Requirements for Secure Data Communication in the Automotive Industry

Thomas A. Goltermann
EZTI
38436 Wolfsburg, Germany
Letter box 1781
+ 49 5361 9 78883
thomas.goltermann@volkswagen.de
Initial situation: OFTP data exchange with Volkswagen and its CAD partners

Data exchange with external partners

- OFTP-Partner
- Online-Partner
Potential attacks during OFTP transmission

- **Eavesdropping**: Unauthenticated access (indirect damage)
- **Tampering**: Of data during transmission (direct damage)
- **Forgery**: External station sends out data in the name of Volkswagen or receives data in the name of Volkswagen (direct damage)
- **Potential misroutings**: (direct damage)
Volkswagen has decided to encrypt all CAD data exchanged with partners.

Speedy integration of an encryption component into the OFTP software used by Volkswagen had to be realised to comply with this requirement.

It was decided to use the Com-Secure software, based on the assessment of the pros and cons of various software solutions.
Volkswagen has decided to use the Com-Secure software solution by gedas deutschland GmbH.

Why? existing software, platform-independent, PKI-compatible

What is Com-Secure?

Com-Secure is a product designed for data encryption within the context of asynchronoulsy encrypted data communication on file level.

Com-Secure applies established encryption methods such as RSA and 3DES.
Continued: **What is Com-Secure?**

Com-Secure is available for IBM z/OS, IBM MVS, IBM AIX, HP-UX, SunOS, SGI IRIX, Reliant UNIX, Linux, WinNT, Win2000 and WinXP.

Com-Secure's uncomplicated interface allows easy integration in existing system environments and workflows (command line interface and API).

Com-Secure has been accepted by the other German OFTP companies as an encryption product.
Requirements for Secure Data Communication in the Automotive Industry

HyperKVS

1. Make key management available to the recipient for sending

2. Encryption and signature

Data

PKI

Certificates

OCSP

LDAP

4. Key search and check signature

5. Encrypt, deliver

Com-Secure

Volkswagen Partner

Com-Secure

vrs®

Volkswagen

CAD / PLM / PDM

Com-Secure

1. Make available to the recipient for sending

2. Encryption and signature

Data

Volkswagen public keys + own private keys

3. Send

OFTP

Requirements for Secure Data Communication in the Automotive Industry

Volkswagen
EZTI
Thomas A. Goltermann

gedas your IT partner
Requirements for Secure Data Communication in the Automotive Industry

Process of implementing and assigning a certificate during operation:

1. Installing Com-Secure
2. Creating a certificate request
3. Forwarding the request to Volkswagen by e-mail and fax/letter
4. Incorporating the certificate in the Volkswagen PKI
5. Loop testing the partner until everything is correctly configured
6. Activating mandatory encryption
Cooperation with the OFTP software vendors

All relevant OFTP software vendors have been integrated from the start.

The first pilot partners among the engineering companies contracted by Volkswagen could be integrated after internal tests at the OFTP software vendors.

417 Volkswagen engineering companies have adopted the new method. (status 09/2005)

The following OFTP software vendors offer encryption components:

<table>
<thead>
<tr>
<th>ATOS ORIGIN</th>
<th>Beratungsbüro Kasch</th>
<th>Hüngsberg GmbH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Datentechnik Mertens</td>
<td>gedas deutschland GmbH</td>
<td>Seeburger AG</td>
</tr>
<tr>
<td>Schmitt Unternehmensberatung GmbH</td>
<td></td>
<td>Brain Development GmbH</td>
</tr>
</tbody>
</table>
Further steps

Volkswagen pays the Com-Secure licensing costs for the engineering companies.

Volkswagen's engineering companies did not have to carry any further costs except for expenses arising from adapting the OFTP software solution.

The engineering companies are supported free of charge by the Service Support Center (SSC) of gedas deutschland GmbH within the framework of the network access contract CAx Supplier Network (CSN).
Small but mean obstacles encountered in the process

All engineering companies connected to Volkswagen via OFTP were supposed to receive a server-based PKI* certificate.

Volkswagen's engineering companies did install the encryption component, however, shrunk back from the next step: "mandatory encryption" in the Com-Secure software.

* PKI = Public Key Infrastructure
Server to server encryption, not merely router to router

All Research and Engineering data shall be treated confidentially. Requirement specified in the internal organization guideline ORL 49

Requirement / wording from Volkswagen-internal audit report
## Glossary

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>SSC</td>
<td>Service Support Center</td>
</tr>
<tr>
<td>CSN</td>
<td>CAx Supplier Network</td>
</tr>
<tr>
<td>PDM</td>
<td>Product Data Management</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
</tbody>
</table>
Requirements for Secure Data Communication in the Automotive Industry

Thomas A. Goltermann
EZTI
38436 Wolfsburg, Germany
Letter box 1781
+ 49 5361 9 78883
thomas.goltermann@volkswagen.de