

Security is a top priority

JSCRIBE SECURE PRINT SOLUTION

Data protection throughout the network – from the workstation via the server to the printer

:: HIGHLIGHTS

PROTECTS PRINT DATA AGAINST THEFT AND MANIPULATION

SECURE TRANSMISSION AND DELIVERY THROUGHOUT THE NETWORK

CENTRAL ADMINISTRATION – CENTRALIZED DEPLOYMENT

READY-TO-RUN SOLUTION FOR SMB AND ENTERPRISE

VENDOR-INDEPENDENT, THUS HIGHLY FLEXIBLE AND EFFICIENT

:: THE DANGER COMES FROM THE INSIDE

Security is a word with a capital S.

86.7% of all managers taking part in a Cap Gemini survey would agree to that: they put security at the top of their priority list.

Consequently, the IT department has network security and the protection against external attacks (e.g. viruses or spam) mostly under control. But regardless of those efforts there's a largely unnoticed security hole at every workplace: Every print job is a potential risk.

The potential damage is not limited to confidential documents being forgotten at the printer, or read by people other than their intended recipient (an IDC study proves that 26% of all German employees have found confidential documents at a printer at least once, almost half of these containing sensitive company data).

In fact there is no technical problem in intercepting and manipulating print data

themselves (for example bank transfer data) on their way through the network – the requisite "sniffer" tools are freely available on the Internet. Even in the memories of the printers you will find confidential data. And so the inevitable happens: whether intentionally or just carelessly – information about salaries and commissions, personnel related data or research and financial key data will end up in the wrong hands.

Gartner's research specialists think that inside jobs take a share of 70% of all security relevant incidences. This is why despite increasing IT security budgets the problems relating to print data security haven't been recognized properly yet.

:: METHODS OF RESOLUTION

Unauthorized access to printed documents shall be prevented by routing print jobs to printers placed in closed areas, protected by access control mechanisms. Still the print data themselves are vulnerable while passing the network.

Sometimes confidential data are sent to printers connected directly, locally to a workplace PC – and as a matter of fact they can not be sniffed from there. During cost analysis processes however especially these printers are – justifiably – stigmatized as the most cost ineffective devices and get substituted by multifunctional printers on department level. And that leads to even more print data being sent over the network.

Sufficient protection for these data can only be provided by a solution that offers secure document transmission via the network – easy to use and cost efficient.

THE JScribe SECURE PRINT SOLUTION

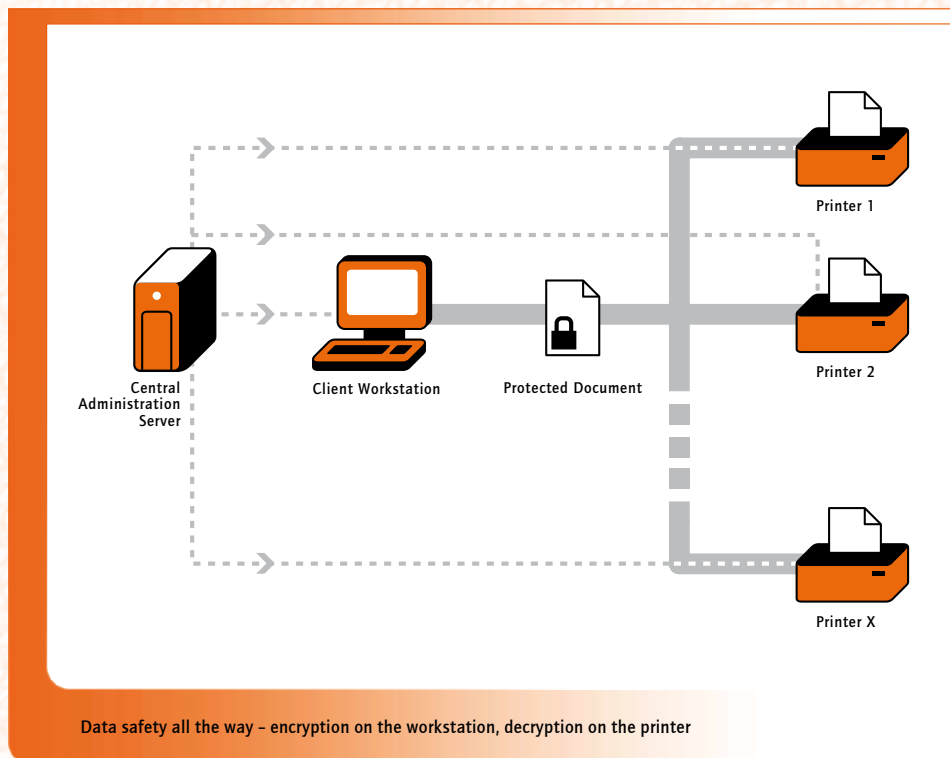
The JScribe Secure Print Solution is a framework of software and hardware components that protects your confidential print data against unauthorized access, from the workstation all through the network to the printer.

This is achieved via sophisticated Public Key/Private Key encryption, more efficient than the commonly used SSL encryption. The JScribe Secure Print Solution offers security in three steps:

- ❑ The print data are encrypted on the workplace PC and can no longer be scanned from the network in a readable form.
- ❑ Decryption is done no earlier than on the printer itself.
- ❑ The data will not be stored anywhere.

The only precondition is that the printer has to be equipped with the patented JScribe technology – either as an embedded technology integrated with the device itself or provided by externally connected devices. The installation of the encryption client on the workplace PC is easily done via the network. The central administration will also recognize any JScribe enabled device and is used to manage the whole system. The print device needs no further configuration. Protect your sensitive data against theft, manipulation and misuse with the JScribe Secure Print Solution.

Close the security hole. Security is a top priority.



:: ABOUT JScribe®

The JScribe Secure Print Solution is an application developed by CCP Systems AG, based on their patented JScribe technology.

JScribe is an open application and communication platform for servers, workstations, MFDs and printers to exchange information proactively in every direction. Devices can easily be integrated into various types of computing environments for making business processes communicative and manageable.

On top of that, JScribe acts as a basic technology for the development of customer individual or standardized solutions for output and document management, enabled to be run on the device itself and thus - while unifying the way of interchanging the information and the handling of the various types of computing environments and disburdening the network - creates additional value for the customer without changing or replacing existing IT infrastructures.

This makes CCP a technological leader in the field of process optimization for business output. In 2006 several concerns started to gradually equip their output product ranges with integrated JScribe technology.

JScribe and the CCP Logo are registered trademarks of CCP Systems AG in Germany and/or other countries and may, therefore, not be used commercially without explicit consent of CCP. All other brand and product names may be registered trademarks of other producers with applicable protection.

This product information reflects the status as of 04/2010 and is intended to be used for general guidance in regard to the products' functionalities only, which can be subject to changes without notice and anytime. For latest information regarding CCP's products and its services please contact CCP or any of its authorized dealers.

CCP Systems AG does not warrant or guarantee that prices or specifications mentioned will be correct. The subject matter and specific scope of any products or services are exclusively designated in the according contracts.

© CCP Systems AG 2010 - All rights reserved.

CCP Systems AG

Stammheimer Straße 35
D-70435 Stuttgart, Germany

Phone +49 (0)711 | 82 03 42-10

Fax +49 (0)711 | 82 03 42-19

www.ccp.de | info@ccp.de

:: ABOUT CCP

CCP Systems AG develops technologies and solutions for managing and controlling output processes.

More than 20 years of experience in manufacturing printer drivers and document solutions are the foundation for the patented JScribe® technology, a worldwide unique application and communication platform for digital printers and multifunctional devices, workstations and server.

JScribe and the applications based on it are marketed worldwide by various partners.

System requirements for Administration Server

Hardware Requirements:
Intel Pentium 4, 1 GByte RAM, 2 GByte of free Hard Disk space, DVD-ROM drive, Network Interface

Operating Systems supported:
:: Windows 2000 Server, Service Pack 4
:: Windows 2003 Server, Service Pack 1

System requirements for Secure Clients

Hardware Requirements:
Intel Pentium or compatible processor, 256 MByte RAM, 50 MByte of free Hard Disk space, Network Interface

Operating Systems supported:
:: Windows 2000 Professional, Service Pack 4
:: Windows 2000 Server, Service Pack 4
:: Windows 2003 Server, Service Pack 1
:: Windows XP Professional Service Pack 2

JScribe application supports the following languages

:: Chinese (simplified)
:: English
:: German
:: Japanese