Biometrics Technology

Steve Whelan, with contributions from CGAP Staff and echange, LLC

Biometrics technology measures an individual's unique physical or behavioral characteristics, such as fingerprints, facial characteristics, voice pattern, and gait, to recognize and confirm identity. Although the technology is still new, growing awareness of the importance of data security is increasing adoption steadily. For some organizations, low-cost biometric solutions may be more convenient and secure than the passwords and personal identification numbers (PINs) that these institutions currently use to restrict access to financial data.

Who Should Consider Biometrics Technology?

Biometrics technology may be an option for any organization that uses physical cards, documents, passwords, or identification numbers to secure data stored in electronic format on a computer or Automated Teller Machine (ATM). Since biometric applications can be simple—off-the-shelf packages can be installed to restrict staff access to systems or files—the technology is available to almost any computerized microfinance institution (MFI). However, biometrics technology to secure individual client transactions generally requires additional implementation. With these biometric applications, some portable client-held device, such as a Smart Card, is also required to store each client's biometric template. (See the *Smart Cards* article of the CGAP IT Innovation Series.)

How Does Biometrics Technology Work?

The general purpose of all biometric technologies is to capture and store information at an enrollment stage to compare at a later verification stage. In the capture process, software assigns values to a biometric image and stores these values in a template that requires far less storage than the image itself.

During verification, when the client initiates a transaction, the system scans the client's biometric (e.g., voice pattern, retinal image, fingerprint, etc.), matches this scan against the stored template, and approves or rejects it. It sends this result to the business software to either proceed with or halt the client's transaction. A secure audit trail is also recorded for each match attempt.

The False Rejection Rate measures how often an authorized user's biometric data is rejected by the system; and the False Acceptance Rate measures how frequently an unauthorized person gains access to secure resources. Manufacturers use these measures to monitor and determine the effectiveness (security and ease of use) of their systems.

The table below compares biometric technologies and suggests why fingerprint technology is among the most commonly used applications.

Table 1. Comparison of Biometrics

Characteristic	Finger-prints	Hand Geometry	Retina	Iris	Face	Signature	Voice
Ease of Use	High	High	Low	Medium	Medium	High	High
Reasons for Errors	Dryness, dirt, age	Hand injury, age	Glasses	Poor lighting	Lighting, age, glasses, hair	Changing signatures	Noise, colds, weather
Accuracy	High	High	Very High	Very High	High	High	High
User Acceptance	Medium	Medium	Medium	Medium	Medium	Medium	High
Required Security Level	High	Medium	High	Very High	Medium	Medium	Medium
Long-term Stability	High	Medium	High	High	Medium	Medium	Medium

Source: Simon Liu and Mark Silverman, "A Practical Guide to Biometric Security Technology," *IT Professional* (January/February 2001).

Requirements for Biometrics Technology

- Reliable electrical power for card or biometric readers
- Solid processes and adequate staff for managing card systems and enrolling clients
- Software integration between cards, readers, and central MIS

Benefits and Costs of Biometric Technology

Benefits

- Greater security—biometrics link a person to an action.
- Convenience—clients have no identification number or password to remember.
- Local verification—clients hold their identity information (e.g., on a Smart Card), so there is no need to verify identity via a central repository or server.
- Verification is swift and does not require staff.
- User identity is stored safely and is tamper-free.

Costs

The following are indicative costs of a biometric fingerprint system that verifies identity and passes match/no-match results to other software (e.g,. the transaction application). The costs below assume the use of Smart Cards, since these systems furnish the greatest potential and flexibility for MFI applications.

- A Smart Card for each client costs US$ 6–$ 10 per card.
- Software programming routines to develop the reader-MIS interface cost US$ 1,000–$ 1,900.
- A set-up or installation fee to deploy card readers will be charged.
- Basic fingerprint readers run US$ 60–$ 130, or fingerprint/card readers are US$ 100–$ 240.

Some smart card readers come with built-in fingerprint capability to authenticate the bearer of the actual card. This raises the price of the reader but increases

security and eliminates the need to integrate multiple components.

Microfinance Implementations

Few microfinance institutions have opted for biometrics technology, but a case study in Bolivia illustrates its potential.

Prodem FFP (Bolivia)

For Prodem FFP, a combination biometric fingerprint and Smart Cards was appealing for security, ease of use, and cost. With enrollment and reader equipment supplied by Digital Persona, Prodem FFP tasked an in-house development team to write software to integrate the biometric and card software with its MIS. Prodem FFP's configuration uses separate fingerprint and smart card readers, and the MFI is now evaluating combination readers now that low-cost readers with combined fingerprint and smart card technology have been developed.

In general, the equipment has been reliable, affordable, and easy to integrate. Used in conjunction with a smart card system, Prodem FFP's fingerprint verification has reduced fraud, error, and repudiation of transactions. Although the MFI has not conducted a detailed cost-benefit analysis, it has identified a number of benefits.

- ***More staff availability.*** Customers have been satisfied with the speed with which Prodem FFP's biometrics system verifies client identities. Retries due to false rejections have been well within the range of acceptable performance. By combining Smart Cards and biometrics technology, Prodem FFP staff has not had to deal with forgotten PIN numbers or unauthorized use of cards or accounts, so they have more time to provide personal service and advice to clients.

- ***Better customer experience.*** A fingerprint template stored directly on the card during enrollment lets clients access their accounts without remembering passwords or PINs. Once PCs configured with card and fingerprint readers were set up at Prodem FFP offices, clients were authenticated quickly, and transaction times sped up. All of Prodem FFP's 54 offices are equipped with smart card and biometric readers. By the end of 2003, over half will have full ATM capabilities as well. In many cases, customers will be able to conduct transactions without waiting in line for tellers.

Prodem FFP CEO Eduardo Bazoberry considers biometrics with Smart Card to be an excellent tool to deliver better financial services to Prodem's clients. Although Prodem FFP offers only savings, transfers, and loan disbursements through its biometrics and smart card system, it envisions using the system to offer additional products over time.

Lessons for Implementation

Client experience

Positive client experience is critical to successful biometrics implementation. Prodem FFP combined fingerprint technology, Smart Cards, and ATMs to allow its customers to conduct transactions themselves, without waiting in long lines for tellers. This reduces transaction times and eliminates the need for clients to remember PINs or passwords. The biometrics system must also be user-friendly in the way it captures biometric information. Of Prodem FFP's 43,000 clients with smart cards, only two cardholders have been unable to use the system due to the condition of their fingerprints. In these cases, Prodem FFP resorted to traditional passbooks to record their transactions.

Phased implementation

Some MFIs should introduce simpler biometric applications at first to test the pros and cons of a biometric system without incurring great expense. For example, MFIs can easily install off-

the-shelf software packages that include a reader on their computers to restrict staff access to particular systems or client files.

Maintain system security

A biometrics system protects the privacy of the individual because identity templates are not centrally stored or communicated. In the system adopted by Prodem FFP, client templates exist only on the card, so client identity cannot be manipulated, compromised, or misused. If the card is lost or stolen, the client must return to a branch to take another thumb reading in order to be issued a new card. It is a minimal administrative burden relative to the level of security gained.

General guidance

The unique challenges of implementing biometric systems are well documented by the UK Biometrics Working Group.

- All security systems, biometric or otherwise, require time, money, and energy to setup, administer, and maintain properly.
- System throughput rates must be carefully addressed, for both enrollment and operational use.
- Enrollment sessions and training for all users is (almost) always required.
- Although studies show strong acceptance of biometric technology, some users will object to it, so a policy must be developed for this.
- The system integrator should be carefully chosen because hardware/software integration will be the hardest task. Biometric technologies are too complex to plug in and activate immediately.
- System integration may require changes in other pieces of hardware that cannot readily be anticipated.
- It is important to use proven products and stable vendors.
- The implemented biometric system must be more efficient than the alternatives or the use of the biometric will be seen as a mistake.

To Learn More

Biometrics providers

The popularity of fingerprint identification technology has helped drive down the cost of readers and associated software components. Integrators can help speed the deployment of applications, but software packaged with readers is becoming more powerful and easier to use.

The main international suppliers of biometric fingerprint readers include:
AuthenTec, **http://www.authentec.com/**
Digital Persona Inc., **http://www.digitalpersona.com**
SecuGen, **http://www.secugen.com/**
Identix, **http://www.identix.com/**
Gemplus, **http://www.gemplus.com**
Oberthur, **http://www.oberthur.com**
Schlumberger-SEMA, **http://www.slm.com**

CGAP has not reviewed their products nor does it endorse them in any way.

Organizations surveyed

Prodem FFP, Eduardo Bazoberry, **ebazoberry@prodemffp.com.bo,** 591 2 214 7580

Other resources

UK Biometrics Working Group, **http://www.cesg.gov.uk/site/ast/index.cfm?menuSelected=4&displayPage=4**
Biometrics Consortium, **http://www.biometrics.org**
World Resources Institute's *Digital Dividend Project,* **www.digitaldividend.org**