pixidgroup

Mesures communes applicables à l'ICP

C1 - publique

SOMMAIRE

1. Introduction

Le présent document rassemble les les mesures « non techniques » applicables dans l'Infrastructure de Confiance PIXID.

Ce document est référencé dans les documents suivants :

- Certification Policy - AC Root - PIXID Group;
- Certification Policy - AC Users Simple - PIXID Group;
- Certification Policy - AC Users Advanced - PIXID Group;
- Certification Policy - AC Users - PIXID Group;

Les Déclaration des Pratiques associées ;
Les Conditions Générales de Vente et d'Utilisation associées aux Services commercialisés.

2. Mesure de sécurité non techniques

Les différents contrôles décrits ici visent, par une gestion des risques adéquate, à assurer un niveau de confiance fort dans le fonctionnement de l'AC PIXID ROOT CA.

2.1 Mesures de sécurité physique

2.1.1 Situation géographique et construction des sites

La situation géographique des sites de productions est conforme aux exigences du document.

2.1.2 Accès physique

Les zones hébergeant les systèmes informatiques de l'AC PIXID ROOT CA sont physiquement protégées contre un accès extérieur non autorisé.
La liste des personnels autorisés à y accéder existe et est limitée au strict besoin du bon fonctionnement du service. L'accès des personnels autorisés est contrôlé par un moyen physique et enregistré.

2.1.3 Alimentation électrique et climatisation

Les installations électriques et de conditionnement d'air sont suffisantes pour le bon fonctionnement des systèmes informatiques de l'AC PIXID ROOT CA.

2.1.4 Vulnérabilité aux dégâts des eaux

Les systèmes informatiques de l'AC PIXID ROOT CA ne sont pas situés en zone inondable, ni du fait d'intempéries, ni du fait de tuyauteries défaillantes.

2.1.5 Prévention et protection incendie

Les locaux d'hébergement des systèmes informatiques de l'AC PIXID ROOT CA sont protégés contre les incendies (détection et extinction automatiques). La distribution des machines permet par ailleurs d'assurer une disponibilité maximale des services.

2.1.6 Conservation des supports

Les supports contenant des données sauvegardées ou archivées doivent être conservés avec un niveau de sécurité au moins égal à celui des systèmes les ayant générés.
Les moyens mis en œuvre pour atteindre cet objectif seront précisés dans la DPC.

2.1.7 Mise hors service des supports

La destruction ou la réinitialisation des supports seront assurées avec un niveau de sécurité au moins égal à celui des systèmes les ayant générés.
Les moyens mis en œuvre pour atteindre cet objectif seront précisés dans la DPC.

2.1.8 Sauvegarde hors site

L'organisation des sauvegardes des informations sera adaptée de façon à assurer une reprise après désastre la plus rapide possible, en particulier pour les services impliqués dans la révocation de certificats.
Les informations sauvegardées hors site doivent respecter les exigences de la présente PC en matière de protection en confidentialité et en intégrité de ces informations.
Les moyens mis en œuvre pour atteindre cet objectif seront précisés dans la DPC.

2.2 Mesures de sécurité procédurales

Des contrôles des procédures sont mis en place par l'AC PIXID ROOT CA et sont détaillés dans la DPC correspondant à cette PC, autour des thèmes suivants :

2.2.1 Rôles de confiance

Chaque composante de l'IGC doit distinguer au moins les rôles fonctionnels de confiance suivants :

- **Responsable sécurité** : Le responsable de sécurité est chargé de la mise en œuvre de la politique de sécurité de la composante. Il gère les contrôles d'accès physiques aux équipements des systèmes de la composante. Il est habilité à prendre connaissance des archives et est chargé de l'analyse des journaux d'évènements afin de détecter tout incident, anomalie, tentative de compromission, etc. ;

- **Responsable d'exploitation** : Le responsable d'exploitation est chargé, au sein de la composante à laquelle il est rattaché, de la mise en œuvre de la politique de certification et de la déclaration des pratiques de certification de l'IGC au niveau de l'application dont il est responsable. Sa responsabilité couvre l'ensemble des fonctions rendues par cette application et des performances correspondantes ;

- **Opérateur** : Un opérateur au sein d'une composante de l'IGC réalise, dans le cadre de ses attributions, l'exploitation des applications pour les fonctions mises en œuvre par la composant ;

- **Ingénieur système** : Il est chargé de la mise en route, de la configuration et de la maintenance technique des équipements informatiques de la composante. Il assure l'administration technique des systèmes et des réseaux de la composante ;

- **Auditeur** : Personne désignée par une autorité compétente et dont le rôle est de procéder de manière régulière à des contrôles de conformité de la mise en œuvre des fonctions fournies par la composante par rapport aux politiques de certification, aux déclarations des pratiques de certification de l'IGC et aux politiques de sécurité de la composante.

- **Porteur de part de secret** : Personne ayant la responsabilité d'assurer la confidentialité, l'intégrité et la disponibilité des parts de secrets qui leur sont confiés.

Les attributions nominatives de chaque rôle sont décrites dans la DPC.

2.2.2 Nombre de personnes requises par tâches

Selon la tâche à effectuer, une ou plusieurs personnes devront être présentes lors de l'exécution de la tâche. La DPC précisera pour chacune des tâches liées à la gestion des certificats le nombre et le rôle de personnes nécessaires.

2.2.3 Identification et authentification pour chaque rôle

Chaque composante de l'AC PIXID Root CA doit vérifier l'identité et les autorisations de son personnel devant intervenir, avant :

- que son nom soit ajouté aux listes des personnes ayant accès physiquement aux systèmes informatiques de l'AC ;
- qu'un compte lui soit ouvert dans les systèmes informatiques de l'AC PIXID Root CA ;

2.2.4 Rôle exigeant une séparation des attributions

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre. Pour les rôles de confiance, il est néanmoins recommandé qu'une même personne ne détienne pas plusieurs rôles et, au minimum, les exigences ci-dessous de non cumul doivent être respectées.
Concernant les rôles de confiance, les cumuls suivants sont interdits :

- responsable de sécurité et ingénieur système / opérateur
- auditeur/contrôleur et tout autre rôle
- ingénieur système et opérateur

Les attributions associées à chaque rôle sont décrites dans la DPC de l'AC et sont conformes à la politique de sécurité de la composante concernée.

2.3 Mesures de sécurité vis-à-vis du personnel

2.3.1 Qualifications, compétences et habilitations requises

Tous les personnels amenés à travailler au sein de composantes de l'IGC sont soumis à une clause de confidentialité vis-à-vis de leur employeur.

Chaque entité opérant une composante de l'IGC s'assure que les attributions de ses personnels, amenés à travailler au sein de la composante, correspondent à leurs compétences professionnelles.

Le personnel d'encadrement possède l'expertise appropriée à son rôle et être familier des procédures de sécurité en vigueur au sein de l'IGC.

L'AC s'assure que tous les membres du personnel qui accomplissent des tâches relatives à l'exploitation d'une AC:

- sont nommés à leur poste par écrit ;
- sont tenus par contrat ou par la loi de respecter les obligations, notamment de confidentialité, du poste qu'ils occupent ;
- n'ont pas de tâches ou d'intérêts susceptibles d'entrer en conflit avec les obligations qui leur incombent à l'égard de l'AC.

2.3.2 Procédures de vérification des antécédents

Chaque entité opérant une composante de l'IGC met en œuvre tous les moyens légaux dont elle peut disposer pour s'assurer de l'honnêteté de ses personnels amenés à travailler au sein de la composante.
Ces personnels n'ont pas de condamnation de justice en contradiction avec leurs attributions. Ils devront remettre à leur employeur une copie du bulletin n°3 de leur casier judiciaire avant l'attribution du rôle de confiance puis à tout moment sur simple demande.
Les personnes ayant un rôle de confiance ne souffrent d'aucun conflit d'intérêts préjudiciables à l'impartialité de leurs tâches.
Ces vérifications sont menées préalablement à l'affectation à un rôle de confiance et revues régulièrement (au minimum tous les 3 ans), sauf pour le bulletin de casier judiciaire.

2.3.3 Exigences en matière de formation initiale

Le personnel est formé aux logiciels, matériels et procédures de fonctionnement et de sécurité de la composante au sein de laquelle il opère.
L'AC s'assure que tous les membres du personnel qui accomplissent des tâches touchant la gestion de l'AC ont reçu une formation adaptée concernant les principes de fonctionnement et des mécanismes de sécurité de l'AC, et sont familiarisés aux règles de sécurité en vigueur.

2.3.4 Exigences et fréquence en matière de formation continue

Le personnel concerné reçoit une information et une formation adéquates préalablement à toute évolution dans les systèmes, dans les procédures, dans l'organisation, etc. en fonction de la nature de ces évolutions.

2.3.5 Fréquence et séquence de rotation

L'AC n'impose pas la rotation de son personnel habilité.

2.3.6 Sanctions en cas d'actions non-autorisées

Sur faute avérée ou soupçonnée d'un membre de l'AC dans l'accomplissement de ses tâches, l'AC lui interdit l'accès aux systèmes et, le cas échéant, prend toutes sanctions disciplinaires adéquates.

2.3.7 Exigences vis-à-vis du personnel des prestataires externes

Les exigences vis-à-vis des prestataires externes sont contractualisées.

2.3.8 Documentation fournie au personnel

L'AC s'assure que son personnel dispose de l'accès à toute loi, ou tout contrat qui s'applique aux postes occupés.
Les documents dont dispose le personnel sont notamment les suivants :

- la PC supportée par la composante à laquelle il appartient ;
- la DPC propre au domaine de certification ;
- les procédures internes de fonctionnement ;
- les documents constructeurs des matériels et logiciels utilisés.

2.4 Procédures de constitution des données d'audit

La journalisation d'évènements consiste à les enregistrer sous forme manuelle ou sous forme électronique par saisie ou par génération automatique.
Les fichiers résultants, sous forme papier ou électronique, doivent rendre possible la traçabilité et l'imputabilité des opérations effectuées.

2.4.1 Type d'évènements à enregistrer

L'IGC journalise au minimum les évènements suivants, automatiquement dès le démarrage d'un système et sous forme électronique, concernant les systèmes liés aux fonctions qu'elle met en œuvre dans le cadre de l'IGC :

- création / modification / suppression de comptes utilisateur (droits d'accès) et des données d'authentification correspondantes (mots de passe, certificats, etc.) ;
- démarrage et arrêt des systèmes informatiques et des applications ;
- évènements liés à la journalisation : démarrage et arrêt de la fonction de journalisation, modification des paramètres de journalisation, actions prises suite à une défaillance de la fonction de journalisation ;
- connexion / déconnexion des utilisateurs ayant des rôles de confiance, et les tentatives non réussies correspondantes.

En plus de ces exigences de journalisation communes à toutes les composantes et toutes les fonctions de l'IGC, des évènements spécifiques aux différentes fonctions de l'IGC sont journalisés, notamment :

2.4.1.1 Evénements enregistrés par l'AE

Les évènements enregistrés par l'AE sont :

- réception d'une demande de certificat ;
- validation / rejet d'une demande de certificat ;
- réception d'une demande de révocation ;
- validation / rejet d'une demande de révocation ;
- sollicitation et accusés de réception de l'AC.

2.4.1.2 Evénements enregistrés par l'AC

Les évènements enregistrés par l'AE sont :

- événements liés aux certificats d'AC (génération (cérémonie des clés), sauvegarde / récupération, révocation, renouvellement, destruction,…) ;
- publication et mise à jour des informations liées à l'AC (PC, certificats d'AC, etc.) ;
- génération puis publication des CRL.

2.4.1.3 Description d'un évènement

Chaque enregistrement d'un évènement dans un journal contient au minimum les champs suivants :

- type de l'événement ;
- nom de l'exécutant ou référence du système déclenchant l'événement ;
- date et heure de l'événement ;
- résultat de l'événement (échec ou réussite).

2.4.1.4 Imputabilité

L'imputabilité d'une action revient à la personne, à l'organisme ou au système l'ayant exécutée. Le nom ou l'identifiant de l'exécutant figure explicitement dans l'un des champs du journal d'événements.
De plus, en fonction du type de l'évènement, chaque enregistrement contient également les champs suivants :

- destinataire de l'opération ;
- nom du demandeur de l'opération ou référence du système effectuant la demande ;
- nom des personnes présentes (s'il s'agit d'une opération nécessitant plusieurs personnes) ;
- cause de l'événement ;
- toute information caractérisant l'événement (par exemple, pour la génération d'un certificat, le numéro de série de ce certificat).

Les opérations de journalisation sont effectuées au cours du processus.
En cas de saisie manuelle, l'écriture se fait, sauf exception, le même jour ouvré que l'événement.

2.4.1.5 Evénements divers

D'autres évènements sont aussi recueillis, par des moyens électroniques ou manuels. Ce sont ceux concernant la sécurité et qui ne sont pas produits automatiquement par les systèmes informatiques, notamment :

- les accès physiques ;
- les actions de maintenance et de changements de la configuration des systèmes ;
- les changements apportés au personnel ;
- les actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, données d'activation, renseignements personnels sur les porteurs,…).

2.4.2 Fréquence de traitement des journaux d'évènements

Cf. chapitre …

2.4.3 Période de conservation des journaux d'évènements

Les journaux d'événements sont conservés sur site pendant au moins 1 mois.
Ils sont archivés au plus tard 1 mois après.

2.4.4 Protection des journaux d'événements

La journalisation est conçue et mise en œuvre de façon à limiter les risques de contournement, de modification ou de destruction des journaux d'évènements. Des mécanismes de contrôle d'intégrité permettent de détecter toute modification, volontaire ou accidentelle, de ces journaux.
Les journaux d'évènements sont protégés en disponibilité (contre la perte et la destruction partielle ou totale, volontaire ou non). Les journaux d'événements sont accessibles uniquement au personnel autorisé de l'AC.

2.4.5 Procédure de sauvegarde des journaux d'événements

Les procédures de sauvegarde des journaux sont quotidiennes et globale. Ces journaux sont ensuite archivés par l'AC.
Chaque entité opérant une composante de l'IGC met en place les mesures requises afin d'assurer l'intégrité et la disponibilité des journaux d'évènements pour la composante considérée, conformément aux exigences de la Politique de Sécurité du Groupe PIXID et en fonction des résultats de l'analyse de risque de l'AC.

2.4.6 Système de collecte des journaux d'événements

Un système automatique de collecte des journaux d'événements est mis en place. Ce système permet de garantir l'intégrité, la confidentialité et la disponibilité de ces journaux d'évènements.

2.4.7 Evaluation des vulnérabilités

Les journaux d'évènements sont contrôlés quotidiennement afin de pouvoir d'anticiper toute vulnérabilité.
Les journaux d'évènements sont contrôlés suivant la fréquence 1 fois par 24h, afin d'identifier des anomalies liées à des tentatives en échec.
Les journaux sont analysés dans leur totalité au moins à une fréquence 1 fois par semaine et dès la détection d'une anomalie. Cette analyse donnera lieu à un résumé dans lequel les éléments importants sont identifiés, analysés et expliqués. Le résumé fera apparaître les anomalies et les falsifications constatées.
Par ailleurs, un rapprochement entre les différents journaux d'évènements de fonctions qui interagissent entre elles (autorité d'enregistrement et fonction de génération, fonction de gestion des révocations et fonction d'information sur l'état des certificats, etc.) est effectué à une fréquence au moins égale à 1 fois par mois, ceci afin de vérifier la concordance entre évènements dépendants et contribuer ainsi à révéler toute anomalie.

2.5 Archivage des données

2.5.1 Type de données à archiver

L'AC procède en propre à l'archivage des données ci-dessous, et se réserve le droit de déléguer tout ou partie de ces obligations à un tiers avec lequel elle contractera sur la base de ces obligations.

Cet archivage permet d'assurer la pérennité des journaux constitués par les différentes composantes de l'IGC. Il permet également la conservation des pièces papier liées aux opérations de certification, ainsi que leur disponibilité en cas de nécessité.
Les données à archiver sont les suivantes :

- les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;
- les PC et DPC ;
- les accords contractuels avec d'autres AC ;
- les certificats et CRL tels qu'émis ou publiés ;
- les récépissés ou notifications (à titre informatif) ;
- les engagements signés des MC ;
- les justificatifs d'identité des porteurs et, le cas échéant, de leur entité de rattachement ;
- les journaux d'évènements des différentes entités de l'IGC.

2.5.2 Période de conservation des archives

2.5.2.1 Dossiers de demande de certificat

Les dossiers d'enregistrement (demandes de certificats d'AC subordonnée) sont archivés pendant 10 ans.

2.5.2.2 Certificats et CRL émis par l'AC

Les Certificats d'AC subordonnées, ainsi que les crl produites par l'AC PIXID ROOT CA sont archivés pendant une durée de dix ans à compter de la date de génération du certificat.

2.5.2.3 Journaux d'événements

Les journaux d'évènements sont archivés pendant dix ans après leur génération.
Les moyens mis en œuvre par l'AC pour leur archivage offrent le même niveau de sécurité que celui visé lors de leur constitution. En particulier, l'intégrité des enregistrements est assurée tout au long de leur cycle de vie.

2.5.3 Protection des archives

Pendant tout le temps de leur conservation, les archives, et leurs sauvegardes, sont :

- protégées en intégrité ;
- accessibles aux personnes autorisées ;
- lisibles et exploitables sur l'ensemble de leur cycle de vie ;

2.5.4 Exigences d'horodatage des données

Cf. chapitre 3.4.4 pour la datation des journaux d'événements

2.5.5 Procédures de récupération et de vérification des archives

Les archives (papier et électroniques) sont récupérées dans un délai inférieur à 2 jours ouvrés, sachant que seule l'AC peut accéder à toutes les archives (par opposition à une entité opérant une composante de l'IGC qui ne peut récupérer et consulter que les archives de la composante considérée).

2.6 Reprise suite à compromission et sinistre

2.6.1 Procédures de remontée et de traitement des incidents et des compromissions

Des procédures (sensibilisation, formation des personnels) et des moyens de remontée et de traitement des incidents (analyse des différents journaux d'événements) sont mises en œuvre.
Dans le cas d'un incident majeur, tel que la perte, la suspicion de compromission, la compromission, le vol de la clé privée de l'AC, l'évènement déclencheur est la constatation de cet incident au niveau de la composante concernée, qui doit en informer immédiatement l'AC. Le cas de l'incident majeur doit être impérativement traité dès détection et la publication de l'information de révocation du certificat, s'il y a lieu, doit être faite dans la plus grande urgence, voire immédiatement, par tout moyen utile et disponible (presse, site Internet, récépissé …).
L'AC prévient directement et sans délai le contact identifié sur le site : www.ssi.gouv.fr.

2.6.2 Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et/ou données)

L'équipe en charge de l'exploitation de l'AC dispose d'un plan de continuité dans lequel sont décrites les procédures de reprise.

2.6.3 Procédures de reprise en cas de compromission de la clé privée d'une composante

Les cas de compromission des éléments secrets des autres composantes sont traités dans le plan de continuité d'activité.

2.6.4 Capacités de continuité d'activité suite à un sinistre

Les différentes composantes de l'IGC disposent des moyens nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les exigences de cette PC.