PMPRO 10.2

PA-DSS implementation guide

Document version D01_PMPRO.4.1

By Jan Kelderman

iTesso
Breda
The Netherlands

Note

This PA-DSS Implementation Guide must be reviewed on a yearly basis, whenever the underlying application changes or whenever the PA-DSS requirements change. Updates should be tracked and reasonable accommodations should be made to distribute or make the updated guide available to users. iTesso will distribute the IG to new customers together with the proposal.

Confidential information

The information contained in this document is iTesso confidential and has been prepared to establish internal policies and procedures. Distribution of this document outside of iTesso is strictly prohibited. Do not copy or distribute without the permission of the Chief Technology Officer.

Table of contents

Notice

THE INFORMATION IN THIS DOCUMENT IS FOR INFORMATIONAL PURPOSES ONLY. ITESSO MAKES NO REPRESENTATION OR WARRANTY AS TO THE ACCURACY OR THE COMPLETENESS OF THE INFORMATION CONTAINED HEREIN. YOU ACKNOWLEDGE AND AGREE THAT THIS INFORMATION IS PROVIDED TO YOU ON THE CONDITION THAT NEITHER ITESSO NOR ANY OF ITS AFFILIATES OR REPRESENTATIVES WILL HAVE ANY LIABILITY IN RESPECT OF, OR AS A RESULT OF, THE USE OF THIS INFORMATION. IN ADDITION, YOU ACKNOWLEDGE AND AGREE THAT YOU ARE SOLELY RESPONSIBLE FOR MAKING YOUR OWN DECISIONS BASED ON THE INFORMATION HEREIN.

NOTHING HEREIN SHALL BE CONSTRUED AS LIMITING OR REDUCING YOUR OBLIGATIONS TO COMPLY WITH ANY APPLICABLE LAWS, REGULATIONS OR INDUSTRY STANDARDS RELATING TO SECURITY OR OTHERWISE INCLUDING, BUT NOT LIMITED TO, PA-DSS AND DSS.

THE RETAILER MAY UNDERTAKE ACTIVITIES THAT MAY AFFECT COMPLIANCE. FOR THIS REASON, ITESSO IS REQUIRED TO BE SPECIFIC TO ONLY THE STANDARD SOFTWARE PROVIDED BY IT.

1. Change log and approval

1.1. Change log

Version	Date	By	Details
1.0	12 SEP 2008	Jan K	Draft and delivered version
3.0	12 NOV 2013	JK	Updated to iTesso standard and added latest requirements
4.0	11 MAR 2014	JK	Adapted to findings by Acertigo
4.1	29 MAR 2014	JK	Added missing details after review by TUV SUD

1.2. Approval and signatures

On behalf of Management Name Date

On behalf of Sales Name Date

On behalf of Development Name Date

2. About this document

This document describes the steps that must be followed in order for your Brilliant PM^{PRO} installations to comply with Payment Application – Data Security Standards (PA-DSS). The information in this document is based on PCI Security Standards Council Payment Application Data Security Standards program (version 2.0).

iTesso instructs and advises its customers to deploy applications by iTesso in a manner that adheres to the PCI Data Security Standard (v2.0). Subsequent to this, best practices and hardening methods, such as those referenced by the Center for Internet Security (CIS) and their various "Benchmarks", should be followed in order to enhance system logging, reduce the chance of intrusion and increase the ability to detect intrusion, as well as other general recommendations to secure networking environments. Such methods include, but are not limited to, enabling operating system auditing subsystems, system logging of individual servers to a centralized logging server, the disabling of infrequently-used or frequently vulnerable networking protocols and the implementation of certificate-based protocols for access to servers by users and vendors.

If you do not follow the steps outlined here, your Brilliant PM^{PRO} installations will not be PA-DSS compliant.

3. Executive summary

Brilliant PM^{PRO} 10.2 has been PA-DSS (Payment Application Data Security Standard) certified, with PA-DSS Version 2.0. For the PA-DSS assessment, we worked with the following PCI SSC approved Payment Application Qualified Security Assessor (PAQSA):

TÜV SÜD Management Service GmbH Büchensstr. 20, 70174 Stuttgart

This document also explains the Payment Card Industry (PCI) initiative and the Payment Application Data Security Standard (PA-DSS) guidelines. The document then provides specific installation, configuration, and ongoing management best practices for using Payment Application as a PA-DSS validated Application operating in a PCI Compliant environment.

3.1. PCI Security Standards Council Reference Documents

The following documents provide additional detail surrounding the PCI SSC and related security programs (PA-DSS, PCI DSS, etc):

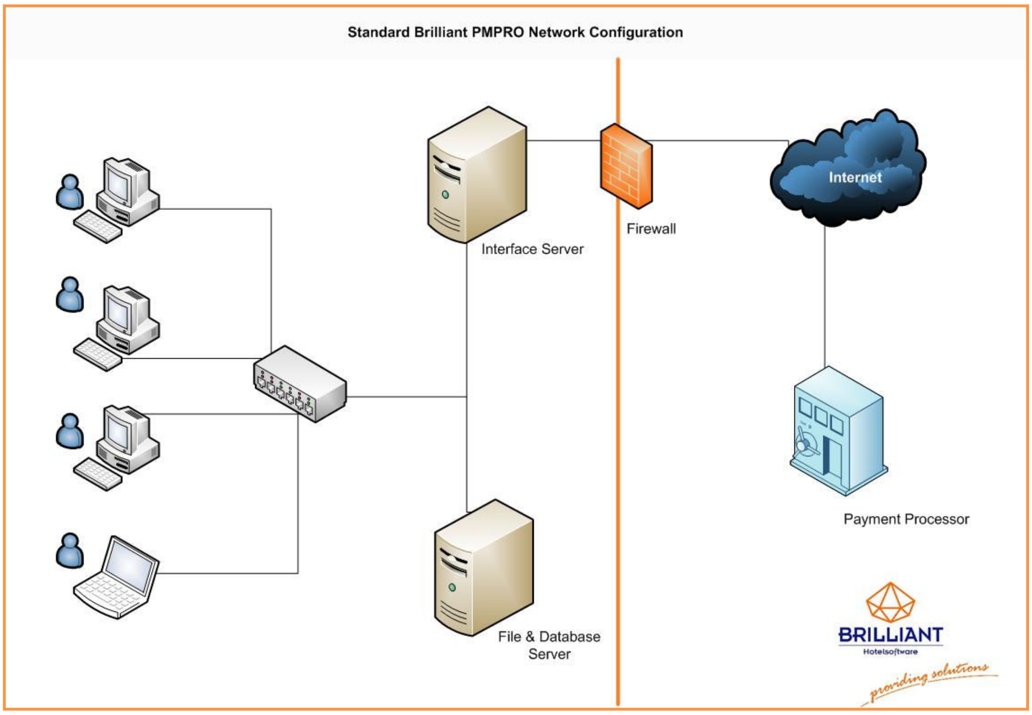
- Payment Applications Data Security Standard (PA-DSS)
  https://www.pcisecuritystandards.org/security_standards/pa_dss.shtml
- Payment Card Industry Data Security Standard (PCI DSS)
  https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml
- Open Web Application Security Project (OWASP)
  http://www.owasp.org

3.2. Application summary

Payment Application Name:	Brilliant PM^{PRO}
Payment Application Version:	10.2.xxx
Application Description:	Brilliant PM^{PRO}, Integrated Distribution Property Management System, will help increase the yield and lower the cost for a hotel. It is a powerful set of software tools for efficient and effective management of hospitality operations, with special functionality for controlling distribution channels. Brilliant PM^{PRO} has a modular design so it caters to all types of properties
Application Target Clientele:	Hospitality
Components of Application Suite (i.e. POS, Back Office, etc.)	Brilliant PM^{PRO} consists of a single application that does all the tasks
Required Third Party Payment Application Software:	Brilliant PM^{PRO} uses ProtoBase for Credit Card transactions
Database Software Supported:	Brilliant PM^{PRO} uses Microsoft SQL Server for PCI data and for property data the native Visual Foxpro tables are used
Other Required Third Party Software:	Brilliant PM^{PRO} uses the standard reporting of Visual Foxpro for reporting purposes
Operating System(s) Supported:	Brilliant PM^{PRO} runs on Microsoft Windows, including, but not limited to Windows 7 and Server 2008R2.
Application Functionality Supported	Reservations, front office, back office, reporting, etc.
Payment Processing Connections:	Credit cards are processed through the ProtoBase gateway, using a TCP/IP connection.
Description of Versioning Methodology:	Brilliant PM^{PRO} versioning has three levels: Major, Minor and Build: 10.2.xxx **Major**: changes include significant changes to the application and would have an impact on PA-DSS requirements. **Minor**: changes include small changes such as minor enhancements and may or may not have an impact on PA-DSS requirements. **Build**: changes include bug fixes and would have no negative impact on PA-DSS requirements.

4. Typical network implementation

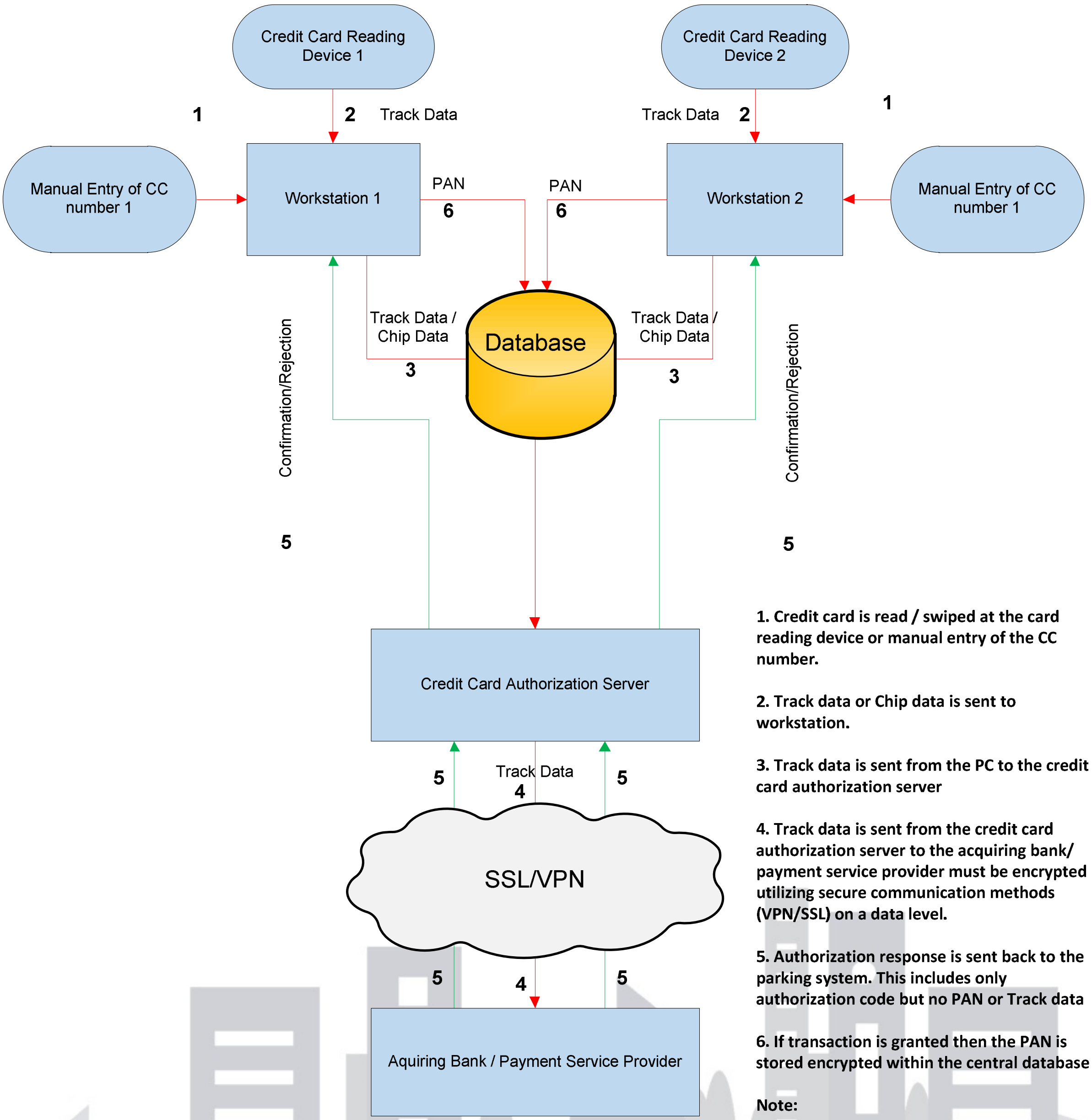
The PCI DSS requires that firewall services be used (with NAT or PAT) to segment network segments into logical security domains based on the environmental needs for internet access. Traditionally, this corresponds to the creation of at least a DMZ and a trusted network segment where only authorized, business-justified traffic from the DMZ is allowed to connect to the trusted segment. No direct incoming internet traffic to the trusted application environment can be allowed. Additionally, outbound internet access from the trusted segment must be limited to required and justified ports and services.



5. Dataflow diagram

IDPMS Data Flow Diagram

Colored lines represent the type of data in transit as follows:
- Red represents encrypted or unencrypted Sensitive Authentication data or Cardholder data in Transit
- Green represents data that is not considered Cardholder or Sensitive Authentication Data.


Credit Card Reading Device 1
Credit Card Reading Device 2
1
2
Track Data
Track Data
2
1
Manual Entry of CC number 1
Workstation 1
PAN
6
PAN
6
Workstation 2
Manual Entry of CC number 1
Track Data / Chip Data
Database
Track Data / Chip Data
3
3
Confirmation/Rejection
Confirmation/Rejection
5
5
Credit Card Authorization Server
5
Track Data
4
5
SSL/VPN
5
4
5
Aquiring Bank / Payment Service Provider

1. Credit card is read / swiped at the card reading device or manual entry of the CC number.

2. Track data or Chip data is sent to workstation.

3. Track data is sent from the PC to the credit card authorization server

4. Track data is sent from the credit card authorization server to the acquiring bank/ payment service provider must be encrypted utilizing secure communication methods (VPN/SSL) on a data level.

5. Authorization response is sent back to the parking system. This includes only authorization code but no PAN or Track data

6. If transaction is granted then the PAN is stored encrypted within the central database

Note:
No Track data is stored at any Time.

6. Difference between PCI compliance and PA-DSS Validation

As a software vendor, our responsibility is to be “PA-DSS Validated”.

We have performed an assessment and certification compliance review with our independent assessment firm, to ensure that our platform does conform to industry best practices when handling, managing and storing payment related information.

PA-DSS is the standard against which Payment Application has been tested, assessed, and validated.

PCI Compliance is then later obtained by the merchant, and is an assessment of your actual server (or hosting) environment.

Obtaining “PCI Compliance” is the responsibility of the merchant and your hosting provider, working together, using PCI compliant server architecture with proper hardware & software configurations and access control procedures.

The PA-DSS Validation is intended to ensure that the Payment Application will help you achieve and maintain PCI Compliance with respect to how Payment Application handles user accounts, passwords, encryption, and other payment data related information.

The Payment Card Industry (PCI) has developed security standards for handling cardholder information in a published standard called the PCI Data Security Standard (DSS). The security requirements defined in the DSS apply to all members, merchants, and service providers that store, process or transmit cardholder data.

The PCI DSS requirements apply to all system components within the payment application environment which is defined as any network device, host, or application included in, or connected to, a network segment where cardholder data is stored, processed or transmitted.

6.1. The twelve requirements for PCI DSS

These are the twelve requirements of the PCI-DSS

Build and Maintain a Secure Network

1. *Install and maintain a firewall configuration to protect data*
2. *Do not use vendor-supplied defaults for system passwords and other security parameters*

Protect Cardholder Data

3. *Protect Stored Data*
4. *Encrypt transmission of cardholder data and sensitive information across public networks*

Maintain a Vulnerability Management Program

5. *Use and regularly update anti-virus software*
6. *Develop and maintain secure systems and applications*

Implement Strong Access Control Measures

7. *Restrict access to data by business need-to-know*
8. *Assign a unique ID to each person with computer access*
9. *Restrict physical access to cardholder data*

Regularly Monitor and Test Networks

10. *Track and monitor all access to network resources and cardholder data*
11. *Regularly test security systems and processes*

Maintain an Information Security Policy

12. *Maintain a policy that addresses information security*

7. Considerations for the Implementation of Payment Application in a PCI-Compliant Environment

The following areas must be considered for proper implementation in a PCI-Compliant environment.

- Sensitive Authentication Data requires special handling
- Remove Historical Cardholder Data
- Set up Good Access Controls
- Properly Train and Monitor Admin Personnel
- Key Management Roles & Responsibilities
- PCI-Compliant Remote Access
- Use SSH, VPN, or SSL/TLS for encryption of administrative access
- Log settings must be compliant
- PCI-Compliant Wireless settings
- Data Transport Encryption
- PCI-Compliant Use of Email
- Network Segmentation
- Never store cardholder data on internet-accessible systems
- Use SSL for Secure Data Transmission
- Delivery of Updates in a PCI Compliant Fashion

7.1. Remove Historical Sensitive Authentication Data (PA-DSS 1.1.4.a)

Versions before 10.1 stored sensitive authentication data, no PINs or Pinblock Data was stored by these earlier versions of PM^{PRO}. See the document "BHS Update procedure from non-PCI to PCI". The document is still valid when updating customers to 10.2.

Notice that it is absolutely necessary to securely remove historical sensitive authentication data for PCI DSS compliance.

7.2. Sensitive Authentication Data requires special handling (PA-DSS 1.1.5a and 1.1.5.c)

Brilliant PM^{PRO} does store Sensitive Authentication – the PAN encrypted and Expiration Date – and sensitive data is never used for any troubleshooting at all.

7.2.1. Collect sensitive authentication

Sensitive data should not be used to find / solve problems in the application. In the rare case that live data is required the PCI DSS related procedures must be followed.

7.2.2. Store such data with limited access

The data that is collected from a live (customer) environment should only be stored on the specific development network location that is available to those software engineers that are working on PM^{PRO}.

7.2.3. Collect only the limited amount of data

Only collect the data that is necessary to pin-point the specific issue, like only a specific date or a specific guest related record or data set.

7.2.4. Encrypt sensitive authentication data while stored

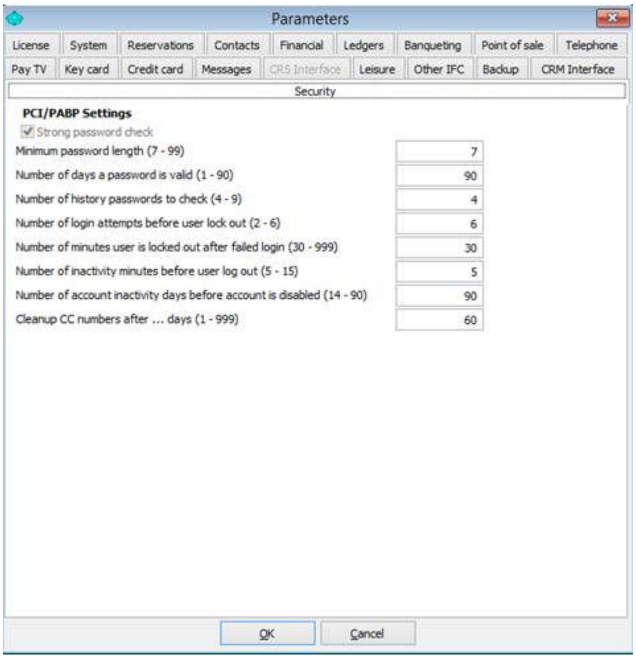
The data used is always encrypted, using the mechanism used throughout the entire product for encrypting sensitive data.

7.2.5. Securely delete such data immediately after use

After the problem has been resolved the data of entire environment is wiped out using Eraser.

7.3. Cardholder Data (PA-DSS 2.1)

The encrypted cardholder data is stored in a single SQL Server table in the SQL Server database in the pm_creditcards table. This data is stored for a limited period of time, 'old' cardholder data is automatically purged from the database by a daily procedure (the so-called audit) in the hotel. The number of days the data can be kept in the table is configurable in the settings of PM$^{\text{PRO}}$ (see screenshot *Cleanup CC numbers after … days (1 – 999)*). These setting can only be accessed by the users that have this right configured – super users.



PCI/PABP Settings

☑ Strong password check

Minimum password length (7 - 99)	7
Number of days a password is valid (1 - 90)	90
Number of history passwords to check (4 - 9)	4
Number of login attempts before user lock out (2 - 6)	6
Number of minutes user is locked out after failed login (30 - 999)	30
Number of inactivity minutes before user log out (5 - 15)	5
Number of account inactivity days before account is disabled (14 - 90)	90
Cleanup CC numbers after … days (1 - 999)	60

7.4. Removal of Cryptographic material (2.7a)

Brilliant PM$^{\text{PRO}}$ has the following versions that previously encrypted cardholder data: Brilliant PM$^{\text{PRO}}$ 10.0 and before. This data is purged during the update process, see also 7.3.

Notice that it is absolutely necessary for PCI DSS to securely delete any historical sensitive authentication data from the system.

For the older versions of PM$^{\text{PRO}}$ (10.0 and before) the Eraser tool is used to delete old material. See the "Secure deleting of sensitive data" (D10) for details on how to act.

7.5. Set up Good Access Controls (3.1.c and 3.2)

The PCI DSS requires that access to all systems in the payment processing environment be protected through use of unique users and complex passwords. Unique user accounts indicate that every account used is associated with an individual user and/or process with no use of generic group accounts used by more than one user or process. The next points are applicable:

- Do not use administrative accounts for application logins (e.g., don't use the "sa" account for application access to the database).
- Assign strong passwords to these default accounts (even if they won't be used), and then disable or do not use the accounts.
- Assign strong application and system passwords whenever possible.

- Create PCI DSS-compliant complex passwords to access the payment application, per PCI Data Security Standard 8.5.8 through 8.5.15
- Changing the "out of the box" settings for unique user IDs and secure authentication will result in non-compliance with the PCI DSS

The PCI standard requires the following password complexity for compliance (often referred to as using "strong passwords"):

- Do not use group, shared, or generic user accounts (8.5.8)
- Passwords must be changed at least every 90 days (8.5.9)
- Passwords must be at least 7 characters (8.5.10)
- Passwords must include both numeric and alphabetic characters (8.5.11)
- New passwords cannot be the same as the last 4 passwords (8.5.12)

PCI user account requirements beyond uniqueness and password complexity are listed below:

- If an incorrect password is provided 6 times the account should be locked out (8.5.13)
- Account lock out duration should be at least 30 min. (or until an administrator resets it) (8.5.14)
- Sessions idle for more than 15 minutes should require re-entry of username and password to reactivate the session (8.5.15)

These same account and password criteria must also be applied to any applications or databases included in payment processing to be PCI compliant. Brilliant PM^PRO, as tested to in our PA-DSS audit, meets, or exceeds these requirements.

Brilliant PM^PRO requires unique usernames and complex passwords for all administrative access and for all access to cardholder data.

[Note: These password controls are not intended to apply to employees who only have access to one card number at a time to facilitate a single transaction. These controls are applicable for access by employees with administrative capabilities, for access to servers with cardholder data, and for access controlled by the application.]

- Control access, via unique username and PCI DSS-compliant complex passwords, to any PCs or servers with payment applications and to databases storing cardholder data.

7.6. Properly Train and Monitor Admin Personnel (3.2)

It is your responsibility to institute proper personnel management techniques for allowing admin user access to cardholder data, site data, etc. You can control whether each individual admin user can see credit card PAN (or only last 4).

In most systems, a security breach is the result of unethical personnel. So pay special attention to whom you trust into your admin site and who you allow to view full decrypted and unmasked payment information.

7.7. Key Management Roles & Responsibilities (PA-DSS 2.5c)

Since in the Hotel industry credit card information is taken to guarantee reservations as well as to guarantee charges incurred during a stay, it is likely that Brilliant PM^PRO customers store credit card data. To facilitate that storage in a PCI compliant manner, Brilliant PM^PRO has introduced data encryption for all sensitive data, together with a SQL Server database to store this information.

Brilliant PM^PRO uses the Advanced Encryption Standard (AES), sometimes referred to as Rijndael Encryption. Brilliant PM^PRO uses the 256 bits key variant, which is the maximum under the current AES standard.

Brilliant PM^{PRO} uses a unique dynamic key approach where the encryption key is different for each transaction. This method eliminates the PCI requirement for key changes at certain intervals. The Brilliant PM^{PRO} approach helps save our customer's time and money while maintaining a secure environment.

Data retention is allowed under PCI compliance standards for as long as there is a business reason. Therefore, credit card data on reservations will be retained until after check-out, even for reservations that are made well in advance. Credit card information on cancelled or checked-out folios will be discarded after a configurable time.

There is no access to any key material by the customer.

A new key is generated when the user choose to do so and the user is given the opportunity to store the binary file, where the key is generated from, on a memory stick and store that in their vault. When a new key is generated, all encrypted data in PM^{PRO} is decrypted against the old key and then encrypted against the new generated key. This process is done per credit card entry, first a decryption with the old key and then an encryption with the new key. Once all records are encrypted with the new key, the old key is destroyed.

7.8. Logs (PA-DSS 4.x)

The PCI logs are stored in a SQL server table, see the below for the events that are logged. This logging is also send to Microsoft Event Logging and the format of the Event Logging is *not* configurable in PM^{PRO}.

The Microsoft Event Log can be configured to send event log information to a centralized server, the Windows Event Collector. The Windows Event Collector functions support subscribing to events by using the WS-Management protocol.

Event collection allows administrators to get events from remote computers and store them in a local event log on the collector computer. The destination log path for the events is a property of the subscription. All data in the forwarded event is saved in the collector computer event log (none of the information is lost). Additional information related to the event forwarding is also added to the event.

How to fully configure the Microsoft Event Collector is beyond the scope of this document, please see the Microsoft website under "Windows Event Collector" (http://msdn.microsoft.com/en-us/library/windows/desktop/bb427443(v=vs.85).aspx).

Brilliant PM^{PRO} has logging that cannot be turned off as per PCI DSS 10.2 and 10.3 as follows:

Implement automated assessment trails for all system components to reconstruct the following events:

10.2.1 All individual user accesses to cardholder data

10.2.2 All actions taken by any individual with root or administrative privileges

10.2.3 Access to all assessment trails

10.2.4 Invalid logical access attempts

10.2 5 Use of identification and authentication mechanisms

10.2.6 Initialization of the assessment logs

10.2.7 Creation and deletion of system-level objects.

Record at least the following assessment trail entries for all system components for each event from 10.2.x:

10.3.1 User identification

10.3.2 Type of event

10.3.3 Date and time

10.3.4 Success or failure indication

10.3.5 Origination of event

10.3.6 Identity or name of affected data, system component, or resource.

<u>Disabling or subverting the logging function of Brilliant PM$^{\text{PRO}}$ in any way will result in non-compliance with PCI DSS.</u>

7.9. PCI-Compliant Wireless settings (PA-DSS 6.1.b and 6.2.b)

Brilliant PM$^{\text{PRO}}$ <u>does not</u> support wireless technologies. However, should the merchant implement wireless access within the cardholder data environment, the following guidelines for secure wireless settings must be followed per PCI Data Security Standard 1.2.3, 2.1.1 and 4.1.1.

1.2.3: Perimeter firewalls must be installed between any wireless networks and systems that store cardholder data, and these firewalls must deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.

2.1.1:

- All wireless networks implement strong encryption (e.g. AES)
- Encryption keys were changed from default at installation, and are changed anytime anyone with knowledge of the keys leaves the company or changes positions
- Default SNMP community strings on wireless devices were changed
- Default passwords/passphrases on access points were changed
- Firmware on wireless devices is updated to support strong encryption for authentication and transmission over wireless networks (for example, WPA/WPA2)
- Other security-related wireless vendor defaults, if applicable

4.1.1:

- Industry best practices are used to implement strong encryption for the following over the wireless network in the cardholder data environment (4.1.1):
    - Transmission of cardholder data
    - Transmission of authentication data
- Payment applications using wireless technology must facilitate the following regarding use of WEP:
- For new wireless implementations, it is prohibited to implement WEP as of March 31, 2009.

- For current wireless implementations, it is prohibited to use WEP after June 30, 2010.

7.10. Encryption Key Renewal

The end-user of Brilliant PM^{PRO} can at any time replace the key that is in use for PCI related data encryption. The key-renewal process can only be started by those users that are granted the right to do so. During the training the iTesso consultant clearly explains the customer this part and adds that this right should be granted to a very limited number of users.

7.10.1. Generate an Encryption Key

The Encryption Key is generated by the application and a user *must* have rights inside the application to do so. The process cannot be influenced in any way, since it is part of the application.

7.10.2. Distribution

The Encryption Key does not need to be distributed. The generated Encryption Key is automatically updated in the application data, and where needed the data is encrypted against the new key.

7.10.3. Encryption Key Protection

The Encryption Key is protected with a Key Encryption Key. A 10MB data stream is the core for the key and this data stream can be saved to an USB memory Stick and then stored in a vault.

7.10.4. Key renewal

There is no access to any key material by the customer.

When a new key is generated, all encrypted data in PM^{PRO} is decrypted against the old key and then encrypted against the new generated key. This process is done per credit card entry, first a decryption with the old key and then an encryption with the new key. Once all records are encrypted with the new key, the old key is destroyed.

7.11. Centralized Logging

The PCI specific logging of user actions can be exported in any desired format. To do so, the standard exporting tools of Brilliant PM^{PRO} are used.

7.11.1. Export the Logging

Export of the logging can be performed at any time by selecting the specific export/report. It is possible to export the information during the so-called night audit, since the export is embedded in the standard workflow in Brilliant PM^{PRO}.

7.12. Use of necessary and secure services and protocols (PA-DSS 5.4)

PA-DSS states that the payment application must only use necessary and secure services, protocols, components, and dependant software and hardware, including those provided by third parties. iTesso does not transport any information over the internet, so no recommendation for protocols in this area are necessary.

In case a separate Database Sever is in use, iTesso recommends using ISEC between the Application and the Database servers to secure communications.

Communications to a so-called Gateway of the Credit Card Merchant (like SIX Cards) is over the LAN using a direct TCP/IP socket.

7.13. Never store cardholder data on internet-accessible systems (PA-DSS 9.1.b)

Never store cardholder data on Internet-accessible systems (e.g., web server and database server must not be on same server)

7.14. PCI-Compliant Delivery of Updates (PA-DSS 10.1)

The development process for updates and patches is described in the "Product Lifecycle Manual".

As a development company, we keep abreast of the relevant security concerns and vulnerabilities in our area of development and expertise.

Once we identify a relevant vulnerability, we work to develop & test a patch that helps protect Brilliant PM^PRO against the specific, new vulnerability. We attempt to publish a patch within days of the identification of the vulnerability. Typically, merchants are expected to respond quickly to and install available patches within 30 days.

We deliver software and/or updates via remote access to customer networks, using Fast Viewer.

For receiving updates via remote access, merchants must adhere to the following guidelines:

- Secure remote access technology use, per PCI Data Security Standard 12.3.9:

> *12.3.9 Activation of remote access technologies for vendors only when needed by vendors, with immediate deactivation after use*

7.15. PCI-Compliant Remote Access (11.2 and 11.3.b)

The PCI standard requires that if employees, administrators, or vendors are granted remote access to the payment processing environment; access should be authenticated using a two-factor authentication mechanism (username/ password and an additional authentication item such as a token or certificate).

In the case of vendor remote access accounts, in addition to the standard access controls, vendor accounts should only be active while access is required to provide service. Access rights should include only the access rights required for the service rendered, and should be robustly audited.

If users and hosts within the payment application environment may need to use third-party remote access software such as RDP, Terminal Server, etc. to access other hosts within the payment processing environment, special care must be taken.

In order to be compliant, every such session must be encrypted with at least 128-bit encryption (in addition to satisfying the requirement for two-factor authentication required for users connecting from outside the payment processing environment). For RDP/Terminal Services this means using the high encryption setting on the server, and for FastViewer it means using symmetric or public key options for encryption. Additionally, the PCI user account and password requirements will apply to these access methods as well.

When requesting support from a vendor, reseller, or integrator, customers are advised to take the following precautions:

- Change default settings (such as usernames and passwords) on remote access software (e.g. VNC)
- Allow connections only from specific IP and/or MAC addresses

- Use strong authentication and complex passwords for logins according to PCI DSS 8.1, 8.3, and 8.5.8-8.5.15
- Enable encrypted data transmission according to PCI DSS 4.1
- Enable account lockouts after a certain number of failed login attempts according to PCI DSS 8.5.13
- Require that remote access take place over a VPN via a firewall as opposed to allowing connections directly from the internet
- Enable logging for auditing purposes
- Restrict access to customer passwords to authorized reseller/integrator personnel.
- Establish customer passwords according to PCI DSS Requirements 8.1, 8.2, 8.4, and 8.5.

7.16. Data Transport Encryption (PA-DSS 12.1.b)

The PCI DSS requires the use of strong cryptography and encryption techniques with at least a 128 bit encryption strength (either at the transport layer with SSL or IPSEC; or at the data layer with algorithms such as RSA or Triple-DES) to safeguard cardholder data during transmission over public networks (this includes the Internet and Internet accessible DMZ network segments).

PCI DSS requirement 4.1: Use strong cryptography and security protocols such as secure sockets layer (SSL) / transport layer security (TLS) and Internet protocol security (IPSEC) to safeguard sensitive cardholder data during transmission over open, public networks.

- Refer to the Dataflow diagram for an understanding of the flow of encrypted data associated with Brilliant PM^{PRO}

PM^{PRO} does not require nor permit the use of any insecure service or protocol. Here are those that PM^{PRO} does use:

- SSL
- HTTPS

7.17. PCI-Compliant Use of End User Messaging Technologies (PA-DSS 12.2.b)

Brilliant PM^{PRO} does not allow or facilitate the sending of PANs via any end user messaging technology (for example, e-mail, instant messaging, and chat).

7.18. Non-console administration (PA-DSS 13.1)

Although Brilliant PM^{PRO} does not support non-console administration and we do not recommend using non-console administration, should you ever choose to do this, must use SSH, VPN, or SSL/TLS for encryption of this non-console administrative access.

7.19. Network Segmentation

The PCI DSS requires that firewall services be used (with NAT or PAT) to segment network segments into logical security domains based on the environmental needs for internet access. Traditionally, this corresponds to the creation of at least a DMZ and a trusted network segment where only authorized, business-justified traffic from the DMZ is allowed to connect to the trusted segment. No direct incoming internet traffic to the trusted application environment can be allowed. Additionally, outbound internet access from the trusted segment must be limited to required and justified ports and services.

Refer to the standardized Network diagram for an understanding of the flow of encrypted data associated with Brilliant PM^{PRO}.

7.20. Maintain an Information Security Program

In addition to the preceding security recommendations, a comprehensive approach to assessing and maintaining the security compliance of the payment application environment is necessary to protect the organization and sensitive cardholder data.

The following is a very basic plan every merchant/service provider should adopt in developing and implementing a security policy and program:

- Read the PCI DSS in full and perform a security gap analysis. Identify any gaps between existing practices in your organization and those outlined by the PCI requirements.
- Once the gaps are identified, determine the steps to close the gaps and protect cardholder data. Changes could mean adding new technologies to shore up firewall and perimeter controls, or increasing the logging and archiving procedures associated with transaction data.
- Create an action plan for on-going compliance and assessment.
- Implement, monitor and maintain the plan. Compliance is not a one-time event. Regardless of merchant or service provider level, all entities should complete annual self-assessments using the PCI Self Assessment Questionnaire.
- Call in outside experts as needed.

7.21. Application System Configuration

Below are the operating systems and dependent application patch levels and configurations supported and tested for continued PCI DSS compliance.

- Microsoft Windows XP Professional with Service Pack 2, Windows 7 (with or without SP1) and Windows 2003/2008 Server
  All latest updates and hot-fixes should be tested and applied
- 256 MB of RAM minimum, 2GB or higher recommended for Payment Application
- TCP/IP network connectivity
- SQL Server 2005/2008R2
  All latest updates and hot-fixes should be tested and applied

7.22. Payment Application Initial Setup & Configuration

The initial setup as it is performed by the Brilliant PM^{PRO} consultant. The consultant will always check the SHA of the application – calculated with the HashCalc utility – with the SHA published on the iTesso Intranet. The consultant will not install (or update) the version of PM^{PRO} when the published SHA does not match with the calculated SHA.

7.22.1. New Installation

The following configuration will be performed by iTesso representatives, oftentimes in close conjunction with the customers' System Administrator and is listed here for your reference.

- In SQL Management Studio, create 2 new users
  User ID: **PMPRO**, password: **to be assigned by the property**, password policy on, password expiry **off**

7.22.2. Defining the Payment Gateway

The payment gateway is installed by payment processor, this is not within the scope of an Brilliant PM^{PRO} install.

7.22.3. Tests

Once the install is completed several tests are performed, also tests together with the payment processor.