ID4D
IDENTIFICATION FOR DEVELOPMENT

G2Px
PAYMENTS THAT EMPOWER

Biometrics Deep Dive

WORLD BANK GROUP

Digital Public Infrastructure and Biometrics

- Identity is a foundational pillar of DPI
- Identity processes need to support both asserting identity and establishing credentials
- Strongly establish identity is key for e-payments and provision of services

When establishing identity there are some key principles:

- a person should only have single foundational ID
- establishing or re-establishing identity should be as accurate and - easy for the citizen as is possible

When using an identity

- Individuals should have a way to securely **bind** to that foundational ID

Biometrics can both establish "uniqueness" and provide convenient secure identity binding (usually in combination with other attributes) .

Biometric system risks and mitigations

Why face biometrics?

Benefits

- Faces are standard on most existing identity documents
- Easy and inexpensive to capture for enrolment
- Able to be used easily on mobile devices
- Can be easily manually assessed
- 1:1 accuracy is quite high

Risks

- Faces are public
- Subject to a range of enviornments
- Faces allow easy scope creep / cross match
- Subject to a range of attacks

Why fingerprint biometrics?

Benefits

- Fingerprint technology accurate and stable
- Well proven for large population de-deduplication
- Many readers available
- Multiple fingers provides high population coverage

Risks

- Fingerprints potential for cross match
- Mostly Contact
- Can be expensive
- Can be difficult to use for some users
- Subject to quality variations

Why iris biometrics?

Benefits

- Very fast, stable and accurate
- Non-contact
- Hard to spoof
- Provides significant population coverage, especially when combined with fingerprints

Risks

- Sometimes difficult to use
- Can be expensive
- Subject to eye conditions

Key Risks Biometric Recognition

Function Creep

The risk that a FRT system will be used for something other than its original purpose or that it is used for new or additional

Cross Matching

Use cases where a system designed for verification could, for instance, be cross matched with another eg for surveillance system.

Data Leaks

The risk of biometric data being accessed, read or removed by an unauthorized source. FRT systems are often more sensitive to such breaches.

Trust

The risk of public opinion and trust in the system being diminished by poor management or breaches of the system.

Key Risks for Biometric Recognition

2/2

Liveness detection

Face recognition systems can be subject to a range of vulnerabilities including masks or presentation of photo or videos.

Potential discrimination

(1) positive discrimination, against people (e.g., race or sex), and (2) the burden of inaccuracy falling disproportionately on particular races or genders.

Morphing

Taking two or more images of different people and creating a single look-alike facial image can be matched with either or both of the source facial image identities.

Genetic distinctiveness

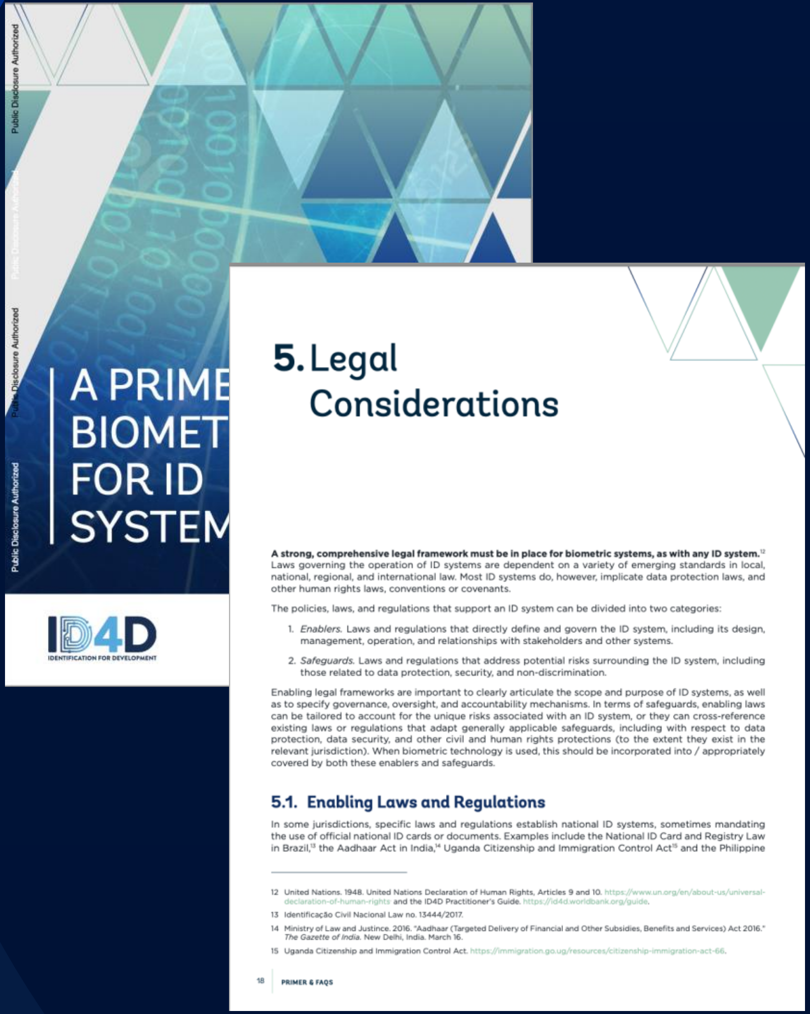
There is an intrinsic limitation of the distinctiveness of the face due to genetic factors (e.g., twins may be identified as the same individual).

Legal Considerations

Interface of laws and biometrics

Most ID systems involve data protection laws, and other human rights laws, conventions or covenants.

- Enablers. Laws and regulations that directly define and govern the ID system, including its design, management, operation, and relationships with stakeholders and other systems.
- Safeguards. Laws and regulations that address potential risks surrounding the ID system, including those related to data protection, security, and non-discrimination.


Public Disclosure Authorized
Public Disclosure Authorized
Public Disclosure Authorized
Public Disclosure Authorized
A PRIME
BIOMET
FOR ID
SYSTEM
ID4D
IDENTIFICATION FOR DEVELOPMENT

5. Legal Considerations

A strong, comprehensive legal framework must be in place for biometric systems, as with any ID system.[12] Laws governing the operation of ID systems are dependent on a variety of emerging standards in local, national, regional, and international law. Most ID systems do, however, implicate data protection laws, and other human rights laws, conventions or covenants.

The policies, laws, and regulations that support an ID system can be divided into two categories:

1. *Enablers.* Laws and regulations that directly define and govern the ID system, including its design, management, operation, and relationships with stakeholders and other systems.
2. *Safeguards.* Laws and regulations that address potential risks surrounding the ID system, including those related to data protection, security, and non-discrimination.

Enabling legal frameworks are important to clearly articulate the scope and purpose of ID systems, as well as to specify governance, oversight, and accountability mechanisms. In terms of safeguards, enabling laws can be tailored to account for the unique risks associated with an ID system, or they can cross-reference existing laws or regulations that adapt generally applicable safeguards, including with respect to data protection, data security, and other civil and human rights protections (to the extent they exist in the relevant jurisdiction). When biometric technology is used, this should be incorporated into / appropriately covered by both these enablers and safeguards.

5.1. Enabling Laws and Regulations

In some jurisdictions, specific laws and regulations establish national ID systems, sometimes mandating the use of official national ID cards or documents. Examples include the National ID Card and Registry Law in Brazil,[13] the Aadhaar Act in India,[14] Uganda Citizenship and Immigration Control Act[15] and the Philippine

[12] United Nations. 1948. United Nations Declaration of Human Rights, Articles 9 and 10. https://www.un.org/en/about-us/universal-declaration-of-human-rights and the ID4D Practitioner's Guide. https://id4d.worldbank.org/guide.

[13] Identificação Civil Nacional Law no. 13444/2017.

[14] Ministry of Law and Justince. 2016. "Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016." *The Gazette of India*. New Delhi, India. March 16.

[15] Uganda Citizenship and Immigration Control Act. https://immigration.go.ug/resources/citizenship-immigration-act-66.

18 | PRIMER & FAQS

Interface of laws and biometrics

ID system that includes face recognition should demonstrate:

- will bring **concrete and tangible benefits** to the public.
- is a **targeted and proportionate** way of achieving such aims.
- has a **clear basis in a law** that applies to the ID system owner is proportionate to the public interest aims pursued and provides adequate data protection safeguards.

Oversight

- Institutional Oversight
- Independent Government Authority
- External and Internal Access
- Inclusion

Technical Mitigations

Data Security and Storage

- Securing Raw Enrollment Data
- Use of Cloud Storage
- Biometric Template Protection and Biometric Encryption

Restrictions can be placed on:

- Identification. The searching (1:N) of a database for a matching identity.
- Authentication. The validation of an identity (1:1) using a biometric.
- Inspection. Allowing a visual inspection of an image by an operator or officer.
- Resolution and adjudication. The process of manually examining the outcomes of close biometric matches.
- Cross matching. The cross-linking of biometric databases based on template-to-template matching.

Template Protection

Template Protection Techniques

Crypto biometrics.

Cryptographic biometrics, or "crypto biometrics," refers to the practice of separately encrypting each template with a unique key. This ensures that the templates cannot be easily searched, since this involves decrypting each template that requires matching. It can provide an effective limitation against using a biometric system for unauthorised identification.

Unique template key.

To prevent the use of stolen templates, unique templates can be created that are specifically designed for the deployed algorithm. This means that any stolen templates would not be useful on any other system. It also restricts the ability to match templates across systems (this does not prevent such matching where the raw biometric is retained).

Homomorphic encryption.

Homomorphic encryption is an emerging technique that allows computations to be carried out on encrypted templates, thus generating a result without decrypting the templates. The value of this encryption is that stolen templates are of limited value since they cannot be easily decrypted without the correct keys. While this does allow for identification, it prevents cross-matching against other data sources where the original biometric is still accessible.

Data Storage and Transmission

Standard IT Security Good Practice should be followed

- Data Encryption at Rest and in Transit
- Encryption of Backups
- Vulnerability and Penetration Tests

Limiting Functional Use Cases

Segregation of duties for individuals operating the system and exclude use cases outside of the current functional requirements

Limit to 1:1

Some systems limit the use of face biometrics to verification (1:1 facial matching) or simply printing pictures on IDs for manual authentication and so do not feature 1:N type facial matching..

Restrict matching

Restrict search (1:N) capability to only deduplication. Other uses have the potential for function creep of surveillance and so should be only enabled where essential

Access

What data is exposed to different types of system operators? Not all system operators need access to the raw biometric image or other personal data.

External matching

How will access to the system by external parties be managed or restricted? Will it be possible to enable matches from other jurisdictions?

Watchlist

How large can a watchlist become, and who has access to the results?.

Audit

How will inappropriate uses of the system be detected and resolved?

Export

How does the system prevent the unauthorized viewing, use, or extraction of data (biometrics or other personal data)?

Adjudication

When close matches occur, how will such cases be decided? How does the system define “close,” and what is the threshold?

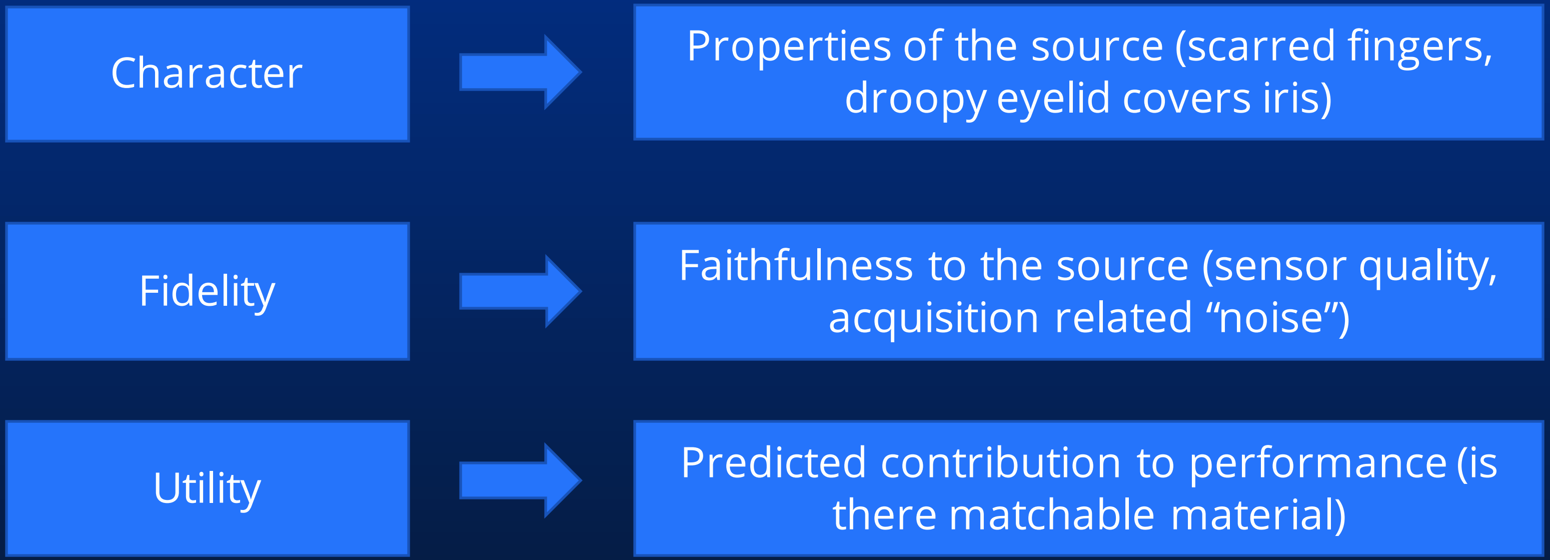
Biometric Recognition Performance

Performance depends on multiple highly technical factors

- The data set. Performance accuracy depends on the degree to which the underlying test data matches the real data that is expected to be seen by the system. Where the data is different, the performance results are unlikely to be fully valid
- Statistical measures. The two best-known accuracy statistics are false accept and false reject; however, there is also a range of other different types of statistics. These include the rank one correct identification rate, the false non-match identification rate, and the failure to enroll rate.
- Configuration and tuning. Biometric systems have several parameters that control accuracy, such as the threshold and quality settings. Assessed performance is dependent upon the configuration and tuning.
- Population size (gallery size). Performance of biometric systems when undertaking identification changes depending on the size of the gallery. As the gallery size increases the overall identification rate decreases

Biometric Quality

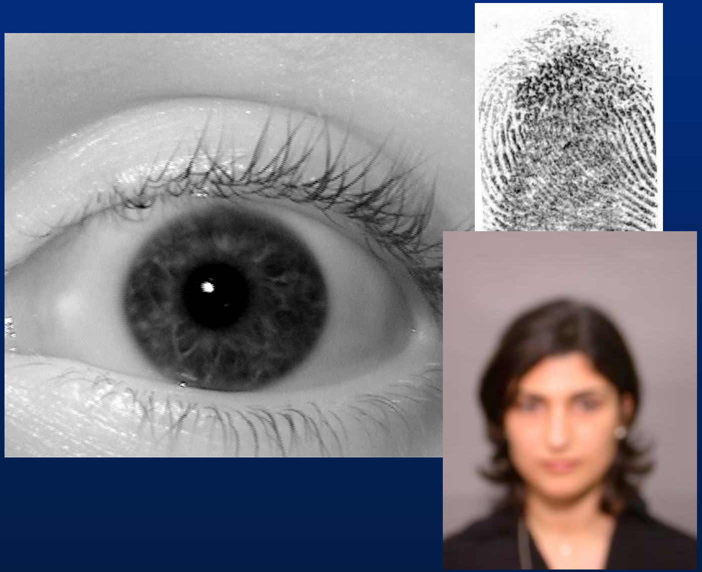
Biometric Sample Quality



Character → Properties of the source (scarred fingers, droopy eyelid covers iris)

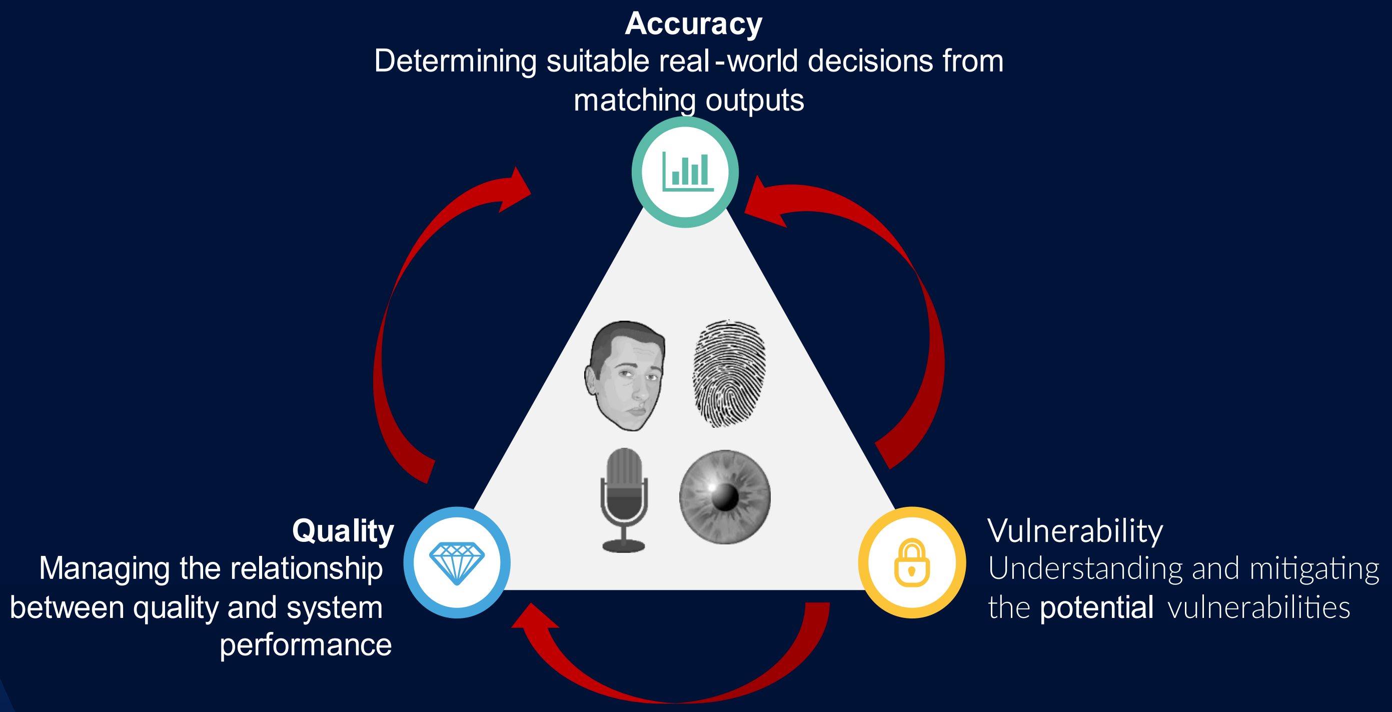
Fidelity → Faithfulness to the source (sensor quality, acquisition related “noise”)

Utility → Predicted contribution to performance (is there matchable material)



ISO/IEC WD 29794-1 Biometric Sample Quality - Part 1: Framework

Biometric Performance Triangle



Accuracy
Determining suitable real -world decisions from matching outputs

Quality
Managing the relationship between quality and system performance

Vulnerability
Understanding and mitigating the **potential** vulnerabilities

Biometric Quality

Causes and Techniques

Biometric Quality:

- Acquisition Device Characteristics
- Capture Environment
- User presentation

Quality techniques:

- User instruction
- User direction
- Operator training and guidance
- Automated quality assessment tools
- Quality analysis over time

Usage:

Forensic Investigation vs Machine Matching

Quality Examples

Example Causes

- Sensor & Hardware
  - Image resolutions, capture devices
- Application Factors
  - Time of day, age of template

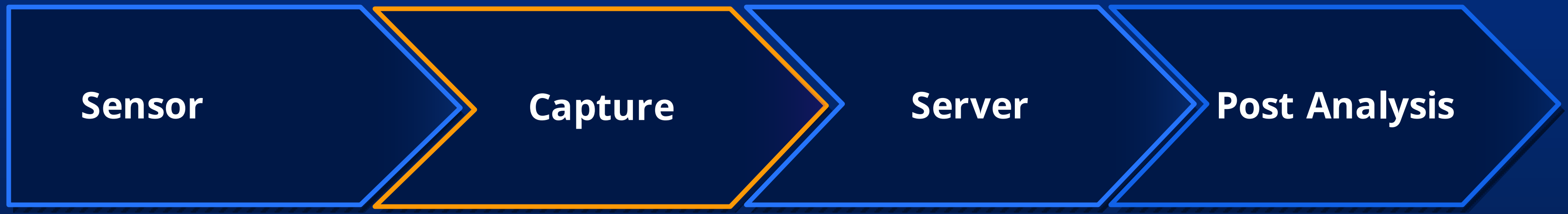
- User Physiology
  - Unique characteristics, scars, injury
- User Behaviour
  - Pose, expression, finger placement
- User Appearance
  - Hats, makeup, glasses, jewellery

- Environmental Influences
  - Backgrounds, lighting
- Compression
  - Artefacts due to image compression

Good data quality is essential for overall system performance

Acquiring "good" quality can be time-consuming

Stages of Quality Analysis



Sensor

Capture

Server

Post Analysis

On the device

In built quality to ensure capture is good quality by rejecting poor quality during acquisition – ideally provides proactive feedback

On the workstation

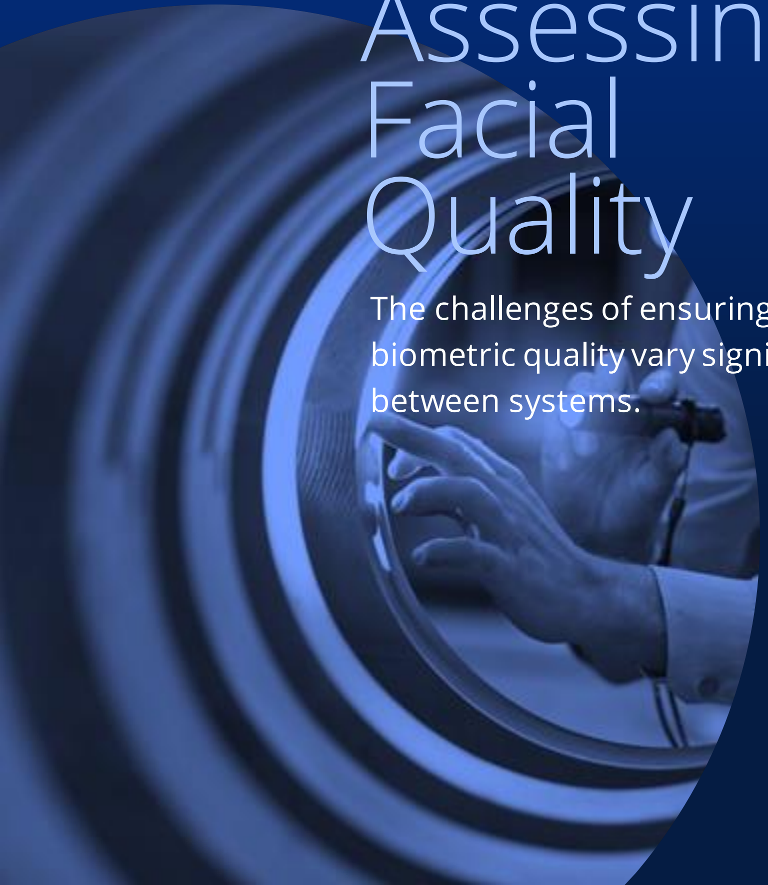
Once the biometric sample has been captured it can be subject to additional QA checks on the workstation, which might prompt another acquisition

On backend enrolment

After the biometric has been transmitted for enrolment or matching, it can be subject to more rigorous assessment to see if an perhaps manual review is required, or the potential for storing in different database.

For Analytics

Analysis of the capture quality to identify issues that are causing poor matching. These may only be apparent in a retrospective analysis. (BQAT)



Assessing Facial Quality

The challenges of ensuring biometric quality vary significantly between systems.

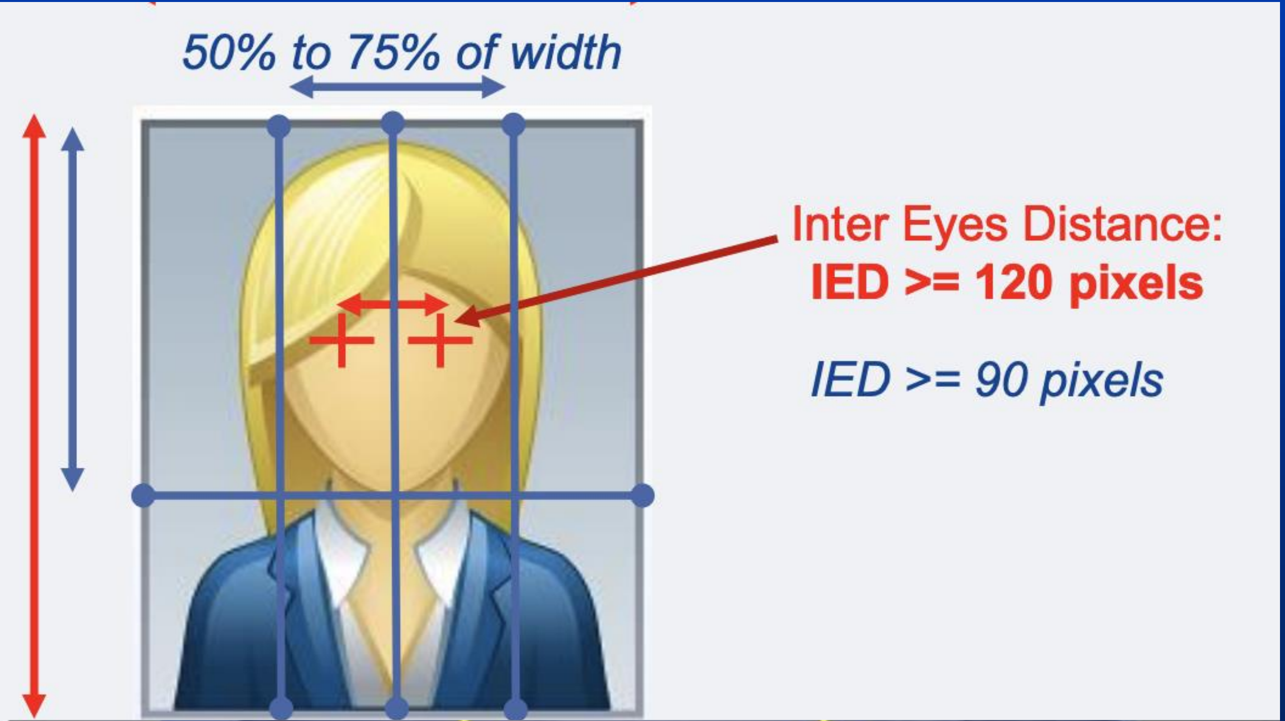
Consider:

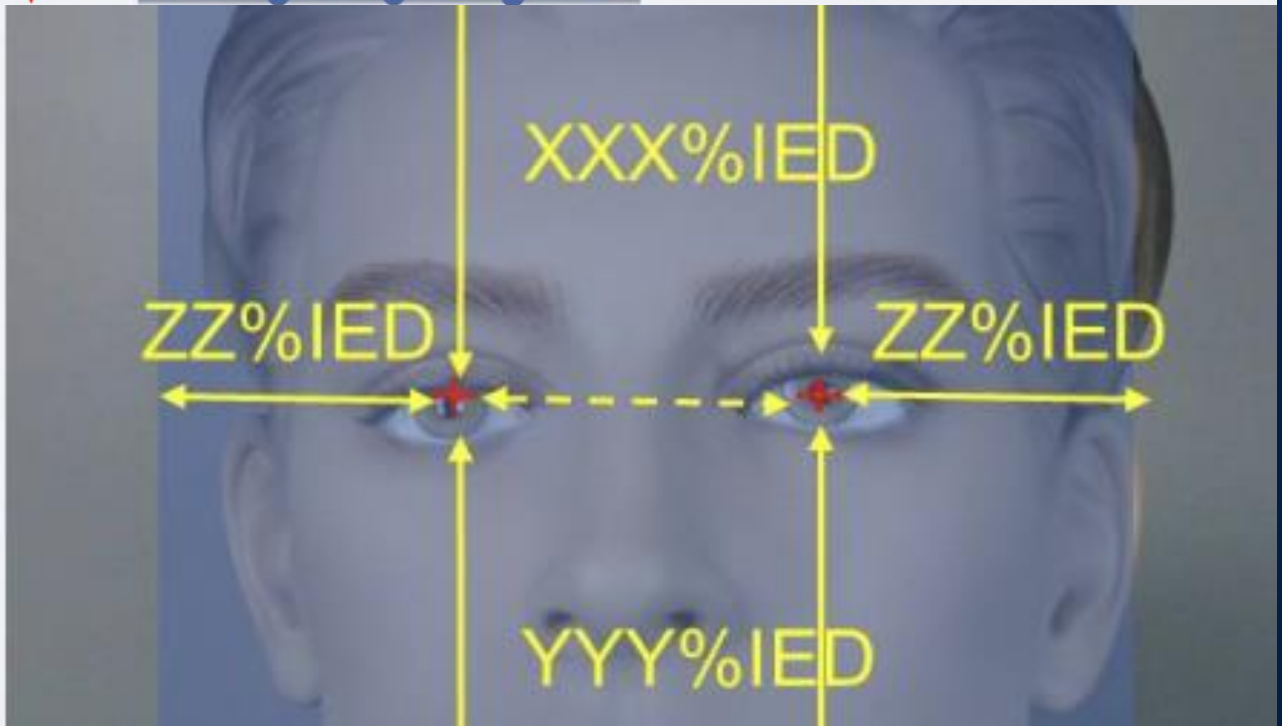
- How is quality affected where the acquisition is unsupervised? (e.g. customer takes a selfie on their device)
- What variables can be controlled?
- What are the behaviours or characteristics of the user base?

Some of the factors of image quality as per ISO 29794-5

- Lighting symmetry (Shadows)
- Pose symmetry (Angle)
- Image resolution
- Noise
- Illumination intensity
- Image contrast
- Exposure
- Focus, blur, and sharpness
- Colour
- Subject-camera distance
- Other considerations include the presence of glasses, head coverings, hats, hair, and facial hair.

All of these aspects will have potential quality impacts that could **reduce accuracy** or **introduce vulnerabilities**





ISO Face Quality Standard

Facial image quality is not standardized yet.
− ISO/IEC 29794-5 will give us a common understanding of measuring facial image quality in a specific application scenario.

sFIQ – EU Lisa

- EES Regulation (2017/226) and ISO 19794-5
- Best efforts / Still propietary

Open Face Image Quality

Open Face Image Quality (0-100) : generalised quality score
• A reference implementation of the OFIQ is being build by BSI / SecureNet it uses the output from the the ISO/IEC 29794-5 standard

BQAT (Biometric Quality Assessment Tool)

BQAT (Biometric Quality Assessment Tool) is an open-source framework to evaluate the quality of biometric samples. BQAT is designed to strengthen capabilities across all biometric systems by flexibly integrating biometric quality control across any modalities in an open-source package that is easy to deploy and use

https://biometix.github.io/

Universal

Works across all modalities and can support any quality algorithm. Currently supports face, fingerprint and iris.

Standard

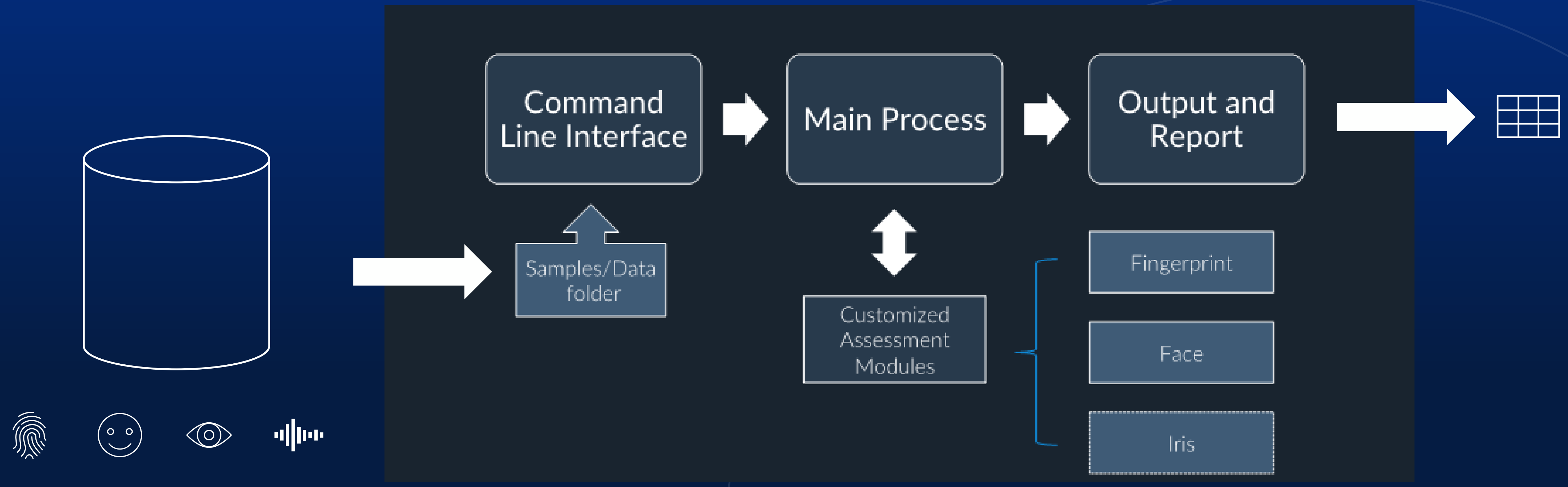
Works the same and creates the same output format regardless of modality or quality algorithm

Open-Source

Active open-source community extended and using the framework. Ease to use and setup.

BQAT Process

https://biometix.github.io/



Command Line Interface

Main Process

Output and Report

Samples/Data folder

Customized Assessment Modules

Fingerprint

Face

Iris

ID4D
IDENTIFICATION FOR DEVELOPMENT

G2Px
PAYMENTS THAT EMPOWER

Thank you

WORLD BANK GROUP