Chapter 2 – ValidateMe! Basics & Management

Everyone knows what a fingerprint is, the natural pattern of ridges and valleys across the pad (or tip) of your finger. The combination of loops, swirls, and whorls are unique to each of your fingers. Like snowflakes, no two fingerprint patterns are alike. Even identical twins have different fingerprints.

So what is biometrics? The word itself is a combination of the Greek words “bio” (meaning “life”) and “metrics” (the science of measuring). Measuring life.

To put it more precisely, biometrics is the science behind measuring a vast variety of physical characteristics that can be used in *verifying* someone's identity. Examples of physical characteristics that are unique to each person include DNA, fingerprints, footprints, palm prints, and retinal patterns.

Today's laptops often come equipped with embedded finger sensors; external readers are also available to plug into your laptop or your desktop via a USB port. Thus, fingerprint biometrics is a convenient and inexpensive means of adding an extra layer of security to protect the sensitive data stored on your computer.

The technology behind fingerprint biometrics involves comparing the ridges and valleys of one fingerprint against those of another. An image of the fingerprint must first be captured, then converted to a digital representation (or bio-template) and stored in a database. This process is known as enrollment.

Subsequent scans of a fingerprint can then be compared against those already stored in the database; if a match occurs, the identity of the fingerprint owner is considered to be authenticated.

ValidateMe! focuses on fingerprint biometrics technology. It allows for the enrollment and management of fingerprint biometrics through the creation and use of multiple biometric templates for each user.

Now that we have an idea of what fingerprint biometrics is, let's take a quick look at what it is not.

Your **ValidateMe!** application does not scan nor store fingerprint images. Rather, it creates a unique encrypted user key from each scan of a fingerprint. Think of the user key as a mathematical description of the finger scan. The

description is accurate enough to ensure that any one finger scan will never be confused with a different finger. Yet, the description is also simple enough to make matching fast and efficient.

A one-to-one algorithm uses a specific unique identifier (such as a username) to determine which person is about to attempt authentication. The algorithm compares the submitted finger scan only against finger scans from that one individual.

What is Enrollment?

The process of associating fingerprints with a specific username to create user credentials. When an individual fingerprint was initially scanned, distinctive features and patterns of that print were converted into a mathematical representation. The resulting biometric template was stored in a central database where it can be retrieved and compared against finger scans to validate an enrolled person's identity.

What is Authentication?

The process of verifying a match between two fingerprints: the one that's just been scanned against one that was previously scanned (enrolled) and is now part of a biometric template contained in the central database. When a match has been made, the just-scanned fingerprint is authenticated. Think of it as fingerprint recognition.