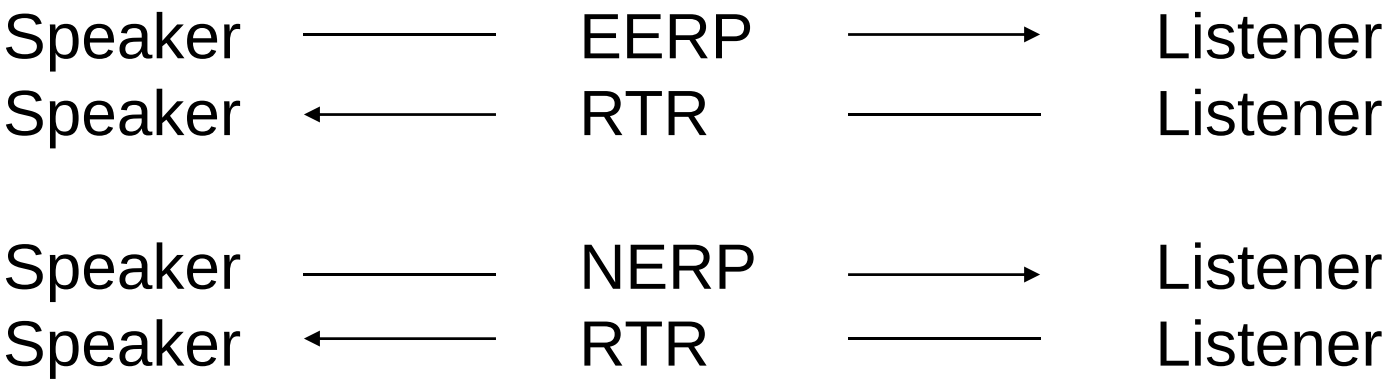
EFPA End of File Positive

Command	4
Change direct.	Y/N
	Request to become speaker

EFNA End of File Negative

Command	5
Answer reason	As in list of arguments

End to End Control



Speaker could send any of:

SFID
NERP
EERP
CD

NERP*	Negative End Response
Command	N
Filename	Bilateral agreement
Date	YYMMDD
Timestamp	Se slide ”Timestamp”
User data	Not used
Destination	OFTP code
Origin	OFTP code
Creator of NERP	
Reason code	See ESID/EFNA Code
Reason text length	max 999
Reason text	Text UTF-8
VF Hash Len	Virtual file hash length
VF Hash	Virtual file hash
NERP Len	NERP Signature length
NERP Sign	NERP signature

* New from version 1.4

EERP	End to End Response
Command	E
Filename	Bilateral agreement
Date	YYMMDD
Timestamp	Se slide ”Timestamp”
User data	Not used
Destination	OFTP code
Origin	OFTP code
Reason code	See ESID/EFNA Code
Reason text length	max 999
Reason text	Text UTF-8
VF Hash Len	Virtual file hash length
VF Hash	Virtual file hash
EERP Len	EERP Signature length
EERP Sign	EERP signature

RTR	Ready to Receive
Command	P

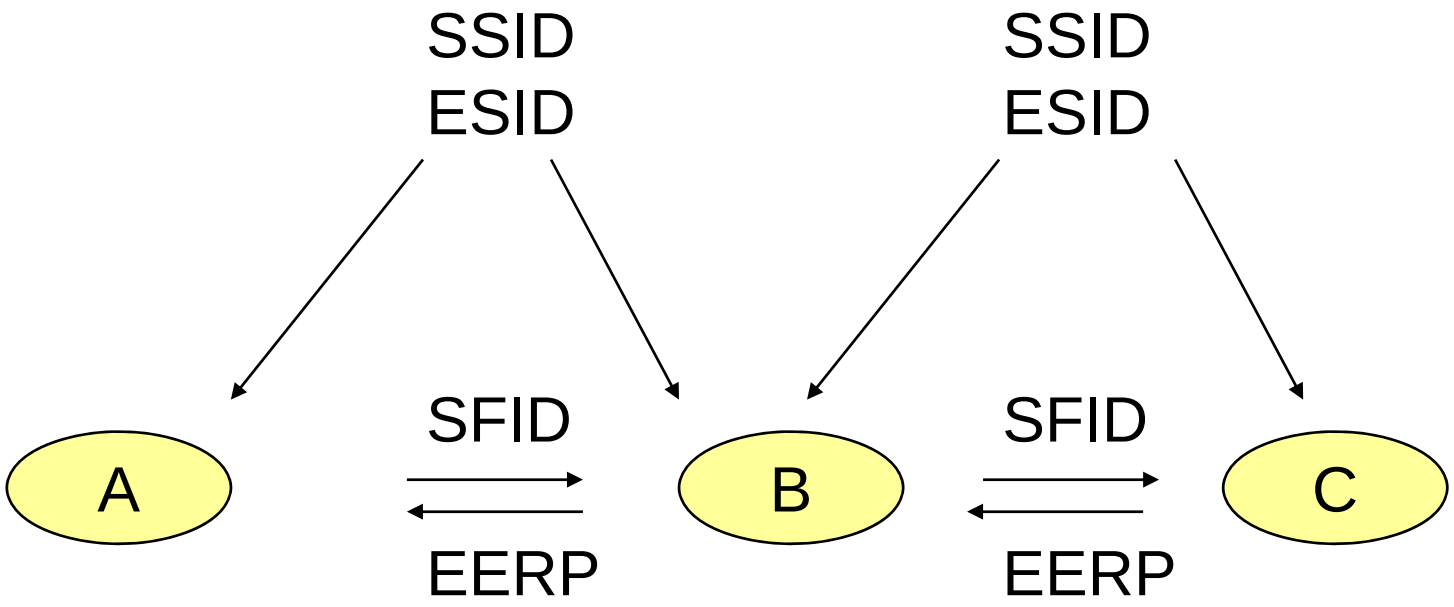
EERP/NERP

EERP/NERP is a ”mirror” of SFID

Is used to control a route and is normally interpreted as a handover confirmation

RTR is used solely to prevent from an uncontrolled flow of EERP

Routing



Origin	A	Origin	A	Origin	A
Destination	C	Destination	C	Destination	C
Filename		Filename		Filename	
Date		Date		Date	
Time		Time		Time	

Routing

If C asks A to connect to B, who addresses C, A must be able to handle this

If A asks C to get his files via B with origin A, C must be able to handle this

All OFTP systems must in SFID/NERP/EERP be able to

- Give another destination
- Receive another origin

than the one you are connected to in a session

ODETTE SWEDEN

Virtual File

File organization : Sequential

File identity: File name + date/timestamp identifies uniquely

Record format:

F (Fixed): Each record in the file has the same length.
V (Variable): The records in the file can have a different length.
U (Unstructured) Character stream of data, no structure
T (Text File): A sequence of ASCII characters, no transparent data

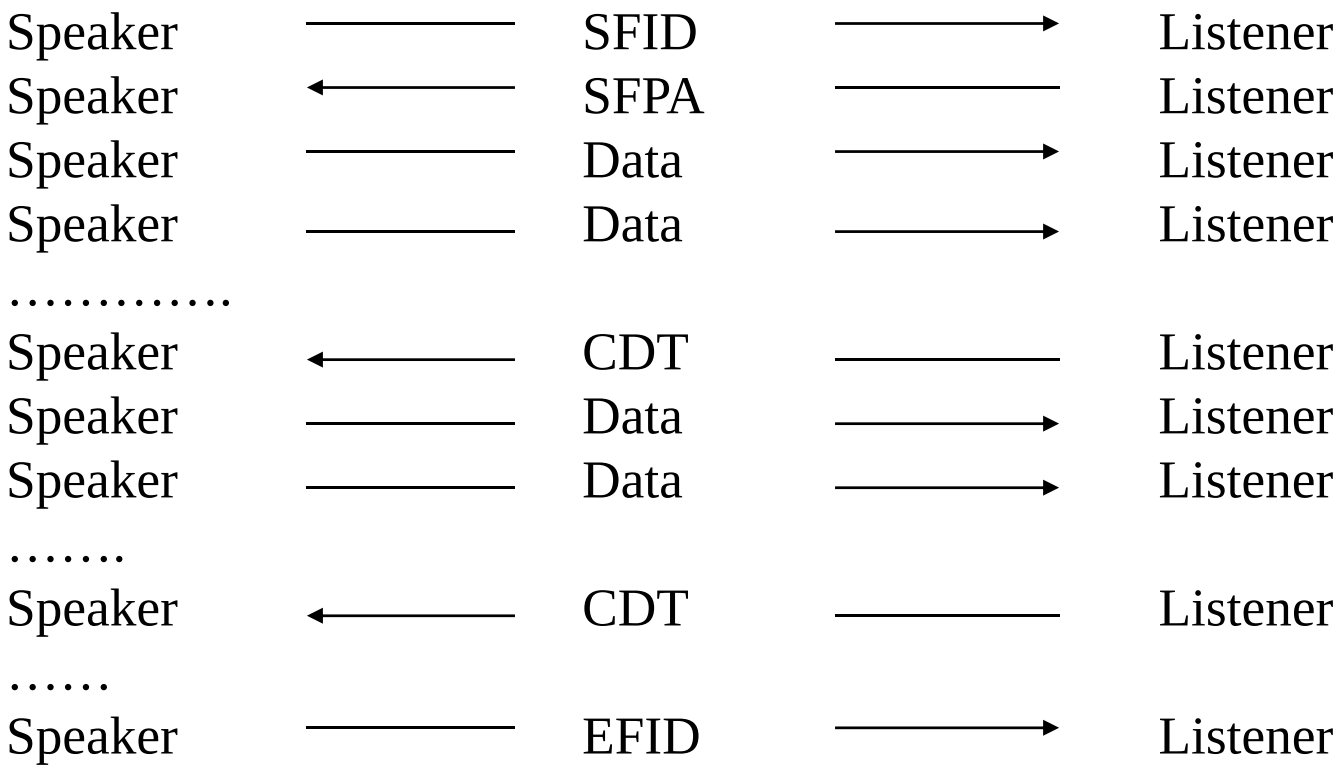
Data Exchange Buffer

Number of bytes in each packet
It will effect the communication speed

Higher value equals higher speed up to 25 K maximum limit (OFTP V1)

The max limit is 65 K for OFTP2

Data flow control



Listener could send any of:

EFPA
EFNA

DATA	Data Flow
Command	D
Data	Data
CDT	Set Credit
Command	C

The number of Data Exchange Buffers that the speaker is allowed to send is negotiated in the Start Session phase

The Listener gives the Speaker permission to send more data (or EFID) by sending CDT.

Terminology: Communications Agreement

Term	Definition
SSID	EDI Code Sender/Receiver
Physical Adress	EDI Code Sender/Receiver
EDI Code	EDI Code Sender/Receiver
Network adress	X.25/ISDN Number/DNS-adress (from Network Service Order)
NUA	X.25/ISDN Number/DNS-adress (from Network Service Order)
Password	Password from/to Partner
Network service	Type of service e.g X.25/ Internet
Port	Assign logical port according to choice of communication channel
Certificate	TLS management

Terminology: Applications Agreement

Term	Definition
Logical address	UNB code in message UNB.0004/0010
Qualifier	Define UNB code usage
Sub-address	Internal address at sender/receiver
Code representation	Character set, eg ascii,ebcdic
Message version *	Version of message
Message type	Type of message
File format	Format of the file, eg F/80 unspecified file length
Virtual file name	Name of the file during the file transfer
Authentication	Certificate for identification
Confidentiality	Certificate for encryption of file

* Next slide

Identification of message versions (profiles) in DE 0057

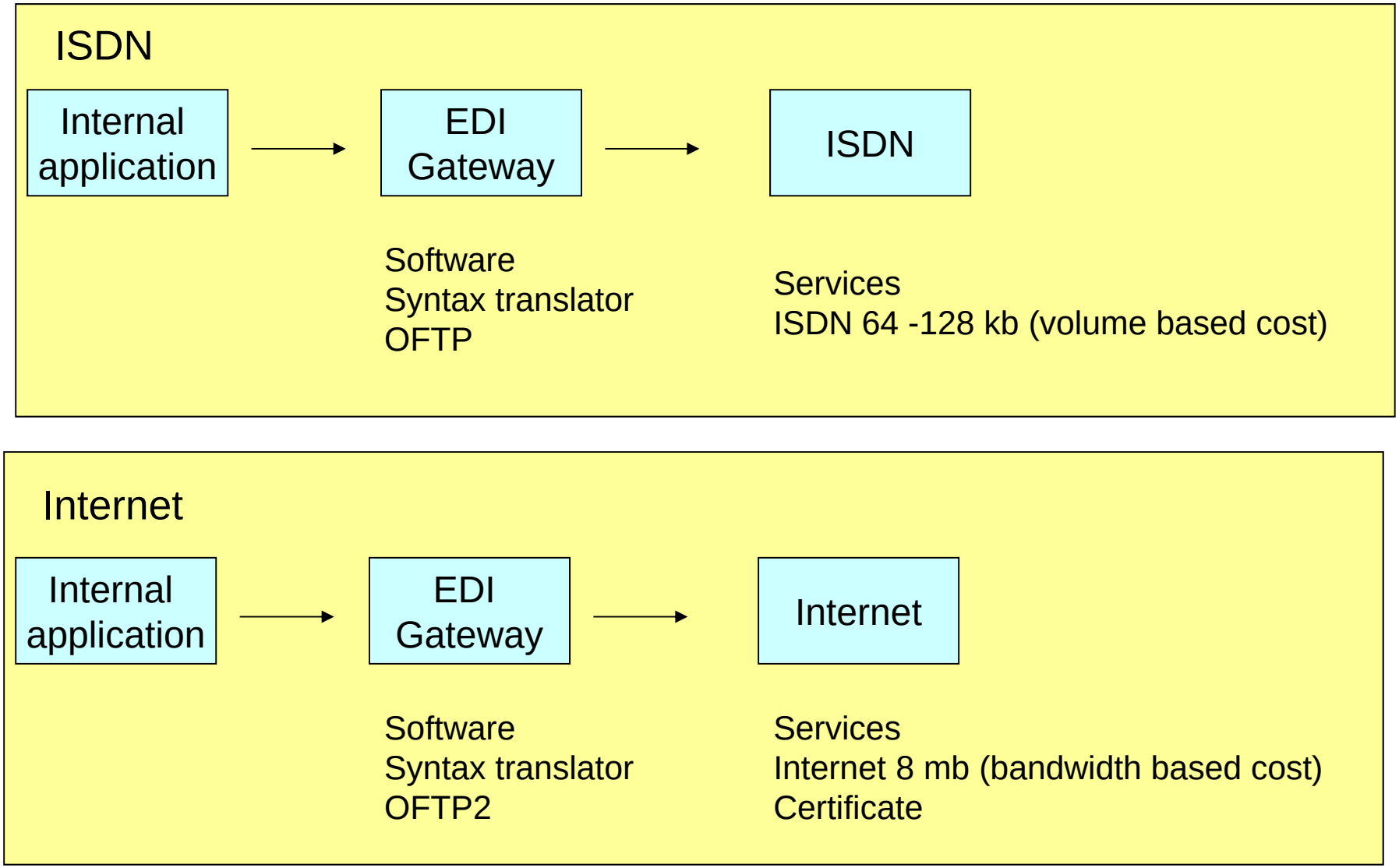
Character 1: G (Global Automotive EDI message)
Character 2: X (Regional Automotive organisation)
Characters 3 - 4: XX (Regional Subset/Profile identifier)
Character 5: X (Regional Subset/Profile Version number)
Character 6: X (Regional Subset/Profile Release number)
Initial Code Values for Character 2:

JAI	A
Odette International	B
AIAG	C
JAMA	D
SASIG	G

Odette Sweden Subsets/Profiles = S1 – S9, SA – SZ, examples:

GBS112	SMSI General
GBS212	SMSI freight
GBS311	SMSI Service
GBSA11	Scania Global DESADV for Sequence Deliveries
GBSB11	Scania Global DESADV for Batch Deliveries

Differences between ISDN based and Internet based EDI



ODETTE SWEDEN

What you need to communicate

- OFTP2 software
- Network service
- Communications hardware
- Application agreement/specification with trading partner
- Communications agreement/specification with trading partner
- Security Certificate
- Agreed delivery dates for solution components and services
- … and
- You need help from several providers, agree individual time schedules

ODETTE SWEDEN

Exempel på leverantörer av OFTP system

- **Freeware**
  Mendelson

- **För små företag (5 000 - 30 000 kr)**
  Encode (RedOftp) , Xware (xWare), Data Interchange (Odex Pro)

- **För medelstora och större företag (+ 30 000 kr)**
  Seeburger(BIS),Data Interchange (Epic),Axway,Hungsberg,Numlog,T-Systems

ODETTE SWEDEN

OFTP2 Certification Phase 1

Interoperability Tests Phase 1 (CMS and OFTP2 Basics)
Status: Dec 15, 2009

Vendors	Axway	ICD	DIP	Hüngs-berg	Numlog	See-burger	SSC/ c-works	Trubi-quity	T-Systems	Xware
Axway				1)						
ICD										
DIP										
Hüngsberg										
Numlog										
Seeburger										
SSC/c-works										
Trubiquity										
T-Systems										
Xware										

Notes:
All software vendors listed above have past the Odette qualifications according to the OFTP2 Interoperability Test Cases Phase 1 (CMS and OFTP2 Basics)

Vendors have carried out the tests successfully against the others

1) Certified by Axway based on the special Odette schema for "late" software vendors

ODETTE SWEDEN

OFTP2 Phase 2 Interoperability Test

Automatic Exchange of Certificates
Status: Dec 15, 2009

Vendor	Axway	ICD	DIP	Hüngs-berg	Numlog	See-burger	SSC/ c-works	Trubi-quity	T-Systems	Xware
Axway										
ICD										
DIP										
Hüngsberg										
Numlog										
Seeburger										
SSC/c-works										
Trubiquity										
T-Systems										
Xware										

Notes:
All software vendors listed above have passed the Odette qualifications according to the OFTP2 Interoperability Test Cases Phase 1 (CMS and OFTP2 Basics)

- Vendors have concluded Phase 2 tests against the others successfully
- Phase 2 tests started
- Final certification by Odette (interoperability tests Phase 1 + 2 finished)

ODETTE SWEDEN

Status of OFTP2 implementation in Europe
Usage of Communications Protocols for B2B File Transfer

	OFTP	OFTP2 L Logistics E Engineering	AS2	ebXML	SFTP	X.400	FTP	Web services
AB Volvo	x	(x) L E			x		x	x
BMW	x	(x) L E			x			
Conti	x	x L E	x		x	x	x	x
Daimler	x	(x) L E						x
FORD	x	(x) L E					x	x
Hella	x		x		x	x	x	x
Johnson Controls	x	(x) L E	x				x	x
PSA	x	x E					x	
Renault	x						x	x
Scania	x	(x) L E	(x)					
SKODA	x	(x) L E				x		x
Valeo VMS	x						x	
Volvo Cars	x	x L E			x		x	
VW	x	x L						x

This list explains what protocols are used within a company, the character (x) means that the protocol is planned to be used. An “x” means that a specific protocol is used within at least one business process but it does not mean that the protocol could be used for any business process. ”L” and ”E” indicate intentions for Logistics and Engineering as interpreted by the Project team.

ODETTE SWEDEN

Odette International OFTP2 Directory

https://forum.odette.org/OFTP/oftp2-directory

Företag erbjuds möjlighet att registrera att man använder OFTP2, drygt 600 företag har gjort det

OFTP2 Directory

by Joerg Walther — last modified Jan 15, 2013 15:36 by Stephanie Bioux

This directory lists those companies who have told us that they have implemented OFTP2 in their EDI infrastructure and are ready to start data exchange implementation worldwide. New companies are being added all the time, so please come back and check regularly for updates.

If your company is ready to use OFTP2 but is not yet listed, you can register here. Latest entries are highlighted in **bold.**

Consult the list of interoperability tested software. If you are a software provider and wish to get your products tested, click here for more information.

Manufacturers

Company	Location	Country	EDI	CAD
BMW	Munich	Germany	x	x
Ford Motor Company	All Plants	Worldwide	x	
Hyundai Motor Europe Technical Center	Rüsselsheim	Germany		x
MAN Truck & Bus	Munich	Germany		x
PSA Peugeot Citroen		France		x
Scania	Södertälje	Sweden	x	x
Skoda	Mlada Boleslav	Czech Rep	x	x
Volkswagen	Wolfsburg	Germany	x	
Volvo Car Corporation	Gothenburg	Sweden	x	x
Volvo IT for Volvo Group	Gothenburg	Sweden	x	x

Suppliers

Company	Location	Country	EDI	CAD
1zu1 Prototypen	Dornbirn	Austria		x
3D Tech	Ondrejov	Czech Rep.		x
3 Dimensional Services	Bad Homburg	Germany	x	x
3M Deutschland	Neuss	Germany		x
4D Concepts	GroB-Gerau	Germany		x

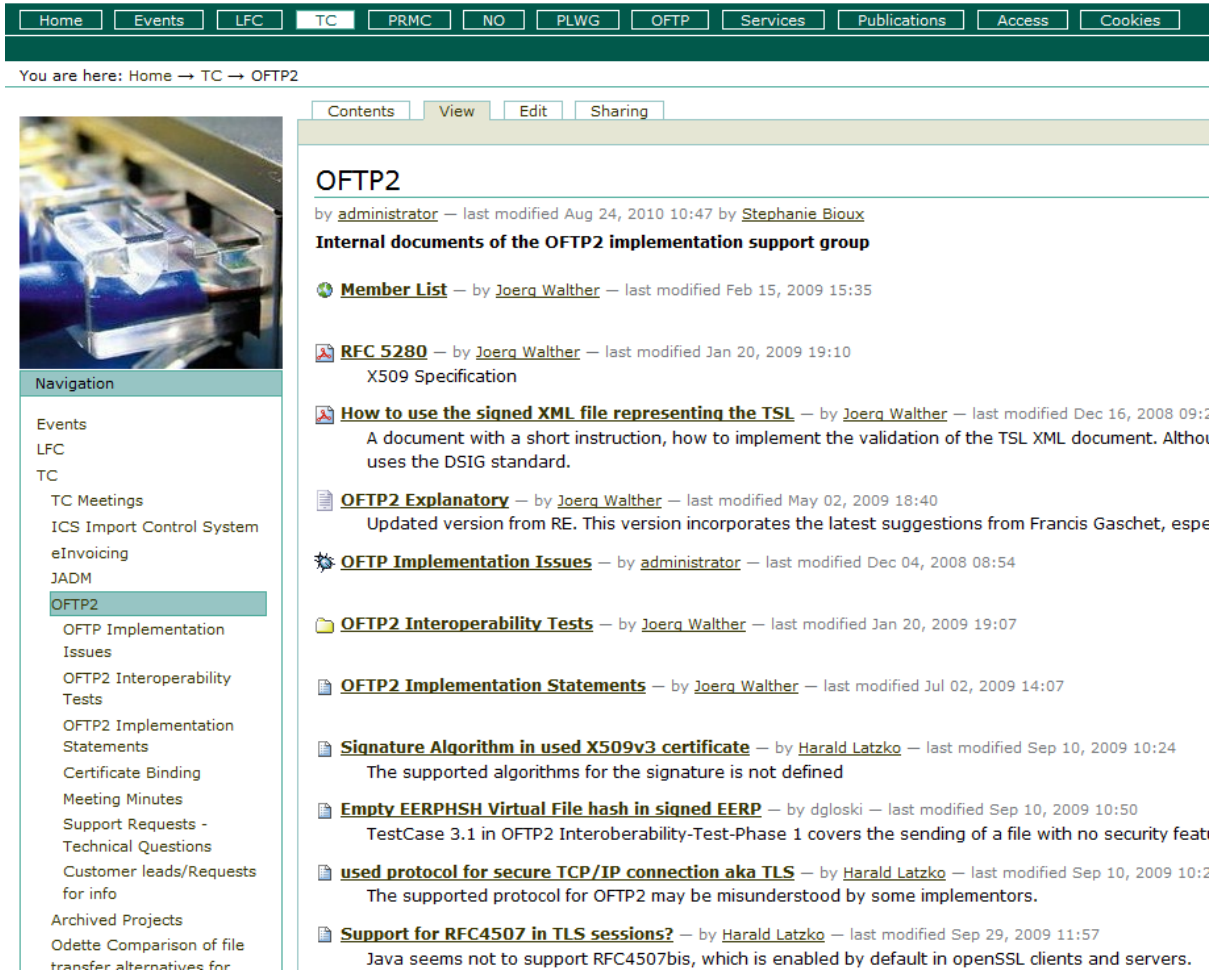
ODETTE
SWEDEN

Implementation issues

ODETTE SWEDEN

Odette OFTP2 Implementation Group

Odette International is running an Implementation Group where any kind of implementation issues could be raised. There is participation from Odette Sweden member companies in the group



Implementation issues

- Prepare yourself
- Practical implementation issues
- Certificate
- TSL
- ICD codes
- Oscar codes – identification – authentication - how to request from Odette
  - Form for acquiring Oscar
  - Form for acquiring Certifikate
  - Ordering TSL
  - CA who wish to qualify for the TSL
- Questions and answer

Implementation issues

From experience we know that certain steps are necessary for a successful implementation:

Information gathering

- Obtain documentation through your Odette National Organisation (NO)
- If possible take part in training courses organised by your NO or by IT Providers
- Discuss OFTP2 implementation with your communication software provider. They should have the necessary knowledge about security and certificates.

Migration planning and/or new implementation

- If there is a need to upgrade your software, ask in-house and ask your trading partners
- If there is a demand to upgrade, make a timetable together with your trading partners, your communication software provider and your IT Provider.
- Collect information to clarify when older network services could be phased out

Implementation issues

Security Solution (Certificate)

- It is important to clarify Trading Partner requirements for the security solution:
  - Security Certificate and CA Service - how to reduce the number of options
  - Trading Partner security policy (session encryption, file encryption, signing, signed acknowledgement of receipt)

ODETTE
SWEDEN

Odette CA

- Established to provide all items necessary for a reliable data exchange in the automotive industry manged by the Odette organisation
- Easy to use
- State of the art certificates, may even include the Odette ID of the station
- „One stop shop“ principle

How to get security certificates for OFTP2

- Security Certificates for OFTP2 must come from CA:s listed on the Odette TSL (Trust Service Status Lists)
- Therefore the first step is to check this list
- The second step is to see if your company already has obtained certificates that could be used also for OFTP2 (beside other use such as secure websites)
- If you have a preferred CA services provider which is not listed on the Odette TSL you can suggest your CA to apply for being listed
- Another potential providers of security certificates is the Odette CA, or possibly your OFTP2 software provider or a major customer (OEM)

ODETTE
SWEDEN

https://www.odetteca.com/

There is also information available in Swedish on the Odette Sweden website about how to register

ODETTE SWEDEN

ODETTE CA
www.odetteca.com

11 November 2009

Certificate Registration and Authorisation Data Sheet

Order Number: xxxxxx Order Date: xxxxx

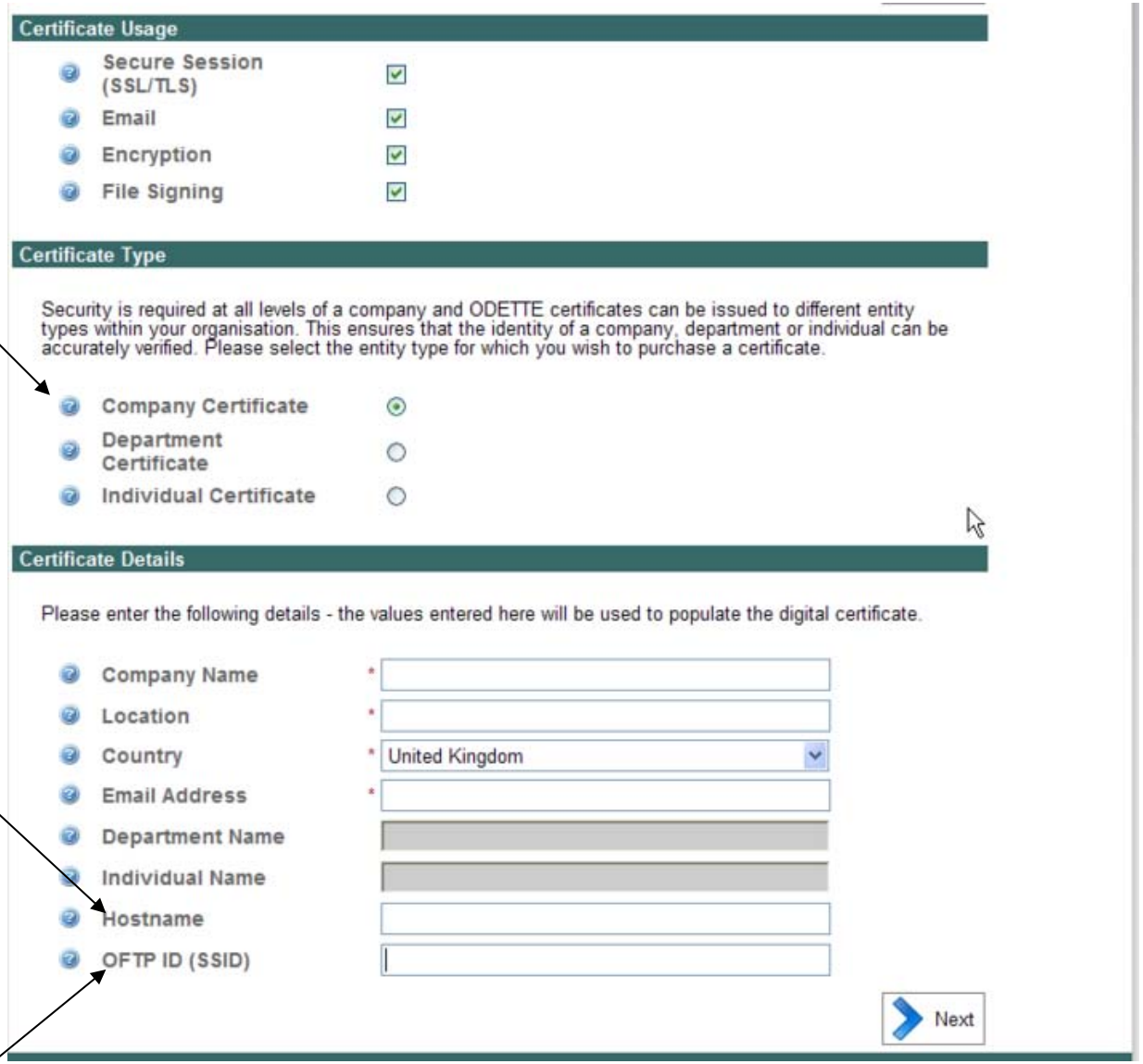
Certificate Details

Certificate type	Company	
Email		
Location		
Country		
Organisation		
Department		
Name		
Domain / IP Address	"Host name" in the web form – mandatory for AB Volvo	
OFTP ID		
Validity		Year(s)

Recommended to use the actual OFTP2 server for ordering and installation

Standard (but not the only) option is "company"

Host name
Not mandatory, but required for AB Volvo, should be DNS or IP address as called by Volvo



OFTP ID: Not mandatory

ODETTE SWEDEN

ODETTE SWEDEN

Not same person

Technical Contact Details

Name	
Company	
Position	
Email	
Address Line 1	
Address Line 2	
City	
Postcode	
Country	
Telephone	

Authentication Contact Details

Name	
Company	
Position	
Email	
Address Line 1	
Address Line 2	
City	
Postcode	

The person that would sign this document

ODETTE CA
www.odetteca.com

11 November 2009

Order Number:

I authenticate the certificate request with the details shown above. I authorise the Technical Contact to initiate further actions such as download the certificate, issue a revocation request if necessary or obtain a new certificate at the end of the validity period.

I accept the Odette CA Subscriber Agreement[1] as general terms and conditions of registration on and usage of Odette CA Certification Services as laid out in the Odette CA Subscriber Agreement.

I agree with data collection and its use according to chapter 12 of Terms of Use[2].

I confirm my authorisation and approve the certification request.

_____ _____

Location and Date Stamp and Signature

Annexe:

- Copy of company registration form [3] [ ]
- Copy of ID card/drivers licence/passport [4] [ ]
- Other document: _____[ ]

SCX Implementation

- The work to build the TSLs is carried out by Odette CO supervised by a permanent Odette committee
- TSLs and their associated policies are published on the Odette Web site **http://www.odette.org/tsl/pol_basic.txt** **http://www.odette.org/tsl/pol_oftp2.txt**
- Enabled software will download it according to a special policy in order to avoid bottleneck
- The software will be able to automatically trust or distrust a certificate, basing its decision on the trusted CA list
- **OFTP2** will be the first application which will benefit of these features
- Other applications will have their own TSL according to their own need in mater of certificate policy (e.g. secure email).

Practical implementation issues

There are some aspects that individually might not be so complicated to handle, but could still cause certain issues. It is therefore recommended that you discuss the following items with your IT support and with your IT provider:

Firewall

- The firewall will have to be adapted for OFTP2, Port 3305 (OFTP) plus 6619 (TLS). Ports must be open in both directions in order to enable dialling out and dialling in.

DNS address (fixed) or IP address

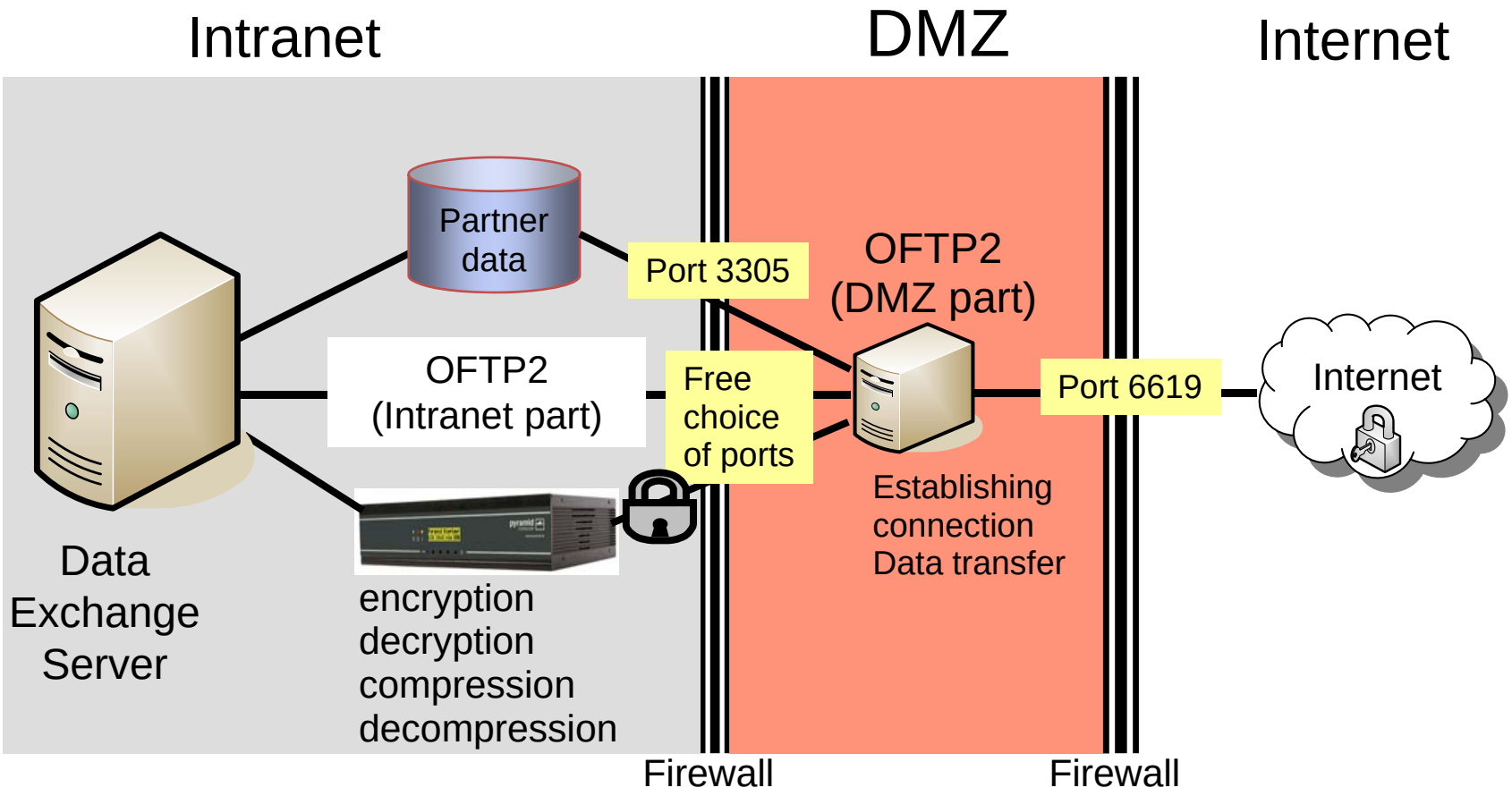
- We recommend choosing a fixed IP address together with a DNS name (e.g. oftp.supplier.com) instead of IP address.
- This would minimise the risk for problems when changing ISP (Internet Service Provider).
- We do not recommend using dynamic DNS Services since this would make you dependant on a third party.
- Some free services can be closed down after 30 days of inactivity, for example if an IP address has not been changed.

Practical implementation issues

Public IP address and the link to certificates

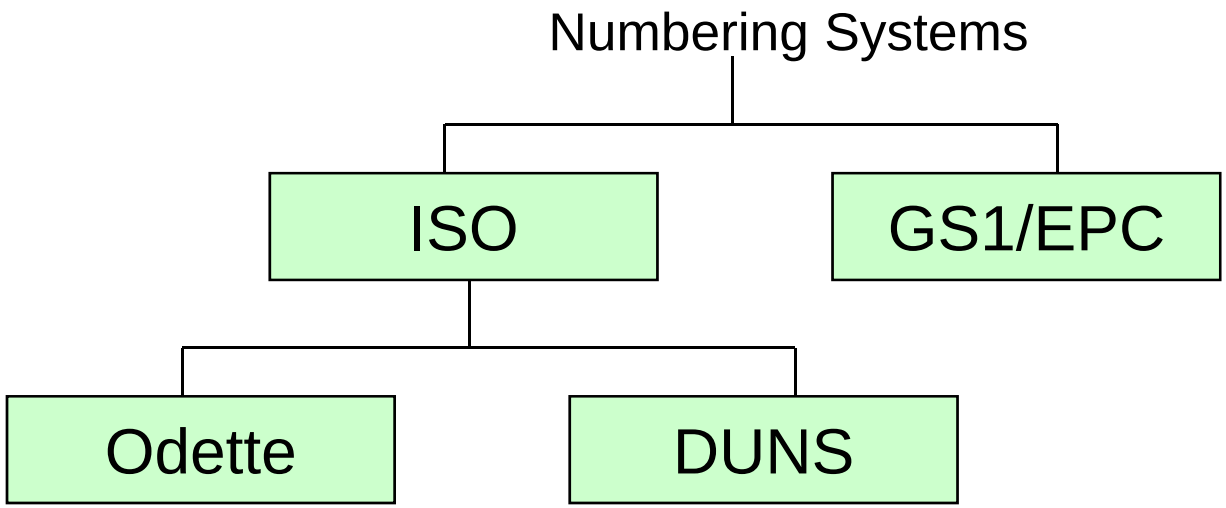
- The DNS name should be listed in the certificate.
- Tests
- Select a suitable business partner for testing, certificate handling and others.

Example of secure OFTP2 configuration by Swedish OEM



OSCAR: Odette System for Coding And Registration

- The Oscar system provides:
  - An issuing service (issuing codes)
  - An information service (a user can query information on the registered entity)
- ISO compliant



ODETTE SWEDEN

Usage of OSCAR Codes

AutoID

- Consignment ID (Licence Plate)
- Asset ID (e.g. Containers)
- Product ID (Parts Marking)

Organisation codes:
Trading partners
Locations, business functions and departments within a company
Logistics handling units
Company Assets
Individual parts/components
Computer network addresses
Engineering changes

EDI messaging

- Technical Partner ID (Sender/Receiver)
- Business process related Party ID (NAD ID)

File transfer station identification (OFTP)

ISO ID					OFTP code from the OSCAR System													Sub address					
0	0	1	7	7	0	0	0	0	0	0	0	0	0	0	X	0	0	A	0	0	0	0	0	0

Maintain Business Entity Datasets

Provide Business Entity Datasets for use in Partner Databases

OSCAR code for OFTP only:
175 EUR per OFTP code, no maintenance fee
Entitles to get 1 Odette Certificate for one year for free.

Full OSCAR Code (for All Purposes)
MBE Code 180 EUR each
SBE Codes (can be generated by Users free of charge)
Annual Maintenance: 96 EUR per MBE Code

Odette Certificate for OFTP2 (but also usable for other purposes):
Certificate 180 EUR
Annual Renewal 180 EUR

Adresses
www.odette.se
https://oscar.odette.org/
https://forum.odette.org/service/oscar/oscar-explained
www.odetteca.com

ODETTE
SWEDEN

Questions and answers

Vad gör AB Volvo och Scania med OFTP2?

- Scania har ca 100 OFTP2 relationer av totalt ca 600 OFTP relationer. Man byter löpande men har ingen uttalad sluttid för migreringsprojektet
- AB Volvo och Volvo Cars har ca 1800 OFTP2 relationer. OFTPv1 är nedstängt sedan September 2012.

Documentation and websites

Documentation

Training course slides
OFTPV2 specifications
OFTPV2 Implementation Guidelines
Security Certificate Exchange (SCX)
OFTP2 Explanatory paper (in Swedish)
CA Help document

Where to find

Go to http://www.odette.se/web/Seminarier_o_kurser.aspx

Select Endast tillgänglig för kursmedlemmar

User name: odettekurs
Password: kurssamverkan

Final discussion

Sten Lindgren, VD
Odette Sweden AB
Box 26173
SE-100 41 Stockholm
T +46 8 700 41 20
sten.lindgren@odette.se

Peter Nilsson
Senior Business Analyst
Volvo Information Technology
+46 (0) 31 323 6033
peter.nilsson.8@volvo.com