PAN-NORDIC CARD ASSOCIATION

Merchants
Mobile App Developers
Payment Service Providers
Terminal Vendors

Card in the Cloud and Mobile

Best Practice: Card In The Cloud And Mobile - Ver A Final
Type: Security
11 June 2013

Cloud computing is a form of distributed computing that is yet to be standardised. As cloud computing is still an evolving technology, evaluations of risks and benefits may change as the technology becomes more established and its implications become better understood.

Cloud security is a shared responsibility between the payment service provider (PSP) and the merchant. If payment card data is stored, processed or transmitted in a cloud environment, PCI DSS will apply to that environment, and will typically involve validation of both the PSP's infrastructure and the client's usage of that environment.

This document presents a requirements checklist for card in the cloud, i.e. cloud services, that is applicable to the PNC acquirers.

This document also presents a tool to classify of Mobile Solutions in **Appendix A**.

It is assumed that a web-based solution is used to access the cloud services. The browser can be a computer client or a web browser on a mobile phone or similar device. Other solutions, such as text-message-based, i.e. SMS-based, or proprietary applications, can be accepted but are subject to special reviews.

Version history

Date	Version	Description	Issued/revised by
2013-06-11	A Final	A new document	PNC SAC

Related documents

"**Information Supplement, PCI DSS Cloud Computing Guidelines, Version 2.0.**" February 2013. PCI Security Standards Council. 14 May 2013 <https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Cloud_Guidelines.pdf>.

"**Recommendation for the security of internet payments.**" April 2012. The European Central Bank - Eurosystem. 14 June 2013 <http://www.ecb.europa.eu/pub/pdf/other/recommendationsforthesecurityofinternetpaymentsen.pdf>.

"**VISA BEST PRACTICES - Data Field Encryption, Version 1.0.**" 5 October 2009. Visa Europe Downloads & resources. 14 May 2013 <http://www.visaeurope.com/en/businesses__retailers/payment_security/idoc.ashx?docid=a06621cc-9666-4ccd-9045-ecec84c7a94c&version=-1>.

"**Visa Europe Data Field Encryption: Device and Key Management Guidance Version 1.0.**" March 2010. Visa Europe Downloads & resources. 14 May 2013 <http://www.visaeurope.com/en/businesses__retailers/payment_security/idoc.ashx?docid=849b2be1-10b9-4bb5-8b8e-74f546777440&version=-1>.

PAN-NORDIC CARD ASSOCIATION

Requirements checklist for cloud services

Best Practice	Security requirement	Comments
The merchant		
A:1	The merchant must be approved by the acquirer.	
A:2	The cardholder must be authenticated against the merchant's acquirer.	
The Payment Service Provider (PSP)		
A:3	The PSP who stores and handles card data must be PCI DSS certified.	
A:4	The PSP must self assess that it complies with all services in this document before any merchant is connected to the service.	
A:5	The app should be revalidated annually and every time a major changes to the app.	
Transaction flagging		
A:6	Both the initial registration and subsequent purchases must be marked as ecommerce transactions[1].	
A:7	The ecommerce indicator (EC) must be set to 5 for the initial registration and to 7 for subsequent purchases.	
Identification of merchants against the PSP The identification of merchants against the PSP must be performed with strong authentication. This means:		
A:8	Both parties' identity must be verified. The merchant host must be able to identify the PSP host. The PSP host must be able to identify the merchant host. Industry best practices are to be followed for both cases.	
A:9	The PSP's key management procedures must meet industry best practices.	
A:10	The communication to the PSP must be protected by SSL or equal.	
Cardholder registration with a PSP		
A:11	The cardholder registers himself to the service and gets user credentials from the PSP. The cardholder registration is verified via a 3-D Secure[2] transaction. The 3-D Secure transaction, either a purchase or a registration transaction, shall be performed prior to the third purchase.	
A:12	Cardholder data must only be stored in PCI DSS approved services provided by a PSP.	
A:13	The PSP and the merchant are not allowed to store security codes (CVV/CVC) data.	
A:14	The cardholder must "sign" an agreement in which the PSP shall be entitled to charge pre-registered card number(s) after transaction approval.	

[1] The initial registration transaction will from the autumn 2013 be a card validation transaction.
[2] Please note other strong authentication mechanisms, such as BankID and chip-and-PIN, can replace 3-D Secure but needs to be discussed with the acquirer.

Best Practice	Security requirement	Comments
A:15	The cardholder must be able to deactivate and activate the service.	
A:16	When adding an additional card, a 3-D Secure purchase, where the cardholder is connected to 3-D Secure, shall be conducted. The validation shall be performed in accordance with A:8.	
A:17	The cardholder should upon installation of the service be reminded to install and use both virus protection and a firewall on the mobile device. The cardholder should also be advised to update to the latest operating system version available.	
A:18	For mobile apps: The cardholder should be informed upon installation that it is not allowed to install the service on jail-broken devices.	

Data to the merchant from the PSP

A:19	The merchant shall not have access to any cardholder data except the last four digits of the card number and the card brands in PCI. Cardholder data must only be sent directly to the PSP. No intermediate host must exist for distribution of cardholder data.	
A:20	It is suggested that sequence numbers are used to create aliases. If a hash or token are used to create an alias from a card number, the card number must be combined with a random factor, i.e. a salt. Salts, tokens and hashes must be calculated in accordance with industry best practices.	

The cardholder identification against the merchant

A:21	The cardholder must be identified by user ID and password.	
A:22	The user ID must be at least six characters.	
A:23	The password must be at least six characters. Minimum two and maximum four characters shall be numbers.	
A:24	The dialogs for managing user IDs and passwords are to be protected according to industry best practices for data communication (SSL/TLS).	

Change of cardholder data

A:25	Any change of cardholder data shall be made in direct dialogue between the PSP and the cardholder.	
A:26	The PSP must notify the cardholder through e-mail or text message (SMS) when any account data is updated.	

The payment dialogue

A:27	The PSP can choose to display the last four digits of the card number to give the cardholder the opportunity to choose which credit card to be charged.	
A:28	An approval of a payment is only valid for one purchase.	
A:29	After 15 minutes' inactivity, a logon shall expire	

Best Practice	Security requirement	Comments
A:30	Receipts must not contain more than the last four digits of the cardnumber.	

Special requirements for Mobile apps

A:31	The app must not store any cardholder data in the cardholder mobile device except in truncated form in accordance with PCI DSS.	
A:32	Logs in the mobile device must not contain any cardholder data.	
A:33	Any information about previously performed purchases that have been sent to the mobile device must not be available to the consumer without user authentication.	
A:34	The app must not have backdoors for error-searching or remote administration.	
A:35	The app should, if possible, detect whether the device is jail-broken and deny installation if this is the case.	

Recommendations

- It is appropriate that the PSP hosts the choice of payment method and the final confirmation of the purchase. This is to enable CVV2/CVC2 input and possible future support for 3-D Secure. In addition, it provides better means for detecting who carried out the purchase.
- It is advisable that fraud checks are made on these types of purchases, i.e. buying patterns are tracked, amounts are checked and geographic controls are made.
- It is recommended that maximum daily amounts are used.

Appendix A – Classification of Mobile Solutions

Four scenarios for card payments via mobile devices

1. A terminal connected to a mobile phone or similar mobile device which can perform mobile traffic.
    a. No cardholder data should be entered via the mobile phone or similar device. If the device is used as an Electronic Cash Register, it must be validated that it does not handle electronic cardholder data.
    b. The terminal must be E2EE-validated or P2PE-certified.

    The validation requirements are presented on http://www.pan-nordic.org/PanNordicCard/PCI-and-Security/Validation.aspx under the header **Terminals and Electronic Cash Registers (ECR)**.

2. Cloud services accessed via a mobile phone or a similar device.
    a. Enrolment: The cardholder shall be verified with strong authentication via an approved method[3] either against the cloud or against the application before the first transaction is performed or during one the first three purchases. Enrolment at the merchant site could also be possible, but needs to be discussed with the acquirer.
    b. A hosted cloud service shall be used.
    c. All parts of the cloud service shall be PCI DSS validated. Guidelines are found in PCI DSS 2.0 Cloud Computing Guidelines.
    d. All parts of the closed service should confirm via self assessment that they comply with all requirements presented below.
    e. The app in the mobile phone or similar device shall comply with PCI DSS, meaning no cardholder data is stored after the transaction.

    A requirements checklist is presented above.

3. NFC on the mobile: NFC sticker on the mobile phone.
    a. No acquirer-related requirements.

4. NFC in a secure element[4] in the mobile device: An application residing on a Secure Element performing the payment functions, as dictated by the Mobile Contactless Payment issuer, over NFC.
    a. Please contact PNC on: mail (a) pan-nordic.org for further information.

[3] The method must be approved by the issuer. One example is 3-D Secure.
[4] A tamper-resistant platform (device or component) capable of securely hosting applications and their confidential and cryptographic data (e.g. key management) in accordance with the rules and security requirements set forth by a set of well-identified trusted authorities. Examples include UICC, embedded Secure Elements and removable Secure Elements such as secure micro SD cards (to be inserted in the mobile phone or embedded in a carrier, e.g., a sleeve).