Référentiel et Règles attestant de la qualité des Auditeurs des Prestataires et Services de confiance au Togo

Version janvier 2024

Table des matières

1. Objet du Référentiel

Le présent Référentiel a pour objectif de déterminer les exigences auxquelles doivent répondre les Auditeurs afin de mener à bien leur mission.

Conformément à l'article 97 de la LTE, l'Organe de contrôle a pour rôle de contrôler a priori et a posteriori les PSCQ établis sur le territoire national afin de s'assurer que ces PSCQ et les services de confiance Qualifiés fournis sont conformes aux exigences légales et réglementaires nationales ;

Les Auditeurs devront à ce titre :

- Vérifier la conformité des Services de Confiance aux Référentiels, à savoir et selon le cas :
  - le Référentiel Certification Electronique ;
  - le Référentiel Archivage Electronique ;
  - le Référentiel Recommandé Electronique et ;
  - le Référentiel Horodatage Electronique ;
- Proposer des mesures, si nécessaire, en ce qui concerne la mise en conformité des PSC non-qualifiés, établis sur le territoire national, qui ne seraient pas conformes aux exigences légales et réglementaires nationales.
- Disposer de compétences techniques dans le domaine du/des Référentiel/s pour lesquels ils sont accrédités ;
- Se maintenir à niveau des évolutions techniques en suivant des formations régulièrement ;
- Répondre à des exigences déontologiques de rigueur, d'indépendance et d'impartialité ;

2. Définitions

2.1 Accréditation de l'Auditeur : reconnaissance par l'Autorité de Certification Togolaise, de la capacité d'évaluation par l'Auditeur de la conformité des PSC conformément aux exigences des Référentiels et du Cadre légal et Règlementaire applicable notamment la LTE et son Décret n°2018-062.

2.2 Audit : expertise fonctionnelle réalisée par un Auditeur :

i. afin de s'assurer qu'un Service de Confiance est conforme aux exigences découlant du cadre légal et réglementaire applicable évalué par rapport aux exigences du Référentiel applicable et ;

ii. proposer des mesures correctives pour y parvenir

L'Audit consiste soit en un Audit Initial de Qualification, soit un Audit de Contrôle de Qualification.

2.3 Audit Initial de Qualification : Audit réalisé par l'Auditeur, sur demande d'un PSC non Qualifié souhaitant obtenir la Qualification pour fournir ses Services de Confiance.

2.4 Audit de Contrôle de Qualification : Audit réalisé par l'Auditeur soit à l'initiative de l'Autorité de Certification Togolaise, soit sur une demande d'un PSCQ soumis à un Audit qui doit être effectué, tous les 24 mois, à ses frais afin de confirmer le respect des Référentiels et du cadre légal et réglementaire applicable par un PSCE.

2.5 Auditeur : évaluateur expert compétent au regard du présent Référentiel et du Service de Confiance, dont la fonction est de réaliser un Audit. L'Auditeur peut être interne à l'Autorité de Certification Togolaise ou externe.

2.6 Autorité de Certification Togolaise : autorité chargée de la certification et organe de contrôle, créée par la LTE, dans les conditions fixées par le Chapitre IV du Décret n°2018-062. Elle est chargée de définir la politique togolaise de certification et de la faire appliquer notamment par l'Accréditation, la Qualification et le contrôle a priori et a posteriori des PSC.

2.7 Constat d'Audit : résultats de l'évaluation des Preuves d'Audit recueillies dans le cadre de la Prestation d'Audit et devant faire partie intégrante du Rapport d'Audit.

2.8 Convention de prestation de service d'Audit : convention écrite entre le PSC Audité et l'Auditeur pour la réalisation de la mission d'Audit.

2.9 Critères d'Audit : critères au regard desquels est examinée la conformité du Service de Confiance aux Référentiels applicables

2.10 Décret n°2014-088 : Décret du 31 mars 2014 portant sur les régimes applicables aux activités de communications électroniques modifié par le Décret n° 2018-145 du 3 octobre 2018

2.11 Décret n°2014-112 : Décret du 30 avril 2014 portant sur l'interconnexion et l'accès aux réseaux de communications électroniques modifié par le Décret n° 2018-144 du 3 octobre 2018.

2.12 Décret n°2016-103 : Décret du 20 décembre 2016 portant sur des modalités de gestion administrative, technique et commerciale du domaine internet national « .tg ».

2.13 Décret n°2018-062 : Décret n°2018-062 portant sur la réglementation des transactions et services électroniques au Togo en application de la LTE.

2.14 Donnée : toute information élémentaire présente dans un Système d'Information.

2.15 Etat de l'art : ensemble des bonnes pratiques, des technologies et des documents de références relatifs à la Sécurité des Systèmes d'Informations publiquement accessibles à un instant donné. Ces documents peuvent notamment être issus d'organismes de référence, d'origine réglementaire ou des documents partagés par la communauté de la sécurité des systèmes d'information.

2.16 LCE : La loi n°2012-018 du 17 décembre 2012 sur les communications électroniques modifiée par la loi n°2013-003 du 19 février 2013.

2.17 LOSITO : loi n°2017-006 du 22 juin 2017 d'orientation sur la société de l'information au Togo.

2.18 LTE : la Loi 2017-007 du 22 juin 2017 relative aux transactions électroniques modifiée par la loi n° 2023-012 du 19 juillet 2023 entrée en vigueur en 2017 au Togo.

2.19 Périmètre d'Audit : environnement physique, logique et organisationnel dans lequel se trouve le Système d'Information utilisé pour la fourniture du Service de Confiance

2.20 Preuve d'Audit : enregistrements, copies d'écran, tout élément tangible permettant d'apporter la preuve et traçabilité au Rapport d'Audit.

2.21 Prestataire de Service de Confiance ou PSC : prestataire de Service de Confiance délivrant des Services de Confiance au sens de la LTE, du Décret n°2018-062 et des Référentiels applicables.

2.22 PSC non Qualifié : Prestataire de Service de Confiance délivrant des Services de Confiance qui ne sont pas qualifiés au sens du cadre légal et réglementaire applicable notamment la LTE, le Décret n°2018-062 et les Référentiels applicables.

2.23 PSCE : prestataire de Service de Certification Electronique délivrant des Services de Certification Electronique qui peut fournir des Certificats Electroniques pour différents usages, niveaux de sécurité et pour différents types d'utilisateur. Un PSCE est identifié, dans le champ « *issuer* » du Certificat de l'AC dont il a la responsabilité.

2.24 PSCE Accrédité : PSCE justifiant une Accréditation valide.

2.25 PSC Audité : PSC ayant sollicité un Audit pour obtenir la Qualification et/ ou étant soumis à un Audit en raison de son statut de PSCQ.

2.26PSCQ : Prestataire de Service de Confiance Qualifié c'est-à-dire justifiant d'une Qualification valide.

2.27 Prestation d'Audit : prestation effectuée par un Auditeur afin d'évaluer la qualification d'un PSC dans le cadre d'un Audit Initial ou d'un Audit de Contrôle.

2.28 Qualification : reconnaissance, par l'Autorité de Certification, de la conformité des Services de Confiance Electroniques fournis par un PSC comme répondant aux exigences du Référentiel et au cadre légal et réglementaire applicable.

2.29 Référentiels : chacun des référentiels permettant d'apprécier la conformité des Services de Confiance, aux lois, règlements et normes en vigueur, notamment, les Référentiels pour les Services d'archivage électronique, d'horodatage électronique, de recommandé électronique et de certification électronique.

2.30 Rapport d'Audit : document de synthèse élaboré par l'Auditeur et remis au PSCE ou PSCQ Audité à l'issue de l'Audit. Ce rapport comporte notamment les Constats de l'Audit, les Preuves d'Audit ainsi que les Recommandations Associées.

2.31 Recommandations Associées : les recommandations délivrées par l'Auditeur en vue de la mise en conformité d'un PSC ou d'un Service de Confiance.

2.32 Sécurité d'un Système d'Information : ensemble de moyens techniques et organisationnels de protection permettant à un Système d'Information de résister à des évènements susceptibles de remettre en cause son intégrité, sa disponibilité, la protection des informations qu'il contient et/ou la confidentialité des données traitées ou transmises ou rendues accessibles par son intermédiaire.

2.33 Service de Confiance Qualifié : prestation normalement fournie contre rémunération et définie comme telle dans la LTE et le Décret.

2.34 Service de Confiance Qualifié : Service de Confiance qui a été Audité et reconnu comme répondant aux exigences du Référentiel et du cadre légal et réglementaire applicable par l'Autorité de Certification Togolaise notamment la LTE et son Décret n°2018-062.

2.35 Service de Confiance Non-Qualifié : services de Confiance qui n'a pas été reconnu comme répondant aux exigences du Référentiels et au cadre légal et réglementaire applicable par l'Autorité de Certification Togolaise.

2.36 Service d'Archivage Electronique : services dont l'objet principal est la conservation de données électroniques et notamment de permettre et d'assurer la conservation numérique de documents et de

données pendant une durée déterminée et dans des conditions assurant l'intégrité, l'interopérabilité et la sécurité de ces éléments.

2.37 Service de Certification Electronique : service dont l'objet principal est la délivrance, la validation et la conservation de Certificats de Signature ou de Cachet Electronique.

2.38 Service d'Horodatage Electronique : service visant à dater des ensembles de données électroniques.

2.39 Service de Recommandé Electronique : tout service de transmission de données électroniques visant à fournir une preuve de la réalité et de la date de leur envoi et, le cas échéant, de leur réception par le destinataire des données.

2.40 Système d'Information : ensemble organisé de ressources matérielles, immatérielles, humaines, et organisationnelles, ainsi que des données et des procédures permettant de traiter et de diffuser l'information d'une entreprise et/ou d'un prestataire.

2.41 Vulnérabilité : faiblesse d'un bien ou d'une mesure pouvant être exploitée par un attaquant et représenter une menace pour le système d'information.

3. Présentation générale

L'Autorité de Certification Togolaise a pour rôle de :

(i) définir les Référentiels et les Critères d'Audit ;

(ii) accréditer les Auditeurs ;

(iii) délivrer les Accréditations des PSCE ;

(iv) délivrer les Qualifications des PSCQ.

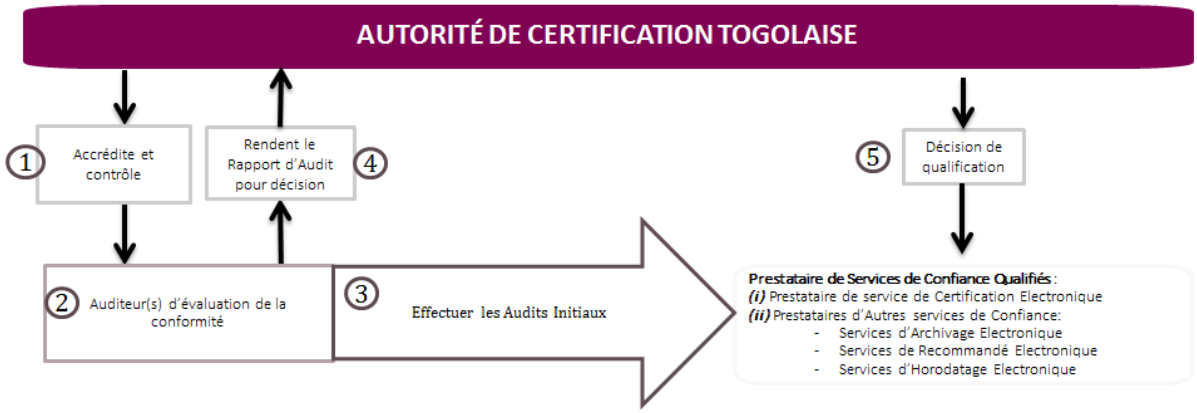
L'Autorité de Certification Togolaise dispose d'une Sous-Direction d'évaluation de la conformité, laquelle est notamment chargée de vérifier la qualité des Auditeurs et de les Qualifier.

Il existe différents Prestataires de services électroniques :

(i) Les Prestataires de Services de Certification Électronique (PSCE)

(ii) Les Prestataires de Services de Confiance qui peuvent, cumulativement ou non, fournir des Services (i) d'Archivage Electronique, (ii) d'Horodatage Electronique, (iii) de Recommandé Electronique.

Tous les Prestataires de services de confiance qualifiés (PSCQ) ou non qualifiés sont soumis au contrôle de l'Autorité de Certification Togolaise [1] selon le schéma suivant :



L'Accréditation de l'Auditeur d'évaluation de la conformité lui permettra de faire valoir ses compétences dans les domaines correspondants à son Accréditation.

[1] Articles 97 ; 98 ; 98-1, 99, 100 et 101 de la LTE

4. Exigences générales relatives aux Auditeurs

I. Exigences générales

Les Auditeurs doivent exercer leurs fonctions dans l'impartialité avec compétences.

- L'Auditeur doit respecter la réglementation applicable sur le territoire national et notamment en matière de sécurité informatique, protection des données personnelles, prêt de main d'œuvre illicite et fraude informatique.
- L'Auditeur doit être partie d'une entité dotée de la personnalité morale de façon à pouvoir être responsable juridiquement de ses activités d'Audit. Ainsi, l'Auditeur pourra être tenu responsable en cas de dommages éventuellement causés au PSCE ou PSCQ Audité dans le cadre de l'Audit ;
- Préalablement à toute activité d'Audit, l'Auditeur devra conclure une Convention d'Audit avec le PSCE ou PSCQ Audité afin de déterminer précisément le Périmètre de l'Audit.
- L'Auditeur devra souscrire à une police d'assurance adaptée au regard des risques encourus et en justifier auprès de l'Autorité de Certification Togolaise.
- La sous-traitance est interdite sauf autorisation écrite expresse et préalable de l'Autorité de Certification Togolaise. En tout état de cause, l'Auditeur sera tenu responsable des actions de ses sous-traitants.
- Afin d'assurer son impartialité dans la réalisation de la Prestation d'Audit, l'Auditeur devra documenter les modalités du fonctionnement desdites Prestations d'Audit, notamment financières, afin de démontrer que ces modalités de fonctionnement ne sont pas de nature à compromettre son impartialité ni la qualité de ses prestations d'Audit ou de provoquer des conflits d'intérêt.
- L'Auditeur devra réaliser ses Prestations d'Audit de manière loyale et de bonne foi, dans le respect du PSCE ou PSCQ Audité, de son personnel et de ses infrastructures.
- En tout état de cause, l'Auditeur devra respecter la Charte Ethique applicable à ses activités.

II. Aptitudes générales des Auditeurs

Les Auditeurs doivent maitriser le cadre légal et réglementaire applicable notamment la LTE et son Décret n°2018-062 sur le territoire national concernant le Périmètre d'Audit.

Les Auditeurs doivent disposer de qualités rédactionnelles et de synthèse et savoir s'exprimer à l'oral de façon claire et compréhensible.

Les Auditeurs devront suivre une formation continue afin de toujours être à jour des évolutions de la réglementation nationale applicable et en justifier auprès de l'Autorité de Certification Togolaise.

III. Engagements

L'Auditeur doit avoir un contrat avec l'Autorité de Certification Togolaise ou avec un Organisme d'évaluation de la conformité externe.

L'Auditeur doit également avoir signé la Charte Ethique et avoir accepter d'exercer ses missions dans le respect de ses dispositions.

5. Exigences approfondies correspondant aux différentes prestations d'Audit

I. Exigences approfondies pour les Auditeurs des Services de Certification Electronique

Les Auditeurs d'évaluation de la conformité des Services de Certification Electronique devront disposer des compétences approfondies décrites ci-dessous.

(a) Dans les domaines techniques

- Dispositifs de chiffrement et d'authentification ;
- Infrastructures à clefs publiques (ICP ou PKI) ;
- Solutions de gestion de journalisation ;
- Mécanismes cryptographiques ;
- Principes et méthodes d'intrusion applicatives ;
- Contournement des mesures de sécurité logicielle ;

(b) Dans le domaine organisationnel

- Maîtrise des domaines relatifs à l'organisation de la sécurité des systèmes d'information :
  - Analyse des risques ;
  - Politique de sécurité des systèmes d'information ;
  - Chaîne de responsabilités en sécurité des systèmes d'information ;
  - Gestion de l'exploitation et de l'administration du Système d'Information ;
  - Contrôle d'accès logique au Système d'Information ;
  - Gestion des incidents liés à la sécurité de l'information ;
  - Gestion du plan de continuité de l'activité ;
  - Sécurité physique
- Maîtrise des pratiques liées à l'Audit :
  - Conduite d'entretien ;
  - Visite sur site ;
  - Analyse documentaire ;

(c) Dans le domaine des Référentiels

- Maîtrise des référentiels applicables aux Services de Certification Electronique
- Maîtrise des annexes complètes et techniques, conformément au Référentiel d'exigences applicables aux Services de Certification Electronique
- Maîtrise du cadre normatif

II. Exigences approfondies pour les Auditeurs des Services d'Archivage Electronique

Les Auditeurs d'évaluation de la conformité des Services d'Archivage Electronique devront disposer des compétences approfondies décrites ci-dessous.

(a) Dans les domaines techniques

- Dispositifs de chiffrement et d'authentification ;
- Infrastructures à clefs publiques (ICP ou PKI) ;
- Solutions de gestion de journalisation ;
- Mécanismes cryptographiques ;

(b) Dans les domaines organisationnels

- Maîtrise des domaines relatifs à l'organisation de la sécurité des systèmes d'information :
  - Analyse des risques ;
  - Politique de sécurité des systèmes d'information ;
  - Chaîne de responsabilités en sécurité des systèmes d'information ;
  - Gestion de l'exploitation et de l'administration du Système d'Information ;
  - Contrôle d'accès logique au Système d'Information ;
  - Gestion des incidents liés à la sécurité de l'information ;
  - Gestion du plan de continuité de l'activité ;
  - Sécurité physique
- Maîtrise des pratiques liées à l'Audit :
  - Conduite d'entretien ;
  - Visite sur site ;
  - Analyse documentaire ;

(c) Dans le domaine des Référentiels

- Maîtrise des référentiels applicables aux Services d'Archivage Electronique
- Maîtrise des annexes complètes et techniques, conformément au Référentiel d'exigences applicables aux Services d'Archivage Electronique
- Maîtrise du cadre normatif

III. Exigences approfondies pour les Auditeurs des Services d'Horodatage Electronique

Les Auditeurs d'évaluation de la conformité des Services d'Horodatage Electronique devront disposer des compétences approfondies décrites ci-dessous.

(a) Dans les domaines techniques

- Dispositifs de chiffrement et d'authentification ;
- Infrastructures à clefs publiques (ICP ou PKI) ;
- Solutions de gestion de journalisation ;

- Mécanismes cryptographiques ;

(b) Dans les domaines organisationnels

- Maîtrise des domaines relatifs à l'organisation de la sécurité des systèmes d'information :
  - Analyse des risques ;
  - Politique de sécurité des systèmes d'information ;
  - Chaîne de responsabilités en sécurité des systèmes d'information ;
  - Gestion de l'exploitation et de l'administration du Système d'Information ;
  - Gestion des incidents liés à la sécurité de l'information ;
  - Gestion du plan de continuité de l'activité ;
- Maîtrise des pratiques liées à l'Audit :
  - Conduite d'entretien ;
  - Visite sur site ;
  - Analyse documentaire ;

(c) Dans le domaine des Référentiels

- Maîtrise des référentiels applicables aux Services d'Horodatage Electronique
- Maîtrise des annexes complètes et techniques, conformément au Référentiel d'exigences applicables aux Services d'Horodatage Electronique
- Maîtrise du cadre normatif

IV. Exigences approfondies pour les Auditeurs des Services de Recommandé Electronique

Les Auditeurs d'évaluation de la conformité des Services de Recommandé Electronique devront disposer des compétences approfondies décrites ci-dessous.

(a) Dans les domaines techniques

- Dispositifs de chiffrement et d'authentification ;
- Infrastructures à clefs publiques (ICP ou PKI) ;
- Solutions de gestion de journalisation ;
- Mécanismes cryptographiques ;
- Principes et méthodes d'intrusion applicatives ;

(b) Dans les domaines organisationnels

- Maîtrise des domaines relatifs à l'organisation de la sécurité des systèmes d'information :
  - Analyse des risques ;
  - Politique de sécurité des systèmes d'information ;
  - Chaîne de responsabilités en sécurité des systèmes d'information ;
  - Gestion de l'exploitation et de l'administration du Système d'Information ;
  - Contrôle d'accès logique au Système d'Information ;

- Gestion des incidents liés à la sécurité de l'information ;
- Gestion du plan de continuité de l'activité ;
- Sécurité physique

- Maîtrise des pratiques liées à l'Audit :
  - Conduite d'entretien ;
  - Visite sur site ;
  - Analyse documentaire ;

(c) <u>Dans le domaine des Référentiels</u>

- Maîtrise des référentiels applicables aux Services de Recommandé Electronique
- Maîtrise des annexes complètes et techniques, conformément au Référentiel d'exigences applicables aux Services de Recommandé Electronique
- Maîtrise du cadre normatif

6. Prestations d'Audit

I. Modalités des prestations d'Audit

Les Prestations d'Audit consistent soit :

- en un Audit Initial ; ou

- en un Audit de Contrôle.

L'Auditeur dispose d'un délai de trois (3) mois pour effectuer sa mission. Ce délai peut éventuellement être prolongé avec l'accord de l'Autorité de Certification Togolaise et moyennant une justification.

A l'issue de ces Audits, les Auditeurs fournissent un rapport d'évaluation de la conformité que le PSC Audité devra conserver.

L'Auditeur remet un Constat d'Audit à l'Autorité de Certification Togolaise.

Si, au vu de ce Constat d'Audit, l'Autorité de Certification Togolaise estime que le PSC Audité répond aux exigences du Référentiel, elle lui attribuera le statut prévu dans un délai de trois (3) mois.

L'Autorité de Certification Togolaise publie et tient à jour les listes de confiance ainsi que les informations relatives aux Auditeurs ayant réalisé les Audits[2].

Si l'Auditeur conclu que le PSC ou son Service de Confiance n'est pas conforme au Référentiel, l'Auditeur indique les Recommandations Associées permettant au PSC Audité de se mettre en conformité dans un délai fixé par l'Auditeur après approbation de l'Autorité de Certification Togolaise.

II. Exigences relatives au déroulement d'une prestation d'Audit

Étape 1. Établissement de la convention

L'Auditeur doit conclure une convention avec le PSC Audité avant l'exécution de l'Audit.

Cette Convention d'Audit doit être signée par le représentant légal du PSC Audité et par l'Auditeur.

(i) Modalités de la prestation

La Convention d'Audit doit :

- Décrire le Périmètre de l'Audit, la démarche générale d'Audit, les activités et les modalités de la prestation : objectifs, champs et Critères de l'Audit, jalons, livrables attendus en entrée, prérequis etc.
- Préciser les livrables attendus par le PSC Audité, les réunions d'ouverture et de clôture de la mission d'Audit, le niveau de sensibilité ou de classification des informations du PSC Audité ;
- Décrire les moyens techniques (matériels et outils) et organisationnels et moyens de communication mis en œuvre par l'Auditeur dans le cadre de sa mission ;
- Prévoir les moyens logistiques devant être mis à disposition de l'Auditeur par le PSC Audité ;
- Définir les moyens assurant la traçabilité entre le PSC Audité et l'Auditeur sur les informations et les supports matériels remis pour analyse.

[2] Article 56 Décret n°2018-062

(ii) Organisation

La Convention d'Audit doit :

- Préciser le nom du responsable du suivi de l'Audit chez le PSC Audité, chargé de mettre en relation l'Auditeur avec les différents correspondants impliqués ;
- Préciser les noms, rôles, responsabilités ainsi que les droits et besoins d'en connaître des personnes désignées par l'Auditeur et le PSC Audité dans le cadre de la mission ;

(iii) Responsabilités

La Convention d'Audit doit :

- Stipuler que l'Auditeur ne réalisera sa mission qu'après autorisation formelle et écrite du PSC Audité ;
- Stipuler que l'Auditeur informera le PSC Audité en cas de manquement à la Convention d'Audit ;
- Stipuler que l'Auditeur s'engage à ce que les actions réalisées dans le cadre de l'Auditeur restent strictement en adéquation avec les objectifs de l'Audit et du Périmètre d'Audit ;
- Stipuler que l'interlocuteur désigné par le PSC Audité garantit disposer de l'ensemble des droits d'accès et de propriété sur le périmètre de la prestation (systèmes d'information, supports logiciels et matériels) ou d'avoir recueilli l'accord des éventuels tiers dont les systèmes d'information entreraient dans le périmètre ;
- Stipuler que les personnes désignées chez le PSC Audité et les Auditeurs remplissent toutes les obligations légales et réglementaire nécessaires aux Prestations d'Audit ;
- Stipuler que le PSC Audité autorise provisoirement l'Auditeur, aux seules fins de réaliser la prestation d'Audit, d'accéder et de se maintenir dans tout ou partie de son Système d'Information et d'effectuer des traitements sur les données hébergées, quelle que soit la nature de ces données ;
- Stipuler que le PSC Audité autorise provisoirement l'Auditeur à reproduire, collecter et analyser aux seules fins de réaliser la Prestation d'Audit, des données appartenant au périmètre du Système d'Information cible ;
- Définir les responsabilités et les précautions d'usage à respecter par l'ensemble des parties concernant les risques potentiels liés à la prestation, en matière de confidentialité des informations collectées et analysées ainsi qu'en matière de disponibilité et d'intégrité du Système d'Information cible ;
- Stipuler que l'Auditeur dispose d'une assurance professionnelle couvrant les éventuels dommages causés lors de la réalisation des Prestations d'Audit et, le cas échéant, préciser la couverture de celle-ci et inclure l'attestation d'assurance.

(iv) Confidentialité

La Convention d'Audit doit :

- Prévoir la non-divulgation à un tiers par l'Auditeur, de toute information relative à l'Audit et au PSC Audité, sauf autorisation écrite ;
- Stipuler que l'Auditeur puisse, sauf refus écrit de la part du PSC Audité, conserver certains types d'information liés à la Prestation d'Audit une fois celle-ci terminée. Les types d'information concernés devront être listés dans la Convention d'Audit ;
- Stipuler que l'Auditeur anonymise et décontextualise l'ensemble des informations que le PSC Audité l'autorise à conserver ;

- Stipuler une obligation de destruction de l'ensemble des informations relatives au PSC Audité à l'issue de la prestation à l'exception de celles pour lesquels l'Auditeur a reçu une autorisation écrite ;
- Préciser les modalités de rédaction des recommandations (contenu, forme, portée etc.) ;
- Prévoir une procédure de recueil du consentement des personnes Auditées et des éventuels partenaires pour la réalisation de l'Audit ;
- Prévoir que tous les documents relatifs à l'Audit sont communicables à l'Autorité de Certification Togolaise.

(v) Cadre légal et réglementaire

La Convention d'Audit doit :

- Être rédigée en français ;
- Stipuler que la législation applicable à la convention de Prestation d'Audit est la législation togolaise ;
- Préciser les moyens techniques et organisationnels mis en œuvre par l'Auditeur pour le respect du cadre légal et réglementaire applicable en matière de (i) protection des données, (ii) secret des correspondances privées, (iii) fraude informatique ;
- Préciser les éventuelles exigences légales et réglementaires spécifiques auxquelles serait soumis le PSC Audité en raison notamment de son secteur d'activité ;
- Définir la durée de conservation des informations liées à la Prestation d'Audit et notamment les évènements collectés et les incidents de sécurité détectés ;
- Décrire le Périmètre de l'Audit ;
- Décrire l'organisation de l'Audit en fonction du Périmètre de celui-ci et en fonction de chaque PSC Audité ;
- Préciser les modalités de partage de responsabilité dans le cadre de la réalisation de l'Audit. Notamment que l'Auditeur pourra s'exonérer de sa responsabilité si les dommages survenus résultent d'un défaut d'information par le PSC Audité ;
- Préciser les conditions financières.

(vi) Sous-traitance

La Convention d'Audit devra préciser si l'Auditeur a été autorisé par l'Autorité de Certification Togolaise pour recourir à des sous-traitants et dans quelles conditions.

En outre, l'Auditeur, s'il a recours à un sous-traitant, devra conclure une convention ou un cadre contractuel avec lui.

La Convention d'Audit devra préciser que l'Auditeur peut faire intervenir un expert sur une partie des activités pour des besoins ponctuels sous réserve d'avoir informé et reçu une acceptation formelle de la part du PSC Audité et d'avoir conclu une convention avec l'expert. En tout état de cause, l'expert sera encadré par l'Auditeur.

(vii) Qualification

Lorsque la Convention d'Audit est conclue avec un Auditeur externe à l'Autorité de Certification Togolaise, la Convention d'Audit devra préciser que l'Auditeur est qualifié et inclure l'attestation de Qualification de l'Auditeur.

Étape 2. Préparation et déclenchement de la Prestation d'Audit

L'Auditeur doit désigner une personne en charge du suivi de la mission : le responsable de suivi de l'Audit.

L'Auditeur devra, s'il ne peut réaliser l'Audit seul, constituer une équipe d'Auditeurs ayant les compétences adaptées à la mission d'Audit.

L'Auditeur devra mettre en place, avec son interlocuteur privilégié chez le PSC Audité, un programme de suivi de la Prestation d'Audit, comprenant la durée de la mission, la mise en place de points d'étapes et l'émission de comptes rendus réguliers si cela s'avère nécessaires.

L'Auditeur devra donc définir le Périmètre de l'Audit, lequel devra prévoir :

- Les objectifs, champs et Critères de l'Audit ;
- Le périmètre technique et organisationnel de la prestation ;
- Les dates et lieux où seront menées les activités d'Audit et notamment celles éventuellement menées dans les locaux du PSC Audité ;
- Les informations générales sur les réunions de démarrage et de clôture de la prestation ;
- Les Auditeurs qui constituent l'équipe d'Audit le cas échéant ;
- La confidentialité des données récupérées et l'anonymisation des constats et des résultats.

En fonction de la Prestation d'Audit, l'Auditeur devra se voir communiquer au préalable toute la documentation existante du PSC Audité telle que la politique de sécurité, les procédures d'exploitation de sécurité, d'éventuelles analyses de risques etc.

L'Auditeur devra sensibiliser le PSC Audité sur la sauvegarde et la préservation de ses données, applications et systèmes, préalablement à la Prestation d'Audit.

Étape 3. Exécution des prestations

Toute constatation et observation réalisée par l'Auditeur devra faire l'objet d'une description factuelle et basées sur des Preuves d'Audit.

Les Constats d'Audits doivent être documentés, tracés et conservés par l'Auditeur et illustré par des Preuves d'Audit pendant toute la durée de l'Audit.

Étape 4. Restitution

A la fin de l'Audit et avant que le Rapport d'Audit ne soit achevé, l'Auditeur devra informer le PSC Audité des constats et des premières conclusions de l'Audit.

Il présentera notamment le cas échéant les point de non-conformité majeurs et critiques qui nécessitent une action rapide en décrivant les Recommandations Associées.

Étape 5. Elaboration du Rapport d'Audit

Un Rapport d'Audit doit être élaboré à l'issue de chaque Prestation d'Audit.

Le Rapport d'Audit doit contenir en particulier :

- Une synthèse, compréhensibles par des non-experts et précisant :
    - Le contexte et le périmètre de la prestation de manière très succincte, le Périmètre de l'Audit ayant déjà été décrit dans la Convention d'Audit ;
    - Les points de non-conformité critiques, d'origine technique ou organisationnelle et les Recommandations Associées ;

- L'appréciation du niveau de sécurité des Services de Confiance Audité par rapport à l'Etat de l'art et en considération du Périmètre d'Audit et les Référentiels applicables ;

- Un tableau synthétique des résultats de l'Audit précisant :
  - La synthèse des points de non-conformité relevés, classés selon une échelle de valeur de criticité et en fonction de leur impact sur la sécurité du Système d'Information et leur difficulté d'exploitation ;
  - La synthèse des mesures correctives proposées, classées par criticité et par complexité ou coût estimé de correction et permettant d'améliorer le niveau de sécurité afin d'atteindre la conformité au Référentiel ;
- Une analyse de la sécurité des Services de Confiance Audités, qui présente les résultats des différentes Prestations d'Audit réalisées ;
- Le cas échéant, l'Auditeur devra préciser les réserves relatives à l'exhaustivité de ses Constats d'Audit et les raisons de cette exhaustivité par rapport au délai imparti pour réaliser l'Audit ou aux informations sommaires obtenues de la part du PSC Audité par exemple.
- Les coordonnées des personnes ayant réalisé l'Audit devront être précisées dans le rapport.

Étape 6. Clôture de la Prestation d'Audit

A l'issue de la Prestation d'Audit et après avoir communiqué le Rapport d'Audit, l'Auditeur organise une réunion de clôture avec les interlocuteurs du PSC Audité.

Cette réunion sera l'occasion pour le PSC Audité de poser ses questions sur les Recommandations Associées pour la mise en conformité du PSC et de ses Services de Confiance aux Référentiels.

L'Auditeur devra faire signer au PSC Audité une attestation selon laquelle le Système d'Information Audité n'a pas été dégradé par l'Audit afin de préserver l'Auditeur de tout engagement de sa responsabilité post-Audit.

La Prestation d'Audit sera considérée comme terminée lorsque le PSC Audité aura attesté formellement et par écrit que le Rapport d'Audit convient aux objectifs fixés dans la Convention d'Audit.

Si l'Autorité de Certification Togolaise l'estime pertinent au regard des Constats d'Audit, elle pourra ordonner la réalisation d'un Audit de validation afin de s'assurer que les Recommandations Associées ont été correctement appliquées et ne nécessitent pas d'ajustements particuliers.

7. Désignation et contrôle des Auditeurs

Les Auditeurs sont désignés et contrôlés par l'Autorité de Certification Togolaise au sein de l'ARCEP (Autorité de Régulation des Communications Electroniques et des Postes au Togo).

Le présent Référentiel décrit les exigences auxquelles doivent répondre les Auditeurs pour prétendre être en mesure de contrôler les PSCE et les PSCQ dans les meilleures conditions et de façon à assurer la pérennité de la chaîne de confiance au Togo.

Le respect des exigences par les Auditeurs sera régulièrement contrôlé par l'Autorité de Certification Togolaise et à minima tous les vingt-quatre (24) mois.

Le respect de ces exigences fera l'objet d'une Qualification dont l'objectif est d'attester la valeur des prestations d'Audit effectuées et qui participe à la construction de la confiance dans les prestations de services électroniques Audités.

8. Charte Ethique

Les Auditeurs doivent signer la Charte éthique de l'Autorité de Certification Togolaise prévoyant notamment que

- Les Prestations d'Audit sont réalisées avec loyauté, impartialité, discrétion et indépendance ;
- Les Auditeurs ne recourent qu'aux méthodes, outils et techniques validés par l'Autorité de Certification Togolaise ;
- Les Auditeurs s'engagent à ne pas divulguer, même de manière anonymisée ou décontextualisée, y compris aux autres Auditeurs non concernés par l'Audit, d'informations obtenues ou générées dans le cadre de leurs missions sauf autorisation du PSC Audité ;
- Les Auditeurs signalent au PSC Audité tout contenu manifestement illicite découvert durant l'Audit ;
- Les Auditeurs s'engagent à respecter la loi et la réglementation nationale en vigueur ainsi que les bonnes pratiques liées à l'Audit