

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 équipements que des modèles de marques existantes
- Vu les délais contraints, il est déconseillé de tout intégrer de suite. L'anti-intrusion ne doit pas forcément 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 dysfonctionnement
- Il faut se concentrer uniquement sur le contrôle d'accès et éventuellement uniquement sur L1 et L2... (n'élimine pas les clés)
- Il faut sortir l'intégration de la MdE dans un premier temps. Elle n'apporte que des contraintes et avec le système de badge avec photo les élèves ne devraient plus pouvoir prêter leur clé à leur guise.
- Prévoir une MCO de 5 ans (Maintenance en Condition Opérationnelle)

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
- Prévoir des serrures à coupure en déclenchement
- Faire chiffrer L3 filaire et L3 radio
- La technologie RADIO offre très peu de sécurité (facilement piratable via USB, ...) et surtout peut être brouillée par le WIFI qui utilise les mêmes fréquences
- Le cout de maintenance est moindre sur un système filaire que sur un système radio.
- Garder un système double (clé/badge) va nous permettre un déploiement beaucoup plus souple

Infrastructure

- L'intelligence doit être au niveau des RIO (Remote Input Output)
- En cas de panne de l'UTL, le lecteur doit pouvoir fonctionner
- Pour la gestion des traces il faut demander des filtres précis et pertinents (par ID, ...) et surtout pas par lecteur
- Pour le déploiement il faut impérativement installer les nouveaux concentrateurs en premier

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 badge. Un code peut être transmis à un tiers.
- Un système ANTI PASS BACK est obligatoire pour assurer le comptage. Il devra être relié au SSI.
- Compter environ 10k€ par porte L1

Biométrie

- Seules les personnes devant avoir des accès de niveau 1 (ou 2 double authentification) devront fournir leur empreinte. L'enroulement se fera à la remise du badge sur des lecteurs dédiés (à prévoir).
- 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 badge 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 gérée 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).

From:

<https://portail.emse.fr/dokuwiki/> - **DOC**

Permanent link:

<https://portail.emse.fr/dokuwiki/doku.php?id=sg:gt:controleacces2017:dgsi-100217&rev=1486657315>

Last update: **09/02/2017 17:21**

