

**Entrust**<sup>®</sup> Securing Digital Identities & Information



**Securing Your  
Digital Life**

***Protecting Identities and Information***

How to tackle the toughest requirements of the PCI Data Security Standard

October 2006

Entrust is a registered trademark of Entrust, Inc. in the United States and certain other countries. Entrust is a registered trademark of Entrust Limited in Canada. All other company and product names are trademarks or registered trademarks of their respective owners. The material provided in this document is for information purposes only. It is not intended to be advice. You should not act or abstain from acting based upon such information without first consulting a professional. ENTRUST DOES NOT WARRANT THE QUALITY, ACCURACY OR COMPLETENESS OF THE INFORMATION CONTAINED IN THIS ARTICLE. SUCH INFORMATION IS PROVIDED "AS IS" WITHOUT ANY REPRESENTATIONS AND/OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, BY USAGE OF TRADE, OR OTHERWISE, AND ENTRUST SPECIFICALLY DISCLAIMS ANY AND ALL REPRESENTATIONS, AND/OR WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT, OR FITNESS FOR A SPECIFIC PURPOSE.

© Copyright 2006 Entrust. All rights reserved.

## Table of Contents

<b>Introduction</b> .....	<b>3</b>
<b>Protecting Identities, Protecting Information</b> .....	<b>4</b>
Protecting Information .....	5
Protecting Identities.....	7
<b>About Authentication</b> .....	<b>8</b>
<b>Entrust Expertise</b> .....	<b>8</b>
<b>Conclusion</b> .....	<b>8</b>
<b>About Entrust</b> .....	<b>9</b>

## Introduction

Brand damage, lost customers, missed revenue targets; the impacts of a breach are well known to organizations that collect, store or process credit card information. Improving the security of critical cardholder information has to be a priority for organizations today, because the potential damage of a breach can be paralyzing. With each having different security requirements, credit card companies have debated how best to protect cardholder data, and the result has been considerable confusion among merchants and processors about which security standards to follow.

In response to member, merchant and service provider feedback on the need for a single approach to stronger information security for all card brands, credit card companies collaborated to create the common industry security requirements known as the Payment Card Industry (PCI) Data Security Standard. Compliance with the PCI Data Security Standard is required for all merchants or service providers that store, process, or transmit cardholder data. The standard consists of 12 detailed requirements that are organized into six categories as follows:

<b>Build and Maintain a Secure Network</b>	
<b>Requirement 1:</b>	Install and maintain a firewall configuration to protect data
<b>Requirement 2:</b>	Do not use vendor-supplied defaults for system passwords and other security parameters
<b>Protect Cardholder Data</b>	
<b>Requirement 3:</b>	Protect stored data
<b>Requirement 4:</b>	Encrypt transmission of cardholder data and sensitive information across public networks
<b>Maintain a Vulnerability Management Program</b>	
<b>Requirement 5:</b>	Use and regularly update anti-virus software
<b>Requirement 6:</b>	Develop and maintain secure systems and applications
<b>Implement Strong Access Control Measures</b>	
<b>Requirement 7:</b>	Restrict access to data by business need-to-know
<b>Requirement 8:</b>	Assign a unique ID to each person with computer access
<b>Requirement 9:</b>	Restrict physical access to cardholder data
<b>Regularly Monitor and Test Networks</b>	
<b>Requirement 10:</b>	Track and monitor all access to network resources and cardholder data
<b>Requirement 11:</b>	Regularly test security systems and processes
<b>Maintain an Information Security Policy</b>	
<b>Requirement 12:</b>	Maintain a policy that addresses information security

Today, organizations want to help prevent damaging their brand or goodwill by an information breach and also want to minimize the possibility of penalties for non-compliance with the PCI

standard. Formulating a plan to achieve PCI compliance requires insight into many complex systems and processes, and a vision of the requirements not only as standalone pieces of an organization's security solution, but as a whole security policy and infrastructure.

## Protecting Identities, Protecting Information

At first glance, achieving PCI compliance for all 12 requirements may seem like a daunting task. Many technology vendors have entered the market claiming to solve PCI compliance issues, which has added to the confusion. However, when we break it down in to specific action plans and examine the common issues that span the PCI requirements, the process can become quite manageable. Some of the requirements are procedural and require the creation and implementation of policies. Often small changes are all that is needed, such as discontinuing the use of default passwords. The measures specified in other requirements are likely already in place: firewalls and virus scanning are critical components of most infrastructures today and although small changes to these systems may be needed, organizations are generally well on their way in addressing the requirements.

It is important to note that compliance cannot be achieved by any single vendor, any single process or any single product. And—because regular scanning and annual assessments are required, the process cannot be approached as a one-time project. Maintaining PCI compliance is an ongoing process that may require the implementation of several new processes and new security solutions over a period of time.

While no one product or process can solve all the requirements, there are some solutions that can span multiple PCI requirements. Consider that there are two main issues central to many of the requirements; *protecting identities and protecting information*. Seen this way, the 12 requirements can be organized more simply as follows:

### Protecting Information

Requirement 3:	Protect Stored Data
Requirement 4:	Encrypt transmission of cardholder and sensitive information across public networks
Requirement 6:	Develop and maintain secure systems and applications

### Protecting Identities

Requirement 7:	Restrict access to data by business need-to-know
Requirement 8:	Assign a unique ID to each person with computer access

These central issues can be used to develop an action plan that can help an organization to make decisions, implement policy changes and authorize purchases that can be leveraged across other security requirements. Entrust's suite of security solutions provide some of the most complete capabilities available to meet PCI requirements. Protecting identities and information has been the cornerstone of Entrust solutions for over 10 years.

## Protecting Information

The PCI standard was established to protect cardholder data, and at the heart of this is protecting information. Whether stored or being transmitted, all critical information must be protected to ensure cardholder data is not compromised. Requirements three, four and six detail the critical areas of protecting information.

Whether protecting information in storage or while in transit, the PCI requirements point to **encryption** as the only acceptable method of protecting information. Requirement six takes this protection of information a step further by requiring systems and applications to be built securely using standard best practices and integrating security functions into the core of the applications. The guidelines for the protection of information are sweeping and introduce the need for a common set of tools to manage security that crosses applications, systems and processes.

### **Requirement 3: Protect Stored Data**

*Encryption is the ultimate protection mechanism because even if someone breaks through all other protection mechanisms and gains access to encrypted data, they will not be able to read the data without further breaking the encryption. This is an illustration of the defense in depth principle.*

*PCI Data Security Standard*

Many of Entrust's security solutions are built upon standards-based public key technology and allow data in any organization to be quickly and easily encrypted using your choice of security products. **Entrust Intelligence** products can help protect information by encrypting data stored just about anywhere including on a server, a laptop or a mobile device or even within custom applications through the use of Entrust's powerful cryptography and content analysis toolkits.

### **Requirement 4: Encrypt transmission of cardholder and sensitive information across public networks**

*Sensitive information must be encrypted during transmission over the Internet, because it is easy and common for a hacker to intercept and/or divert data while in transit.*

*PCI Data Security Standard*

There are two important aspects to this requirement. The first is that strong encryption should be used to protect information as it is transmitted over public networks and the second speaks to the encryption of email, specifically.

**Entrust Authority Toolkits** can be used to integrate security into applications that need to encrypt data transmissions over public networks via SSL or TLS.

The more difficult part of this requirement is the encryption of email. For many organizations, changing their policies to require the encryption of email will result in a change of user behavior and many users will accidentally overlook the need for encryption or may choose not to follow the new policy at all. With this fact in mind, the **Entrust Intelligence Messaging Server** email security solution was designed to automatically encrypt messages leaving the company network via email, without any user intervention, and encrypted messages can be sent to diverse external recipients regardless of their particular email application (i.e., they are not required to have email encryption software installed on their machines – they need only web-based email to retrieve and reply to encrypted messages sent via Messaging Server). Policy can be set and enforced without having to educate or train users, helping organizations to achieve compliance and ensure

protection of their sensitive cardholder information without relying on users to take any specific security action.

In partnership with Vericept, a leading content control solution provider, Entrust offers Vericept Content 360°, a multi-protocol content monitoring and control solution that provides visibility into how sensitive content is handled in an organization. Utilizing a suite of content detection techniques and over 70 risk categories, Content 360° works with Entrust Entelligence Messaging Server to identify which messages need to be encrypted before they leave the boundary of an organization. With Content 360°, email content can be monitored with greater accuracy to detect intellectual property, personally identifiable employee information or sensitive cardholder data. When this type of content is detected, the system can be configured to take immediate action such as automatically encrypt the email, or even block delivery—thereby helping to meet the data security requirements of PCI. The combination of Messaging Server and Vericept Content 360° enables organizations to:



- enforce email security policies through automatic detection and encryption of sensitive information such as credit cardholder data
- protect sensitive email while in transit and while stored in inboxes and on mail servers
- perform content monitoring and remediation on both inbound and outbound email messages

For organizations that are familiar with PKI and have already deployed digital certificates on desktops or within web applications, Entrust offers comprehensive end-to-end email security solutions. Using **Entrust Entelligence Security Provider** and/or the Entrust Entelligence Email Plug-in, PKI deployments can be expanded to include Microsoft, Lotus and Macintosh email security capabilities.

**Requirement 6: Develop and maintain secure systems and applications**

*Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed via vendor security patches, and all systems should have current software patches to protect against exploitation by employees, external hackers, and viruses. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.*

*PCI Data Security Standard*

To address requirement six, applications must be built using current best practices and coding methodologies. Secondly, core security tasks must be built into applications and systems. Not every developer can be an expert in cryptography and some of these elements need to be replicated in every application creating a large volume of applications to be managed and changed as security needs evolve. Using a common set of security tools such as the **Entrust Authority Toolkits** lets developers rapidly develop applications that have best-in-class centralized security built in, but that they didn't have to create. Leveraging the centralized security management provided by the Entrust security solutions suite means that as security needs or policies change, applications do not need to be individually updated, providing consistent security across applications.

## Protecting Identities

Protecting identities is the process for authenticating users and granting access to applications and information. At the heart of these requirements (numbers seven and eight) is the need to be able to determine with certainty who you are dealing with (authentication) and then controlling what they are allowed to see and do based on who they are and their role within the organization (access control).

### **Requirement 7: Restrict access to data by business need-to-know**

*This ensures that critical data can only be accessed in an authorized manner.*

*PCI Data Security Standard*

To address the requirement to restrict access across all applications, a high performance, centrally-managed access control tool is needed. **Entrust GetAccess™** software is a scalable Web access control solution. It centrally manages access to multiple applications through a single portal, providing users with single sign-on to the applications and content they are authorized to see. With the broadest support for user authentication methods, flexible roles and rules-based access control, self-service features, and proven performance to millions of users, the Entrust GetAccess solution can enable organizations to reduce administration costs while addressing requirement seven's mandate to restrict access to data.

### **Requirement 8: Assign a unique ID to each person with computer access**

*This ensures that actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.*

*PCI Data Security Standard*

Many organizations assign a unique ID to each person in the form of a username and password, but this requirement demands more. Password-based authentication or single factor authentication to critical enterprise resources leaves networks and data exposed to unnecessary risk and compromises compliance with the PCI Data Security requirements.

Authentication methods that depend on more than one factor are more difficult to compromise than single-factor methods. Strong or multi-factor authentication is needed to identify users accessing corporate resources such as VPN remote access, Microsoft Windows desktops, servers and Web-based or custom applications.

When evaluating authentication solutions for PCI compliance, investing in a single, enterprise authentication platform provides the most flexible solution. Organizations need a platform that offers control and flexibility in determining how to secure users and their connectivity, based on the risks associated with the transactions they are performing.

**Entrust IdentityGuard** is a risk-based, strong, multi-factor authentication platform that can enable companies to apply the right level of authentication tailored to the risk associated with the connectivity and particular actions that a user is performing. It enables organizations to deploy one or more authentication methods from a wide range available—security grid, knowledge authentication, Q&A, machine authentication, mobile out-of-band or token—to protect access to

sensitive cardholder data. Custom applications can still leverage the Entrust platform using Entrust's Java Toolkits in any Operating System.

## About Authentication

Authentication factors are independent ways to establish identity and privileges. Factors simply ask and answer "How do we know you are who you say you are?" Existing authentication methodologies can involve up to three factors:

- Knowledge something the user knows (password, PIN)
- Possession something the user has (ATM card, smart card)
- Attribute something the user is (biometric, fingerprint, retinal scan)

Adding factors of authentication can add security and limit vulnerability to identity attacks. Properly designed and implemented multifactor authentication methods are more reliable and stronger fraud deterrents, and can have varying levels of user impact. **Why don't we all use multifactor authentication today?** Most organizations have relied on their own innate ability to manage risk through business means and have considered it unnecessary, given the cost and energy required to manage and deploy multifactor solutions. Often, organizations worry that users will find the process of authenticating with multiple factors scary or intimidating, and this has inhibited the use of multifactor solutions. But as risks increase, breaches continue, brands are impacted by fraud incidents and PCI penalties loom, the true importance and necessity of multifactor authentication becomes clear and the old arguments seem increasingly less valid.

## Entrust Expertise

By providing innovative and flexible security solutions, Entrust helps organizations address PCI compliance requirements without radically changing user behavior or abandoning established technology processes and technologies. For over ten years, Entrust has played a leading role in securing digital identities and information. Through security technologies such as encryption, authentication and advanced content scanning, Entrust has enabled customers to apply security policies and procedures that protect information and help fulfill regulatory demands, while still empowering users.

Entrust solutions provide a unified approach to managing digital identities and information security across a wide variety of devices, applications, platforms and environments. Entrust offers one of the most complete suites of products for PCI compliance that are cost effective and can be easily incorporated into existing business processes. The Entrust suite of products for **authentication, email security and data encryption** can integrate best-in-class security with minimal user impact and smooth integration into existing applications. Central policy management, administration and control provide responsive security that can be easily audited.

## Conclusion

Organizations want to achieve compliance for PCI as quickly and cost effectively as possible. Protecting identities and information across the twelve requirements means investing in a single security platform that will adapt easily as needs and requirements evolve. Protecting identities and information has been the cornerstone of Entrust solutions for more than 10 years. Entrust's suite of solutions provide some of the most complete capabilities for addressing the PCI-DSS requirements. For more information about how Entrust can help assess your needs for achieving PCI compliance, please contact us at [entrust@entrust.com](mailto:entrust@entrust.com) or call **1-888-690-2424**.

## About Entrust

Entrust, Inc. [NASDAQ: ENTU] is a world leader in securing digital identities and information. Over 1,500 enterprises and government agencies in more than 50 countries use Entrust solutions to help secure the digital lives of their citizens, customers, employees and partners. Our proven software and services can help customers in achieving regulatory and corporate compliance, while helping to turn security challenges such as identity theft and email security into business opportunities. For more information on how Entrust can help secure your digital life, please visit: [www.entrust.com](http://www.entrust.com)