ACCUEIL CONTRÔLE D'ACCÈS 2017

Contrôle d'accès : présentation COMEX du 06.03.2017

- David MICHALON – Dominique BERTHET
    - Présentation PDF

CONTEXTE

- Système de clés coûteux, vieillissant et peu sécurisé (accès par groupes de salles, beaucoup de passes qui circulent, risque de perte du passe général).
- Organigramme complexe.
- Accès trop permissifs aux laboratoire de recherche (portes ouvertes, codes partagés…).
- Contrôle d'accès actuel peu sécurisé ; coûts d'exploitation et d'évolution élevé.

ÉTUDE DE FAISABILITÉ

- Visite d'écoles de l'IMT pour valider différents fonctionnements (TEM-TSP, TPT).
- Rencontres avec la DGSI…
- Réalisation du CCTP en se basant sur le guide fourni par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information).

PÉRIMÈTRE DU PROJET

- Reprise des points d'accès existants (Accès bâtiments, laboratoires, salles serveurs…).
- Bureaux et laboratoires pour les sites 158CF, CIS, Gardanne (Espace Fauriel en option).
- Maison des élèves de Gardanne non incluse (usages différents).
- Quid des systèmes « anti-intrusion » existants sur les sites CIS, La Rotonde, Gardanne (logiciels différents, recommandation DGSI).

OBJECTIFS

- Élever le niveau de sécurité et sûreté de l'école.
- Déployer un système résilient aux pannes (électriques ou informatiques).
- Disposer d'un système de gestion des droits (attribution / révocation) sécurisé et efficace.
- Se séparer des clés (utilisateurs).
- Disposer d'un système évolutif (évolutions patrimoine, Vigipirate, ZRR…).
- Faire maintenir la solution en mode opérationnel pour une durée initiale de 5 ans.

INFRASTRUCTURE LOGICIEL

- Choix d'une solution ouverte interopérable avec d'autres briques du SI (RH, Formation…).
- Système virtualisé et résilient (réplication Saint-Étienne / Gardanne).
- Réseaux isolés dédiés pour la solution (VLAN, VPN…).

NIVEAUX DE SÛRETÉ

- Utilisation de la biométrie.
- Unique solution pour garantir que « le porteur du badge = le propriétaire du badge » (DGSI).
- Déploiement uniquement en double authentification sur des zones stratégiques et sensibles.
- Données biométriques chiffrées et stockées sur le badge (pas de base biométrique) – Déclaration CNIL AU-052.

3 Niveaux de sûreté

- Niveau 3 : infrastructure filaire + biométrie + anti-pass back (salle blanche).
- Niveau 2 : infrastructure filaire simple ou double authentification (biométrie pour les salles serveurs, les labos sensibles : nanotechnologie, nucléaire…).
- Niveau 1 : infrastructure radio (serrure clé en secours) : bureaux, laboratoires, salles de réunion, salles de cours.

Étude sur plans validée au niveau COMDIR, RAF.

TYPE DE BADGES

- Technologie Mifare Desfire EV1 dernière génération (données chiffrées et multi-services), format carte de crédit.

3 Familles :

- Personnels + « visiteurs longue durée » : Photo + Numéro, pas de signe distinctif (logo école…).
- Élèves : équivalent carte étudiant avec mise à jour annuelle par hologramme autocollant.
- Visiteurs : Gestion à l'accueil via un module dédié.

USAGES INDUITS

- Port du badge obligatoire pour les personnels et les visiteurs (affichage à l'entrée des bâtiments).
- Si possible, organisation de l'accueil des visiteurs 24h à l'avance (quid de l'Espace Fauriel et CIS).
- Droits initiaux = accès aux bâtiments + accès restreints par profil (équipes ou services)

automatisés via l'annuaire LDAP et personnalisable par la suite.
- Circuits de validation pour la gestion des droits (application interne à prévoir).
- Laboratoires avec ferme porte obligatoire + hublots (niveau de sûreté).
- Programmation des ouvertures possible (exemple : plage horaire).
- Possibilité de verrouillage ou déverrouillage manuel en cas de problème.

BADGES MULTI-SERVICES

- Accès au locaux.
- Impressions centralisées.
- Services de restauration.

RISQUES / CONTRAINTES

- Coût global de l'opération.
- Délais de réalisation.
- Topologie actuelle des bâtiments (Saint-Étienne), contraintes sur le zonage.
- Interrogation à priori du personnel à prendre en compte (communication à prévoir).
- Déploiement en sites occupés (coactivité, planning à faire, coupures à prévoir…).

SANTÉ PUBLIQUE ET RÈGLES ASSOCIÉES

- Organisation de l'accès au logiciel et traces : groupe de travail CHSCT.
- Étude des contraintes en termes de santé publics (Onde radio) : CHSCT.
- Charte des usages et circuits de validation à produire.

PHASAGE

- Compilation des données, des plans, des questions et réponses au plus tard le 8 mars
- Publication du marché se fera au plus tard le 21 mars 2017
- Principales étapes de la phase travaux :
    - Début des prestations : Début septembre 2017
    - Serveurs et logiciel : Début septembre
        - Installation
        - Intégration des données (renseignement de la base des badges et profils)
    - Travaux, phasage par sites et bâtiments comprenant :
        - Repérage sur l'infrastructure existante
        - Pose et câblage matériels (UTL, GPI, câbles, …)
        - Modifications / adaptation des portes (Pose verrouillage, création hublot…)
        - Essais matériels
    - Formations : Début novembre
    - Bascule définitive et prise en main du logiciel : Début décembre
    - Montée en charge et mise en production : Décembre

RETOUR COMEX

- Prévoir présentation simplifiée au COMDIR du 20.03.2017.
- Prévoir présentation pour l'AG de rentrée.