Achieving Universal Secure Identity Verification with Convenience and Personal Privacy

A PRIVARIS BUSINESS WHITE PAPER

PRIVARIS®

version 0.2
Aug.18, 2007

WHITE PAPER CONTENT

Introduction

The modern world has an unprecedented need for security. More than ever before, sensitive information, ranging from personal account numbers to government intelligence, is stored in databases that can be accessed via the Internet, cellular phones, and other networks. This information is a target for those who wish to exploit it for illegal purposes. E-commerce, online banking and equity trading are booming, exposing millions of transactions to potential threat; the response to the terrorist attacks of September 11, 2001 has placed much greater emphasis on identity verification; and "identity theft" is now commonplace, reportedly costing businesses almost $48 billion in 2002, and costing consumers over $5 billion the same year[1]. Our modern society needs to better protect both physical facilities and electronic data files containing sensitive information. In contrast to the need for increased security, however, is the need to simplify our increasingly complex world. In fact, complexity is often the key issue hampering the adoption of more rigorous security measures.

Recognizing the need for heightened security, the federal government has instituted a number of mandatory data security regulations. Some of these include:

- The Health Insurance Portability and Accountability Act of 2003 (HIPAA) regulates how health care providers, health care plans, and health care clearinghouses protect, use, and release patient data.
- The Federal Financial Institutions Examination Council issued guidelines in 2005 calling for all U.S. banks to implement two-factor authentication for online banking transactions by the end of 2006. This has encouraged major banks outside the United States – in the United Kingdom and Hong Kong, for example – to similarly adopt a two-factor authentication standard for online transactions.
- The Sarbanes-Oxley Act, passed in the wake of the Enron scandal, mandates that CEOs and CFOs attest to their companies' having proper "internal controls;" the validity of these "internal controls" is directly dependent on the companies' data security, identity management, and identity verification.

Government agencies and private industry have developed security solutions to protect both physical assets and electronic data in order to satisfy these regulations and generally increase security.

In many respects, all security solutions are based on a similar model. The organization must specify the asset to be protected and identify who has permission to access the asset, and the level of privileges that these individuals have with respect to the asset. For example, a particular individual may be permitted to read an electronic file, but not write to it, or he might be able to access a server room, but only during specific hours. The foundation for all of these solutions is identity verification – to positively confirm the individual's identity when they attempt to access an asset. Without positively determining who is attempting to access the asset, it is impossible to determine their associated privileges. Effective identity verification and management is the most significant challenge in the implementation of security solutions for many enterprises.

Federal Trade Commission, *FTC Releases Survey of Identity Theft in U.S. 27.3 Million Victims in Past 5 Years, Billions in Losses for Businesses and Consumers (2003), http://www.ftc.gov/opa/2003/09/idtheft.htm*

Identity verification and multi-factor authentication

The most common security solutions use credentials as a proxy for identity. For example, in a password-based IT security system, individuals are only required to present their password and user name to obtain access to data on the network. The identity of the individual is not actually verified and authenticated to the system; he is permitted access by providing the password – the proxy – that is authenticated to the system. Because the password may be stolen, hacked, or given to an unauthorized person, this approach is not very secure against unauthorized access. This is known as single factor – in this case something you know - authentication.

Multi-factor authentication – the combination of two or more factors - strengthens this approach. This can be accomplished by requiring the individual to provide another credential; such as a proximity card or smart card - something you have - in addition to the password. Generally, as the number of required credentials (factors) increases, the system becomes more secure by virtue of the fact that an intruder must collect all of the required pieces of information in order to gain access. While stronger than single factor authentication, it is easy to see how the password/card approach is still vulnerable to attack. Passwords are easily compromised. Cards can be stolen. Once the password has been discovered, or the card obtained, anyone can use them. Because both the password and proximity or smart cards are proxies for identifying the individual, the weak link in the system is the verifiable connection between the credential and the user.

Biometric technology – the measurement of human characteristics unique to the individual – eliminates this weak link by connecting the credential to the specific user. It provides the strongest possible authentication factor – something you are. Rather than serving as a proxy for identification, biometrics positively verify the identity of the user.

Biometric technology ties the physical characteristics of the specific individual, such as facial features, fingerprints, hand geometry, or irises, to the security system. With fingerprint recognition, the most commonly used biometric technology; an individual's fingerprint is electronically scanned and stored, usually as a template (not an actual image). When the individual wishes to access a resource, the finger is rescanned and digitally compared to the stored fingerprint template to determine a match. Combining fingerprint recognition with our previous example, the individual could be required to present something he knows (the password), something he has (the proximity card), and something he *is* (the fingerprint). Because the biometric factor cannot be stolen or replicated, it is a stronger factor than the others and may be used as a single factor or as part of a multi-factor implementation.

Market adoption

Biometric solutions hold great potential. While widespread adoption is accelerating, it has been slower than anticipated for a combination of reasons. Some biometric technologies are costly, difficult to install and maintain, or non-user friendly. Some companies are deterred from using biometric solutions because they generally require the organization to implement an entirely new security infrastructure. Another significant impediment to widespread acceptance is the security and privacy issues that arise with respect to the protection of biometric information.

Enterprise level security solutions typically include a database associating each individual with his credential (e.g. individual with password, prox card ID, etc) and level of privileges. If a password or card ID database is compromised, passwords can be changed or new cards issued and the privileges associated with the compromised credential cancelled. Those compromised credentials are then void and of no value to the intruder. When the credential is a biometric, the system cannot be so easily changed and the biometric cannot be replaced. If a database stores users' fingerprints and the

database is compromised, there is no way to disassociate those fingerprints from the user. The effectiveness and usability of the biometric system becomes dependent on the organization's ability to protect the stored biometrics.

Individuals are also understandably concerned about nefarious use of their biometrics in the event of compromise. Privacy concerns about something as permanent as a fingerprint must be overcome to gain user acceptance. The security risk of a biometric database and the potential liability to the organization are therefore much greater than a typical credential database.

Making biometrics simple, secure and private

Since its inception in 1999, it has been the mission of Privaris® to solve this problem – to create a security solution based on biometric identity verification that protects the privacy of individuals while eliminating the installation and usability hurdles typically associated with biometrics, and the risks associated with collecting, maintaining and securing a database of biometric information. Privaris' patented plusID™ is that solution.

The plusID is a portable, personal device with a built-in fingerprint sensor and the ability to deliver card IDs, passwords and other access-related credentials wirelessly or via USB.

plusID protects personal privacy and overcomes the other problems mentioned by performing all biometric processing - fingerprint sensing, template encoding and storage, and matching - on the device. The fingerprint template never leaves the device and the need for an external database of biometric information is eliminated.

The plusID is designed to meet the FIPS 140-2 level 3 security standard. It is based on a tamper-resistant secure processor and is built to withstand electronic and physical attack.

Applications

The multifunctional plusID™ provides the capability to use a single device for numerous physical access control and IT access applications. The plusID is a consolidating force as more enterprises seek the benefits of this convergence of physical and logical security.

An application programmer's interface (API) enables development of custom applications for the plusID. With a far greater amount of user space, the plusID allows the incorporation of applications that are beyond what normal smart cards can provide.

Compatibility with existing security infrastructure

The plusID uses multiple wireless interfaces and USB to communicate with proximity and smart card readers, PCs, networks, and other security infrastructure. Different plusID™ models offer various combinations of:

- 125 kHz RFID (proximity cards)
- 13.56 MHz RF (contactless smart cards - supporting ISO 14443 A and B, ISO 15693, and NFC)
- ISO 7816 & CCID compliant − compatible with standard Microsoft® Windows smart card infrastructure for computer logon
- Bluetooth™
- IEEE 802.15.4 (for long range applications such as gate access)
- one-time password capability (displayed via LCD and delivered wirelessly or over USB)

plusID is compatible with more than 85% of the existing installed base of proximity readers in the U.S. (HID, Indala, Kantech and CASI), enabling users to move to biometrically assured access without installing new equipment or replacing existing systems. This also means that plusID can be phased in incrementally, allowing for a mixed population of biometric devices and proximity cards for different areas of a facility. With the ability to store up to four different proximity card IDs, for readers from different manufacturers, plusID eliminates the need for multiple proximity cards for different facilities.

The device also provides a standard 7816 smart card interface and supports the applicable ISO standards for contactless smart cards. Support for HID *iCLASS* is under development.

The plusID model that uses the IEEE standard 802.15.4 interface is ideal for applications requiring biometric authentication and subsequent long range transmission (up to 100 meters) of credentials. With functionality from within moving vehicles it is particularly well suited for facility gate implementations.

The same device also provides logical access control for securing PC's and networks. The plusID can provide logon credentials to PCs, networks, websites, and software applications over Bluetooth™, 13.56MHz, or USB. Several models also feature an LCD and one-time password (OTP) functionality.

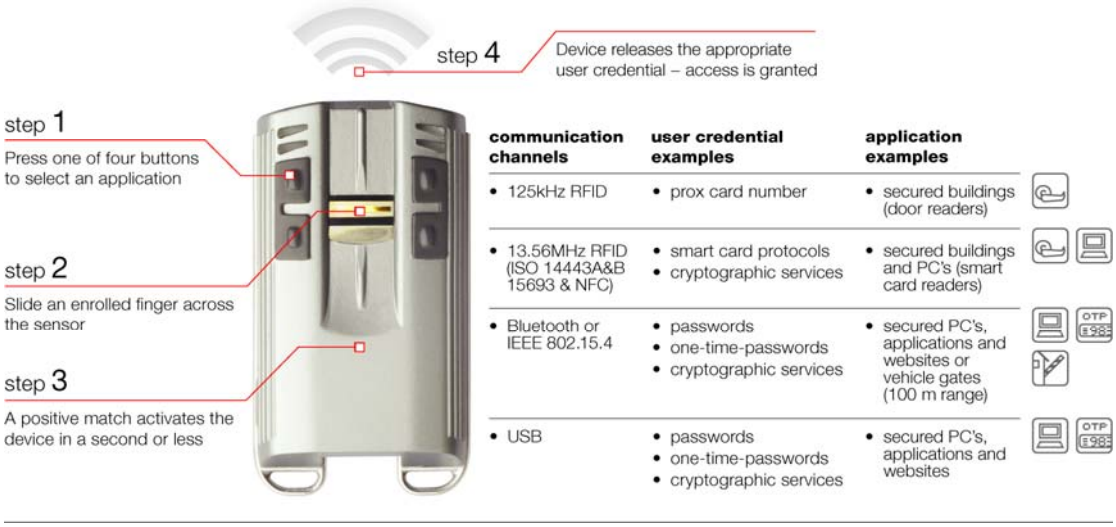
The device API supports the development of a wide range of custom applications, such as using the device to store and present personal credentials such as passports, military ID cards, and driver licenses. It can also support the delivery of payment information for credit card or other types of transactions.

plusID is a cryptographic service provider. The device supports industry standard encryption algorithms including AES 256, RSA keys up to 4096 bits, and SHA 256 hashing algorithms. It can also deliver x509 certificates and perform digital signature operations.

Using the device

The plusID device is issued to individuals in an organization in the same manner as a proximity card or a contactless smartcard, but adds biometric verification capabilities. Device issuance takes approximately two minutes and consists of 1) the user enrolling one or more fingerprints via the device's built-in fingerprint sensor, and 2) the issuing authority downloading card IDs, passwords, or other credentials to the device. It is then ready for use. The average verification time during regular device usage is a second or less.

Diagram 1: The plusID device is convenient and simple to use:



plusID from Privaris is a powerful solution to today's increased security needs, working across multiple applications wherever reliable identity verification is required. The plusID device makes biometric security convenient enough to be a part of everyday life, while ensuring that its user's privacy is protected.

About Privaris

Privaris Inc. focuses its technology expertise on the intersection of high security biometric applications and an individual's right to personal privacy. Privaris products authenticate the identity of an individual prior to that individual being granted access to facilities, resources, services, and transactions. Privaris Inc. is a privately-held Delaware corporation with its headquarters in Charlottesville, Virginia.

Authorized reseller

PRIVARIS®

Security with personal privacy