

ESUP-SGC, Système de Gestion de Cartes sur-mesure pour l'ESR

Vincent Bonamy

DSI, Université de Rouen Normandie
Place Emile Blondel
76821 Mont-Saint-Aignan

David Lemaigent

DSI, Université de Rouen Normandie
Place Emile Blondel
76821 Mont-Saint-Aignan

Jean-Pierre Tran

DSI, Université de Rouen Normandie
Place Emile Blondel
76821 Mont-Saint-Aignan

Résumé

ESUP-SGC est un Système de Gestion de Cartes multi-services libre (open-source) écrit pour et par le monde de l'Enseignement Supérieur et de la Recherche.

Plus qu'un simple système permettant d'éditer (imprimer et encoder) des cartes, ESUP-SGC est fortement intégré au Système d'Information de l'établissement, pour lequel il constitue un élément structurant. Le produit propose ainsi la possibilité de mise à jour synchrone du Système d'Information : annuaires LDAP (Supann), dispositifs de contrôles d'accès, services CROUS/IZLY, Carte Étudiante Européenne (ESC), système de gestion d'impression, prêts en bibliothèque, etc.

Libre (licence Apache V2) et développé par le consortium EsupPortail au travers de l'Université de Rouen Normandie, les établissements ont toute latitude pour ajouter des fonctionnalités dans le code d'ESUP-SGC pour une adaptation encore plus spécifique à leur contexte d'usage.

Doté d'un back-office web riche, moderne et réactif à destination des administrateurs et gestionnaires, ESUP-SGC propose également une vue web à tout utilisateur final: étudiant, personnel, invité ... mais aussi extérieur (fédération d'identité RENATER).

Cet article et cette présentation reviendront ainsi sur les motivations de ce développement, la couverture fonctionnelle et les aspects techniques qui font d'ESUP-SGC un SGC taillé sur mesure pour l'ESR, et de fait une solution crédible face aux logiciels propriétaires du marché.

Mots-clefs

Carte multi-service, SGC, Logiciel Libre, ESUP, CROUS, IZLY, ESC, NFC, Desfire, Shibboleth, contrôle d'accès, mutualisation, Spring, Java

1 Introduction

ESUP-SGC est un Système de Gestion de Cartes sans contact (NFC¹ tags) libre (Apache License, Version 2.0), développé par l'université de Rouen Normandie.

1. Near Field Communication

Il est distribué par le consortium national EsupPortail, sa page officielle est

<https://www.esup-portail.org/wiki/display/SGC/>.

Depuis l'été 2018, la COMUE Normandie Université l'a adopté en remplacement de l'ancien système (EasyId d'Horoquartz).

ESUP-SGC est ainsi aujourd'hui en production dans 9 établissements normands et gère au quotidien plus de 100 000 cartes.

Le projet est soutenu par EsupPortail, la COMUE Normandie Université et ses établissements membres, mais aussi par le Comité National Carte Etudiante (CNCE) ainsi que les CROUS. ESUP-SGC suscite, par ailleurs, un intérêt particulier auprès d'autres établissements du supérieur.

Développé spécifiquement pour s'intégrer dans un Système d'Information de l'Enseignement Supérieur et de la Recherche déjà en place, il constitue un Système de Gestion de Cartes sur-mesure pour le monde de l'ESR.

ESUP-SGC a fait l'objet d'un certain nombre de présentations et de documents de présentation, dès son développement initial.

ESUP-SGC a vocation à s'adapter facilement à tout type d'établissement ou regroupement (COMUE, etc.).

Dans un contexte où la souplesse, la mutualisation, l'agilité, la sécurité, la transparence sont des objectifs établis par nos instances dirigeantes, ESUP-SGC a un rôle à jouer dans le domaine de la carte multi-services sans contact étudiante et professionnelle.

2 Motivations et choix initiaux

Au sein de l'Université de Rouen Normandie, ESUP-SGC a été développé en mode agile par une équipe de développeurs de la DSI² (Direction des Systèmes d'Information) en lien constant avec la DEPE (Direction des Enseignements et du suivi des Parcours Etudiants). En 2017, l'objectif était alors d'offrir des fonctionnalités plus intégrées, plus souples, plus avancées par rapport aux solutions existantes du marché.

Aujourd'hui, ESUP-SGC fait parti des projets mis en avant par le consortium EsupPortail dans son catalogue de services³.

2.1 Multi-établissements

ESUP-SGC a été développé pour permettre la mise en œuvre d'un projet de carte-multiservice commune à plusieurs établissements. Il est né dans le cadre du projet de carte multi-service porté par la COMUE Normandie Université (Léocarte).

En Normandie, ce logiciel permet, via Shibboleth et un annuaire LDAP fédérateur commun, d'importer et de synchroniser des cartes d'un établissement à un autre.

Cette fonctionnalité offre la possibilité à tout usager de l'ESR normand, d'utiliser une carte unique pour accéder à divers services offerts dans d'autres établissements de la région.

La prise en compte du Règlement Général sur la Protection des Données (RGPD) est facilitée par la possibilité donnée à l'utilisateur d'accéder aux instances ESUP-SGC des différents établissements. Via l'authentification Shibboleth, l'utilisateur peut ainsi librement donner son consentement pour la synchronisation d'information entre instances ESUP-SGC.

2.2 Workflow et cycle de vie d'une carte

Le cycle de vie de la carte est géré à la fois par les éléments issus du Système d'Information et par les utilisateurs eux-mêmes.

2. Les auteurs de cet article !

3. <https://www.esup-portail.org/catalogue-des-services>

Ainsi l'utilisateur peut désactiver sa carte à tout moment, la réactiver, en demander un renouvellement, avec éventuellement un paiement préalable. De même, un gestionnaire peut imprimer, encoder, activer une carte...

Les mécanismes de synchronisation depuis le Système d'Information permettent enfin à ESUP-SGC de rendre caduques les cartes lorsque les ayants droit n'ont plus d'inscription (ou contrat) valide dans l'établissement. De même les modifications de date de fin de droits, de tarif CROUS, etc. sont resynchronisées avec les services cibles (CROUS, ESC⁴, contrôle d'accès...).

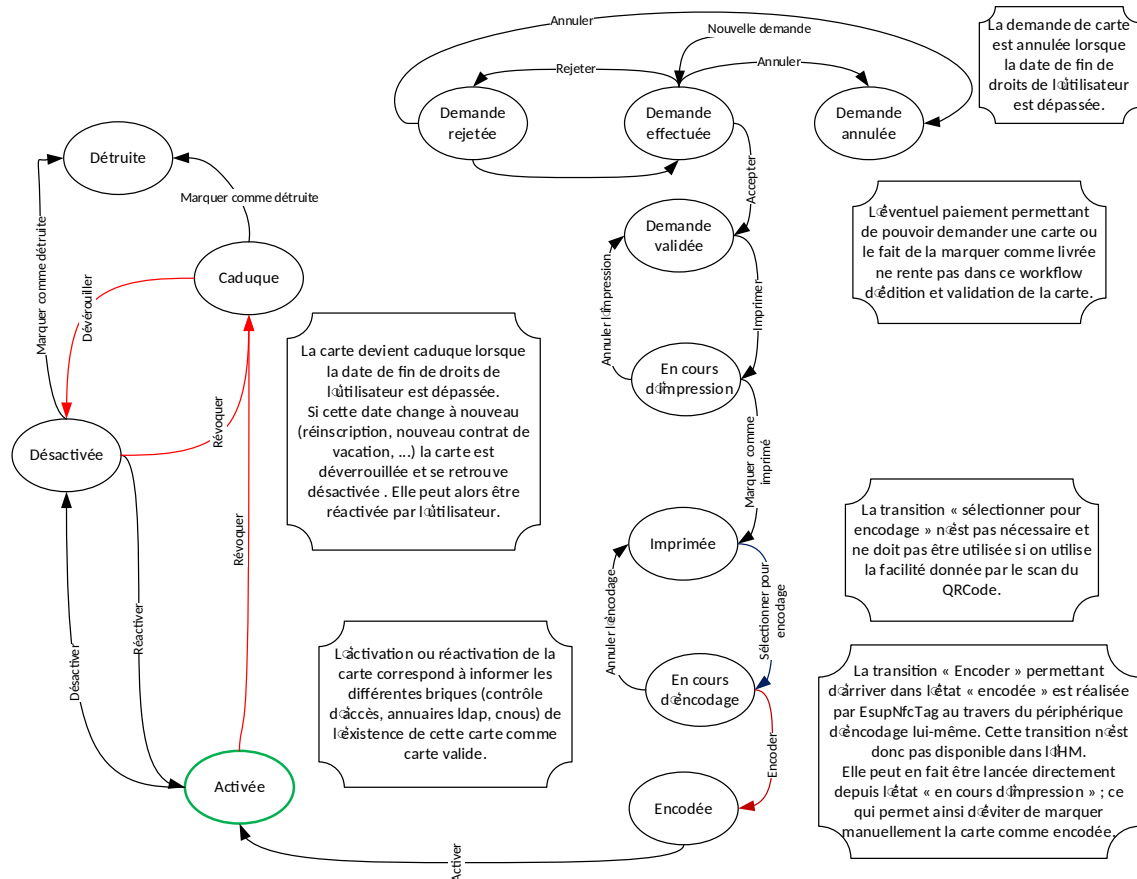


Figure 1 - Workflow d'une carte dans ESUP-SGC.

4. Cf 13 le projet de carte étudiante européenne ESC (european student card) a pour objet la propagation du statut étudiant afin que sur simple présentation de sa carte, un étudiant puisse faire valoir ses droits auprès des établissements adhérents au projet. ESUP-SGC intègre nativement son intégration.

2.3 Compatibilité RGPD

L'étude et le début du développement d'ESUP-SGC a eu lieu alors que le RGPD était un sujet hautement d'actualité puisque adopté et mis en œuvre par l'Union européenne à ces mêmes dates (2016-2018)⁵.

Une attention toute particulière a été portée au respect des bonnes pratiques en matière de protection des données. Par construction, ESUP-SGC a toutes les qualités pour permettre à un établissement de proposer à ses utilisateurs un Système de Gestion de Cartes respectant au mieux le RGPD et par extension garantir la sécurité et la maîtrise des processus métiers liés à l'usage de la carte :

- libre (open-source), l'établissement a la maîtrise de la gestion des cartes et de l'ensemble du logiciel de gestion de cartes ;
- synchronisé au Système d'Information, il contribue à le rendre cohérent, il s'inscrit dans les procédures de gestion du cycle de vie des comptes utilisateur, de la création jusqu'à leur purge ;
- il propose des interfaces web permettant aux utilisateurs de consulter et agir sur leurs cartes :
 - page permettant de consulter les cartes connus du système d'information ;
 - contrôler la diffusion de leurs informations (photos, données transmises...) ;
 - formulaires permettant de désactiver une carte suite à un vol ou perte avec une répercussion immédiate sur les services tels que le CROUS, le contrôle d'accès...

3 Couverture fonctionnelle

3.1 Édition de cartes Mifare Desfire

La couverture fonctionnelle d'ESUP-SGC comprend bien évidemment l'impression et l'encodage de la carte NFC Desfire⁶, avec tout ce que cela sous-entend, entre autre :

- la génération d'identifiants de carte ;
- la configuration intégrale de la structure Desfire de la carte : clefs, applications et fichiers Desfire EV1/EV2 ;
- le paramétrage du rendu de la carte via CSS.

3.2 Interfaces

3.2.1 Vue utilisateur

ESUP-SGC propose nativement une interface web moderne à l'utilisateur, lui permettant de visualiser, contrôler et intervenir durant tout le cycle de vie de sa carte.

Citons :

- la demande de carte par le web (compatible avec l'usage d'une webcam ou d'un smartphone facilitant le transfert de la photo de l'utilisateur) ;
- la visualisation de l'état de la carte (de la demande à sa destruction) ;
- la possibilité donnée au porteur de désactiver/réactiver sa carte (avec effet immédiat sur les services comme le contrôle d'accès, la restauration CROUS, etc.) ;
- le paiement en ligne (actuellement par paybox uniquement) permettant de faire des renouvellements de cartes payantes ;
- la possibilité d'accepter que la photo puisse être utilisée pour « un usage interne » ; d'accepter que les données soient transmises au CROUS pour pouvoir avoir le service CROUS/IZLY sur la

5. <https://fr.wikipedia.org/wiki/RGPD>

6. Les cartes Mifare Desfire (EV1 et maintenant EV2) de la société NXP sont des cartes reconnues comme très sécurisées, elles sont ainsi utilisées pour du paiement ou du contrôle d'accès. De fait c'est vers ce type de cartes que les établissements s'orientent aujourd'hui pour implémenter leurs cartes multi-services. Voir 13

carte ; d'accepter que les données soient transmises à ESCR pour bénéficier de l'activation de la carte en tant que Carte Étudiante Européenne (ESC) ;

- la possibilité pour un membre externe à l'établissement mais appartenant à un établissement partenaire du même projet de carte (dans le cas d'un projet de carte porté par une COMUE par exemple) d'accepter que sa carte (issue d'un autre SGC) soit 'importée'.

3.2.2 Vue gestionnaire

De même, via le backoffice, un gestionnaire se voit proposer des fonctionnalités avancées lui offrant une gestion facilitée des cartes :

- recherche et consultation avancées ;
- workflow permettant la gestion du cycle de vie de la carte ;
- livraison de la carte.

Au travers de ce backoffice web, le gestionnaire a la possibilité :

- d'imprimer les cartes simplement via la fonction « impression de pages web » du navigateur ;
- de lancer les clients Java permettant l'encodage d'une carte ou son badgeage ;
- d'activer/désactiver une carte ou relancer une synchronisation avec un service spécifique ;
- d'avoir accès à des tableaux de bord aux graphiques élaborés.

3.2.3 Vue administrateur

L'administrateur dispose quant à lui, de fonctionnalités avancées :

- la visualisation des sessions en cours ;
- les configurations modifiables directement via l'interface web par simple formulaire ;
- la visualisation de journaux présentant les activités de l'ensemble des cartes ;
- la visualisation des transactions paybox ;
- l'importation de « cartes » existantes non connues du SGC (utile notamment en cas de migration depuis un ancien SGC) ;
- la resynchronisation/revalidation de l'ensemble des cartes ;
- la modification/ajout de mailing automatique à des listes pour gestionnaires ou détenteurs de cartes lors des transitions du workflow de la carte ;
- la modification/ajout de « thèmes de carte », correspondant à l'implémentation de gabarits (ie *visuels*) des cartes pour l'impression ;
- la visualisation des données CROUS des cartes : c'est dans ce même outil que l'on peut intégrer le fichier CSV des cartes si on choisit de les acheter pré-encodées pour le CROUS/IZLY ;
- l'interface permettant de visualiser les éventuelles erreurs CROUS lors de l'appel de l'API CROUS ;
- la purge des cartes ou/et ayants droit n'ayant plus besoin ou ne devant plus être référencés dans la base de données d'ESUP-SGC (RGPD).

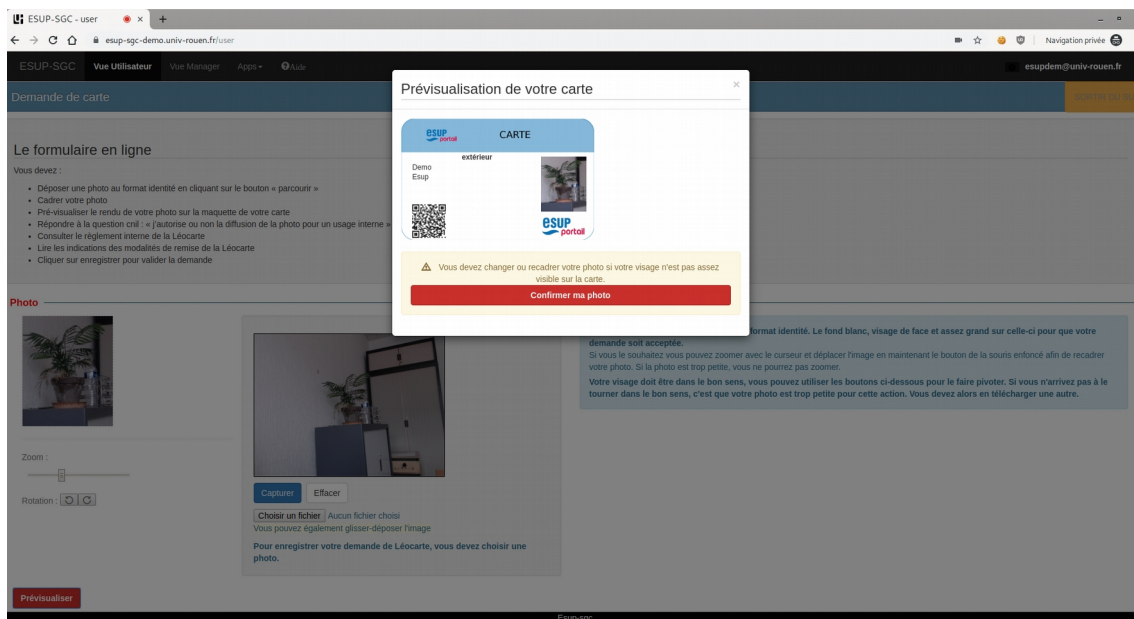


Figure 2 - Interface web de demande de carte, ici avec capture webcam

3.2.4 Badgeage

Enfin, suivant leurs rôles et les éventuels services supplémentaires connectés à l'écosystème ESUP-SGC, les utilisateurs peuvent accéder à des « salles » de badgeage telles que :

- la recherche ESUP-SGC qui permet de retrouver et rediriger le navigateur du gestionnaire sur la fiche de la carte de l'utilisateur,
- la livraison qui permet de noter la carte comme livrée dans ESUP-SGC,
- le « verso dématérialisé » qui affiche les informations dits de « verso » de la carte badgée,
- l'intégration à un logiciel de bibliothèque via l'émulation clavier proposée par esup-nfc-tag-keyboard,
- et toutes applications nécessitant la lecture (voir l'écriture) de la carte.

Le badgeage peut s'effectuer au travers de différents périphériques : Android, Lecteur NFC USB, Arduino...



Figure 3 - Badgeage d'une carte depuis l'application Android esup-nfc-tag-droid

4 Architecture et intégration

ESUP-SGC se compose de plusieurs briques interconnectées entre elles. Son architecture est hybride, à la fois monolithique et micro-services.

4.1 ESUP-SGC

Au cœur du dispositif, ESUP-SGC est une application monolithique garantissant l'interaction entre les différents composants logiciels la constituant et le Système d'Information.

En effet, ESUP-SGC n'est pas seulement un outil permettant d'imprimer et encoder une carte, il constitue le lien entre le (ou les) système(s) de gestion d'identités de l'établissement et les services reposant sur la carte multi-services, dont le contrôle d'accès, la restauration, l'impression, le prêt en bibliothèque, la délivrance de « coupons culture »⁷, la gestion de l'émargement...

4.2 ESUP-NFC-TAG

Les autres composants logiciels de la solution assurant l'encodage, la lecture de la carte, l'impression peuvent être vus comme des micro-services. Parmi eux, citons notamment l'application web ESUP-NFC-TAG et ses applications clientes (client de bureau, client sous android...), spécialisés dans la mise en œuvre de la technologie NFC DESFIRE EV1/EV2 ; elles effectuent l'encodage et le décodage électronique des cartes pour ESUP-SGC.

4.3 Intégration et interfaces avec le Système d'Information

L'application propose nativement une authentification/identification Shibboleth. Une instance ESUP-SGC d'un établissement s'intègre donc dans la fédération d'identités RENATER.

ESUP-SGC propose des mécanismes de synchronisation en temps-réel avec le(s) Système(s) d'Information grâce à des **connecteurs intégrés nativement**⁸ pour :

- récupérer les informations des ayants droit nécessaires à son fonctionnement (impression/encodage) ainsi qu'aux services qu'il peut gérer :
 - champs Shibboleth ;
 - requêtes LDAP ;
 - requêtes SQL ;
 - règles de calcul .
- activer les cartes sur :
 - la plateforme CROUS/IZLY avec le calcul du tarif de restauration (<http://www.etudiant.gouv.fr>) ;
 - le Registre numérique des Cartes Étudiant Européennes (ESC-R) ;
 - les applications de contrôles d'accès via export CSV (Horoquartz P2S, PC Pass de Synchronics, Micro-Sésame de Til Technologies...) ;
 - des annuaires LDAP (OpenLdap Supann, Microsoft AD) en vue d'intégration à d'autres services ;
 - la solution d'impressions Papercut ;
 - une API REST simple permettant une intégration d'autres services.

Le format de données et leur contenu correspondent, autant que possible, à des attributs issus des recommandations SUPANN⁹.

7. L'application ESUP-Carte-Culture est une application de gestion de coupons culture utilisant esup-nfc-tag pour permettre le badgeage des cartes NFC dans les salles de spectacle – elle est utilisée à l'Université de Rouen Normandie et à l'INSA de Rouen Normandie depuis 2016 : <https://www.esup-portail.org/wiki/display/ECC>

8. La solution offre ainsi aux établissements une véritable mutualisation de l'implémentation complète (et non partielle) de l'interfaçage avec le SI.

9. <https://services.renater.fr/documentation/supann>

D'un point de vue fonctionnel, ces synchronisations peuvent être pilotées directement depuis l'interface graphique. Pour l'intégration avec l'API du CROUS/IZLY par exemple, ESUP-SGC propose via l'IHM des retours en ligne sur les commandes à l'API CROUS ; notamment quand celles-ci sont tombées en erreur (compte clôturé, anonymisation du compte, etc.).

En ce sens, ESUP-SGC a une couverture fonctionnelle large (voir 4).

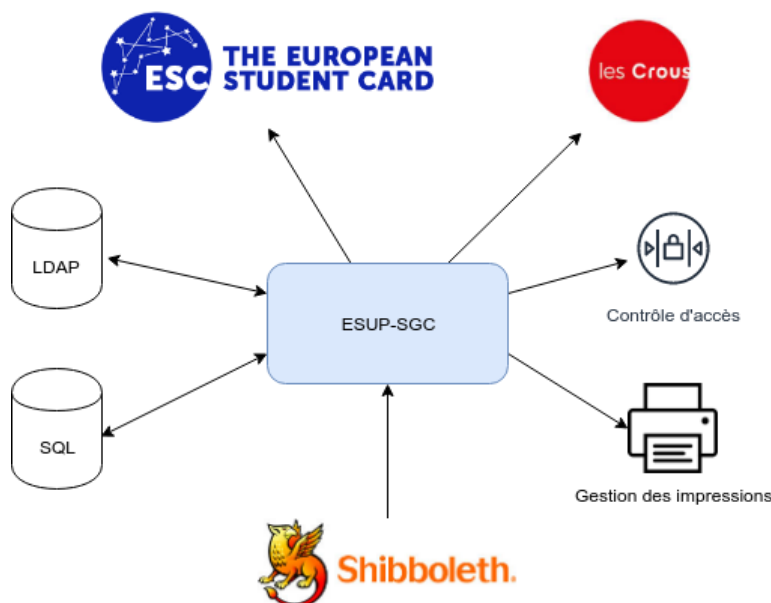


Figure 4 - Interconnexion au Système d'Information

5 Réalisation et technologies utilisées

Les technologies utilisées sont celles communément rencontrées dans les applications ESUP (et par voie de conséquence dans nos établissements).

Les différentes applications constituant ESUP-SGC sont bâties avec Java, Spring et ses modules (dont spring-webmvc et spring-security), HTML/Javascript/CSS, JPA (Hibernate), PostgreSQL...

Dans ce paragraphe, sont soulignés quelques choix structurants de l'application.

5.1 Application WEB paramétrable

Écrit en Java/Spring et dans une logique de logiciel libre, ESUP-SGC propose une configuration fine permettant de choisir et personnaliser son installation.

Au travers de fichiers descripteurs XML Spring, sont configurées les différentes sources de données, permettant à ESUP-SGC d'accéder aux comptes utilisateurs du Système d'Information. Y sont renseignés, les paramètres de connexion aux sources de données (LDAP, SQL...) ainsi que le « mapping » permettant, pour un individu, de relier les attributs issus de ces sources à ceux attendus par ESUP-SGC.

Dans ces mêmes descripteurs XML sont configurés les services à éclairer lors de l'activation de la carte (API CROUS, contrôle d'accès, etc.).

Via ces fichiers de configuration sont également gérés les identifiants de cartes qu'ESUP-SGC doit générer et transmettre à ESUP-NFC-TAG pour être encodés électroniquement dans la carte.

Le micro-service ESUP-NFC-TAG dépend également de fichiers XML décrivant le format des données à lire ou écrire sur la carte Desfire, nommées *applications Desfire* avec clefs et fichiers (et leurs configurations associées).

La récupération d'informations et l'envoi dans le Système d'Information ont été pensés pour être extensibles.

Nativement, nous proposons des méthodes classiques via LDAP, SQL, API REST, CSV dans des points de montage.

Ces implémentations peuvent également être facilement étendues. Pour ce faire, des documentations techniques sont disponibles sur le site/wiki ESUP-SGC www.esup-portail.org.

5.2 Usage de protocoles standards

Privilégiant les standards, ESUP-SGC est faiblement adhérent au matériel utilisé :

- tout encodeur NFC USB compatible Desfire et PC/SC est théoriquement supporté ;
- toute imprimante à carte plastique est théoriquement supportée ;
- toute webcam (utilisée pour la lecture des QR Codes permettant l'affectation de la carte) est théoriquement supportée.

Techniquement le logiciel ESUP-SGC s'appuie sur le standard ouvert HTML/CSS (feuilles de style CSS spécifiques à l'impression) pour agencer et imprimer les cartes. Ainsi, l'impression se résume simplement à l'envoi d'une page HTML vers une imprimante à carte, en lieu et place d'une imprimante traditionnelle !

Couplé à une édition en ligne de la CSS (avec un rendu d'exemple HTML synchronisé depuis l'interface web), la déclinaison de la charte graphique de l'établissement est simple et facile à mettre en œuvre.

En d'autres termes, et contrairement (à notre connaissance) à la majorité des solutions du marché (voire toutes), ESUP-SGC permet d'éditer (imprimer et encoder) les cartes Desfire sans recours aux API propriétaires des imprimantes à carte, rendant **ce logiciel potentiellement compatible avec tout type de matériel**.

Ce choix impose les prérequis suivants pour l'édition des cartes :

- l'impression et l'encodage en 2 temps (permettant la parallélisation des tâches) ;
- l'usage d'un QR Code¹⁰, établissant une correspondance entre la carte imprimée et son enregistrement en base ESUP-SGC.

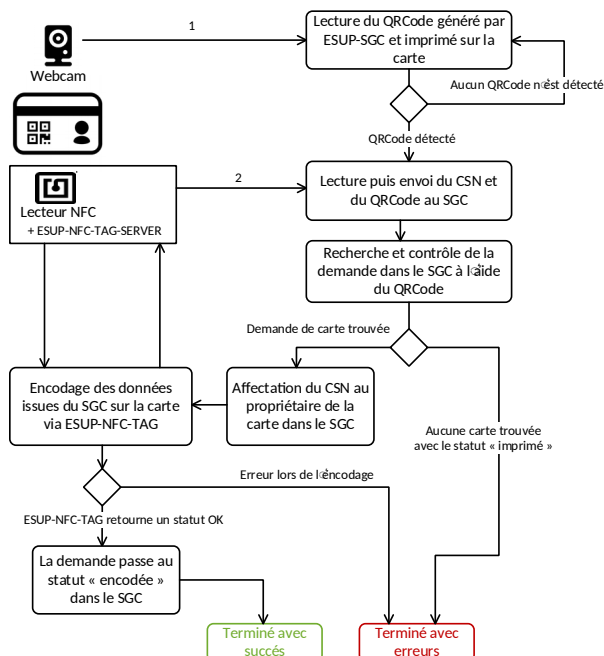


Figure 5 - Encodage et enrôlement d'une carte à l'aide du QR Code

10. Intégrant le projet ESC, ESUP-SGC utilise naturellement le QR Code de la carte étudiante européenne.

Ce choix, assumé dès la phase d'avant projet (13), tient toutes ses promesses :

- les établissements choisissent en toute liberté les imprimantes à cartes leur convenant au mieux (marque, modèle, distributeur, etc.) ; rappelons que le choix est large et les critères nombreux : imprimante réseau, imprimante à taille réduite, imprimante pour de gros volume, imprimante de bureau, coût de l'imprimante, coût des rubans, capacité de chargement, cadence d'impression, garantie, support en français... ;
- les établissements, tels l'Université de Rouen Normandie, peuvent ainsi réutiliser des imprimantes à carte acquises dans le cadre de marchés précédents ;
- ne dépendant pas d'API propriétaire, la maintenance du code ESUP-SGC est facilitée : ainsi, l'application propose simplement l'impression de pages HTML/CSS interprétées directement par le navigateur et envoyées de manière standardisée (PCL/PS) dans une file d'impression ;
- les installations et maintenances des postes d'impression sont facilitées, un simple déploiement d'un pilote d'impression d'une part, et NFC d'autre part, suffisent ;
- les imprimantes peuvent être utilisées connectées en USB ou en réseau, de manière transparente pour ESUP-SGC.



Figure 6 - Différentes imprimantes à cartes utilisées à l'Université de Rouen Normandie au travers d'ESUP-SGC

5.3 Usage de PostgreSQL

PostgreSQL est requis dans ESUP-SGC.

Celui-ci utilise en effet 2 de ses fonctionnalités avancées.

5.3.1 Indexation PostgreSQL

Les mécanismes d'indexation et de recherche plein texte sur différents champs sont très efficaces en PostgreSQL (rank, vector, weight...).

ESUP-SGC les utilise pour proposer une recherche avancée et efficace aux gestionnaires. L'usage de ces fonctionnalités d'indexation/recherche intégrée à PostgreSQL est moins efficace que ce que peut fournir un logiciel spécialisé comme lucène (et dérivées type solr, elasticsearch ...) mais ici suffisant et présentant l'avantage d'être intégrée nativement à PostgreSQL sans nécessiter le recours à un outil tiers dédié.

5.3.2 PostgreSQL blob

PostgreSQL propose des mécanismes de sauvegarde de fichiers binaires via streaming en lecture/écriture particulièrement puissant et parfaitement apte à stocker des milliers de fichiers de plusieurs Mo.

ESUP-SGC exploite ce mécanisme pour stocker l'ensemble des photos des utilisateurs.

Par-delà les performances, stocker l'ensemble des données utilisateurs dans une seule base PostgreSQL facilite l'exploitation et la maintenance de la solution, la sauvegarde (backup) de l'ensemble des données s'effectuant via une simple commande de dump PostgreSQL.

5.4 Application Android et Application de Bureau Java orientée WEB

L'usage des technologies sans contact NFC n'est actuellement pas nativement disponible au travers d'interfaces web, il nécessite donc le recours à une solution de type *client lourd*.

A cet effet, les applications clientes ESUP-SGC/ESUP-NFC-TAG ont été codées en Java (avec JavaFX) et sous Android.

Elles demeurent toutefois des applications « WEB » à part entière ; d'un point de vue graphique, leurs vues sont essentiellement des pages web dynamiques interprétées dans les navigateurs internes (webview) de JavaFX ou Android.

L'authentification qu'elles proposent se base également sur Shibboleth.

Ainsi la partie purement « client lourd » en Java se limite à l'interaction avec le matériel tels le lecteur/encodeur NFC et la webcam lisant le QRcode permettant l'encodage/enrôlage. Le lien technique entre la partie webview en HTML et la partie client lourd se fait au travers du partage d'un localstorage propre.

L'usage de cette mémoire partagée permet ainsi de propager l'authentification, récupérée par webview (via Shibboleth) à la partie client lourd¹¹.

D'autre part, le mécanisme http « long polling »¹² est prépondérant dans l'implémentation ESUP-SGC ; il permet de faire dynamiquement le retour du badgeage (en passant par le serveur) dans la webview de l'utilisateur.

C'est ce même mécanisme qui est utilisé pour proposer une recherche de fiche-utilisateur dans une instance ESUP-SGC ouverte dans un navigateur par badgeage (via un lecteur USB ou un téléphone NFC).



Figure 7 - Dispositif d'encodage des cartes, comprenant webcam et encodeur

5.5 Mise en œuvre des technologies NFC Desfire

D'un point de vue technique, et en l'état des compétences d'une DSI d'un établissement de l'ESR, le défi majeur relevé par ESUP-SGC a été l'implémentation complète de la technologie Desfire garantissant la lecture et l'écriture des cartes.

Ce défi technique a pu être relevé grâce à des ressources multiples et précieuses librement disponibles sur Internet et notamment le code de la librairie *nfcjlib* de Daniel Andrade¹³.

Ici encore, il a été décidé d'implémenter le maximum d'intelligence (code) côté serveur au détriment de développements côté client. Ainsi, la librairie *nfcjlib* a été adaptée pour un usage massivement orienté client/serveur.

Aussi l'algorithmie, le chiffrement et le calcul des commandes NFC (APDU : Application Protocol Data Unit) sont effectués par l'application web ESUP-NFC-TAG, les clients Java (ou APK) ne faisant que transmettre les APDUs calculés par la carte d'une part et par ESUP-NFC-TAG d'autre part : ils jouent un rôle de mandataire (proxy) véhiculant des commandes chiffrées. Dans notre contexte d'usage,

11. Ces mécanismes se retrouvent dans des clients lourds « shibbolethisés » ; citons le client seafile.

12. Voir https://fr.wikipedia.org/wiki/Server_push#Long_polling

13. <https://github.com/Andrade/nfcjlib> - disponible depuis 2013 sous licence BSD

- les inconvénients sont minimes (une connexion réseau de bonne qualité demeure obligatoire)...
- ... les avantages sont multiples : **la lecture et l'encodage de cartes sont très sécurisés, les clefs DESFIRE n'étant utilisées que par le serveur et ne sont, par conséquent, jamais véhiculées (ni en clair ni chiffrées) sur le poste client** ; le serveur contrôle donc tout et les journaux demeurent accessibles directement aux administrateurs système, le code client reste marginal et donc maintenable et portable aisément sur d'autres architectures (Android, Java, Arduino).

6 Retour d'usage et perspectives

En 2019, l'université de Rouen Normandie débute sa 3ème campagne d'utilisation d'ESUP-SGC. Dans son sillage, l'ensemble des établissements du périmètre de la COMUE Normandie a migré en production sur ESUP-SGC à la rentrée 2018.

En 3 ans, près de 100.000 cartes (Léocarte) ont été éditées avec ESUP-SGC par des établissements de toutes tailles.

Sur le périmètre de la COMUE Normandie Université, par rapport à l'ancienne solution utilisée, les gains apportés par ESUP-SGC sont multiples :

- fiabilité ;
- performance ;
- coût ;
- couverture fonctionnelle ;
- appropriation de la carte et des services associés ;
- sécurité ;
- mutualisation ;
- interfaçage ;
- interopérabilité.

Cette solution, développée sur mesure, de manière ouverte, évolutive, fortement couplée au Système d'Information mais faiblement dépendante des solutions matérielles propriétaires, sont autant d'atouts pour mener à bien un projet de carte multi-services.

ESUP-SGC est un projet abouti qui devrait encore implémenter de nouvelles fonctionnalités prochainement, notamment dans le cadre de l'intégration avec la Carte Etudiante Européenne et les possibilités offertes par la V2 du système Mifare Desfire (voir 13).

Les perspectives de développement de la solution sont axées sur l'implémentation de nouveaux services institutionnels à destination des étudiants et personnels.

ESUP-SGC est d'ores et déjà déployé dans une dizaine d'établissements, notamment au travers de son adoption par la COMUE Normandie Université.

Proposé en open-source, tout établissement peut librement adapter le code pour implémenter une fonctionnalité manquante (activation spécifique d'un contrôle d'accès, etc.) et le soumettre à l'ensemble de la communauté.

Au delà du code, dans une logique de partage « à la ESUP », tout établissement peut également exprimer ses besoins propres. Les contributions de tous par échanges via liste mails¹⁴ ou wiki interposé¹⁵ permettent

- de partager ouvertement la documentation ou des contributions spécifiques¹⁶ ;
- de faire évoluer le projet pour qu'il réussisse maintenant son principal défi : son adoption à large échelle par la communauté de l'ESR !

14. esup-sgc-devel@esup-portail.org permet d'échanger techniquement et fonctionnellement sur la mise en oeuvre d'ESUP-SGC dans les Etablissements de l'Enseignement Supérieur.

15. <https://www.esup-portail.org/wiki/display/SGC/ESUP-SGC>

16. La page wiki ESUP-SGC « Contributions d'établissements » regroupe déjà quelques retours d'établissements: <https://www.esup-portail.org/wiki/pages/viewpage.action?pageId=614989948>

7 Ressources

De nombreuses ressources sont disponibles autour d'ESUP-SGC. Elles sont référencées sur sa page officielle <https://www.esup-portail.org/wiki/display/SGC/>

Elles regroupent notamment :

- des articles d'études validant les orientations technologiques retenues ;
- des vidéos et diaporamas de présentations, notamment celles issues d'ESUP-DAYS ;
- un site de démonstration en ligne ainsi qu'une VM de démonstration ;
- des documentations techniques ;
- du code ;
- et bientôt cet article issu de JRES 2019 !

8 Remerciements

ESUP-SGC est un projet stratégique qui n'aurait pu aboutir sans un soutien important de collègues, organismes, structures ; aussi les auteurs de cet article tiennent ici à remercier :

- les membres de la DSI de l'Université de Rouen Normandie, et notamment son directeur et son adjoint pour leur soutien indéfectible dans ce projet ayant nécessité un temps de développement très conséquent ;
- les collègues des établissements de la COMUE Normandie Université et plus particulièrement les membres du Groupe de Travail Léocarte ; c'est l'intérêt manifesté pour cette solution sur-mesure qui a permis de transformer la maquette initiale en un SGC mutualisé, leur contribution directe à la documentation wiki a également été très précieuse ;
- les instances dirigeantes de la COMUE Normandie Université et de leurs établissements membres ; notamment la Directrice Générale des Services de l'Université de Rouen Normandie ; la confiance témoignée a permis à ce projet d'aboutir ;
- les collègues du département Monétique du CNOUS pour leur aide sur l'implémentation dans ESUP-SGC de
 - l'encodage de l'application Desfire « CROUS/IZLY » ;
 - l'interaction avec l'API CROUS ;
 - l'interaction avec les API ESC.
- le soutien constant du consortium EsupPortail.

Nos remerciements vont enfin au comité de programme des JRES 2019 qui nous offre une tribune pour présenter notre projet à la communauté de l'ESR.

9 Bibliographie

- [1] Document « VERS UN SGC LIBRE » :
<https://www.esup-portail.org/wiki/download/attachments/610336977/sgc-v3.pdf>
- [2] Document «ESUP-SGC : UN SGC LIBRE » :
<https://www.esup-portail.org/wiki/download/attachments/610336977/ESUP-SGC.pdf>
- [3] Sylvain Cammas et Geoffroy Vibrac. Proposition pour la mise en œuvre d'une carte multiservices pour les universités européennes. JRES 2017 Dijon.
https://conf-ng.jres.org/2017/document_revision_2630.html?download
- [4] Frédéric Pauget. Cartes sans contact Mifare DESFire EV1. JRES 2015 Montpellier.
https://conf-ng.jres.org/2015/document_revision_1632.html?download