VERS UN SGC LIBRE

Table des matières

1 - Introduction

Le présent document tente de retranscrire l'état des travaux menés à l'Université de Rouen Normandie visant à devenir techniquement autonome dans la gestion des cartes étudiants et personnels (cartes NFC multi-services appelées Léocarte). Ce document a été initié début Mars 2017, la version donnée ici a été finalisée début Avril 2017 et ne tient pas forcément compte de l'ensemble des toutes dernières réflexions, échanges et avancées.

2 - Un SGC propriétaire actuellement utilisé

A ce jour, l'Université de Rouen Normandie utilise, pour la gestion de ses cartes, un progiciel nommé EasyId et proposé par la société Horoquartz.

Ce logiciel est actuellement opéré par la COMUE Normandie Université pour les établissements membres, et couvre l'installation, la maintenance et le paramétrage logiciel du socle.

Il est ensuite utilisé et mis en œuvre par les établissements eux-mêmes.

Ce logiciel EasyId consiste en une application WEB de gestion d'identités. Au travers de *web services* et de systèmes d'export/import de fichiers plats (CSV), les établissements ont pu interfacer leur système d'information avec ce logiciel.

Cette solution mise en place est actuellement fonctionnelle mais soulève des questions, en regard notamment des points suivants:

- cette application, monolithique, a été conçue pour constituer le socle (ie le cœur) du système d'identification d'une structure telle qu'une université ; elle rentre -de fait- en concurrence avec l'architecture des SI déjà en place dans les établissements ;
- l'intégration avec le système d'information est en partie réalisée mais pas sur l'ensemble du domaine fonctionnel; exemple : l'invalidation de carte est une information qui ne peut pas être remontée par web service ou export CSV (limitation EasyId), une personne ne pouvant avoir, à un instant t, qu'une seule carte valide ;

- la solution ne couvre pas non plus tout le périmètre fonctionnel désiré ; aussi c'est à chaque établissement de développer les interfaces pour permettre aux utilisateurs finaux de demander leurs cartes (formulaire de demande de carte, mais aussi workflow de validation, paiement en ligne si nécessaire, opposition de la carte), ou encore les connecteurs pour déverser les informations de la carte dans leurs annuaires LDAP (cf paragraphe sur l'échange données) et dans les solutions de contrôle d'accès (P2S, TIL, Synchronic, …) ;
- l'application est propriétaire et l'entreprise qui nous la fournit la fait évoluer selon sa propre feuille de route ; c'est donc l'ensemble des systèmes d'information des établissements qui doivent s'adapter aux contraintes et règles édictées par l'éditeur ;
- des mises à jour ont déjà généré des instabilités, voire la perte de configurations précédemment paramétrées ;
- les matériels et technologies utilisés pour mettre en œuvre cette gestion de cartes sont relativement lourds et coûteux : pilotes et lecteurs NFC spécifiques, des machines virtuelles *java* embarquées sur le poste client, des bornes de mises à jour, … ;
- le modèle centralisé retenu peut poser potentiellement des problèmes, notamment pour planifier les opérations de maintenance, avec des impacts non négligeables sur la disponibilité voire les performances pour les établissements partenaires ; de plus, ce modèle pourrait induire des choix en matière d'échange et d'interopérabilité des SI de la COMUE qui seraient alors spécifiques au logiciel propriétaire choisi et poserait la problématique du passage à l'échelle (interopérabilité et échanges au-delà de la seule COMUE Normandie Université) ;
- citons qu'à de nombreuses reprises, des lenteurs et des problèmes de tenue à la charge ont été constatés.

Ces points soulèvent la question du coût d'une telle solution, sur le plan financier, matériel mais aussi humain (au regard de l'argumentaire avancé ci-dessus, l'impact humain en périphérie s'avère finalement lourd à très lourd).

3 - Travaux menés et montée en compétence

L'Université de Rouen Normandie a investi beaucoup de temps sur la mise en place de nouveaux services institutionnels utilisant la Léocarte (carte NFC de type Mifare Desfire).

Ces travaux ont été très concluants. Il en résulte :

- de nouveaux services, mis en production très rapidement ; citons notamment, la mise en place de la **carte culture dématérialisée** bénéficiant aux étudiants de l'Université de Rouen Normandie et de l'INSA de Rouen Normandie ; ce projet consiste en la possibilité donnée
  - aux responsables culturels des 2 établissements suscités de créditer par simple badgeage (au moyen d'un smartphone fourni par l'Université de Rouen Normandie) la Léocarte de l'étudiant.
  - aux salles de spectacles de l'agglomération rouennaise (cinéma, théâtre, opéra ...) de débiter par simple badgeage (et au travers d'un smartphone fourni par l'Université de Rouen Normandie) la Léocarte de l'étudiant pour faire bénéficier à l'étudiant d'une réduction correspondant à environ 5€ du prix initial demandé.
- la mise à disposition d'une application générique libre (*open source*) proposée et soutenue par le consortium EsupPortail (EsupNfcTag). Elle constitue désormais la brique applicative permettant d'intégrer les cartes NFC sans contact dans nos services institutionnels (à l'instar du projet carte culture).
- et enfin une montée en compétence dans le domaine des cartes sans contact de type NFC (Mifare Desfire EV1) ; l'objectif étant à terme, de pouvoir gérer ces technologies sans recours à des prestations externes ou à la sous-traitance.

4 - Architecture et fonctionnement de EsupNfcTag

Le projet EsupNfcTag a été présenté le 21 septembre 2016 à Paris-Descartes lors des EsupDays #22.

La documentation et l'ensemble des briques logicielles distribuées en open source (licence Apache V2) est également disponible sur le site officiel du consortium EsupPortail :

https://www.esup-portail.org/wiki/display/ESUPNFC

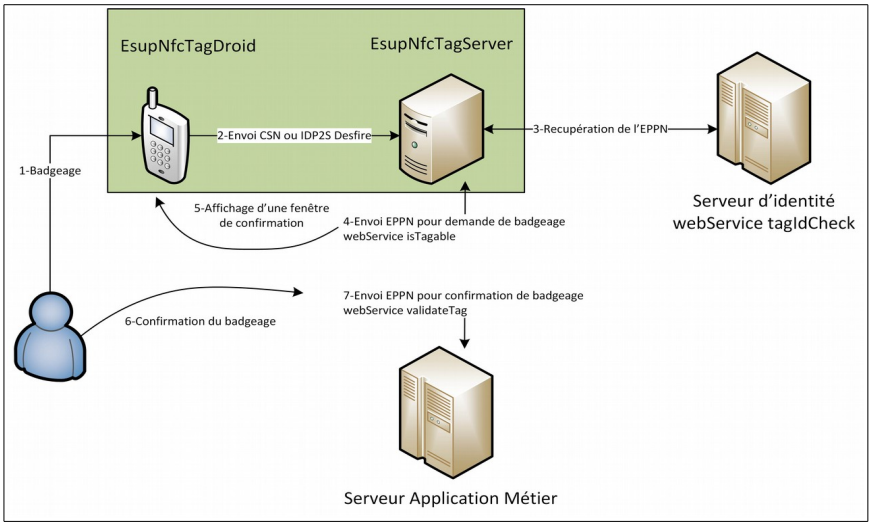
Dans les faits et pour résumer, **EsupNfcTag propose une application web et une application Android permettant à une application tierce de récupérer un identifiant stocké dans une carte NFC de type Mifare Desfire**.

Fonctionnellement, EsupNfcTag est donc très spécialisé. Techniquement, il permet à une application tierce de se décharger complètement de la complexité des technologies utilisées, à savoir la carte NFC avec sa problématique de badgeage : NFC, chiffrage et développement Android pour la partie lecteur.

EsupNfcTag peut être vu comme un micro-service et ne peut donc fonctionner seul ; dès sa conception, il a été pensé pour être facilement intégré dans une application (web) tierce ainsi qu'un système d'information existant. Aussi il propose des API permettant cette intégration, en utilisant la technologie Web «*REST*».

Ces API doivent être implémentées par les applications tierces à EsupNfcTag, notamment :

- l'obtention de l'EPPN (EduPersonPrincipalName, identifiant unique, pérenne et normalisé de l'utilisateur) depuis un identifiant de carte (CSN ou identifiant stocké dans un fichier d'une application Mifare Desfire de la carte) ; cette correspondance peut être fait depuis le LDAP de l'établissement par exemple ou depuis une base interne interfacée par web-service REST (voir à ce propos le paragraphe sur l'échange des données en fin de ce document) ; EsupNfcTag n'impose rien à ce sujet.
- la prise en compte du badgeage d'un EPPN donné.



Synoptique d'implémentation d'EsupNfcTag

L'application EsupNfcTag a été développée pour supporter l'intégration de plusieurs services d'identification (basé sur le CSN ou des identifiants de cartes différents) ainsi que plusieurs services se basant sur le badgeage, et fonctionnant dans un contexte multi-établissements.

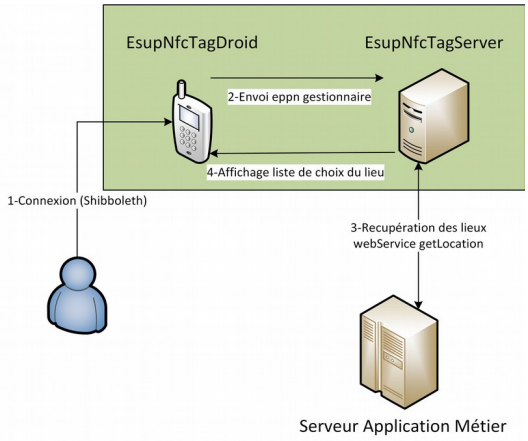
Aussi, l'utilisateur badgeant sur le téléphone, s'authentifie via le mécanisme de fédération d'identités de RENATER basé sur Shibboleth ; il choisit une «salle» correspondant à la fois à :

- un service donné par l'application tierce et disponible à l'utilisateur connecté ;
- un couple service d'identification / service consommateur de badgeage.

Cette association est configurée par un administrateur, via l'Interface Homme-Machine d'EsupNfcTag.

Cette notion de « salle » requiert l'implémentation d'une API supplémentaire pour l'application tierce consommatrice de bageages qui doit ainsi proposer une liste de « salles » pour un utilisateur badgeur donné. L'API permettant la consommation du badgeage (mentionné plus haut) prend ainsi en paramètre un nom de « salle ».

Le schéma suivant illustre le fonctionnement présenté.



5 - Perspectives : développement d'un SGC

Les connaissances et l'expérience acquises à la fois autour de la solution propriétaire *EasyId* et des projets tels que la gestion de la carte-culture nous amènent aujourd'hui à penser que l'intégration, la manipulation et la gestion des cartes des étudiants et personnels au sein des Systèmes d'Information des établissements devraient pouvoir se réaliser au moyens de mécanismes fonctionnels simples, souples, et à coûts réduits.

Les technologies NXP Mifare Desfire sont complexes et peuvent potentiellement constituer un frein à la mise en place de solutions internes autour des cartes NFC. Ceci peut expliquer en partie le quasi monopôle de quelques sociétés sur ces marchés dits de niche, avec comme conséquence de se voir imposer leurs solutions clé-en-main.

Le projet EsupNfcTag a permis dès aujourd'hui de mettre en œuvre, à coût faible (y compris en développement), des solutions simples, fonctionnant et s'intégrant harmonieusement dans un système d'information déjà établi.

Dans le but de remplacer le SGC propriétaire en place, l'application dite « microservice » EsupNfcTag peut simplement être enrichie et proposer non pas seulement la lecture de la carte mais également l'écriture. EsupNfcTag fournit alors le service d'écriture / encodage / lecture de cartes à intégrer dans un système d'information déjà en place (à intégrer à l'application de gestion de comptes de l'établissement par exemple).

EsupNfcTag ne sait « que » lire dans sa version 1.0.0. Aussi dans le cadre de cette étude, nous avons mené de nouveaux travaux permettant à EsupNfcTag (version de développement, cad future version 2) d'écrire des applications complètes sur une carte Mifare Desfire EV1 (ou EV2) : création d'applications, création et écriture defichiers en clair ou de manière chiffrée, modification des clefs (DES, AES ou autre).

Au 3 Avril 2017, la version de développement (2.0) intègre désormais l'écriture d'applications DESFire complètes.

Quant à l'impression de cartes sur une imprimante spécialisée, elle a pu être réalisée en faisant appel à une simple page web en HTML avec une CSS adaptée, ou encore en utilisant directement un pdf.

Dans un premier temps on a ainsi pu imaginer un fonctionnement visant à imprimer et coder la carte de manière indépendante : l'impression par une imprimante et le codage par un smartphone via EsupNfcTag.

Dans une première approche l'idée a donc été d'enrichir EsupNfcTag pour en faire un outil permettant à un établissement d'intégrer l'encodage et donc -in fine- la gestion de cartes à son propre système d'information. On se place ici dans une **architecture de type microservices** dans laquelle **EsupNfcTag** fournit le **service de lecture et d'encodage des cartes**.

Par rapport au fonctionnement de la v1 d'EsupNfcTag présenté ci-dessus, l'idée est de proposer des « salles » permettant la lecture d'identifiants portés par la carte, ainsi que des salles permettant leur écriture.

Le lien entre la carte à chiffrer et l'utilisateur de la carte (vierge au départ) peut être réalisé par l'opérateur : le fait qu'il soit authentifié à la fois sur l'application Android et sur l'application issue du SI (dans laquelle il pourra avoir pointé l'utilisateur pour lequel il souhaite chiffrer la carte) suffit.

6 - Points divers

6.1 - Application Izly du CNOUS / CROUS

La prise en compte de Izly requiert l'utilisation d'un module sécurisé de type SAM (Secure Access Module) pour écrire l'application dans une carte.

Cela se matérialise dans les établissements par l'usage d'une clef USB (SAM) et d'un programme windows (DLL) permettant de chiffrer les éléments Izly dans la carte.

Ce procédé permet :

- d'éviter le problème de communication des clefs Desfire AES Izly.
- un déploiement simple, ce système type « boite noire » est autonome/indépendant.

Cela requiert l'usage d'une station Windows sur laquelle sont branchés la clef SAM ainsi que le lecteur Desfire permettant l'encodage Izly de la carte.

Après échange sur le sujet avec les personnels du CNOUS, on a pu constater que la mise en place effective de cet encodage Izly était relativement aisée.

6.2 - Impression réinscriptible au verso

La solution utilisée actuellement au niveau de la COMUE Normandie Université propose un verso réinscriptible.

Cela permet d'y renseigner l'année et la composante de rattachement de l'inscription en cours.

Cette fonctionnalité nécessite matériellement des bornes de mise à jour coûteuses, complexes et sujettes à des pannes.

6.3 - Impression et encodage de carte simultané

L'impression de carte et l'encodage d'une carte peut actuellement se faire en une seule action par une imprimante spécifique telle que les Zebra (ZXP series 3). Ces imprimantes sont également capables de faire des impressions par lot.

Ces possibilités ne sont disponibles que sur les environnements windows et avec des SDK spécifiques et propriétaires ; là encore on a pu constater que leur intégration dans un programme adhoc (en C# voire en Java) est à portée.

6.4 - Technologies NXP

Les technologies de cartes utilisées ici (Mifare Desfire EV1) sont des technologies propriétaires de l'entreprise américaine (hollandaise jusqu'en 2016) NXP.

Pour protéger ces technologies, NXP semble avoir mis en place un certain nombre de mesures : sans doute des brevets mais aussi des accords de non-divulgation lorsqu'il s'agit de prendre connaissance de certaines documentations.

Nous avons réussi à effectuer nos travaux en nous basant sur des recherches et outils disponibles librement sur le WEB et n'avons donc jamais signé de quelconque accord jusque-là.

Cependant la question de l'adéquation de ces technologies avec un projet libre (open-source) peut être posée.

Cette technologie de carte est certifiée ANSSI

https://www.ssi.gouv.fr/certification_cc/mifare-desfire-ev2/

6.5 - Application Desfire portant des services d'identification

Même si c'était implicite jusque ici, il convient de rappeler que l'objectif initial est de faire porter à la carte des services d'authentification et d'identification ; par exemple pour :

- s'identifier sur des bornes d'accès pour ouvrir des portes ;
- s'identifier et donc “payer”, via son compte “Izly”, dans les restaurants du CROUS ;
- s'identifier sur des copieurs pour “payer” ses éditions, libérer ses impressions ou encore numériser des

documents ;

- s'identifier et badger sur tout autre service institutionnel ; citons, la carte culture, le contrôle de présence, l'émargement à des élections, examens, etc.

Il s'agit donc d'**utiliser la carte de manière connectée**, en lien avec un (ou plusieurs) système d'information permettant, depuis un identifiant unique spécifique à la carte, de retrouver l'individu dans sa propre base ; pour suite à donner à l'action initiée par le badgeage.

6.6 - Échange des données

Au niveau de la COMUE Normandie Université, un des objectifs de la Léocarte mutualisée est qu'un étudiant et personnel d'un établissement donné puisse être reconnu dans un autre établissement ; au niveau des bornes d'accès par exemple, mais aussi, entre autres, pour des services spécifiques comme pour la carte culture (mutualisée dès maintenant entre l'INSA de Rouen Normandie et l'Université de Rouen Normandie).

Il paraît intéressant ici de préciser la manière dont peut s'opérer cet échange d'informations, tout en soulignant cependant que, dans une architecture de type microservices, ce n'est pas au service d'encodage de cartes de porter cette fonctionnalité.

Au-delà de l'échange de clef(s) des applications Desfire entre les DSI, devant se faire de manière sécurisée à un instant donné (secret partagé) ou encore de l'établissement d'éventuelles affectations de plages d'identifiants pour chaque établissement, on privilégiera, pour un tel échange d'informations, d'utiliser simplement ce qui se fait déjà par ailleurs (pour l'échange des identifiants portés par les cartes donc).

On pense notamment au recours à un annuaire LDAP, à la norme **SUPANN**, pour lequel l'attribut **supannRefId** semble consituer une cible intéressante pour porter ces identifiants.

Etiquetté, multi-valué, il pourrait par exemple contenir (à réfléchir) :

- {ISO15693}503f5cb2723304 pour le CSN de la carte ;
- {NXP:F585C1}0A7300000004B5X pour un identifiant de l'application déclarée au niveau de NXP avec un identifiant de F585C1 (application COMUE Normandie Université ici permettant le contrôle d'accès) ;
- voire {NFC:COMUE-NU:ACCESS} 0A7300000004B5X pour ce même identifiant ;
- le code UAI pourrait aussi être utilisé, plutôt que COMUE-NU ;
- etc.

Le support, le transport ou l'échange de cet identifiant porté par l'attribut supannRefId défini dans SUPANN peut alors se faire de la même manière que pour les autres attributs, notamment au travers des mécanismes de fédération d'identités Shibboleth, portée par Renater, ou/et encore via l'usage d'un annuaire LDAP type SUPANN.