DGSI - Analyse du CCTP - RDV du 10.02.2017

- Présents pour l'EMSE : David Michalon et Dominique BERTHET
- Présents pour la DGSI : Laurent BASTY, XXX, XXX

Contenu du CCTP

- CCTP trop ambitieux pour les délais souhaités
- Il faut plutôt décrire les normes de sécurité souhaitées sur les équipement que des modèles de marques existants
- Vu les délais contraints, il est déconseillé de tout intégrer de suite. L'anti-intrusion ne doit pas forcement être incluse dans ce CCTP. Idem pour le SSI. Les remontées d'alertes de chaque système pouvant maintenant facilement être agrégées via des API.
- Il faut éliminer toutes contraintes liées à un disfontionnement

Serrures Portes

- Il est conseillé de garder la possibilité d'ouvrir avec une clé en cas de panne du système. Un organigramme de gestion des clés devra être proposé. Les utilisateurs rendront leurs clés à la remise des nouveaux badges
- Pour les barillets, demander la reprise de l'existant

Réseaux et Equipements

- L'intelligence doit être au niveau des RIO (Remote Input Output)
- En cas de panne de l'UTL, le lecteur doit pouvoir fonctionner

Résilience

Le système dit être le plus résilient possible, il faudrait donc :

- Il faut évoquer le cas des coupures réseaux dans le CCTP (fonctionnement en mode dégradé, niveau d'autonomie souhaité
- prévoir une réplication et une synchronisation des données entre Saint-Étienne et Gardanne afin de garantir que chaque campus puisse fonctionner en cas de coupure réseau ou de panne du serveur principal. (VM réplicat à installer à Gardanne).

Niveau de sécurité

- Il faut impérativement décrire les niveaux de sécurité et définir les priorités.

Niveau 1

- La biométrie est la seule façon de réellement prouver que le porteur du badge est le propriétaire du badges. Un code peut être transmis à un tiers.
- Un système ANTI PASS BACK est obligatoire pour assurer le comptage. Il devra être relier au SSI.

Biométrie

- Seules les personnes devant avoir des accès de niveau 1 devront fournir leur empreinte au moment de la remise du badge sur des lecteurs dédiés.
- Cette empreinte sera stockée avec un niveau maximal de chiffrement directement sur le badge. Ainsi aucune base biométrique ne sera gérée par le système. Il y aura juste un échange (hashage) entre le badges et le lecteur.
- La demande d'autorisation à la CNIL devra être faite rapidement. Avec ce système de stockage sur le badge, elle sera simplifiée.
- Il faudra déterminer précisément les populations pouvant pénétrer en niveau 1 (Direction/DRH)

Badges

- l'authentification et les services devront être sur une carte comprenant uniquement une photo et un numéro afin de pouvoir identifier le porteur,
- Le port visible du badge dans les locaux pour tous les permanents et visiteurs devra être la règle. Des signalisations devront être mise en place à l'entrée des bâtiments pour le rappeler.
- les étudiants devront toujours avoir un badge sur eux.
- la carte d'étudiant devra être gérer de façon autonome au système.
- les badges devront être à minima du type Desfire EV1 4k afin de pouvoir héberger l'empreinte biométrique et l'ID0 du porteur chiffrée en 4096 bits (à voir pour restauration).