MAGTEK®
SECURITY FROM THE INSIDE

ExpressCard 1000, 2000, and 3000

Device Security Policy

ExpressCard 1000

ExpressCard 2000

ExpressCard 3000

About MagTek

MagTek is a leading provider of electronic transaction security. As a manufacturer of card and PIN personalization equipment, MagTek is responsible to secure its products throughout their entire life-cycle. This includes the manufacturing, delivery, activation, key management, implementation, on-going use, and final disposition of its personalization devices.

ExpressCard 1000, 2000, and 3000 (ExpressCard) make Debit, Credit, ATM and Gift cards immediately. Nearly all the financial transaction cards produced by these machines are equivalent to legal currency that can be used throughout the world. In cooperation with the Card Organizations and the US Secret Service, MagTek honors its obligation to the industry and the public at large to ensure that its machines are only used by responsible, authorized parties and to minimize any consequential damage that may result from the theft or unauthorized use of the products.

Credit card service bureaus have traditionally provided card personalization services from controlled, secure and restricted environments. Consider that ExpressCard is a portable service bureau, requiring comparable security measures. Guidelines established by Visa and MasterCard, require that card personalization devices must ship in a deactivated state requiring the financial institution to work in concert with the manufacturer to enable the machine for card production. ExpressCard uses a Digital Certificate - Device Authentication method that enables the machine for first use and provides on-going controlled activation. This method ensures that if the device is reported stolen or falls into the hands of an unauthorized user, it can be automatically deactivated, thus minimizing potential damage to the payment industry, reducing the card issuer's exposure to fraud and limiting its liability. This service to our customers, provided at no charge by MagTek, does not view, gather or store any proprietary user information or cardholder data. It is a responsible, cooperative approach to secure, distributed card issuance.

MagTek also recognizes the threat posed by creative, brazen, organized criminal enterprise. They steal cardholder data, and copy or create financial transaction cards to commit Identity Theft and Payment Card Fraud on an international scale. In view of the growing need for stronger security to thwart criminal enterprise, it is incumbent on manufacturers, financial institutions and card associations to create, implement and maintain a secure infrastructure. Only then can we defeat such motivated, highly skilled and well-funded lawbreakers. In addition to honoring card association rules, and PCI DSS compliance MagTek has made a commitment to protect the interests of the industry it serves, and has taken a strong leadership role in this security effort.

We welcome and rely on your unwavering and continued support.

Authentication Process

The authentication process is a process whereby ExpressCard devices send an encrypted challenge for device authentication to MagTek's authentication web service. No cardholder data is ever sent during the authentication process.

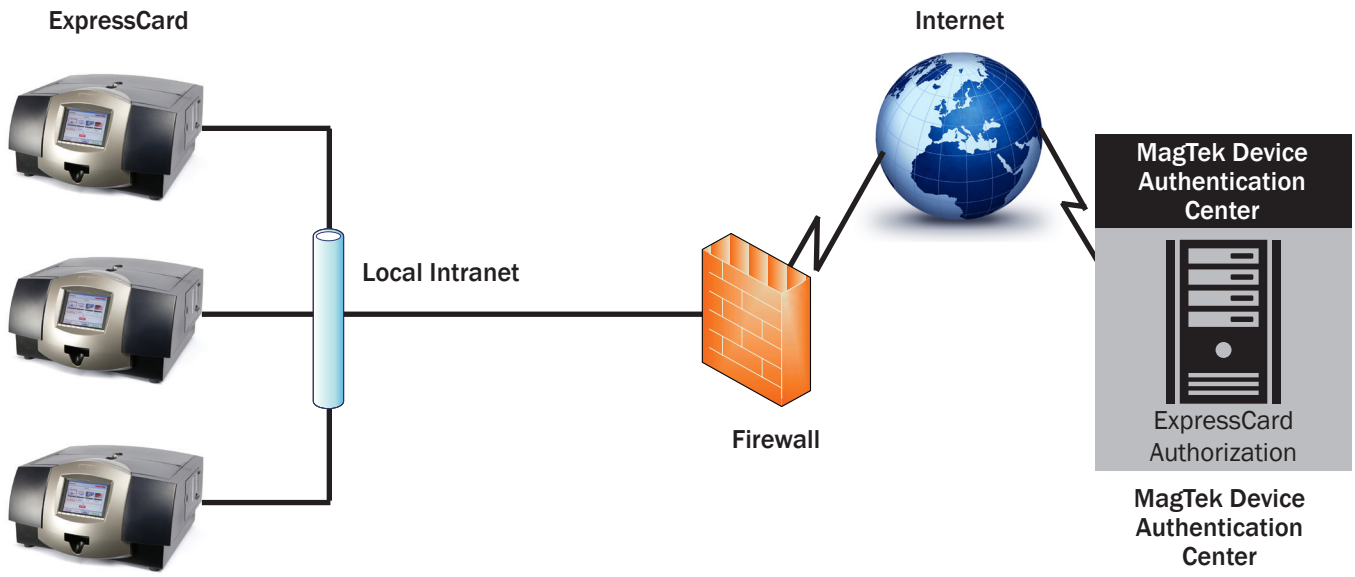
1. Retrieve an Encrypted challenge from the ExpressCard.
2. Retrieve the Chip ID From the ExpressCard.
3. Call MagTek Authorization Web Service with ChipID and Encrypted Challenge (only MagTek can validate the Encrypted Challenge).
4. If the Authorization is successful, "Device Options and Hours to Live" are sent from the web service to the ExpressCard.
5. If Authorization is unsuccessful, "Device Options and Hours to Live" are not sent from the web service to the ExpressCard.

There are two methods of enabling ExpressCard. See reverse for further details.

Questions on this policy are welcome and will be addressed personally by Annmarie D. Hart, the CEO and President of MagTek, Inc. She may be contacted at Mimi.Hart@MagTek.com.

Option #1

In the first method, ExpressCard generates an encrypted challenge and communicates directly to the MagTek Device Authentication Center (MDAC) using an TLS connection. Once ExpressCard and the MDAC have been mutually authenticated, a new digital certificate is transmitted to ExpressCard, enabling the machine to operate for a predetermined period of time, determined by the customer. It is usually set for seven days. Only responses to requests from ExpressCard will be allowed through the firewall. This prevents unauthorized access to ExpressCard, i.e. processing of card(s), to be initiated from an outside source.



Option #2

The second method utilizes the same process. However, a gateway on the financial institution's network provides the channel by which the request for and the delivery of the Digital Certificate is provisioned. Use of the gateway affords financial institutions the opportunity to monitor the traffic to and from the MDAC and avoids the need for direct communication with ExpressCard. Only responses to requests from the proxy server will be allowed back through the firewall. This prevents unauthorized access to ExpressCard, i.e. processing of card(s), to be initiated from an outside source. Additionally, with a proxy server inserted in between ExpressCard, a level of obfuscation is achieved as the local IP address of the individual ExpressCard is known only to the proxy server. This can be locked down by IP address.