# COMPTE-RENDU REUNION

# RoadMap CNS

# 06 Septembre 2016

# Systematic Paris Région (Palaiseau)

## Table des matières

## Nos axes prioritaires

La thématique confiance numérique et sécurité représente à la fois une technologie clef «horizontale » pour le Pôle, et un marché (ou plus exactement un ensemble de segments verticaux), à l'intersection de toutes les thématiques du pôle. L'objectif de la feuille de route CN&S est de décrire les besoins, capacités ou évolutions technologiques prévisibles, enjeux, priorités et points de passage à horizon 3 à 10ans que le GT devra adresser pour garantir à la fois une maîtrise de la technologie clef « Confiance Numérique » et sa diffusion dans les marchés adressés par l'ensemble des Groupes Thématiques du Pôle.

Les réunions précédentes ont conduit à une segmentation de la feuille de route en **9 domaines d'application prioritaires** s'appuyant sur un **socle technologique commun.** Les domaines d'application prioritaires identifiés couvrent :

1. **Grands évènements / Infrastructures critiques**
2. **Ville et Territoire Numérique**
3. **Energie et fourniture de services (« Utilities »)**
4. **Industrie 4.0**
5. **Transports**
6. **Santé**
7. **Entreprise IT**
8. **Finance / Délégataires d'autorités publiques**
9. **Divertissement (« Entertainment »)**

## Capacités/besoins identifiés pour les domaines marchés

1. **Grands évènements/OIV**

    - Echange / Partage de données + support à la décision ;
    - Coordination de services ;
    - Résilience de l'infrastructure ;
    - Surveillance semi auto (analytique) ;
    - Gestion des accès ;
    - ERP de sécurité ;
    - Continuité IT/OT ;
    - Drones et capteurs, fusion de données ;

2. **Ville et Territoire Numérique**

    - Gestion des identités et de la vie privée ;
    - Plateformes transactionnelles de confiance (ex: Blablacar, eBay) ;
    - Réseaux sociaux ;
    - Echange / Partage de données + support à la décision ;
    - Objets connectés: agrégation, anonymisation des données ;
    - Mobile Edge Computing/FOG : Distribution sécurisée du calcul, stockage ;
    - connectivité … dans la ville/le territoire ;
    - Infrastructure bas coût : SCaaS ;
    - Multi tenants, multi party ;

3. **Energie et Fourniture de serviecs (Eau, …)**

- Système de contrôle C2 nouvelle génération ;
- Continuité IT/OT ;
- Systèmes ouverts et multi connectés ;
- Anonymisation et accounting de confiance (billing) ;
- Compteurs intelligents et protection de la vie privée ;
- Surveillance de l'infra (prod, distribution, …),objets connectés ;
- Données : Plateforme d'intermédiation / Services de sécurité (tiers de confiance?) ;
- Gestion des données et autorisations personnelles ;

4. **Industrie 4.0**

- Infrastructure locale (C2, réseaux, capteurs & activateurs) ;
- Migration de l'existant ;
- Utilisation de consommables / Cots ;
- Support de maintenance à distance / Télé opération  lien avec virtuel ;
- Objets connectés et réseaux WL ;
- Automatisation flux matière ;
- Sécurité manufacturing additif (gestion licences , intégrités des datas, confidentialité datas) ;
- Traitement dans le cloud ;
- Continuité IT / OT (inclus analyse de risques) ;

5. **Transports**

- Introduction d'Infrastructures ICT standard pour le contrôle (Fer.) ;
- Contrôle et signalisation (Fer.) ;
- Véhicules connectés : architecture de sécurité interne et externe
- Sécurité connectivités interne et externes ;
- « Cloudification & Appstores » ;
- Cycle de vie des logiciels embarqués et/ou téléchargés ;
- Schémas de délégation/responsabilisation ;
- Certification ;

6. **Santé**

- Anonymisation & confidentialité ;
- Télé médecine (résilience/sécurité de la chaine de bout en bout, entre médecin et patient, objets connectés) ;
- Capteurs sécurisés, basse consommation ;
- HCSS ;
- Formalisation & Standardisation des services templates (SLA avec attributs de sécurité) ;
- Vérification, Monitoring ; …

7. **Entreprise IT**

- Virtualisation --> sécurité doit s'adapter à la même vitesse que le changement des systèmes ;
- Intégrité ;
- Continuité IT (Enterprise/home) ;
- Software defined security, NFV (Network Function Virtualization), data centric security ;
- Avoir un package cyber (services / systèmes) (pour PME / Grand Public) (ex : permettre de détecter un botnet, firewall, suivi de vulnérabilités, …) ;
- Partage de données B2B : Plateformes multi modales, plateformes mutualisées ; ...

8. **Finance + délégataires d'autorités publiques**

- Sécurité du domaine financier en relation avec la régulation ;
- Anti Fraudes ;
- Crypto monnaies : usages, traçabilité, réglementation ;
- Utilisation de technologies Blockchain ;

9. **Divertissement**

- Fraudes ;
- Protection contre le vol d'identité (défense et attaque) ;
- Protection du droit des œuvres (diffusion, distribution logicielle, etc.) ;
- Sécurité de bout en bout avec restriction d'usage ;

## Socle technologique commun

Les briques ci-dessous constituent un socle commun de technologies en évolution constante et qui conditionneront de plus en plus le déploiement de solutions « de confiance » dans les domaines d'applications cités précédemment.

| **SOCLE DE CONFIANCE** | Gds événements/ OIV | Ville / territoire numérique | Energie & Utilities | Industrie 4.0 | Transports | Santé | Entreprise IT | Finances / Délégataires d'autorités publiques | Entertainement |
|---|---|---|---|---|---|---|---|---|---|
| Security as a service | X | X | X | X | X | X | X | | |
| Analytics for Security | X | X | X | X | X | X | X | X | |
| SOC | X | X | X | X | X | X | X | X | |
| Software Defined Security (détection, confinement, remédiation, reinforcement) | X | X | X | X | X | X | X | X | |
| Data security and privacy (Data life cycle, data security on privacy, multi-party computation, …) | X | X | X | X | X | X | X | X | X |
| Confiance and supply chain (Hardware/software/service) | X | | X | X | X | X | X | X | |
| Sécurité des systèmes distribués et pervasifs /ambiants / omniprésents (IoT, FOG, blockchain, …) | X | X | X | X | X | X | | | |
| Crypto (post quantique, light crypto, homomorphe, …) | X | | X | X | X | X | X | X | |
| Authent / identification / droits … des personnes / objets | X | X | X | X | X | X | X | X | X |
| Sécurité by design et logiciel (au niveau composant, à un niveau encore maitrisé) | X | | X | X | X | X | X | X | |
| Certification et homologation | X | X | X | X | X | X | X | X | X |
| Résilience | X | X | X | X | X | X | X | X | X |
| ERP de sécurité : intégration sécurité physique / logique | X | | X | X | X | X | X | | |