



# Carte étudiante européenne

## Spécifications générales de la mise en œuvre technique

16 juin 2017  
v2.0



# Objet du document

Ce document décrit les spécifications fonctionnelles et techniques de la carte étudiante européenne. Il a pour objectif de décrire l'ensemble des éléments permettant la mise en œuvre du support physique et numérique de la carte.

**Dans une première partie**, le document aborde le contexte, les objectifs et les enjeux du projet. Les principes fondateurs d'une carte étudiante européenne sont mis en exergue.

**La deuxième partie** propose la création d'un identifiant européen unique de l'étudiant. Celui-ci est obtenu par construction d'identifiants existant.

**La troisième partie** aborde la carte étudiante en tant que support physique. Deux versions sont proposées. D'abord un support passif, compatible avec l'ensemble des cartes émises aujourd'hui dans tous les pays d'Europe. Puis la perspective d'un support électronique moderne permettant de proposer d'avantages de services. Il est proposé que les spécifications de ce support électronique constituent une cible de convergence lors de la modernisation des cartes étudiant de chaque pays.

Les usages de la carte, démontrant sa valeur pour son porteur, seront décrits dans un document dédié, qui détaille les interactions possibles entre l'étudiant et les différents fournisseurs de service. **Le quatrième chapitre** explicitera quels usages seront possibles en fonction des choix techniques de l'établissement concernant sa carte étudiante, et en fonction du degré d'avancement du projet.

**La cinquième partie** détaille toutes les interactions des établissements et des étudiants avec un router numérique des cartes étudiants européennes (appelé ESC-R) permettant la propagation numérique du statut d'étudiant. Les fournisseurs de service peuvent certifier le support physique de la carte auprès de ce router.

**La sixième partie** récapitule les règles de fonctionnement, les conditions d'usage et les exigences techniques qui pèsent sur le router ESC-R.

## Glossaire français

**BU** : bibliothèque universitaire.

**CNCE** : comité national de la carte multiservice étudiante et de ses usages (en France).

**eduGAIN** : eduGAIN est un service d'interconnexion des fédérations d'identité pour l'éducation et la recherche au niveau international. Tous les utilisateurs faisant partie d'une fédération d'identité au niveau national font automatiquement partie d'eduGAIN si leur fédération participe au regroupement, sauf refus explicite de l'utilisateur.

**eIDAS** : le règlement européen eIDAS s'applique à l'identification électronique, aux services de confiance et aux documents électroniques. Il vise à établir un cadre d'interopérabilité pour les différents systèmes mis en place au sein des États membres afin de promouvoir le développement d'un marché de la confiance numérique.

**Emrex** : solution de transfert électroniques des dossiers des étudiants entre établissement d'enseignement supérieur en Europe, en cours d'expérimentation au Danemark, en Finlande, en Italie, en Norvège et en Suède.

**ESC** : carte européenne de l'étudiant

**ESCN** : identifiant/numéro de la carte étudiante européenne

**ESI** : identifiant européen de l'étudiant

**EWP - Erasmus without paper** : ce projet vise à faciliter les échanges de données entre

établissements pour permettre la mobilité des étudiants entre les pays.

**Eucor – le campus européen** : groupement européen de coopération territoriale associant sept universités du Rhin Supérieur, situées entre la Forêt-Noire, le Jura et les Vosges.

**INE** : numéro d'identification national des étudiants en France. Il est composé de 10 chiffres et une lettre.

**Izly** : solution de carte de paiement électronique privative, utilisée pour régler les services fournis par les Crous (restauration, distributeurs automatiques)

**PIC** : Participant identification code. Numéro d'un attribué par la Commission européenne à tout établissement participant au programme Erasmus+.

**RNE** : répertoire national des établissements en France, pour identifier les établissements. Le code RNE a été remplacé par le code UAI.

**SGC** : système d'information de gestion de carte, pilotant l'impression de cartes étudiantes, en général en lien avec le système d'information de scolarité.

**SI** : système d'information.

**UAI** : unité administrative immatriculée. Ce code désigne de manière unique un établissement d'enseignement en France.

## Journal des mises à jour

Révision	Date	Auteur(s)	Description de la modification
V1.0	15/03/2017	Cabinet Infhotep, pour le CNOUS	Présentée à Berlin les 6 et 7 avril 2017
V2.0	06/22/2017	Cabinet Infhotep, pour le CNOUS	Màj avec le guide utilisateur + intégration des propositions faites lors de la réunion de Berlin

# Sommaire

Objet du document .....	2
Glossaire français .....	3
Journal des mises à jour .....	4
Sommaire .....	5
1. Le contexte et les enjeux .....	7
Les principes fondateurs .....	7
Les acteurs de la carte étudiante européenne.....	8
Les contraintes du projet .....	9
Les acteurs du projet.....	9
Le phasage du projet.....	10
2. Le numéro européen de l'étudiant.....	11
Règle de construction.....	11
Exemple.....	12
Remarques .....	12
3. Le support physique de la carte étudiante européenne.....	13
Le cycle de vie d'une carte étudiante.....	13
Le numéro de la carte étudiante européenne .....	14
Les types de reconnaissance attendus de la carte étudiante européenne.....	15
Une empreinte graphique commune.....	17
Vers une empreinte électronique commune .....	19
L'impact sur le processus de fabrication.....	20
4. La faisabilité des usages de la carte étudiante européenne.....	21
5. Les interactions avec le router numérique des cartes étudiant européennes (ESC-R) .....	23
Un établissement s'inscrit à la plateforme d'échange .....	24
Un fournisseur de service demande à certifier le statut étudiant d'un porteur de carte.....	28
Un établissement invalide une carte étudiante .....	32
Un établissement se retire du dispositif de la carte étudiante européenne .....	33
Synthèse des règles de fonctionnement.....	34
Synthèse des droits par rôles des utilisateurs de la plateforme d'échange.....	34
6. Architecture technique de la plateforme d'échange.....	35

Le format pivot d'échange des données .....	35
Le fichier d'import des cartes étudiant européennes.....	38
Conditions d'utilisation et niveau de service attendu.....	38
La technologie .....	39
Règles communes à toutes les implémentations.....	39
Règles sur l'implémentation REST XML.....	40
Règles sur l'implémentation RPC SOAP.....	40
7. Analyse de risques (work in progress) .....	41
Les risques encourus .....	41
Les scénarios de menace.....	41
Synthèse des mesures de protection en place.....	43
Le traitement des données à caractère personnel .....	43
Conservation des données dans le router.....	44
Annexes .....	45
Synthèse des exigences qui pèsent sur un établissement qui souhaite délivrer une carte étudiantee européenne.....	45
La carte étudiantee et l'identification des étudiants dans chaque pays.....	45

# 1. Le contexte et les enjeux

Le projet de carte étudiante européenne a pour objet de créer un statut d'étudiant à l'échelle européenne.

Grâce à cette carte, un étudiant inscrit dans un établissement adhérent peut faire valoir ses droits en tout lieu et auprès de tous les fournisseurs ayant défini une offre de service réservée aux étudiants.

Cette carte étudiante européenne établit une identité numérique et graphique commune à tous les étudiants d'Europe. Elle a vocation à devenir un véritable passeport numérique permettant l'émergence de services numériques sans couture entre les systèmes d'information de tous les acteurs.

Les services aux étudiants rendus accessibles par le biais de cette carte favoriseront et simplifieront sa mobilité dans les pays de l'Union, et également à l'intérieur de son propre pays. Ils visent à améliorer le quotidien des étudiants et favoriser leur réussite. Une recherche de mise à niveau et d'homogénéisation des services proposés aux étudiants en Europe se feront sur le principe de la réciprocité.

Ces services peuvent comprendre, notamment, à titre d'exemples le paiement électronique (restauration, distributeur automatique, billetterie, laverie, impressions, photocopies), le prêt de livre ou de matériel, l'accès à une consigne, le contrôle d'accès et la réservation de salle, l'attestation de présence aux cours, l'émargement aux examens, la signature électronique, l'accès aux transports en commun ou encore l'authentification pour accéder à du matériel informatique.

Dans le cadre du projet de partenariat stratégique, la priorité est mise sur le développement des services suivants :

- le paiement électronique ;
- l'accès et l'usage des bibliothèques ;
- les usages de la mobilité Erasmus par l'articulation avec le projet *Erasmus without paper* ;
- les usages du transfert électronique des dossiers des étudiants par l'articulation avec le projet EMREX.

## Les principes fondateurs

L'adhésion au dispositif carte européenne est choisi librement par tout établissement d'enseignement supérieur. L'adhésion peut être effectuée et dénoncée à tout moment par l'établissement.

Tout étudiant inscrit dans un établissement adhérent à la carte européenne garde la liberté de valider ou non son inscription dans le dispositif de la carte européenne.

Chaque établissement garde l'entière maîtrise du processus de création, de production et de délivrance de sa carte étudiante.

## Les acteurs de la carte étudiante européenne



Figure 1 : Synoptique des acteurs de la carte étudiante européenne

Quatre types d'acteurs gravitent autour de la carte étudiante européenne.

**Les utilisateurs** sont tous les étudiants porteurs de carte. Leur nombre est en croissance chaque année. On estime qu'ils sont 20 millions en Europe. Parmi eux, au moins 270 000 sont en mobilité internationale dans le cadre d'Erasmus. La carte est pour eux un facteur de simplification de leurs échanges avec les établissements et les fournisseurs de services.

**Les fournisseurs de service** sont les organisations publiques et privées qui proposent un service réservé aux étudiants. Il peut s'agir des établissements de l'enseignement supérieur eux-mêmes, d'associations d'établissements, d'organisations dédiées à la vie étudiantes, des bibliothèques universitaires, d'opérateurs de transport en commun, de centrales d'achats, etc. La carte étudiante européenne a l'avantage de les rassurer sur le statut étudiant du porteur avec un haut niveau de confiance.

**Les fournisseurs de données** sont les établissements de l'enseignement supérieur européen, seuls habilités à certifier qu'une personne est bien inscrite dans un cursus de formation au sein de leur institution. L'inscription de la carte étudiante de l'établissement dans un cadre européen est un service rendu à leurs étudiants. Elle participe au rayonnement international de l'institution. Détentrices d'informations structurées sur l'étudiant, les établissements peuvent fournir cette information aux fournisseurs de services, à la demande expresse de l'intéressé.

Un fournisseur de données peut également être un fournisseur de service. C'est le cas d'un établissement qui propose des services à ses étudiants, par exemple via sa bibliothèque universitaire.

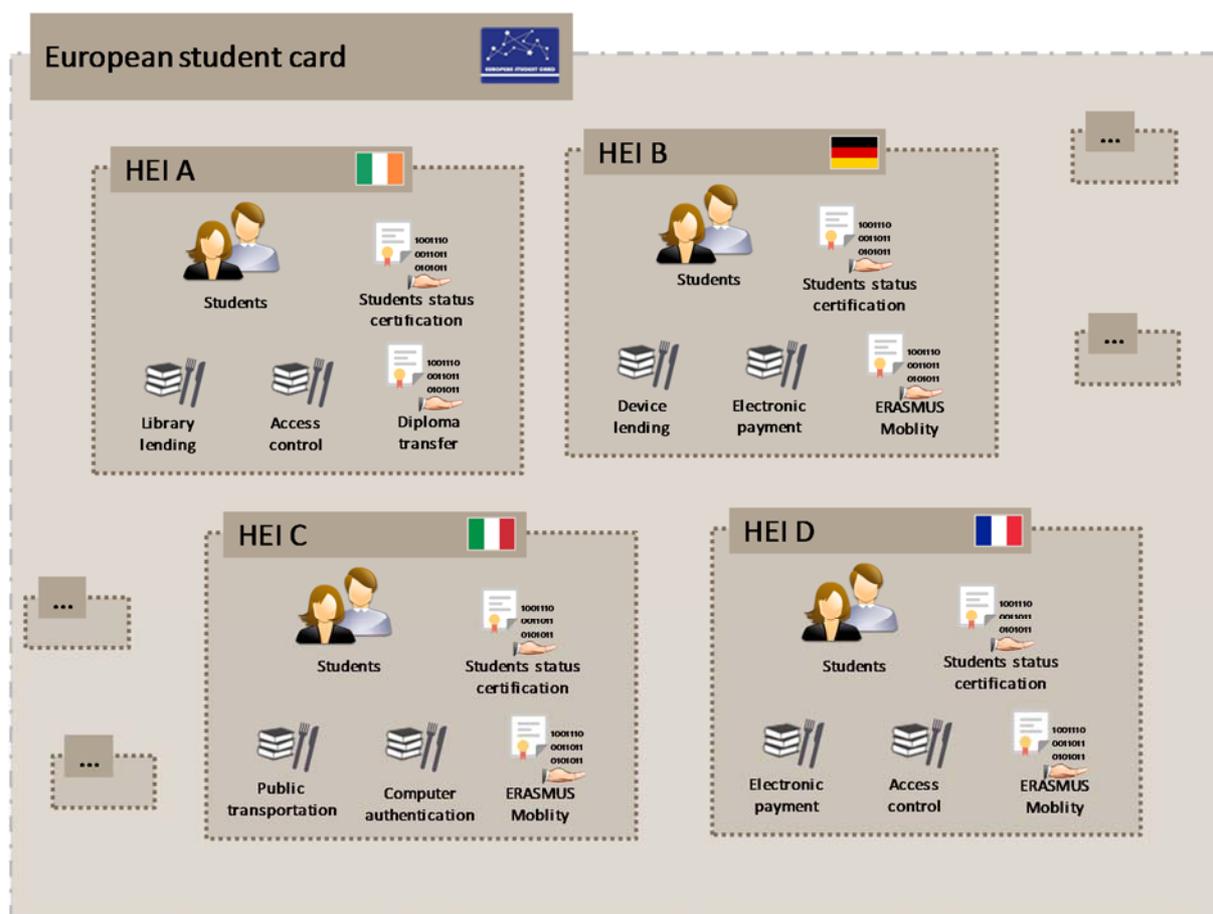


Figure 2 : Illustration des rôles des acteurs de la carte étudiante européenne

## Les contraintes du projet

La carte doit rester un dispositif simple, respectant les procédures propres à chaque pays.

Les cartes étudiantes délivrées en Europe sont très diverses tant en termes de support physique que de technologies utilisées. Leur production peut être coordonnée à un échelon national, régional ou local.

D'autres types de cartes coexistent avec les cartes étudiant, visant un public similaire. Il s'agit essentiellement de cartes de réduction. La carte étudiante européenne se distingue de ces dispositifs par son caractère institutionnel.

Les offres de services adossées aux cartes étudiants montrent une grande disparité d'un établissement à l'autre, même au sein de chaque pays. Le périmètre de nombre d'entre elles est réduit.

Les établissements certifiant de l'inscription dans l'enseignement supérieur disposent de systèmes d'information de gestion des cartes (SGC) hétérogènes, édités par plusieurs acteurs. Un des leviers de réussite de la création de la carte étudiante européenne est la création d'un standard d'échange avec ces SI, et l'adoption de ce standard par les éditeurs de SGC.

## Les acteurs du projet

Ce projet de carte européenne se fait dans le cadre d'une coopération entre les établissements qui sont habilités à certifier l'inscription dans l'enseignement supérieur. Il s'appuie également sur les réseaux

nationaux de vie étudiante de chaque pays. Une première phase d'expérimentation implique l'Allemagne, la France, l'Irlande et l'Italie.

En France, la création de la carte étudiante européenne est une mesure du plan national de la vie étudiante visant à promouvoir le statut étudiant sur les campus et les villes, ainsi qu'à développer l'offre de service à laquelle elle s'adosse. Un accord bilatéral entre la France et l'Italie pour mettre en place d'une carte commune a été contracté en 2013 entre la Conférence des présidents d'université (CPU) et la *Conferenza dei rettori delle università italiane* (CRUI). Il a été complété début 2016 par un protocole d'entente impliquant le Centre national des œuvres universitaires et scolaires (CNOUS) en France, la fondation *Ente nazionale per il diritto allo studio* (ENDISU) en Italie, le Deutsches Studentenwerk (DSW) en Allemagne et la *Confederation of student services* (CSSI) en Irlande. Enfin, un partenariat stratégique a été noué entre ces partenaires et des partenaires associés pour constituer le groupe *Erasmus+* qui vise à faire aboutir ce projet. Le CNOUS est l'organisme coordinateur du projet.

## Le phasage du projet

Le projet se découpe en trois phases :

- **Phase 1 (2016-2017)** : pour valider le principe du router des cartes étudiant européennes et le format d'échange de données proposé, un prototype sera réalisé et expérimenté sur des campus, notamment EUCOR, le campus européen, où les cas d'usages de mobilité et de droits partagés de l'étudiant entre établissements sont identifiés ;
- **Phase 2 (2017-2018)** : extension de l'expérimentation en vue de sa généralisation ;
- **Phase 3 (rentrée 2018)** : ouverture du service à tous.

## 2. Le numéro européen de l'étudiant

Pour identifier les étudiants sans ambiguïté dans l'ensemble des pays de l'Union, il est nécessaire que l'ensemble des acteurs disposent d'un numéro unique commun pour désigner chaque étudiant.

Plutôt que de créer un nouvel identifiant, il est proposé de s'appuyer sur les numéros existant déjà dans chaque pays région, ou établissement, à l'instar des identifiants SEPA basés sur un IBAN (numéro de compte local) et un BIC (désignation d'un établissement bancaire au sein d'un pays ou d'une ville).

### Règle de construction

Le numéro étudiant européen est composé de la concaténation des informations suivantes, séparées par un tiret :

1. **Le code pays** de l'établissement émetteur de la carte, sur deux caractères, selon la norme ISO 3166-1 (qui précise que les codes sont en exclusivité en majuscules) :
  - DE pour Allemagne ;
  - FR pour France ;
  - IE pour Irlande ;
  - IT pour Italie.
2. **Le code région** de l'établissement émetteur de la carte. La présence de ce code région est optionnelle. Le code région est libre. Cependant, il est proposé d'utiliser la nomenclature des unités territoriales statistiques (NUTS). Le code NUTS comprenant déjà le code pays comme préfixe, celui-ci ne doit pas être repris.
3. **Le Participation Identification Code (PIC) de l'établissement.** Il s'agit du code identifiant l'établissement dans le cadre d'Erasmus. Tous les établissements en Europe disposent d'un tel code, ou peuvent l'obtenir par une démarche administrative simple. Il s'agit d'un nombre comportant 9 chiffres. Il peut être trouvé en consultant le site <http://ec.europa.eu/education/participants/portal/desktop/en/home.html>. Dans le cas exceptionnel d'absence de code PIC, un pseudo code PIC sera généré.
4. **Le numéro unique de l'étudiant** dans l'établissement où il est inscrit. Selon les cas, ce numéro peut être national, régional ou propre à l'établissement.

## Exemple

Par exemple, pour un étudiant de l'université Paris 13, les données sont les suivantes :

- FR pour la France ;
- Pas de code région ;
- 99948994 pour le code PIC de l'université ;
- L'identifiant national étudiant (INE) composé de 10 chiffres et une lettre, par exemple 1234567890G.

Ce qui donne :

FR-999489941-234567890G

## Remarques

Par construction, l'unicité de ce numéro est garantie. Deux étudiants n'auront jamais le même numéro.

En revanche, un même étudiant dispose d'autant de numéros étudiants européens qu'il est inscrit à des établissements différents. Ce numéro n'est donc pas stable pendant la période de ses études.

Par ailleurs, l'étudiant peut disposer de deux numéros étudiants européens en même temps ou plus, sur autant de cartes étudiant différentes, dès lors qu'il est inscrit à un diplôme co-habilité par plusieurs établissements.

Enfin, le code établissement faisant partie du numéro étudiant, la fusion ou la séparation d'établissements modifient le numéro étudiant européen.

## 3. Le support physique de la carte étudiante européenne

Pour permettre une large diffusion de la carte étudiante européenne, tout type de support émis par un établissement doit pouvoir être intégré au dispositif, en respectant le processus de l'établissement en matière de création, de production et de délivrance de sa carte.

### Le cycle de vie d'une carte étudiante

Usuellement, la carte étudiante est délivrée lors de l'inscription d'un étudiant à un établissement, en général quand son dossier a été accepté et qu'il a payé les éventuels droits d'entrée.

La carte l'accompagne tout au long de son cursus, potentiellement plusieurs années, sans être nécessairement mise à jour. Il est donc possible que des informations inscrites sur la carte ne soient plus d'actualité au moment où elle est présentée. C'est en particulier le cas du nom de famille, en cas de mariage, de la discipline étudiée en cas de réorientation, voire du niveau d'étude s'il est indiqué.

En cas de perte, de vol ou de carte détruite, l'étudiant doit usuellement le signaler pour que l'établissement lui délivre une nouvelle carte, gratuitement ou à titre onéreux. Les établissements s'interdisent en général de délivrer une nouvelle carte sans cette déclaration.

Lorsque l'étudiant se réinscrit, il est courant que l'établissement ajoute un sticker pour prolonger la durée de validité de la carte pour l'année universitaire à venir. La durée de vie d'une carte est donc potentiellement de plusieurs années.

Un étudiant peut être inscrit à plusieurs établissements. C'est notamment le cas pour les diplômes co-habilités. Pour permettre à l'étudiant d'accéder à son campus et à ses services numériques, une inscription administrative est effectuée dans chaque établissement. Suite à celle-ci, l'étudiant dispose d'une carte étudiante par établissement.

Pendant une année de césure, l'étudiant ne conserve pas ses droits et n'a normalement plus de carte étudiante.

Certains établissements font partie de regroupements ou d'alliance, qui prennent différentes formes juridiques. Ces regroupements peuvent eux-mêmes bénéficier du statut d'établissement d'enseignement supérieur et délivrer des diplômes et des cartes en leur nom propre, indépendamment des établissements qui les composent. Il est proposé que la carte étudiante européenne connaisse le code PIC du regroupement éventuel auquel l'établissement participe.

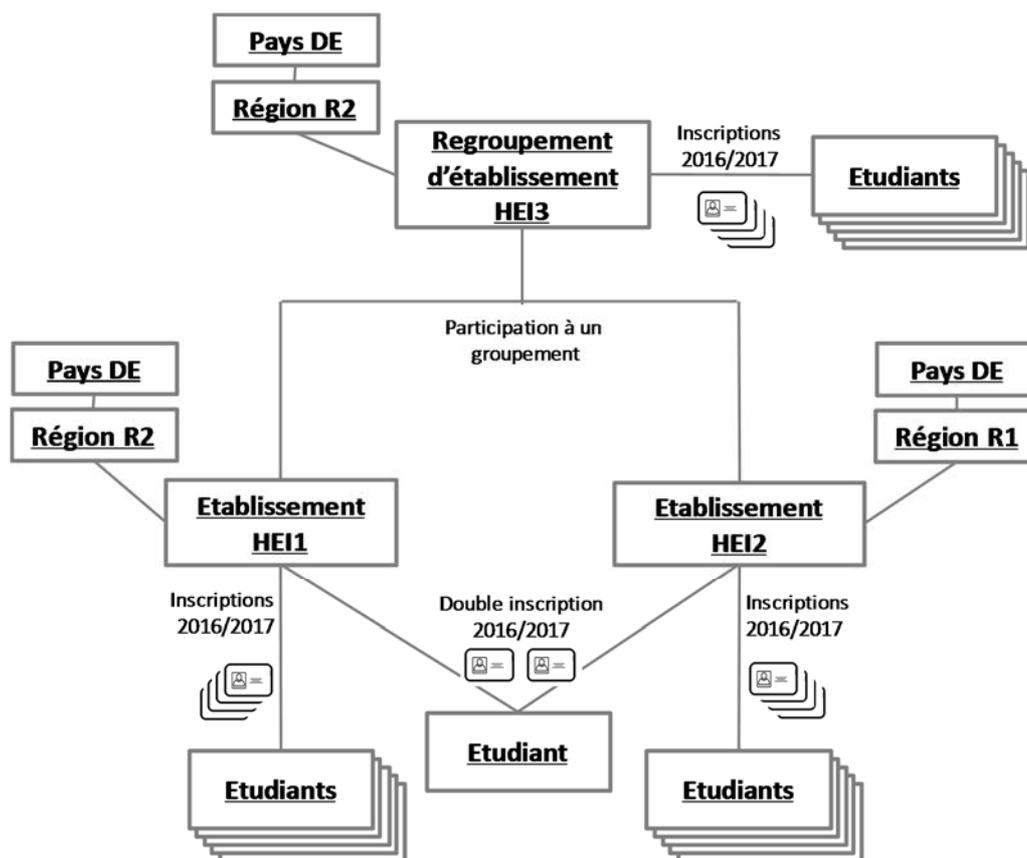


Figure 3 : Relations entre étudiants, établissements et regroupements d'établissements

## Le numéro de la carte étudiante européenne (ESCN)

Toute carte européenne doit porter un numéro unique qui permet sa liaison avec le router, inscrit sur les différents supports de stockage de la carte, optique ou électronique.

Ceci concerne autant les cartes passives que les cartes électroniques.

Ce numéro est distinct des numéros présents sur les cartes électroniques, qui ne sont pas exploitables systématiquement car souvent protégés en lecture exclusive par l'émetteur de la carte, ou généré aléatoirement à chaque lecture.

Pour permettre à chaque établissement de générer un numéro unique, sans pour autant avoir à se synchroniser avec un router central, il est proposé que ce numéro soit un identifiant universel unique (UUID). Cet identifiant binaire sur 16 octets est en général représenté textuellement sous la forme d'une chaîne de caractères hexadécimale séparée par des tirets, par exemple :

573ad632-0009-11e7-bc64-92361f002671

L'algorithme de génération est standardisé selon la norme RFC-4122 (<https://tools.ietf.org/html/rfc4122>) et implémenté dans la grande majorité des langages de programmation. Il en existe plusieurs versions. La version retenue est la version 1, qui garantit l'unicité du numéro en combinant l'adresse MAC du serveur où le l'identifiant est généré, un horodatage précis à la milliseconde, et un numéro arbitraire. Au lieu

d'utiliser l'adresse physique MAC du serveur réalisant le calcul pour assurer l'unicité du numéro, celui-ci sera remplacé, comme le chapitre 4.5 de la RFC le permet. Il est proposé de déduire une empreinte SHA-2 de la combinaison du code PIC de l'établissement et de celui du regroupement (s'il existe). Les 47 derniers bits de l'empreinte sont extraits et remplacent l'adresse MAC dans l'UUID.

La génération d'un numéro de carte étudiante est obligatoire, quelle que soit la technologie de la carte. Pour que l'établissement puisse le transmettre au router européen des cartes ESC-R, ce numéro doit être enregistré dans le SGC de l'établissement.

## Les types de reconnaissance attendus de la carte étudiante européenne

La carte étudiante européenne est conçue pour permettre différents types de reconnaissance :

1. **Une reconnaissance visuelle humaine** par n'importe quel gestionnaire, qui peut contrôler la présence du logo ou de l'hologramme, la photo du porteur de la carte ;
2. **Une reconnaissance optique automatique** réalisée par un scanner, pour interroger la plateforme d'échange certifiant l'authenticité de la carte et obtenir une information à jour ;
3. **Une reconnaissance électronique sans contact automatique** réalisée par un lecteur de carte pour interroger la plateforme d'échange certifiant l'authenticité de la carte, obtenir une information à jour, voire installer des applications pour interagir avec les services locaux.

Les reconnaissances visuelles humaine et automatique (points 1 et 2) sont possibles grâce à une empreinte graphique commune décrite ci-après.

La reconnaissance électronique (point 3) nécessite une empreinte électronique commune. Celle-ci est en cours de définition et est totalement optionnelle à ce stade du projet.

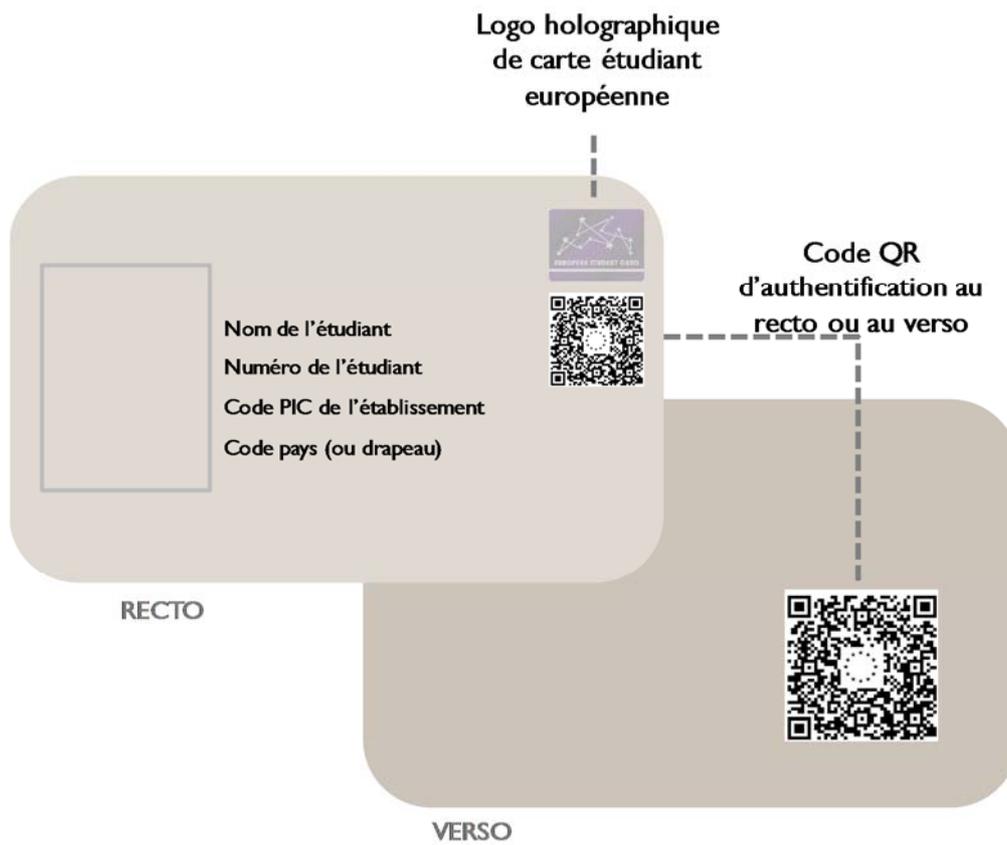


Figure 4 : Synoptique de la carte étudiante européenne

## Une empreinte graphique commune

Dans le cadre de son adhésion à la carte européenne, l'établissement doit à *minima* :

- Apposer le logo de la carte étudiante européenne au recto de la carte ;
- Afficher les informations constitutives du numéro étudiant européen, ainsi que le nom complet de l'étudiant ;
- Imprimer un code optique permettant de valider son statut en interrogeant automatiquement une plateforme numérique d'échange décrite dans le chapitre suivant.

Toutes les autres options de personnalisation d'une carte restent au libre choix des établissements d'enseignement supérieur. En particulier, l'ordre d'affichage est libre. La présence d'une photo n'est pas obligatoire. Seul le logo a une position standardisée, avec plusieurs variantes.

### Le logo de la carte étudiante européenne

Pour rendre sa duplication difficile, le logo prend la forme d'un hologramme. Il est imprimé avec de l'encre optiquement variable, dont la couleur des pigments varie en fonction de l'angle d'observation ou de l'éclairage.

Le logo doit apparaître sur la face de la carte qui comporte la photo, le nom et le prénom de l'étudiant, etc.

Le logo doit être positionné dans un des coins de la carte. Ceci est valable que la carte soit conçue en mode portrait ou en mode paysage. L'orientation du logo doit être cohérente avec le sens de lecture de la carte.

La taille du logo est standardisée : *12mm de haut et 16mm de large*. Elle ne peut pas être diminuée ou augmentée.



Figure 5 : Une simulation de logo holographique pour la carte étudiante européenne

## Les composantes du numéro européen de l'étudiant

---

Par souci de visibilité, les éléments qui composent le numéro européen de l'étudiant doivent être affichés sur la carte de manière séparée :

- Le code pays – celui-ci peut être remplacé par une image représentant le drapeau. ;
- Le code PIC de l'établissement ;
- Le numéro de l'étudiant dans le pays, la région ou l'établissement.

Le code région est optionnel.

## L'empreinte optique

---

Pour garantir sa compatibilité avec tout type de support passif, les données permettant la vérification automatique du statut de l'étudiant sont inscrites sous la forme d'un code-barres à deux dimensions (au format code QR). Ce type de code-barres peut être lu et interprété par une large gamme de dispositifs de lecture optique extrêmement répandus.

Le positionnement du code QR n'est pas standardisé. Il peut apparaître au recto comme au verso de la carte. L'établissement sera vigilant de ne pas positionner avec une trop grande proximité deux codes QR de manière à ne pas générer d'erreur de ciblage lors des scans.

Le code QR de la carte étudiante européenne doit être personnalisé graphiquement pour se distinguer d'autres codes du même type. Le choix de la couleur est laissé libre.



**Figure 6 : Code QR avec URL de vérification du statut, logo incorporé et redondance forte**

Le code QR stocke l'URL d'interrogation du service de vérification de statut de l'étudiant proposé par la plateforme d'échange en intégrant le numéro européen de la carte. L'URL est alors de la forme :

<https://api.esc.eu/card/573ad632-0009-11e7-bc64-92361f002671>

Stocker cette URL en profitant d'un haut niveau de correction d'erreur nécessite au moins 60 caractères. En conséquence, la version du code QR utilisée est au moins 5, soit un carré de 37 pixels de côté au moins (<http://www.qrcode.com/en/about/version.html>). Un établissement peut choisir un niveau de correction d'erreur plus bas pour diminuer la taille de l'image.

Le service web renvoie dans ce cas une représentation HTML de la carte étudiante européenne lisible par un humain.

## Vers une empreinte électronique commune

Au-delà de cette empreinte graphique commune, des travaux sont engagés pour faciliter des usages croisés de cartes embarquant un microprocesseur. L'objectif de ces travaux est de préconiser un masque de personnalisation commun adapté à un grand nombre d'usages et le moins intrusif possible vis-à-vis des établissements. En dehors de ce masque commun, les autres options de personnalisation du microprocesseur sont librement choisies par tout établissement.

Aujourd'hui, à titre d'information, la plupart des cartes sans contact des établissements d'enseignement supérieur européens utilisent la technologie MIFARE de la société NXP dans différentes déclinaisons. La technologie la plus ancienne, dite *Classic*, est en train d'être remplacée par de véritables cartes à microcontrôleur conformes au standard ISO 14443 sous le nom de DESFire EV1 et aujourd'hui DESFire EV2. Par ailleurs, le consortium Campus Card Berlin envisage le recours à la technologie JAVA qui permet d'intégrer les cartes de transport tout en permettant une émulation des MIFARE DESFire EV 2. Un *Memorandum of understanding* est en cours de signature pour rapprocher les projets berlinois et de la carte étudiante européen.

**Une piste de masque commun** consiste à créer une zone de donnée standardisée lisible librement, intitulée DEUInfo (Data European University Info), comprenant :

- le code PIC de l'établissement (sur 4 octets) ;
- le code PIC de l'éventuel regroupement auquel il appartient (sur 4 octets). En cas d'absence, celui-ci est identique au code PIC de l'établissement ;
- le numéro européen de la carte étudiante (binaire sur 16 octets).

Compte tenu de la place occupée par les clés d'écriture, qui dépend de la technologie employée, cette zone occupe en tout 192 octets sur la carte. Pour une carte typique de 2k, ceci représente un taux d'occupation de moins de 10%.

N'importe quelle carte implémentant la norme ISO 14443 peut héberger cette zone. La carte permet alors tous les usages où le statut étudiant est déterminé par lecture de la puce.

**Un usage plus avancé** est de permettre un fournisseur de service d'installer son application dans le microcontrôleur d'une carte émise par un autre établissement, et ce sans que cet établissement ait eu à le prévoir lors de la fabrication de la carte. L'installation reste soumise à une autorisation de la part de l'établissement propriétaire de la carte. La demande passe par la plateforme d'échange de la carte étudiante européenne. La phase d'expérimentation s'appuiera sur la technologie MIFARE DESFire EV2 pour réaliser ses tests.

Note : la description détaillée de la zone et du processus d'installation d'une application locale sur une carte émise par un autre établissement est au-delà du périmètre de ce document. Une proposition de spécification détaillée fera l'objet d'un autre document.

## L'impact sur le processus de fabrication

Ces contraintes sont conçues de manière à impacter le processus de fabrication le moins possible.

L'impression du logo de la carte étudiante européenne et optionnellement du drapeau font partie de personnalisations simples qui peuvent être demandées au fabricant de la carte. Le surcout lié à l'impression du logo holographique est estimé à dix centimes d'euro par carte. La génération de l'UUID désignant la carte peut également être déléguée au fabricant. Celui-ci est alors en mesure de générer et imprimer le code QR, ainsi que d'électrifier la carte (pour un coût estimé à 7 centimes d'euros).

L'établissement a à sa charge l'adaptation de la conception graphique de la carte, pour intégrer les nouveaux éléments visuels et textuels. Ceci nécessite l'émission d'un nouveau bon à tirer (BAT) vers l'encarteur. Par ailleurs, lors de la post-impression, l'imprimante de carte doit lire l'UUID et l'enregistrer dans le système de gestion de carte de l'établissement. Cette lecture peut être automatique dans le cas d'une carte à puce, et nécessite d'installer un scanner dans le cas de cartes passives à code QR.

Il n'y a pas d'impact sur le matériel de l'établissement, qui peut continuer à utiliser ses imprimantes à carte habituelles.

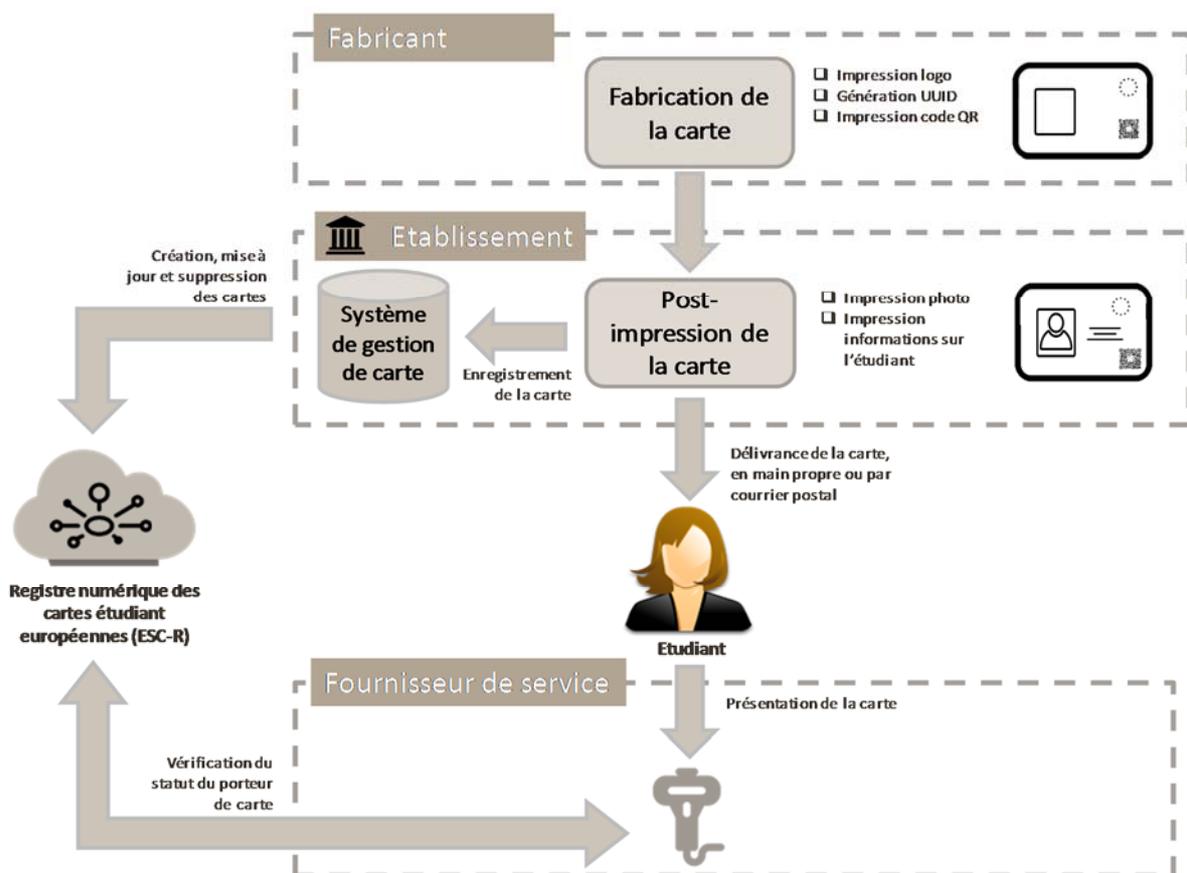


Figure 7 : Schéma global de circulation de la carte étudiante

## 4. La faisabilité des usages de la carte étudiante européenne

Ce chapitre montre comment les usages souhaités pour la carte sont réalisables grâce aux différentes composantes de la carte étudiante européenne et de la plateforme numérique ESC-R.

Le document qui sera produit par les groupes de travail dédiés aux usages exposera les interactions possibles entre le porteur de carte et les différents acteurs de l'enseignement supérieur et de la recherche en Europe, publics comme privés. Ces usages démontrent la valeur de la carte étudiante à la fois pour son porteur mais également en termes de simplification pour les fournisseurs de services, qu'ils soient administratifs ou logistiques.

*Ces usages seront ici mis en regard avec les différents modes d'implémentation de la carte dès que le document des usages sera finalisé.*

L'objectif est de montrer ce qu'apporte chaque moyen technique décrit dans ce document en termes de gains pour l'utilisateur et le fournisseur de services. Typiquement, plus la carte et les systèmes d'information associés font appel à une technologie sophistiquée, plus les coutures s'effacent lors de l'usage de la carte. Voici un exemple d'une telle progression :

1. **Carte étudiante européenne avec logo** : l'étudiant montre sa carte au guichet d'un fournisseur de service, où elle est examinée par un gestionnaire. L'étudiant attend que la gestionnaire émette une carte locale spécifique en saisissant manuellement ses informations.
2. **Carte étudiante européenne avec contrôle optique** : l'étudiant montre sa carte à un guichet, où son code QR est scanné. Ses droits sont vérifiés automatiquement auprès de la plateforme ESC-R (voir chapitre 5). Le gestionnaire lit sur son écran les informations à jour. Il émet alors une carte locale, potentiellement sans ressaisie d'information.
3. **Carte étudiante européenne avec contrôle électronique** : l'étudiant montre sa carte à un guichet. Elle est glissée dans un terminal qui lit les informations de la puce. Ses droits sont vérifiés automatiquement auprès de la plateforme ESC-R (voir chapitre 5). Le gestionnaire lit sur son écran les informations à jour. Il émet alors une carte locale, potentiellement sans ressaisie d'information.
4. **Carte étudiante européenne avec microprocesseur compatible** : l'étudiant passe sa carte dans le guichet automatique d'un fournisseur de service. Ses droits sont vérifiés automatiquement. Les informations nécessaires à l'usage du service sont inscrites sur la carte. La carte étudiante européenne devient porteuse du service et peut être utilisée en lieu et place de la carte locale.

La faisabilité de ces différents usages, en fonction du degré d'avancement du projet et du choix de chaque pays d'inclure ou non des données sur la carte, sera également exposée.

	Données de base sur la carte	Avec niveau d'étude L/M/D	Avec discipline
Reconnaissance visuelle	▪ <i>A compléter</i>	▪ <i>A compléter</i>	▪ <i>A compléter</i>
Reconnaissance optique ou électronique	▪ <i>A compléter</i>	▪ <i>A compléter</i>	▪ <i>A compléter</i>
Carte électronique compatible	▪ <i>A compléter</i>	▪ <i>A compléter</i>	▪ <i>A compléter</i>

**Tableau 1 : Matrice de la faisabilité des usages en fonction des données et de la technologie de la carte**

	Phase d'expérimentation sur le campus Eucor	Phase d'expérimentation	Phase de généralisation
Reconnaissance visuelle	▪ <i>A compléter</i>	▪ <i>A compléter</i>	▪ <i>A compléter</i>
Reconnaissance optique ou électronique	▪ <i>A compléter</i>	▪ <i>A compléter</i>	▪ <i>A compléter</i>
Carte électronique compatible	▪ <i>A compléter</i>	▪ <i>A compléter</i>	▪ <i>A compléter</i>

**Tableau 2 : Matrice de la faisabilité des usages en fonction de la technologie et des phases projet**

## 5. Les interactions avec le router numérique des cartes étudiant européennes (ESC-R)

Le router numérique des cartes étudiant européennes est un ensemble de services numériques permettant la propagation du statut étudiant entre les systèmes d'information des établissements d'enseignement supérieur de l'espace européen et les fournisseurs de service.

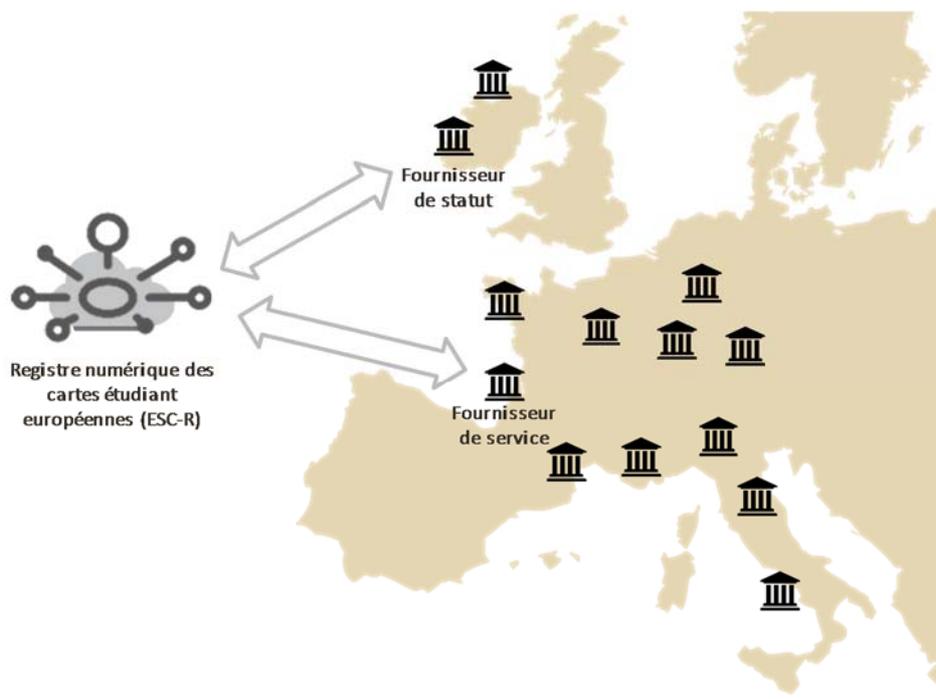
Quel que soit la méthode de lecture de la carte (optique ou électronique), le router numérique informe le demandeur sur le statut étudiant du porteur de carte.

La cohérence des informations fournies par la carte physique et la carte numérique renvoyée par le router induit un fort niveau de confiance dans la carte européenne.

Ce chapitre décrit les interactions des établissements et des étudiants avec la plateforme d'échange :

1. Un établissement s'inscrit à la plateforme d'échange ;
2. Un établissement délivre une carte à un étudiant ;
3. Un fournisseur de service demande à certifier le statut étudiant d'un porteur de carte ;
4. Un établissement met à jour la carte ;
5. Un établissement invalide une carte étudiante ;
6. Un établissement annule son inscription à la plateforme d'échange.

La description du format d'échange des données est détaillée au chapitre 6.



**Tableau 3 : Interactions entre établissements d'enseignement supérieur et le router numérique des cartes étudiant européennes (ESC-R)**

## Un établissement s'inscrit à la plateforme d'échange

Une organisation propre à chaque pays ou région inscrit les établissements qui le souhaitent.

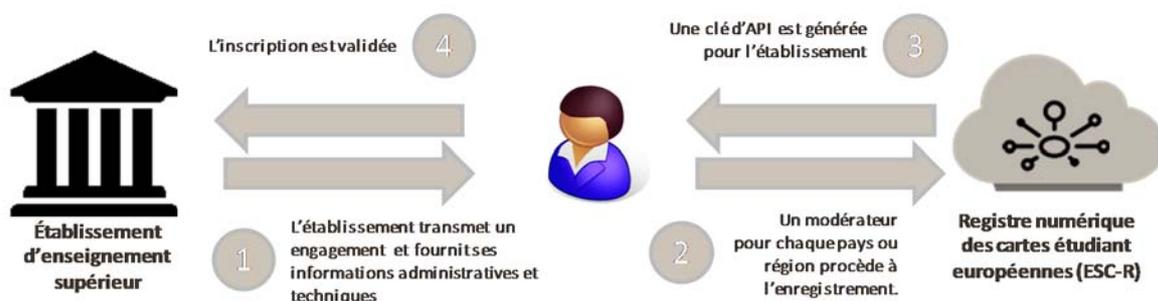


Figure 8 : L'établissement s'inscrit au router numérique des cartes étudiant européennes (ESC-R)

### Type d'interaction

Le représentant légal de l'établissement signe une charte l'engageant à respecter les obligations de la carte étudiante européenne. Elle est transmise à un superviseur selon une organisation propre à chaque région ou pays. Sur la base de ce document, celui-ci procède à l'inscription de l'établissement dans le router numérique.

### Accès

Seul le superviseur peut inscrire un établissement sur la plateforme.

### Données en entrée

Une fois autorisé par le superviseur, l'établissement doit fournir les informations suivantes :

- Données d'identification :
  - Code pays ;
  - Code région ;
  - Code PIC de l'établissement ;
  - Code PIC du regroupement d'établissement ;
  - Nom complet officiel de l'établissement ;
- Données de contact :
  - Adresse mail de l'administrateur fonctionnel des cartes étudiantes ;
  - Adresse mail de l'administrateur technique des cartes étudiantes ;
- *D'autres informations techniques (certificat X.509, API) seront précisées ultérieurement.*

### Traitement des données

L'inscription est validée par le superviseur. Les vérifications suivantes sont recommandées :

- Existence juridique de l'établissement ;
- Vérification de l'exactitude du nom ;

- Existence des codes PIC sur Erasmus ;
- Echange écrit avec les deux contacts indiqués.

En cas d'acceptation, les opérations suivantes sont effectuées :

- Programmation de l'obtention des fichiers d'import des cartes ;
- Génération d'une clé d'API autorisant l'établissement à interroger les services web de la plateforme d'échange ;
- Transmission du logo hologramme à inscrire sur la carte, s'il n'est pas déjà connu du fabricant de carte.

## Données en retour

---

Une fois son inscription validée, l'établissement reçoit la procédure pour envoyer ses fichiers de création et suppression de carte. Dans une seconde phase, il recevra également via un canal sécurisé sa clé d'API.

# Un établissement délivre une carte à un étudiant

Une fois l'établissement inscrit, il peut délivrer des cartes étudiantes européennes. À la délivrance de cette carte, les données minimales permettant la certification de la carte sont enregistrées sur le router des cartes étudiantes européennes (ESC-R).

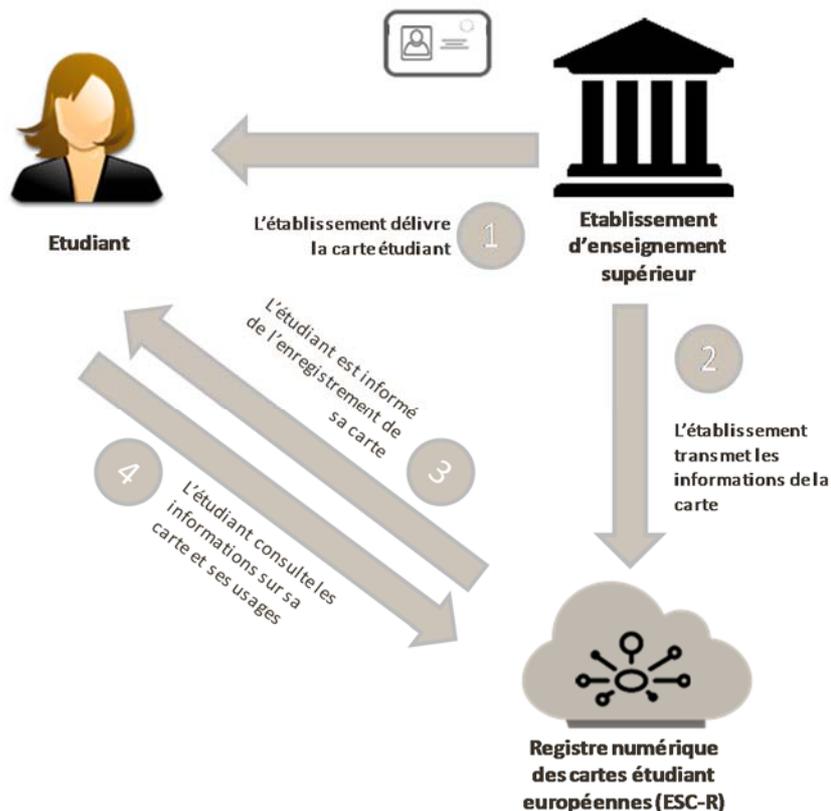


Figure 9 : La carte d'un étudiant est enregistrée dans le router numérique européen (ESC-R)

## Type d'interaction avec la plateforme

Dans un premier temps, il s'agit d'un envoi asynchrone de fichier contenant le lot des cartes à enregistrer. Le format du fichier est précisé au chapitre 6.

Dans un second temps, il s'agira d'un appel à une API synchrone, au fil de l'eau.

## Accès

Cette interaction n'est accessible qu'aux établissements enregistrés.

## Données en entrée

Pour chaque carte, l'établissement transmet les données suivantes :

- Un bloc de données obligatoire :

- Code PIC de l'établissement ;
- Numéro d'identification de l'étudiant dans le pays ou la région ;
- Numéro européen de la carte (ESCN);
- Date d'échéance des droits de l'étudiant ;
- Niveau d'étude : licence, master ou doctorat ;
- Adresse mail de l'étudiant (optionnel);
- Type de carte (passive, électronique, avec quel niveau de compatibilité) ;
- Technologie de la carte.
- Un bloc de données académiques et personnelles optionnelles :
  - Nom complet de l'étudiant ;
  - Téléphone portable de l'étudiant.

La présence ou non du bloc optionnel est à la discrétion de l'établissement. Elle doit se faire en conformité avec la législation de son pays et ses déclarations CNIL. L'inclusion du nom complet de l'étudiant permet de croiser cette information avec celle inscrite sur la carte physique.

## Traitement des données

---

Le traitement vérifie l'unicité du numéro européen de la carte. En cas de doublon, la création de la carte est rejetée. Le support physique de la carte doit être mis au rebut.

Le code PIC est vérifié. L'établissement ne peut émettre des cartes que pour lui-même, ou dans certains cas à déterminer pour son regroupement d'établissement.

La date de fin d'effet ne peut pas être antérieure à la date du jour.

L'étudiant est ensuite informé de son inscription sur l'espace partagée européen. Il reçoit un mail, un SMS ou les deux avec un lien lui permettant de consulter les informations de la carte qui ont été enregistrées dans la plateforme, et des informations sur les usages qu'elle permet, en anglais ou dans sa langue. S'il ne souhaite plus apparaître sur la plateforme, il dispose du mail de l'administrateur fonctionnel des cartes dans son établissement pour lui signaler.

## Données en retour

---

Le service peut renvoyer les réponses suivantes :

- Confirmation d'enregistrement de la carte ;
  - Un étudiant peut avoir plusieurs cartes, même dans un seul établissement. C'est à l'établissement d'invalider les cartes précédentes si elles ne sont plus utilisables. S'il existe déjà au moins une autre carte pour cet étudiant dans cet établissement, un code spécifique le signale.
- Un message d'erreur indiquant :
  - L'absence d'une donnée obligatoire ou une donnée mal formée ;
  - L'existence d'une carte étudiante déjà enregistrées sous ce numéro de carte ;
  - Le numéro européen de la carte ne comporte pas le bon code PIC ;
  - La date de fin de droit est antérieure à la date du jour.

## Un fournisseur de service demande à certifier le statut étudiant d'un porteur de carte

L'étudiant présente sa carte qui fait l'objet d'une lecture automatique et d'une vérification du statut auprès du router numérique ESC-R.

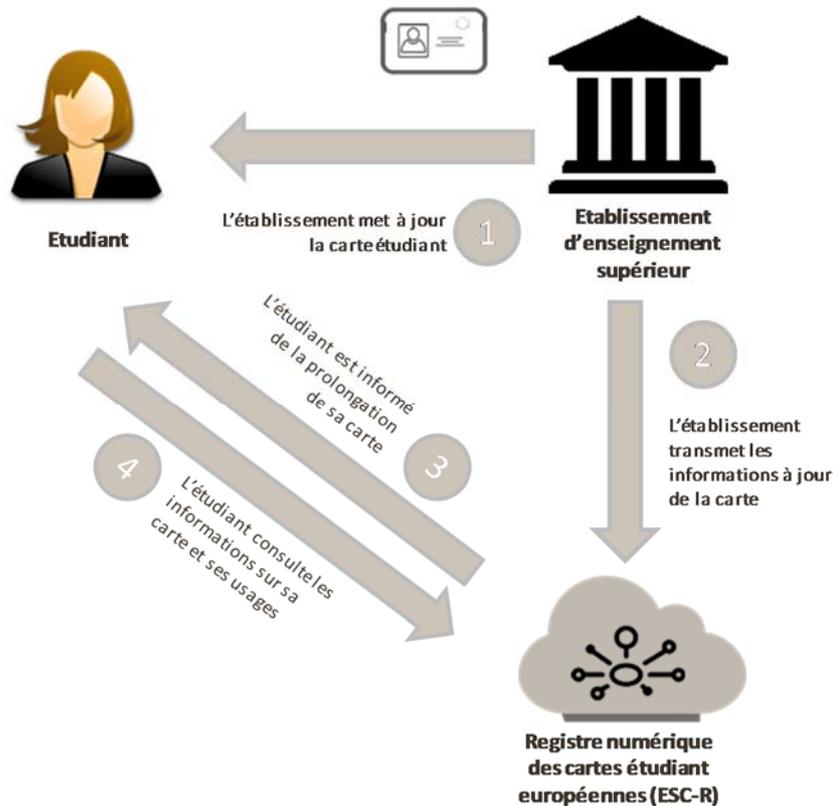


Figure 10 : un étudiant fait valoir ses droits auprès d'un fournisseur de service

### Type d'interaction

Cette opération peut se faire techniquement des deux manières :

- Par scan du code QR, où l'URL à appeler est directement encodée ;
- Par lecture de la carte à puce. L'URL est à construire à partir des données enregistrées dans la zone mémoire dédiée.

Dans les deux cas, un appel d'API de la plateforme est effectué.

### Accès

Ce service est en accès libre.

### Données en entrée

La donnée en entrée est le numéro européen de la carte.

Le fournisseur de service n'a pas besoin de s'identifier.

## Traitement des données

---

La carte est recherchée en base de données.

Il est proposé de journaliser les demandes de certification, en conservant l'adresse IP du demandeur.

Lorsqu'un nouveau fournisseur interroge le router pour la première fois, l'étudiant peut être informé par mail ou SMS de l'utilisation de sa carte auprès de ce nouveau fournisseur. Mais actuellement le fournisseur n'est pas identifiable. L'absence d'identification du fournisseur pose également une difficulté dans la détermination de la langue d'affichage du retour, que ce soit pour afficher la carte étudiante ou un message d'erreur. Par défaut la langue restera l'anglais.

## Données en sortie

---

Le service peut renvoyer les réponses suivantes :

- Confirmation du statut étudiant du porteur de la carte, avec affichage des données présentes dans le router en vue de croisement avec celles inscrites sur le support physique de la carte ;
- Carte étudiante invalide (sans préciser si c'est parce qu'elle n'a jamais été présente dans le router, ou si elle a été invalidée) ;
- Message d'erreur indiquant :
  - L'absence de la donnée en entrée, ou donnée mal formée (erreur potentielle de scan ou de lecture).

Si la langue du fournisseur de service est indiquée dans l'en-tête HTTP lors de l'interrogation du router, les messages sont affichés dans cette langue. Sinon, l'anglais est choisi par défaut. L'interface graphique permet de changer la langue.

# Un établissement met à jour une carte étudiante

Chaque année au moins, les établissements mettent à jour leurs cartes étudiantes. Usuellement, elles se contentent d'ajouter un sticker précisant la nouvelle date de fin de droits de l'étudiant. Le niveau d'étude ou la discipline peuvent également être modifiées de la même manière.

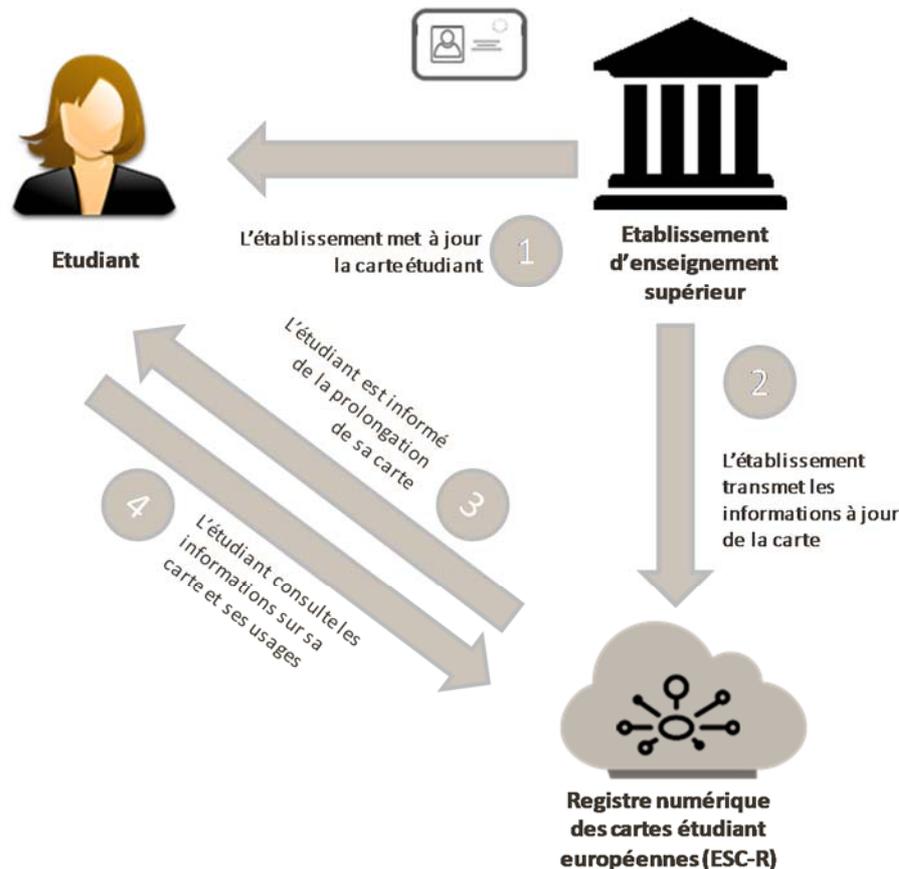


Figure 11 : La carte d'un étudiant est mise à jour sur le router numérique (ESC-R)

## Type d'interaction avec la plateforme

Dans un premier temps, il s'agit d'un envoi asynchrone de fichier contenant le lot des cartes à enregistrer. Le format du fichier est précisé au chapitre 6.

Dans un second temps, il s'agira d'un appel à une API synchrone, au fil de l'eau.

## Accès

Cette interaction n'est accessible qu'aux établissements enregistrés.

## Données en entrée

Pour chaque carte, l'établissement transmet les mêmes données que lors de la création de la carte (voir interaction « Un établissement délivre une carte à un étudiant »).

## Traitement des données

---

Le traitement vérifie l'existence de la carte dans la plateforme.

La date de fin d'effet ne peut pas être antérieure à la date du jour.

L'étudiant est ensuite informé de la prolongation de son inscription sur l'espace partagé européen par SMS ou mail, comme dans le cas de la création.

## Données en retour

---

Le service peut renvoyer les réponses suivantes :

- Conformation de mise à jour de la carte ;
  - Un étudiant peut avoir plusieurs cartes, même dans un seul établissement. C'est à l'établissement d'invalider les cartes précédentes si elles ne sont plus utilisables. S'il existe déjà au moins une autre carte pour cet étudiant dans cet établissement, un code spécifique le signale.
- Un message d'erreur indiquant :
  - L'absence d'une donnée obligatoire ou une donnée mal formée ;
  - L'absence de carte étudiante enregistrée sous ce numéro de carte ;
  - La date de fin de droit est antérieure à la date du jour.

## Un établissement invalide une carte étudiante

Un établissement peut invalider la carte pour des multiples raisons : carte perdue, carte volée, carte détruite, étudiant ne bénéficiant plus du statut, etc.

### Type d'interaction

---

Dans un premier temps, il s'agit d'un envoi asynchrone de fichier contenant le lot des cartes à enregistrer. Le format du fichier est précisé au chapitre 6.

Dans un second temps, il s'agira d'un appel à une API synchrone, au fil de l'eau.

### Accès

---

Cette interaction n'est accessible qu'aux établissements enregistrés.

### Données en entrée

---

L'établissement transmet le numéro européen de la carte.

Aucune explication sur la raison de la suppression de la carte n'est demandée.

L'étudiant est informé par mail ou SMS de l'invalidation de sa carte.

### Traitement des données

---

Les données concernant la carte sont supprimées.

Une trace de la suppression est conservée, enregistrant uniquement le code PIC de l'établissement, le numéro étudiant, l'identifiant européen de la carte et la date et l'heure de suppression. Cette trace est utile pour répondre qu'une carte est invalide plutôt que de dire qu'elle est inconnue. Elle est conservée durant 18 mois.

### Données en retour

---

Le service peut renvoyer les réponses suivantes :

- Confirmation de la suppression de la carte ;
- Message d'erreur indiquant :
  - L'absence d'une donnée en entrée, ou donnée mal formée ;
  - La carte désignée n'existe pas ;

# Un établissement se retire du dispositif de la carte étudiante européenne

## Type d'interaction

---

Par simple courrier, le représentant légal de l'établissement informe le superviseur de son pays ou sa région qu'il souhaite se retirer du dispositif. Aucune justification n'est demandée. Sur la base du courrier, le superviseur retire l'établissement du router numérique ESC-R.

## Accès

---

Seul le superviseur peut retirer un établissement sur la plateforme.

## Données en entrée

---

La donnée en entrée est le code PIC de l'établissement.

## Traitement des données

---

L'établissement est désactivé. Sa clé d'API est révoquée. Ses certificats sont supprimés. Une trace horodatée de sa désactivation est conservée.

Toutes les cartes étudiant de cet établissement sont invalidées. Les étudiants en sont informés par mail et/ou SMS.

En cas de fusion d'établissement, ou de séparation, il est demandé de désactiver les établissements de départ et d'enregistrer les établissements finaux. De nouvelles cartes étudiantes doivent alors être délivrées.

## Données en retour

---

Le service peut renvoyer les réponses suivantes :

- Confirmation de la désactivation de l'établissement et de l'invalidation de toutes ses cartes ;
- Message d'erreur indiquant :
  - L'absence d'une donnée en entrée, ou donnée mal formée ;
  - L'établissement désigné n'existe pas ;

## Synthèse des règles de fonctionnement

- Un établissement peut avoir plusieurs cartes étudiantes européennes actives par étudiant.
- Le lendemain de la date d'échéance des droits d'étudiant, la carte statut étudiant est automatiquement supprimée de la plateforme d'échange. L'étudiant est informé par mail ou SMS de l'invalidation de sa carte.
- La trace de la suppression est conservée 18 mois.

## Synthèse des droits par rôles des utilisateurs de la plateforme d'échange

- Administrateur fonctionnel global
  - *Ces droits restent à préciser.*
- Administrateur technique global
  - Programmer de l'intégration des fichiers de cartes d'un établissement ;
- Superviseur pour un pays ou une région
  - Inscrire un établissement ;
  - Accepter ou refuser l'inscription d'un établissement ;
  - Générer une clé d'API pour un établissement ;
  - Révoquer la clé d'API d'un établissement ;
  - Désactiver un établissement ;
  - Paramétrer le besoin ou non d'un code région dans son périmètre ;
  - Paramétrer les recommandations sur les blocs optionnels sur son périmètre.
- Administrateur fonctionnel pour un regroupement d'établissements :
  - *Ces droits restent à préciser.*
- Administrateur d'un établissement :
  - Enregistrer une carte étudiante dans le router ESC-R ;
  - Mettre à jour une carte étudiante dans le router ESC-R ;
  - Invalider une carte étudiante dans le router ESC-R ;
  - Modifier des informations sur son établissement : données de contact, données techniques, certificats.

## 6. Architecture technique de la plateforme d'échange

Ce chapitre détaille le volet technique de la plateforme d'échange, avec en particulier les formats d'échange de données, les conditions d'utilisation et le niveau de service attendu.

### Le format pivot d'échange des données

Les données stockées dans la plateforme sont :

- Les établissements participants ;
- Les cartes étudiant européennes actives, comprenant des données limitées sur l'étudiant.

### L'établissement d'enseignement supérieur

Un établissement est décrit de la manière suivante, dans un bloc obligatoire.

Nom	Description	Type de données	Taille	Obligatoire	Valeurs types
<b>country-code</b>	Code pays de l'établissement	Chaîne de caractère de taille fixe	2	Obligatoire	Code ISO
<b>region-code</b>	Code de la région de l'établissement	Chaîne de caractère de taille variable	3	Optionnel	Code NUTS (niveau 1, 2 ou 3)
<b>hei-pic-code</b>	Code PIC de l'établissement	Chaîne de caractère de taille fixe	9	Obligatoire	Fourni par ERASMUS
<b>hei-group-pic-code</b>	Code PIC du regroupement auquel appartient l'établissement	Chaîne de caractère de taille fixe	9	Obligatoire	Fourni par ERASMUS
<b>hei-name</b>	Nom de l'établissement	Chaîne de caractère de taille variable	300	Obligatoire	Le nom officiel de l'établissement
<b>cards-admin-email</b>	Mail de l'administrateur fonctionnel des cartes étudiant	Chaîne de caractère de taille variable	320	Obligatoire	
<b>technical-admin-email</b>	Mail de l'administrateur technique des cartes étudiant	Chaîne de caractère de taille variable	320	Obligatoire	

Tableau 4 : descripteur des données administratives et de contact d'un établissement d'enseignement supérieur

Un conteneur décrivant les API fournies par l'établissement sera défini ultérieurement.

## La carte étudiante européenne

Une carte étudiante est décrite par deux conteneurs :

1. Le premier conteneur contient toutes les données identifiant la carte de l'étudiant, l'étudiant et ses droits. La présence de bloc et de toutes les informations dont il est composé est obligatoire ;
2. Le second conteneur décrit les données académiques et personnelles de l'étudiant. Elles sont toutes optionnelles. Leur présence ou non relève du choix de l'établissement. Les pays et les régions peuvent recommander des règles communes.

Nom	Description	Type de données	Taille en octets	Obligatoire	Valeurs types
<b>hei-pic-code</b>	Code PIC de l'établissement émetteur de la carte	Chaîne de caractères de taille fixe	9	Obligatoire	Fourni par ERASMUS
<b>student-code</b>	Numéro de l'étudiant	Chaîne de caractères de taille variable	32	Obligatoire	Le numéro de l'étudiant dans le pays, la région ou l'établissement d'origine
<b>europen-card-id</b>	Numéro européen de la carte	Chaîne de caractères	36	Obligatoire	UUID version 1, avec code Pic à la place de l'adresse MAC
<b>expiry-date</b>	Échéance des droits au statut étudiant	Chaîne de caractères	10	Obligatoire	YYYY-MM-DD
<b>student-email</b>	Adresse mail de l'étudiant	Chaîne de caractères de taille variable	320	Obligatoire	Adresse mail valide
<b>card-type</b>	Type de carte	Chaîne de caractères de taille fixe	1	Obligatoire	1 : carte passive 2 : carte électronique sans zone de donnée commune 3 : carte électronique avec zone de données commune 4 : carte électronique acceptant les applications tierces

<b>card-electronic-standard</b>	Le standard normatif avec laquelle la carte à puce est compatible	Chaîne de caractères hexadécimaux de taille fixe	2	Obligatoire	00 : non reconnu ou carte passive 03 : ISO 14443 type A jusqu'au niveau 3 06 : ISO 14443 type B jusqu'au niveau 2 07 : ISO 14443 B jusqu'au niveau 3
<b>card-electronic-brand</b>	Le constructeur fournissant la technologie de carte à puce	Chaîne de caractères hexadécimaux de taille fixe	2	Obligatoire	00 : carte passive ou marque non reconnue, C0 : Calypso D1 : NXP Desfire EV1
<b>card-electronic-technology</b>	La technologie d'un constructeur qui implémente la norme	Chaîne de caractères hexadécimaux de taille fixe	4	Obligatoire	0000 : carte à microprocesseur ou type de carte non reconnue ou information indisponible, 0001 : mifare classic 1k 0002 : mifare classic 4k 0003 ou 003A : mifare ultralight c

Tableau 5 : conteneur de données obligatoire de la carte étudiante européenne

Nom	Description	Type de données	Taille en octets	Obligatoire	Valeurs types
<b>student-name</b>	Noms et prénoms de l'étudiant	Chaîne de caractère de taille variable	100	Optionnel	Tous les composants du nom séparés par des espaces, dans l'ordre attendu par la culture d'origine Standard OpenIDConnect
<b>student-phone-number</b>	Téléphone mobile de l'étudiant	Chaîne de caractère de taille variable	15	Optionnel	Format international E164 Par exemple +3323456789
<b>student-academic-level</b>	Niveau d'étude suivi par l'étudiant	Chaîne de caractères de taille fixe	1	Optionnel	Le référentiel du cadre européen des certifications est utilisé (EQF) classant les formations tout au long de la vie de 1 à 8. Le processus de Bologne attribue à un étudiant en enseignement supérieur un niveau entre 6 et 8. 6 : premier cycle, niveau licence. 7 : second cycle, niveau master. 8 : troisième cycle, niveau doctorat.

Tableau 6 : conteneur des données académiques et personnelles optionnelles de l'étudiant, associé à une carte

## Le fichier d'import des cartes étudiant européennes

Les établissements choisissant de transmettre un fichier plutôt que de faire appel aux API doivent fournir sur un canal chiffré un fichier XML horodaté intitulé **eupean-student-cards [code PIC de l'établissement]-yyyymmdd-hhmm-numero-dordre.xml**.

Le numéro d'ordre commence à 1 et augmente de 1 à chaque nouveau fichier transmis.

Le fichier est mis à disposition sur un espace sécurisé SFTP dont le login et le mot de passe sont transmis à la plateforme d'échange. C'est cette dernière qui se connecte pour aller télécharger le fichier.

Le jeu de caractère attendu est UTF-8.

Les données attendues sont une liste d'ordres structurés de la manière suivante :

- Soit un ordre d'enregistrement de carte, avec les trois descripteurs ;
- Soit un ordre de mise à jour de carte, avec les trois descripteurs ;
- Soit un ordre de suppression de carte avec l'identification de la carte.

Pour que le service de certification en ligne de la carte soit actif rapidement après la délivrance de la carte, il est demandé à ce que ce fichier soit transmis au moins une fois par jour.

## Conditions d'utilisation et niveau de service attendu

Dans son fonctionnement courant, la plateforme d'échange devra respecter un niveau de service et les exigences formulées ci-dessous. Elles s'appliquent à l'environnement de production.

La plateforme d'échange peut être interrogée 24/24 7/7. Les plages de maintenance doivent être réduites au maximum et située aux périodes où les cartes sont moins utilisées, soit avant 5h et après 22h en jour ouvré, ou pendant les week-ends.

Le nombre de cartes étudiantes européennes attendues pendant la période d'expérimentation est de 200 000. La volumétrie attendue est de l'ordre d'une centaine de méga-octets.

Le nombre d'interactions attendu avec la plateforme est en moyenne d'une certification par carte et par jour. La grande majorité (80%) de l'activité est concentrée sur les horaires d'ouverture des établissements, soit entre 8h et 19h du lundi au vendredi. En fin d'expérimentation, une fois les 200 000 cartes actives, ceci représente une charge moyenne de 15 000 certifications par heure, soit 4 par seconde.

L'exigence de performance sur le temps de réponse est la suivante :

- 90% des transactions s'effectuent en moins d'1 seconde ;
- 95% des transactions s'effectuent en moins de 2 secondes ;
- 99% des transactions s'effectuent en moins de 5 secondes ;
- Maximum de 10 secondes.

L'exigence de disponibilité est la suivante :

- Le taux de disponibilité est de 99%, soit pas plus de 15 minutes d'indisponibilité par jour en moyenne ;

- La fréquence admissible des incidents : pas plus d'une indisponibilité par jour
- La durée maximale d'indisponibilité acceptable suite à un incident est d'une heure ;

La perte maximale de données admissible est d'une journée. Autrement dit, en cas de perte de données, la dernière sauvegarde date au plus tard d'une journée.

Ces exigences imposent de :

- mettre en place des mécanismes de haute disponibilité, basés sur la redondance des briques techniques ;
- mettre en place un outil de supervision pour être automatiquement alerté en cas d'incident ;
- mettre en place un outil de métrologie pour mesurer le taux de disponibilité réel.

## La technologie

En termes techniques, cette plateforme est implémentée sous la forme de services HTTP d'une part et d'un bus de données de type ESB.

Les services peuvent être conçus de deux manières :

- Soit dans un paradigme d'appel de procédure à distance où les échanges sont réalisés selon la norme SOAP avec HTTP comme protocole de transport. Leur sécurisation se base usuellement sur la mise en place d'un VPN. L'usage de SOAP entraîne en général complexité et adhérence entre client et serveurs. Les clients sont typiquement des serveurs.
- Soit dans un paradigme orienté ressources (dit REST) qui s'appuie sur http comme protocole applicatif. La sécurisation des échanges repose sur OAuth2 ou OpenId (comme France Connect) et un chiffrement TLS du canal. Les clients typiques sont des serveurs, des applications mobiles natives, des navigateurs, etc.

Ces deux ne sont pas irréconciliables. Il est possible de concevoir l'API RPC en s'inspirant des méthodes de conception REST. Il s'agit de définir des ressources, potentiellement imbriquées, en implémentant des méthodes RPC standardisées : lister, lire, créer, mettre à jour et supprimer. Ceci permet de profiter de la lisibilité promue par REST, et assure une certaine proximité entre les l'API. Un standard est proposé par Google : <https://cloud.google.com/apis/design/resources>.

Le bus de données sera en particulier en charge de réceptionner les fichiers d'imports et les convertir en appels à l'API.

## Règles communes à toutes les implémentations

Les services de la plateforme d'échange obéissent à une gestion sémantique des versions (décrite complètement sur <http://semver.org/lang/fr/>).

La compatibilité ascendante des API sera maintenue autant que possible.

Lorsque c'est possible, les nouveaux paramètres seront optionnels, avec une valeur par défaut compatible avec le fonctionnement actuel. En cas de changement incompatible, le serveur peut maintenir plusieurs versions de l'API pour faciliter la connexion des clients qui ne sont pas encore à jour.

## Règles sur l'implémentation REST XML

Le format de réponse préféré est XML, selon un schéma valide.

Les connexions seront chiffrées en TLS.

Les paramètres envoyés avec la méthode POST doivent être transmis au format *application/x-www-form-urlencoded*.

### Gestion des erreurs

---

La sémantique des codes erreurs HTTP est utilisée.

Condition	Code réponse HTTP
Les paramètres de l'appel ne sont pas convenables	400
L'authentification fournie par le client est insuffisante	403
La méthode d'appel n'est pas convenable	405
Une anomalie se produit lors du traitement côté serveur	500
Le service est en maintenance ou ne répond pas pour se protéger	503

Le contenu de la réponse doit être une chaîne de caractère XML dont la racine est <error-response>, contenant un message d'erreur pour le développeur, et un message d'erreur pour l'utilisateur.

## Règles sur l'implémentation RPC SOAP

*Les règles restent à déterminer.*

## 7. Analyse de risques (work in progress)

L'objectif de la carte étudiante européenne étant de créer un haut niveau de confiance sur le statut réel d'étudiant du porteur de carte. Des mesures de protections adaptées doivent être mise en place contre les tentatives d'abus du système.

Ce chapitre analyse de quelle manière le système proposé peut être détourné, et propose des mesures pour les empêcher.

*Note : le contenu de ce chapitre constitue une analyse préliminaire partielle.*

### Les risques encourus

Risques identifiés	Conséquences
<b>Le porteur de carte n'est pas étudiant.</b>	<ul style="list-style-type: none"><li>✓ Cout pour le prestataire de service qui propose une offre économiquement avantageuse ;</li><li>✓ Accès indu à des espaces réservés aux étudiants en général (entrées/sorties des campus).</li></ul>
<b>Le porteur de carte n'est pas celui dont l'identité est inscrite sur la carte</b>	<ul style="list-style-type: none"><li>✓ Empreint de ressources à un autre nom, risque de vol ;</li><li>✓ Accès indu à un espace réservé à l'étudiant (salle libre-service) ;</li></ul>
<b>Le porteur de carte est étudiant mais la plateforme dit le contraire.</b>	<ul style="list-style-type: none"><li>✓ Déni de droit ;</li></ul>

*L'inventaire des risques est à poursuivre, et la qualification de leur degré de criticité reste à faire.*

### Les scénarios de menace

#### Identification frauduleuse d'un établissement

Un tiers se fait passer pour un établissement et souhaite s'inscrire à la plateforme, ou détourner l'inscription d'un établissement légitime pour enregistrer de fausses cartes étudiantes. La question posée ici est de savoir comment garantir que la personne ou le programme qui interagit avec la plateforme est légitime.

#### Mesures de protection :

- L'inscription d'un établissement dans la plateforme n'est pas de sa propre initiative. Seul le superviseur de son territoire peut l'effectuer.
- ERASMUS joue le rôle de tiers de confiance dans l'identification des établissements. Le superviseur doit vérifier que l'établissement n'est pas déjà inscrit et que son code PIC existe officiellement.
- L'établissement dispose d'une clé d'API qui est un « mot de passe » pour les programmes clients qui interrogent l'API de la plateforme d'échange. Cette clé lui est transmise sur un canal sécurisé et peut être révoquée unilatéralement par le superviseur.

- Toutes les communications réseau entre l'établissement et la plateforme d'échange sont chiffrées à l'aide de certificats.
- Le filtrage par adresse IP est-il utile ?

Quels sont les risques de transmettre les éléments de génération de carte à un acteur non légitime (clé d'API, logo, algorithme, etc.) ?

## Création d'un support de carte frauduleux

---

*Scénarios de menace à développer*

### Router ESC-R frauduleux

---

Un tiers se fait passer pour le router et reçoit les inscriptions et la suppression de cartes d'un établissement.

Un tiers se fait passer pour la plateforme et veut répondre aux certifications à la place de la plateforme.

### Inscription frauduleuse de carte

---

Un tiers enregistrer une fausse carte dans le router numérique.

Un tiers enregistre dans le router des cartes qui n'ont pas été délivrées réellement par l'université. Ce volant de cartes reconnues peut être utilisé pour imprimer de fausses cartes plus tard.

Les données enregistrées dans le router sont fausses : date de validité, nom, prénom, etc.

La carte présentée a été volée.

Une carte est reproduite en changeant la photo.

Une fausse carte est émise en imitant le logo. Variante en recopiant le code QR d'une autre carte.

#### **Mesures de protection :**

- A déterminer.
- Limiter la durée de vie de la carte à un an ?

### Invalidation frauduleuse de carte

---

Un tiers invalide une carte dans le router.

### Vol de données

---

Un tiers interroge le router de carte avec des identifiants de carte aléatoires.

Un tiers parvient à recopier le router des cartes.

### Rendre la plateforme d'échange indisponible

---

L'indisponibilité de la plateforme peut être provoquée par une attaque de déni de service distribuée s'attaquant au router ESC-R.

Cette indisponibilité empêche les niveaux de contrôle automatique par scan optique ou électronique, obligeant le fournisseur de service à se contenter d'un contrôle visuel. Par ailleurs, le temps de réponse de la plateforme est augmenté, ce qui peut désorganiser les services si ceci a lieu à un moment où les étudiants se présentent en nombre.

#### **Mesures de protection :**

- Protéger la plupart des API avec une clé identifiant le fournisseur de service ;
- Les API qui ne peuvent pas être protégées par une clé doivent être protégées par ?
  - Limite sur le nombre d'interrogations de la même source (évident mais inefficace et risque de gêner un vrai usage) ;
  - Ajouter une empreinte sur la carte pour s'en servir de mot de passe et rejeter automatiquement les requêtes invalides ?
- Proposer un temps d'attente maximum très court lors d'un scan, de l'ordre de 5 secondes.

## Synthèse des mesures de protection en place

*Cette synthèse sera effectuée une fois l'analyse terminée.*

## Le traitement des données à caractère personnel

Les données personnelles stockées dépendent des choix de chaque établissement, voire des choix de chaque pays.

Au minimum le router ESC-R stocke les adresses mails des étudiants.

Au plus, le router stocke son nom, prénom, niveau académique et téléphone portable.

Une étude d'impact sur la vie privée doit être réalisée. Elle doit en particulier étudier s'il existe un risque de traçabilité avec l'introduction d'un numéro de carte européen unique.

Les formalités de déclarations aux CNIL des quatre pays participant à l'expérimentation doivent être étudiées. Il est également nécessaire de vérifier si les déclarations CNIL des établissements sont impactées par l'envoi des informations au router ESC-R.

Le projet impliquant de nombreux acteurs, il est certainement opportun de partager un code of conduct commun définissant les bonnes pratiques que les fournisseurs de service et de données s'engagent à respecter. Les pratiques d'eduGAIN peuvent être une source d'inspiration

(<https://www.geant.org/uri/Pages/dataprotection-code-of-conduct.aspx>) :

- Publication d'une Privacy Policy (en Anglais au moins) mentionnant
  - l'entité légale,
  - la finalité des traitements,
  - la catégorie des attributs utilisateurs,
  - le destinataire des données,
  - les modalités d'accès/rectification des données.
- Demande d'attributs utilisateurs minimale pour le bon fonctionnement du service,

- Pas d'utilisation des données pour d'autres traitements,
- Pas de traitement secondaire des données,
- Sécurisation des données.

## Conservation des données dans le router

Les données concernant une carte sont conservées 18 mois après :

- Leur demande de suppression par l'établissement propriétaire ;
- La date de fin de droit.

Pendant cette période, seules sont conservées les données permettant d'identifier la carte et l'étudiant. Ses données personnelles et académiques sont supprimées.

## Annexes

### Synthèse des exigences qui pèsent sur un établissement qui souhaite délivrer une carte étudiante européenne

Référence	Thème	Règle
<b>R001</b>	Protection des données personnelles	Recueillir le consentement de l'étudiant avant d'enregistrer les cartes délivrées dans la plateforme d'échange
<b>R002</b>	Support physique de la carte	Intégrer le logo holographique selon les règles définies au chapitre 2
<b>R003</b>	Support physique de la carte	Intégrer le pays de l'établissement, son code PIC et le numéro de l'étudiant
<b>R004</b>	Support physique de la carte	Générer un identifiant unique pour la carte
<b>R005</b>	Support physique de la carte	Intégrer le code barre de contrôle optique selon les règles définies au chapitre 2
<b>R006</b>	Plateforme d'échange	Transmettre les informations permettant d'inscrire l'établissement sur la plateforme d'échange
<b>R007</b>	Plateforme d'échange	Transmettre un fichier des mises à jour (nouvelles cartes, cartes prorogées et cartes invalidées) au moins une fois par jour
<b>R008</b>	Sécurité des données	?

### La carte étudiante et l'identification des étudiants dans chaque pays

En attendant l'état des lieux qui sera transmis par les différents pays, les informations connues sont rappelées ici.

#### En France

Le comité national de la carte multiservice étudiant et de ses usages (CNCE) est piloté par la CPU et le CNOUS. Toutes les cartes émises par les établissements bénéficient de la reconnaissance d'un statut d'étudiant pour l'année universitaire en cours, et du porte-monnaie privatif Izly pour les services marchands des Crous. Selon les établissements, les cartes permettent le contrôle d'accès, l'emprunt d'ouvrage en BU, la réservation de salle, les photocopies et la libération d'impressions.

Les technologies employées sont principalement la DESfire EV1, qui supporte plusieurs applications (80%), l'Ultralight C (pour Izly seulement) et des MIFARE « Classic » pour des raisons de compatibilité avec le contrôle d'accès ou les transports en commun.

Il existe principalement deux systèmes de gestion de carte en France :

- Uni'Campus, édité par Monecarte ;
- Un concurrent.

Les étudiants sont identifiés par un numéro national appelé INE : identification nationale des étudiants. Il est composé de 10 chiffres et une lettre. Depuis 2012 il est émis par le répertoire national des identifiants élèves, étudiants et apprentis (RNIE).

Les établissements utilisent aussi leur propre identifiant, mais l'INE est systématiquement connu pour chaque étudiant.

## En Allemagne

---

*À compléter.*

## En Italie

---

*À compléter*

Il existe en Italie un numéro d'étudiant national.

## En Irlande

---

*À compléter.*

