



Automotive Supply Chain Best Practices

OFTP2 EXPLAINED

Version No 1.0

Date: October 2009

CONTENTS

What is OFTP2 and what are its advantages? 2

 Secure OFTP2 3

 How does OFTP2 work? 4

 What are the main advantages of OFTP2? 4

 Globalisation of the automotive industry 4

 Changes in IT infrastructure 4

 Changes in communications needs 5

 Advantages compared to other (newer) communication alternatives 5

 What are the main players doing? 6

 What are the links between OFTP2 and network services? 6

 The “OSCAR” - Odette ID - service 6

 Implementation 6

 Information gathering: 6

 Migration planning and/or new implementation: 7

 Security Solution (Certificate) 7

 Practical Implementation issues 8

OFTP2 Products 9

WHAT IS OFTP2 AND WHAT ARE ITS ADVANTAGES?

The Odette File Transfer Protocol (OFTP) has long been one of the most established protocols for automated standardised data exchange between trading partners.

The major components in an automated standardised data exchange are:

- The information which is collected from various applications and put into standardised EDI messages
- Network services like ISDN, X.25, TCP/IP (Intranet/Internet (Extranet)/VPN) used for transporting the data
- The OFTP protocol which monitors the data transport through OFTP software products used by the sender and by the receiver

OFTP is a de facto standard within business sectors such as Automotive, Engineering and Transport. OFTP is also used for data exchange with partners in the public sector. One example is the Swedish Customs Data System.

The OFTP Protocol was created by Odette, the European Automotive standards body. The first version of OFTP was released in 1986 and was aimed at being used with network services that were available at that time, mainly X.25 services.

Odette also took into account that VAN (Value Added Network) Services could be one part of the communication chain.

Since 1986 the OFTP protocol has been published in several versions reflecting changes in network services with the introduction of ISDN, X.28 and X.31 and more recently the public Internet (TCP/IP). The latest version of the OFTP protocol is version 2, known as **OFTP2**. This version is mainly intended for secure data exchange over the public Internet, where security is guaranteed by the use of security certificates.

The implementation of **OFTP2** is expected to take off in 2009, due to factors such as:

- Old network services (X.25/ISDN) being phased out or reshaped in many countries
- Moving from old network services, such as ISDN and X.25, to secure data exchange over the Internet will reduce data transport costs and increase bandwidth dramatically
- **OFTP2** is the first solution that can be used across the world.

SECURE OFTP2

Information security requirements in connection with data exchange between trading partners vary depending on the field of application. Some examples of information that users would normally like to protect are:

- Product data and CAD data
- Financial information
- Pricing information
- Sourcing information

Since **OFTP2** is primarily intended for use over the public Internet there is a need for additional security techniques that were not required for ISDN/X.25 services.

The leading automotive companies have agreed on a level of security that is considered as sufficient and reliable for business processes in the automotive industry and beyond.

The security level that has been chosen is high and is equal to that used for payment services over the Internet. Solutions are based on the use of security certificates.

An **OFTP2** session is usually more complex than a normal Internet payment transaction. This is something that is reflected in **OFTP2** security solutions.

OFTP2 was developed with active participation by the majority of key players in the automotive industry, including large IT providers. Companies supporting **OFTP2** from the beginning include:

BMW	Bosch
Daimler	JCI
Karmann	PSA
Scania	Volkswagen
Volvo	

When it comes to IT Providers offering **OFTP2** products, you will learn how to find available software at the end of this brochure.

HOW DOES OFTP2 WORK?

The OFTP protocol is aimed at executing and monitoring data exchanges between trading partners. Some of the most useful functions in OFTP are the ability to:

- Establish a direct communication link between trading partners, after initial negotiation
- Create acknowledgement of receipt
- Restart file transfers
- Automatic information exchange without any manual intervention

In addition to the above, **OFTP2** brings several improvements and new functions:

- Data Compression
- Establishment of trust and facilitation of secure communication over the Internet between trading partners (SSL/TLS, authentication, signing, encryption, etc)
- Handling of very large files (> 500 GB)
- Longer file description
- Availability of additional character sets (e.g. Chinese, Japanese etc.)

OFTP2 is backwards compatible with earlier versions of OFTP for X.25/ISDN connections.

WHAT ARE THE MAIN ADVANTAGES OF OFTP2?

GLOBALISATION OF THE AUTOMOTIVE INDUSTRY

Many companies are operating globally with purchasing, manufacturing and sales spread worldwide. Up to now it has been necessary to choose solutions for data exchange with trading partners that are specific to regional conditions (e.g. US, Europe, Asia etc.)

With the global availability of the Internet it will now be possible to use the same solution everywhere. This is true not only in a geographical sense, but also when it comes to communicating with different types of trading partners; from small local suppliers to large multi-national companies.



CHANGES IN IT INFRASTRUCTURE

One example of such changes is the closing down and/or reshaping of ISDN/X.25 network services. This has already started in the Nordic countries, in Germany and in France.

At the same time we can also see that Internet access is now available almost everywhere. Today more or less any company has access to the Internet as one of the services in their IT infrastructure. Introducing **OFTP2** would then only mean using the available infrastructure for another function.

Even if sizing of the infrastructure must take into account any new application, the introduction of **OFTP2** should only incur marginal extra costs.

CHANGES IN COMMUNICATIONS NEEDS

The amount of data being communicated between partners has been growing steadily. This has meant that older network services are becoming increasingly difficult to use, due to low speed and because of volume related pricing models.

Transmission speed could increase by as much as 25 times when moving from ISDN to an **OFTP2** 8 Mbit/s Internet service. At the same time network service cost will fall dramatically.

Transmission times would decrease even more if **OFTP2** compression is used.

ADVANTAGES COMPARED TO OTHER (NEWER) COMMUNICATION ALTERNATIVES

OFTP2 is one of several protocols that could be used for EDI communication over the Internet. 'Competitors' are mainly the protocols SFTP (SSH File Transfer Protocol) and AS2.

Advantages of OFTP2 when compared to these protocols:

- OFTP2 is the only protocol that is able to handle both older network services like X.25/ISDN, ENX, TCP/IP over Internet
- OFTP2 is designed for easy handling of very large files (> 500 GB)
- Only OFTP2 (and earlier OFTP versions) has functions for restarting and acknowledgement of receipt
- Only OFTP2 (and earlier OFTP versions) has functions for negotiation and acceptance of file size and file type.
- OFTP2 (and earlier OFTP versions) is the only protocol that is designed for handling product data exchange using the latest Version 3 of the global ENG DAT EDI message.

WHAT ARE THE MAIN PLAYERS DOING?

Many of the leading companies in Europe are already involved in testing OFTP2:

- Daimler, Volkswagen, PSA and BMW have started testing
- Scania and Volvo are planning to start testing

Skoda Auto was the first company to start using it for regular CAD exchanges in April 2009.

WHAT ARE THE LINKS BETWEEN OFTP2 AND NETWORK SERVICES?

All communication products that support OFTP2 will be able to handle data exchange using older OFTP versions and older services such as ISDN, X.31 and X.25.

Therefore nothing should stop users preparing for new requirements from trading partners by upgrading their communication products to a version that is ready for OFTP2.

We can expect that migration will be spread over a period of time since all users will not be able or willing to migrate at once. Therefore there will be a transition period where earlier and later versions will be used in parallel.

THE “OSCAR” - ODETTE ID - SERVICE

OSCAR (Odette System of Coding and Registration) assigns worldwide unique codes to any business or technical entity in the industry. OSCAR codes are intended for several purposes, one of them is the identification of individual OFTP stations.



Similar coding is already in use, but with OSCAR it will be easier to maintain one global system of OFTP station codes. It will no longer be a problem of where to find a suitable code (ICD code), for example on emerging markets.

IMPLEMENTATION

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

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)

Choosing a certificate solution

Trust and security in OFTP2 transactions is obtained by using security certificates and all users will need at least one such certificate.

Security certificates are issued and sold by specialised companies known as, 'Certification Authorities' (CAs). For a general overview of Security Certificates and how they work, go to:

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

Users have a certain degree of freedom when selecting their own CAs, but of course trading partner requirements must be taken into account.

To avoid a situation where customers and other leading trading partners ask for specific certificate solutions, Odette members have agreed to accept a number of CAs that meet a list of specific criteria.

Odette is publishing the list of approved CAs (Trust Service-status Lists, TSL), information is available on www.odette.org/tsl/tsl_oftp2.xml

This list contains the certificates recognised as being 'trustworthy', according to an agreed policy for OFTP2 applications. New CAs will be added to this list when they have been validated by Odette.

The basic principles behind the Odette Trust List are:

- Users would normally only have to select one CA in the list from which to obtain user certificates
- Every OFTP2 user shall accept certificates from any of the CAs in the TSL list

This will dramatically reduce administrative efforts for the management of the exchange of certificates.

Within the Odette community the first choice would be to select a CA from this list. An easy solution is choosing Odette as a CA, and then you would have no problem finding the right security service. You could also consult the Odette Trust List to see what other CAs such as those of industry partners (Daimler, Ford, Volvo, Bosch etc.) or third party providers (Verisign, Thawte a.o.) are listed.

Users should be aware that certificates for OFTP2 are able to handle both 'Server and Client Authentication'.

If you take part in the Odette security framework you will not have to discuss security level for data exchange individually with your trading partners, you will be able rely on security standards set up for the whole automotive industry.

Business partners will agree on which security functions (e.g. encryption and signing of files) they would apply for their business processes beyond secure communication.

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.

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.

OFTP2 PRODUCTS

There are many OFTP2 software options available from the very simple ones costing around €300 with an annual licence fee below €100, to more complex and expensive products containing several software modules at the other end of the market.

In order to validate the compliance of products to its specifications, Odette has introduced **OFTP2** Interoperability tests. Click [here](#) to check the list of Software products that have passed these tests. For more information, please go to www.odette.org or to your Odette National Organisation website.

Acknowledgements

This document has been made by a project team within Odette where the following companies and national organisations were represented:

Data Interchange	Ford-Werke GmbH	Galia
Hella	Odette Spain	Odette Sweden
PipeChain	SAP	Scania Infomate
Teledin	T-Systems Enterprise Services	VDA
Volvo Cars IT	Volvo IT	