

Applying BIOPASSWORD® Technology

The keystroke biometric technology in BIOPASSWORD® has a number of practical identification and authentication applications.

Banking Security

Banking security functions such as electronic fund transfers, ATM security, e-commerce, check cashing, credit card transactions, etc. are a natural fit for this software-only biometric. In each case, secure transactions are conducted over heterogeneous, often decentralized, business systems. Establishing the identity of the person authorizing the transaction is paramount to protecting the integrity of the accounts involved.

The keystroke biometric can be cost-effectively layered over legacy authentication mechanisms without changing the underlying business rules involved in the process. The individual businesses involved in the transaction need not abandon their existing policies. With the biometric software in place, they can realize an order-of-magnitude greater security at a fraction of the cost of other similar-performing biometrics.

Physical Access Control

Physical access control systems, such as airport access control, sensitive zone access control, defense, etc. can be augmented with the keystroke biometric. The firmware in these systems can be upgraded to support the BIOPASSWORD® technology. Multiple biometric authentication devices, such as fingerprint readers and facial geometry scanners, can be combined with a standard keyboard to provide the tightest access control possible.

Keystroke biometrics may also be employed in a stand-alone configuration at a lower cost in certain "low-security" areas. Here, the BIOPASSWORD® technology is less intrusive than other physical biometrics and simpler to maintain.

Customs and Immigration

Customs and immigration agencies may also benefit from this unique biometric. Passport control, authentication of visa, etc. are natural for the keystroke technology. BIOPASSWORD® enrollment adds very little to the already lengthy application process in these agencies. Tight budgets make hardware-based biometric authentication cost-prohibitive, giving BIOPASSWORD® an edge where financial resources are scarce.

Voter Identity

Voter identity systems could be built with the BIOPASSWORD® technology that would not allow the voter to access the machine without automatic positive identification of the voter against his or her voter registration record.

Telecommunications

Cellular access control is a nice fit for the keystroke biometric. As wireless services blur the line between voice, data, and electronic commerce, the need to secure digital mobile devices beyond simple encryption will increase attractiveness of the BIOPASSWORD® technology. Future wireless devices will protect consumers from fraud due to theft by authenticating users as well as pin numbers and passwords.