Certificate

The certification body of TÜV Informationstechnik GmbH
hereby confirms that

Heidelberger Druckmaschinen AG

Kurfürsten-Anlage 52-60
69115 Heidelberg

has passed

Security Qualification

for the

Web-Based Remote Service

The extent of the parts of the installation included in this qualification as well as the considered security objectives are specified in the document *SQ Heidelberg, version 1.0.* The qualification was performed by TÜV Informationstechnik GmbH on the basis of the requirements of the specification SQ® version 9.0.

This certificate is valid only in conjunction with the SQ evaluation report *SQ Heidelberg, version 1.0* of 2007-01-31, provided that the measures for the installation described therein are respected.

This certificate entitles to use the certification mark

Security SQ9533.07 2007 Trusted Site

Voluntary Validation

Certificate Registration No.:
TUVIT-SQ9533.07

Essen, 2007-02-28 **signed by Dr. Sutter**
Certification Body

TÜV Informationstechnik GmbH - Member of TÜV NORD Group
Langemarckstraße 20 45141 Essen Germany

Summary of the requirements for the Security Qualification (SQ), version 9.0

1 Technical security requirements

Technical security requirements are defined based on recognized criteria, specifications or standards. The technical security requirements are free of internal contradictions and satisfy accepted security requirements.

2 Documentation of the architecture

For the qualification of the IT product and its application environment or of the IT system, appropriate descriptions of all necessary components are available. From these, the mutual utilization relationships and data flows as well as the fulfillment of security requirements can be recognized.

3 User, administration and other operational documents

Suitable manuals for installation, administration and usage are available. These particularly include notes on configuration of necessary system and product components as well as environmental measures and personnel responsibilities which satisfy the security requirements.

4 Security of the components used

All sub-components that implement security functionalities could be classified as trustworthy based on previously performed formal evaluations and/or publicly accessible information.

5 Means of system management

Suitable configuration facilities as well as appropriate monitoring and logging guarantee the secure operational state. Tools used for system management are subject to the same security requirements as the IT product/IT system itself.

6 Tests and inspections

Comprehensive penetration testing and technical vulnerability analyses have been performed during testing. The vulnerabilities determined during testing and analyses have been rated according to their risk potential.

7 Change management

A concept for the planning and implementation of new configurations and the import of updates exists in order to adequately evaluate risks and their effects as well as to guarantee maintenance of the intended protective level. The concept describes the way in which changes may take place and how the documentation is adapted where necessary.

8 IT systems: operational environment

Suitable operational conditions exist. The personnel responsibilities and environmental conditions satisfy the security claim of the IT system.

9 Security analyses

In a final analysis documented in the evaluation report the results of the previously listed evaluation aspects are compared to the security requirements. The result is that all security requirements have been met and the resulting residual risks are bearable.