Rapport du PCI DSS

PCI DSS

Version 1 le 02/07/2019

I. Definition of PCI

- PCI denotes debit, credit, prepaid , e-purse, ATM and Pos cards and associated business.
- PCI consists of all organizations which store, process and transmit cardholder data, most notably for debit cards and credit cards

II. History

2006 : PSI SSC
2014 : 688 organizations / 61 financial institutions / 275 merchants
2014 : Magnetic stripe system
2015 : EMV system for IC cards capable of POS and ATM

III. 6 Groups 'Control Objectives'

1) Build and maintain a secure network and systems
2) Protect cardholder data
3) Maintain a vulnerability management program
4) Implement strong access control measures
5) Regularly monitor and test networks
6) Maintain an information security policy

IV. 12 Requirements for compliance

1. Installing and maintaining a firewall configuration to protect cardholder data
2. Changing vendor-supplied defaut for systems passwords and other security parameters
3. Protecting stored cardholder data
4. Encrypting transmission of cardholder data over open/public networks
5. Protecting all systems against malware and performing regular updates for anti-virus software
6. Developing and maintaining secure systems and applications
7. Restricting access to cardholder data to only authorized personnel
8. Identifying and authenticating access to system components
9. Restricting physical access to cardholder data
10. Tracking and monitoring all access to cardholder data and network resources
11. Testing security systems and processes regularly
12. Maintaining an information security policy for all personnel

V. Methodology

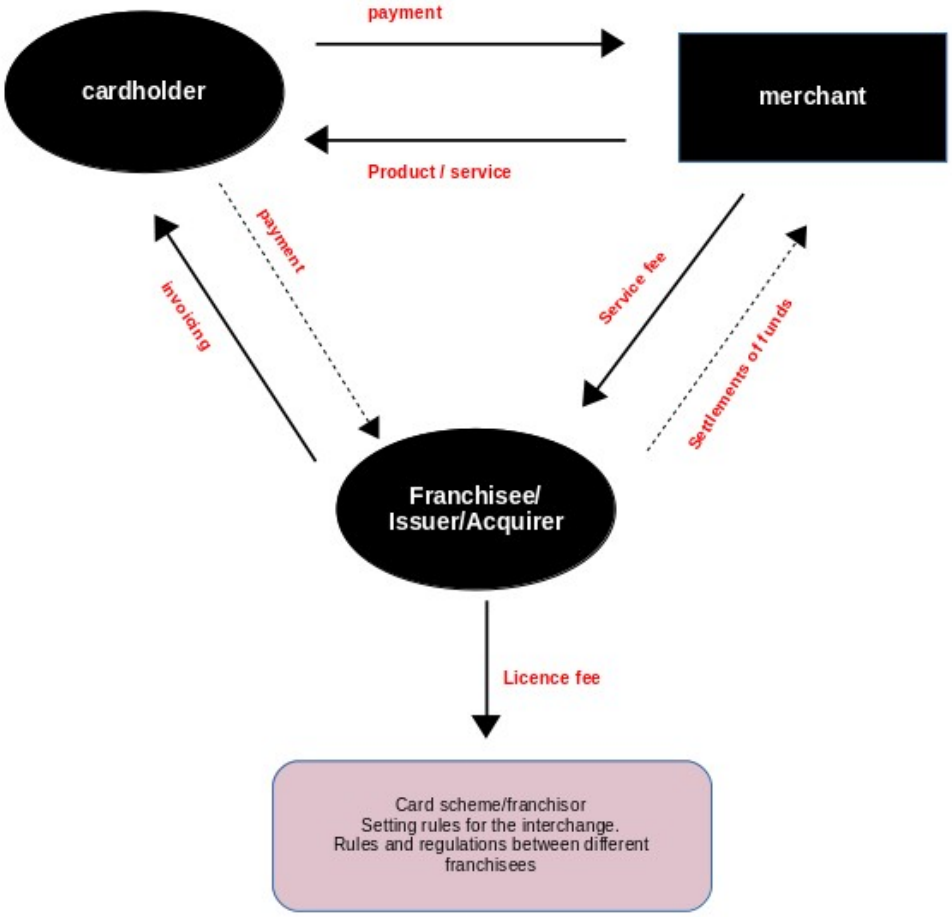
VI. Card brands

- American Express

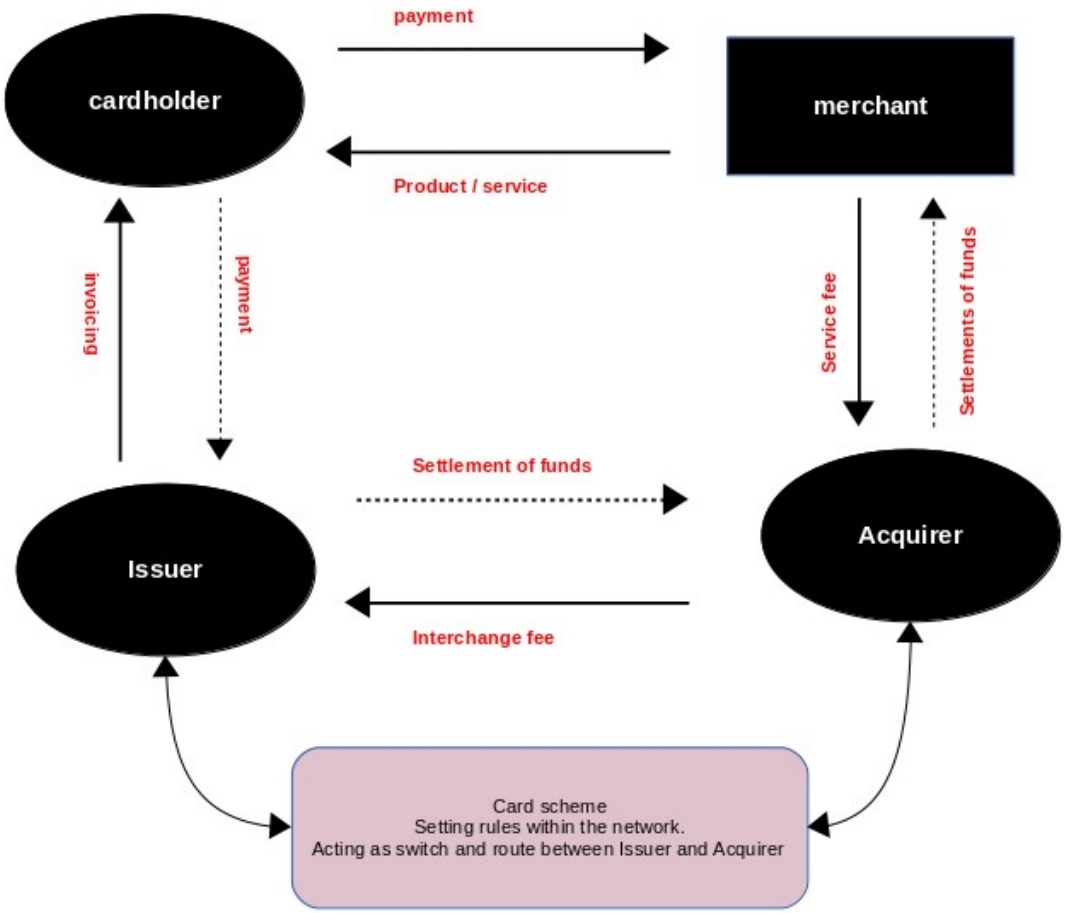
- Discover Financial Services
- China UnionPay
- Japan Credit Bureau
- MasterCard Worldwide
- Visa International

VII. Card schemes

Three-party scheme (closed scheme) :



Four-party scheme (open scheme) :



VIII. Compliance levels

- L1 : Over 6 million transactions annually
- L2 : Between 1 and 6 million transactions annually
- L3 : Between 20,000 and 1 million transactions annually
- L4 : Less than 20,000 transactions annually

IX. Documents

- Infographics
- ATM
- Authentication
- e-Commerce
- EMV
- Intro to PCI
- Logging
- Mobile
- Payment Terminal Security
- PCI DSS General
- Penetration Testing
- Phishing
- RFC Process
- Risk Assessment Guidance
- Security Awareness Program
- Skimming prevention
- Small merchants
- SSL/TLS
- Telephone-based payments
- Third-party relations
- Tokenization
- Virtualization & Cloud
- Wireless

X. Annexes

PCI : Payment card industry
DSS: Data security standards
SSC: Security standards council
EMV: Europay, Mastercard and Visa
POS : Point of sale
ATM: Automated Teller Machine
QSA: Qualified security assessor (**External**)
ISA : Internal security assessor (**Internal**)
ROC: Report on compliance (**large volumes of transactions)**
SAQ: Self-assessment questionnaire (**small volumes of transactions)**
CDE: Cardholder data environment
WLAN : Wireless LAN
RFC : Request for comments