WHITE PAPER

Implementing Secure Print

What is a Trusted Identity?

A trusted identity is a validated ID that uses a biometric or a credential provisioned onto a card, mobile or a wearable device. In a Connected Workplace, one trusted identity can be used to access multiple systems like building access, time and attendance, and secure print.

How to Leverage Your Existing Trusted Identity Credentials for Easier, Safer Printing

A More Secure and Simpler Printer Experience

Once a sensitive document is printed, it can very easily fall into the wrong hands, posing a huge—and often overlooked—security risk. In fact, 70% of organizations have suffered a print-related data breach. Many also struggle with complicated tracking allocation and errors when users aren't correctly identified. In addition, many common "secure" printing methods are either far too cumbersome for users or far too susceptible to breaches. For example:

- Pin pads offer the convenience of nothing to carry, but require the user to actually remember their code—and not divulge it to anyone else
- Passwords are frequently lost, forgotten or shared, requiring an organization's IT department to constantly update, change or retrieve them
- QR codes are astonishingly easy to copy and clone, creating a false sense of security

An effective way to address these concerns is to employ the identification credentials already in use to power secure printing programs. Adding secure printing to existing trusted identity credentials like badges, mobile devices, and biometrics not only improves security but offers a more user-friendly experience—and is fairly simple to implement with the help of an experienced printer manufacturer or managed printing partner. This white paper helps organizations begin exploring the world of secure print by breaking down its two most vital components: credentials and readers. After reading, you'll understand the basics of secure print and how it can work within your current trusted identity management solution.

Safer, Greener & Leaner: Secure Print

Without secure print, documents are sent to the printer and released immediately. This works just fine if the user immediately retrieves the printout, but that requires the user to be at the printer the moment it is released (for example, when the printer is right next to the user's computer). Since it's not feasible for every user to have their own printer, however, most jobs are printed to a central printer some distance from the user.

This scenario is common in healthcare, where doctors treat patients in exam rooms, enter the patient's information into a laptop and print to a central office printer. The patient's private information then sits on the printer until retrieved by office personnel—or anyone else nearby.

Privacy isn't the only thing receiving increased attention; green certification and a reputation for environmental friendliness are increasingly attractive to consumers.

With secure print using a trusted identity, the document is not immediately released for print. Instead, it is not printed until the doctor or authorized user authenticates their identity at the printer using the same card, device or biometric that they use for other access control systems (like building entry or parking permission). The doctor and patient—as well as HIPPA auditors—know that this confidential information can only be accessed with permission. Businesses in all industries can benefit from this level of privacy, especially with new, more stringent regulations like GDPR and the growing emphasis placed on locked down business systems.

Of course, privacy isn't the only thing receiving increased attention; green certification and a reputation for environmental friendliness are increasingly attractive to consumers. Triple bottom line companies are eager to add sustainability initiatives, but even those without expressed green philosophies have an interest in saving money. Secure print can help. An estimated 20% of print jobs are never retrieved by the original user, resulting not only in significant financial and environmental waste day after day, but also unnecessarily complicating and over-inflating departmental cost allocations. With secure print, documents remain in the print server queue until they are released—reducing unnecessary expenses while saving the planet.

All secure printing methods are not, however, the same. Building the right program involves understanding your systems and needs, as well as bringing in allies at the beginning of the project. After all, it's neither green nor fiscally responsible to build a system only to tear it down and replace it with a new one. To ensure success, IT managers should consider the following:

Understand Your Current Credentials

Begin by asking: what authentication mechanism would your organization like to use for secure printing? Most prefer to work with their existing access control credentials, which allow them to build on their current systems rather than start from scratch. Unless, of course, your current system is out of date and an upgrade is in order. Consider how you'd like your users to experience secure print now and in the future.

If you're using cards/badges:

Cards are the most common credential type to extend to secure print. There are plenty of new technologies in use today, and in the future cards may become less dominant, but they will still be around for a long while. Your card type, needs and brand will determine the readers your printer manufacturer will supply, as well as the level of security achieved. The most common types of cards are:

> **Proximity (prox) cards:** These 125 kilohertz cards are incredibly easy to use: just hold the card up to the printer, and the job will be released. Unfortunately, they offer the lowest level of security. Prox cards assign a serial number to an individual that the reader verifies, but this number can be cloned with relative ease.
>
> **Smart cards:** Smart cards like HID Seos® use random serial numbers to establish communication with the reader, making cloning nearly impossible. They also help avoid card collision—if two prox card users are in the same space, the card reader may not work, while smart cards allow the reader to select the right one.
>
> **Tags/Stickers:** If you have outdated cards or cards not supported by your current vendor, you could just add a tag or sticker to the card to facilitate communication with the reader. These tags are, however, 125 kHz and thus not as secure as smart cards.

Be sure to investigate mobile and wearable options not tied to a specific brand.

Multiple card types: Larger organizations may have different card types depending on location and security level. For example, a company's main headquarters may use Seos® for building access while satellite offices use prox. Some readers can be configured to read multiple card types—make sure your printer manager or manufacturer understands this need.

If you're using or considering using mobile/wearable credentials:

Mobile access is definitely on the rise—if you aren't using it now, you likely will in the future. If you currently use cards, opting for readers that work with both mobile and cards will allow you to make the switch with minimal disruption.

Mobile and wearables, like every option, have varying degrees of security: QR codes displayed on a mobile phone are relatively insecure and can be easily copied. Bluetooth beacons and NFC tags, on the other hand, offer additional security and cannot be copied. Mobile is also much easier to deploy and manage than cards—updates can be sent immediately without onsite help.

Be sure to investigate mobile and wearable options not tied to a specific brand. For example, your mobile secure print solution should work for both iPhone and Android users.

If you're using biometric credentials:

Biometrics like fingerprint scans offer an extremely high level of security and user convenience. Considering this advanced security, it's not surprising that they are also an expensive option. Many organizations opt to use biometrics in conjunction with another credential like mobile and cards. Also, even biometrics offer varying levels of security. Governments and other highly secure organizations benefit from added services like liveness detection that ensures a living, breathing trusted identity is attached to a fingerprint.

Identify Your Reader Needs

Once you have a firm understanding of your credentials and their capabilities, it's time to consider the best reader option to enable secure print. First, determine whether you need a reader to release a print job from several feet away, or would you require the user to be directly in front of the printer before releasing? Cards, biometrics and some mobile/wearable applications need the user to tap or touch their credential at the printer, ensuring the user is there to immediately pick up the document. On the other hand, you may want the ease of a reader that picks up a credential's signal from up to several feet away.

Next, consider whether you'd prefer the reader to be embedded inside the printer or installed to the outside. Embedded readers are more aesthetically pleasing but need space inside the printer housing and robust technical capabilities to install and maintain. Desktop or housed readers, on the other hand, look like a small hard drive that can be plugged into the printer and swapped out as needed. Desktop readers also prevent the printer's housing from interfering with the signal.

Readers also vary in interoperability; even if an organization uses all Seos® cards, a reader may not be able to verify cards established at one site and used at another. In addition, not every reader works with every credential; for example, if you use cards currently but are considering moving to mobile, choose a reader that works with both.

The right secure print solution combines security and convenience, taking you one step closer to a truly Connected Workplace.

Finally, identify the connections and connectors available. For example:

- USB connections attach externally, allow auto-tuning of the card reader's antenna and are easily adjusted onsite. For biometric readers, USB connectivity is easiest to configure and implement.
- UART connections require installation internally into the printer and can be difficult to adjust.

Consult Your Key Ally—Your Printer Manufacturer or Managed Printing Partner

Finally, you'll need to have a thorough conversation with your printer manufacturer or printer manager. While it is technically possible to purchase readers independently and have your experienced IT team install them, as mentioned above this route is not advised and could be a waste of time and money. Discussing your identified credential preference for today and future, desired user experience for distance and proof of presence, and placement of readers with your printer manufacturer or managed print partner in the ensures a smooth and cost-efficient implementation.

Discover Your Solution

Understanding the basics of secure print and your current and future needs will help guide the conversation with your printer manufacturer or managed printing partner. They are the most important variable when implementing secure print, able to advise on exactly what your organization needs—or might not need at all. The right secure print solution combines security and convenience, taking you one step closer to a truly Connected Workplace. Organizations achieve substantial savings by eliminating personal printers and unnecessarily printed documents, reducing waste and better allocating costs.

Best of all, leveraging the current credentials already familiar to users and IT means very little training. You can feel confident that your secure printing solution is simply an extension of your trusted identity solution, and the next step to a truly Connected Workplace.

Visit our website to learn more about the market-leading secure print reader portfolio.

[1] *Quocirca research: http://quocirca.com/wp-content/uploads/2018/06/Quocirca-Print-Security-Jan-2017-Report-Excerpt.pdf*

[2] *Nuance research: https://whatsnext.nuance.com/office-productivity/orphaned-print-jobs-silent-security-leak/*

2019-05-06-hid-eat-secure-print-wp-en

PLT-04442