



PLATEFORME MUTUALISÉE DE SIGNATURE ÉLECTRONIQUE

Conclusion d'une étude juridico-technique



11 décembre 2013
emmanuelle.prevost@recherche.gouv.fr

Problématique / Contexte ?

- ***Pourquoi vouloir faire des signatures électroniques au ministère ?***
- ***Qu'est-ce que la signature ?***
 - => Valeur juridique
 - => Fiabilité
- ***Par quel moyen technique peut-on signer simplement ?***
 - => peu coûteux,
 - => facile à déployer,
 - => pour tous les groupes d'utilisateurs
- ***Comment doter les applications du SI de fonction de signature ?***
- ***Comment choisir le bon niveau de signature, adapté pour chaque usage et chaque utilisateur de la signature (l'exemple Dem'Act) ?***

Origine du besoin

Dématérialisation entamée il y a 15 ans...

- ***Rationaliser***

- => Simplification (processus, procédures)
- => Optimisation (échanges, flux, suppression de « bruits »)
- => Alignement stratégique et organisationnel

- ***Moderniser***

- => Augmenter la qualité des services rendus
- => Enrichir la diversité des services offerts aux usagers

- ***Sécuriser et offrir des garanties dans les échanges devenus électroniques***

- => Authentification
- => traçabilité
- => authenticité et valeur juridique

- ***Économie d'échelle => gain de productivité et enrichissement à coûts constants***

Enjeu de la signature électronique

- **Moins onéreux en terme de consommation papier**
- **Plus accessible et susciter de l'adhésion des différentes parties prenantes**
 - => même niveau de service pour tous
 - => gare à la fracture numérique
- **Confiance ?**
 - => transparence et sécurisation,
 - => **valeur juridique identique entre document numérique et document papier**
comment transformer la signature d'un document papier ?
 - => offrir des garanties contre : falsification, détournement...
- **Modifier les textes légaux (réglementaires, etc.) de manière à maintenir la réponse au besoin de signature lors du passage au tout numérique ?**

Qu'est ce qu'un Acte, et qu'est ce qui garanti sa valeur ?

- Un acte modifie ou affecte la situation des ses destinataires, ou l'ordre juridique
- Un acte est exécutoire, décisoire ou faisant grief
- Ne sont pas considérés comme acte
 - documents relevant de mesures d'ordre intérieur
 - motion ne donnant pas lieu à délibération
 - rapport
 - note de service ...
- Est considéré comme acte les délibérations d'un CA formalisées

▪ Conditions de forme et de fond :

Mentions :

- Signature de l'auteur de l'acte
- son nom, son prénom
- sa qualité

▪ Transmission et publication

Doit être publié ou notifié pour être exécutoire :

- Acte « non transmissible » : immédiat
- Acte « transmissible » : après transmission à l'AC

Qu'implique la dématérialisation des actes ?

Plate-forme mutualisée de signature électronique : Services offerts

(non exhaustifs)

- ***Signature de documents soumis***

- => à la demande de façon récurrente
- => à la demande de façon ponctuelle
- => via une application cliente

- ***Selon le besoin de synchronisation et/ou le besoin maîtrise du flux***

- => via un parapheur
- => via un web service...

- ***Selon le besoin du niveau d'homologation et au regard du risque de contentieux***

- => authentification forte, exemple carte à puce physique ou clef cryptographique,
- => authentification renforcée, exemple clef OTP
- => autre : QR code

- ***Selon la nature des documents soumis et au regard du risque de contentieux***

- => Signature à la volée / génération de certificat éphémère
- => Carte à puce virtuelle

Quelle signature à mettre en œuvre sur la plateforme ?

- **Scannée, Digitale, Numérique = NON**

- => Pas de lien avec le document signé

- => Pas de prestataire de confiance

- **Cachet électronique = OUI**

- => Dérivé de la signature électronique

- => Identité Machine/Institution

- => Pas d'existence juridique, pas de jurisprudence, mais existence RGS

- => Utilisation ? -> Accusés de réception

- **Électronique simple et électronique sécurisée = OUI**

- => Fonction cryptographique

- => Scelle l'acte et l'identité du signataire

- => Signature électronique simple pour une homologation de niveau RGS une *

- => Signature électronique sécurisée pour bénéficier de la présomption de fiabilité du procédé de signature

Nécessité de la fiabilité de la signature électronique

- **La signature électronique « présumée fiable » protège les acteurs**

=> La fiabilité de ce procédé est présumée, jusqu'à preuve du contraire

Article 4 de la loi 2000-230 du 13 mars 2000

La preuve de la non-fiabilité du procédé de signature est à la charge du contestataire

- **Présomption de fiabilité => Signature électronique sécurisée utilisant :**

=> Dispositif sécurisé de création de signature

(procédé de génération du bi clé de signature et sa mise en œuvre pour signer un condensat de document)

=> Certificat qualifié

=> Utilisation de systèmes et de produits garantissant la sécurité technique et cryptographique des fonctions assurées.

- **CONCLUSION : Rendue possible par les textes de lois depuis mars 2000, la signature électronique est devenue aujourd'hui une nécessité**

Exemple : Application cliente de gestion électronique de processus et dématérialisation des Actes en EPLE : Dem'Act

▪ **Différents types d'accès :**

- => via le réseau Agriates / Racine pour les personnels de l'éducation nationale (instruction, pas fonctions sensibles)
- => via une authentification renforcée pour les signataires, en plus du réseau privé (accès aux fonctions sensibles)
- => via une clef OTP pour tout extérieur (Collectivité Locale, Préfecture ...)

▪ **Exigences fonctionnelles :**

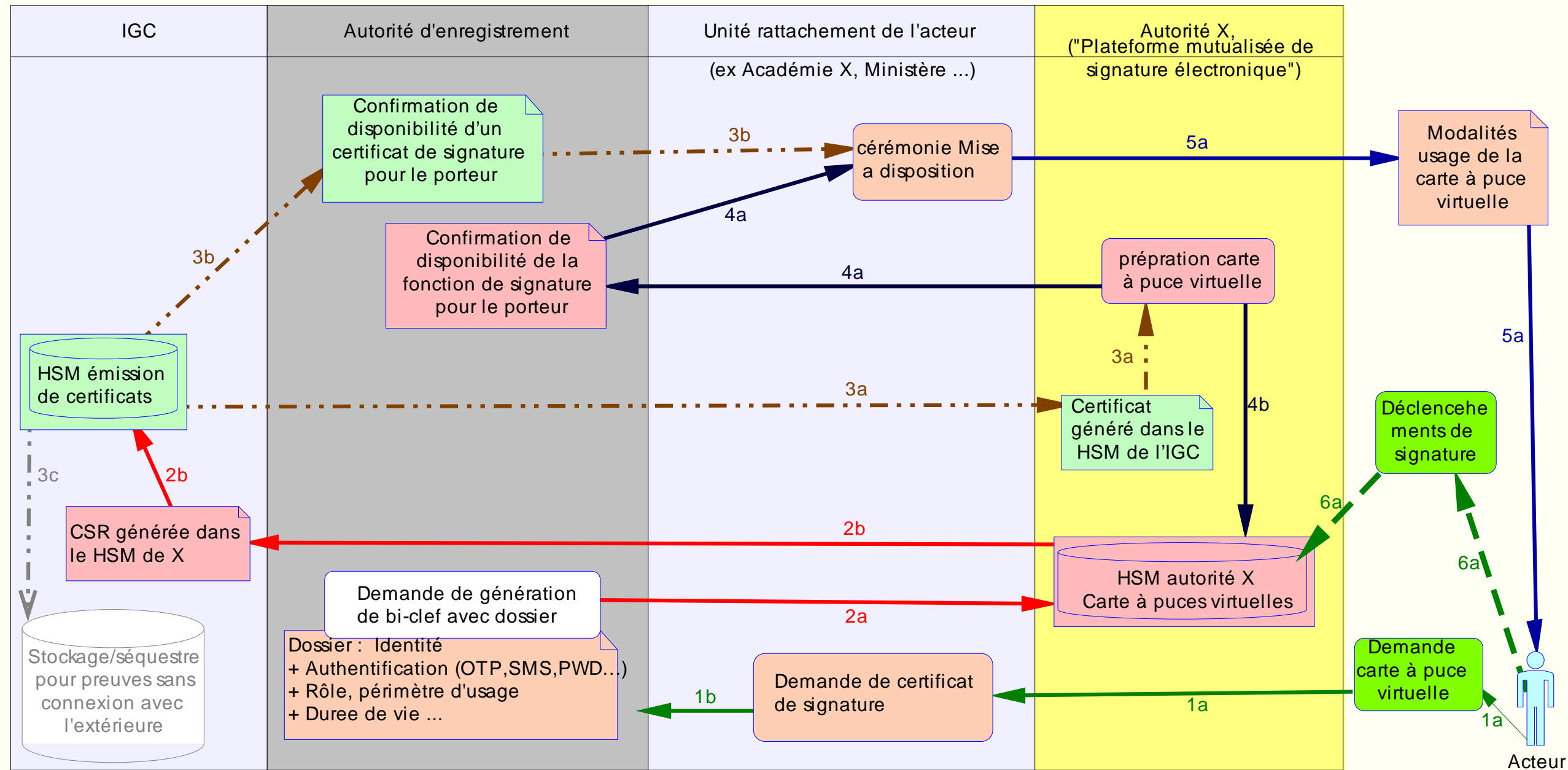
- => Documents générés au format PDF
- => Signature : incorporée au document, signalé par un visuel imprimable et interactif (montrant l'identité et qualités du signataire, et donnant accès au code)
- => Vérification de signature : au sein et hors application
- => Apposition de signature : déclenchée au sein du processus électronique, à distance

▪ **Exigences de sécurité :**

- => RIEN sur poste client (parc non maîtrisé) : ni client lourd/clef crypto., ni magasin de certificat
- => TOUT se passe de serveur à serveur (au sein de flux et parc maîtrisé)
- => PAS DE SORTIE du document soumis à signature tant que le processus n'est pas terminé
 - éviter interception et modification entre déclenchement et apposition
 - ni via le poste client (application de signature / certificat de personne par un procédé local (clef crypto., magasin ...))
 - ni via un système de traitement différé sur la plateforme (par de dépôt dans un parapheur ...)
- => Homologation RGS souhaitée = une étoile ou analogue, avec certificat de personne préalablement enregistrée.

CONCLUSION : BESOIN DU SERVICE « carte à puce virtuelle »

Proposition de mise en œuvre organisationnelle et technique de la carte à puce virtuelle en vue d'une conformité RGS *



Premiers services offerts sur la plateforme et avenir de la plateforme

- **Carte à puce virtuelle, une solution d'avenir** (besoin de création d'une autorité X)

- => Analysée en profondeur pour offrir une réponse aux besoins de Dem'Act en 2014

- => A privilégier pour :

- applications de dématérialisation des circuits / chaînes de validations impliquant la création d'actes
 - nécessitant un besoin de sécurité équivalent au RGS une étoile, et ...
 - nécessitant une logistique modérée et maîtrisée en dépit des diversités de populations et parcs
 - demandes récurrentes

- **Signature à la volée / génération de certificat éphémère** (besoin de création d'une autorité X)

- => Analyse complémentaire sur les contraintes et la portée juridique à prévoir

- => A privilégier pour :

- applications visant des documents non considérés comme des actes
 - demandes ponctuelles et/ ou demandes hors application...

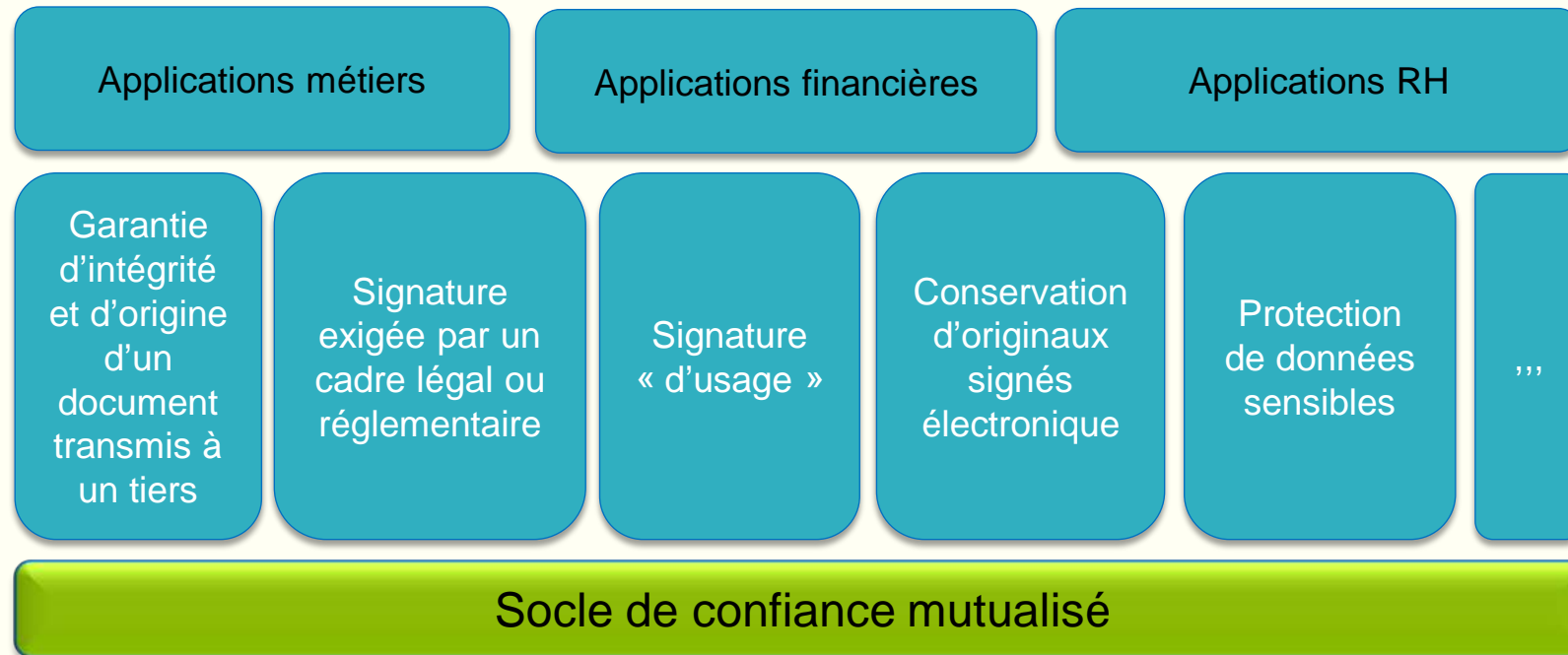
« **Carte à puce virtuelle** » et « **Signature à la volée / génération de certificat éphémère** » = **Complémentaires**

- **Compléments d'analyse (organisationnel / impact et portée juridique) nécessaires pour :**

- => Signature à la volée (conflit de notions : « à la volée » et « enregistrement préalable »)

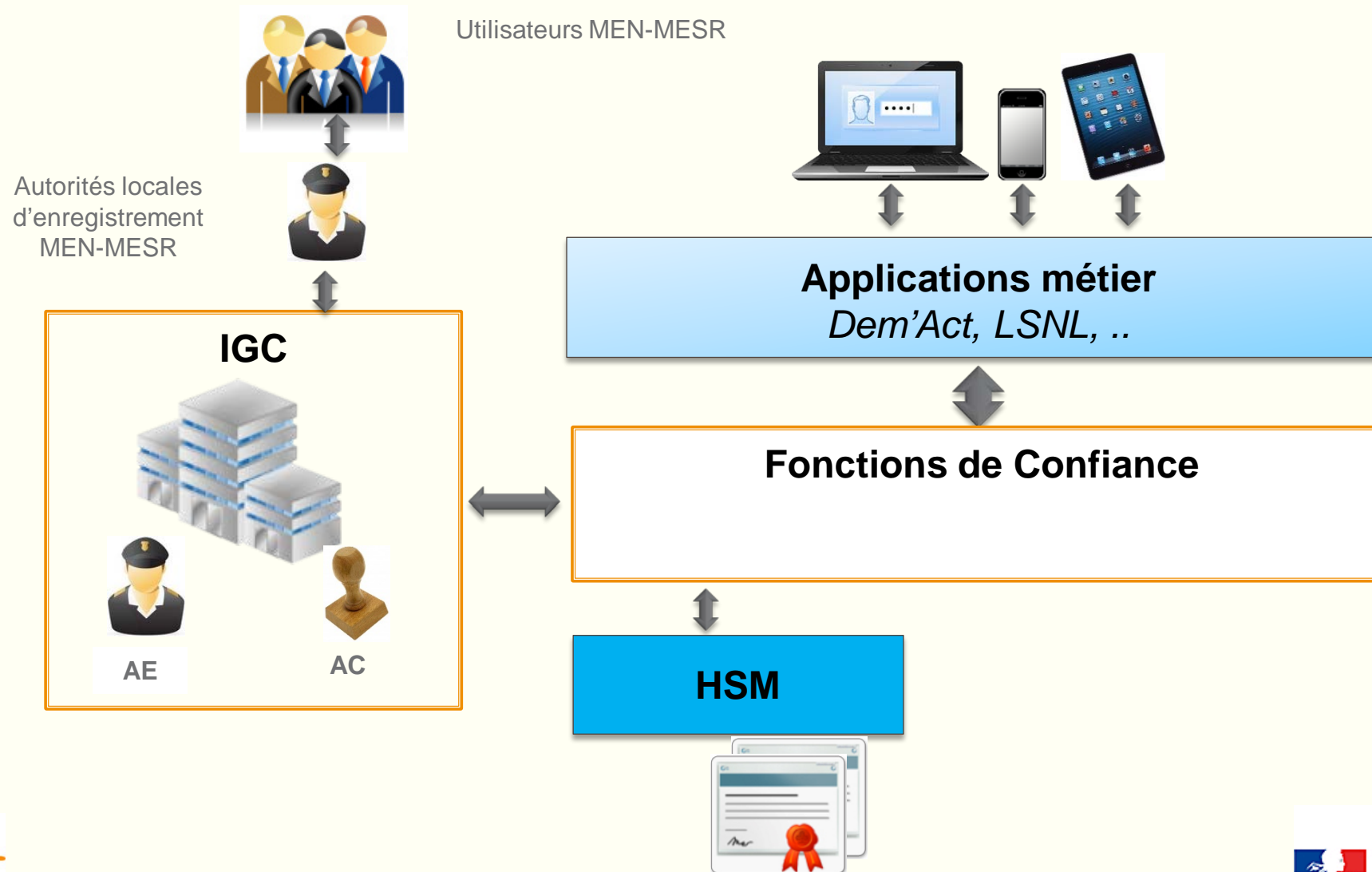
- => Les autres services

Les moyens de mise en œuvre...



- Mise en place d'un **socle technique mutualisé** proposant des services aux applications
- Cadre d'accompagnement des équipes métiers et MOA
- Adaptation des articulations IGC / autorité X (nouvelle autorité administrative) sans lien direct :
 - => pour la mise en place de carte à puce virtuelle, alternative du support physique pour les actes à fort risque de contentieux,
 - => en réponse aux contraintes RGS,
 - => avec nécessité d'arbitrage par le SG, et saisie de l'ANSI.

Plateforme mutualisée de signature électronique => plateforme mutualisée de confiance





PLATEFORME MUTUALISÉE DE SIGNATURE ÉLECTRONIQUE

Travaux réalisés sur la base d'une étude menée avec le concours du cabinet ALAIN BENSOUSSAN AVOCATS et de la société Demaeter

Merci

A retenir : mise en œuvre de la carte à puce virtuelle

Piste pour respecter l'annexe A8 VI 1.2 du RGS:

Carte à puce virtuelle =

=> stockée dans un HSM dédié à son utilisation, hébergé à distance, au sein d'une autorité administrative X, différente de l'IGC.

=> placée sous le contrôle exclusif de l'utilisateur, par opération de déclenchement à distance

Remise des modalités d'accès et d'utilisation = même circuit que celui actuellement en vigueur pour les cartes à puce physiques.

Aucun lien direct entre IGC (émission/création) et l'autorité administrative X qu'est la plateforme (contrôle d'accès et utilisation)

Dispositif transitoire à étudier...

Du point de vue de la sécurité, la signature électronique par carte à puce virtuelle est un excellent compromis approprié à l'application Dem'Act. Du point de vue de la conformité au RGS, cela nécessite une dérogation devant être validée par la commission d'homologation RGS, et auprès de l'ANSI.