NAF OFTP2 Webinar Del 2
(Version 05)

NAF OFTP2 Webinar

5 oktober 15.00 - 17.00	**Genomgång av aktuella förändringarna avseende X.25/ISDN från TeliaSonera. Genomgång av olika framtida kommunikationsalternativ med för- och nackdelar. Vilka är alternativen?** *Sten Lindgren, Odette Sweden* *Patrik Patriksson, TeliaSonera* *Mikael Carlsson, PipeChain* *Bengt Andersson, Scania*
19 oktober 15.00 - 17.00	**Vad är OFTP2 – översikt. Genomgång av olika funktioner i OFTP2-protokollet** **AB Volvo går live med OFTP2!** *Sten Lindgren, Odette Sweden* *Peter Nilsson, PipeChain* *Bengt Andersson, Scania* *Lars Cederholm, Volvo IT*
9 november 14.30 - 16.30	**Genomgång av hantering säkerhetscertifikat för OFTP2** *Sten Lindgren, Odette Sweden* *Håkan Enquist, Saab Technology och Handelshögskolan i Göteborg* *Lennart Jakobsson, Scania* *Jörg Walther, Odette International*
23 november 15.00 - 17.00	**OFTP2 – implementeringsaspekter.** **What is ENX?** *Sten Lindgren, Odette Sweden* *Peter Nilsson, PipeChain* *Lars Cederholm, Volvo IT* *Lennart Oly, ENX*
7 december 15.00 - 17.00	**Genomgång av några cases bland deltagande företag.** **In depth comparison of various file transfer protocols, (AS2 and more)** *Sten Lindgren, Odette Sweden* *Alla* *Ronny Samuelsson, PipeChain* *Gavin Fowler, Data Interhange*

ODETTE SWEDEN

NAF
Nätverk för Affärsutveckling i Försörjningskedjan

NAF OFTP2 Webinar den 19 Oktober kl 15.00 – 17.00

- **Introduktion**
- **Vad är OFTP2 – översikt, bakgrund, viktigaste skillnader mot OFTP1**
- **Genomgång av olika funktioner i OFTP2-protokollet**
- **AB Volvo går live med OFTP2!**

Sten Lindgren, Odette Sweden
Peter Nilsson, PipeChain
Bengt Andersson, Scania
Lars Cederholm, Volvo IT

ODETTE SWEDEN

NAF OFTP2 Webinar den 19 Oktober kl 15.00 – 17.00

Introduktion

ODETTE SWEDEN

Introduktion

Webinaret

- Presentationer
- Frågor
- Innehållet: Första delen allmän, andra delen på konkret detaljnivå

Om området som webinaret behandlar

- Huvudsyftet är att beskriva de förändringar som är på gång
- Dessa är nära knutna till “svenska” fordonstillverkares övergång till OFTP2 över TCP/IP
- Dessutom är förändringar inom TeliaSonera tjänsteutbud en viktig aspekt
- Vi tar gärna emot kompletterande information och frågor från deltagarna i webinaret, det kan även gälla situationen ute i Europa och/eller vad OEM:s ute i Europa gör

ODETTE SWEDEN

Hur får man tag i information om OFTP2?

Publikationer

- Odette OFTP2 Implementation Guidelines
- Odette Security Certificate Exchange
- Odette OFTP2 Explained

För att få tillgång till Odettes publikationer måste man vara medlem i Odette Sweden eller abonnent. För villkor för abonnemang se
http://www.odette.se/web/Medlemskap_o_abonnemang.aspx

Utbildning i OFTP2

Odette Sweden erbjuder en endagskurs som tar upp alla aspekter i detalj (protokollet, nättjänster, säkerhetsadministration).

Kursen vänder sig till support- och implementeringsfunktioner samt till utvecklingspersonal.

Kursen kan ges både företagsinternt och som öppna kurser

ODETTE SWEDEN

Hur får man tag i information om OFTP2?

IT-företag

För allmän information om IT-företag som erbjuder OFTP-produkter, se **http://www.odette.se/web/Programvaruhus.aspx?Guid=69dc2461-7a14-46d8-bc3e-50b7fc8ae5cd**

När det gäller OFTP2-produkter finns en lista som bygger på genomförda Interoperabilitetstester

OFTP2 Phase 2 Interoperability Test: Automatic Exchange of Certificates. Status: September 26, 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										

Vendors have carried out the tests successfully against the others

Test started

ODETTE SWEDEN

NAF OFTP2 Webinar den 19 Oktober kl 15.00 – 17.00

Vad är OFTP2 – översikt, bakgrund, viktigaste skillnader mot OFTP1

ODETTE SWEDEN

Background

SASIG XMTD Software Providers Meeting September 2004:

Question: How to exchange ENGDAT data globally?

Existing transfer based on OFTP Version 1

Defined in 1986 by Odette
Used extensively in Europe for ENGDAT/CAD and Trade EDI by
- Automotive
- Retail
- Transport
- Government Organizations, …

Used over secure networks ISDN, X.25
VPN, ENX IP-services

ODETTE SWEDEN

Challenges

- **ENGDAT involves very large (>100 MByte) files**
- **Fast and low cost network services are important**
- **ENGDAT have become a global standard that shall support global data exchanges**
- **These characteristics are valid also for trade EDI**

- **ISDN and X.25 network services**
  - **Slow**
  - **Expensive (especially international calls)**
  - **Are mostly used in Europe**
  - **In the long term they will be closed country by country**

- SOLUTION:
  Extend OFTP for secured transmissions on the public Internet

Working Group Objectives

Objectives

"To develop an OFTP (Version 2) suitable for the exchange of EDI files and large files, such as CAD/CAM drawings, between trading partners under the auspices of a cryptographically secure environment necessary to meet the increasingly sensitive needs for data transfer within the automotive community on a world wide basis."

Deliverables:

- Define and publish an OFTPV2 protocol as an Internet RFC
- Publish the OFTPV2 protocol also as a new Odette recommendation
- Create Implementation Guidelines for sw-implementers and users
- Conduct basic interoperability tests between different softwares and platforms
- Initiate pilot projects

OFTP2 RFC5024. New security protocol spec.

Security services

Secure authentication, Confidentiality, Integrity, non-repudiation of files and of receipts by

- Transport session authentication and encryption (TLS)
- OFTP authentication
- File encryption
- File signing
- Receipts signing

Based on security certificates with asymmetric and symmetric keys

OFTP2 RFC5024. Other new protocol spec.

File compression

- compressing on file level, better than existing on data buffer level.
- Down to 10 %, dependant on file contents
- Reduces transmission times and costs

•

Additional file description

- UTF-8 encoded file description
- Allows companies to send descriptive text with a file in any language
- Maximum file description (999 octets)

Larger files

- Maximum files size extended to 9,3 PetaBytes

Networks

OFTP2 may be used by

- **X.25 Native**
- **X.25 over ISDN**
- **ENX/ANX/JNX / Private Links**
- **TCP/IP, Public Internet**

OFTP 1.0 – OFTP 1.3	OFTP 1.4	OFTP 2.0

ODETTE SWEDEN

Implementation Guideline

For OFTP-users:

General information about OFTP2 and security certificates.

For OFTP software developers:

Information about implementing OFTP2 software, especially about handling of certificates in the software.

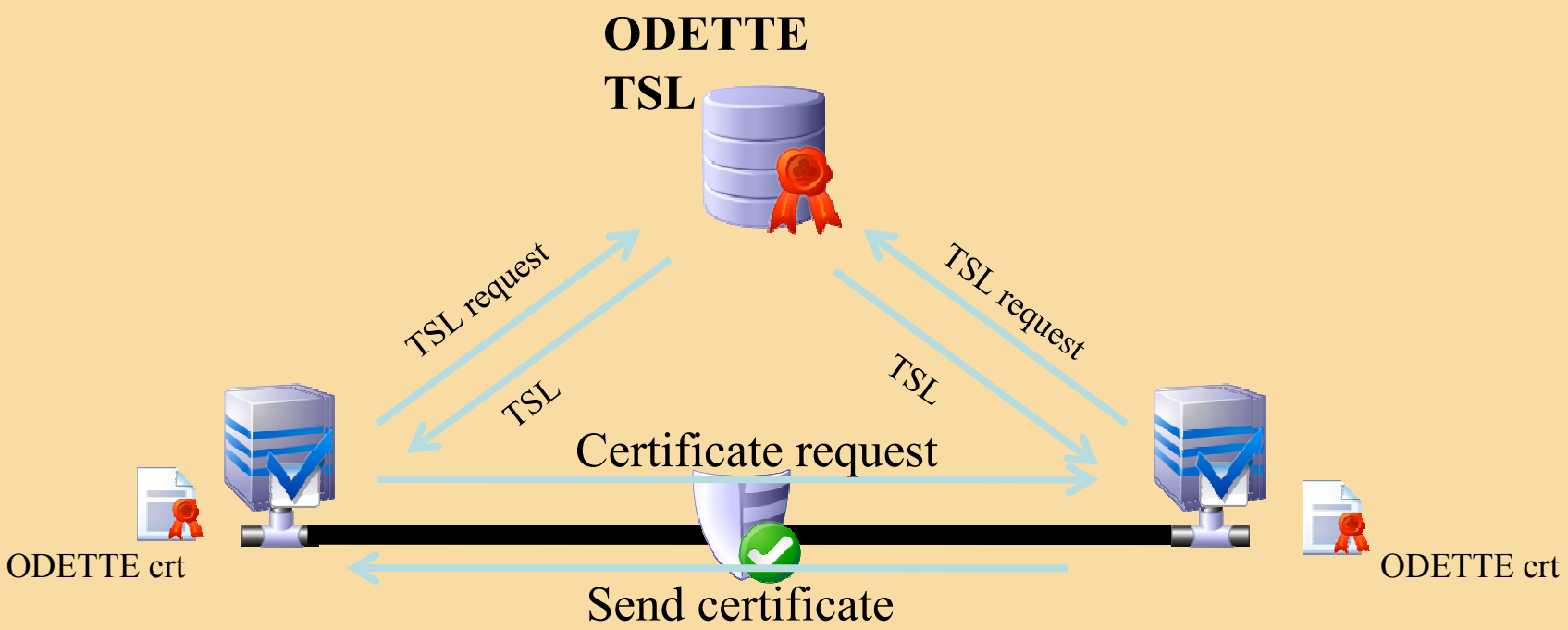
Information regarding implementation of a complete function for exchanges of user certificates between OFTP-systems.

Odette TSL Service

- Distribute the certificate policy associated with the TSL to CA:s 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
  - If a CA's policy becomes incompatible with the TSL policy, this CA will finally be discarded.

ODETTE SWEDEN

Odette – **T**rust **S**tatus signed **L**ist –TSL Administration



Finally – a secure, trusted connection!

ODETTE SWEDEN

The Odette SCX recommendation

What's a TSL?

Trust **S**ervice **S**tatus **L**ists

- An ETSI standard using XML formatting
- Contains the list of the CA:s certificates recognised as "Trustworthy", 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

Lists for different applications will be managed by Odette, so far a general purpose "Basic" list and a specific OFTP2 list are provided.

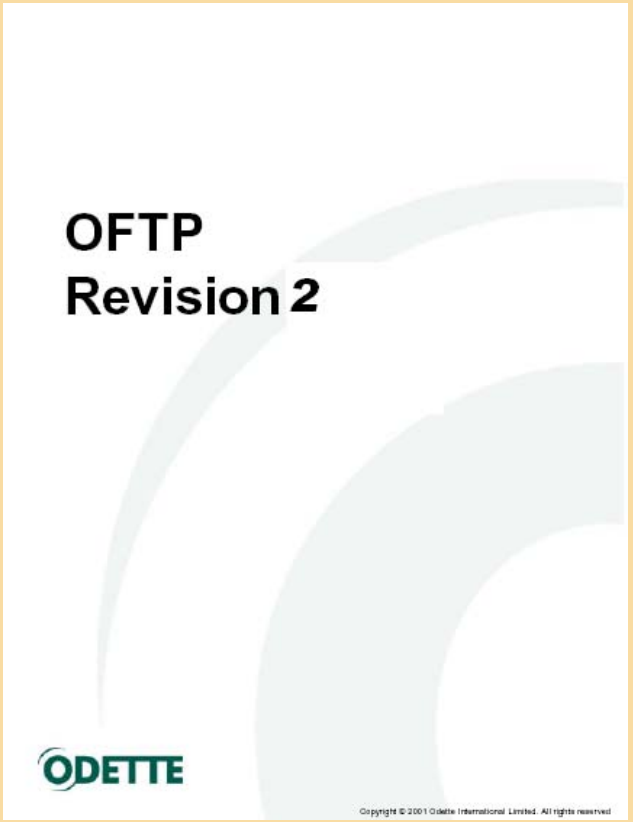
ODETTE SWEDEN

NAF OFTP2 Webinar den 19 Oktober kl 15.00 – 17.00

Genomgång av olika funktioner i OFTP2-protokollet

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.

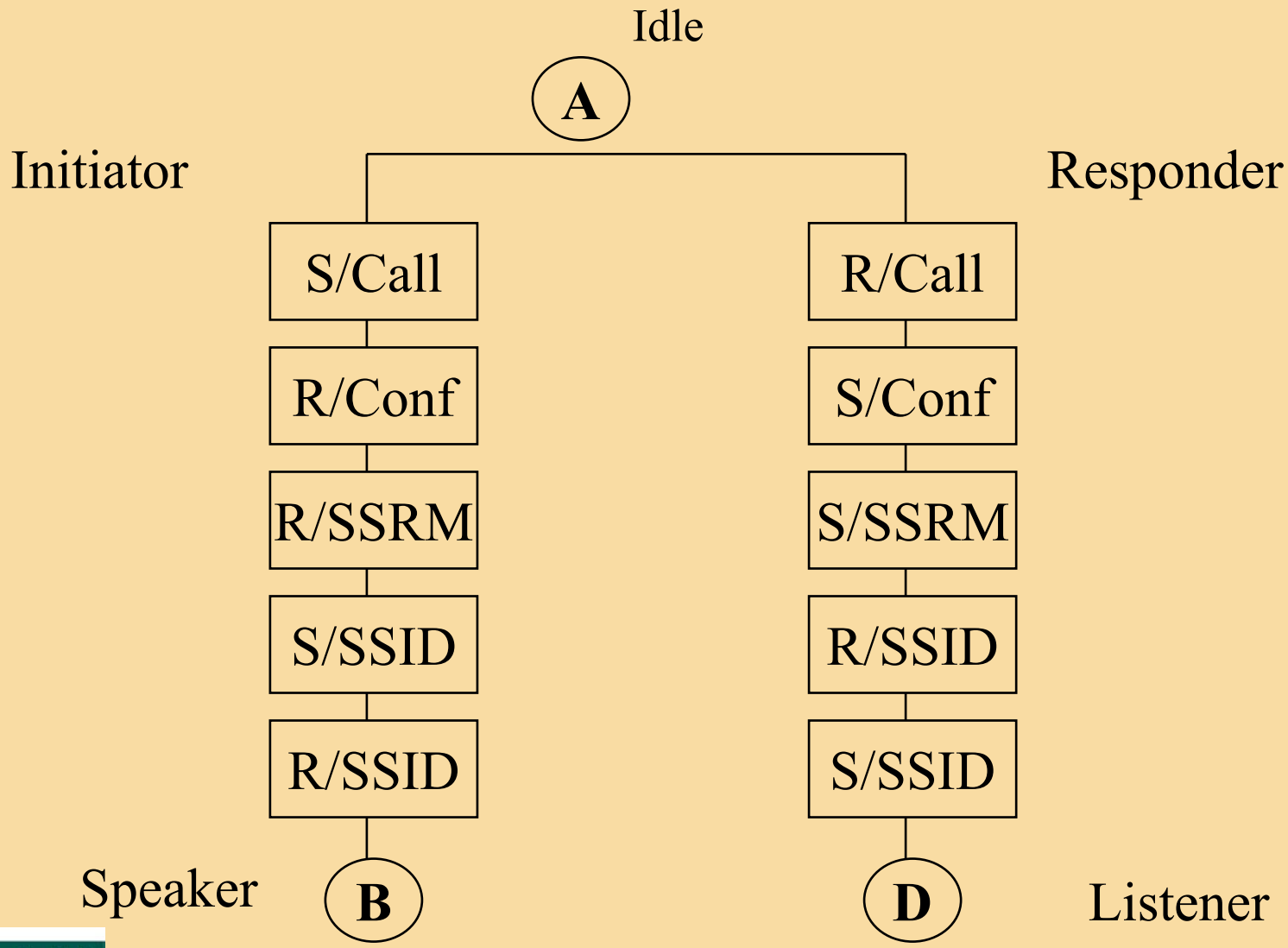
Speaker/Listener

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

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):

Initiator	———	Call	——→	Responder
Initiator	←———	Clear	———	Responder

Start session (alt 2):

Initiator	———	Call	——→	Responder
Initiator	←———	Confirm	———	Responder
Initiator	←———	SSRM	———	Responder
Initiator	———	SSID	——→	Responder
Initiator	←———	ESID(R)	———	Responder
Initiator	———	Clear	——→	Responder

ODETTE SWEDEN

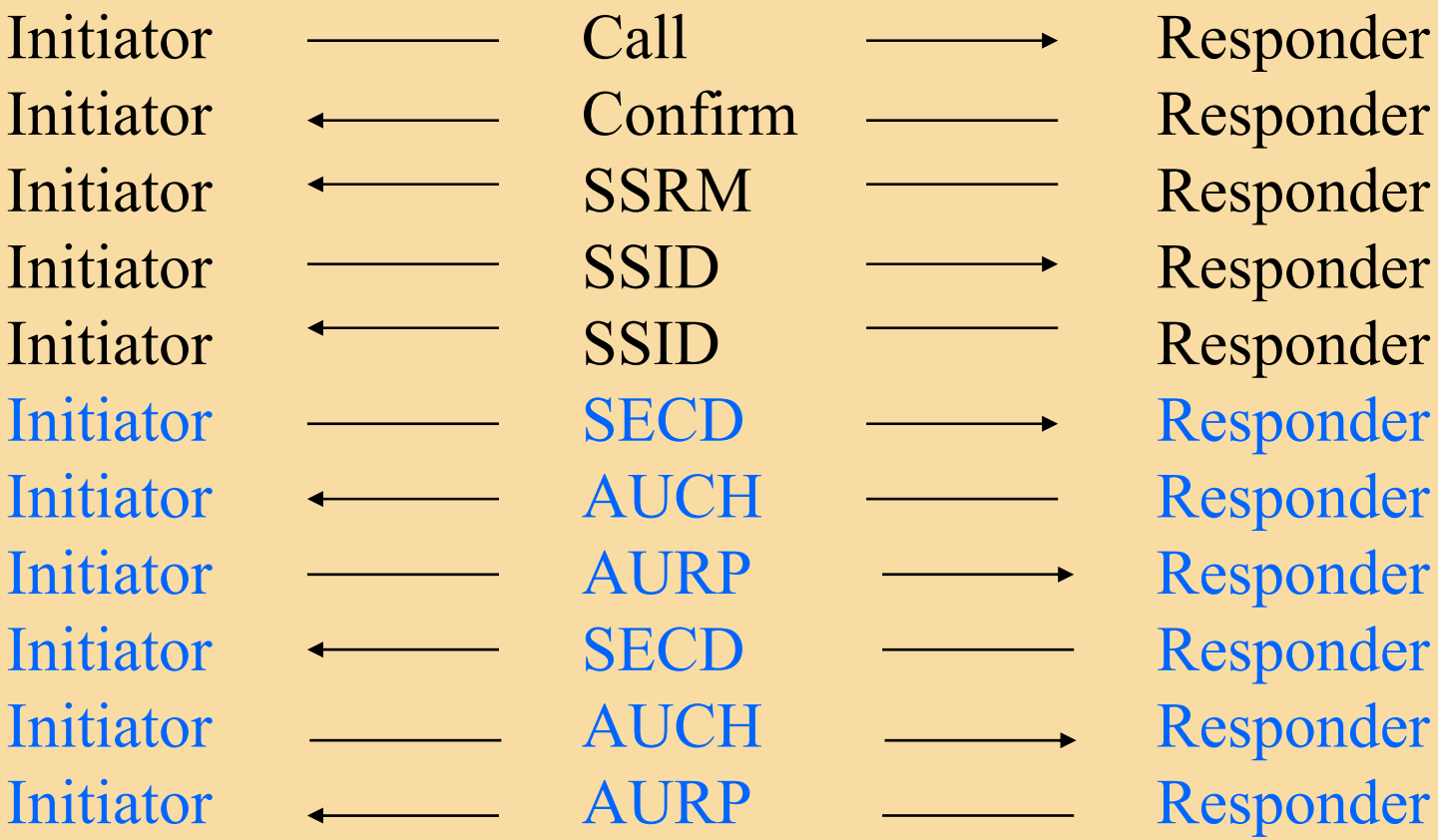
Start session (alt 3):

Initiator	———	Call	——→	Responder
Initiator	←———	Confirm	———	Responder
Initiator	←———	SSRM	———	Responder
Initiator	———	SSID	——→	Responder
Initiator	←———	SSID	———	Responder
Initiator	———	ESID(R)	——→	Responder
Initiator	←———	Clear	———	Responder

Start session (alt 4 V 1.4):

Initiator	———	Call	——→	Responder
Initiator	←———	Confirm	———	Responder
Initiator	←———	SSRM	———	Responder
Initiator	———	SSID	——→	Responder
Initiator	←———	SSID	———	Responder

Start session (alt 5 V 2.0):



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 Challenge**
SECD	**Security Change Direction**
AURP	**Authentication Respons**

ODETTE SWEDEN

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	

ODETTE SWEDEN

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

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
O093100000918234455251551
O093200000000341001AND001

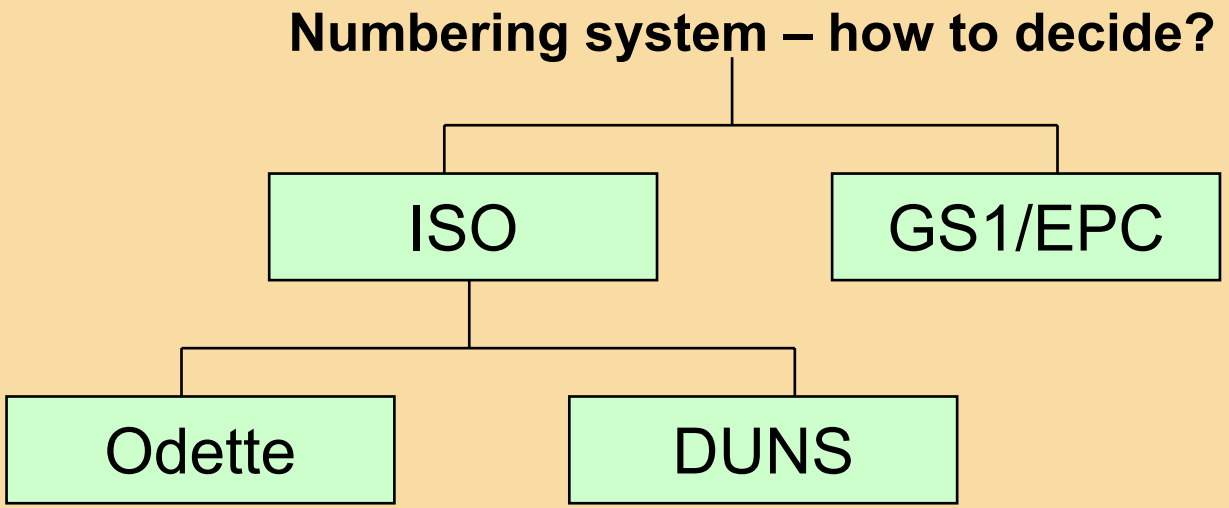
ODETTE SWEDEN

OSCAR: Odette System for Coding And Registration

OSCAR will provide two key offerings:

1) An **issuing agency service** for the coding of business Organisations

2) An **information service** which allows access to detailed and up to date information about the organisations of registered entities.



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)

Maintain Business Entity Datasets

Provide Business Entity Datasets for use in Partner Databases

Advantages of OSCAR

- More flexible then DUNS
  - Business units / entities beyond legal entities
- Cheaper than GS1/EPC
- Short enough for parts marking and RFID applications
- Alphanumeric – 4 Characters for main and additional 2 characters for sub-codes (1679616 main and 1296 sub-codes per main code)
- Tailor-made for the automotive industry

https://www.odetteca.com/

Home | Learn More | Contact Us | Repository | Terms & Conditions | odette.org

ODETTE Certificate Authority

Welcome to the ODETTE Certification Authority

The increasing use of the internet for data exchange and collaboration in the automotive and other Industries requires state-of-the-art security means. Odette CA offers the necessary **Digital Certificates** for OFTP2 data exchange, document and email signing & encryption and internet application protection.

Certificates issued by Odette CA are recognised by the Odette Trust Service and ensure security and interoperability with your business partners in the automotive industry.

ODETTE SWEDEN

Price List

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

AB Volvo går live med OFTP2!

Lars Cederholm, Volvo IT

Leverantörer till Volvo gruppen som är intresserade av att vara piloter kan maila **support.edi@volvo.com**

ODETTE SWEDEN

OFTP2 – Nya kommunikationsprinciper

Nätverk för Affärsutveckl
i Försörjningskedjar

Fråga ställd inom NAF

- Ska vi undersöka intresset för någon form av samverkan avseende implementeringsprinciper för OFTP2?

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.

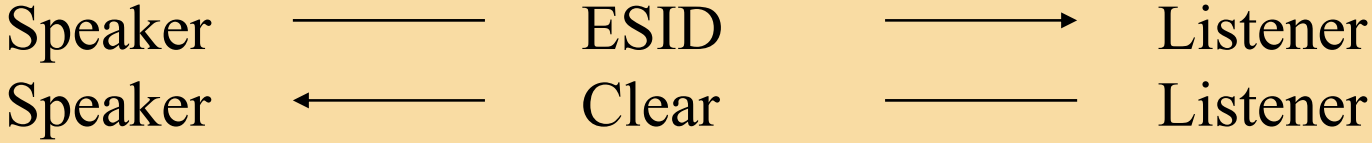
ODETTE SWEDEN

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**

ODETTE SWEDEN

Session termination



ESID End of Session

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

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

ODETTE SWEDEN

Frågestund alternativt kortare paus

ODETTE SWEDEN

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 max 9,3 PB
	Before compression or encrypting
Original file size	**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**

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.

SFPA Send File Positive

Command	2
Answer count	Restart
	Lower or equal to SFID restart

SFNA Send File Negative

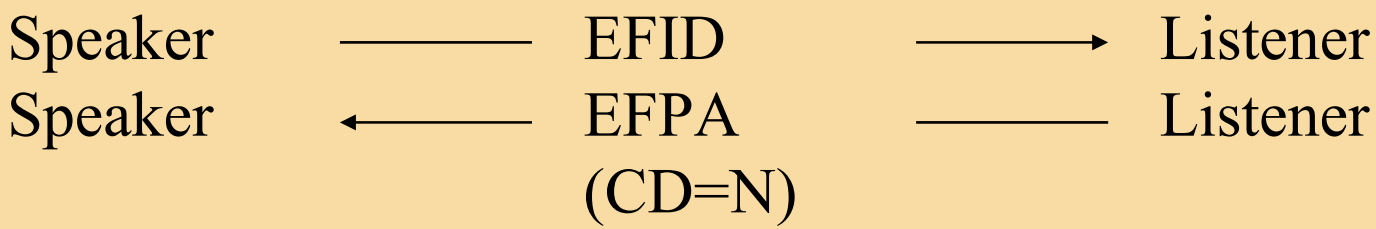
Command	3
Answer reason	As in list of arguments
Retry	Y/N
	Y retry later
	N the file should not be sent
Answer reason	**Answer reason text length**
Answer reason	**Answer reason text**

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

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 ——— EERP ———→ Listener
Speaker ←——— RTR ——— Listener

Speaker ——— NERP ———→ Listener
Speaker ←——— RTR ——— Listener

Speaker could send any of:

SFID
NERP
EERP
CD

ODETTE SWEDEN

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

ODETTE SWEDEN

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

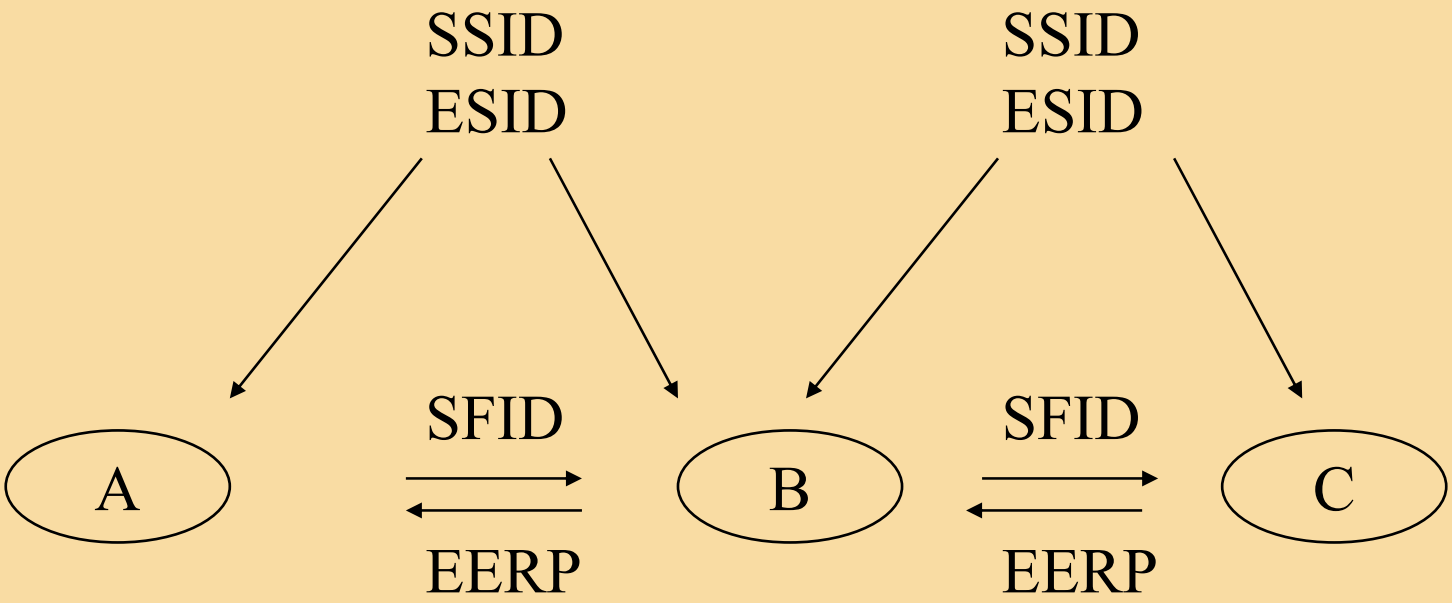
Is used to control a route and is normally interpreted as a handover confirmation

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

Frågestund alternativt kortare paus

ODETTE SWEDEN

Routing



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

ODETTE SWEDEN

Routing

Routing is no option:

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

Virtual File

File organisation: Sequential

File identity: File name + date/timestamp identifies uniquely

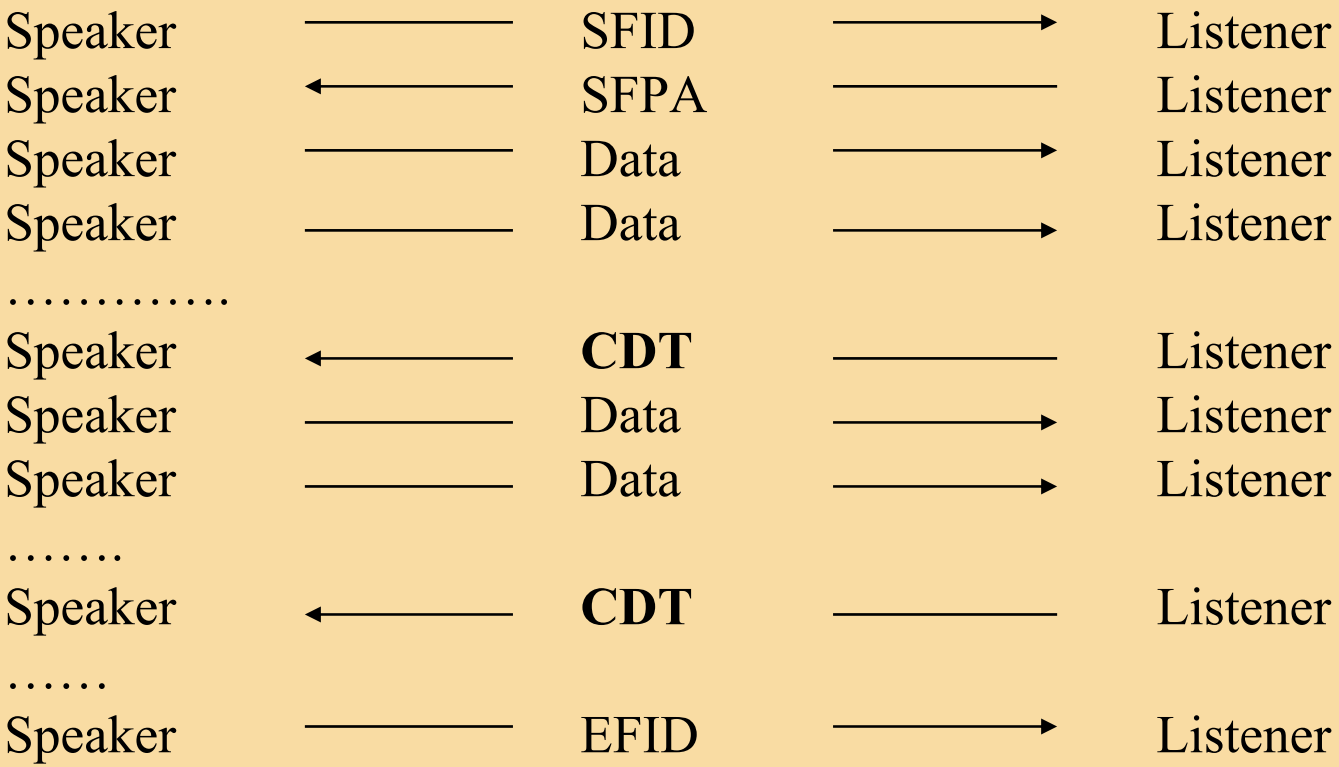
Record format:

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
The max limit is 65 K for OFTP2

Data flow control



Listener could send any of:

EFPA
EFNA

Data Flow

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.