FAQ

Questions générales

Qu'est-ce qu'Esup-Signature ?

Esup-Signature est une application web qui propose un espace utilisateur permettant :

- d'envoyer des documents à la signature
- de signer
- de démarrer des processus prédéfinis
- de remplir des documents en ligne

L'outil prend en charge les fonctions suivantes :

- signature de tous types de documents (avec plusieurs niveaux de signature),
- gestion de circuits de signatures (parapheur électronique),
- dématérialisation de documents (avec un système de pré-remplissage des champs),
- gestion des délégations et des alertes mails,
- contrôle de validité de documents signés,
- import/Export de documents.
- web services permettant une forte intégration dans le SI

Vous pourrez retrouver des informations sur cette présentation faite aux Esup Days : https://www.esup-portail.org/wiki/download/attachments/813400065/ED29_AP2020--04-ESUP_signature.pdf?version=2&modificationDate=1580911121000&api=v2

"Je n'ai pas Esup Portail", est-ce que je peux installer Esup-Signature ?

OUI.

Esup-Signature est une application indépendante de l'ENT EsupPortail.

Esup-Signature est soutenu par le consortium EsupPortail. Il est distribué sous license open sources Apache v2 (et donc gratuitement)

Quelles sont les briques techniques d' Esup-Signature ?

Esup-Signature est développé en Java / Spring Boot. Le stockage des données et des documents est assuré par PostgreSQL.

Les signatures électroniques ainsi que leurs validations sont prises en charge par la bibliothèque DSS Signature de la Commission Européenne, voir : https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/DSS+releases

La documentation de DSS Signature est disponilble ici : https://ec.europa.eu/digital-building-blocks/DSS/webapp-demo/doc/dss-documentation.html

L'horodatage des signatures électroniques est assuré par un serveur dont l'adresse est configuré, par défaut, avec le service proposé par la Belgique et présent d'origine dans le projet DSS Signature.

`http://tsa.belgium.be/connect`

Attention toutefois, ce service est limité à 100 jetons par jours.

Voici une liste de services de timestamps gratuits disponibles (attention, certains ont des restriction d'utilisation) : https://gist.github.com/Manouchehri/fd754e402d98430243455713efada710

Il est, bien sûr, possible d'utiliser un autre service en modifiant l'adresse dans la configuration. Plus de détails ici : Configuration#dss

La conversion des documents est faite via Ghostscript. L'affichage et la manipulation des PDF sont assurés par PDF.js et PDFBox

Peut-on avoir une présentation des fonctionnalités ou une démonstration d'esup-signature ?

La signature électronique est un sujet hautement d'actualité, encore plus depuis la crise sanitaire qui a mis en exergue les avantages de la dématérialisation des procédures de parapheurs classiques.

Aussi, beaucoup d'établissements sont intéressés par esup-signature et souhaiteraient une présentation de la solution.

Solution libre, esup-signature propose dès maintenant quelques documentations en libre accès, et son installation est possible dès aujourd'hui.

Pour ce qui est d'une présentation fonctionnelle, vous pouvez :

- retrouver les vidéos de présentation de EsupDays 29 autour de la signature électronique : la 2ème partie est consacrée à esup-signature (même si celui-ci a depuis beaucoup évolué déjà) mais la 1ère partie est également très intéressante à visionner car elle remet en perspective la problématique de signature au sein d'un établissement de l'ESR.
- tester rapidement esup-signature au travers de son instance de démonstration accessible depuis ce lien : https://esup-signature-demo.univ-rouen.fr
- vous inscrire dès maintenant à EsupDAys 30 depuis le lien suivant https://www.esup-portail.org/conference - le programme n'est pas encore précisé, mais il est possible qu'esup-signature y soit présenté !

Esup-Signature est en production dans un établissement ?

Esup-Signature est en production à l'université de Rouen Normandie depuis avril 2020. La crise sanitaire aidant, en l'espace de 2 mois ce sont près de 2000 documents qui ont été signés via cette application.

Lors de cette première phase de mise en production, les documents qui ont été signés par cette application sont les documents courants signés simplement habituellement sous format papier et ne demandant pas une validité juridique forte (pas d'actes juridiques, pas de documents susceptibles d'être contestés par recours, ...).

Ainsi ont été signés de manière dématérialisée via esup-signature des déclarations de déplacements, bons de commandes, entretiens professionnels, demandes de congés, justificatifs, ...

Actuellement plusieurs établissements (on en compte plus d'une vingtaine en 2024) utilisent esup-signature en production. Certains d'entre eux signent leurs marchés publiques à l'aide de clés cryptographiques.

Pourquoi utiliser Esup-Signature plutôt qu'un autre outil ?

Si vous mettez en œuvre un projet de signature électronique dans votre établissement de l'ESR, choisir Esup-Signature peut être une option.

L'offre sur le marché est de plus en plus riche, chaque solution met en avant ses possibilités techniques avancées de signatures, l'argument phare d'actualité étant le respect du règlement eIDAS.

Sont disponibles ainsi des solutions (en SaaS ou non) telles que (liste non exhaustive) : i-Parapheur, DocaPost, YouSignOn, DocuSign, CertSign, HelloSign, EchoSign, RightSignature, SignNow, Universign, Oodrive, Tessi, EchoSign, AdobeSign, ...

Le choix peut être difficile. Il faut cependant (re)considérer l'usage que l'on souhaite faire. Que souhaite-t-on signer ? Que doit-on signer dans l'établissement avec une signature conforme à eIDAS ?
La mise en œuvre d'une signature conforme eIDAS est lourde (en terme de matériel, certificat, archivage) et donc coûteuse. Mais elle ne doit être considérée que pour les actes qui le requièrent, c'est à dire pour une part minime de l'ensemble des actes de signatures réalisés dans un établissement et par peu d'agents !
Notez que (même si Esup-Signature le permet grâce à DSS) ce type de signature très pointue ne nécessite cependant pas forcément un outil supplémentaire aux outils que vous utilisez quotidiennement ! Une signature de ce type peut être mise en place directement avec le logiciel Adobe Reader : https://helpx.adobe.com/fr/sign/using/digital-signatures.html

Si les aptitudes à permettre d'être conforme juridiquement à la réglementation en vigueur sont intéressantes, un outil de signature doit aussi (surtout ?) permettre, par sa souplesse et son agilité, de s'intégrer dans votre établissement et de répondre aux besoins fonctionnels en matière de parapheur.

Par rapport aux solutions du marché, Esup-Signature a par construction plusieurs avantages :

- porté par notre communauté de l'ESR, il permet de se retrouver autour d'un socle commun, d'échanger et mutualiser les travaux
- pensé pour s'intégrer dans un ESR,
    - il intègre le support de l'authentification CAS, Shibboleth
    - il se base sur un annuaire LDAP / Supann
    - il est candidat à s'interfacer avec les logiciels de l'environnement ESR
- ESUP-Signature est un logiciel libre qui vous appartient sans restriction, cela apporte de multiples avantages :
    - indépendance vis à vis d'un prestataire et d'un logiciel propriétaire, dont la pérennité ne peut être garantie
    - confiance dans le logiciel dont vous disposez de l'ensemble des codes sources et documentations (véritablement ouvert, vous n'avez pas à nous envoyer un mail pour obtenir le code source : vous pouvez l'obtenir directement dès maintenant depuis le github Esup)
    - pas de coût de licence, de coût par signature, ...
    - possibilité de tester et mettre en place l'outil simplement
    - ...

Actuellement le choix d'Esup-Signature implique cependant un investissement humain, sans accompagnement d'un prestataire de service vendant une solution générique et clef en main.

Peut-on disposer d'un accompagnement à l'installation et à l'utilisation

Le projet esup-signature fait parti de l'incubateur Esup. À ce titre il est distribué par le consortium ESUP-Portail avec les assurances minimales suivantes :

- identification des acteurs du projet ;
- application des patches de sécurité nécessaires à l'intégrité des systèmes sur lesquels ils sont installés ;
- application des correctifs nécessaires aux anomalies découvertes et empêchant un fonctionnement normal de l'application.

Questions réglementaires

Quels documents peuvent être signés avec Esup-Signature ?

Esup-Signature permet de signer tout type de document, l'usage du format pdf est très recommandé, ce pour des questions d'archivage, de standardisation, du support natif de la technologie de signature et horodatage.

Esup-Signature intègre la solution DSS de la Commission Européenne qui est l'implémentation de référence pour proposer des signatures électroniques respectant le règlement eIDAS (electronic IDentification, Authentification and trust Services). Établi en juillet 2014, c'est ce règlement qui fixe techniquement les conditions de validité des signatures électroniques dans l'Union Européenne et donc en France (https://fr.wikipedia.org/wiki/Electronic_identification_and_trust_services).

Configuré en ce sens, allié à des certificats électroniques avancés spécifiques (et nécessitant des clefs électroniques via périphériques matériels) Esup-Signature peut permettre de signer des documents à valeur juridique forte au même titre que les solutions du marché qui sont spécialisées sur ces aspects de signatures juridiquement incontestables (avec archivage en sus).

Cependant, la grande majorité des documents signés dans nos établissements par la majorité des agents ne nécessite pas un niveau de sécurité aussi élevé.
Ces signatures (ou visas) demandent souvent d'être consultées ou signées par un certain nombre d'agents, avec une certaine souplesse, en suivant un cheminement de validation dans le contexte du référentiel utilisateurs du Système d'Information de l'établissement.

Esup-Signature peut se révéler très adapté à ces cas d'usage, notamment par rapport à d'autres solutions non créées et pensées pour être intégrées dans un Système d'Information d'un Établissement de l'Enseignement Supérieur et de la Recherche.

Je dispose d'un certificat RGS** ou RGS*** (EIDAS). Esup-Signature me permet-il de signer des documents officiels avec ce type de certificats ?

Oui. La partie signature est prise en charge par DSS Signature (commission européenne).

Les clés cryptographiques (RGS...) sont prises en charge par l'application Esup-DSS-Client associée à DSS pour accéder aux keystores locaux et saisir la passphrase (voir Esup-DSS-Client)

À l'université de Rouen la signature est concluante avec un certificat obtenu auprès de certinomis : Offre SERVEUR 2 étoiles / Cachet 2 étoiles G2 - sur carte. L'autorité de certification est reconnue par la trustlist française sous le nom "Certinomis - Prime CA G2"

Le materiel reçu est une clé Feitian Technologies, Inc. SCR301 avec une carte Gemalto pris en charge par OpenSC (pilote "idprime : Gemalto IDPrime")

Vous trouverz la liste des matériels supportés ici : https://github.com/OpenSC/OpenSC/wiki/Supported-hardware-%28smart-cards-and-USB-tokens%29

Les certificats cachet d'établissement sont aussi pris en charge, coté serveur, pour verrouiller des documents en fin de circuit (pas de passphrase à saisir).

Quels types de certificats sont pris en charge par Esup-Signature ?

Deux solutions sont possibles pour les certificats personnels :

- déposer un keystore (magasin de clés au format PKCS12) dans son profil d'Esup-Signature. Le magasin sera stocké dans la base d'Esup-Signature. Le keystore est protégé par un mot de passe, demandé à chaque recours à la signature électronique d'un document,
- vous pouvez utiliser tous les certificats reconnus par le magasin de certificats de Windows et OpenSC à l'aide de l'application Esup-DSS-Client (Esup-DSS-Client)

Pour les certificats cachet, il faudra brancher la clé cryptographique sur le serveur hébergeant esup-signature. Après configuration, la signature avec ce certificat sera disponible de 2 manières :

- par l'utilisateur s'il possède le rôle ROLE_SEAL
- automatiquement en fin de circuit et fonction de la configuration d'esup-signature

Quel contrôle de validité pour les documents signés ?

Voici comment esup-signature contrôle la validité des signatures :

- Toutes les signatures faites avec un certificat non eIDas sont considérées comme invalide ou partiellement invalide. Cependant cela ne remet pas en cause la valeur juridique de ce type de signature (signature avancée), le document est bien vérouillé.
- Il n'y a pas de contrôle de révocation lors de la signature d'un document avec un certificat que n'est pas dans la trustlist européenne, non eIDas (ni lors de l'ajout du certificat dans le profil de l'utilisateur)
- DSS-Signature contrôle la révocation lors la vérification d'un document signé par un certificat eIDas (signature qualifiée)

En conclusion, le seul moyen d'avoir une signature 100% valide lors de la vérification (tous les voyants au vert), c'est de signer avec un certicat eIDas non révoqué et un timesamps, tous deux présents dans la trustlist européenne (voir "Statut DSS" dans la partie admin)

Est-il possible de "sur-signer" un document déjà signé ?

Oui, il est possible d'ajouter des signatures supplémentaires à un document PDF déjà signé. Les normes AdES, en conformité avec eIDAS, définissent les critères des signatures électroniques avancées, permettant l'ajout de nouvelles signatures sans altérer celles déjà existantes. DSS-Signature, se conformant à ces normes, offre la flexibilité de "sur-signer" un document PDF en ajoutant de nouvelles signatures tout en préservant l'intégrité des signatures précédemment apposées.

Mes signatures seront-elles compatibles avec la validation à long terme

Le principe de la validation du document à long terme (VLT ou ALT) est d'inclure les révocations dans le PDF (signature type baseline_lt long-term). Pour obtenir la compatibilité ALT, il faut donc signer avec un certificat eIDas pour lequel les révocations sont gérées. Les informations sur la révocation seront incluses dans le PDF ce qui augmente sa taille. Si esup-signature ne trouve pas les révocations pour un certificat donné, on passe automatiquement en baseline_t (timestamp), donc plus compatible ALT / VLT. Le niveau baseline est configurable ici Configuration#sign

L'archivage légal est-il géré par Esup-Signature?

Les librairies SEDALib du projet Vitam sont intégrées dans esup-signature (https://www.programmevitam.fr/pages/ressources/sedalib/). Une implémentation à minima (POC) est proposée via cette classe https://github.com/EsupPortail/esup-signature/blob/master/src/main/java/org/esupportail/esupsignature/service/export/SedaExportService.java. Cette partie est à affiner avec l'aide d'une personne compétente en matière archivage électronique.

Fonctionnalités

Quel formats de documents sont supportés

Pour la signature électronique, tous types de documents. Seuls le format PDF permet apposer un visuel de la signature (les images sont converties en PDF pour permettre ce type de signature). Dans ce cas il est possible de faire une signature simple (apposition d'une image) ou une signature PAdES visuelle.

Pour tout autre format, esup-signature proposera une signature du fichier au format XAdES.

Puis-je contrôler la validité d'un document PDF signé électroniquement avec Esup-Signature ?

Oui. Deux cas se présente en fonction du type de signature :

- Si vous êtes en possession d'un document signé par esup-signature via l'apposition d'image (signature simple), vous pourrez, en cliquant sur l'image de la signature, accéder à une page de vérification qui contrôlera l'intégrité du document (checksum) et qui affichera le dossier de preuve.
- Si le document est signé à l'aide d'un certificat électronique, esup-signature permet sa vérification à l'aide du moteur DSS Signature

Quels types de signatures sont gérés dans Esup-Signature ?

Esup-Signature gère plusieurs niveaux de signature :

- le visa, l'utilisateur authentifié valide simplement son étape. Ce type d'estampille numérique permet de valider un document électronique, sans forcément y apposer un sceau image ou un sceau électronique. Toutes les étapes d'un circuit de signature sont systématiquement journalisées, permettant d'apporter la preuve du visa a posteriori (horodatage, login),
- la signature calligraphique, utilisable pour les fichier PDF. L'image du signataire est ajoutée au sein du PDF. Ca n'est pas, à proprement parler la signature électronique d'un document,
- la signature électronique au format PAdES, CAdES ou XAdES peut se faire via un certificat X509 téléchargé sur le profil de l'utilisateur ou via une clé cryptographique.

Voici un tableau des formats utilisés en fonction des cas d'usages. Le format XAdES ou CAdES est configuré de manière globale par l'administrateur

	Signature visuelle	**Signature détachée**
Document PDF	PAdES	XAdES/CAdES
Document autre	N/A	XAdES/CAdES

L'utilisation d'un certificat eIDAs sur support cryptographique nécessite le logiciel Esup-DSS-Client .

Pourquoi préférer l'usage d'un PDF/A en entrée d'esup-signature ?

Le PDF/A, souvent utilisé pour l'archivage à long terme, garantit une lecture optimale et stable sur la durée.

Le PDF/A assure notamment que les polices de caractères sont embarquées (embed) dans le document PDF/A, ce qui garantit que le document aura le même aspect visuel quel que soit le système d'exploitation ou le logiciel de lecture utilisé. Cela assure une expérience cohérente pour tous les utilisateurs, indépendamment de leur environnement informatique, et sur le long terme.

Lorsque vous utilisez esup-signature, il est recommandé d'utiliser un PDF/A en entrée : bien que esup-signature produise toujours un PDF/A en sortie, fournir un PDF/A en entrée évite toute modification de forme (formatage) non intentionnelle du document lors de sa conversion en PDF/A par esup-signature.

Comment obtenir un PDF/A depuis LibreOffice (ou Word) ?

En suivant ces étapes, vous pouvez facilement convertir vos documents en PDF/A pour une utilisation optimale avec esup-signature (cf question ci-dessus).

1. LibreOffice :
    - Ouvrez votre document dans LibreOffice.
    - Accédez à "Fichier" > "Exporter au format PDF".
    - Cochez l'option "PDF/A-1a" ou "PDF/A-1b" dans les paramètres d'exportation.
    - Cliquez sur "Exporter" pour générer votre PDF/A.
2. Microsoft Word :
    - Ouvrez votre document dans Word.
    - Accédez à "Fichier" > "Enregistrer sous".
    - Choisissez "PDF" dans la liste des formats.
    - Cliquez sur "Options".
    - Sélectionnez l'option "Standard ISO 19005-1 (PDF/A)".
    - Cliquez sur "OK", puis sur "Enregistrer" pour créer votre PDF/A.

Quels systèmes d'exploitations sont supportés par Esup-Signature pour effectuer des signatures eIDas (RGS**) ?

Conformément aux deux questions précédentes, à savoir : "Je dispose d'un certificat RGS** ou RGS*** (EIDAS). Esup-Signature me permet-il de signer des documents officiels avec ce type de certificats ?" et "Quels types de certificats sont pris en charge par Esup-Signature ?", Esup-Signature offre la possibilité de signer des documents de manière sécurisée avec différents types de certificats :

1. **Certificats personnels sécurisés :** Esup-Signature permet aux utilisateurs de signer des documents avec des certificats personnels, qu'ils soient stockés matériellement (dispositifs USB) ou logiciellement (dans des magasins de certificats). L'utilisation de l'outil libre et gratuit **esup-dss-client** est possible sur les systèmes d'exploitation Windows, **macOS** et Linux, offrant ainsi une compatibilité avec les trois principaux systèmes de bureau du marché. Des installateurs sont disponibles pour chaque système d'exploitation.

2. **Cachets d'établissement :** Esup-Signature prend également en charge l'utilisation de cachets d'établissement, qui correspondent à des certificats RGS**. Dans ce cas, le cachet doit être positionné au niveau du serveur à l'aide d'un dispositif USB sécurisé. La signature avec ce cachet est ensuite possible grâce au logiciel esup-signature, comme décrit dans la question "Quels types de certificats sont pris en charge par Esup-Signature ?". Cette approche présente de nombreux avantages, tant fonctionnels (le certificat n'est pas lié à une personne spécifique mais à l'établissement, ce qui permet une économie substantielle en termes d'achat et de mise en œuvre) que techniques (aucune installation ou configuration spécifique requise sur le poste utilisateur). En outre, ce mode de fonctionnement permet à un utilisateur de signer avec un certificat RGS** depuis n'importe quel navigateur, y compris un simple navigateur sur un smartphone.

En résumé, par rapport aux autres solutions disponibles sur le marché, et dans ses dernières versions, Esup-Signature se distingue comme un logiciel offrant la possibilité de réaliser des signatures qualifiées sur tous les systèmes d'exploitation, tout en étant l'une des options les plus abordables : logiciel libre et gratuit de bout en bout, dont le client et ses installateurs associés.

Esup-Signature gère-t-il L'authentification par SMS pour les personnes extérieures à l'établissement ?

Oui. Il s'agit d'envoyer un mail suivi d'un SMS (One Time Password) au destinataire externe à l'établissement. Une fois celui-ci authentifié, il aura accès à toutes les fonctionnalités d'esup-signature pour la durée de sa session.

Pour l'envoi de SMS, il existe une implémentation pour Esup-SMSU. Un développeur pourra éventuellement implémenter une autre méthode (utilisation d'une API d'un opérateur par ex).

Attention si les personnes concernées font partie de la fédération d'identité, il est possible d'utiliser l'authentification Shibboleth

Esup-Signature peut-il signer des documents en masse ?

Oui, il existe deux façons de faire de la signature en masse avec esup-signature :

- Dans l'interface graphique, on peut cocher plusieurs demandes puis cliquer sur "Signer". Dans ce cas, esup-signature va "essayer" de signer tous les documents. Les documents seront signés s'ils possèdent un emplacement de signature ou s'il s'agit d'une signature avec certificat (donc sans signature visuelle mais avec un sceau numérique). Dans tous les autres cas, aucune modification n'est apportée au document. Après l'opération un rapport est émis pour résumer les documents signés et non signés.
- L'autre solution est de passer par un circuit comportant une étape automatique. Ce système n'est utilisable qu'avec un certificat électronique (cachet d'établissement). Les documents sont injectés dans le circuit via un web service ou manuellement et sont directement signés avec le cachet (signature de diplômes, attestations...)

Esup-Signature assure-t-il la fonction de parapheur électronique ?

Oui, Esup-Signature peut être utilisé comme un parapheur électronique. Pour ce faire, il s'appuie sur un système de circuits (spécifiques ou génériques), un système d'annotation, de post-it ainsi que la possibilité d'ajouter des pièces jointes.

A quoi correspond la notion de "circuits" dans Esup-Signature ?

Il est possible créer des circuits à l'aide de l'interface d'Esup-Signature.

Un circuit est une succession d'étapes comportant les paramètres suivants :

- la liste des signataires pour l'étape donnée,
- le type de signature,
- si tous les signataires doivent signer à cette étape.

Un utilisateur peut construire un circuit, à l'aide de l'assistant, lorsqu'il crée une demande de signature.

Les administrateurs peuvent aussi ajouter des circuits spécifiques avec des paramètres plus poussés (source/destination/des documents, affectation de gestionnaires)

Est-il possible d'injecter des documents dans Esup-Signature ?

Esup-Signature propose 3 modes d'intégration des documents :

- intégration manuelle à l'aide de l'interface graphique,
- récupération automatique dans un dossier (**un** dossier spécifique est associé à **un** circuit),
- injection via web service (voir https://esup-signature-demo.univ-rouen.fr/swagger-ui.html).

Esup-Signature permet-il de dématérialiser totalement les documents ?

Pour des documents dont le format est bien structuré, Esup-Signature dispose d'un outil permettant une dématérialisation complète (pré-remplissage automatique du document en fonction du contexte, saisie des données, validation, signature)

Ce système s'appuie sur PDF Forms. Le modèle du document doit être un PDF disposant de champs de formulaire. Lorsque celui-ci sera intégré dans Esup-Signature, il sera analysé et un formulaire web sera généré.

Les champs des formulaires peuvent être édités au niveau de l'interface d'administration voir : Documentation administrateur#Lesformulaires

A quoi correspond la notion de "formulaires" dans Esup-Signature ?

La partie formulaire d'Esup-Signature correspond à un ensemble d'outils permettant de dématérialiser des procédures simples s'appuyant sur un document comme des demandes de mission par exemple.

L'université de Rouen Normandie utilise cette fonction pour dématérialiser l'attestation de déplacement lors de la période de COVID.

Esup-Signature peut-il pré-remplir des formulaires avec des données issues du système d'information de mon établissement?

Oui, c'est une des fonctionnalités proposée par la gestion des formulaires PDF d'esup-signature. Il est possible de configurer des sources de données pour chaque champ de formulaire et donc permet de les pré-remplir à l'aide des données issues de l'annuaire LDAP de l'établissement. Il est aussi possible de développer d'autres sources de données depuis des applications métiers (SIHAM, APOGEE, etc.) à l'aide de classes d'interface voir : Documentation administrateur#Classedepr%C3%A9-remplissage

Esup-Signature propose-t-il un système de délégations ?

Un système de délégation est proposé par Esup-Signature. Il permet à un utilisateur (mandant) de déléguer la signature ou la saisie de documents. Les délégués pourront "switcher" facilement sur le compte d'un des mandants.

Esup-signature propose aussi une fonction de transfert des demandes en cours et à venir vers une autres personne. Cette fonction est utilisée dans le cas d'un départ ou du remplacement, d'un utilisateur, elle est définitive.

Comment est-on identifié sur Esup-Signature ?

Esup-Signature dispose de 3 modes authentification :

- CAS : surtout dédier à l'authentification des utilisateurs de l'établissement (nécessite la configuration du LDAP),
- Shibboleth : pour authentifier les utilisateurs d'autres établissement,
- Oauth : pour authentifier des utilisateurs externes en utilisant d'autres plateformes : France Connect, Microsoft, Google...

Ces 3 modes peuvent être activés simultanément.

Un utilisateur peut-il stocker plusieurs signatures dans son profil ?

Oui, dans son profil, un utilisateur a la possibilité de stocker plusieurs signatures calligraphiques (ie images). On peut imaginer une signature sans tampon, avec tampon spécifique (en fonction des rôles ou missions d'un utilisateur), avec mentions ("Lu et approuvé", "bon pour...", etc.)

Esup-Signature intègre-t-il une gestion de groupes ?

Non, le système repose sur l'attribution de rôles obtenus lors de la connexion en fonction d'un mapping paramétrer au niveau du fichier de configuration d'esup-signature. Tous les détails sur l'attribution des rôles sont disponible sur cette page : Configuration de la sécurité

Mise en oeuvre

Comment mettre en place Esup-Signature ?

Pour l'instant Esup-Signature n'est pas proposé en mode hébergé. Il faut donc l'installer sur un serveur local de l'établissement.

Développé en Java/Spring Boot, esup-signature demande de connaitre à minima Java, Maven, Git, PostgreSQL. Pour l'exploiter totalement il est bien de connaitre aussi Spring, CAS, Shibboleth, Apache, Tomcat.

Pour plus de détail vous pouvez consulter la documentation ici : Installation

Quels sont les pré-requis ?

Voir la page dédiée : Prérequis

Doit-on disposer d'une GED pour faire fonctionner Esup-Signature?

Non. Esup-signature fonctionne de manière autonome, et dispose de sa propre base de données pour stocker les documents.

Toutefois, ESUP-Signature accepte en entrée ET en sortie différentes sources documentaires, telles :

- une GED (Nuxeo, Alfresco, etc.) via le standard ouvert CMIS,
- un partage réseau orienté fichier de type SMB/NFS,
- un stockage local (dossier),
- etc.

Peut-on développer/personnaliser Esup-Signature ?

Esup-Signature est libre, open-source, donc ouvert aux contributions.

Par ailleurs des classes "interface" sont disponibles pour implémenter des comportements spécifiques à plusieurs niveaux :

- workflow spécifiques,
- récupération de données externes,
- pré-remplissage automatique des formulaires.

Questions juridiques

Sans être experts juridiques, nous nous aventurons ici à retranscrire des informations générales sur la valeur juridique ou probante d'une signature dématérialisée en France.

Est-ce que la simple numérisation d'un document signé a une valeur juridique ?

Le marché de la signature électronique est tel que les entreprises vendant ces dispositifs de signature électronique ont tendance à inciter leurs clients à utiliser des signatures avancées pour tout type de documents, en se permettant parfois d'avancer que telle ou telle procédure n'a aucune valeur juridique.

Tout comme un email ou même un simple tweet, **un document signé manuellement puis simplement scané peut avoir une valeur juridique**.

Les actualités, et la jurisprudence qui en découle, le prouvent très régulièrement.
Aussi, si en recherchant sur un moteur de recherche à savoir si une signature numérisée a une valeur juridique, il est fort probable que vous tombiez sur des articles et documentation de sites d'éditeurs de logiciel de signature affirmant que ce n'est pas le cas. Mais si vous faites l**a même recherche sur le fil d'actualités de ce même moteur de recherche**, vous serez étonné du nombre de résultats vous prouvant tout le contraire ; dont cet exemple sur service-public.fr.

A contrario, même un document signé avec un niveau de sécurité le plus élevé possible et avec le logiciel le plus avancé qui soit (dont esup-signature allié à DSS signature 😉), peut être contesté : erreur humaine, consentement non éclairé, vice de forme, fraude, preuve de l'identité de l'auteur, abus de confiance, signature sous la contrainte, ...

Quelle est la valeur probante d'une signature dématérialisée via esup-signature ?

En France, la signature électronique est régie par le règlement européen eIDAS (Règlement (UE) n° 910/2014) et le Code civil français (articles 1366 à 1377).

La valeur probante d'une signature dématérialisée peut dépendre du contexte et des exigences spécifiques de chaque transaction ou contrat.

1. Signature électronique simple : une signature dématérialisée réalisée avec une simple image scannée (apposition d'image) peut être considérée comme une signature électronique simple. Si cette forme de signature est généralement valide pour la plupart des transactions courantes et a une force probante légale, elle peut être sujette à contestation si sa validité est mise en doute lors d'un litige : elle offre un niveau de sécurité moindre par rapport à d'autres types de signatures.
2. Signature électronique avancée et qualifiée : pour une valeur probante plus élevée et une meilleure reconnaissance légale, il est recommandé d'utiliser une signature électronique avancée ou qualifiée. Ces signatures exigent des niveaux de sécurité plus élevés et doivent respecter certaines conditions spécifiques pour être reconnues comme ayant une valeur probante équivalente à celle d'une signature manuscrite.

Dans les deux cas, les logs d'authentification et d'action de signature des usagers conservés sur esup-signature peuvent aussi servir de preuve de l'identification et de l'intégrité du processus de signature. Ils peuvent renforcer la valeur probante de la signature dématérialisée en démontrant que l'utilisateur a effectivement signé le document et qu'il s'est authentifié de manière appropriée.