NOSCIFEL : authentification forte des acteurs

SOMMAIRE

1. Présentation du RGS

Les abréviations utilisées

- Politique de Certification (PC)
- Déclaration des Pratiques de Certification (DPC)
- Prestataire de certification électronique (P.S.C.E.) : Personne ou entité responsable de la gestion de certificats électroniques tout au long de leur cycle de vie. Un P.S.C.E. comporte au moins une A.C.
- Conditions Générales d'Usage (CGU)
- Autorité de Certification (AC)
- Autorité d'Enregistrement (AE)
- Opérateur de Certification (OC)
- Infrastructure de Gestion de Clés (IGC / PKI) pour délivrer les certificats qui seront insérés dans les cartes à puces et qui permettront d'identifier le propriétaire
- Responsable Légal (RL)
- Mandataire de Certification (MC)

Au fait, c’est quoi le RGS

- Le Référentiel général de sécurité (RGS) a été créé par l’article 9 de l’ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives. Ses conditions d’élaboration, d’approbation, de modification et de publication sont fixées par le décret n° 2010-112 du 2 février 2010 pris pour l’application des articles 9, 10 et 12 de l’ordonnance citée relatif à la sécurité des informations échangées par voie électronique

- Nous sommes actuellement dans la version RGS 1.0, composée du document RGS lui-même et de 14 documents annexes fournissant différent modèles pour les documents essentiels au dossier à construire pour se faire qualifier

RGS – cadre juridique

2005 (France) : Ordonnance n°2005-1516 du 8 décembre 2005, relative aux échanges [...] entre les autorités administratives

- Texte fédérateur relatif aux métiers de la dématérialisation dans la sphère publique rédigé par l'ADAE (maintenant SGMAP) et définissant la notion de « téléservice »
- Définit les principes de RGS (Référentiel Général de Sécurité) et RGI (Référentiel Général d'Interopérabilité)
- « Annule et remplace » les termes « LRAR » par « signature électronique » par exemple
- Promulgue positivement les effets de la signature électronique dans TOUS les échanges administratifs

2010 (France) : Décret n° 2010-112 du 2 février 2010, dit décret RGS (Référentiel Général de Sécurité)

- Définit les règles et exigences de sécurité, qui s'appliquent aux autorités administratives, et aux systèmes d'information qui communiquent avec elle, selon plusieurs niveaux de « force sécuritaire » : une, deux ou trois étoiles (*, **, ***)
- Définit un ensemble de règles de sécurité pour la gestion de la sécurité de l'information
- Référence un ensemble de documents annexes définissant la marche à suivre pour émettre des certificats suivant :
  - Le type : Particulier, Entreprise, Administration, Serveur
  - Le service : Authentification, Signature, Confidentialité, Horodatage
  - Le niveau : *, **, ***

Exigences relatives au RGS (pour les ACs)

Le RGS, pour les certificats de niveau *, **, *, impose une série d'exigences, décrites dans les Politiques de Certification Type.**

Ces exigences couvrent de nombreux aspects, notamment :

Processus de gestion des certificats (délivrance, révocation, renouvellement) :
Niveau de sécurité physique et logique des infrastructures techniques ;
Niveau d'engagement juridique de l'Autorité de Certification vis à vis des porteurs, de tiers ;
Traçabilité des opérations effectuées par tous les participants au sein de la chaine de confiance ;
Continuité du service, et plan de reprise en cas d'incident ;
Niveau de disponibilité des infrastructures ;
Gestion des habilitations des personnels faisant partie de la chaîne de confiance ;
Archivage de toutes les pièces permettant de reconstituer le cycle de vie des certificats émis (formulaires d'enregistrement, validations internes, certificats, CRLs...) ;
Engagements en matière de qualité de service (sur tous les aspects liés à la gestion des certificats, et pas seulement sur le niveau de disponibilité des serveurs).

L'obtention d'un label *, **, ***, pour une Autorité de Certification, est conditionnée par :

Un audit de qualification initial (conditions de sécurité), se déroulant en deux phases :
- Audit documentaire ;
- Audit opérationnel.

La vérification des gabarits des certificats effectuée à l'issue de l'audit (conditions d'interopérabilité)
Un audit annuel permettant de vérifier que les pratiques décrites, et auditées initialement, sont effectivement mises en œuvre par l'ensemble des participants à la chaîne de confiance.

Exigences RGS structurantes pour les certificats*

Fonctions	*	**	***
Organisation de l'AC	Analyse de risques recommandée	Analyse de risques obligatoire	Analyse de risques obligatoire
Utilisation des certificats	Applications « moyennement critique »	Applications « fortement critique »	Applications « très fortement critique »
Contrôle d'accès pour la modification des informations publiées (PC / CRL...)	Nom et mot de passe	Nom et mot de passe, sauf pour les CRLs (deux facteurs)	Contrôle d'accès fort à deux facteurs pour toutes les informations publiées
Enregistrement du porteur	Process papier ou électronique à distance	Face à face, ou signature électronique des pièces (avec un certificat **)	Face à face obligatoire
Renouvellement du certificat**	Renouvellement automatique possible	Renouvellement automatique possible, mais limité à 1 renouvellement	Renouvellement automatique possible, mais limité à 1 renouvellement
Demande de révocation	Authentification moyennement forte du demandeur (1-2 questions réponses téléphoniques)	Authentification assez forte du demandeur (3-4 questions réponses téléphoniques)	Authentification forte du demandeur (4-5 questions réponses téléphoniques)
Remise du certificat	Possible par message électronique	En main propre si le face à face n'a pas encore eu lieu. En s'assurant que le porteur destinataire est bien celui pour lequel une demande de certificat a été faite	
Support du certificat	Pas d'exigence sur le support (certificat logiciel possible)	Sur support physique	Sur le support physique identifié pour ce porteur

Exigences RGS structurantes pour les certificats*

Fonctions	*	**	***
Acceptation du certificat	Tacite	Demande de confirmation demandée au porteur, et trace conservée par l'AC	Confirmation par accord signé (papier ou électronique)
Mesures de sécurité : accès physique	Locaux sécurisés Personnels tracés	L'accès doit être strictement limité aux seules personnes nominativement autorisées	Idem ** + le matériel de l'AC doit être situé dans un périmètre dédié
Sauvegardes hors site	Recommandées	Obligatoires	Obligatoires
Rôles de confiance	Séparation des rôles, et interdiction de cumul « responsable de sécurité et ingénieur système »	Idem * + interdiction de cumul « contrôleur et tout autre rôle, responsable de sécurité et opérateur, ingénieur système et opérateur »	
Cérémonie des clés	Au moins 1 personne ayant un rôle de confiance	Plusieurs personnes de confiance et témoins, dont au moins 1 externe	Deux personnes de confiance, un huissier ou notaire, et manipulation des secrets dans un « environnement protégé »
Gestion des clés de l'AC	Personnel de confiance	Séparation des secrets (k sur n)	
Activation des clés d'AC	1 personne	2 personnes minimum	
Matériel du porteur	Pas d'exigence	SSCD qualifié standard	SSCD qualifié renforcé
Matériel de l'AC (HSM)	Qualifié au niveau élémentaire	Qualifié au niveau standard	Qualifié au niveau renforcé

Exigences en matière de "variable de temps" (1/3)

Objet	*	**	***
Fréquence de contrôle de conformité de l'ensemble de l'IGC	1 fois tous les 3 ans	1 fois tous les 2 ans	1 fois par an
Fréquence d'analyse complète des journaux d'évènements	1 fois toutes les 2 semaines et dès la détection d'une anomalie	1 fois par semaine et dès la détection d'une anomalie	1 fois par jour ouvré et dès la détection d'une anomalie
Fréquence de contrôle des journaux d'évènements pour identification des tentatives en échec d'accès ou d'opération	1 fois par jour ouvré		
Fréquence de rapprochement des journaux d'évènements	1 fois par mois		1 fois par semaine
Fréquence minimale de publication des LCR (et Delta)	72h	24h	
Fréquence de test du plan de continuité	1 fois tous les 3 ans	1 fois tous les 2 ans	1 fois par an
Disponibilité des systèmes publiant les certificats d'AC	24/24 7j/7		
Durée de rétention des archives	5 ans		
Durée de vie maximale d'un certificat d'AC	10 ans		
Délai minimum d'information en cas de cessation d'activité programmée	1 mois		

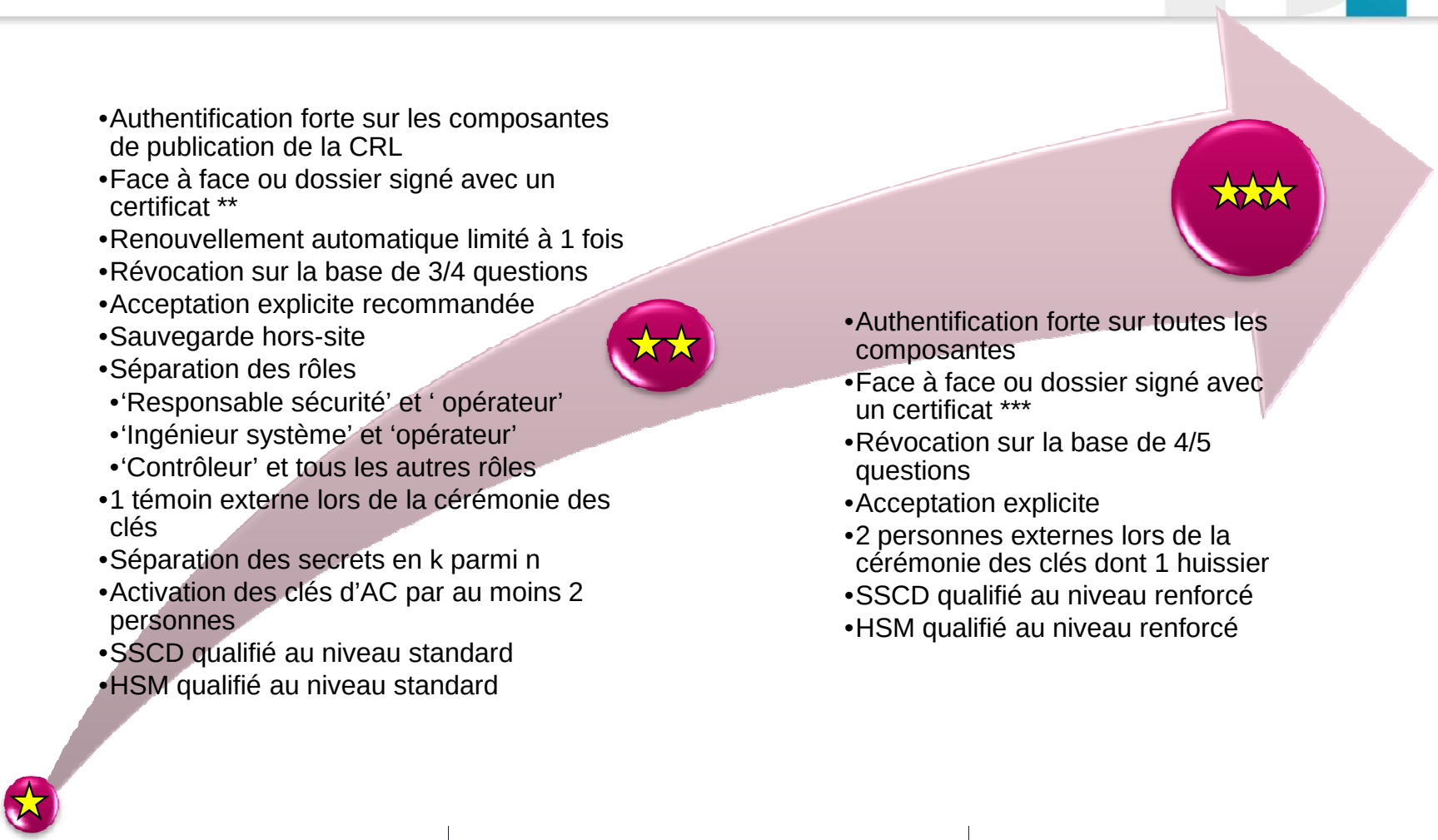
Exigences en matière de "variable de temps" (2/3)

Objet	*	**	***
Disponibilité de la fonction d'information sur l'état des certificats	24 h / 24 - 7j / 7		
Durée maximale d'indisponibilité par interruption (panne ou maintenance) de la fonction d'information sur l'état des certificats	4 h (jours ouvrés)	4 h	2 h
Durée maximale totale d'indisponibilité par mois de la fonction d'information sur l'état des certificats	32h (jours ouvrés)	16h	8 h
Disponibilité de la fonction de publication des informations (hors informations d'état des certificats)	Jours ouvrés		
Délai de conservation des journaux d'évènements sur site et de mise en archive	1 mois		
Durée de vie maximale d'une bi-clé et d'un certificat porteur : •Particulier •Agent •Entreprise Serveur / cachet	 5 ans 3 ans 3 ans 3 ans		
Délai maximum de publication d'une LCR suite à sa génération	30 min		
Délai maximum de récupération des archives	2 jours ouvrés		
Disponibilité de la fonction de gestion des révocations	Heures ouvrées	24 h / 24 - 7j / 7	

Exigences en matière de "variable de temps" (3/3)

Objet	*	**	***
Durée maximale d'indisponibilité par interruption (panne ou maintenance) de la fonction de gestion des révocations	2h (jours ouvrées)	2 h	1 h
Durée maximale totale d'indisponibilité par mois de la fonction de gestion des révocations	16h (jours ouvrées)	8 h	4 h
Délai maximum de traitement d'une demande de révocation	72 h	24 h	
Temps de réponse maximum du serveur à une requête reçue portant sur l'état d'un certificat	10 sec		

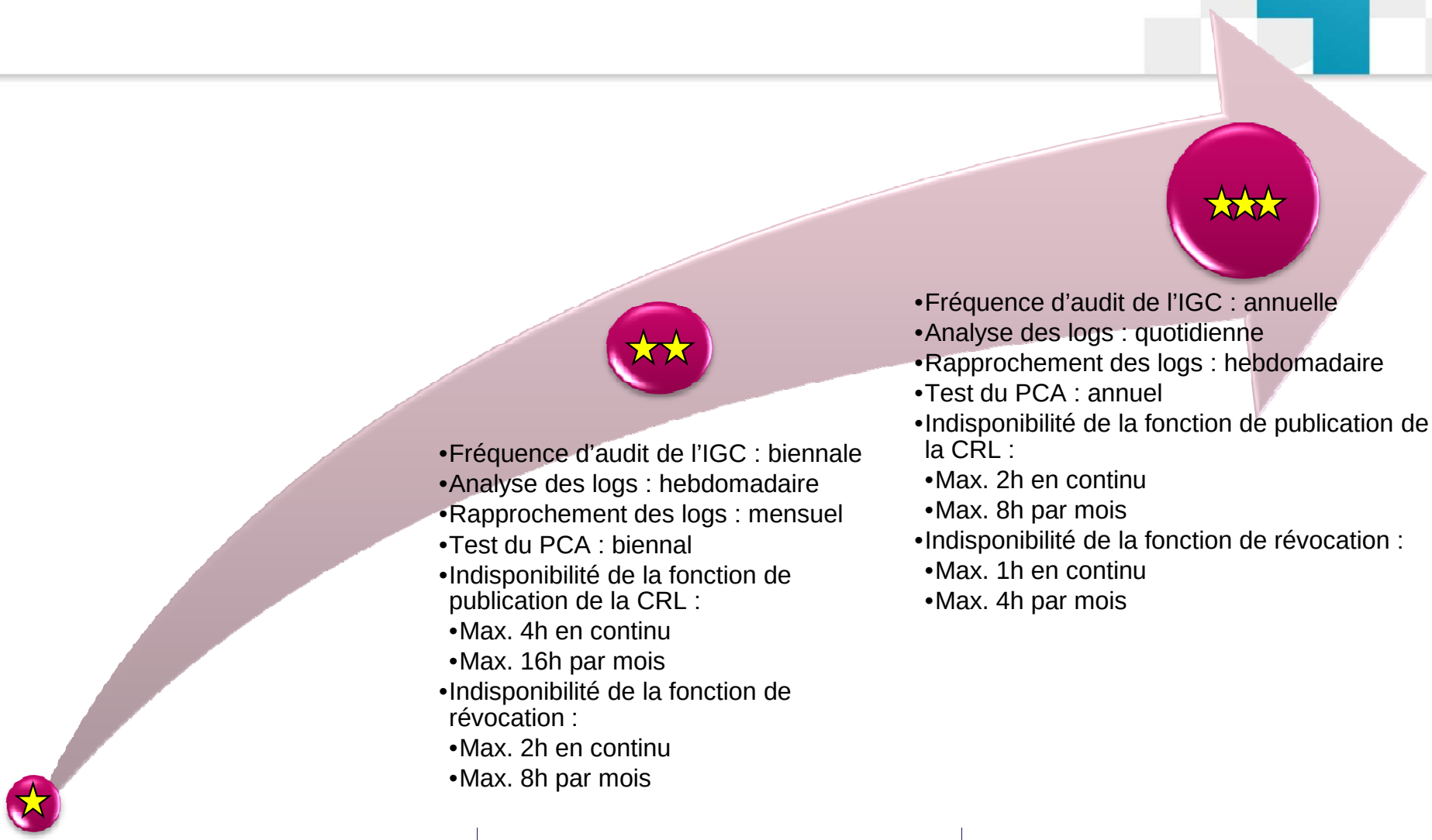
Passage du niveau * au niveau *** (1/2)



- Authentification forte sur les composantes de publication de la CRL
- Face à face ou dossier signé avec un certificat **
- Renouvellement automatique limité à 1 fois
- Révocation sur la base de 3/4 questions
- Acceptation explicite recommandée
- Sauvegarde hors-site
- Séparation des rôles
  - ‘Responsable sécurité’ et ‘ opérateur’
  - ‘Ingénieur système’ et ‘opérateur’
  - ‘Contrôleur’ et tous les autres rôles
- 1 témoin externe lors de la cérémonie des clés
- Séparation des secrets en k parmi n
- Activation des clés d’AC par au moins 2 personnes
- SSCD qualifié au niveau standard
- HSM qualifié au niveau standard

- Authentification forte sur toutes les composantes
- Face à face ou dossier signé avec un certificat ***
- Révocation sur la base de 4/5 questions
- Acceptation explicite
- 2 personnes externes lors de la cérémonie des clés dont 1 huissier
- SSCD qualifié au niveau renforcé
- HSM qualifié au niveau renforcé

Passage du niveau * au niveau *** (2/2)



- Fréquence d'audit de l'IGC : biennale
- Analyse des logs : hebdomadaire
- Rapprochement des logs : mensuel
- Test du PCA : biennal
- Indisponibilité de la fonction de publication de la CRL :
  - Max. 4h en continu
  - Max. 16h par mois
- Indisponibilité de la fonction de révocation :
  - Max. 2h en continu
  - Max. 8h par mois

- Fréquence d'audit de l'IGC : annuelle
- Analyse des logs : quotidienne
- Rapprochement des logs : hebdomadaire
- Test du PCA : annuel
- Indisponibilité de la fonction de publication de la CRL :
  - Max. 2h en continu
  - Max. 8h par mois
- Indisponibilité de la fonction de révocation :
  - Max. 1h en continu
  - Max. 4h par mois

Comment est-on qualifié RGS ?

- On met en œuvre une infrastructure technique pour délivrer des certificats électroniques qui vont servir à sécuriser les échanges soit entre usagers et administrations, soit entre administrations
- On définit les politiques que l'on souhaite appliquer pour la délivrance des certificats
- En parallèle de l'infrastructure technique, on met en place des procédures de demande, de contrôle, de délivrance, de suivi du cycle de vie des certificats, et des procédures d'exploitation et de supervision des systèmes informatiques. Dans ces procédures, des acteurs se voient affecter des rôles
- On construit un référentiel documentaire à partir des politiques que l'on souhaite mettre en œuvre et des procédures, et on fait qualifier le tout, politiques, procédures et systèmes informatiques par un auditeur accrédité

Actuellement l'Imprimerie Nationale est en cours de qualification RGS et RGS****

2. Niveau de fiabilité choisi pour le projet NOSCIFEL

Le niveau de « fiabilité » attendu dépend du niveau de risque pris lors de la contractualisation…

Au travers de ces différents textes, la législation française et le cadre européen distinguent trois niveaux de validité juridique différents : (Cf livrable 1.6.1)

- la « signature électronique » ou « signature simple » (pas de moyen spécifique prédéterminé, en pratique un scellement technique est au moins nécessaire pour garantir l'intégrité de la transaction),
- La « signature sécurisée » (**),
- la « signature électronique présumée fiable » (***)

Selon le niveau de garantie souhaité par le client, les certificats RGS sont classés RGS*, RGS** et RGS***, avec des procédures de plus en plus sécurisées pour garantir l'identité du porteur de certificat.

Consciente de la sensibilité des données commerciales échangées dans le cadre du projet Noscifel et pour couvrir les risques d'usurpation d'identité, de falsification, de répudiations identifiées, le niveau de sécurité et de signature ne peut être simple.

Le haut niveau de garantie adapté au projet Noscifel que CHS va mettre en place dans son démonstrateur est le RGS **.

Carte d'identité électronique professionnelle RGS **

Véritable carte d'identité électronique professionnelle certifiée par un tiers de confiance, l'Imprimerie Nationale (en cours de qualification au RGS**) va, dans le cadre du projet Noscifel, distribuer sur cartes à puces des certificats permettant une authentification forte et la signature de document.

Ce certificat permet 2 utilisations :

Authentification : Ce certificat permet de remplacer le login/mot de passe afin de sécuriser vos accès à des serveurs professionnels, à des sites de téléprocédures, à des plateformes de dématérialisation ou encore à votre PC.

Signature : Ce certificat permet également à son titulaire de prouver son identité et de signer électroniquement dans le cadre de son activité professionnelle. La signature électronique utilisée avec ce certificat est sécurisée et présumée fiable. La charge de la preuve de l'absence de fiabilité du procédé repose alors sur celui qui conteste la valeur juridique de la signature.

Pass'IN est l'offre innovante de l'IN, construite en partenariat avec les meilleurs solutions du marché (Sopra, Dictao et OpenTrust).

Comment commander un certificat

1. Constitution du dossier de demande de carte

Véritable pièce d'identité professionnelle, il est nécessaire pour constituer le dossier d'avoir des éléments pour connaitre :

- l'identité du titulaire du certificat et de la délégation de pouvoir vis-à-vis de son organisme professionnel
- l'identité de l'organisme professionnel

2. Face à face

Les certificats RGS** font obligatoirement l'objet d'un rendez vous, de réception et de contrôle de toutes les pièces obligatoires pour la constitution du dossier de l'organisme professionnel, conformément au Référentiel Général de Sécurité. Le responsable légal (RL) de l'entreprise devra désigner un mandataire de certification (MC) qui réalisera le face le face.

AE
(Agent Clientèle de l'Imprimerie Nationale)

RL et MC
(Entité Cliente)

3. Création de la demande de carte, création et envoie de la carte…

4. Archivage du dossier de demande..

Détaillé dans le chapitre suivant

Dossier de demande de carte : Pièces à fournir

1. Identité du titulaire et délégation

Formulaire de demande de certificat RGS
Formulaire Désignation du MC et Engagements du MC annexe du contrat
Copie des CGU signé par le porteur et l'AE et ou RL/MC
Copie de la pièce d'identité du porteur (CNI, Passeport, carte de séjour) signée par porteur et l'AE e ou RL/MC « copie certifiée conforme à l'original ».
PV de face à face signé par le MC et l'AE.

2. Identification de l'organisation professionnelle

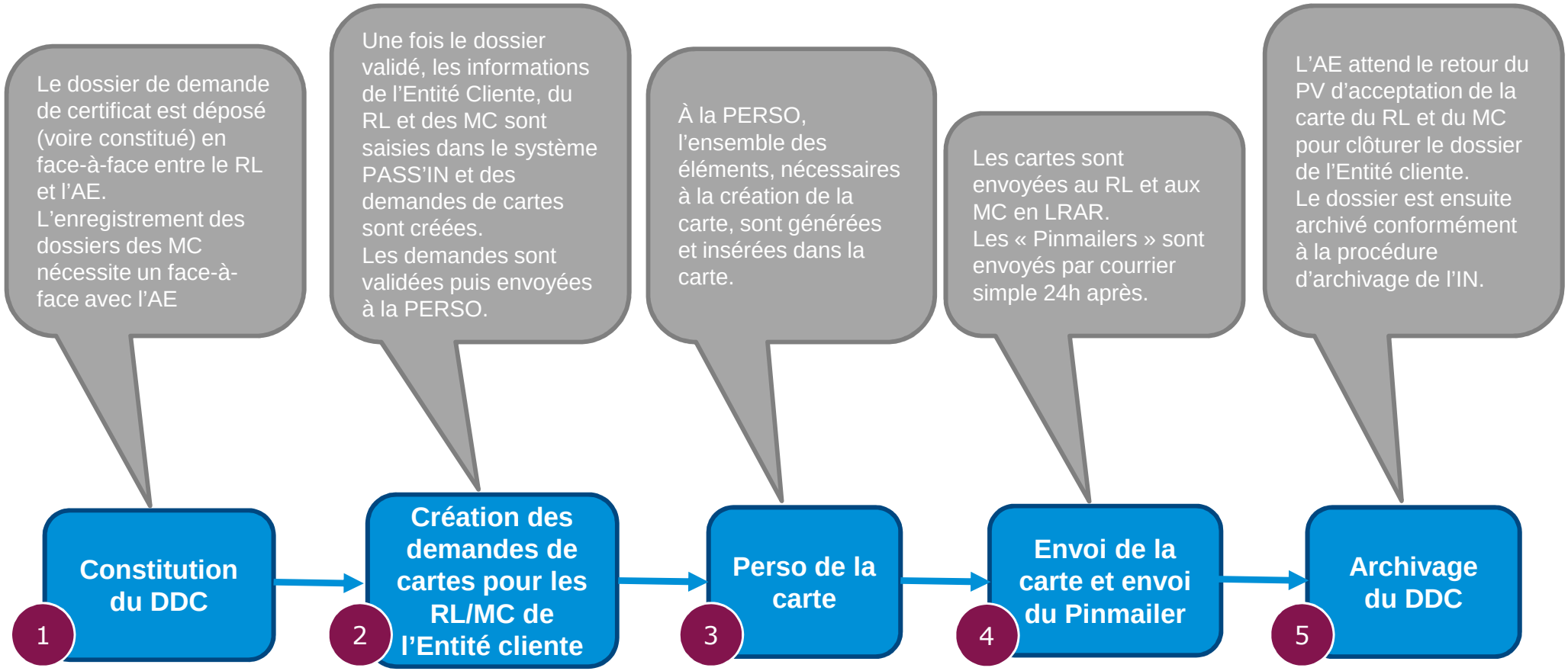
Extrait K-bis de moins de 3 mois (si entreprise)
Un avis de situation juridique de l'INSEE (avis SIRENE) pour une administration.
Une pièce, valide au moment de l'enregistrement, portant délégation ou subdélégation de l'autorité responsable de la structure administrative. les éventuelles délibérations, décrets et/ou arrêtés de nomination, désignation concernant l'autorité administrative)

3. Présentation de la solution PASS'IN de CHS pour le projet NOSCIFEL

Processus d’une demande de carte RL/MC

Processus de demande de carte

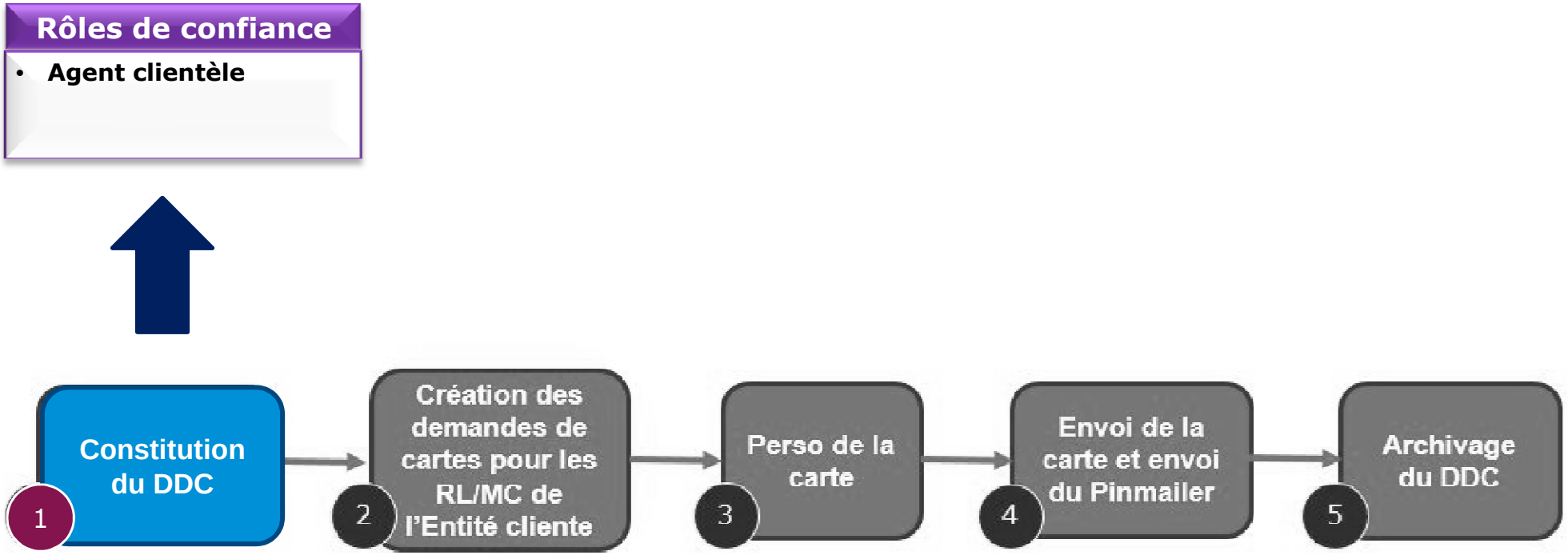
Processus global pour un RL/MC(1/2)



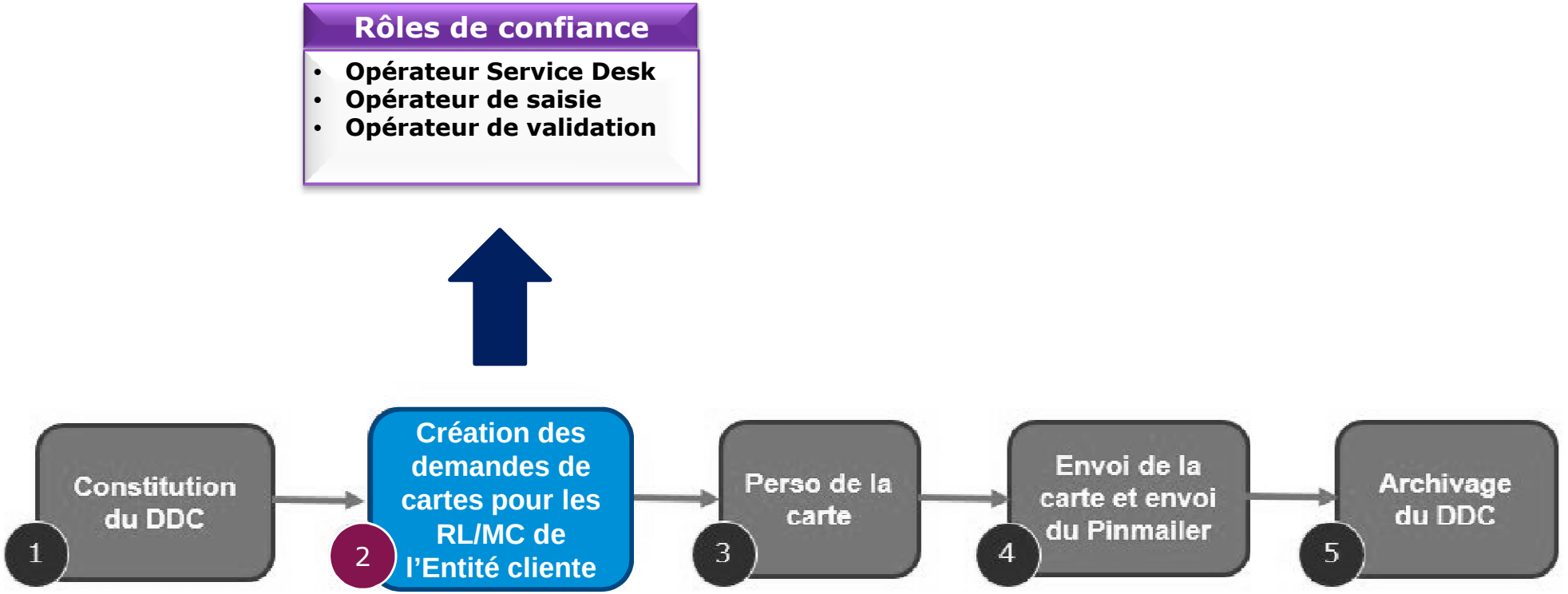
Processus de demande de carte
Processus global pour un RL/MC (1/5)

Rôles de confiance

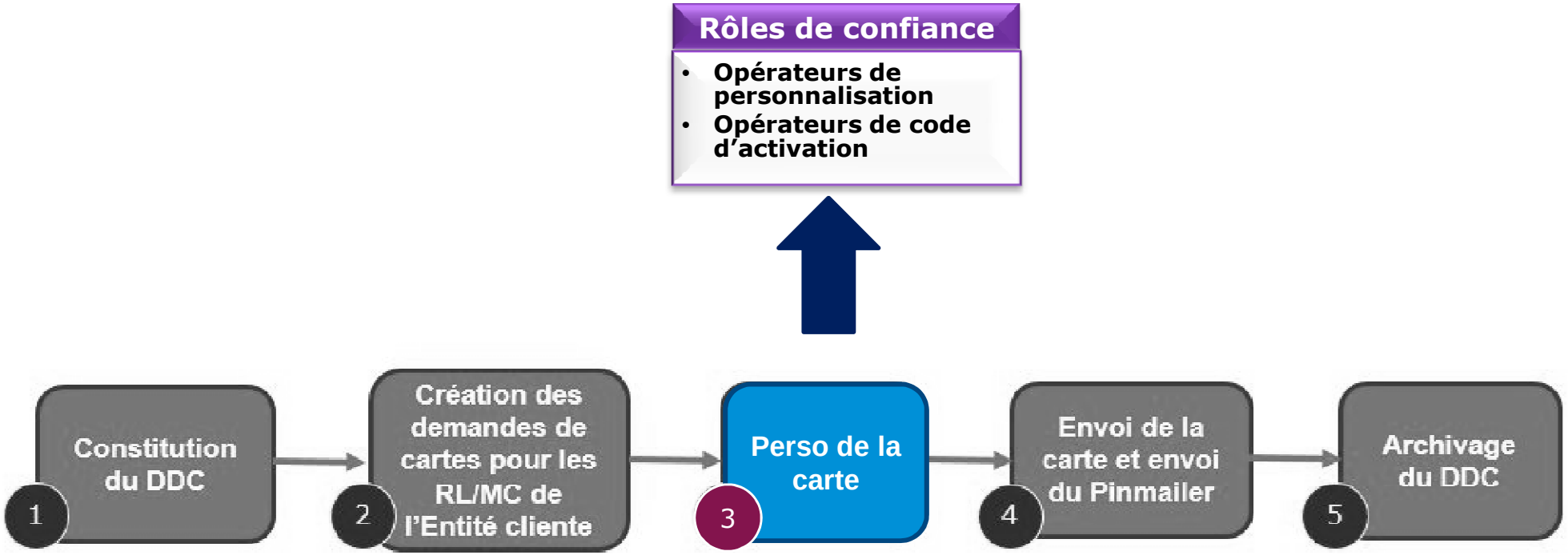
- **Agent clientèle**



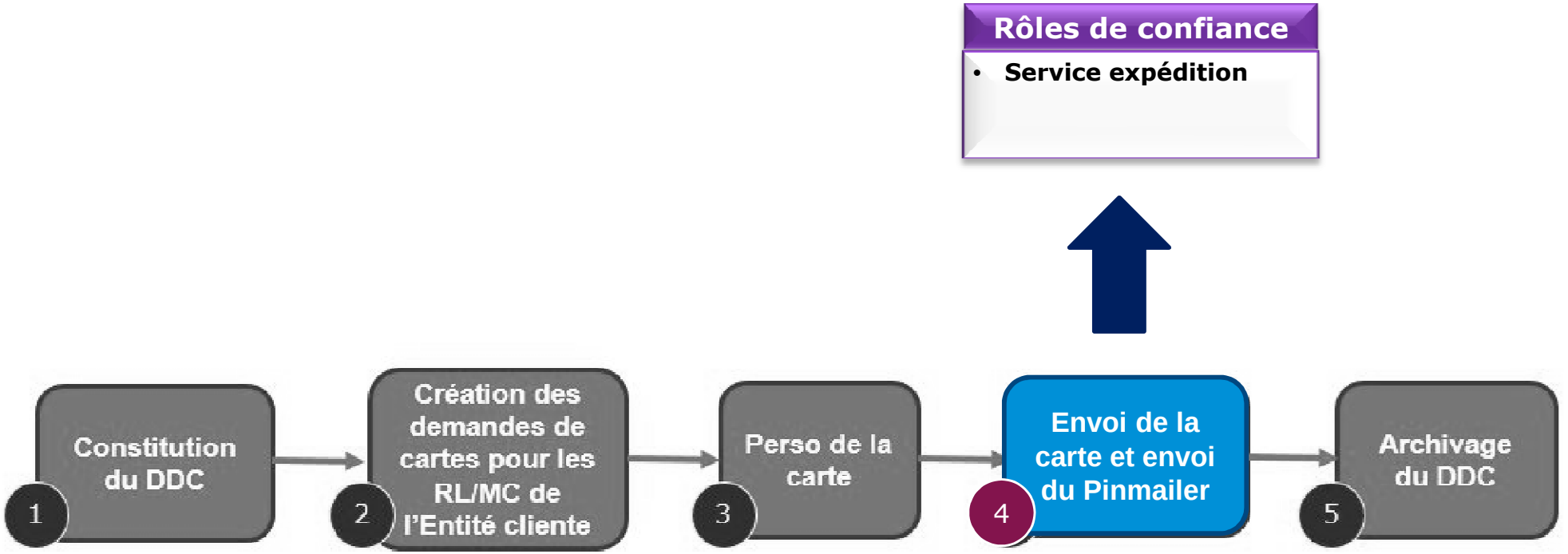
Processus de demande de carte
Processus global pour un RL/MC (2/5)



Processus de demande de carte
Processus global pour un RL/MC (3/5)



Processus de demande de carte
Processus global pour un RL/MC (4/5)

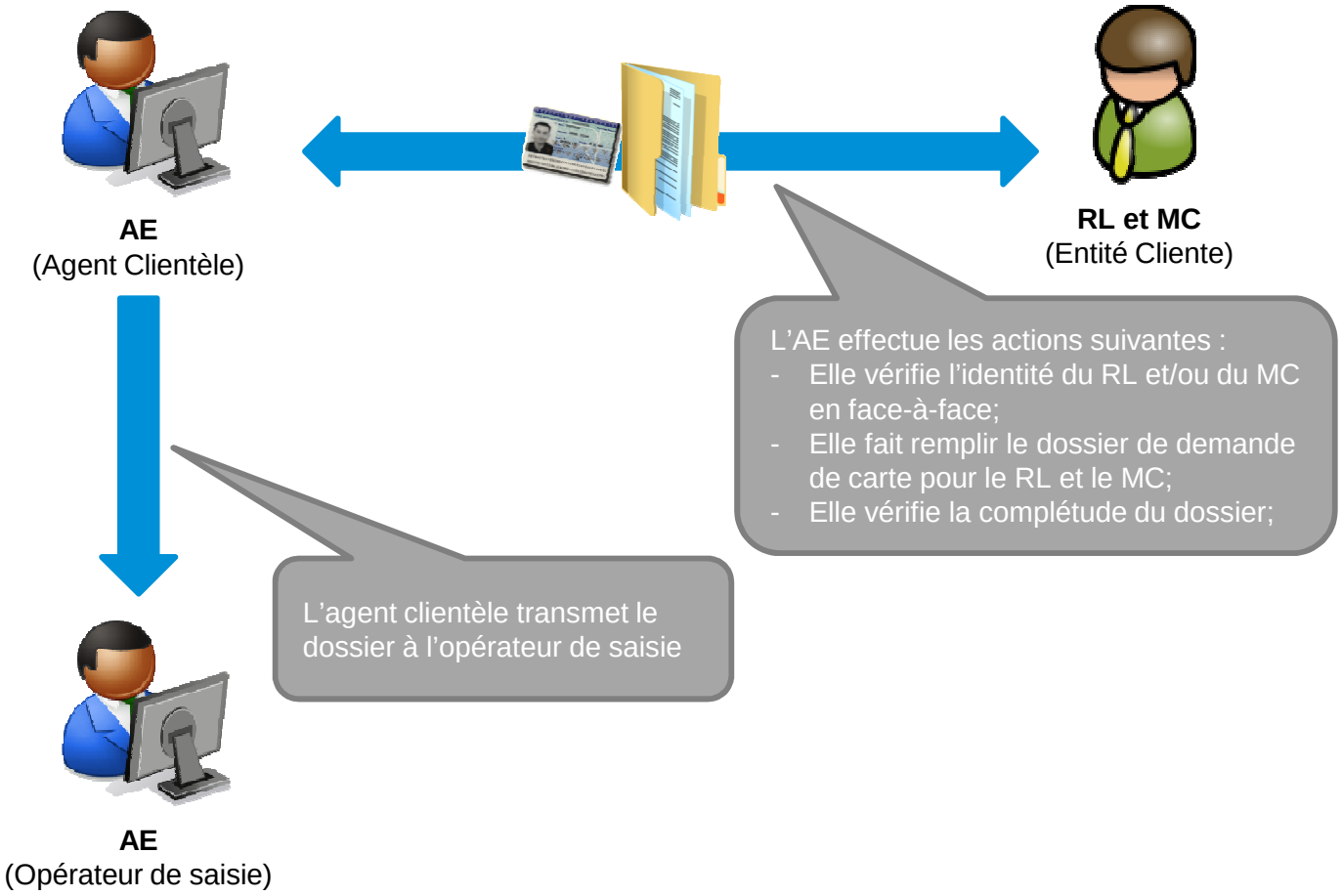


Processus de demande de carte
Processus global pour un RL/MC (5/5)

Rôles de confiance

- **Opérateur de saisie**
- **Opérateur de validation**

Processus de demande de carte
Constitution du dossier Entité cliente



Processus de demande de carte
Enregistrement de l'Entité cliente et des RL/MC

Les informations du dossier nécessaires à la création de l'organisation sont transmises à l'Opérateur Service Desk de l'AC :
- Nom de l'organisation
- N° SIRET de l'organisation
- Prénom/Nom et @email du RL
- Prénom/Nom du et @email du MC

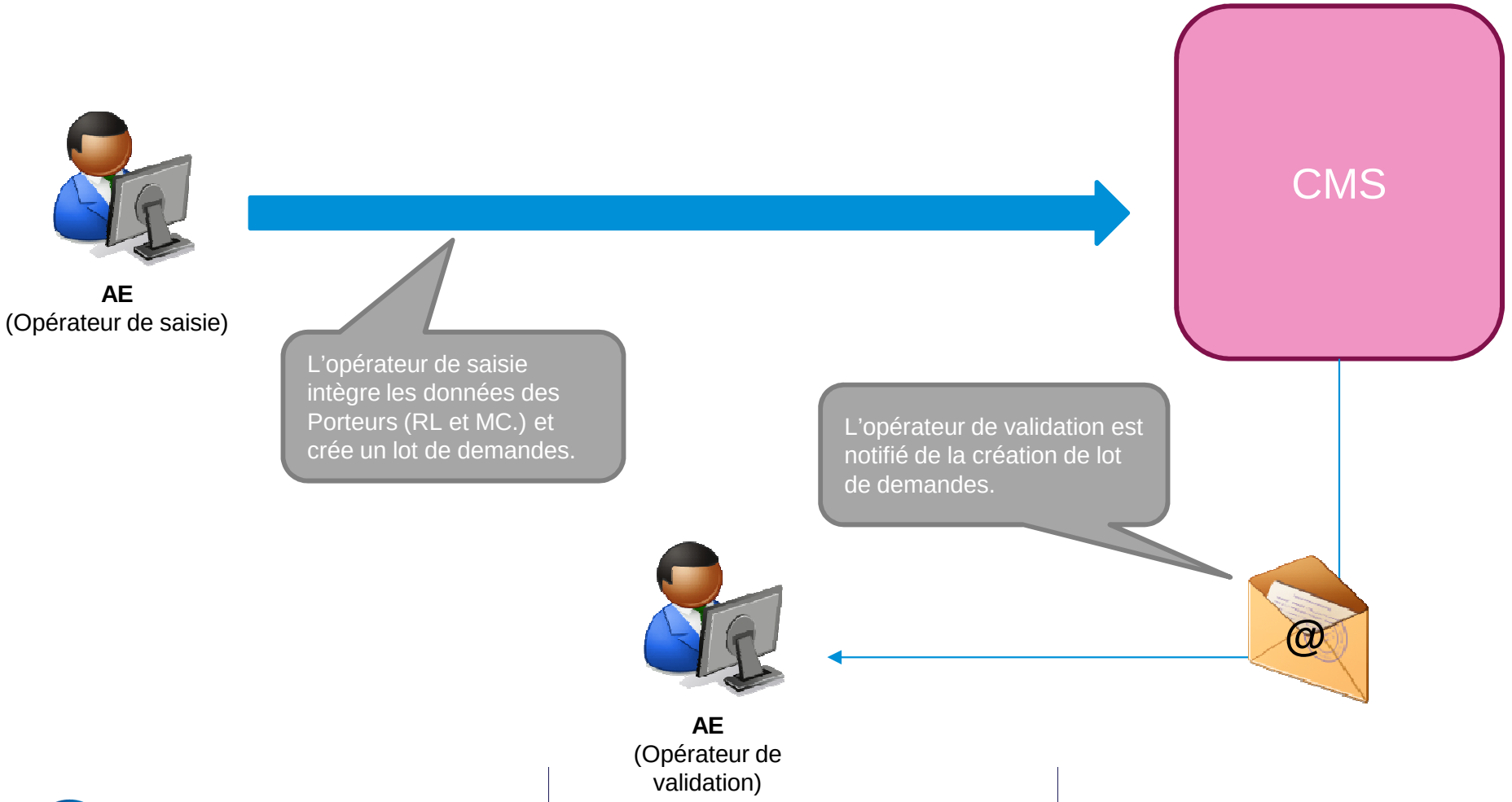
AC
(Opérateur Service Desk)

L'Opérateur Service Desk de l'AC crée l'organisation et définit le RL et le ou les MC associés.

CMS

Un Credential Managment System (CMS) pour traiter les demandes de certificat / carte en relation avec la PKI et envoyer les informations à la plateforme de personnalisation et traiter les demandes de révocation

Processus de demande de carte
Saisie des données des RL/MC



Processus de demande de carte
Validation des données des RL/MC

AE
(Opérateur de validation)

L'opérateur de validation vérifie et valide le lot de demandes.

CMS

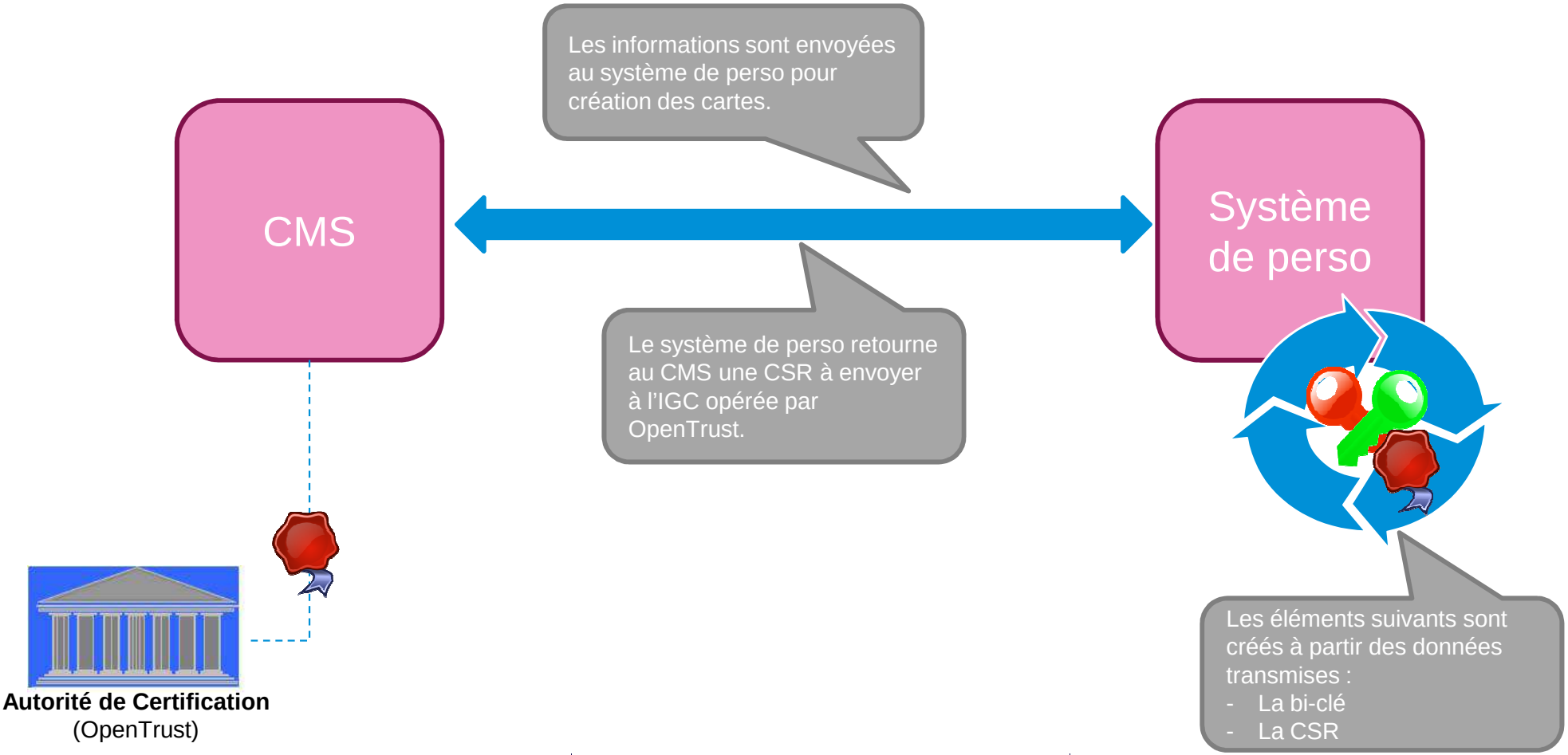
Vers les opérateurs de production en charge de la personnalisation et du Pinmailer.

Système de perso

Envoi du mot de passe du compte du RL/MC.

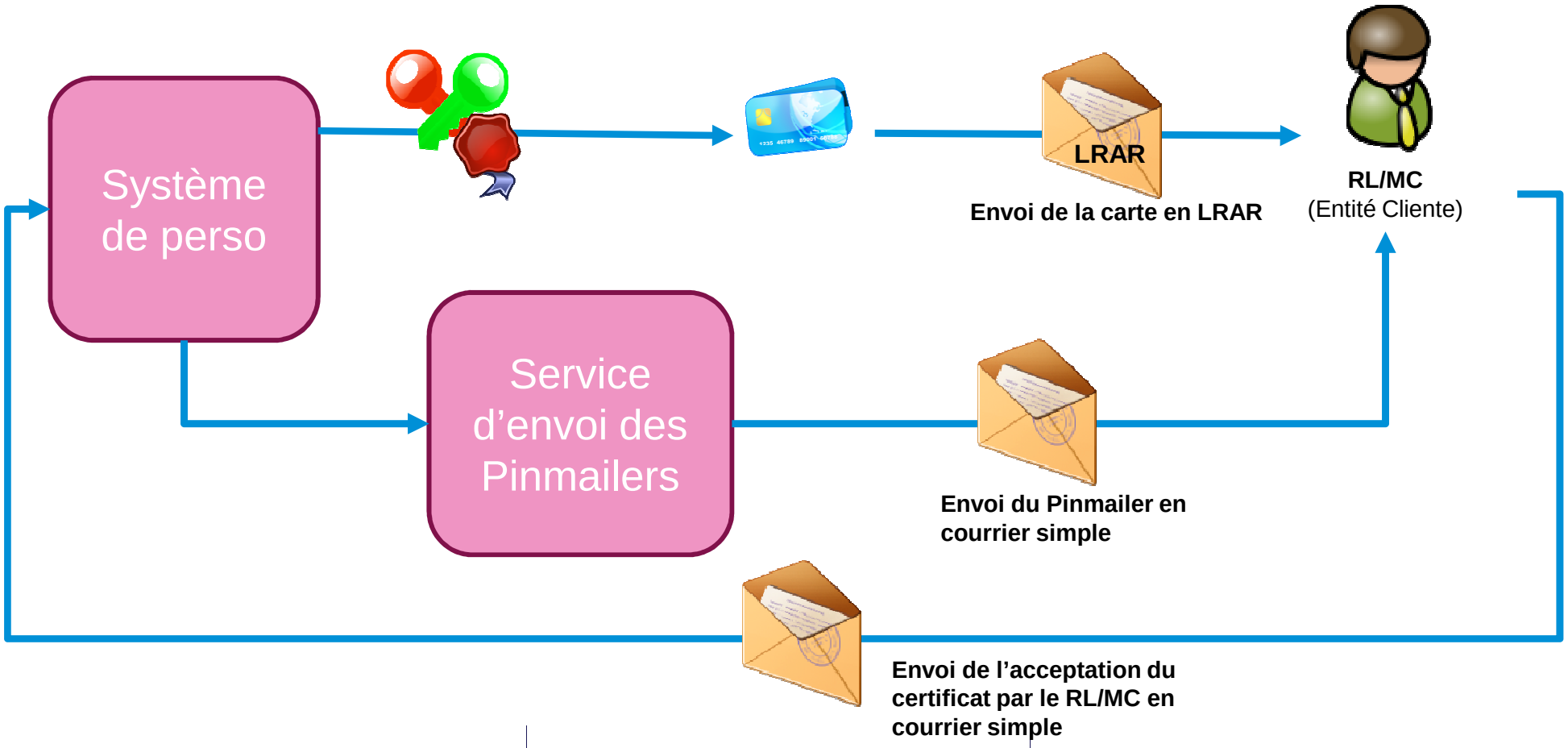
RL et MC
(Entité Cliente)

Processus de demande de carte
Personnalisation/création des cartes des RL/MC



Processus de demande de carte

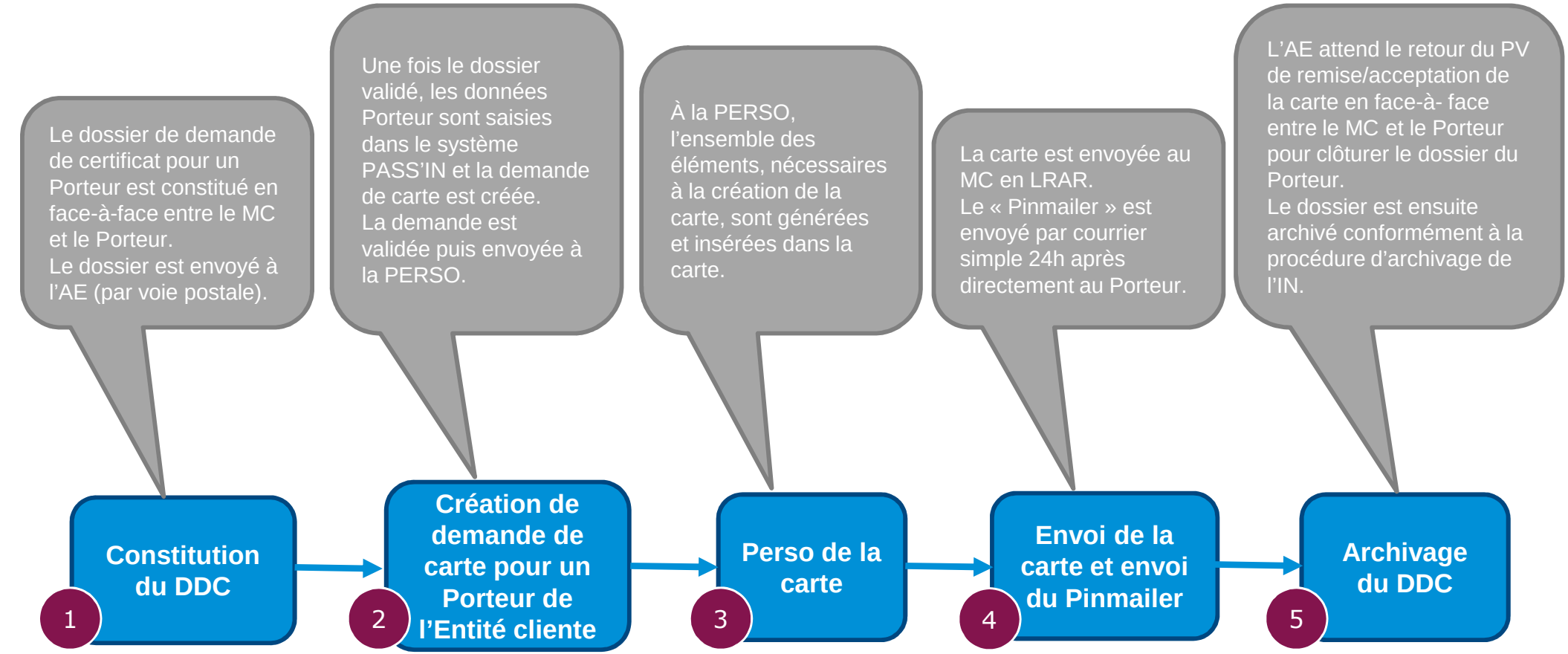
Personnalisation/création des cartes et envoi des éléments aux RL/MC



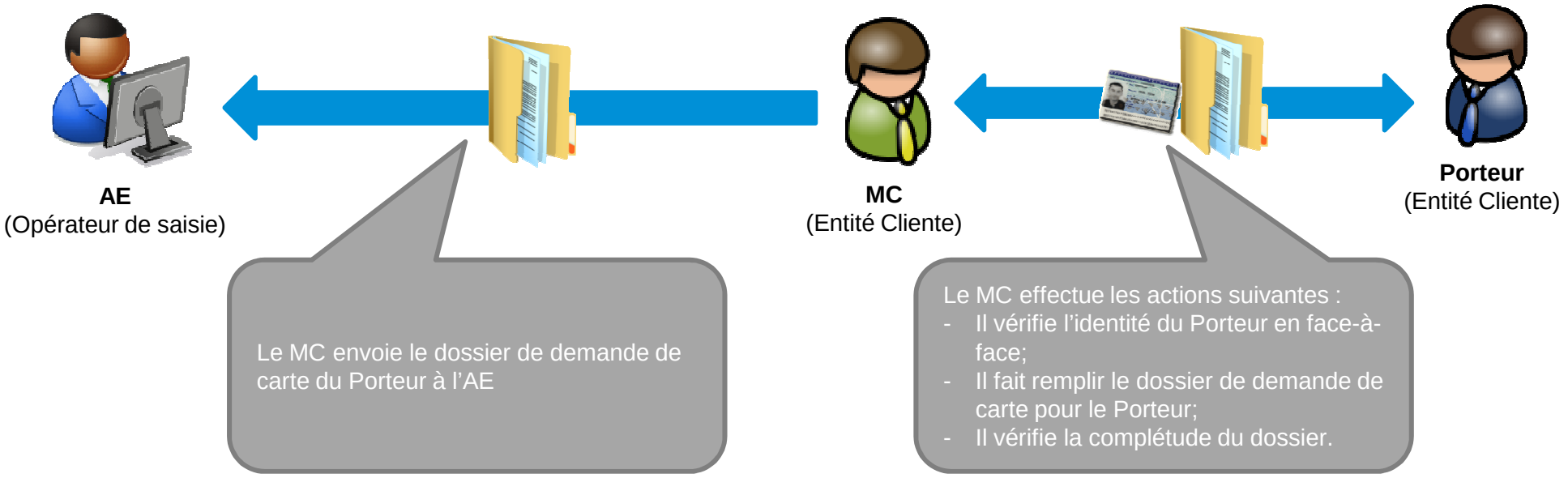
Processus d’une demande de carte Porteur

Processus de demande de carte

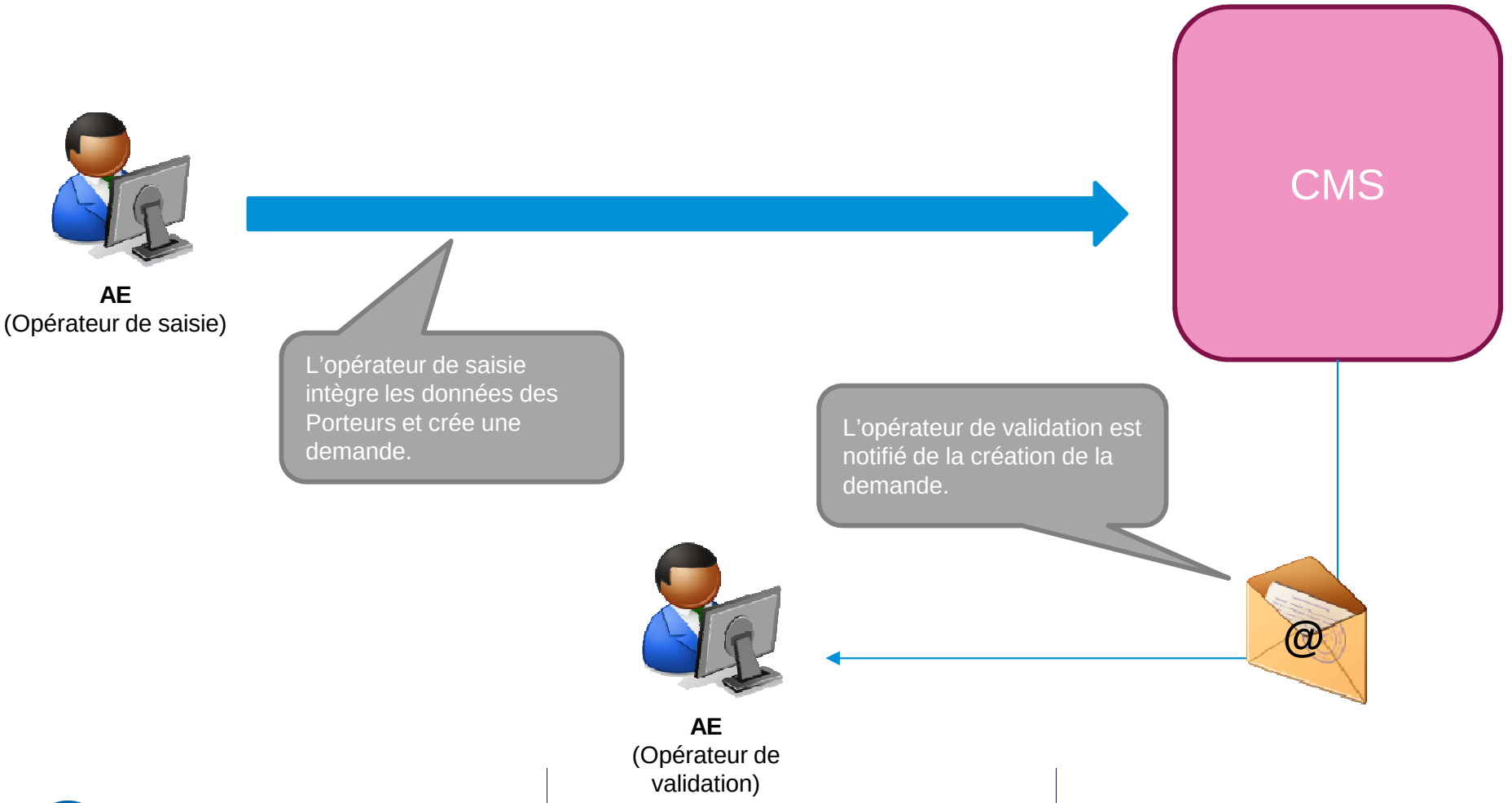
Processus global pour un Porteur



Processus de demande de carte
Constitution du dossier Porteur



Processus de demande de carte
Saisie des données du Porteur



Processus de demande de carte
Validation des données du Porteur

AE
(Opérateur de validation)

L'opérateur de validation vérifie et valide la demande.

CMS

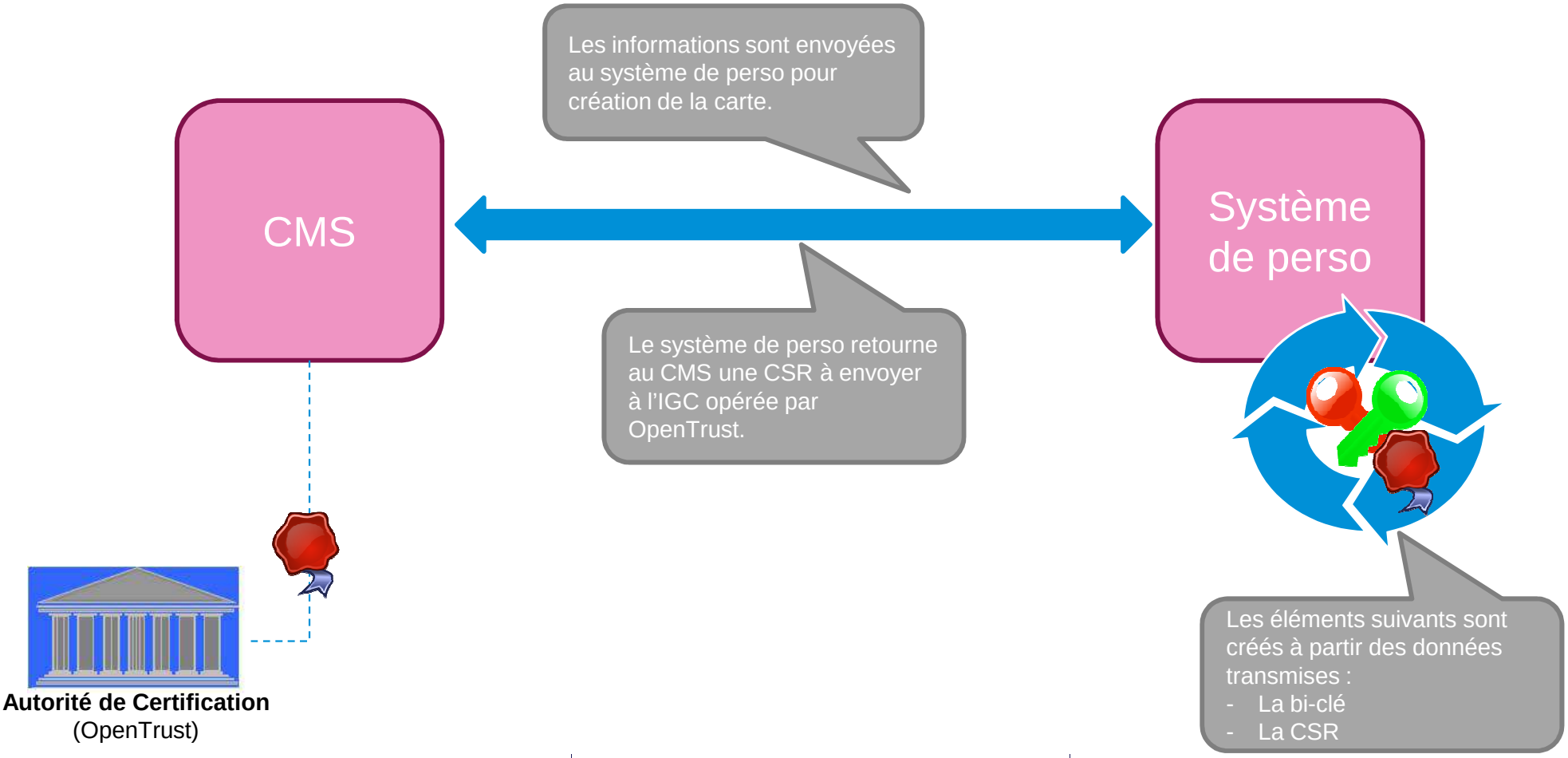
Vers les opérateurs de production en charge de la personnalisation et du Pinmailer.

Système de perso

Envoi du mot de passe du compte du Porteur.

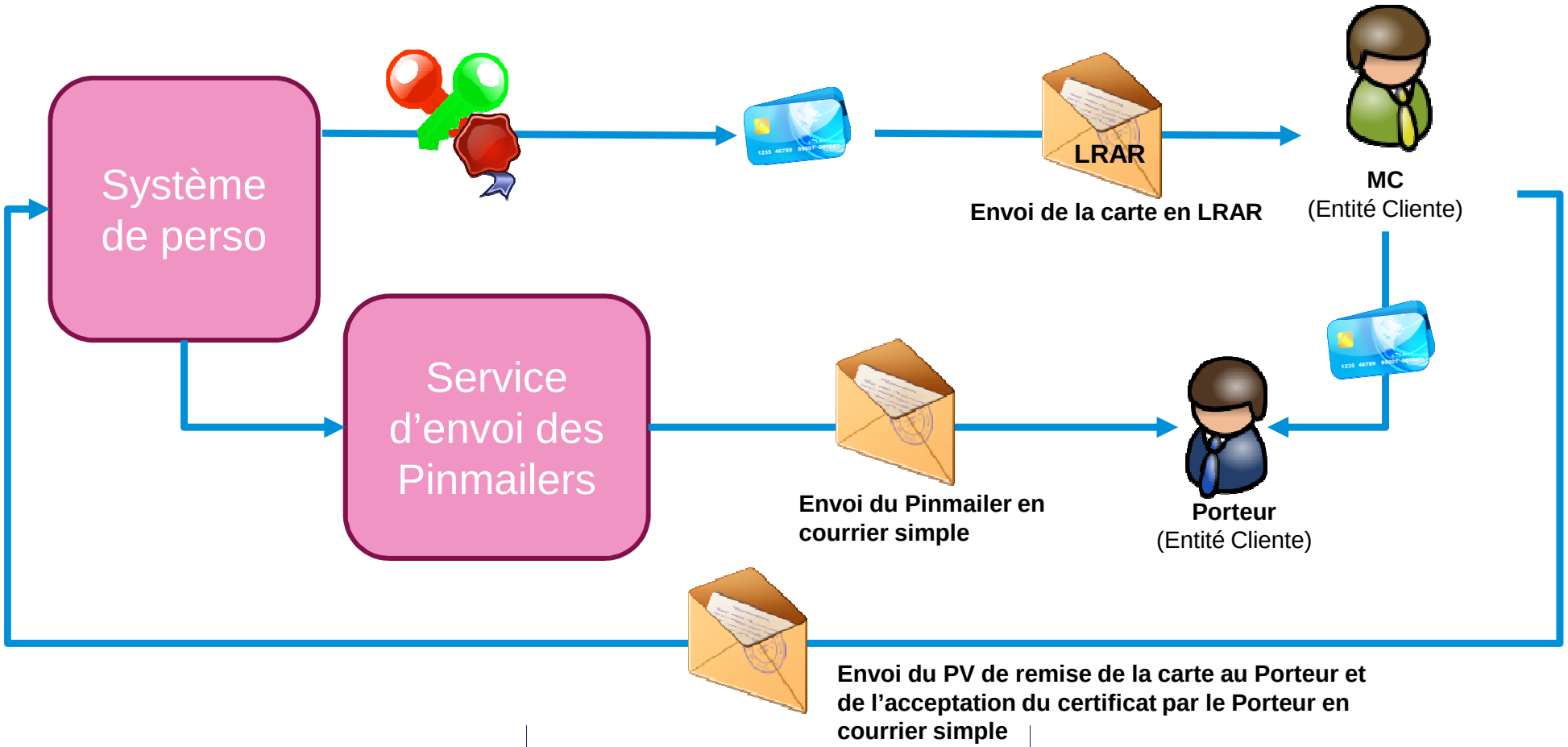
Porteur
(Entité Cliente)

Processus de demande de carte
Personnalisation/création de la carte du Porteur



Processus de demande de carte

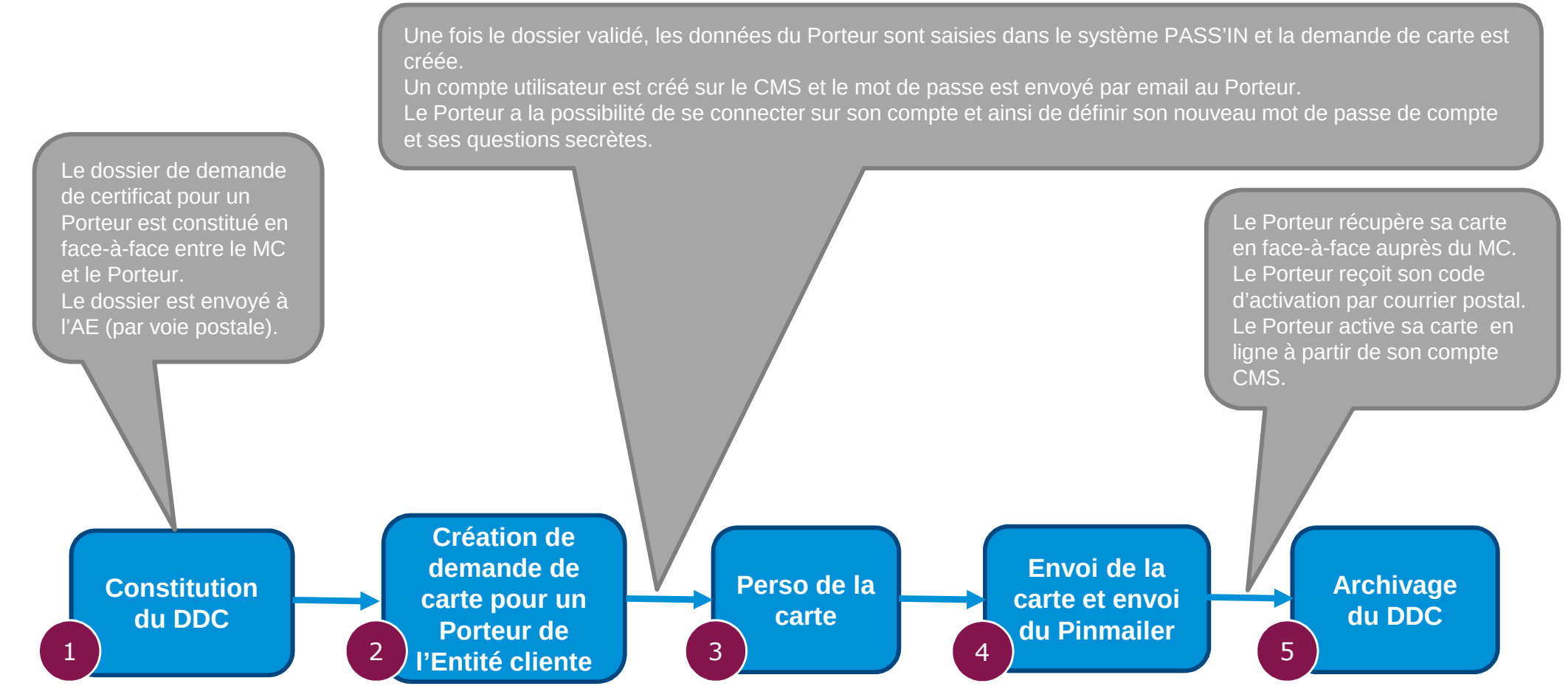
Personnalisation/création des cartes et envoi des éléments au Porteur



Processus d’une demande de carte Porteur côté Client

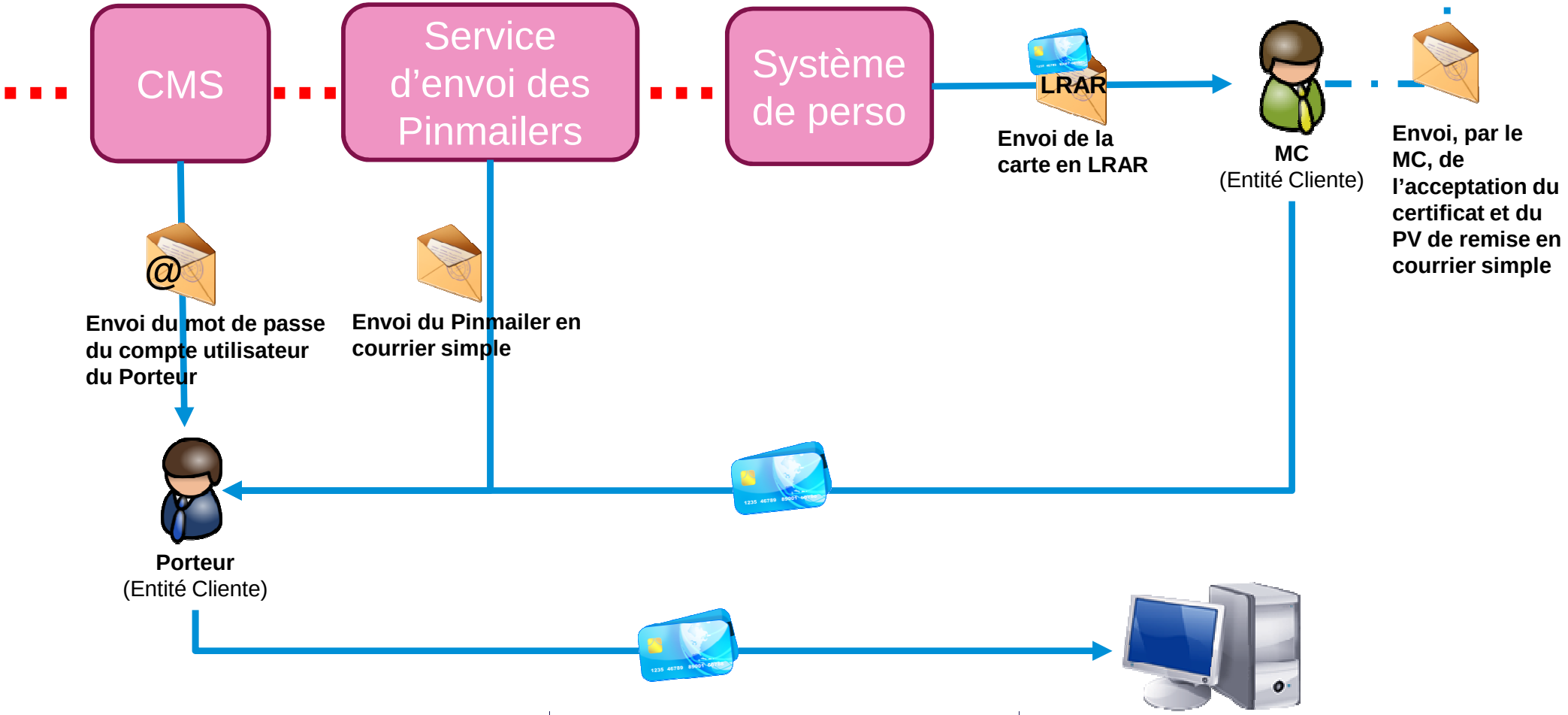
Processus de demande de carte

Processus global pour un Porteur



Processus de demande de carte

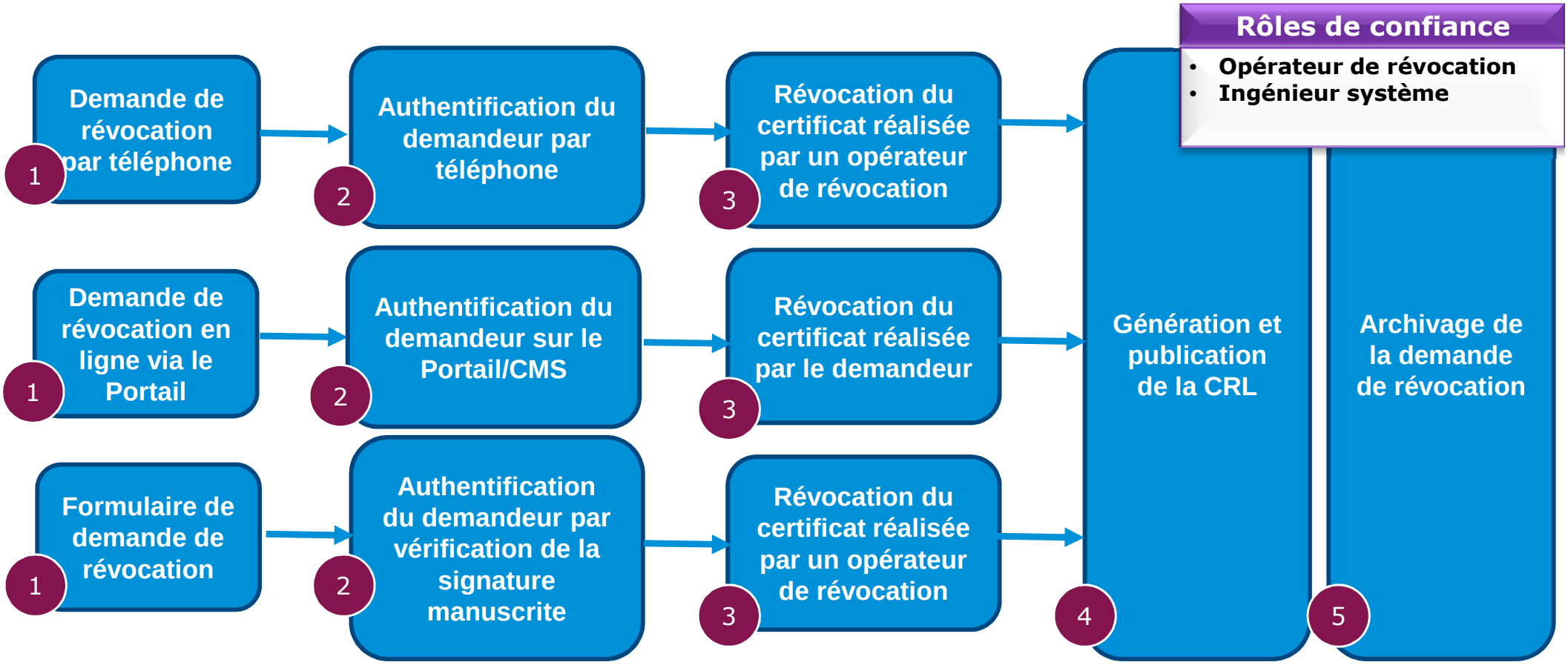
Personnalisation/création des cartes et envoi des éléments au Porteur



Processus d’une demande de révocation d’un certificat RL/MC/Porteur

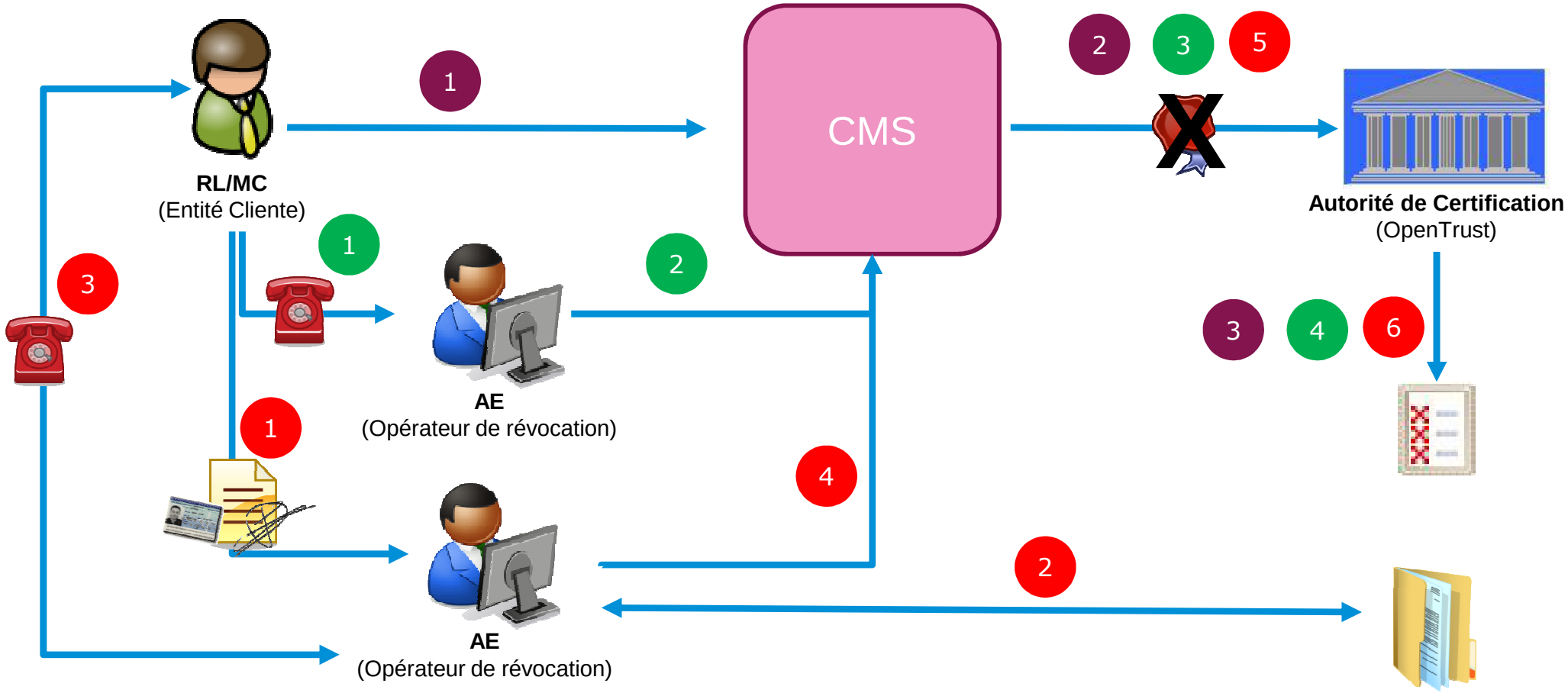
Processus de demande de révocation

Processus global pour un RL/MC/Porteur



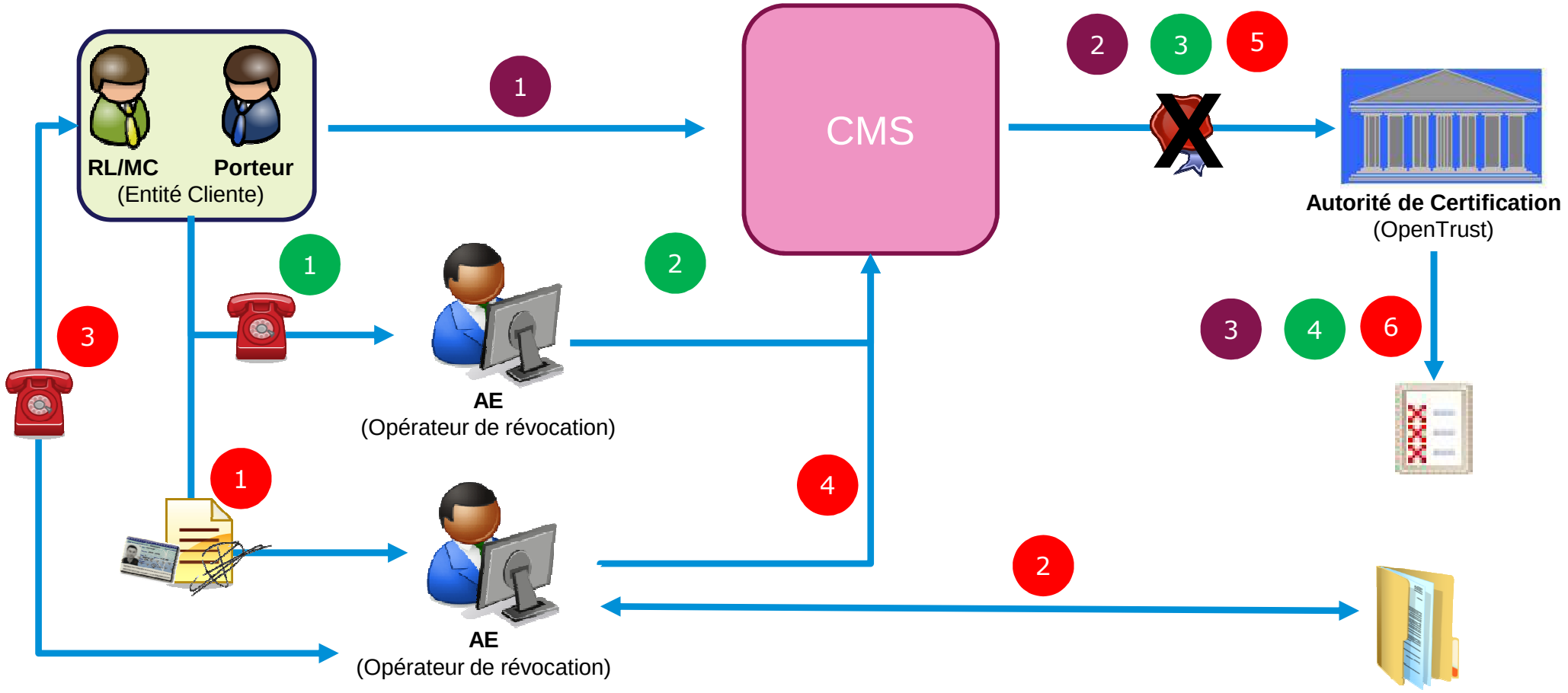
Processus de demande de révocation

Révocation d'un certificat RL/MC



Processus de demande de révocation

Révocation d'un certificat Porteur



Merci de votre attention