

# Print Security and Identity Authorization



# Agenda

- Why Be Concerned about Security in Imaging and Printing?
- Security Vulnerabilities
- In the Press
- HP's Approach to Imaging and Printing Security
- Implementing a Secure Environment
- Identity Authorization

Why be concerned  
about Security in your  
Imaging and Printing  
environment

# How do you protect your property?



# Security is on everyone's radar

## 🔒 Corporations reflecting vulnerabilities from a growing number of security breaches

- Information theft (avg. cost \$2.7M/incident)
- \$59B proprietary and intellectual property loss each year by US companies
- 70% is unauthorized employees; 95% result in financial losses.
- Unauthorized Access is the second biggest cause of financial loss in the US

## 🔒 Consumers increasingly concerned

- 82% of consumers list security as their most important concern when they consider the electronic data they save through digital services
- Decline in online transactions

## 🔒 Government strengthening security *internally* & protecting the public *externally*

- Security policy Mandates to protect government data: US Federal Government's IPv6/IPsec Mandate
- Regulations that protect the Public: Sarbanes-Oxley, HIPAA & Identity Theft Protection Act (pending), California 1387

# Why be concerned about imaging & printing security?

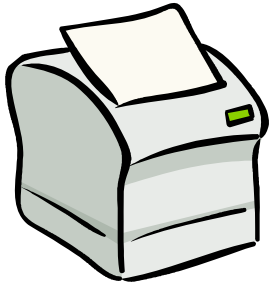
## **Printers/MFPs are intelligent devices, similar to servers and desktops**

- Use many of the same network ports and protocols
- Have many of the same components like hard drives, expandable memory, graphical user interfaces, USB capability

## **Like servers and desktops, printers/MFPs are vulnerable to attack if steps are not taken to secure the environment**

## **Critical business workflows are dependent on printers/MFPs. If printers/MFPs go down, revenue is lost**

# Why Care about Security for Imaging and Printing?



**Confidential Documents Accessible**

**Device Configuration Changes**



**Network Sniffing**

**Information Disclosure**

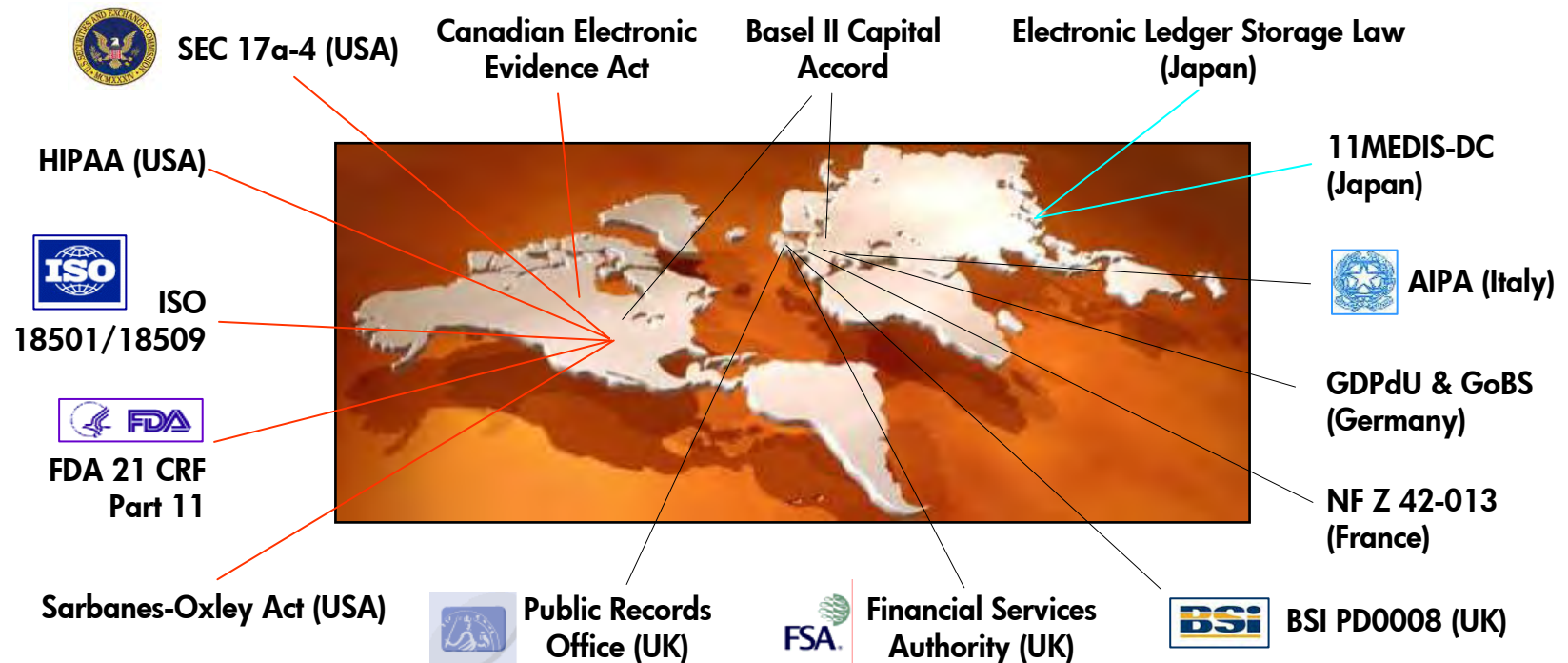


**Hardware Theft**

**Compliance Requirements**



# Compliance... it is everywhere



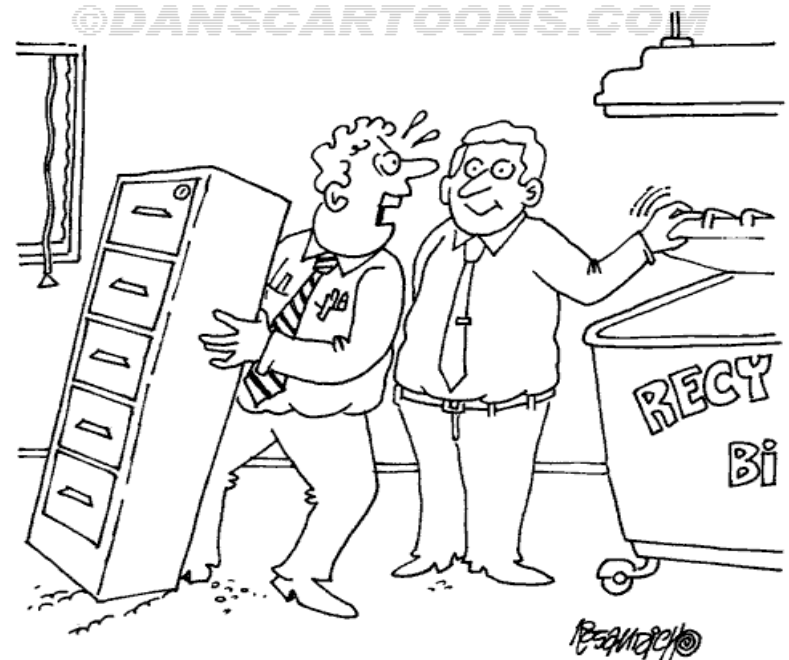
These are just a few examples as there are over 20,000 compliance requirements worldwide

If your company isn't directly affected by compliance, think about your suppliers and partners; they may be and may pass down the request directly to you



# Value of Information Assets

- What type of assets need to be protected?
  - Physical assets & People, Software, Information/Data
- Paper Based Assets (printed information)
- Electronic Based Assets
- Challenge is to strike the balance between PBAs and EBAs
- Secure Printing as the interface between paper and electronic assets
  - must be a controlled environment



**“You sure this is the proper way to drag files to the recycle bin?!”**

**Imaging and Printing Security must be part of the overall IT security strategy!**

# Security Vulnerabilities

# How vulnerable can printing environments be ?

- How much attention do users pay to their print jobs?
  - Leave print outs uncollected
  - Print several copies when only one is needed
  - Users may plug in and install unsupported printing devices
  - Users may scan, copy, fax and e-mail documents without permission using MFPs
- How much attention do organizations pay to their printing environments?
  - Typically only driven by cost control not security considerations
  - Organizations rarely document their printing environment (device type, user/device ratio, MFP features, etc...)
  - Do not integrate or manage their printing rights (+MFP rights) centrally
  - Typically feel safe from Internal abuse and only consider External abuse

# “Printer attacked!!!”

- 1999: Space and Naval Warfare Systems Command (SPAWAR) in San Diego
- Intruder hacked into printer and re-configured routing tables on SPAWAR equipment
- Files in the print queue were directed to Russia and then back to SPAWAR printer
- Hijacker could keep a copy or even modify its contents
- Noticed only when an impatient network ops engineer noticed that his local print job took an unusually long time to start printing
- Like most hacks, it has not been determined who perpetrated this attack – Russian spies or someone else



# Results of no security policy in place

- Sensitive documents are exposed
  - On the network
    - Client to print server and from print server to printer
  - On the print server
    - In the printer memory awaiting print
    - In the printer output tray to other than intended recipient
- Inadequate authentication and record of
  - Who initiated the printing of what, when, how many times
  - Who picked up the document at the printer

*Inconsistent security methods from multiple print vendors across document management systems, servers, and clients weakens overall system security*

In the Press

**The New York Times**

Get Home Delivery

# Business

WORLD

U.S.

N.Y. / REGION

BUSINESS

TECHNOLOGY

SCIENCE

HEALTH

SPORTS

OPINION

MEDIA &amp; ADVERTISING

WORLD BUSINESS

SMALL BUSINESS

YOUR MONEY

DEALBOOK

MARKETS

RESI

## Wall St. Banker Jailed in Trading on 9 Deals

By ERIC DASH

Published: May 4, 2007

Federal authorities arrested an investment banker yesterday and charged him with illegally leaking confidential information on nine deals, including the \$45 billion buyout of the Texas energy giant [TXU](#).

The junior investment banker, Hafiz Muhammad Zubair Naseem, 37, who worked in [REDACTED] energy banking group in Manhattan, is accused of calling an unidentified banker in Pakistan and tipping him about deals shortly before they were publicly announced.

The Pakistani banker, in turn, traded Naseem and himself. He also leaked information to a banker in Pakistan, who also profited. All told, the federal prosecutors said.

The accusations were made in criminal complaints filed last week by the United States attorney's office in New York.

After an inquiry from federal investigators in March, [REDACTED] helped identify Mr. Naseem as someone of interest. Although Mr. Naseem continued to work at the bank, he returned to Pakistan for a visit and did not return until a few days ago.

He is accused of leaking information about pending deals between April 2006 and this February, prosecutors said. He joined [REDACTED] in March 2006 after a stint at [REDACTED]. His desk at [REDACTED] was near a printer that turned out documents with information about potential deals for both his group and for others, investigators said.

# Printing Security in the Press

January 15, 2007, Computer World:

## "The Surprising Security Threat: Your Printers"

The screenshot shows a web browser window displaying the Computer World website. The article title is "The Surprising Security Threat: Your Printers" by Deb Radcliff, dated January 15, 2007. The article text discusses the Blaster worm and the Sasser worm, highlighting the security risks posed by networked printers. A sidebar on the left contains navigation links, and a right sidebar features "MORE RELATED CONTENT" and "TODAY'S TOP STORIES". An Oracle advertisement for Identity Management is also present.

**COMPUTERWORLD Security**

### The Surprising Security Threat: Your Printers

Networked printers — yes, printers — can open your corporate network to malicious attacks. They need security patches, too. By Deb Radcliff

Deb Radcliff Today's Top Stories + or Other Security Stories +

Comments (7) Recommendations: 490 — Recommend this article

**January 15, 2007 (ComputerWorld):** The Blaster worm hit McCormick and Co. hard and fast. It entered the famous spice company through a service provider connection and ripped across plants and offices in a matter of hours. What was most vexing, however, was that the virus kept coming back on disinfected network segments.

Upon further investigation, it turned out that Blaster, as well as some instances of the Sasser worm, were trying to repropagate from infected network printers.

"Printers were just one of several types of systems contributing to the nightmare at the time," says Michael Roszman, who'd just taken over as global director of IT services and information security at McCormick at the time of the worm outbreak in 2003. "Blaster went to all our PCs, our radio frequency units, our handhelds. And, we learned belatedly, it also spread to our printers."

Blaster and Sasser gave IT execs some religion about the vulnerabilities network printers can introduce to corporate networks, Roszman says. Since then, however, there has been little evidence of printer-based attacks spreading across large networks. Corporate IT shops haven't been concerned about printer security. Instead of patching and hardening printers, they have been complacent. Security experts say that printers are loaded with more complex applications than ever, running every vulnerable service imaginable, with little or no risk management or oversight.

If these systems aren't hardened, users may soon find their printers rendered inaccessible by

**ORACLE**  
Oracle Identity Management  
Increase governance;  
decrease risk

**MORE RELATED CONTENT**

- Cisco discloses three router vulnerabilities
- Microsoft jells up security at DC Vista launch
- Google anti-phishing site reveals names, passwords

[Read More +](#)

**TODAY'S TOP STORIES**

- Fla. governor opts for e-voting systems with paper trail
- The Trouble With Vista
- For sale on eBay: Georgia e-voting equipment

[More top stories +](#)

**IDG RELATED CONTENT**

- InfoWorld.com Best of the Week: Jan. 29, 2007 Slide 1
- Vista here opens door to 'shoot hacking' - Network World InfoWorld



# Printing Security in the Press

January 25, 2007, eWeek.com:

"Our Printer Got Hacked?!?!"

The screenshot shows the eWeek website interface. At the top, there are navigation links for 'SUBSCRIBE TO eWEEK', 'My Account / Sign In / Not a member? Join now', and 'eWEEK'. Below this is a 'Solutions Center' banner with the AMD logo and 'ZIFF DAVIS MEDIA' branding. The article title is 'Our Printer Got Hacked?!?!' by Larry Seltzer, dated January 25, 2007. The article text includes the sentence: 'It's one of those "not really a big deal yet but could blow up soon" problems (IP printers, especially higher-end multifunction business printers, have become so intelligent and complicated that they have serious security risks. They are, in fact, really desktop computers, even workstations in disguise.)'. A red circle highlights this sentence, and a red arrow points from a callout bubble to it. The callout bubble contains the text: 'It's one of those "not really a big deal yet but could blow up soon" problems: Printers'. Below the article text, there is an advertisement for anti-virus software and a 'NEW WHITE PAPERS' section.

It's one of those "not really a big deal yet but could blow up soon" problems: Printers

# Printing Security in the Press

January 17, 2007, Computer World Blog:

## "Network printers are a security threat"

www.computerworld.com/blogs/node/4376

t Now: Normal Quick Black and White Text Only Photos (1) Preview

Vista A to Z Computerworld special coverage

COMPUTERWORLD Blogs

IDG

JUMP TO More Resources

SEARCH Google Custom Search GO

- Home
- News
- E-mail Newsletters
- + Shark Bait
- + Knowledge Centers
- Opinion/Blogs
- Columnists
- Blogs
  - IT Blogwatch
  - Business Intelligence
  - Careers
  - Cool Stuff
  - Data Management
  - Development
  - Emerging Technology
  - Government
  - Hardware
  - IT Management
  - Mobile/Wireless
  - Networking
  - Operating Systems
  - Security
  - SMB
  - Software
  - Storage
  - SharkTank
- Webcasts
- Podcasts
- White Papers
- Executive Briefings
- + Zones
- RSS Feeds
- Events
- Print Subscriptions

### Networked printers are a security threat

By C. J. Kelly on Wed, 01/17/2007 - 2:04pm

I want to take a moment to reinforce the major points of this article by Deb Radcliff [The Surprising Security Threat: Your Printers](#). Many years ago when I managed security for a financial firm, the company decided to remove the existing networked printers and replace them with multi-function devices. Multi-function devices can print, staple, collate, copy, scan, and send email. They have hard drives and operating systems. The security department refused to sanction the email capability.

I recall that someone made the decision for the replacement as a "cost saving measure". They dumped all the existing printers, copiers, and fax machines. I remember sticking my little color printer up in a cabinet above my desk, hiding the cable that directly connected to my laptop. I wanted to be able to print confidential schematics and diagrams in color without having to go to the Marketing department to use the only color printer. At the time I thought we could modify the "no printers in user's offices" policy to account for the printing of confidential documents. I wasn't the only one who refused to part with their personal printer and I didn't want confidential documents being stored on the printer hard drive.

Where I am currently employed, we did the same thing. We replaced all the copiers, printers, and fax machines with MFDs. I call these devices MFDs instead of "printer" or "copier" because I am secretly cursing the security issues they present. We recently realized that when documents that are scanned and saved to a network file share are also saved on the system's hard drive. We deal with protected health information every day. I learned that we needed to buy a software package that would enable us to securely wipe the hard drives on a regular schedule. Otherwise, the documents will sit there forever.

The risks that I can tell you are real, as stated in the article are:  
**Risk:** Network printers have more vulnerable services running on them than networked PCs do.  
**Risk:** Network printer applications have a growing number of vulnerabilities.  
**Risk:** Web interfaces, Web servers, Web pages and e-mail are opening printers directly to the World Wide Web.

And at this moment, I don't have any idea what operating system runs on those things. I have to figure out how to patch them. A call to the vendor this week is in

#### ABOUT THIS BLOGGER

C. J. Kelly: C.J. Kelly is a real world Information Security Officer whose identity has been hidden to protect her employer.

[View full profile](#) -  
[Subscribe](#) [XML](#)

**FREE**  
30-DAY TRIAL  
OF SOPHOS ENDPOINT  
SECURITY SOLUTIONS

**SOPHOS**  
secured.

#### BLOG SEARCH

SEARCH  [GO](#)

#### BLOGS WE LIKE

# HP's Approach to Imaging and Printing Security

# Different customers need different security approaches

## Advanced

- Organizations need advanced security capabilities

## Proactive

- Specific hot button issues

## Limited awareness or action

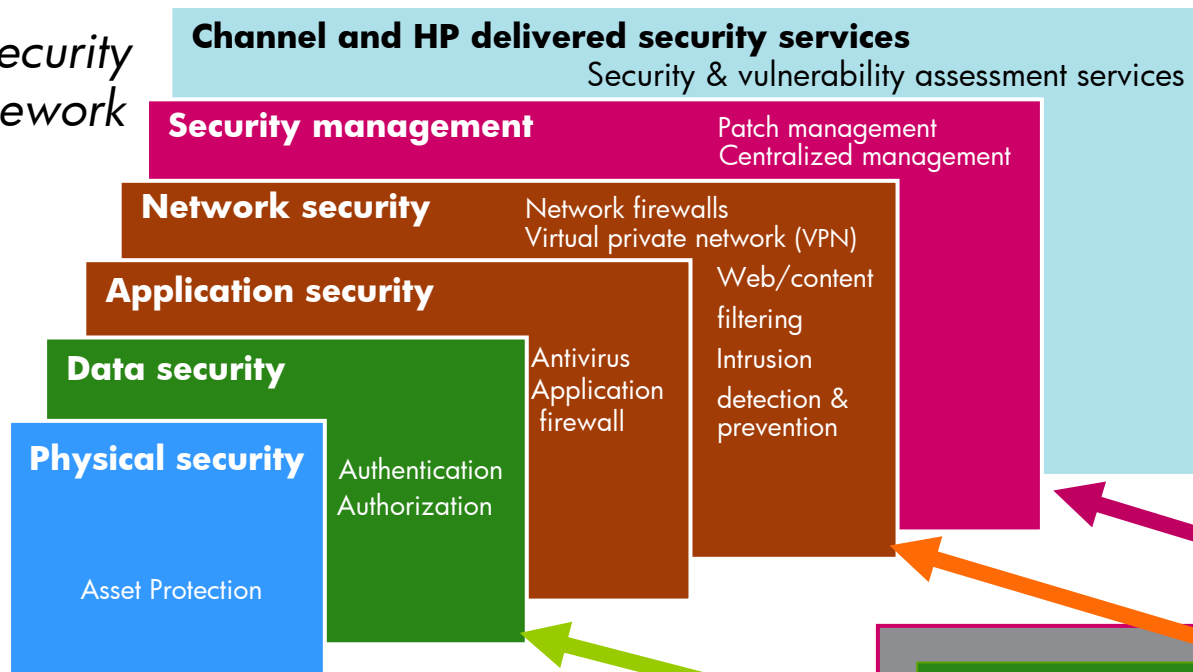
- Make sure that basic security is implemented

**One size does not fit all!**

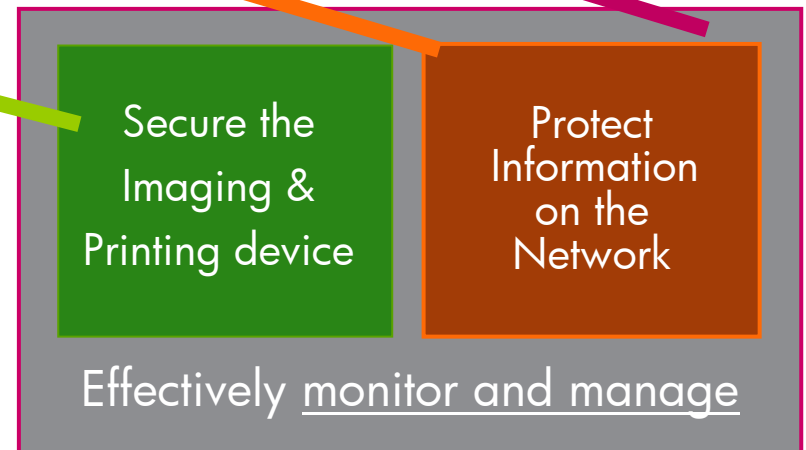


# HP + IPG Security Framework

*HP Security Framework*



*HP Commercial Imaging & printing Security Framework*



# HP's Imaging and Printing Security Framework

Secure the I&P  
device

Protect  
information on  
the network

Effectively monitor & manage

# HP's End to End Security Offerings

## Secure the I&P device

Secure Storage  
Erase

PIN retrieval  
Pull Printing

Passwords  
Protocols  
Secure administration

### User Authentication

- LDAP, secure LDAP
- NTLM, Kerberos
- Swipe cards, proximity cards, smart cards
- Biometrics

## Protect information on the network

### HP Jetdirect

- IPSec
- 802.1X (device auth.)
- SNMPv3
- HTTPS
- Secure IPP support

Fax line  
isolated from LAN

Encryption of  
scan data

Encryption of  
print data

## Effectively monitor & manage

Discovery of un-password  
protected EWS

User Level Tracking and Control

Security Configuration Checklists

Common Criteria Certification Level 3  
Secure File Erase, Secure Storage Erase, and Separation of Fax from LAN

# HP: Leading in Security for Imaging and Printing

- First to implement SNMPv3
- First to ship with IPSec
- First with 802.1X supplicant support
- First with SSL/TLS management
- First with NIST approved security checklist
- First and only printing vendor with IPv6 Consortium Gold approval
- First with CCC certification on Level 3



# HP Printing and Imaging Security

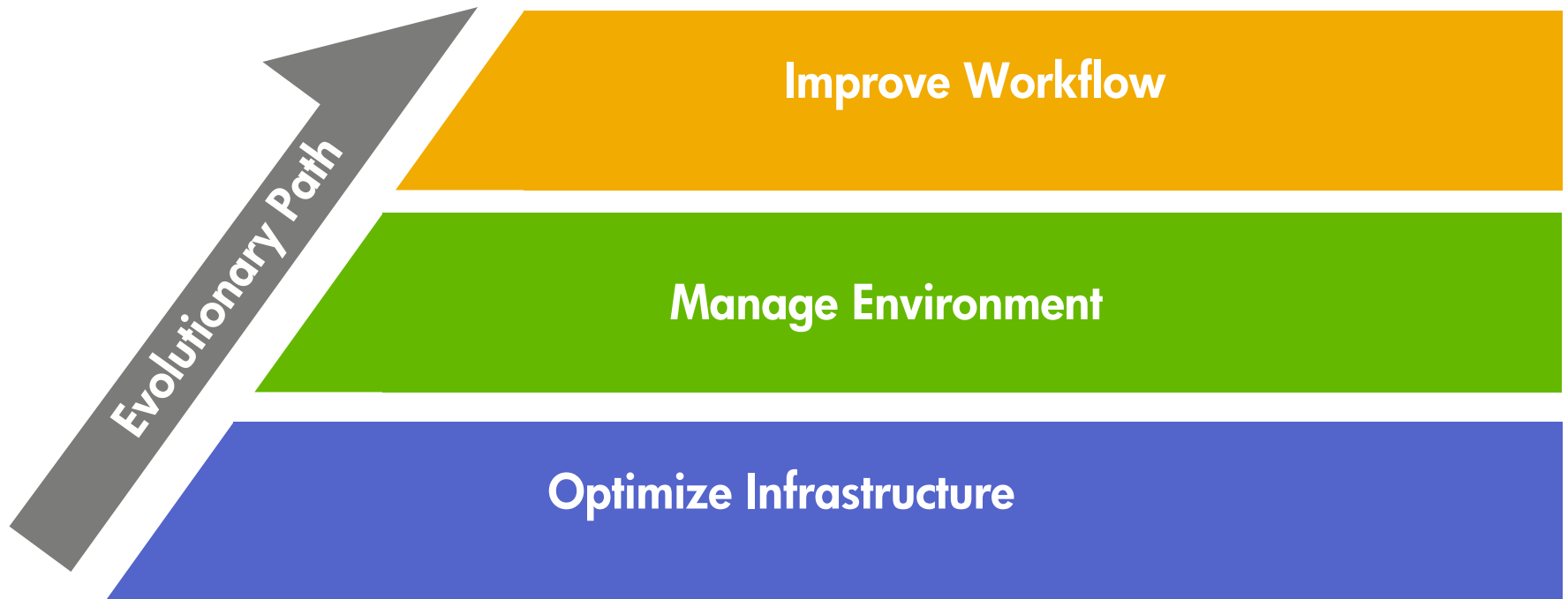
## Common Criteria Certification

Product Name	Status	Conformance Claim
HP LaserJet M3027 MFP, HP LaserJet M3035 MFP, HP LaserJet M5025 MFP, HP LaserJet M5035 MFP, HP LaserJet M4345 MFP, HP Color LaserJet 4730 MFP	Completed June 2007	EAL3
HP LaserJet 9040 MFP, HP LaserJet 9050 MFP, HP LaserJet 4345 MFP, HP Color LaserJet 9500 MFP, HP LaserJet CM4730 MFP	Pending Feb 2008	EAL3

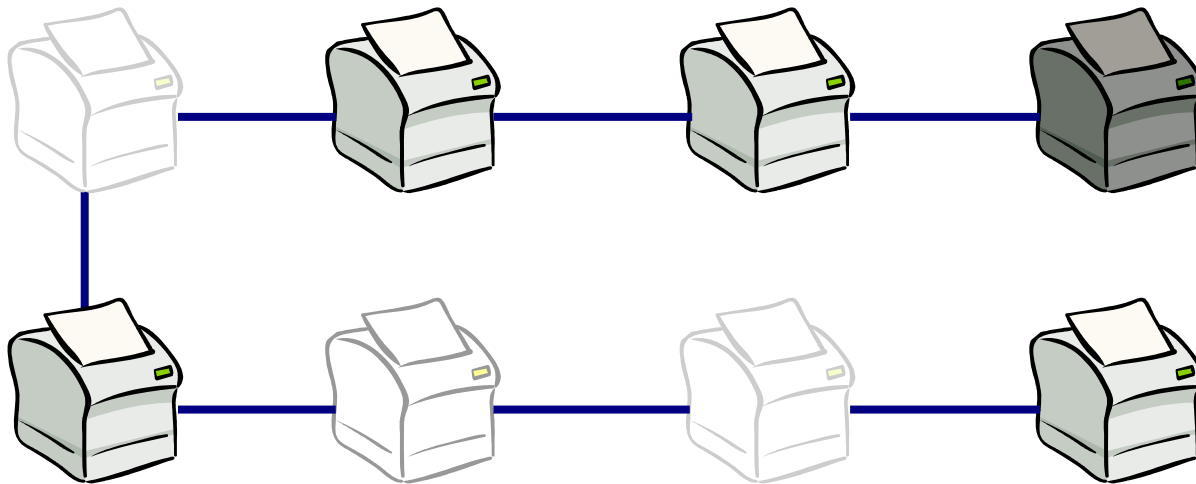
- National Information Assurance Partnership (NIAP) – Common Criteria Certification (CCC)
  - Fax/Network Isolation and Disk Overwrite
  - <http://www.niap-ccevs.org/cc-scheme/vpl/>

# Securing your Imaging and Printing Environment

# Security Implementation Plan

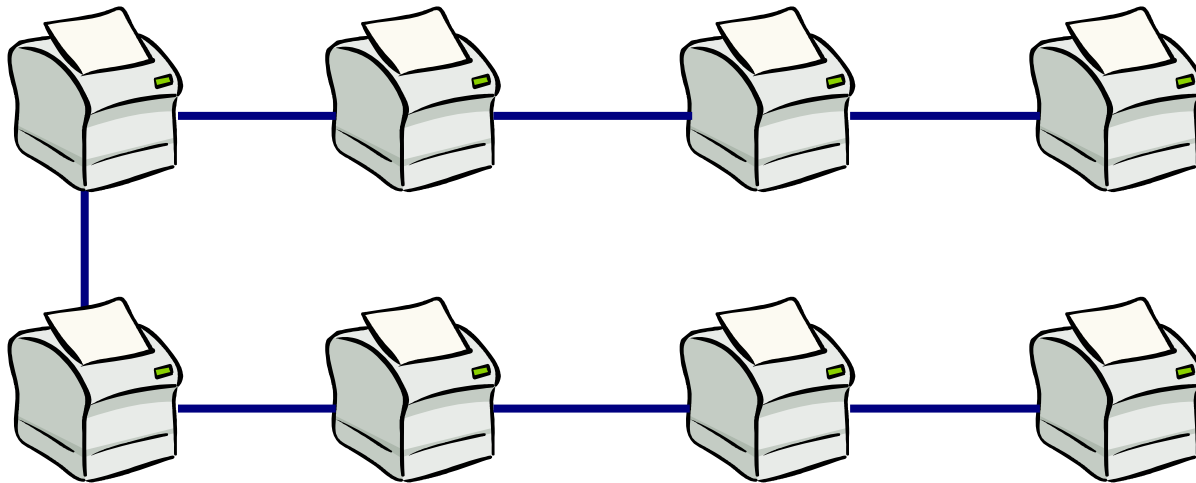


# Steps to Secure the Printing Environment



# Step 1: Get in Control of the Device Fleet

Through HP Web JetAdmin



# Step 1: Get in Control of the Device Fleet

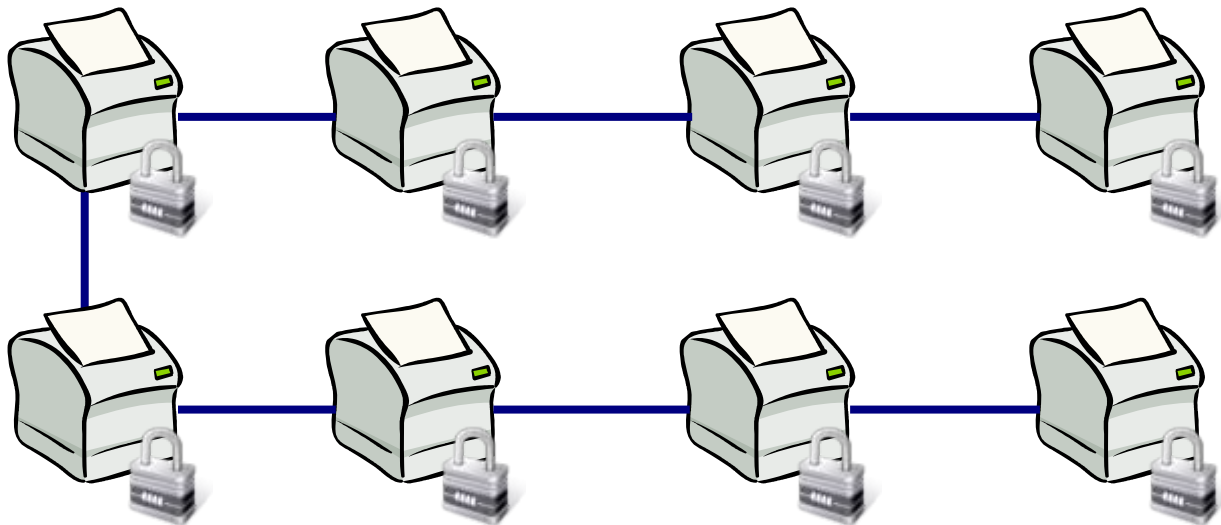
Use HP/Web Jetadmin to:

1. Identify how many printers are networked and direct connected
2. Identify types/models of printers
3. Standardize configurations based on model, capabilities, etc.
4. Bring printers and jetdirect cards up to latest firmware revisions
5. Manage printer status on an as needed basis
6. Create groups based on lines of business, types of printers or location
7. Develop security and profile models



# Step 2: Secure Devices

Through certified checklist (e.g. U.S. National Institute of Standards and Technology)



# Step 2: Secure Devices

Use the NIST check list to define policy that covers settings for:

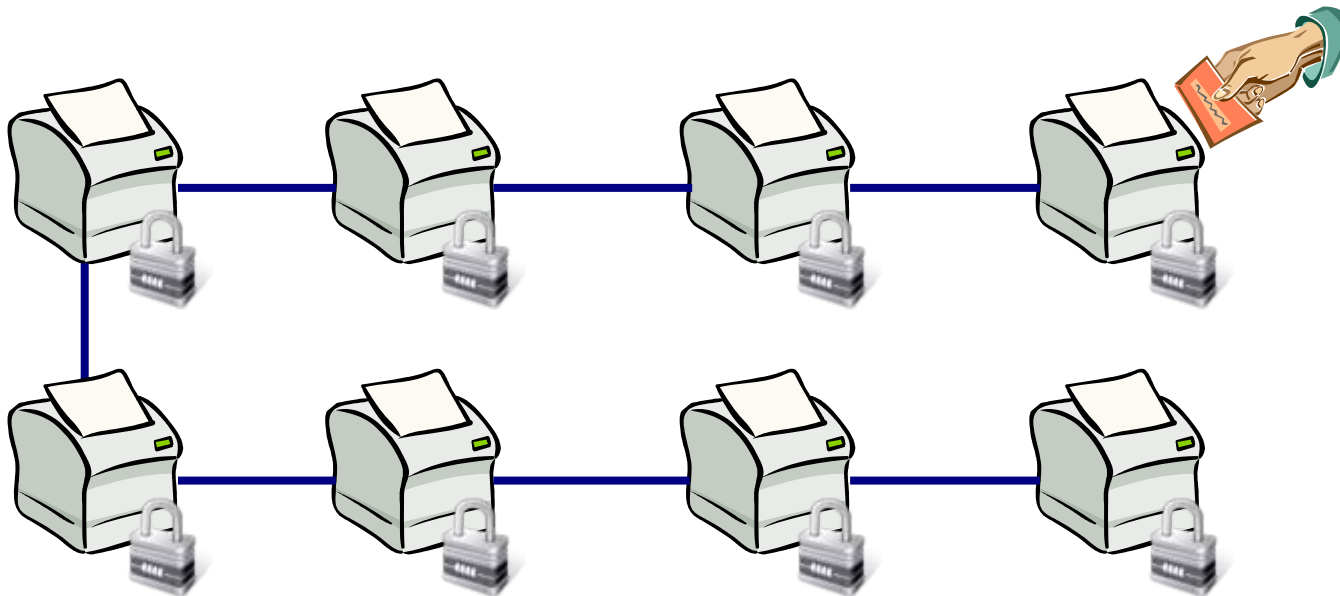
- Device passwords
- Secure admin data exchange
- PJJL commands
- Secure erase options
- Digital sending options
- Job Retention timeout
- Network Access
- Protocols stacks
- Additional device functions (e.g. job cancel button)





# Step 3: Implement Authentication

The most convenient for every MFP function



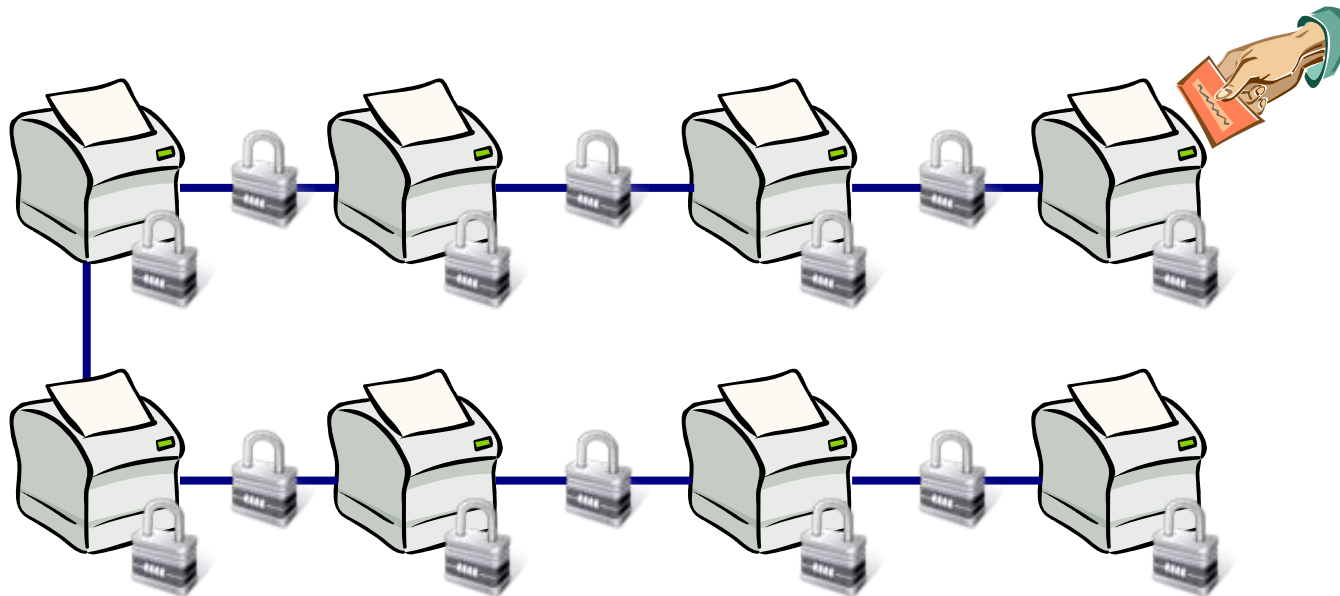
# Step 3: Implement Authentication

- Avoids access to confidential printouts
- Typical authentication methods
  - Group PIN
  - User PIN
  - Magnetic card
  - Proximity badge
  - Smart Card / USB key (PIN + certificate)
  - Biometrics
  - any combination (AND/OR)
- Authentication can be configured for Print, Fax, Copy, Digital Send



# Step 4: Implement Encryption

Complete / Partial



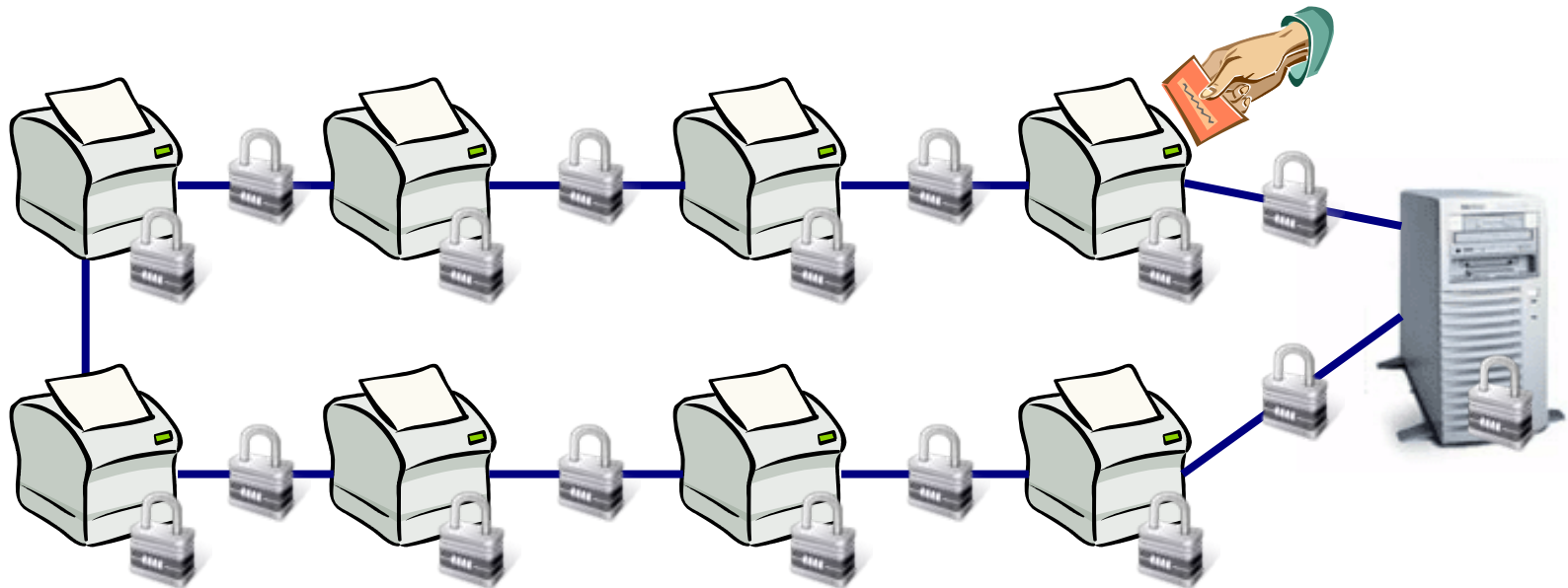
# Step 4: Implement Encryption

- Needs are different depending on scope
  - Integrate printers into overall IPsec strategy
  - Implement separately for printing
    - All / some users
    - All / some devices



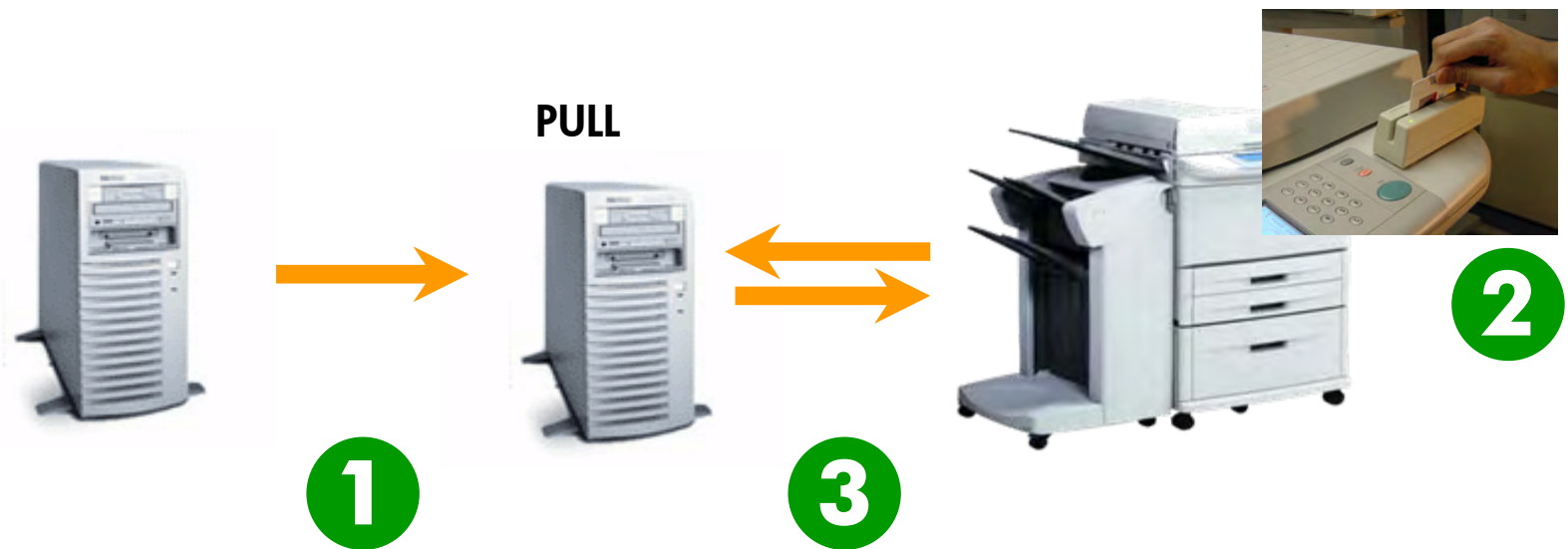
# Step 5: Implement Pull Printing

No more documents in the output trays



# Step 5: Implement Pull Printing (1)

1. Send print job to generic queue on the server
2. Authenticate at any device
3. Pull print job from server

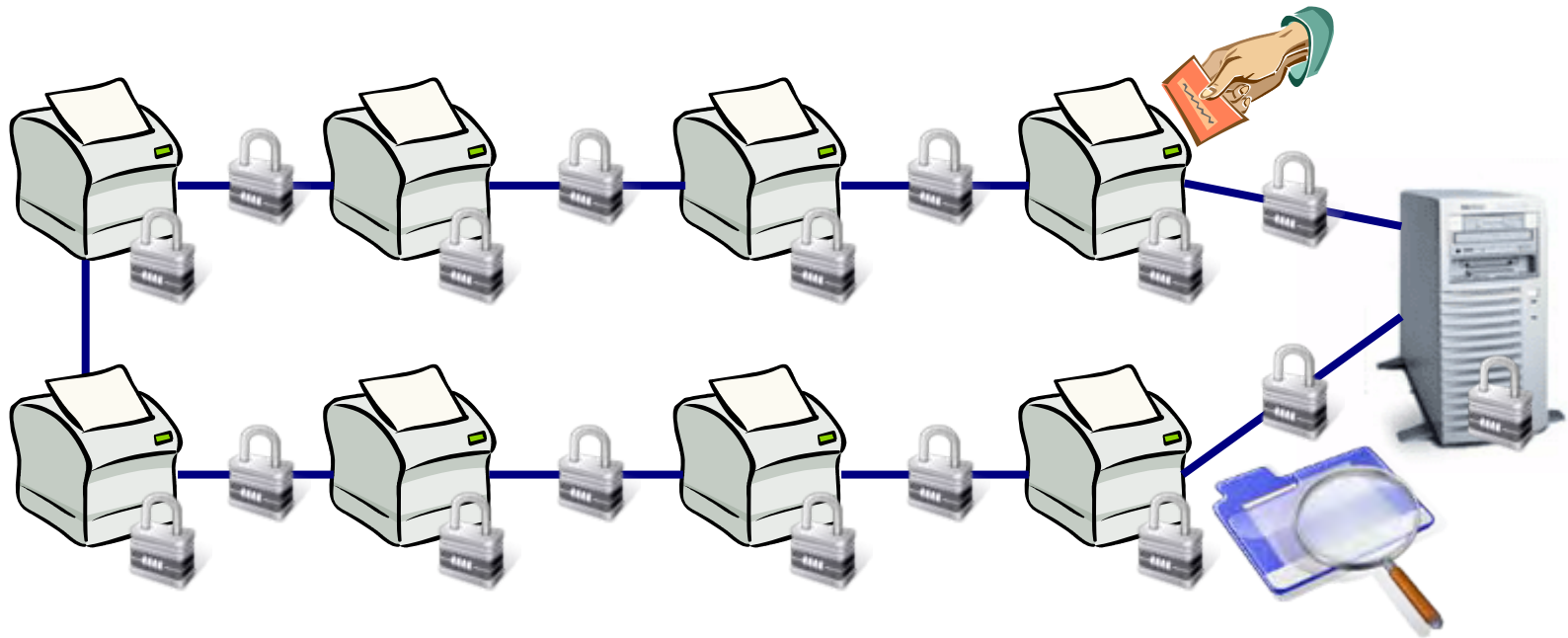


# Step 5: Implement Pull Printing (2)

- To print confidential documents
- To support an Optimized Infrastructure strategy
- For travelling users – to find and access printers
- For travelling users – to get printouts forwarded
- When printers are out of service
- When printers are exchanged

# Step 6: Implement Job Level Tracking

Tracking abuse & avoiding misuse





# Step 6: Job Level Tracking

- Tracking of print/fax/copy/scan jobs
  - Collect and archive job information per function (print, copy, fax, scan)
  - Eventually archive the whole document
  - Be consistent with general email policy
- Additional benefit:  
Cost allocation and bill back to departments



# Summary

- Security is everyone's concern
- Your technical solutions are only as strong as the policies they support and the procedures built around them
- To successfully implement security strategies you need to get management to drive them, IT and HR to implement them and staff to understand and respect them.
- Security is a value add and a business enabler
- **Imaging and Printing Security must be part of the overall IT security strategy!**


# [www.hp.com/go/secureprinting](http://www.hp.com/go/secureprinting)

United States-English

» HP Home » Products & Services » Support & Drivers » Solutions » How to Buy

» Contact HP Search:

Printing and imaging  All of HP United States



## Secure imaging and printing

Solutions for user authentication, data integrity, secure document printing


» Large Enterprise Business

- » Products
- » Business & IT services
- » Solutions
- » Technologies
- » Partners
- » Support & Drivers
- » Business Technology
- » Media Center & Library

» Printing & imaging

- » **Secure printing**
- » Featured offers
- » Events
- » Success stories
- » White papers
- » News

» Trade in your old HP Jetdirect for the new HP Jetdirect 635n IPv6/IPsec print server network card



**Protect data**  
Manage risk and workflow between users, administrators and devices.

**Eliminate internal and external threats to your equipment and data with HP's imaging and printing security framework.**

HP provides a wide array of secure printing and imaging solutions for HP LaserJet printers and HP MFPs to help you simply and easily elevate the status of these devices to active components of your overall security plan. We use security standards and recommended protocols to help safeguard your business with capabilities that better **secure your devices, protect critical information on the network**, and simplify the way you **monitor and maintain** your printing and imaging environment.

HP devices support a wide range of industry standard security protocols, as well as class-differentiating functions and solutions allowing for secure management, device integrity, privacy and access control.

- HP devices have the ability to address security needs of specific industries, such as **Healthcare, Financial Services and Government**.
- IP security available through JetDirect allows for strong authentication, confidentiality and integrity of communications, and can secure network printing and scanning protocols.
- HP is the first printer vendor with a security checklist approved by the **National Institute of Standards and Technology (NIST)**.

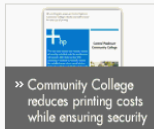
» Support & Troubleshooting

» Software & Driver Downloads

» More printing & imaging support

**Contact HP**

» Call, email or chat. It's easy.



» Community College reduces printing costs while ensuring security

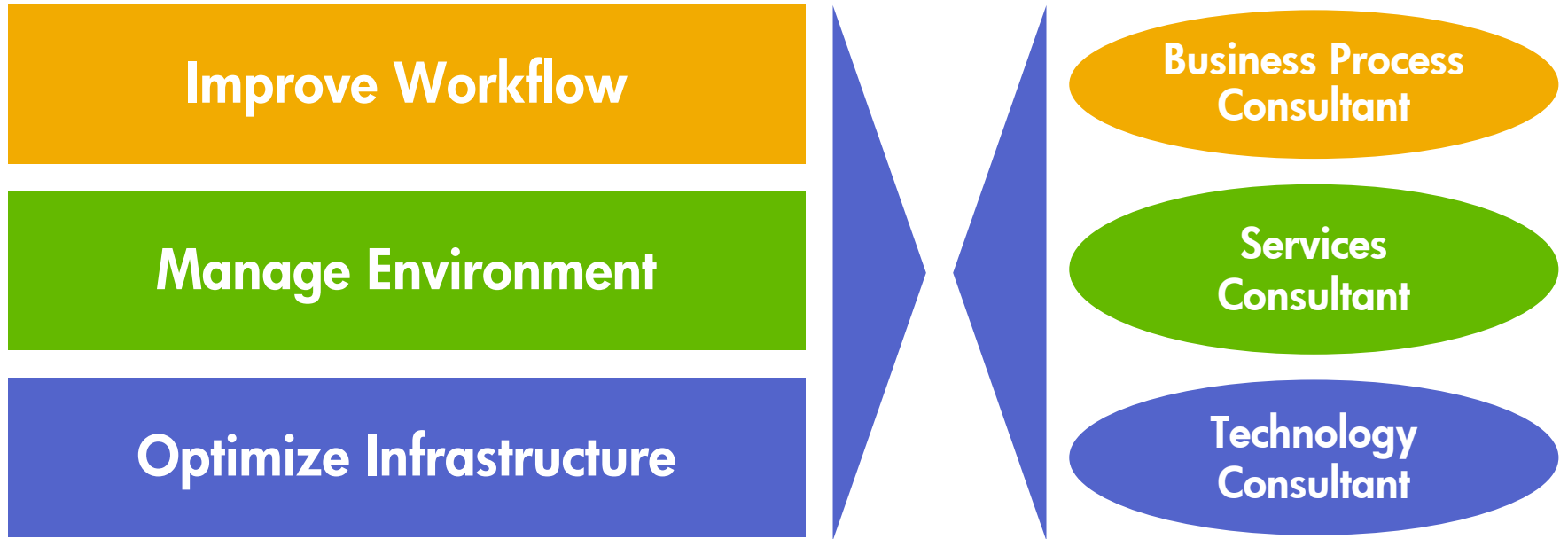
**Spotlight**  
On-demand webinars for secure printing.

- » Secure Devices
- » Protect the Network
- » Monitor and Manage

**Printable resources**

- » White Paper - Key Data and Privacy Regulations for Businesses (288KB, PDF) **NEW!**
- » White Paper - Practical

# We're here to help




Engage your Account Manager to get started

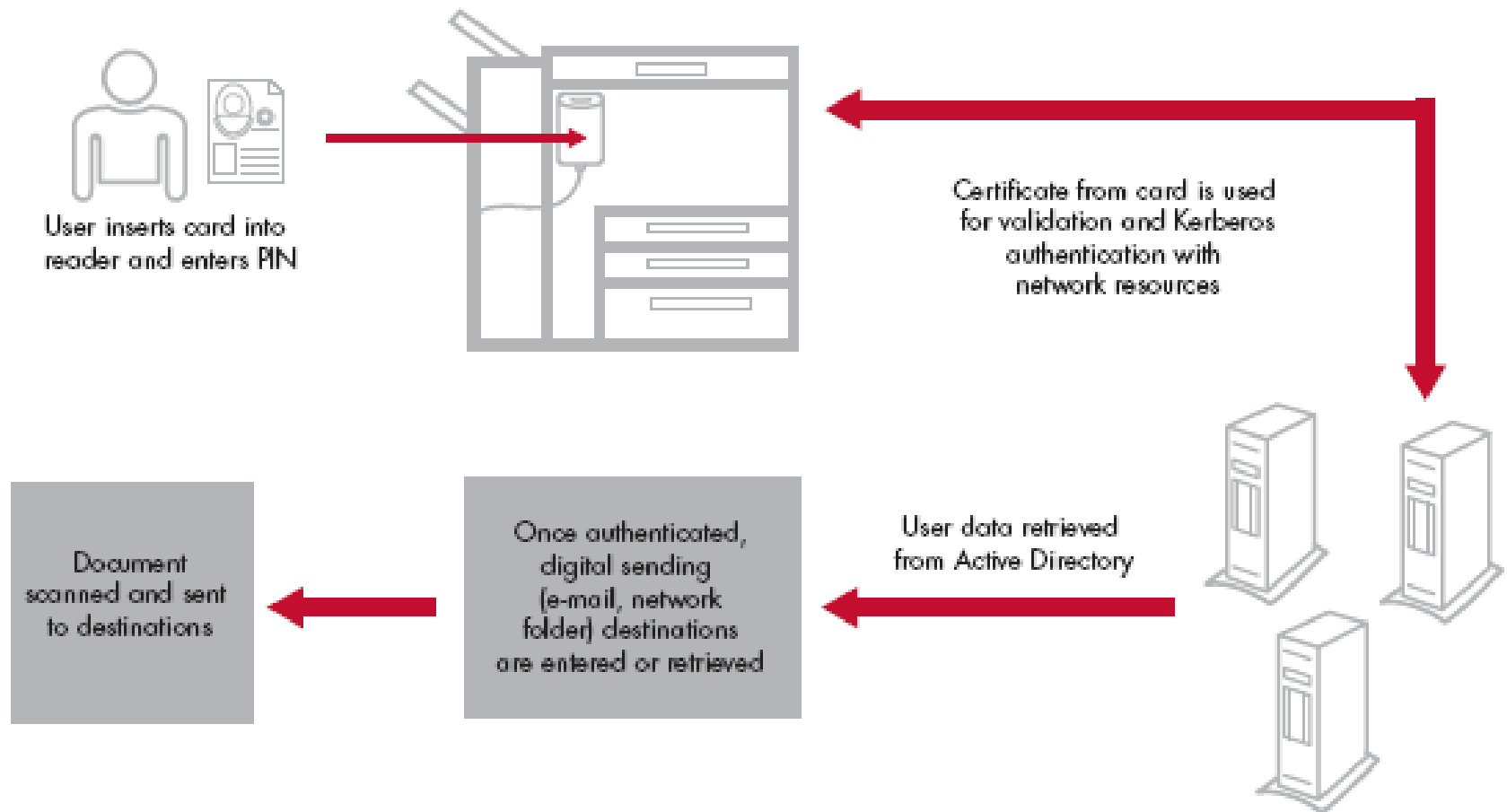
# Identity Authorization

# HP Imaging and Printing Security

## HP Common Access Card (CAC) for MFP

- HP CAC for MFP solution launched in Summer 2007 
- Components
  - HP CAC firmware and authentication agent
  - HP CAC reader
- Feature and infrastructure support
  - CAC Authentication, send to folder, and send to email (signed)
  - Active Directory, Kerberos, OCSP, and CRL infrastructure
- Product support
  - HP LaserJet M4345, M3035, M5035 MFP
  - HP LaserJet CM4730 MFP, HP Digital Sender 9250C
  - HP Edgeline in Spring 2008

# Smartcard Process Flow



WHAT DO YOU HAVE TO SAY?

