

Melissa Karolewski  
Background Research Report  
CREU 2006 – 2007  
Fall 2006

Definition of Biometrics .....	3
Current Types of Biometric Devices .....	3
RFID's (Radio Frequency Identification Devices) .....	3
<i>What is RFID?</i> .....	3
<i>Types of RFID Devices</i> .....	4
<i>Implantable RFID's</i> .....	4
<i>RFID Technology in the Industry</i> .....	4
<i>Current Uses of Implantable RFID Devices</i> .....	5
<i>Current Uses of RFID Devices</i> .....	5
<i>VeriChip – “RFID For People”</i> .....	6
<i>VeriChip – Implantable RFID's</i> .....	6
<i>Problems with RFID's</i> .....	6
<i>USA RFID Legislation</i> .....	7
Smart cards .....	9
<i>Contact Smart Cards</i> .....	9
<i>Contactless Smart Cards</i> .....	9
Iris Recognition.....	12
Fingerprint Recognition .....	12
<i>Optical</i> .....	13
<i>Ultrasonic</i> .....	13
<i>Capacitance</i> .....	13
<i>Current Applications</i> .....	14
Voice Recognition.....	14

## ***Definition of Biometrics***

According to “The Biometric Consortium”, biometrics:

are automated methods of recognizing a person based on a physiological or behavioral characteristic. Among the features measured are face, fingerprints, hand geometry, handwriting, iris, retinal, vein, and voice. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. As the level of security breaches and transaction fraud increases, the need for highly secure identification and personal verification technologies is becoming apparent. (Biometrics Consortium)

Another definition is that:

Biometrics is the science and technology of measuring and analyzing biological data. In information technology, biometrics refers to technologies that measure and analyze human body characteristics, such as fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements, for authentication purposes.” (Bittype).

Yet another definition defines it as:

Biometrics (ancient Greek: bios = "life", metron = "measure") is the study of automated methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits.

In information technology, biometric authentication refers to technologies that measure and analyze human physical and behavioral characteristics for authentication purposes. Examples of physical characteristics include fingerprints, eye retinas and irises, facial patterns and hand measurements, while examples of mostly behavioral characteristics include signature, gait and typing patterns. Voice is considered a mix of both physical and behavioural characteristics. However, it can be argued that all biometric traits share physical and behavioral aspects. (Wikipedia)

From the few definitions listed a concise definition can be discerned. Biometrics is an emerging technology that includes the study of using methods to analyze human features and behavior in order act to serve as a security and verification device. There are many uses of biometrics’, which include access control and authentication and verification.

## ***Current Types of Biometric Devices***

### RFID’s (Radio Frequency Identification Devices)

*What is RFID?*

RFID stands for Radio Frequency Identification Device. RFID is an automatic biometric authentication device. According to Wikipedia, “An RFID tag is a small object that can be attached to or incorporated into a product, animal, or person.” The actual date that RFID

was first invented is not precisely know, but some say the technology has been around since 1920's, but others say the 1960's. RFID tags were first inserted in animals in order to find lost pets.

### *Types of RFID Devices*

#### 1. Passive

Passive RFID devices have no internal power supply. These types of RFID devices also use backscattering, which is the reflection of the signal to back where it came from. These are cheaper to manufacture and have no battery allowing them to be used as I “disposable” RFID tracking tool. These can contain more than just a unique identity but EEPROM that can store information. According to Wikipedia, the “smallest such devices measured 0.15 mm × 0.15 mm”(Wikipedia). They have an average read distance of 10 cm and cost about 5 cents to make. Some examples of places that use Passive RFID's are Wal-Mart and Target. They also have an unlimited life span, since they do not require an onboard battery to function.

#### 2. Semi-Passive

These RFID's are the same as passive, except they often contain a small battery.

#### 3. Active

Active RFID's are also known as “beacons”. They are used to track objects when they may me moving, or in an area that is not conducive for Radio frequency waves to move freely, such as water and animals, even humans. The average battery life of these sensors is 10 years and an average range of reading of about 300 feet. Currently, the smallest Active RFID's are the size of a coin and sell for a few dollars. The U.S. Department of Defense (DoD) have been using active RFID tags to track packages along the supply chain for about 15 years. These types of tags also use PML (Physical Markup Language).

### *Implantable RFID's*

Currently, many companies offer implantable Radio Frequency Identification (RFID) devices that are used in pets and the human body. RFID is a unique identifier that has many different uses. The use of RFID devices allows for the tracking of items from state to state, and country to country, even the position of humans. VeriChip, a leading company that produces implantable RFID devices even offers the opportunity to be implanted while at night clubs, in other countries. Storage space on the devices can be used to unlock doors, cars, and log in to personal website accounts, e-mail, and personal banking accounts. The implantable RFID devices are being considered for the health care system, as a means to access heath care records and to prevent mix-ups between sperm and ova. RFID devices are a unique way to combine access control and security. These types of devices will continue to evolve and will become a common daily occurrence. Are you ready?

### *RFID Technology in the Industry*

There are many uses of RFID technology in the industry from chipping /tagging clothing to people. Implantable RFID technology has already been successfully used in pets in order to track lost pets. It is now occurring more in humans. A company, CityWatcher.com is requiring employees to get implanted in the bicep in order to get into the company's secure

data center. This is an example of biometrics used for security and authentication where the user is not using a physical attribute to gain access, but rather using a device implanted in them to gain access. Currently the most well know implantable RFID chip manufacturer is VeriChip. VeriChip is the leading company to offer implantable RFID microchip. VeriChip used implantable RFID's and cameras were used by forensic scientists to track the deceased after Hurricane Katrina. There is also information indicating that implantable RFID's are and can be used to fight against the avian flu. "Chipping" as it is called is not confined to a doctor's office. Currently; you can be chipped in other countries at night clubs. According to "Spy Chips" by Katherine Albrecht and Liz McIntyre, RFID's technology has the ability to become quite intrusive and ethically questionable. Another example of a RFID device is Champion Chip, which is used for precise timing of athletic events also they have used them on prisoners to track prisoner movement and in car keys as anti-theft protection. The EZPass system used for paying tolls is also a RFID device as well as Mastercard's Pay Pass.

#### *Current Uses of Implantable RFID Devices*

1. For accessing medical records.
  - a. VeriChip – medical database
    - i. VeriChip has implemented a medical database that can be accessed using a unique identifier that is read off the chip. The unique identifier is then entered into a computer program/database and the patient's medical information can be brought up on the screen. This technology clearly has many drawbacks and advantages. Currently, very few hospitals are adopting this type medical database. However, it can be a lifesaver if someone were to have a very life threatening health problem and could not communicate with the doctors.
  - b. Replacement to medical alert bracelets and tags.
    - i. It is being called a replacement to medical alert bracelets and tags, since a doctor could obtain a patients medical information. Yet, a problem with this is that the doctor must have access to the VeriChip database and the chip reader therefore the first responder could actually treat a person with the wrong type of medicine and make the persons condition worsen.

#### *Current Uses of RFID Devices*

1. Access Control
  - a. Securing areas
    - ii. By using the implantable chip or a card outside the body companies would have the ability to use RFID as a form as authentication and access control to secure areas. Therefore adding to the level of security of the organization.
  - c. Opening doors
    - i. Relates directly to securing areas. If the implantable RFID or another RFID is required for entrance to an area, it can help to ensure that only the authorized users are allowed through a locked door into either a secure or non-secure area. The problem with this is still the

people factor and the need to hold the door as a kindness towards others.

- d. Tracking employee movement.
    - i. Allows for companies to track the movement of not only things in their organization, but their employees as well. This could be used to locate a person during an emergency or further track a person while they are at work to make sure they are doing their jobs and adhering to their expectations.
2. Credit Card Access
    - a. Connect chip to bank account
      - i. Allows one to just pass the card or implanted chip near the reader in order to pay for purchases.

#### *VeriChip – “RFID For People”*

- Applied Digital Solutions produces the VeriChip.
- VeriGuard
  - Controls access using both smart cards and implantable RFID devices.
- VeriMed
  - Used for viewing medical records.

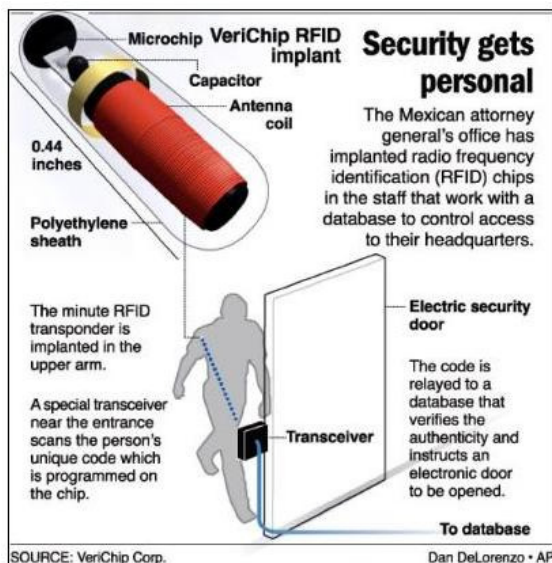
#### *VeriChip – Implantable RFID’s*

- Inserted just below the skin.
- Outpatient procedure
- Uses a dormant microchip to access a number (unique 16 digit number) that is used to access a database with medical information.
- Made of silicon glass, so the body does not reject.
- Approved by FDA in 2004.
- Potential Risks
  - Electrical hazards.
  - MRI incompatibility & severe patient burns.
  - adverse tissue reaction.
  - migration of the implanted.

#### *Problems with RFID’s*

1. Clonability
  - RFID’s are easily cloned.
2. Identity Theft
  - If these are mandated for access control and medical reasons, what stops someone from reading the implantable chips and stealing ones identity.
3. Susceptible to virus attacks.
  - In addition to requiring no authentication, RFID devices also have no program or software implemented that would protect the device from virus attacks. Ex. Buffer Overflow
4. Can silently ID people 25 feet away.
  - Currently, many RFID’s do not have the ability to restrict unauthorized readers from reading the information stored on the chip.

- In “Spy Chips” the authors indicate the ability for one to be able to scan users with a device and see a description of everything they are wearing or even what they are carrying in their purse or briefcase, such as high end technical devices.
5. Outpatient medical procedure.
    - Since the procedure is outpatient, the question arises on whether or not RFID’s would begin to be implanted by about anyone who wants to make money. Also, if they are required will there be places that one can go and get their RFID removed.
  6. There for life.
    - Cannot be easily removed from the body after insertion.
  7. Capability for constant tracking of movement
    - In “Spy Chips” the concern about physical tracking or a person by satellite through the clothes they are wearing, the shows they are wearing or an implantable chip makes many question whether the government could use these tags to track ones every movement, hence an increased idea of “big brother” watching.
  8. Moral & ethical concerns.
    - Wisconsin Governor Jim Doyle signed a law making it illegal to require an individual to be chipped. This law went into affect in May 2006.
    - Some Christians believe that implantable RFID’s are the mark of the beast that is referenced in the *Book of Revelation*.
  9. Privacy concerns.
    - Related directly to ability to track ones movement, scan someone’s clothes or luggage in order to commit crimes.



NO NEED FOR A KEY Sean Darks, chief executive of CityWatcher.com, shows how he unlocks a door Monday in Cincinnati with a VeriChip implant that he had inserted in his right forearm.

Thu Jul 15, 9:33 AM ET

**AP** Associated Press

*USA RFID Legislation*

The following legislation information was obtained from <http://en.wikipedia.org/wiki/RFID>

- California – SB1834
  - Restrict the way businesses and libraries in California use RFID tags attached to consumer products or using an RFID reader that could be used to identify an individual.
  - Defeated by members of the California state assembly on June 25, 2005.
- California - SB768 (Identity Information Protection Act of 2006)
  - Would establish interim protections to apply to RFID tags used both for government mandated forms of identification and also for non-governmental purposes such as individual tracking; it would establish interim civil and criminal penalties for cases in which personal information is collected via RFIDS without proper disclosure and prior consent.
  - Passed by the California Senate with a vote of 30 to 7 on August 31, 2006 (it was already passed by the State Assembly). Now with Governor Arnold Schwarzenegger to veto or sign into law.
- Massachusetts – HB 1447, SB 181
  - Requires labels regarding use and purpose of RFID on consumer products; requires the ability to remove tags; and restricts info on tags to inventory and like purposes.
- Maryland – HB 354
  - Creates a task force to study privacy and other issues related to RFID and report on whether legislation is needed.
  - Failed
- Missouri – SB 128
  - Requires a conspicuous label on consumer packaging with RFID disclosing existence of the tag and that the tag can transmit a unique ID before and after purchase.
- Nevada – AB 264
  - Requires manufacturers, retailers and others to ensure placement of a label regarding existence of RFID on product prior to sale.
- New Hampshire – HB 203
  - Requires written or verbal notice of existence of a tracking device on any product prior to sale.
- New Mexico – HB 215
  - Requires businesses purveying tagged items to post notices on their premises and labels on the products; requires removal or deactivation of tag at point of sale.
- Ohio – SB 349
  - Prohibits an employer from requiring an employee of the employer to insert into the employee's body an RFID tag.
- Rhode Island – H 5929
  - Prohibits state or local government from using RFID to track movement or identity of employees, students or clients or others as a condition of a benefit or service.
- South Dakota – HB 1114
  - Prohibits requiring a person to receive implant of an RFID chip.

- Tennessee – HB 300, SB 699
  - Requires conspicuous labeling of goods containing RFID disclosing existence of RFID and that it can transmit unique information.
- Texas – HB 2953
  - Prohibits school district from requiring student to use an RFID device for identification; requires school to provide alternative method to those who object to RFID.
- Utah – HB 185
  - Amends computer crime law to include RFID.
- Wisconsin – Assembly Bill 291
  - Prohibits anyone, including employers or government agencies, from requiring people to have microchips implanted in them. Violators would face fines of up to \$10,000 per day per offense until the chip is removed.

### ***Smart cards***

Smart cards are another type of biometric device in which a user inserts a credit card like card into a device in order to authenticate the device for use by the user. Smart cards were created and patented in the 1970's. They were first used in 1983 to in French pay phones. In the 1990's smart cards became popular due to SIM cards, which implement their technology. Currently, there are two types of smart cards: contact and contact-less readers.

#### *Contact Smart Cards*

The contact smart cards actually make contact with the reader. They contain a 1/2 inch gold chip which makes contact with the wires in the reader. The ISO/IEC 7816 and ISO/IEC 7810 series of standards define the requirements for contact smart cards. These chips do not contain batteries; all energy is provided by the reader. A current chip system is in affect at Indiana University of PA through the university issued I-card's. The I-card's "smart chip" allows students or parents to load money onto the I-card in order for student to buy snacks and drinks from on campus vending machines and to wash and dry their clothes in the on campus washers and dryers.

#### *Contactless Smart Cards*

Contactless smart cards use RFID technology, in which the chip communicates wireless with reader. The card need only be in close proximity for the card to be read. A common use of contactless smart cards is subway passes. The ISO/IEC 14443 from 2001 defines two types of contactless cards, called "A" and "B". These cards allow for communication from up to 10 cm away. Other proposals have been made for "C", "D", "E" and "F" but have not completed the standardization process. Another standard for contactless smart cards is ISO 15693. This standard allows communication for distances up to 50 cm.

Below is a table of current contactless smart cards

<b>Place</b>	<b>Card</b>	<b>Provider</b>	<b>Introduction</b>
<a href="#">Atlanta, Georgia</a>	<a href="#">Breeze Card</a>	<a href="#">Metropolitan Atlanta Rapid</a>	Dec-05

		<a href="#">Transit Authority</a>	
<a href="#">Beijing</a>	<a href="#">Yikatong card</a>		2003
<a href="#">Brisbane</a>	Translink SmartCard	<a href="#">Translink/Cubic</a>	End of 2006
<a href="#">Colombia</a>	<a href="#">HID Corp</a>	<a href="#">Transmilenio</a>	1995
<a href="#">Boston</a>	<a href="#">Charlie Card</a>	<a href="#">Massachusetts Bay Transportation Authority</a>	2006
<a href="#">Chicago</a>	<a href="#">Chicago Card</a>	<a href="#">Chicago Transit Authority</a>	2002
<a href="#">New Delhi</a>	<a href="#">Delhi Metro Smart Card</a>	<a href="#">Delhi Metro Rail Corporation</a>	2005
<a href="#">Dublin</a>	<a href="#">Luas smartcard</a>	<a href="#">ITS</a>	<a href="#">Mar-05</a>
<a href="#">Gatineau</a>	<a href="#">Passe-Partout PLUS</a>	<a href="#">Société de Transport de l'Outaouais</a>	Announced in 1997, fully implemented in 2004
<a href="#">Guangzhou</a>	<a href="#">Yang Cheng Tong</a>	Yang Cheng Tong Corporation	<a href="#">Dec-01</a>
<a href="#">Guernsey</a>	<a href="#">Multi Journey "Wave &amp; Save"</a>	<a href="#">Island Coachways</a>	Unknown
<a href="#">Hamamatsu</a>	<a href="#">NicePass</a>	<a href="#">Enshu Railway</a>	<a href="#">Oct-04</a>
Hamilton, NZ	<a href="#">BUSIT! Cards</a> [1]	<a href="#">Environment Waikato</a>	Unknown
<a href="#">Hong Kong</a>	<a href="#">Octopus</a>	<a href="#">Octopus Cards Limited</a>	1997
<a href="#">Izmir</a>	<a href="#">Kentkart</a>	<a href="#">Kentkart</a>	1997
<a href="#">Kaohsiung</a>	<a href="#">TaiwanMoney Card</a>	MasterCard, Cathay United Bank, Acer e-Service	<a href="#">Jun-06</a>
<a href="#">Kagoshima</a>	<a href="#">RapiCa</a>	<a href="#">Kagoshima City Transportation Bureau, Nangoku Kotsu, and JR Kyushu Bus</a>	<a href="#">Apr-05</a>
<a href="#">Kanazawa</a>	<a href="#">ICa</a>	<a href="#">Hokuriku Railway</a>	<a href="#">Dec-04</a>
<a href="#">Kraków</a>	<a href="#">Cracow City Card</a>		<a href="#">Oct-05</a>
<a href="#">Lisbon</a>	<a href="#">LisboaViva card</a>	<a href="#">Transport for Lisbon</a>	<a href="#">Nov-01</a>
<a href="#">Lisbon</a>	<a href="#">Lisboa card</a>	<a href="#">Transportation and Culture</a>	<a href="#">May-05</a>
<a href="#">London</a>	<a href="#">Oyster card</a>	<a href="#">Transport for London</a>	<a href="#">Jan-04</a>
<a href="#">Malaysia</a>	<a href="#">Touch 'n Go</a>	Teras Teknologi Sdn Bhd	1997
<a href="#">Matsuyama</a>	<a href="#">IC e-card</a>	<a href="#">Iyo Railway</a>	<a href="#">Oct-05</a>
<a href="#">Melbourne</a>	<a href="#">myki</a>	<a href="#">Kamco</a>	2007
<a href="#">México</a>	Metrobús Card	<a href="#">Mexico City Metrobús</a>	Jun-05
<a href="#">Minneapolis-St. Paul</a>	<a href="#">Go-To card</a>	<a href="#">Metro Transit (Minnesota)</a>	
<a href="#">Moscow</a>	<a href="#">Transport Card</a>	<a href="#">Moscow Metro</a>	September 1 1998
<a href="#">Moscow</a>	<a href="#">Transport Card</a>	<a href="#">Mosgortrans</a>	started on May 12 2001. fully implemented on April 2006
<a href="#">Nagasaki</a>	<a href="#">Nagasaki Smart Card</a>	<a href="#">Nagasaki Prefecture Transportation Bureau and other 5 bus operators</a>	<a href="#">Jan-02</a>

<a href="#">Greater Nagoya</a>	<a href="#">TOICA</a>	<a href="#">JR Central</a>	<a href="#">Nov-06</a>
<a href="#">New York City</a>	<a href="#">MetroCard</a>	<a href="#">Metropolitan Transportation Authority</a>	<a href="#">Dec-03</a>
<a href="#">Nottingham</a>	<a href="#">EasyRider</a>	<a href="#">Nottingham City Transport</a>	<a href="#">Sep-00</a>
<a href="#">The Netherlands</a>	<a href="#">OV-chipkaart</a>	<a href="#">Trans Link Systems</a>	2006 / 2007
<a href="#">Okayama</a>	<a href="#">Hareca</a>	<a href="#">Okayama Electric Tramway, Ryobi Bus, Shimotsui Dentetsu</a>	<a href="#">Oct-06</a>
<a href="#">Osaka-Kobe-Kyoto</a>	<a href="#">ICOCA</a>	<a href="#">JR West</a>	<a href="#">Nov-01</a>
<a href="#">Osaka-Kobe-Kyoto</a>	<a href="#">PiTaPa</a>	<a href="#">Surutto Kansai Association, comprised of various private operators</a>	<a href="#">Oct-04</a>
<a href="#">Oulu</a>	<a href="#">Bus Card</a>	<a href="#">Koskijinjat OY</a>	<a href="#">Jan-92</a>
<a href="#">Paris</a>	<a href="#">Navigo card</a>	<a href="#">STIF</a>	<a href="#">Oct-01</a>
<a href="#">Perth</a>	<a href="#">SmartRider</a>	<a href="#">Transperth and Wayfarer Transit</a>	<a href="#">Apr-06</a>
<a href="#">Petaling Jaya, Malaysia</a>	<a href="#">Sri KDU eWallet</a>	<a href="#">Sekolah Sri KDU</a>	2003
<a href="#">Porto</a>	<a href="#">Andante</a>	<a href="#">Transportes Intermodais do Porto</a>	2002
<a href="#">Saint Petersburg</a>	<a href="#">Contactless Smart Card</a>	<a href="#">Saint Petersburg Metro</a>	<a href="#">2004</a>
<a href="#">San Francisco Bay area</a>	<a href="#">TransLink card</a>	<a href="#">Metropolitan Transportation Commission</a>	testing since 2002
<a href="#">Santiago de Chile</a>	<a href="#">Multivía</a>	<a href="#">Metro de Santiago de Chile</a>	2003
<a href="#">São Paulo</a>	<a href="#">Bilhete Único</a>	<a href="#">Digicon (Architecture; Central System; Security; Devices); and others providers for devices</a>	2004
<a href="#">Seoul</a>	<a href="#">T-Money</a>	<a href="#">Korea Smart Card Co. Ltd.</a>	<a href="#">Jul-04</a>
<a href="#">Shanghai</a>	<a href="#">Shanghai Public Transportation Card</a>		<a href="#">Dec-99</a>
<a href="#">Shenzhen</a>	<a href="#">Shenzhen TransCard</a>	<a href="#">Shenzhen TransCard Corporation</a>	<a href="#">Dec-04</a>
<a href="#">Shizuoka</a>	<a href="#">LuLuCa</a>	<a href="#">Shizuoka Railway and Shizutetsu Just Line</a>	March 2006 (Shizutetsu Just Line), October 2006 (Shizuoka Railway)
<a href="#">Singapore</a>	<a href="#">EZ-Link</a>	<a href="#">EZ-Link Pte Ltd</a>	2001
<a href="#">Sydney</a>	<a href="#">Tcard</a>	<a href="#">NSW Ministry of Transport</a>	<a href="#">2005 (schoolchildren)</a> 2006-2007 (general public)
<a href="#">South Jutland (Sønderjylland)</a>	<a href="#">Elektronisk Klippekort</a>	<a href="#">Sydbus</a>	2001
<a href="#">Taichung</a>	<a href="#">ECard</a>	<a href="#">Taiwan Smart Card Corporation</a>	<a href="#">Aug-04</a>
<a href="#">Taipei</a>	<a href="#">EasyCard</a>	<a href="#">Taipei Smart Card Corporation</a>	<a href="#">Mar-00</a>

<a href="#">Takamatsu</a>	<a href="#">IruCa</a>	<a href="#">Takamatsu-Kotohira Electric Railroad and Kotoden Bus</a>	<a href="#">Feb-05</a>
<a href="#">Tehran</a>	<a href="#">Metro Card (Tehran)</a>	<a href="#">Processing World Co./ASCOM</a>	<a href="#">Implemented on 2002</a>
<a href="#">Thailand</a>	<a href="#">ThaiSmartCard</a>	<a href="#">Thai Smart Card Co.,Ltd.</a>	<a href="#">Dec-05</a>
<a href="#">Greater Tokyo Area</a>	<a href="#">PASMO</a>	PASMO Corporation, associated with various private operators	<a href="#">Mar-07</a>
Greater Tokyo Area, Sendai and Niigata	<a href="#">Suica</a>	JR East, <a href="#">JR Bus Kanto</a> , Saitama New Urban Transit, <a href="#">Sendai Airport Transit</a> , Tokyo Monorail, and Tokyo Waterfront Area Rapid Transit	<a href="#">November 2001 (JR East)</a>
<a href="#">Tokyo</a>	<a href="#">Setamaru</a>	Tokyo Kyuko Electric Railway ( <a href="#">Setagaya Line</a> only)	<a href="#">Jul-02</a>
<a href="#">Toronto</a>	<a href="#">GTA Farecard</a>	<a href="#">GO Transit</a>	2007
<a href="#">Toyama</a>	<a href="#">Passca</a>	<a href="#">Toyama Light Rail (Portram)</a>	<a href="#">Apr-06</a>
<a href="#">Warsaw</a>	<a href="#">Warsaw City Card</a>	ZTM	<a href="#">Oct-01</a>
<a href="#">Washington, D.C.</a>	<a href="#">SmarTrip</a>	<a href="#">Cubic Transportation Systems</a>	1999

Source: [http://en.wikipedia.org/wiki/Smart\\_card](http://en.wikipedia.org/wiki/Smart_card)

#### *Current Issues with Smart Cards*

Real Id Act

Western Hemisphere Travel Initiative PASS Card

[http://www.smartcardalliance.org/about\\_alliance/index.cfm](http://www.smartcardalliance.org/about_alliance/index.cfm)

### ***Iris Recognition***

The use of the iris for means of security and authentication.

### ***Fingerprint Recognition***

Fingerprint recognition is also referred to as fingerprint authentication. Fingerprint recognition is the process of comparing a copy of ones fingerprint to the print currently on the reading device. There are many different types of fingerprint scanners available from door locks to USB devices that can used with a computer.

Fingerprints are compared using key features found on a fingerprint. These key patterns are as follows 1) arch pattern, 2) loop pattern and 3) whorl pattern. What makes fingerprint authentication a unique method from authentication is due to the fact that finger prints cannot be easily removed from the person and no one person has the same fingerprint.

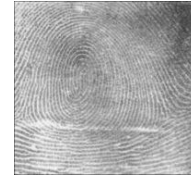
When ones finger is being scanned the current fingerprint is compared to the biometric template. There are three types of fingerprint sensors.



Arch Pattern



Loop Pattern



Whorl Pattern

Images from [http://en.wikipedia.org/wiki/Fingerprint\\_authentication](http://en.wikipedia.org/wiki/Fingerprint_authentication)

### *Optical*

Involves capturing digital image of a fingerprint by using visible light. This sensor can be seen as a digital camera. The sensor is broken into layers. Where the finger is placed on is considered the top layer, or the touch surface. Below the top layer is a layer which lights up the surface of the finger. The light is reflected back from the finger and passes through to an array of solid state pixels (a charge coupled device) which captures the image of the fingerprint.

This sensor will not work correctly if the touch surface is scratched or dirty. This sensor will also not work correctly if the finger is dirty or the fingerprint is no longer very visible on the finger. (wikipedia.com)

### *Ultrasonic*

Uses ultrasonic wave to create visual images of the fingerprint. The waves penetrate the upper layers of the skin. With this type of fingerprint reader the visual image is taken from the dermal layer of the skin, because the dermal layer of skin has the same characteristic pattern of the fingerprint. This type of fingerprint reader is still effective even if the epidermal skin is damaged or unclean. (wikipedia.com)

### *Capacitance*

Uses the idea of capacitance in order to capture the image of the fingerprint.

$$C = \frac{Q}{V}$$

$$C = \epsilon_0 \epsilon_r \frac{A}{d}$$

where

$C$  is the capacitance in [farads](#)

$Q$  is the charge in [coulombs](#)

$V$  is the potential in [volts](#)

$\epsilon_0$  is the [permittivity of free space](#), measured in farad per metre

$\epsilon_r$  is the [dielectric constant](#) of the insulator used

$A$  is the area of each plane electrode, measured in [square metres](#)

$d$  is the separation between the electrodes, measured in [metres](#)

In this method of imaging, the sensor array pixels each act as one plate of a parallel-plate [capacitor](#), the dermal layer (which is electrically [conductive](#)) acts as the other plate, and the non-conductive epidermal layer acts as a dielectric. (wikiperdia.com)

There are two types of capacitance fingerprint readers

1. Passive
2. Active

#### *Current Applications*

Disney uses fingerprint recognition to verify that a person who holds a season pass is that person.

### ***Voice Recognition***

Is a biometric device that requires nothing but one's voice. Voice recognition involves a user speaking into a microphone and a device authenticating a user by the patterns in their voice. It is important to not that voice recognition is not the same as speech recognition, which id the recognition of words for non authentication purposes.

“The various technologies used to process and store voiceprints includes frequency estimation, hidden Markov models, pattern matching algorithms, neural networks, matrix representation and decision trees. Some systems also use "anti-speaker" techniques, such as cohort models, and world models” ([http://en.wikipedia.org/wiki/Speaker\\_recognition](http://en.wikipedia.org/wiki/Speaker_recognition)).

## Resources Used

<http://www.biometrics.org/>  
<http://www.bitpipe.com/tlist/Biometrics.html>  
<http://www.itsc.org.sg/synthesis/2002/biometric.pdf>  
[http://www.cc.gatech.edu/classes/cs6751\\_97\\_winter/Topics/quest-design/](http://www.cc.gatech.edu/classes/cs6751_97_winter/Topics/quest-design/)  
<http://tibs.org/biometrics/>  
<http://biometrics.cse.msu.edu/>  
<http://www.biometrics.dod.mil/>  
<http://www.idlinksystems.com/>  
<http://www.ringdale.com/accesscontrol/>  
[http://www.homesecuritystore.com/ezStore123/DTPProductList.asp?p=2\\_1\\_1\\_1\\_0\\_0\\_191](http://www.homesecuritystore.com/ezStore123/DTPProductList.asp?p=2_1_1_1_0_0_191)  
<http://www.c4ads.org/?gclid=CL-4nfHw5YQCFQQdSAodET5ejw>  
<http://www.networkworld.com/research/biometrics.html>  
[http://www.pcmag.com/encyclopedia\\_term/0,2542,t=biometrics&i=38651,00.asp](http://www.pcmag.com/encyclopedia_term/0,2542,t=biometrics&i=38651,00.asp)  
<http://en.wikipedia.org/wiki/Biometric>  
[http://en.wikipedia.org/wiki/Biometric\\_passport](http://en.wikipedia.org/wiki/Biometric_passport)  
[http://en.wikipedia.org/wiki/Facial\\_recognition\\_system](http://en.wikipedia.org/wiki/Facial_recognition_system)  
<http://en.wikipedia.org/wiki/RFID>  
[http://www.rfidgazette.org/2005/08/implantable\\_rfi.html](http://www.rfidgazette.org/2005/08/implantable_rfi.html)  
<http://www.verichipcorp.com/>  
<http://www.iris-recognition.org/>  
Clarke, V., Teague, G., Siann, G. Gender and computing: Persisting differences, Educational Research, 37, (21).  
[http://www.biometricgroup.com/reports/public/reports\\_iris-scan.html](http://www.biometricgroup.com/reports/public/reports_iris-scan.html)  
<http://www.digitalidworld.com/modules.php?op=modload&name=News&file=article&sid=98>  
Coon, A, Karolewski, M. "Is Big Brother Watching You? Implantable RFID's".  
<http://en.wikipedia.org/wiki/RFID>  
<http://www.wired.com/news/technology/0,1282,61357,00.html>  
<http://www.spychips.com/>  
<http://www.verichipcorp.com/>  
<http://www.techworld.com/mobility/features/index.cfm?featureid=1314&Page=1&pagePos=2>  
[http://www.ischool.washington.edu/tabrooks/163\\_GIS/2004/Images/rfidImplant.jpg](http://www.ischool.washington.edu/tabrooks/163_GIS/2004/Images/rfidImplant.jpg)  
<http://www.cantonrep.com/photos/February2006/14securitychip.jpg>  
<http://www.firstcoastnews.com/tech/news/news-article.aspx?storyid=51694>  
<http://www.msnbc.msn.com/id/6237364/>  
[http://www.rfidgazette.org/2005/08/implantable\\_rfi.html](http://www.rfidgazette.org/2005/08/implantable_rfi.html)  
<http://wistechnology.com/article.php?id=2384>  
<http://www.wired.com/news/privacy/0,1848,68271,00.htm>  
<http://global-elite.org/?q=node/416>  
<http://www.theconservativevoice.com/article/13283.html>  
<http://www.championchip.com/>