bioconnect.id

User Choice in Selecting Modalities for Authentication

Four Modalities, Four Choices for Users

Different users will be more comfortable authenticating with different modalities and the situation the user finds themselves in during time of authentication will play a major factor in the chosen modality used. For example, authenticating with Voice in a busy downtown food court during lunch time probably isn't the best idea as ambient noise may affect the success rate. Perhaps Face or Eye would be better suited for the situation.

There are many situations where the user will have a preferred modality for authentication, the important thing to remember is that BioConnect ID allows for users to have this choice – bringing convenience and security into every transaction.

Eye.ID

Eye.ID uses the built-in cameras on a user's mobile device to image and then pattern match blood vessels in the whites of users' eyes, ensuring highly accurate, fast and convenient digital identity protection.

Enrollment

Enrollment takes place by holding a mobile device so that the front facing camera captures the user's eyes. The user looks into the camera with their eyes in the viewfinder for ~15 seconds.

Verification

Verification is extremely quick – Holding your phone up to your eyes just as you did during enrollment will verify your eyes within 1-2 seconds.

Face.ID

Face.ID is a face recognition solution that allows the user to verify by just taking a "selfie" with their mobile device. It offers high tolerance against lighting/expression changes and a unique and non-transferable features coding algorithm.

Enrollment

Users are prompted to follow the motions shown through an animated head looking up, down, left, and right. The capture process takes about 10 seconds.

Verification

Users are prompted to frame their face within a circle image feed. The interface then asks the user to "Blink" – Once the blink occurs they are granted access. Total verification time is <5 seconds.

Voice.ID

Voice.ID allows the end user to authenticate by simply reading a set of digits into their on-device microphone. It offers a unique voice adaption feature to improve for environment variables, effects on the voice due to ageing, etc.

Enrollment

Users are prompted to read a series of a set of 4 digits into the on-device microphone. Total enrollment time is about 10-20 seconds.

Verification

Users are prompted to read a set of 4 digits into the on-device microphone. Total verification time is < 5 seconds.

Finger.ID

FingerPrint.ID technology provides a convenience benefit to the user allowing them to authenticate into their devices by just simply scanning their fingerprint. That is already enrolled in their mobile device.

Enrollment

The enrollment process will be driven by the base OS through the Settings function. Enrollment is usually completed by placing your finger multiple times across the embedded fingerprint scanner.

Verification

An SDK function is used to trigger a verification using the embedded fingerprint scanner. The fingerprint is matched against the data stored locally within the device.

While we strive to be as accurate as possible, costs change over time and further, BioConnect makes no representation as to the costs and savings set out here. You must complete your own assessment based on your unique business situation.

Sources: Securing the Global Village Technical Whitepaper, Lexis Nexis Risk Solutions, All Business.

bioconnect.id

Layered Security: Multi-factor Authentication

Different Levels of Security for Different Levels of Trust

BioConnect realizes that not all transactions or access attempts require the same level of security, or trust, in the the identity of the user.

For this reason, BioConnect identifies below the suggested set of modalities and contextual data to ensure the highest level of security for transactions or access attempts.

HIGH SECURITY

Transaction or access attempts of “High Security” are considered to need the highest level of trust, therefore BioConnect suggests the following combination of biometric modalities for verification.

Suggested Verification Combination

- 3 Biometric Modalities (Face, Eye and Voice)

MEDIUM SECURITY

Transaction or access attempts of “Medium Security” are considered to need a medium level of trust, therefore BioConnect suggests using two of the following biometric modalities for verification.

Suggested Verification Combination

- 2 Biometric Modalities (Face, Eye, Voice or Finger)

LOW SECURITY

Transaction or access attempts of “Low Security” are considered to need a lower level of trust, therefore BioConnect suggests the following method requiring a single biometric modality verification.

Suggested Verification Combination

- 1 Biometric Modality (Face, Eye, Voice or Finger)

While we strive to be as accurate as possible, costs change over time and further, BioConnect makes no representation as to the costs and savings set out here. You must complete your own assessment based on your unique business situation.

Sources: Securing the Global Village Technical Whitepaper, Lexis Nexis Risk Solutions, All Business.

bioconnect.id

Defining Modalities for User Authentication

Combining Modalities, Securing High Value Transactions

Allowing users the choice of which biometric modality to use at the time of authentication is a valuable feature, but we must also remember that not all transactions or access attempts are rated equal in terms of their value and significance.

That's why BioConnectID offers selective modality authentication, this means that the enterprise requesting the authentication event can select which single or set of modalities must be authenticated by the user in order to complete the transaction or access attempt.

FAR & FRR Rates (Lab Testing)

False Acceptance Rate (FAR)

The likelihood that a biometric technology will incorrectly accept an access attempt by an unauthorized user.

False Rejection Rate (FRR)

The likelihood that a biometric technology will incorrectly reject an attempt by an authorized user.

Voice.ID

Template Size	>10,000	>20,000	>50,000
FAR	0.010%	0.005%	0.002%
FRR	3.000%	5.000%	9.000%

Finger.ID

Template Size	>10,000	>20,000	>50,000
FAR	0.010%	0.005%	0.002%
FRR	0.600%	0.700%	0.900%

Eye.ID

Template Size	>10,000	>20,000	>50,000
FAR	0.010%	0.005%	0.002%
FRR	0.400%	1.200%	1.400%

Face.ID

Template Size	>10,000	>20,000	>50,000
FAR	0.010%	0.005%	0.002%
FRR	1.000%	1.200%	1.500%

What does all of this mean?

Say there are 1,000,000 fraudulent user attempts and a single modality with a FAR of 1/50,000. The modality will stop 99.998% of fraudulent attempts, therefor 20 users of the 1,000,000 attempts will gain access.

Using 2 modalities rather than 1 to secure a transaction drops this fraudulent level to 99.9999996% or 0.0000004 fraudulent users in the 1,000,000 attempts. We can even decrease this to and even lower number when 3 or more modalities are required for a single authentication event.

While we strive to be as accurate as possible, costs change over time and further, BioConnect makes no representation as to the costs and savings set out here. You must complete your own assessment based on your unique business situation.

Sources: Securing the Global Village Technical Whitepaper, Lexis Nexis Risk Solutions, All Business.

Note: Template size and the corresponding security thresholds are non-configurable. Template size differences are reflected in lab testing only.