SWANcloud

Security Aspects

SSC-Services GmbH
Herrenberger Straße 56
71034 Böblingen
Deutschland

Document: SWANcloud Security Aspects

Doc-Version: V4_EN_07-08-2014
Author: SSC-Services GmbH

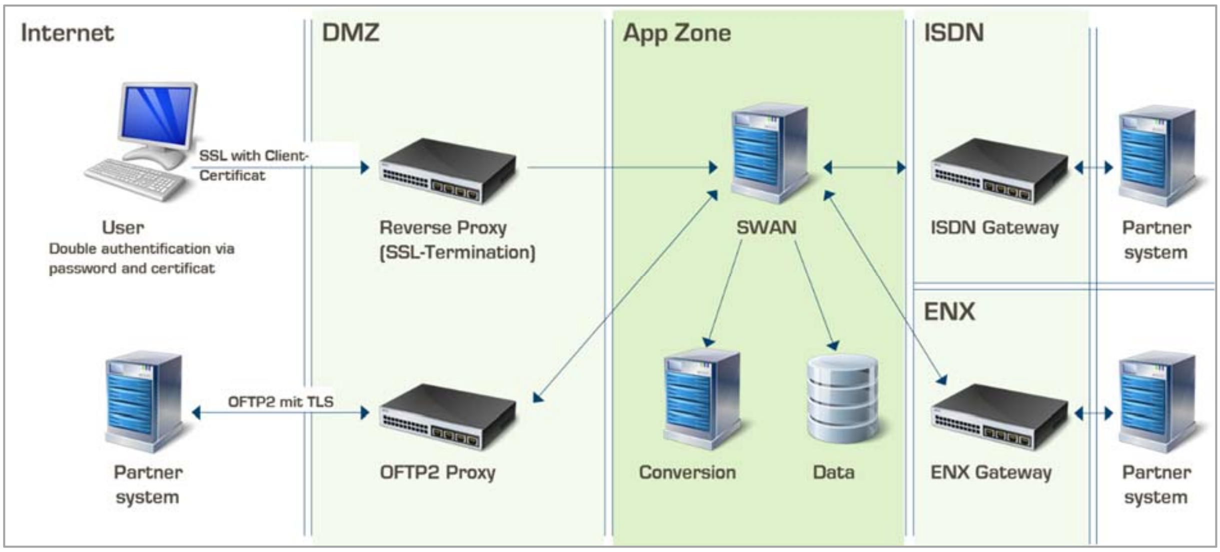
SSC-Services GmbH
Herrenberger Straße 56
71034 Böblingen
Germany

Phone: +49 (0) 70 31/49 13 - 0
Fax: +49 (0) 70 31/49 13 55
Mail: kontakt@ssc-services.de
Internet: http://www.ssc-services.de

Managing director: Matthias Stroezel
Domicile: Böblingen
Court of Registry: Stuttgart
Commercial Register No.: 21439

Content

SWANcloud Security Aspects



Hosting at SSC data processing center

The entire SWANcloud infrastructure is being operated at SSC data processing center (Böblingen, Germany). Among other things, it fulfills the following requirements:

» Connection types: Internet (OFTP2, VPN), ENX (OFTP), ISDN

» Redundant firewall systems

» Redundant server farm (virtualized server environment)

» Redundant power supply

» Multistage backup strategy (backup to disk / disaster recovery at a 2nd computing center)

» Fire prevention (fire-proof walls, smoke detectors, gas extinguishing system)

Software as a Service (SaaS) model is the basis for SWANcloud

The customers of SWANcloud access the SWAN installation hosted at SSC data processing center over the Internet. SWAN is a web-based solution developed under Java, which doesn't require any special client demands (Internet Explorer or Firefox, Java Runtime Environment). SWANcloud as SaaS provides the same comfort as the in-house solution SWANenterprise.

Encrypted communication between user and SWANcloud

The communication between the user and SWANcloud is made through the web browser. The HTTPS protocol is used for encrypting the communication. The HTTPS encryption consists of a public and a private key. The public key is stored at SWANcloud and the private key is stored on a client of the SWANcloud user.

The private key is a personal SSL certificate with a 2048 Bit RSA encryption, which is individually issued for every SWANcloud user. Anonymous access is technically blocked, so that the access SWANcloud is not possible unless a valid, personal SSL certificate is available.

Line encryption during the data transmission

The line between SWANcloud and the communication partner is protected by standard methods in ensuring the safety during the data transmission process. SWANcloud uses the following line types.

» ISDN with OFTP

The connection via ISDN is a direct connection (1:1) between two communication partners. The electronic data transmission is made through the OFTP protocol. As a 1:1 connection, it isn't encrypted.

» ENX with OFTP

The ENX network is a special network for car manufacturers and their suppliers. In technical terms, it is an encrypted VPN network, which is exclusively operated by certified providers of ENX Association. Like ISDN, the electronic data transmission is made through the OFTP protocol.

» Internet with OFTP2

A standard Internet access with a public IP address is the basis for the data transfer over OFTP2. In contrast to the ENX connection, it has the advantage of using a line that is already available; furthermore, the Internet access is usually cheaper than the ENX access. Present Internet connections have enormous speed advantage compared to the ISDN line. The electronic data transfer is made via through the OFTP2 protocol, using a TLS encrypted communication channel with X.509 certificates. The user data are additionally encrypted through the X.509 certificates, for the line encryption during the data transmission process between SWANcloud and the communication partner.

Multistage authentication concept

The authentication of a user on SWANcloud is achieved by the two factors "individual SSL user certificate" + "personalized login with user name and password". The data access to the SWAN application is selectively controlled by a fine-grained concept of rights and roles.

Traceability of send and receive history

A summary of all sent and received jobs is available at any time by means of a detailed logging of the SWAN history.

Server side logging of the single process steps

Our support staff is always able to trace the single process steps of the SWAN server (sending, receiving, transmission process, etc.) by means of the server log files.

Penetration tests for verifying application security

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

An external service provider entrusted from us assumes the role of a potential attacker ("hacker"), trying to get unauthorized access to the SWAN system (SWAN application or middleware components). For this purpose, the external provider uses known methods and tools from the "hacker scene" (scripts, software packages), as well as special IT know-how from the software development and networking area.

In the event that it is possible to get unauthorized access to the system through one of these methods, these security breaches will be analyzed and eliminated. Afterwards, another penetration test is performed for quality assurance.

Update and patch management

The timely installation of security-relevant updates and patches is indispensable for nowadays IT systems. Therefore, we regularly examine and maintain all components of our data processing center (firewalls, operating system, application server, database, ...) by means of a specifically designed process sequence.