bioconnect.id

Defining Modalities for User Authentication

Three Modalities, Three 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 Finger 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.

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.

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.

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 or 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.

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.

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, Voice and Finger)

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 + 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, Voice or Finger)