OFTP 2
Secure Data Exchange
Via the Internet

A guideline for the practical application

Version 1.1
### History:

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Description</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>04-10-2007</td>
<td>VDA guideline for the application of OFTP2</td>
<td>D. Kaschmieder</td>
</tr>
<tr>
<td>1.1</td>
<td>01-06-2010</td>
<td>VDA guideline for the application of OFTP2 To new security recommendations and process flows updated OFTP2 quick start guideline added</td>
<td>D. Kaschmieder</td>
</tr>
</tbody>
</table>
Contents:

1 Introduction ........................................................................................................................................4
2 Overview ..........................................................................................................................................4
3 OFTP2 Security Engineering ...........................................................................................................5
   3.1 Session Security .......................................................................................................................... 5
   3.2 Data Encryption ............................................................................................................................ 5
   3.3 Signatur and Verifikation .............................................................................................................. 5
   3.4 Odette Service TSL (Trust Service Status List) ........................................................................... 5
4 Certificates for Authentication ...........................................................................................................6
   4.1 Self Signed Certificate .................................................................................................................. 6
   4.2 Certificate Authority CA ............................................................................................................. 6
   4.3 Mutually-signed Certificates ....................................................................................................... 7
5 Installation of a secure OFTP2 connection .......................................................................................7
   5.1 Basic connection for TLS encryption ........................................................................................... 7
   5.2 Exchanging encrypted and signed data files ............................................................................... 8
   5.3 Obtaining and implementing certificates .................................................................................... 8
      5.3.1 Applying for root certificate at Certificate Authority (CA) ..................................................... 8
      5.3.2 Storing Root Certificate in own OFTP2 system ..................................................................... 8
   5.4 Certificate exchange .................................................................................................................... 8
      5.4.1 Exchange via OFTP2 ............................................................................................................ 8
      5.4.2 Exchange via email and other media ................................................................................. 9
   5.5 Verification and Clearance ........................................................................................................... 9
   5.6 Process flow “Establishing of an OFTP2 Connection” ................................................................. 9
      5.6.1 Certificate request (one-time process) .................................................................................. 10
      5.6.2 Implementation of certificates in own OFTP2 system (one-time process) ............................ 10
      5.6.3 Exchange of the filled-in OFTP2 data sheet (with every new partner) ................................. 10
      5.6.4 Initial automated exchange of certificates (with every new partner) .................................. 11
      5.6.5 Encoded data transfer can be started ................................................................................... 11
6 Implementation .................................................................................................................................11
7 Functional range of the OFTP2 software .........................................................................................12
8 Future prospects ...............................................................................................................................12
9 References .........................................................................................................................................13
10 Author .............................................................................................................................................13
11 Glossary ..........................................................................................................................................13

Appendix:
OFTP2 Quick Start Up .........................................................................................................................16
1 Introduction

This guideline is designed for supporting the implementation of security mechanisms, in order to exchange engineering data with the Odette File Transfer Protocol OFTP2 by communication interfaces, such as the Internet, ISDN and ENX.

It is therefore essential to show solutions, according to security requirements of the involved parties, company-specific safety policy and subject to classification of the exchanged data, and to provide assistance with decisions on the practical application.

Applying in particular for operating OFTP2 via the Internet, the procedural method can also be adopted when operating via ISDN, however. Additional security measures for the data exchange via ENX are suggestive, if the installed OFTP2 software can provide extra protection between the ENX router at the company’s Border Gateway and the OFTP2 server, or if authentication by signature shall be increased, once again.

Furthermore, this guideline serves on the one hand for describing the procedure and use of the security mechanisms as accurately as possible, in order to keep the effort for the application, in close coordination with the safety policy of the companies, to a minimum, and on the other hand, to ensure a standardised approach among the data exchange partners, allowing the interoperability to flow as smoothly as possible.

In addition, the VDA OFTP2 data sheet form will serve for an easier connecting process between the OFTP2 systems by a regular process of the parameter data exchange with the partner and serves primarily the OFTP2 software developers as a working basis.

2 Overview

The Odette recommendation of Odette File Transfer Protocol Version 2 (OFTP2) describes in particular security mechanisms, such as encryption and signature, but also features like data compression and TLS layers. The installation process of the security mechanisms within the partner connection, comprising its features and parameters, is documented in the Odette OFTP2 Implementation Guidelines with examples, in detail.

This VDA guideline is intended as a complement to the Odette recommendation and to the Odette Implementation Guidelines, as a help for the better understanding for connecting the OFTP2 application within the engineering environment.

The process flow presents, without claiming to be exhaustive, the application for OEMs and major suppliers, but also the application for small suppliers. In either case, the approach and process must be brought into agreement with the company-internal terms of data security and aligned, if necessary.

The guideline is based upon the OFTP2 recommendation, where again standard security methods such as X509 V3, are underlying.

The classification and operation of the security measures is dependent on form and confidentiality of the transferred data and on the needs of security requirements, involved for unauthorized access and feint of another sender or recipient. The sender of the data must therefore weight the expense against the avail of the security solutions for the respectively exchanged data, and decide on the best solution for him and his partner, by means of the security mechanisms, described in this guideline.
With the choice of the OFTP2 software products is to be paid attention to the fact that the offered software has passed the process of the Odette Interoperability tests successfully and listed as certified OFTP2 software on the Odette homepage. This reduces the danger of being not compatible with other OFTP2 data exchange systems.

3 OFTP2 Security Engineering

The data transfer via the Internet and also via other communication media, requires high security standards. The approach and the employment of certificates for data encoding was fixed by an Odette working group SCX (Security Certificate Exchange) with participation of European OEM's, suppliers and system manufacturers. The results are summarised into the Odette document OFTP2 Certificate Policy and are a base for the security policy in the individual enterprises.

Three security levels have been defined for OFTP2:

3.1 Session Security

A TCP/IP connection is established with SSL/TLS encryption. In this progress, every single TCP/IP package is encrypted. The certificates are based on the X509 format, a crucial standard for the Public Key Infrastructure (PKI), and on the CMS format (Cryptographic Message Syntax) to create a digital signature for the data transfer.

3.2 Data Encryption

The data is encrypted asymmetrical. The encryption is based on the assignment of a linked key pair (public and private key), whereas one key is used for encryption and the other one for decryption. Thereby the Public Key, one of the two keys, is made public, i.e. disclosed and respectively transmitted to the partner, and can be used by each sender to encrypt a data packages for the recipient, the owner of the private key. Only the recipient is therefore able to decrypt the message.

3.3 Signatur and Verifikation

In this progress, a “Hash” of the data is created. The function of Hash values is significant. They are used for searching and identifying files, and also for detecting and checking transferred file fragments. In this way, large data can be exchanged reliable into small segments. The Hash values are encrypted (signed) by the own private key.

3.4 Odette Service TSL (Trust Service Status List)

A result from the Odette working group SCX is the establishment of a service of the so-called TSL (Trust Service status List). This service contains a list of all certificate providers (CA’s), who have asked for an admission in the OdetteTSL list and therefore are checked by Odette International according to agreed criteria and are taken up with positive result in this list. With receipt of a partners certificate the OFTP2 system is accessing this TSL list and therefore the trustworthiness of the certificate providers is checked.
4 Certificates for Authentication

Three mechanisms for creating the certificate are described. These methods serve for highly reliable identification of the partner’s authentication. The real encryption method for the sent data will remain unaffected. Following methods are available:

<table>
<thead>
<tr>
<th>Method for creating a certificate</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self-signed Certificate</td>
<td>Partner creates own certificate. Verification by call back via phone or alike is essential for this progress.</td>
</tr>
<tr>
<td>Certificate Authority (CA)</td>
<td>Partner gets certificate from one or more accredited Certificate Authorities. Verification of authentication is recommended.</td>
</tr>
<tr>
<td>Mutually-signed certificate</td>
<td>Certificate verification is counter-signed by data transfer partner and certificate is sent back. Security will be increased once more, if counter insurance for authentication takes place.</td>
</tr>
</tbody>
</table>

As a rule, the certificates include the public key and the signature of the partner. The necessary applications for both, generating certificates and importing the received certificate – after verified authentication – should be provided by the system developers within the data exchange systems. Interfaces between external security systems are also helpful, e.g. the connection to a captive security system for the certificate administration (Key-Server).

4.1 Self-signed Certificate

The “Self-signed Certificate“ is in many cases sufficient for an encrypted data exchange. The advantage of this method is a relatively simple way of generating the certificate and to exchange, without additional costs. The disadvantage consists in the fact that for the partner (receiver of the certificate) it is not transparent and costly, such a certificate to authenticate, as with a certificate of an authorised service provider (CA).

Before such a certificate is entered in the OFTP2 system, an examination of the authentication of the partner has to be carried out, e.g., by a phone call.

Therefore, the use of a Self Signed Certificates is not recommended by Odette on reasons of the higher manual examination expenditure.

4.2 Certificate Authority CA

In this case, a certificate is issued by an authorized position (Certified Service Provider) according to the requirements, and placed to the applier’s disposal. This is carried out only once before starting OFTP2 operation and is associated with a low fee.

Furthermore, the decision which authorized institution (CAs) shall be used for this service, has to be made. A large number of services providers is available, e.g. Odette International, VeriSign, ValiCert, etc., offers also these services. Some OEMs see themselves as Certificate Authority and place the generated root certificates to the partners’ disposal.
The list of root certificates can be loaded into the OFTP2 software by the CA via Internet. As a result, authentication of the partner can be effected directly with the own OFTP2 system, for incoming data.

4.3 Mutually-signed Certificates

In the course of jointly-signed certificates, a certificate request is made to the partner at first. The request is counter-signed by the other partner and will be sent back as certificate on a secure way, after authentication. Only now, the original sender of the request is able to import the certificate and decrypt incoming data with his own private key.

5 Installation of a secure OFTP2 connection

OFTP2 has been developed for the implementation and operation of secure partner connections and thus for a secure data exchange over these connection devices.

For the encrypted data transfer, the respective contractor of the business connection must get involved and request a certificate from the partner, unless this has already been exchanged during the installation of the connection and was imported into his system. Accordingly, he takes the role of “Partner A” in the following description of process flows.

The facility of certificates should be functionally supported by the OFTP2 software as a widely automated process.

As a rule for a data exchange connection, data is transferred in both directions. It is therefore recommended, that both partners give order to create certificates and send it, respectively to send a certificate yet created to the other partner, before sending CAD data.

For exchanging data with lower security requirements, session encryption of the built-up OFTP2 connection, as described under 5.1, will be sufficient.

5.1 Basic connection for TLS encryption

For the most simple installation of an OFTP2 connection via TCP/IP, only the data stream is encrypted (TLS), i.e. only the point-to-point connection is encrypted before transfer, but not the data itself. Authentication of the data packages by signature verification isn’t performed either.

Consequently, the data files themselves are not encrypted and won’t be signed. Data compression can be used as an option of the OFTP2 system. This is to be recommended particularly by the transfer of big amounts of data.

A certificate is automatically exchanged for the session build-up. When selecting the Self-signed Certificate however, a certificate has to be exchanged manually with the partner in advance. This isn’t necessary in case of using Root Certificates of a CA the flow gets automated, in the sense of “Chain of Trust”.

The partners should decide in individual cases, whether the session encryption (TLS) is sufficient for the transferred data, regarding confidentiality and authentication.
5.2 Exchanging encrypted and signed data files

In this case, certificates must be generated first of all, respectively a Root Certificate obtained by Certification Authority (CA), and exchanged with the partner as preliminary measure.

5.3 Obtaining and implementing certificates

As a rule it is advised to apply for a certificate at a certificate authority (CA) listed in the Odette TSL outside the OFTP2 system. Different certificate graduations, in dependence of own security standards, can be requested.

If Odette International is chosen as a certificate authority (CA) an application form can be filled in on-line. Odette passes on the application for verification of the applicant to the national car organisation, e.g., for German companies to the VDA which checks the application for trustworthiness according to agreed criteria. This is an on-line process and takes usually only a few days and it enhances the security for all involved partners, the have chosen Odette International as a CA.

5.3.1 Applying for root certificate at Certificate Authority (CA)

With the application of a certificate should be considered which kind of certificates should be applied for, e.g., only for session encoding (TLS) or also for file encoding and signature. One is prepared for the future if the full functionality of a root certificate is applied for.

5.3.2 Storing Root Certificate in own OFTP2 system

After receipt of the applied certificate this should be installed in the own OFTP2 system. It is a self-evident fact to protect this certificate in the system against not authorised access and giving access only to few, for it authorised personal. A secure option is to store the certificate or private key in a „Key Server“ especially assigned for it and establish a secure access to it within the OFTP2 system.

5.4 Certificate exchange

5.4.1 Exchange via OFTP2

The certificate owner transfers the public part of the certificate (Public Key) to the partner. The certificate will be imported by its recipient into the database of his own OFTP2 system, by means of the respective software after a check in the TSL list. He is now able to transfer encrypted data to the sender of the certificate.

An automated process via OFTP2 with verification by fax, email or phone would be preferred for the initial implementation of an encrypted data transfer. Automated processes are throughout preferred for revoked keys or cyclic renewals.

The exchange of the certificate (Public Key) is to be carried out only once before the beginning of the first data transfer with every partner with special commands using the OFTP2 connection and should be for security reasons accompanied in parallel by using other media (phone, fax or email) for verification.
The software manufacturer should provide the opportunity of an automated management of certificate exchange by OFTP2 commands in his OFTP2 software. The software must be in the position to detect specific certificate commands and support the entire process of generating, exchanging and installing certificates, in association with an appropriate user interface. Consequently, the exchange can be easily operated by an automatic generation of separate messages, e.g. fax for verifying the certificate’s authentication.

5.4.2 Exchange via email and other media

Sending the certificate via email is only approvable, if the recipient is verifying the certificate’s authentication manually, at the same time. For secure assignment and authentication of the certificate’s sender, an accompanying fax with the certificate notice must be sent, parallel to email, to the administrator of the certificate’s recipient, or verified by phone call.

The certificate’s recipient should confirm either by email, phone or fax, that he’s ready to send encrypted data to the sender of the certificate, taking instantly effect on his data exchange process with the partner.

Certificates can also be exchange by offline media, such as CD. However, it is recommended to deliver these media personally or by a reliable courier service. The residual course of confirmation should be carried out, as already described.

By Odette it is recommended to choose this way only if the OFTP2 software supports no automated exchange.

5.5 Verification and Clearance

The responsibility for verification and clearance on the certificate import is assumed by the certificate’s recipient. He should therefore provide secure authentication of the partner and gain certainty about the verification of the certificate via phone or fax, before providing clearance for the productive operation, in case of doubt.

5.6 Process flow “Establishing of an OFTP2 Connection“

The use of a CA service is recommended by Odette if not own security systems in big companies are prescribed for generating certificates. As already mentioned above, the chosen CA must be listed in the Odette TSL as a trustworthy CA or the Odette CA service is taken up directly.

Decisions for filling in of a certificate application:

- Which CA should be chosen for applying a certificate (only CAs listed in the Odette TSL or with Odette itself)
- Which kind of certificate
  - with session encoding (TSL)
  - with file encoding
  - with signature (validation of the data authenticity)
This process is carried out only once by installation of the OFTP2 system. The management and the validity of the certificate, as a rule for two years, has to pay attention the owner himself.

5.6.1 Certificate request (one-time process)

Remark: The partners A and B of course can apply for a certificate also at the same CA.

5.6.2 Implementation of certificates in own OFTP2 system (one-time process)

Implementation of the received certificate in the own OFTP2 system is performed in general manually with system support.

5.6.3 Exchange of the filled-in OFTP2 data sheet (with every new partner)

The OFTP data sheet serves as a submission for the exchange of the OFTP parameters with the partner. The information necessary for establishing an OFTP connecting is to be filled-in in each case. For OFTP2 connections information about the own encoding method and the encoding method expected from the partner, as for example only session encoding, file encoding or also signature of the files, must be filled-in.
5.6.4 Initial automated exchange of certificates (with every new partner)

This is a standard OFTP2 function carried out "at the touch of a button". The sender receives back a receipt about the successful exchange and with it also the feedback that the system is ready for encoded date transfer.

![Diagram of OFTP2 exchange]

A certificate request of an OFTP2 system is also possible. The request is sent automated to the partner and a certificate of the partner is then sent back automatically when the partner has implemented his certificate in his system.

An exchange of several certificates with one partner with different attributes is also possible. The intension in this case is to set up the system for transferring data with different security classifications.

5.6.5 Encoded data transfer can be started

![Diagram of encoded data transfer]

6 Implementation

Before implementing the OFTP2 software, following issues must be cleared by the person in charge in accordance with the responsible person for security:

- What security level shall be arranged with which partner, respectively is predetermined by the partner.
- Does encryption of the connection meet the requirements or should the data itself also be encrypted - and possibly be signed, as well.
- Which communication media (Internet, ISDN and ENX) does the partner supports.
- Is an established Key server available for the encryption, or would the integrated Key Management system of the OFTP2 software be operated.
- Expense and costs should be weight up for minor installations. A fully-automated certificate exchange with supported verification process, against a semi-automated process with manual verification, for example.
The hardware resources should be checked for the OFTP2 system, as encryption and decryption of transferred data require considerable computer resources.

For a frictionless and unobstructed operation with sufficient performance, as claimed by the user, a pilot operation with some partners would establish once more security and experience.

A step-by-step implementation of the encryption is easily possible, as OFTP2 is therefore compatible downwards, i.e. OFTP V1.4 and older versions are still supported by OFTP2.

In order to set up an OFTP2 connection efficient, either the form of the Odette OFTP2 Implementation Guide Lines, included in the annex, or the more simplified VDA form should be used for the exchange of OFTP2 parameters. These forms support and accelerate a quick implementation of an OFTP data exchange connection, by means of predefined parameter fields and options to be marked.

### 7 Functional range of the OFTP2 software

Apart from the real data exchange, the following functional range of the OFTP2 software is designed:

- Support of implementation of the own certificate
- Automatic exchange of certificates
- Set-up of secure connections via the Internet, ISDN und ENX
- Validation after every OFTP2 connection start up in TSL and CA list if certificate of the partner is valid

Other functions are integrated for the efficient data transfer, beside the implementation of security relevant measures for the connection setup of OFTP2, which can be used optional:

- Data compression / decompression
- Encryption / Decryption of data files
- Signing of data files (authentication) / Verification of authentication
- CRL-check (Certificate Revocation List) to verify validity of the certificates
- Data transfer of large-volume data packages

Furthermore, OFTP2 is compatible downwards and is also supporting data transfer connections with partner lower than OFTP V1.x, including the associated functional range and security levels.

### 8 Future prospects

OFTP2 will gain more in importance by using the Internet for the data transfer, even beyond Europe. The implemented security mechanisms provide more safety to the OFTP2 data transfer, not only via the Internet, but also via previous communication media, such as ISDN and ENX.
Easily operated security functions and their implementation, according to a generally accepted, widely automated approach, will be essential for an effective, broad and worldwide application. The security measures and the software-implemented technology must be therefore presented transparent to the company’s responsible person, in order to meet the high standard of a secure, high-performance data transfer, at any time.

9 References

RFC 2204 (Request for Comments) of the Network Working Group by Odette OFTP2 Working Group
Odette OFTP2 Implementation Guide Lines
Request for Registration on Odette’s Trust-Service Status List (TSL)
SCX Proposal for “Odette recommended” CA’s

10 Author

Dietmar Kaschmieder, KCS Kaschmieder Consulting & Services
By order of VDA working group “DFÜ” and in collaboration with the Odette OFTP2 Support Group

11 Glossary

Asymmetric cryptography: Is a form of cryptography in which a user has a pair of cryptographic keys, a public key and a private key. The private key is kept secret while the public key may be widely distributed. The keys are related mathematically, but the private key cannot be practically derived from the public key. A message encrypted with the public key can be decrypted only with the corresponding private key.

Authentication: Is the act of establishing or confirming something (or someone) as authentic, that is, that claims made by or about the thing are true. Authenticating an object may mean confirming its provenance, whereas authenticating a person often consists of verifying their identity.

Border Gateway: Controls the availability of communication lines between networks of autonomic systems

Certificate: In this case a digital certificate for establishing encryption

Certification Authority (CA): Is an entity which issues digital certificates for use by other parties. It is an example of a trusted third party. CAs are characteristic of many public key infrastructure (PKI) schemes.

Certificate Request: Request of a certificate for data encryption

CAD data: Digital design data

Chain of Trust: Is established by validating each component of hardware and software from the bottom up. It is intended to insure that only trusted software and hardware can be used while still remaining flexible.

CMS-Format: (Cryptographic Message Syntax): Is the IETF’s standard for cryptographic protected messages. It can be used to digitally sign, digest, authenticate or encrypt any form of digital data

CRL: (Certificate Revocation List): Is a list of certificates (more accurately: their serial numbers) which have been revoked, are no longer valid, and should not be relied on by any system user
Data compression / decompression: Is the process of encoding information using fewer bits (or other information-bearing units) than an un-encoded representation would use through use of specific encoding schemes.

Digital signature: Is a type of asymmetric cryptography used to simulate the security properties of a signature in digital, rather than written, form. Digital signature schemes normally give two algorithms, one for signing which involves the user's secret or private key, and one for verifying signatures which involves the user's public key. The output of the signature process is called the "digital signature."

Engineering data: Is data of technical content, for example CAD data

ENX: Stays for European Network Exchange and is a private network for the European automotive industry

ENX-Router: Is a router dedicated to the ENX network for the control of network sections

„Hash“ of data: Is a reproducible method of turning some kind of data into a (relatively) small number that may serve as a digital "fingerprint" of the data

Internet: Is a worldwide, publicly accessible series of interconnected computer networks that transmit data by packet switching using the standard Internet Protocol (IP)

ISDN: Integrated Services Digital Network (ISDN) is a circuit-switched telephone network system, designed to allow digital transmission of voice and data over ordinary telephone copper wires, resulting in better quality and higher data speeds than are available with analog "plain old telephone service"

IP address: Internet Protocol address is a unique address that certain electronic devices use in order to identify and communicate with each other on a computer network utilizing the Internet Protocol standard (IP)

Key server: Is a server on which public keys are stored for others to use

Odette: Organization for Data exchange by Tele Transmission in Europe is a non profit organization that represents the interests of the automotive industry in Europe; equivalent of AIAG in America.

OEM: Original Equipment Manufacturer, the original manufacturer of a product, which may be resold by another company, in this case a car manufacturer

Off-line media: Data storage media like CDs, DVDs, Tapes, which can be transported and be recorded or read in other computer

OFTP parameter: For establishing of an OFTP data link which is exchanged with partners and stored into an OFTP system

OFTP2 Implementation Guidelines: A guideline created by the Odette working group OFTP2 for implementing the OGTP2 software.

OFTP V1.4, V1.x: Older software version for technical and business data in the automotive industry

PKI: Public Key Infrastructure, is an arrangement that binds public keys with respective user identities by means of a certificate authority (CA). The user identity must be unique for each CA. This is carried out by software at a CA, possibly under human supervision, together with other coordinated software at distributed locations.

Public-Key: Also known as asymmetric cryptography, is a form of cryptography in which a user has a pair of cryptographic keys - a public key and a private key. The private key is kept secret, while the public key may be widely distributed. The keys are related mathematically, but the private key cannot be practically derived from the public key. A message encrypted with the public key can be decrypted only with the corresponding private key.

Revoke: Revoke also means "To cancel or annul". Is withdrawal of a public key in case of misuse or can be revoked periodically after a certain period of time

Root Certificate: Is either an unsigned public key certificate or a self-signed certificate. A root certificate is part of a public key infrastructure scheme.

SCX: Security Certificate Exchange: Is a recommendation for the handling of certificates for secure data exchange with OFTP2 issued by the Odette working group SCX.

Secure Session https: Hyper Text Transfer Protocol Secure is a URI scheme used to indicate a secure HTTP connection. It is syntactically identical to the http:// scheme normally used for accessing resources using HTTP. Using an https: URL indicates that HTTP is to be used, but with a different default TCP port (443) and an additional encryption/authentication layer between the HTTP and TCP. This system was designed by Netscape Communications Corporation to provide authentication and encrypted communication and is widely used on the World Wide Web for security-sensitive communication such as payment transactions and corporate logons.
Self signed certificate: Is an identity certificate that is signed by its own creator. That is, the person that created the certificate also signed off on its legitimacy.

Service Provider: In this case IT service provider

Signature: In this case the digital signature of a data transfer

SSL/TLS: Secure Sockets Layer (SSL) or Transport Layer Security (TLS), SSL is a communications protocol, predecessor to Transport Layer Security

TCP/IP: Transmission Control Protocol (TCP) and the Internet Protocol (IP), is the set of communications protocols that implement the protocol stack on which the Internet and most commercial networks run.

TLS layer: Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide secure communications on the Internet for such things as web browsing, e-mail, Internet faxing, instant messaging and other data transfers.

Secure Sockets Layer (SSL): Is a communications protocol, predecessor to Transport Layer Security (TLS)

TLS encryption: Encryption protocol for data transmission on Internet

TSL: Trust Service Status List, a list of Odette International certificated CA’s. Only these CA’s are admitted for issuing certificates for the OFTP2 application.

X509 V3: Is a standard for Public Key Infrastructure (PKI)
### OFTP2 Quick Start Up

Check list as a help to the OFTP2 system administrator for setting up of an OFTP2 connection

<table>
<thead>
<tr>
<th>Action Item</th>
<th>Done</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Purchase OFTP2 system</td>
<td></td>
<td>Only software certified by Odette. List on Odette homepage available.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="https://forum.odette.org/OFTP/oftp2">https://forum.odette.org/OFTP/oftp2</a></td>
</tr>
<tr>
<td>2 Requesting Odette ID</td>
<td></td>
<td><a href="http://forum.odette.org/service/oscar">http://forum.odette.org/service/oscar</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>If no OFTP connection exists so far</td>
</tr>
<tr>
<td>3 Obtain certificate</td>
<td></td>
<td>Direct at Odette <a href="https://www.odetteca.com/">https://www.odetteca.com/</a> or at other Certification</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Authorities (CA) listed on the Odette Trust Service List (TSL)</td>
</tr>
<tr>
<td>4 Choosing of the security level for encrypted</td>
<td></td>
<td>Choice depending to the demanded security</td>
</tr>
<tr>
<td>data transfer (the partner should chose the</td>
<td></td>
<td>quality for the data transfer</td>
</tr>
<tr>
<td>same level)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5 Filling out the OFTP2 data sheet and send it</td>
<td></td>
<td>Referring to „OFTP / OFTP2 Data and Parameter</td>
</tr>
<tr>
<td>to partner by Fax or email (section &quot;Partner A&quot;</td>
<td></td>
<td>Sheet“ of the VDA</td>
</tr>
<tr>
<td>or &quot;B&quot; depending on sender or receiver of the</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sheet )</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6 OFTP2 data sheet returned back from partner</td>
<td></td>
<td>Date of the partner should be checked before setting up the connection</td>
</tr>
<tr>
<td>filled in with his parameters</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7 Setting up OFTP2 basic connection</td>
<td></td>
<td>SSID, SFID, etc.</td>
</tr>
<tr>
<td>8 After reception of own certificate entering</td>
<td></td>
<td>Automated setting up should be supported by the OFTP2 system</td>
</tr>
<tr>
<td>this in own OFTP2 system</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9 Sending own certificate (public key) to partner</td>
<td></td>
<td>Automated sending by OFTP2 system</td>
</tr>
<tr>
<td>10 Certificates (public key) of the partner</td>
<td></td>
<td>Automated reception by OFTP2 system</td>
</tr>
<tr>
<td>received</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11 Storing partner's certificate in own system</td>
<td></td>
<td>Automated storing after validity check in Odette TSL list by OFTP2</td>
</tr>
<tr>
<td>after validity check via Odette TSL list</td>
<td></td>
<td>system</td>
</tr>
<tr>
<td>12 Announcing completion of the OFTP2 connecting</td>
<td></td>
<td>By phone or fax</td>
</tr>
<tr>
<td>to partner and agree on tests</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13 Carrying out test date exchange</td>
<td></td>
<td>Encrypted data exchange in both directions</td>
</tr>
<tr>
<td>14 After tests successful completed</td>
<td></td>
<td>Feedback to partner is recommended</td>
</tr>
<tr>
<td>Ready for productive use</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**VDA DFÜ AG**

**Dietmar Kaschmieder**

**Version:** 1.1

**Date:** June 2010