White Paper

ELATEC
RFID Systems

SECURE PRINTING IN THE IoT ERA

RFID SOLUTIONS FOR PRINT MANAGEMENT AND SECURITY

RFID SOLUTIONS FOR PRINT MANAGEMENT AND SECURITY

Networked multifunction printers (MFPs) offer unparalleled productivity and convenience, allowing users to print and fax from a desk across the hall or a workstation across the country. Sophisticated managed print service (MPS) software also enables better tracking and cost control.

But convenience and functionality can come with a hidden price. Today's networked printers are part of an expanding business ecosystem of "Internet of Things" (IoT) devices. As an IoT endpoint, MFPs have security vulnerabilities that can create costly headaches for businesses.

Why Print Security Matters

Information security is more important than ever. Companies need to protect sensitive intellectual property (IP), financials, customer data and personnel data. Stronger data privacy regulations, such as the European Union's General Data Protection Regulation (GDPR), leave businesses vulnerable to fines and lawsuits if certain kinds of data are exposed. Companies in some industries, such as the healthcare industry, may have additional information security requirements.

In addition to putting data at risk, unsecured printers often create cost control problems. Printer output picked up by the wrong person leads to waste if the original user has to resend the job. And without proper controls in place, individuals and departments may not consider costs and material use when making printing decisions. A print management system can track costs by user and department and designate who is allowed to print, how much they can print, and what types of documents (e.g., color vs. black-and-white) they can print.

Most companies have taken steps to secure electronic data. In this environment, printers may be the weakest link. Printers are usually located in easily accessible areas and designed for convenience rather than security. MFPs can expose data in several ways.

- Completed print jobs may be intentionally or accidentally intercepted by the wrong person while they are sitting in the printer tray.
- The print queue may be hacked, allowing an unauthorized user to complete and pick up a print job.
- A networked printer may be hacked to print unauthorized jobs from outside of the network or to send jobs from the printer to an outside recipient. (For example: in 2016, a hacker was able to print out anti-Semitic propaganda from multiple networked printers at more than a dozen universities.)
- The hard drive itself may be stolen or hacked to recover information about upcoming print jobs stored in printer memory.

Of these threats, the first is by far the most common. According to an industry survey, 59% of companies reported a print-related data loss in 2018, with most of those losses involving accidental or intentional actions of internal users . With more than 90% of businesses still reporting that they rely heavily on paper for daily operations, print security must be taken every bit as seriously as digital information security.

[1] Quocirca (2019) Global Print Security Landscape, 2019.

USER AUTHENTICATION & ACCESS CONTROL FOR SECURE PRINTING

Companies must take steps to secure access to the physical hard drive on the printer and to the network that the printer is connected to. In addition, companies should put security systems in place to prevent unauthorized people from gaining access to printer functions or to materials that have been sent to the printer by another user.

Pull printing is a system that delays printing until an authorized user is physically present at the printer. Users can send materials to the print queue at any time from their workstations, but the documents will not start printing until they release the job at the printer itself. This may be accomplished by:

- Entering a user ID and password or PIN on the printer user interface.
- Using a physical card or token that is presented to or scanned by a reader connected to the printer. These may be based on optical, magnetic (magstripe), radio frequency identification (RFID), or emerging smartphone-based technologies such as Bluetooth Low Energy (BLE) or Near-Field Communication (NFC).
- Biometric identification, such as fingerprint or facial recognition.

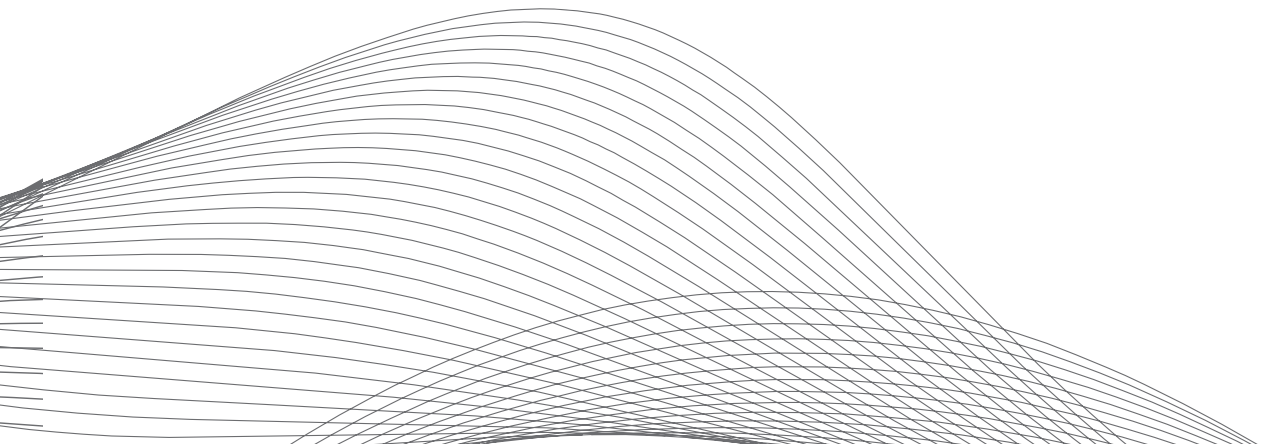
These security systems must do two things. First, they must be able to accurately identify the individual user who has requested access to the printer (user authentication). Second, they must ensure that only people with the right authorization level are able to access printer functions (access control).

User authentication is the ability to correctly identify an individual user and match their information to the device, equipment or systems they are using.

Access control is the ability to ensure that only authorized users are able to gain access to a device, asset or system.

For print management, user identification and access control must be reliable, cost-effective for deployment on dozens or hundreds of individual print devices, fast and simple for end users, and easy for IT departments to manage. Biometric identification is generally too complex, expensive and unreliable, and puts companies in the position of having to manage sensitive personal data for their users. Password and PIN systems have been widely used for print management but have drawbacks of their own. Employees often share or forget printer passwords and PINs, reducing security and creating IT headaches. Printer user interfaces can also be unwieldy, slowing employees down as they enter their user ID and password multiple times each day.

The best solution for secure printing may be one that most corporate employees already have in their pockets: an ID card or badge with Radio-Frequency Identification (RFID).



USING RFID FOR PRINT SECURITY

RFID cards are widely used for employee identification and building access control across all industries. In most large companies today, employees are issued a card on their first day that they use to get in the front door and wear or carry with them while on the job. The ID cards improve building security by ensuring that only current employees can enter and provide a visual confirmation of employment status. These same cards can be leveraged to enable access and authenticate users for secure printing.

RFID has a number of benefits for printer manufacturers, MPS software providers and the end-user customers they serve.

+ It leverages a technology most corporations are already using (RFID-enabled employee ID cards), simplifying adoption and rollout of new applications for end users.
+ RFID technologies are more secure and easier to manage than password/PIN systems and harder to counterfeit than competing magstripe or optical reader technologies.
+ RFID readers can be easily integrated with MFPs as well as other business IT systems and devices, allowing employees to use a single card for access to all of the systems they need.
+ RFID enables rapid, contactless user identification and access control, speeding up workflows and reducing hygiene concerns presented by touch-screen applications on shared printers.
+ RFID cards provide a unique identification that can be used to match users with systems or devices. RFID systems not only prevent access by unauthorized users but enable tracking of exactly who has accessed a printer, when, and what they did. In addition to improving security, RFID combined with MPS software enables better cost accounting and control.

+ RFID cards provide a unique identification that can be used to match users with systems or devices. RFID systems not only prevent access by unauthorized users but enable tracking of exactly who has accessed a printer, when, and what they did. In addition to improving security, RFID combined with MPS software enables better cost accounting and control.

HOW RFID WORKS

RFID cards have two main components:

+ an integrated circuit that can store and process information
+ an antenna to transmit or receive a signal

Each RFID card stores a unique data set—such as a number—that serves to identify the card and, by extension, the person carrying it. When a card with an embedded RFID tag is in close proximity with an RFID reader, the reader transmits a radio signal to interrogate the tag. The radio signal activates the tag, which then uses the power in the radio signal to respond to the reader with its unique ID.

Although the use of unique identifiers is common, more sophisticated cards utilize more complex data structures for identification and authentication, including encryption and digital signing functions.

CREATING A SECURE PRINT ENVIRONMENT WITH RFID

RFID cards are generally more secure than other access control measures. Employees are less likely to share a picture ID card than a password or PIN, and cards can be quickly deactivated from a central system if they are lost or compromised or if an employee is terminated. They can also utilize cryptographic keys to further increase security.

Security solutions for RFID must ensure that:

- The cards themselves cannot be easily cloned or tampered with to allow someone to impersonate another user or change their level of access.
- Signals exchanged between the RFID card and reader cannot be intercepted and read.
- The RFID reader cannot be compromised to unlock print functions in the absence of a card with proper authorization.

The simplest RFID cards store a unique identification number in an unencrypted format. This number identifies the cardholder and tells the reader whether or not they have permission to access the protected asset. These unencrypted RFID cards can be easily read and cloned. Unencrypted signals between the card and reader can also be intercepted and used to create a cloned card or otherwise signal the reader to unlock access to the asset.

Encryption substantially increases the security of RFID technologies for print management. With encryption, the identification number stored on the RFID card is masked using a complex encryption algorithm. The only way to unlock the information and read the number is to have the correct electronic "key." Because some information is stored on the card and some on the reader itself, it is impossible to decrypt the information on the card or in the signal that passes between the card and the reader. Without the right key, the card cannot be cloned or altered to change permissions.

SOLUTION: SECURE PRINTING WITH ELATEC

ELATEC readers support advanced encryption technologies. The readers act as mini computers that can be programmed to meet nearly any encryption scheme, including advanced cryptographic methods requiring a higher computing load. These may include the use of multiple or hierarchical keys and symmetrical cryptographic methods. ELATEC readers can also facilitate multi-factor authentication with the help of Secure Access Modules (SAM). The readers support multiple SAM slots that help in integrating these modules. This enables the readers to perform cryptographic computations using SAM as well as facilitate key management in a secure way. Customized encryption schemes can be programmed in advance by ELATEC. For even higher security, printer manufacturers or MPS software providers can program the readers themselves, so even ELATEC will not possess the encryption key.

SELECTING THE RIGHT RFID READER FOR SECURE PRINTING

There are many different RFID reader technologies to choose from. Printer manufacturers and MPS software providers wishing to integrate RFID into their secure printing solutions need to understand the differences and select a reader technology that meets the needs of their clients and end users. In particular, developers should ask:

- Will the reader work with the card technologies already in use by clients and end users?
- Does the reader support the functionality and security requirements needed by my application?
- How easily can the reader be reconfigured or updated as end user requirements or market conditions change?

Challenge: A Highly Diverse RFID Market

There are dozens of RFID card transponder technologies in use around the world, each with their own data formats, communication frequencies and security capabilities. Cards can be broadly separated into high frequency (HF) and low frequency (LF), depending on the radio frequency band range they use to communicate. However, within these categories, cards by different manufacturers have their own unique formats.

Printer manufacturers and software developers intending to sell to a diverse market may need to be able to accommodate 60 or more unique card technologies. End users often do not know what kind of card technology they are using and may have little choice in the matter; if companies lease building space, they generally must use the card technology put in place by the building owner. Fortune 500 companies with multiple locations, or that have expanded through mergers and acquisitions, may end up with multiple card technologies used within a single network. Most organizations are not willing or able to change their existing ID card technology to accommodate user authentication and access control for print management, and do not want to make employees carry multiple cards.

Most RFID readers can only read a few different card technologies, and some are created by card manufacturers to read only their own technologies. This means that manufacturers wishing to expand their market opportunities may have to stock different readers for different customers. This creates both sales and inventory management challenges. Salespeople must discover the card types being used by prospects before placing an order to determine which part to use or whether their card technology can be accommodated at all. For large companies using more than one card technology, there may not be a single reader in inventory that can read all of their card types. Printer manufacturers and MPS developers intending to sell internationally or to multinational customers face additional challenges, since most RFID readers are only certified for use in a few countries or regions.

SOLUTION: ELATEC UNIVERSAL RFID READERS

ELATEC RFID readers are "universal"; some can read more than 60 card technologies, including HF and LF RFID as well Near Field Communication (NFC) and Bluetooth Low Energy (BLE) technologies increasingly used with mobile devices. They are also certified for use in as many as 110 countries. This means they can accommodate virtually any card technology an end user may have in place, providing a single part number solution that simplifies sales and inventory management. Sales or customer support staff can simply scan an example card from the end user to identify the technologies they are using. Final configuration can be completed on installed readers, so MFP manufacturers can usually stock one version of their system for all potential customers.

Challenge: Widely Dispersed Devices or Systems

A large company may have dozens or hundreds of printers distributed throughout their organization. This makes it extremely difficult to update or reconfigure the RFID readers and ensure that none of them have been missed.

There are several reasons why RFID readers may need to be updated or reconfigured. End users may adopt a new card technology. Emerging security threats may require manufacturers to enable advanced encryption or other security features for identity management. Or software developers may want to add new functionality to their print management solutions.

Field reconfiguration of most RFID readers is time-consuming and expensive. Technicians must physically access each reader, in some cases removing it from the printer in which it has been installed. If the installed reader cannot be configured to meet the new requirements, it must be removed and replaced. For IT managers, this means that every single RFID-enabled printer throughout the building or campus must be tracked down and updated. Missing a reader may result in an unexpected device failure. Printer manufacturers may also face significant expenses if they have unsold inventory in stock that must be replaced or reconfigured.

Changing Market Requirements

The business ecosystem has become increasingly sophisticated and complex with the growth of networked IT solutions and the proliferation of connected printers and other IoT devices. Businesses want to be able to take advantage of the benefits of networked systems and devices while maintaining privacy, confidentiality and security. Some companies are also moving towards emerging identification systems enabled by Bluetooth Low Energy (BLE) or Near Field Communications (NFC) through smartphones or other mobile devices. RFID readers will need to adapt to support these evolving functionality requirements.

SOLUTION: REMOTE CONFIGURATION WITH ELATEC READERS

ELATEC readers support remote configuration for fast, easy updates. Manufacturers or end-user IT managers can push updates out to all installed readers at once without tracking down individual printers or requiring extensive technician time and expense. This increases customer satisfaction and provides a significant competitive advantage for printer manufacturers and MPS providers.

Most readers are limited in both their current functionality and potential upgradability. Printer manufacturers and software developers may find themselves "locked-in" to current functionality and security capabilities around user identification, authorization and access control by their RFID reader solution. Addressing emerging market opportunities, in this case, would require physically replacing the RFID readers in their systems. This limits the shelf life of their products and their ability to respond to customer needs.

SOLUTION: ELATEC READERS ARE "FUTURE PROOF"

ELATEC readers have a robust open API that makes them highly adaptable and practically "future proof." The readers can be programmed to enable unique functionality for sophisticated IT solutions and support mobile access control technologies such as BLE and NFC. The API is powerful and flexible, so manufacturers will be able to reconfigure their existing readers to address new opportunities and requirements in the future that have not yet been imagined. This vastly increases the shelf life of both installed systems and inventory. And since they can be easily reconfigured after installation, manufacturers will be able to respond to new customer requirements and maintain customer loyalty.

THE ELATEC ADVANTAGE FOR SECURE PRINTING

ELATEC's powerful, flexible reader technology gives printer manufacturers and MPS providers a real competitive advantage, both now and in the future. ELATEC can help companies creating secure printing solutions:

+ **Expand internationally:** ELATEC readers are certified for sale in as many as 110 countries globally.
+ **Maximize market opportunities:** ELATEC readers support nearly every card technology available, including both HF and LF, as well as emerging smartphone mobile access control solutions via BLE and NFC.
+ **Reduce total lifecycle costs:** ELATEC readers simplify inventory management with a virtual single part number solution and can be easily and remotely updated or reconfigured without replacing inventory.
+ **Deliver customer advantage:** ELATEC readers reduce configuration expenses, extend product life, and support advanced functionality and security requirements, providing meaningful product differentiation for printer manufacturers and software developers.
+ **Prepare for the future:** With ELATEC, you'll be ready for whatever comes next. Our readers can be reconfigured to address emerging opportunities and customer requirements.

CASE STUDY: REMOTE FIELD UPDATES OVER PRINTER NETWORKS

An international multifunction Printer (MFP) manufacturer needed a solution that would enable rapid reconfiguration of RFID readers in their devices to meet emerging security and functionality demands. Most card readers must be physically removed from the printer and connected to a computer to update firmware using a configuration tool. This was costly and time consuming for end users, resulting in increased IT expenses and lost operational time. ELATEC worked with the manufacturer to develop the Remote Firmware Update Tool. This tool allows the manufacturer to send updates to their customers' IT centers, where they can be distributed remotely to all printers on the network. The Remote Firmware Update Tool allowed them to meet the demands of one of their largest customers and increase satisfaction and brand loyalty for all of their clients.

elatec.com

EMEA
Puchheim, Germany
+49 89 552 9961 0
sales-rfid@elatec.com

AMERICAS
Palm City, Florida, USA
+1 772 210 2263
americas-info@elatec.com

ASIA
Shenzhen, China
+86 158 1759 1668
apac-info@elatec.com

AUSTRALIA
Sydney, Australia
+61 449 692 277
apac-info@elatec.com

JAPAN
Tokyo, Japan
+81 355 799 276
japan-info@elatec.com