Biometric ID & Mobile Voting

FINGERPRINTS
- 5-9 Second Processing Time
- Commonly Used in Border Management
- Also Used in Law Enforcement

FACIAL RECOGNITION
- Non-invasive Collection
- Currently Used for Passports and National ID Documents

IRIS
- Low False Acceptance Rates
- Difficult to Replicate
- Two Second Processing Time

DNA
- Establishes Familial Relationship
- Commonly Used in Law Enforcement
- Highly Unique/Impossible to Replicate

What about other biometrics?

Voice and fingerprints are just two forms of biometric identification. Other technologies that are currently in use and in development include:

- Heart-rate recognition, which uses the unique beat pattern of each person's heart.

- Vein-pattern recognition, which detects the unique pattern of your veins under your skin, typically in your hand, wrist and arm.

- Iris recognition, which uses a camera to photograph the pattern of your iris.

- Retina recognition, which works in a similar way to vein-pattern recognition but within the eye.

Quantum cryptography for mobile phones

Date: April 3, 2014

Source: University of Bristol

Summary: An ultra-high security scheme that could one day get quantum cryptography using Quantum Key Distribution into mobile devices has been developed and demonstrated. Secure mobile communications underpin our society and through mobile phones, tablets and laptops we have become online consumers. The security of mobile transactions is obscure to most people but is absolutely essential if we are to stay protected from malicious online attacks, fraud and theft.

Application of Biometrics in Mobile Voting

Donovan Gentles[1], Suresh Sankaranarayanan [2,3]
[1]Mona Institute of Applied Sciences, University of WestIndies, Jamaica
dongen02@gmail.com
[2]Computing & Information Systems, Institut Teknologi Brunei, Brunei
[3]Department of Computing, University of WestIndies, Jamaica
pessuresh@hotmail.com