Jetmobile®
information traceability, security and mobility

SecureJet™ 5.1

White paper

V3 - January 2007

THIS DOCUMENT IS NON-CONTRACTUAL.

TECHNICAL SPECIFICATIONS ARE SUBJECT TO MODIFICATIONS WITHOUT ANY PRIOR NOTICE.

P/N CMWPSJ061110

Jetmobile S.A.S.
89 Avenue du Gouv. Général Eboué
F-92130 Issy les Moulineaux
FRANCE

WEB: http://www.jetmobile.com
Mail: info@jetmobile.com
Tel: +33 (0) 1-46-94-80-10
Fax: +33 (0) 1-46-94-00-83

Table of content

I – Presentation of SecureJet *5*

SecureJet markets **6**

II – Cases studies *7*

III – SecureJet Lite *10*

IV – SecureJet 5 overview *11*

A modular design **11**

SecureJet 5 modules **12**

SecureJet 5 examples of modules combination **14**

SecureJet 5 Support pack **15**

V – SecureJet technical information *16*

SecureJet 5.1 Pre-requisites **16**

SecureJet Installation **17**

SecureJet Admin software **18**

SecureJet Enrollment Station **19**

VI – Secure access and authentication *20*

SecureJet Auth-PX **20**

SecureJet Auth-PXT **21**

SecureJet Auth-FP **22**

SecureJet Auth-Fingerprint **23**

Markets: **23**

Authentication Manager configuration: 25

User enrollment process 26

User login process once he is enrolled 26

SecureJet Auth-SC **27**

SecureJet Auth-SW **28**

VII - Smart Printing *29*

PUSH printing or PULL printing? **29**

SecureJet PRINT-SMP **30**

SecureJet PRINT-PS **31**

Live authentication against Active Directory/LDAP database 32

Support for multiple databases 32

Failover capability 32

Support for multiple user logins (Alias system) 32

Pre-requirement for roaming printing 33

VIII – Jobs tracking *35*

Conditions for tracking job titles and print job owners: 36

SecureJet Track TRP can email tracking data, and features a web reporting tool: 36
If you use SecureJet in association with MegaTrack™: 37
SecureJet tracking information file format 37
Important notes: 37
IX – Using SecureJet, some examples *38*
How to make a copy on lj4730mfp using SecureJet Auth-PX? **38**
How to secure a document? **39**
Sending a document to yourself under Windows 39
Sending a document to other users under Windows 39
Sending a document to a department: example 39
Sending a document to a department under Windows 40
Sending a document to a user or department under UNIX 40
Unencrypted secure printing for ERPs 40
Encrypted secure printing for ERPs 40
How to release jobs on MFPs? **41**
How to release user print jobs on non MFP printers? **42**
How to authenticate for secure printing using Auth-SW? **43**
How to release user jobs using SecureJet Auth-SC? **45**
X – Where to buy? *47*
XI - Company overview *48*

I – Presentation of SecureJet

SecureJet was first created in 1997 and an extensive patent for mobile secure printing was requested in the US in 2001 and delivered in 2005.

The SecureJet 5 product line is available for most hp LaserJet printers and MFPs and is composed of 3 families of modules:

- **Authentication**
- **Smart printing**
- **Tracking & reporting**

SecureJet Authentication modules allow authenticating users on printers and MFPs using various technologies ranging from PIN codes to biometrics:- PIN codes, proximity badges, magstripe swipe cards, smartcards, and biometrics. All proximity and smartcard readers are designed and manufactured by Jetmobile to ensure the highest quality and the best integration on hp devices. Such authentication can be used for MFPs built-in and optional applications such as copy, email, fax, hp Autostore, hp DSS Workflow etc.

The patented **SecureJet Smart Printing** modules allow ensuring documents are secure and only retrieved by an authorized person, following the user to any printer on the intranet: print jobs are encrypted, then stored on the printer or MFP hard drive until their release by their owner or stored on servers then routed where they are requested by a user upon authentication.

The **SecureJet Tracking & Reporting** module provides device-based jobs tracking and device and server-based reporting.

SecureJet presents the following benefits for you:

- Highest features, most flexible solution at the lowest price, even for high tech solutions using proximity readers, biometrics…
- Works natively on the hp printer/MFPs (no external box), easy to install and maintain, works with MFP applications
- Highly flexible functionalities, such as live AD/LDAP, SAP interface etc
- Multilingual application, incl. on the MFP and printers front panels
- SecureJet is truly available worldwide, with regional & local delivery & support
- Worldwide network of VARs with yearly technical certification

SecureJet markets

Example of requests for SecureJet from vertical markets:

- Hospitals, to secure the printing of patients documents
- Oil companies, to control MFP access and ease mobile printing
- IT companies, where mobile workers IT setup needs pull printing
- Banks, to secure access to MFPs and financial documents printing
- General industry where MFP control and pull printing rise productivity
- Government, army, police to secure MFPs and documents printing

Example of major needs expressed for horizontal markets:

- Control access to email sending on MFPs, and fill&lock FROM field in outgoing emails
- Roaming mobile pull printing from printers & MFPs
- Job tracking

SecureJet is the appropriate solution for:

- Worldwide deployment of secure printing
- Replacement of all personal printers with network printers + secure jobs release
- Authentication of email senders address on MFPs
- Allocation of MFP walk-up activity cost to departments/users
- Bill-back of the print/copy/fax/scan cost to your clients and projects
- Hotdesk printing with only 1 print queue on every PC, to reach all printers
- Solution to release documents without any PC (factories, hospitals, oil rigs, warehouses…)
- Securing the printing of confidential information (banks, lawyers, hospitals, police, pharmaceutical companies, aerospace, army…)

SecureJet is not the appropriate solution for:

- Prepayment deals (typically the education market) where users credit accounts to print, copy, email, fax.
- Internet open pull printing (i.e.: printing for hotel guests)

II – Cases studies

VZP uses SecureJet to protect personal information of its clients.

VŠEOBECNÁ ZDRAVOTNÁ POISŤOVŇA

Vseobecn Zdravotna poistovna (VZP) is the largest health insurance company in Slovakia. Today, the company insures approximately 65% of the Slovak population and stores in its IT systems medical records of its clients. At the same time, the company operates the broadest network of regional offices providing services to clients in 87 locations throughout Slovakia.

Nowadays, it would be impossible to seamlessly process the agenda generated by such high number of clients without using state-of-the-art information technology systems, especially in the healthcare arena which represents a very important sector.

That was why Vseobecn Zdravotna poistovna recently made a decision to build with SecureJet a new Comprehensive Information System that would answer the most demanding challenges relating to the operation of a healthcare insurer of this size.

1. Finding a solution

One of vital requirements of all health insurers is to secure printing of documents in a way so that no unauthorized persons are able to gain access to such documents. Medical records contain information about health condition and other highly sensitive personal information of clients - information that must be protected by insurance companies against possible misuse not only because that is what the legislation requires but also with regard to ethical reasons. The trust of clients and patients is the highest imperative in this field.

Until recently, it was impossible to secure in case of systems that used network printers located outside of offices (mostly in corridors due to accessibility reasons) the prevention of access to printed documents by unauthorized persons. Inevitably, there was a certain time period between the moment of placing the print job and the moment of retrieving printed documents from the printer (based on how accessible the particular printer was), during which time period anybody was able not only to read the information but, in extreme cases, to steal the documents. And these cases had to be prevented.

"We've been contemplating this task for some time, says Tibor Tark, Project Manager, Comprehensive Information System, VZP. *We calculated how many printers we in fact needed and then we looked for a method that would secure a situation in which users would not be able to print anything they wanted. At the same time, we required that everything these users actually printed was recorded, i.e. a system that could not be fooled. We found this system with HP, which company recommended SecureJet product for our new printers. We found that this product fully met our requirements.*

2. SecureJet, the right solution

How does this secure printing work? SecureJet represents in fact the extension of network printers that contains the so-called "pin terminal" and the respective software. The solution is built on a principle which requires storing of all print tasks in the print server before any printing takes place. The entire system is managed and controlled by a network administrator who assigns specific pin codes (or chip cards, provided that the respective printers are fitted with card readers) enabling access to print jobs to all users who wish to print secured documents.

The employees generate their print jobs just like any other common network printers. However, the information sent does not travel to the selected printer but is rather stored in the print server. An employee may approach a

printer at any time later (although this time period may be limited so that the printer is not overloaded by an excessive number of print tasks) and enter his/her pin code using the terminal's keyboard. Upon successful validation of a users id, the chosen network printer downloads the respective print task from the print server and prints the document in question.

Very important with regard to security of printed documents is the fact that printers print such documents only when the employees who generatied the respective print tasks are present at the printer. Also, print tasks may be stored in the print server for a specified time period so that it is possible to search back in time and find out who printed what document. Whereas Vseobecn Zdravotna poistovna (VZP) operates 83 access points in its Slovak network, a given print task may be downloaded from the print server equipped with SecureJet Print-PS (there are **38 servers equipped with SecureJet Print-PS**) and printed at any of these locations after entering the a user is successfully authenticated.

"Within the framework of building our Comprehensive Information System, we purchased 330 HP printers. The delivery comprised various models of LaserJet network printers, including the latest 9000dn series. In total, ***149 printers were fitted with SecureJet security terminals****"* says Tark. "*I am glad that it was Hewlett-Packard Slovakia s.r.o. that succeeded in the tender, especially as this company did not offer us just printers but rather a comprehensive security solution"*. He continues in explaining his good feeling about the transaction: "*It looks like HP still has the best printers in the world and the largest market share. Another big advantage for us was the fact that the servicing and support would be secured by such a huge company"*

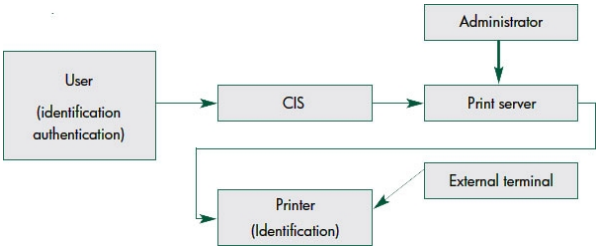
3. Customers require consistent solutions

To summarize the features used in case of secure printing solution:

- protection of documents against theft from the printer
- printing of documents is possible on any network printer equipped with SecureJet; it is only after sending the respective print task to the system that a user decides which printer the document will be downloaded from the print server to.
- ability to record and identify users and secured documents printed by them
- monitoring of the number of copies printed by individual users with the opportunity to limit this number
- broad range of user identification methods? pin codes, smartcards, corporate magnetic or proximity badges and biometric.

"We must understand that a printer is no longer a dumb tool but a smart device just like a PC. It features its own processor, memory, control panel... all this enables us to create new exciting solutions", says Vladimír Páleník, IPG Commercial Sales Manager, Hewlett-Packard Slovakia s.r.o.. "That is also why these days customer requirements are not limited just to delivery of printers. More frequently customers ask for consistent solutions and HP is able to tailor these solutions to their needs, as happened in case of the secure printing solution for VZP. Tibor Tarabek adds: "I am convinced that our investment was a good one. Our clients may rest assured that the personal information is well protected and shall not get into the hands of unauthorized individuals."

Implementation Project of I/O Devices of the Comprehensive Information System for VZP



Requirements: Printing (exporting) of outputs from CIS system may be performed only by authorized users. The printed output may be retrieved only by the owner of the given printed output providingl confidentiality of the printed output.

An American university hospital

turns to SecureJet for HIPPA compliant patient care reports.

Eighty nursing units—providing clinical services to 1,100+ beds in the areas of perioperative, medical/surgical, ambulatory and critical care—produce highly confidential **patient care reports** (about medications, diet, IVs, etc.) that can number in the hundreds of pages. And, depending on the nursing unit, new reports get printed out on HP LaserJet 4100 and 4200 workgroup printers every one-to-four hours.

"We were expending a lot of resources for large volumes of volatile information," said the project manager. Every four hours, all reports become obsolete, requiring output of a completely new set of reports—by patient and by nursing unit. Each unit generates 10-12,000 pages of output per day.

"We needed better control of printed output because, with so many nursing units spread across four main hospital buildings, security is always an issue. Though these printers are not in public access areas, they do store information that only authorized personnel should access."

Confidentiality is also an issue. All that paper falls under HIPAA and JCAHO compliance rules. Both the Health Insurance Portability and Accountability Act of 1996 and the Joint Commission on Accreditation of Healthcare Organizations (the nation's predominant standards-setting and accrediting body in health care) set standards for the management of and access to patient health data stored or transmitted in electronic form.

Another issue was downtime due to power outages and other emergencies. Patient care reports are stored in the printers. When the hospital loses power, workers fall back to a paper system. The project manager wanted to be able to deliver online information even during downtimes.

To deal with these and other matters, the project manager evaluated the existing reporting process and turned to the **SecureJet™ Smartcard (SC) Printing Solution** from Jetmobile. The SecureJet SC printing solution consists of:

- A software component (SecureJet solution and the appropriate driver installed on originating computers).
- "Smart cards" (plastic cards—about the size of credit cards and containing electronic memory—that are inserted into readers).
- SecureJet reader terminals (with display and heavy-duty keyboard) installed on destination printers (each reader terminal is plugged into the printer parallel port on a selected printer).
  Now, all authorized users (physicians, nurses) are given secure Smartcards that are used to identify individuals. User identification is required for ALL print jobs—documents are printed only when users identify themselves at the printer by inserting their Smartcards into the SecureJet readers.

Computers and printers in the hospital nursing units do demand printing. SecureJet SC secures print jobs all the way from the application to the controlled delivery onto paper. Print jobs are "wrapped" (encrypted) on PCs, ERP and Unix systems, sent electronically over the network, stored on the destination HP printer hard drive, and decrypted at print time, when only the appropriate nursing units can retrieve them. And all print jobs are tracked and logged.

Of the 650 HP LaserJet printers on the University hospital campus, it was initially sought to convert 100 printers in the nursing units to SecureJet. He originally ordered 15 units, installing the first in January 2003 in postoperative nursing units.

The hospital does its own SmartCard administration through a desktop support group. SecureJet installation and software updates are done remotely.

"Jetmobile created a win/win situation with the use of SecureJet at the hospital. They were very helpful in getting product pilot review, pitching the product to senior management, and then tailoring to our needs. Without the success this first installation has achieved, we wouldn't be rolling out across all of hospital. The SecureJet solution may eventually reach even further into the hospital system."

On the hospital campus, four main hospital buildings cover an area eight square city blocks wide. The hospital has 5,853 full-time employees, 131 fellows, 928 active medical staff, 932 licensed acute care beds, and 180 subacute and long-term care beds.

For the modern hospital, the term “critical care” means lots of paper. In the nursing units that provide clinical services, nursing assignments carry a substantial patient care load. For the restoration of patient health, the essential nursing personnel who attend the needs of sick persons must rely greatly on the computerized POE process. The electronic ordering of medications significantly reduces risks posed **by handwritten orders, and computerized alerts and guidance help prevent medication errors.**

> “We chose the SecureJet solution because it saves resources and is HIPPA compliant so that only those persons who need to review a report can do so. Compatibility with hospital’s installed base of HP LaserJet printers is crucial. The installed base of printers is 85 percent 4100s and 10-15 percent 4200s.That ratio will reverse in twelve months” said the project manager.

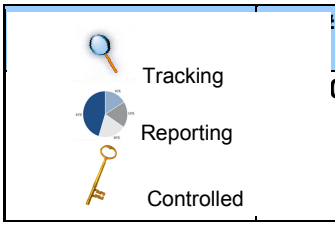
III – SecureJet Lite

SecureJet Lite is an all-in-one solution for MFPs/Digital Senders, featuring PIN authentication + Billing codes + tracking + database + full reporting solution.

It is intended for clients who just want to:

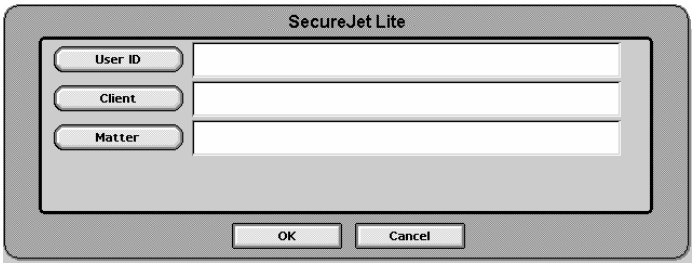
- control the access to MFPs using alphanumeric PIN codes
- bill back projects or clients using alphanumeric billing codes
- collect job tracking information by email (from each device)
- benefit from the extensive reporting capabilities of the MRT server module which stores all tracking data in a MSDE or SQL Server database.

Notes:
- SecureJet Lite does not perform PULL or push printing
- SecureJet Lite is not compatible with the SecureJet full version family
- SecureJet Lite cannot work with other SecureJet modules
- SecureJet Lite is not upgradeable to SecureJet 5

		Authentication process	Functionalities
	001	PIN codes entered on the printer or MFP front panel	

- PIN Code Authentication
- Support Alpha Numeric PIN codes
- Supports multiple Alpha Numeric Billing codes

- Custom configuration of all Input Fields and Validation (PIN, billing codes)
- Detailed tracking and reporting
- Reporting and data storage for up to 30,000 MFPs
- Tracking data goes through firewalls (http or ftp)
- Server or printer report, as client wishes
- Printer web page reporting included
- Reporting and database server included
- Email reports from printer and server reporting
- Not for secure mobile printing usage, not compatible with SecureJet 5 modules
- Available for the following MFPs and Digital Senders: 4345mfp, 4730mfp, 9040mfp, 9050mfp, 9500mfp, 9200C, m4345mfp, m5035mfp, m3035mfp



IV – SecureJet 5 overview

A modular design

SecureJet 5 is made of functional modules classified in 3 families:

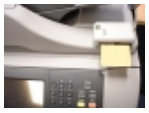
- Authentication
- Smart & Secure Printing
- Job tracking & reporting

Those modules can be purchased independently and combined together.

SecureJet Authentication	SecureJet Secure Pull Printing	SecureJet Tracking & Reporting
Modules: **Auth-FP** PIN codes on MFP front panel **Auth-PXT** PIN codes on keypad (printers) **Auth-PX** Proximity badges reader HID/Mifare/Legic/Em-Marin/Hitag **Auth-SW** ISO Swipe magnetic cards reader **Auth-SC** Smartcards reader **Auth-Fingerprint** Biometrics finger authentication	Modules: **Print-PS** Server software for: - server-based job retention (PULL printing) and - remote LDAP/AD authentication **Print-SMP** Client module for Printer/MFP providing - jobs release with secure PUSH/PULL printing and - decryption of print jobs	Module: **Track-TRP** -Print/Copy/Fax/E-mail jobs tracking and -Extensive printer & server-based web reporting

User authentication modules for printers and MFPs

Restricts access on printers, MFPs and Digital Senders to authenticated users

Product		Part-#	Identification using
Auth-FP		**SJFP004**	**PIN codes** entered on the printer or MFP front panel
Auth-PXT		**SJPXT002x0**	**PIN codes** entered on an external terminal connected to the printer
Auth-PX		**SJPX001x** **SJPX002x** **SJPX003x** **SJPX005x** **SJPX005x**	**Proximity badges** Mifare proximity badges HID proximity badges EM-Marin proximity cards Hitting proximity badges Legic proximity badges
Auth-SC		**SJSC0010**	**Smartcards** (please contact us for any project to know if your smartcard is supported)
Auth-SW		**SJSW001x**	ISO 1/2/3 **magnetic cards** with user ID on one of the tracks
SecureJet-Fingerprint		**SJFGP0010**	**Biometrics**, fingerprint

Tracking Reporting module


Tracks printers, MFPs and Digital Senders usage, web-based & email reports

Product	Part-#	OS	Functionalities
Track-TRP	**SJTRP001**	Windows 2000, XP and 2003 Server (MRT)	*Tracking & Reporting*

Smart and secure printing modules

Product	Part-number	OS	Functionalities
Print-SMP	**SJSMP001**	Printer software	*Encryption and decryption, mobile secured release of print jobs*
Print-PS	**SJPS001**	Windows 2000, XP and 2003 Server	*Server software for server-based job retention (PULL) & remote LDAP/AD authentication*

Outputs documents on printers/MFPs only when/where their owner requests them

SecureJet 5 examples of modules combination

SecureJet 5 modules can be combined to achieve the required functionality. Here are a few examples. Please contact your Jetmobile VAR for more information on your specific needs.

A company wants to **control** the access to their 4345mfp and 9500mfp using the MFP built-in LDAP, **track** the MFP walkup usage and perform **PULL** printing. The following modules are required:

SJTRP001	**Tracking-TRP** 1*4345mfp + 1*9500mfp
SJSMP001	**Print SMP** 1*4345mfp + 1*9500mfp
SJPS001	**Print PS** for the server
JMW50S	**Support pack**

A company equipped with **a mix** of 4345mfp and 4250 wants to **control** the access to MFP functions using individual PIN codes, **track** the printer and copier usage and perform **PULL** printing. The following modules are required:

SJFP004	**Auth-FP** for 4345mfp
SJPXT0021	**Auth-PXT** for 4250
SJSMP001	**Print SMP** 1* 4345mfp + 1*4250
SJPS001	**Print PS** for servers
SJTRP001	**Tracking-TRP** 1*4345mfp + 1*4250
JMW50S	**Support Pack**

A company equipped with HID badges wants to **control** the printer access, **track** and **secure** the printouts on LJ5550 **(PUSH** printing). The following modules are required:

SJPX0011	**Auth-PX / Mifare** for LJ 5550
SJTRP001	**Tracking-TRP** for LJ 5550
SJSMP001	**Print SMP** for LJ 5550

A company equipped with swipe cards wants to **control** the printer access on 4350, **track, secure** the printouts on LJ4350 and perform **PULL** printing. The following modules are required:

SJSW0011	**Auth-SW** for LJ4350
SJTRP001	**Tracking-TRP** for LJ4350
SJSMP001	**Print SMP** for LJ4350
SJPS001	**Print PS** for servers

SecureJet 5 Support pack

SecureJet warranty is the following:

- Hardware (memory modules, readers, power supplies, cables): 1 year from purchase date
- Software and firmware (in readers, MFPs, Digital Senders and printers): 90 days from purchase date

3 and 5 years support extension packs are available at purchase time:

- They include support from your local certified VAR
- They cover hardware, software and firmware updates (both minor and major releases)
- They must be purchased within 90 days of the initial purchase and start from the product purchase date.
- Because of the high frequency and impact of MFP firmware upgrades, they are mandatory for SecureJet on MFPs and strongly recommended for SecureJet on printers.

1-year support pack 18% of solution price
3-year support pack 45% of solution price
5-years support pack 68% of solution price

Note:

- Clients under maintenance contract for SecureJet 4 are updated to SecureJet V5 (except for the new MRT reporting server, available separately).
- Client who are not under maintenance contract with a product not older than 3 years can either purchase a retroactive maintenance or purchase the upgrade at the product list price with a 50% discount

V – SecureJet technical information

SecureJet 5.1 Pre-requisites

as of November 1st, 2006

m4345mfp	20061005 48.010.9	256 MB
m3035mfp	20061005 48.010.9	256 MB
m5035mfp	20061005 48.010.9	256 MB
LJ9050MFP	08.051.7	256 MB
LJ9040MFP	08.051.7	256 MB
LJ9000MFP	08.051.7	256 MB
LJ4730MFP(1)	46.121.2	256 MB
LJ4345MFP	09.051.7	256 MB
LJ4100MFP	03.804.6 or higher	256 MB
P3005	*Release pending*	
LJ9050	08.102.2	128 MB
LJ9000	02.516.0	128MB
LJ4250/4350	08.009.3A or higher	128 MB
LJ4200/4300	04.020.3 or higher	128MB
LJ4100(2)	01.040.2	128MB
LJ2410/2420/2430(3)	08.109.2A	128 MB
DS9200c (no printing)	09.051.7	256 MB
CLJ9500MFP	08.051.7	512 MB
CLJ9500	05.007.1 or higher	256 MB
CLJ5550	07.007.3 or higher	256 MB
CLJ5500	04.020.3 or higher	128MB
CLJ4700(1)	46.027.2 or higher	256 MB
CLJ4650	07.003.3 or higher	256 MB
CLJ4600	03.015.0 or higher	128MB
CLJ 3800	46.033.0	256 MB
CLJ3700(3)	06.006.0 or higher	192 MB

- Hard-drive required on CF-based printers (except on hp24X0):

(1) One EIO slot must be available to route the Auth-PX, SW and SC readers cable out

(2) No tracking features on this printer

(3) Can not accept any hard disk: release from SecureJet Print-PS server only

Important: Please verify on www.jetmobile.com what printers and MFP models are supported by each SecureJet module

pre-requisite for the PC:

Operating Systems: Windows 98/Me/NT/2000/XP/2003
(Workstation or Server) with local or remote Printer Driver (PCL5, PostScript).
PCL6/XL drivers are not recommended as they are specific to the device they were developed for.

pre-requisites for Linux systems:

Operating Systems: Linux Red hat

pre-requisites for SAP R/3:

No encryption: Any Sapscript or Smartforms output, server-independant
Operating Systems for encryption option: HP-UX, Sun Solaris, Linux Red hat print server

SecureJet Installation

SecureJet is plug&play on printer & MFPs

- Ordered on memory module (DIMM, CF/USB) or as a file (PJL file)
- Includes all modules (active or inactive, based on the license)

Delivery on memory module

- Install the memory module in the printer
- Reboot the printer
- The printer reboots again
- SecureJet is now installed, the license is included in the memory module

Delivery as a file

- You receive a PJL file to install on the printer/MFP hard drive.
- Reboot the printer
- The printer reboots again
- SecureJet is now installed, and its license needs to be activated

License activation

Needed:

- only for pure file delivery (not for authentication with readers)
- and when licensing new modules

Procedure:

- Install SecureJet
- Send the printer(s) configuration page(s) to your Jetmobile VAR
- You receive license activation PJL files from your Jetmobile VAR, one per device
- You send the appropriate file to each printer to expand/activate the license

Please consult the installation guides for the readers installation.

SecureJet Admin software

The **SecureJet Admin Software** is a Windows utility used to :

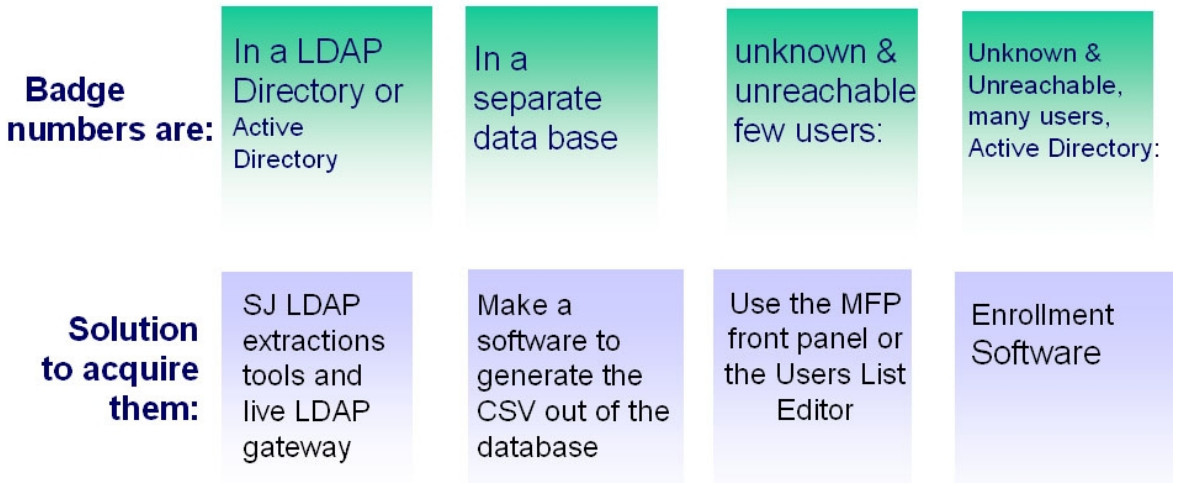
- Centrally configure SecureJet on printers and MFPs
- Centrally define a list of authorized users and their cards ID, and propagate it on all devices
- Synchronize that list with a LDAP directory (Active Directory, Exchange, Unix LDAP…) for up to 30.000 users
- Analyze badges content

The **SecureJet Batch Admin software** is a DOS command-line utility, without graphical interface or user interaction. It be can used in batch files with a scheduler, for example in automatic users updates and SecureJet install and configuration. Please use the Windows SecureJet Admin software should you require a graphical interface.

SecureJet users list editor is installed together with the SecureJet admin Software. It allows you to conveniently create/edit users list.

The **SecureJet Enrollment Station** Software (optional) is used with a special SecureJet Auth reader (PX or SW) connected to the PC to acquire the badge number.

Which solutions to admin cards in SecureJet? Where to get the user from the ID?



SecureJet Enrollment Station

This optional software is used with special SecureJet reader (PX or SW) connected to the PC to acquire the badge number. It is useful when the IT department does not know the user badge numbers. It requests users to perform an Active Directory login, then reads their badge to record the full user information in the SecureJet users list.

Configuration :

- An administrator configures the software with Active Directory settings (address and port). The administrator also defines where the .db SecureJet database file is (it could be shared by multiple stations) and if the csv file should be automatically generated after each enrollment and where it should be written (i.e. in a directory where it is automatically used by the SJ batch admin software to upload information to printers/MFPs).

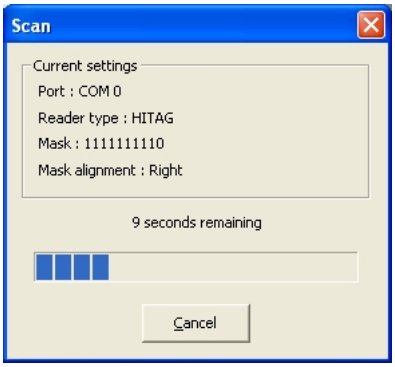
How it works :

Users access the SJ enrollment station where a simple window with 3 fields greets them. Fields are: login, password, domain (pre-filled with a default value by the admin setup)

The user enters their login/pwd and may modify the domain name. The user then clicks on OK.

The captured credentials are checked against Active Directory and the users personal data extracted for SJ.

The user prompted to show their badge to the SJ reader. The badge number is acquired (modified with the mask if necessary).



The captured user data is then written to the SJ database file. If another user has the same badge number, an error number is displayed. If the user was already in the base their data is updated.

The .db file is updated, and if required by the admin a mirror csv is instantly generated for upload to printers/MFPs. The generated file can be used by the batch admin software (in a scheduler) or manually by the admin with the Users List Editor or the Windows Admin Software. There is no real time upload to SecureJet.

Benefits :

The purpose is to provide an easy walkup system for users to register their badge and profile with SecureJet.

NB : Please contact us if you need to write the badge number in Active Directory

VI – Secure access and authentication

SecureJet Auth-PX

If you need to control access to HP Multi Function Printers (MFPs) and printers in your organization, install **SecureJet Auth-PX**. Users will then use their corporate proximity badge to gain access to the device functions such as email, fax, copy or scan. No more login/password to type on the MFP front panel!

Up to 1 million badges supported

SecureJet Auth-PX is a sophisticated badge reader directly connected to the hp LaserJet MFP motherboard, combined with software running inside the printer.

Up to 1 million users can be recognized per MFP. The badge and users list can be securely stored on every MFP hard drive or validated against LDAP or Active Directory upon authentication*. SecureJet Auth-PX offers the fastest authentication at the best price.

Authenticate for MFP applications
The administrator can define which MFP functions users must show their badge to get access. Upon badge number validation, the MFP knows the user name, login and email address of the authorized user. The captured information is then used by the MFP application such as email sending (FROM field), copy tracking or secure printing to reclaim user print jobs.

Authenticate for Secure Printing
On printers and MFPs, Authentication can apply to SecureJet Secure Mobile Printing.

Users reclaim their print jobs stored on the printer/MFP disk or on remote servers by simply showing their badge. *This requires SecureJet Print SMP and PS modules.*

Usable with all MFP functions
Authentication can apply to fax, email, copy, print jobs, scan to folder, DSS Workflow™, hp Autostore™, job tracking and any other MFP function.
*: SecureJet Print PS module required

Supported Proximity badges
HID Prox, HID iCLASS, Mifare, DESFire, Hitag1, EM-Marin and Legic SecureJet Auth-PX readers are available. Please contact us for projects involving other badges. With badge numbers list local to the printer/MFP (securely stored on the device hard drive), the badges number must have a value greater than 999, and 19 digits maximum.

Simple to install
SecureJet Auth-PX connects directly inside the MFP without external box.

System requirements
Supports most hp LaserJet printers, hp LaserJet MFPs and Digital Senders.
Full list at www.jetmobile.com, with device-specific pre-requirements.

Package includes
SecureJet Auth-PX reader
Cable routing adhesive brackets
Internal memory board
Power supply if required and setup guide

Regulation
CE and FCC Certified
WEEE and RoHS compliant

SecureJet Auth-PXT

Users can now authenticate on hp LaserJet printers using a simple PIN code entered on the **SecureJet Auth-PXT** heavy-duty keypad. When combined with the SecureJet Print SMP module, SecureJet Auth-PXT lets users instantly release their pending print jobs stored on the printer hard drive or on SecureJet Print PS print servers.

Up to 1 million users
SecureJet Auth-PXT is a heavy-duty numeric keypad reader directly connected to the hp LaserJet printer motherboard, combined with software running inside that printer/MFP.

Up to 1 million users/PIN codes can be recognized per printer. The PIN codes and users list are securely stored on every printer hard drive or validated against LDAP or Active Directory upon authentication*.

Authenticate for Secure Printing
Authentication on printers is to be combined with the SecureJet Print SMP Secure Mobile Printing module. Users can then reclaim their print jobs stored on the printer disk or on remote servers*, by simply entering their PIN code on the keypad then pressing the # key.
*: SecureJet Print PS module required

Compatible with MFP PIN codes
You have a mix of printers and MFPs? SecureJet Auth-PXT is fully compatible with the Auth-FP module. You can then configure printers and MFPs in one unique operation and end-users have the exact same PIN code on both types of devices.

PIN codes generation
SecureJet can extract users list from LDAP and ActiveDirectory, generate random PIN codes and email them to end-users.

PIN codes range
PIN codes can have any value from 1000 to 999999999.

A robust keypad
The Auth-PXT is water and dust-proof. Its key contacts are heavy-duty.

Simple to install
SecureJet Auth-PXT connects directly inside the printer without an external box.

System requirements
Supports most hp LaserJet printers. Full list at www.jetmobile.com, with printer-specific pre-requirements.

Package includes
SecureJet Auth-PXT Keypad
Cable routing adhesive brackets
CF internal card
Power supply and setup guide

Regulation
CE and FCC Certified
WEEE and RoHS compliant

SecureJet Auth-FP

Users can now authenticate on hp LaserJet MFPs using a simple PIN code entered on the front panel touch screen. Once authenticated users can then gain access to the device functions such as email, fax, copy, scan or secure mobile printing. No more login/password to type on the MFP front panel!

Up to 1 million PIN codes

SecureJet Auth-FP runs directly on the MFP front panel touch screen. It does not require any extra hardware, power supply or network plug.

Up to 1 million users/PIN codes can be recognized per MFP. The PIN codes and users list can be securely stored on every MFP hard drive or validated against LDAP or Active Directory upon authentication*. SecureJet Auth-FP offers the fastest authentication at the best price.

Authenticate for MFP applications
The administrator can define which MFP functions require users to enter their PIN code to obtain access. Upon PIN code validation, the MFP knows about the user name, login and email address. That information is then used by the MFP application such as email sending (FROM field), copy tracking or secure printing to reclaim user print jobs.

Compatible with printers PIN codes
You have a mix of printers and MFPs? SecureJet Auth-FP is fully compatible with the Auth-PXT module. You can then configure MFPs and printers in one unique operation and end-users have the exact same PIN code on both types of devices to retrieve print jobs.

Usable with all MFP functions
Authentication can apply to fax, email, copy, print jobs, scan to folder, DSS Workflow™, hp Autostore™, job tracking, secure mobile pull printing* and many other MFP functions.
*: SecureJet Print PS&SMP modules required

PIN codes generation
SecureJet can extract users list from LDAP and ActiveDirectory, generate random PIN codes and email them to end-users.

PIN codes range
PIN codes can have any value from 1000 and 9999999999999999999.

Simple to install
Just insert the SecureJet Auth-FP memory card inside the MFP.

System requirements
Supports most hp LaserJet MFPs and Digital Senders. Full list available at www.jetmobile.com, with printer-specific pre-requirements.

Package includes
MFP internal card
Setup guide

Regulation
CE and FCC Certified
WEEE and RoHS compliant

SecureJet Auth-Fingerprint

If you need to control access to hp Multi Function Printers (MFPs) in your organization, install **SecureJet Auth-Fingerprint** on your hp MFPs.

Users will then use their finger to authenticate and get access to the device functions such as email, fax, copy or scan.

No more PIN code to remember, no more lost badge!

Designed:

- for Digital Sender 9200C, LaserJet 4345mfp, 4730mfp, 9040mfp, 9050mfp, 9500mfp
- to be fully compliant with the Auth Manager II
- to be installable and usable in 10mn to be heavy-duty
- to be compliant with US government requirements
- to accept up to 500 regular users per MFP, 2 fingers per user
- to recognize one user across 500 in less than 2s
- to be compatible with alternative authentications

Markets:

Small and Medium Business:

- Easy authentication
- Self-management through NTLM, LDAP/AD, Kerberos…
- Avoids to use badges that might not be used for doors
- Supports up to 500 users without any administration

Enterprise:

- Easy authentication
- Self-management through LDAP/AD, Kerberos…
- Compatible with Autostore, DSS, SecureJet pull printing, MIPA, MegaTrack etc

Top-quality fingerprint recognition

SecureJet Auth-Fingerprint is a sophisticated biometrics sensor allowing users to enroll and authenticate on hp LaserJet MFPs using their finger instead of their login and password.

Users enroll using the MFP built-in LDAP, Active Directory or Kerberos network authentication.
Up to two fingers can be enrolled per user, and up to 500 users can be enrolled per MFP.
SecureJet Auth-Fingerprint offers the fastest enrollment and recognition speed at the best recognition rate.

Authenticate for MFP applications
The administrator can define what MFP functions requires authentication. Users show their finger to get access to those functions.
Upon recognition of the user, the MFP knows about the user name, login and email address.
That information is then used by the MFP application such as email sending (FROM field), copy tracking or secure printing to reclaim the user print jobs.

Usable with all MFP functions
Authentication can apply to fax, email, copy, print jobs, scan to folder, DSS Workflow™, hp Autostore™ SecureJet Secure Mobile Printing and any other MFP function.

Fits any business size
Up to 500 users can be enrolled per MFP, directly on the device.

No management required
Inactive users are deleted automatically and users are notified by email.

Simple to install
The SecureJet Auth-Fingerprint reader connects directly inside the MFP and requires no external box, PC or server.
It is configured through the printer embedded web page.

System requirements
Supports most hp LaserJet MFPs and Digital Senders devices.

Full list in chapter V of this white paper.

One EIO card slot and one CF slot must be available inside the device.

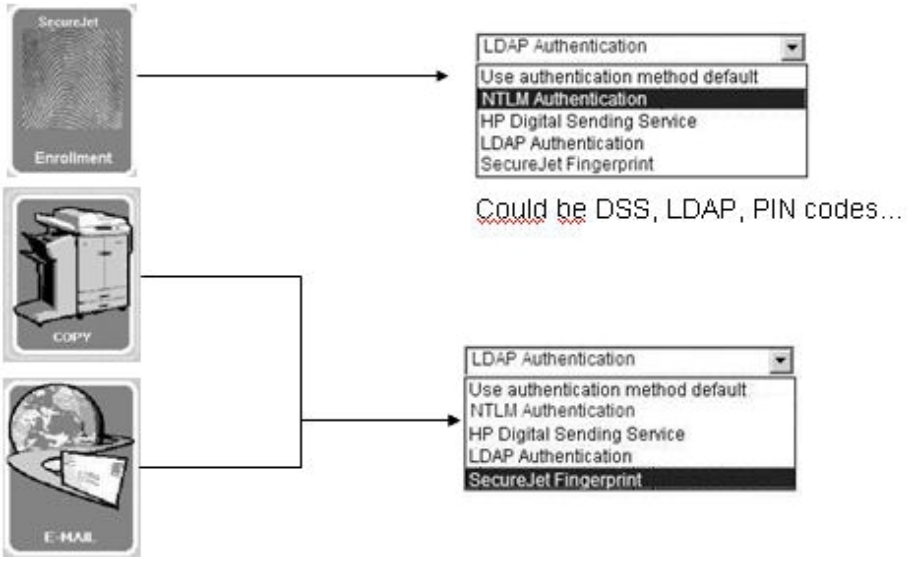
Package includes
Auth-Fingerprint sensor
Cable routing adhesive brackets
MFP internal
cards and Setup guide

Usage of SecureJet Auth-Fingerprint

SecureJet Auth-Fingerprint makes it very easy to control MFP usage with biometrics. It requires virtually no management and runs interactively from the MFP screen.

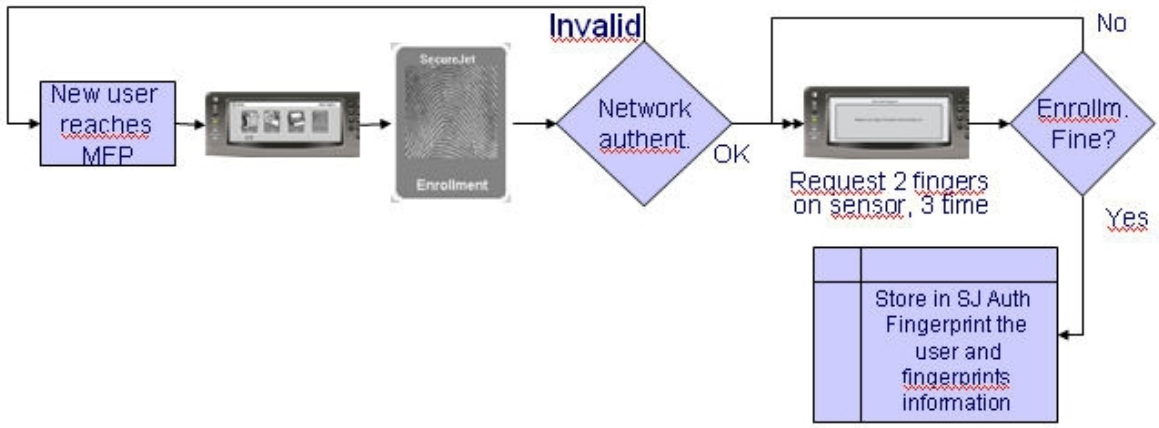
You only need to configure the MFP Authentication manager, to select the authentication to use during enrolment and what MFP functions should be accessible only upon biometrics authentication:

Authentication Manager configuration:



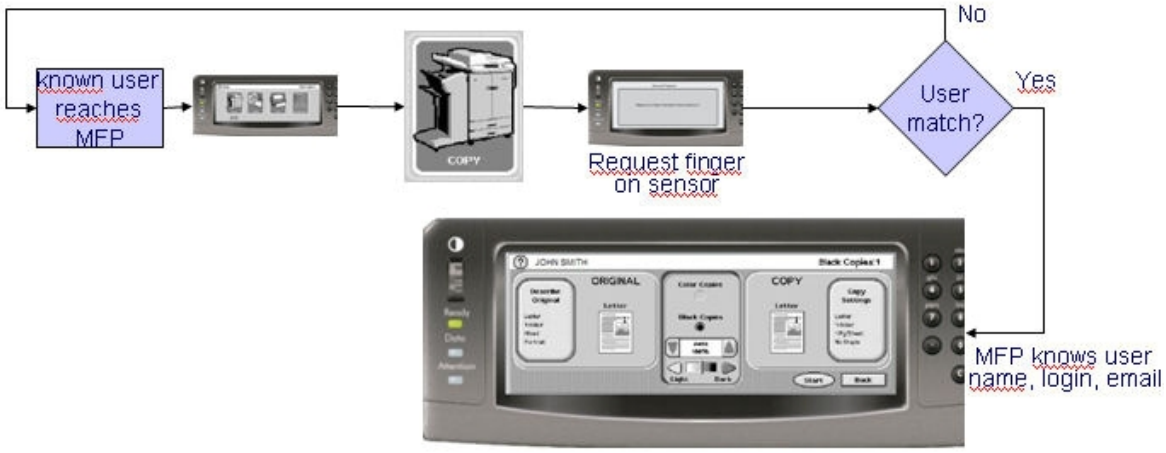
User enrollment process

- Up to 500 users recognized
- Up to 2 fingers per user
- Detection of re-enrolment
- Time to enroll (after ID): 1 to 3s



User login process once he is enrolled

- Recognition time for 1 user across 500 users: < 3s
- Users inactive for more than X days are removed from the system (admin – defined)
- User biometrics data and FW is not affected by Disk Init and HW changes



SecureJet Auth-SC

If you need to control access to hp Multifunction Printers (MFPs), Digital Senders and printers in your organization and your employees are equipped with a supported smartcard, install SecureJet Auth-SC. Employees will then use their corporate smartcard to get access to the device functions such as email, fax, copy, scan or secure mobile printing. No more login/password to type on the MFP or digital sender front panel, and secure user authentication on printers!

Up to 1 million users & smartcards

SecureJet Auth-SC is a sophisticated smartcards reader directly connected to the hp LaserJet printer, MFP or DigitalSender motherboard, combined with a software running inside the printer. Users insert the smartcard in the reader, type their PIN code and get authenticated.

Up to 1 million users can be recognized per device. The smartcard contains all user information in a X509 certificate. That can be the user name, email address and login. It is also possible to read a user PID (unique identifier) from a X509 certificate inside the smartcard and validate it live against a LDAP or Active Directory server to obtain the user profile.

X509 certificates Validation, CRL, OCSP
SecureJet can optionally verify the repudiation of the smartcard certificate against an OCSP server or a CRL, providing a state of the art secure authentication.

Authenticate for MFP applications
The administrator can define for what MFP functions users must use their smartcard to get access. Upon smartcard validation, the MFP knows about the user name, login and email address. That information is then used by the MFP application such as email sending (FROM field), copy tracking or secure printing to reclaim the user print jobs.

Authenticate for Secure Printing
On printers and MFPs, Authentication can apply to SecureJet Secure Mobile Printing. Users can reclaim their print jobs stored on the printer/MFP disk or on remote servers, by simply swiping their badge. *This requires the SecureJet Print SMP and PS modules.*

Usable with all MFP functions
Authentication can apply to fax, email, copy, print jobs, scan to folder, DSS Workflow™, hp Autostore™, job tracking and any other MFP function.
*: SecureJet Print PS module required

Supported smartcards
Most Axalto, Schlumberger, Gemplus and Gemalto smartcards. For other smartcards please contact Jetmobile.

Simple to install and secure
The SecureJet Auth-SC reader connects directly inside the MFP and printers without external box.

System requirements
Supports most hp LaserJet printers, MFPs and Digital Senders.
Full list at www.jetmobile.com, with device-specific pre-requirements.

Package includes
SecureJet Auth-SC reader
Cable routing adhesive brackets
MFP internal card
Setup guide

Regulation
CE and FCC Certified
WEEE and RoHS compliant

SecureJet Auth-SW

If you need to control access to hp MultiFunction Printers (MFPs) and printers in your organization, install **SecureJet Auth-SW**. Users will then use their corporate magnetic swipe card badge to get access to the device functions such as email, fax, copy or scan. No more login/password to type on the MFP front panel!

Up to 1 million badges

SecureJet Auth-SW is a sophisticated swipe badge reader directly connected to the hp LaserJet printer/MFP motherboard, combined with a software running inside that printer/MFP.

Up to 1 million users can be recognized per printer/MFP. The badge and users list can be securely stored on every printer/MFP hard drive or validated against LDAP or Active Directory upon authentication*. SecureJet Auth-SW offers the fastest authentication at the best price.

Authenticate for MFP applications
The administrator can define for what MFP functions users must show their swipe badge to get access. Upon badge number validation, the MFP knows about the user name, login and email address. That information is then used by the MFP application such as email sending (FROM field), copy tracking or secure printing to reclaim the user print jobs.

Authenticate for Secure Printing
On printers and MFPs, Authentication can apply to SecureJet Secure Mobile Printing. Users can reclaim their print jobs stored on the printer/MFP disk or on remote servers, by simply swiping their badge. *This requires the SecureJet Print SMP and PS modules.*

Usable with all MFP functions
Authentication can apply to fax, email, copy, print jobs, scan to folder, DSS Workflow™, hp Autostore™, job tracking and any other MFP function.
*: SecureJet Print PS module required

Supported magnetic badges
Swipe cards with ISO 1, 2 and 3 magnetic tracks. For special requirements please contact us. With badge numbers list local to the printer/MFP (securely stored on the device hard drive), the badges number must have a value greater than 999, and 19 digits maximum

Simple to install
The SecureJet Auth-SW reader connects directly inside the MFP without external box.

System requirements
Supports most hp LaserJet printers, MFPs and Digital Senders.
Full list at www.jetmobile.com, with device-specific pre-requirements.

Package includes
SecureJet Auth-SW reader
Cable routing adhesive brackets
MFP internal card
Setup guide

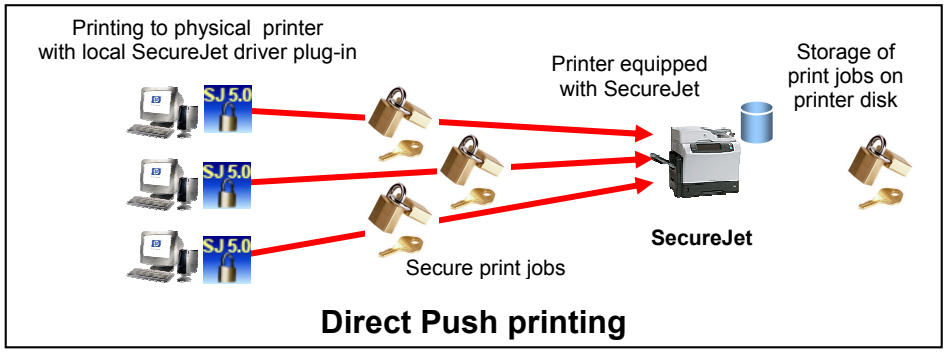
Regulation
CE and FCC Certified
WEEE and RoHS compliant

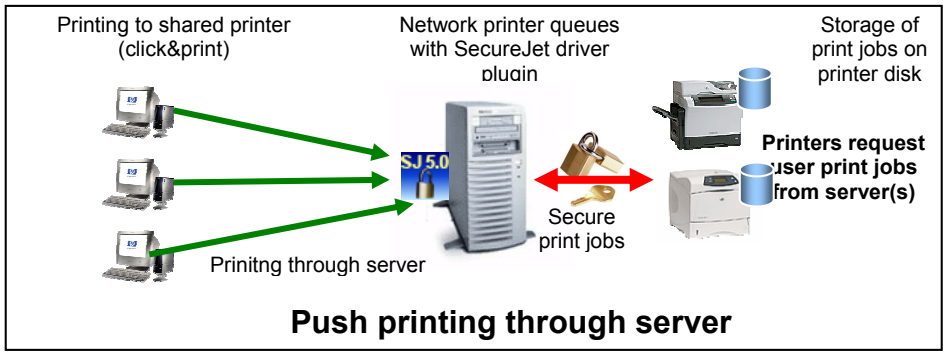
VII - Smart Printing

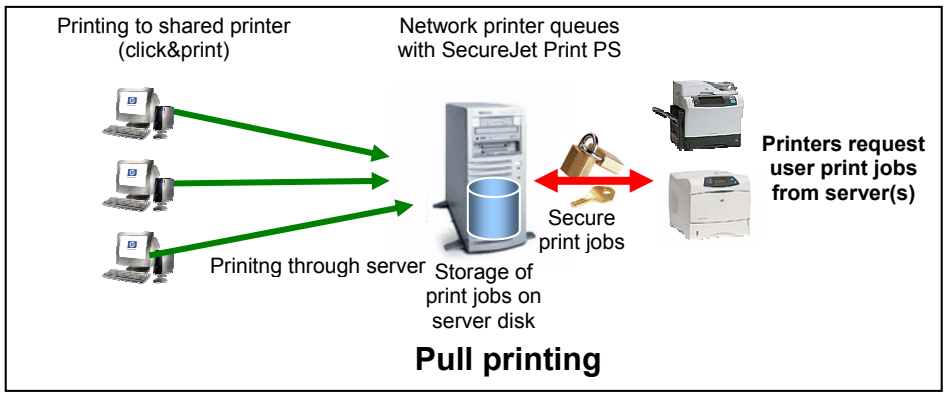
What if end-users in your organization could release their print jobs on any hp printer or MFP in the company, when and where they want, just by authenticating?
This would definitely create very significant productivity gains and reduce cost by getting rid of unclaimed documents on the printers' output tray.
This is now possible with the **SecureJet Print PS** software on server with **SecureJet Print SMP** modules installed on hp LaserJet printers and MFPs.

PUSH printing or PULL printing?

SecureJet Smart Printing allows you to secure the delivery of documents by storing the print jobs on hard drive until their owner authenticates to reclaim them. That storage can happen on the target printer (Push printing) or on print server (Pull printing).







Push printing requires the SecureJet Print-SMP module, and Pull printing requires in addition the SecureJet Print PS-module on print servers. Authentication can be performed by SecureJet Auth modules or built-in MFP authentication providing the user login name information.

Note: when SecureJet Print-PS is installed on the print server, it is only required to install the Driver Plug-in on client PCs if print jobs must be encrypted between the clients and the server, or if a Novell Netware server is between the client PC and SecureJet Print-PS server.

SecureJet PRINT-SMP

Beyond their high cost, all those unclaimed documents on your printers output tray are a very critical security leak: any confidential information that falls into the wrong hands can be detrimental to your company. Imagine the consequences if printouts of your human resource or financial documents were whisked away by an unauthorized employee or a visitor before you can pick them up at the printer's output tray. The SecureJet Print SMP modules installed on hp LaserJet printers and MFPs is the solution, securing both the print jobs data and release.

Print Jobs are securely retained
SecureJet Print SMP is a module running inside the printer or MFP. It provides secure push printing by storing incoming secure jobs on the print or MFP hard disk drive. When the owner walks to the printer and authenticates, his print jobs are decrypted on the fly and printed instantly.

Productivity & security gains
Documents won't be printed until their owner is facing the printer, waiting for them. This reduces printing waste, increases documents confidentiality and lets users reclaim all print jobs in one shot when they need them.

Unclaimed print jobs self-delete
Print jobs have an expiration date after which they are deleted if not printed.

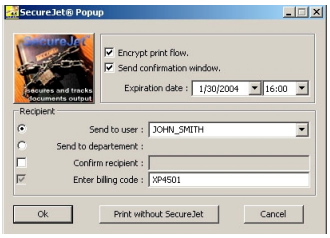
Data encryption included
To protect your confidential data en-route to the printer/MFP, Print-SMP comes with print job data encryption.

Jobs list on MFPs screen
On MFPs the user jobs are listed can be released or deleted individually.

- Local printer HD is checked (Push printing)
- SecureJet Print-PS are checked (Pull printing)
- All push and pull print jobs are listed together
- User can select print jobs for info/print/delete
- Also possible: Print all by just showing your badge
- Direct keyboard prompt of PIN code or billing code

User authentication
Users may authenticate on MFPs using any built-in authentication such as LDAP, Kerberos or Active Directory.
On printers and MFPs, SecureJet Auth modules authenticate using PIN codes, proximity badges, magnetic swipe cards, smartcard or biometrics.

Optional roaming pull printing
Your printer is not available? When SecureJet Print PS is combined with Print SMP, jobs can be stored on remote print servers and released from any printer equipped with Print SMP.



Driver plug-in on client or server
A driver plug-in is available for client and servers, to secure SMP print jobs in PCL5 and Postscript.
To perform the SecureJet Driver Plug-In installation, you must have downloaded (from www.jetmobile.com) the SecureJet Driver Plug-in on disk, and sufficient rights to install printers, create ports and install system DLLs on the machine. The best profile is the ADMIN rights profile. The Driver Plug-In installation can be copied to network drive and launched from there.

Supported clients and servers
Windows 98, Me, NT, 2000, XP, 2003
SAP R/3, HPUX, Linux Red Hat/Fedora
Novell servers Windows clients (LPR)
Any ERP with editable print driver.

Simple to install
Just insert the SecureJet Print SMP card inside the MFP or printer, or activate the license in SecureJet Auth.

SecureJet PRINT-PS

Print Jobs are retained on print servers until their release

SecureJet Print PS is a distributed server-based application capturing print jobs and storing them on the server hard drive. Nothing else happens until the owner authenticates on any SecureJet Print SMP enabled printer or MFP, to reclaim their print jobs. The reclaimed print jobs are then directly sent to the printer operated by the user.

Productivity & security gains
Documents won't be produced until their owner is at the printer, waiting for them. This reduces printing waste, increases documents confidentiality and lets users reclaim documents when and where they need them.

Quotas and expiration for print jobs
Limits can be set for users: max size for stored print jobs and max storage time.

One print queue for all printers
Reduce the number of print queues you manage as only one printer queue is necessary on every PC.

Data encryption included
To protect your confidential data en-route to the printer/MFP, Print-PS can encrypt all the print job data.

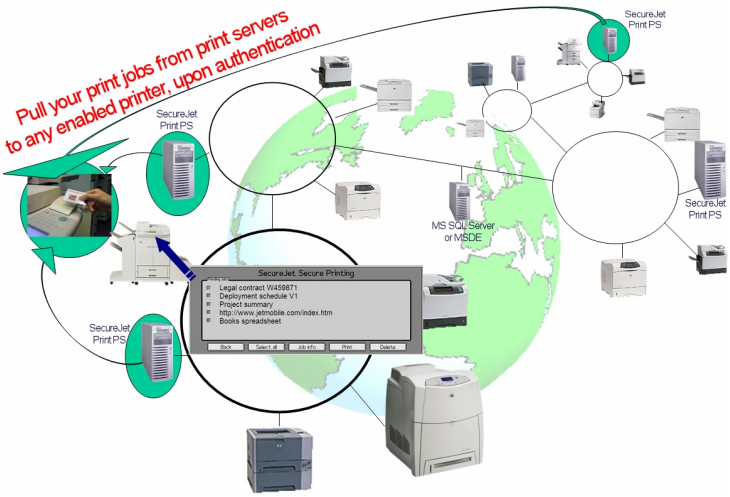
Other functions of Print PS
Print PS performs live ID validation (badge number, PIN code) for SecureJet Auth modules, against LDAP and Active Directory servers.

User authentication
Users may authenticate on MFPs using any built-in authentication such as LDAP, Kerberos or Active Directory.
On printers and MFPs, SecureJet Auth modules authenticate using PIN codes, proximity badges, magnetic swipe cards, smartcard or biometrics.

Supported system features
Cluster servers, Citrix Metaframe
Windows Terminal Server
SAP R/3, HPUX, Linux Red Hat/Fedora
Roaming printing across servers

Simple to install
SecureJet Print PS installs in just a few minutes and requires no database when less than 6 servers are queried from one same printer or MFP.

System requirements
Windows 2000 Server/XP/2003 Server
PCL5 or Postscript printer drivers
HDD capacity to store all print jobs
TCP/IP between printers and server
MS SQL Server for roaming printing



Live LDAP and Active Directory authentication service

SecureJet Print-PS also hosts a service for SecureJet FP/PX/PXT/ FXT/SW adding:

- live user authentication against Microsoft Active Directory and LDAP directories
- management of alias, to allow multiple logins for the same user and ID

Live authentication against Active Directory/LDAP database

The SecureJet authentication module on the printer/MFP gets all user information (login name, department, email address, full name) from Active Directory/LDAP through the server hosting SecureJet Print-PS.

When the live authentication is activated, there is no need to load the users list on every printer/MFP, all badge numbers and PIN codes are validated on-line. On the other hand, authentication won't be available if the communication with the SecureJet Print-PS server is not available (failing cable, router, switch or server).

Support for multiple databases

In some environments, multiple Active Directory and/or LDAP databases are used. One handles the badge number, another one the user Information etc. SecureJet features a highly flexible system to gather data from multiple databases, using common information to retrieve the correct record.

Failover capability

Up to 5 SecureJet Print-PS server addresses can be entered in the Authentication Module configuration. If the first server does not respond the next one will be used and so on. This allows setting up multiple SecureJet Print-PS servers for live authentication and to have a complete failover capability, should one server not respond in a timely manner.

Support for multiple user logins (Alias system)

In a corporate IT environment, a user can have more than one login: one for Windows, one for the mainframe, one for the Unix system, one for the ERP etc. That means print jobs from those various systems come with a different login name, while the jobs owner is unique and has a unique ID (badge, PIN code etc). Furthermore, each login and user information might be in a system-specific Active Directory or LDAP database.

SecureJet allows defining alias search in multiple Active Directory and/or LDAP databases, using common information like employee number to find the appropriate record. All print jobs for one user, whichever logins is used, are allocated to one unique (main) login. The user can then authenticate using one unique ID.

Roaming mobile printing

Roaming mobile printing allows to store print jobs on various servers and to release them from anywhere, even on a MFP or printer not linked to that server. This feature is particularly useful when securing print jobs for third party users, who might be located in another region.

Pre-requirement for roaming printing

Roaming printing **requires a database on one server** (that server does not need to have SecureJet Print-PS installed):

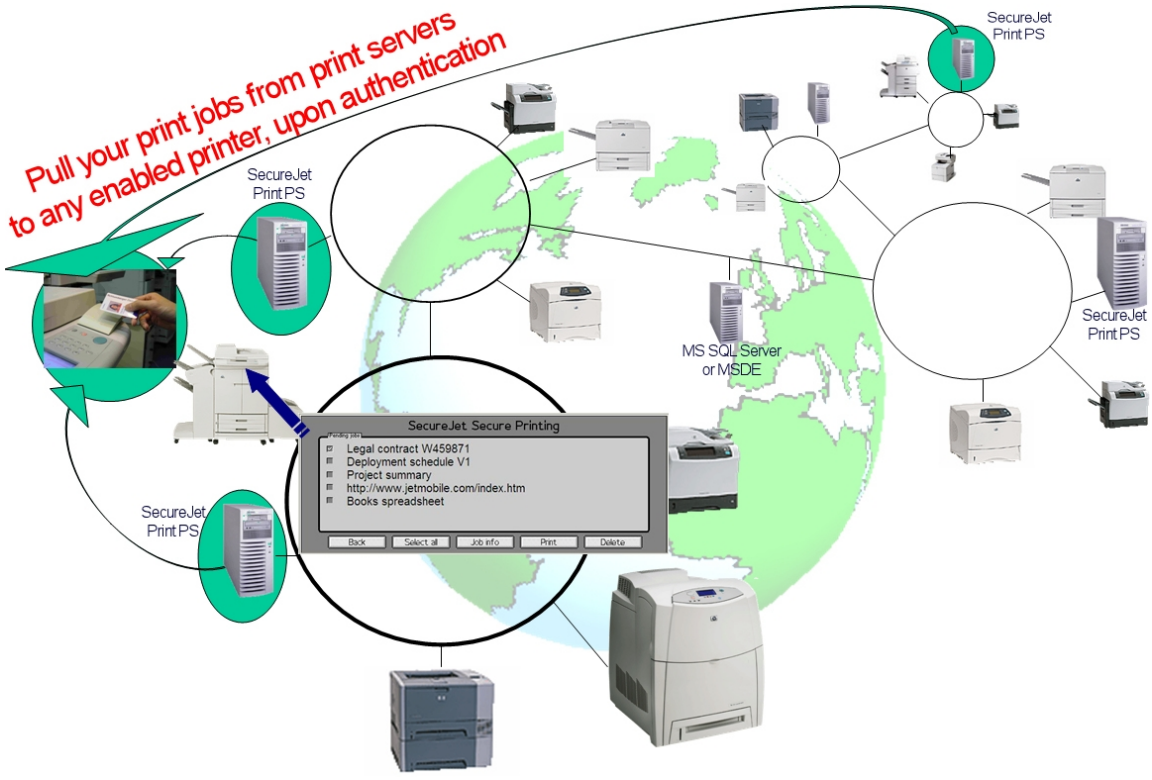
- a functional Microsoft SQL Server 2000 or newer (with SQL or mixed Windows/SQL authentication),)

or

- a MSDE database (SP3A with SQL or mixed Windows/SQL authentication), and administrator access.

- SQL/MSDE network configuration: TCP (default port 1433)

The SecureJet roaming printing allows to release from a printer or MFP equipped with SecureJet Print SMP documents stored on any SecureJet Print-PS servers on the Intranet.



This allows many powerful workflow capabilities, such as:

- A user in Europe prints a document for his colleague in New-York
- The job is securely stored on the server closest to the European user
- The addressee in the US reaches a MFP in New-York and authenticates
- The document output by his European colleague is listed
- The addressee in the US request the job release
- The document is sent directly from the European server to the NY MFP

The SecureJet Print-PS architecture ensures no useless communication happens between servers and MFPs.

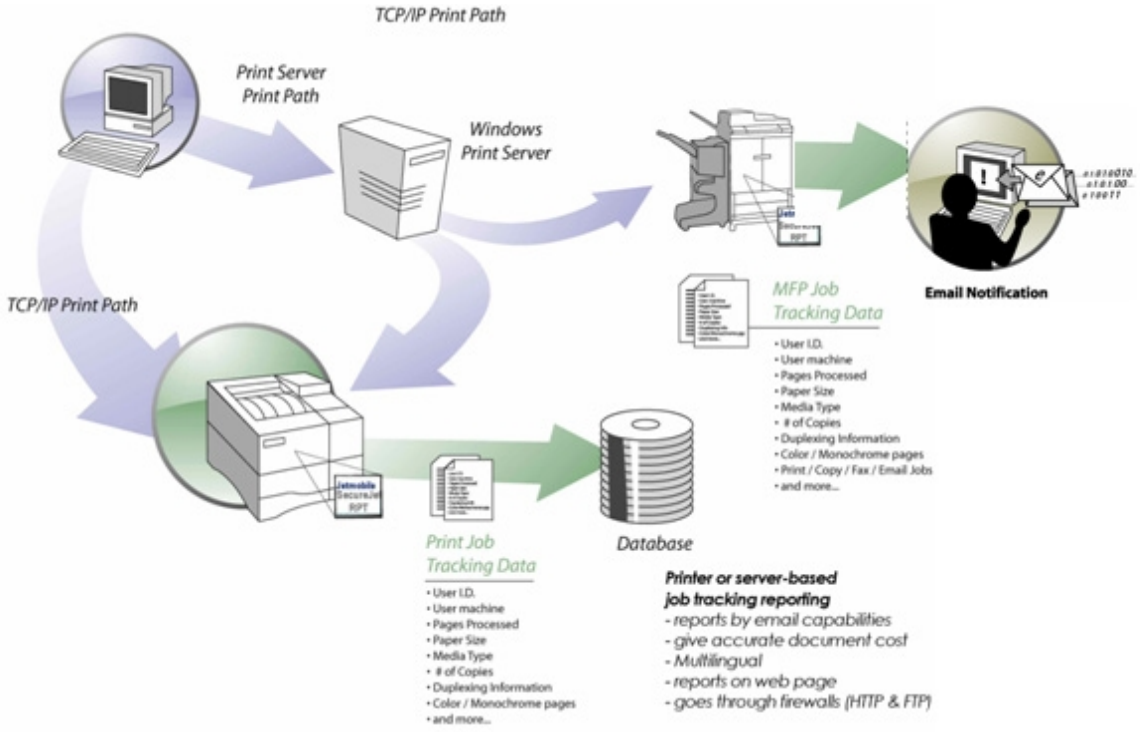
- Only 1 print queue on PCs
- Print to any retention server
- Receive documents on any jobs retention server
- List and release those job from any hp MFP/printer equipped with SecureJet
- Intranet solution
- Driver Plug-in included in the Print PS monitor (no more print processor)
- Compatible with current hp drivers (hp UPD: Q3/06)
- No billing code, secure for sender only

VIII – Jobs tracking

How to track and report print, copy, fax, email usage & cost? By using the **SecureJet Track-TRP** module:

- Built-in reporting from the printer/MFP web page, with email capabilities
- Reporting through a server and MSDE/SQL, for multiple MFPs/printers
- Encrypted HTTP and FTP communication
- Plug&play with MegaTrack and advanced features (billing codes, local printers…)

    - Total confidentiality for printed documents through data encryption
    - Release of documents at the exact time/location they are needed
    - No disruption of the work, users collect documents when they have time
    - Documents can be secure for release by another user
    - Unclaimed documents are not output, and automatically erased at expiration time



Information tracked and reported by SecureJet Track TRP on current generation printers, with the latest drivers and firmware:

User login	✓
User domain (Active Directory)	✓
User group (Active Directory)	✓
Computer name	✓
Job name	✓
Submit date	✓
Total page count	✓
Simplex page count	✓
Duplex page count	✓
Color pages count	✓
Economode	✓
Media type	✓
Media size	✓
Paper orientation (Portrait/Landscape)	✓
Job size	✓

Conditions for tracking job titles and print job owners:
SecureJet uses information added by hp printer drivers at the beginning of print jobs data. If the application and driver do not add user and job information to the print flow, SecureJet won't be able to report that information. You can get SecureJet to stop those anonymous jobs from being printed by activating the STOP ANONYMOUS JOBS option on the configuration page.

SecureJet Track-TRP can email tracking data, and features a web reporting tool:

A web page in the printer offers all management functionalities in order to retrieve information by email, in the CSV format.

SecureJet Track-TRP also includes a MRT (MegaTrack Reporting Tool) license for Windows 2000, XP and 2003. MRT stores centrally in a MS-SQL or MSDE database the tracking information from all printers and MFPs equipped with SecureJet Track-TRP. MRT also provides full web and email reporting and analysis capabilities, including toner usage forecast and detailed color usage reports.

- Graph of print jobs volume per hour/day/month/year
- Total Cost of Ownership of a printer
- Cost of all jobs sent by a user to any printer
- Volume printed by a printer, volume printed by a group, a user …
- Usage of color vs. Black & White
- Pie chart for allocation of print jobs amongst MFPs and printers, company-wide …

If you use SecureJet in association with MegaTrack™:

MegaTrack is used to track legacy printers not equipped with SecureJet Track-TRP via print servers, SecureJet Print TRP can also send data to MegaTrack to track all printer usage.

MegaTrack is a print/copy/fax/digital sending tracking and accounting software running under Windows platforms. It is an easy way to monitor, allocate and, ultimately, optimize your printing costs. By monitoring local and remote print-servers it provides you with comprehensive real-time and statistical information on printer usage and the cost of printing - data that can be broken down according to the department, cost-center, project or even employee or printer. The end result is data you can use to optimize the cost-efficiency of your printing.
The MegaTrack Web-Server prepares detailed, customized reports, combining graphics and text that show you the composition of your printing costs. These statistics and reports can be accessed and administered from anywhere in your organization, using any standard web-browser.
Examples of information generated by MegaTrack:

- Graph of print jobs volume per hour/day/month/year
- Total Cost of Ownership of a printer
- List of all jobs printed through all print servers
- Cost of all jobs sent by a user to any printer
- Volume printed by a printer, volume printed by a group, a user …
- Usage of economode, duplex
- Usage of color vs. B&W on hp LaserJet 5500/9500/…
- Pie chart for allocation of print jobs amongst printers, company-wide …

For more information please go to www.capellatech.com

SecureJet tracking information file format

SecureJet Track-TRP generates CSV (semi-colon delimited file format) files that can be loaded in spreadsheet software like Microsoft Excel and also in databases.

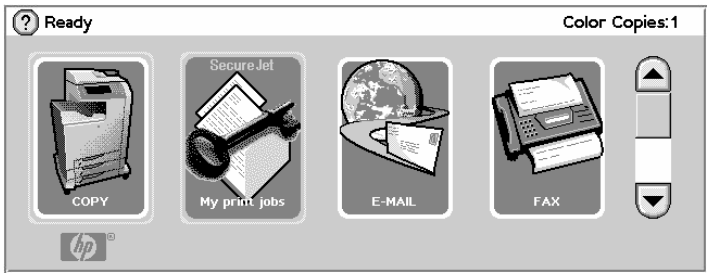
Important notes:

- SecureJet Track-TRP is a technology licensed from Capella Technologies, and also available from Capella as MIPA.
- SecureJet Track-TRP is proposed only in Europe, Middle-East and Africa.
- In other regions, please use MIPA and contact Capella Technologies for pricing and information about distribution. http://www.capellatech.com

IX – Using SecureJet, some examples

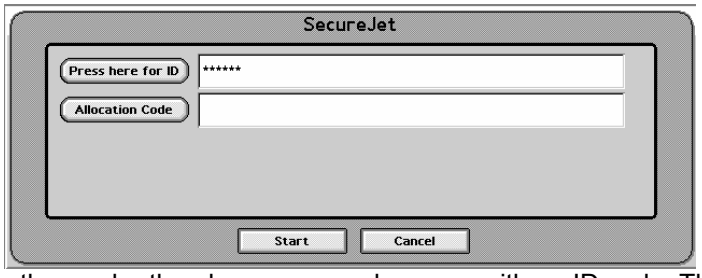
How to make a copy on lj4730mfp using SecureJet Auth-PX?

The hp LaserJet 4730mfp works in a manner similar to the LJ4345mfp, 9040mfp, 9050mfp, 9500mfp and Digital Sender 9200C.



Reach the MFP, press the “COPY” button to make a copy and put some pages in the document feeder. The SecureJet authentication screen or message shows up, requesting to show the badge.

After the beep, show your badge to the reader, at a distance up to 3 cm.
The reader beeps and the confirmation screen shows up, with the card ID appearing in the ID field as *****.



If no card is shown to the reader the above screen shows up with no ID code. The user can then enter manually his ID (badge number, PIN code) in case he forgot his badge at home. This is done by pressing on the 

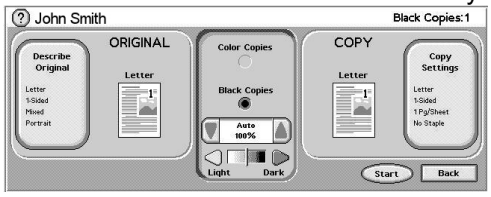
. A new screen shows up, in which the ID can be entered (decimal value only, no hexadecimal values).

Note: This screen can be skipped by activating the “no billing code” in the SecureJet configuration. That creates a shortcut to directly access the function upon card reading.

Press the OK button in that screen to validate the entry and go back to the main screen.

If you wish to enter a billing code, press the “Allocation Code” button. A new screen appears, in which you can enter the billing code. Press the OK button in that screen to validate the entry.

You are now authenticated, the copy screen shows up, your name shows up on the top left corner.
Logout happens after an admin-defined time-out or by using the RESET or Logout buttons.



How to secure a document?

SecureJet secures documents in the following way:

- Print jobs data encryption, using DES or AES with dynamic keys (unique for each job)
- With AES, SecureJet uses an exclusive 128bits AES+ 2048 RSA PKI public/private keys scheme to ensure the highest possible security for print jobs data.
- Documents are not printed when they reach the printer
- Release made possible only by a specified user or team
- Automatic deletion of a print job when its expiration date/time is reached, before it is even decrypted

SecureJet allows securing documents for:

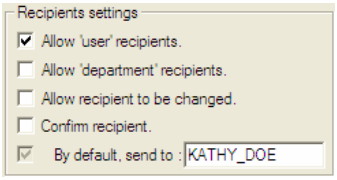
- The person who prints
- Another person from the intranet
- A team/department

Sending a document to yourself under Windows

When printing from Windows, by default your login name shows up in the “Send to user” field. Just click on OK to secure the document for yourself.
If you are only securing documents for yourself (never for other people) then you may even disable the SecureJet popup window. Printing will be as simple as clicking on the Print icon of your application. The driver plug-in can then be installed locally on the PC or on a remote server.

Sending a document to other users under Windows

You must have the driver plug-in installed locally to type in a recipient addressee login name in the SecureJet popup windows. If the driver plug-in is on a network printer the popup appears on the server and not on the client (the server spooler runs as system and not with your credentials). SecureJet remembers the last 10 entries, unless the “No history” option is selected in the driver plug-in configuration.



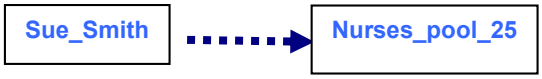
You can also send a document to another user by forcing all print jobs of a queue to be secure for that specific user. In the Windows printer configuration SecureJet tab, enter the recipient login name in the “By default, send to:” field. You then must check only the “Allow ‘user’ recipients” to indicate this is a user login and not a department name.

Note: The driver plug-in can then be installed on the print server and multiple queues can be setup, each securing jobs for a specific user.

Sending a document to a department: example

When sending a document to a department, any user from that department can release the document, which is then immediately deleted. Here this concept is applied to a hospital as an example:

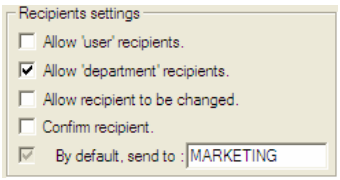
Nurses receive documents from doctors, indicating the care to provide to patients. Nurses are organized in pools (teams) and any nurse from the pool may take care of a patient, based on availability. They release documents using their badge, making sure only authorized people release and read documents containing confidential medical information about patients.
In our example, Sue Smith is in cardiology and needs to send document for a patient hospitalized in the department under the care of a team of nurses grouped in department “Nurses_pool_25”.



That document can be released on a MFP (only) either by any nurse from the pool (SecureJet knows the department for each user). Nurses just need to ask on the MFPs for “Department Jobs”, and they are deleted after the first user releases it. If the documents are not reclaimed they are never decrypted and deleted.

Sending a document to a department under Windows

You must have the driver plug-in installed locally to type in a department addressee name in the SecureJet popup windows. If the driver plug-in is on a network printer the popup appears on the server and not on the client (the server spooler runs as system and not with your credentials).
SecureJet remembers the last 10 entries, unless the “No history” option is selected in the driver plug-in configuration.



You can also send a document to a department by forcing all print jobs of a queue to be secure for that specific department. In the Windows printer configuration SecureJet tab, enter the department login name in the “By default, send to:” field. You then must check only the “Allow ‘department’ recipients” to indicate this is a department name and not a user login.

Note: The driver plug-in can then be installed on the print server and multiple queues can be setup, each securing jobs for a specific department.

Note: Department jobs are currently only supported on MFPs

Sending a document to a user or department under UNIX

For information about securing a document for a user or department under UNIX please refer to the corresponding previous chapter.

Unencrypted secure printing for ERPs

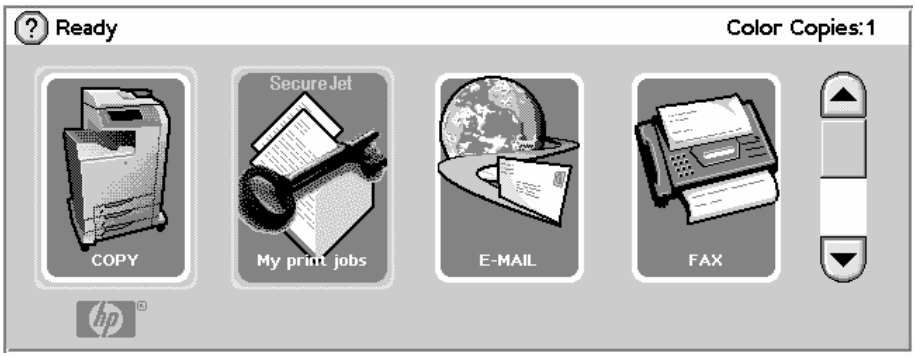
SecureJet can secure the release of unencrypted jobs sent directly to the SecureJet-enabled printer or to SecureJet Print-PS. Those jobs are controlled and tracked as “SJ non-encrypted jobs”. Note that jobs are not encrypted; only their release is made secure by being only accessible by the addressee.

Encrypted secure printing for ERPs

SecureJet can encrypt and secure SAP SAPScript and SmartForms print jobs sent directly to the SecureJet-enabled printer or to SecureJet Print-PS. Those jobs are controlled and tracked as “SJ encrypted jobs”. The document header must include the job information.

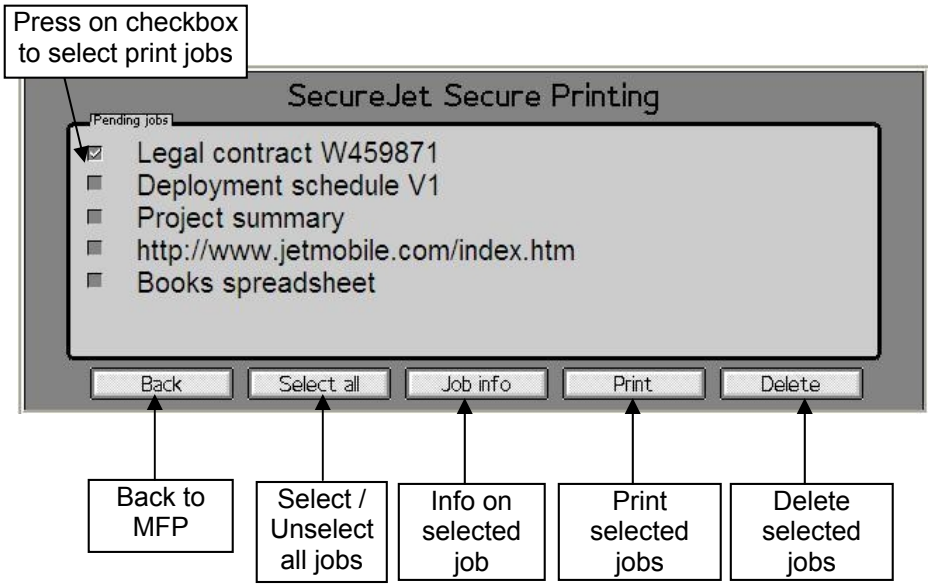
How to release jobs on MFPs?

Current MFPs include icons on their front panel to release print jobs. When you reach the MFP, the following display greets you:



Press the SecureJet button to reclaim your jobs. Authentication is required, using your PIN code or card (depending on the SecureJet product installed).

This screen lists all your jobs, retained locally or remotely (on SecureJet Print-PS servers), and shows action buttons.



You may press the RESET (yellow) button on the MFP front panel to log-out. An internal login time-out is also featured by the MFP, its time-out is defined in the standard printer menu.

Note that the first user who prints a job sent to a department also deletes it. No other department member will be able to access it.

How to release user print jobs on non MFP printers?

Your user print jobs are retained securely by SecureJet on the printer hard disk or on remote SecureJet Print-PS servers until their release or deletion upon expiration.

On Non MFP printers, it is only possible to release User jobs. Department jobs can't be released on non-MFP printers!

Reach the printer and ID yourself (show your proximity badge to the reader, enter your PIN code or swipe your card). After authentication the reader beeps one time and the light goes off.

If the SecureJet option ☑ Release without confirmation. ***is activated:***

- If your badge ID is valid the reader beeps, a message on the front panel indicates how many jobs are to be released fro the printer disk and/or on the SecureJet Print-PS servers and asks if you wish to them.

  The reader will flash as long as you have not answered the question. Press **Go** (on LJ4100) or ✓ **(**on other printers) to decrypted and release jobs. To cancel jobs release press the ▲ key on top of ✓.

- If your badge ID is invalid the reader flashes its red light and beeps one time.

If the SecureJet option ☐ Release without confirmation. ***is deactivated:***

- All your print jobs are released instantly.

If a setup error happens (like SecureJet users list not initialized) the printer beeps 3 times, the red light flashes 3 times and the error message shows up on the printer display. The reader will flash as long as you have not acknowledged the status.

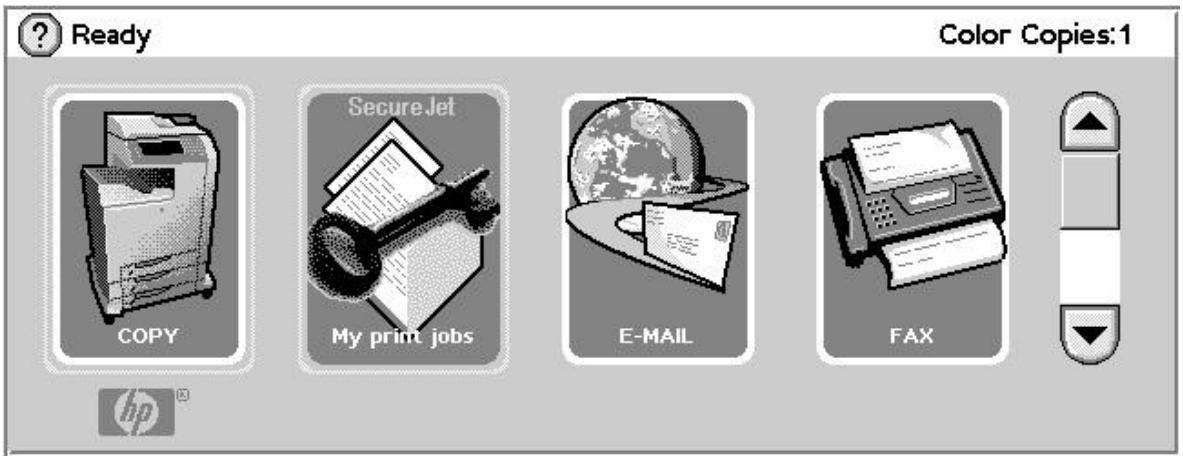
How to authenticate for secure printing using Auth-SW?

On printers:

Reach the printer, and swipe your badge on the SW reader. The printer looks on its hard drive and on remote servers for your jobs, and releases them.

On MFPs:

Reach the MFP to release the job. The following screen is displayed, with the “SecureJet – My print jobs” button next to the COPY button:



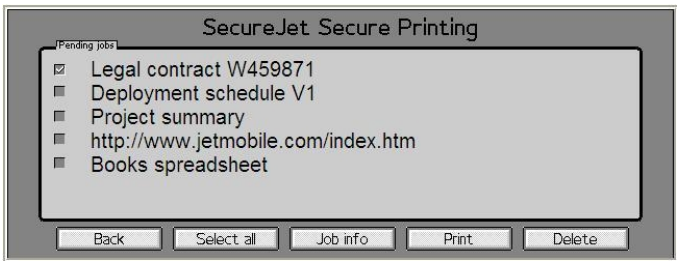
Press the SecureJet button to reclaim your jobs. The SecureJet authentication screen or message shows up, requesting to show the badge.

After the beep, swipe your badge in the reader.

After your badge number is validated the SecureJet screen shows up:

The screen lists all your jobs, retained locally or remotely.

The bottom part of the screen displays available action buttons.



To select print jobs, navigate through the jobs list and select print jobs by pressing on their name or checkbox. Then select an action using Print or Delete.

Printed jobs are tracked by SecureJet Track-TRP.

Use the Back button to go back to the main menu and keep your identity or press the RESET button on the MFP front panel to log-out. An internal login time-out is also featured by the MFP, its time-out is defined in the standard printer menu.

If the badge number is invalid,
the following error messages shows up:

Optionally, if no card is used in the reader, after the time-out a screen shows up where the user can type his ID (badge number) in case he forgot his badge at home. This is done by pressing on the 

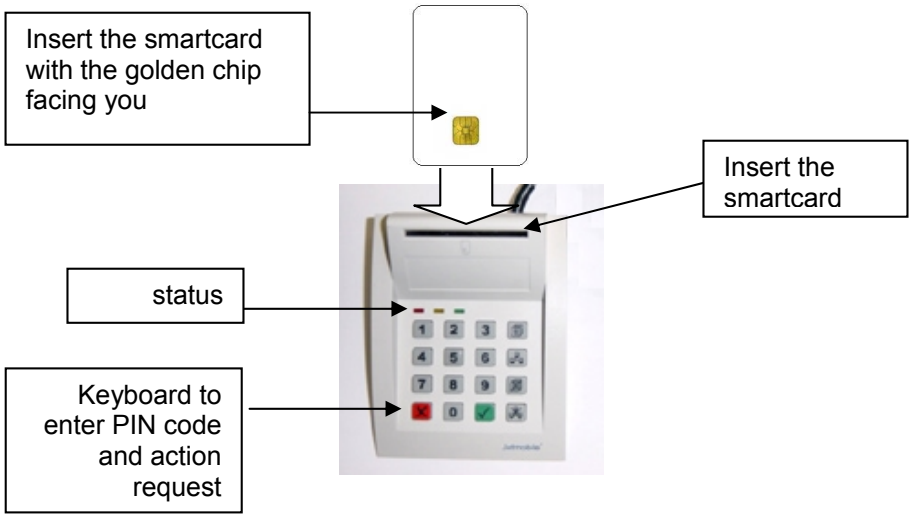
button. A virtual keyboard shows up, where the ID can be entered.

Note: the “no billing code” allows deactivating the virtual keyboard appearance. That allows making a shortcut.

How to release user jobs using SecureJet Auth-SC?

Releasing user jobs on non-MFP printers

Your print jobs can be retained securely by SecureJet on the printer hard disk or on remote SecureJet Print-PS servers. Reach the printer and insert your smartcard in the reader.



The smartcard must be inserted with the golden contacts facing you. Once the smartcard is inserted, the yellow LED changes from blinking to permanently lit. This indicates the card is waiting for its PIN code.

Enter the PIN code on the keypad, then press ✓ to validate. If the PIN code is not initialized, just press ✓.

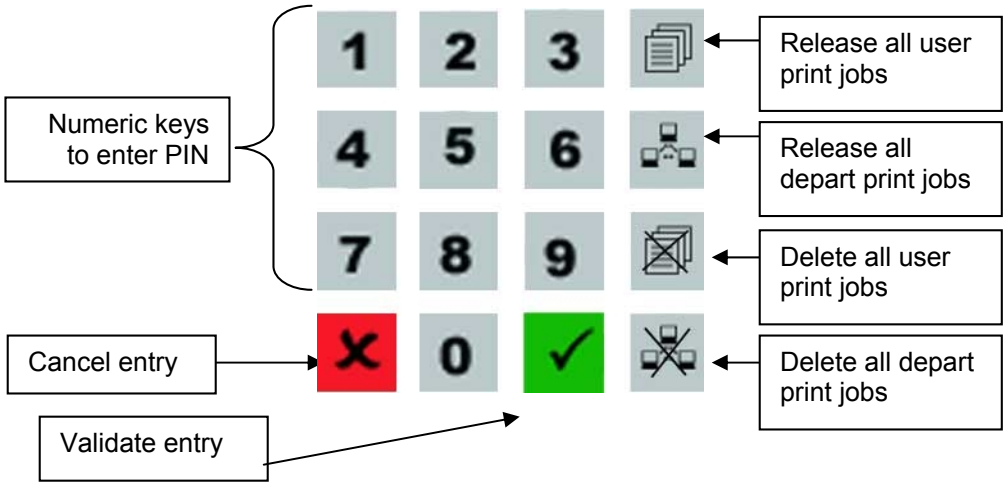
If you make a mistake whilst entering the PIN code, press the ✗ key and start again.

- If the PIN code entered on the keypad is rejected by the smartcard, the red LED highlights and the yellow LED blinks as many times as you have PIN code entry attempts remaining before the card locks itself. The red LED goes off after the last yellow LED count.

- If the PIN code is valid, the green LED blinks, indicating the reader is logged in the smartcard and is awaiting for instructions (jobs release/delete). The yellow LED is off.

You are now logged in your smartcard. You must use one of the 5 action buttons on the right side of the keypad to release and delete, or only delete, your print jobs, or print jobs sent to your department group (please refer to the secure printing chapter for more information on user jobs and department jobs).

You will find below the SecureJet card reader keypad instructions.



Press the  button to release you own jobs and jobs sent to you. Your test print job should be released by the printer.

- Press the  button to release jobs sent to your department. Jobs are erased after release.
- Press the  button to delete your own jobs and jobs sent to you. Warning: Deletion is instantaneous and can't be recovered.
- Press the  button to delete your department jobs.
  Warning: Deletion is instantaneous and can't be recovered.

If the secure document is printed instantly when the job is printed from Windows, either the SecureJet printing was deselected in the SecureJet pop-up window, or the Windows Printer driver configuration was not performed correctly and must be done again.

Releasing user jobs on MFPs

Press the "My print jobs" button on the MFP front panel. The MFP requests the smartcard authentication. Authenticate like on a printer, and your jobs list shows up.

Closing the SC reader session

Just remove the smartcard from the reader once all operations are done or press the MFP RESET button, which purpose is to logout the current user.

X – Where to buy?

Distribution of Jetmobile solutions is performed through a network of VARs who are document solutions experts. This gives you access to an unparallel array of expertise to help you meet virtually any printing challenge.

North and Latin Americas:

For North, Central and South Americas, Jetmobile has formed a strategic partnership with Capella Technologies, where VARs, integrators and clients can find Jetmobile products, information and support. Capella Technologies features an extensive network of VARs in North and Latin America. Please contact Capella Technologies to locate the VAR closest from your company.

Capella Technologies
2099 S. State College Blvd.
Suite 500
Anaheim, CA 92806
Telephone: (714) 385-4900
Fax: (714) 385-7936

Web: www.capellatech.com

email: sales@capellatech.com

Europe, Middle-East, Africa and Asia-Pacific:

There are two categories of VARs in EMEA and Asia-Pacific: Platinum and Gold VARs .

An integrator reaching the **Gold VARs status** for a Jetmobile product becomes part of the Elite of Jetmobile VARs. They manage a large number of deals involving our solutions and have shown a strong expertise. An integrator must go every year through heavy technical training and a certification exam to keep his status. He must also proactively propose Jetmobile solutions to his clients, to resellers and provide complete integration service.

An integrator focusing less on a specific Jetmobile product can be a **Silver VAR** for that product. Whereas they go through yearly training, they are not specialized in the product and usually collaborate with Gold VARs to deliver complete service and integration on that Jetmobile product

Please check http://www.jetmobile.com for the latest list of Jetmobile VARs in your region.

XI - Company overview

Jetmobile®

information traceability, security and mobility

Jetmobile is a privately-owned company created in 1994 to invent firmware-based solutions for HP LaserJet printers, targeted at the corporate world. Its focus is the information traceability, security and mobility.

Since 1994, Jetmobile has developed 2 major products which have become industry-standards (BarDIMM and MicrDIMM) sold at more than 15,000 units per year, and a third (SecureJet) which is also quickly becoming a best seller for authenticating users on hp devices and providing secure mobile printing. Jetmobile has built marketing, technological or strategic alliances and partnerships with industry leaders such as SAP (ERP), HID (corporate badges), Gemalto (Smartcards), hp (Servers, systems, printers and MFPs), ActiveCard (smartcards) to build a bridge between the hp printers & MFPs world and the corporate infrastructure.

Jetmobile clients are primarily corporate 1000 companies, from all oil companies to food industry and airlines. Thanks to its worldwide integration capability Jetmobile is the most international printing solution provider on the market.

Every year Jetmobile invests a very significant budget in R&D and patents, with a major patent in mobile secure printing (delivered in 2005 in the US and 2006 in Singapore, pending in the European Union), and other pending patents with distributed printing innovations.

Jetmobile has also built a worldwide VARs network around a contract focusing on expertise and quality. An exam is conducted every year, covering sales, marketing and technical matters, to select only the best companies. VARs must maintain the proper skills to propose Jetmobile products.

Jetmobile EMEA is located in Issy les Moulineaux in Paris, France (a few blocks west of Paris). It handles sales, marketing and manufacturing for the EMEA region as well as R&D. In its 2005 FY, Jetmobile EMEA enjoyed a 34% growth and has always been profitable since 1994.

Jetmobile Asia is located in Malaysia in Kuala Lumpur, 200 miles north of Singapore. It handles sales, marketing and manufacturing for the Asia-Pacific region as well as quality testing for the Jetmobile R&D team. Jetmobile Asia was setup in February 2006 as an evolution of a previous distribution structure and employs 12 people.

For North and Latin America Jetmobile has teamed with Capella Technologies, distributor for its solutions through its VAR channel. Capella performs all the marketing, sales, training and technical support and is located in California, and in Costa Rica.