Sécurité des systèmes d'information des MCS
Thématique « IGC-Santé »

Atelier du 21 avril 2016

Intervenants :

- David DECROIX – Responsable activité PSCE
- Alexandre SALZMANN – Chef de projet MOA IGC-Santé

Sécurité des systèmes d'information des MCS
Thématique « IGC-Santé »

Atelier du 21 avril 2016

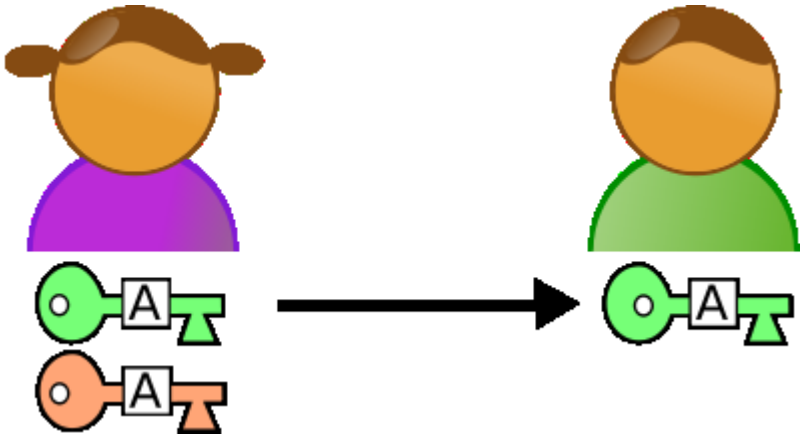
Sommaire

asipsanté
AGENCE DES SYSTÈMES D'INFORMATION PARTAGÉS DE SANTÉ

CHAPITRE 1

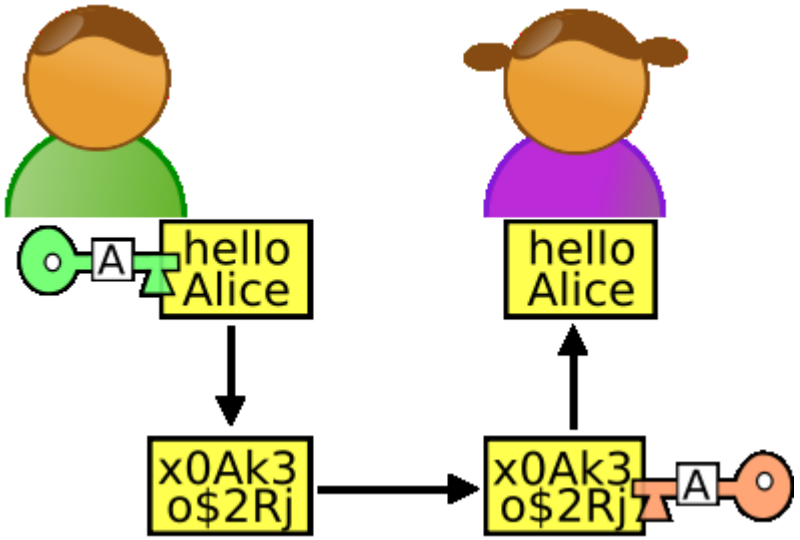
Rappels sur les IGCs

Cryptographie à clé publique
Principes – Bi-clés



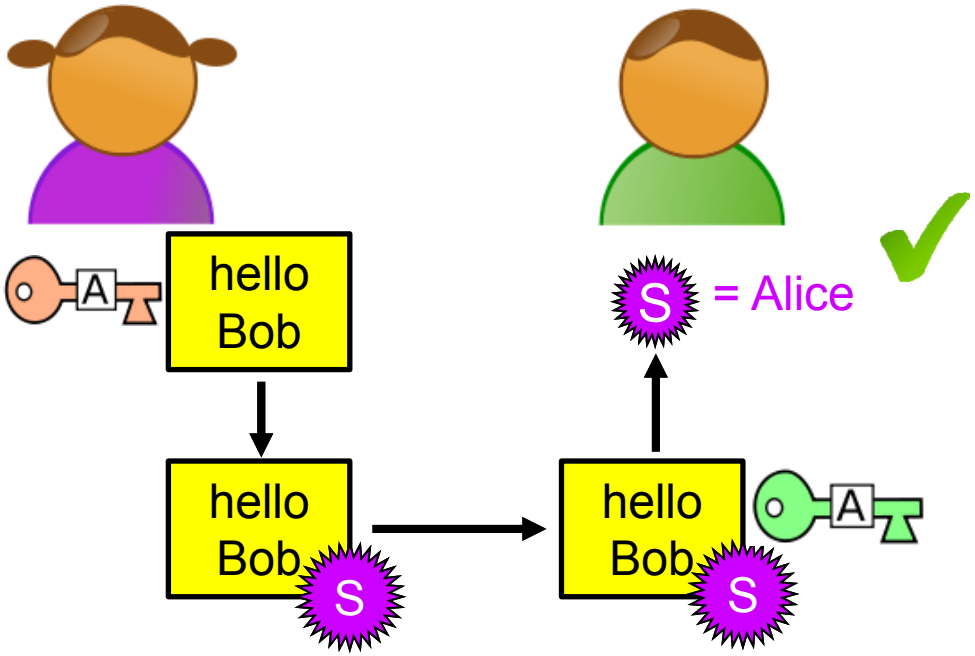
Alice génère deux clés (un bi-clés) :
La clé publique qu'elle envoie à Bob et la clé privée qu'elle conserve précieusement sans la divulguer à quiconque.

Cryptographie à clé publique
Principes – Chiffrement



Bob chiffre le message avec la clé publique d'Alice et envoie le texte chiffré.
Alice est la seule à pouvoir déchiffrer le message grâce à sa clé privée.

Cryptographie à clé publique
Principes – Signature



Alice signe le message avec sa clé privée et envoie le texte accompagné de cette signature.
Bob vérifie que la signature est bien celle d'Alice grâce à sa clé publique.

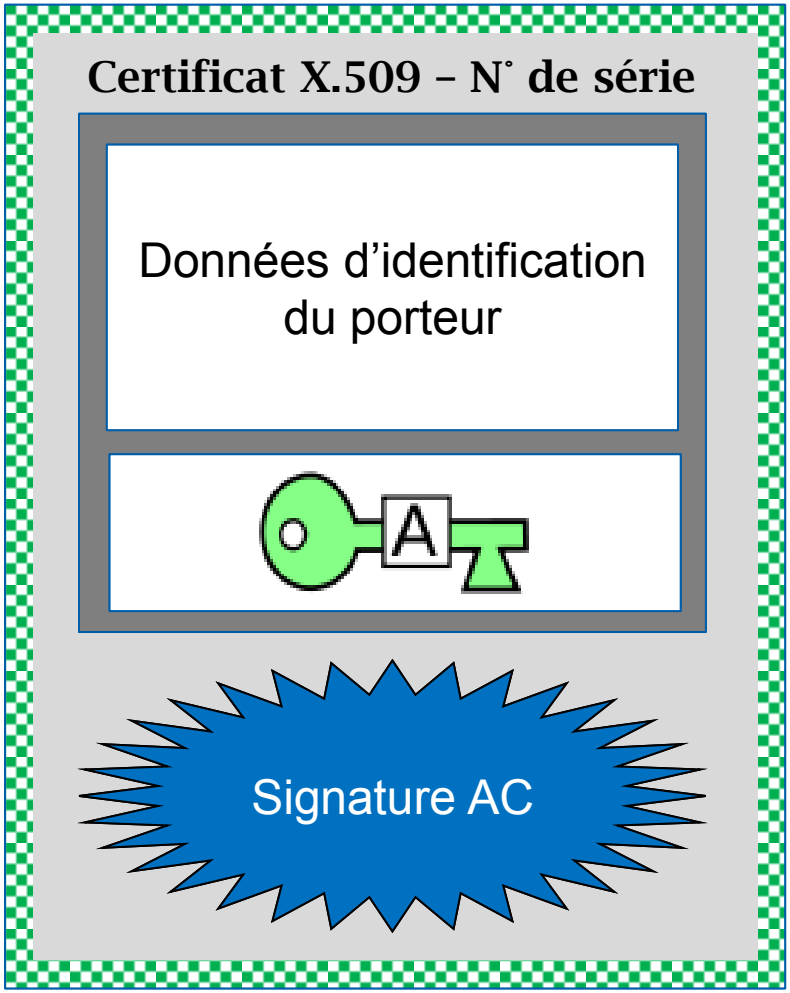
Cryptographie à clé publique
Principes – Certificat numérique X.509

Un certificat numérique est une **pièce d'identité électronique**.
Il sert également à transporter la **clé publique**.

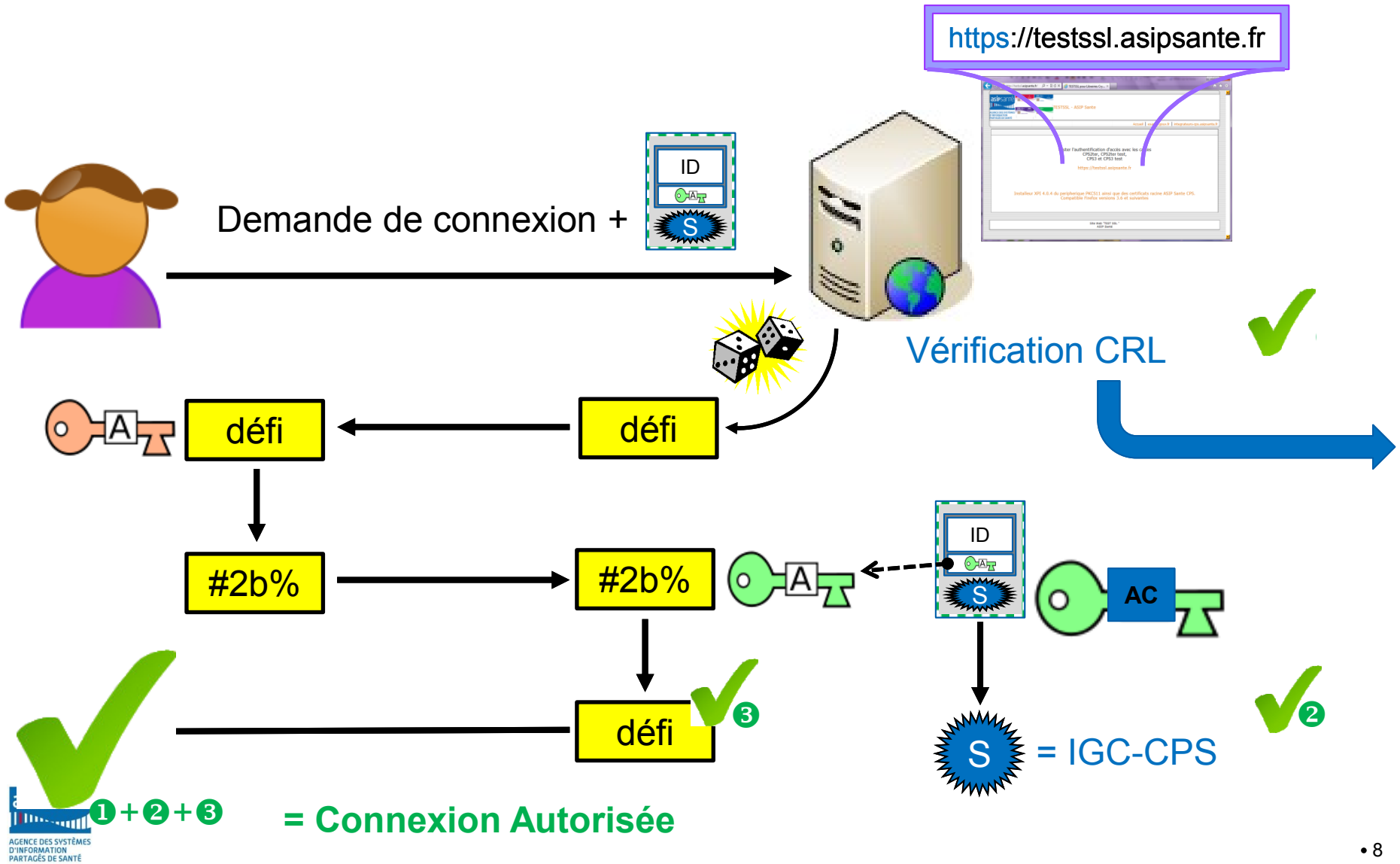
Il est émis par une **Autorité de Certification** qui fait foi de tiers de confiance et qui atteste du lien entre l'identité physique et l'identité numérique.
Chaque certificat émis est référencé par un **numéro de série** unique au sein de cette AC.

Un certificat contient, outre **l'identité** du porteur, sa **clé publique** et son usage autorisé (signature, authentification, chiffrement, …).
L'ensemble de ces données est **signé** par l'Autorité de Certification.

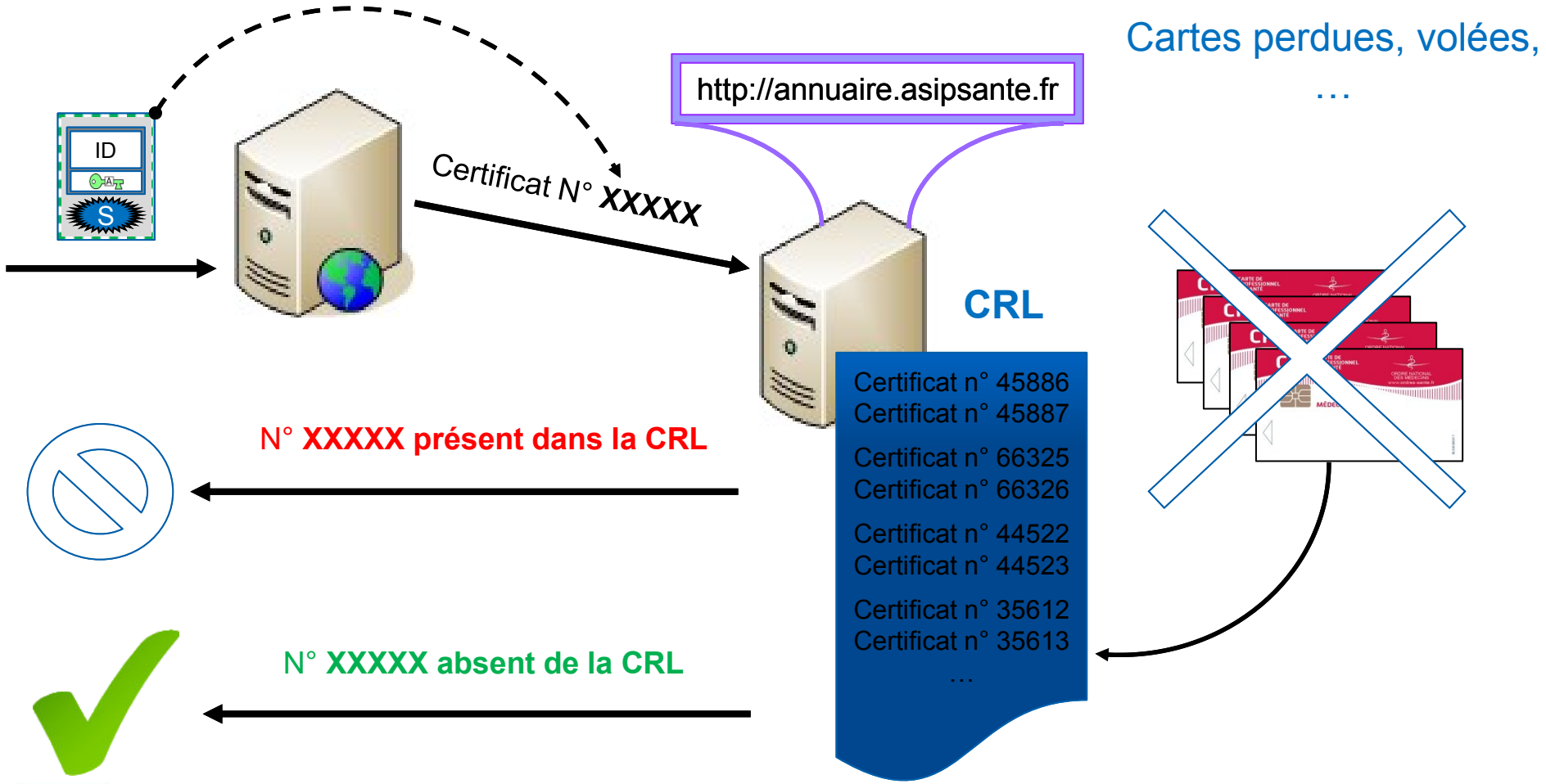
Cette structure de certificat est normalisée par le standard **X.509**.



Cryptographie à clé publique
Principes – Authentification de l'utilisateur (exemple : Testssl)

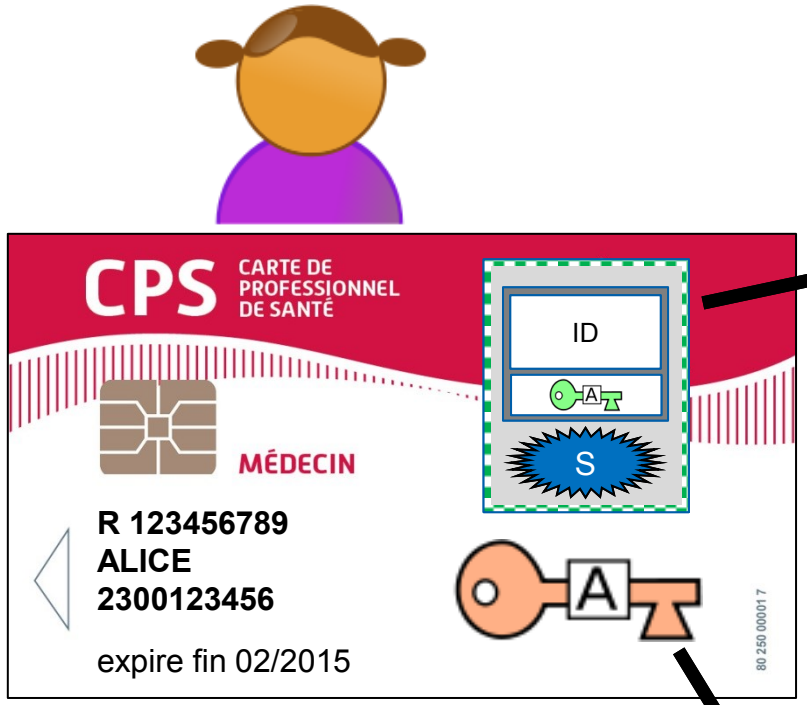


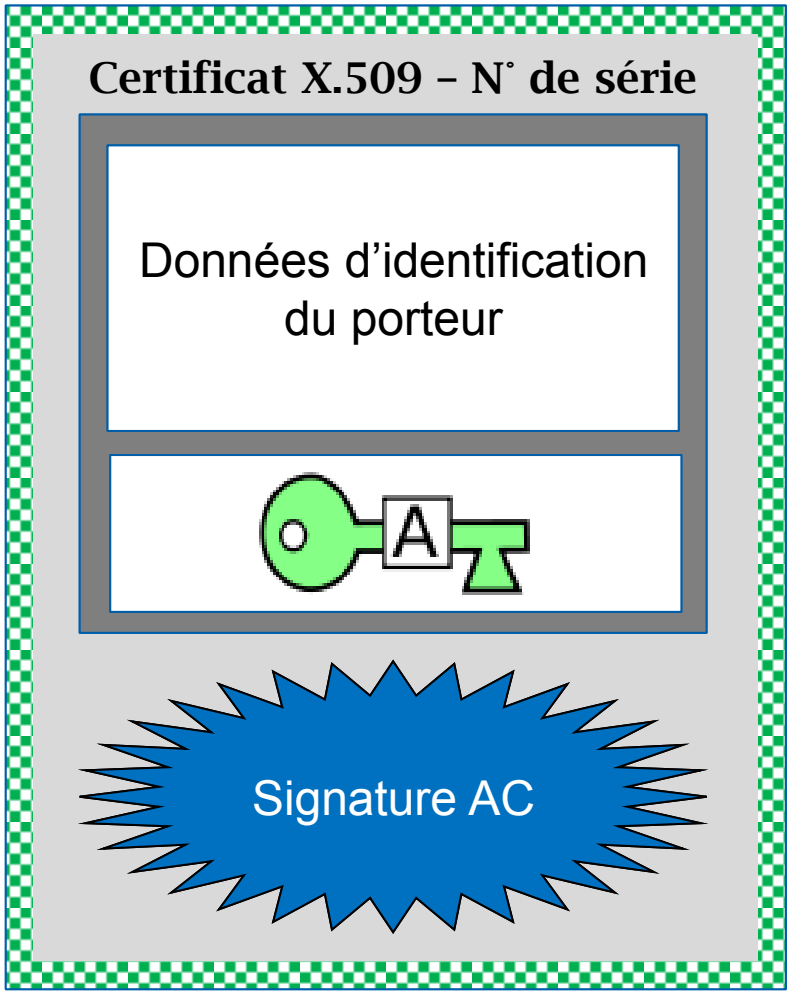
Cryptographie à clé publique
Principes – Vérification de la CRL



asipsanté
AGENCE DES SYSTÈMES D'INFORMATION PARTAGÉS DE SANTÉ

Cryptographie à clé publique
Clés et certificats stockés dans la CPS





2 bi-clés dans la CPS:
- ❑ Authentification
- ❑ Signature

Infrastructure de gestion de clés : définition

Un certificat électronique est un fichier informatique contenant des informations sur son propriétaire et qui sont certifiées par un tiers de confiance appelé Autorité de Certification.

L'ASIP Santé est une Autorité de certification qui garantit la confiance dans les échanges et le partage de données de santé grâce à la mise en œuvre d'une Infrastructure de Gestion de Clés (IGC).

Infrastructure de gestion de clés

L'IGC est un **ensemble de personnes, procédures, matériels, logiciels, pour créer, délivrer, révoquer et publier des certificats électroniques au profit d'une communauté d'utilisateurs**(1).

L'IGC-Santé :

- **respecte des procédures rigoureuses** de recueil des données d'identification professionnelle qui mettent en jeu les autorités compétentes (Ordres, Délégations territoriales des ARS, CPAM, Directeurs d'établissements de santé, …) ;
- **émet des certificats électroniques** qui constituent des pièces d'identité électroniques ;
- **assure la publication de ces certificats dans un annuaire et la prise en compte de leur révocation**, signalée aux applications utilisatrices par des listes de révocation de certificats.

Ces garanties sont précisées dans les « Politiques de certification », indiquant les conditions d'applicabilité d'un certificat pour la communauté de la santé ainsi que les modalités de gestion et d'usage de ce certificat.

asipsanté
AGENCE DES SYSTÈMES D'INFORMATION PARTAGÉS DE SANTÉ

Note : (1) Archimbaud Jean-Luc, « Les IGC, infrastructures de gestion de clés. », *Les Cahiers du numérique* 3/2003 (Vol. 4) , p. 111-134

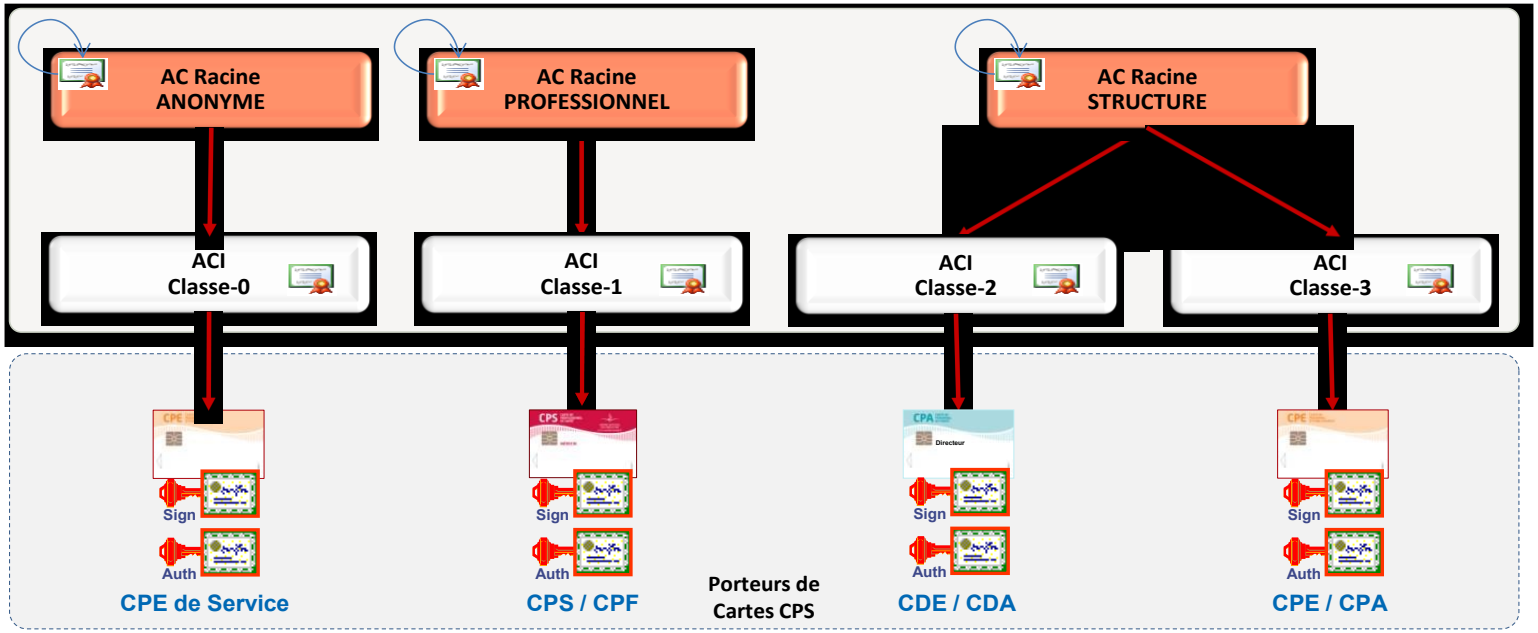
CHAPITRE 2

Les IGC CPS historiques

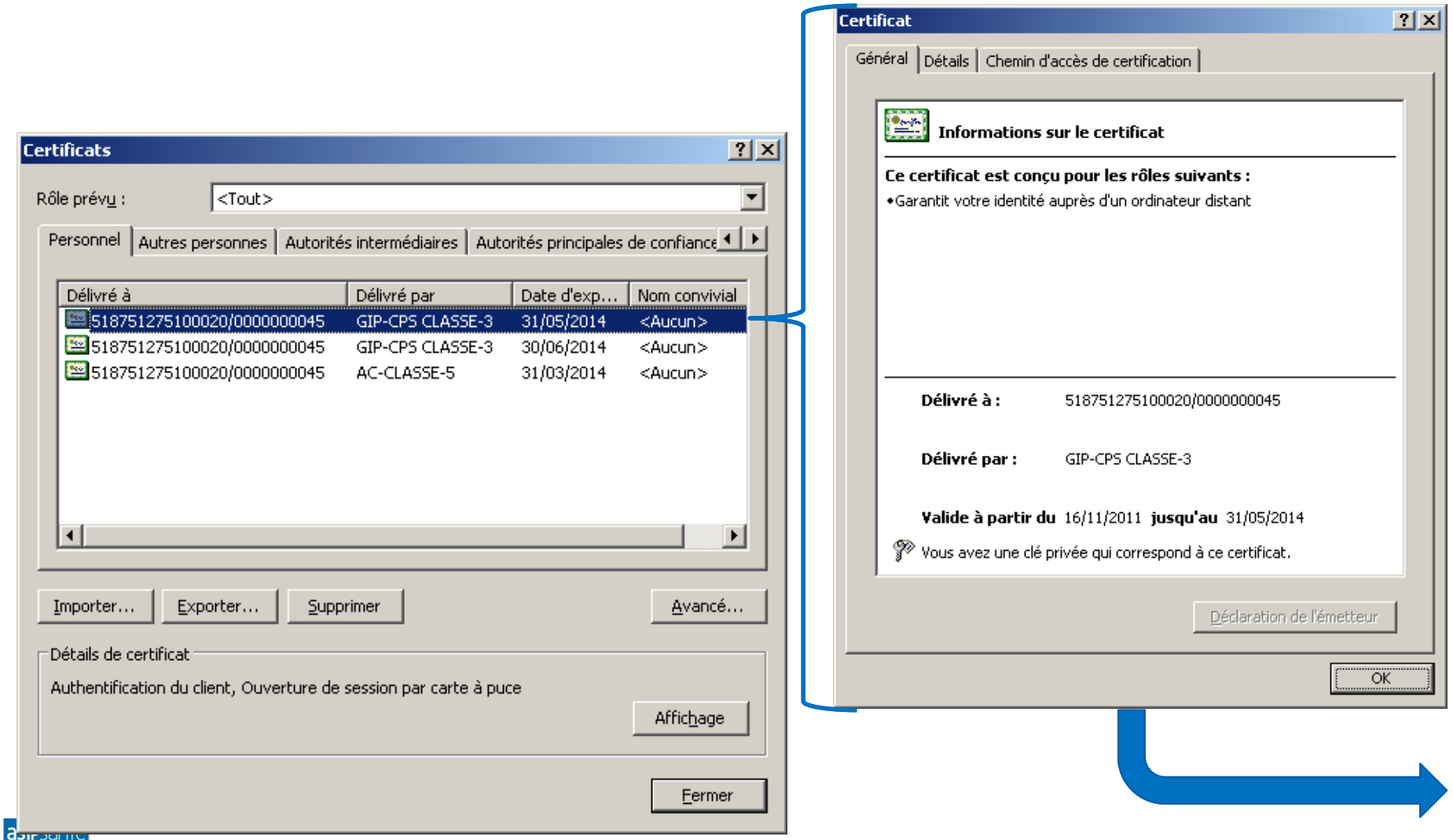
L'IGC CPS-2ter
Certificats embarqués sur cartes CPx

Certificats émis par l'IGC-CPS2ter (Classes 0 à 3)

- **Ils sont embarqués dans les cartes de la famille CPS**
- **Les porteurs finaux sont porteurs de :**
  - Cartes CPS : Professionnels de Santé (professions réglementées)
  - Cartes CPF : Professionnels de Santé en Formation
  - Cartes CDE : Directeurs (non PS) d'Établissement de Santé
  - Cartes CPE : Personnels salariés de structures libérales ou d'Établissements de Santé
  - Cartes CDA : Directeurs de structures autorisées
  - Cartes CPA : Personnels de structures autorisées
- **Fonctions assurées par les certificats : Identification, Authentification et Signature**

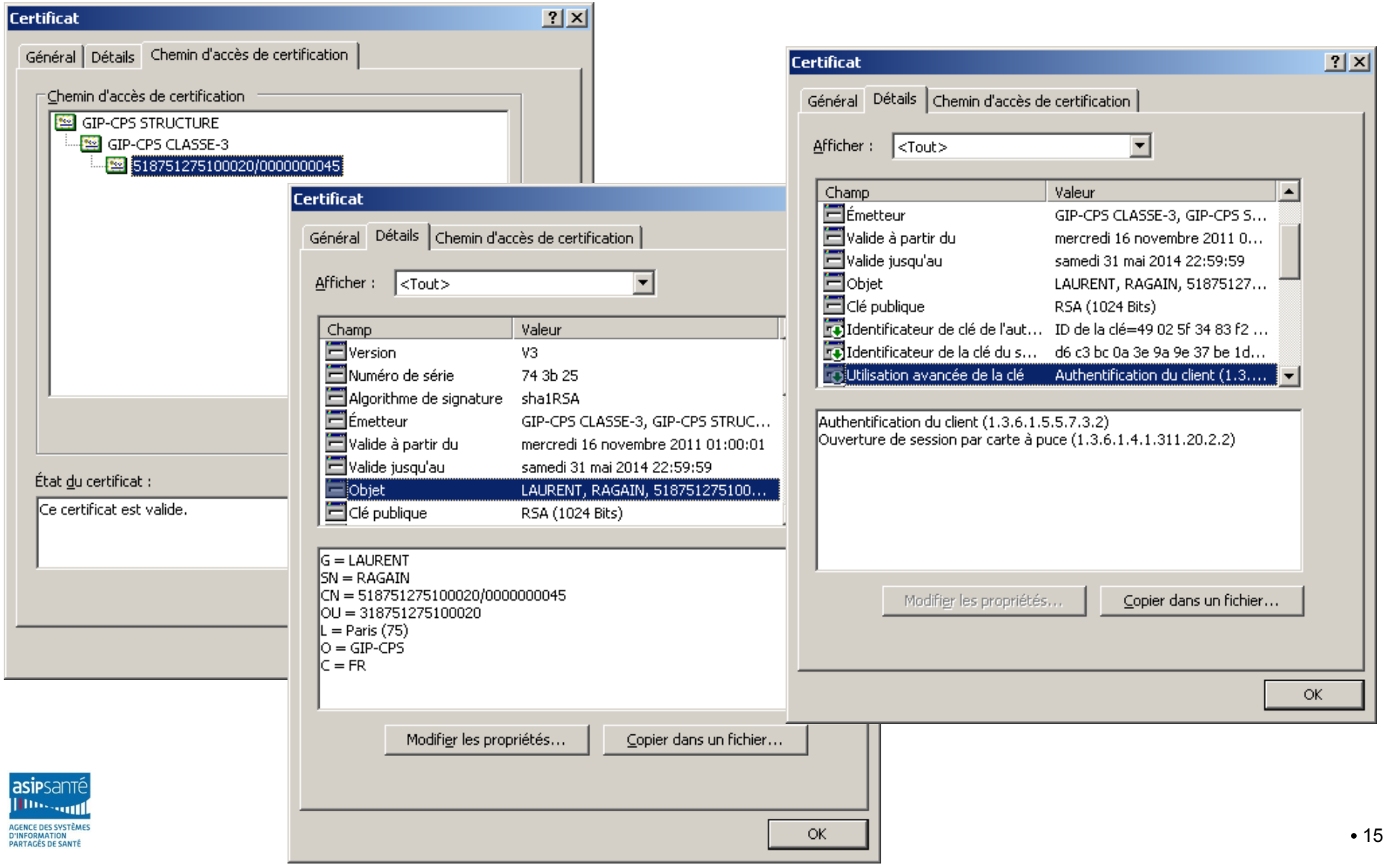


L'IGC CPS-2ter
Certificats utilisateur



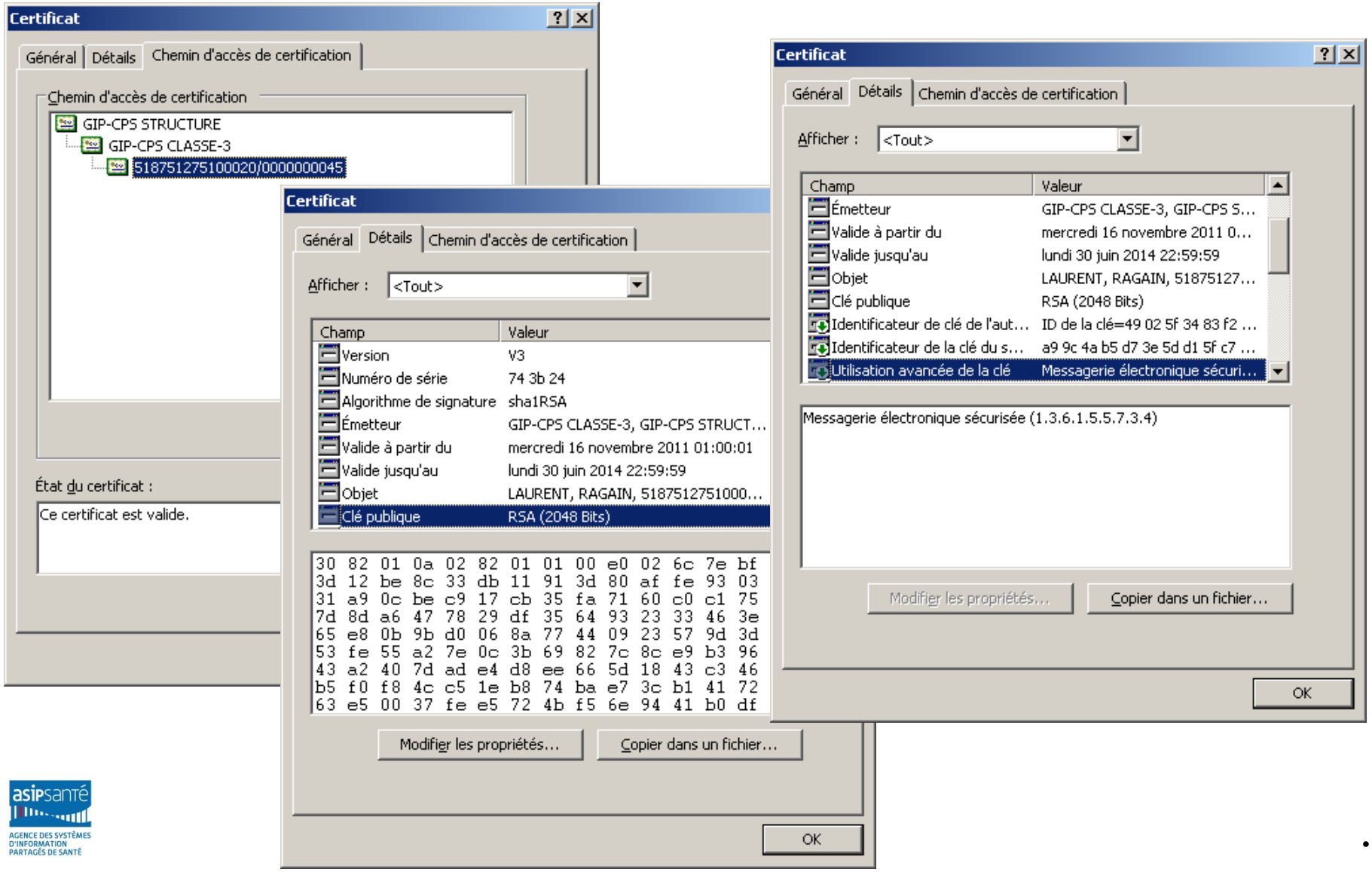
L'IGC CPS-2ter

Certificat utilisateur – usage authentification



L'IGC CPS-2ter

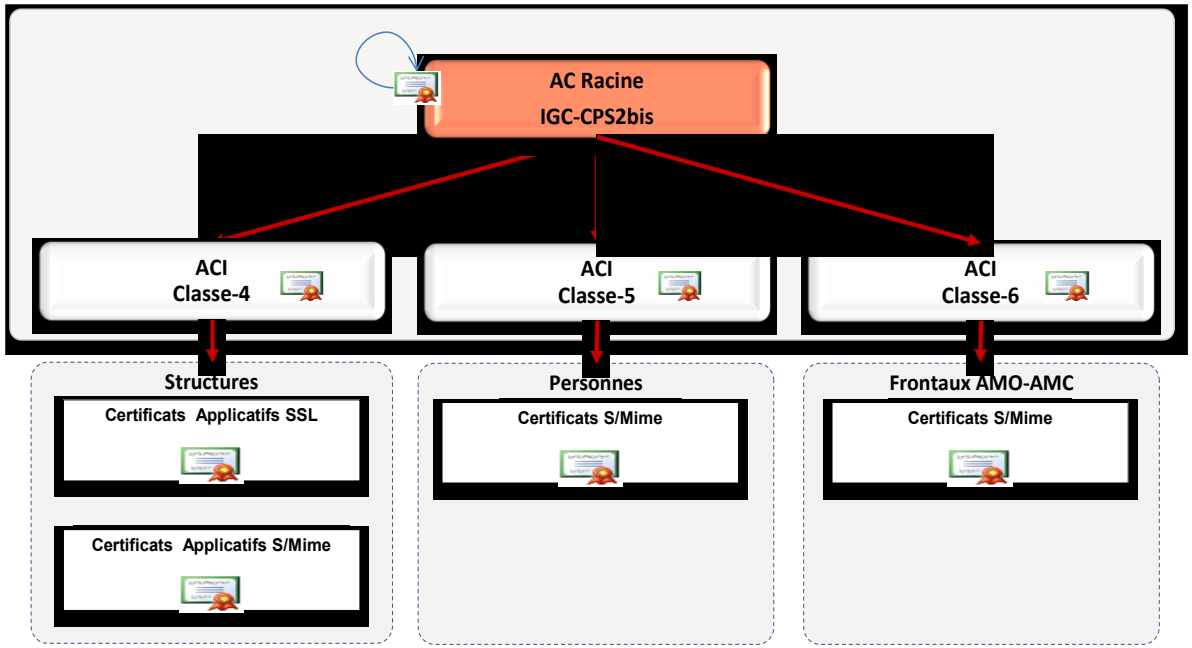
Certificat utilisateur – usage signature



L'IGC CPS-2bis
Certificats logiciels

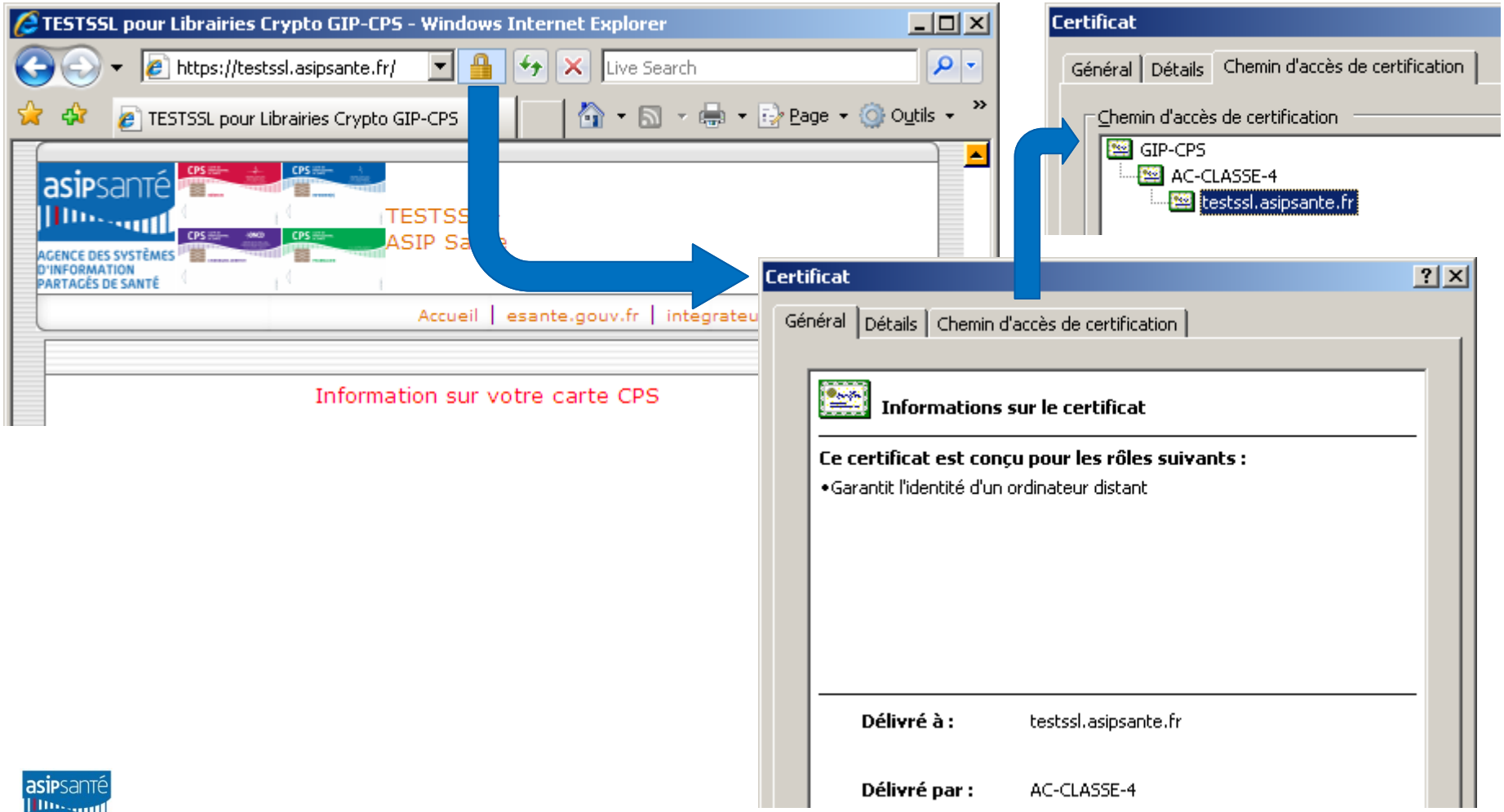
Les certificats émis par l'IGC-CPS2bis (Classes 4 à 6)

- **Ils sont logiciels**
- **Les utilisateurs finaux et les fonctions assurées sont :**
  - Serveurs et clients SSL exploités par des structures, pour des fonctions Authentification client et serveur
  - Modules S/MIME exploités par des structure, pour des fonctions S/MIME (Signature et Chiffrement)
  - Personnes Physiques porteurs de cartes CPx, pour des fonctions S/MIME (Chiffrement uniquement)



L'IGC CPS-2bis
Exemple de certificat serveur SSL

Exemple du certificat serveur du site Testssl :



CHAPITRE 3

L'IGC-Santé

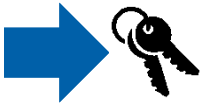
asipsanté
AGENCE DES SYSTÈMES D'INFORMATION PARTAGÉS DE SANTÉ

IGC-Santé - Contexte : changement d'Infrastructure de gestion de clés (IGC)

Toute IGC a une durée de vie limitée

L'ASIP Santé remplace et modernise ses IGC (dont tous les certificats expireront fin 2020) :

- **IGC-2bis (certificats logiciels)**
- IGC 2-ter (certificats confinés dans les cartes)



IGC santé (gérée par l'imprimerie nationale)

1ère étape : remplacement de l'IGC-2bis qui délivre actuellement les certificats logiciels (CL) suivants :

- **Certificats de serveurs applicatifs (CSA) de classe 4 SSL (authentification) et S-MIME (signature et chiffrement)**

  Certificats serveurs attachés à des **personnes morales**

  Usages : Sécuriser les échanges avec le DMP (création/alimentation en authentification indirecte), dans le cadre de "bureautique santé", entre opérateurs MSSanté, pour récupérer des informations contenues dans le RASS via les webservices…

  Volume : ~1500 CSA

- **Certificats de confidentialité de classe 5 S/MIME**

  Associé à une **personne physique**, porteuse de carte de la famille CPS (commande directe par le PS via son logiciel, ou par un administrateur).

  Usages : chiffrement (cyptage) des données de santé pour les échanges par messagerie sécurisée (OSM)

  Volume : ~9000 certificats de confidentialité

Bénéfices de l'IGC Santé

L'IGC Santé apporte plusieurs évolutions :

① ➢ sur l'offre de produits de certification :

Elle permet d'élargir la gamme de Produits de Certification pour Personnes Morales et Personnes Physiques :

- en couvrant les principaux usages de certificats (authentification, signature, chiffrement, …).
- dans le respect des référentiels de la PGSSI-S
- en tenant compte de l'évolution des contextes de travail (utilisation de dispositifs mobiles, LPS hébergés en mode SaaS, …)

② ➢ sur les services de demande et de gestion des certificats:

Elle propose deux nouvelles interfaces pour les services associés à la plateforme IGC (Demande / Retrait / Révocation) :

- Portail Internet
- Web Services

Elle permet le contrôle en ligne de la validité d'un certificat (protocole OCSP)

- pour éviter la gestion quotidienne des listes de révocation de certificats

③ ➢ sur le plan technique et sécuritaire :

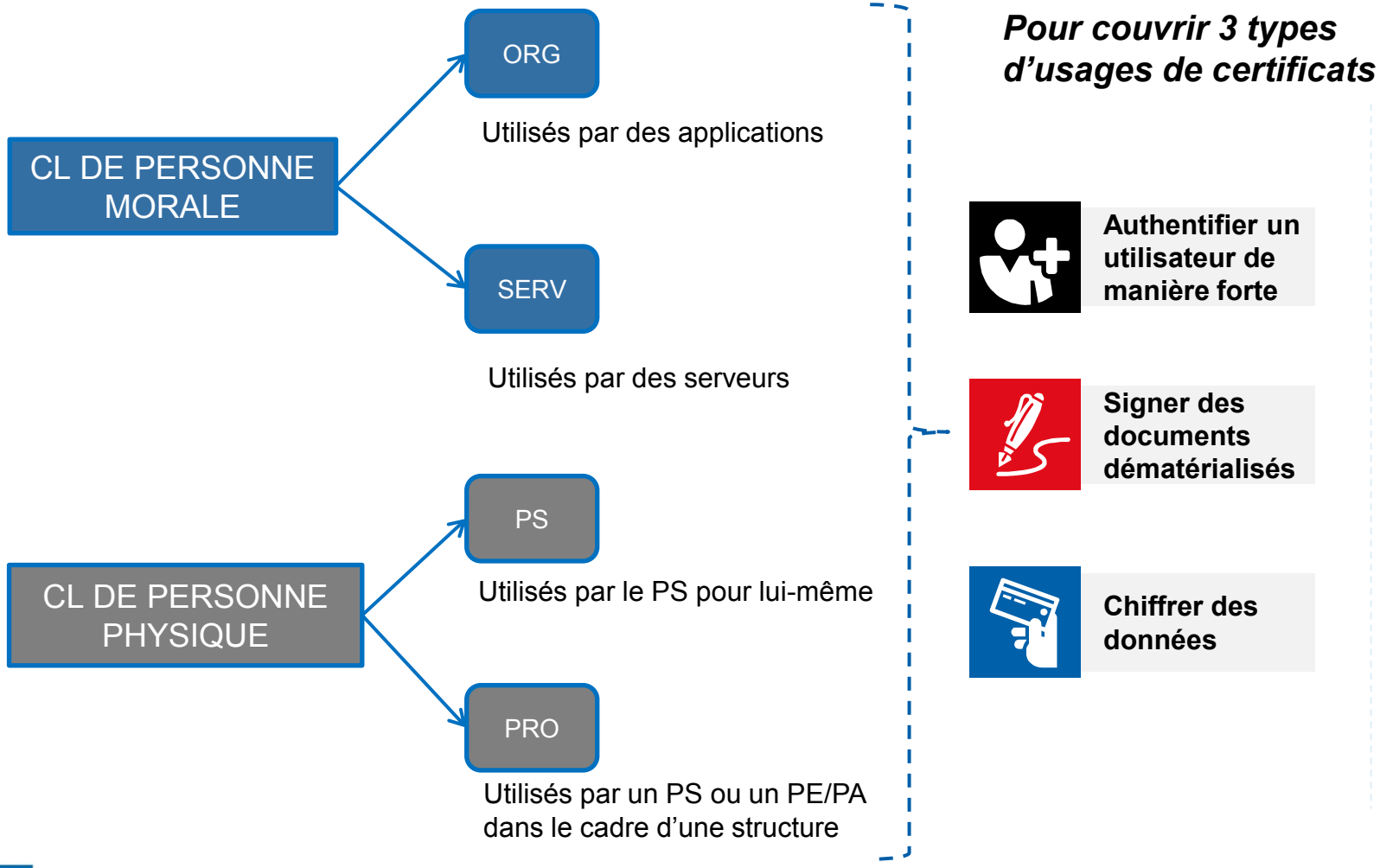
Elle assure le renouvellement des plateformes IGC actuelles

Elle augmente le niveau de qualité des Produits de Certification ASIP Santé :

- Conformité RGS et standards internationaux de gestion des identités et des signatures/cachets électroniques.
- Mise à niveau des caractéristiques techniques de l'IGC (taille de clés, algorithmes utilisés, …)

asipsanté
AGENCE DES SYSTÈMES D'INFORMATION PARTAGÉS DE SANTÉ

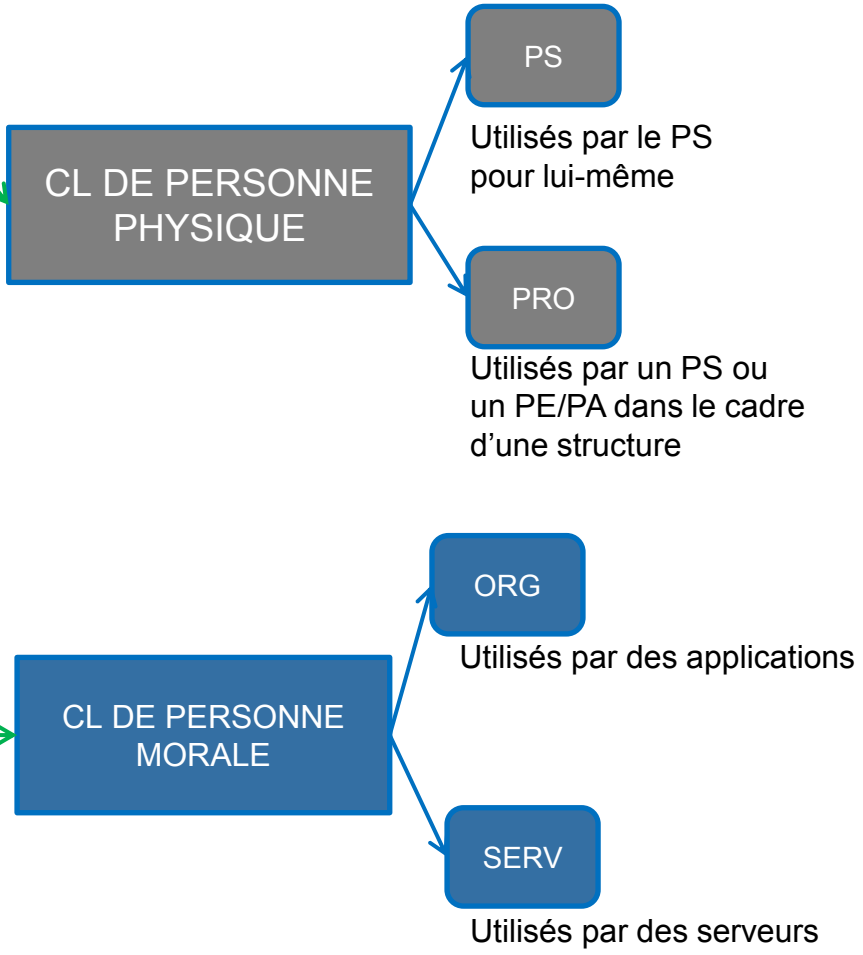
IGC Santé : permet de délivrer des CL pour différents contextes et usages



IGC Santé : Lien avec la PGSSI-S

La nouvelle offre IGC Santé a été conçue en intégrant les principes énoncés dans la PGSSI-S :

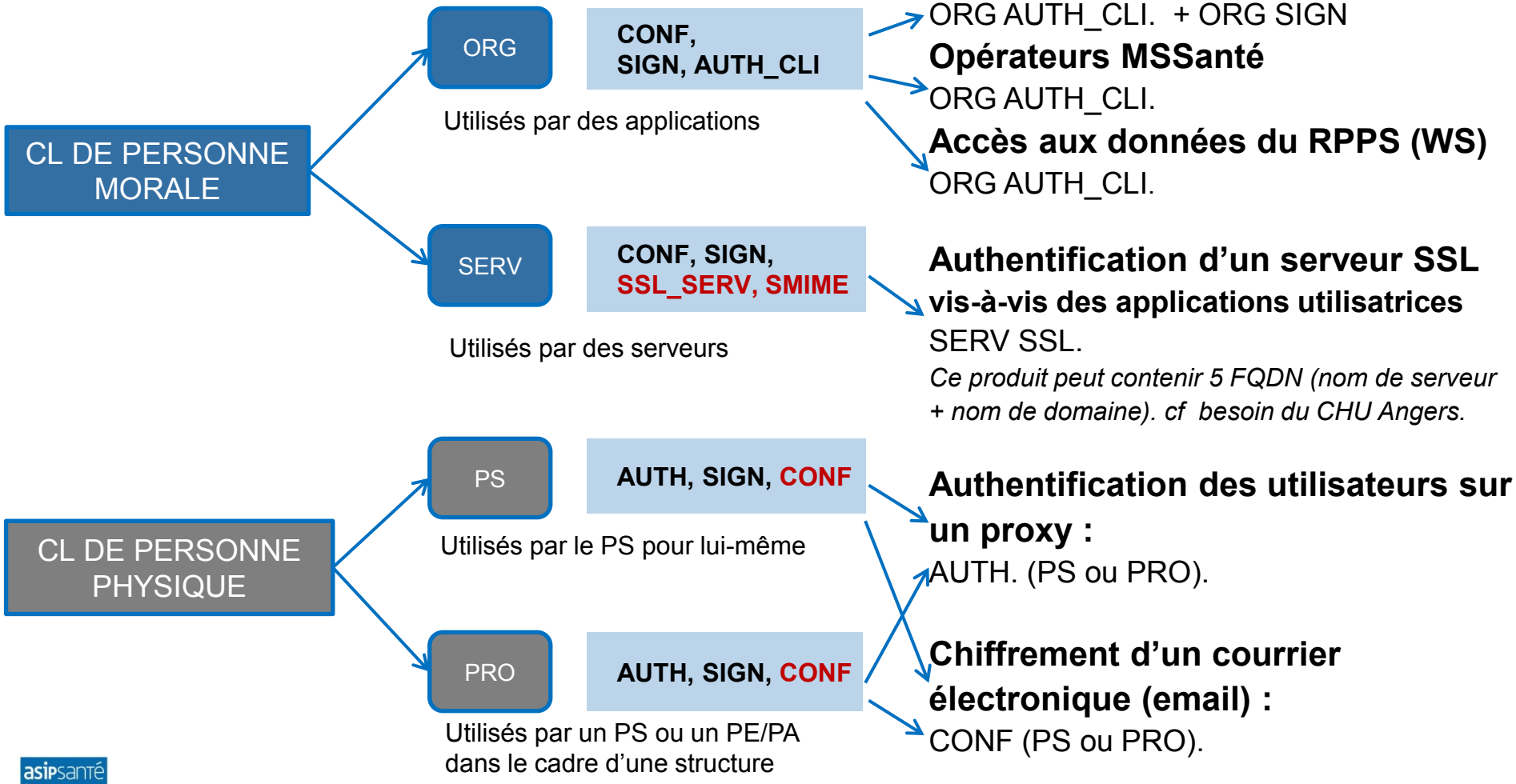
		Palier 1	Palier 2	Palier 3
Authentification « publique » des personnes physiques	Directe		Certificat logiciel de personne physique	• Carte de la famille CPx • Dispositifs alternatifs : Mot de passe à usage unique (OTP Push, à défaut OTP SMS, à défaut OTP Mail)
	Architecture d'authentification (indirecte ou par délégation)		Authentification indirecte : • Authentification « publique » de la personne morale • Identification de portée nationale ou locale de la personne physique • Authentification « privée » de la personne physique	Authentification par délégation : • Authentification « publique » de la personne morale • Identification de l'acteur de santé de portée nationale • Authentification « publique » de la personne physique • Exigences de sécurité imposées par le système d'information cible
Authentification « publique » des personnes morales			Certificat serveur Référence à la personne morale responsable du serveur et identifiée dans le certificat. L'identifiant de la personne morale utilisé est national (FINESS, SIRET / SIREN).	Certificat logiciel de personne morale L'identifiant de la personne morale utilisé est national (FINESS, SIRET / SIREN).



IGC Santé : Nouvelle Offre de Certificats Logiciels

Certificats logiciels de production et de test

Possibilités techniques : 13 types de certificats logiciels (versus 4 dans l'offre actuelle)



IGC Santé : Nouvelle Offre de Certificats Logiciels

La nouvelle offre de certificats logiciels IGC Santé est accessible au travers d'une nouvelle plateforme de services : la PFCNG (Plateforme de Fourniture de Certificats Nouvelle Génération).

La PFCNG permet de Demander et Renouveler / Retirer / Révoquer /Suivre des produits de certification.

Ces actions peuvent être réalisées par 3 canaux :

- **Interface Web** — Nouveaux canaux
- **Web Service** — Gestion des renouvellements à échéance.
- **Mail**

L'utilisateur, en fonction d'une matrice des habilitations, pourra agir :

- **Pour son compte propre**
- **Pour le compte d'un tiers**
- **Pour le compte d'une personne morale**

IGC Santé : Impacts sur les serveurs et applications

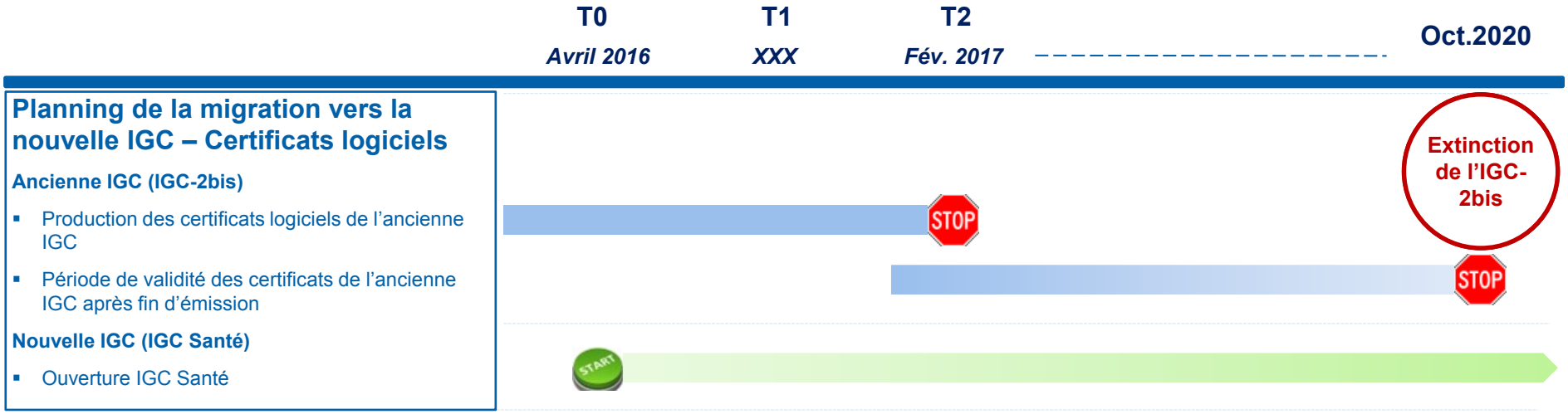
Évolutions nécessaires sur les serveurs et applications centraux et les postes de travail des utilisateurs

- Ajout des chaînes de confiance de l'IGC-Santé dans le coffre-fort de l'application (serveurs et postes de travail). *Ces chaînes de confiance sont déjà disponibles et intégrées aux installeurs de la Cryptolib v5.*
- Prise en compte de la nouvelle cryptographie de l'IGC-Santé (algorithme RSA avec clés de 4096 bits et algorithme de hachage SHA-2 pour les certificats d'AC)
  - Vérification ou adaptation des traitements cryptographiques des clés privées (signature, authentification et/ou déchiffrement)
  - Vérification ou adaptation des vérifications des certificats présentés par des acteurs distants (traitements cryptographiques, usage des CRL et/ou du service OCSP)
- Des adaptations peuvent être nécessaires en fonction du traitement applicatif réalisé pour récupérer certaines données du certificat.
- Renouvellement des certificats existants pour migrer vers la nouvelle IGC.

Certaines applications, en particulier les serveurs applicatifs, doivent être capables de gérer une cohabitation terrain durant lesquels certains interlocuteurs ont déjà migrés (certificats IGC-Santé) et d'autres non (certificats IGC-CPS2bis)

IGC-Santé : Planning Etape 1

L'ouverture de l'IGC-Santé sur le périmètre certificat logiciel est effective à partir d'avril 2016 :



- Dès T0, il est possible techniquement de délivrer des certificats de test et de production.
- Néanmoins, la communication généralisée pour la commande de certificats de production n'aura lieu qu'à partir de T1 (date à déterminer avec les éditeurs), afin que les éditeurs aient le temps d'effectuer et de tester les développements nécessaires sur leurs applications.
- A T2 : arrêt d'émission de certificats logiciels par la plateforme actuelle (IGC-CPS2bis). Les certificats émis restent valides et utilisables jusqu'à leur expiration – les CRLs continuent à être fournies.

L'étape 2 (intégration dans les cartes CPS des certificats IGC-Santé) commencera début 2017 et fera l'objet d'une communication courant 2016 (2ème trimestre).

IGC Santé : Documentation disponible

Référentiel documentaire IGC-Santé disponible sur le site « intégrateur CPS » :

- Note de présentation générale de l'IGC-Santé :
  http://integrateurs-cps.asipsante.fr/IGC-Sante

- Note technique détaillée sur les impacts et la migration :
  http://integrateurs-cps.asipsante.fr/IGC-Sante-migration

- Autres ressources disponibles :

Merci pour votre attention