Les services de la Plateforme Nationale de Confiance Numérique du Ministère de l'Éducation Nationale

Bruno REINE
MENESR/SG/DNE/B1
61-65 rue Dutot
75015 Paris

Jean-Michel LOPEZ
Pôle PNCN/ Rectorat de Toulouse
75 Rue Saint Roch
31077 Toulouse

Résumé

La dématérialisation et la confiance numérique sont des enjeux clés du secteur public, au cœur de la stratégie de transformation numérique impulsée par l'Etat. Les actions engagées par notre Ministère s'inscrivent dans la réforme de l'État et de la modernisation de l'action publique. Dès 2014, les besoins métiers du MEN, du MESR et de ses établissements ont donné naissance à la Plateforme Nationale de Confiance Numérique du Ministère de l'Education Nationale, totalement opérationnelle pour les besoins du MEN.

La présentation se déroulera en 2 temps. Tout d'abord, nous présenterons en détail les moyens mis en œuvre, les solutions technologiques, l'architecture, l'organisation permettant d'opérer la solution pour répondre aux enjeux métiers de notre ministère. Nous aborderons également les aspects coûts et réglementaires liés au projet et à son exploitation.

Ensuite nous parlerons de la nouvelle offre de service en ligne à destination de l'ensemble de la communauté Enseignement et Recherche, offre élaborée au regard des besoins exprimés par nos RSSI respectifs et portée par notre RSSI National.

Pour conclure, nous exposerons les évolutions envisagées de l'infrastructure, les travaux menés en vue d'une certification eIDAS afin de répondre aux contraintes légales en mesure de signature, d'améliorer le service global et de développer de nouveaux usages.

Mots-clefs

Signature, certificats, coffre-fort, transfert de fichiers sécurisés

1 Introduction

Dans un premier temps nous présenterons rapidement l'Infrastructure de Gestion de Clés (IGC), en exploitation depuis 2014, puis la Plateforme de Confiance Numérique du MEN (PNCN). La PNCN a permis non seulement de délivrer quelques millions de certificats de tout ordre, d'opérer l'IGC France Grilles de RENATER mais aussi de signer tout acte dématérialisé via ses webservices des applications métiers du Ministère.
Face aux demandes récurrentes de besoin de signature personnelle ou cachet ponctuelle via nos certificats ou pas, face au besoin de recherche et de publication de certificats, demandes par ailleurs relayées et élargies par notre RSSI à l'ensemble de la communauté éducative, il a été décidé la mise en place d'un portail de services dédié à la signature en ligne et à la publication de certificats.

A ces fonctionnalités s'ajoutent un accès de type coffre-fort numérique et un outil de transferts de fichiers sécurisé.
In fine, nous évoquerons les démarches de la PNCN dont l'objectif est d'obtenir la certification eIDAS[1] (electonic Identification, Authentication and trust Services) à l'horizon 2021 et les impacts sur le service délivré.

2 La Plateforme Nationale de Confiance Numérique

2.1 Contexte, objectifs et besoins du MEN et du MESR

Les ministères de l'Education Nationale, de l'Enseignement Supérieur et de la Recherche souhaitaient mettre en place une plateforme de confiance numérique portés par une volonté de sécurisation des opérations numériques les impliquant ainsi que leurs établissements sous tutelle.

Cette plateforme est constituée d'une nouvelle infrastructure de gestion de clés, issue de la migration de notre ancienne IGC par une IGC SH-2 à l'état de l'art incluant une branche dédiée au Ministère de l'Enseignement Supérieur et de le Recherche et reposant sur un module HSM (Hardware Security Module)[2] qualifié ANSSI (Bull Proteccio HR (Eal4+)) et de solutions de confiance mettant à profit les certificats délivrés par l'IGC qui donnent la possibilité aux utilisateurs de :

- ✓ signer électroniquement suivant différents canaux et modalités (signature personnelle, signature cachet serveur, signature en mobilité, etc.) ;
- ✓ vérifier les signatures électroniques et les certificats utilisés ;
- ✓ conserver des objets numériques sur long terme avec une vocation probatoire.

Les approches de dématérialisation des échanges permettent, en effet, au Ministère, de répondre à plusieurs objectifs :

- ✓ simplifier les relations et les échanges ;
- ✓ améliorer l'efficacité de l'organisation (approche 'sans papier' et 'sans rupture').

Fonctionnellement, cette plateforme a été bâtie afin de :

- ✓ permette de donner valeur probante aux opérations dématérialisées au travers de l'utilisation de la signature électronique, en conformité avec les exigences du droit français ;
- ✓ pouvoir être simplement intégré par les applications métiers ;
- ✓ pouvoir simplement évoluer pour lui permettre de rester à l'état de l'art et en ligne avec le cadre réglementaire ;
- ✓ permettre d'intégrer les composants logiciels ou éléments de solution déjà existants.

Techniquement, elle propose un système complet assurant, sans qu'il soit besoin d'avoir recours à des documents papiers et garantir:

1 https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-reglement-eidas/

2 https://fr.wikipedia.org/wiki/Hardware_Security_Module

- ✓ l'opposabilité de la preuve ;
- ✓ la validité des documents signés électroniquement ;
- ✓ le support technique et juridique en cas de contentieux.

2.2 Les briques techniques

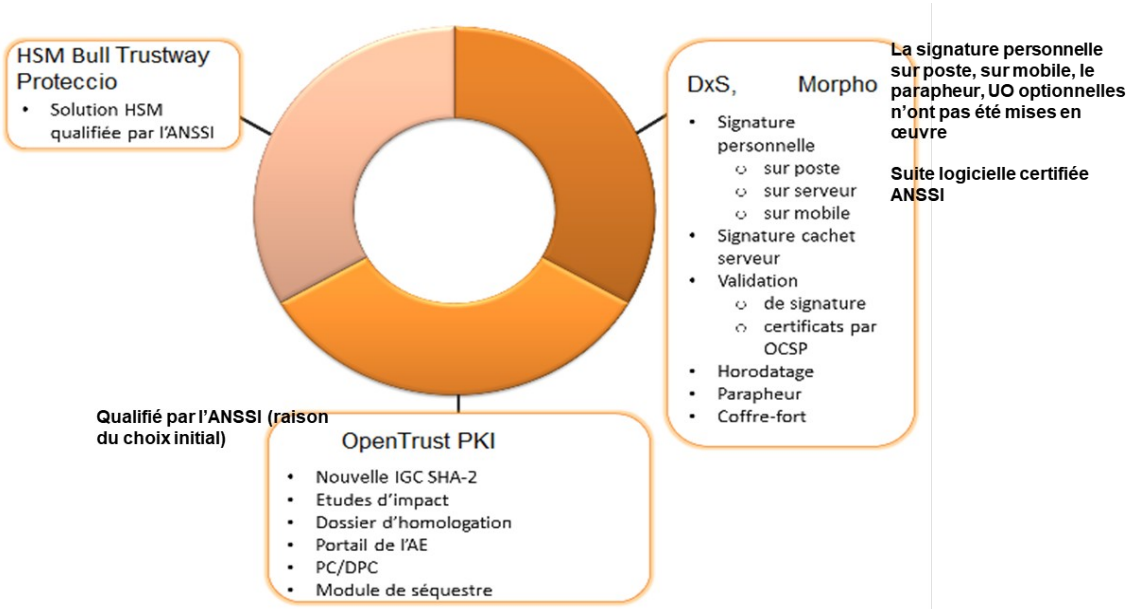

Figure 1 – Les briques techniques

2.3 L'architecture simplifiée

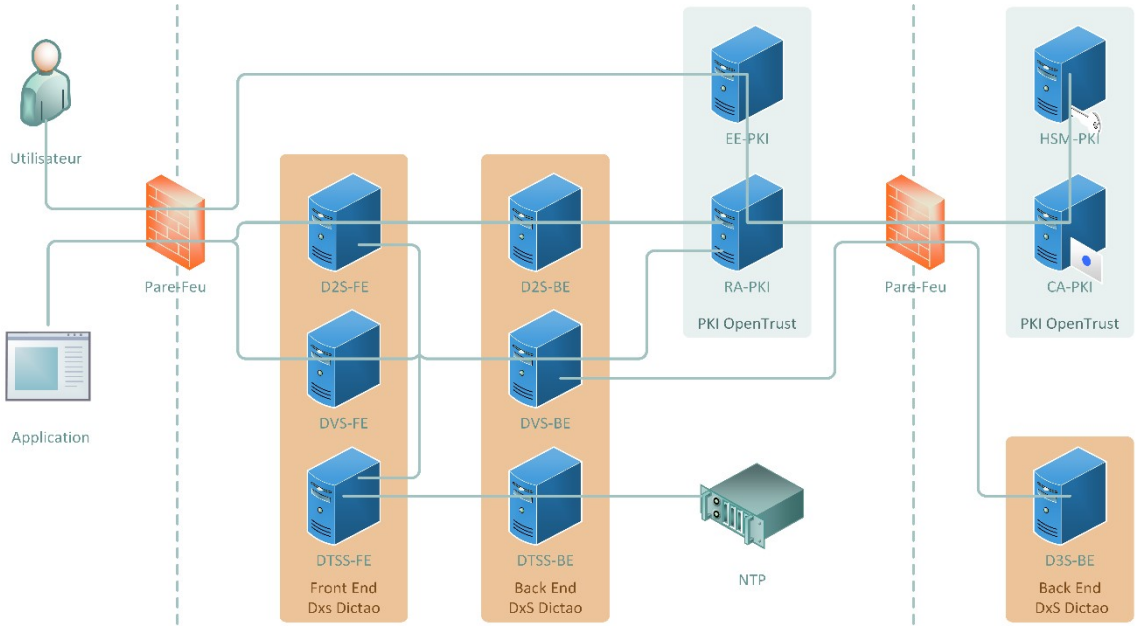

Figure 2 – L'architecture simplifiée

2.4 Le pôle PNCN, ses missions, son hébergement

2.4.1 Ses missions

Au quotidien le pôle assure les tâches :

- ✓ d'exploitation pour le MENESR ;
- ✓ de mise à disposition de l'IGC France Grille ;
- ✓ de mise en place des évolutions fonctionnelles, techniques, sécuritaires ;
- ✓ de développement du portail de services ;
- ✓ d'assistance aux utilisateurs ;
- ✓ de guichet d'entrée aux demandes de certificats Certigna.

Il assiste les maîtrises d'œuvre et maîtrises d'ouvrage :

- ✓ en interne au niveau national par Dema'ct, Chorus, RIO, STRADA, PLACE, LSL, SIRHEN, SAND, CLOE, etc. ;
- ✓ en externe :par les collectivités territoriales, Interministériel, MESR, RENATER, CNRS, …

Il mène en outre une veille technologique et fonctionnelle continue

- ✓ alertes sécuritaires ;
- ✓ homologation au RGS[3] (Référentiel Général de Sécurité), eIDAS , sur signature ;
- ✓ supervision, site Web, démonstrateurs, statistiques, …

2.4.2 Son hébergement

Notre infrastructure occupe un espace dédié, à accès restreint (biométrique et code d'accès), au sein du Data Centre de la DSI du Rectorat de Toulouse.

Son exploitation technique est assurée par de Département des Infrastructures Applicatives de ladite DSI :

- ✓ le cœur de réseau : connectivité, éléments actifs, FW, DNS, …
- ✓ le système : une soixantaine de serveur à ce jour pour moitié physique, baie de stockage, ….
- ✓ la sauvegarde : 40 To globaux, 200 Go quotidiens.

3 https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/

Son exploitation fonctionnelle métier est bien entendu à la charge du pôle

Un autre pan d'exploitation est partagé entre la DSI et le pôle, il s'agit :

- ✓ de la sécurité spécifique (sudo, ansible, …)
- ✓ de la supervision, de la centralisation des logs ;
- ✓ du serveur de temps.

2.5 Ses services

La Plateforme Nationale de Confiance Numérique propose deux services principaux :

- ✓ un service d'Infrastructure de gestion de Clés, : trois sont actuellement exploitées au pôle
  - o une IGC de production pour le MENESR ;
  - o une IGC de pré-production-qualification, ;
  - o une IGC France Grille pour RENATER.
- ✓ Le service socle de signature est quant à lui composé de fonctions:
  - o de signature électronique ;
  - o de validation de signature ;
  - o d'horodatage ;
  - o de coffre-fort numérique.

2.6 Quelques usages

Infrastructure de Gestion de Clés :

- ✓ Notre IGC est utilisée pour la gestion de tout certificat à usage interne au MEN :
  - de type personne (authentification, chiffrement, signature, éphémère, …) sur support logiciel ou matériel ;
  - de type infrastructure (SSL, IPSEC, …).

- ✓ France Grille, anciennement hébergée par le CNRS, l'AC GRID-FR est utilisée pour la délivrance de certificats électroniques X509 pour la sécurisation de l'accès aux ressources des grilles de calculs relevant de l'Enseignement supérieur et de la Recherche publiques et privés en France. Opérée par le pôle, c'est le GIP RENATER qui en assure l'administration.

Socle de Signature :

- ✓ **Dém'act** : La dématérialisation en actes

  Cette application s'adresse aux Etablissement Public Local d'Enseignement [4](EPLE) et aux autorités chargées du contrôle de légalité de leurs actes : les services académiques et, sous réserve de volontariat, les collectivités locales.

  Ce service concerne plus de 8 000 collèges et lycées, 130 services académiques (rectorats et directions des services départementaux de l'Éducation nationale) et l'ensemble des régions et départements.

  Dém'Act est la première application ministérielle à s'inscrire dans le cadre de la plate-forme nationale de confiance numérique (signature électronique : personnelle).

- ✓ **LSL** : le Livret Scolaire Numérique du Lycée

  Afin de répondre à la nécessité de moderniser l'action publique et de faire entrer l'Ecole dans l'ère numérique, le livret scolaire papier, utilisé depuis 1890, est dématérialisé sous la forme du Livret Scolaire numérique du Lycée (LSL) pour toutes les séries des voies générale et technologique et dans toutes les académies.

  C'est lui qui est envoyé signé au jury de délibération concernant le baccalauréat.

4 https://www.education.gouv.fr/cid4526/l-e.p.l.e.-et-ses-missions.html

2.7 Données chiffrées

Des centaines de milliers de certificats ont été émis par nos autorités de certification depuis 2014 pour celles du MEN et 2017 pour celles de France Grille pour un taux de disponibilité remarquable.

AC	Emission
AC_EN_Acces_Distants	6
AC_EN_Infrastructures	2188
AC_EN_Personnes	4261
AC_EN_RPV	918
AC_EN_Scolarite_Formation	11516
AC_EN_Signatures_Ephemeres	3126283

AC	Emission
AC_GRID_FR_Personnels	769
AC_GRID_FR_Robots	20
AC_GRID_FR_Services	1177

Figure 3 – Nombre de certificats émis

Au regard des coûts du marché, l'investissement initial est déjà largement amorti ne serait-ce que sur la partie « SSL » au sens large et les certificats personnes (à hauteur de plusieurs millions d'€).

Le coût de revient estimatif d'un certificat PNCN sur cinq ans est de 1,15 €.

Services	Taux Dispo	Taux Indispo
Plateforme PNCN Globale	96.739%	3.261%
Signature - Socle Signature	96.739%	3.261%
Validation - Socle Signature	97.307%	2.693%
PKI OpenTrust	99.947%	0.053%

Figure 4 – Taux de disponibilité

3 L’offre de services en ligne

L’offre de services du pôle s’enrichit d’une offre de service en ligne

3.1 Les accès

Pour être accessible au plus grand nombre, l’accès se fera via la fédération Education-Recherche de RENATER, toute personne dûment identifiée se verra offrir l’accès au portail de services.

C’est en fonction des éléments fournis par le fournisseur d’identité ad hoc que sera déterminée votre établissement de provenance.

Un annuaire spécifique permettra une gestion des rôles dédiée au portail, toute personne non présente dans cet annuaire se verra proposer les services les plus basiques, elle pourra elle-même s’y abonner.

3.2 Les rôles

Les rôles sont au nombre de cinq: BASE, VIP, MFT, ADMIN.Local, ADMIN.Global et ils peuvent être cumulatifs.

Les éléments du profil de BASE sont communs à chaque profil, à chacun d’eux sont associés des usages.

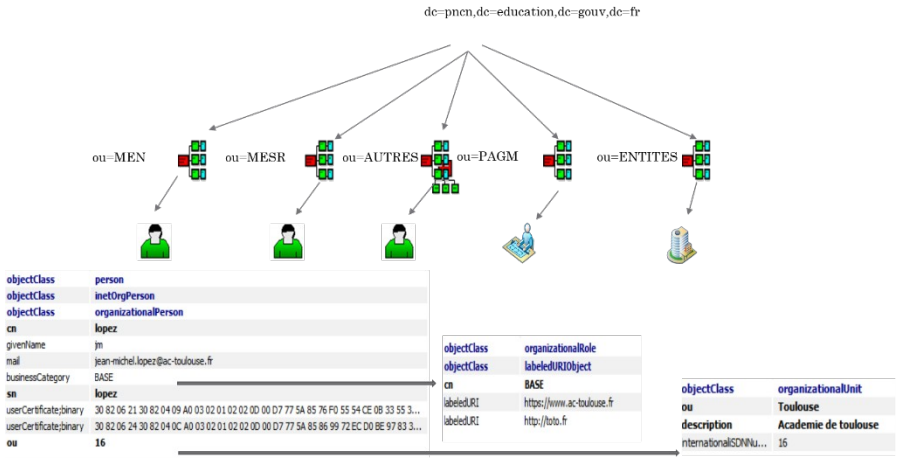

Figure 5 – DIT illustré de l’annuaire du portail

3.3 Les briques et concepts techniques

Outre une infrastructure sécurisée et hautement disponible d’annuaires OpenLDAP, sont utilisés la brique Shibboleth Service Provider ainsi qu’un connecteur SOAP (Simple Object Access Protocol) vers l’autorité d’enrôlement (EE) et l’API DIGICERT.

Pour tout besoin de chiffrement et/ou de signature cachet c’est notre HSM Bull Proteccio HR (Eal4+) qui est sollicité.

3.4 Les services

Figure 6 – Le Portail des Services

3.5 Le service de signature en ligne

Basé sur le projet DSS (Digital Signature Services) de la commission européenne tout comme celui de PLACE, il est accessible au profil de BASE et permet la signature personnelle sur poste client quelle que soit la provenance du certificat de signature (MENESR ou commerciale).

3.6 Recherche/publication de certificats

Comme son nom l'indique ce service permet de rechercher un certificat en fonction de l'adresse mail de son détenteur ou de publier son ou ses propres certificats s'ils émanent de notre propre IGC, ou de celle de DIGICERT, manuellement pour tout autre fournisseur.

C'est lors de la première publication d'un certificat que l'entrée annuaire d'un utilisateur est créée.

Ce service fait aussi partie du bouquet de services du profil BASE

3.7 La signature cachet institutionnelle

Utilisable uniquement par les détenteurs du profil VIP, elle pourra être utilisée pour apposer ce type de signature à tout document officiel hors workflow métier.

Un certificat commercial pourra au besoin être associé à chaque entité.

3.8 Le coffre-fort numérique

Du simple objet numérique au plus complexe (DublinCore ou encore propriété intellectuelle), ils pourront être déposés au coffre et lus par tout VIP. Seuls ses propres dépôts lui seront accessibles.

3.9 Le service de transfert de fichiers sécurisé

A destination des domaines métiers (RSSI, DEC, …) sous profil MFT, il peut éventuellement être autorisé aux VIPs. Il permet non seulement le dépôt chiffré de fichiers à transférer, les documents au format pdf pourront être également signés, mais aussi leur transfert avec une option de chiffrement. Les certificats de signature et biclés de chiffrement sont générés et stockés sur les HSMs de la plateforme.

Ce service est basé sur la solution MFT de la société EQUISIGN, déjà utilisée dans d'autres Ministères et/ou cabinet de Ministre.

3.10 Les services de boîtes à outil

Ils permettent à tout Administrateur Local de rechercher, d'ajouter, de supprimer une feuille de type personne, ils lui permettent de leur attribuer tout profil à l'exception de ceux d'Administrateur Local et Global.

L'Administrateur Global pour sa part aura les mêmes services qu'un Administrateur Local étendu à l'attribution du rôle Administrateur Local, il pourra en outre créer tout nouveau profil, toute nouvelle entité et la rattacher à un Administrateur Local.

4 Evolutions

4.1 Réglementaires EIDAS

Le règlement eIDAS est exécutoire et s'impose donc aux pays de l'UE. Il est entré en vigueur le 1er juillet 2016.

Dans le cadre de la dématérialisation de la commande publique, l'arrêté du 12 avril 2018 redéfinit les modalités d'utilisation de la signature électronique et du certificat qualifié nécessaire pour que le signataire d'un marché public puisse être considéré comme ayant valablement donné son consentement.

Cet arrêté opère la transition entre le certificat de signature électronique conforme au référentiel général de sécurité (RGS), précédent standard, et le certificat « eIDAS » prévu par la réglementation européenne.

Depuis le 1er octobre 2018, les acheteurs publics doivent se doter d'une signature électronique avancée reposant sur un certificat qualifié, conforme au règlement européen n°910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques (eIDAS). La signature peut être qualifiée, au sens du même règlement. (Arrêté du 12 avril 2018 sur l'utilisation de la signature électronique dans les marchés publics).

C'est donc le cas de PLACE et CHORUS pour lesquels nous délivrons des certificats. Mais tous devraient l'être.

Le certificat de signature utilisé selon le standard RGS reste cependant valable jusqu'à son expiration (2021).

La certification eIDAS permet en outre de faire partie de la liste EUTL (European Union Trusted Lists), liste publique des fournisseurs TSP (Trust Service Provider) actifs et existants spécifiquement accrédités pour fournir les niveaux les plus élevés de conformité avec le règlement de l'Union Européenne sur les signatures électroniques. Cette appartenance peut être vue comme un palliatif à la sur-signature dans l'Union Européenne.

4.2 Impacts

Au regard de ces contraintes, un vaste chantier de refonte du corpus documentaire existant est en cours, il sera complété de tout nouveau document nécessaire, nous en profiterons pour être aussi conforme au RGPD.

Un effort supplémentaire est à apporter à l'auditabilité et de la traçabilité des processus d'exploitation sous l'égide de notre RSSI et du pôle SSI de notre Ministère.

Un vaste projet de sécurisation de notre infrastructure a débuté, il doit nous conduire de deux branches (IGC, socle) hautement disponibles sur le data centre du Rectorat de Toulouse à une branche dans chacune des salles du site d'hébergement étendu du Ministère de l'Agriculture à Auzeville et de la réplication d'une d'entre elles sur le site des Douanes à Osny couvrant ainsi les problématiques de PCI/PRI ou PCA/PRA.

Figure 6 – Les différentes phases de la sécurisation

Les futures infrastructures sont en cours de déploiement ou seront déployées, sécurisées et exploitées par les Centres de Ressources Techniques du MEN.

A ce jour, l'infrastructure physique est en cours de finalisation sur le data centre du Ministère de l'Agriculture, dès que la migration sera opérationnelle nous lancerons l'audit en vue de la certification eIDAS et parallèlement sera installé le site d'Osny.

5 Conclusion

Cette présentation est destinée avant tout à présenter nos services à notre communauté. Le service Portail en ligne est et sera accessible à tous au même titre que le sont ceux de Renater. Le MEN souhaite contribuer à l'effort collectif, en apportant son savoir-faire dans le domaine de la signature électronique et de l'usage des certificats.