CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

« Recommandations pour la sécurité des paiements par internet », de la BCE, et PCI-DSS

Annabelle Travers-Viaud

Responsable Pôle Conseil et Audit SSI

Bull Security Solutions

Agenda

- Recommandations de la BCE, et PCI-DSS : Convergence et divergence :
  - Objectifs
  - Cibles visées
  - Applicabilité / exigibilité
  - Périmètre
  - Exigences
  - Les futures recommandations

Les textes de la BCE et de PCI-SSC

- BCE : « Recommendations for the security of internet payments »
  - Par le Forum SecuRe Pay, créé en 2011
  - Participants : Banques Nationales européennes, autorités de contrôle et Commission européenne
- PCI-DSS : Payment Card Industry – Data Standards Security
  - Par le PCI-SSC , réunissant les grands réseaux de cartes (« card brand »)

Objectifs

- Des buts partagés :
  - lutte contre la fraude
  - Et prévention des fuites des données sensibles permettant le paiement
    - 56% de la fraude par les transactions « Carte-non-présente »
    - **Soit : 665 M€ en 2011 !**
- Mais aussi :
  - Pour le Forum : protection du consommateur
  - Pour PCI-DSS : limitation des fuites massives de numéros de cartes bancaires

Deux démarches parallèles

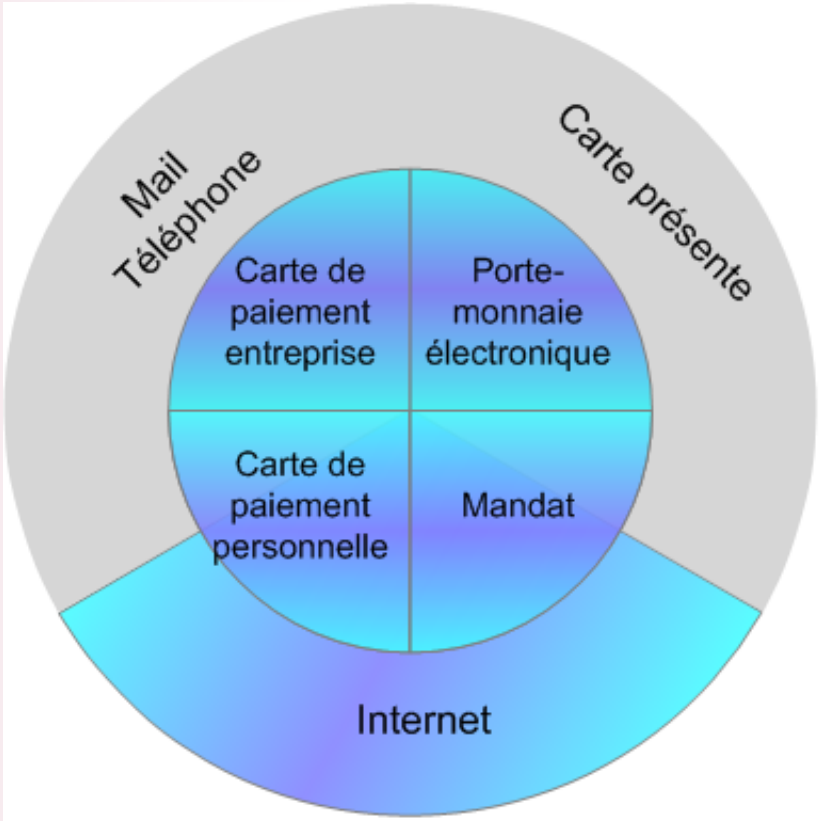
- 2006 : PCI-DSS v1.1
- 2007 : Directive n°2007/64/EC « Payment Services » (PSD)
- 2010 : PCI-DSS V2
- Janv. 2013 : Parution de "Recommendations for the security of internet payments"
- Nov. 2013 : Parution de PCI-DSS V3
- **1/02/2015 :** Application obligatoire des Recommandations
- 2016 : Application de PCI-DSS V3

Des cibles communes

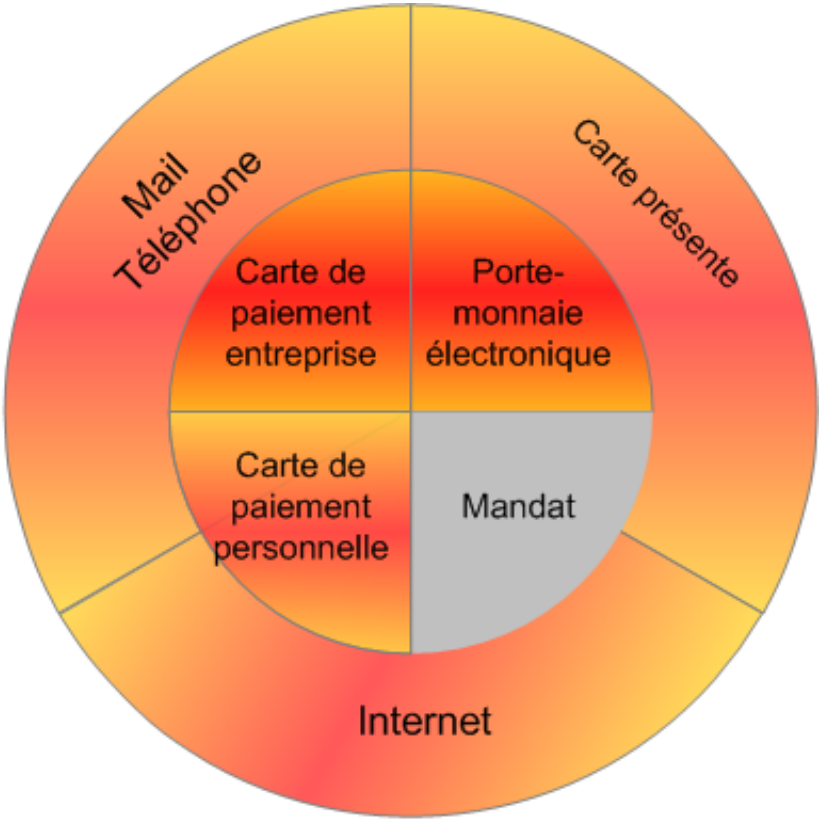
- BCE : « tout fournisseur de service de paiement sur Internet, installé dans l'UE »
  - PSP (Payment Service Provider) & GA (Governance Authorities)

- PCI-DSS : « toute entité stockant, recevant ou traitant des numéros de cartes bancaires (PAN) »
  - Banques acquéreurs
  - Marchands (e-Commerce et boutiques physiques)
  - PSP
  - Emetteurs

Des périmètres complémentaires



Recommandations de la BCE



PCI-DSS

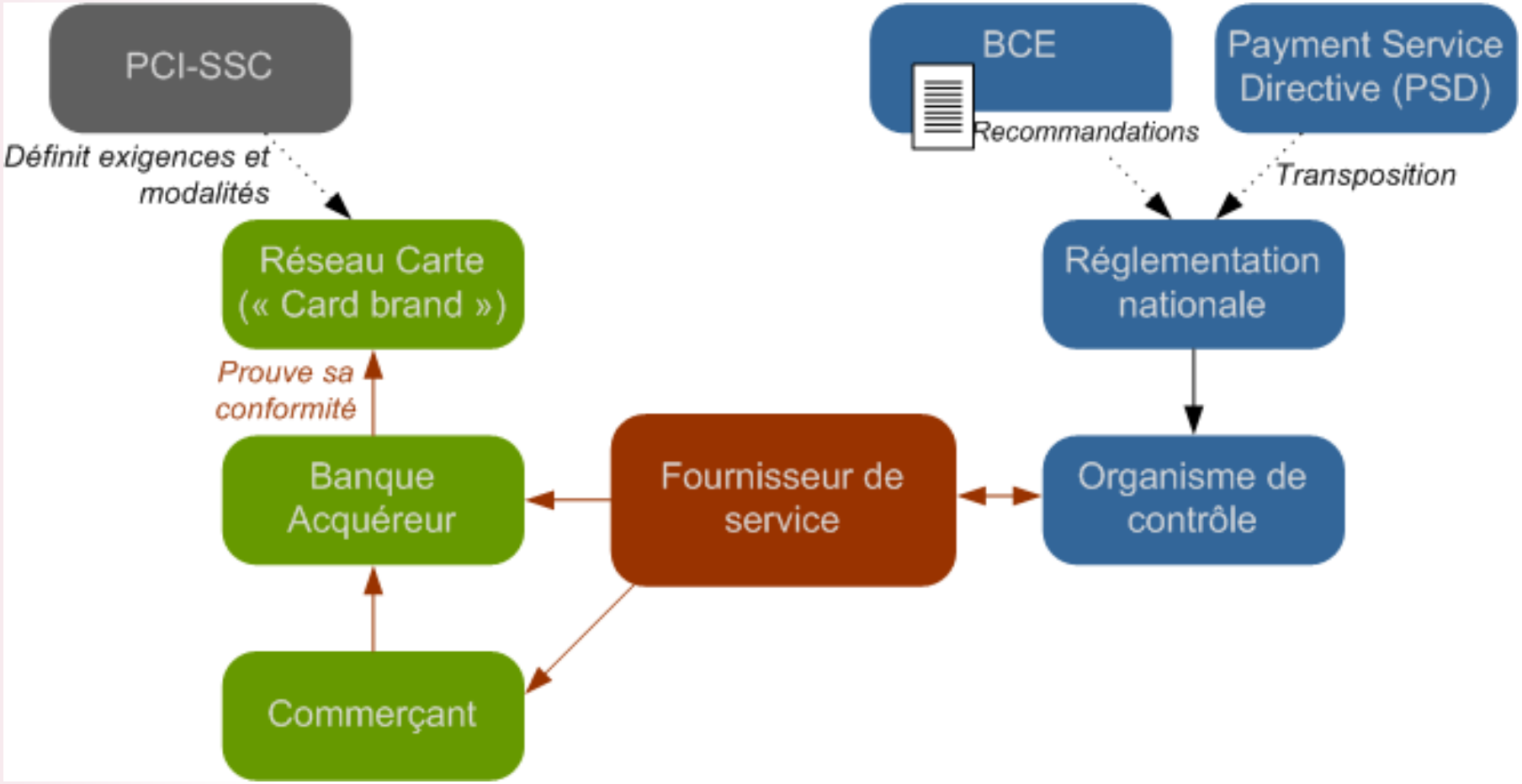
Des gestions de la conformité…

Principes retenus

- Par la BCE :
  - Démarche « comply or explain » plutôt que conformité stricte
  - Key Considerations (KC) vs Best Practice (BP)
  - Analyse des risques

- Par PCI-DSS :
  - Conformité stricte à 100% des exigences

… Et de l'applicabilité distinctes



… mais des exigences concordantes

BCE	Exigences	PCI-DSS
KC 4.1	Séparation des rôles et responsabilité Droits d'accès au « plus juste » Séparation des environnements de développement	6.4.1, 7.1.1
KC 4.3	Tracer et contrôler les accès logiques et physiques	7.2, 10.2, 10.6
KC 4.4 KC 4.5	Contrôle des risques liés aux changements Scans réguliers de vulnérabilités	11.2, 11.3
KC 4.7	Responsabilisation des tiers	12.8.2
KC 11.2	Chiffrement des flux	4.1, 3.4
KC 11.3	Conservation minimale de données sensibles	3.1, 3.2
BP 11.1	Sensibilisation des personnels	12.6

Prochaines recommandations de la BCE

- PAAS : Payment Account Access Service
  - ❖Gestion de « porte-feuille / e-Wallet »
  - ❖Consolidation de comptes de paiement sur internet
  - ❖Initialisation de transactions à partir d'un PAAS
    - Janvier-Avril 2013 : Consultation publique

- Mobile payments :
  - Novembre 2013 : consultation publique

Grands principes retenus par la BCE

- Applicables aux : PAAS / Internet Paiements / Mobile

- 4 grands principes :
  1. Appréciation régulière des **risques**
  2. **Authentification forte** du consommateur
  3. Processus efficaces de **surveillance** des transactions
  4. Education et **sensibilisation** des consommateurs

Textes de référence :

- PCI-DSS V3.0 :
  - https://www.pcisecuritystandards.org/documents/pci_dss_v3.pdf
- Directive européenne n°2007/64/EC « Payment Services Directive » (PSD) :
  - http://ec.europa.eu/internal_market/payments/framework/text/index_en.htm
- Recommendations for the security of internet payments :
  - http://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf
- Recommendations for the PAAS services :
  - http://www.ecb.europa.eu/pub/pdf/other/recommendationspaymentaccountaccessservicesdraftpc201301en.pdf
- Recommendations for the security of mobile payments :
  - http://www.ecb.europa.eu/paym/cons/pdf/131120/recommendationsforthesecurityofmobilepaymentsdraftpc201311en.pdf

Merci de votre attention

- Merci également à :
  - Romain Santini
    - » Consultant Sécurité, Bull
  - Sébastien Gelgon
    - » Ingénieur d'affaires, Bull