



## **AUTHENTICATION STRATEGIES**

UNDERSTANDING THE TRADEOFFS

## IT'S ALL ABOUT THE WORKFLOW •

---

At first glance, the choice of authentication and identification solutions might seem to be a fairly low-level security-technology decision. What users require what access to which systems? What are your password policies?

In healthcare, however, that perspective only scratches the surface of the larger issue because the dictates of HIPAA are raising the profile of information security. From a more tactical perspective, authentication and identification are ultimately workflow issues. For caregivers, the real imperative is to take care of patients efficiently - not deal with information security. They will, therefore, avoid - and even reject - security practices that impede care delivery.

What's also true is that workflows vary based on the type of caregiver, the task at hand, the patient's condition, and venue, and a productive means for authentication in one situation can be an impediment in another. In an emergency room, you'll find dozens of caregivers, visitors, public-safety personnel, and visitors coming and going in a swirl of activity. With different beds, patients, computers, and situations, the environment is hectic and the information-security workflow needs are urgent and rapid.

Contrast that with an operating theater, a highly secure environment with low traffic and low turnover. Information security needs are well-defined and fairly static in this situation. And there are other variations in ICUs, pharmacies, and other clinical settings. Although there are numerous authentication technologies in the market today, the effective choices for hospitals must address key problems:

- Speed – Security that introduces delays is unacceptable to the clinical community. Ideally, new technologies should accelerate authentication.
- Security – Hospitals need authentication that is non-corruptible and cannot be easily repudiated.
- Environmental Adaptability – Whether it's latex-gloved workers, sterile environments, or high-traffic areas, the authentication choices must be suitable for the environment.
- Regulatory Compliance – New regulatory frameworks, such as the Ohio State Board of Pharmacy's Positive Identification requirements make it more important than ever to close security loopholes and demonstrate commitment and effort to ensuring privacy of healthcare information.

## FINDING COMMON GROUND •

---

Borrowing from Hippocrates' "First, do no harm," a healthcare authentication technology's should be credo is "First, do not make things more difficult." It's no secret that clinicians focus on their patients, not their patience. If an authentication technology requires an inordinate change to their customary work processes or creates inconsistent or difficult experiences, it will not succeed.

As you evaluate different options, it's a good idea to reflect on some important considerations. How does the proposed authentication technology change the user's experiences with the application(s)? For instance, will caregivers accustomed to using generic accounts now be required to individually authenticate? What work must IT do to prepare users? What maintenance issues does the technology present?

From a user's perspective, the ideal scenario is where she doesn't need to remember anything, do anything, or possess anything – secure access is granted instantaneously. From an IT perspective, the ideal scenario ensures that every computer user is correctly authenticated – and cannot be accidentally or intentionally impersonated - before access to computer systems are granted. As an IT professional, your job is to balance these competing and conflicting demands and deploy a feasible solution that is acceptable to all parties.

Increasingly, password protection is no longer viewed as adequate by either camp. Multiple systems requiring multiple accounts and passwords, frequent password rotation, and the inherent susceptibilities they present have led many hospitals to pursue more sophisticated authentication strategies.

## FINGERPRINT BIOMETRICS •

---

From a usability perspective, using the fingerprint as the basis of authentication is a very attractive proposition. There's nothing for the user to remember and the gesture required is trivial. However, from an IT administrator's perspective, fingerprint biometrics presents some limitations that merit careful consideration.

- Enrollment – The initial enrollment of the user should involve scanning at least three fingers for each user. This is because not all fingers will reliably image when the user subsequently attempts to authenticate – injury, humidity, and other factors can affect the reliability of subsequent scans.
- Speed – When used for authentication, (that is, proving that the user is who she claims to be) fingerprint biometrics is quite fast. The identification hash of the user's fingerprint is computed from the scan and compared to the numerical hash of that fingerprint stored on file (as produced during the enrollment process). The authentication is accepted or rejected based upon the results of the comparison of hash values. However, when the fingerprint is used for identification (that is, to determine who the person is), the security application must compare the scanned fingerprint with an entire list (perhaps thousands) of users. Although biometric identification algorithms are improving, it's presently an unacceptably slow process.
- Reliability – What's more, fingerprint authentication generates anywhere from 2-20 percent false rejects. While a user can always fall back to using his password, in a high-pressure healthcare setting, this can be a recipe for caregiver frustration and ultimately rejection of the technology.

## ACTIVE PROXIMITY •

---

Active proximity technology uses a low-power radio signal from a battery-powered card that's worn by the user. Each PC or workstation in the healthcare facility is equipped with an antenna that detects the arrival and departure of each user's card. The system automatically identifies the user who then simply enters a password to gain access to the computer.

Active proximity provides a significant benefit that's often overlooked in the authentication process: the log-out. Active proximity systems monitor the immediate area of the PC (the range can be configured for each computer) for the continued presence of the radio signal from the user's card. If the user leaves the proximity, the computer can immediately hide and lock the screen or even log the user off.

If multiple authorized users are in proximity of the same computer, it's no problem: the list of detected users is presented, and only the user who picks his/her identifier and enters the associated password has access to the computer. If a user is engaged in a computing session and another user walks up within proximity of the computer, the technology simply ignores the signal since the computer already is engaged with an active user session.

However, there are some compromises with active proximity implementations. The low-power RF signal is very sensitive and requires careful fine-tuning. Each individual user requires tuning with respect to where they wear their card. A lanyard vs. a belt-clip does matter, and being tuned for one and then switching to the other can dramatically impact the reliability of the detection process. Variables like body mass and even jewelry can also affect reception. And if the antenna is moved (perhaps by a cleaning person), signal strength (and therefore the proximity range) can change in ways that can result in unexpected behaviors. The tuning process involves each computer and each user and requires careful and constant maintenance. The result: a potentially inconsistent user experience.

## PASSIVE PROXIMITY WITH ENHANCED AUTHENTICATION •

---

Aiming to simplify the authentication challenge, healthcare organizations have sought to leverage the ubiquitous basic access-card that caregivers and other hospital workers carry to gain physical access to buildings, floors, and wards. In a simplified model, the user presents/swipes the ID card (or badge) at a computer (equipped with a badge reader) and enters their password. This action identifies and then authenticates the user.

The shortcoming of this model is that it does not buy much, as users must still swipe their cards and enter a passwords many times during the day, which clearly is tedious.

To enhance the usability of passive proximity cards, Sentillion developed its Tap & Go solution. With Tap & Go, the user logs on to a workstation by presenting his standard passive proximity card and then entering his password. Once this two-part authentication is complete, the Tap & Go technology initiates an institution-defined authentication grace period, during which the user can access any other workstation in the immediate vicinity (e.g. department, unit, or ward) simply by presenting his badge to the workstation's reader. No additional authentication is required during the grace period.

The user only needs to repeat the authentication when his grace period expires or when he moves to an area of the hospital with a different policy. The duration of the grace period is centrally controlled by IT and can be set for the entire enterprise or by workstation group, enabling security protocols to be matched to specific clinical venues and patient care workflows. If the card is lost or misplaced during the grace period then a help desk technician can easily revoke the grace period, rendering the card useless without the accompanying password.

Tap & Go enables healthcare organizations to strike a balance between security and usability. It also enables healthcare organizations to leverage existing assets in the form of their existing passive proximity cards. Best of all, Tap & Go does not require any special enrollment process or tuning. It just works.

## CONCLUSION •

---

Identification and authentication technologies are bringing new levels of power and sophistication to healthcare IT. As organizations strive to deploy stronger security, new approaches using proximity and biometrics present a series of advantages and tradeoffs that merit careful consideration. IT evaluators should carefully analyze their own environments and seek to match their needs with the right technologies.

For more information on authentication technologies, please visit the Sentillion Web site at [www.sentillion.com](http://www.sentillion.com)

sentillion®

Sentillion, Inc.  
40 Shattuck Road  
Andover, MA 01810

(978) 689-9095 phone

(978) 688-2313 fax

[www.sentillion.com](http://www.sentillion.com)