

EVIDIAN

A Groupe Bull Company

PCI DSS compliance

How to reduce risks with Single Sign-On and IAM

This white paper explains how Evidian's
IAM Suite can help you comply with the
Payment Card Industry Data Security
Standard.

white
paper

Laurent de Jerphanion
July 2008

39 A2 08LV 00

Executive overview

With the rise of electronic commerce, there is a growing public awareness of the dangers of theft of confidential payment card information.

The Payment Card Industry Data Security Standard (PCI DSS) is designed to address these concerns. Merchants handling card data are expected to fulfill detailed security requirements to protect payment card data.

While the goals of the standard are very legitimate – reducing fraud and maintaining the public's trust in card and electronic payment – many organizations have encountered some difficulties and delays in implementing PCI DSS.

- Can you restrict access to card data to employees whose jobs require it?
- Even then, can you really identify users of an authorized account?
- How do you review and correlate access logs for all card-handling applications?
- How can you track default accounts in all resources that handle card data?

This white paper describes how an integrated identity and access management (IAM) solution can help you comply with many areas of PCI DSS. Properly implemented, it can do so without burdening your users and administrators with unnecessary, time-consuming procedures.

Of course, as is the case with all compliance projects, an IAM solution must be part of a larger PCI DSS compliance drive. But it can ensure that your decisions are enforced, and that you can demonstrate to auditors that payment card data related risks are considerably reduced.

Using IAM to achieve PCI DSS compliance

Identity and access management toolbox

Identity and access management (IAM) is a set of solutions that strengthen and systematize control of access to resources. Some of these solutions, which can play a major role in PCI DSS compliance, are:

- **Single sign-on (SSO):** each user has a unique ID and a single way to access all resources and applications: password, biometrics, smart card etc. As passwords can be changed automatically, you control access to IT resources. SSO systems typically include authentication management functions.
- **User provisioning:** user accounts in resources are listed, created and deleted from a single location. This is a great time-saver for administrators, and helps identify and eliminate default accounts.
- **Policy management:** each user's access rights are deduced from his or her role in the organization. This systematizes and automates your IT security policy. Policy management systems can usually be extended with workflow functions.

Individually, each of these functions can be very useful in pursuit of compliance. But they bring in a particular value when two or more modules are used together. For instance:

- **Using user provisioning *with* SSO:** whenever an account is created or modified in an application, single sign-on data is updated. Users are immediately operational as you do not need to send them their application passwords.
- **Using SSO *with* policy management:** as soon as SSO is active, it determines which applications are actually used, by which user, and with which account. This means that you can design an access policy based on actual IT usage.
- **Using policy management *with* user provisioning:** you can reconcile existing user accounts in line with your policy, and update them. You will discover a large percentage of dormant or obsolete accounts. But when policy management drives account creation and deletion, no account exists without justification.

Therefore, it is important to look beyond “point” solutions – for instance, tools that only perform access management. It is advisable to anticipate future upgrades toward more global identity and access management.

Using IAM for PCI DSS compliance

As part of a PCI DSS project comprising audit and organization, an IAM solution enables you to ensure – and prove – that your decisions are implemented.

PCI DSS requirements	Evidian IAM modules	Overview – contribution to PCI DSS
Build and maintain a secure network		
Install and maintain a firewall configuration to protect cardholder data.		
Do not use vendor-supplied defaults for system passwords and other security parameters	Enterprise SSO User Provisioning	Automatically change default passwords to new, strong passwords. Take an inventory of all application accounts, detect default accounts, and see which ones are in use.
Protect cardholder data		
Protect stored cardholder data.		
Encrypt the transmission of cardholder data across open, public networks.	Enterprise SSO	Encrypt all web traffic with SSL, even if the card-handling application does not support SSL natively.
Maintain a vulnerability management program		
Use and regularly update anti-virus software.		
Develop and maintain secure systems and applications.		
Implement strong access control measures		
Restrict access to cardholder data by business need-to-know.	Enterprise SSO Policy Manager	Access to cardholder data management applications is restricted to those users that require them, based on their roles.
Assign a unique ID to each person with computer access	Enterprise SSO	All users have a unique ID, and can be required to use strong authentication to access card data management applications. Extensive password and authentication policy ensures proper user identification.
Restrict physical access to cardholder data.	Enterprise SSO	The same access card is used to enter buildings, access a Windows session and launch applications.
Regularly monitor and test networks		
Track and monitor all access to network resources and cardholder data.	Enterprise SSO	Enterprise SSO maintains a central database of attempted accesses to cardholder data management applications. Accesses are linked to individual users. This provides a secure assessment trail that is linked to users, date and time and even the individual workstation used.
Regularly test security systems and processes.	Enterprise SSO	Enterprise SSO keeps a list of all application-access attempts. The result of vulnerability tests can therefore be consulted easily.
Maintain an information security policy		
Maintain a policy that addresses information security.	Enterprise SSO Policy Manager	You can use Enterprise SSO to define role-based application access, strong-authentication and password policies. The centralized access event log enables you to review policies for effectiveness.

PCI Data Security Standard: meeting requirements

PCI DSS aims to reduce payment card user data related risks. Therefore, auditors look at the risks in each of the PCI DSS requirement categories, and check whether the control activities you have put in place cover those risks adequately.

The following sections describe some typical risks contained in several PCI DSS requirement categories, and how Evidian's IAM solutions can help you be compliant.

Build and maintain a secure network

“Do not use vendor-supplied defaults for system passwords and other security parameters.”

Typical risks:

- An employee with some knowledge of the application can try out a default account and gain access to payment card data.
- If a default account is used as a shared account by the administrative team, it will be impossible to determine which administrator has used the account.
- Default system accounts have a high access privilege, so damage (whether intentional or not) is more likely to occur when this account is used.

How Evidian can help

PCI DSS requires organizations to “*change vendor-supplied defaults before installing a system on the network*”. Using *Evidian User Provisioning*, administrators can check centrally that this change has been performed, and if not, correct the situation.

When initially deployed as part of a PCI DSS compliant drive, *Evidian User Provisioning* will gather account data from applications that handle payment card data, but also from other elements of the chain: databases, web interfaces, web servers etc. Default accounts can then be detected and eliminated.

In addition, *Evidian Enterprise SSO* can ensure that account passwords are changed automatically. You can decide whether or not the user will still know his or her password. This means that default user passwords are eliminated, making it impossible to guess an employee's password.

Protect cardholder data

“Encrypt transmission of cardholder data across open, public networks”

Typical risks:

- Some of your employees may access applications remotely, whether from other sites or outside your intranet. Unencrypted data (or application passwords) may thus be captured.

- Even if transmitted data is encrypted, the remote user may need to write down application passwords on paper. These passwords can get stolen.

How Evidian can help

Evidian Enterprise SSO functions are not confined to your intranet. An employee who accesses a web application from his or her station can continue to do so (if authorized by you) from a web browser outside your intranet. No client software needs to be installed. Single sign-on will still work, which means employees do not need to write down application passwords.

Moreover, *Evidian Enterprise SSO* can encrypt all traffic between the browser and your intranet using SSL, even if the web application itself is not configured for SSL.

Implement strong access control measures

“Restrict access to cardholder data by business need-to-know“

Typical risks:

- An employee in charge of payment card data entry is moved to another position – but can still access the original account.
- A secretary can access the application containing card data, just because he or she works in the relevant organization.

How Evidian can help

Evidian Policy Manager ensures that only relevant users are granted access to applications that manage payment card data. These users may, for instance, be part of a special group with such access rights. As required by PCI DSS, a “deny-all” policy can be implemented to reject access requests from other users.

With *Evidian Enterprise SSO*, the policy thus defined is enforced at the desktop level. Passwords for critical applications are changed, and users do not know the new passwords; secure SSO is then the only way to access the applications in question. All access events are audited. Once an employee changes job roles and no longer requires access to the applications, his or her rights are cancelled.

“Assign a unique ID to each person with computer access“

Typical risks:

- Passwords are weak and not changed regularly. Administrative accounts have easy-to-guess passwords.
- An employee goes on vacation and asks a colleague to fill in for him or her. Therefore, said employee reveals his/her ID/password to the colleague.

- An employee guesses a colleague's password and gains access to payment card data in an application.

How Evidian can help

With *Evidian Enterprise SSO*, each employee has a unique user name throughout the organization. This identifier is used to access workstations and applications. Moreover, a range of strong authentication methods can be used to verify his or her user identity.

Of course, *Evidian Enterprise SSO* can enforce a stringent and strong password policy for both workstation access and applications. This covers format, duration, reset policy etc. However, passwords are sometimes not enough to ensure secure access to card data.

Therefore, you may require users to use multiple forms of authentication such as biometrics, passwords, tokens or a combination thereof to access applications that handle card data. This requirement can be location-dependent – e.g. users can only access applications from specific places, with token authentication.

For instance, you can decide that on the intranet, a user can only launch the payment card application from a biometrics-protected workstation, and that remote access is only possible with two-factor authentication.

Not only is Evidian compatible with a large range of strong authentication systems, it also provides features that manage them directly. It includes a Card Management System (CMS) that administrators use to grant, revoke and lend access cards or tokens.

“Restrict physical access to cardholder data”

Typical risk:

- An employee uses the stolen password of an absent colleague.
- An application containing card data is accessed at 1:00 AM, by an employee who should be at home.

How Evidian can help

In many cases, passwords should not be considered sufficient to authenticate a user. However, if a card or USB token is required to access a station, many employees will leave them plugged to their PC for convenience reasons.

One solution: the same access card can be used to enter and leave the company premises, launch a Windows session and access applications. As this card is an important part of the employee's corporate life, this ensures that it will always remain with the employee.

Regularly monitor and test networks

“Track and monitor all access to network resources and cardholder data”

Typical risks:

- The log retention and backup policy is not enforced on all resources.
- Access audit is rarely done, because it means going through large numbers of disparate application logs.
- Application logs do not show who accessed an account, or the access location.
- Only payment card data handling applications are audited. A user’s web and network path is not looked at.

How Evidian can help

Gathering a large quantity of access log data is not enough, PCI DSS requires you to “*track user activity*”, not just application activity. The difference is significant, as “*determining the cause of a compromise*” is the ultimate goal.

To be useful, access logs need to be easily accessible, with the same interface, whatever the origin of the data. That way, you can reconstitute in a few minutes what a suspected user did on the day of a breach.

Each time *Evidian Enterprise SSO* grants a user access to an application, this results in a new log entry in a central, consolidated database. This database also stores failed denials, password changes, administration actions, session starts/stops, etc. It can be easily queried by date, user, location, etc., and backup needs only to be performed on a single location.

PCI DSS specifically requires that logs store “*user identification*” and “*origination of event*”. This information is typically not present in application logs. However, it is present in the *Evidian Enterprise SSO* log.

Application log: “*Somebody accessed account **GMAR_01** on **02/03/2009** at **1:02 AM**.”*”

SSO log: “*User **George Martin** accessed account **GMAR_01** from station **PC_027** on **02/03/2009** at **1:02 AM**.”*”

Maintain an information security policy

“Maintain a policy that addresses information security”

Typical risk:

- Application administrators are not aware of security policy changes; they assign accounts based on their own interpretation of rules.
- When the security policy changes, there is no general review of existing application accounts.

How Evidian can help

Defining and updating access rights on tens of applications, for thousands of employees, can quickly become a significant challenge.

The solution: Evidian Policy Manager makes it easy to “*administer user accounts, including additions, deletions, and modifications*”. From a central console, you can define which user categories have access to which applications, and from which locations.

It is then a matter of reconciliation to check whether your policy is reflected in application accounts and employee access, and to remedy the situation if necessary. Account updates can be performed automatically with *Evidian User Provisioning* or a workflow procedure.

Moreover, with *Evidian Enterprise SSO*, you can ensure that only the right users access the accounts you have defined. In the words of PCI DSS, you can “*monitor and control all access*” to applications and therefore the payment card data they contain.

For more information, please visit our website: www.evidian.com/

Email: info@evidian.com

© 2008 Evidian

The information contained in this document represents the view of Evidian on the issues discussed at the date of publication. Because Evidian must respond to changing market conditions, it should not be interpreted as a commitment on the part of Evidian, and Evidian cannot guarantee the accuracy of any information presented after the date of publication.

This is for informational purposes only. EVIDIAN MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

We acknowledge the rights of the proprietors of trademarks mentioned in this book.

white
paper

EVIDIAN
A Groupe Bull Company