POLITIQUE DE SIGNATURE ELECTRONIQUE ET GESTION DE PREUVE

Titre

DEMATERIALISATION OUVERTURE DE COMPTE

GROUPE BANQUES POPULAIRES

1. CONTEXTE & OBJECTIF

Acteur de tout premier plan du développement économique et social du Maroc, le Groupe Banque Populaire (GBP) est aujourd'hui engagé dans une dynamique de transformation vers un groupe multi-métiers, de conquête de nouveaux territoires et de nouveaux relais de croissance à savoir la transformation digitale.

Pour le Crédit Populaire du Maroc, le digital est davantage un vecteur d'évolution naturelle que de révolution. Une situation qui découle notamment de l'importance stratégique des systèmes d'information existants qui ont accompagné la dématérialisation amorcée depuis longtemps déjà. Toutefois, la banque s'engage dans un vaste processus de transformation digitale pour s'adapter aux nouvelles caractéristiques de son marché.

Le Crédit Populaire du Maroc a adapté une vision de refonte des ces processus autour d'un programme de digitalisation de bout-en-bout, avec une nouvelle logique centrée client, qui se base sur l'amélioration durable de l'expérience client grâce à des processus simples et fluides. Ainsi que l'augmentation nette de la productivité du réseau grâce à des processus automatisés réduisant massivement la charge administrative des agents et leur permettant de se focaliser sur le conseil au client. C'est dans cette optique que s'inscrit le présent projet « Entrée en relation digitale, visant notamment la dématérialisation de l'ouverture de compte au niveau des agences de CPM, cette dématérialisation intègre le processus de signature électronique des documents contractuels.

Cette contractualisation en ligne est conforme aux dispositions légales en vigueur, notamment :

- La loi n°53-05 relative à l'échange électronique de données juridiques ;
- La loi n°09-08 relative à la protection des données personnelles ;

Une signature électronique, étant un procédé d'identification de l'auteur d'un document électronique, doit permettre de garantir l'authentification et la vérification de l'identité du signataire, le lien avec l'acte avec lequel elle s'attache et l'intégrité de l'acte. La signature électronique doit émaner d'un procédé fiable d'identification garantissant le lien avec l'acte avec lequel elle s'attache.

A veiller à l'existence d'un Certificat Electronique contenant notamment les données de vérification de la signature électronique.

Lorsque les fonctions de signature électronique sont mises à disposition des signataires, il est important qu'ils aient connaissance du contexte dans lequel cette signature électronique est produite, des rôles, obligations que chaque acteur endosse, et des conditions dans lesquelles cette signature sera ultérieurement traitée, conservée, disponible pour vérification.

2. POLITIQUE DE SIGNATURE ET GESTION DE PREUVE

2.1 Champ d'application

Une politique de signature et gestion de preuve est un document décrivant les conditions de recevabilité d'un fichier sur lequel sont apposées une ou plusieurs signatures électroniques dans le cadre d'échanges électroniques prédéfinis.

La présente politique de signature et gestion de preuve s'applique à la « Dématérialisation de l'ouverture de compte » au niveau des agences CPM, visant la signature de :

- ✓ La convention d'ouverture de compte
- ✓ Le compte rendu de l'entretien de vigilance (compte rendu du KYC),
- ✓ Les conditions générales des produits et services,
- ✓ Les annexes liées aux spécificités des comptes.

Tout client se présentant à l'agence pour l'ouverture d'un compte doit signer dans tous les cas les documents suivants :

- ✓ La convention d'ouverture de compte
- ✓ Le compte rendu du KYC

Les autres documents à signer dépendent du pack et/ou des produits et services choisis par le client et aussi du type du compte.

Le nombre de document à signer est proportionnel au nombre de produits et services choisis, un pack est considéré comme un produit. Les documents de plus à signer dans ce cas sont les conditions générales des produits et services et les annexes liées aux comptes spécifiques.

Cette présente politique de signature concerne les produits et services suivants.

- ✓ Pack
- ✓ Carte et assistance
- ✓ Chaabi net
- ✓ Pocket bank

L'ouverture de compte se fait en agence avec le chargé de clientèle.

Dans le cadre de cette « Dématérialisation d'ouverture de compte », les acteurs qui ont la capacité de signer électroniquement sont : le chargé de clientèle et le client majeur

La signature électronique permet de répondre à plusieurs contextes :

- Contexte fonctionnel :
    - La signature électronique reprend deux fonctions de la signature sur support papier (authentification et consentement) et requiert une fonction supplémentaire: la fiabilité (procédé fiable d'identification garantissant le lien entre la signature électronique et l'acte auquel elle s'attache).
    - La signature électronique doit permettre d'apposer la signature du chargé de clientèle et du Client sur le document, dans le délai le plus bref après son consentement. Ces signatures sont réalisées à partir des certificats générés à la volée par une Autorité de certification du Groupe Banques Populaires.
- Contexte règlementaire :
    - La solution s'inscrit dans le contexte réglementaire et juridique, notamment la Politique de certification associée à l'AC émettrice des certificats utilisés.
- Contexte économique :
    - La mise en œuvre de la signature électronique a pour objectif de réduire les coûts d'impression en multi-exemplaire des contrats.
    - La mise en œuvre de la signature électronique dans le cadre de la dématérialisation d'ouverture de compte au niveau des agences de CPM s'inscrit dans le projet global de l'Infrastructure de Confiance « Chaabi - eSign » du Groupe Banques Populaires

La présente Politique de signature électronique et gestion de preuve est portée à la connaissance du client lors du processus d'ouverture de compte et avant l'opération de signature électronique. De cette façon, le signataire est en capacité de prendre connaissance de ces conditions de signature au moment de la réalisation de cette action. Respectivement, cette Politique de signature électronique et gestion de preuve est mise à disposition des destinataires, pour leur permettre de prendre connaissance des conditions dans lesquelles les signataires ont signé les documents.

2.2 Identification

La présente politique de signature et gestion de preuve est identifiée par l'O.I.D : 1.2.504.1.1.2.1.1.6.1

Cette référence, ainsi que le numéro de version de la politique de signature et gestion de preuve utilisée, figure dans le document, afin d'attester du régime sous lequel le signataire adresse ses informations.

2.3 Publication du document

Avant toute publication officielle, la politique de signature et gestion de preuve est validée par le comité BCP digital

La présente Politique de signature et gestion de preuve :

- est présentée au client lors du processus d'ouverture de compte avant l'étape de signature
- est publiée sur l'URL :

http://www.gbp.ma/Documents/Politique_Signature_Gestion_de_preuve_CPM_Digital.pdf

Les demandes d'informations ou commentaires sur cette politique doivent être adressés à

responsablepki@cpm.co.ma
Banque Centrale Populaire
Angle Mohamed El Bakri & Angle Mohamed Diouri
Casablanca Maroc

2.4 Processus de mise à jour

2.4.1 Circonstances rendant une mise à jour nécessaire

La mise à jour d'une politique de signature et gestion de preuve est un processus impliquant tous les acteurs et faisant l'objet d'une démarche rigoureuse. Il est enclenché essentiellement pour procéder à des modifications importantes, pour prendre en compte de nouveaux besoins, de nouveaux acteurs, de nouvelles dispositions légales et réglementaires, ou combler des lacunes.

La présente politique est réexaminée lors de toute modification majeure du processus d'ouverture de compte.

2.4.2 Prise en compte des mises à jour

Les remarques et demandes d'amélioration sont examinées par le comité BCP digital, qui engage si nécessaire, le processus de mise à jour de la présente politique de signature et gestion de preuve.
Une signature électronique est toujours valide, par rapport à la politique de signature et gestion de preuve qui s'appliquait au moment de la signature électronique. Toutes les versions des Politiques de Signature et gestion de preuve, et leur durée respective de validité sont donc conservées par CPM, et accessibles sur demande.

2.4.3 Information des acteurs

Lorsqu'une mise à jour a été planifiée, les informations relatives à cette modification sont mises en ligne sur les lieux de publication. Indépendamment de ce mode de communication, les acteurs peuvent à tout moment se renseigner auprès du comité d'approbation pour obtenir plus d'informations. La publication d'une nouvelle version de la politique de signature et gestion de preuve consiste à archiver la version précédente et mettre en ligne dans le répertoire prévu à cet effet, les éléments suivants :

- Document au format PDF
- OID du document
- Empreinte du document
- Algorithme de hachage utilisé (condensat SHA256 pour cette version)
- Date et heure exacte d'entrée en vigueur.
- Le document archivé porte, en filigrane sur ses pages, la mention « Document obsolète ».

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

Lorsqu'une nouvelle version de la politique de signature et gestion de preuve est mise en ligne, un message électronique est diffusé sur le portail www.gbp.ma accessible de tous les signataires pour les informer de la nature et de la date et heure du changement.

La nouvelle version de la politique de signature et gestion de preuve entre en vigueur dès sa publication sur le site identifié à la section 2.3. La nouvelle version reste valide jusqu'à la publication de la version suivante.

3. ACTEURS & RÔLES

3.1 Les acteurs

3.1.1 Signataires disposant du profil « Client »

Les signataires sont des personnes physiques. Il s'agit nécessairement de Client majeur, se présentant en agence pour l'ouverture de compte. Le Client utilise un moyen d'authentification forte, One time Password (OTP) qu'il reçoit par sms, qui permet de l'authentifier avant d'entamer le processus de signature.

Dans le cadre de ce processus de signature, les clients signent électroniquement les documents contractuels d'ouverture de compte cités précédemment, reprenant les rôles et obligations contenues dans la présente politique.

3.1.2 Signataire agent CPM « Chargé clientèle »

Les signataires sont les chargés de clientèle ayant l'habilité d'ouvrir un compte pour des personnes physiques ou morales. Ils entament le processus d'ouverture de compte par une authentification, ils remplissent des informations liés au client et ils l'aident à choisir ses produits et services.

A l'étape de la signature électronique, le chargé de clientèle s'authentifie une deuxième fois et signe électroniquement les documents contractuels d'ouverture de compte cités précédemment reprenant les rôles et obligations contenues dans la présente politique.

3.1.3 Destinataires des contrats signés électroniquement

Les destinataires des documents signés électroniquement sont :

- D'une part, les Clients eux-mêmes qui reçoivent par mail les documents, dont la signature électronique matérialise leur consentement par rapport aux clauses;
- Chargé de clientèle qui apporte sa signature sur les documents ;
- Directeur d'agence
- CTN (Centre de traitement national Epargne et comptes)

3.1.4 Déroulement de la signature

- Le client valide ses informations fournies lors de son enregistrement en ligne, ou corrige d'éventuelles erreurs ;
- Le chargé de clientèle s'authentifie dans la plateforme de dématérialisation d'ouverture de compte sur une tablette ou équipement adapté ;
- Le chargé de clientèle clique sur Signer, le système signe les documents avec son certificat généré automatiquement ;
- Le client accepte les Conditions générales d'utilisation et valide ;
- Le système envoie au client un code d'authentification unique par sms (OTP), pour valider son identité ;
- Le client saisit L'OTP ;
- Le client clique sur signer, le système génère un certificat pour l'utilisateur qui sera utilisé par la suite pour signer les documents ;
- Ensuite les destinataires reçoivent par mail les documents signés.

3.2 Rôles et obligations du client

Dans le processus de signature, le client doit vérifier que les informations fournis sont exactes avant de donner son consentement et de signer électroniquement les documents à l'aide de son certificat personnel de signature généré par le système pour cette transaction.

Le client doit vérifier le détail des informations fournies et de corriger d'éventuelles erreurs, et ce avant de confirmer pour exprimer son acceptation.

Pour l'ouverture d'un compte pour mineur, son tuteur en plus des autres documents doit signer les annexes liées au compte (lettre d'autorisation d'ouverture de compte à un mineur)

3.2.1 Environnement de travail

L'opération de création de la signature est réalisée sur une tablette ou équipement adapté à l'agence face à face avec le chargé de clientèle.

3.2.2 Type de certificat utilisé

Dans le cadre de cette signature, la Bi-clé et le certificat associé du client sont générés à la volée et stockés dans un support cryptographique (HSM certifié EAL4+) et supprimés automatiquement à la fin de la transaction.

3.3 Rôles et obligations de CPM

3.3.1 Environnement de l'application de signature

L'application de signature pour la dématérialisation de l'ouverture de compte au niveau des agences CPM utilisée par le client et le chargé de clientèle est l'élément sensible du processus de signature. L'application est installée dans des Datacenter du GROUPE BANQUES POPULAIRES.

En particulier, il est mis en œuvre :

- La surveillance de l'accès physique et logique au système et de le protéger contre les intrusions,
- Une limitation d'accès et d'administration de l'application signature à un minimum de personnes de confiance, ayant les compétences requises.
- Le suivi des recommandations du fournisseur relatives à la sécurité du système.

3.3.2 Type de certificat utilisé

Le chargé de clientèle sous couvert de CPM, avec qui le document est signé, dispose également d'un certificat de signature généré à la volée. Ce certificat est émis par une Autorité de Certification du GROUPE BANQUES POPULAIRES.

Dans le processus de signature, les documents signés sont horodatés, ces certificats techniques d'horodatage sont émis par une Autorité de Certification du GROUPE BANQUES POPULAIRES.

3.3.3 Données de Vérification

Pour effectuer les vérifications, CPM utilise les données présentes dans le système mis en œuvre, notamment :

- Les données publiques relatives aux certificats des signataires, telles que les listes de révocations.
- Les habilitations des signataires à signer;

Le contrat signé fait l'objet d'un horodatage permettant :

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

3.3.4 Protection du certificat Client

Le certificat « éphémère » de signature du client est généré dans le boitier cryptographique associé au serveur de signature. Aucun support n'est remis au Client.

CPM en s'appuyant sur l'IGC de GROUPE BANQUES POPULAIRES, au niveau de la plateforme de signature est en charge de :

- Générer une nouvelle bi-clé (clé publique et clé privée) pour créer le certificat client.
- Protéger cette bi-clé dans le boitier cryptographique qualifié du serveur.
- Réaliser les opérations de signature.
- Détruire la bi-clé à la fin de l'opération du processus de signature.

CPM autorise l'utilisation de certificats personnels référencés pour la signature d'un client

- Le client est enrôlé par l'autorité d'enregistrement (CPM) à l'autorité de certification
- La bi-clé est générée par une Autorité de Certification référencée
- Cette bi-clé est stockée dans un support matériel « qualifié »
- Le certificat est de courte durée, utilisé uniquement dans le cadre d'une seule transaction.
- Les opérations de signature sont effectuées sur l'équipement de l'agence (tablette ou équipement adapté) avec le certificat personnel « déclaré »
- Le serveur de signature consulte la liste de révocation émise par l'Autorité de certification qui a émis le certificat afin de s'assurer de sa validité.

3.3.5 Révocation du certificat

Le client a la possibilité de demander la révocation du certificat électronique utilisé pour signer auprès de l'agence .

Il est à préciser que les certificats éphémères ayant une durée de validité de quelques minutes, le cas de révocation d'un tel certificat ne pourra être qu'extrêmement ponctuel.

En tout état de cause, l'Autorité de Certification qui a émis le certificat de signature assure un service de révocation et publie la Liste des Certificats Révoqués.

3.3.6 Protection des moyens

GROUPE BANQUES POPULAIRES, via l'équipe IGC, s'assure de la mise en œuvre des moyens nécessaires à la protection des équipements fournissant les services de signature et de validation.

Les mesures prises concernent à la fois :

- La protection des accès physiques et logiques aux équipements aux seules personnes habilitées;
- La disponibilité du service ;

- La surveillance et le suivi du service.

3.3.7 Journalisation

CPM, via l'équipe IGC, s'assure de la conservation des traces relatives :

- A la circulation des échanges au sein des réseaux et des équipements informatiques.
- Au traitement des données échangées.

CPM s'assure que les preuves de traitement relatives à la vérification des signatures électroniques sont conservées pendant toute la durée règlementaire.

3.3.8 Reprise en cas d'interruption de service

CPM, via l'équipe IGC, s'assure de la mise en œuvre des moyens nécessaires à la reprise d'activité en cas d'interruption de service d'un des composants nécessaire aux tâches dont il a la responsabilité.

Il s'assure en particulier que ces moyens font l'objet de tests à intervalles réguliers.

3.3.9 Assistance aux utilisateurs

Les clients peuvent communiquer avec CPM pour toute information complémentaire ou pour signaler tout dysfonctionnement en s'adressant au :

responsablepki@cpm.co.ma
Banque Centrale Populaire
Angle Mohamed El Bakri & Angle Mohamed Diouri
Casablanca Maroc

3.3.10 Audit technique et juridique

Le GROUPE BANQUES POPULAIRES fait réaliser sur son infrastructure de confiance :

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

4. SIGNATURE ÉLECTRONIQUE ET VALIDATION

4.1 Caractéristiques de l'équipement du signataire

Le terminal sur lequel est produite la signature est une tablette ou équipement adapté, fonctionnant dans un environnement sous le contrôle du signataire.

Les certificats utilisés pour la signature suite à une authentification forte (OTP) sont des certificats éphémères, valables le temps de l'opération de signature.

Ce certificat est produit par une Autorité de Certification du GROUPE BANQUES POPULAIRES.

4.2 Données signées

Au moment de la signature électronique, le Client signe électroniquement les documents définis dans la section 2.1

4.3 Opération de signature électronique

Les fonctionnalités minimales suivantes sont assurées, pour permettre au client d'avoir connaissance et conscience de l'action qu'il est sur le point d'effectuer :

Présentation du document à signer:

Le signataire a la possibilité de visualiser les informations du document que la plateforme de dématérialisation d'ouverture de compte lui propose de signer.

Présentation des attributs de la signature au signataire :

La fonction de signature est intégrée à la plateforme de dématérialisation d'ouverture de compte avec lequel le client signe le document. Les Conditions Générales d'Utilisation du Service de signature sont présentées au client et précisent notamment les conditions dans lesquelles sa signature électronique sera réalisée et traitée :

Interaction avec le signataire : consentement explicite et possibilité d'arrêt du processus de signature

Le client a les moyens d'exprimer explicitement (c'est-à-dire, de manière volontaire et non ambiguë) son consentement en confirmant sa volonté de signer les conditions particulières et déclencher le processus de signature du document sélectionné.

4.4 Caractéristiques des signatures

4.4.1 Type de signature

Les signatures électroniques apposées sur les documents sont des signatures PDF

4.4.2 Norme de signature

La signature mise en œuvre est basée sur la norme PaDES.

4.5 Algorithmes utilisables pour la signature

4.5.1 Algorithme de condensation

L'algorithme de condensation utilisé est SHA-256.

4.5.2 Algorithme de chiffrement

L'algorithme de chiffrement utilisé est RSA Encryption

4.6 Conditions pour déclarer valide le contrat signé

Un contrat signé est considéré comme valide par CPM lorsque les conditions suivantes sont remplies :

- vérification positive de la signature électronique du signataire.
- vérification positive des droits du signataire en fonction des données transmises.

4.6.1 Vérification de la signature

La vérification de la signature porte sur :

- La vérification du respect de la norme de signature ;
- La vérification que le certificat du Client est émis par l'AC du GROUPE BANQUES POPULAIRES dédiée à l'émission de certificats éphémère reconnue et acceptée par le GROUPE BANQUES POPULAIRES;
- La vérification du certificat du Client et de tous les certificats de la chaîne de certification:
    - Validité temporelle,
    - Statut,
    - Signature cryptographique ;
- La vérification de l'intégrité des données transmises par calcul de l'empreinte et comparaison avec l'empreinte reçue.
- La vérification de la signature électronique du client apposée sur le document en utilisant la clé publique du Client contenue dans le certificat transmis.
- La vérification des données d'horodatage apposées sur la signature électronique du document;
- La vérification que les certificats utilisés au moment de la signature n'étaient pas dans une Liste de Certificats Révoqués. Cette vérification est basée sur la constitution d'une liste blanche lors de la génération ou la révocation d'un certificat de signature.
- La vérification de l'identifiant de la politique de signature et gestion de preuve référencée.

4.6.2 Vérification des droits du signataire en fonction de données transmises

La vérification porte sur :

- L'identification du signataire à l'aide de son certificat ;
- La vérification des droits associés à ce certificat en fonction du type de données signées.

4.7 Gestion de la preuve

Pour conserver une trace de chaque transaction de signature, la plateforme de signature met en place une preuve électronique signée et horodatée, qui recense les éléments associés au processus de signature effectuée :

- Document original avant signature ;
- Document signé par le chargé de clientèle
- Document signé par l'ensemble des Parties (Client d'un côté et CPM de l'autre) ;
- Certificat de signature utilisé par le Client ;
- Certificat de signature du chargé de clientèle (CPM) ;
- Numéro de téléphone du client ;
- OTP envoyé au client par SMS ;
- La date exacte de chaque action
- Fichier de preuve signé et horodaté.

Cette preuve peut être exploitée ultérieurement en cas de litige pour restituer exactement les informations utilisées lors de la transaction.

5. POLITIQUE DE CONFIDENTIALITÉ ET RESPECT DES DISPOSITIONS DE LA LOI 09-08 RELATIVE A LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

5.1 Classification des informations

Les informations suivantes sont considérées comme confidentielles :

- les données secrètes associées au certificat (clé privée),
- les journaux de l'application « Dématérialisation des contrats »,
- les procédures internes à l'équipe IGC permettant d'assurer la disponibilité de l'application « Dématérialisation des contrats » mise à disposition dans le portail CPM.
- les rapports d'audit sur cette application et sur les différents composants de l'infrastructure.
- Les données personnelles du Client.

6. DISPOSITIONS JURIDIQUES

6.1 Droit applicable

Le présent document est régi par la loi marocaine.

6.2 Règlement des différents

Tout différend découlant du procédé de signature doit, en premier lieu, et dans toute la mesure du possible, être réglé au moyen de négociations amiables entre les parties.

Toutes contestations et litiges survenant dans l'interprétation et la mise en œuvre du présent document seront soumis à la juridiction des tribunaux compétents.

6.3 Données à caractère personnel

En conformité avec les dispositions de Loi n° 09-08 du 18 février 2009 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, le traitement automatisé des données nominatives réalisées par GBP ont fait l'objet d'une déclaration auprès de la CNDP.

Les données personnelles demandées par CPM ont un caractère obligatoire pour l'ouverture de compte et souscription aux produits et services. Elles sont utilisées exclusivement à cette fin par CPM

Les données sont protégées aussi bien sur support physique qu'électronique, de sorte que leur accès soit impossible à des tiers non autorisés. CPM s'assure que les personnes habilitées à traiter les données personnelles connaissent leurs obligations légales en matière de protection de ces données et s'y tiennent.

Les données à caractère personnel peuvent à tout moment faire l'objet d'un droit d'accès, de modification, de rectification et d'opposition auprès de CPM, mail : …, Tél : …, Fax : ……..

7. DEFINITIONS

Authentification
Processus permettant de vérifier l'identité déclarée d'une personne ou de toute autre entité, ou de garantir l'origine de données reçues.
Bi clé
Un bi clé est un couple composé d'une clé privée (devant être tenue secrète) et d'une clé publique, nécessaire à la mise en œuvre de techniques cryptologiques basées sur des algorithmes asymétriques.
Certificat
Clé publique d'un utilisateur, concaténée à d'autres informations rendues infalsifiables par signature avec la clé privée de l'autorité de certification qui l'a délivré
Infrastructure de gestion de Clés (IGC)
Ensemble de composantes fournissant des services de gestion de clés et de certificats au profit d'une communauté d'utilisateurs.
Liste de Certificats Révoqués (LCR)
Liste contenant les identifiants des certificats révoqués ou invalides.
PAdES
PDF Advanced Electronic Signatures : Norme émise par l'ETSI (European Telecommunications Standards Institute) permettant de produire des signatures électroniques avancées pour le format PDF.
Politique de certification (PC)
Ensemble de règles relatives à l'applicabilité d'un certificat à une communauté et / ou à une classe d'applications ayant des besoins de sécurité communs.
Politique de signature et gestion de preuve
Document qui décrit les conditions dans lesquelles sont réalisées, traitées, conservées les signatures électroniques, les conditions et contextes dans lesquels ces signatures électroniques seront ultérieurement consultables, utilisables et vérifiables.
Politique d'horodatage
Ensemble de règles relative à l'émission de jetons d'horodatages.
Référentiel Général de Sécurité (RGS)
Le Référentiel Général de Sécurité (RGS) définit un ensemble de règles de sécurité qui s'imposent aux autorités administratives dans la sécurisation de leurs systèmes d'information. Il propose également des bonnes pratiques en matière de sécurité des systèmes d'information que les autorités administratives sont libres d'appliquer.
Signataire
Personne physique utilisant son ordinateur pour signer par voie électronique un document.
OTP
One time password (mot de passe à usage unique)
ETSI
European Telecommunications Standards
OID
Object Identifier
SHA-256
Secure Hash Algorithm (algorithme de hachage)
Empreinte du document
Condensat ou haché du document obtenu avec la fonction de hachage
IGC
Infrastructure de gestion de clés
Equipe IGC
L'équipe IGC est chargée d'administrer et d'exploiter l'IGC, la plate-forme de signature, ainsi que le serveur d'horodatage permettant d'horodater les transactions à l'issue de leur signature, puis de valider et d'archiver ces informations signées.
AC
Autorité de certification