techtalk.travel

BIOMETRICS

Biometric solutions

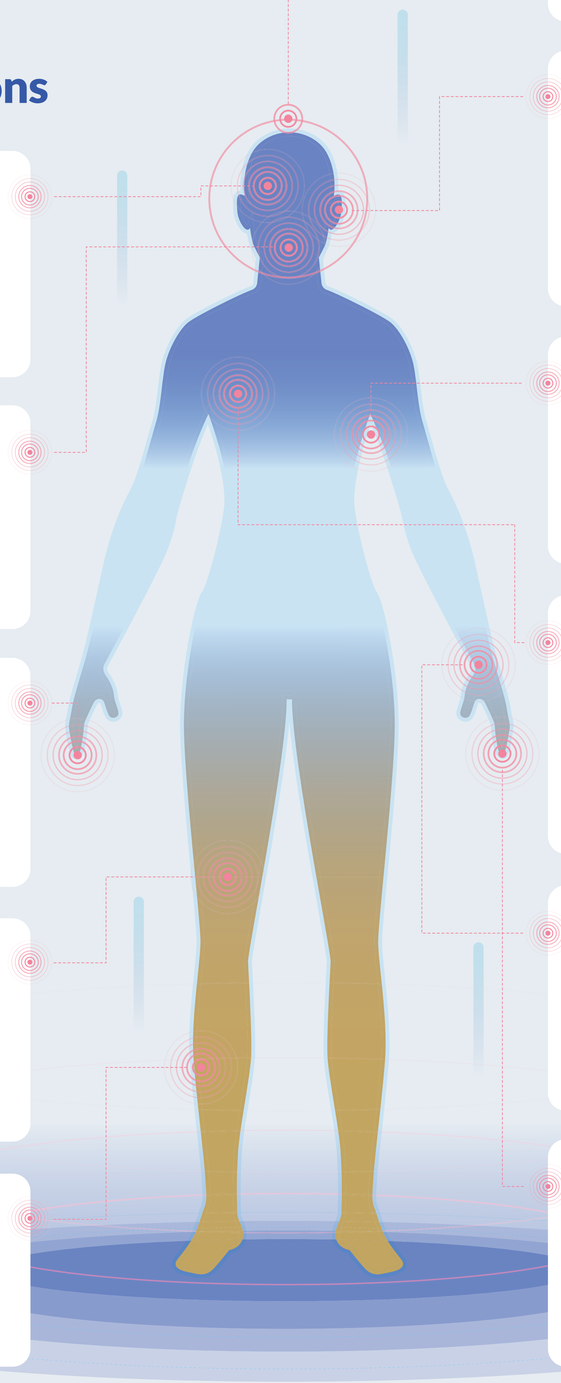
IRIS
Captures an infrared picture of the person's eye which is processed to obtain the spectral information of the iris.

VOICE RECOGNITION
The voice's features are based on the shape and size of the appendages used to create the sound.

FINGERPRINT
A map of the fingerprint's peaks and troughs is registered using optical, thermal and/or ultrasound technology.

VASCULAR
An infrared image of the skin is taken to detect the veins and a map of their distribution is obtained.

GAIT
The way one walks can be observed and measured to determine identity.



FACE RECOGNITION
The face's features are obtained using a low-resolution camera.

EARS
Analyzing ear shape might be as effective as facial recognition - and the shape remains consistent as individuals age.

ODOR
An individual's body chemistry provides an olfactory signal that can be identified by biosensors.

RAPID DNA TESTING
DNA, the ultimate identifier, used to take months to analyze and profile. Now there are machines that can do the work in less than 90 minutes.

SIGNATURE
Recording of the act of signing on a piece of paper or tablet. The movement, not the image, is recorded.

TYPING RECOGNITION
The force, speed and rhythm with which an individual taps the keys produce a personal signture of a different sort.

The phases of adoption of biometrics in mobile, websites and IoT devices.

MOBILE APPS

Generation 1

WEBSITES & DESKTOP APPS

Generation 2

KIOSK, ATM & IOT DEVICES

Generation 3

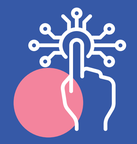
While most companies are still developing a strategy, there is no doubt that the ease and added security will propel biometrics to the forefront of identification and authentication. As technology grows in sophistication, it will only become more prevalent.

Identification VS Verification

Determines an individual's identify. The biometric data is compared against all the data held in the database.

Confirms an individual's identify by comparing a sample with one or more templates obtained previously.

✓ Good ✗ Bad ✗ Ugly



FINGERPRINTS

- ✓ It's much harder to fake someone's fingerprint.
- ✗ Often rely on partial matches and/or can be faked.
- ✗ If not stored securely, presentslifelon g risk of being hacked.

FACIAL RECOGNITION

- ✓ Users can authenticate without even making a gesture.
- ✗ Photos or 3D prints can trick iris scanners or facial recognition systems.
- ✗ May not recognize People of Colour or non-CIS gender people as accurately.

VOICE RECOGNITION

- ✓ Users cant' forget their voice as they could their password or physical keys.
- ✗ May not recognize the voice of a sick user.
- ✗ Unknown who has access to the voice of a user.