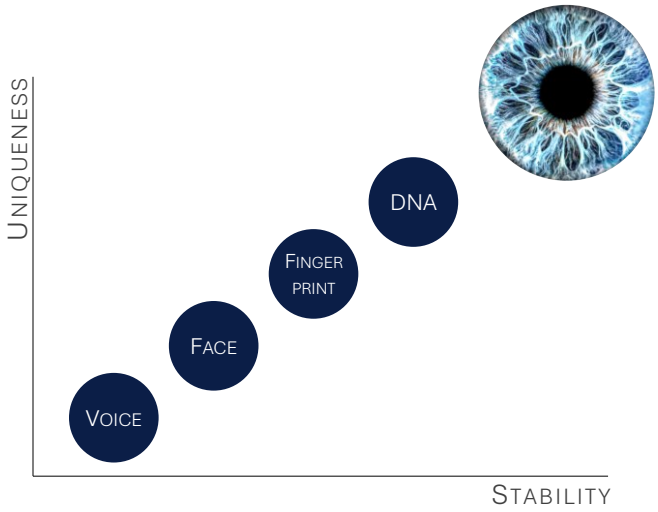
princeton IDENTITY

"Iris – not face nor fingerprint – is BEST for intentional identity assurance."

Iris vs Fingerprint **Biometrics**

Passwords, PINs, cards, and mobile credentials all suffer from the same flaw: they can be shared, stolen, lost, or spoofed. Biometrics change the equation by tying identity to a physical characteristic inseparable from its owner.

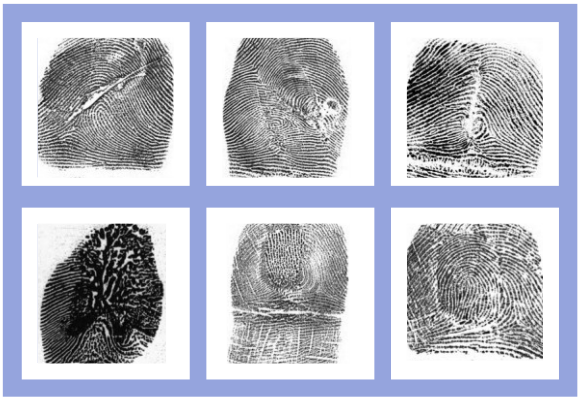
Fingerprint is the most common biometric for access control, but it is prone to many known performance issues. These limitations are pronounced in environments with manual labor, PPE, or high-volume access points. Modern organizations need identity assurance without these constraints. *The solution is your iris!*



Attribute	Iris Recognition	Fingerprint Recognition
Capture Method	Touchless near-infrared imaging	Contact-based surface reader
Information Density	Extremely high, rich detail for highly accurate matching	Low to medium, limited by surface detail
Stability Over Time	Fully stable for life by age 3	Degrades with age, wear, or injury
Environmental Sensitivity	Works through glasses/shields; unaffected by dirt/light	Affected by moisture, dryness, gloves, dirt / oils, etc.
Throughput	Fast, no retries	Slower, frequent retries
Spoof Resistance	Very high, internal biometric	Medium, susceptible to latent print/mold replication
Hygiene	Fully touchless	Shared contact surface
User Cooperation	Low, only your natural gaze	High, precise finger placement/pressure
Database Scalability	Excellent for large N:N matching; can scale to global populations	Limited accuracy for large-scale matching

Iris vs Fingerprint: **Identity Assurance**

Where Fingerprint Fails in the Real World



Your fingerprint works well as a credential under ideal conditions – but almost nowhere else. The weaknesses listed below make fingerprint a poor choice for high-security, high-throughput, or high-variability environments.

- **Wear, damage, and aging** Occupational wear, as well as natural aging, degrades fingerprints, leading to enrollment and matching failures.
- **Environmental sensitivity** Moisture, dirt, lotions, grease, sweat, and cracked, dry skin from cold weather cause frequent misreads.
- **Gloves and PPE** Any protective glove —latex, rubber, leather — prevents every reader from capturing your fingerprint.
- **Hygiene concerns** Shared-contact sensors create unavoidable sanitation issues and user resistance.
- **Slow throughput** Finger placement retries, poor read rates, and frequent cleaning of the touch surface cause delays that multiply during peak flow. It also requires at last one hand to be free, meaning people must put down laptops, tools, etc. before authentication, further slowing lines.
- **Spoofability** Fingerprint sensors have been fooled by silicone molds that mimic lifted or copied fingerprints.

Why Iris Recognition Succeeds Where Fingerprint Fails

The iris delivers a level of accuracy, speed, and convenience that far exceeds what fingerprints can offer. In short: the iris works consistently for everyone, every day, in every environment. Fingerprints don't. Iris recognition advantages include:

- **Extreme uniqueness** The iris' structure contains orders of magnitude more detail than a fingerprint, is completely independent of genetics, and no two irises are alike – even the two on your own face. It is the most distinctive biometric marker available, more so than DNA!
- **Extreme stability** The iris is formed by age three and remains unchanged throughout adulthood, ensuring a life-long identity credential.
- **Touchless and hygienic** Reading your iris requires no physical contact, eliminating user hesitation around shared surfaces and removing the constant cleaning and sensor wear that plague touch-based systems.
- **PPE-friendly** Works through safety glasses, goggles, and face shields – a major differentiator in labs, clinics, cleanrooms, industrial sites, etc.
- **Operationally fast** PI's iris recognition occurs in a fraction of a second, while users hands remain free for bags, tools, or mobile devices.
- **High spoof resistance** The iris can't be lifted, molded, or stolen like a fingerprint.
- **Indoor and Outdoor suitability** PI's readers perform reliably in low light, rain, snow, glare, and variable temperatures. Hats, gloves, and cold skin – all common fingerprint disruptors, do not affect the iris.

Conclusion

Princeton Identity's exclusive **Iris on the Move**™ technology delivers exceptional speed, convenience, and reliability for every intentional identity assurance application. Fingerprint (or face, for that matter) just doesn't measure up.

Princeton Identity is a leading innovator of iris-biometric and multi-factor authentication technologies, transforming how businesses and governments around the globe achieve secure and reliable identity assurance. Backed by over two decades of research and product design, our solutions are trusted by some of the most recognized names in banking, industry, higher education, healthcare, transit, and border control. Princeton Identity systems are proudly manufactured in the USA, and deliver unparalleled flexibility, accuracy, convenience, and scalability.

300 Horizon Dr. Suite 308
Hamilton, NJ 08691
609-270-3220