Esup-Signature : une plateforme open-source pour la dématérialisation des actes administratifs

David Lemaignent
Ingénieur d'études
Pôle études et développement
DSI - Université de Rouen Normandie

Résumé

Esup-signature est une application ayant pour but la dématérialisation et la simplification des circuits de visas et de signatures (parapheurs électroniques).

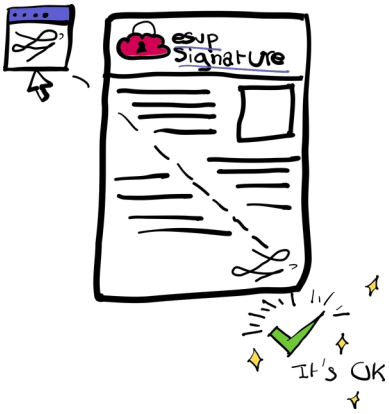
Esup-signature permet de signer des documents à l'aide de certificats électroniques ou par simple apposition d'une image dans un PDF. La prise en charge de cette signature électronique est assurée par le socle logiciel « DSS Signature », mis à disposition par la Commission Européenne. Ceci confère à la plateforme la compatibilité avec la certification eIDas (requise pour la signature des marchés publics, etc.).

L'objectif principal d'esup-signature est de mettre à disposition un micro-service permettant à un établissement d'intégrer la signature numérique au sein des services institutionnels. De plus esup-signature gère les circuits de signature dans une optique « zéro papier ». Pour tendre vers une dématérialisation intégrale des processus, l'application propose un module permettant de saisir en ligne des formulaires PDF simples et normalisés. Toutes ces fonctions sont paramétrables via un backoffice complet ou appelables automatiquement via web-service ou via planificateur.

Esup-signature s'appuie sur des technologies communes aux établissements de l'Enseignement Supérieur et de la Recherche que sont Shibboleth (fédération d'identité Renater), LDAP (supann) et TCS (Trusted Certificate Service) de Renater. Cela fait de lui un outil parfaitement adapté à l'écosystème d'un ESR.

Mots-clefs

dématérialisation, signature, parapheur électronique, formulaire, open source, consortium ESUP-Portail



1 Introduction

En 2019, l'Université de Rouen Normandie (URN) s'est fixée pour objectif la dématérialisation des flux de documents circulant dans les parapheurs mais également tout type de documents identifiés dans des processus métiers (ordres de mission, bons de commandes, marchés, etc.). Dans ce cadre, une étude des outils existants a été conduite, ainsi qu'une réflexion sur l'opportunité de développer une solution autour du projet européen « DSS Signature » (et des librairies PDF.js et PDFBox).

Avec l'appui du **consortium ESUP-Portail1**, l'URN a initié le développement d'une application de signature et de gestion de parapheur électronique, pleinement intégrée à son système d'information, adaptée à ses besoins de dématérialisation des procédures administratives, et répondant aux besoins associés (visas, signatures calligraphiques , certificats électroniques, etc.).

Nous présentons, dans cet article, les différentes fonctionnalités de l'outil permettant de répondre aux besoins des établissements. Une deuxième partie précisera certaines notions techniques propres à l'outil, ainsi que les modalités de sa mise en œuvre.

2 Esup-Signature : bien plus qu'un simple outil de signature

2.1 Bienvenue sur esup-signature !

L'accès à l'outil est soumis à une authentification s'appuyant sur CAS, Shibboleth ou encore sur un système d'OTP (One Time Password) pour les personnes extérieures à l'établissement. Au besoin, l'interfaçage est également possible avec FranceConnect.

L'authentification réalisée, l'utilisateur découvre la page d'accueil comportant des accès à un tableau de bord ainsi qu'à différents outils, dont un système de contrôle de validité de documents signés. Une iconographie moderne permet d'initier de nouvelles demandes de visas, de signatures, via des circuits ou des formulaires. L'utilisateur dispose en outre d'un aperçu des demandes qu'il a à signer. En cliquant sur son nom en haut à droite, l'utilisateur peut paramétrer son environnement (profil). Cela lui permet, entre autres, de déposer une ou plusieurs images de sa signature qu'il pourra apposer ultérieurement sur les documents à signer (avec ou sans tampon).

1 https://www.esup-portail.org/

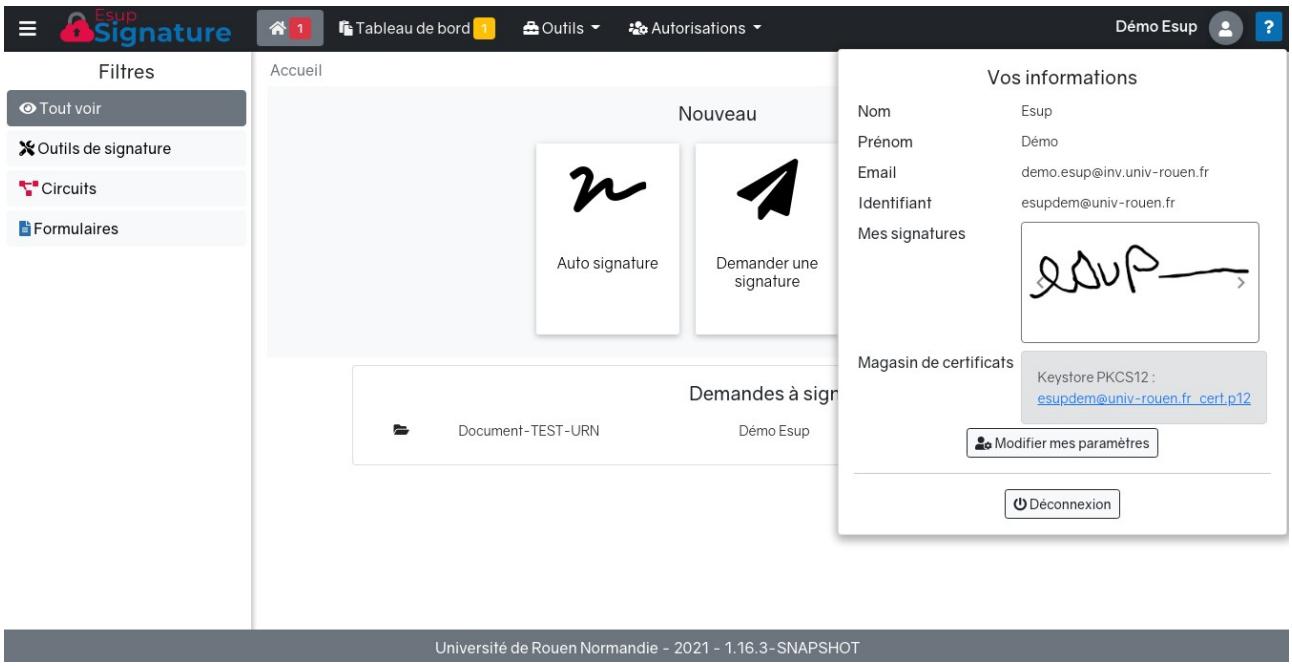


Figure 1 – Page d'accueil et le panneau du profil utilisateur

2.2 La signature

Bien entendu, la fonction principale d'esup-signature est de signer différents types de documents, directement depuis une interface web moderne et conviviale.

Même si esup-signature permet de signer tous types de documents (à l'aide de certificats électroniques), le principal usage rencontré aujourd'hui reste l'apposition de signatures visuelles (dites calligraphiques) sur des fichiers de type PDF (esup-signature gère aussi des fichiers au format image, en les convertissant automatiquement en PDF).

Les utilisateurs ont la possibilité de déposer des documents sur la plateforme, soit pour les signer eux-mêmes (auto signature) soit pour en demander la signature à un ou des destinataires.

Pour signer les demandes, esup-signature propose une interface riche permettant de consulter, d'annoter, et de placer la ou les signatures dans un document. L'atout principal de l'outil est de mettre à disposition ces fonctionnalités sans recours à une application lourde, accessible via un simple navigateur web ; ce service est très vite devenu incontournable lors des confinements liés à la crise sanitaire.

Dans le cadre de l'utilisation du service de parapheur (circuit), l'interface propose un suivi visuel des étapes du circuit en affichant, dans la barre de gauche, les signataires de chaque étape ainsi qu'un code couleur en fonction du statut (en attente, signé, refusé, etc.).

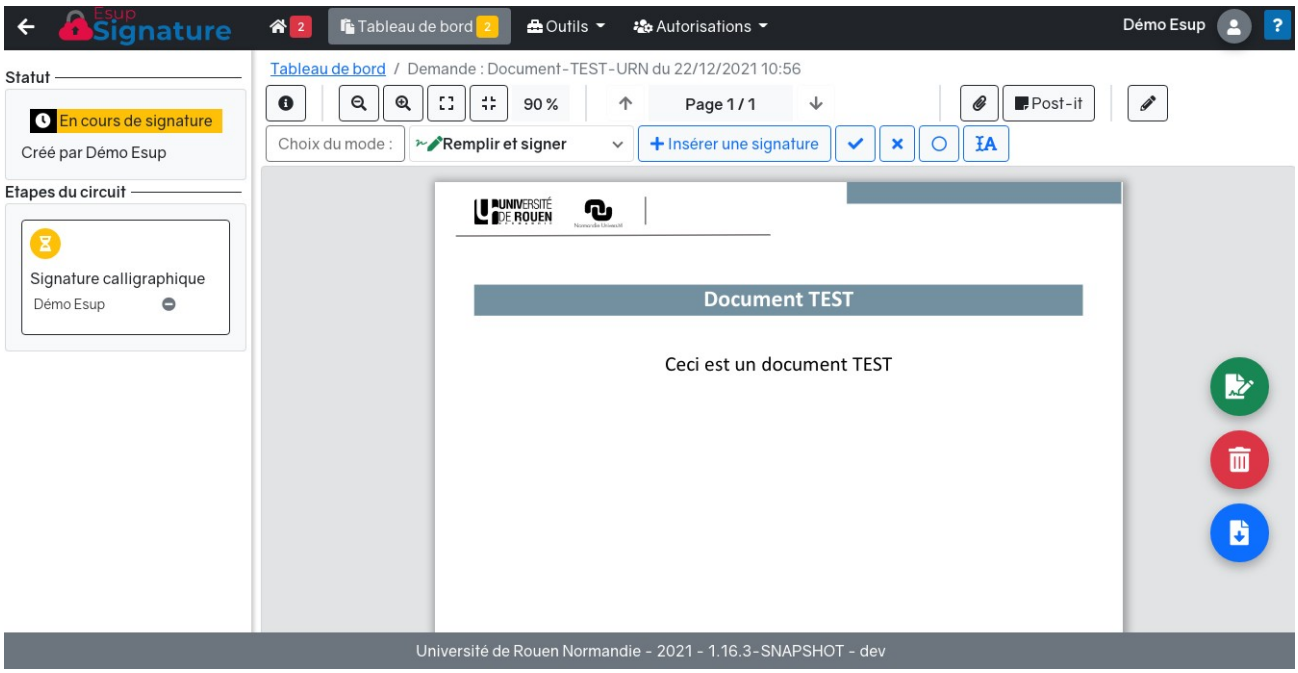


Figure 2 – Interface de signature

2.3 Les parapheurs

Esup-signature offre également des fonctionnalités de parapheur électronique.

En premier lieu, l'application permet le dépôt de plusieurs documents dans une même demande de signature. Les documents se matérialisent alors par autant d'onglets sur l'interface de signature. A l'instar des dispositifs papier, les demandes ainsi créées vont ensuite suivre des circuits de visas ou de signatures, librement configurables et paramétrables au sein de l'outil.

Du circuit à *1 étape*, pour une demande simple, au circuit à *n étapes*, l'application propose une grande finesse dans le paramétrage. Citons par exemple :

- la possibilité de renseigner plusieurs signataires à une étape donnée (avec signature requise ou optionnelle) ;
- le niveau de signature exigé à chaque étape du processus (visa visuel, visa caché, signature calligraphique, signature via certificat électronique, etc.).

Ces paramètres sont accessibles à tout utilisateur de l'application .L'implémentation d'une gestion de rôles permet de déclarer des administrateurs qui disposent de possibilités de paramétrage étendues.

À chaque étape, les signataires sont avertis par mail d'une demande à signer. Lorsque tous les documents d'une demande sont signés (ou refusés !), le créateur de la demande est prévenu par mail de la fin du circuit.

2.4 Les formulaires

Pour aller plus loin dans le processus de dématérialisation des actes papier, rapidement, a été retenue l'idée de proposer des formulaires directement au sein du produit. Dans la mesure où esup-signature intégrait toutes les fonctions de manipulation des PDF (via PDFBox, pdf.js), il est apparu naturel d'exploiter encore davantage les fonctionnalités des « PDF Forms » (décrites et documentées dans le format PDF).

Concrètement, un administrateur peut ainsi générer un formulaire dans l'application, à partir d'un simple fichier PDF contenant un formulaire, élaboré facilement, à partir de LibreOffice, par exemple.

Ce formulaire est alors associé à un circuit de signature. De ce fait, la saisie de certains champs (y compris les champs de signature) peut être restreinte ou requise à certaines étapes du processus (et par voie de conséquence, à certains participants).

Le formulaire est ensuite mis à disposition d'une population cible donnée (définie par l'administrateur) sous forme d'une tuile sur la page d'accueil de l'utilisateur.

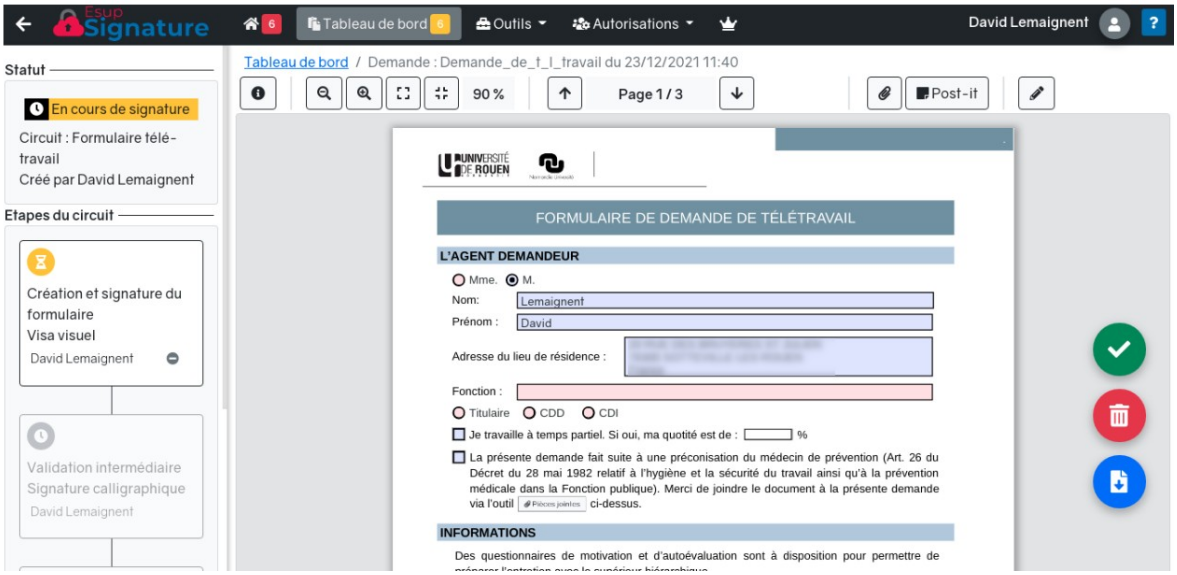


Figure 3 – Exemple de formulaire hébergé par esup-signature

De plus, l'intégration native d'esup-signature au système d'information local permet automatiquement et simplement de pré-remplir certains champs du formulaire en fonction de l'utilisateur connecté, lui évitant les ressaisies classiques si fastidieuses (nom, prénom, adresse, etc.).

2.5 Une intégration native au SI de nos établissements

Pour les utilisateurs déclarés dans le SI, esup-signature peut s'appuyer sur l'annuaire LDAP (et les attributs SUPANN associés), permettant la complétion rapide et automatique de certains champs des formulaires.

En parallèle, le produit est très ouvert et prend d'ores et déjà en charge les protocoles *smb*, *cmis et vfs*, lui permettant de récupérer automatiquement des documents à signer ou de déposer des documents signés en fin de circuit sur des plateformes (file-systems, ged, etc.) distantes.

Enfin la mise à disposition de *web-services* permet à des applications tierces de solliciter esup-signature pour y injecter un document à signer, démarrer un nouveau formulaire pour un utilisateur défini ou récupérer un document signé.

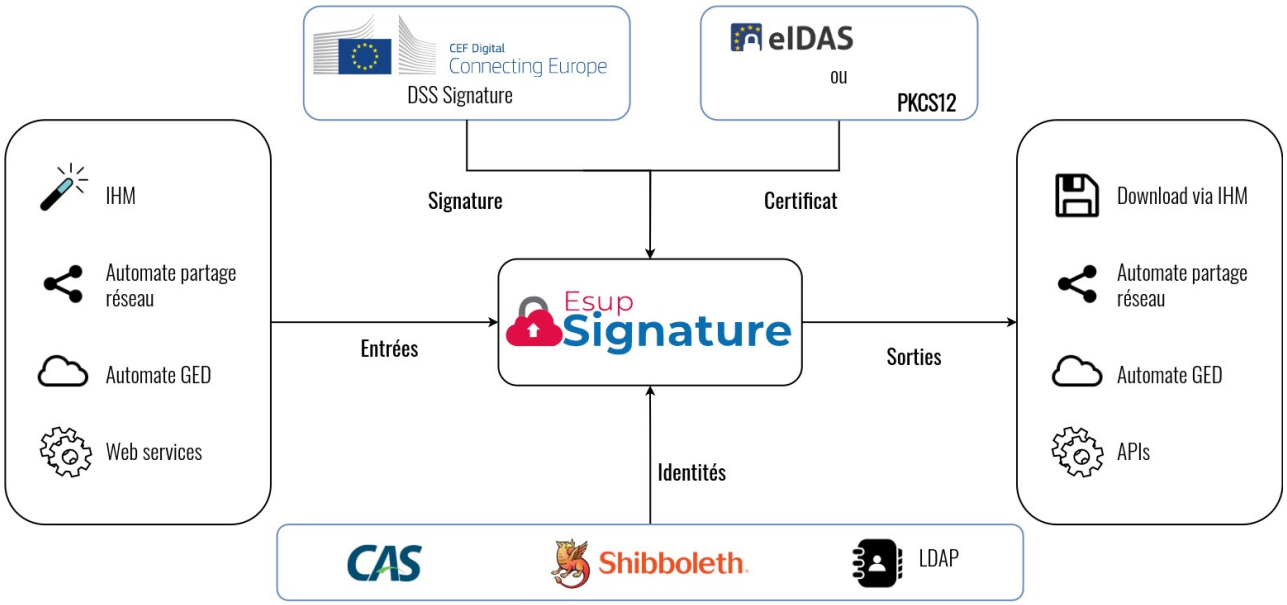


Figure 4 – Écosystème autour d'esup-signature

2.6 Des retours d'expérience

Depuis 2019, esup-signature est utilisé quotidiennement au sein de l'Université de Rouen Normandie. Lors du premier confinement (printemps 2020), la fonction de formulaire à été très sollicitée permettant à l'exécutif de signer à distance, et valider les demandes de déplacement des personnels.

Depuis sa mise en production, plusieurs milliers de documents ont été signés via la plateforme dont une partie correspondent à des processus totalement dématérialisés à l'aide de formulaires. Citons :

- les demandes de télétravail ;
- les procurations pour les élections ;
- les ordres de mission.

Le processus de signature des bons de commandes a été totalement dématérialisé et automatisé à l'aide du planificateur d'esup-signature. Ce dernier récupère les bons de commande issus de SIFAC dans un répertoire réseau défini et l'adresse aux signataires en fonction de métadonnées (gestionnaire, ordonnateur, etc.) présentes dans le document PDF généré.

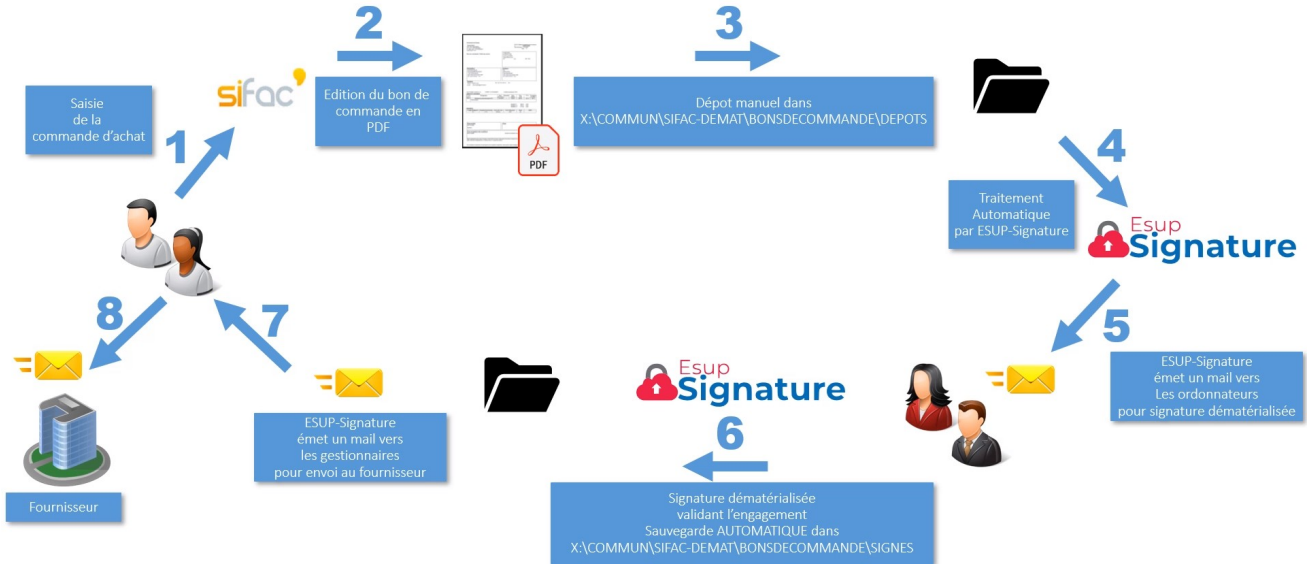


Figure 5 – Circuit complet des bons de commande à l'URN

3 Et sous le capot ?

3.1 L'authentification

L'authentification repose sur le composant logiciel *Spring Security*. Après authentification, les utilisateurs sont identifiés à l'aide de l'EPPN (eduPersonPrincipalName) à l'exception des extérieurs pour lesquels le numéro de mobile est utilisé (ou encore le « sub », pour FranceConnect).

Si l'on souhaite que l'instance d'esup-signature soit accessible à toute la communauté ESR, il convient de configurer l'authentification par Shibboleth. Dans ce cas, un contrôle est effectué sur l'EPPN en le comparant au domaine local pour déterminer s'il s'agit ou non d'un utilisateur de l'établissement. Dans le cas d'une instance ouverte seulement aux utilisateurs locaux, il suffit de configurer l'authentification via CAS.

Toutefois, une autre option disponible est l'authentification via OAuth 2. Elle peut être utilisée dans le cadre du recours au service FranceConnect. Dans ce cas, plusieurs possibilités s'offrent à l'utilisateur en fonction des modes d'authentification configurés.

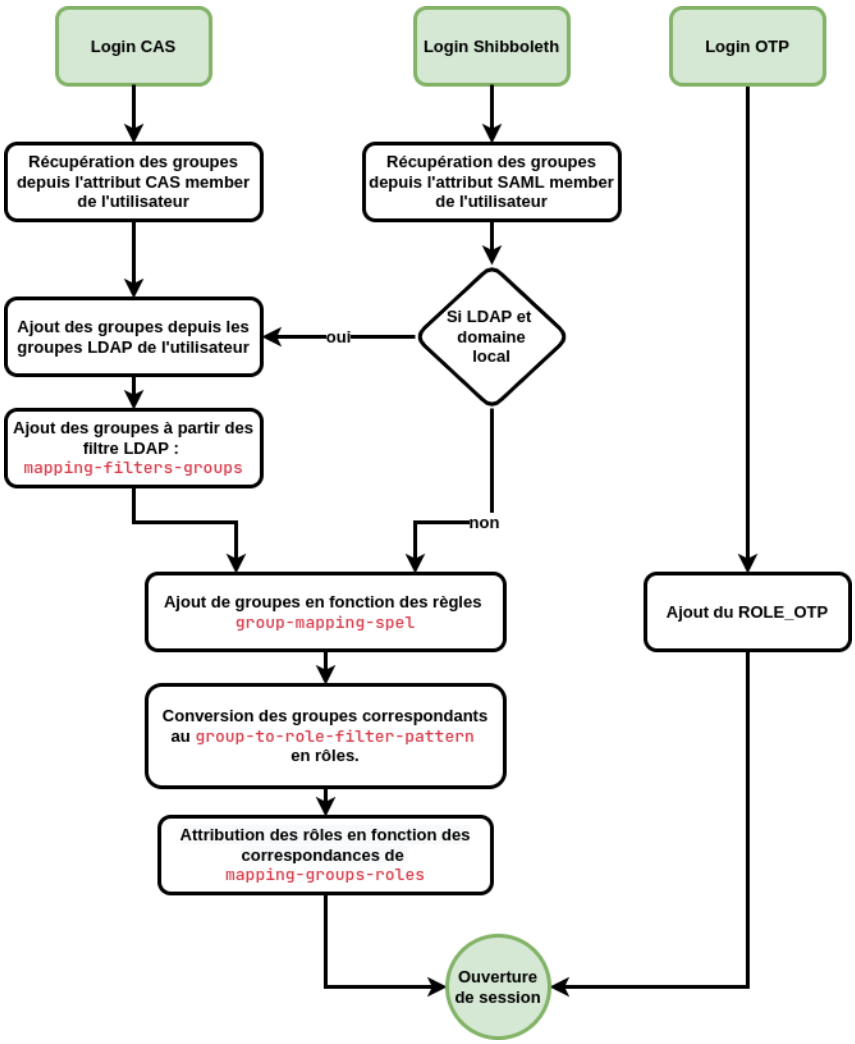


Figure 6 : Les différents cas d'authentification

Sans le recours à FranceConnect, l'authentification des personnes extérieures est possible à l'aide de l'implémentation d'un mécanisme dit OTP (*One Time Password*), proposé par esup-signature.

Lorsque l'on saisit le mail d'un destinataire, esup-signature détecte s'il s'agit d'un mail externe ou non :

- si Shibboleth est configuré, un mail est qualifié d'externe si le domaine n'est ni celui de l'établissement ni un des domaines présents dans la liste de la fédération Renater ;
- si CAS est configuré, tous domaines différents de celui de l'établissement est considéré comme externe.

Quand un destinataire est déterminé comme externe, l'application demande de saisir le numéro de téléphone mobile du signataire. Ce dernier reçoit alors un mail contenant un lien unique lui permettant d'accéder temporairement à esup-signature. Classiquement, grâce au mécanisme OTP, il reçoit sur son mobile un code, lui aussi, unique, à saisir lors de la connexion.

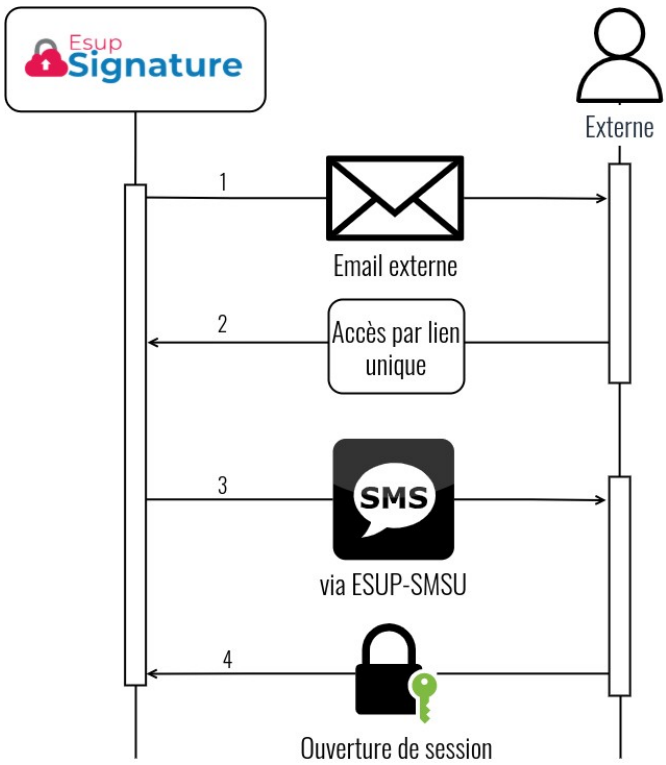


Figure 7 : Connexion OTP

3.2 Les différents types de signature (DSS Signature en action)

En ce qui concerne la signature électronique, esup-signature se repose entièrement sur la librairie DSS Signature, mise à disposition par la Commission Européenne. **Cette librairie, écrite en Java/Spring, a, en grande partie, motivé le projet esup-signature, car elle garantit la conformité des signatures électronique vis à vis du règlement de l'union Européenne sur l'identification électronique (eIDas).**

Une signature eIDas, appelée **signature qualifiée,** est exigée pour la signature des marchés publics. Pour pouvoir effectuer une telle signature, on affecte au signataire patenté un certificat eIDas, embarqué sur un support cryptographique matériel (dit *keystore USB*). Esup-signature, s'appuyant sur DSS Signature, permet l'utilisation d'un tel dispositif via l'installation du logiciel NexU, installé sur le poste client, de manière transparente. L'utilisateur passe par esup-signature comme à son habitude mais il est alors sollicité pour saisir le mot de passe de sa clé cryptographique. En ce sens, esup-signature peut être perçu comme un moyen simple d'intégrer DSS Signature (en tant que micro service) dans nos établissements.

Esup-signature ne se limite pas aux certificats eIDAS, mais propose aussi le recours à des *keystores logiciels* (sous forme de fichier PKCS12). Dans ce cas, l'utilisateur peut déposer son keystore (de fait, non eIDas) dans son profil. Il peut ensuite l'utiliser librement pour signer électroniquement des documents n'exigeant pas le niveau eIDas ; on parle alors de processus de **signature avancée**. Comme tous les documents déposés dans esup-signature, le certificat est stocké en base de données. Il reste cependant sécurisé par la *passphrase* que l'usager doit saisir à chaque nouvelle signature.

Enfin, pour offrir une plus grande souplesse et répondre à des cas d'usages classiques ne nécessitant pas un niveau de signature avancée ou qualifiée (**signature simple**), il est possible d'apposer une image de sa signature directement sur un document. Dans ce cas, le document n'est pas scellé par un certificat. Néanmoins, esup-signature conserve toutes les traces des actions effectuées et propose une page de contrôle de visibilité publique, renforçant notablement la validité du dispositif.

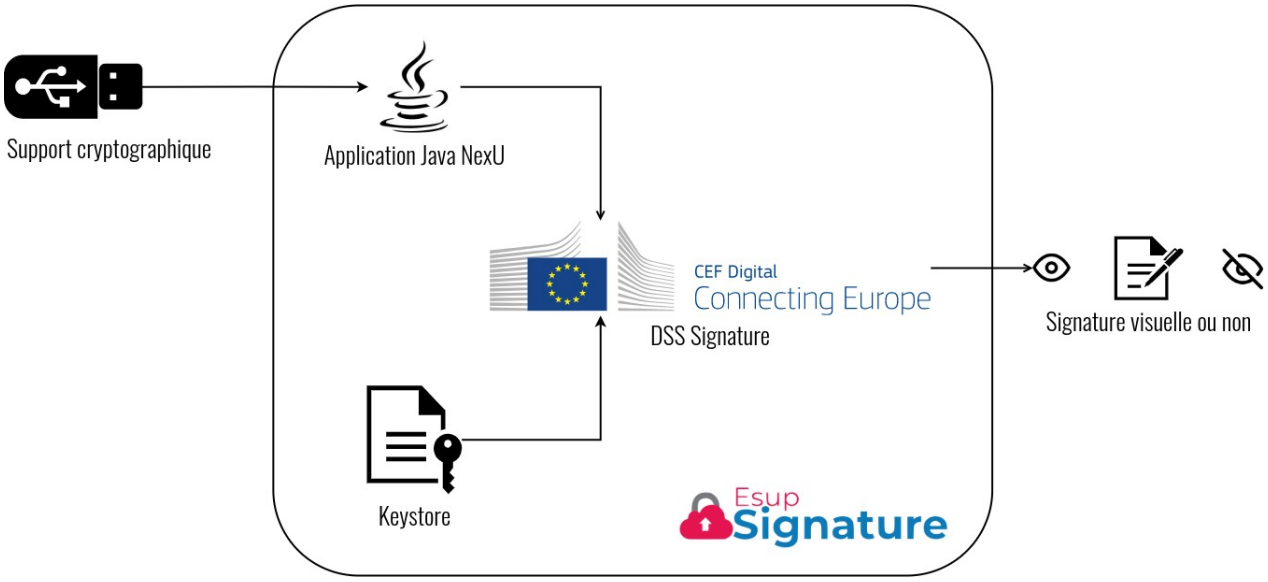


Figure 8 : Signature DSS

Par-delà la signature, DSS est aussi utilisé pour contrôler la **validité** de documents signés, qu'ils soient d'origine extérieure à l'établissement ou signés avec esup-signature.

La page officielle du projet DSS Signature :

https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Digital+Signature+Service+-++DSS

3.3 Cycle de vie des documents dans esup-signature

De manière classique, les documents n'ont pas vocation à demeurer définitivement dans esup-signature2. Dès lors, un certain nombre de mécanismes permettent d'exporter/archiver les documents hors de la base de données d'esup-signature.

Les principaux états que peuvent prendre les demandes de signature sont : en cours, signé, refusé, terminé, exporté et archivé.

2 esup-signature n'est pas une GED !

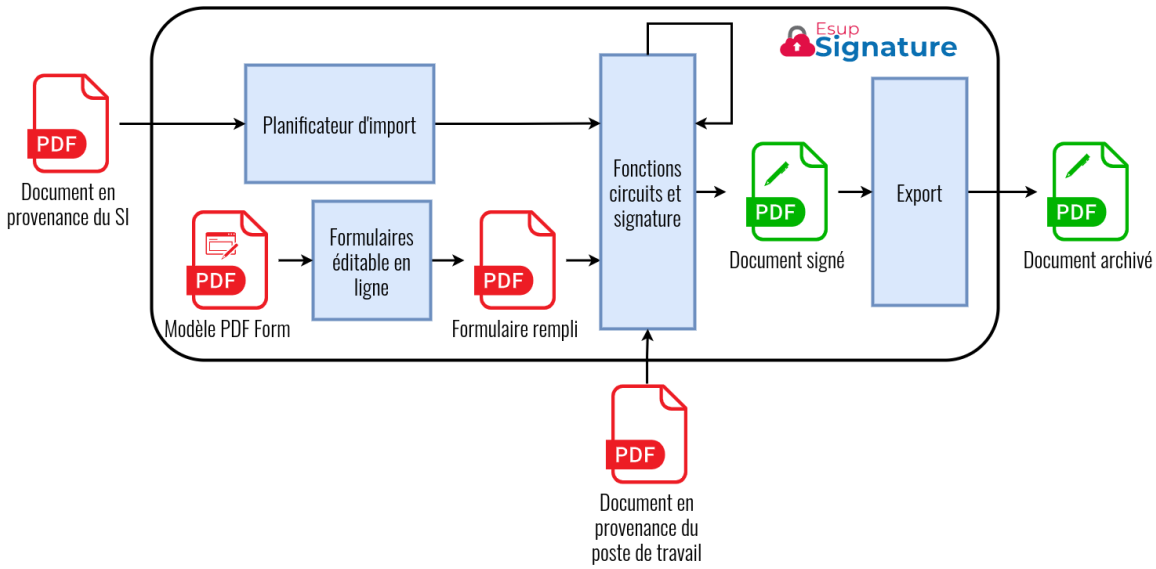


Figure 9 : Cycle de vie des documents dans esup-signature

3.4 Les circuits « administrateur »

Un utilisateur peut se construire et utiliser ses propres parapheurs (circuits) à l'aide d'un assistant pas à pas. Esup-signature lui permet de créer des circuits de signatures puissants, dont les paramètres pour chaque étape sont :

- la liste des signataires ;
- le type de signature ;
- la signature requise ou optionnelle à une étape donnée du processus.

Les administrateurs peuvent, eux, créer des circuits dont les paramètres sont encore plus élaborés. Citons :

- la configuration des autorisations sur les circuits (« qui peut initier tel ou tel circuit ?»), à l'aide de rôles ;
- la configuration des entrées/sorties pour une récupération et/ou un dépôt automatique des documents (via smb, etc.) ;
- la possibilité donnée aux utilisateurs de modifier les participants à une étape donnée ;
- l'activation d'une fonction d'étapes indéterminées (ajout d'étape à la volée lors d'un processus défini).

Un parapheur peut être instancié de plusieurs manières :

- l'administrateur peut mettre à disposition une tuile en page d'accueil à une certaine population. Elle permet de déposer manuellement des documents pour créer un nouveau parapheur qui suivra le circuit pré-défini ;
- l'administrateur peut paramétrer un emplacement source (partage réseau SMB, ou GED compatible CMIS) dans lequel le planificateur d'esup-signature vient récupérer les documents qu'il injecte dans un circuit donné ; cette méthode générant une demande par document ;

– enfin par le recours à des *web services* afin de déposer un document et instancier un circuit depuis une autre application.

3.5 Les formulaires basés sur *PDF Form*

Comme vu précédemment, esup-signature propose de mettre en ligne des formulaires basés exclusivement sur le format PDF. À l'Université de Rouen Normandie, nous utilisons LibreOffice pour construire nos formulaires et les convertir au format PDF. Parfois, le recours à un éditeur PDF spécifique est parfois requis pour une bonne gestion des champs signature.

Pour créer un nouveau formulaire, l'administrateur dépose simplement le PDF et l'associe à un circuit construit préalablement. Esup-signature parcourt alors tous les champs du formulaire pour se constituer un modèle de stockage et repérer les emplacements de signature. L'administrateur associe ensuite chaque champ de donnée à une ou plusieurs étapes, et associer chaque champ signature à une seule étape du circuit.

Esup-signature gère différents types de champs, tels les champs texte simple, numérique, date et heure, liste déroulante, checkbox, bouton radio.

A l'instar des circuits, l'administrateur peut affecter un formulaire à une population donnée, via l'affichage d'une tuile en page d'accueil. Il est aussi possible d'instancier un formulaire de manière automatique à l'aide d'un web service. *Exemple : une application tierce de gestion du temps lançant un formulaire de demande de CET pour le compte d'un utilisateur désigné.*

Une fois créé, le formulaire se comporte comme un document qui va suivre un circuit, dans lequel les champs de saisie sont accessibles en fonction de l'étape courante.

Pour chaque champ, il est possible de configurer une valeur pré-remplie en fonction de l'utilisateur courant comme les noms, prénoms ou toute autre donnée de l'utilisateur rendues accessibles à esup-signature. En général, les données issues de l'annuaire (notamment les champs supann) doivent suffire. Cela dit, il est possible d'implémenter d'autres sources de données (SIRH, etc.).

3.6 Quels moyens pour la mise en œuvre ?

Esup-signature n'est pas proposé en mode hébergé, il doit donc être installé sur un serveur de l'établissement. Ceci permet de faciliter une parfaite intégration avec le système d'information local.

L'installation d'esup-signature requiert une bonne connaissance des environnements Maven, Git, PostgreSQL, CAS et/ou Shibboleth. Pour l'exploiter au mieux, étendre le champ fonctionnel du produit (implémenter de nouvelles sources de données, etc.) et potentiellement proposer des corrections ou améliorations (via *pull-requests*), des compétences Java, Spring et Javascript sont nécessaires.

L'application, de type *Spring Boot*, reste toutefois simple à installer. Si les pré-requis sont satisfaits, un seul et unique fichier de configuration est à paramétrer. Reste alors la compilation du projet à l'aide de Maven. Lors de la compilation, un jeu de tests contrôle la validité de la configuration. L'application peut ensuite être déployée dans un serveur d'application *Tomcat*, voire être lancée de manière autonome.

Un espace dédié sur le wiki reprend toutes les informations détaillées concernant l'installation, l'exploitation et les usages d'esup-signature [1].

Le code source est librement accessible sur le dépôt Github du consortium ESUP-Portail à cette adresse : https://github.com/EsupPortail/esup-signature

Nous conseillons fortement le recours à GIT pour récupérer les sources du projet, maintenir un historique de ses configurations, et éventuellement proposer des améliorations ou corrections via des *pull-requests*. Là est aussi tout l'intérêt d'un projet libre partagé.

4 Des perspectives d'évolutions

4.1 Blockchain EBSI

Un atout majeur d'esup-signature est de proposer un mode de signature simple et puissant au travers de la signature calligraphique. La priorité vis à vis de ce type de signature va être de maximiser sa valeur probante. D'ores et déjà, cette signature s'appuie sur l'authentification de l'utilisateur ainsi que sur la conservation fine de journaux d'actions. De plus, ces preuves sont consultables librement via une page dédiée d'esup-signature.

Grâce au projet de blockchain européenne, de nouvelles opportunités s'ouvrent, dans la mesure où celle-ci proposera de « notarier » des documents. Ceci permettra aux utilisateurs d'esup-signature de déposer des empreintes (*hashes*) de documents signés, de manière transparente, dans la blockchain européenne. La plateforme européenne propose ensuite un module de recherche permettant de contrôler, à partir d'un document, son intégrité, ainsi que les dates et signataires de celui-ci.

4.2 Signatures d'établissement

Pour avoir recours à un niveau de **signature avancée**, les signataires doivent avoir recours à un certificat électronique (X509). Cette logistique technico-technique impose des manipulations fastidieuses aux utilisateurs finaux (génération d'un certificat sur une plateforme tierce, importation du fichier dans le profil esup-signature, etc.).

Ici, l'idée serait de proposer l'utilisation d'un certificat d'établissement afin de valider (par scellement) le document pour le compte d'un utilisateur de la plateforme. Une autre approche consisterait à générer, à la volée, un certificat temporaire (à l'aide d'un outil comme OpenXPKI) pour signer à la volée avec un certificat au nom du signataire. Dans ce cas, se pose *potentiellement* le problème de l'autorité racine du certificat émis, ne permettant pas la validation totale de la signature dans une liseuse PDF grand-public, type Adobe Reader. Une autre alternative consisterait à trouver un prestataire (moyennant rétribution), délivrant à façon, de manière dynamique, au nom du signataire, un certificat personnel valide.

5 Que retenir ?

La signature électronique, et plus largement la dématérialisation, est un sujet d'actualité pour l'ensemble des établissements de l'ESR. Pour le traiter, l'Université de Rouen Normandie développe une solution libre, clef en main, intégrée, efficace et pragmatique : esup-signature.

Souvent, les outils du marché mettent en avant les technologies avancées de signature électronique ; celles-ci peuvent en effet être facilement valorisées dans le cadre d'une prestation. Si esup-signature propose également ces possibilités en embarquant le projet DSS, il s'efforce aussi de prendre en charge, simplement, une écrasante majorité de documents ne requérant pas un niveau de signature avancée ou de signature qualifiée. Pour ce faire, esup-signature fournit un arsenal d'outils opérationnels et parfaitement intégrés au Système d'Information d'un ESR.

Pour que ce projet corresponde aux attentes de la communauté de l'ESR, l'URN investit beaucoup de temps et de moyens dans son développement et sa mutualisation via le consortium ESUP-Portail. Rapidement en effet, un certain nombre d'établissements se sont montrés intéressés par esup-signature ; certains l'ont adopté dès les premières versions disponibles ! Bien sûr, la crise sanitaire a servi de catalyseur dans l'adoption rapide d'esup-signature, mais cela prouve aussi la capacité de la solution à répondre à des besoins existants et émergents, notamment ceux imposés par le recours au télétravail.

Esup-signature est un ensemble de composants logiciels visant pragmatiquement à faciliter la dématérialisation de tous les processus gravitant autour de la signature : parapheurs, actes administratifs, structurés ou non. Cependant, cela n'exonère en rien le travail à conduire en amont pour identifier et déterminer les flux de documents éligibles à ces process. Si esup-signature peut être un élément constitutif d'un projet de dématérialisation d'un établissement, ne serait-ce qu'en tant que micro-service de signature, son usage doit se faire en fonction du niveau de criticité et de complexité des processus à mettre en œuvre.

6 Remerciements

Nous souhaitons remercier le consortium ESUP-Portail pour son soutien dans ce projet et plus particulièrement Canica Sar (Université Paris 1 Panthéon-Sorbonne), Henri Jacob (Université de Rennes 1) et Fabien Rocher (Université de Caen Normandie) pour leurs tests et leur participation à l'amélioration d'esup-signature.

§ Bibliographie

1 Documentation esup-signature sur le wiki ESUP-Portail :
https://www.esup-portail.org/wiki/display/SIGN

2 Article dans "la collection numérique" de l'AMUE :
http://www.amue.fr/fileadmin/amue/systeme-information/documents-publications/la-collection-numerique/N_10__Des_usages_numeriques_multiples_et_varies_dans_ESR.pdf

3 Assises du CSIESR 2021 : CSIESR - Esup-Signature - 14-10-2021.pdf