



GORE™ Secure PCMCIA Card

Protect Your Crypto Keys, Critical Program Information, or Intellectual Property From Physical Hackers

Electronic modules often store highly sensitive information. Communication devices store cryptographic keys and software waveforms, handhelds can store passwords and records, and embedded systems maintain sensitive algorithms in memory. These devices can easily fall into the wrong hands.

Attackers can gain access to your information in many ways. Once inside, information stored in solid state memory can be read even if the device is inoperable. A proven means of defense against these attacks is volume protection.

A GORE™ Tamper Respondent Envelope can surround and protect your electronic module. Acting as an anti-tamper sensor, this specialized envelope is designed to detect any means of entry into the module. With such protection, the attacker comes up empty as the module automatically erases the target of his attack.

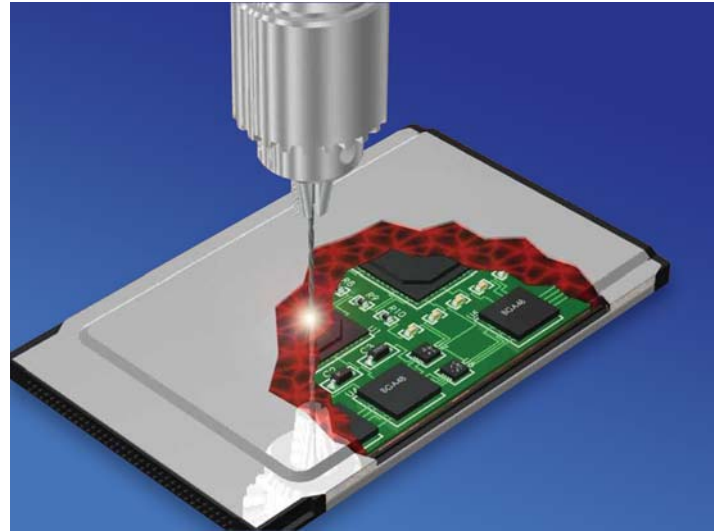
PRODUCT SUMMARY

The GORE™ Secure PCMCIA Card is another high security offering from a broad range of unique tamper respondent sensors and technology. Gore offers multiple solutions to secure a PCMCIA card format.

The GORE™ Secure PCMCIA Card is targeted to meet the requirements of FIPS 140-2, Level 4, DoD, NSA Type 1, and CESSG Enhanced Grade security.

GORE™ Tamper Respondent Technology offers secure, yet easy-to-adopt solutions for volume tamper protection. The GORE™ Secure PCMCIA Card detects physical intrusions by sensing attempts to open, remove, or penetrate the envelope surrounding the PCMCIA card. The application of the GORE™ Tamper Respondent Sensor is designed to provide complete coverage around the board with no direct openings at any corner or overlap. Detection typically triggers erasure of critical security information such as cryptographic keys or sensitive algorithms.

The sensor is extremely low power and, being non-metallic, is impossible to analyze by X-ray. It is designed to detect penetration by drills and probes as well as by erosive and chemical attacks.

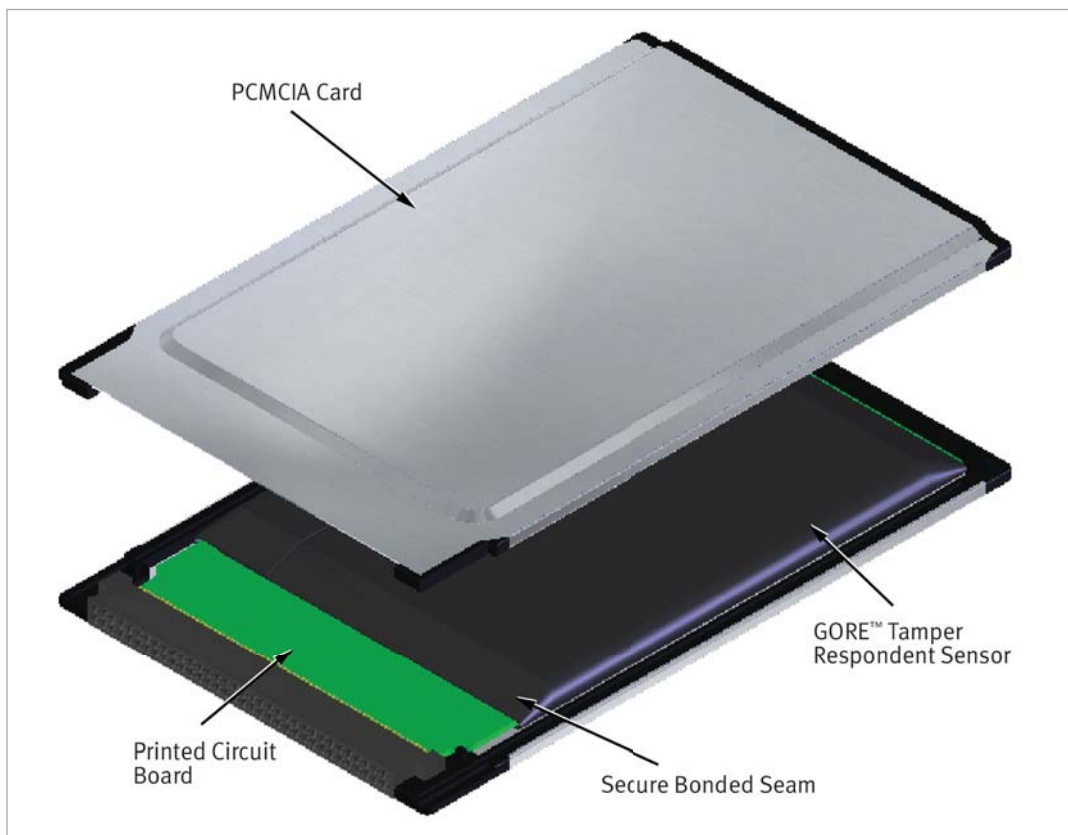


FEATURES AND BENEFITS

- Provides anti-tamper volume protection in a convenient form factor
- Generic offering protects a PCMCIA card—Other sizes available
- Enclosure acts as a tamper sensor that enables zeroization of critical keys or information stored within the protected volume
- Attempted penetration (cutting, drilling) or case separation causes detectable permanent change in electrical state
- All-polymer sensor construction precludes X-ray analysis by an attacker
- Targeted at FIPS 140-2, Level 4, DoD, NSA Type 1 security and CESSG Enhanced Grade security
- Easy to monitor with low power consumption
- OEM needs only simple design rules
- From the only commercial supplier of protection of secure electronics having many independent certifications



GORE™ Secure PCMCIA Card



APPLICATIONS

- High security cryptocards and tokens
- Highly secure communications (COMSEC)
- PCMCIA Hardware Security Modules (HSMs)
- Key management cards
- PCMCIA secure storage cards
- Any sensitive electronic modules in a similar form factor (e.g., ExpressCard)

GORE and designs are trademarks of W. L. Gore & Associates, Inc. ©2007 W. L. Gore & Associates, Inc.

W. L. GORE & ASSOCIATES, INC.
402 Viewe's Way • Elkton, MD 21921 • USA
Phone: 1.800.445.4673 • Phone: 1.302.292.5100
E-mail: electronics.usa@wlgore.com

gore.com

W. L. GORE & ASSOCIATES (U.K.), LTD.
Mariner Drive • Dundee Technology Park
Dundee DD2 1JA SCOTLAND
Phone: 44.1382.561551

