



LOCAL TRUST SIGN I

SERVICE ATEXO DE SIGNATURE A LA VOLEE

POLITIQUE DE SIGNATURE

IDENTITÉ DU DOCUMENT	
Client	LOCAL TRUST SIGN I
Affaire	Service Atexo de signature à la volée
Titre	Politique de signature
Référence	Atexo – LT-SIGN-I – PS
État	Final
Révision	1.0
Du	3 décembre 2025
Dernière page	15

ÉVOLUTION DU DOCUMENT			
Date	Version	Rédacteur	Commentaires
03/12/2025	1.0	Atexo	Validation du document et diffusion

APPROBATION DE LA VERSION		
Entreprise ou Service	Nom	Visa
CLIENT		
Atexo	Atexo	

DIFFUSION DE LA VERSION				
Entreprise ou Service	Destinataires	Fonction	Pour action	Pour info
CLIENT			X	
Atexo	Atexo			X

Table des matières

1	OBJET DU DOCUMENT	5
2	IDENTIFICATION DU DOCUMENT	6
3	INTRODUCTION	7
3.1	CHAMP D'APPLICATION DE LA POLITIQUE DE SIGNATURE	7
3.2	GESTION DE LA PS	7
3.2.1	Entité gérant la PS.....	7
3.2.2	Point de contact.....	7
3.2.3	Déclaration de conformité de la PS.....	7
3.2.3.1	Entité déterminant la conformité d'une PS	7
3.2.3.2	Procédures d'approbation de la conformité de la PS	7
3.2.4	Circonstances rendant une mise à jour nécessaire	7
3.2.5	Information des acteurs.....	7
3.2.6	Entrée en vigueur de la nouvelle version et période de validité.....	8
3.2.7	Publication de la PS.....	8
3.2.8	Archivage des anciennes versions.....	8
3.3	DOCUMENTS ASSOCIES	8
4	DECLARATION DES PRATIQUES DE SIGNATURE	9
4.1	EXIGENCES SUR LE FOURNISSEUR.....	9
4.2	EXIGENCES SUR L'APPLICATION DE CREATION/VERIFICATION DE SIGNATURE	9
4.3	ACTEURS ET ROLES	9
4.3.1	ATEXO	9
4.3.2	Plateforme applicative.....	9
4.3.3	Utilisateur/Signataire	9
5	PARAMETRES METIER (BSP)	10
5.1	PARAMETRES RELATIFS AU CAS D'USAGE.....	10
5.1.1	BSP (a) : Séquencement des signatures	10
5.1.2	BSP (b) : Données signées	10
5.1.2.1	Signature utilisateur	10
5.1.3	BSP (c) : Lien entre les données signées et les signatures	10
5.1.4	BSP (d) : Population cible	10
5.1.5	BSP (e) : Responsabilités quant à la validation et l'extension des signatures	10
5.2	PARAMETRES D'ORIGINE JURIDIQUE/LEGALE/REGLEMENTAIRE	10
5.2.1	BSP (f) : Nature juridique des signatures	10
5.2.2	BSP (g) : Engagement des signataires.....	10
5.2.3	BSP (h) : Garanties sur la date des signatures	10
5.2.4	BSP (i) : Formalités de signature	11
5.2.4.1	Rôle et obligation de l'Utilisateur	11
5.2.5	BSP (j) : Pérennité des signatures.....	11
5.2.6	BSP (k) : Archivage	11
5.3	PARAMETRES RELATIFS AUX MOYENS ET INTERVENANTS IMPLIQUES DANS LE CYCLE DE VIE DES SIGNATURES	11
5.3.1	BSP (l) : Identité des signataires.....	11
5.3.2	BSP (m) : Niveau de garantie pour l'authentification des signataires.....	11
5.3.3	BSP (n) : Dispositif de création des signatures	11
5.4	AUTRES PARAMETRES	12
5.4.1	BSP (o) : Informations supplémentaires associées aux signatures	12
5.4.2	BSP (p) : Dimensionnement cryptographique	12
5.4.3	BSP (q) : Environnement technique.....	12
6	EXIGENCES SUR LES MOYENS ET STANDARDS	13

7	AUTRES PROBLEMATIQUES METIERS ET LEGALES	14
7.1	<i>LIMITATIONS DES RESPONSABILITES D'ATEXO</i>	14
8	AUDITS ET CONFORMITE.....	15

1

OBJET DU DOCUMENT

Une politique de signature (PS) est un document, identifié par OID, qui décrit l'ensemble des exigences auxquelles un prestataire se conforme dans la mise en place et la fourniture de ses prestations de signature électronique. La PS peut aussi définir les obligations applicables aux autres entités impliquées dans la fourniture de ce service.

La présente politique couvre les signatures électroniques produites dans le cadre du service « Signature à la volée » proposé par ATEXO aux Utilisateurs de son logiciel LOCAL TRUST FORCE.

Le présent document décrit aussi la mise en œuvre et les pratiques de signature de ce service.

2 IDENTIFICATION DU DOCUMENT

La présente *Politique de Signature* [PS] est identifiée par l'OID 1.3.6.1.4.1.60316.2.2.1.

Cela correspond au chemin suivant dans la hiérarchie des OID d'ATEXO :

iso(1) org(3) dod(6) internet(1) private(4) entreprise(1) atexo(60316)
signature(2) politique-local-trust-sign1(2) version(1)

3 INTRODUCTION

La société ATEXO a pour activité l'édition de logiciels et de services en ligne. Dans le cadre de ces services en ligne, certains processus comprennent la signature électronique de documents par les utilisateurs. Afin d'expliciter la portée, les modalités de création et de vérification de ces signatures électroniques, ATEXO publie et maintient la présente politique de signature (PS).

Le plan et le contenu de cette politique visent la conformité aux spécifications techniques décrites dans [TS_119172].

3.1 Champ d'application de la politique de signature

L'objet d'une politique de signature est la description des règles qui conditionnent la création et la validation des signatures électroniques dans le cadre d'échanges prédéfinis.

La présente PS décrit notamment les règles respectées par ATEXO dans les processus de :

- Signature électronique de documents, simple ou avancée au sens du règlement [eIDAS], par des utilisateurs des plateformes d'ATEXO (agent public ou personne physique particulière ou représentant d'une personne morale) et du logiciel LOCAL TRUST FORCE (logiciel Client).

La présente PS est de la responsabilité de ATEXO.

3.2 Gestion de la PS

3.2.1 Entité gérant la PS

ATEXO gère la PS via ses instances de pilotage et de décision.

3.2.2 Point de contact

Les demandes d'informations ou questions concernant la PS peuvent être adressées par courriel à : crypto@atexo.com.

3.2.3 Déclaration de conformité de la PS

3.2.3.1 Entité déterminant la conformité d'une PS

Le Comité Sécurité ATEXO détermine la conformité de la PS, la publie et la diffuse.

3.2.3.2 Procédures d'approbation de la conformité de la PS

L'approbation de la conformité de la PS est mise à l'ordre du jour du Comité Sécurité ATEXO.

Ce dernier se base sur des résultats d'audits ou de revue menés par le contrôle interne de ATEXO et sur les P.-V. de mise en production.

3.2.4 Circonstances rendant une mise à jour nécessaire

La mise à jour de la présente PS est un processus impliquant tous les acteurs et faisant l'objet d'une démarche rigoureuse. Il est enclenché essentiellement pour procéder à des modifications importantes, pour prendre en compte de nouveaux besoins, de nouveaux acteurs, améliorer le cadre juridique ou combler des lacunes.

3.2.5 Information des acteurs

Lorsqu'une mise à jour a été planifiée, les informations relatives à cette évolution sont disponibles sur demande. Les acteurs peuvent à tout moment se renseigner auprès d'ATEXO pour obtenir plus d'informations.

La publication d'une nouvelle version de la PS est réalisée sous la responsabilité du Comité sécurité ATEXO et consiste à archiver la version précédente et mettre en ligne, dans le répertoire prévu à cet effet, les éléments suivants :

- Document au format PDF,
- OID du document.

3.2.6 Entrée en vigueur de la nouvelle version et période de validité

Lorsqu'une nouvelle version de la PS est disponible, elle est mise à disposition de tous les acteurs.

Sauf mention contraire, la nouvelle version de la PS entre en vigueur dès qu'elle est publiée dans le système documentaire d'ATEXO et mise à disposition de tous les acteurs.

La PS est publiée pour une durée de validité indéterminée. Elle est rendue obsolète par la publication d'une version incrémentée.

3.2.7 Publication de la PS

La PS est publiée sur le site atexo.com.

3.2.8 Archivage des anciennes versions

Les versions antérieures de la présente politique sont archivées pendant la durée de vie du service.

3.3 Documents associés

[eIDAS]	<i>Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC</i> http://data.europa.eu/eli/reg/2014/910/oj/eng Modifié par (eIDAS v2) : <i>Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework</i> https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng
[GDPR]	Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 https://www.cnil.fr/fr/reglement-europeen-protection-donnees
[TS_119172]	<i>ESI – Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents, Version 1.1.1 de juillet 2015</i>
[PAdES]	<i>PAdES digital signatures, ETSI EN 319 142, v. 1.1.1</i>

4.1 Exigences sur le fournisseur

Sans objet : ATEXO développe et met en œuvre l'application de signature.

4.2 Exigences sur l'application de création/vérification de signature

L'application de création de signature électronique utilisée pour générer les signatures doit respecter les exigences de format définies ci-après et doit être exploitée dans des conditions conformes à la présente politique.

La présente politique ne formule aucune exigence sur les applications de vérification de signature électronique utilisées par ATEXO ou des tiers pour valider les signatures électroniques produites par le service.

4.3 Acteurs et rôles

4.3.1 ATEXO

ATEXO est le fournisseur des services mettant en œuvre la signature électronique.

4.3.2 Plateforme applicative

La plateforme applicative est le système d'information qui fait appel au service de signature à la volée d'ATEXO. Cette plateforme peut elle-même être opérée par ATEXO, mais il peut aussi s'agir d'une plateforme tierce, opérée par un client d'ATEXO, ou du logiciel LOCAL TRUST FORCE, installé sur l'ordinateur de l'Utilisateur.

4.3.3 Utilisateur/Signataire

Le signataire est la personne physique qui appose sa signature de façon électronique sur les documents qui lui sont présentés pour approbation via le service de signature à la volée ou qu'il choisit lui-même en vue de leur signature.

5 PARAMETRES METIER (BSP)

Remarque : le terme « BSP » désigne les « *Business Scoping Parameters* » dans [TS_119172].

5.1 Paramètres relatifs au cas d'usage

5.1.1 [BSP \(a\) : Séquencement des signatures](#)

Les signatures sont produites unitairement et séquentiellement, à raison d'une signature par document signé.

5.1.2 [BSP \(b\) : Données signées](#)

5.1.2.1 Signature Utilisateur

La signature électronique de l'Utilisateur est une signature d'approbation, matérialisant son accord avec le document signé.

La signature est déclenchée par un Utilisateur via les services ATEXO (voir 5.3.2).

5.1.3 [BSP \(c\) : Lien entre les données signées et les signatures](#)

Les signatures gérées par le portail ATEXO répondent aux spécifications de la norme [PAdES], de type LT : les CRL et les certificats sont inclus explicitement pour chaque signature électronique, et un jeton d'horodatage est inclus dans la signature produite.

5.1.4 [BSP \(d\) : Population cible](#)

Les documents signés sont à destination des Utilisateurs du service.

5.1.5 [BSP \(e\) : Responsabilités quant à la validation et l'extension des signatures](#)

Les tiers ou entités souhaitant s'assurer de l'authenticité des documents signés peuvent vérifier la signature cryptographique qu'ils contiennent.

Les signatures sont horodatées et étendues avec les données de vérification des certificats (format LT) par les Services ATEXO, concomitamment à leur création.

5.2 Paramètres d'origine juridique/légale/réglementaire

5.2.1 [BSP \(f\) : Nature juridique des signatures](#)

Les signatures sont des signatures électroniques simples au sens de l'article 36 du règlement [eIDAS].

5.2.2 [BSP \(g\) : Engagement des signataires](#)

Les signatures sont des signatures électroniques de documents à des fins d'approbation : elles garantissent l'intégrité et l'authenticité des documents sur lesquels elles sont apposées, ainsi que le consentement du signataire à leur contenu.

5.2.3 [BSP \(h\) : Garanties sur la date des signatures](#)

Toutes les informations signées font l'objet d'un horodatage permettant :

- de s'assurer de la traçabilité des informations de date et heure de signature de ces transactions;
- de déterminer la liste de révocation à utiliser pour valider cette transaction.

La date d'application d'une signature est indiquée par un horodatage électronique fourni par les plateformes d'ATEXO.

5.2.4 [BSP \(i\) : Formalités de signature](#)

5.2.4.1 [Rôle et obligation de l'Utilisateur](#)

L'Utilisateur doit contrôler les données à signer avant d'y apposer sa signature électronique. Il utilise pour cela l'application de signature mise à disposition par ATEXO et dont les différentes étapes du processus de signature les amènent à :

- Accepter les *Conditions générales d'utilisation* de la plateforme d'ATEXO et/ou la *Politique de signature* du service
- Contrôler le contenu du ou des documents présentés par la plateforme d'ATEXO ou directement sélectionnés par l'Utilisateur,
- Fournir des informations exactes quant à son identité : l'identité du signataire est entièrement déclarative (nom, prénom, adresse courriel, données qui seront reprises dans sa signature électronique),
- Donner formellement son accord pour apposer sa signature électronique sur les documents. L'authentification de l'Utilisateur est réalisée par la saisie d'un OTP¹ reçu par courriel à l'adresse qu'il/elle a déclarée sur la plateforme d'ATEXO ou dans la configuration du logiciel LOCAL TRUST FORCE.

5.2.5 [BSP \(j\) : Pérennité des signatures](#)

Les signatures sont valables sans limitation de durée. L'intégrité des documents signés est vérifiable cryptographiquement.

Les certificats émis sont à usage unique et ont une durée de vie courte (inférieure à une heure).

Les algorithmes mis en œuvre sont à l'état de l'art de la cryptographie (voir 5.4.2) de façon à permettre une robustesse des mécanismes compatible avec les usages métiers.

5.2.6 [BSP \(k\) : Archivage](#)

L'archivage des signatures électroniques n'est pas dans le périmètre de la présente politique.

5.3 [Paramètres relatifs aux moyens et intervenants impliqués dans le cycle de vie des signatures](#)

5.3.1 [BSP \(l\) : Identité des signataires](#)

Voir **Erreur ! Source du renvoi introuvable.**

5.3.2 [BSP \(m\) : Niveau de garantie pour l'authentification des signataires](#)

Les signataires sont authentifiés sur la plateforme d'ATEXO ou le logiciel LOCAL TRUST FORCE par la saisie d'un mot de passe à usage unique (OTP). Celui-ci est reçu par courriel, à l'adresse déclarée par le/la signataire.

5.3.3 [BSP \(n\) : Dispositif de création des signatures](#)

Le certificat et la clé privée de signature de l'Utilisateur sont générés à la volée sur le serveur de signature. Aucun support n'est remis au signataire.

ATEXO utilise un serveur de signature qui a la charge de :

- Présenter fidèlement les documents à signer,
- Générer une nouvelle bi-clé pour l'Utilisateur,

¹ *One time password* (mot de passe à usage unique)

- Protéger cette bi-clé le temps de la transaction,
- Réaliser les opérations de signature après authentification de l'Utilisateur,
- Détruire la bi-clé à la fin de l'opération de signature.

5.4 **Autres paramètres**

5.4.1 BSP (o) : Informations supplémentaires associées aux signatures

Sans objet.

5.4.2 BSP (p) : Dimensionnement cryptographique

Les signatures mises en œuvre respectent les règles de dimensionnement et de paramétrage conformes aux recommandations de l'ANSSI.

Présentement : SHA256 et clés RSA 3072 bits.

5.4.3 BSP (q) : Environnement technique

Aucune restriction.

La présente politique ne formule aucune exigence supplémentaire sur les moyens et standards.

Les informations d'identification et d'authentification de l'Utilisateur sont fournies par ce dernier et restent de sa responsabilité quant à leur maintien et mise à jour.

L'Utilisateur est responsable du contenu des informations présentes dans le Document signé, et de la bonne utilisation des certificats de signature dans ce cadre.

ATEXO est à la disposition de ses clients pour accompagner la réalisation des audits suivants :

- Un audit technique pour s'assurer que les mises en œuvre techniques correspondent bien aux exigences prévues dans les documents de politique,
- Un audit juridique pour s'assurer que les exigences réglementaires sont respectées