esup portail

17 NOVEMBRE 2026
@Distance

ESUP-DAYS 42

ESUP-SIGNATURE 2.0

David Lemaignent — Université de Rouen Normandie

INTRODUCTION

Pourquoi une v2 ?

- Stabiliser le périmètre fonctionnel
- Améliorations focalisées sur le process de signature
- Pas de retour arrière possible après migration
- Disparité des versions

Trois axes d'améliorations

- Technique
- Fonctionnel
- Ergonomie

Projet piloté avec un comité d'utilisateurs

- Et boosté avec l'IA…



PÉRIMÈTRE ET ÉVOLUTIONS

- Signatures : simple, avancée et qualifiée (selon le mode utilisé)
- Modes de signature : visa, image, PAdES / CAdES / XAdES (DSS, eIDAS)
- Parapheur mis en œuvre via des circuits paramétrables
  - Étapes, emplacements de signatures, niveaux de signature, formulaires
- Intégrations : APIs, SMB / CMIS, SEDA, LDAP, CAS / Shibboleth, OIDC
- Signature des extérieurs : SMS, FranceConnect, ProConnect

- Évolution modulaire : développement depuis l'extérieur
  - Ex : nettoyage, archivage, export SEDA, connecteur paperless, …
- Maintien et développement des APIs

ORGANISATION DU PROJET

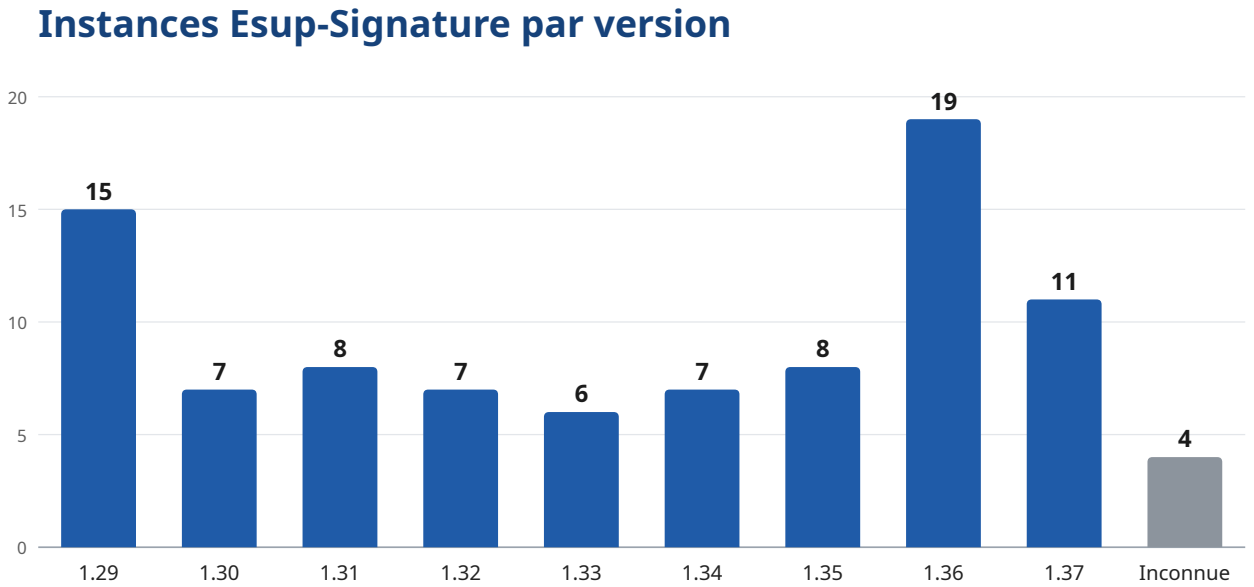
- ## Passage en « mode LTS »
  - Support de la version 1.37 jusqu'à la sortie de la v2
  - Pas de support des versions antérieures

- ## Projet piloté avec un comité d'utilisateurs représentatifs des différents usages
  - Rôle : arbitrer et prioriser les corrections et évolutions, recetter
  - Composition : Caen, Paris 1 Panthéon-Sorbonne, Rennes, Nantes, Avignon, Strasbourg
  - Fonctionnement : Points réguliers (~2 par releases), remontées au fil de l'eau via canaux dédiés
  - … et merci aux contributeurs de GitHub

- ## Le recours à l'IA
  - Sécurisation et fiabilisation
  - Réactivité en cas d'urgence
  - …mais : complexification du projet (plus difficile à suivre sans IA)

USAGES

- Installé dans plus de 90 établissements :



- Exemples d'usages :
  - Esup-Stage
  - Applications maison : esup-emargement, virements inter UB, esup-agape, flotte mobile, bons de commande
  - Formulaires : télétravail, procurations pour le vote, ordres de mission

ESUP-DAYS 42

Socle modernisé
Migration
Qualité

TECHNIQUE

esup portail

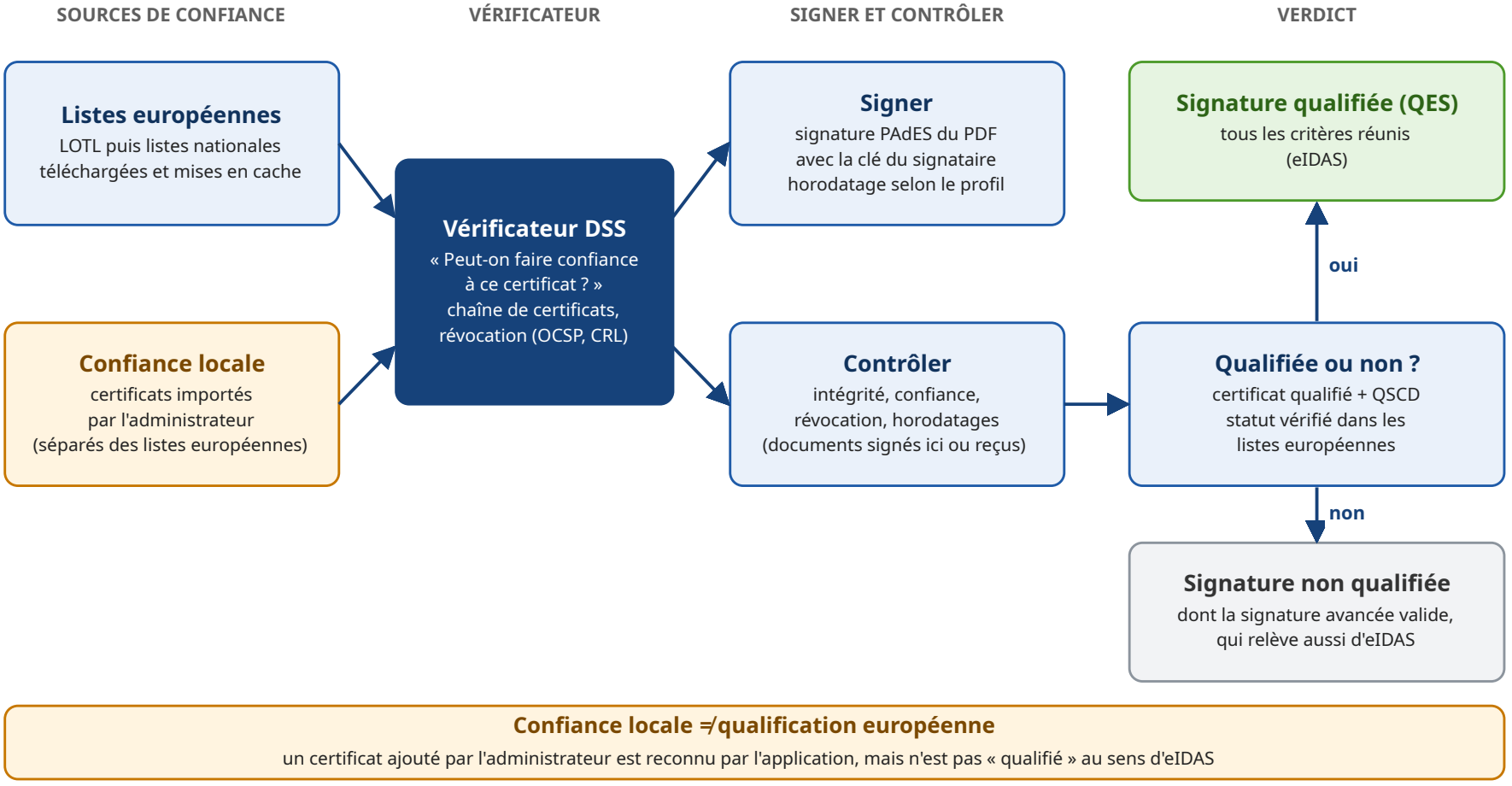
UN SOCLE MODERNISÉ

- Spring Boot 4.1, DSS 6.5, PDF.js 6, ECharts, Slim Select 4…
- Flyway : migrations additives, sans reprise de l'historique
- Front : modules JS, Thymeleaf + htmx, CSS et IDs nettoyés
- JPA : suppression des chargements EAGER, workflows en lazy
- Journaux métier mieux structurés (comprenant log des actions, audit des signatures)
- > 1000 Tests : sécurité, services, parcours Playwright
- Sécurité : Esup-DSS-Client en WSS, mise en place de Content Security Policy (suite à l'audit des Mines Saint-Étienne)

DSS ET CERTIFICATS eIDAS

- DSS : bibliothèque européenne de validation et de signature (eIDAS)
- Listes de confiance (LOTL / trusted lists) : à tenir à jour dans l'instance
- Signature qualifiée (eIDAS, RGS**) : indicateur vert
  - Ajout automatique du certificat seal dans la trustlist
- Signature avancée : indicateur en avertissement (warn)
  - Sans impact sur la validité de la signature
- Avec DSS, Esup-Signature peut produire des signatures eIDas LTA !

DSS SIGNATURE



CONNEXION FRANCECONNECT ET PROCONNECT

- Depuis 1.37 : amélioration de la conformité
- Prérequis : Esup-Signature 1.34 ou plus récent, instance en HTTPS
- Demander l'accès sur les portails partenaires
  - identifiants de test reçus
- Configurer l'instance, puis tester
  - ProConnect : réservé aux externes, les agents restent sur CAS
- FranceConnect : faire qualifier le service
  - demande d'accès aux données (DataPass) et formulaire
- Configurer la production avec les identifiants de production

SIGNATURE SIMPLE : PAS SI SIMPLE

- Avant : une image apposée sur le PDF

- Maintenant : révision PDF incrémentale + calque dédié
  - Empreinte SHA3-256, UUID de preuve, URL de l'instance émettrice
  - Preuve embarquée dans le PDF (ESUP_SignatureProofs), liée au journal serveur

- Formulaires : champs de l'étape remplis inclus dans la même révision

- Contrôle en ligne auprès de l'instance émettrice
- Limite : sans preuve centralisée, le document ne se suffit toujours pas à lui-même pour le contrôle

SIGNATURE SIMPLE : PAS SI SIMPLE

DANS LE FICHIER PDF

Révision 1
Document d'origine, inchangé

Révision 2 : ajout incrémental

Calque de signature
dédié

Champs de l'étape
(même révision)

ESUP_SignatureProofs
Empreinte SHA3-256 du document
UUID de preuve
URL de l'instance émettrice

lié par
l'UUID

SUR L'INSTANCE ÉMETTRICE

Journal serveur

UUID	Empreinte	Signataire, date
3f9a...	a41c...	...
b72e...	09d5...	...
c018...	7be3...	...

Source de référence de la preuve :
une signature se contrôle auprès de l'instance qui l'a émise.

CONTRÔLE EN LIGNE

PDF déposé sur la page de contrôle → Lecture de la preuve embarquée → Interrogation de l'instance émettrice → Empreinte comparée au journal : résultat

Preuve et contrôle

Reprise du travail, échéances

Collaboration et signature

FONCTIONNEL

CONTRÔLE ET DOSSIER DE PREUVE

- Contrôle des unifié : pages de validation et page publique
- Résultats plus lisibles : signatures simples et cryptographiques, PDF/A
- Dossier de preuve PDF : annexes, export ZIP, envoi par courriel
- API : récupération du dernier rapport (get-last-report)
- Performance du contrôle de certificat améliorée

REPRISE DU TRAVAIL EN COURS

- Brouillons des champs de formulaire PDF
- Sauvegarde automatique des placements de signature
- Placement des zones : copier-coller, résumé dans la barre de signature
- Relance d'une demande refusée
  - À partir d'une étape choisie
  - Relance depuis le début

SIGNATURE ET CIRCUITS

- PDF protégés : tentative de déverrouillage
- Visuel de signature via mobile : capture depuis le téléphone
- Échéance : date fixe ou délai après création via les paramètres des circuits
- Nouveau statut « expirée »
- Affectation d'un emplacement par étape et par signataire
- Forcer l'aspect des signatures : configurable par étape

COLLABORATION AUTOUR DE LA DEMANDE

- Chat sur la demande, avec état de lecture par utilisateur
- Notifications regroupées : un courriel de synthèse si non lu en direct
- Post-it : refonte et corrections de placement
- Suppression, transfert, refus : notifications et doublons corrigés
- Externes : OTP, renvoi, PIN par courriel si pas de SMS

ESUP-DSS-CLIENT : LE NOUVEAU CLIENT DE SIGNATURE

- Remplace NexU : non maintenu depuis 2018
  - abandon du système basé sur serveur web local
- Poste utilisateur : certificat local ou matériel (clé, carte)
- OpenSC natif : Linux, Windows, macOS, sans pilote à installer
- Connexion WSS vers Esup-Signature
- Plusieurs documents signés en une seule session
- Installateurs : Windows, Linux, macOS (Intel et Apple Silicon)

ESUP-DSS-CLIENT : LE NOUVEAU CLIENT DE SIGNATURE

Signature électronique : évolution des échanges

ANCIEN FONCTIONNEMENT — IMPORT JAVASCRIPT LOCAL

Le navigateur communique directement avec NexU sur le poste utilisateur.



NOUVEAU FONCTIONNEMENT — WEBSOCKET SÉCURISÉ (WSS)

Le serveur eSup-Signature communique avec l'application installée sur le poste.



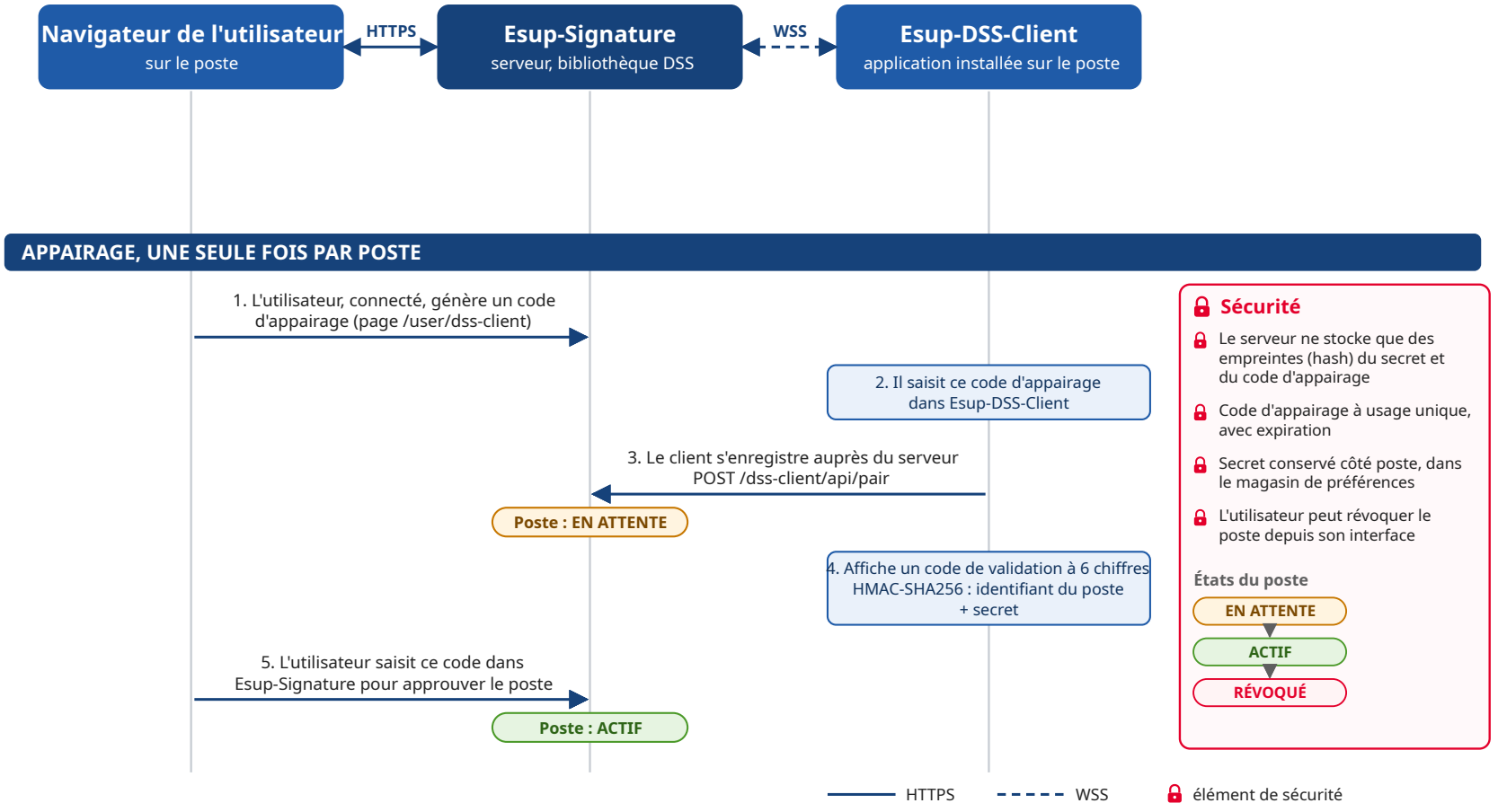
Aucun import de script depuis localhost
Les échanges de signature passent par le serveur

Certificats et demande de signature via WSS
PIN et clé privée restent sur le poste

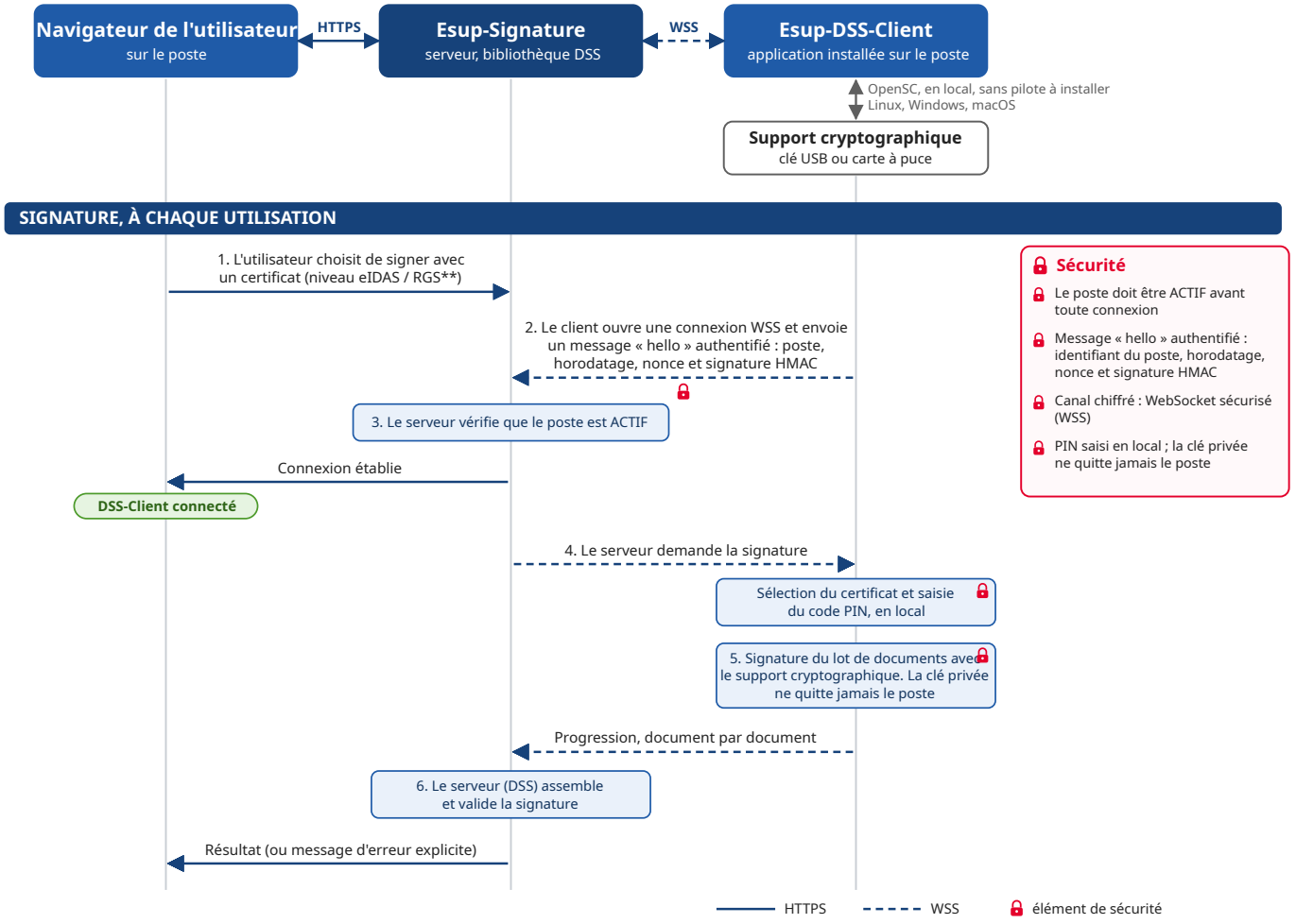
ESUP-DSS-CLIENT : ASSOCIATION SÉCURISÉE DU POSTE

- 1. Code d'association généré par l'utilisateur dans Esup-Signature
- 2. Enregistrement du poste par le client : poste « en attente »
- 3. Code de validation à 6 chiffres (HMAC) saisi pour approuver
- 4. Poste actif : connexions WSS authentifiées (HMAC, nonce)
- Révocation possible depuis l'interface utilisateur
- Sécurité : le serveur ne stocke que des empreintes des secrets
- Plus complexe à configurer sur le poste client

ESUP-DSS-CLIENT : ASSOCIATION SÉCURISÉE DU POSTE



ESUP-DSS-CLIENT : SIGNATURE



INTÉGRATIONS ET PILOTAGE

- Attributs LDAP, OIDC, personnalisés : pour le pré-remplissage
- Recherche améliorée
- SEDA : export externalisé, erreurs mieux gérées
- Statistiques : ECharts et graphique des délais de workflow

Nouvelle interface
Multilingue
RGAA

ERGONOMIE

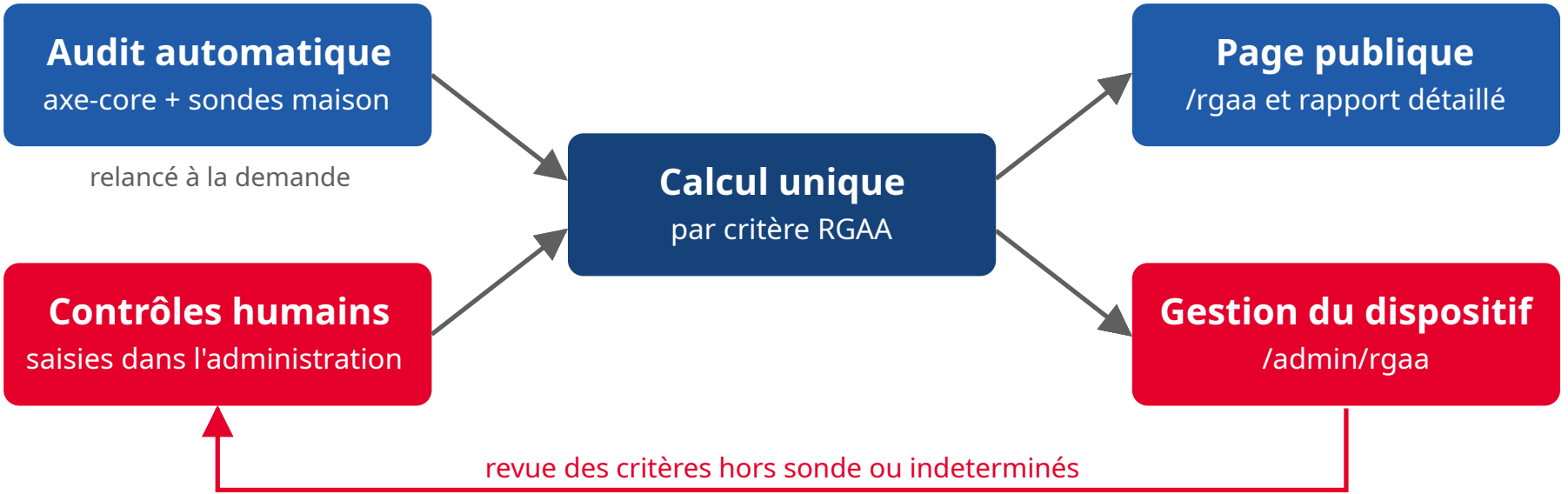
UNE INTERFACE REPENSÉE

- Panneau de signature unifié et nouvelle barre latérale
- Responsive : vues adaptées aux petits écrans et au mobile
- Design harmonisé : accueil, listes, administration, connexion
- Multilingue : français, anglais, espagnol
- Recherche, onglets, tableaux et assistants refaits

ACCESSIBILITÉ : DÉMARCHE RGAA

- Audit RGAA automatisé dans l'interface d'administration
- Export EARL et page des règles
- Corrections en plusieurs passes : focus, libellés, composants
- Documentation : audit tenu dans le dépôt
- Taux de conformité 53,4 % en sortie de version 2

ACCESSIBILITÉ : DÉMARCHE RGAA



MISE EN ŒUVRE

- Code :
  https://github.com/EsupPortail/esup-signature

- Documentation :
  https://www.esup-portail.org/wiki/display/SIGN

- Démonstration :
  https://esup-signature-demo.univ-rouen.fr

esup portail

17 NOVEMBRE 2026
@Distance



MERCI

Des questions ?

— Université de Rouen Normandie