ESUP-SGC - Juin 2017

Vincent BONAMY

Université de Rouen Normandie
Normandie Université

Plan

ESUP-SGC / ESUP-NFC-TAG – Cartes MultiServices

- **Contexte, objectif, mise en œuvre**
- **Environnement technique**
- **Cycle de vie d'une (demande de) carte**
- **Matériel**
- **Architecture logicielle**
- **Démo**
- **Suites et perspectives**
- **Misc**

Contexte 1/2

- D'un SGC propriétaire vers une solution Libre

  - Pour mieux maîtriser l'outil
    - Paramétrage, encodage, tenue à la charge, procédure d'invalidation, ...
  - Pour élargir la couverture fonctionnelle
    - Interface homme machine pour l'utilisateur final, désactivation, intégration forte au SI, aux solutions de contrôle d'accès, ...
  - Pour mutualiser les développements internes
    - Dématérialisation de la demande de carte, envoi de photos, gestion des demandes, …

Contexte 2/2

- D'un SGC propriétaire vers une solution Libre

  - Pour structurer l'échange et l'interopérabilité
    - Standardisation & bonnes pratiques SUPANN/LDAP/SHIBBOLETH, échange de l'identifiant carte COMUE via un annuaire LDAP, …
  - Pour proposer des services institutionnels au travers de la carte
    - En s'intégrant et en généralisant l'éco-système EsupNfcTag

EsupNfcTag 1/2

EsupNfcTag en point de départ technique

- Objectif
  - Permettre et faciliter le développement de services autour des cartes NFC dites "multiservices".
- Moyens
  - Une architecture standardisée et connectée autour du badgeage d'une carte présentant un identifiant (CSN ou identifiant codé en Desfire AES) correspondant à une carte valide d'un individu connu du système d'information.
- Applications
  - Intégration **simple** et générique de l'usage de la carte dans des applications institutionnelles telles que du contrôle de présence, émargement électronique, coupons cultures, etc.

EsupNfcTag 2/2

EsupNfcTag en point de départ technique

- En version 1.0,
  - EsupNfcTag sait lire
  - Lecture ~= écriture
- En version 2.0,
  - EsupNfcTag sait aussi écrire
- Plus-value d'un SGC :
  - ==lecture/écriture NFC des cartes Mifare Desfire
  - EsupNfcTag propose ce service sous forme de micro-service.

Service cartes Université de Rouen Normandie

Intégration technique spécifique

- Intégration dans l'ETL de l'UR Normandie
  - Spécifique à l'Université de Rouen Normandie
  - Non mutualisable directement
  - Intègre le SGC dans le SI de l'établissement
  - Elargit le périmètre fonctionnel du SGC

Développement d'ESUP-SGC

Motivations

- Motivations techniques :
  - Mutualiser les développements faits en interne
  - Remplacer la partie codage de cartes propre au SGC propriétaire par l'usage d'EsupNfcTag
- Motivations fonctionnelles :
  - Meilleure intégration dans le SI
  - Couverture fonctionnelle élargie : invalidation, services instutitionnels
- Motivations organisationnelles :
  - Encouragement des différents partenaires : ESUP, COMUE, Groupe national carte, CNOUS, ...
  - ...

Mise en œuvre d'ESUP-SGC

Phase pilote à l'Université de Rouen Normandie

- 15 Juin 2017
  - Abandon de la solution EasyId pour usage exclusif de l'écosystème ESUP-SGC / ESUP-NFCTAG
- Validation de la solution
  - Validation technique du dispositif : impression et codage de la carte, workflow technique, ...
  - Validation fonctionnelle vis à vis des utilisateurs
- Retours et participation à des groupes de travail
  - Fin Juin : réunion groupe national carte
  - Septembre : retour d'expérience GT Léocarte COMUE Normandie Université
  - Septembre : retour d'expérience ESUP-DAY # 24 ?
  - ...

Plan

ESUP-SGC / ESUP-NFC-TAG – Cartes MultiServices

- Contexte, objectif, mise en œuvre
- Environnement technique
- Cycle de vie d'une (demande de) carte
- Matériel
- Architecture logicielle
- Démo
- Suites et perspectives
- Misc

• Environnement technique de fonctionnement

- Authentification, identification et récupération d'attributs utilisateurs
  - Usage de Supann
  - Shibboleth : pour authentification et éventuellement identification
  - LDAP : utilisateurs et groupes
  - SQL : champs spécifiques (libellés recto/verso, indice inm, ...)
- CNOUS/CROUS
  - ESIST.XML pour calcul des règles
  - API CROUS
- Contrôles d'accès -> export CSV
  - Horoquartz (P2S)
  - Synchronic
  - TIL
- Peuplement du SI – identifiants cartes
  - LDAP (Openldap / Active Directory Microsoft)
- Paiement
  - Paybox (hmac)

- Environnement
  - Champs utilisateur

Nom du champ esup-sgc	Usage	Obligatoire
Eppn	Identifiant métier	Oui
email	Envoi d'email d'information lors de l'évolution de la carte ; ticket paybox, ...	Non
eduPersonPrimaryAffiliation	Catégorisation population – moteur de recherche	Non
supannEtuId	moteur de recherche	Non
supannEmpId	moteur de recherche	Non
supannEntiteAffectationPrincipale	moteur de recherche	Non
firstname	Affichage / moteur de recherche	Oui
name	Affichage / moteur de recherche	Oui
schacDateOfBirth	Obligatoire dans les contrôles d'accès	Oui
referenceStatut	Population crous (etd, stg, prs, psg, …) - permet de calculer le tarif et société crous depuis le fichier ESIST.xml	Oui
indice	Indice du personnel - permet de calculer le tarif et société crous depuis le fichier ESIST.xml	Non
dateFinDroits	Date de fin de droits – les cartes de l'individu sont marquées comme caduques cette date passée.	Non
secondaryId	Identifiant secondaire quelconque – affichage / moteur de recherche / web service	Non
institute	Établissement	Oui
supannEtablissement	Code RNE Établissement - permet de calculer le tarif et société crous depuis le fichier ESIST.xml	Oui

- Environnement
  - Champs utilisateur

Nom du champ esup-sgc	Usage	Obligatoire
recto1	Libellé position recto1	Non
recto2	Libellé position recto2	Non
recto3	Libellé position recto3	Non
recto4	Libellé position recto4	Non
recto5	Libellé position recto5	Non
verso1	Libellé position verso1	Non
verso2	Libellé position verso2	Non
verso3	Libellé position verso3	Non
verso4	Libellé position verso4	Non
verso5	Libellé position verso5	Non

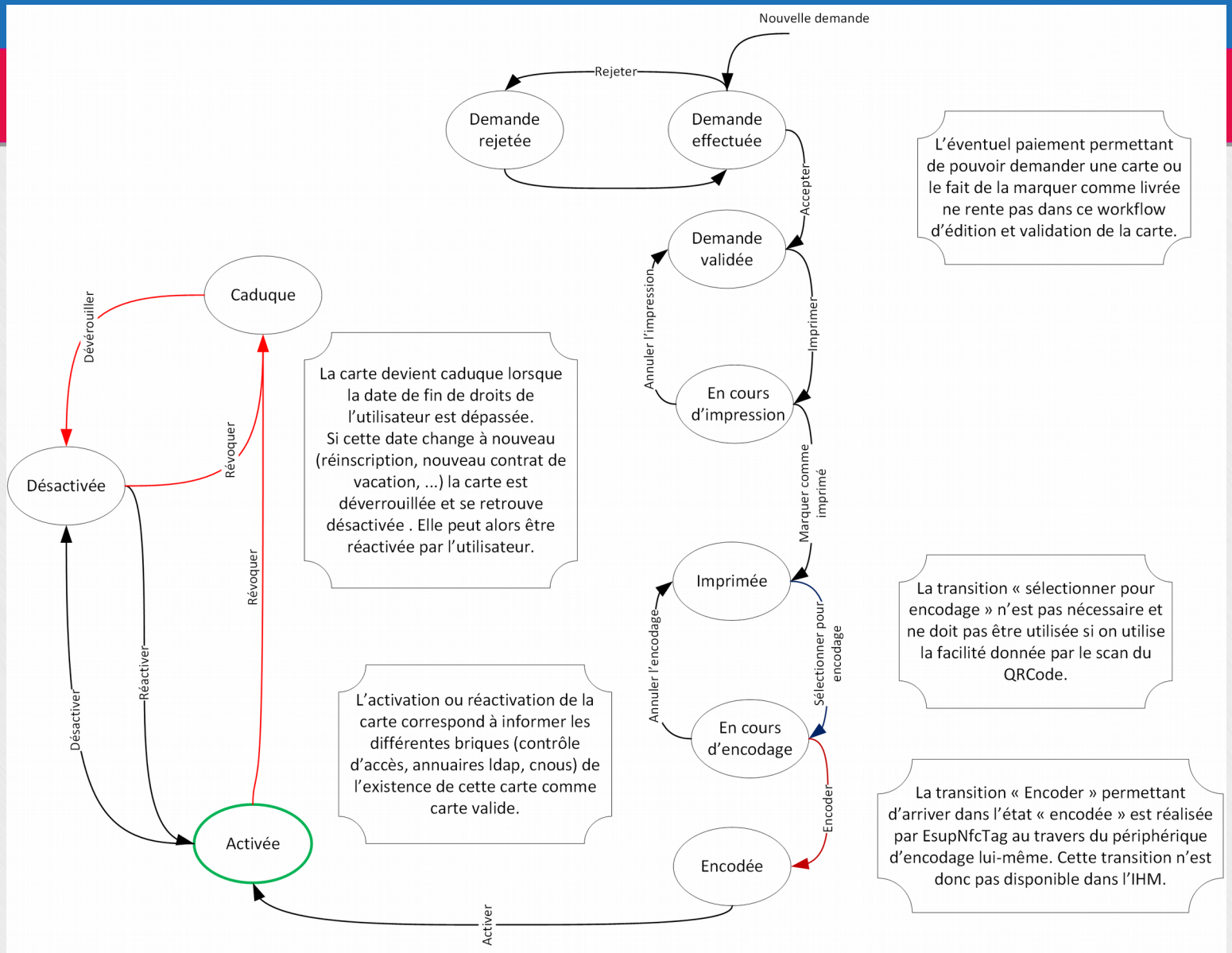
- Environnement
  - Groupes utilisateurs
    - USER → peut demander une carte
    - USER_NO_EDITABLE → ne peut pas obtenir de carte
    - USER_RENEWAL_PAYED → doit payer pour demander une carte
    - ROLE_LIVREUR → peut marquer comme livré une carte – et a accès à 'ensemble des cartes
    - ROLE_MANAGER → peut en plus imprimer une carte, l'encoder, l'activer, etc.
    - ROLE_ADMIN → configurations et outils avancés + « Switch User »

Plan

ESUP-SGC / ESUP-NFC-TAG – Cartes MultiServices

- Contexte, objectif, mise en œuvre
- Environnement technique
- Cycle de vie d'une (demande de) carte
- Matériel
- Architecture logicielle
- Démo
- Suites et perspectives
- Misc

Cycle de vie - Workflow



Cycle de vie

Etats des cartes

- Demande effectuée
  - Demande de leocarte initiale encore non traitée ou demande rejetée "rebasculée".
- Demande validée
  - L'administrateur indique cet état pour valider le fait que la demande est recevable.
- Carte en cours d'impression
  - La carte est en cours d'impression et associée à un administrateur.
- Carte imprimée
  - La carte est imprimée et non encodée.
- Carte en cours d'encodage
  - La carte est en cours d'encodage et associée à un administrateur.
- Carte encodée
  - La carte est encodée et prête à être activée.

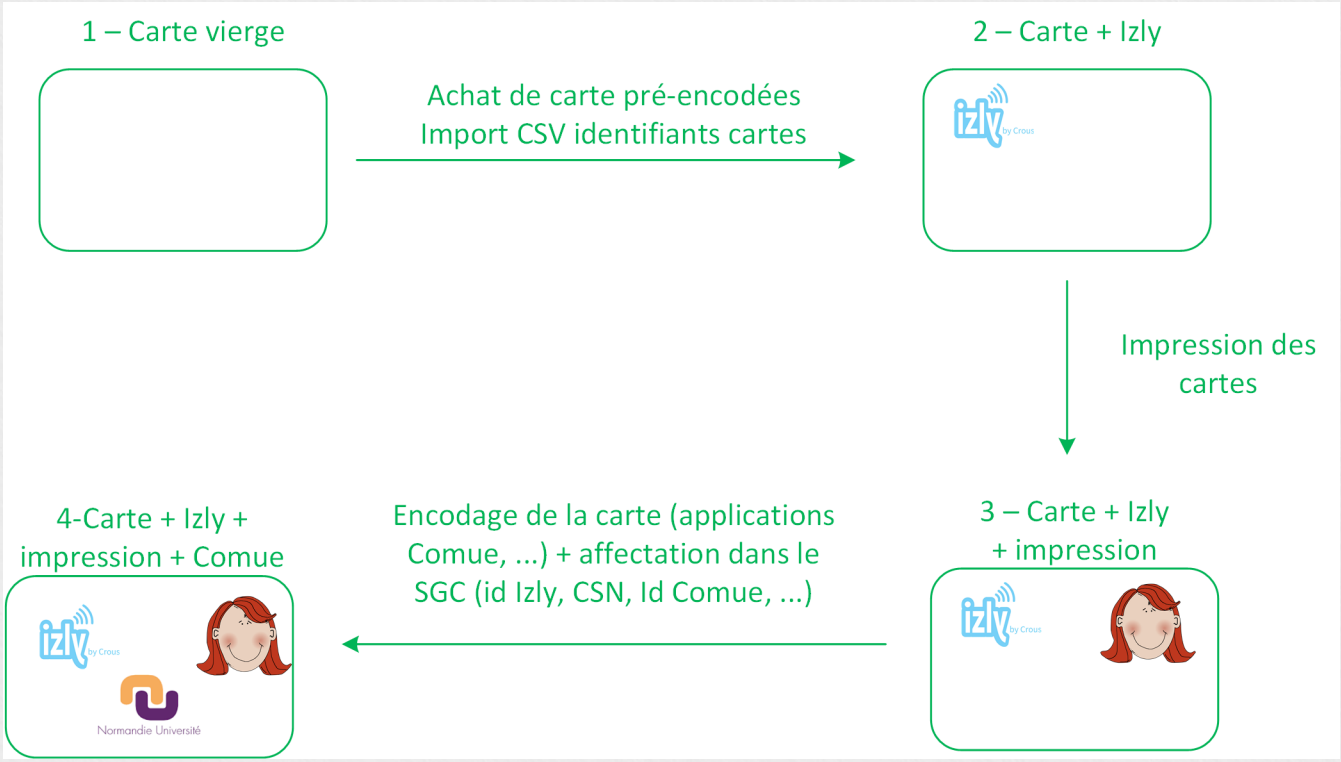
Cycle de vie

Etats des cartes

- Carte activée
  - La carte a été activée/validée/renseignée dans les différentes briques liées au Système d'Information de l'individu (Crous, contrôle d'accès, annuaires, ...) et peut être utilisée.
- Demande rejetée
  - Lors d'une demande, l'administrateur estime que celle-ci n'est pas valide (souvent pour une photo de mauvaise qualité) et l'indique alors avec un commentaire associé. L'utilisateur peut de nouveau faire une demande.
- Carte désactivée
  - L'individu, un manager ou le SGC a déclaré que la carte était invalide pour une raison précise. Elle peut être réactivée par l'utilisateur lui-même.
- Carte caduque
  - La date de fin de droits"" de l'individu a été dépassée, cette carte est donc désactivée et ne peut pas être réactivée directement par l'utilisateur. Si la date de fin de droits change pour une date future, elle changera d'état pour être dans l'état Carte désactivée et elle pourra alors être réactivée à la demande de l'utilisateur.

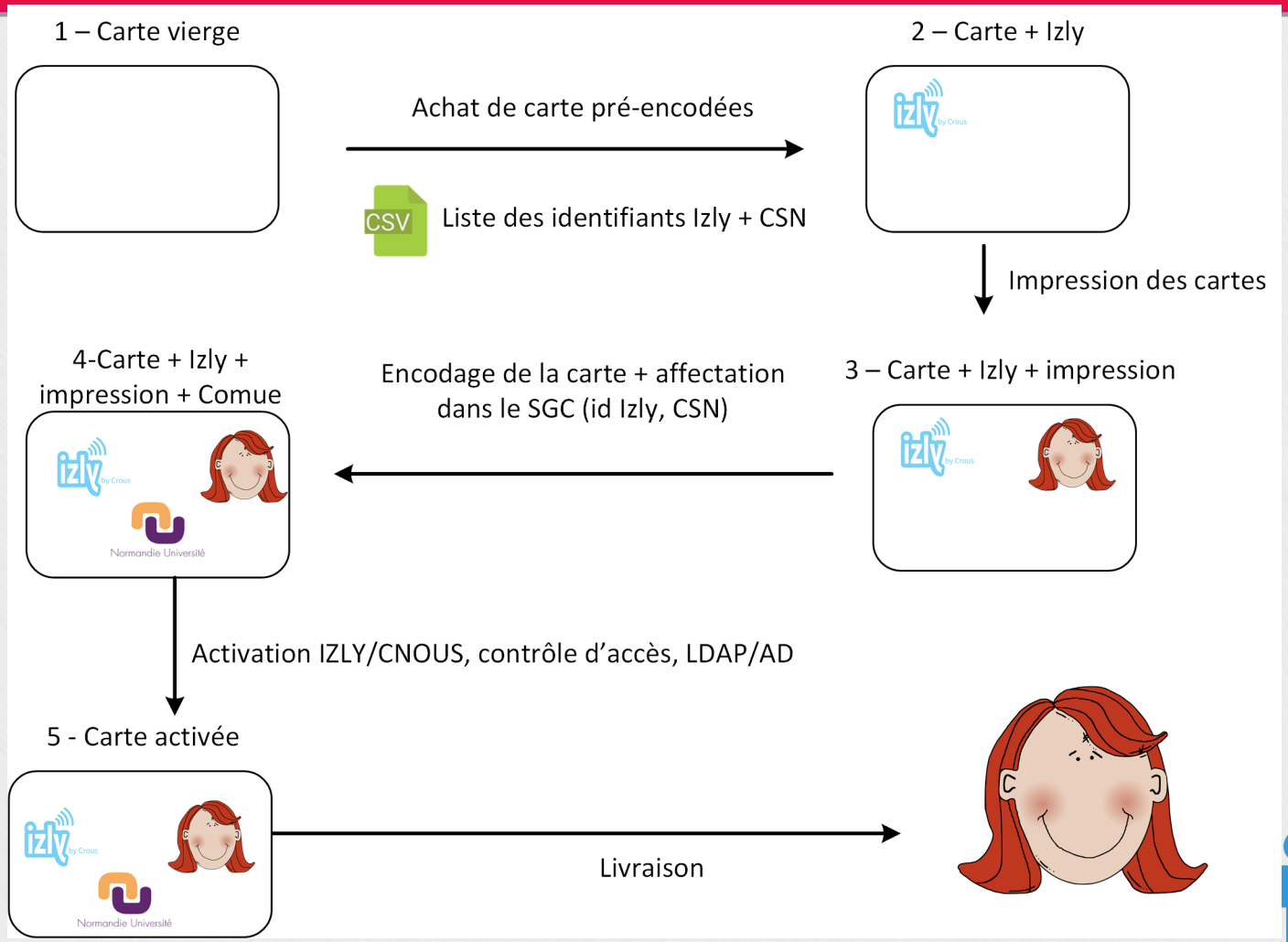
Processus d'édition des cartes

Edition des cartes



Processus d'édition des cartes

Edition des cartes



Plan

ESUP-SGC / ESUP-NFC-TAG – Cartes MultiServices

- Contexte, objectif, mise en œuvre
- Environnement technique
- Cycle de vie d'une (demande de) carte
- **Matériel**
- Architecture logicielle
- Démo
- Suites et perspectives
- Misc

- Matériel d’édition des cartes
  - Imprimante et encodage

Matériel d'édition des cartes

QR Code → EPPN

- QR Code pour associer lors de l'encodage
  - Demande de carte
  - Carte physique vierge imprimée
- Choix d'un identifiant utilisateur et non d'un identifiant de carte
  - EduPersonPrincipalName : normalisé, usuel, généralisé.
  - Peut permettre d'imaginer d'autres usages :
    - Appli android faciliant le paramétrage eduroam …
- Contrainte
  - n'est pas un identifiant de carte

    → dans Esup-SGC, on n'autorise pas l'utilisateur à avoir 2 demandes de cartes en même temps : contrainte acceptable et suffisante

Plan

ESUP-SGC / ESUP-NFC-TAG – Cartes MultiServices

- Contexte, objectif, mise en œuvre
- Environnement technique
- Cycle de vie d'une (demande de) carte
- Matériel
- Architecture logicielle
- Démo
- Suites et perspectives
- Misc

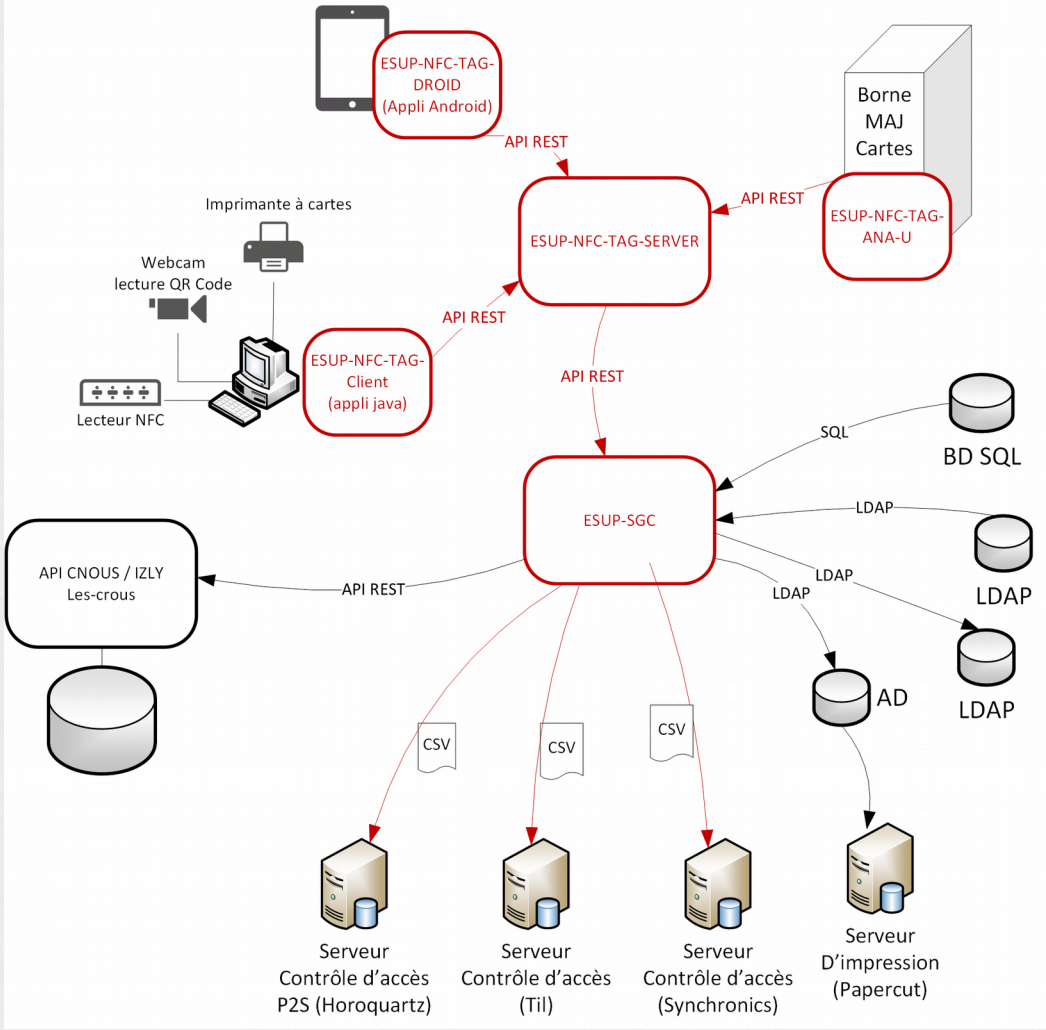
Architecture logicielle

Esup SGC et ESUP NFC TAG

- ESUPSGC
  - Intégration avec le Système d'Information, la gestion du cycle de vie de la carte, l'interface web pour le gestionnaire de cartes et l'utilisateur final.
- ESUP NFC TAG
  - MicroService de lecture / écriture cartes NFC.
  - Composé d'un serveur
  - Et d'au moins un client (EsupNfcTagDroid … EsupNfcTagClient)

- Architecture logicielle

- Esup SGC et ESUP NFC TAG



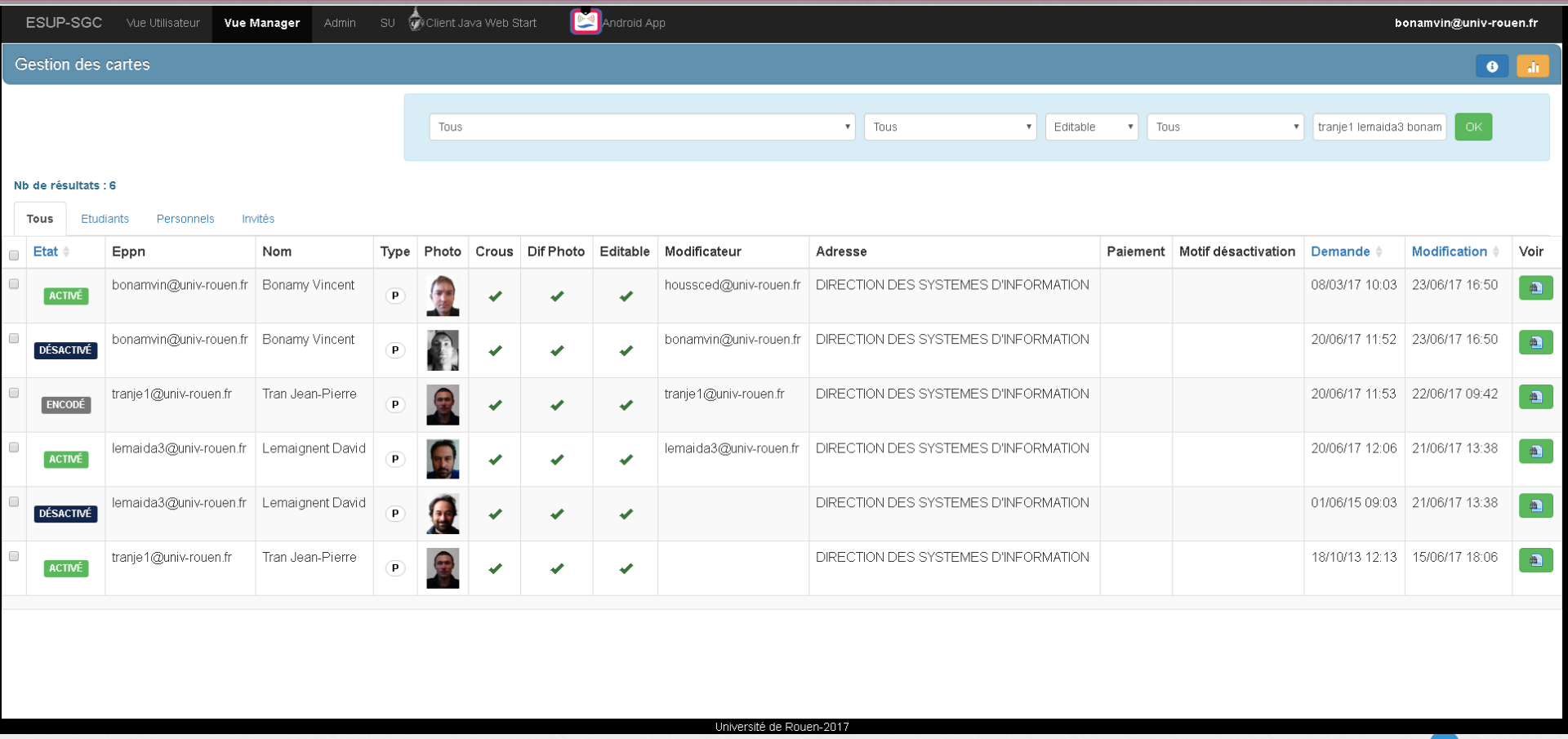
Plan

ESUP-SGC / ESUP-NFC-TAG – Cartes MultiServices

- Contexte, objectif, mise en œuvre
- Environnement technique
- Cycle de vie d'une (demande de) carte
- Matériel
- Architecture logicielle
- Démo
- Suites et perspectives
- Misc

- Démo

- Démo … ou/et copies d'écran



Etat	Eppn	Nom	Type	Photo	Crous	Dif Photo	Editable	Modificateur	Adresse	Paiement	Motif désactivation	Demande	Modification	Voir
ACTIVÉ	bonamvin@univ-rouen.fr	Bonamy Vincent	P		✔	✔	✔	houssced@univ-rouen.fr	DIRECTION DES SYSTEMES D'INFORMATION			08/03/17 10:03	23/06/17 16:50	
DÉSACTIVÉ	bonamvin@univ-rouen.fr	Bonamy Vincent	P		✔	✔	✔	bonamvin@univ-rouen.fr	DIRECTION DES SYSTEMES D'INFORMATION			20/06/17 11:52	23/06/17 16:50	
ENCODÉ	tranje1@univ-rouen.fr	Tran Jean-Pierre	P		✔	✔	✔	tranje1@univ-rouen.fr	DIRECTION DES SYSTEMES D'INFORMATION			20/06/17 11:53	22/06/17 09:42	
ACTIVÉ	lemaida3@univ-rouen.fr	Lemaignent David	P		✔	✔	✔	lemaida3@univ-rouen.fr	DIRECTION DES SYSTEMES D'INFORMATION			20/06/17 12:06	21/06/17 13:38	
DÉSACTIVÉ	lemaida3@univ-rouen.fr	Lemaignent David	P		✔	✔	✔		DIRECTION DES SYSTEMES D'INFORMATION			01/06/15 09:03	21/06/17 13:38	
ACTIVÉ	tranje1@univ-rouen.fr	Tran Jean-Pierre	P		✔	✔	✔		DIRECTION DES SYSTEMES D'INFORMATION			18/10/13 12:13	15/06/17 18:06	

Université de Rouen-2017

Plan

ESUP-SGC / ESUP-NFC-TAG – Cartes MultiServices

- Contexte, objectif, mise en œuvre
- Environnement technique
- Cycle de vie d'une (demande de) carte
- Matériel
- Architecture logicielle
- Démo
- Suites et perspectives
- Misc

Suites et perspectives

Echange de données

Echange d'identifiants de cartes

- Pour les établissements avec applicatif **commun**, tels que COMUE Normandie Université
  - via attribut supann **supannRefId**
  - ou/et **swissEduPersonCardUID** ?
- Identifiants positionnés das un/des ldap partagés ou partagés via shibboleth
- prise en compte de ces identifiants extérieurs comme nouvelle carte déjà éditée → validation et peuplement dans les contrôles d'accès notamment.

→ interopérabilité

- Suites et perspectives

Diffusion d'EsupSGC et EsupNfcTag

- Release, documentation, …
- Retour phase pilote Université de Rouen Normandie :
  - Groupe leocarte COMUE Normandie Université
  - Groupe National carte
  - EsupDay #24
- → généralisation à l'ensemble de la COMUE Normandie Université ?
- D'autres établissements intéressés ?

- Suites et perspectives
  - Diffusion d'EsupSGC et EsupNfcTag
    - Modifier, adapter la solution en fonction des retours
    - La rendre souple et configurable tout en en faisant un produit assez facilement appropriable
    - ...

- Suites et perspectives

Contrôles d’accès

- Privilégier l’usage de LDAP (au lieu d’exports CSV).
- Utiliser les groupes instutionnels … confectionnés avec grouper d’Internet 2 !
- Usage de l’EPPN comme identifiant
- …

Plan

ESUP-SGC / ESUP-NFC-TAG – Cartes MultiServices

- Contexte, objectif, mise en œuvre
- Environnement technique
- Cycle de vie d'une (demande de) carte
- Matériel
- Architecture logicielle
- Démo
- Suites et perspectives
- Misc

- Misc
  - Identifiants
    - Identifiant utilisateur unique = EPPN
      - Utilisé massivement dans les applications de l'ESR :
        - Eduroam
        - Applications / Fédération Renater : Renavisio, Renashare, foodle, etc.
        - Applications inter-établissements OAE, ENT, FileX, etc.
        - ...
    - → Un équivalent à trouver pour la carte ?
      - Identifiant de carte unique inter-application ?

- Misc
  - Sécurité
    - Dans EsupNfcTag, les clefs Desfire restent sur le serveur !
      - Ne se retrouvent jamais en RAM sur aucun des postes clients
      - Contrairement à d'autres solutions …

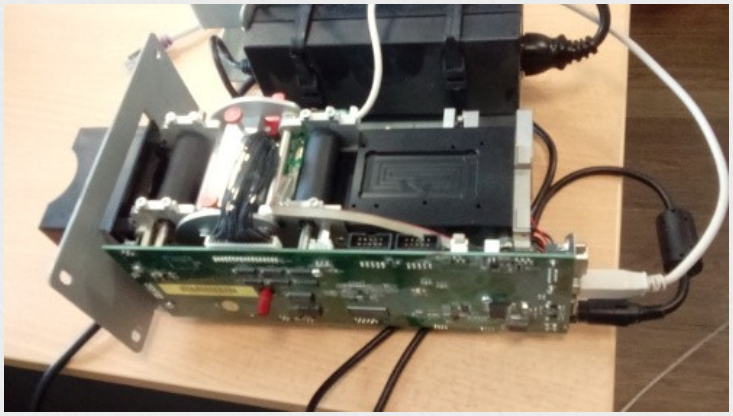
- Misc
  - Appli BU / simulation clavier
    - Fait partie des fonctionnalités d'EsupNfcTag
    - Utilisé dans nos BU pour retrouver
      - l'utilisateur
      - à partir d'un identifiant utilisateur récupéré via
        - la carte
        - et connexion (WS) à ESUP-SGC

- Misc

Borne - réinscription

- Codé également et utilisé à l'Université de Rouen:
  - Utilisation du SDK propriétaire de l'imprimante
  - Ne fonctionne donc qu'avec un matériel très spécifique
  - A été implémenté pour être iso-fonctionnel avec la solution utilisée précédemment au travers d'un SGC propriétaire

Code spécifique à l'Imprimante EasyPrint de chez Ana-U uniquement actuellement



Imprimantes

- Équivalentes fonctionnellement et sur le papier
- Certaines sont à l'usage plus robustes que d'autres, plus fiables …
- En France :
  - la société Evolis fabrique des imprimantes intéressantes