ALLEGION™

High security applications for biometrics

Biometrics are the most advanced security solutions on the market today. Commonly used in commercial main entrances, industrial settings and high-security areas (labs, pharmacies, bank vaults), biometrics work by measuring one or more unique physiological human characteristics: the shape of a body, fingerprints, structure of the face, DNA, hand geometry, iris or vein patterns.

Unlike other forms of security, biometrics can never be forgotten, lost or copied. Best of all, they let your clients protect their most valuable assets with the highest level of security.

Types of biometric technologies

There are five main types of biometric technologies:

- **Hand geometry:** Hand geometry reduces privacy concerns because it relies on the size and shape of a user's hand—something that can't be duplicated. It is larger in size but is ideal for production and industrial environments because a user's hand doesn't have to be clean or sterile for the reader to work.
- **Fingerprint:** Fingerprints are the most commonly used biometric because of the reader's compact size and low-point price. Fingerprint technology, however, generally only works in clean or sterile environments. Fingerprint technology has a tendency to fail if a user's hands are dirty or dry. Additionally, since fingerprints are easy to lift and duplicate, there are privacy concerns with this technology.
- **Iris recognition:** Iris recognition is a contactless biometric technology, often used in high-end environments or government buildings. It uses mathematical pattern-recognition techniques on video images of an individual's eyes. Iris readers must be installed and used at specific heights. Iris readers tend to be more expensive than fingerprint and hand geometry technologies.
- **Facial recognition:** Priced comparably to iris recognition, facial biometric technology is widely used in banking, labs and clean environments due to its accuracy. Lighting, however, can affect readings and impact reliability.
- **Vein authentication:** Among the newest biometric technology, this biometric uses the vascular patterns of an individual's hand as personal identification data. Vein biometrics can be used for computer log-ins, POS authentication and physical access control.

Choosing the right biometric

Identifying the right biometric solution for your client's building depends on several factors. Discussing the following will help your clients to set priorities and determine which biometric solution best fits their needs:

- What's unique about the environment? (i.e. industrial, sterile, etc.)
- Will readers be placed inside or outside?
- Do you want contact or contactless technology?
- How important are aesthetics?
- Are there privacy concerns?
- Are there cost limitations?
- What are the top priorities? (i.e., reliability, convenience, cost, privacy, accuracy)

ALLEGION™

How do they compare?

	Cost	Size	Ease of Use	Industrial/ Robust Settings	FAR (False Accept Rate)	FRR (False Reject Rate)	FTE (Failure to Enroll)	Privacy Concerns
Hand Geometry	Medium	Large	High	Yes	Medium	Low	Low	Low
Fingerprint	Low	Small	Medium	No	Medium	High	High	High
Iris (Eye)	High	Medium	Low	Yes	Low	Medium	High	High
Facial Recognition	Medium	Medium	High	Yes	High	Medium	Low	High
Vein	Medium	Small	Medium	Yes	Low	Medium	Medium	Low

Multi-factor authentication

Biometrics can be paired with cards and/or a PIN to provide multi-factor authentication. Access to highly sensitive and secure areas—such as data centers, bank vaults and pharmacies—often requires multi-factor authentication in order to ensure a higher level of security.

Allegion has partnered with Iris ID Systems (IrisAccess 7000) and XiD Technology (REVOFace) to integrate our aptiQ™ smart card reader technology into their biometric readers to provide a single product that offers multi-factor authentication.

IrisAccess 7000

ALLEGION™

Hand geometry vs. other biometrics

Use the chart below to learn how the other types of biometric technologies compare to the biometric HandReader manufactured by Allegion.

Technology	Advantages vs. Hand Geometry	Disadvantages vs. Hand Geometry
Fingerprint	▪ False accept rate can be lower (depends on product) ▪ Pricing may be lower (depends on application)	▪ Larger template, fewer users per reader, requires more readers ▪ Higher false reject rate (depends on product) ▪ Privacy issues/law enforcement association with fingerprints ▪ One in 50 people have unreadable fingerprints ▪ Sensitive to dirt, dry skin, etc.
Iris scanning	▪ Low false accept rate (probably lowest of all biometrics)	▪ Higher false reject rate ▪ Larger template, fewer users per reader ▪ Problems with lighting, eyeglasses and contact lenses ▪ Sometimes perceived as more intrusive
Facial	▪ Pricing may be lower (depending on number of employees) ▪ Touch-free	▪ Larger template, fewer users per reader ▪ Higher false reject rate ▪ Perceived as more intrusive ▪ Problems with lighting, eyeglasses, hats, hair styles, weight gain and facial hair
Vein	▪ Smaller in size ▪ Runs in ID mode (one-to-many comparison)	▪ Difficult to enroll without guidance ▪ Slightly higher false reject rate ▪ Slightly higher false accept rate

About Allegion

Allegion (NYSE: ALLE) helps keep people safe and secure where they live, work and visit. A $2 billion leading provider of security products and solutions, Allegion offers products under 23 brands in more than 120 countries. Allegion's portfolio includes CISA®, Interflex®, LCN®, Schlage® and Von Duprin®. For more, visit **allegion.com.**

aptiQ ■ **LCN** ■ SCHLAGE ■ **STEELCRAFT** ■ **VON DUPRIN**

010160 Rev. 1/31/2014
allegion.com/us