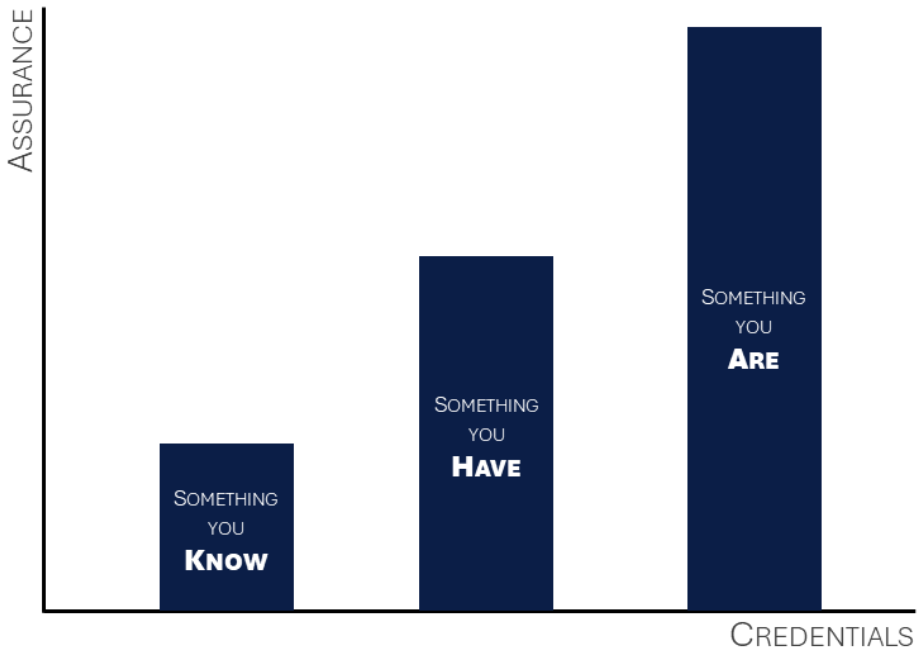
Princeton IDENTITY

About iris biometrics

www.PrincetonIdentity.com

NEED IDENTITY ASSURANCE? **BIOMETRICS ARE BEST!**

There are various mechanisms of identity assurance. When based on “something you know” (passwords, PINs) or “something you have” (cards, your phone) assurance is vulnerable because credentials can be lost, stolen, or even given away for fraudulent use. That’s not the case with biometrics (“something you are”) where credentials are based on physical attributes and inseparable from the owner. Biometrics also avoid the complexities and inconvenience of credentials you have to carry and remember. It’s no wonder biometric identity assurance use is exploding globally, especially for access control, point of sale, and time & attendance applications.



MATERIALS AND RECURRING CONSUMABLES

- NO PER-USE TOKEN COSTS
- NO BLANKS, FABRICATION EQUIPMENT
- NO REPLACEMENT (~10-15% / YR) OR TURNOVER PROCESSES

ORGANIZATIONAL RISKS AND LIABILITIES

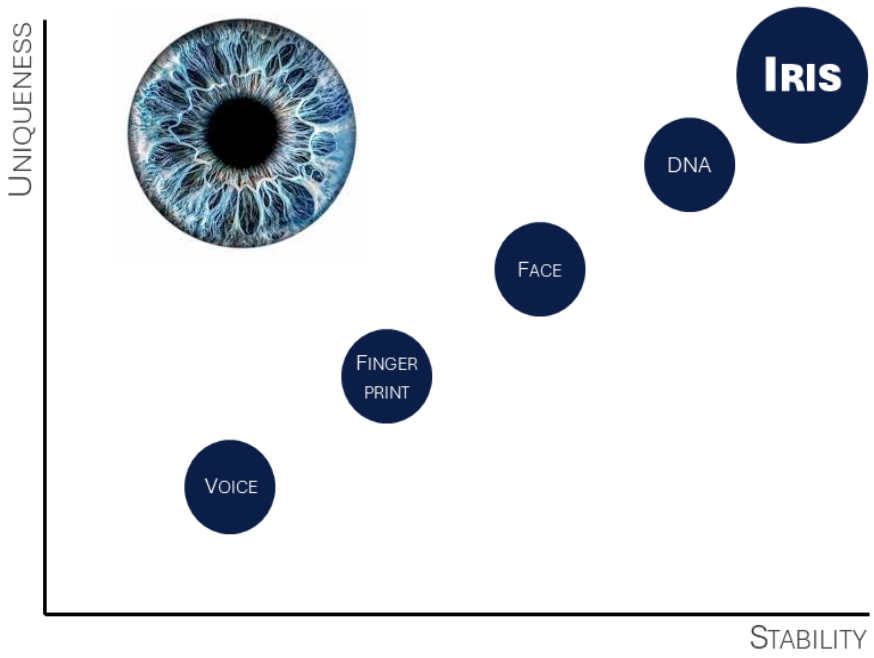
- HARDENED SECURITY = LESS LOSS, CONSEQUENCES
- MORE INVESTIGATION TIME FOCUSED ON FRAUD, NOT MISDEMEANOR

EMPLOYEE PRODUCTIVITY, ORGANIZATIONAL EFFICIENCY

- NO MORE FORGOTTEN OR LOST KEYS, PHONE, BADGE, ETC...
- IMPROVED ACCOUNTABILITY (CARD SHARING, BUDDY-PUNCHING)
- REDUCED CREDENTIAL-ADMINISTRATION OVERHEAD

Another factor driving adoption is Return on Investment (ROI). Employing biometric identity assurance offers clear, quantifiable economic incentives compared to traditional alternatives. Although commoditized card scanners can be inexpensive, you will find greater savings from eliminating assigned credentials altogether (Cards, Digital Mobile, etc) and optimizing credential issuance and replacement resources. Hardening security with high-assurance, un-sharable biometrics also drives risk reduction and efficiency gains – both enabling positive bottom-line growth. When viewed from this broader perspective, the ability of biometrics to provide a significant and enduring return on investment is undeniable.

WANT BIOMETRICS? **IRIS IS BEST!**



Many different biometrics exist, and it's important to consider their relative merits when designing for application requirements. However, for intentional and secure identity assurance, the choice is clear: THE IRIS – not the face – is the definitive gold standard.

Why? For one, the iris is non-intrusively accessible. This is not the case with fingerprints which require physical touch. Yes, the face is similarly accessible, but now consider that the iris is the most stable out of all the human biometrics. Your face will change quite a bit with age and condition (weight fluctuations, beard growth), but your iris is fully formed by age three and remains unchanged for the rest of your life. The iris is also the most unique human biometric... yes, more unique than even your DNA! Your iris' structure – the folds and wrinkles seen in the image above – is formed randomly and is genetics independent. That means while your face may bear a strong familial resemblance to your parent / sibling / cousin, your iris never will.

Finally, your iris contains an astounding amount of readable information (far more than your face). No two irises on the planet are identical – not among family, twins, or even the two above your nose. This fact is particularly important when considering applications with a large user base, or ones constrained to a particular demographic.

In short, iris biometrics are like having two perfectly unique, self-cleaning, and randomly assigned high-density QR codes installed on your forehead! This is why the iris – and not the face – is THE perfect biometric and will be the foundation for all future identity assurance.

IRIS	CHARACTERISTICS	FACE
✓	UNIQUENESS	
✓	STABILITY	
✓	HIGH INFORMATION CONTENT	
✓	GENETICS INDEPENDENT	
✓	ACCESSIBLE / NON-INTRUSIVE	✓
✓	HARD TO OBSCURE / ALTER	
✓	SELF CLEANING	
✓	REDUNDANCY	

IRIS & FACE RECOGNITION: **PRACTICE, PERFORMANCE**

The process of iris recognition is simple, and much like that of face recognition. Both involve capturing an image of the feature – typically visible spectrum for face and near-IR for iris. This data is then segmented and converted into a non-reversible mathematical form (a template), which is algorithmically compared to a database of those for stored users. Because the face is much larger than the iris, it can be recognized more easily from distances beyond 1m. Otherwise, as shown to the right, the practice of iris recognition and face recognition are mostly equivalent.

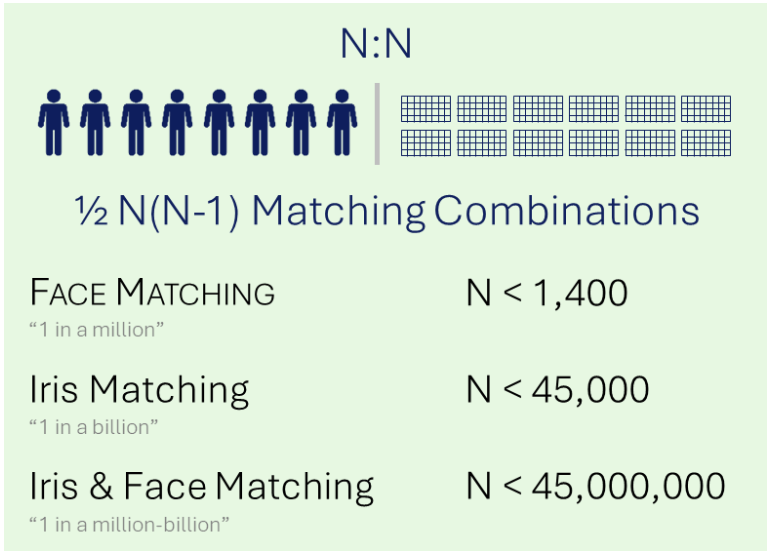
	IRIS	CHARACTERISTICS	FACE
Practice, Usability	-	TOUCHLESS / FRICTIONLESS	-
		OPTICS REQUIREMENTS	✓
	-	POWER, COMPUTING, & STORAGE	-
	-	ALGORITHMIC COMPLEXITY	-
	-	INSTALLATION COMPLEXITY	-
	-	COST	-
	1m	'EASY' SUBJECT PROXIMITY	**5m**
	-	SUBJECT MOTION TOLERANCE	-
	-	SPEED	-
Performance	✓	POSE, EXPRESSION, & APPAREL TOLERANCE	
	✓	USER CONVENIENCE	
	✓	SPOOF-RESISTANCE	
	✓	DEMOGRAPHIC-BIAS FREE	
	✓	ACCURACY	
	✓	SCALABILITY	
	✓	PRIVACY	

However, with performance, there is a clear winner between the two because iris biometrics' substantial intrinsic advantages enable iris recognition to be orders of magnitude more accurate. Additionally, note that iris recognition fundamentally avoids the demographic bias issues that plague face recognition. Iris recognition is also far more convenient for the user - no need for a specific pose, neutral expression, or even removal of your mask / hat / scarf / helmet / etc. And because sunglasses and other eyewear are transparent in the near IR (used for iris image capture), they are not a hinderance.

Because you can easily alter your facial appearance, facial recognition is burdened with an easier path to 'spoofing' compared with iris recognition. Because you only have one face but two independent irises, biometric matching on iris is more robust with built-in redundancy. And the ability to capture images of faces –but not irises – from a non-intentional distance means that iris recognition does not generally suffer from the privacy issues common to face recognition, aiding in over-all security.

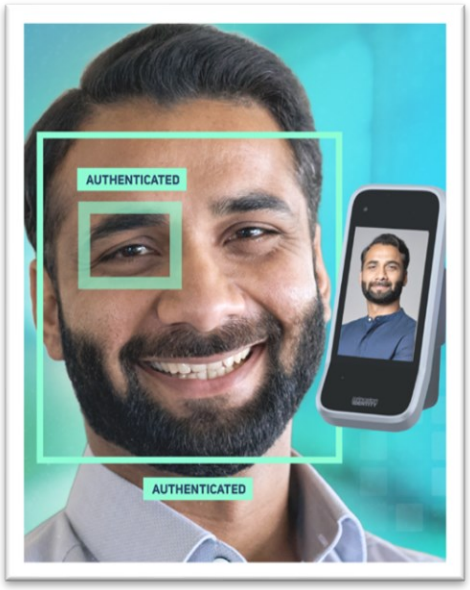
IRIS & FACE RECOGNITION: **USER-GROUP SCALE**

False Match Rate (FMR) and False Non-match Rate (FNMR) are important concepts but are easy to misinterpret. The complexity of biometrics reading and matching requires accuracy to be quantified statistically as FMR and FNMR, and never as a *'percentage error rate'*. It is important to know that these two metrics are mutually dependent, meaning you can always trade better FMR for worse FNMR and vice versa. For now, let's assume that FNMR is maintained constant at about 1 out of a hundred.



High-quality face recognition typically has an FMR quoted at about "one in a million". This seems lofty but realize that "one in a million" refers to one false positive identification every million *comparisons*. Each time you approach a biometric reader to be identified, N individual comparisons are performed between your biometric and the database of all users' biometrics (N = user base size). For a campus with N students or a company with N employees, there are ~ N^2 possible combinations of subject and database entries.

More rigorously, if your organization has 1,400 members and every day each one approaches a biometric reader only once, that requires about a million individual comparisons to be performed a day, expectedly resulting in one false positive identification daily. If there are more than 1,400 users or more identification attempts per day, the daily false positives will grow.



Now instead, consider high-quality iris recognition with FMR quoted lower at about "one in a billion" due to iris' superior biometric qualities. This lower FMR results in a larger practical user population: 45,000. Further increased user base is achieved if identification requires matching on both iris AND face, in which both biometrics' FMRs contribute: 45,000,000.

Due to face recognition's higher FMR and limited practical user population, **Princeton Identity recommends using face recognition only for casual applications with a smaller user base. That's why our solutions all include iris recognition, better accommodating rigorous identity assurance and a larger user pool.** For situations that demand the highest assurance (laboratories, critical IT infrastructure, etc.), nothing comes close to our **Iris AND Face** or **Iris AND Iris** matching multi-factor authentication.

You.

Not your appearance.

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