

About Improved Electronic Access Control using PassFree

The PassFree improved electronic access control system will enable customers to leverage public-key infrastructure (PKI) wherever they are and not just at their work desk.

The practical applications for PKI are many, and therefore the total opportunities for this invention across several markets are very exciting.

PKI is a means to exchange information securely over insecure networks by providing certainty that the information has not been altered en route, certainty that the information was really sent by the undersigned, and certainty that only the intended recipient can read the information. The certainty is delivered by a mathematical technique called public key cryptography.

There are many personal and enterprise applications based on PKI, but the vast majority of these are not portable. The user must be at his or her work desk in order to use the private cryptography keys that enable the applications. In addition, there are more potential applications for PKI that have not yet been realized because of the immobility of the private keys.

The design of the PassFree improved electronic access control system is versatile and will allow PassFree to be used in many applications. Furthermore, it has advantages over traditional lock and key systems, over modern identification systems such as driving licenses and membership cards, over modern electronic commerce systems such as credit cards and quick-pass cards, and over biometric access control systems using biometric databases.

Crimes of identity theft are made possible by reliance on insecure information such as a social security number and names and birthdays of relatives to establish trust. Biometric access control currently relies on storing the biometric data in a central database, which is itself vulnerable to compromise. Identity theft is also possible by photographing the information on a victim's license or credit card during use and using the photographed information later to obtain more information about the victim. In these cases, a person can be made victim by use of what is essentially public information.

Modern physical access control systems rely on personal identification cards such as licenses, credit cards, and smart cards, which must come in contact with a reader not owned by the user but which accesses all the sensitive information on the user's key card. The user must also carry a separate key card for every application. Furthermore, smart cards that use PIN and/or fingerprint authentication depend on separate hardware to read the user's PIN and/or fingerprint and then compare it to the data on the smart card. This method is susceptible to a man-in-the-middle attack wherein the reader is replaced with a Trojan that acts like a normal reader but secretly records the PIN and/or fingerprint data of the user.

Even though modern cryptographic authentication mechanisms have secured the transfer of information, a large number of merchants rely on entering information such as name, credit card number, and/or social security number, all of which are vulnerable to identity theft, because a practical way for a user to carry and use his or her own private cryptographic key had not yet been invented - until now.

PassFree is the next generation of access control and it is going to revolutionize the way people interact with security systems.

Cheyenne Software, Inc. is developing three product lines for PKI applications: access control devices (locks), corresponding keys, and Internet services.

All products communicate using industry standard protocols.

In addition, the company is working on a web browser plugin which facilitates communication between a customer's personal computer access control device - and therefore the customer's key device - and any website employing public key infrastructure (PKI) for access control.

The key product line allows people to access any of the locks mentioned above and consists of software for smartphones such as the iPhone, Blackberry, Android, and others, taking advantage of their computing power and built-in bluetooth capabilities to communicate with all of the lock models, an iPod-style device to act as a dedicated key device, a passport key device targeted to the US Government, and an aural key device for the blind.

The Kensington USB Bluetooth Adapter costs only \$29.99 and adds bluetooth capability to any computer with a USB port. That device can be purchased separately by users not having bluetooth already installed, and other products like container locks and door locks can integrate something like it (wholesale) internally. That allows customers to easily add PassFree locks to any system by installing PassFree software and an inexpensive USB-Bluetooth adapter.

For more information about improved electronic access control using PassFree, contact:

Cheyenne Software, Inc.
(800) 935-9637
someone@mypassfree.com