Contrôle d'accès à l'Université de Rouen Normandie

Cette page décrit la mise en place de l'interaction d'ESUP-SGC (et ESUP-NFC-TAG) avec les solutions de contrôle d'accès de l'Université de Rouen Normandie.

Ainsi un établissement qui souhaite faire une intégration de sa carte Mifare Desfire dans ses solutions de son contrôle d'accès via ESUP-SGC peut s'y référer. Si vous en avez la possibilité, et pour une intégration facilitée d'ESUP-SGC avec vos contrôles d'accès, on vous suggère en effet de prendre exemple sur cette mise en œuvre effectuée à la COMUE Normandie Université et à l'Université de Rouen Normandie plus précisément.

La page Tags NFC - getting started peut être intéressante à consulter.

Plusieurs dispositifs de contrôle d'accès existent dans l'établissement :

- HOROQUARTZ
- TIL TECHNOLOGIES
- SYNCHRONICS
- …

Ils fonctionnent tous avec la technologie de badge Mifare Desfire.

Ils utilisent des serveurs différents (parfois multiples pour un même constructeur).

Intégration multi constructeurs

Pour permettre d'intégrer de multiples constructeurs de systèmes de contrôle d'accès, une application Mifare Desfire de contrôle d'accès “ComUE-NU Access Control” neutre vis à vis des constructeurs est mise en place sur les badges.

Pour cela, une demande auprès de NXP a été effectuée pour obtenir une plage d'identifiants d'application propre à l'ensemble de la COMUE Normandie Université (et à sa Léocarte) .

Cf la liste des applications enregistrées : http://www.nxp.com/documents/other/MAD_list_of_registrations.pdf (*lien cassé, il semble que cette liste ne soit plus rendue publiquement disponible par NXP*) - on y retrouve donc Normandie Université (585C).

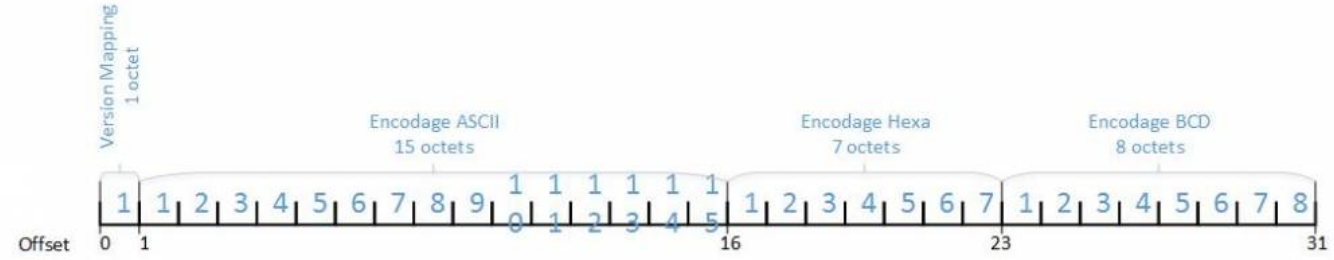
L'idée est ainsi de positionner une et une seule application Desfire de contrôle d'accès sur la carte (commune à tous les établissements normands) et de demander à chacun des constructeurs de s'y référer pour mettre en place le contrôle d'accès.
Les constructeurs ont sinon tendance à vous proposer d'utiliser "leur" application Desfire de contrôle d'accès ... sans ensuite autoriser les autres constructeurs à l'utiliser également. Cela complique alors l'intégration d'un nouveau constructeur, et n'apporte aucune plus-value. Disposer de sa propre application Desfire de contrôle d'accès ne présente de plus aucun inconvénient : pas de coût supplémentaire, etc.

Spécification de l'application Desfire de contrôle d'accès

Cette application Desfire de contrôle d'accès de la COMUE NU a pour identifiant (F5 85 C1) ; les éléments techniques retenus sont les suivants :

- l'identifiant de contrôle d'accès sur 15 chiffres
- 1 clé maitre qui protège l'application
- L'application comporte 3 fichiers, chacun étant associé à une clé de lecture différente
    - Pour chaque fichier, le “communication mode” est CYPHERED (la communication entre le badge et le lecteur est chiffrée)
- Chaque fichier commence par un octet représentant la version du mapping du fichier (valeur '30', correspondant au code ASCII de '0' pour commencer)
- Chaque fichier comporte l'identifiant de contrôle d'accès encodé dans 3 formats différents (ASCII, Hexa, BCD)
    - 15 car encodés en ASCII 15 octets
    - 15 car encodés en Hexa 7 octets
    - 15 car encodés en BCD 8 octets

Le mapping d'un fichier est donc le suivant:



Exemples:

```
Identifiant = 10720 01234 56789
=> Fichier: 0x30 - 0x31 0x30 0x37 0x32 0x30 0x30 0x31 0x32 0x33 0x34 0x35 0x36 0x37 0x38 0x39 - 0x00 0x61 0x7F
0x79 0x47 0x4D 0x15 - 0x01 0x07 0x20 0x01 0x23 0x45 0x67 0x89


Identifiant = 99999 99999 99999
=> Fichier: 0x30 - 0x39 0x39 0x39 0x39 0x39 0x39 0x39 0x39 0x39 0x39 0x39 0x39 0x39 0x39 0x39 - 0x03 0x8D 0x7E
0xA4 0xC6 0x7F 0xFF - 0x09 0x99 0x99 0x99 0x99 0x99 0x99 0x99
```

Ainsi, on peut communiquer aux différents constructeurs:

- Le N° AID MAD (F5 85 C1)
- L'ID du fichier à lire (de 0 à 31) - (0 pour le premier fichier)
- La clé de lecture (AES) (clé associée au fichier 0 pour commencer) (32 car hexa) - ! Un accord de confidentialité est signé avant ! - Les 3 clés de lecture sont stockées dans un coffre fort numérique.
- Offset et la longueur à lire selon l'encodage souhaité:
    - Offset=1 - Longueur=15 pour l'encodage en ASCII
    - Offset=16 - Longueur=7 pour l'encodage en Hexa
    - Offset=23 - Longueur=8 pour l'encodage BCD

A noter que l'ensemble des contrôle d'accès sont capables de lire directement les 15 premiers caractères (version ASCII des 15 octets) et l'encodage de ce même identifiant en Hexa et BCD ne sert finalement pas (à présent).

Génération de l'identifiant par ESUP-SGC

Pour la génération de tels identifiants et son formatage, on paramètre dans ESUP-SGC un "CardIdService" de type org.esupportail.sgc.services.cardid.ComueNuAccessControlCardIdService.

CF Configuration spécifique COMUE Normandie Université#src/main/resources/META-INF/spring/applicationContext-services.xml

Implémentation de l'application de contrôle d'accès dans esup-nfc-tag pour l'encodage de la carte

La structure de l'application de contrôle d'accès est ainsi défini dans applicationContext-desfire.xml, cf le lien suivant :

Configuration spécifique COMUE Normandie Université#src/main/resources/META-INF/spring/applicationContext-desfire.xml

Dans cette configuration, on trouve en plus de la structure Desfire, le lien qui est fait entre esup-nfc-tag et l'identifiant "access-control" - cf le bean idp2sTagWriteEsupSgc dans ce même fichier applicationContext-desfire.xml

Import des accédants et des identifiants de carte

Les différents contrôles d'accès rencontrés fonctionne de la même manière :

- On dépose un (ou plusieurs) fichier(s) CSV dans un dossier du serveur sur lequel se trouve le contrôle d'accès.
- Le fichier est automatiquement 'consommé' par le serveur (renommage avec un timestamp et modification de l'extension, le cas échéant création d'un fichier d'erreur).

Suivant les contrôle d'accès, en cas de désactivation d'une carte (on parle souvent de badge dans le contrôle d'accès), le CSV pourra contenir une ligne concernant l'ancienne carte (modification des dates de validité et du statut).

Certains contrôles d'accès ne permette également d'avoir qu'un seul identifiant de carte pour un individu. Les anciennes cartes sont de fait révoqués automatiquement si une nouvelle carte (identifiant de carte) est proposée.

L'import CSV permet en fait d'importer les identifiants de cartes et les utilisateurs eux-mêmes. Évidemment, les accès aux bâtiments sont positionnés sur les utilisateurs et non les cartes : ainsi les utilisateurs conservent leurs droits en cas de changement de carte.

Format du CSV et import depuis ESUP-SGC

Suivant le contrôle d'accès, le format de CSV en tant que fichier d'import diffère.

De plus ce format est souvent paramétrable au niveau du contrôle d'accès.

L'identifiant de la carte correspond à l'identifiant généré et stocké dans l'application Desfire de la carte.

Pour l'utilisateur, on conseille si possible d'utiliser l'eppn.

Le dépôt du ou des CSV peut être fait par ESUP-SGC lors de l'activation/désactivation/... de la carte, ce en configurant le fichier applicationContext-acces-control.xml comme on peut le voir dans cet exemple :
Configuration spécifique COMUE Normandie Université#src/main/resources/META-INF/spring/applicationContext-acces-control.xml

Le formatage du CSV est proposé par différentes implémentations de Export2AccessControlService : https://github.com/EsupPortail/esup-sgc/tree/master/src/main/java/org/esupportail/sgc/services/ac

Si l'on souhaite définir un format de CSV spécifique et non proposé par défaut dans ESUP-SGC, on peut réimplémenter dans ESUP-SGC l'interface Java Export2AccessControlService.

La transmission du fichier peut se faire en cifs, ssh, en local, etc. via VFS2 d'Apache Commons ou JCIFS : https://github.com/EsupPortail/esup-sgc/tree/master/src/main/java/org/esupportail/sgc/services/fs

Consommation du fichier CSV d'import par le contrôle d'accès.

Une fois les CSV déposés par ESUP-SGC dans un répertoire du contrôle d'accès, il faudra paramétrer ou scripter (sous power-shell) le lancement de la consommation de ces CSV par le contrôle d'accès.

- Pour Horoquartz par exemple, l'import est paramétré via le logiciel Builder (accès réservé horoquartz) et il s'exécute en tant que 'ImportEasyID' (opérateur défini dans 'Studio').
- Pour Til, une tâche programmée (sous power-shell), toutes les 5 mn, concatène tous les fichiers *.csv du répertoire d'import considéré et positionne ensuite un fichier sémaphore qui déclenche l'import.