

CV d'Eric Poupon
Expert Monétique, sécurité, conformité PCI, LCLF¹

SYNTHESE PROFIL

- Professionnel expérimenté, avec :
 - Une **connaissance fonctionnelle très complète de la monétique**, tant bancaire que privative. Cette expertise concerne à la fois les cartes, les terminaux, les serveurs d'autorisations, les outils émetteurs et acquéreurs de surveillance et de lutte contre la fraude, la réglementation (**PCI...**), 3D-Secure, le **sans-contact**, le **paiement par mobile...**
 - Une maîtrise de l'implémentation des **fonctions cryptographiques** (symétriques et asymétriques, mise en œuvre de **boîtiers cryptographiques « HSM »**).
 - Une solide culture financière, juridique et bancaire permettant une grande adaptabilité.
 - Une capacité à **traiter tout problème de fraude et de sécurité**, même dépassant le périmètre de la monétique.
- **Corédacteur de deux standards internationaux de sécurité** qui font référence dans la monétique pétrolière.
- Anglais courant (TOEIC 930)

DOMAINES D'EXPERTISE

Métiers

- MONETIQUE EMETTEUR
 - Traitement des cartes EMV, CPA, M/Chip Advance, à piste ISO 2 (bancaires ou privatives), sans-contact NFC (avec ou sans secure element), PME, porte-jetons, applications puce privatives (lavage, café...) ...
 - Serveurs d'autorisations, systèmes de surveillance et d'analyse comportementale...
- MONETIQUE ACQUEREUR
 - Systèmes d'acquisition et d'acceptation (CB5...), vente à distance
 - Terminaux de Paiement Electronique (TPE/TPV), Connexion sous IP
 - Systèmes de surveillance commerçants
 - Echange des transactions financières ISO 8583 et variantes : bancaires (CB2A/CB2C...), pétrolières (IFSF)...
- MONETIQUE GENERALE
 - Traitement ou prévention des problèmes de fraude (domaine de compétence applicable en partie à la fraude non monétique)
 - Sans-contact (ISO 14443 et déclinaisons : Paypass...), nouveaux modes de paiement (GSM, SIM-centrique ou µSD (micro-SD), HCE, wallets OTA non NFC...)
 - Environnement juridique et réglementaire : SEPA, PCI-DSS, litiges interbancaires... Evolution de la réglementation interbancaire, Mastercard, Visa, PCI, participation à un comité international de normalisation de la monétique pétrolière
- AUTRES DOMAINES DEPASSANT LE DOMAINE DE LA MONETIQUE STRICTO-SENSU
 - Cryptographie : proposition et implémentation d'algorithmes cryptographiques, mise en place d'architectures de clés (en HSM, hors HSM)
 - Compliance avec les standards et obligations de sécurité : ISO 27k, PCI, CRBF 97-02, CNIL...
 - Environnement réglementaire des jeux en ligne (ARJEL...)
 - Connaissances juridiques, comptables et financières étendues.
 - Gestion budgétaire

¹ LCLF = Lutte Contre La Fraude

Méthodes

- Gestion de projet (méthode du Crédit Agricole MCPC V7, proche de Merise)

Techniques

- PRODUITS : HSM Bull BNT/Crypt2Pay, Crypt2Protect, TIM Risk, TIM Fraude, simulateur Integri.
- SGBD : (à rafraichir) Access, Proclarity, tableaux croisés dynamiques Excel.
- LANGAGES : (à rafraichir) Visual Basic, divers langages de macro-commandes de tableurs.
- AUTRES : Divers logiciels de cryptographie symétrique ou asymétrique (implémentation de 3DES, AES, RSA, dérivation de clés, DUKPT, hashage...), PKI, organisation et procédures afférentes...

Exemples d'interventions possibles

- Audits de sécurité, évaluation de la sécurité d'un système de paiement et préconisation de mesures correctives
- Conseil achat de systèmes monétiques et de sécurité, de cartes, de terminaux, de prestations bancaires (pour les commerces)...
- Conseil vis-à-vis de la conformité à PCI-DSS, analyse d'écart entre l'état d'un SI et ce standard
- Identification de scénarii de fraude, proposition et mise en œuvre de parades organisationnelles ou techniques
- Etudes d'opportunités, d'impacts, études et cartographies de risques.
- Définition des contrôles et paramètres du serveur d'auto, sur terminaux, dans la puce, pour un nouveau moyen de paiement par exemple...
- Assistance au déploiement de logiciels (outil de surveillance de l'activité monétique des commerçants...)
- Vérification de cahiers de recette et pilotage de recettes utilisateurs pour des système réclamant une forte expertise technique (cryptographie, sécurité) ou/et métier (monétique), organisation et encadrement d'alpha tests, conception de tableaux de bord de suivi (déploiement de nouvelles technologies cartes)
- Rédaction et mise en place de Procédures
- Formation, Rédaction des documentations

TRAVAUX DE NORMALISATION

- Corédacteur de deux standards internationaux de sécurité pour la monétique pétrolière :
 - IFSF RECOMMENDED SECURITY STANDARDS FOR POS TO FEP AND HOST TO HOST EFT INTERFACES
 - IFSF RECOMMENDED KEY MANAGEMENT METHODS FOR POS TO FEP AND HOST TO HOST EFT INTERFACESCadre juridique et réglementaire : pour le compte d'un client à l'association internationale des pétroliers « IFSF » - cf. www.ifsf.org
- Participation à la constitution d'un corps de règles de protection physique des PKI applicable à la monétique acquéreur bancaire française à l'association d'acteurs de la monétique « Concert International » - www.concert.asso.fr

PUBLICATIONS ET CONFERENCES

- Le Courrier de la Monétique n° 498 (15 mai 2009) : interview « Sur l'authentification forte, les banquiers sont partagés »
- 01 Informatique n° 1990 (16 avril 2009) : article « Peu de cohésion dans la protection des données de cartes bancaires »
- Club CSA (27 mars 2009) : conférence « Standards et obligations de protection des données cartes : PCI-DSS et autres »

FORMATION ET LANGUES

Formation

- Formation académique initiale (1988-1991) :
 - DESCAF (diplôme de fin d'études d'ESC obtenu à Sup de Co Montpellier, électif "Marchés Financiers" en seconde année, option "Contrôle de Gestion" en troisième année). Major de l'option et 2^{ème} de la promotion 1991 de l'ESC.
 - Bac C (mathématiques et sciences physiques, 1985)
- Formations professionnelles postérieures aux études initiales :
 - 2005-2007 Business Object, boîtiers cryptographiques HSM Crypt2pay (par Bull), formations managériales (Logica/Unilog (à présent CGI)), sécurité du SI.
 - 2001 Formation MCPC V7 : méthode de conduite de projets du Crédit Agricole, proche de Merise.
 - 1996-2005 Formations informatiques diverses :
 - Progiciel de crédit-bail immobilier ORFI CBI.
 - Visual Basic.
 - Access, Proclarity, Business Object.
 - 1998-2004 Formations techniques :
 - - Réseaux de télécommunication.
 - - Moyens de paiement (interne Crédit Agricole), monétique, EMV.
 - - Cryptographie (interne Crédit Agricole).
 - Deux formations comptables par Francis Lefebvre :
 - Arrêté des comptes (2001) et intégration fiscale (2004).
 - 1996 UV relations juridiques du DECF (Conservatoire National des Arts et Métiers) :
 - - Droit social.
 - - Droit commercial.
 - - Droit pénal des affaires.
 - - Droit des sociétés.

Langues

- Anglais Courant (TOEIC : 930 points)
- Espagnol Aisé
- Turc, russe, hindi Conversation de base (capable d'une conversation de base après quelques heures de révision)
- Vietnamien, arabe Notions

EXPERIENCE

2005 – aujourd’hui UN DES LEADERS MONDIAUX DU PÉTROLE – Directions OCE (Opérations Cartes Europe) & SMR (Stratégie, Marketing et Recherche)

Expert en cryptographie et sécurité monétique

- Support et conseil métier en LCLF² et sur la composante sécurité de tous les projets cartes
 - Conseil opérationnel sur le volant sécurité de tous les projets monétique sur le périmètre Europe.
 - Choix des techniques de chiffrement de données monétiques sensibles.
 - Conception et gestion de l’architecture cryptographique des systèmes monétiques. Inventaire et description des clés de service, des clés techniques de stockage et de diffusion, du chiffrement, des choix d’authentification (PKI, choix des primitives (AES vs 3DES)...)
 - Rédaction d’une procédure complète de gestion des clés cryptographiques dans le système actuel.
 - Description des apports, impacts et fonctions cryptographiques du futur système monétique (comparatif entre plusieurs grands choix) et participation aux choix d’arbitrage.
 - Elaboration d’une solution innovante d’authentification porteur et carte.
 - Conseil LCLF².
 - AMOA, rédaction des expressions de besoins et assistance à la mise en œuvre (en particulier pour les réseaux de HSM).
 - Proposition de solutions de sécurisation compatibles avec le matériel d’acceptation hétérogène de différents pays (Portugal, Russie, Afrique du Sud...)
 - Assistance à l’achat du matériel cryptographique (rédaction de l’appel d’offre, short-listage des fournisseurs, participation au choix final en tant qu’expert métier), conseil achat pour des systèmes monétiques non dédiés à la sécurité (participation aux commissions d’appels d’offres).
 - Participation à la définition des contrôles des serveurs d’autorisations européens SAE & SAA.
 - Participation à des travaux relatifs à PCI-DSS.
 - Travaux communautaires sur la sécurité et la prise en compte d’EMV et du sans-contact dans le contexte international du monde pétrolier.
 - Participation à des négociations avec d’autres acteurs monétiques : normalisation internationale de la monétique pétrolière, négociations sur le contenu du SEPA Cards Standardisation “Volume”, négociations directes avec PCI-SSC, interopérabilité avec des partenaires dans le cadre d’acceptations croisées...
 - Conseil métier sur les processus monétiques actuels : procédures dégradées...
- Environnement : Monétique privative, implémentations à base de primitives cryptographiques symétriques et asymétriques, EMV, applications de paiement privatives, normes pétrolières IFSF, HSM (Bull Crypt2Pay et autres).

2015 – aujourd’hui MISSIONS PONCTUELLES POUR DIVERS CLIENTS

Missions ponctuelles en sécurité auprès de divers clients, principalement des entreprises innovantes de tailles intermédiaires

- Contenu des missions confidentiel comme lié à des nouveaux produits / marchés : évaluation de sécurité et/ou conseil de politique opérationnelle vis-à-vis des obligations réglementaires en termes de sécurité.

² LCLF = Lutte Contre La Fraude

2013 - 2014

ENTITE MONETIQUE D'UN DES PREMIERS GROUPES BANCAIRES EUROPEENS

Gestion des clés et déploiement de HSM pour le Département Sécurité et contrôle des Risques

- Design et règles de gestion des clés cryptographiques pour les projets nouveaux
 - Création de clés de test
 - Rédactions de règles de gestions afférentes
 - Rédaction des actions à faire en cérémonie de clés de production
- Assistance au déploiement d'un réseau de HSM pilotés à distance
 - Documentation des paramètres de personnalisation et de connexion
 - Rédaction des procédures d'exploitation
 - Support technique
- Prestation générale de conseil en cryptographie : analyse et suggestion de remarques sur des documents supports des réunions au Groupement des Cartes Bancaires (GCB) par exemple...

- Environnement : monétique bancaire EMV, dématérialisation, KMC & HSM Bull Crypt2Pay et Crypt2Protect, plus marginalement Thales CM 2xx & IBM 4764 (prédécesseur du 4765), Cardink.

2013

UN EMETTEUR DE CARTES DE PAIEMENT

Mission de conseil pour la création d'une nouvelle carte à puce

- Conseils correctifs quant aux choix technologiques et à la conception générale.
- Encadrement d'un autre consultant sénior affecté à plein temps sur la mission.
- Mise en place d'une PKI.

- Environnement : monétique privative, ISO 7816 et applications de paiement associées, PKI.

2012 – 2013

ENTITE MONETIQUE D'UN DES PREMIERS GROUPES BANCAIRES EUROPEENS

Mission PCI-DSS pour le Département Sécurité et contrôle des Risques

- Conformité PCI-DSS des systèmes monétiques du Groupe non centralisés chez le client.
 - Accompagnement des entités régionales et filiales du Groupe.
 - Les filiales concernées sont surtout les filiales européennes (langue de travail = Anglais).
 - Nature de l'intervention : conseil sur la méthodologie de conformité, formation, analyse d'écart pour certains systèmes monétiques régionaux.
- Adaptations ponctuelles de la politique de sécurité du client
- Assistance ponctuelle à la communication et à la négociation avec des interlocuteurs anglophones.
- Conseil achat dans les acquisitions de systèmes ou solutions monétiques
- Intervention seul en 2012 et en pilotage d'un autre consultant en 2013 et jusqu'en janvier 2014.

- Environnement : monétique bancaire, sécurité des opérations cartes, contexte juridique et réglementaire associé.

2011

MASTERCARD

PSI - Politique de Sécurité de l'Information

- Examen de l'ensemble des documents et procédures de sécurité de Mastercard Worldwide et de Mastercard France.
- Analyse critique en termes de pertinence et de conformité aux normes sectorielles (PCI-DSS en particulier), et formulation des améliorations à apporter.
- Réécriture de certains des documents.

- Environnement : règles juridiques et réglementaires du domaine bancaire (PCI-DSS et autres).

2011

ENTITE MONETIQUE D'UN DES PREMIERS GROUPES BANCAIRES EUROPEENS

Intérim d'un Chargé d'Etudes Sénior et Expert Sécurité en congé longue durée

- Adaptations des paramètres EMV de personnalisation carte et des serveurs d'autorisations aux évolutions réglementaires Mastercard.
- Etude risques et spécification de paramètres d'un nouveau moyen de paiement sur téléphone mobile utilisant une micro-SD (μ SD) plutôt que la carte SIM.
- Etude sur les possibilités offertes par le futur standard EMV Mastercard M/Chip Advance.
- Conseil pour la sécurisation des implémentations EMV contact et sans contact.
- Etudes et expressions de besoins concernant l'implémentation de 3D-Secure (internet sécurisé)
- Suivi du déploiement et de la fraude en mode 3D-Secure.

- Environnement : EMV, M/Chip, VSDC, PayPass, VCPS, paiement sur téléphone mobile, 3D-Secure, μ SD.

2010 - 2011

PMU

Accompagnement en matière de sécurité d'un programme de refonte du SI client, dans le nouveau contexte réglementaire applicable aux jeux en ligne

- Analyses de risques sur chaque projet du programme de refonte du SI.
- Accompagnement des projets en matière de sécurité, adapté à leur stade d'avancement en début de mission :
 - Audit sécurité sur un projet de gestion des campagnes marketing déjà en cours de développement au moment du début de la mission et préconisation de mesures correctives.
 - Analyses de risques.
 - Participation à la rédaction d'un appel d'offres pour un projet support client via un outil de support en ligne puis participations au dépouillement (analyse et notations des réponses pour les aspects sécurité).
 - Relecture corrective d'expressions de besoins ou de spécifications fonctionnelles sur divers projets en début de cycle pour prendre en compte les impératifs de sécurité et réglementaires (ARJEL...)
- Conseils ponctuels sur certains aspects réglementaires spécifiques (ARJEL, PCI...)

2009 - 2010

ENTITE MONETIQUE D'UN DES PREMIERS GROUPES BANCAIRES EUROPEENS

Suivi des risques sur l'ensemble des chantiers d'une refonte complète des fonctions monétiques et moyens de paiement du client, y compris un membre principal français et filiales étrangères

- Travaux d'organisation et de pilotage pour s'assurer du traitement exhaustif des aspects risques et sécurité de chaque chantier de la refonte.
 - Animation de comités de suivi des risques
 - Relecture de livrables sécurité (vérification des analyses de risques...)
- Conseil métier sur certains chantiers :
 - Accompagnement dans le choix de systèmes de gestion du risque et de détection de fraude, y compris participation à des commissions d'appel d'offres
 - Relectures correctives de cahiers des charges
 - Compatibilité des solutions avec PCI-DSS...

2009

iBP (Informatique des Banques Populaires)

Expertise PCI-DSS

Support à la demande à une équipe du prestataire GFI Monetic en charge d'évaluer le coût de la conformité au standard de sécurité des données cartes PCI-DSS.

2009

UN PRESTATAIRE DE SERVICES DE PAIEMENT

Accompagnement d'un nouvel entrant sur le marché de l'acquisition monétique

- Accompagnement / dossier CECEI de création d'un Etablissement de Paiement tel que prévu par la récente directive européenne sur les services de paiement (2007/64/CE).
 - Etat des lieux, constitution du dossier en binôme avec un autre consultant senior.
 - Traitement de tous les aspects liés aux obligations de sécurité.
 - Première phase du dossier acceptée par la Banque de France (livrable de la mission).

2009

CLUB MED

Mission de conseil sur la politique de sécurité du Groupe – Directeur de mission

- Etat des lieux, écarts entre l'existant et les différents standards professionnels de sécurité (PCI-DSS en particulier) et obligations légales.
- Contexte d'acceptation de cartes de paiement dans 40 pays avec autant d'environnements juridiques et réglementaires.
- Identification des scénarii possibles, recommandations.

2008 – aujourd'hui

Interne employeur

Responsable Offre Sécurité ou Sécurité et Monétique selon les périodes

- Formalisation, gestion et promotion de l'offre monétique, sécurité & LCLF (lutte contre la fraude)
 - Identification et fédération des compétences.
 - Conception des documentations à usage commercial et interne.
 - Formation interne.
 - Représentation de l'employeur à diverse instance nationales d'acteurs de la profession (Concert...)
- Conception et enseignement de formations commercialisées
 - Cryptographie.
 - PCI-DSS et standards de sécurité des données monétiques.

1997 - 2005

CREDIT AGRICOLE CARDS & PAYMENTS (à l'époque CEDICAM)

Chargé d'Etudes Senior - poste « en interne »

- Fonctions d'assistance à la maîtrise d'ouvrage et d'expert en sécurisation contre la fraude par cartes bancaires
 - Etudes préalables, collecte et expression des besoins, cahiers de charges, cahiers de recettes fonctionnelles, organisation d'alpha tests, accompagnement au déploiement d'outils monétiques...
 - Etudes et propositions de systèmes de couverture (assurances, provisions...) des scénarii de fraudes les plus graves, en collaboration avec les équipes en charge de la conformité aux normes prudentielles Bâle 2, participation aux travaux interbancaires relatifs à ce dossier.
 - Définition, pour le Crédit Agricole, de tous les paramètres risque des cartes et terminaux en conformité avec le nouveau standard international EMV.
 - Création et enseignement d'une formation interne Crédit Agricole à la gestion du risque en mode EMV.
 - Support aux autres entités de CREDIT AGRICOLE CARDS & PAYMENTS et du Groupe Crédit Agricole en matière d'expertise risque et EMV.
 - Expertise et assistance vers le Crédit Agricole (services de maîtrises d'ouvrage et de gestion bancaire de CREDIT AGRICOLE CARDS & PAYMENT, Caisses Régionales) en matière de lutte contre la fraude par cartes en général, réalisation de documentations risque, représentation du Crédit Agricole à des travaux et négociations interbancaires (évolution de la réglementation...)
- Environnement : EMV 96, EMV 2000, B0', ISO 2, CB5, Moneo, SSL, 3D, Moneo, méthodes de contrefaçon cartes, fraude commerçant, fraude VAD (Internet...), cadre juridique et réglementaire interbancaire CB, Mastercard, Visa.

1991 - 1997

CRÉDIT AGRICOLE LEASING (GROUPE CREDIT AGRICOLE SA)

Direction Informatique : chef de projet (1996-1997) – poste « en interne »

- Correction d'une reprise des données suite au changement d'un progiciel de crédit-bail immobilier.
- Correction des déversements des chaînes de gestion vers la comptabilité.

- Environnement : Orfi CBI, Règles du jeu, SIGA Comptabilité.

Direction Financière, puis rattaché la Direction Générale (1991 -1996) : contrôleur budgétaire – poste « en interne »

- Mise en place d'une comptabilité analytique.
- Rédaction de procédures comptables.
- Etablissement et contrôle des budgets de dépenses de fonctionnement (frais généraux du Groupe Crédit Agricole Leasing ramenés de 217 à 182 MF en trois ans).
- Suivi et prévisions du Produit Net Bancaire et des risques.
- Reporting et supports de communication utilisés par le Directeur Général de Crédit Agricole Leasing.
- Planification à moyen terme.
- Encadrement et formation d'une personne sur le suivi budgétaire.

- Environnement : SIGA Comptabilité, logiciels de reporting internes au Crédit Agricole, Macro-commandes Excel.