ITUPublications

Union internationale des télécommunications
Secteur du développement

Cadre de mise en place de l'infrastructure à clés publiques du Gouvernement du Mali

Cadre de mise en place de l'infrastructure à clés publiques du Gouvernement du Mali

2022

DÉNI DE RESPONSABILITÉ

Les appellations employées dans la présente publication et la présentation des données qui y figurent n'impliquent, de la part de l'UIT et du Secrétariat de l'UIT, aucune prise de position quant au statut juridique des pays, territoires, villes ou zones, ou de leurs autorités, ni quant au tracé de leurs frontières ou limites.

Les références faites à certaines sociétés ou aux produits de certains fabricants n'impliquent pas que l'UIT approuve ou recommande ces sociétés ou ces produits de préférence à d'autres de nature similaire, mais dont il n'est pas fait mention. Sauf erreur ou omission, les noms des produits propriétaires sont reproduits avec une lettre majuscule initiale.

L'UIT a pris toutes les précautions raisonnables pour vérifier les informations contenues dans la présente publication. Cependant, le document publié est distribué sans garantie d'aucune sorte, ni expresse, ni implicite. Son interprétation et son utilisation relèvent de la responsabilité du lecteur.

Les avis, résultats et conclusions reproduits dans la présente publication ne reflètent pas nécessairement la position de l'UIT ou de ses membres.

ISBN

978-92-61-35932-4 (version électronique)
978-92-61-35942-3 (version EPUB)
978-92-61-35952-2 (version Mobi)

Avant d'imprimer ce rapport, pensez à l'environnement.

Table des matières

Liste des tableaux et des figures

Tableaux

Figures

Sigles

2FA | A2F	2-Factor Authentication | Authentification à deux facteurs
AGETIC	Agence des technologies de l'information et de la communication
AMRTP	Autorité malienne de régulation des Télécommunications, des Technologies de l'Information et de la Communication et des Postes
AE	Autorités d'enregistrement
AED	Autorités d'enregistrement déléguées
AEL	Autorité d'enregistrement locale
AC	Autorité de certification
CP | PC	Certificate Policy | Politique de certification
CPS | DPC	Certification Practice Statement | Déclaration des pratiques de certification
CRL | LRC	Certificate Revocation List | Liste de révocation de certificats
DMZ	Zone démilitarisée
DPE	Déclaration de politique d'enregistrement
DR | RS	Disaster Recovery | Reprise après sinistre
ETSI	Institut européen des normes de télécommunications
eIDAS	Electronic IDentification, Authentication and Trust Services
ISO	Organisation internationale de normalisation
FIPS	Federal Information Processing Standards
HSM	Hardware Security Module
UIT	Union internationale des télécommunications
ICT | TIC	Information and ccmmunication technologies | Technologies de l'information et de la communication
LDAP	Lightweight Directory Access Protocol
MCENMA	Ministère de la Communication, de l'Économie numérique et de la Modernisation de l'administration
OAC	Organe d'accréditation et de contrôle
OCSP	Online Certificate Status Protocol
OTP	One-Time Password
PKCS	Public Key Cryptography Standard

(suite)

PKI | ICP	Public Key Infrastructure | Infrastructure à clés publiques
PSC	Prestataire de services de confiance
RFC	Request for comment
SMTD	Société malienne de transmission et diffusion
SCSE	Service de certification et de signature électronique
SSL	Secure Socket Layer
SIEM	Security Information and Event Management
TLS	Transport Layer Security
TSA	Time Stamping Authority

1 Introduction

1.1 Contexte général

Le Gouvernement du Mali a mis en place une stratégie «Mali numérique 2020». Cette stratégie s'aligne sur la vision du gouvernement de positionner le Mali comme un hub technologique en Afrique, avec pour objectifs de favoriser le développement social et économique, de révolutionner le mode de vie et les relations de travail des personnes, mais aussi de stimuler la culture et l'éducation – entre autres.

Pour mettre en œuvre cette stratégie, le gouvernement a mis en place, à travers les ministères et ses agences, différents services numériques tels que: e-Impôts, OfficeManager, CoRe, eGESCO, AGIC, etc. pour moderniser l'administration et les services publics fournis.

Aussi, le gouvernement s'est lancé dans le développement d'une infrastructure de connectivité Internet: trois mille (3000) kilomètres de fibre ont été déployés, plus de 108% connectés au téléphone, plus de trois millions (3 000 000) connectés sur Internet, dix-huit (18) services publics ont été dématérialisés. Il existe bien d'autres initiatives, dont celle en cours de créer un parc technologique.

Ce développement technologique transforme la vie des sociétés maliennes et améliore la prestation de services, ce qui contribue au développement social et économique. Toutefois, ce progrès notable a également engendré de nouveaux risques de sécurité, des menaces et des pratiques indésirables telles que l'usurpation d'identité, l'accès non autorisé à l'information, la modification non autorisée d'informations électroniques, etc.

Conscient du danger que constituent ces menaces pour la sécurité, le Gouvernement du Mali a choisi de sécuriser les transactions électroniques, les réseaux de communication et les systèmes informatiques. À cet effet, la loi 2016-012/ du 6 mai 2016 relative aux transactions, échanges et services électroniques a été promulguée, conférant à la signature électronique qualifiée la même valeur juridique que la signature manuscrite.

Il devient donc impérieux de fournir au Mali un cadre de mise en place d'une infrastructure à clés publiques (cadre ICP) pour renforcer les capacités nationales en matière de transactions électroniques, de protection contre la fraude à l'identité, d'intégrité des données, de confidentialité des données, d'authentification forte et de non-répudiation, de confiance et de facilité d'utilisation des services en ligne pour les citoyens et les résidents.

Pour mettre en œuvre ce cadre légal, le Gouvernement du Mali, en collaboration avec l'Union internationale des télécommunications (UIT), a lancé le développement du cadre d'infrastructure à clés publiques du Mali (ICP). Le cadre ICP définit tous les composants nécessaires pour mettre en œuvre un système ICP national. La mise en place du système ICP national est conforme au plan directeur de transformation numérique du Mali. L'infrastructure ICP est un catalyseur de la transformation numérique des services publics en ligne, des services bancaires en ligne et du commerce électronique car elle augmente la confiance des utilisateurs dans l'environnement numérique. Elle permettra aux utilisateurs de services en ligne d'authentifier et de signer des transactions électroniques en toute sécurité.

1.2 Infrastructure à clés publiques (ICP)?

L'ICP est l'ensemble du matériel, des systèmes cryptographiques, des rôles, des personnes, des politiques et des procédures nécessaires pour créer, gérer, stocker, distribuer et révoquer les certificats de clé publique basés sur la cryptographie à clé publique. Il s'agit d'une infrastructure capable de prendre en charge la gestion des clés publiques pour assurer les principales fonctions de sécurité, de confidentialité (grâce à l'utilisation du chiffrement), d'intégrité des données et d'authentification et constituer une base raisonnable de non-répudiation grâce à l'utilisation de signatures numériques.

Globalement, l'ICP est un mécanisme de sécurité fiable pour garantir que les communications et les transactions en ligne sont authentiques et privées. Il permet la mise en place d'une communication efficace ainsi que de transactions électroniques en ligne sécurisées, apportant ainsi une solution aux principales préoccupations liées aux transactions électroniques en ligne, notamment pour les services publics en ligne, le commerce électronique, les services bancaires en ligne et les courriels ou documents électroniques confidentiels.

1.3 Avantages d'une infrastructure à clés publiques (ICP)

Les systèmes ICP fournissent non seulement des services de sécurité, mais ils présentent également plusieurs avantages, notamment celui de réaliser une dématérialisation complète des processus et procédures de bout en bout («Zéro Papier, Zéro Impression et Zéro Voyage»), offrant ainsi:

- **Efficacité**: les signatures électroniques simplifient les processus et réduisent fortement le temps de gestion des documents. Le processus de signature peut être automatisé, laissant de côté toutes les tâches manuelles telles que l'obtention d'une signature, l'impression, la numérisation, la publication, l'archivage et la vérification.
- Réduction du **temps** d'approbation: des études de cas ont montré une réduction moyenne de 60 à 80 % du délai d'exécution requis pour faire approuver les documents, lorsqu'ils sont remplis par voie électronique plutôt que par procédure manuelle.
- Réduction des **coûts** d'impression et de numérisation: les documents sont signés et partagés électroniquement sans qu'il soit nécessaire de les imprimer.
- **Mobilité**: les documents peuvent être signés partout et sur tous les appareils, ce qui est pratique pour les responsables en déplacement.
- **Conformité légale**: les signatures électroniques assurent l'authenticité et garantissent que l'identité du signataire est vérifiée. Un document signé électroniquement est recevable par n'importe quel tribunal comme tout autre document papier signé.
- **Protection de l'environnement** grâce à un environnement de travail sans papier.

1.4 Objectifs et étendue de la mission

L'objectif de cette mission est de développer un cadre ICP pour le Mali qui définisse les composants nécessaires pouvant permettre d'établir un système ICP national fonctionnel, la mission comportant les phases suivantes:

Phase I:

- Étude comparative – Plateformes de signature électronique.

Phase II:

- Analyse de l'état actuel de l'ICP au Mali:
  - développement d'un cadre national de l'ICP;
  - cadre de politiques et normes de certification;
  - structure de gouvernance de système de certification électronique;
  - architecture conceptuelle du système national racine (AC racine ou *Root CA*);
  - architecture conceptuelle du système de l'AC gouvernementale (*Gov CA*);
  - exigences relatives au centre informatique de l'ICP nationale (si nécessaire);
  - exigences techniques de mise en œuvre du système ICP national;
- Budget estimatif de la mise en œuvre de l'architecture du système ICP national proposé;
- Méthodologie/phasage de la mise en place de l'ICP nationale;
- Trois (3) jours de formation sur le cadre ICP.

2 Méthodologie appliquée

Le développement du cadre ICP a été géré par le MCENMA avec le soutien de l'UIT. Le projet a été planifié en cinq phases principales:

1. Étude comparative des plateformes de signature électronique sur les marchés;
2. Analyse de l'état actuel de l'ICP au Mali (analyse en l'état): lois, normes internationales et régionales relatives à la signature électronique, applications nécessitant les services de confiance et l'infrastructure pour héberger les systèmes ICP;
3. Élaboration du modèle futur (modèle envisagé);
4. Élaboration du plan de mise en œuvre et du budget;
5. Présentation et approbation du rapport final.

Pour réaliser l'étude comparative des plateformes de signature électronique, l'équipe du Service de certification et signature électronique (SCSE) avec le support de l'expert de l'UIT a défini les critères de sélection de la plateforme de signature électronique. Ces critères prennent en compte les cas d'usages, ainsi que les exigences fonctionnelles et techniques. Les plateformes ont été sélectionnées sur la base des critères définis. Après cette sélection, l'équipe projet a organisé des sessions de travail avec les éditeurs des plateformes sélectionnées afin de mieux comprendre leurs fonctionnalités.

L'élaboration du cadre ICP a ensuite été menée de manière consultative par le biais de groupes de travail établis (le groupe de travail juridique, le groupe de travail e-Gouvernement et le groupe de travail Infrastructure). Les groupes de travail étaient composés de représentants du MCENMA, du ministère de l'Économie et des Finances (MEF), de l'AGETIC, du SMTD et de l'Autorité malienne de régulation des télécommunications, des technologies de l'information et de la communication et des postes (AMRTP).

L'expert de l'UIT a recueilli des informations à travers des questionnaires, des entretiens et des ateliers avec les groupes de travail, et par le biais d'une revue de la documentation relative à la signature électronique. Cette documentation comprenait la loi 2016-012/ du 6 mai 2016 relative aux transactions, échanges et services électroniques, le décret n° 2019-0037/P-RM du 28 janvier 2019, déterminant l'organisation et les modalités de fonctionnement du Service de

certification et de signature électronique et la stratégie d'opérationnalisation du Service de certification et de signature électronique, et le cadre ICP de l'UIT.

Les ateliers techniques ont également permis d'analyser les applications de l'administration en ligne (actuelles et futures) et l'état actuel du centre de données destiné à héberger l'infrastructure à clés publiques (ICP) nationale.

C'est sur cette base qu'un cadre de mise en place d'une ICP nationale adapté à l'environnement du Gouvernement de la République du Mali, y compris le plan de mise en œuvre, a été développé.

3 Partie I: Analyse de l'existant (analyse en l'état)

3.1 Cadre juridique relatif aux services de certification électronique

La loi 2016-012/ du 6 mai 2016, régissant les transactions, les échanges et les services électroniques en République du Mali, aborde la nécessité d'établir des réglementations pour développer et promouvoir l'utilisation de la signature numérique dans les transactions électroniques, ainsi que pour établir la structure de gouvernance des services de certification et de signature électronique au Mali.

Le TITRE VI de ladite loi définit les services de sécurisation des transactions électroniques, y compris: la signature électronique, le certificat électronique, l'archivage électronique et les prestataires de services électroniques de sécurisation. Dans cette loi nous comprenons que l'expression **prestataires de services électroniques de sécurisation** signifie **prestataires de services de confiance**. L'expression «prestataires de services de confiance» est souvent utilisée dans les lois et réglementations internationales relatives à l'identification électronique et aux services de confiance, comme par exemple le cadre eIDAS de l'UE.

3.1.1 Signature électronique

En vigueur depuis 2016, la loi 2016-012/ du 6 mai 2016 relative aux transactions, échanges et services électroniques a créé un cadre juridique pour que les signatures électroniques soient acceptées et légalement reconnues au Mali au même titre que la signature manuscrite. Ladite loi définit la signature électronique comme une «*signature obtenue par un algorithme de chiffrement asymétrique permettant d'authentifier l'émetteur d'un message et d'en vérifier l'intégrité*».

> L'article 110 de ladite loi précise que «*Lorsqu'un procédé fiable de signature électronique préserve les fonctions minimales de la signature énoncée à l'article 108 de la présente loi et qu'en outre, il constitue une* ***signature électronique avancée****, réalisée sur la base d'un* ***certificat qualifié*** *et conçu au moyen d'un* ***dispositif sécurisé de création de signature électronique****, ce procédé est assimilé de plein droit à une* ***signature manuscrite****, qu'il soit réalisé par une personne physique ou morale*».

Recommandation 1: l'aspect juridique relatif au cachet électronique n'est pas clairement défini dans la loi 2016-012/ du 6 mai 2016, régissant les transactions, les échanges et les services électroniques. Il est donc recommandé, en plus de la signature électronique, de définir le cadre juridique du cachet électronique. Les cachets électroniques sont techniquement équivalents aux signatures numériques mais ont une signification juridiquement différente, puisqu'ils peuvent être exécutés sans le consentement direct d'une personne physique et permettent par conséquent l'apposition automatique d'un cachet électronique. Un cachet électronique est défini comme «des données électroniques, jointes ou associées logiquement à d'autres données électroniques pour garantir l'origine et l'intégrité des données». La loi 2016-012/ du 6 mai 2016 relative aux transactions, échanges et services électroniques ne définit pas l'utilisation et les exigences d'un cachet électronique authentique. L'expert de l'UIT recommande d'amender l'actuelle loi relative aux transactions, échanges et services électroniques pour prendre en compte l'utilisation et les exigences d'un cachet électronique dans les services publics en ligne, le commerce électronique et les services bancaires en ligne au Mali.

Recommandation 2: il est recommandé de promulguer un décret rendant obligatoire l'utilisation d'une signature numérique ou signature électronique qualifiée dans les services publics en ligne, le commerce électronique et les services bancaires en ligne.

«Toutes les institutions gouvernementales et entreprises privées fournissant des services en ligne (services publics en ligne, commerce électronique et services bancaires en ligne) à leurs clients doivent exiger l'utilisation de "signatures numériques qualifiées" dans leurs services pour garantir la confidentialité, l'authenticité, l'intégrité et la non-répudiation des transactions électroniques».

3.1.2 Certificat électronique

Le certificat électronique est un document électronique attestant le lien entre des données de vérification de signature électronique et un signataire. Il est délivré par une autorité de certification (AC) accréditée ou qualifiée.

La loi 2016-012/ du 6 mai 2016 relative aux transactions, échanges et services électroniques reconnaît et définit les exigences d'un «certificat qualifié».

Article 114: Un certificat électronique ne peut être considéré comme qualifié que s'il est délivré par un prestataire de services de certification qualifié.

Est considéré comme qualifié, le prestataire de service de certification qui:

1. Se conforme aux dispositions des articles 109 à 114 et 130 à 136 de la présente loi,
2. Fait l'objet d'une accréditation auprès de la structure administrative en charge de la certification, dans des conditions fixées par voie réglementaire.

Article 115: Un certificat électronique qualifié comporte les mentions suivantes:

1. Une mention indiquant que ce certificat est délivré à titre de certificat électronique qualifié;
2. L'identité du prestataire de services de certification électronique ainsi que l'Etat dans lequel il est établi;
3. Le nom du signataire et, le cas échéant, sa qualité;
4. Les données de vérification de la signature électronique correspondant aux données de création de celui-ci;
5. L'indication du début et de la fin de la période de validité du certificat électronique ainsi que le code d'identité de celui-ci;
6. La signature électronique avancée du prestataire de services de certification qui délivre le certificat électronique;
7. Les conditions d'utilisation du certificat électronique, notamment le montant maximum des transactions pour lesquelles ce certificat peut être utilisé.

Recommandation 3: en plus de l'exigence de disposer d'un «certificat qualifié», il est recommandé de mettre en place un cadre réglementaire et des politiques de certification définissant les exigences relatives aux certificats électroniques ou identités électroniques et à leur niveau d'assurance.

3.2 Prestataire de services électroniques de sécurisation et cryptologie

La loi 2016-012/ du 6 mai 2016 relative aux transactions, échanges et services électroniques établit le cadre institutionnel de la certification électronique. Elle crée, dans l'article 151, un service de certification et de signature électronique. Ce cadre institutionnel est un élément très important qui établit les fondements du développement de services de confiance au Mali.

Article 151: Il est créé sous l'autorité du ministère chargé des Technologies de l'Information et de la Communication, un service de certification et de signature électronique. Le service de certification et de signature électronique est chargé de:

- La promotion et la gestion de la certification électronique,
- La promotion et la gestion de la signature électronique.

Par ailleurs, le décret n° 2019-0037/P-RM du 28 janvier 2019 déterminant l'organisation et les modalités de fonctionnement du Service de certification et de signature électronique définit les

organes d'administration et de gestion du Service de certification et de signature électronique, ainsi que leurs rôles et responsabilités.

> **Article 4:** Les organes d'administration et de gestion du Service de Certification et de Signature électronique sont:
>
> - Le Comité de Certification et de Signature électronique;
> - Le Service de Certification et de Signature électronique.

Selon la loi 2016-011/ du 6 mai 2016 portant sur les règles applicables aux moyens, modalités, services et systèmes de cryptologie au Mali, chapitre II, l'Autorité malienne de régulation des télécommunications, des technologies de l'information et de la communication et des postes (AMRTP) est chargée de la régulation des activités et services de cryptologie. La plupart des autorités de certification électronique fournissent des services de chiffrement pour assurer la confidentialité des informations confidentielles ou secrètes.

> **Article 6:** L'autorité de régulation des télécommunications, des technologies de l'information et de la communication et des postes, sans préjudice des missions qui lui sont assignées par les lois et règlements en vigueur, est chargée de la régulation des activités et de services de cryptologie.

Après l'analyse du cadre juridique, il a été constaté que les éléments manquants relatifs à l'accréditation et au contrôle des autorités de certification et des prestataires de services de confiance au Mali ne sont pas bien définis. Le comité a aussi pour rôle d'accréditer les AC, d'attribuer ou de retirer le statut «qualifié» et de contrôler les activités des prestataires de services de confiance, avec l'objectif d'assurer leur conformité aux lois, politiques et règlements relatifs aux services de certification électronique.

En outre, le cadre juridique ne définit pas d'une manière claire les rôles et responsabilités de tous les acteurs intervenant dans la gestion du système de certification électronique nationale.

Recommandation 4: restructurer le Comité de Certification et de Signature électronique existant et le transformer en un «organe d'accréditation et de contrôle» chargé de qualifier, de contrôler et d'évaluer les autorités de certification (AC) électronique et les **prestataires de services de confiance**, ainsi que les services qu'ils fournissent au Mali.

Une fois cette recommandation prise en compte, le décret n°2019-0037/P-RM du 28 Janvier 2019 déterminant l'organisation et les modalités de fonctionnement du service de certification et de signature électronique devrait être révisé pour prendre en compte la création de «l'Organe d'accréditation et de contrôle».

Recommandation 5: restructurer le SCSE. La mise en place d'une structure dédiée pour la certification et la signature électronique est un choix stratégique pour accélérer le développement du SCSE au Mali. Elle pourra non seulement assurer la fourniture de SCSE, mais également rechercher et développer des solutions de signature et de cachet électronique et des solutions de chiffrement, mettre en œuvre une stratégie d'identité numérique (*Digital ID*), participer et contribuer à la mise en œuvre de la stratégie de transformation numérique, etc.

Une fois cette recommandation prise en compte, le décret n°-2019-0037/P-RM du 28 janvier 2019 déterminant l'organisation et les modalités de fonctionnement du service de certification et de signature électronique devrait être révisé, pour prendre en compte la création d'une Autorité nationale de certification électronique (ANCE), avec ses rôles et responsabilités.

Recommandation 6: il est fortement recommandé de prendre en compte les représentants des fournisseurs des services, en particulier les banques et les opérateurs de télécommunications, dans le comité de certification et de signature électronique.

3.3 Étude comparative des cadres de gouvernance ICP dans d'autres pays

Tableau 1: Synthèse de l'étude comparative des AC d'autres pays

Pays modèle	Implication du gouvernement	Implication du secteur privé	Services
Rwanda			Au Rwanda, l'Autorité de régulation des services publics du Rwanda (RURA) est l'autorité de certification racine (*Root CA*). Elle contrôle les activités des autorités de certification, gère et exploite le système *Root CA*. L'Autorité rwandaise de la société de l'information (RISA) est l'autorité de certification gouvernementale (*Gov CA*). La RISA a établi une autorité d'enregistrement (AE) centrale qui identifie et délivre les certificats aux abonnés (employés du gouvernement, personnes morales et personnes physiques).
Kenya			Au Kenya, l'Autorité des communications du Kenya (CA) est l'autorité de certification racine. Elle contrôle les activités des autorités de certification, gère et exploite le système *Root CA*. L'ICT Authority (ICTA) est l'autorité de certification gouvernementale (*Gov CA*). Elle délivre les certificats numériques pour l'authentification et la signature numérique aux employés du gouvernement. L'ICTA dispose d'une autorité d'enregistrement (AE) centrale qui identifie et délivre les certificats aux abonnés (employés du gouvernement).
Tunisie			En Tunisie, l'Agence nationale de certification électronique (ANCE) – TUNTRUST contrôle les activités des autorités de certification, gère et exploite le système de l'autorité de certification (*Root CA*), de l'autorité de certification gouvernementale (*Gov CA*) et de l'autorité de certification privée (*Private CA*). L'ANCE – TUNTRUST est une entreprise publique non-administrative sous tutelle du ministère des Technologies de la communication et de l'économie numérique. Elle vend les services de confiance aux clients finaux. Pour créer un écosystème, TUNTRUST a créé un cadre d'agrément avec les autorités d'enregistrement déléguées (AED) pour vendre les certificats aux abonnés.

(suite)

Pays modèle	Implication du gouvernement	Implication du secteur privé	Services
Bénin			Au Bénin, l'Organe de contrôle (OC) est le contrôleur des prestataires de service de confiance. Cet organe fait partie du ministère de l'Économie numérique. L'Agence nationale de sécurité du système d'information (ANSSI) est l'autorité de certification racine, qui gère et exploite le système *Root CA*. L'Agence des services et des systèmes d'information (ASSI) est l'autorité de certification gouvernementale (*Gov CA*). Elle délivre les certificats numériques aux employés du gouvernement, aux personnes physiques et morales. L'ASSI a mis en place une autorité d'enregistrement (AE) centrale qui identifie et délivre les certificats électroniques aux abonnés (employés du gouvernement, personnes morales et personnes physiques).
Inde			En Inde, le ministère de l'Électronique et des technologies de l'information est le contrôleur des autorités de certification. À ce titre, il gère et exploite le système *Root CA*. L'infrastructure à clés publiques (ICP) en Inde est mise en œuvre par la création d'autorités de certification (AC) agréées. Les AC agréées gèrent et exploitent leurs systèmes ICP, vendent les certificats aux abonnés et fournissent les services de confiance. Les AC privées, via leurs AE, identifient et délivrent les certificats aux abonnés (personnes morales et personnes physiques).
Luxembourg			Au Luxembourg, LuxTrust est l'autorité de certification (AC) et le prestataire de services de confiance qualifié, détenu par le gouvernement et le secteur privé, principalement les banques. Il gère et exploite son système de certification et de signature électronique. Les banques et la chambre de commerce sont des autorités d'enregistrement déléguées. LuxTrust a mis en place une autorité d'enregistrement (AE) qui identifie et délivre les certificats électroniques aux abonnés (employés du gouvernement, personnes morales et personnes physiques).

(suite)

Pays modèle	Implication du gouvernement	Implication du secteur privé	Services
Estonie			En Estonie, SK est l'autorité de certification (AC), qui gère et exploite son système d'autorité de certification électronique à travers l'Autorité de système d'information (RIA). Le gouvernement assure l'existence et le fonctionnement de l'ICP. SK est un prestataire de services de confiance privé. La Police nationale est l'autorité d'enregistrement. Elle incorpore les certificats électroniques dans la puce de la carte d'identité électronique (eID) et les opérateurs mobiles incorporent les certificats électroniques dans les cartes SIM (*Mobile ID*). Les identités électroniques (SMART ID) sont livrées en ligne aux abonnés à partir de leur carte d'identité électronique (eID).

Recommandation 7: Modèle pour le Mali

Pays modèle	Implication du gouvernement	Implication du secteur privé	Services
Mali			En République du Mali, le gouvernement doit mettre en place une structure de gouvernance de la certification électronique. Le comité de certification et signature électronique peut être restructuré pour jouer le rôle de l'organe d'accréditation et de contrôle des AC au Mali, et le Service de certification et signature électronique (SCSE) peut être transformée en une Autorité nationale de certification électronique (ANCE). L'ANCE gère et exploite le système de l'autorité de certification (*Root CA*) et l'autorité de certification gouvernementale (*Gov CA*). L'ANCE fournit les services de certification et signature électronique à l'administration publique, aux entreprises et aux personnes physiques. Sa structure organisationnelle comporte une autorité d'enregistrement (AE) centrale et il y est créé un cadre d'agrément avec les autorités d'enregistrement déléguées (AED) pour délivrer les certificats aux usagers finaux.

3.4 Règlements relatifs aux autorités de certification (AC)

Après analyse des différents documents, il a été constaté qu'aucun règlement ne définit les exigences et les procédures d'accréditation des autorités de certification qualifiées, ainsi que leurs services de certification et de signature électronique au Mali. La première étape pour améliorer le cadre juridique consiste à instituer un cadre réglementaire relatif aux autorités de certification, à mettre en place une directive et à notifier les AC en vertu de la loi relative aux transactions, échanges et services électroniques. Le MCENMA, à travers l'organe ou le service de contrôle des autorités de certification, a la responsabilité de mettre en place la réglementation des systèmes de l'ICP nationale au Mali.

Recommandation 7: sur la base de l'article 142 de la loi 2016-012/ du 6 mai 2016 relative aux transactions, échanges et services électroniques, le MCENMA, à travers l'organe ou le service de contrôle des autorités de certification, a la responsabilité d'établir les lignes directrices et les règlements suivants:

- Critères d'accréditation, procédure d'accréditation et d'audit des AC:
  - normes relatives aux systèmes et équipements des AC;
  - normes relatives à l'ICP ;
  - cadre de la politique de certification (PC) et déclaration des pratiques de certification (DPC).
- Projet de décret pour:
  - institutionnaliser un système de certification et de signature électronique au Mali;
  - réviser la loi 2016-012/ du 6 mai 2016 déterminant l'organisation et les modalités de fonctionnement du service de certification et de signature électronique pour désigner les organes ou entités gouvernementales chargés de mettre en œuvre le programme de certification;
  - définir par décret l'utilisation et l'application obligatoires de signatures numériques dans tous les services publics en ligne, le commerce électronique et les services bancaires en ligne.

3.5 Services publics en ligne

3.5.1 Applications existantes et futures

Le Gouvernement du Mali, à travers l'AGETIC, avait initié différents projets visant à dématérialiser les processus et procédures, avec l'objectif de moderniser l'administration publique. Plusieurs projets sont en cours d'exécution, comme par exemple la dématérialisation des marchés publics (*e-Procurement*), etc. Il est également prévu que la plateforme de signature électronique soit mise en service avant la fin de l'année 2021, et le système *e-Procurement* en 2022.

Les applications existantes et celles en cours de développement utilisent un mécanisme d'authentification (avec nom d'utilisateur et mot de passe) pour authentifier les utilisateurs et une signature électronique de base (une signature manuscrite scannée) pour signer les documents électroniques.

Le tableau ci-dessous présente un résumé des principales applications existantes et futures. Les services de sécurité requis sont également indiqués, afin d'assurer la confiance des utilisateurs de ces applications.

Tableau 2: Applications existantes et en cours de développement

N°	Application	Structure	Priorité	Services requis
1	**Egesco:** application de gestion de courriers	AGETIC	Élevée	Signature numérique
2	**AGIC:** système d'archivage électronique	AGETIC	Élevée	Signature numérique
3	**Core:** système de gestion des dossiers d'appel d'offre	AGETIC	Élevée	Authentification, signature numérique et chiffrement
4	**Démarches administratives**	AGETIC	Élevée	Signature numérique et chiffrement
5	**Office Manager:** système unifié de gestion des ressources humaines, de pilotage financier et de suivi des activités des utilisateurs	AGETIC	Élevée	Signature numérique
6	**e-Procurement:** système de gestion des marchés publics	Ministère des Finances	Élevée	Authentification, signature numérique et chiffrement
	e-Impôts	Direction générale des impôts	Élevée	Authentification et signature numérique
7	Etc.			

3.5.2 Applications cibles et prioritaires des services ICP

Dans le cadre de la stratégie de transformation numérique de l'AGETIC, le gouvernement envisage de dématérialiser les services publics. Tous ces services nécessitent l'usage de signatures numériques basées sur la technologie ICP.

Le tableau ci-dessous présente un résumé des applications cibles qui nécessitent des services de sécurité basés sur l'ICP. Ces applications utilisent la signature numérique à grande échelle dans les processus et procédures.

Tableau 3: Applications cibles des services ICP

N°	Applications	Services de sécurité
1	e-Procurement	Authentification, signature numérique et chiffrement
2	e-Impôts	Authentification et signature numérique
3	eGesco, Agic et Core	Authentification, signature numérique et chiffrement
4	e-Payment / e-Banking	Authentification et signature numérique

Tableau 3: Applications cibles des services ICP (suite)

N°	Applications	Services de sécurité
6	Portail des services publics	Authentification et signature numérique
7	e-Santé	Authentification et signature numérique
8	e-Education	Authentification et signature numérique

Recommandation 8: les applications ci-dessus nécessitent une signature électronique sécurisée, une authentification forte et un chiffrement pour assurer l'intégrité, la non-répudiation et la confidentialité des données traitées par ces applications. L'ICP est la seule technologie capable de fournir ces services de sécurité. L'AGETIC et la SCSE doivent donc planifier l'intégration de ces applications avec l'ICP nationale après sa mise en place.

3.6 Infrastructure des centres de données

Pour assurer la sécurité et la disponibilité des services de certification, les systèmes ICP doivent être hébergés dans un centre de données ultra-sécurisé par des moyens physiques et logiques. Le Gouvernement du Mali, à travers ses agences, a mis en place deux centres de données, l'un géré par la Société malienne de transmission et de diffusion (SMTD), et l'autre par l'Agence des technologies de l'information et de la communication (AGETIC).

3.6.1 Société malienne de transmission et de diffusion (SMTD)

La SMTD est une société chargée de la distribution et de la gestion des infrastructures de télécommunications de l'État. Elle fournit des services publics relatifs au développement numérique incluant des services de centre de données, comme par exemple un service de colocalisation, centre de données intégré (IDS), Infrastructure as a Services (IaaS), Software as a Service (SaaS) et un service de sauvegarde (Backup). La SMDT est en train d'établir le site de reprise après sinistre (DR, *disaster recovery*) pour assurer la disponibilité et la restauration des services en cas d'incident ou sinistre sur le site principal.

La SMTD est en train d'améliorer les centres de données existants pour se conformer aux exigences du niveau de disponibilité Tier III de l'Uptime Institute. Les projets en cours sont:

- la planification de la mise en place du site secondaire pour les services de reprise après sinistre. Les locaux et infrastructures de base tels que les baies, l'infrastructure réseau, l'énergie, etc. sont déjà en place;
- la certification ISO 27001 pour assurer la sécurité des systèmes et services de leurs clients;
- le développement des locaux du centre de données pour se conformer aux exigences du niveau de disponibilité Tier III en assurant la redondance des infrastructures d'énergie, de télécommunications, de refroidissement, d'incendie, de contrôle d'accès et de vidéosurveillance.

Pour contrôler l'accès aux locaux du centre de données, la SMDT a mis en place les différents contrôles de sécurité suivants:

- systèmes de contrôle d'accès biométrique et par badge, système de vidéosurveillance (CCTV) et agents de sécurité;

- systèmes de sécurité tels que pare-feu et pare-feu d'applications Web (WAF, *Web application firewall*). En fonction des besoins du client, la SMDT peut fournir des services de sécurité supplémentaires tels qu'un équilibreur de charge (F5), un pare-feu et un WAF spécifique, des services de surveillance (SOC) ainsi que des gestionnaires de services;
- politiques de sécurité en cours d'élaboration dans le projet ISMS 27001, pouvant être partagées avec les clients.

3.6.2 Agence des technologies de l'information et de la communication (AGETIC)

L'AGETIC est une agence gouvernementale sous la tutelle du MCENMA, chargée de la modernisation de l'administration publique. Elle met en œuvre la stratégie nationale en matière de TIC, d'infrastructures, de dématérialisation des processus dans l'administration, etc. L'AGETIC a mis en place une administration des centres de données; elle met à disposition de l'administration des services d'hébergement, comme par exemple, Infrastructure as a Service (IaaS), Software as a Service (SaaS), sauvegarde (Backup) et assure la sécurité de ces systèmes grâce à l'équipe spécialisée en cybersécurité. Pour contrôler l'accès aux locaux du centre de données, l'AGETIC a mis en place les différents systèmes de contrôles de sécurité suivants:

- les infrastructures énergétiques (source d'énergie, générateurs, onduleurs, etc.) ne sont pas redondantes, sauf pour les UPS qui sont installées en redondance;
- l'AGETIC dispose d'un site de secours (DR) qui synchronise la réplication en temps réel;
- les systèmes hébergés dans le centre de données sont protégés par des pare-feux, des serveurs proxy de pare-feu et un système SIEM de gestion des événements de sécurité pour surveiller la sécurité des systèmes dans le centre;
- le centre de données est sécurisé par des systèmes de contrôle d'accès biométrique et par badge, un système de vidéosurveillance (CCTV), des portes blindées et des agents de sécurité.

Recommandation 9: le choix du centre de données destiné à héberger les systèmes de l'ICP nationale étant critique, il est recommandé de choisir le centre pouvant assurer la confidentialité, l'intégrité et la disponibilité du service de certification et de signature électronique. Le centre de données doit être conforme aux normes ISO 27001 et aux exigences du niveau de disponibilité Tier III. Le choix doit prendre en compte les exigences suivantes:

- la redondance des infrastructures du centre de données (par exemple énergie, télécommunications, refroidissement, système d'extinction des incendies, etc.);
- les systèmes de contrôle d'accès (combinaison d'un contrôle d'accès biométrique et par badge), les systèmes de vidéosurveillance (CCTV) et les agents de sécurité du centre de données;
- le système de prévention, de détection et de surveillance des intrusions (cyber-attaques);
- le site de reprise après sinistre (DR, *Disaster Recovery*) qui réplique ou synchronise les données en temps réel avec le site principal ou le site de production;
- la possibilité de mettre en place des confinements dédiés à l'hébergement du système ICP national (AC racine, AC gouvernementale et autres infrastructures informatiques).

Recommandation 10: le centre de données de la SMDT semble répondre aux exigences minimales pour héberger l'infrastructure des services de certification et de signature électronique, mais la SMDT doit finaliser le site de reprise après sinistre (*Disaster Recovery*) pour le rendre opérationnel. La SMDT doit fournir des confinements ou des centres de données intégrés (IDS) dédiés pour la zone du système ICP national isolé. L'accès au confinement du

système ICP doit être strictement contrôlé et interdit, sauf au personnel habilité ou autorisé par la SCSE.

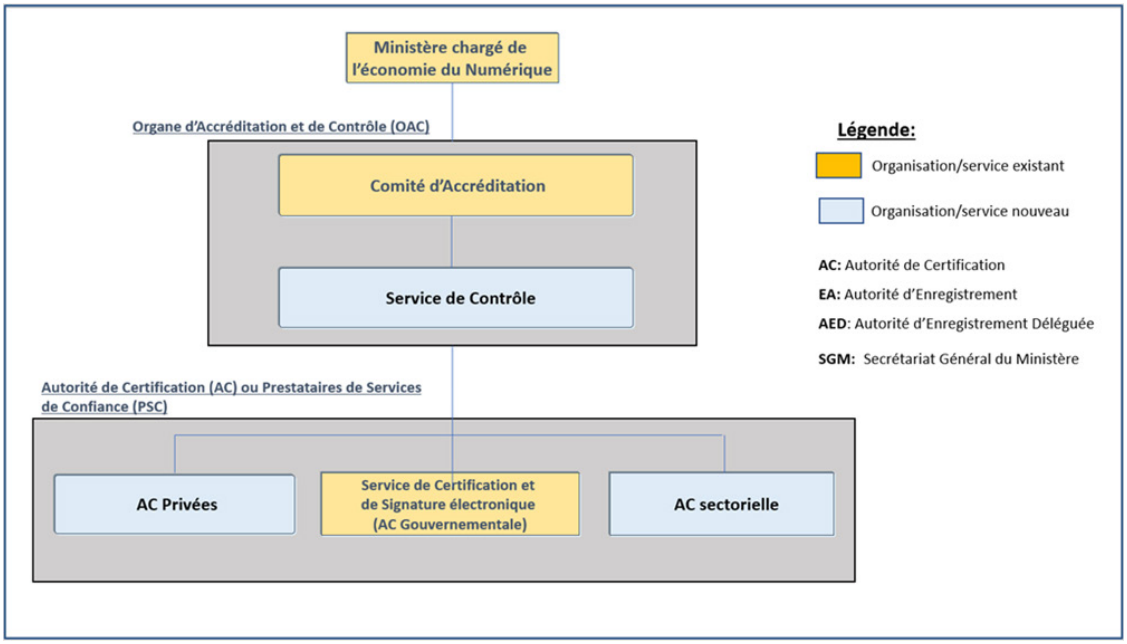
4 Partie II: Modèle futur de l'ICP nationale (modèle envisagé)

4.1 Structure de gouvernance du système de certification électronique national

Pour assurer le bon fonctionnement du système national de certification et de signature électronique, il est recommandé d'établir une structure de gouvernance du système de certification national qui garantisse la mise en place et la mise en service dudit système, afin de fournir les services de certification et signature électronique au Mali. La structure de gouvernance de la certification électronique comprend trois composantes principales:

- l'organe d'accréditation et de contrôle (OAC);
- les autorités de certification électronique ou prestataires de services de confiance;
- les autorités d'enregistrement (AE) ou autorités d'enrôlement déléguées (AED).

Figure 1: Structure organisationnelle



4.1.1 Organe d'accréditation et de contrôle (OAC)

L'organe d'accréditation et de contrôle est chargé de contrôler les activités des prestataires de services de confiance accrédité et établis en République du Mali afin de s'assurer que leurs prestations satisfassent, d'une part, aux exigences prévues par la loi 2016-012/ du 6 mai 2016 relative aux transactions, échanges et services électroniques, et, d'autre part, aux règlements, politiques de certification et normes en la matière. L'organe d'accréditation et de contrôle est chargé de mettre en place un écosystème pour tous les prestataires de services de

confiance, dans l'intérêt général des consommateurs. La structure organisationnelle de l'organe d'accréditation et de contrôle comprend:

- un comité d'accréditation;
- un service de contrôle.

a) Comité d'accréditation

Le comité d'accréditation est l'organe décisionnel des services de confiance, ayant pour mission principale d'accréditer et de contrôler les AC et prestataires de services de confiance au Mali. Il est assisté dans cette mission par le service de contrôle. Il est chargé:

- d'établir les orientations stratégiques de développement du système national de certification de la signature numérique;
- de statuer et de délibérer sur les spécifications techniques de certification et de signature électronique;
- d'émettre des avis sur les questions relatives aux services de sécurisation électronique ou services de confiance visés par la loi 2016-012/ du 6 mai 2016 relative aux transactions, échanges et services électroniques, à la demande de l'autorité de tutelle ou de sa propre initiative;
- d'élaborer des rapports périodiques et un rapport annuel à l'attention de l'autorité de tutelle;
- d'initier toute étude susceptible de soutenir des réformes en matière de certification et de signature électronique;
- de valider le plan d'audit soumis par le service de contrôle;
- d'émettre un avis en matière d'octroi, de renouvellement, ou de retrait des accréditations ou de la qualification des autorités de certification ou des prestataires de services de sécurisation électronique;
- d'approuver les règlements, les politiques et les normes de certification et de signature électronique;
- de coopérer, pour le compte du Gouvernement de la République du Mali, avec les instances internationales compétentes pour la reconnaissance mutuelle des signatures électroniques avec les gouvernements étrangers et les organisations internationales;
- de promouvoir l'usage de la signature électronique dans les services publics en ligne, le commerce électronique et les services bancaires en ligne.

b) Service de contrôle

Le service de contrôle est une branche technique du comité d'accréditation, ayant pour mission principale d'évaluer et d'auditer les AC et prestataires de services de confiance au Mali. Il est chargé:

- de mettre en place les règles, politiques et normes nécessaires à l'exploitation des systèmes du système de certification électronique et les critères d'accréditation des autorités de certification électronique;
- d'étudier les demandes d'accréditation des autorités de certification accréditées;
- d'effectuer les audits réguliers des autorités de certification accréditées et d'assurer le suivi des non-conformités et de la mise en œuvre des recommandations du comité d'accréditation;
- de suivre les procédures d'octroi, de renouvellement ou de retrait d'accréditation des AC et des services qu'elles fournissent;
- de soumettre des rapports périodiques au comité d'accréditation et à l'attention de l'autorité de tutelle;

- d'assurer la mise en œuvre des délibérations du comité d'accréditation;
- d'assurer la conformité aux lois, aux règlements, aux politiques de certification et aux normes en la matière;
- de contribuer à la coopération internationale en matière de services de certificats, y compris la reconnaissance mutuelle et la certification croisée avec les ICP d'autres domaines.

Note 1: l'Article 3 de la loi 2016-012/ du 6 mai 2016 déterminant l'organisation et les modalités de fonctionnement du service de certification et de signature électronique le rattache au secrétariat général du ministère chargé de l'Économie numérique.

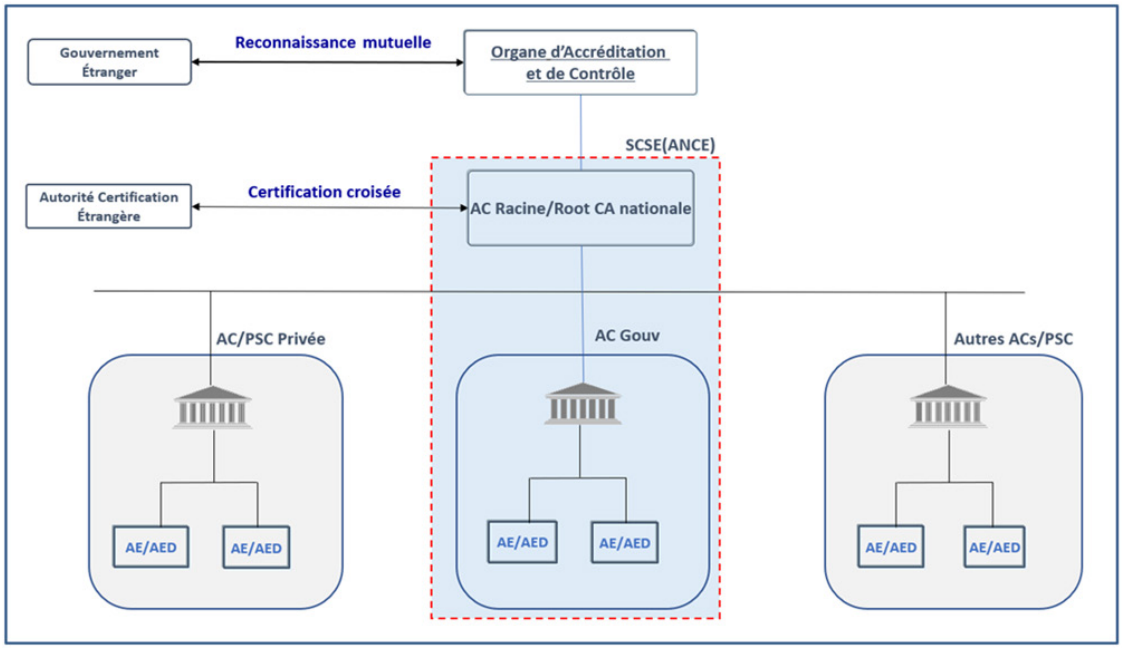
Note 2: la loi 2016-011/ du 6 mai 2016 portant sur les règles applicables aux moyens, modalités, services et systèmes de cryptologie au Mali indique, au Chapitre II, que l'AMRTP est chargée de la réglementation des activités et services de cryptologie. La plupart des prestataires de certification électronique fournissent des services cryptographiques. Les systèmes de certification électronique sont basés sur la technologie cryptographique. Dans le cadre de la mutualisation des services, il est également possible de rattacher le service de contrôle des AC et des prestataires de services de confiance à l'AMRTP.

4.1.2 Autorités de certification (AC)

Les autorités de certification électronique ou prestataires de services de confiance sont chargés:

- de faire la demande d'accréditation à l'autorité ou à l'organe d'accréditation et de contrôle;
- de fournir des rapports périodiques d'activité et d'audit à l'autorité ou à l'organe d'accréditation et de contrôle;
- de fournir les services de confiance comme par exemple: le service de certification électronique, le service de signature électronique, le service d'archivage électronique, le service d'horodatage électronique, le service d'authentification de sites internet, etc., aux usagers finaux;
- d'exploiter leurs systèmes de certification électronique.

Figure 2: Structure fonctionnelle des AC/PSC



4.1.2.1 Autorité de certification racine (Root CA) nationale

L'autorité de certification racine est le plus haut niveau d'autorité de l'ICP et représente le «point d'ancrage de confiance» de la chaîne de confiance, dans le contexte des services de certification électronique. L'autorité de certification racine nationale est auto-signée et utilisée pour certifier ou «signer» les autorités de certification accréditées, renouveler et révoquer les certificats de l'autorité de certification et publier les listes de révocation des autorités (LRA).

Rôles et responsabilités de l'autorité de certification racine nationale:

- exploiter les systèmes de l'autorité de certification racine (*Root CA*);
- émettre et signer les certificats des autorités de certification avec la clé privée de l'autorité de certification racine;
- renouveler ou révoquer les certificats des AC en cas de non-respect de la loi, des politiques, des réglementations et des normes applicables;
- publier les listes de révocation des autorités (LRA);
- auditer périodiquement les AC accréditées par l'AC racine nationale pour s'assurer de leur conformité aux politiques de certification;
- soutenir la coopération internationale en matière de services de certification, y compris la reconnaissance mutuelle et la certification croisée;
- promouvoir l'utilisation de la signature numérique au Mali.

Note: l'Article 151 de la loi relative aux transactions, échanges et services électroniques crée le **Service de Certification et Signature Électronique (SCSE)**. À cet effet, le SCSE gère et exploite le système de l'autorité de certification racine (*Root CA*) nationale.

4.1.2.2 Autorités de certification émettrices (AC accréditées)

Une AC accréditée est une entité publique ou privée répondant aux critères d'accréditation. Il n'existe actuellement aucune AC accréditée au Mali pour fournir des services de certification numérique. Au stade initial, l'équipe de consultants recommande au gouvernement de diriger la

mise en place d'une autorité de certification accréditée pour commencer à fournir des services de sécurité dans les domaines des services publics en ligne, du commerce électronique et des services bancaires en ligne au Mali. L'AC accréditée doit être établie par la loi. Conformément à la politique du gouvernement en matière d'«identité numérique», l'autorité compétente accréditée peut être une structure gouvernementale existante ou une entité privée.

L'autorité de certification est l'autorité chargée de délivrer et gérer les certificats numériques pour assurer l'authentification et l'identification des utilisateurs et leur fournir une signature numérique visant à garantir l'intégrité des données et la non-répudiation des transactions électroniques au niveau des services en ligne tels que les services publics en ligne, le commerce électronique, les services bancaires en ligne, etc. Les rôles et les responsabilités de l'AC sont les suivants:

- exploiter les systèmes de l'autorité de certification;
- émettre et gérer (créer/délivrer/révoquer/réactiver/suspendre) les certificats numériques des utilisateurs finaux (citoyens, entreprises et équipements);
- fournir des services de signature et d'horodatage électronique;
- publier les listes de révocation des certificats (LRC);
- fournir des services de vérification de la validité des certificats en temps réel;
- gérer et superviser les opérations de l'autorité d'enregistrement (AE) et vérifier si elles sont conformes aux règles, politiques et normes de l'ICP.

Note: l'Article 151 de la loi relative aux transactions, échanges et services électroniques crée le **Service de Certification et Signature Électronique (SCSE)**. À cet effet, le SCSE constitue l'autorité de certification gouvernementale (*Gov CA*) de la République du Mali. Il gère et exploite le système *Gov CA*.

Pour développer les capacités et promouvoir les services de certification électronique au Mali, il est recommandé de transformer la SCSE en une **Agence Nationale de Certification Electronique (ANCE)** capable de fournir ces services à l'administration publique, aux entreprises privées et aux citoyens.

4.1.2.3 Autorités d'enregistrement (AE)

Les autorités d'enregistrement (AE) constituent l'interface entre les utilisateurs de certificats numériques et l'autorité de certification. Les AE jouent un rôle majeur dans l'identification et l'authentification des demandeurs de certificats numériques en s'assurant que les contraintes liées à l'usage d'un certificat sont remplies. En outre, les requêtes des utilisateurs de certificats numériques sont traitées par l'autorité d'enregistrement conformément à la politique de certification. Une AC peut fonctionner avec une AE centrale et des autorités d'enregistrement déléguées (AED). Les rôles de l'AE sont les suivants:

- effectuer une vérification d'identité en face à face avec ses agents de confiance;
- tenir des registres des vérifications d'identité effectuées;
- certifier que l'identité du représentant de l'AED a été validée conformément à la PC;
- créer et gérer les certificats des AED;
- assister les AED dans l'élaboration de leurs déclarations de pratiques d'enregistrement (DPE) respectives;
- s'assurer que les DPE soumises par les AED sont conformes à la PC; et
- veiller à ce que les AED émettent et gèrent les certificats conformément à leurs DPE.

Note: le service de certification et signature électronique (SCSE) ou l'ANCE comporte une autorité d'enregistrement (AE) centrale dans sa structure organisationnelle.

4.1.3 Autorités d'enregistrement déléguées (AED)

Les AED délivrent les certificats numériques au profit ou au nom de l'AC, elles ne sont pas dans la structure organisationnelle de l'AC. Toute structure conforme aux politiques et approuvée par l'AC peut délivrer des certificats aux utilisateurs. L'AC et l'AED doivent signer un accord ou un agrément pour la délivrance de certificats aux usagers. Les rôles des AED sont les suivants:

- soumettre une DPE définissant la manière dont l'AED va délivrer et gérer les certificats à l'AC pour examen et approbation;
- effectuer une vérification d'identité des abonnés en face à face lorsque nécessaire;
- délivrer les certificats aux abonnés;
- tenir des registres des vérifications d'identité effectuées;
- certifier que l'identité des abonnés a été validée conformément à la DPE;
- créer et gérer les informations de certificats des abonnés.

Note: les ministères sont les autorités d'enregistrement déléguées (AED) pour les employés dans leur secteur respectif. Le ministère de l'Administration Territoriale est l'AED chargée de délivrer les certificats dans la puce de la carte d'identité nationale. D'autres structures publiques ou entreprises privées (par exemple les banques ou opérateurs télécom) peuvent demander à devenir une AED en sollicitant l'ANCE, pour pouvoir délivrer les certificats numériques aux utilisateurs de leurs services.

4.2 Cadre juridique

La loi de 2016 relative aux transactions, échanges et services électroniques du Mali reconnait la signature et le certificat électronique ou certificat qualifié et l'horodatage électronique. Cette loi définit également les exigences relatives aux prestataires techniques de services de sécurisation des transactions, des échanges et services électroniques.

Cependant, certains éléments importants ne sont pas clairement définis dans la loi, tels que: l'identification électronique, le cachet électronique, l'utilisation de la signature numérique et du cachet électronique dans les services publics. De plus, il n'existe pas de règlement définissant les critères, les exigences et les procédures d'accréditation des autorités de certification ou des prestataires de confiance au Mali.

4.2.1 Identification électronique

La loi de 2016 relative aux transactions, échanges et services électroniques prévoit les exigences minimales relatives à un «certificat numérique». Un certificat numérique est une identité électronique utilisée dans l'environnement numérique, il est équivalent d'une carte d'identité nationale ou d'un passeport. Pour assurer la confiance dans l'environnement numérique, il est important de mettre en place un cadre juridique et réglementaire relatif à l'identification électronique au Mali. Le cadre juridique et réglementaire du Mali doit prendre en compte les différents niveaux d'assurance des identités électroniques suivants.

- **Niveau d'assurance faible:** une identité électronique faible offre un degré de confiance limité dans l'identité revendiquée d'une personne. Elle se caractérise par une référence

aux spécifications techniques, normes et procédures qui s'y rapportent, y compris les contrôles techniques, dont le but est de réduire le risque d'usurpation ou d'altération de l'identité.

- **Niveau d'assurance substantiel:** une identité électronique substantielle fournit un degré substantiel de confiance dans l'identité revendiquée d'une personne. Elle se caractérise par une référence aux spécifications techniques, normes et procédures qui s'y rapportent, y compris les contrôles techniques, dont le but est de réduire considérablement le risque d'usurpation ou d'altération de l'identité
- **Niveau d'assurance élevé:** une identité électronique élevée offre un degré de confiance plus élevé dans l'identité revendiquée d'une personne que les moyens d'identification électronique avec un niveau d'assurance substantiel. Elle se caractérise par une référence aux spécifications techniques, normes et procédures qui s'y rapportent, y compris les contrôles techniques, dont le but est d'empêcher l'usurpation ou l'altération de l'identité.

Les spécifications techniques, normes et procédures minimales de l'identification électronique sont les suivantes:

a) procédure de preuve et de vérification de l'identité des personnes physiques ou morales qui demandent la délivrance d'une identification électronique;
b) procédure de délivrance des identifications électroniques;
c) mécanisme d'authentification, par lequel la personne physique ou morale utilise les moyens d'identification électronique pour confirmer son identité à une partie utilisatrice;
d) entité délivrant les moyens d'identification électronique;
e) tout autre organisme impliqué dans la demande de délivrance du moyen d'identification électronique;
f) spécifications techniques et de sécurité des moyens d'identification.

4.2.2 Cachet électronique

Un cachet électronique est un moyen d'apposer un tampon sur des documents au nom d'une entité publique ou d'une entreprise privée. Le cachet électronique garantit l'origine des documents numériques et il est destiné aux personnes morales. Il est recommandé de réviser la loi actuelle de 2016 relative aux transactions, échanges et services électroniques pour prendre en compte l'usage du cachet électronique au Mali. Les éléments suivants doivent être pris en compte:

a) un cachet électronique doit être lié au créateur du cachet d'une manière unique;
b) il doit permettre d'identifier le créateur du cachet;
c) Il doit être créé à l'aide de données de création de cachet électronique que le créateur du cachet peut, avec un niveau de confiance élevé, utiliser sous son contrôle pour créer un cachet électronique;
d) il doit être lié aux données auxquelles il est associé, de telle sorte que toute modification ultérieure des données soit détectable;
e) il doit être basé sur un «certificat numérique qualifié» délivré par une autorité de certification accréditée au Mali ou une autorité de certification étrangère reconnue par l'autorité.

En outre, les éléments suivants doivent être pris en compte lors de la définition des exigences relatives à un cachet électronique:

a) exigences de cachet électronique avancées;
b) exigences de certificats de cachet électronique qualifiés;
c) utilisation de cachet électronique dans les services publics;

d) exigences applicables aux dispositifs pour la création et la validation de cachets électroniques qualifiés.

4.2.3 Décret relatif à l'utilisation de la signature numérique dans les services en ligne

La loi de 2016 relative aux transactions, échanges et services électroniques ne prévoit pas l'utilisation obligatoire des certificats numériques basés sur l'ICP. L'une des méthodes les plus efficaces pour promouvoir l'utilisation d'une signature numérique consiste à promulguer une loi sur l'utilisation obligatoire d'une signature numérique dans les services publics en ligne, le commerce électronique et les services bancaires en ligne. Outre les clauses relatives à la signature numérique dans la loi de 2016 relative aux transactions, échanges et services électroniques, il est recommandé de réviser ladite loi ou de promulguer un décret rendant obligatoire l'utilisation de la signature numérique dans les services publics en ligne, le commerce électronique et les services bancaires en ligne au Mali. Les éléments suivants doivent être pris en compte:

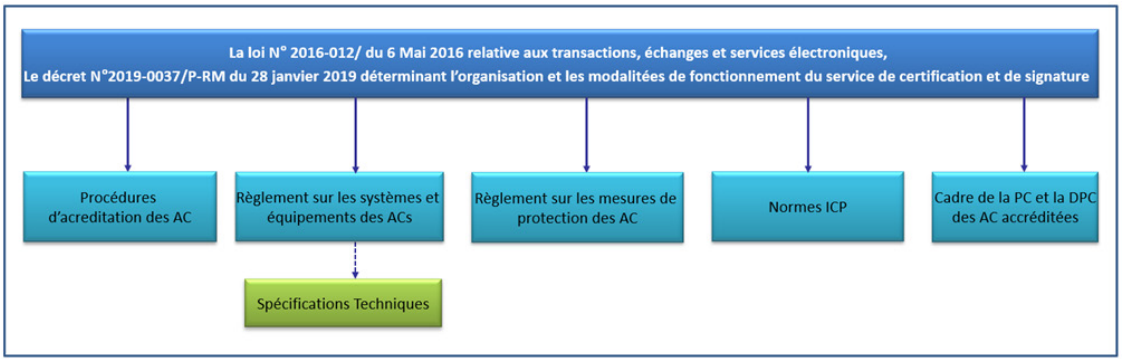
- application des signatures numériques dans les services d'administration électronique dans le secteur public: «toutes les agences et institutions gouvernementales fournissant des services électroniques à leurs clients doivent exiger l'utilisation de signatures numériques dans leurs services respectifs, afin de garantir la confidentialité, l'authenticité, l'intégrité et la non-répudiation des transactions électroniques au sein du gouvernement».
- Application des signatures numériques dans le commerce électronique et les services bancaires en ligne dans le secteur privé: «conformément à son mandat de promotion du commerce électronique au Mali, le gouvernement doit promouvoir l'application des signatures numériques dans les services de commerce électronique et les services bancaires en ligne dans le secteur privé, afin de garantir la confidentialité, l'authenticité, l'intégrité et la non-répudiation des transactions électroniques avec le secteur privé».

4.3 Cadre réglementaire des AC

La première étape dans la mise en œuvre des services de certification et de signature et d'accréditation des AC est la rédaction et la promulgation du règlement en vertu de la loi de 2016 relative aux transactions, échanges et services électroniques. Le MCENMA, en concertation avec les parties prenantes, a la responsabilité de rédiger et de faire promulguer le règlement énonçant les exigences d'accréditation des AC et des prestataires de services de confiance qualifiés au Mali.

Sur la base de l'analyse des lois et décrets en vigueur, sont proposées une réglementation, une directive et une notification nouvelles en vertu de la loi en vigueur, à savoir la loi de 2016 relative aux transactions, échanges et services électroniques, et du décret déterminant l'organisation et les modalités de fonctionnement du service de certification et de signature électronique.

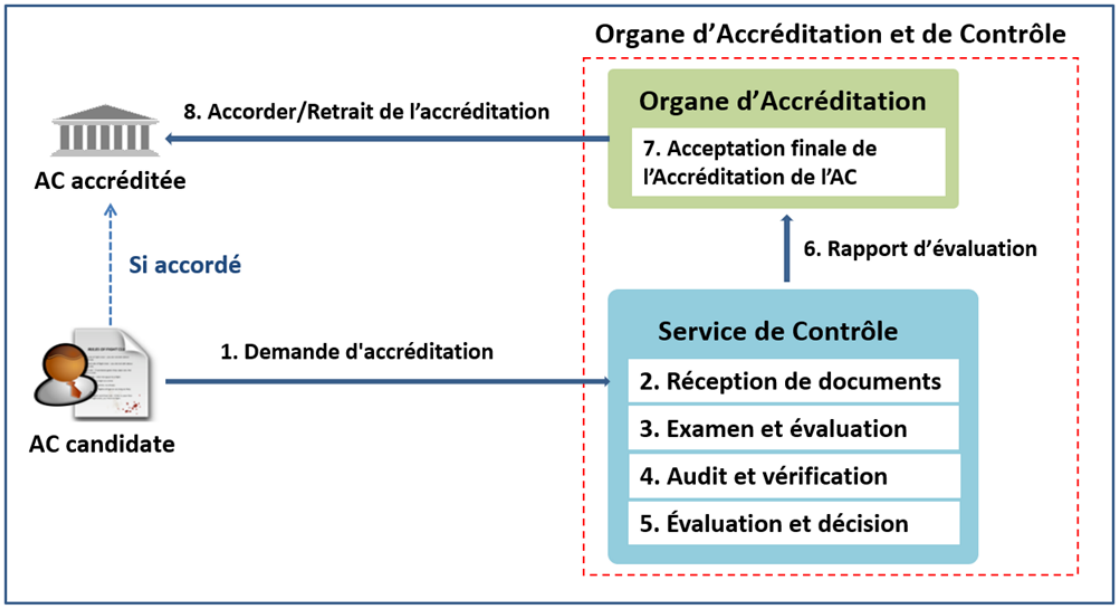
Figure 3: Cadre réglementaire



4.3.1 Procédure d'accréditation des AC

Pour permettre l'accréditation et l'audit efficaces des AC, les procédures relatives aux critères d'accréditation et d'audit doivent être mises en place et les éléments suivants doivent être pris en compte.

Figure 4: Procédure d'accréditation



1. L'AC candidate doit envoyer une **demande d'accréditation** à la structure publique en charge, avec les autres documents requis. Les documents requis sont les suivants:

   - demande d'accréditation de l'AC;
   - certificat d'identification du représentant commercial (carte d'identité nationale, naissance, changement de nom, etc.);
   - statuts;
   - preuve documentaire de la capacité technique, de la capacité financière et de la possession des installations et de l'équipement requis pour être une autorité de certification, conformément à la loi de 2016 relative aux transactions, échanges et services électroniques;
   - modèle économique;

- politiques de certification et déclaration des pratiques de certification (PC et DPC);
- architecture du système ICP;
- (le cas échéant) autres documents demandés par le service de contrôle.

2. La structure publique en charge **réceptionne** la demande d'accréditation ou qualification;
3. Le service de contrôle doit **examiner et évaluer** la demande d'accréditation de l'AC sur la base des critères d'accréditation;
4. Le service de contrôle doit effectuer **une vérification et un audit** réels de l'AC candidate. L'audit doit prendre en compte les politiques de certification et les systèmes ICP ainsi que les rapports d'audits internes de l'AC;
5. Le service de contrôle doit présenter les résultats de l'audit au comité de certification et de signature électronique pour une décision finale **d'accord ou de rejet** d'accréditation de l'AC.

4.3.2 Règlement relatif aux systèmes et équipements des AC accréditées

Le service de contrôle et d'accréditation des AC doit mettre en place des exigences applicables aux systèmes et équipements des AC accréditées. L'autorité de certification doit prouver que les systèmes et équipements satisfont à toutes les exigences énoncées dans les critères d'accréditation de l'autorité de certification. Après l'évaluation des documents, l'organisme d'accréditation doit visiter les sites où sont installés les systèmes et les équipements du demandeur de l'autorité de certification pour mener une inspection effective. L'AC qui souhaite exercer les activités de service de certification et de signature électronique qualifiée doit satisfaire aux exigences suivantes:

- exigences relatives aux systèmes de gestion des informations d'enregistrement des utilisateurs;
- exigences relatives aux systèmes et équipements de création et de gestion des clés de signature numérique;
- exigences relatives aux systèmes de création/émission/gestion des certificats électroniques;
- exigences relatives aux systèmes d'horodatage électronique;
- exigences relatives aux systèmes de protection;
- exigences relatives aux outils logiciels de signature électronique des abonnés.

4.3.3 Règlement relatif aux mesures de protection des AC

Pour assurer la haute sécurité des systèmes et équipements de l'AC, il est important de mettre en place un règlement portant sur les mesures de protection des AC accréditées. Le règlement a pour objet de préciser les mesures de protection que les autorités de certification doivent prendre pour assurer la sécurité des installations du service de certification conformément à la loi 2016-012/ du 6 mai 2016 relative aux transactions, échanges et services électroniques.

Ce règlement s'applique aux mesures de protection du centre de donnée de l'ICP de l'AC. Il doit inclure les exigences suivantes pour protéger les systèmes de certification ou l'ICP avec l'objectif d'assurer la « confidentialité, l'intégrité et la haute disponibilité » des services de certification:

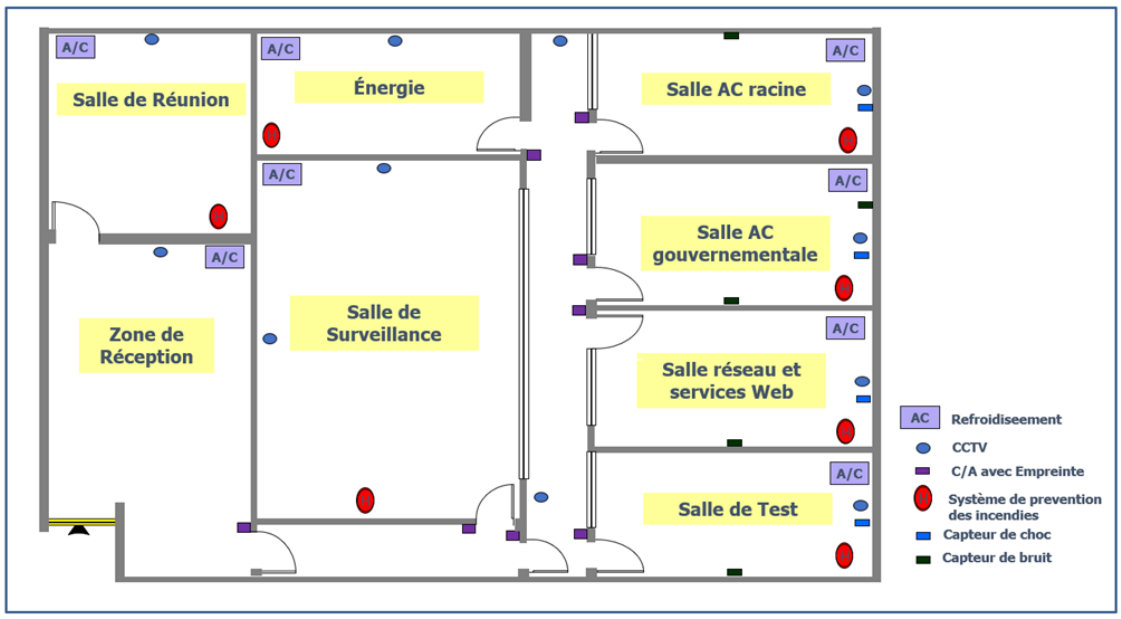
a) Mesures de **contrôles administratifs** pour assurer la mise en œuvre d'un environnement de sécurité. Les contrôles administratifs incluent les règles, les procédures et les lignes directrices relatives à l'exploitation sécurisée des systèmes ICP.

b) Mesures de **contrôles techniques** pour la protection des systèmes de certification contre les intrusions électroniques. Les contrôles techniques incluent les contrôles d'accès aux systèmes de l'AC, la sécurité des réseaux, la sécurité des systèmes, la sécurité des applications et des systèmes de monitoring ou de surveillance de l'infrastructure à clés publiques (ICP).

c) Mesures de **contrôles physiques** pour la protection des systèmes de certification contre les accès non autorisés ou les intrusions physiques. Les locaux ou le centre hébergeant l'ICP nationale doivent être suffisamment et physiquement sécurisés pour garantir un certain niveau de sécurité; à défaut, il ne sera pas possible d'établir la confiance requise. Les **contrôles physiques** incluent l'identification biométrique et par carte RFID, les systèmes de contrôle d'accès et les enregistrements d'audit, des systèmes de vidéo-surveillance (CCTV) et de contrôle, des verrous physiques, un système anti-incendie, un système de prévention des catastrophes et un système de gestion de l'hygrométrie.

Les composants du système ICP national, par exemple le local du système de l'AC racine, le local du système de l'AC émettrice, le local d'infrastructure réseau, le local de l'environnement de test, etc. doivent être installés dans des pièces séparées ou des confinements hautement sécurisés.

Figure 5: Conception de disposition physique d'un centre ICP national

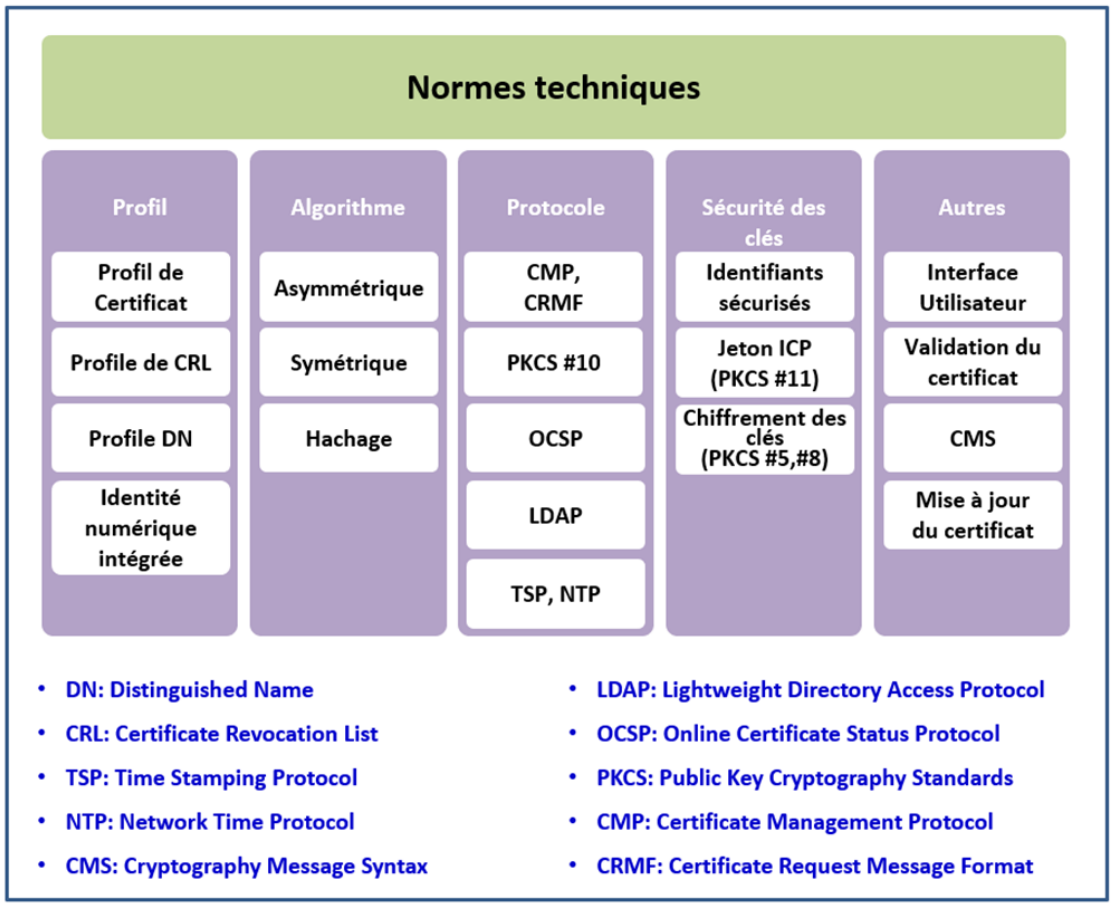


4.4 Normes relatives à l'infrastructure à clés publiques (ICP)

Les normes relatives à l'ICP sont importantes pour assurer l'interopérabilité avec les autorités de certification accréditées au Mali et les autorités de certification étrangères. L'autorité de certification nationale doit établir des normes ICP adaptées à l'environnement du Mali. Le Mali n'ayant pas encore de normes ICP, il est donc ouvert à l'adoption de toute norme ICP reconnue à l'échelle internationale.

Il est nécessaire de définir des normes adaptées au Mali pour assurer l'interopérabilité technique entre les AC accréditées ainsi que d'autres systèmes liés à l'ICP. Les normes techniques doivent être conformes aux normes internationales telles que l'IETF RFC (*Internet Engineering Task Force, Request for Comments*) et les RSA PKCS (*PUBLIC-KEY Cryptography Standards*). La figure ci-après détaille les normes ICP qu'il est nécessaire de prendre en compte.

Figure 6: Normes techniques



4.4.1 Profil du certificat

Le profil est une définition qui spécifie le format d'un certificat, la LRC, le nom distinctif (DN, *distinguished name*) et le numéro d'identification unique, par exemple le numéro NINA du Mali pour une personne physique, ou le numéro d'identification fiscale unique pour une personne morale associée à un certificat numérique.

Le certificat définit des éléments tels que la version, la signature, l'objet, le sujet, la validité, une clé publique associée au sujet, le numéro de série, la signature, les identifiants uniques et d'autres informations associées.

Le certificat doit être conforme à la RFC 5280 et aux champs de base du certificat X.509 v3 et de la liste de révocation de certificats X.509 v2 (LRC) pour une utilisation sur Internet. Tous les certificats et LRC émis par l'AC accréditée doivent conserver les fonctionnalités d'interopérabilité entre AC accréditées.

4.4.2 Algorithme de chiffrement

La technologie ICP utilise des algorithmes de chiffrement asymétrique, symétrique et de hachage pour assurer sa fonction de sécurité avec chiffrement. Les algorithmes de normes suivantes doivent être pris en compte dans les normes de l'ICP nationale:

- Algorithme de chiffrement asymétrique: RSA (*Rivest Shamir Adleman*), DSA (DSS: *Digital Signature Standard*) et ECDSA (*Elliptic Curve Digital Signature Algorithm*);
- Algorithme de chiffrement symétrique: AES (*Advanced Encryption Standard*), IDEA (*International Data Encryption Algorithm*);
- Algorithme de hachage: SHA (*Secure Hash Algorithm*) 256 et SHA-512.

Il est nécessaire de spécifier dans le profil toutes les fonctionnalités de l'algorithme, telles que la taille de la clé et le paramètre, pour assurer l'interopérabilité avec d'autres systèmes ICP.

4.4.3 Protocole ICP

La technologie ICP utilise différents protocoles pour délivrer un certificat et sécuriser les données de transmission entre les systèmes ICP. Les protocoles ICP suivants doivent être pris en compte dans les normes de l'ICP nationale:

- Le protocole CMP (*Certificate Management Protocol*) est un protocole Internet utilisé pour obtenir des certificats numériques X.509. Il est décrit dans la RFC 4210 et est l'un des deux protocoles à ce jour à même d'utiliser le format CRMF (*Certificate Request Message Format*) décrit dans la RFC 4211, l'autre protocole étant le *Certificate Management over Cryptographic Message Syntax* (CMS), décrit dans la RFC 5273. Les messages CMP sont codés en ASN.1 (*Abstract Syntax Notation.1*), en utilisant la méthode DER (*Distinguished Encoding Rules*) et généralement encapsulés en HTTP.
- Le protocole CSR (*Certificate Signing Request*) est un message envoyé par un demandeur à une autorité de certification pour demander un certificat numérique. Le format le plus courant pour CSR est la spécification PKCS n° 10.
- Le protocole OCSP (*Online Certificate Status Protocol*) permet aux applications de déterminer l'état de révocation des certificats. Il est décrit dans la RFC 6960. Le protocole OCSP est l'alternative à la LRC; il s'agit d'un protocole Internet utilisé pour obtenir immédiatement l'état actuel de la révocation d'un certificat numérique X.509.
- Le protocole LDAP (*Lightweight Directory Access Protocol*) est décrit dans la RFC 3494. Il s'agit d'un protocole Internet utilisé pour accéder aux services d'annuaire basés sur X.500. Le protocole LDAPv3 doit être utilisé dans l'ICP nationale.
- Le protocole d'horodatage ou *Time Stamp Protocol* (TSP), tel que décrit dans la RFC 3161, devrait être utilisé pour horodater les données afin d'établir des preuves indiquant que les données existaient avant un moment particulier. Par exemple, il doit être utilisé pour vérifier qu'une signature numérique a été appliquée à un message avant que le certificat correspondant ne soit révoqué. Le protocole TSP permet d'utiliser un certificat révoqué pour vérifier une signature créée avant le moment de la révocation. Il s'agit d'une opération importante d'une infrastructure à clés publiques. Le protocole TSP peut également être utilisé pour indiquer l'heure de soumission, lorsqu'une date limite est critique.

4.4.4 Sécurité des clés privées

La norme pertinente pour les modules cryptographiques est FIPS PUB 140-2. Ce cadre définit les exigences de sécurité minimale pour les modules cryptographiques inviolables. Les mesures suivantes de protection des clés privées doivent être prises en compte dans la politique et les normes nationales de l'ICP:

Tableau 4: Exigences de sécurité applicables aux HSM des AC et des abonnés

AC	Modules cryptographiques
AC racine (*Root CA*)	Matériel certifié HSM, FIPS 140-2 niveau 3 + certifié
AC émettrice	Matériel certifié HSM, FIPS 140-2 niveau 3 + certifié
Abonnés (Certificat Classe 3)	Matériel certifié HSM, FIPS 140-2 niveau 3 + certifié
Abonnés (Certificat Classe 2)	Matériel ou logiciel HSM, FIPS 140-2 niveau 2 ou + certifié
Abonnés (Certificat Classe 1)	Aucune exigence FIPS 140-2

4.5 Cadre politique de certification

4.5.1 Politique de certification (PC) et déclaration des pratiques de certification (DPC)

L'autorité de certification électronique nationale doit établir la PC et la DPC sur la base des recommandations de l'IETF (*Internet Engineering Task Force*) relatives à l'infrastructure à clés publiques conformément aux normes RFC 3647, afin de garantir l'interopérabilité et le haut niveau de sécurité du service de certification au Mali. La PC et la DPC doivent être publiées sur la page d'accueil de l'AC afin que les AC accréditées et les abonnés puissent facilement connaître le contenu détaillé et les procédures du service de certification.

- Une politique de certification (PC), telle que définie dans la norme X.509, est un ensemble de règles qui indiquent l'applicabilité d'un certificat à une communauté particulière et/ou à une application de classe avec des exigences de sécurité communes. Une PC fournit des conseils aux parties de confiance, pour les aider à savoir si un certificat est approprié pour une utilisation en conjonction avec une application spécifique. Une PC fournit une protection en responsabilité à une autorité de certification, en déclarant la gamme d'utilisations prévue pour les certificats qu'elle délivre.
- La déclaration des pratiques de certification (DPC) est une description plus détaillée de la PC employée par une AC lors de l'émission et de la gestion des certificats numériques. Elle est adaptée aux procédures d'exploitation du système ICP de l'AC, à la structure organisationnelle, aux installations et à l'environnement informatique de l'autorité de certification. Généralement, la PC indique à quoi il faut adhérer, tandis que la DPC indique comment la PC est respectée.

Les PC et DPC des autorités de certification accréditées doivent être conformes aux PC et DPC de l'autorité de certification racine. Les éléments suivants doivent être pris en compte lors d'élaboration des PC et DPC détaillées de l'autorité de certification électronique de la République du Mali.

Tableau 5: DP et DPC

Rubriques	Contenu
Introduction	• Contexte et objectifs des PC et DPC • Informations sur les parties concernées, les certificats et l'administration • Organisation et définitions

Tableau 5: DP et DPC (suite)

Rubriques	Contenu
Responsabilités de publication et de dépôt	• Publication des informations de certification et de l'état des certificats des AC et des abonnés dans le répertoire et la LRC • Protection de toute information du répertoire de l'autorité de certification électronique
Identification et authentification	• Procédures d'enregistrement pour authentifier l'identité d'un demandeur de certificat • Critères d'acceptation des candidats des entités souhaitant devenir AC ou AE • Procédures d'authentification pour une demande de récupération de clé ou de révocation
Exigences opérationnelles relatives au cycle de vie du certificat	• Exigences imposées aux AC, AE, abonnés ou autres participants en ce qui concerne le cycle de vie d'un certificat
Contrôles de gestion, opérationnels et physiques	• Contrôles de sécurité non techniques (contrôles physiques, procéduraux et personnels) utilisés par l'AC • Contrôles physiques des locaux abritant les systèmes de l'ICP • Exigences relatives à la reconnaissance des rôles de confiance, et responsabilités pour chaque rôle • Procédures de journalisation des audits, d'archivage de dossiers, de chargements de clé, de changement des clés, de systèmes compromis et de reprise après sinistre et de résiliation d'une AC ou d'une AE.
Contrôles techniques de sécurité	• Mesures de sécurité prises par l'AC pour protéger ses clés de chiffrement et ses données d'activation • Contrôles de sécurité utilisés par l'AC pour exécuter en toute sécurité les fonctions de génération et d'installation de paires de clés, d'authentification des utilisateurs, d'enregistrement de certificats, de révocation de certificats, d'audit et d'archivage • Autres mesures de sécurité de l'AC pour les contrôles de sécurité du cycle de vie, la sécurité des réseaux et l'horodatage.
Profils de certificat, LRC et OCSP	• Définition du profil de certificat pour se conformer à la RFC 3280 • Définition du profil LRC pour se conformer à la RFC 3280 • Définition du profil OCSP pour se conformer à la RFC 2560
Audit de conformité et autres évaluations	• Mécanisme d'audit de conformité pour assurer que les exigences de la PC et de la DPC de l'autorité de certification électronique sont mises en œuvre et appliquées • Fréquence de l'audit de conformité ou autre évaluation pour chaque entité qui doit être évaluée • Identité et qualification du personnel effectuant l'audit ou toute autre évaluation
Autres affaires et questions juridiques	• Enjeux commerciaux des honoraires à facturer pour divers services • Responsabilité financière des participants, lesquels s'engagent à maintenir les ressources pour les opérations en cours et à s'acquitter de toute somme issue de jugements ou de règlements en réponse aux réclamations formulées à leur encontre

4.5.2 Politique de l'autorité d'horodatage (Politique TSA)

L'autorité de certification électronique doit mettre en place une politique d'horodatage (TSA), qui définit les politiques et pratiques utilisées pour l'exploitation et la gestion du service d'horodatage (TSA) de l'autorité de certification, afin que les abonnés et les prestataires de services tiers puissent évaluer le niveau de confiance du fonctionnement de ce service. La TSA doit utiliser un chiffrement à clé publique, des certificats de clé publique et des sources de temps fiables pour fournir des horodatages fiables basés sur des normes et conformes aux modèles mondialement acceptés.

Les services d'horodatage (TSA) sont utilisés en appui des signatures électroniques et doivent être basés sur le temps universel (Référence: Article 133 de la loi de 2016 relative aux transactions, échanges et services électroniques en République du Mali).

> Article 133: La datation fournie par un prestataire de **service d'horodatage électronique est basée sur le temps universel** coordonné et y fait expressément référence.

Les services d'horodatage (TSA) peuvent être utilisés à toutes autres fins nécessitant la preuve que certaines données ont existé à un moment précis.

4.5.3 Politique d'identification des objets (OID, *Object Identifier*)

Le mécanisme OID est un mécanisme d'identification utilisé, développé conjointement par l'UIT-T et l'ISO/IEC pour nommer tout type «d'objet» ou de «chose» avec un nom globalement non ambigu qui nécessite un nom persistant (à longue durée de vie). Il est important, pour l'interopérabilité entre les autorités de certification électronique, d'identifier de manière unique un objet lié à l'ICP. Un nom, une fois alloué, ne doit pas être utilisé pour un objet/une chose différente.

Tableau 6: Politique OID

Nom de la politique	Object Identifier (OID)	Cible
P-Classe1	2.16. xxx .x	Citoyens
P-Classe2	2.16. xxx.x	Organisations
P-Classe3	2.16. xxx.x	Serveurs

Note: si le Mali ne dispose pas encore d'un mécanisme OID, l'autorité de certification électronique devra en faire la demande auprès de l'UIT ou de l'ISO.

4.6 Architecture du système d'ICP national

4.6.1 Architecture du système de l'AC racine nationale

Le système de l'autorité de certification racine (*Root CA*) nationale est le point d'ancrage de confiance dans la structure hiérarchique de l'infrastructure à clés publiques (ICP) de la

République du Mali, auquel tous les utilisateurs et prestataires de services feront confiance. Il sera utilisé pour émettre et signer des certificats pour:

- le certificat de l'autorité de certification racine (auto-signé);
- les autorités de certification (AC) émettrices ou subordonnées au Mali;
- la liste de révocation des autorités (LRA);
- les certificats croisés des AC partenaires;
- et l'autorité d'horodatage (TSA).

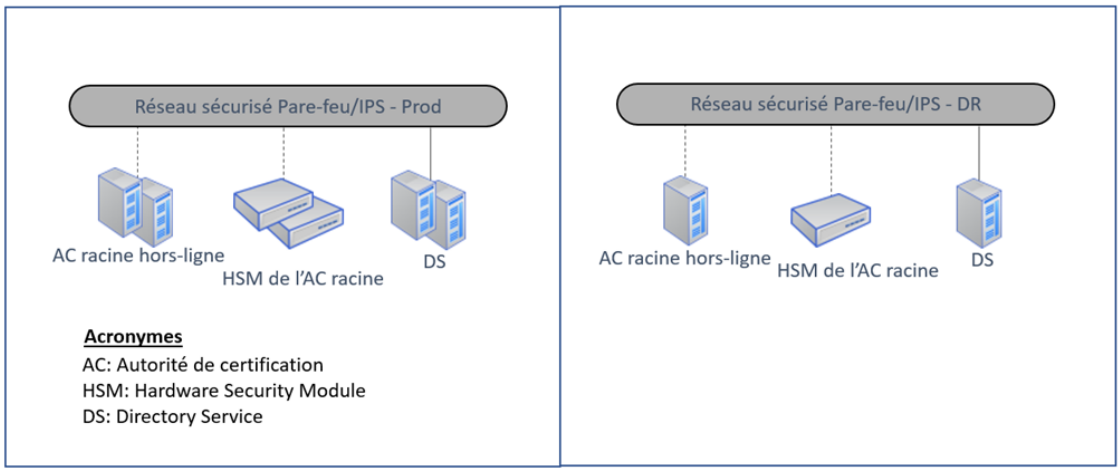
Pour garantir une protection élevée, le système de l'AC racine doit toujours fonctionner en mode hors ligne (*offline*) et être hébergé dans un environnement hautement sécurisé. Trois environnements sont recommandés lors de la mise en place du système de l'AC racine:

1) Site principal: héberge le système de l'AC racine en production, pour la fourniture des services de certification des AC, du TSA et la publication des LRC des AC;
2) Site secondaire: héberge le système de l'AC racine dans l'environnement de récupération après sinistre (DR), pour la fourniture des services de certification des AC, du TSA et la publication des LRC des AC en cas d'incidents ou de panne de l'environnement de production;
3) Environnement de test: le système d'AC racine dans l'environnement de test est exploité uniquement pour la fourniture des services de test.

Tous les équipements actifs (serveurs, équipements réseaux et sécurité) de l'environnement de l'AC racine en production doivent être configurés en mode haute disponibilité (HA) pour assurer la redondance. Un pare-feu redondant doit être mis en œuvre pour contrôler l'accès entre les différentes zones du réseau (réseau externe ou Internet, réseau DMZ et réseau interne).

L'architecture de l'environnement de reprise après sinistre (DR) de l'AC racine ne se configure pas en HA; chaque composant (serveurs, équipements réseaux et sécurité) est déployé en un seul mode. Un pare-feu doit être mis en œuvre pour contrôler l'accès entre les différentes zones du réseau (réseau externe ou public, réseau DMZ et réseau interne).

Figure 7: Architecture conceptuelle du système d'AC racine



4.6.2 Architecture du système de l'AC gouvernementale (*Gov CA*) – site principal

L'AC accréditée doit être en mesure de délivrer des certificats numériques aux abonnés (personne physique, personne morale et équipements ou serveurs). L'AC accréditée émettra les types de certificats numériques suivants:

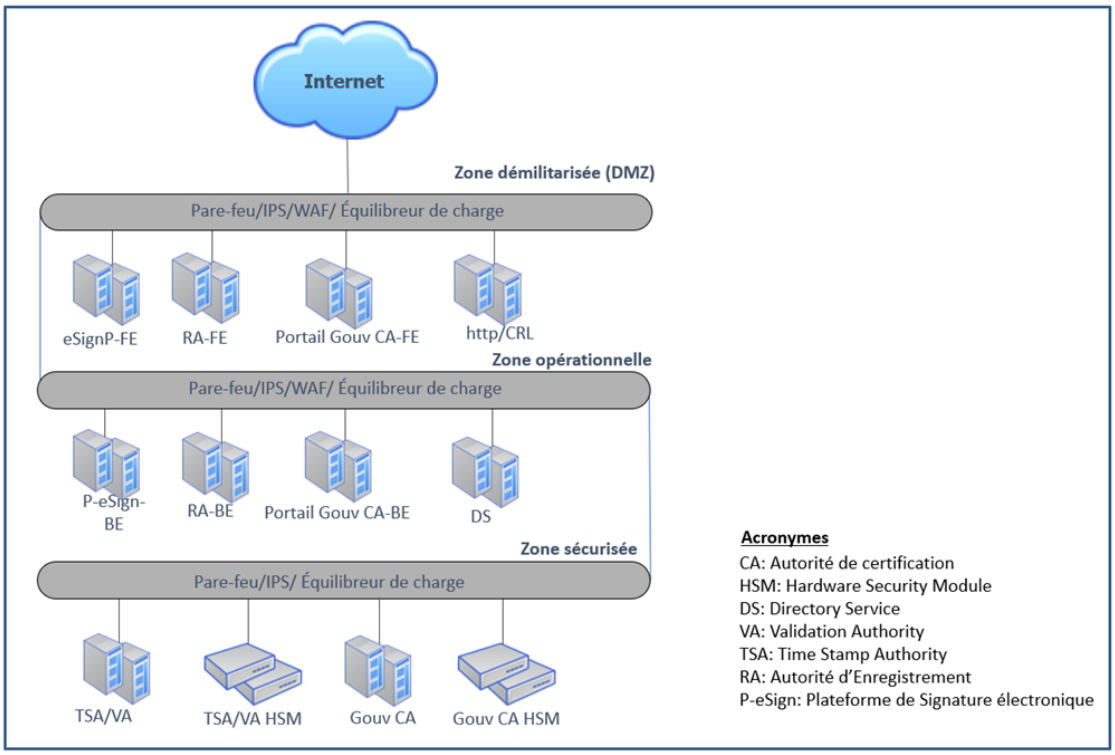
- certificat d'authentification pour authentifier les utilisateurs accédant aux services en ligne de l'administration, du secteur bancaire et du commerce électronique;
- certificat de signature numérique pour signer des transactions électroniques ou un document électronique;
- certificat de cachet numérique, pour apposer un cachet sur les transactions électroniques ou les documents électroniques;
- certificat de chiffrement, pour chiffrer des données ou des documents confidentiels;
- certificat de signature et de chiffrement des courriels, pour signer et chiffrer les courriels importants;
- certificats de signature de code, pour signer les fichiers exécutables des logiciels;
- certificats de serveurs et de clients, pour sécuriser la communication entre les serveurs et les machines clientes;
- certificats VPN, pour authentifier les utilisateurs de VPN lors d'une connexion sécurisée.

L'AC accréditée sera l'AC émettrice. À ce titre, elle jouera un rôle essentiel dans la délivrance de certificats numériques aux abonnés (personne physique, personne morale et serveurs ou équipements) dans le système ICP national. Dans le système de l'AC accréditée, l'équipe de consultants recommande trois environnements ICP, à savoir:

1) un environnement de production (site principal): tous les composants de l'AC accréditée dans l'environnement de production seront configurés en haute disponibilité (HA) pour garantir un fonctionnement et une disponibilité stables des services ICP;
2) un environnement de reprise après sinistre (DR) (site secondaire): l'environnement DR de l'AC accréditée ne sera pas configuré HA;
3) un environnement de test: l'environnement de test de l'AC accréditée ne sera pas configuré HA.

Dans l'environnement de production de l'autorité de certification accréditée, tous les composants doivent être configurés en mode haute disponibilité (HA) pour garantir la disponibilité des services. Un pare-feu doit être mis en œuvre pour contrôler l'accès entre les différentes zones du réseau (réseau externe ou public, réseau DMZ et réseau interne).

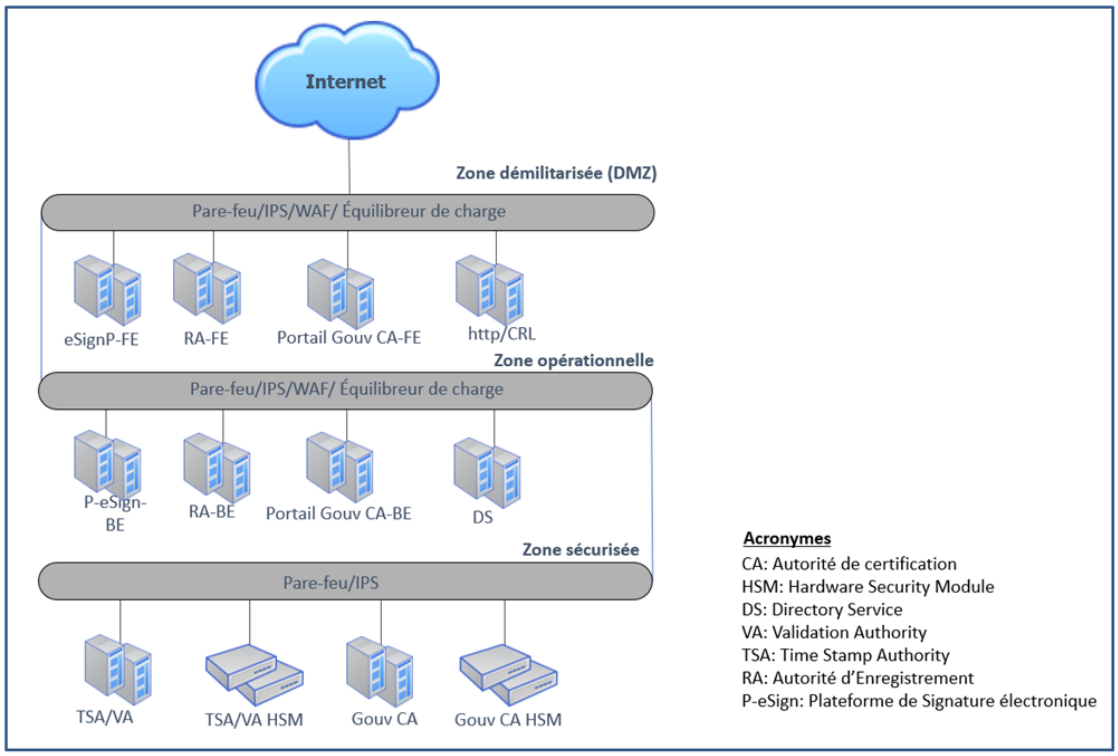
Figure 8: Architecture conceptuelle du système de l'AC gouvernementale (site principal)



4.6.3 Architecture du système de l'AC gouvernementale – site secondaire et DR

Il n'y a pas de haute disponibilité dans l'environnement de reprise après sinistre. Un pare-feu doit être mis en œuvre pour contrôler l'accès entre les différentes zones du réseau (réseau externe ou public, réseau DMZ et réseau interne).

Figure 9: Architecture conceptuelle de l'AC gouvernementale (site secondaire et test)



4.7 Spécifications techniques

Le tableau ci-dessous résume les composants d'un système et les spécifications techniques de l'autorité de certification gouvernementale (*Gov CA*) nécessaires pour l'émission et la gestion de certificats numériques aux abonnés, conformément aux lois de la République du Mali et aux normes internationales.

Tableau 7: Composants essentiels du système de l'AC gouvernementale (*Gov CA*)

Composants	Exigences techniques pour les systèmes des AC accréditées
Système de l'autorité de certification racine (*Root CA*)	Le système d'autorité de certification racine (*Root CA*) doit prendre en charge les fonctions suivantes: • fonctionnement hors ligne pour maintenir une sécurité physique stricte; • certification, renouvellement et révocation des AC; • publication périodique des LRC et des LRA; • auto-signature et norme de certificat X.509 version 3; • les clés privées de l'AC émettrice doivent être créées et protégées dans un matériel HSM certifié FIPS 140-2 niveau 3; • conformité aux normes internationales (RFC 5280).

Tableau 7: Composants essentiels du système de l'AC gouvernementale (Gov CA) (suite)

Composants	Exigences techniques pour les systèmes des AC accréditées
Système de l'AC gouvernementale (*Gov CA*) émettrice	Le système d'autorité de certification émettrice (*Gov CA*) doit prendre en charge les fonctions suivantes: • configuration HA dans l'environnement de production, mais pas de HA dans l'environnement DR ni dans l'environnement de test; • création et gestion du cycle de vie des certificats (émission/renouvellement/révocation/suspension des certificats); • publication périodique des LRC; • conformité aux normes X.509 version 3; • conformité aux normes internationales lors de l'émission (RFC 5280); • les clés privées de l'AC émettrice doivent être créées et protégées dans un matériel HSM certifié FIPS 140-2 niveau 3; • conteneurs de stockage des certificats et des clés d'abonnés (par exemple, jeton crypto USB, cartes à puce, carte crypto SIM, Apple Secure Enclave (SE), Android Trusted Execution Environment (TEE) et HSM centralisé).
HSM (*Hardware security Module*)	• Configuration HA dans l'environnement de production. Pas de haute disponibilité dans l'environnement DR ni dans l'environnement de test; • algorithmes asymétriques (par exemple: RSA, DSA, KCDSA, ECDSA,), algorithmes symétriques (par exemple: AES) et hachages (par exemple SHA-1, SHA-2 [224, 256, 384, 512 bits]); • différentes interfaces de programmation d'applications (API) : PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI, etc.; • protection des clés de signature numériques de l'AC racine et de l'AC émettrice. Ce logiciel doit être certifié FIPS 140-2 niveau 3 ou plus. • configurations de contrôle multifactoriel (facteur k-sur-n).
Service d'annuaire (DS)	Le service d'annuaire (DS, *directory service*) doit prendre en charge les fonctions suivantes: • demande, gestion et stockage des certificats de chiffrement; • publication des LRC et LRA; • services LDAP courants; • conformité aux normes internationales (par exemple RFC 3494, RFC 4519); • prise en charge des protocoles LDAP v3, HTTPS, HTTP, FTP et TLS 1.0, conformément aux RFC 4510 et 8615; • prise en charge du LDAP maître et public.

Composants	Exigences techniques pour les systèmes des AC accréditées
Système de l'AE	Le système de l'autorité d'enregistrement (AE) doit prendre en charge les fonctions suivantes: • réception des demandes et traitement du processus de création de certificats; • processus d'identification et d'inscription des abonnés en ligne; • intégration avec la base de données externe (par exemple NINA) pour valider le numéro d'identification des personnes physiques; • communication en toute sécurité avec l'AC via une API et signature numérique de toutes les communications avec la clé de signature privée de l'AE; • émission de certificats dans un conteneur cryptographique sécurisé contenant les paires de clés des abonnés; • exécution des fonctions de gestion du cycle de vie du certificat, telles qu'une demande de révocation/suspension ou une opération de récupération de clé pour le compte de l'abonné.
OCSP (*Online Certificate Status Protocol*)	Le système OCSP doit prendre en charge les fonctions suivantes: • utilisation d'un répondeur OCSP de confiance pour traiter les demandes d'informations de vérification et d'état du certificat; • réponse aux demandes via le protocole OCSP par le répondeur, conformément à la RFC 6960; • signature numérique des demandes et/ou des réponses OCSP; • application des normes internationales lors de l'émission (RFC 6960); • transparence des certificats selon la RFC 6292; • prise en compte de plusieurs autorités de certification (AC).
Système TSA	Le système TSA doit prendre en charge les fonctions suivantes: • horodatage suivant la date et l'heure locale et l'heure universelle; • configuration HA; • signature de chaque jeton d'horodatage avec la clé de signature privée du TSA; • conformité à la RFC 3820; • conformité à la RFC 3161; • conformité des demandes d'horodatage, des réponses de jeton et des messages d'erreur à la RFC 3161; • signature des réponses TSA par le TSA; • utilisation d'une source de temps fiable; • inclusion d'une valeur horaire fiable pour chaque jeton d'horodatage.

Composants	Exigences techniques pour les systèmes des AC accréditées
Plateforme de signature électronique (*P-eSign*)	La plateforme de signature électronique doit prendre en charge les fonctions suivantes: • signature locale (certificat de signature stocké dans un jeton sur clé USB ou une carte à puce) et signature à distance sur un HSM dans le cloud; • génération et vérification de signatures électroniques de différents formats (PDF, XML, CMS, PKCS # 7, PAdES, CAdES et XAdES et RSA PKCS # 1, etc.); • différentes API d'intégration avec les applications métiers (API REST et SOAP); • protocoles pour l'identité fédérée (OpenID connect, SAML et OAuth dernière version); • intégration avec les AC pour gérer les certificats et protéger les clés de signature des utilisateurs dans un HSM; • application mobile (*Mobile ID*) d'authentification et de signature supportée par les appareils mobiles iOS et Android; • différentes méthodes d'authentification (SSO, OTP, 2FA, certificat numérique); • création de circuits de signature, pour signer et faire signer les documents électroniques; • suivi du processus de signature, notification et délégation de signature; • application mobile (iOS et Android) pour signer, faire signer et suivre le processus de signature; • signature de plusieurs documents en une seule fois; • sécurité des documents signés, comme par exemple le chiffrement, la gestion des permissions, etc.; • gestion et archivage des documents électroniques; • mutualisation (*multi-tenancy*).
API	• Les API s'intègrent de manière transparente au système ICP et aux applications métiers; • Les API prennent en charge plusieurs langages de programmation et de script, cadres de développement et systèmes d'exploitation; • Les API doivent encapsuler les différentes opérations ICP et masquer la complexité de l'intégration ICP; • Les API doivent être conformes, dans les opérations de leurs appels de fonction, à la plupart des normes/RFC du marché telles que: PKCS#11, PKCS#12, X.509, GSS, CDSA, RFC2743, ISO 7498; • Les API doivent prendre en charge les formats de signature suivants, par exemple: niveaux XAdES, PAdES, CADES, PKCS#7, B-B, B-T, B-LT, B-LTA; • Les API doivent prendre en charge les canaux de communication API suivants: API SAML, OAuth, OpenID Connect, REST et SOAP au minimum; • Les API doivent prendre en charge les formats de documents suivants: XML, PDF et MS Office.

5 Partie III: Étude comparative des plateformes de signature électronique

5.1 Introduction

Aujourd'hui, le processus de signature manuscrite sur papier physique n'est plus efficace, car l'application de la signature électronique aux processus métier devient de plus en plus populaire. Avec la pandémie du COVID-19, les exigences de distanciation physique ont accéléré l'adoption de la signature électronique par plusieurs organisations, entreprises et gouvernements, ce type de signature s'imposant même à ceux qui résistent à son adoption.

Le basculement du processus papier vers le processus numérique avec la signature électronique devient de plus en plus **la nouvelle méthode** qui reflète la transformation numérique du monde des affaires. Ainsi, le développement des technologies de signatures électroniques continue à introduire de nouvelles façons de signer et faire signer les documents (courriers, contrats, conventions, accords, etc.). Les acteurs doivent avoir l'assurance que les documents signés électroniquement et reçus proviennent de personnes ou d'entreprises de confiance, que le contenu n'est pas modifié pendant le transit et que lesdits documents parviennent aux personnes ou entreprises auxquelles ils sont destinés.

Le Gouvernement du Mali a besoin d'une plateforme de signature électronique complète, sécurisée et efficace permettant une optimisation rapide de la façon dont les ministères et les agences publiques gèrent les processus de signature, font signer et approuver les documents dans l'administration à tout moment et sur n'importe quel terminal. Ceci est en étroite ligne avec loi 2016-012/ du 6 mai 2016 qui réglemente les transactions, les échanges et les services électroniques en République du Mali, conférant à la signature électronique la même valeur juridique que la signature manuscrite.

5.2 Avantages d'une signature électronique

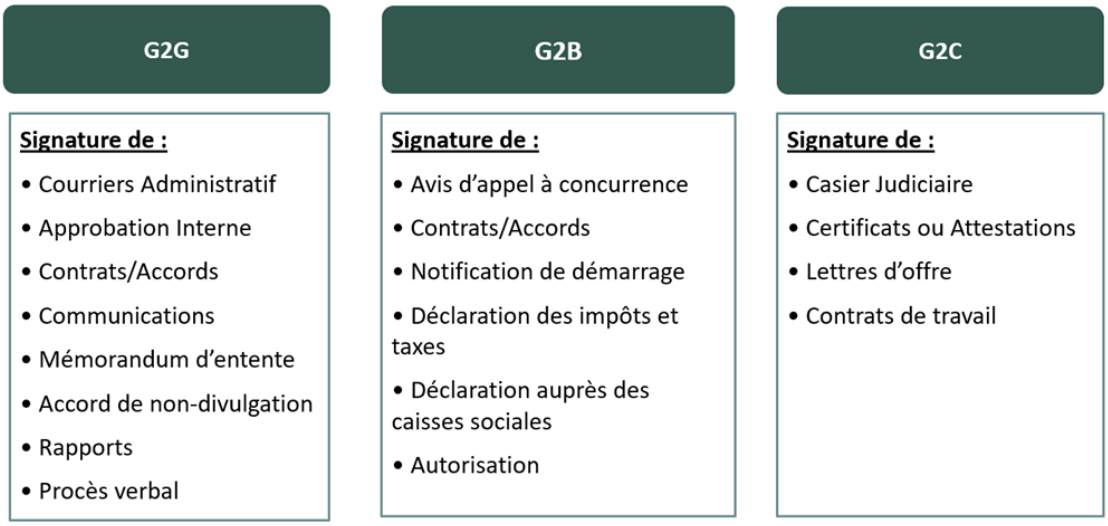
Très souvent, la finalisation d'un processus métier prend du temps: celui passé à effectuer des tâches administratives répétitives plutôt qu'à atteindre des objectifs productifs. L'introduction des signatures électroniques dans les processus métier peut être une étape majeure dans la stratégie de transformation numérique.

La signature électronique apporte de nombreux avantages, à savoir: la **sécurité** des documents électroniques, l'**efficacité** des processus métier, la réduction du **temps** et des **coûts** liés au processus papier, la **mobilité** et une meilleure expérience utilisateur.

5.3 Exemples de cas d'usage d'une plateforme de signature électronique

La première étape – et la plus critique – lors du choix d'une plateforme de signature électronique consiste à recenser et catégoriser les cas d'usage. Les cas d'usage de la plateforme de signature électronique consistent à signer, faire signer par un ou plusieurs signataires, ou apposer un cachet sur des documents électroniques à distance. Les cas d'usage peuvent être classés en trois (3) catégories principales, à savoir:

- Du gouvernement au gouvernement (G2G);
- Du gouvernement aux entreprises ou au monde des affaires (G2B);
- Du gouvernement aux citoyens (G2C).



5.4 Catégories de plateformes de signature électronique

Il existe plusieurs types de plateformes de signature électronique. Certaines plateformes offrent simplement les services de signature électronique, tandis que d'autres étendent leurs capacités frontales à la prise en charge des circuits ou «flux» (*workflow*) de signature de documents électroniques et à l'intégration avec les applications métiers (par exemple système de gestion des courriers et des documents, système de gestion des clients, système de gestion de contrats, système de gestion des marchés publics, etc.). Dans cette étude comparative, nous avons identifié trois catégories de plateformes de signature électronique:

a) **Plateforme de signature électronique axée sur le flux de signature :** ces plateformes offrent des services de signature électronique de base ou standard et appliquent le niveau d'assurance faible pour l'authentification des utilisateurs avec un **mot de passe** ou **mot de passe à usage unique (OTP, One Time Password)**. Les plateformes dans cette catégorie prennent rarement en compte la preuve d'identité et ne prennent pas en charge les intégrations avec les services des autorités de certification pour assurer la confiance.

b) **Plateforme de signature électronique axée sur la signature numérique à distance**: ces plateformes ne fournissent pas le flux de signature; par contre, elles prennent en charge une variété de services de sécurité: authentification à deux facteurs (2FA), signature numérique à distance, horodatage et cachets électroniques.

c) **Plateforme de signature électronique à service complet (flux et signature numérique à distance)**: ce type de plateforme fournit un portail frontal pour les utilisateurs finaux, le flux pour signer et faire signer des documents électroniques, ainsi que les services de sécurité: authentification à deux facteurs (2FA), signature numérique à distance, horodatage et cachets électroniques.

Recommandation 1: dans le cadre de ce projet, nous recommandons la mise en place d'une plateforme de signature électronique complète (intégrant le flux et la signature numérique à distance), sécurisée et efficace pour gérer les processus consistant à signer, faire signer et approuver les documents dans l'administration, à tout moment et sur n'importe quel terminal, ainsi que la **gestion des identités numériques**.

5.5 Exigences fonctionnelles et techniques

5.5.1 Portail Web

La plateforme fournit un portail Web qui permet aux utilisateurs de se connecter soit avec un nom d'utilisateur, OTP, 2FA, soit avec une authentification forte à travers un certificat numérique X.509 v3. Le portail fournit un tableau de bord des utilisateurs avec des informations en temps réel sur l'état de leurs processus de signature des documents (documents signés, en cours ou rejetés). La plateforme de signature électronique doit fournir un portail utilisateur offrant des flux avancés de signature des documents ou des formulaires Web.

5.5.2 Flux de signature

La plateforme fournit le flux qui prend en charge le processus pour signer et faire signer les documents par une ou plusieurs personnes, en parallèle ou en séquentiel. Elle offre également la possibilité de déléguer le pouvoir de signature à un autre utilisateur, des flux flexibles à configurer et personnaliser, la possibilité de configurer la sécurité pour contrôler ce que les autres utilisateurs signataires peuvent et ne peuvent pas faire avec les documents partagés pour la signature (par exemple signer, approuver, pour information, télécharger, sauvegarder, imprimer, etc.), la possibilité de configurer les notifications automatiques pour rappeler aux utilisateurs de signer et de gérer les flux et distribuer le document signé à tous les utilisateurs concernés, une fois le flux de signature terminée, ainsi que plusieurs autres options.

La plateforme doit prendre en compte toutes les activités de préparation des documents à signer ou à faire signer, comme l'ajout des signataires, les champs prévus pour les initiales, l'ordre de signature, etc. Elle doit aussi configurer les méthodes d'authentification de signataires et des types de signature.

La plateforme de signature électronique doit prendre en charge le stockage et la gestion des documents signés ou approuvés et offrir un moyen facile pour y accéder rapidement, ainsi qu'une capacité de recherche des documents et de sécurité appropriée pour garantir que seuls les utilisateurs autorisés parviennent à accéder aux documents archivés.

5.5.3 Création et validation de signature électronique

La plateforme de signature électronique doit être conforme aux normes et réglementations internationales, par exemple eIDAS, ETSI, ISO, etc., prendre en charge le mode de signature locale (clé de signature stockée dans un jeton sur clé USB) et la signature à distance (clé de signature stockée sur un HSM central) pour que l'utilisateur puisse l'utiliser partout et sur n'importe quel terminal où la clé de signature est stockée, de même que dans un terminal mobile. Les utilisateurs sont authentifiés avant d'utiliser leur clé de signature et toutes les interactions sont enregistrées.

La plateforme doit également prendre en charge les trois niveaux de signature électronique que sont: la signature électronique simple, la signature électronique avancée et la signature électronique qualifiée, sur la base d'un certificat numérique émis par une AC accréditée ou un prestataire de service de confiance qualifié.

La plateforme doit pouvoir créer et valider des signatures électroniques conformes aux normes PAdES, XAdES et CAdES.

La plateforme de signature électronique doit pouvoir s'intégrer avec les systèmes des infrastructures à clés publiques (ICP), tels que l'autorité de certification (AC), pour gérer la demande et l'émission des certificats aux utilisateurs, l'OCSP et la LRC, pour valider les signatures numériques, et l'autorité d'horodatage (TSA) pour les services d'horodatage.

5.5.4 Identification et authentification

Les plateformes de signature électronique prennent en charge différentes méthodes d'identification et d'authentification. Pour l'identification, elles s'intègrent avec des bases de données externes comme par exemple la base de données d'identification nationale (NINA) pour valider les identités des utilisateurs. Chaque utilisateur devra posséder un numéro d'identification unique (NINA) qui doit être validé lors de l'enregistrement des utilisateurs.

La plateforme doit pouvoir authentifier les utilisateurs avec une authentification par mot de passe + OTP et un certificat numérique X.509 v3 avant de leur donner accès aux ressources de la plateforme de signature électronique.

5.5.5 Intégration avec les applications métiers

La plateforme de signature électronique doit exposer les fonctions de signature via les protocoles d'API standard, par exemple l'API RESTful ou SOAP, faciles à utiliser par les développeurs pour intégrer les fonctions de signature électronique dans leurs applications métiers existantes comme Microsoft SharePoint, Office 365, GEC, GED, etc.

La plateforme doit également prendre en charge les API standard comme SAML, OAuth 2.0 / OpenID Connect pour assurer l'intégration avec les plateformes de fournisseurs de services et fournisseurs d'identités pour les services d'authentification électronique des utilisateurs.

5.5.6 Conformité

Les signatures apposées via la plateforme doivent être acceptées juridiquement, conformément à la loi 2016-012/ du 6 mai 2016 relative aux transactions, échanges et services électroniques.

La plateforme électronique doit être conforme aux normes internationales (règlement eIDAS de l'Union Européenne, normes ETSI, Adobe AATL, normes RFC 3161, RFC 6960 et RFC 2986, etc.).

La plateforme doit conserver une piste d'audit conformément aux exigences du W3C. La piste d'audit doit conserver toutes les activités de chaque utilisateur et chaque flux doit être accompagné d'un rapport d'achèvement de flux.

5.5.7 Modèle de licence et déploiement

La plupart des fournisseurs disposent de trois options de modèle de déploiement de la plateforme de signature électronique: sur site, hybride et dans le cloud.

Recommandation 2: si le MCENMA dispose d'un centre de données conforme aux bonnes pratiques de sécurité pouvant assurer l'intégrité, la confidentialité et la disponibilité de services, il est recommandé de déployer la plateforme de signature électronique au Mali, c'est-à-dire sur site et en version «entreprise», pour assurer la protection et la souveraineté des données du Gouvernement du Mali.

Les plateformes de signature électronique en version «entreprise» offrent des avantages, comme par exemple l'intégration avec les bases de données d'identification et d'authentification existantes, la signature déléguée, la gestion organisationnelle, la personnalisation des flux de travail complexes, les intégrations avec d'autres applications métiers internes, etc.

5.8 Conclusion et recommandations

Sur la base du comparatif technique et financier, quatre plateformes de signature électronique conformes aux exigences fonctionnelles et techniques ont été identifiées. Ces plateformes de signature électronique sont complètes, sécurisées et efficaces. Elles peuvent permettre au Gouvernement du Mali d'atteindre l'objectif de transformer et d'améliorer les processus de signature et de faire signer les documents avec une signature électronique à tout moment et sur tout support. Ces plateformes sont:

1. **SignHub:** la plateforme SignHub est conforme à toutes les exigences fonctionnelles et techniques de gestion des flux de signature de document avec une signature électronique et fait partie des plateformes les moins chères.

   Elle intègre facilement la signature électronique dans les applications métiers existantes comme Microsoft SharePoint et Microsoft Word. Elle permet la délégation de signature, le chiffrement des documents signés, la configuration de la permission d'accès, etc. SignHub fournit une application mobile (iOS et Android) pour signer et faire signer les documents.

   Note: la plateforme SignHub est livrée avec un module AC intégré. Deux prestataires (Entrust et LawTrust) ayant participé à l'étude comparative ont proposé la solution SignHub, LawTrust propose SignHub avec son module AC intégré alors que Entrust propose l'intégration de SignHub avec son système ICP.
2. **emSigner:** la plateforme emSigner est conforme à toutes les exigences fonctionnelles et techniques de gestion des flux de signature de document avec une signature électronique.

   emSigner fournit une séquence avancée et pré-personnalisée, il peut permettre la délégation de signature, la configuration d'un cachet pour chaque ministère ou agence, le chiffrement des documents confidentiels, etc. emSigner fournit une application mobile (iOS et Android) pour signer et faire signer les documents. emSigner est livré avec un système d'AC pour délivrer des certificats de signature aux utilisateurs.
3. **Doc MSB:** la plateforme Doc MSB est conforme à toutes les exigences fonctionnelles et techniques de gestion des flux de signature de document avec une signature électronique.

   Elle s'intègre de façon souple dans les applications métiers existantes comme Microsoft SharePoint et est livrée avec une application mobile (iOS et Android) pour signer et faire signer.
4. **NGSign:** la plateforme NGSign est conforme aux exigences fonctionnelles et techniques de gestion des flux de signature de document avec une signature électronique, à l'exception de l'application mobile pour signer et faire signer un document.

   La plateforme est livrée avec un module de signature électronique visible (QR Code Secure) et un module d'AC (Remote Trust) pour délivrer des certificats de signature aux utilisateurs. NGSign est la plateforme la moins chère.

5.6 Synthèse de l'étude comparative des plateformes de signature électronique

Tableau 8: Synthèse de l'étude comparative des plateformes de signature électronique

Plate-forme de signature électro-nique	Flux de signature	Signa-ture numé-rique	Appli mobile de signature	Authentifi-cation	Mutua-lisation (*multi-te-nancy*)	Description
Lex-Persona	●	●	○	●	●	**Lex-Persona** fournit un portail Web utilisateur pour se connecter. La plateforme fournit une séquence pour signer, faire signer et cacheter, séquentiellement ou en parallèle, un VISA de signature, une délégation de signature. La plateforme fournit le module de signature numérique qui prend en charge la signature locale et la signature à distance. Elle prend en charge les niveaux de signature basique, avancé et qualifié. Pour la signature à distance, les clés de signature des utilisateurs sont protégées dans un HSM central. La plateforme s'intègre avec le service OCSP, TSA pour l'horodatage et l'AC de l'ICP EJBCA pour la génération du certificat à la volée. Elle fournit les API Rest pour l'intégration avec les applications métiers. Elle prend en charge les protocoles SMAL, Open ID Connect, LDAP, Open Source (Quik Lock) pour l'authentification. La plateforme est mutualisée (*Multi-tenant/Multi-Admin*).

(suite)

Plate-forme de signature électro-nique	Flux de signature	Signa-ture numé-rique	Appli mobile de signature	Authentifi-cation	Mutua-lisation (*multi-te-nancy*)	Description
SIGNIUS						**SIGNIUS** fournit un portail Web utilisateur pour se connecter. La plate-forme fournit une séquence pour signer et faire signer les documents séquentiellement ou en parallèle, avec délégation de signature. SIGNIUS prend en charge la signature locale et la signature à distance, mais pour la signature à distance elle s'intègre avec une plateforme de signature tierce (CRYPTOMATIC Sign Server et Authenticator). Elle s'intègre aussi avec les services OCSP, TSA pour l'horodatage et l'AC tierce de CRYPTOMATIC. SIGNIUS fournit des interfaces basées sur les API REST, signNOW, fastTRACK, fullSTACK pour s'intégrer avec les applications métiers. SIGNIUS prend en charge les différentes méthodes d'authentification basées sur SMS, le mot de passe à usage unique (OTP), Mobile Token, OATH Token, SAML v2, OAuth2, Active Directory et LDAP. La plate-forme est mutualisée (*Multi-tenant/Multi-Admin*).

(suite)

Plate-forme de signature électro-nique	Flux de signature	Signa-ture numé-rique	Appli mobile de signature	Authentifi-cation	Mutua-lisation (*multi-te-nancy*)	Description
NGSign	●	●	○	●	●	**NGSign** fournit un portail Web utilisateur, la séquence pour signer et faire signer les documents séquentiellement ou en parallèle, la délé-gation de signature et le suivi de signature. NGSign fournit un cachet électronique visible (QR Code Secure). La plateforme fournit un module de signature numérique qui prend en charge la signature locale et la signature à distance. Elle prend en charge les niveaux de signature basique, avancé et qualifié. Pour la signature à distance, NGSign s'intègre avec le HSM central de l'AC qui gère les clés de signature des utilisateurs. L'intégration de NGSign avec d'autres AC nécessite un développement spécifique. NGSign fournit les API Rest pour l'intégration avec les applications métier. Il authentifie les utilisateurs avec nom d'utilisateur et mot de passe, peut authentifier les utilisateurs avec 2FA double ou avec certi-ficat. NGsign est mutualisé (*Multi-tenant/Multi-Admin*).

(suite)

Plate-forme de signature électro-nique	Flux de signature	Signa-ture numé-rique	Appli mobile de signature	Authentifi-cation	Mutua-lisation (*multi-te-nancy*)	Description
emSigner						**emSigner** fournit un portail Web utilisateur pour se connecter, une séquence avancée pour signer et faire signer les documents, la revue de document, la délégation de signature, des documents prédéfinis, la personnalisation du flux, etc. La plateforme permet la configuration du cachet électronique visible (QR Code). Elle sécurise les documents signés avec un chiffrement des documents. La plateforme fournit une application mobile (iOS et Android) pour la signature et le suivi de signature. La plateforme fournit un module de signature numérique qui prend en charge deux modes de signature: la signature locale et la signature à distance tierce ADHAAR. La plateforme prend en charge les niveaux de signature avancé et qualifié. Elle s'intègre avec les services OCSP/ LRC pour la validation de certificat et TSA pour l'horodatage. emSigner fournit des API RESTful et SOAP pour l'intégration avec les applications métiers. La plateforme s'intègre à un système d'authen-tification d'entreprise externe (par exemple AD/LADP). emSigner est mutualisé (*Multi-tenant/Multi-Admin*).

(suite)

Plate-forme de signature électro-nique	Flux de signature	Signa-ture numé-rique	Appli mobile de signature	Authentifi-cation	Mutua-lisation (*multi-te-nancy*)	Description
TrustedX						**TrustedX** ne fournit pas de portail Web utilisateur, ni de séquence de signature de document. La plateforme se focalise sur le moteur de signature numérique seulement. La plateforme prend en charge la signature locale et la signature à distance, elle supporte les niveaux de signature avancé et qualifié, les clés de signature des utilisateurs sont protégées dans un HSM central et la plateforme s'intègre avec le service OCSP et TSA pour l'horo-datage. TrustedX fournit une application Mobile ID (iOS et Android), utilisée pour l'authentification et l'autorisation de la signature numé-rique de l'utilisateur. La plateforme fournit les API Rest et SOAP pour l'intégration avec les applications métiers. Elle prend en charge les protocoles SMAL, OATH 2.0, Open ID Connect, LDAP, pour l'authentification. La plateforme est mutualisée (*Multi-tenant/Multi-Admin*).

(suite)

Plate-forme de signature électro-nique	Flux de signature	Signa-ture numé-rique	Appli mobile de signature	Authentifi-cation	Mutua-lisation (*multi-te-nancy*)	Description
MSB DOC						**MSB Doc** fournit un portail Web utilisateur pour se connecter, une séquence avancée pour signer et faire signer, une revue de document, une délégation de signature, des documents prédéfinis, une personnalisation de flux, etc. Il fournit une application mobile (iOS et Android) pour signer et assurer le suivi de signature. La plateforme prend en charge la signature locale et la signature à distance et prend en charge les niveaux de signature basique, avancé et qualifié. Pour les signatures à distance, la plateforme peut s'intégrer avec un HSM central (optionnel) afin de protéger les clés de signature. La plateforme s'intègre avec le service OCSP et TSA pour l'horodatage. MSB Doc fournit des API RESTful et SOAP pour l'intégration avec les applications métier. La plateforme peut s'intégrer à un système d'authentification d'entreprise externe (par exemple AD/LADP). MSB Doc est mutualisé (*Multi-tenant/Multi-Admin*).

(suite)

Plate-forme de signature électro-nique	Flux de signature	Signa-ture numé-rique	Appli mobile de signature	Authentifi-cation	Mutua-lisation (*multi-te-nancy*)	Description
SignHub						**SignHub** fournit un portail Web utilisateur pour se connecter, une séquence avancée pour signer et faire signer, une revue de document, une délégation de signature, des documents prédéfinis, une personnalisation de flux, etc. Il permet à l'utilisateur de définir les permissions (enregistrer, imprimer, télécharger, modifier, commenter, etc.). SignHub fournit une application mobile (iOS et Android) pour signer et assurer le suivi des signatures. La plateforme fournit le module de signature numérique qui prend en charge deux modes de signature (signature locale et signature à distance) et prend en charge les niveaux de signature avancé et qualifié; pour les signatures à distance les clés de signature des utilisateurs sont protégées dans un HSM central et la plateforme s'intègre avec le service OCSP, TSA pour l'horodatage. SignHub fournit les API RESTful pour l'intégration avec les applications métiers. SignHub fournit aussi modules d'extension pour Office 365, Word, SharePoint, salesforce, CRM, etc. Il prend en charge les protocoles SMAL, Open ID Connect, LDAP, pour l'authentification. La plateforme est mutualisée (*Multi-tenant/Multi-Admin*).

(suite)

Plate-forme de signature électro-nique	Flux de signature	Signa-ture numé-rique	Appli mobile de signature	Authentifi-cation	Mutua-lisation (*multi-te-nancy*)	Description
SignOK	●	○	○	●	●	**SignOK** fournit un portail Web utilisateur pour se connecter, une séquence pour signer et faire signer les documents séquentiellement ou en parallèle, la délégation de signature et le suivi de signature. SignOk prend en charge la signature locale et la signature à distance (*ICP Cloud*). La plateforme s'intègre avec une ICP dans le cloud pour pouvoir appliquer la signature à distance. Elle supporte les niveaux de signature basique, avancé et qualifié. Elle valide la signature électro-nique et s'intègre avec le service OCSP/LRC et TSA pour l'horodatage. SignOK est mutualisé (*Multi-tenant/Multi-Admin*). SignOk ne prend pas en charge l'intégration avec d'autres applica-tions métier.
LÉGENDE ● Conforme aux exigences ● Partiellement conforme aux exigences ○ Sans objet						

5.7 Synthèse financière des plateformes de signature électronique

Tableau 9: Synthèse financière

	Fonctionnalités	Lex-Persona ($)	emSigner ($)	MSB Doc ($)	SignHub ($)	NGSign ($)	SignOK ($)	TrustedX ($)	SIGNIUS ($)
1	Acquisition de la plate-forme de signature électronique	247 000	265 000	250 000	455 464	94 000	200 000	410 000	420 000
2	Services professionnels	90 000	79 000	25 000	61 000	21 000	30 000	90 000	50 000
3	Formation	52 000	50 000	50 000	50 000	50 000	50 000	50 000	50 000
4	Support et maintenance	44 200	58 300	55 000	181 518	20 000	50 000	65 000	63 000
5	ICP de base + HSM	679 000	305 000	150 000	**255 000**	107 750	1 000 000	**232 000**	150 000
Prix Total sans ICP de base		**433 200**	**452 300**	**380 000**	**747 982**	**185 000**	**330 000**	**615 000**	**583 000**
Prix Total avec ICP de base		**1 112 200**	**757 300**	**530 000**	**1 002 982**	**292 750**	**1 330 000**	**847 000**	**733 000**

Autres éléments à considérer dans le budget du projet de mise en place de la plateforme de signature électronique:

- serveurs, baie de stockage et NAS;
- équipements réseau, de sécurité et d'équilibrage de charge;
- licence du système d'exploitation, base de données et virtualisation;
- certificat SSL/TLS;
- hébergement de la plateforme de signature électronique.

6 Partie IV: Plan de mise en œuvre et budget

6.1 Phases de mise en œuvre du système ICP national

Le système ICP national est une infrastructure critique. Il nécessite le respect des normes de sécurité et les meilleures pratiques pour garantir la sécurité de l'infrastructure. Compte tenu du besoin urgent du ministère des Finances d'appliquer la signature électronique à la plateforme de marchés publics (*e-Procurement*), il est recommandé de mettre en œuvre le projet du système ICP national en 3 phases. Cela permettra au Gouvernement du Mali de répondre aux besoins du ministère des Finances.

- **Phase I:** mise en place d'une plateforme de signature électronique et d'un système ICP basique intérimaire pour les utilisateurs de ladite plateforme;
- **Phase II:** mise en place d'un système ICP national complet ;
- **Phase III:** stabilisation du système ICP établi et sensibilisation à l'utilisation de la signature numérique.

Figure 10: Résumé des phases du projet ICP

6.2 Plan d'action et budget de la Phase I

N°	Activités	Description	Responsable	Coût ($)
1	Acquisition de la plateforme de signature électronique et du système ICP de base	– Plateforme de signature électronique	SCSE	450 000
		– ICP de base pour livrer les certificats de signature aux utilisateurs de la plateforme de signature électronique	SCSE	250 000
2	Services professionnels	– Rédaction et approbation de la politique de certification de l'AC racine et de l'AC gouvernementales intérimaires – Conception des architectures de la plateforme de signature électronique, flux de tâches, systèmes et réseaux et système ICP intérimaire – Déploiement de la plateforme de signature électronique – Formation des ingénieurs et des formateurs – Intégration avec la base de données NINA et autres applications métiers	SCSE	150 000
3	Autres (réseaux, serveurs, licences, etc.)	À déterminer	SCSE	
4	Support et Maintenance * 2 ans	– Support et maintenance	SCSE	50 000
COÛT TOTAL DE LA PLATEFORME DE SIGNATURE ÉLECTRONIQUE				$ 1 000 000

6.3 Plan d'action et budget des Phases II et III

N°	Activités	Description	Responsable	Coût ($)
Établissement de la structure de gouvernance de certification électronique				
1	Validation du cadre ICP	Le cadre doit être validé par le cabinet.	– MCENMA	sans objet
2	Mise en œuvre de la structure de gouvernance nationale	Rédiger un décret et attribuer les rôles suivants aux entités identifiées: – autorité nationale chargée de la politique de l'ICP (AP); – autorité de certification racine (*Root CA*); – autorité de certification gouvernementale (*Gov CA*).	– MCENMA	sans objet
Services professionnels/cabinets-conseils ICP				
3	Amélioration du cadre juridique et réglementaire de l'ICP	– Rédaction du règlement de l'autorité de certification couvrant les critères d'accréditation, la procédure d'accréditation des AC et l'audit du demandeur d'accréditation des AC – Rédaction des exigences légales pour l'identification électronique, le cachet électronique (*eSeal*), l'authentification du site Internet, l'horodatage électronique et l'archivage électronique – Rédaction du décret rendant obligatoire l'utilisation de la signature numérique dans les services publics en ligne, les services bancaires en ligne et le commerce électronique	– MCENMA – Ministère de la Justice – Ministère du Commerce – SCSE	100 000 $

(suite)

N°	Activités	Description	Responsable	Coût ($)
4	Définition ou élaboration des politiques et procédures ICP	– Rédaction et approbation de la politique de certification (PC) de l'AC racine – Rédaction et approbation de la déclaration des pratiques de certification (DPC) – Rédaction et approbation de la politique de certification (PC) de l'AC gouvernementale – Rédaction et approbation de la déclaration des pratiques de certification (DPC) de l'AC gouvernementale – Élaboration et approbation du plan national de reprise des activités (PRD) – Rédaction et approbation de la politique de certification TSA	– Comité – SCSE	150 000 $
5	Élaboration de l'architecture du système ICP détaillé	– Conception de l'architecture du système de l'AC racine en mode LLD (*Low Level Design*) – Conception de l'architecture du système de l'AC gouvernementale en mode LLD	– SCSE	150 000 $
6	Recrutement d'un expert ICP pour accompagner la mise en œuvre du projet	– Recrutement d'un consultant/expert ICP pour l'assistance technique à la mise en œuvre du projet ICP national pour la durée du projet (*2 ans).	– SCSE	300 000 $
		Aménagement des locaux/centre de données de l'ICP		
7	Aménagement des locaux ou centre de données ICP (Optionnel)	– Conception de l'architecture intérieure du centre de données ICP – Conception de l'architecture des installations du centre de données ICP (réseau électrique, sécurité physique, système de refroidissement, etc.) – Conception de l'architecture du réseau et du système de sécurité	– SCSE	50 000 $
		– Fourniture du matériel et aménagement du centre de données ICP principal et DR	– SCSE	500 000 $

(suite)

N°	Activités	Description	Responsable	Coût ($)
		Déploiement du système ICP		
9	Achat et déploiement des systèmes de l'AC racine (*Root CA*)	– Fourniture et installation des systèmes *Root CA* (serveurs, HSM et licences des systèmes) pour l'environnement de production – Fourniture et installation des systèmes *Root CA* (serveurs, HSM et licences des systèmes) pour l'environnement DR – Fourniture et installation des systèmes *Root CA* (serveurs, HSM et licences des systèmes) pour l'environnement de test	– SCSE	500 000 $
10	Achat et Déploiement des systèmes de l'AC gouvernementale (*Gov CA*)	– Fourniture et installation des systèmes *Gov CA* (serveurs, HSM et licences des systèmes) pour l'environnement de production – Fourniture et installation des systèmes *Gov CA* (serveurs, HSM et licences des systèmes) pour l'environnement DR – Fourniture et installation du système *Gov CA* (serveurs, HSM et licences des systèmes) pour l'environnement de test	– SCSE	2 700 000 $
		Éducation et formation		
11	Formation des ingénieurs au système ICP	– Formation professionnelle des opérateurs de systèmes ICP (formation de base et avancée) – Transfert de connaissance sur les technologies ICP	– MCENMA – SCSE	100 000 $
12	Formation de sensibilisation	– Organisation d'ateliers et de séminaires sur l'ICP et l'utilisation de la signature numérique pour le grand public, dans les institutions gouvernementales et privées	– MCENMA – SCSE	50 000 $
		Projet pilote d'intégration avec l'ICP		
16	Intégration des applications métiers au système ICP	– Définition du plan d'intégration et intégration d'au moins cinq applications pilotes avec le système ICP national	– SCSE – Ministères/Agences	100 000 $
		AE et AED		

(suite)

N°	Activités	Description	Responsable	Coût ($)
13	Procédure de délivrance des certificats aux abonnés	– Définition du formulaire d'enregistrement des demandeurs de certificat et d'accord pour les abonnés	– SCSE – AED	
14	Établissement du bureau de l'AE	– Mise en place d'un bureau d'AE central	– SCSE	20 000 $
15	Lancement officiel des services de certification et signature électronique	– Définition du modèle de déclaration de procédure d'enregistrement (DPE) pour les AE et les LRA	– MCENMA – SCSE	
		COÛT TOTAL DU PROJET D'ICP NATIONALE		4 750 000

Annexe: Équipe du projet

Les ressources suivantes ont participé à l'élaboration et à la révision de ce cadre de mise en place d'ICP.

Nom	Structure	Titre	Courriel
Fanta Coumba KAREMBE	MCENMA-SCSE	Directrice du SCSE et Chef du projet ICP	directeur@certification.gouv.ml cfantakarembe@gmail.com
Mme Coulibaly Batoma Aminata SOGOBA	MCENMA	Conseillère technique	bsogoba@numerique.gouv.ml batoma.sogoba@yahoo.fr
Abdoul Kader KY	Direction nationale de l'économie numérique	Directeur	kelmeron@yahoo.fr
Ibrahima M'BAYE	Cellule d'appui à l'informatisation des services fiscaux et financiers	Directeur adjoint	i.mbaye@finances.ml
Ousmane COULIBALY	Agence des technologies de l'information et de la communication	Chef de division Développement et applications	cofacoul@agetic.gouv.ml
Souleymane KONATE	Service de certification et de signature électronique	Chef de cellule Système d'information	skonate@certification.gouv.ml konatesoul@gmail.com
Diabé BATHILY	SMTD	Chef de division Système d'information	diabe.bathily@smtd.ml
El Hadj Sekou ASOFARE	AMRTP	Membre du Conseil en charge des TIC	sascofare@amrtp.ml
Lamine Mahamadou DIALLO	AMRTP	Directeur du département Affaires juridiques	ldiallo@amrtp.ml
Mohamadou ZAROU	AMRTP	Directeur du département TIC	mzarou@amrtp.ml
Bureau régional de l'UIT pour l'Afrique	UIT	Coordinateur du projet	ITU-RO-Africa@itu.int
Charles MUGISHA	UIT	Consultant ICP	mugishac@gmail.com

Union internationale des télécommunications (UIT)
Bureau de développement des télécommunications (BDT)
Bureau du Directeur
Place des Nations
CH-1211 Genève 20
Suisse

Courriel: bdtdirector@itu.int
Tél.: +41 22 730 5035/5435
Fax: +41 22 730 5484

Adjoint au directeur et Chef du Département de l'administration et de la coordination des opérations (DDR)
Place des Nations
CH-1211 Genève 20
Suisse

Courriel: bdtdeputydir@itu.int
Tél.: +41 22 730 5131
Fax: +41 22 730 5484

Département des réseaux et de la société numériques (DNS)
Courriel:: bdt-dns@itu.int
Tél.: +41 22 730 5421
Fax: +41 22 730 5484

Département du pôle de connaissances numériques (DKH)
Courriel: bdt-dkh@itu.int
Tél.: +41 22 730 5900
Fax: +41 22 730 5484

Département des partenariats pour le développement numérique (PDD)
Courriel: bdt-pdd@itu.int
Tél.: +41 22 730 5447
Fax: +41 22 730 5484

Afrique

Ethiopie
International Telecommunication Union (ITU) Bureau régional
Gambia Road
Leghar Ethio Telecom Bldg. 3rd floor
P.O. Box 60 005
Addis Ababa
Ethiopie

Courriel: itu-ro-africa@itu.int
Tél.: +251 11 551 4977
Tél.: +251 11 551 4855
Tél.: +251 11 551 8328
Fax: +251 11 551 7299

Cameroun
Union internationale des télécommunications (UIT)
Bureau de zone
Immeuble CAMPOST, 3e étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé
Cameroun

Courriel: itu-yaounde@itu.int
Tél.: + 237 22 22 9292
Tél.: + 237 22 22 9291
Fax: + 237 22 22 9297

Sénégal
Union internationale des télécommunications (UIT)
Bureau de zone
8, Route des Almadies
Immeuble Rokhaya, 3e étage
Boîte postale 29471
Dakar - Yoff
Sénégal

Courriel: itu-dakar@itu.int
Tél.: +221 33 859 7010
Tél.: +221 33 859 7021
Fax: +221 33 868 6386

Zimbabwe
International Telecommunication Union (ITU) Bureau de zone
TelOne Centre for Learning
Corner Samora Machel and
Hampton Road
P.O. Box BE 792
Belvedere Harare
Zimbabwe

Courriel: itu-harare@itu.int
Tél.: +263 4 77 5939
Tél.: +263 4 77 5941
Fax: +263 4 77 1257

Amériques

Brésil
União Internacional de Telecomunicações (UIT)
Bureau régional
SAUS Quadra 6 Ed. Luis Eduardo Magalhães,
Bloco "E", 10º andar, Ala Sul (Anatel)
CEP 70070-940 Brasilia - DF
Brazil

Courriel: itubrasilia@itu.int
Tél.: +55 61 2312 2730-1
Tél.: +55 61 2312 2733-5
Fax: +55 61 2312 2738

La Barbade
International Telecommunication Union (ITU) Bureau de zone
United Nations House
Marine Gardens
Hastings, Christ Church
P.O. Box 1047
Bridgetown
Barbados

Courriel: itubridgetown@itu.int
Tél.: +1 246 431 0343
Fax: +1 246 437 7403

Chili
Unión Internacional de Telecomunicaciones (UIT)
Oficina de Representación de Área
Merced 753, Piso 4
Santiago de Chile
Chili

Courriel: itusantiago@itu.int
Tél.: +56 2 632 6134/6147
Fax: +56 2 632 6154

Honduras
Unión Internacional de Telecomunicaciones (UIT)
Oficina de Representación de Área
Colonia Altos de Miramontes
Calle principal, Edificio No. 1583
Frente a Santos y Cía
Apartado Postal 976
Tegucigalpa
Honduras

Courriel: itutegucigalpa@itu.int
Tél.: +504 2235 5470
Fax: +504 2235 5471

Etats arabes

Egypte
International Telecommunication Union (ITU) Bureau régional
Smart Village, Building B 147,
3rd floor
Km 28 Cairo
Alexandria Desert Road
Giza Governorate
Cairo
Egypte

Courriel: itu-ro-arabstates@itu.int
Tél.: +202 3537 1777
Fax: +202 3537 1888

Asie-Pacifique

Thaïlande
International Telecommunication Union (ITU) Bureau régional
4th floor NBTC Region 1 Building
101 Chaengwattana Road
Laksi,
Bangkok 10210,
Thailande

Adresse postale:
P.O. Box 178, Laksi Post Office
Laksi, Bangkok 10210, Thailand

Courriel: itu-ro-asiapacific@itu.int
Tél.: +66 2 574 9326 – 8
+66 2 575 0055

Indonésie
International Telecommunication Union (ITU) Bureau de zone
Sapta Pesona Building
13th floor
Jl. Merdan Merdeka Barat No. 17
Jakarta 10110
Indonésie

Courriel: itu-ro-asiapacific@itu.int
Tél.: +62 21 381 3572
Tél.: +62 21 380 2322/2324
Fax: +62 21 389 5521

Pays de la CEI

Fédération de Russie
International Telecommunication Union (ITU) Bureau régional
4, Building 1
Sergiy Radonezhsky Str.
Moscow 105120
Fédération de Russie

Courriel: itumoscow@itu.int
Tél.: +7 495 926 6070

Europe

Suisse
Union internationale des télécommunications (UIT)
Bureau pour l'Europe
Place des Nations
CH-1211 Genève 20
Suisse
Courriel: eurregion@itu.int
Tél.: +41 22 730 5467
Fax: +41 22 730 5484

Union internationale des télécommunications
Bureau de développement des télécommunications
Place des Nations
CH-1211 Genève 20
Suisse

ISBN: 978-92-61-35932-4

9 789261 359324

Publié en Suisse
Genève, 2022