docuFORM increases Mercury Suite security standards

Secure end-to-end encryption and SNMPv3 as defined by the DSGVO

The docuFORM GmbH in Karlsruhe offers, as a software company, solutions around the topic printing, as well as the administration of documents. Under the term 'Mercury Suite', various individual modules are made available which, when combined, represent a comprehensive document workflow.

The Mercury Managed Print Services Solution (MPS) serves as the basis for this solution. Within the MPS solution, the availability of the printing systems is monitored, and in addition to statistical evaluations of meter readings and consumables, the entire service logistics can also be planned and managed. In order to guarantee complete data security, docuFORM provides complete encryption of the device data using SNMPv3 as part of the recent launch of the new MPS version. Strictly according to Microsoft specifications, end-to-end encryptions between printing systems and the MPS data collector can be performed by using certificates. The data collector in turn transmits the device data via HTTPS, combined with multiple encryptions, to the MPS Hosting Server. This technology now guarantees that all data from the printing system itself to the secure MPS server can be transferred protected and fully encrypted.

Martin Denk, Dipl.-Ing. (TU), managing partner of docuFORM GmbH: "For some time now, it has been possible to transfer device data securely and repeatedly encrypted from the data collector on site to the MPS Hosting Server. This encryption has always been the basis for a secure cloud operation of the MPS solution. SNMPv3 now closes the gap between the end device and the data collector. In this context, SNMPv3 guarantees complete encryption of all device data up to cloud evaluation - an important step towards data security as postulated from the DSGVO. “

Due to the introduction of the SNMPv3 protocol within the customer network, it became necessary also to upgrade all SNMP communications of the Mercury DMS / OMS Suite to SNMPv3. In order to guarantee the homogeneity of the overall solution, the entire Mercury OMS communication with the end devices themselves was also extended by SNMPv3. It has always been possible to securely print within the Mercury Suite using SNMP. The device states were called up to ensure before printing that the device was available, paper was available, and that it was fully operational. With the new availability of SNMPv3, this important functionality between Mercury OMS and output devices is maintained within the DSGVO requirement.

"Furthermore, the encryption refers not only to device communication via the SNMP network protocol, but also to the encryption of print data itself via IPPS. - says Martin Denk. Martin Denk continues: "With the complete encryption of all print data using the IPPS network protocol and the encryption of all communication paths using SNMPv3, the user is guaranteed comprehensive and complete data security".

Consequently, this technology was also integrated into the Follow "2 "Print solution from docuFORM. Since the SNMPv3 communication differs, depending on the device type or manufacturer, it was a technical challenge to guarantee secure communication even within the Follow "2 "Print workflow. Here docuFORM again made use of its patented technology of the Global Printer Drivers (GPD). In the context of using the docuFORM Global Printer Drivers (GPD), print data is only generated when it is ensured which device is to be used for output. The individual IPPS configurations are transferred with the data stream, so that the device-specific IPPS commands are only integrated shortly before

the printing process itself. This guarantees secure printing up to the end device even with Follow "2 "Print.

By the launch of the current docuFORM MPS as well as Mercury solution, a crucial contribution to the data protection regulation for each user is made. All communication channels within the device ranges and the software can now be encrypted via SNMPv3, as well as the print data itself via IPPS. This also applies to the integration of the patented GPD solution for Follow "2 "Print applications.