

# Système de reconnaissance faciale à base de carte à puce

Vincent Arguenon, André Bergues Lagarde, Jérôme Ferru, Fahim Hasnaoui,  
Christophe Rosenberger

ENSIB / LVR

[\[prenom.nom\]@ensi-bourges.fr](mailto:{prenom.nom}@ensi-bourges.fr)

**Mots clés :** Authentification, contrôle d'accès, biométrie, reconnaissance faciale, carte à puce, certification, cryptographie appliquée.

## Résumé :

La révolution des NTIC n'avait pas été prévue par les créateurs d' Internet, et le manque d'études au niveau de sa sécurité a engendré le développement des phénomènes de virus, spam, intrusions.

Aujourd'hui, comme nous le présentons dans cet article, de plus en plus de spécialistes s'accordent à miser sur un développement majeur de la biométrie. Si celui-ci devient effectif, il serait regrettable de reproduire les mêmes erreurs que celles qui ont été commises au sujet de la croissance d' Internet. En prenant en compte ces considérations, nous avons conçu une solution répondant aux risques éventuellement posés par une distribution de masse.

Notre premier objectif a été de produire une solution d'authentification biométrique dont la sécurité globale ne serait pas mise en péril si le fonctionnement du système devait être rendu public. Nous avons puisé l'originalité de notre solution dans le couplage de la technologie des cartes à puces avec nos derniers résultats dans le domaine de la reconnaissance faciale.

Parallèlement, nous avons cherché à limiter d'éventuels risques sur les plans éthique et juridique. Notre système contourne le stockage de données personnelles sur base de données, vivement critiqué par les organismes de protection des libertés individuelles, en faisant appel à un stockage sur une carte à puce évoluée. Chaque individu devient ainsi l'unique détenteur des informations sensibles le concernant.

Dans cette même logique, nous nous sommes tournés vers l'identification par reconnaissance faciale, car cette méthode, contrairement à l'analyse d'iris ou d'empruntes digitales, est analogue aux mécanismes que nous utilisons quotidiennement pour nous reconnaître.

Enfin, une autre originalité consiste à utiliser des certificats, non seulement pour établir le lien entre un nom et une clé publique, mais aussi entre un nom et une personne physique. Le but étant de s'assurer de l'identité de la personne.

## 1. Etat de l'art

### 1.1. Authentification biométrique

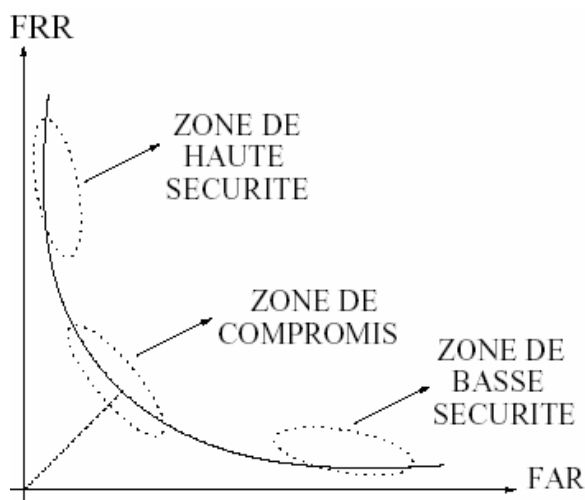
L'Organisation internationale de normalisation s'intéresse vivement à l'utilisation de la biométrie. Lors de la conférence d'Ottawa de 1998, les empreintes digitales, l'iris, les mains, et la géométrie du visage ont été identifiés comme étant les quatre principaux indicateurs biométriques.

La reconnaissance d'un individu à l'aide de données biométriques nécessitent d'une manière générale la mise en place de deux phases : une d'enrôlement et l'autre appelée reconnaissance. La phase d'enrôlement est une phase d'apprentissage de reconnaissance de formes qui a pour but de recueillir des informations sur la personne à identifier. Plusieurs acquisitions de données peuvent être réalisées sous différents angles afin d'assurer une certaine robustesse du système à la reconnaissance d'un individu. Le traitement lié à l'enrôlement n'a pas de contrainte de temps, puisqu'il s'effectue « hors-ligne ».

La phase de reconnaissance compare une donnée acquise sur l'individu à reconnaître avec des données issues de l'enrôlement.

La biométrie occupe une place de plus en plus importante dans notre société, une illustration peut-être par exemple une apparition possible des passeports biométriques en France et en Belgique au cours de l'année 2007.

L'objectif de notre solution est de trouver le meilleur compromis entre les zones de haute et de basse sécurité afin d'obtenir les meilleurs résultats.



FAR : False Acceptation Rate (accepter à tort un individu, ou « taux faux négatif »)

FRR : False Rejection Rate (refuser à tort un individu, ou « taux faux positif »)

### 1.2. Particularité de la reconnaissance faciale

Sur le marché de la biométrie, la reconnaissance faciale n'est pas la méthode la plus utilisée. En effet, l'utilisation des empreintes digitales (entre 40 et 50% de parts de marché contre 15% pour l'identification par le visage) prédomine, car cette méthode offre l'avantage de produire des résultats très satisfaisants en termes de qualité de reconnaissance.

Toutefois, le marché de la reconnaissance faciale pourrait connaître une importante expansion, dans la mesure où cette méthode ne nécessite pas la coopération de l'individu. Ce principe de contrôle devient intéressant pour les zones où un contrôle systématique d'individus est nécessaire (aéroports, lieux publics,...)

Certains chercheurs misent actuellement sur un développement futur des technologies disponibles, permettant ainsi d'arriver à augmenter la qualité des résultats, et développer cette technologie. C'est notamment la position de C. von der Malsburg [1], responsable de plusieurs instituts de recherche, en Europe comme aux États-Unis. Son idée est d'arriver à long terme à un système de caméras intelligentes basant l'identification sur les mêmes critères que ceux qu'utilisent les individus entre eux (visage, démarche, gestuelle, style vestimentaire, etc...) La commercialisation de ses travaux a été confiée à l'entreprise ZN Vision Technology afin d'instaurer, entre autres, un système d'authentification dans l'aéroport de Berlin. Cette société a par la suite été rachetée en 2003 par l'entreprise que beaucoup considèrent comme le leader du marché de la reconnaissance faciale: Viisage. Ceci laisse ainsi penser que le marché de la reconnaissance faciale pourrait très bien connaître prochainement une croissance remarquable.

### *1.3.Aspect éthique*

Les travaux dans le domaine de la biométrie doivent forcément s'accompagner d'une analyse des contraintes de type éthique. Il est nécessaire d'être particulièrement vigilant dans la diffusion de produits biométriques. Si un produit recevait une opposition d'un organisme de protection des libertés personnelles cela pourrait créer une perception négative des produits du domaine de la part de l'opinion publique. Cette situation ralentirait de façon certaine la diffusion de ce genre de produits.

Ainsi, en ce qui concerne la protection des données européennes, tout traitement de données à caractère personnel doit être déclaré auprès de la CNIL (Commission Nationale de l'Informatique et des Libertés). Dans le cadre de la biométrie, tous les traitements automatisés, publics ou privés, comportant des données biométriques nécessaires au contrôle de l'identité des personnes, doivent désormais être soumis à une autorisation préliminaire de l'organisme cité plus haut. Ce point doit absolument être respecté dans le déploiement de solutions.

De plus, au niveau conceptuel, la CNIL s'oppose pour le moment à la constitution de bases centralisées de données personnelles, mais elle tolère en revanche les dispositifs techniques qui stockent ces informations sensibles sur des supports individuels [2]. Comme il le sera présenté plus tard en détails, nous avons étudié notre système afin qu'il corresponde à ces contraintes.

D'autre part, aux USA, la législation en matière de protection des données personnelles est embryonnaire et la préoccupation sécuritaire est prioritaire. C'est pourquoi, plusieurs expérimentations de vidéo surveillance et reconnaissance faciale ont été réalisées.

Il convient également de faire très attention aux différentes associations de consommateurs qui regardent de très près l'ensemble des dérives possibles liées à la biométrie en général. En effet, l'identification faciale est réalisable à l'insu de la volonté de l'individu, nous pouvons donner l'exemple de l'identification de personnes qui seraient interdites d'assister à un match de football dans un stade.

### 1.4.Principe des descripteurs

La solution que nous utilisons pour la reconnaissance faciale est celle des moments de Zernike. Le principe est d'utiliser des points d'intérêts (ou points caractéristiques) d'un objet ou d'une personne. Ainsi, on ne compare pas deux images mais plutôt deux « descriptions » qui doivent avoir des propriétés d'invariance par rotation, par changements d'échelles, etc... Une robustesse vis-à-vis des conditions d'éclairage, de modifications de l'information biométrique (par exemple suppression d'une moustache dans le cas du visage ou d'une coupure au doigt pour les empreintes digitales) est préférable. Le traitement de reconnaissance doit être réalisé en temps réel. Les moments de Zernike  $Z[p,q]$  calculés sur l'image  $I(\rho, \theta)$  en coordonnées polaires sont également invariants par rotation et changement d'échelles de l'objet et sont données par la formule suivante :

$$\mathfrak{S}_{[p,q]}^*(\rho, \theta) = \sum_{s=0}^{(p-|q|)/2} \frac{(-1)^s [(p-s)!] \rho^{p-2s} e^{-jq\theta}}{s! ((p-|q|)/2-s)! ((p-|q|)/2-s)!}$$
$$Z_{[p,q]} = \frac{p+1}{\pi} \int_{\theta=0}^{2\pi} \int_{\rho=0}^{\infty} I(\rho, \theta) \mathfrak{S}_{[p,q]}^*(\rho, \theta) \rho d\rho d\theta$$

## 2. Principes techniques et scénario

### 2.1.Présentation des techniques utilisées

#### 2.1.1. Présentation générale

Ce projet met en œuvre différents procédés de sécurité tels que des mécanismes de chiffrement (génération de clés asymétriques, chiffrement et déchiffrement RSA), l'utilisation de certificats pour la validation des données stockées sur la carte à puce, ainsi que la sécurisation de la carte à puce avec un code PIN par exemple.

D'une manière plus générale, la solution que nous proposons permet de réaliser le lien entre un certificat, une clé publique, et une personne physique donnée.

De plus, les étapes utilisées pour la phase d'enrôlement sont les suivantes :

- Présentation du client devant la borne.
- Capture de l'image par la caméra.
- Transfert de l'image vers la borne biométrique.
- Calculs des descripteurs au niveau de la borne biométrique.
- Stockage des descripteurs dans la carte.
- Envoi de la carte au client.

En ce qui concerne la phase de reconnaissance, les étapes nécessaires à ce processus sont les suivantes :

- La personne se présente devant la borne.
- La caméra prend la photo puis l'envoie à la borne biométrique
- La borne biométrique recalcule les descripteurs puis compare les données ainsi calculées avec une base de données « utilisateur ».
- Si le test est réussi, alors la borne envoie un signal d'acceptation au moniteur de référence.

### 2.1.2. Utilisation de certificat

La création d'un certificat nécessite l'obtention de différentes informations. Ainsi, une phase d'enregistrement est nécessaire pour la création d'un tel document électronique. Il est impératif de pouvoir vérifier l'intégrité et la conformité des données présentes sur la carte à puce.

L'empreinte générée est réalisée à partir d'une signature de l'ensemble des informations de l'utilisateur contenues dans le certificat à l'aide de la clé privée de l'autorité de certification.

La réalisation d'un certificat consiste à générer une empreinte à partir des infos de l'utilisateur en utilisant une clé privée de l'autorité de certification puis à envoyer l'ensemble des données construites sur la carte à puce. Cette opération permettra par la suite de s'assurer que la carte à puce a bien été réalisée par l'autorité de certification souhaitée.

### 2.1.3. Technologie des cartes à puce

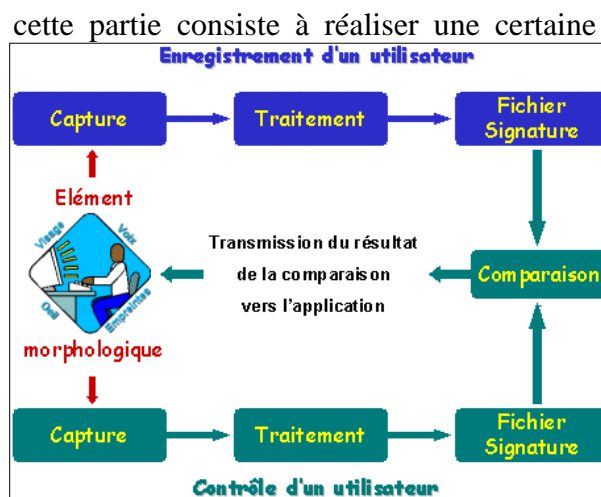
En ce qui concerne la carte à puce, il convient de préciser que la carte que nous utilisons doit posséder un microcontrôleur afin de pouvoir réaliser des traitements comme la vérification du code PIN par exemple. Ainsi, la solution que nous proposons ne permet pas d'utiliser des cartes qui ne servent que de support mémoire.

De plus, le choix de la carte à puce dépend également du langage de programmation qui est utilisé, et en fonction de ce dernier, les capacités de la carte à puce peuvent être influencées [3]. En effet, dans notre cas, nous verrons dans la suite de l'article les raisons de l'utilisation d'un langage comme JavaCard.

## 2.2. Analyse des risques

La démarche que nous allons présentée dans cette analyse des risques possibles liés à l'utilisation de notre système. C'est pourquoi, nous allons détailler les points importants de notre analyse afin de justifier l'intégration de l'ensemble des mécanismes que nous avons évoqués ci-dessus. C'est pourquoi, nous allons présenté un scénario de base pour chacune des phases afin d'aboutir à une solution générale pouvant se prémunir des différentes attaques liées à son environnement.

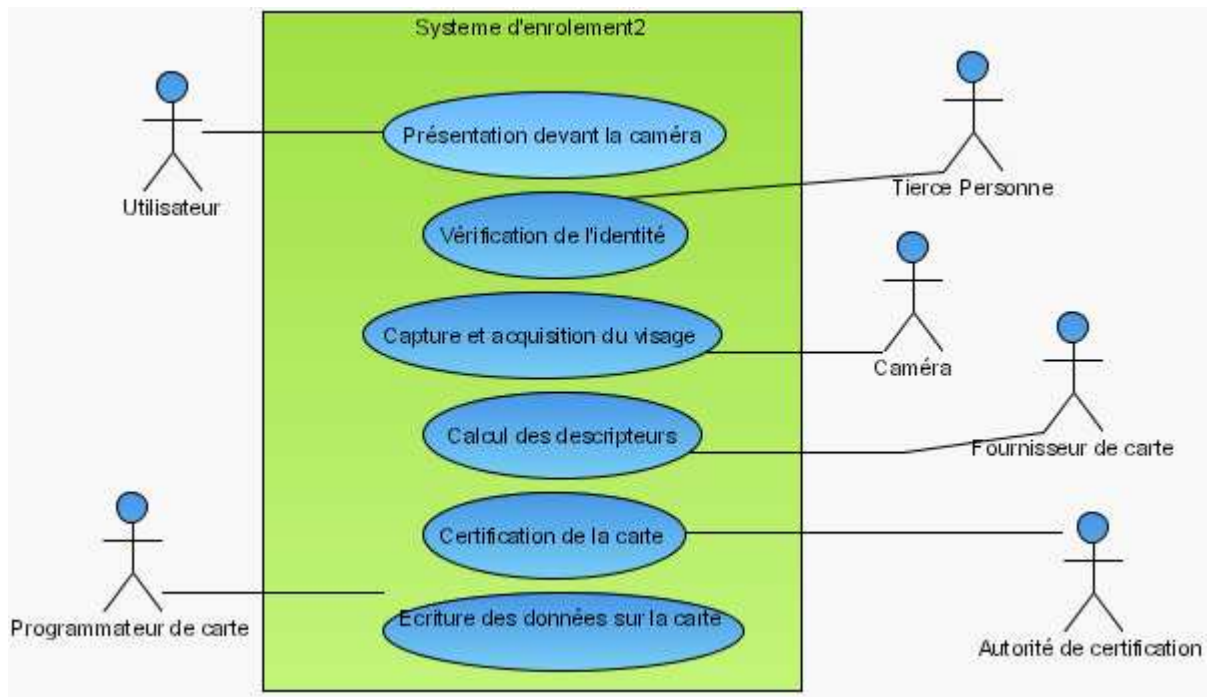
Le schéma ci-contre récapitule l'ensemble des étapes nécessaires à la réalisation des différentes étapes dans le processus biométrique [4].



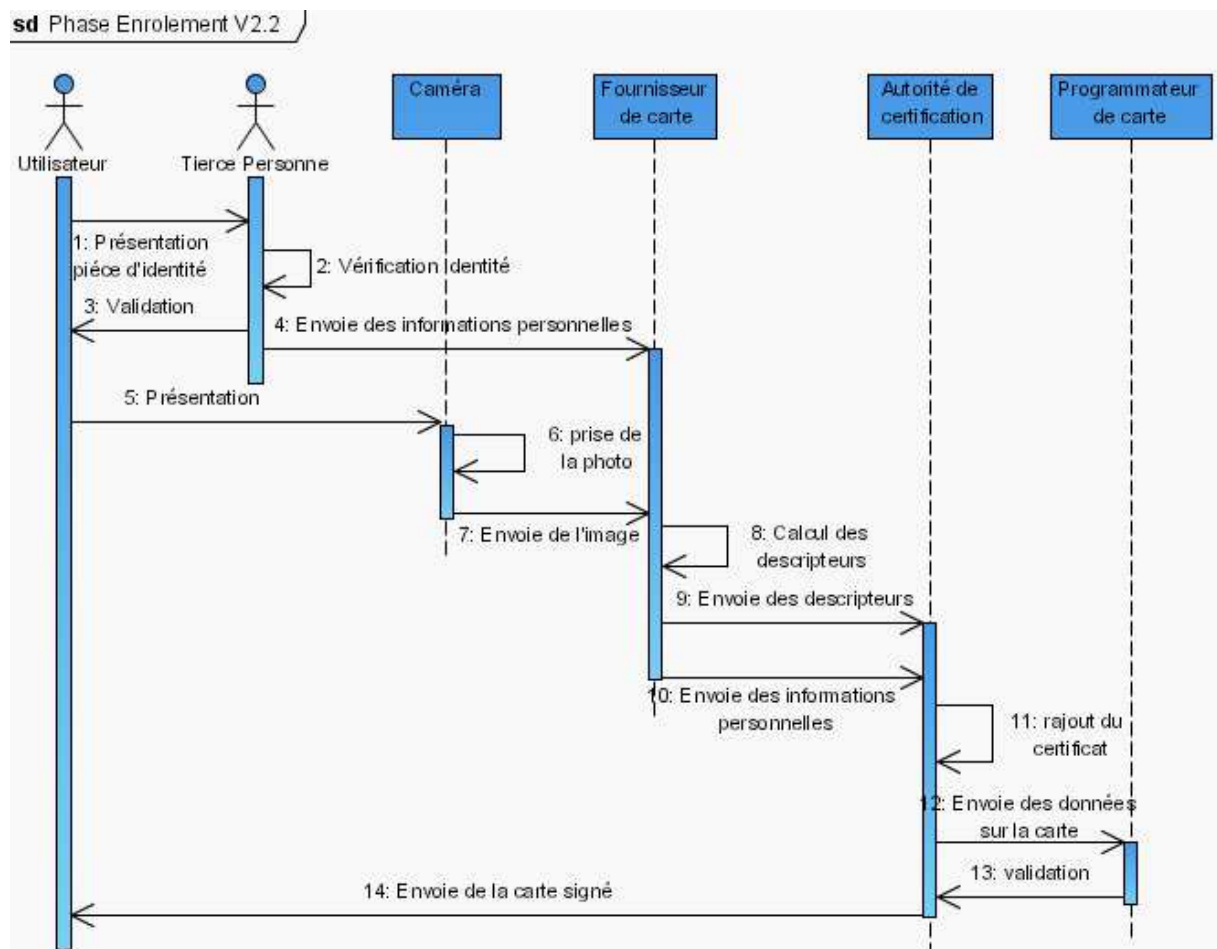
#### 2.2.1. Phase d'enrôlement

Nous allons dans un premier temps, donner les schémas correspondant au scénario obtenu, après nous expliquerons par la suite les raisons de ces choix.

Les acteurs présents dans le scénario retenu pour la phase d'enrôlement sont les suivants :



Le diagramme de séquence correspond à la solution retenue pour la phase d'enregistrement est donné ci-dessous :



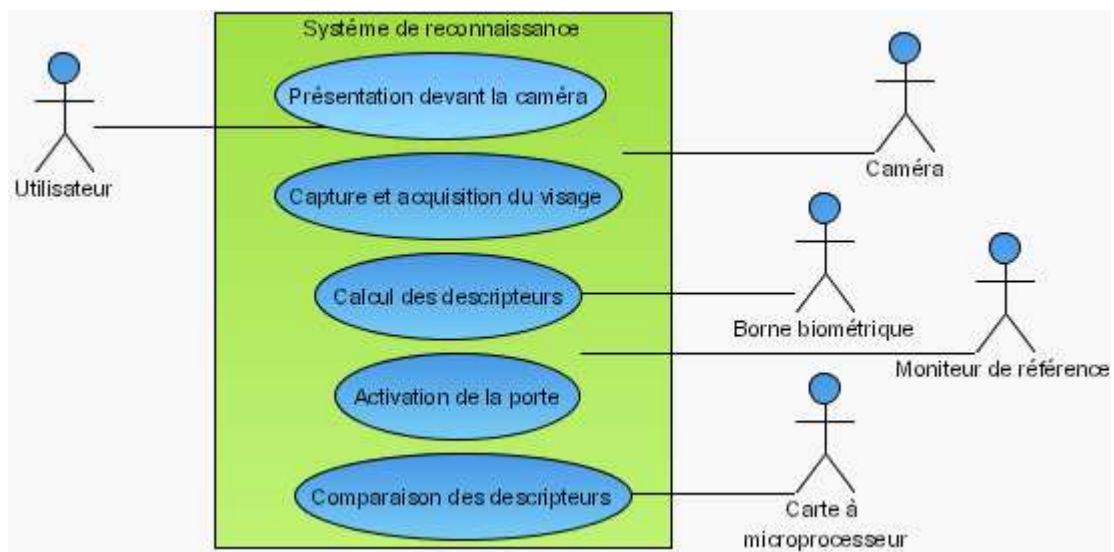
Le premier risque est de s'assurer de l'intégrité des informations transmises lors des échanges. En effet, le transport des données peut subir des altérations au niveau de l'envoi des

descripteurs et des images. C'est pourquoi, un système de vérification des données envoyées est mis en place, une somme de contrôle est réalisée avant l'envoi des fichiers, le résultat de cette somme est envoyé avec les données. A la réception, la somme est recalculée à partir des données reçues, puis est comparée avec la somme d'origine. Toutefois, sur le schéma ci-dessus cette vérification de l'intégrité des données n'est pas détaillée par souci d'allègement du schéma.

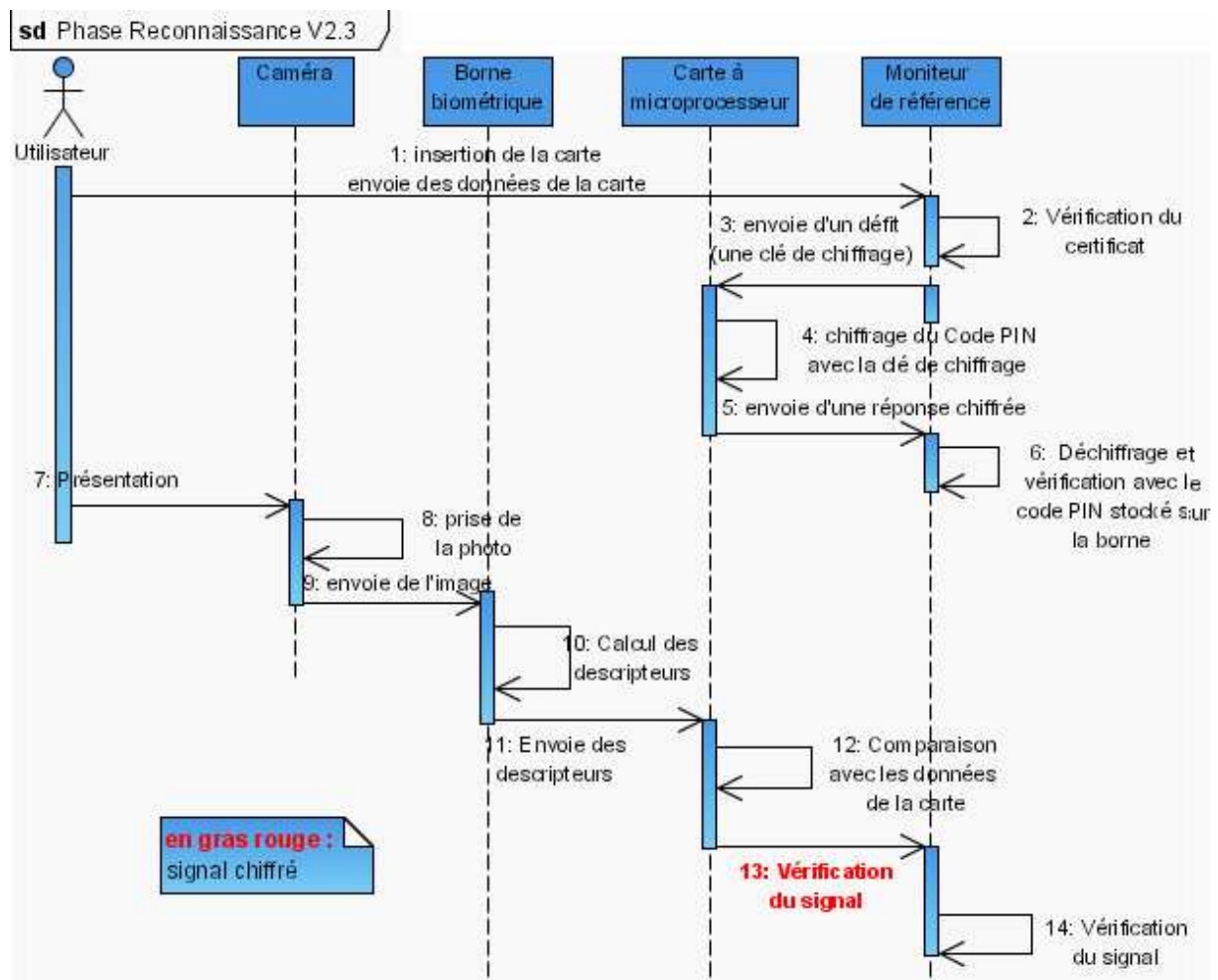
La personne de confiance peut être corrompue ou trompée par des méthodes de social engineering. Ainsi, pour éviter tout risque de piratage de la carte à puce et la création de sa propre carte, une autorité de certification pourrait apposer une signature sur la carte.

### 2.2.2. Phase de reconnaissance

Les acteurs présents dans le scénario retenu pour la phase de reconnaissance sont les suivants :



Le diagramme de séquence correspond à la solution retenue pour la phase d'enregistrement est donné ci-dessous :



Le moniteur de référence est chargé de la vérification de la validité du signal d'ouverture, ensuite si ce test de validité est réussi un signal d'ouverture est envoyé à la porte.

Afin d'éviter tout risque lié à l'utilisation de données personnelles et plus particulièrement les données biométriques, nous avons fait le choix de ne pas utiliser de base de données, les informations de chaque utilisateur seront stockées sur une carte à puce. A l'insertion de la carte, les données contenues dans la carte (descripteurs de l'individu et rôle) seront envoyées vers la borne biométrique. Ensuite, une comparaison aura lieu en local entre les données stockées sur la carte et celles calculées à partir de la photo.

Le problème de la fiabilité de la borne peut également se poser. En effet, la borne est accessible à tous les utilisateurs. Une personne peut donc tenter de pirater la borne de manière logicielle pour obtenir l'accès d'une salle protégée. Ce piratage pourrait se faire par un détournement des processus tournant sur la borne. Imaginons que la borne soit un simple ordinateur équipé d'un lecteur de carte, une personne pourrait essayer d'obtenir un accès physique pour manipuler la borne comme il le désire. Pour pallier au problème des failles de la borne, il existe une autre solution. Il suffirait d'effectuer le traitement des données sur la carte. La carte devrait donc être capable de gérer des processus de façon sécurisée.

Il existe un risque de falsification du signal d'ouverture de la porte. Ce risque porte sur deux transferts :

- l'ordre d'ouverture de la « JavaCard » à la borne biométrique
- le signal d'ouverture de la borne biométrique à la porte

Une solution à ce problème consiste à chiffrer les échanges via un canal sécurisé. Ce chiffrement pourra prendre en compte la date de demande d'accès comme paramètre afin d'éviter une duplication du signal crypté. Le signal de validation envoyé de la « JavaCard » à la borne sera chiffré, de même que l'ordre d'ouverture de la porte. Ensuite, il sera envoyé à un moniteur de référence inaccessible pour l'utilisateur (situé à l'intérieur de la zone sécurisée par exemple). Ensuite, le moniteur se chargera de déchiffrer l'information puis d'envoyer le signal électrique permettant l'ouverture à la porte.

Afin d'éviter tout risque d'usurpation de l'identité d'un individu en utilisant un masque ou une photo par exemples. Il serait possible de mettre en place deux caméras de manière à gérer l'aspect à trois dimensions et de mettre en place le traitement associé au niveau du calcul des descripteurs. De plus, une caméra pourrait prendre plusieurs photos de la personne afin d'augmenter la fiabilité du test et/ou d'introduire dans le processus d'identification, une gestion de l'authentification par une carte avec code PIN.

Une personne pourrait réussir à recréer un masque très fidèle au forme du visage d'une personne autorisée à entrer dans la zone « sécurisée » ou de faire une tête en cire de cette personne.

Un autre scénario possible et envisageable pourrait être de réaliser l'ensemble des traitements sur la carte à puce en incorporant par exemple sur cette dernière un capteur CCD et de réaliser l'ensemble des traitements cités ci-dessus sur cette carte.

### 3. Implémentation

#### 3.1.Kit de développement utilisé

Le kit de développement qui a été utilisé pour la réalisation de ce projet est celui proposé par la société Gemplus. En effet, le kit proposé nommé GemXpresso RAD III kit représente une solution complète pour le développement d'une telle application. En raison de sa facilité d'utilisation, il permet grâce à son simulateur de carte à puce de développer des applications d'une manière efficace et de réaliser des tests sur les applets à mettre en œuvre. De plus, il comprend tous les éléments nécessaires au développement d'un tel projet : lecteur de cartes à puces, cartes à puces javacard, documentation technique, exemples, et un environnement de développement complet. D'autre part, la communication avec la carte à puce est facilitée grâce à une interface graphique appelée « JCardManager ».

#### 3.2.Utilisation du langage JavaCard

Le langage Javacard est une API réduite du langage Java [5]. Ainsi, cette API reprend les caractéristiques générales du fonctionnement du langage Java. Toutefois, cette API ne supporte pas toutes les capacités de Java. En effet, les types primitifs sont limités à « byte », « short », et « boolean ». Le type « int » n'est supporté que dans des cas exceptionnels. De plus, les chaînes de caractères, les caractères, les tableaux à plusieurs dimensions, le chargement dynamique des classes, la sérialisation, le clonage d'objets, les threads, le garbage collector, et le chargement dynamique de classes ne sont pas supportés. L'absence de garbage collector peut provoquer une perte de mémoire car il n'existe pas non plus de désallocation explicite.

Cependant, certaines possibilités du langage Java sont supportées. En effet, la gestion des exceptions, l'appel au constructeur père, les différents mécanismes d'héritage, l'allocation dynamique dans l'EEPROM de la carte à puce, les tableaux unidimensionnels, les méthodes virtuelles, et la création d'applets ou cardlets sont possibles à l'aide de cette API.

Dans le développement d'une application avec une carte à puce Javacard, cette dernière doit avoir une configuration minimale afin de profiter pleinement de cette API. Ainsi, la

configuration requise selon SUN dans le livre « JavaCard Technology for Smart Cards » est de 1 Ko de RAM, 16 Ko EEPROM, et 24 Ko ROM [6].

Il est vrai que l'utilisation de cette API est coûteuse en espace mémoire pour le stockage des applets. Elle présente également les mêmes inconvénients qu'un langage interprété. Cependant, le principal avantage de l'utilisation de cette extension du langage Java réside dans le fait de l'intégration des différents mécanismes permettant d'assurer une sécurité optimale de l'application développée (paquetages spécialement dédiés à ces actions). De plus, il s'agit d'un langage standardisé. Elle permet également une certaine coexistence avec des applications différentes, et une modification dynamique des applications pendant la phase de vie de la carte avec un environnement très ouvert.

### 3.3. Calcul des descripteurs

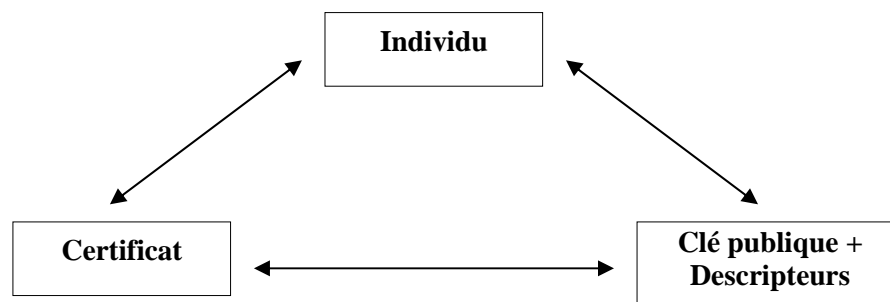
L'implémentation des descripteurs est réalisée à l'aide du langage Java via l'appel d'une DLL. Cette dernière, interfacée via la librairie 'JNI', permet le calcul des moments de Zernike à partir d'une image en niveaux de gris. De ces moments, seront extraits les descripteurs recherchés.

La précision des descripteurs est un facteur primordial pour permettre l'obtention d'un taux de reconnaissance optimal. Ainsi, ils seront stockés sous la forme de variables en virgule flottante. De plus, pour pouvoir être utilisés sur une JavaCard, une conversion sous la forme d'une suite de variables 'short' est nécessaire.

Ensuite, deux méthodes peuvent être utilisées pour réaliser une comparaison entre les descripteurs trouvés et ceux stockés sur la carte à puce. Une méthode simple consiste à comparer les descripteurs un à un avec un seuil de tolérance et l'autre consiste à utiliser une technologie avancée comme les SVM (Support Vecteur Machine).

## 4. Apports et limites de notre solution

L'avantage principal de notre solution est de se fonder sur le concept de « certificat biométrique ». Là où les certificats numériques établissent simplement une correspondance certaine entre une clé publique et un individu, notre concept, en utilisant trois acteurs, permet ainsi de s'assurer directement de l'identité de la personne. Le principe mis en œuvre est récapitulé dans le schéma suivant :



Le deuxième apport de notre solution est de s'intégrer aux conventions éthiques en vigueur en France (cf page 3). En effet, l'utilisation de la carte à puce nous permet de contourner l'usage de bases de données, vivement critiqué par les organismes de protection des libertés personnelles.

De plus, notre solution ne sera pas confrontée aux mêmes problèmes que ceux rencontrés pour la carte d'identité numérique. En effet, cette dernière procède en plus de la création de la carte à un système de fichage systématique des personnes la possédant.

Cependant, quelques critiques peuvent être apportées à notre système. Tout d'abord, au niveau de l'utilisation pratique, la présence de carte présente l'inconvénient de ne pas être applicable dans le domaine de l'authentification en lieu public. Notre système ne permet pas actuellement d'être applicable dans le cadre d'opérations policières.

De plus, nous avons étudié l'ensemble de la solution afin d'apporter une sécurité optimale. Dans des utilisations fréquentes et peu sujettes à risques, le recours au code PIN de manière systématique, et à l'introduction de la carte à puce dans le lecteur, peut s'avérer lourd dans la pratique. Nous pourrions éventuellement améliorer notre solution en imaginant une possibilité de désactiver la saisie du code PIN afin d'accélérer le processus de contrôle.

## 5. Conclusion

Cet article propose d'utiliser la technologie des cartes à puces pour répondre à l'un des soucis récents, mais majeur, engendré par les nouvelles technologies de l'information et la communication : le respect de la vie privée, et la protection de l'individu. Dans ce cadre, il analyse le problème de contrôle d'accès, identifie et étudie un certain nombre de scénarios représentatifs, et présente une démarche d'analyse mettant en correspondance des fonctionnalités de reconnaissance faciale adéquates. Enfin, il propose des procédures génériques, flexibles et adaptées aux besoins, objectifs et exigences de protection de la vie privée. La solution proposée est implémentée à travers un scénario complet et générique allant de l'enregistrement des données à la phase de reconnaissance. Nous avons utilisé le langage JavaCard pour l'implémentation de nos procédures sur les cartes à puces. De plus, la combinaison de plusieurs mécanismes de sécurité afin d'établir le lien entre une personne physique, une clé publique, et un certificat.

## 6. Références

- [1 ] Interview de C. von der Malsburg publiée en Avril 2003 sur le Siemens Webzine  
[http://w4.siemens.de/FuI/en/archiv/pof/heft1\\_03/artikel14/](http://w4.siemens.de/FuI/en/archiv/pof/heft1_03/artikel14/)
- [2] Position de la CNIL au sujet des données biométriques,  
<http://www.cnil.fr/index.php?id=1304>
- [3] Christian Tavernier, « *Les cartes à puce* », Edition DUNOD, 2002, 255 pages
- [4] Site Web consacré à la biométrie, <http://www.biometrie.online.fr>
- [5] J-Jacques Vandewalle, Gemplus Research Group, « *Construction d'applications avec la carte à puce* »
- [6] Zhiqun Chen, « *Java Card Technology for Smart Cards* », 2004, 359 pages