Whitepaper –

Modern platform for secure and traceable data exchange with SWAN

SSC-Services GmbH
Volker Klingenstein (Sales)
v.klingenstein@ssc-services.de
Herrenberger Straße 56
71034 Böblingen
Germany

SSC @ Social Media:

Internet:	http://www.ssc-services.de
Facebook	@SSC-Services GmbH
Instagram	@SSC-Services GmbH
Twitter	@SSC-Services GmbH
LinkedIn	@SSC-Services GmbH
Xing	@SSC-Services GmbH

Contents

1 Exchange of engineering and product data

Data exchange between development partners is characterised by increasing complexity and continuously growing volume. This means supporting standards and providing a high degree of flexibility. The integration of individual requirements with respect to exchange processes and the connection of third-party systems set further requirements to a modern data exchange platform.

In addition to the basic functionalities that technically implement data exchange, other criteria are becoming increasingly important for companies. The priority is to ensure reliability and traceability, as more and more data is exchanged worldwide. However, the number of data exchange partners is constantly increasing, too. Any information about the successful transmission, the exchanging parties, the time, and the data itself, must be mandatory. In addition, high-risk data islands such as email inboxes and insecure transmission paths (e.g. FTP) must be avoided.

2 SWAN - the system for the worldwide exchange of data

Wherever companies work together, data is exchanged and managed. Data exchange between development partners is particularly sensitive. SWAN is a professional data management system for data exchange between development partners (with https and other OFTP/OFTP2 protocols). SWAN offers a modular solution that covers all requirements for secure data exchange in the engineering sector. Basically, any file format can be transferred with SWAN. In the development environment, especially in the area of construction data exchange, the requirements for SWAN have increased more and more in recent years.

During development, care is taken to use existing standard software. Thereby SWAN can guarantee, among others, the following points and support basic functions.

- Simple and intuitive GUI use
- High security mechanisms
- Secure upload of data through TLS encryption
- Complete data archiving
- Outstanding flexibility for individual process design
- Exchange of any data format without size limitation
- Multi-level authentication concept
- Improved administrability
- More flexibility for integration of requirements outside the standard functions
- Line and data encryption via internet and the https/scftp/scp/OFTP standards
- Sending and receiving according to OFTP/OFTP2
- ENGDAT-Standards, Version 2 and 3 (VDA 4951)

- ENGPART for the description of partner profiles
- Data transmission via IP (Internet) and ENX
- We provide an easy way to connect to and from third party systems with a REST API (HTTP-based RESTful web services).

3 The SWAN- Architecture

3.1 Overview

There are various options for installing SWAN. All components such as the application server (SWAN server), database server and Web-Server can be installed on a physical server or a virtual machine (VM) (single installation) or distributed over several units. Installing the web server on one VM and the application server and database server on another VM has proven to be the best solution.

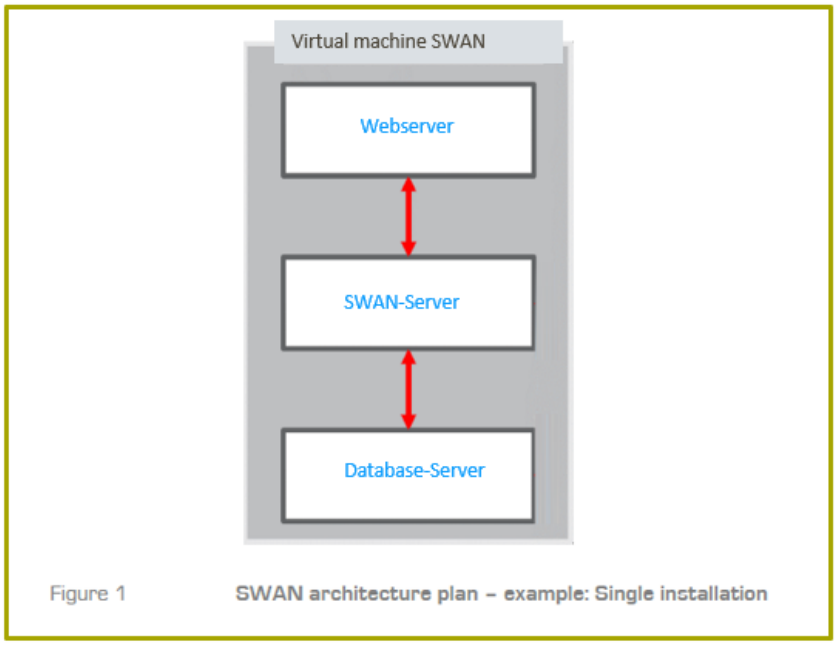


Figure 1 SWAN architecture plan – example: Single installation

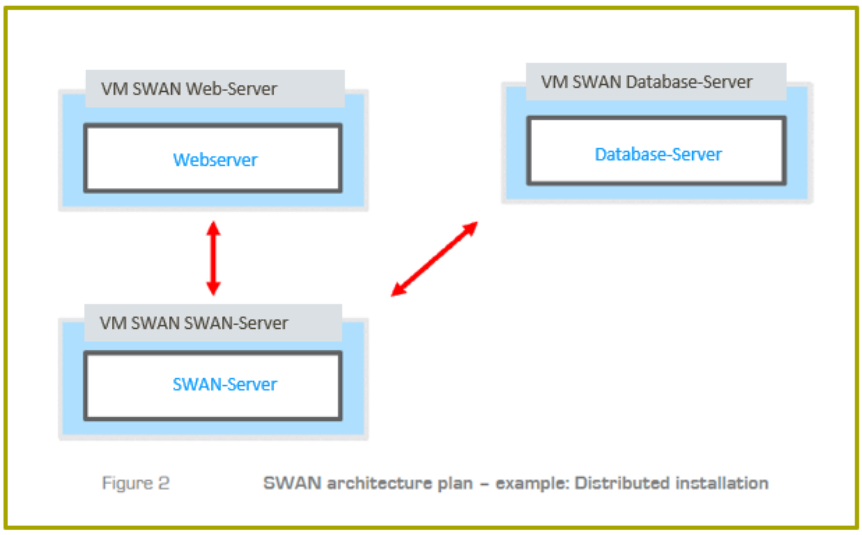


Figure 2 SWAN architecture plan – example: Distributed installation

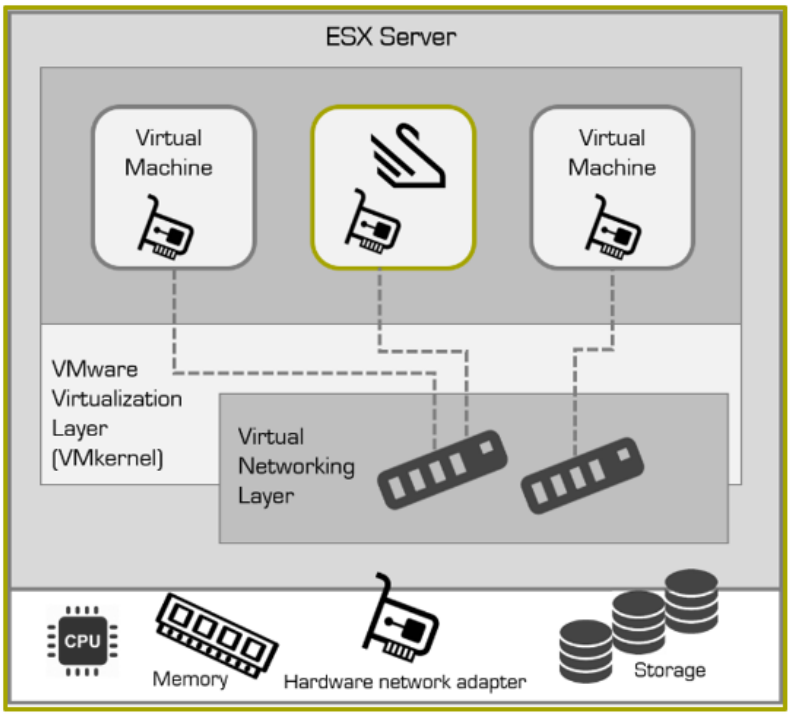


Figure 3

3.2 Database

DB2 Express-C is used as the database server for the SWAN. IBM DB2 Express-C is a royalty-free community edition of DB2 Server with the central functions of the more scalable editions of DB2.

3.3 ActiveMQ

Apache ActiveMQ is a powerful open source message broker that fully implements the Java Message Service 1.1 (JMS). Apache ActiveMQ increases the number of connections of a network between existing applications by converting synchronous communication between applications to be integrated into asynchronous communication. The application server (SWAN) is able to process ActiveMQ messages. It is easily possible to outsource resource-intensive process steps, such as conversion, quality check, etc., to remote systems. By processing these steps asynchronously, an incoming job, for example, is paused until an OK is received from the remote system for further processing of the step.

3.4 Apache Web-Server

Depending on the installation, WildFly is used as a web server, too. "The Apache http server is the most widely used web server on the Internet. Besides Unix and Linux, Apache supports Win32, NetWare and a variety of other operating systems. The Apache web server has a modular structure. By means of corresponding modules, it can, for example, encrypt the communication between browser and web server (mod_ssl), be used as a proxy server (mod_proxy) or carry out complex manipulations of http header data (mod headers) and URLs (mod_rewrite). Apache offers the possibility to create web pages dynamically using server-side scripting languages. Commonly used script languages are PHP, Perl or Ruby. These are not part of the web server, but must also either be integrated as modules or addressed via the CGI [Common Gateway Interface]. Server Side Includes (SSI) can be executed via the mod_include included in the Apache installation. This makes it possible to create simple dynamic websites and to minimise the administration effort of static websites.“ [REFERECE?]

3.5 SWAN-GUI

SWAN has a modern, functional and multilingual interface that makes it easy for you to create and collect your SWAN-Jobs with an intuitive operating concept.

You can use all functions via two individually configurable main views (Job-creating Page and SWAN Joblist) and via the global elements of the GUI (quick search and extras menu) you can go directly to the SWAN_Job you are looking for or access the display and various setting options of your profile data, help pages or SWAN support. You can also find more information in our user manual.

3.6 SWOX

The OFTP2 system SWOX integrated in SWAN, an SSC in-house development, fully complies with the requirements of the OFTP2 specification (RFC 5024) and received the certificate for products tested for OFTP2 compliance and interoperability from the Odette organisation in March 2017 (link to ODETTE).

Classic OFTP data exchange is the core discipline of SWAN. As soon as a recipient with an OFTP address code is known, it can easily be added to the partner database in SWAN and the secure data exchange can begin.


ODETTE OFTP2

This is to certify that the software product

SWOX

from

SSC-Services

has successfully passed the

OFTP2 Interoperability Tests

The software has demonstrated compliance with the OFTP2 (Odette File Transfer Protocol V2) specification as published in RFC-5024, in accordance with the test scenario as described in OFTP2 Interoperability Tests – Test Cases V2.3.9

Certificate N°: 10030

Stephanie Bioux
Odette International Ltd

Date 28 February 2017

Odette International Ltd | 71 Great Peter Street | London SW1P 2BN United Kingdom | Registered in England N° 4039150

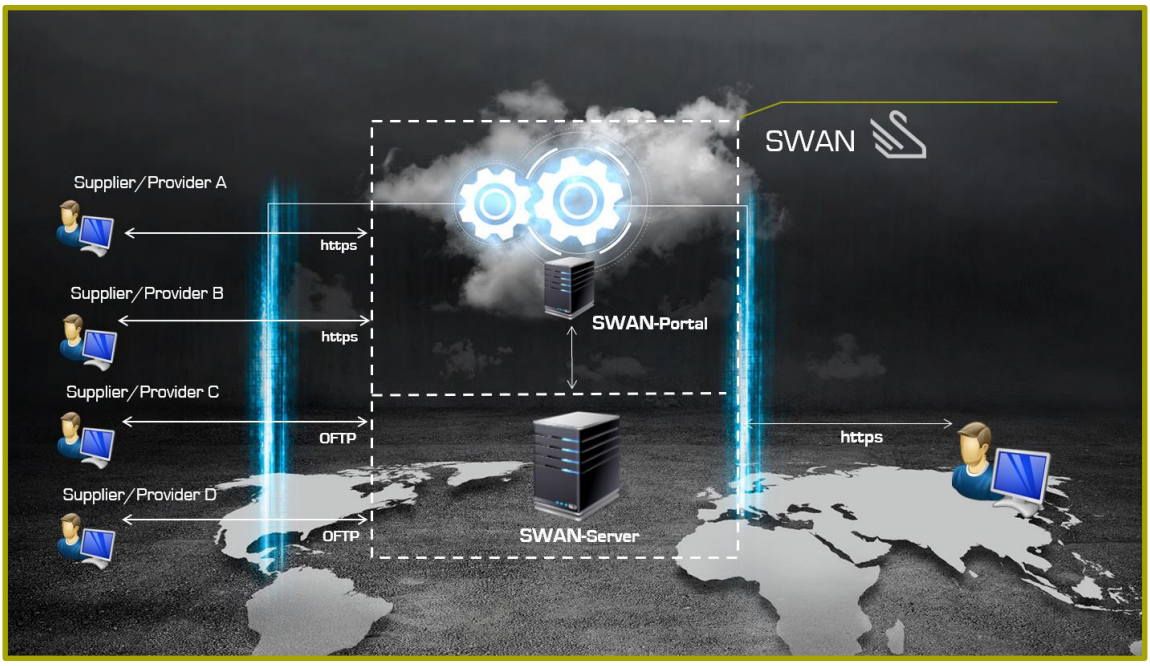
All standards according to OFTP/OFTP2 and ENGDAT standards, version 2 and 3 (VDA 4951) are supported. There are no restrictions regarding file size and file formats. The configuration and management of OFTP partners is done entirely through the SWAN GUI, so you only need to maintain your partners in one place. The SWOX GUI gives you a transparent overview of the current sending and receiving process of jobs to all OFTP partners.

The actual sending and receiving of data is managed by the SWAN GUI, the actual data exchange management tool. The sender of a SWAN job is automatically informed by email when the job has been successfully sent and received.

3.7 SWAN virus scanner

The virus scanner that can be integrated into SWAN checks send and receive jobs for viruses. The SWAN virus scanner is to be understood as an integrated module with which we are able to connect your local anti-virus scanner. The procurement and licensing of the anti-virus software is the responsibility of the customer. If a virus attack is detected, all actions available to a normal user on a job are disabled. This prevents the collection or forwarding of infected files. Depending on the configuration, a SWAN administrator can delete the infected files manually or SWAN can undertake this task. Even after deleting the data of a job, the virus attack is clearly documented and verifiable via log files and information in the job history.

3.8 SWANportal



With the SWANportal, we offer you a reliable, secure and traceable platform for data exchange with your partners. This is a portal solution for the access of your external partners to your customer's own SWAN via the Internet (https). The installation and initial setup of the software takes place on the SWANhosted IT infrastructure. We take care of the administration, operation and support of your users. Together with you, we realise a solution to operate the SWANportal according to your IT security specifications.

3.9 SWaX

The **SW**AN**a**utomated data e**X**change module is used for the regular supply of data to your partners within the framework of an automatic data exchange. Your data can be further processed by SWAN at defined points in time or project statuses in a follow-up process. Using SWaX, it is no longer necessary to send or enter data manually. As with all automated systems, however, it must always be ensured that the necessary authorisations for accessing the source and target directories or source and target systems are available on the corresponding side.

3.10 SWAN Ad-hoc Function

The ad hoc function enables data to be sent directly to the e-mail address of a recipient who is not registered in the SWAN database. The retrieval of data can be protected by a password generated by SWAN.

The recipient is informed of the data dispatch by e-mail and can collect the data via a link contained in the e-mail with a limited lifetime, if necessary, after entering the password, via a special user interface. The SWAN ad-hoc function: “Send to e-mail address with reply” includes the possibility to reply to the sender once and to send data to the sender. With the SWAN ad-hoc function: “Request ad-hoc request”, a SWAN user can request a communication partner not entered in the SWAN database to send data.

3.11 3D CAD preview (optional)

The SWAN preview is available as an optional, chargeable module. All SWAN users are given the option of displaying CAD files contained in a job directly in their browser. With the function, CAD files are displayed directly in the output as well as in the input. The file is displayed directly in the browser on the right-hand side in the reading area in a new display area for both sent and received files. The visualisation also takes place if the files are sent in a ZIP container. Currently, the following file formats are supported in the current version: CATIA V5, Siemens NX and the neutral formats JT, STEP and IGES.

3.12 REST-API

For the simple connection of SWAN to third-party systems or of third-party systems to SWAN, SSC offers a REST API interface. Using this interface and its detailed documentation, it is very easy to realise the integration/connection of your company applications such as EDM (Engineering Data Management), ERP (Enterprise Resource Planning), PDM (Product Data Management), CAD (Computer-Aided Design, ... It should be noted that adjustments are usually

also necessary to the REST interface of the local PDM system, where we are dependent on the corresponding interface developer. If necessary, we provide our detailed REST documentation.

We currently have REST interfaces to the PDM systems Teamcenter, CIM Database and CAD Portal.

4 The SWAN Security concept

4.1 Hosting in a data center

The entire SWAN infrastructure can be hosted in a data center. SSC has its own computing center and it is also possible to run SWAN in the AZURE cloud. Here is an overview of the essential security features of the SSC computing center:

- ISO 27001 certification on the basis of the IT baseline protection methodology of the German Federal Office for Information Security
- TeleTrusT quality mark "IT Security made in Germany"
- Connection options: Internet (OFTP2, VPN), ENX (OFTP)
- Redundant firewall systems
- Redundant server farm (virtualised server environment)
- Redundant power supply
- Multi-level backup strategy (backup-to-disk / disaster recovery to a second data centre)
- Preventive fire protection (fire walls, smoke detectors, gas extinguishing system)

4.2 Line encryption during data transmission

To ensure security during the data transmission process, the line between SWAN and the communication partner is secured by standardized procedures. SWAN uses the following types of lines:

4.2.1 ENX with OFTP

The ENX network is a special network for car manufacturers and their suppliers. Technically, it is an encrypted VPN network that is operated exclusively by certified service providers of the ENX Association. Like with ISDN, electronic data transmission is carried out using the OFTP protocol.

4.2.2 Internet with OFTP2

The basis for data transmission via OFTP2 is a standard internet connection with a public IP address. Compared to the ENX connection, this offers the advantage that an existing line can be used. In addition, internet connections are usually cheaper than ENX connections. Electronic data transmission is carried out by means of the OFTP2 protocol, which uses a TLS-encrypted communication channel with X.509 certificates. During the data transmission process

between SWANhosted and the communication partner via OFTP2, the user data is encrypted with X.509 certificates in addition to the line encryption.

4.3 Multilevel authentication concept

The authentication of a user to SWAN takes place by means of the two factors e-mail TAN" + "personalised login with username and password". Data access to the SWAN application is specifically controlled by means of a fine-grained rights and roles concept. Furthermore, we offer a technical option with a direct connection to your LDAP or AZURE OIDC.

4.4 Traceability of the receipt and send history

Using the server log files, the individual process steps (sending, receiving, transmission process, etc.) of the SWAN server can be traced by our support team at any time.

4.5 Server-side logging of the individual process steps

Based on the server log files, the individual process steps (sending, receiving, transmission process, etc.) of the SWAN server can always be traced by our support.

4.6 Penetration tests to check application security

An integral part of the release cycles of the software development process is the so-called penetration test (the security check).

An external service provider plays the role of a potential attacker (aka "hacker") and attempts to gain unauthorised access to the SWAN system (the SWAN application or the middleware components). For this purpose, the external service provider uses well-known methods and tools (scripts, software packages) of the "hacker scene" as well as its special IT know-how in the area of software development and network technology.

If it is possible to gain unauthorized access to the system via one of these methods, these security vulnerabilities are investigated and eliminated. This is followed by another penetration test for quality assurance.

4.7 Update- and Patch-Management

The prompt installation of security-relevant updates and patches is essential for an IT system nowadays. That is why all components of our data centre (firewalls, operating system, application server, database, ...) are regularly checked and kept up to date at SSC using a process flow defined by us.

Questions?

Phone: +49 (0) 70 31/49 13 -122

E-Mail: mailto:sales@ssc-services.de

Internet: http://www.ssc-services.de