# TECHNICAL WHITE PAPER

## Enterprise Security Architecture for Biometric User Authentication Systems

**Vance Bjorn**
**Chief Technical Officer**
**DigitalPersona Inc.**

## About the Author

### Vance Bjorn

Vance is the CTO of DigitalPersona. He graduated from the California Institute of Technology Electrical Engineering department where he specialized in computation and neural systems (CNS). Mr. Bjorn was a Caltech Merit Scholar and a former employee of Intel Corporation's Neural Network group in Santa Clara, CA. In starting DigitalPersona he went on leave from his studies as a National Department of Defense graduate fellow at the MIT Artificial Intelligence Laboratory.

## The DigitalPersona Technical Advisory Board

### Dr. Yaser S. Abu-Mostafa

Dr. Abu-Mostafa is a Professor of Electrical Engineering and Computer Science and a member of the Computation and Neural Systems faculty at the California Institute of Technology. Dr. Abu-Mostafa received the Clauser Prize for the most original doctoral thesis at Caltech. He received the ASCIT for teaching excellence four times in, 1986,1989, 1991 and 1995 and the Richard P. Feynman prize for excellence in teaching in1996. Dr. Abu-Mostafa has more than 60 publications in the areas of learning theory, neural networks, pattern recognition, information theory, and computational complexity, including two articles in Scientific American.

### Dr. Pietro Perona

Dr. Perona is a Professor of Electrical Engineering at the California Institute of Technology. Dr. Perona is an expert with an extensive number of publications and research papers in the areas of computer and human vision research. He also leads the Computational Vision Group which is engaged on a number of "early vision" research topics at the Caltech Vision Group. Research interests include Recognition, Navigation, Human-Computer interfaces, Texture analysis, Multiresolution image analysis, Diffusions, Perception of shape-from-shading, perception of texture, and Models of early vision.

### Dr. Tomaso Poggio

Dr. Poggio currently holds the Uncas and Helen Whitaker Professorship of Vision Sciences and Biophysics at the Department of Brain and Cognitive Sciences (BCS) at MIT, and is also affiliated with MIT's Artificial Intelligence Laboratory. He has also been Co-Director of MIT's Center for Biological and Computational Learning (CBCL) since 1993. Dr. Poggio's original training was as a theoretical physicist (received a Ph.D. in Theoretical Physics from the University of Genoa in 1970) and his current research focuses primarily on the application of new learning techniques to time series analysis, object recognition, adaptive control and computer graphics.

## I. Introduction

User authentication is the weakest link in the security designs of most networked computing environments. Although a system may utilize 128-bit cryptography for data security, gaining access to use that key is almost certainly via a simple password. Traditional password and access card technology are theoretically very secure. However, in practice, they are expensive and dreadfully unsound when utilized within the corporate environment. Security procedures such as password expiration and complex password generation rules have been shown to backfire by adding cost and reducing security due to strong resistance from most users. Forty percent of help desk calls within security-minded organizations concern forgotten passwords, while many other users post their passwords on their monitors. Inconvenient security procedures impact productivity and encourage dissatisfied users to find ways around the system.

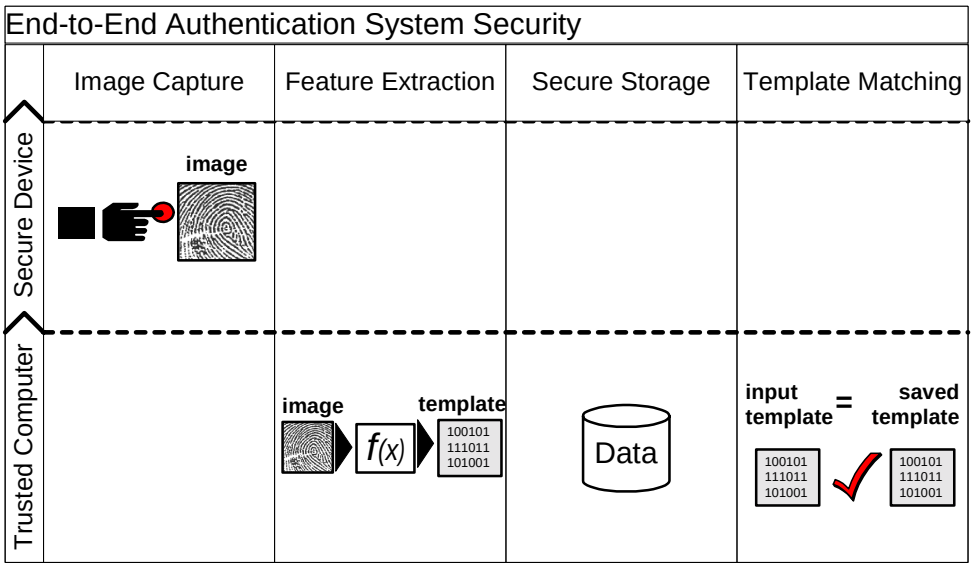
Biometrics technology has recently re-emerged as an ideal answer to this growing problem. Dramatic price-performance improvements in fingerprint recognition technology have enabled many businesses to take advantage of the powerful security and convenience potential inherent in Biometrics-based authentication. As these solutions are evaluated for deployment in many companies, some attention should be made to the security design of the system. Many people erroneously assume that a fingerprint authentication system is inherently secure. This is a scary misconception. It is true that the uniqueness of your fingerprint is such that the chance that it will be falsely recognized as someone else's print is vanishingly small, but this uniqueness says nothing about the end-to-end security of a fingerprint system. This paper will describe the requirements for comprehensive security within a fingerprint authentication system.

## II. Security and Privacy from the Start

Traditional fingerprint systems have not required end-to-end security. In the past, the government hired licensed fingerprint examiners to perform and confirm fingerprint matches. Today, most automated fingerprint (AFIS) systems assume security within the context of a trusted environment that has been installed by trusted people. In this scenario, the end-to-end security of the entire system is not addressed. Fingerprint vendors like Identix operate with the primary assumption that their systems will be installed within the secure environment of a police station or government facility. Using fingerprint authentication in IT or in conjunction with networked applications carries with it vastly different requirements than does a police station. In this vastly challenging setting, numerous scenarios must be addressed. For instance, how can the data coming from the fingerprint sensor be trusted? How does the verifying or authenticating party know that the fingerprint sensor is valid? Was a real finger placed on the sensor? Was fingerprint data tampered with in the client computer? Could fingerprint data be replayed later by someone else? These issues must be solved for biometrics to be a trusted authentication technology for our networked world.

## III. The Required Foundation

In designing the U.are.U® System, we have been guided by a set of principles that define system level security. No one algorithm, patent, or concept can provide the end-to-end security and privacy of a fingerprint authentication system. The entire authentication process or system must have verifiable integrity. Some key security challenges in the authentication process are:




(See, *A Fingerprint Recognition System*, U.S. Pat. No. 6,125,192)

1. *Fingerprint Image Capture.* There are many challenges that must be overcome to ensure and maintain integrity of the whole process. The first decision a system must make is to determine whether what is placed on the sensor is a real finger, and not a rubber stamp or photocopy. (Patent Pending).

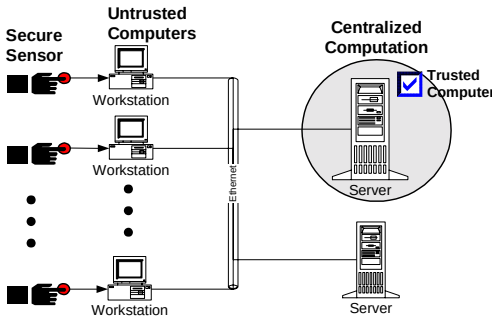
2. *Feature Extraction.* After the sensor has determined it is a real finger then a *complete* and *reliable* set of features from the image of a fingerprint must be extracted. Creating a fingerprint template is beyond the capabilities of a low-cost microcontroller. After a template is created, we must ensure that nobody can insert another set of bits and bytes from a different source into the communications channel to where the fingerprint match will be performed. To prevent this, the fingerprint image must be sent to a fast client host or server.

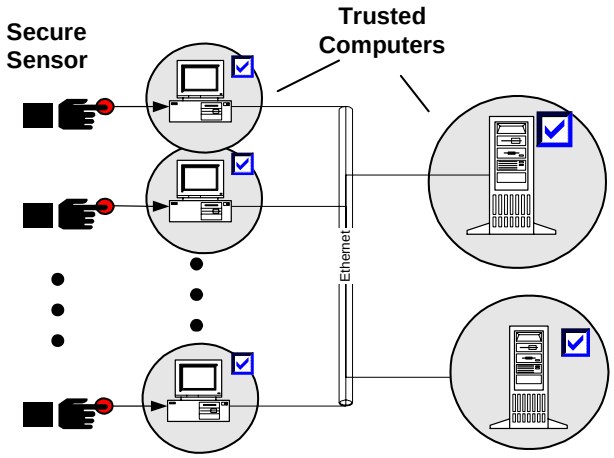
3. *Secure and Trusted Matching Computation.* Even after the fingerprint template data is securely transmitted to where the match is performed, the match process itself could be compromised. The match, or verification process, answers a binary question – does the input fingerprint data match that of User X's stored fingerprint template? The place where the authentication result is to be used – e.g. a file server granting access rights, a smartcard releasing a private key, a PC unlocking its screensaver – must trust this identity determination. The fingerprint

match process must be done in a system that is as secure and trusted as the one requesting the authentication. For example, a Windows NT domain server should not trust a Windows 98 client to perform any aspect of the authentication because it is a much less secure operating system. Nor, should a smartcard trust a PC to give it an unlock command. However, if the user is accessing local resources, say to unlock a screensaver or logon to Windows 98, then a local match (on that PC) is completely appropriate.

4. *Secure and Trusted Credential Storage.* For the same reason that we must ensure that the input fingerprint data has not been tampered with, we must confirm that the stored reference data (credentials) are also secure. Checks must be implemented to determine who has the right to modify the biometric database. The right to perform these operations must be commensurate with their administration rights. If, for instance, any user could just insert their fingerprint data into someone else's record, then they could impersonate anyone on the system. Also, system level issues such as – can the user modify their own record (opening the possibility for them to register someone else's fingerprint into their record) – must be addressed.

5. *Secure Processing in Distributed Systems.* Enterprise environments often require multiple applications and areas where a user can register and use their fingerprint to gain access to services. (See, *Method for Using Fingerprints to Distribute Information Over a Network,* U.S. Pat. No. 6,122,737). It would be costly and time consuming to require users to re-register their fingerprint into several different databases. That is why we provide distributed database support to dramatically decrease the administration burden for the organization. LDAP provides the ideal directory interface for centralizing this data. By using a certificate authority to setup trust relationships between computers we can easily adapt our system to sit on top of any NOS security model. This also facilitates distributing computation among several computers – the feature extraction, matching, and database can be located on different systems. This lends itself to increased scalability and fault tolerance. Providing a secure distributed environment is possible, but only with a well thought-out design. For instance, if we used a single symmetric key, then this key can be compromised on the client and used to impersonate a registration template. By implementing our trust model based on X.509 digital certificates we can easily distribute trust to achieve the benefits outlined above.






## IV. The Technology

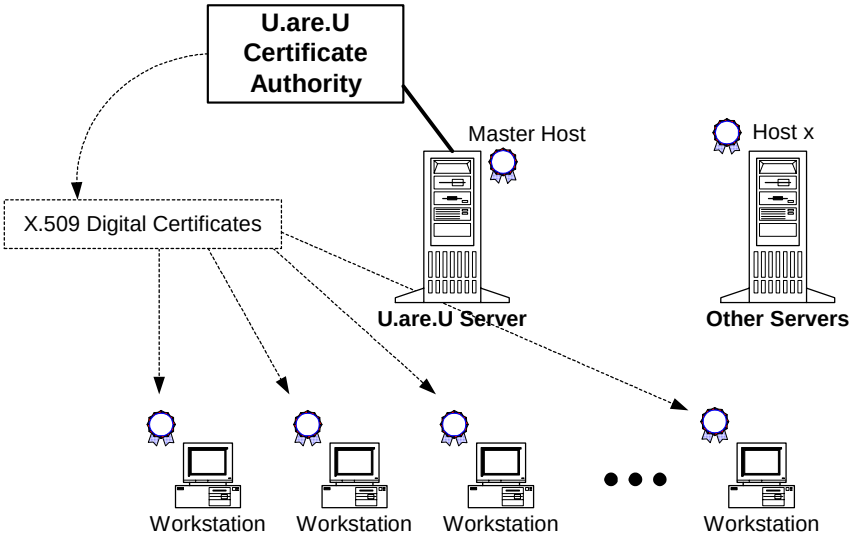
DigitalPersona has developed a biometric authentication architecture that solves these security and privacy issues. Unlike architectures like BAPI, or BioAPI, which were created to address interoperability of biometric devices, our User Authentication Manager (UAM) not only considers interoperability but the critical security issues that arise with biometrics. Security was given the highest priority in the design of our system. U.are.U® is distinguished from any other security solution because security and convenience are combined for both the administrator and the end-users. Strong security with zero administration was our ultimate goal.

*Embedded Certificate Authority*

Each location where fingerprint data is processed, or "host", acts as a certificate authority. When the host is installed onto a computer, it generates a keypair. Any data coming from this host – e.g. a set of fingerprint features, or a fingerprint registration template – is signed by the private key. Other hosts can administratively choose to trust the data coming from other hosts by using the other host's public key. Furthermore, a host can be setup as a "Master Host" and actually certify the public keys of other hosts. Then the trust can be transitive – a host will trust others that are certified as trusted by the "Master Host".

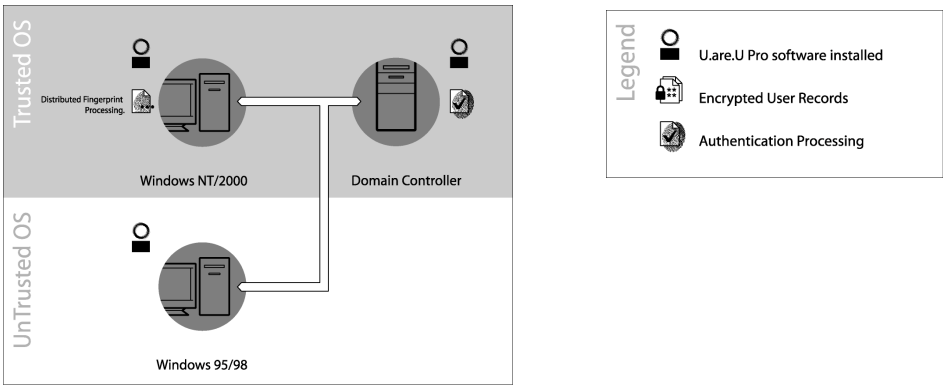
Although there are many CAs commercially available, we implemented our own to achieve *zero administration* for the application of biometric authentication. For instance, within a Windows network, our CA will automatically issue certificates for any hosts on NT workstations that the PDC trusts – note, however, that it will not issue certificates for Windows 98 workstations, which cannot be trusted in any manner.

The use of certificates achieves many goals for us – besides using it to know where a fingerprint template came from, we can use the keypairs to setup a secure channel of communication.

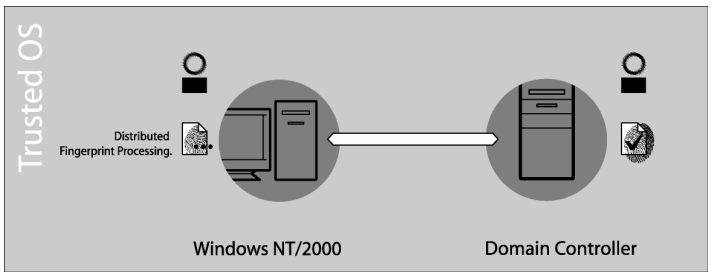



*Trust and the NT Security Architecture*

As mentioned above, our CA and security architecture is designed to complement the Microsoft Security Architecture. U.are.U® will ensure that critical computations are performed on trusted platforms. For instance, if a U.are.U® Sensor is connected to a Windows 98 computer that is authenticating to an NT server, then the local PC merely acts as a pass-thru.

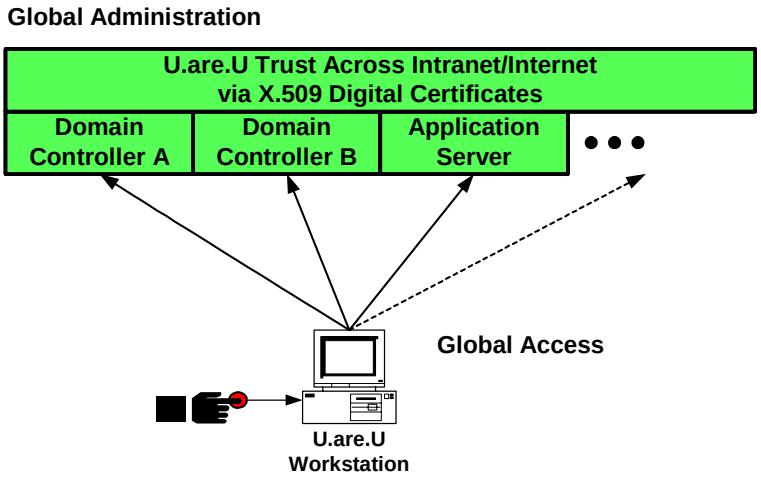



However, if the sensor is connected to an NT workstation that is part of a trusted NT domain, then that local workstation sets up the challenge/response link with the sensor and performs feature extraction on behalf of the authentication server.



*The User Authority*

In addition to using public/private key certificates for secure communication and data integrity, we have developed the concept of the *User Authority*. Before a user authenticates a credential, a keypair is generated for the credentials' unauthenticated state. As the user correctly authenticates the various credentials (fingerprints, passwords, etc.) needed to satisfy the authentication policy for a given service, the public key for each credentials' session is certified by the host that performed the authentication. The session accumulates a certificate (with an expiration time) for each authentication the user performs. The user may have various services to which they must authenticate (e.g. Windows logon, file decryption, an application login, screensaver unlock). Through use of a user authority, each of their authentication credentials are valid up until the expiration time of the certificate. Without this concept, the user would have to repeatedly tap their finger, type in their password, etc, for each authentication request – even if they has just done so only seconds ago. (Of course a lesser design could forgo security to achieve the same convenience for the user)




In addition, by using X.509 certificates we provide an architecture that can extend beyond Microsoft operating systems into the varied environment of an enterprise.

*Secure Link to Sensor*

The sensor is a critical area for security. The integrity of the data transmission must be secure all the way from the sensor to the authentication system. One of the biggest reasons we design our own sensors is to intensify the integrity of this link. Other sensor manufacturers currently do not provide any security to speak of at this level– for the most part a stream of unencrypted data is sent over a cable to the local PC. U.are.U® understands the importance of protecting this link. Our sensors set up a challenge/response, encrypted link with the trusted authentication server. The challenge/response, encrypted link performs two critical security operations: the data

integrity from the sensor is protected by the encryption of the data (nobody can copy in someone else's fingerprint data), and a replay of prior data is protected via the nonce.

*Fake Finger Rejection (Patent Pending)*

Ensuring that our system provides the best fingerprint credential protection is our ultimate mission. Passwords are extremely easy to copy, share, and are prone to dictionary attacks. Fingers are, of course, unique, but are also easily copied using scanners and copiers. Fingerprint images are also left on the surface of the sensor after it is touched. Experts have made elaborate attempts to re-enter latent images with lights, powders, photocopies, and rubber stamps. It is not difficult to make a fake finger to fool one attribute of a real finger – but it is extremely difficult to fool many attributes at the same time. Examples of some attributes of a real finger are temperature, oxygen level of the blood in the finger, translucence, color, impedance/resistance, a 3D ridge structure, among others. As discouraging as this all seems it is possible to ward off these attacks using inexpensive approaches. U.are.U® technology has anticipated this and is designed to counter these threats to security. We incorporate mechanisms to detect some of these attributes and have successfully demonstrated that photocopies and rubber stamp copies are rejected by our system.

Furthermore, our sensor contains a buffer that always keeps an image of the sensor surface. This holds several advantages: 1) it effectively "cleans" the sensor surface because we can subtract out any dirt on the surface, 2) it subtracts out any residue of the fingerprint left from the prior use.

## V. Conclusions

Security can not be taken for granted. Biometric authentication solutions that provide high-tech sensors and input devices without adequate end-to-end security are merely a façade. The U.are.U® Enterprise Security Architecture leads the biometric authentication industry by delivering a comprehensive design that ensures the security of your system while merging reliability, convenience, and simplicity at both the user and administrator level. U.are.U® Biometric Authentication Solutions provide an unprecedented combination of convenience and security that is defining this exciting new era of biometric based security.