Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE
Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil

Guide d'audit des PSC

Version 1.0 du 7 novembre 2003

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01 71 75 84 15 - Fax 01 71 75 84 00

Ce document a été réalisé par le bureau conseil de la DCSSI
(SGDN / DCSSI / SDO / BCS)

Les commentaires et suggestions sont encouragés et peuvent être adressés à l'adresse suivante :

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau Conseil
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP

conseil.dcssi@sgdn.pm.gouv.fr

Historique des modifications

Version	Date	Objet de la modification	Auteur(s)	Statut
0.1	27/03/03	Création du document	BCS	Draft
0.2	25/04/03	Rajout des fiches et prise en compte de modification	BCS	Draft
0.3	24/07/03	Mise à jour suite aux remarques du GT EGAP	BCS	Draft
0.4	31/07/03	Mise à jour suite aux remarques du GT EGAP	BCS	Draft
0.5	06/08/03	Mise à jour suite à commentaires DCSSI ajout des annexes	BCS	Draft
0.6	11/09/03	Mise à jour suite à réunion GT EGAP du 10/09/03	BCS	Draft
0.7	22/09/03	Mise à jour sommaire et références ETSI	BCS	Draft
0.8	4/11/03	Rajout en annexe des tableaux de couverture	BCS	Draft
1.0	7/11/03	Finalisation du document	BCS	Version finale

SOMMAIRE

INTRODUCTION

Ce document est le résultat des travaux menés au sein du groupe de travail Ad Hoc mandaté par la DIGITIP pour l'élaboration d'un guide d'audit et la rédaction d'exemples de Politiques de Certification de clés (PC) dans le cadre du schéma national de qualification des prestataires de services de certification électronique (PSC).
Cette grille d'audit couvre la gestion du cycle de vie des certificats qualifiés, délivrés par un PSC pour des personnes physiques intervenant pour leur propre compte ou pour des personnes physiques intervenant pour le compte de personnes morales ou physiques.

Objectif du document

Ce guide est destiné à être intégré au programme d'accréditation du COFRAC et doit servir de référence dans le cadre du schéma national de qualification des PSC, décrit dans l'arrêté du 31 mai 2002 modifié par l'arrêté relatif à la qualification des PSC.

Ce guide constitue l'outil méthodologique permettant à l'auditeur d'apporter une assurance raisonnable de conformité d'un PSC aux exigences de l'article 6 du décret 272-2001 [D2001-272]. Le référentiel de qualification applicable est basé sur le document AFNOR NF Z74-400 intitulé "Exigences concernant la politique mise en œuvre par les autorités de certification délivrant des certificats qualifiés" traduction en français de la spécification technique de l'ETSI TS n°101 456 (Policy requirements for certification authorities issuing qualified certificates) et complété par l'annexe de l'arrêté relatif à la qualification des PSC.

Ce document constitue également un recueil des exigences minimales du référentiel de sécurité du PSC.

Ce document ne présume pas de la structure fonctionnelle retenue par le PSC (autorités ou service du PSC), il propose un découpage en entités (Autorité de Certification (AC), Autorité d'Enregistrement (AE) et Service de Publication (SP)) et en rôles qui peuvent, selon les choix et besoins du PSC, être ou non confondus.

Il ne présume pas de l'architecture documentaire du PSC, mais s'appuie sur une architecture documentaire de type Politique de Certification de clé (PC), Déclaration des Pratiques de Certification (DPC) et procédures.

Plan du guide d'audit

La partie de ce document constituée des fiches d'audit est construit suivant le plan du document PC2 v2.2 (résultat de travaux menés au sein du groupe Ad Hoc Messagerie Sécurisée de la Sous-Commission Chiffre de la Commission Interministérielle de la Sécurité des Systèmes d'Information (CISSI) sur la base du RFC 2527) :

- MESURES CONSERVATOIRES
- IDENTIFICATION ET AUTHENTIFICATION
- BESOINS OPÉRATIONNELS
- CONTRÔLES DE SÉCURITÉ PHYSIQUE, CONTRÔLES DES PROCÉDURES, CONTRÔLES DU PERSONNEL
- CONTRÔLES TECHNIQUES DE SÉCURITÉ
- PROFILS DES CERTIFICATS ET CRL
- ADMINISTRATION DES SPÉCIFICATIONS

Exploitation du guide

Il est constitué de 124 fiches reprenant les chapitres précités. Dans chacune de ces fiches sont indiquées les références aux chapitres concernés de l'ETSI TS 101456 v1.2.1 ; ainsi que les références à PC2 v2.2 : intitulé du chapitre, du titre, du critère et le numéro du chapitre de PC2.

A titre indicatif, on décrit dans chacune des fiches les exigences minimales documentaires que le PSC doit posséder. Cette indication à deux objectifs : aider l'auditeur dans sa collecte de documentation préparatoire à l'audit et permettre au PSC d'établir son référentiel documentaire de sécurité.

On retrouve dans chacune des fiches un ensemble de questions ou de vérifications permettant de s'assurer que l'ensemble des exigences de l'article 6 du décret [D2001-272] et du référentiel de qualification est couvert.

Certains équipements du PSC ont déjà fait l'objet d'une évaluation-certification, dans ce cas le travail de l'auditeur consiste à vérifier que les politiques et procédures d'emplois de ces équipements sont formalisées, documentées, à jour, disponibles, connues et appliquées.

Les questions portant sur la vérification de procès verbaux (PV), ou sur la vérification des résultats de contrôle, ou encore d'audit ne sont applicables que dans la mesure ou le PSC a été ou est dans une phase d'exploitation (exemple : renouvellement de qualification).

Les réponses aux questions ou vérifications formulées dans les fiches doivent permettre de s'assurer de la conformité de l'audité. Elles seront exprimées comme suit : Conforme, Non Conforme ou Non Applicable.

Les conformités, non conformités ou non applicabilités aux questions doivent faire l'objet d'une justification qui peut être portée dans le bas de la fiche.

L'AUDIT

Identité de l'auditeur

L'organisme auditeur doit être accrédité par le COFRAC. Il procède aux vérifications décrites dans les fiches ci-après. L'organisme accrédité délivre la qualification à l'AC ou l'attestation de conformité à une entité du PSC.

Cet auditeur ne peut avoir partie liée avec l'AC ou l'entité candidate. Il intervient selon les principes établis dans l'arrêté du 31 mai 2002 modifié par l'arrêté relatif à la qualification des PSC.

Modalités de l'audit

L'audit porte sur l'ensemble des documents décrivant les engagements et exigences d'une AC, ainsi que les pratiques, procédures et moyens mis en œuvre pour gérer le cycle de vie des certificats qualifiés qu'elle délivre (PC, Déclaration des Pratiques de Certification (DPC), procédures, politique de sécurité, plan de secours, résultats de l'analyse de risque (en fonction du besoin d'en connaître)…). Cf. annexe " Documents à fournir pour l'audit".

Sujets couverts par l'audit

L'audit porte sur les points suivants :

- L'enregistrement
- La génération de certificat
- La délivrance de certificat
- La révocation
- La publication
- L'archivage

Réalisation de tests

Le contrôle des moyens et de la bonne application des procédures doit se faire par la réalisation de tests.

Dans la mesure du possible, ces tests sont réalisés sur la production ou si cela n'est pas possible, sur un site ou système représentatif de la production. Dans tous les cas, ces tests doivent permettre de valider les procédures et la bonne mise en œuvre des moyens.

L'auditeur peut éventuellement se faire délivrer un certificat (à durée de validité réduite) pour s'assurer du fonctionnement correct de toute la chaîne du certificat qualifié.

FICHES

Fiche n°: 1	**Chapitre : MESURES CONSERVATOIRES**
	Titre : Obligations générales
Origine : PC² 2.1	**Critère :** Obligations
ETSI : 7.4.2, 7.4.4, 7.4.5, 7.4.6, 7.4.7, 7.4.8, 7.4.10.c, 7.4.11. e, j, 7.5.b, c, d, e, g, j, k	

Exigences minimales pour le référentiel de sécurité du PSC :

Les obligations suivantes sont communes à toutes les entités du PSC :

- Préciser les mesures de protection des clés privées et publiques en intégrité et en confidentialité.
- Définir précisément les outils utilisables avec les clés privées et publiques, et leurs utilisations possibles. Mentionner les usages interdits.
- Définir les contrôles de conformité réalisés, leurs modalités et leur fréquence.
- Expliciter le système de Documentation d'Entreprise.

Points de contrôle :		**Réponses**
Q1	Les procédures sont-elles conformes aux déclarations d'intention de la PC ?	
Q2	Les procédures sont-elles effectivement appliquées ?	
Q3	La définition des usages interdits est-elle à jour et complète ?	
Q4	Existe-t-il un système de documentation d'entreprise ?	
Q5	La documentation est-elle complète ?	
Q6	La documentation est-elle appliquée et à jour ?	
Q7	La documentation est-elle disponible ?	
Q8	La documentation est-elle connue ?	
Q9	Les entités du PSC impliquées dans la gestion des opérations de génération et de révocation de certificat ont-elles une autonomie de décision vis à vis de toute autre organisation pour les décisions qui se rapportent à la mise en œuvre, à la préparation, à la continuation ou à l'interruption de ces services ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 2	**Chapitre : MESURES CONSERVATOIRES**
	Titre : Obligations
Origine : PC² 2.1	**Critère :** Obligations qui incombent à l'AC
ETSI : 7.1, a, note1, b, d, h, 7.3.1. note 5, 7.3.4, 7.4.1, a, b, c, e, f, 7.4.3, 7.4.9, 7.4.10.d, 7.5.a, f, h, i	

Exigences minimales pour le référentiel de sécurité du PSC :

Les obligations suivantes incombent à l'AC :

- garantir la définition et l'application de la politique de sécurité du PSC.
- contrôler et valider les pratiques de certification mises en œuvre par les différentes entités du PSC (AE et SP).
- Effectuer ce contrôle et cette validation avant la mise en œuvre du PSC et les renouveler périodiquement.

Points de contrôle :		**Réponses**
Q1	L'ensemble des obligations et des conditions d'usage des certificats sont-elles disponibles pour les utilisateurs (signataire et vérificateur) ?	
Q2	Les règles, directives et procédures régissant l'accès aux services du PSC, les assurances de sécurité mises en place ainsi que la politique concernant les incidents et les désastres existent-elles ?	
Q3	La rédaction des procédures respecte-t-elle la séparation organisationnelle et fonctionnelle définie dans la PC ?	
Q4	La PC et les procédures avec lesquelles l'AC opère ne doivent pas être discriminatoires.	
En cas d'externalisation de certaines des opérations délivrées par le PSC à un ou plusieurs organismes extérieurs (OPE,…) :		
Q5	La responsabilité de tous les aspects des services de certification électronique est-elle conservée par l'AC ?	
Q6	Les responsabilités des organismes sous-traitants ou tiers intervenant dans d'autres relations sont-elles clairement définies ?	
Q7	Existe-t-il un cadre contractuel clairement documenté avec ces organismes ?	
Q8	L'AC reste-t-elle seule responsable de la publication des DPC auprès des tiers en fonction du besoin d'en connaître ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 3	**Chapitre : MESURES CONSERVATOIRES**
	Titre : Obligations
Origine : PC² 2.1.1	**Critère :** Obligations qui incombent à l'AC
ETSI : 7.2.1.a, 7.2.2.a, 7.2.3.a, 7.2.6, 7.2.7, 7.2.8, 7.2.9, 7.3.3, 7.3.6	

Exigences minimales pour le référentiel de sécurité du PSC :

- Préciser les moyens, l'organisation et les procédures définis et mis en œuvre pour informer tous les signataires de la révocation du certificat d'une entité du PSC.
- Préciser les moyens et procédures mis en œuvre dans le cadre des schémas de certifications croisées avec d'autres AC ou PSC.
- Préciser les ressources cryptographiques utilisées; apporter le certificat de conformité aux exigences de l'arrêté modifié du 31 mai 2002, délivré par la DCSSI à la ressource cryptographique du PSC.
- En cas d'accord avec des AC étrangères, fournir la justification de l'acceptation de l'AC, ou au moins la référence de la demande si l'acceptation est implicite ou en cours.
- Les conclusions de l'analyse de risque qui ont permis de déterminer les objectifs de sécurité propres à couvrir les risques métiers de chacune de ces entités et à élaborer le référentiel de sécurité (PC, DPC et procédures).

Contrôles :		**Réponses**
Q1	L'AC met-elle en œuvre les pratiques de certification instanciant les exigences de la PC ?	
Q2	Le module cryptographique de l'AC a-t-il reçu un certificat de conformité aux exigences de l'annexe de l'arrêté relatif à la qualification des PSC ?	
Q3	L'AC garantit-elle la confidentialité et l'intégrité de ses clés privées ?	
Q4	Lorsque l'AC génère les clés privée et publique du signataire, le module cryptographique de l'AC concerné a-t-il reçu un certificat de conformité aux exigences de l'article 3.I du décret 2001-272 du 30 mars 2001, pour la fonction de génération des données de création et de vérification de signature électronique?	
Q5	Les procédures permettant de s'assurer que l'intégrité et l'authentification des clés publiques et de toutes les autres données associées sont préservées lors de leur distribution aux tiers utilisateurs, sont-elles formalisées, documentées et mises à jour ?	
Q6	Est-ce que les clés privées de l'AC ne sont plus utilisées pour signer des certificats et LCR après la fin de leur période de validité ?	
Q7	Les procédures permettant de s'assurer que les clés privées de l'AC ne peuvent être utilisées qu'à des fins de signature de certificats de signataire et de LCR sont-elles formalisées, documentées et mises à jour ?	
Q8	L'AC génère-t-elle et renouvelle-t-elle les certificats des signataires uniquement sous la responsabilité d'une AE qu'elle reconnaît ?	
Q9	L'organisation et les procédures définies pour informer les utilisateurs de la révocation d'un certificat d'une entité du PSC sont-elles formalisées, documentées et mises à jour ?	
Q10	Sur la base d'une demande de révocation validée et autorisée, les moyens et procédures permettent-ils de s'assurer qu'un certificat peut être révoqué sous 24	

	heures ?	
Q11	L'AC génère-t-elle l'ensemble des informations relatives aux obligations du vérificateur pour qu'il puisse faire raisonnablement confiance au certificat qualifié ?	
Q12	En cas d'évolution de la PC et de la DPC, l'AC avertit-elle les utilisateurs ?	
Q13	L'AC documente-t-elle les schémas de certification qu'elle entretient avec d'autres AC ?	
Q14	L'AC communique-t-elle sous une forme claire et compréhensible au souscripteur, avant d'entrer dans toutes relations contractuelles avec lui, les termes et conditions régissant l'AC ?	
Q15	La précision de l'horloge par rapport à laquelle les systèmes d'information du PSC se synchronisent, pour dater les événements journalisés ou archivés et pour la génération des certificats et CR, est-elle de plus ou moins une seconde par rapport au temps UTC ?	
Q16	S'assurer qu'au moins l'un des processus antérieur à la délivrance du certificat, dans la gestion du certificat par le PSC au profit d'un signataire, met en oeuvre un rapport facial entre le PSC et le signataire ou fait appel à un mandataire permettant de garantir le lien entre la personne physique et le certificat.	
Q17	S'assurer que l'AC conserve l'ensemble des informations nécessaires à la preuve en justice de la certification d'un signataire conformément au II)k de l'article 6 du décret 2001-272 du 30mars 2001 et conformément aux lois en vigueurs sur la collecte et la conservation d'informations.	
Q18	S'assurer que les objectifs de l'analyse de risque couvrent toutes les opérations de la gestion de certificat, la classification des informations, la protection physique des entités du PSC, la protection logique, la description des fiches de poste.	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°:.4	**Chapitre : MESURES CONSERVATOIRES** **Titre : Obligations générales**
Origine : PC² 2.1.2 **ETSI :** 7.3.1, k, 7.3.2, 7.4.10 b	**Critère** : Obligations qui incombent à l'AE

Exigences minimales pour le référentiel de sécurité du PSC :

- Fournir la (les) références de la (des) déclarations de traitements nominatifs effectués auprès de la CNIL et le cas échéant, l' (les) avis de la CNIL correspondants.
- Fournir en annexe de la DPC la copie de l'Accusé Réception de déclaration auprès de la CNIL.
- Fournir en annexe de la DPC éventuellement une copie de la déclaration.
- Fournir en annexe de la DPC un formulaire de demande de certification.

Contrôles :		**Réponses**
Q1	Existe-t-il une (des) Déclaration(s) auprès de la CNIL et sont-elles conformes ?	
Q2	Les données d'identification personnelles demandées lors de la demande de certificat sont-elles vérifiées en conformité avec la (les) Déclaration(s) déposée(s) ?	
Q3	L'AE publie-t-elle un formulaire de demande de certificat et de révocation ?	
Q4	L'AE informe-t-elle le signataire de manière complète et exacte des conditions d'emploi du certificat avant que le signataire rentre dans une relation contractuelle avec l'AC ?	
Q5	L'AE contrôle-t-elle l'identité du signataire auquel un certificat électronique est délivré, en exigeant de lui la présentation d'un document officiel d'identité ?	
Q6	L'AE contrôle-t-elle la qualité du signataire auquel un certificat électronique est délivré ?	
Q7	L'AE contrôle-t-elle que la demande de renouvellement de certificat est complète et exacte et que le demandeur est dûment autorisé à procéder à cette demande ?	
Q8	L'AE conserve-t-elle en confidentialité et en intégrité les données personnelles d'identification transmises lors de l'enregistrement ?	
Q9	L'AE protége-t-elle en confidentialité et en intégrité les données personnelles d'identification transmises lors de l'enregistrement ?	
Q10	L'AE journalise-t-elle les demandes de création, de modification, de révocation ?	
Q11	L'AE archive-t-elle les demandes de création, de modification, de révocation ?	
Q12	L'AE contrôle-t-elle l'accès physique à ses locaux ?	
Q13	L'AE limite-t-elle l'accès physique à ses locaux aux personnels autorisés ?	
Q14	En cas d'évolution l'AE avertit-elle l'AC de toute modification de ses procédures impactant la PC et la DPC ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 5	**Chapitre** : **MESURES CONSERVATOIRES**
	Titre : Obligations générales
Origine : PC² 2.1.5	**Critère :** Obligations du Service de Publication (SP)
ETSI : 7.3.1.b, 7.3.5	

Exigences minimales pour le référentiel de sécurité du PSC :

- Préciser la référence de la Politique de Sécurité Interne du SP et les références des procédures, garantissant l'intégrité et la disponibilité des listes publiées.
- Décrire les moyens de protection mis en œuvre garantissant l'intégrité et la disponibilité des listes publiées.
- Définir les rôles et responsabilités relatifs à la modification des listes publiées.
- Préciser les références des procédures d'attribution des droits d'accès et de modification des listes publiées.
- Préciser la référence au plan de secours, prévu pour le cas où certaines listes deviendraient indisponibles. Celui-ci doit traiter au cas par cas les listes publiées selon leurs caractéristiques.

Contrôles :		**Réponses**
Q1	L'intégrité et la disponibilité des listes publiées sont-elles prises en compte dans la Politique de Sécurité Interne et les procédures ?	
Q2	La procédure d'attribution des droits d'accès permet-elle d'assurer leur intégrité ?	
Q3	La procédure d'attribution des droits de modification des listes publiées assure-t-elle leur intégrité ?	
Q4	Procéder à un essai de modification des listes publiées pour s'assurer de leur protection en intégrité. La modification est-elle bien détectée ?	
Q5	Existe-t-il un plan de continuité de service permettant de réaliser les exigences de disponibilité décrites dans la PC ?	
Q6	Le SP fait-il authentifier les données qu'il doit publier ?	
Q7	L'accord du signataire est-il obtenu avant que le SP mette son certificat à la disposition des tiers utilisateurs ?	
Q8	Les moyens mis en place par le SP pour diffuser les certificats sont-ils d'une ampleur internationale ?	
Q9	En cas d'évolution le SP avertit-il l'AC de toute modification de ses procédures impactant la PC et la DPC ?	
Q10	Le SP publie-t-il l'ensemble des informations relatives aux obligations du vérificateur pour qu'il puisse faire raisonnablement confiance au certificat qualifié ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 6	**Chapitre** : **MESURES CONSERVATOIRES**
	Titre : Obligations générales
Origine : PC² 2.1.6	**Critère** : Obligations de l'AC envers les signataires ou mandataires
ETSI : 7.3.1.a, b bis 6.2	

Exigences minimales pour le référentiel de sécurité du PSC :

- Liste des informations qui sont fournies aux signataires.
- Les contrats types ou autres qui sont signés avec le signataire ou le mandataire.

Contrôles :		**Réponses**
Q1	Une information suffisante des utilisateurs est-elle prévue ?	
Q2	Les procédures et les moyens prévus pour l'information des utilisateurs sont-ils suffisants et adaptés ?	
Q3	Les procédures prévues pour l'information des utilisateurs sont-elles effectivement appliquées ?	
Q4	Les clauses du contrat qui lie les utilisateurs au PSC sont-elles formalisées, documentées et à jour ?	
Q5	Existe-t-il des clauses dans le contrat concernant l'obligation du signataire d'informer l'autorité chargée de la révocation, en cas de compromission ou de suspicion de compromission de sa clé privée ?	
Q6	Existe-t-il des clauses dans le contrat concernant l'obligation du signataire ou du mandataire d'informer l'autorité chargée de l'enregistrement, dès qu'il a connaissance d'un changement ou d'une inexactitude de l'une des informations contenues dans son certificat ?	
Q7	Existe-t-il des clauses dans le contrat concernant le respect des conditions d'utilisation des clés privées et publiques et des certificats par le signataire (utilisation du SSCD) ?	
Q8	Existe-t-il une procédure permettant aux signataires de connaître les cas pour lesquels ils doivent demander la révocation de leur certificat ?	
Q9	Les contrats types entre le PSC et un mandataire ou le PSC et un signataire ou le PSC et l'autorité responsable de l'application sont-ils formalisés, documentés et à jour ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°:.7	**Chapitre** : **MESURES CONSERVATOIRES**
	Titre : Responsabilités financières
Origine : PC² 2.3	**Critère :** Néant
ETSI : 7.5.f	

Exigences minimales pour le référentiel de sécurité du PSC :

- Lorsque cela s'applique, les conventions ou contrats liant les composantes, le PSC et les signataires

Contrôles :		**Réponses**
Q1	Les responsabilités financières entre composantes et entre le PSC et les signataires figurent-elles dans le contrat ou la convention ?	
Q2	La composante qui prend en charge des services délégués par une entité du PSC respecte-t-elle les exigences financières relatives aux PSC ?	
Q3	Les entités du PSC ont-elles une stabilité financière et les ressources nécessaires pour opérer conformément à sa PC ?	
Q4	Le PSC justifie-t-il d'une garantie financière suffisante, spécialement affectée au paiement des sommes qu'il pourrait devoir aux personnes s'étant fiées raisonnablement aux certificats qualifiés qu'il délivre, ou d'une assurance garantissant les conséquences pécuniaires de sa responsabilité civile professionnelle ? (LEN article 21)	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 8	**Chapitre** : **MESURES CONSERVATOIRES**
	Titre : Responsabilités financières
Origine : PC² 2.3.1	**Critère :** Indemnisation par le PSC
ETSI : 7.5.f	

Exigences minimales pour le référentiel de sécurité du PSC :

- L'indemnisation par le PSC doit être détaillée et apparaître dans la PC ou y être annexée ou être traitée dans les contrats avec les utilisateurs.

Contrôles :	**Réponses**
Q1 Les termes de l'indemnisation (des signataires et des souscripteurs) par le PSC figurent-ils dans le contrat ou la convention ? FACULTATIF	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 9	**Chapitre** : **MESURES CONSERVATOIRES**
	Titre : Responsabilités financières
Origine : PC² 2.3.2	**Critère :** Relations Financières
ETSI : 7.5.f	

Exigences minimales pour le référentiel de sécurité du PSC :

Il n'est pas souhaitable que le barème de prix détaillé apparaisse dans la DPC, pour des raisons de maintenance du document, mais les principes tarifaires pourront figurer dans la DPC ou dans un document annexe.

- Les relations financières entre l'AC et les organismes sous-traitant doivent être détaillées ou apparaître dans la convention / contrat annexé dans la DPC.
- Un document commercial détaillant les tarifs de génération ou de renouvellement de certificat doit être mis à la disposition utilisateurs.
- Un document commercial détaillant les tarifs de révocation ou d'accès aux informations concernant le statut d'un certificat doit être mis à la disposition des utilisateurs.
- Un document commercial détaillant les tarifs d'accès à un certificat doit être mis à la disposition des utilisateurs.
- Un document commercial détaillant les tarifs pour d'autres services doit être mis à la disposition des utilisateurs.

La politique de remboursement doit être détaillée ou apparaître dans la convention / contrat liant les différentes parties.

Contrôles :		**Réponses**
Q1	Les détails des relations financières entre l'AC et les organismes sous-traitant figurent-ils dans le contrat ou la convention ?	
Q2	Les documents commerciaux énoncés ci-avant sont-ils disponibles pour l'utilisateur et mis à jour ?	
Q3	La politique de remboursement est-elle précisée de manière détaillée et non ambiguë dans le contrat ou la convention liant les différentes parties ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°:.10	**Chapitre** : **MESURES CONSERVATOIRES**
	Titre : Responsabilités financières
Origine : PC² 2.3.3	**Critère :** Processus administratifs
ETSI : 7.5.f	

Exigences minimales pour le référentiel de sécurité du PSC :

- Les processus administratifs doivent être détaillés ou apparaître dans la convention / contrat annexé dans la DPC.

Contrôles :	**Réponses**
Q1 Les détails des procédures interne que le PSC met en œuvre dans ses relations financières figurent-ils dans le contrat ou la convention ? FACULTATIF	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 11	**Chapitre** : **MESURES CONSERVATOIRES**
	Titre : Interprétations de la loi
Origine : PC² 2.4.1	**Critère :** Lois
ETSI : 7.4.10.b	

Exigences minimales pour le référentiel de sécurité du PSC :

Contrôles :	**Réponses**
Q1 Vérifier que la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (Art. 323-1 à 323-3 du Code pénal) est mise en œuvre.	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 12	**Chapitre** : **MESURES CONSERVATOIRES**
	Titre : Interprétations de la loi
Origine : PC² 2.4.2	**Critère :** Résolution de litiges
ETSI : 7.5.h	

Exigences minimales pour le référentiel de sécurité du PSC :

- Indiquer de manière précise dans le contrat (figurant en annexe) la juridiction compétente pour la résolution de litiges.

Contrôles :		**Réponses**
Q1	La juridiction compétente est-elle identifiée dans le contrat ou la convention ?	
Q2	La juridiction compétente proposée est-elle acceptable (en particulier si elle est située dans un pays lié par des accords internationaux avec la France)?	
Q3	Le PSC a-t-il rédigé les procédures applicables aux réclamations et aux résolutions de litiges survenant avec ses clients ou tout autre tiers au sujet de ses prestations de service ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n° : 13	**Chapitre** : **MESURES CONSERVATOIRES**
	Titre : Publications et Services associés
Origine : PC² 2.6.1	**Critère** : Publication d'informations du PSC
ETSI : 7.3.1.a, b, note 2, i, 7.3.4.a, b	

Exigences minimales pour le référentiel de sécurité du PSC :

- La DPC doit décrire les moyens mis en œuvre pour respecter les engagements figurant dans la PC.
- Le(s) moyen(s) de publication des informations publiées concernant le PSC.
- Préciser les modalités d'accès aux informations publiées.
- Préciser les moyens et les références aux procédures mis en œuvre pour distribuer ou fournir à la demande des utilisateurs la liste des certificats et la CRL.

Contrôles :	**Réponses**
Q1 Chacune des informations décrites ci-dessous est-elle mise à disposition du signataire et des tiers utilisateurs : ✓ La PC en identifiant clairement l'usage associé. ✓ Les procédures de validation de certificat (contenant les exigences sur la vérification du statut du certificat). ✓ La limite de responsabilité du PSC. ✓ La période de temps d'archivage des données d'enregistrement et des accords. ✓ Le contenu des accords. ✓ La période de temps d'archivages des journaux. ✓ Les procédures de résolution des litiges. ✓ Les dispositions légales en vigueur. ✓ L'ensemble des obligations et des conditions d'usage des certificats des signataires. ✓ Le schéma de qualification utilisé et le résultat de conformité de la PC. ✓ Formulaires de demande de certificat. ✓ Formulaires de demande de révocation. ✓ Condensat des certificats des AC.	
Q2 Les moyens, l'organisation et les procédures définis et mis en œuvre pour distribuer ou fournir à la demande les informations ci-dessus permettent-ils de s'assurer de leur intégrité, lisibilité, compréhensibilité et clarté ?	
Q3 Existe-t-il une procédure de communication des informations confidentielles ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 14	**Chapitre** : **MESURES CONSERVATOIRES**
	Titre : Publications et Services associés
Origine : PC² 2.6.2	**Critère :** Fréquence de publication
ETSI : 7.3.5.e, f	

Exigences minimales pour le référentiel de sécurité du PSC :

- Préciser les délais de mise à jour selon les différentes modifications.
- Préciser les références des procédures de mise à jour des informations par le PSC.
- Préciser les rôles et responsabilités des personnes intervenant dans la mise à jour des publications.
- Détailler les contrôles permettant de s'assurer du respect des délais et des rôles lors de modification des spécifications.

Contrôles :		**Réponses**
Q1	Les moyens et les procédures mis en œuvre permettent-ils de garantir que les engagements de délai soient tenus ?	
Q2	Les moyens et les procédures spécifiés sont-elles effectivement mis en œuvre ?	
Q3	Vérifier par échantillonnage au cours des dernières périodes le respect des engagements de délai et des rôles dans les rapports de contrôles.	
Q4	Les délais de mise à jour des listes de certificats publiées respectent-ils le délai retenu par le PSC ?	
Q5	Y a-t-il un élément de mesure permettant de s'assurer que le pourcentage de disponibilité du SP est d'au moins de 99% ? (hors périodes de maintenances)	
Q6	Y a-t-il une planification des périodes de maintenance du SP ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 15	**Chapitre** : **MESURES CONSERVATOIRES**
	Titre : Publications et Services associés
Origine : PC² 2.6.3	**Critère :** Contrôle d'accès
ETSI : 7.4.6.j, k, l	

Exigences minimales pour le référentiel de sécurité du PSC :

- Les moyens permettant la mise en œuvre et l'application d'une politique de sécurité adaptée aux contrôles d'accès à ses publications doivent être détaillés.
- Cette politique de sécurité est issue de la PSSI du PSC.

Contrôles :		**Réponses**
Q1	Vérifier qu'il existe une politique de sécurité et qu'elle traite des aspects liés au contrôle d'accès aux différents systèmes, dont celui des publications ?	
Q2	Les moyens techniques de contrôle d'accès requis pour la mise en œuvre de la Politique de Sécurité sont-ils en place et sont-ils exploités selon les règles définies ?	
Q3	Les procédures de contrôle des droits d'accès sont-elles formalisées, documentées, mises à jour et conformes à la Politique de Sécurité ?	
Q4	Vérifier les procédures et moyens de contrôle d'accès	
Q5	Si possible (selon le système d'exploitation), réaliser un test de robustesse des mots de passe et contrôles d'accès.	
Q6	La modification des informations de révocation est-elle protégée par un contrôle d'accès et donne-t-elle lieu à l'émission d'une trace imputable ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 16	**Chapitre** : **MESURES CONSERVATOIRES**
	Titre : Publications et Services associés
Origine : PC² 2.6.4	**Critère :** Service de publication
ETSI : 7.3.5.a, b, c, d	

Exigences minimales pour le référentiel de sécurité du PSC :

- Préciser les moyens mis en œuvre pour la publication des certificats de l'AC ainsi que les modalités d'accès et les moyens requis.
- Préciser les références des procédures et les règles de mise à jour des listes de certificats et CRL.
- Préciser les moyens de transmission des certificats et des révocations au SP ainsi que les règles et les références des procédures de sécurité associées.
- Préciser les moyens de secours prévus pour garantir le respect des délais, y compris en cas de sinistre majeur.
- En cas de sous-traitance :
  - préciser l'identité et les caractéristiques du (des) sous-traitant(s) ;
  - préciser les références des procédures de maîtrise de la sécurité chez le(s) sous-traitants : cahier des charges, procédure d'audit et d'homologation,…
  - fournir le contrat-type et la partie sécurité du cahier des charges imposée aux sous-traitants.

Contrôles :	**Réponses**
Q1 Vérifier que les moyens et les procédures spécifiés par la DPC pour assurer le service de publication sont mis en œuvre de manière effective ?	
Q2 Les moyens de secours sont-ils prévus, sont-ils opérationnels et testés (se faire communiquer les comptes rendus des derniers tests) ?	
Q3 S'assurer qu'une analyse du risque a été conduite ; se faire communiquer les résultats ; vérifier qu'elle a conduit à la mise en place d'un plan d'action et que celui-ci a été effectivement mis en œuvre.	
Q4 En cas de sous-traitance, vérifier que les moyens spécifiés sont conformes aux spécifications et permettent de garantir que les engagements de la PC peuvent être remplis.	
Q5 Le(s) cahier(s) des charges des sous-traitants traduit(sen)t-ils de manière complète les engagements de sécurité du SP résultant de la PC ?	
Si nécessaire (en cas de doute fondé), procéder à une visite de contrôle du sous-traitant	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 17	**Chapitre** : **MESURES CONSERVATOIRES**
	Titre : Contrôles de conformité
Origine : PC² 2.7.1	**Critère :** Fréquence du contrôle de conformité
ETSI : 7.1.g	

Exigences minimales pour le référentiel de sécurité du PSC :

- L'avis favorable de l'AC ayant procédé au premier contrôle de conformité.
- Préciser la fréquence et les modalités des contrôles de conformité.
- Une copie de l'avis de l'autorité ayant procédé au dernier contrôle de conformité.

Contrôles :		**Réponses**
Q1	Existe-t-il un avis favorable initial de l'AC ?	
Q2	Contrôler la date des derniers contrôles de conformité afin de s'assurer de la régularité des contrôles.	
Q3	Vérifier l'avis correspondant au dernier contrôle effectué. Le cas échéant s'adresser au responsable en charge des relations avec l'AC afin de connaître les raisons ayant entraînées des irrégularités dans la fréquence des contrôles.	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 18	**Chapitre** : **MESURES CONSERVATOIRES**
	Titre : Contrôles de conformité
Origine : PC² 2.7.2	**Critère :** Identifications et qualifications du contrôleur
ETSI : 7.1.g	

Exigences minimales pour le référentiel de sécurité du PSC :

- Préciser les mesures d'encadrement prévues pour le contrôle.

Contrôles :	**Réponses**
Q1 Le contrôleur est-il clairement identifié ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 19	**Chapitre** : **MESURES CONSERVATOIRES**
	Titre : Contrôles de conformité
Origine : PC² 2.7.3	**Critère :** Sujets couverts par le contrôle de conformité interne
ETSI : 7.1.g	

Exigences minimales pour le référentiel de sécurité du PSC :

- Préciser la procédure utilisée pour le contrôle de conformité ainsi que les détails pratiques de son application

Contrôles :		**Réponses**
Q1	Se faire communiquer la procédure utilisée pour le contrôle de conformité (si elle n'est pas incluse dans la DPC), si elle est propre à un prestataire sous-traitant se la faire communiquer de lui sous accord de confidentialité.	
Q2	La procédure de contrôle est-elle formalisée ?	
Q3	La procédure de contrôle est-elle appliquée ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 20	**Chapitre** : **MESURES CONSERVATOIRES**
	Titre : Contrôles de conformité
Origine : PC² 2.7.4	**Critère :** Mesures à prendre en cas de non-conformité
ETSI : 7.1.g	

Exigences minimales pour le référentiel de sécurité du PSC :

- Préciser le format et le contenu de l'avis du contrôleur rendu à l'AC compétente ;
- Préciser les procédures mises en œuvre selon l'avis d'un contrôle de conformité ;
- Donner les références des procédures permettant de s'assurer du respect des conséquences logiques des contrôles de conformité.

Contrôles :	**Réponses**
Pour le contrôle de conformité interne :	
Q1 Les procédures à mettre en œuvre suite à un contrôle de conformité sont-elles formalisées, documentées et mises à jour ?	
Q2 Porter une appréciation sur la mise en œuvre des recommandations des derniers rapports internes de contrôles réalisés.	
Q3 Porter une appréciation sur la qualité des derniers rapports internes de contrôles réalisés.	
Pendant la qualification :	
Q4 Porter une appréciation sur la mise en œuvre des recommandations des derniers rapports de qualification du PSC.	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 21	**Chapitre** : **MESURES CONSERVATOIRES**
	Titre : Contrôles de conformité
Origine : PC² 2.7.5	**Critère :** Communication des résultats
ETSI : 7.1.g	

Exigences minimales pour le référentiel de sécurité du PSC :

- Préciser les entités, autres que la composante contrôlée, ayant le besoin d'en connaître, auxquelles les résultats des contrôles de conformité peuvent être communiqués ;
- Spécifier les références de procédures de diffusion de l'avis du contrôleur à l'AC compétente, à la composante contrôlée ainsi qu'aux autres entités mentionnées.

Contrôles :		**Réponses**
Q1	Vérifier la cohérence de la diffusion des résultats des contrôles de conformité suivant le besoin d'en connaître ?	
Q2	Se faire communiquer les procédures de diffusion de l'avis du contrôleur et en vérifier la conformité et le caractère applicable.	
Q3	Vérifier l'application rigoureuse des procédures de diffusion de l'avis du contrôleur lors des derniers contrôles de conformité.	
Q4	Les contrôles de conformité donnent-ils lieu à un plan d'actions correctif et les plans donnent-ils lieu à une réalisation effective et un suivi ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 22	**Chapitre** : **MESURES CONSERVATOIRES**
	Titre : Politique de Confidentialité
Origine : PC² 2.8.1	**Critère :** Informations considérées comme confidentielles
ETSI : 7.4.2.a, 7.4.5.c, e	

Exigences minimales pour le référentiel de sécurité du PSC :

- La politique de protection des informations confidentielles doit être spécifiée, au moins dans ses principes ; on peut renvoyer à un document séparé, mais ses références doivent être fournies ; la politique de protection des informations peut être jointe en annexe de la DPC.
- La politique de protection des informations confidentielles doit au moins couvrir les procédures de protection appliquées aux informations confidentielles.
- Les moyens mis en œuvre pour s'assurer de la bonne application de ces procédures doivent également être décrits.
- Les conditions de divulgation par le PSC aux autorités légales des données d'identification anonyme d'un utilisateur (dans le cas où un utilisateur prendrait un pseudonyme pour être identifié dans ses certificats) doivent être précisées.

Contrôles :		**Réponses**
Q1	La politique de protection des informations existe-t-elle et est-elle conforme à l'analyse de risque ?	
Q2	La politique de protection des informations couvre-t-elle toutes les exigences listées dans l'analyse de risque de l'AC ?	
Q3	La politique de protection des informations est-elle appliquée ?	
Q4	Les conditions de divulgation des données d'identification anonyme d'un utilisateur, par le PSC aux autorités légales sont-elles formalisées ?	
Q5	Vérifier l'application de la politique sur quelques cas récents, le cas échéant (par sondage).	
Q6	Si des extraits de la DPC sont diffusés est-ce fait en fonction du besoin d'en connaître ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 23	**Chapitre** : **MESURES CONSERVATOIRES**
	Titre : Politique de Confidentialité
Origine : PC² 2.8.2	**Critère** : Informations considérées comme non confidentielles
ETSI : 7.4.2.a, 7.4.5.c	

Exigences minimales pour le référentiel de sécurité du PSC :

- Préciser les moyens permettant d'accéder en interne et en externe aux informations publiques du PSC (système de gestion de la documentation de l'entreprise).
- Rappeler les règles de la Politique de Sécurité Interne définissant les niveaux de classification et les modes de gestion associés.

Contrôles :		**Réponses**
Q1	S'assurer de la cohérence des niveaux de protection associés aux documents.	
Q2	Le PSC possède-t-il un système de gestion de la documentation d'entreprise ?	
Q3	L'accès à ce système respecte-t-il les exigences de disponibilité requises ?	
Q4	Son accès est-il géré selon les principes du « besoin d'en connaître » ?	
Q5	Existe-t-il une procédure de protection des documents de l'entreprise ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 24	**Chapitre** : **MESURES CONSERVATOIRES**
	Titre : Politique de Confidentialité
Origine : PC² 2.8.3	**Critère :** Divulgation des causes de révocation et de suspension des certificats
ETSI :	

Exigences minimales pour le référentiel de sécurité du PSC :

- La référence de la procédure d'identification du (des) responsable(s) de la divulgation des causes de révocation et de suspension, et ce selon les différentes causes possibles
- Les références des procédures de divulgation des causes de révocation et de suspension à l'AC et aux personnes ayant le besoin d'en connaître.
- Les références des procédures et règles assurant la non divulgation des causes de révocation et de suspension aux personnes n'ayant pas le besoin d'en connaître.
- Préciser les rôles et responsabilités des personnes ayant en charge la divulgation des causes de révocation et de suspension de certificat.
- Les cas dans lesquels la cause de révocation doit rester confidentielle sont à définir.

Contrôles :	**Réponses**
Q1 Les rôles et responsabilités des personnes ayant en charge la divulgation sont-ils en adéquation avec leurs compétences et leur fonction ?	
Q2 La procédure de divulgation des causes de révocation et de suspension existe-t-elle ?	
Q3 La divulgation des causes de révocation et de suspension des certificats est-elle toujours effectuée suite à un accord du signataire ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 25	**Chapitre** : **MESURES CONSERVATOIRES**
	Titre : Politique de Confidentialité
Origine : PC² 2.8.4	**Critère :** Recouvrement des clés
ETSI : 7.4.10.d	

Exigences minimales pour le référentiel de sécurité du PSC :

- Les mesures mises en œuvre pour s'assurer que les clés de signature et de certification ne sont jamais recouvrées doivent être décrites.

Contrôles :	**Réponses**
Q1 Les procédures et les moyens visant à empêcher le recouvrement des clés de signature et de certification existent-ils ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 26	**Chapitre** : **MESURES CONSERVATOIRES**
	Titre : Politique de Confidentialité
Origine : PC² 2.8.5	**Critère** : Délivrance à la demande du propriétaire
ETSI : 7.4.10.d	

Exigences minimales pour le référentiel de sécurité du PSC :

- Les procédures de divulgation au propriétaire d'informations confidentielles le concernant.
- Les procédures permettant de s'assurer que le demandeur de divulgation d'informations confidentielles est bien authentifié.
- Apporter des garanties permettant de s'assurer de la délivrance d'informations confidentielles d'un signataire uniquement à son propriétaire.

Contrôles :		**Réponses**
Q1	Les procédures de divulgation aux propriétaires d'informations personnelles sont-elles formalisées, documentées et mises à jour ?	
Q2	Les procédures d'authentification du demandeur sont-elles formalisées, documentées et mises à jour ?	
Q3	Les procédures d'authentification du demandeur sont-elles appliquées ? Le cas échéant vérifier grâce aux journaux d'événements.	
Q4	La procédure utilisée dans le cadre de la délivrance d'informations confidentielles d'un signataire à son propriétaire est-elle formalisée, documentée et mise à jour ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 27	**Chapitre** : **MESURES CONSERVATOIRES**
	Titre : Politique de Confidentialité
Origine : PC² 2.8.6	**Critère :** Autres circonstances de délivrance possible
ETSI : 7.4.10.d	

Exigences minimales pour le référentiel de sécurité du PSC :

- Décrire les circonstances exceptionnelles autorisant à divulguer à un tiers les informations définies comme confidentielles et relatives à un signataire.
- Préciser les références des procédures et règles de communication de ces informations.
- Préciser le(s) tiers pouvant recevoir des informations définies comme confidentielles relatives à un signataire.

Contrôles :	**Réponses**
Q1 Existe t-il une procédure pour traiter les circonstances exceptionnelles autorisant à divulguer à un tiers les informations définies comme confidentielles et relatives à un signataire ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 28	**Chapitre** : **MESURES CONSERVATOIRES**
	Titre : Droits sur la Propriété Industrielle
Origine : PC² 2.9	**Critère :** Droits sur la propriété industrielle

Exigences minimales pour le référentiel de sécurité du PSC :

- Les mesures prises par l'entité du PSC pour garantir le respect de la propriété industrielle au bénéfice de tiers doivent être précisées.

Contrôles :	**Réponses**
Q1 L'entité du PSC a-t-elle mis en place des mesures pour garantir le respect en son sein des droits liés à la propriété industrielle ?	
Q2 Ces mesures sont-elles satisfaisantes et permettent-elles de satisfaire les obligations légales ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 29	**Chapitre : IDENTIFICATION ET AUTHENTIFICATION**
	Titre : Enregistrement initial du signataire
Origine : PC² 3.1.1	**Critère :** Conventions de Noms
ETSI : 7.3.3. a	

Exigences minimales pour le référentiel de sécurité du PSC :

- Apporter des éléments garantissant le respect des résultats des travaux interministériels relatifs au nommage notamment en ce qui concerne les conventions de noms (documentation, formation du personnel, etc..).
- Fournir en annexe les documents résultant des travaux interministériels relatifs au nommage.
- Indiquer les références des procédures permettant de satisfaire lors de l'enregistrement initial les travaux interministériels relatifs au nommage.

Contrôles :		**Réponses**
Q1	Les procédures du PSC relatives au nommage garantissent-elles le respect des travaux interministériels relatifs au nommage ?	
Q2	S'assurer par sondage que les procédures relatives au nommage sont bien appliquées.	
Q3	S'assurer par sondage que dans les certificats X509V3 l'emetteur (issuer) et le porteur (subject) sont identifiés par un "Distinguish Name" qui est unique.	
Q4	L'identifiant porté dans le certificat est-il construit à partir du nom du signataire ou d'un pseudonyme récupéré par l'AE ?	
Q5	Lorsqu'un pseudonyme est utilisé, est-il identifié comme tel ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 30	**Chapitre** : **IDENTIFICATION ET AUTHENTIFICATION**
	Titre : Enregistrement initial du signataire
Origine : PC² 3.1.2	**Critère :** Nécessité d'utilisation de noms explicites
ETSI : 7.3.3. a	

Exigences minimales pour le référentiel de sécurité du PSC :

- Apporter des éléments garantissant le respect des résultats des travaux interministériels relatifs au nommage notamment en ce qui concerne le caractère explicite des noms (documentation, formation du personnel, etc..) ;
- Indiquer les références des procédures permettant de satisfaire lors de l'enregistrement initial l'utilisation de noms explicites.

Contrôles :	**Réponses**
Q1 S'assurer par sondage que les procédures relatives au nommage sont bien appliquées en ce qui concerne le caractère explicite des noms.	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 31	**Chapitre** : **IDENTIFICATION ET AUTHENTIFICATION**
	Titre : Enregistrement initial du signataire
Origine : PC² 3.1.3	**Critère :** Règles d'interprétation des différentes formes de noms
ETSI : 7.3.3. a	

Exigences minimales pour le référentiel de sécurité du PSC :

- Apporter des éléments garantissant le respect des résultats des travaux interministériels relatifs au nommage et notamment en ce qui concerne les règles d'interprétation des différentes formes de noms (documentation, formation du personnel, etc..).
- Indiquer les références des procédures permettant de satisfaire lors de l'enregistrement initial les travaux interministériels relatifs au nommage en ce qui concerne les règles d'interprétation des différentes formes de noms.

Contrôles :	**Réponses**
Q1 Les procédures du PSC relatives au nommage garantissent-elles le respect des travaux interministériels relatifs au nommage en ce qui concerne les règles d'interprétation des différentes formes de noms ?	
Q2 S'assurer par sondage que les procédures relatives au nommage sont bien appliquées en ce qui concerne les règles d'interprétation des différentes formes de noms.	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 32	**Chapitre** : **IDENTIFICATION ET AUTHENTIFICATION**
	Titre : Enregistrement initial du signataire
Origine : PC² 3.1.4	**Critère :** Unicité des noms
ETSI : 7.3.3.d	

Exigences minimales pour le référentiel de sécurité du PSC :

- La DPC doit rappeler les règles d'unicité de nommage au sein d'un même domaine de certification.
- Les références des procédures relatives à l'enregistrement initial concernant les règles d'unicité de nommage doivent être précisées et les principes justifiés.

Contrôles :	**Réponses**
Q1 Les procédures relatives aux règles d'unicité du nommage garantissent-elles l'unicité d'un même nom au sein d'un même domaine ?	
Q2 L'unicité du DN porté dans le certificat d'un signataire est-il assuré dans le domaine de sécurité durant tout le temps de vie de l'AC ?	
Q3 Les procédures permettant de s'assurer qu'un DN contenu dans un certificat ne peut être attribué à un autre signataire, durant le cycle de vie d'une AC, sont-elles formalisées, documentées et mises à jour ?	
Q4 S'assurer par des vérifications aléatoires dans les données d'identifications que les procédures relatives aux règles d'unicité du nommage sont bien appliquées en ce qui concerne l'unicité d'un même nom au sein d'un même domaine.	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 33	**Chapitre** : **IDENTIFICATION ET AUTHENTIFICATION**
	Titre : Enregistrement initial du signataire
Origine : PC² 3.1.5	**Critère :** Procédures de résolution des litiges sur la revendication d'un nom
ETSI : 7.5.h	

Exigences minimales pour le référentiel de sécurité du PSC :

- La DPC doit reprendre les engagements figurant dans la PC.
- La réglementation en vigueur concernant la résolution des litiges sur la revendication d'un nom est à rappeler ou à inclure en annexe de la DPC.
- Les rôles et responsabilités des personnes en charge de la résolution des litiges sur la revendication d'un nom doivent être définis.
- Le contrat/convention, les clauses de résolution des litiges sur la revendication d'un nom.

Contrôles :		**Réponses**
Q1	Les procédures concernant la résolution des litiges sur la revendication d'un nom sont-elles formalisées, documentées, mises à jour et conformes à la réglementation et aux exigences de la PC ?	
Q2	Vérifier que les clauses requises figurent dans le contrat / convention.	
Q3	Procéder le cas échéant, par sondage, à une vérification sur des dossiers des litiges passés de la bonne application des règles et de la procédure.	
Q4	Les rôles et responsabilités des personnes en charge de la résolution des litiges sur la revendication d'un nom sont-ils définis ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 34	**Chapitre** : **IDENTIFICATION ET AUTHENTIFICATION**
	Titre : Enregistrement initial du signataire
Origine : PC² 3.1.7	**Critère :** Preuve de la possession d'une clé privée
ETSI : 7.3.1.j, note 11, k	

Exigences minimales pour le référentiel de sécurité du PSC :

- La DPC doit rappeler toutes les méthodes utilisables, sous couvert de la PC applicable, permettant de prouver que le signataire possède la clé privée correspondante à la clé publique contenue dans son certificat.
- Les références des méthodes de fourniture de preuve selon leur type (protocole, produit, etc..) ainsi que les procédures de mise en œuvre doivent être indiquées dans la DPC.

Contrôles :	**Réponses**
Q1 Les procédures et méthodes permettant de garantir que le signataire possède la clé privée correspondante à la clé publique contenue dans son certificat sont-elles formalisées, documentées et mises à jour ?	
Q2 La procédure permettant au PSC de s'assurer que le signataire (s'il génère lui même ses clés) utilise un dispositif sécurisé de création de signature électronique certifié conforme à l'article 3.1 du décret 2001-272 suivant la procédure SIG-P-01 est-elle formalisée, documentée et mise à jour?	
Q3 Si la paire de clés du signataire est générée par le PSC en dehors du dispositif sécurisé de création de signature du signataire, le module cryptographique utilisé par le PSC est-il certifié conforme à l'article 3.I du décret 2001-272 suivant la procédure SIG-P-01 pour la fonction de génération des données de création et de vérification de signature électronique ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 35	**Chapitre** : **IDENTIFICATION ET AUTHENTIFICATION**
	Titre : Enregistrement initial
Origine : PC² 3.1.8	**Critère :** Authentification de l'identité d'un organisme
ETSI : 7.3.1 note 1, c	

Exigences minimales pour le référentiel de sécurité du PSC :

- Fournir en annexe un formulaire de demande de certificat.
- Préciser les procédures administratives et les modes de transfert de l'information acceptées pour l'authentification de l'identité d'un organisme.
- Préciser ou fournir les références des procédures de contrôle du mandataire et de contrôle de l'authentification.

Contrôles :	**Réponses**
Q1 Les procédures administratives et les modes de transfert sont-ils formalisés, en place, à jour, complets et fiables ?	
Q2 Le cas échéant, les procédures de contrôle du mandataire et de contrôle de l'authentification sont-elles formalisées, documentées, et mises à jour et sont-elles appliquées ?	
Q3 Dans le cas d'utilisation d'un système d'information pour authentifier un organisme, la procédure offre-t-elle un niveau de garantie équivalent à une authentification par rapport facial ?	
Q4 Lorsque le demandeur est une personne physique (signataire) ayant une relation définie avec une personne morale identifiée dans le cadre des attributs du certificat, l'AE (en l'absence de mandataire) vérifie-t-elle les cinq éléments décrits ci -dessous : • Nom patronymique complet du demandeur. • Date et lieu de naissance du demandeur, conformément aux dispositions nationales. • Nom complet et statut légal de la personne morale concernée. • Numéro ou code d'identification de la personne morale concernée. • Document établissant le lien entre le demandeur et la personne morale concernée.	
Q5 Lorsque le demandeur est une personne physique (signataire) ayant une relation définie avec une personne morale identifiée dans le cadre des attributs du certificat, le mandataire (si il existe) vérifie-t-il les cinq éléments décrits ci -dessous : • Nom patronymique complet du demandeur. • Date et lieu de naissance du demandeur, conformément aux dispositions nationales. • Nom complet et statut légal de la personne morale concernée. • Numéro ou code d'identification de la personne morale concernée. • Document établissant le lien entre le demandeur et la personne morale concernée.	
Q6 Lorsque le demandeur est une personne physique (mandataire) représentant une personne morale, l'AE vérifie-t-elle les deux éléments décrits ci -dessous : • Nom complet et statut légal de la personne morale concernée. • Numéro ou code d'identification de la personne morale concernée. • Document établissant le lien entre la personne morale et le mandataire.	
Q7 Le demandeur donne-t-il une adresse physique ou tout autre moyen permettant de le	

contacter ?	
Justification des réponses négatives :	
Solutions envisagées ou proposées :	

Fiche n°: 36	**Chapitre** : **IDENTIFICATION ET AUTHENTIFICATION**
	Titre : Enregistrement initial
Origine : PC² 3.1.9	**Critère :** Authentification de l'identité d'un individu
ETSI : 7.3.1. notes 1 et 3, c.	

Exigences minimales pour le référentiel de sécurité du PSC :

- Fournir en annexe un formulaire de demande de certificat.
- Préciser les procédures administratives et les modes de transfert de l'information acceptés pour l'authentification de l'identité d'un individu.
- Décrire ou fournir les références des procédures de contrôle lors du rapport facial.

Contrôles :		**Réponses**
Q1	Les procédures administratives et les modes de transfert de l'information sont-ils formalisés, en place, à jour, intègres et fiables ?	
Q2	Est-ce que des procédures de contrôle de rapport facial ou apportant un degré d'assurance équivalent existent ?	
Q3	Dans le cas d'utilisation d'un système d'information pour authentifier un individu, la procédure offre-t-elle un niveau de garantie équivalent à une authentification par rapport facial ?	
Q4	La procédure de contrôle de l'identité du signataire, lorsque celui-ci est le demandeur: • Existe-t-elle ? • Est-elle documentée et à jour ?	
Q5	La procédure de vérification de l'identité du signataire, lorsque celui-ci n'est pas le demandeur : • Existe-t-elle ? • Est-elle documentée et à jour ?	
Q6	Pour s'assurer des informations figurant dans la demande de certificat, l'AE procède-t-elle à la vérification des éléments décrits ci -dessous : • Le nom patronymique complet du demandeur ? • La date et le lieu de naissance du demandeur ? • Une référence à un numéro d'identification nationale du demandeur ?	
Q7	La procédure permettant d'identifier un mandataire et de vérifier ses pouvoirs : • Existe-t-elle ? • Est-elle documentée et à jour ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 37	**Chapitre** : **IDENTIFICATION ET AUTHENTIFICATION**
	Titre : Re-génération de certificat en fin de validité
Origine : PC² 3.2	**Critère :** néant
ETSI : 7.3.2.a, c, d	

Exigences minimales pour le référentiel de sécurité du PSC :

- Spécifier ou citer la procédure de renouvellement de certificat utilisant la signature par la clé privée (dont le certificat correspondant arrivé au terme de sa validité).
- Spécifier ou citer la référence de la procédure permettant d'écourter la période de validité d'un certificat.

Contrôles :		**Réponses**
Q1	La procédure de demande de régénération de certificat en cas d'expiration est-elle formalisée ?	
Q2	La procédure d'authentification du signataire en cas de régénération du certificat en cas d'expiration est-elle formalisée, documentée et mise à jour ? (procédure identique à l'enregistrement initial)	
Q3	La procédure d'authentification du signataire en cas de demande de régénération électronique signée par sa clé privée arrivant en fin de validité est-elle formalisée, documentée et mise à jour ?	
Q4	Les procédures visées ci-dessus permettent-elles de garantir le respect des engagements décrits dans la PC (mesures conservatoires AE, AC et SP au minimum) et le niveau de sécurité requis ?	
Q6	Le cas échéant, procéder à des tests réels (aveugles).	
Q7	Si cela s'applique, vérifier que la période de validité d'un certificat est limitée par la date d'expiration de l'habilitation de son porteur.	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 38	**Chapitre** : **IDENTIFICATION ET AUTHENTIFICATION**
	Titre : Re-génération de clés de signature du signataire après révocation
Origine : PC² 3.3	**Critère :** néant
ETSI : 7.3.2.d	

Exigences minimales pour le référentiel de sécurité du PSC :

- Préciser les différents cas de révocation entraînant la re-génération de clé.
- Préciser les différents cas de révocation n'entraînant pas la re-génération de clé.
- Préciser les garanties qui permettent de s'assurer que la re-génération de clé est bien effectuée dans les cas le nécessitant.

Contrôles :		**Réponses**
Q1	Les procédures de re-génération de clés après révocation sont-elles formalisées, documentées, à jour et appliquées ?	
Q2	Les moyens mis en place permettant la re-génération de clés après révocation sont-ils adaptés et suffisants ?	
Q3	L'AE vérifie-t-elle que l'identité et les attributs du signataire à inclure dans le nouveau certificat sont toujours valides (procédure identique à l'enregistrement initial) ?	
Q4	L'AC vérifie-t-elle que la sécurité cryptographique est toujours acceptable dans le cadre de la politique de certification concernée pour toute la durée de validité du certificat ?	
Q5	L'AC vérifie-t-elle qu'il n'existe aucune indication suggérant que la clé privée du signataire a été compromise ?	
Q6	S'assurer éventuellement par sondage de l'application effective des règles et des procédures.	
Q7	Si cela s'applique, vérifier que la période de validité d'un certificat est limitée par la date d'expiration de l'habilitation de son porteur.	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 39	**Chapitre** : **IDENTIFICATION ET AUTHENTIFICATION**
	Titre : Authentification d'une demande de révocation
Origine : PC² 3.4	**Critère :** néant
ETSI : 7.3.6.a	

Exigences minimales pour le référentiel de sécurité du PSC :

- Les méthodes d'authentification d'une demande de révocation par l'AC.
- Les références des procédures et des moyens mis en œuvre permettant l'authentification d'une demande de révocation.
- La description des procédures et méthodes d'authentification d'un système d'information.

Contrôles :	**Réponses**
Q1 Les procédures d'authentification d'une demande de révocation sont-elles formalisées, documentées et mises à jour ?	
Q2 Permettent-elles au signataire, (en dehors des cas de compromission ou suspicion de compromission, perte, vol de clé privée), de s'authentifier : • en signant sa demande avec sa clé privée, • en se présentant en personne auprès de l'AE, • ou en utilisant la même procédure que lors d'un premier enregistrement auprès du PSC.	
Q3 S'assurer que les procédures d'authentification d'une demande de révocation sont fiables et permettent de garantir le respect des engagements de la PC.	
Q4 Vérifier par sondage l'application conforme de la procédure.	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n : 40	**Chapitre : BESOINS OPÉRATIONNELS**
	Titre : Demande de certificat qualifié
Origine : PC² 4.1	**Critère :** néant
ETSI : 7.3.1.a, b, d, e, f, k, 7.3.2.b, c	

Exigences minimales pour le référentiel de sécurité du PSC :

- Indiquer la liste des renseignements obligatoires et celle des renseignements facultatifs en fonction du type de certificat qualifiés (professionnel ou personnel). Ces renseignements doivent permettre de remplir le formulaire de demande de certificat.
- La procédure permettant de s'assurer de la preuve de l'autorisation d'associer des attributs ou des droits à un certificat.
- Pour les certificats qualifiés professionnel, indiquer les moyens autorisés permettant l'identification de l'autorité hiérarchique d'un demandeur de certificat (ex : formulaire type, etc..)

Contrôles :	**Réponses**
Q1 Les procédures permettent-elles une vérification suffisante de l'identité du demandeur et des informations fournies, en particulier le signataire lors de l'enregistrement fournit-il au moins les éléments suivants : ✓ Une pièce d'identité en cours de validité avec photo : carte nationale d'identité, un passeport, permis de conduire ou carte de séjour. ✓ Nom patronymique complet du signataire. ✓ Date et lieu de naissance du signataire, conformément aux dispositions nationales établies pour l'enregistrement des naissances. ✓ Lorsque cela s'applique, nom complet et statut légal de la personne morale concernée. ✓ Nom à utiliser dans le certificat ✓ Preuve de l'autorisation d'associer des attributs ou des droits à un certificat (si doivent être portés dans le certificat). ✓ Preuve du grade ou du poste occupé par le signataire (si cette information doit être portée dans le certificat). ✓ Adresse ou toutes autres informations, permettant de contacter le signataire.	
Q2 Dans le cas d'un organisme (Délivrance d'un certificat à une personne physique agissant pour le compte d'une personne morale) : ✓ Lorsque cela s'applique, le numéro ou code d'identification de la personne morale concernée. ✓ Lorsque cela s'applique, un document établissant le lien entre le signataire et la personne morale. ✓ Lorsque cela s'applique, l'identification de son autorité hiérarchique (au sein de son organisme), autorité qui aura le pouvoir par exemple de révoquer son certificat. ➢ Si l'organisme est une société anonyme ou une société de personnes et capitaux : ✓ Nom, raison sociale ✓ Adresse du siège social et numéro de téléphone ✓ Numéro SIRET ✓ Extrait du registre du commerce où la société est enregistrée ✓ Composition et répartition du capital de la société	

- Si l'organisme est une société de personnes :
  - ✓ Nom, dénomination
  - ✓ Adresse et numéro de téléphone
  - ✓ Numéro SIRET
  - ✓ Extrait du registre du commerce où la société est enregistrée
  - ✓ Fiche individuelle d'état civil et de nationalité de chaque associé
  - ✓ Composition et répartition des parts sociales de la société
- Si l'organisme est une entreprise individuelle :
  - ✓ Nom, dénomination
  - ✓ Fiche individuelle d'état civil et de nationalité de l'entrepreneur
  - ✓ Adresse et numéro de téléphone
  - ✓ Numéro SIRET
  - ✓ Extrait du registre du commerce où l'entreprise est enregistrée
- Si l'organisme est une entité administrative :
  - ✓ Nom
  - ✓ Numéro SIRET
  - ✓ Adresse
  - ✓ Numéro de téléphone
  - ✓ Référence des textes portant création de l'organisme.

Q3 Les procédures permettent-elles de vérifier l'accord de l'autorité hiérarchique ?

Q4 Les procédures permettent-elles de vérifier la qualité dont la personne physique se prévaut dans la demande de certificat ?

Q5 Vérifier par sondage que les procédures sont appliquées et laissent des traces fiables.

Q6 Le formulaire de demande de certification et les informations demandées sont-ils cohérents, suffisants et nécessaires ?

Q7 Est-ce que les formulaires, les demandes de certification et les informations demandées sont cohérentes, suffisantes et nécessaires conformément aux indications de la DPC ?

Q8 Le formulaire de demande de certificat prend-il en compte les choix suivants :

- ✓ Publication de son certificat par le SP ;
- ✓ Publications des causes de révocation ;
- ✓ Usage des clés (signature ou non-répudiation) ;
- ✓ Transfert de ses données archivées par le PSC en cas de fin de vie de ce dernier.

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 41	**Chapitre** : **BESOINS OPÉRATIONNELS**
	Titre : Génération de certificat qualifié
Origine : PC² 4.2	**Critère :** néant
ETSI : 7.3.3.b, c, e, f	

Exigences minimales pour le référentiel de sécurité du PSC :

- Les procédures pour les échanges entre l'AC, l'AE, le SP et le signataire.
- Les spécifications des moyens d'échange utilisés entre l'AC, l'AE, le SP et le signataire.
- Les procédures d'authentification entre l'AC, l'AE, le SP et le signataire.
- Les spécifications des moyens d'authentification entre l'AC, l'AE, le SP et le signataire.

Contrôles :		**Réponses**
Q1	Les procédures pour les échanges entre l'AC, l'AE, le SP et le signataire sont-elles formalisées, documentées et mises à jour ?	
Q2	Les procédures d'authentification entre l'AC, l'AE, le SP et le signataire sont-elles formalisées, documentées et mises à jour ?	
Q3	Sont-elles connues et appliquées ?	
Q4	Les communications entre les différentes entités du PSC sont-elles protégées en confidentialité et en intégrité ?	
Q5	Si l'AC génère les clés de signature du signataire, alors le processus de génération de certificat est-il lié de manière sécurisée au processus de génération de clé ?	
Q6	Les moyens mis en œuvre permettent–ils de s'assurer que l'ensemble des procédures de génération, de renouvellement de certificat, d'enregistrement et de génération des clé privée et clé publique sont liées de sorte à garantir l'intégrité du lien entre le contenu du certificat, le signataire et sa clé privée correspondante au certificat ?	
Q7	Ces moyens doivent être testés.	
Q8	L'AC met-elle en œuvre ses ressources cryptographiques de signature de certificat dans des locaux sécurisés ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 42	**Chapitre** : **BESOINS OPÉRATIONNELS**
	Titre : Acceptation d'un certificat qualifié par le signataire
Origine : PC² 4.3	**Critère :** néant
ETSI : 7.3.1. note 8, note 9, note 10, h	

Exigences minimales pour le référentiel de sécurité du PSC :

- Les procédures et les moyens :
  - d'authentification du signataire par l'AC et inversement, lors de l'acceptation du certificat
  - d'utilisation du récépissé et de délivrance du certificat.
- Si un autre procédé approuvé par l'AC est mis en place pour confirmer l'acceptation du signataire, celui-ci doit alors être décrit.

Contrôles :		**Réponses**
Q1	Ces procédures sont-elles formalisées, documentées et mises à jour ?	
Q2	Sont-elles connues et appliquées ?	
Q3	A la réception de son certificat le signataire notifie-t-il à l'AC qu'il accepte son certificat en signant un accord (papier ou électronique) contenant son consentement sur le contenu du certificat ?	
Q4	La procédure permettant de s'assurer de l'acceptation du certificat existe-elle ?	
Q5	La procédure permettant de gérer le refus du certificat par le signataire existe-elle ?	
Q6	Procéder à des tests des moyens utilisés lors de l'acceptation du certificat.	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 43	**Chapitre** : **BESOINS OPÉRATIONNELS**
	Titre : Suspension et révocation de certificat qualifié de signataire
Origine : PC² 4.4.1	**Critère :** Causes possibles de révocation de certificat de signataire
ETSI : 7.3.6.a	

Exigences minimales pour le référentiel de sécurité du PSC :

- La liste minimale des cas dans lesquels il est considéré qu'il y a compromission ou suspicion de compromission de clé privée d'un utilisateur, doit être précisée par le PSC et être communiquée à ses signataires.
- La PC doit préciser :
  - Les références des procédures et moyens utilisés par une AC pour informer les signataires de la révocation de leur certificat.
  - Quelles sont les modifications d'attribut qui entraînent automatiquement la révocation du certificat.
  - Quelles sont les clauses du contrat qui lorsqu'elles ne sont plus respectées entraînent la révocation automatique du certificat.
  - Les cas particuliers entraînant la révocation du certificat.

Contrôles :	**Réponses**
Q1 Les procédures sont-elles formalisées, documentées et mises à jour ?	
Q2 Sont-elles connues et appliquées ?	
Q4 Les cas particuliers de révocation cités dans la PC sont-ils cohérents avec les possibilités de révocation prévues : Les causes de révocations pour un signataire sont les suivantes : • Changement d'informations contenues dans le certificat. • Compromission, suspicion de compromission, vol ou perte de la clé privée. • Compromission, suspicion de compromission, vol ou perte du certificat du signataire. • Cessation du liant entre le porteur et l'identité morale le supportant. • Décès du porteur ou cessation d'activité de l'organisme porteur du certificat. • Non-respect du contrat ou de la convention liant un signataire au PSC. • Révocation du certificat de l'AC émettrice du certificat. Les causes de révocations pour une AC sont les suivantes : • Décision suite à un contrôle de conformité. • Non-respect de la politique de certification et de la déclaration des pratiques de certification par l'AC. • Cessation d'activité de l'AC. • Compromission, suspicion de compromission, vol, perte de certificat de l'AC. • Compromission, suspicion de compromission, vol, perte de la clé privée d'une AC. • Compromission de clé publique d'une AC.	
Q5 La procédure permettant aux signataires de connaître les cas pour lesquels ils doivent demander la révocation de leur certificat est-elle formalisée, documentée et à jour ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 44	**Chapitre** : **BESOINS OPÉRATIONNELS**
	Titre : Suspension et révocation de certificat qualifié de signataire
Origine : PC² 4.4.2	**Critère :** Qui peut demander une révocation ?
ETSI : 7.3.6 a	

Exigences minimales pour le référentiel de sécurité du PSC :

- Si un autre organisme ou une autre personne peut demander la révocation du Certificat dans certains cas particuliers, cela sera précisé dans PC.
- Les modalités précises de ces révocations seront détaillées.

Contrôles :	**Réponses**
Q1 S'assurer de la mise à jour et de la justification de la liste des organismes ou personnes pouvant demander une révocation dans des cas bien définis.	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 45	**Chapitre** : **BESOINS OPÉRATIONNELS**
	Titre : Suspension et révocation de certificat qualifié de signataire
Origine : PC² 4.4.3	**Critère :** Procédure de demande de révocation
ETSI : 7.3.6.a, note 1, b, c, d, e, f, j	

Exigences minimales pour le référentiel de sécurité du PSC :

- Quand l'AC met en œuvre la révocation par un tiers, alors la procédure en tiendra compte et donnera les précisions nécessaires et suffisantes.
- Les références des procédures et les moyens d'échange et d'authentification entre l'AC, l'AE, le signataire et le demandeur de la révocation doivent être indiqués.
- La référence de la procédure de révocation incluant une authentification a posteriori doit être citée. Son approbation par l'AC doit être garantie.

Contrôles :		**Réponses**
Q1	Y-a-t-il cohérence entre les moyens et les procédures d'échange et d'authentification; les procédures sont-elles effectivement appliquées ?	
Q2	Y-a-t-il une procédure précise de révocation quand celle-ci n'est pas effectuée par l'AC ?	
Q3	Y-a-t-il une procédure de révocation incluant une authentification à posteriori ainsi que son approbation formelle par l'AC ?	
Q4	S'assurer, par sondage parmi des cas de révocations récents, de la restitution de la ressource cryptographique, lorsque cela s'applique.	
Q5	La procédure de révocation prévoit-elle d'identifier le tiers déposant la demande de révocation ?	
Q6	La procédure de révocation définit-elle les personnes habilitées à déposer une demande de révocation ?	
Q7	Le signataire dont le certificat est révoqué est-il informé du nouveau statut de son certificat par le PSC ?	
Q8	S'assurer qu'une fois que le certificat est révoqué, il n'est pas réutilisé comme un certificat valide (publication dans l'annuaire, redistribution comme certificat valide…).	
Q9	Contrôler la mise en œuvre pratique des modalités de révocation et apprécier leur qualité.	
Q10	Examiner les justificatifs et les traces de cas récents de révocation et vérifier l'application conforme des procédures.	
Q11	Y-a-t-il une procédure de confirmation des demandes de révocation ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 46	**Chapitre** : **BESOINS OPÉRATIONNELS**
	Titre : Suspension et révocation de certificat qualifié de signataire
Origine : PC² 4.4.4	**Critère :** Temps de traitement d'une révocation
ETSI : 7.3.6.b, h	

Exigences minimales pour le référentiel de sécurité du PSC :

- Les garanties permettant de s'assurer du traitement des demandes de révocation dans les temps impartis doivent être détaillées.
- Donner les références des procédures de contrôle du respect des temps impartis pour la révocation. Celles-ci doivent comporter des mesures correctives en cas de non-respect de ces temps.

Contrôles :		**Réponses**
Q1	Effectuer des contrôles sur les archives afin de vérifier que le délai maximum de demande de révocation est respecté. Est-il inférieur à 1 jour ?	
Q2	S'assurer par des contrôles aléatoires que les procédures sont bien appliquées.	
Q3	Y-a-t-il un élément de mesure permettant de s'assurer que le pourcentage de disponibilité est d'au moins 99% ? (hors périodes de maintenances)	
Q4	Existe-t-il une procédure définissant les mesures nécessaires au rétablissement du service de révocation dans un temps d'indisponibilité inférieur à celui défini dans la DPC, dans le cas d'une défaillance matérielle ou autre ? (La durée d'indisponibilité ne devra pas dépasser les 24h)	
Q5	Vérifier l'existence et l'application des procédures de contrôle du respect des temps impartis pour la révocation. S'assurer de l'application des mesures correctives, le cas échéant.	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 47	**Chapitre** : **BESOINS OPÉRATIONNELS**
	Titre : Suspension et révocation de certificat qualifié de signataire
Origine : PC² 4.4.5	**Critère :** Causes possibles de suspension
ETSI : 7.3.6.a	

Exigences minimales pour le référentiel de sécurité du PSC :

- Les cas particuliers de suspension de certificat non prévus dans la PC
- Le délai maximal autorisé de cessation d'activité pendant lequel le certificat est suspendu.

Contrôles :	**Réponses**
Q1 Les cas particuliers de suspension cités dans la DPC sont-ils cohérents avec les possibilités de suspension prévues ?	
Q2 Le délai maximal de suspension du certificat est-il suffisant (au plus égal à 1 jour) et cohérent avec les moyens mis en œuvre?	
Non obligatoire	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 48	**Chapitre** : **BESOINS OPÉRATIONNELS**
	Titre : Suspension et révocation de certificat qualifié de signataire
Origine : PC² 4.4.6 **ETSI :** 7.3.6	**Critère :** Qui peut demander une suspension ?

Exigences minimales pour le référentiel de sécurité du PSC :

- Si, dans certains cas particuliers, un autre organisme ou une autre personne peut demander la suspension du certificat, cela sera précisé dans la PC.
- Les modalités précises de ces suspensions seront détaillées.

Contrôles :	**Réponses**
Q1 S'assurer de la mise à jour et de la justification de la liste des organismes ou personnes pouvant demander une suspension. **Q2** La procédure de suspension est-elle formalisée, documentée et à jour ? **Q3** Examiner les justificatifs et les traces de cas récents de suspension et vérifier l'application conforme des procédures. Non obligatoire	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 49	**Chapitre** : **BESOINS OPÉRATIONNELS**
	Titre : Suspension et révocation de certificat qualifié de signataire
Origine : PC² 4.4.7	**Critère :** Procédures de demande de suspension
ETSI : 7.3.6	

Exigences minimales pour le référentiel de sécurité du PSC :

- Les procédures et les moyens d'échange et d'authentification entre l'AC, l'AE, le SP, le demandeur de suspension, et le propriétaire du certificat doivent être indiqués.
- La procédure de suspension incluant une authentification à posteriori doit être précisée.
- Si la suspension n'est pas effectuée par l'AC, alors cette procédure doit être redéfinie.

Contrôles :	**Réponses**
Q1 Le formulaire de demande de suspension existe-il, est-il formalisé, documenté et mis à jour ?	
Q2 S'assurer de la cohérence entre les moyens et les procédures d'échange et d'authentification; s'assurer de l'application effective des procédures au travers de l'examen de cas récents (justificatifs et traces).	
Q3 Existe-t-il une procédure formalisée, documentée et à jour de suspension quand celle-ci n'est pas effectuée par l'AC ?	
Q4 Existe-t-il une procédure de suspension incluant une authentification, éventuellement à posteriori, ainsi que son approbation formelle par l'AC ?	
Non obligatoire	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 50	**Chapitre** : **BESOINS OPÉRATIONNELS**
	Titre : Suspension et révocation de certificat qualifié de signataire
Origine : PC² 4.4.8	**Critère :** Limites d'une période de suspension
ETSI : 7.3.6.d	

Exigences minimales pour le référentiel de sécurité du PSC :

- La DPC doit détailler les procédures et moyens de vérification permettant de s'assurer que la procédure de suspension ne s'étend pas au-delà de 24h.

Contrôles :	**Réponses**
Q1 Effectuer des contrôles sur des certificats suspendus afin de vérifier que la suspension ne s'étend pas au-delà de 24 h.	
Q2 Les procédures comportent-elles des mesures correctives applicables en cas d'erreur de période de suspension ?	
Q3 Effectuer des contrôles aléatoires afin de s'assurer que les procédures sont correctement appliquées.	
Non obligatoire	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 51	**Chapitre** : **BESOINS OPÉRATIONNELS**
	Titre : Suspension et révocation de certificat qualifié de signataire
Origine : PC² 4.4.9	**Critère :** Fréquence de mise à jour de la CRL
ETSI : 7.3.6.g, i	

Exigences minimales pour le référentiel de sécurité du PSC :

- Préciser à nouveau le délai de mise à jour des CRL.
- Rappeler les garanties apportées par le SP quant au respect de la fréquence d'émission de nouvelles CRL.

Contrôles :	**Réponses**
Q1 Les moyens mis en œuvre permettent-ils d'obtenir une mise à jour en moins de 24h des CRL ?	
Q2 Contrôler l'adéquation entre les dates limites annoncées d'émission de la prochaine CRL et leur publication réelle.	
Q3 Ces listes contiennent-elles la date et l'heure aux quelles la CRL sera au plus tard mise à jour ?	
Q4 Quand elles sont utilisées, les CRL doivent : ✓ Contenir la date limite de la prochaine CRL. ✓ Etre signées par l'AC ou par une autorité désignée par l'AC.	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 52	**Chapitre** : **BESOINS OPÉRATIONNELS**
	Titre : Suspension et révocation de certificat qualifié de signataire
Origine : PC² 4.4.10	**Critère :** Exigences de contrôle des CRL
ETSI : 7.3.6, 7.3.4 a	

Exigences minimales pour le référentiel de sécurité du PSC :

- La (les) procédure(s) à respecter par le vérificateur pour s'assurer du statut du certificat dans la CRL.
- Les moyens mis en œuvre pour informer le vérificateur de l'intérêt de la vérification du statut du certificat dans la CRL et de la validité de la CRL.

Contrôles :	**Réponses**
Q1 Ces procédures à respecter par le vérificateur sont-elles formalisées, appliquées et mises à jour ?	
Q2 L'AC informe-t-elle le demandeur et le signataire du changement de statut du certificat?	
Q3 La DPC définit-elle la durée maximale d'indisponibilité du service de révocation ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 53	**Chapitre** : **BESOINS OPÉRATIONNELS**
	Titre : Suspension et révocation de certificat qualifié de signataire
Origine : PC² 4.4.11	**Critère :** Publication des causes de révocation et de suspension
ETSI :	

Exigences minimales pour le référentiel de sécurité du PSC :

- Le choix de la publication des causes de révocation et de suspension, par l'AC doit être précisé.
- L'approbation de ces mesures par l'AC doit être incluse dans la DPC.

Contrôles :	**Réponses**
Q1 La publication des causes de révocation des certificats est-elle effectuée suite à un accord du signataire ?	
Q2 La publication des causes de suspension des certificats est-elle effectuée suite à un accord du signataire ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 54	**Chapitre** : **BESOINS OPÉRATIONNELS**
	Titre : Suspension et révocation de certificat qualifié de signataire
Origine : PC² 4.4.12	**Critère :** Contrôle en ligne des CRL
ETSI : 7.3.6.h, note 3, k	

Exigences minimales pour le référentiel de sécurité du PSC :

- Les procédures et les moyens de protection garantissant l'origine et la disponibilité des accès pour la vérification en ligne des CRL.

Contrôles :	**Réponses**
Q1 Les dispositifs offerts aux entités consultant les CRL, leur permettent-ils de contrôler l'intégrité des CRL publiées en ligne ?	
Q2 Les procédures et moyens de protection permettent-ils de garantir l'origine et la disponibilité des accès des contrôles en ligne ?	
Q3 Les procédures sont-elles formalisées, documentées et mises à jour ?	
Q4 L'information consistant à savoir si un certificat a un statut révoqué ou non est-elle : ✓ disponible au moins 99% du temps ? (hors périodes de maintenances) ✓ public ? ✓ et disponible de façon internationale ?	
Q5 Existe-t-il une procédure formalisée, documentée et mise à jour définissant les mesures nécessaires au rétablissement du service de révocation dans un temps d'indisponibilité inférieur à 24h, dans le cas d'une défaillance matérielle ou autre ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 55	**Chapitre** : **BESOINS OPÉRATIONNELS**
	Titre : Suspension et révocation de certificat qualifié de signataire
Origine : PC² 4.4.13	**Critère :** Autres formes de publication des certificats révoqués
ETSI : 7.3.6 note 3	

Exigences minimales pour le référentiel de sécurité du PSC :

- Le fonctionnement et les moyens mis en œuvre dans les cas d'utilisation d'autres formes de publication des certificats révoqués doivent être précisées.
- Les procédures et moyens de protection de l'intégrité et de la disponibilité des contenus en ligne doivent être indiqués.
- Rappeler les garanties apportées par le SP quant au respect de la fréquence de mise à jour des autres formes de publication des certificats révoqués.

Contrôles :		**Réponses**
Q1	Contrôler l'efficacité des méthodes assurant l'origine et la disponibilité des autres formes de publication des certificats révoqués.	
Q2	Vérifier la cohérence et la mise à jour des procédures de protection de l'intégrité et de la disponibilité des autres formes de publication.	
Q3	Vérifier les dates de publication des autres formes de publication des certificats révoqués et s'assurer du respect de la fréquence de mise à jour.	
Q4	Contrôler l'adéquation entre les dates annoncées d'émission de la prochaine publication des certificats révoqués et celles de sa publication réelle.	
Q5	L'information de révocation est-elle protégée en intégrité et authentifiée ?	
Q6	Le statut d'un certificat est-il authentifiable et protégé en intégrité ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 56	**Chapitre** : **BESOINS OPÉRATIONNELS**
	Titre : Suspension et révocation de certificat qualifié de signataire
Origine : PC² 4.4.14	**Critère :** Contrôle en ligne des autres formes de publication des certificats révoqués
ETSI : 7.3.6, 7.3.6.i note 3	

Exigences minimales pour le référentiel de sécurité du PSC :

- La DPC doit préciser les moyens offerts aux entités consultant les listes de certificats révoqués, leur permettant de contrôler leur intégrité.
- Les références des procédures et les moyens de protection de l'intégrité et de la disponibilité des contrôles en ligne doivent être précisés.

Contrôles :		**Réponses**
Q1	Contrôler l'efficacité et la sécurité des dispositifs assurant le contrôle d'intégrité des autres formes de publication des certificats révoqués.	
Q2	Contrôler l'efficacité et la sécurité de la protection de l'intégrité et de la disponibilité des contrôles en ligne.	
Q3	Les procédures sont-elles formalisées, documentées et mises à jour ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°:.57	**Chapitre** : **BESOINS OPÉRATIONNELS**
	Titre : Journalisation des événements
Origine : PC² 4.5.1	**Critère :** Types d'événements enregistrés
ETSI : 7.4.11, a, d, h, k, l, m, n, o	

Exigences minimales pour le référentiel de sécurité du PSC :

- Lister tous les éléments journalisés, qu'il s'agisse d'une journalisation automatique ou manuelle.
- Pour les événements journalisés, préciser les informations enregistrées et les modalités d'enregistrement (système, support, main courante manuelle...).
- Préciser les modalités et procédures d'enregistrement, dans le cas de journalisation automatique comme dans le cas de document papier et de procédure manuelle.
- Préciser les droits d'accès (création, lecture, modification ou suppression, audit) pour tous les types d'événements enregistrés.
- Préciser les modalités de protection des fichiers et des supports contre des accès non autorisés (lecture, modification).
- Préciser le niveau de classification et les protections mises en œuvre pour les paramétrages du système de journalisation.
- Préciser les modalités de sauvegarde des fichiers et des supports (y compris les documents papier) et de protection contre les risques majeurs.
- Préciser la politique et les modalités d'audit des journaux d'événements (automatiques et manuels).

Contrôles :		**Réponses**
Q1	Les événements journalisés correspondent-ils aux exigences et aux engagements de la PC et de la délivrance de certificats qualifiés?	
Q2	Pour chaque événement, les informations enregistrées correspondent-elles aux exigences et aux engagements de la PC ?	
Q3	Les conditions d'enregistrement et de conservation (sauvegardes notamment) garantissent-elles leur disponibilité, même en cas de risque majeur ?	
Q4	Les droits d'accès aux journaux et documents de journalisation sont-ils conformes aux principes et règles de la PC et de la PSSI ?	
Q5	La politique et les modalités d'audit des journaux et documents de journalisation sont-elles conformes aux principes et règles de la PC et de la PSSI ?	
Q6	Vérifier par sondage sur certains journaux que les droits d'accès attribués sont conformes aux règles et principes et à jour.	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 58	**Chapitre** : **BESOINS OPÉRATIONNELS**
	Titre : Journalisation des événements
Origine : PC² 4.5.2	**Critère :** Fréquence de traitement des journaux d'événements
ETSI : 7.4.11	

Exigences minimales pour le référentiel de sécurité du PSC :

- La DPC doit préciser les références des procédures d'analyse des journaux ainsi que les actions à mener en fonction du résultat de ces analyses.
- Les procédures d'analyse doivent être précisées :
  - Quels sont les journaux concernés.
  - Quels sont les rôles et responsabilités.
  - Quelle périodicité.
  - Quels sont les résultats à enregistrer.
- Les événements audités doivent être spécifiés.
- Les références des procédures traitant de la détection d'anomalies ou d'incident doivent être précisées.

Contrôles :	**Réponses**
Q1 S'assurer que les procédures d'analyse des journaux décrites dans la DPC garantissent que les engagements de la PC sont respectés : – Types d'événements analysés – Journaux concernés – Rôles et responsabilités – Périodicité – Résultats à enregistrer – Procédures en cas de détection d'anomalies.	
Q2 Vérifier par sondage au niveau des procédures formalisées et par enquête auprès des agents que les procédures opérationnelles correspondantes sont en place, connues des personnes ayant à les mettre en œuvre et régulièrement appliquées.	
Q3 Se faire communiquer les rapports d'analyse des journaux produits au cours d'une période récente. Vérifier qu'ils correspondent aux règles énoncées.	
Q4 Se faire communiquer des rapports d'anomalie ou d'incident. Enquêter sur les suites données ; apprécier leur conformité aux règles et procédures formelles, ainsi que la pertinence et la qualité des réponses données	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°:.59	**Chapitre** : **BESOINS OPÉRATIONNELS**
	Titre : Journalisation des événements
Origine : PC² 4.5.3	**Critère :** Durée de rétention d'un journal d'événements
ETSI : 7.4.11.e	

Exigences minimales pour le référentiel de sécurité du PSC :

- Les mesures prises contre la perte accidentelle ou la destruction malveillante des journaux.
- Les procédures et moyens mis en œuvre garantissant le respect de la durée minimale de conservation des journaux d'événements.
- Les procédures et moyens mis en œuvre garantissant la destruction effective ou l'archivage des journaux d'événements au terme de la période de rétention.

Contrôles :		**Réponses**
Q1	Les mesures prises contre la perte accidentelle ou la destruction malveillante des journaux (notamment les mesures de sauvegarde) permettent-elles de garantir le respect des engagements de la PC ?	
Q2	Les mesures techniques spécifiées sont-elles en place et utilisées?	
Q3	S'assurer par sondage au cours d'une période donnée que les procédures de sauvegarde et d'externalisation sont appliquées.	
Q4	La procédure de test des sauvegardes et des archives est-elle formalisée, documentée et mise à jour ?	
Q5	Demander copie des rapports correspondants aux dernières opérations de test des sauvegardes et des archives. Vérifier leur existence, leur conformité et apprécier la qualité des résultats des tests, en particulier quant à l'exhaustivité des reconstitutions réalisées.	
Q6	Le cas échéant, procéder ou faire procéder à un test particulier de relecture des archives ou de reconstitution à partir des sauvegardes.	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 60	**Chapitre** : **BESOINS OPÉRATIONNELS**
	Titre : Journalisation des événements
Origine : PC² 4.5.4	**Critère :** Protection d'un journal d'événements
ETSI : 7.4.10.a	

Exigences minimales pour le référentiel de sécurité du PSC :

- Les moyens et les procédures de protection de l'intégrité, contre la perte, la destruction et la falsification des journaux d'événements.
- Le fonctionnement et la mise en œuvre du système de synchronisation des horloges des serveurs.
- Les conditions de conservation des journaux d'événements.
- Selon la sensibilité du journal d'événements, les moyens (techniques et humains) et procédures assurant la confidentialité des journaux d'événements.
- L'avis favorable de l'AC quant à la définition de la sensibilité des journaux d'événements.
- La politique de protection doit être précisée, en particulier si différents niveaux de protection sont définis et gérés. Dans ce cas, les règles de protection associées à chaque niveau doivent être précisées.
- L'attribution des droits d'accès doit être précisée selon le type d'événements ou de journal éventuellement.

Contrôles :		**Réponses**
Q1	Les moyens et les procédures mis en œuvre pour la datation et la protection en intégrité des événements journalisés sont-ils conformes à ce que définit la DPC ?	
Q2	Les niveaux de protection associés aux journaux d'événements et les règles de protection associées sont-ils conformes à la DPC ou à la Politique de Sécurité Interne sur ces points ?	
Q3	Les moyens et les procédures mis en œuvre pour la protection de la confidentialité des événements journalisés sont-ils conformes à la DPC ?	
Q4	Les droits d'accès (création, lecture, modification ou suppression, audit) définis sont-ils spécifiés et sont-ils conformes à la PC et aux règles de séparation des pouvoirs ?	
Q5	La liste des utilisateurs autorisés à accéder aux journaux d'événements est-elle conforme aux règles et à jour ?	
Q6	Les moyens et procédures mis en œuvre pour la synchronisation des horloges utilisées pour la datation des enregistrements sont-ils d'une précision de plus ou moins une seconde par rapport au temps UTC ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 61	**Chapitre** : **BESOINS OPÉRATIONNELS**
	Titre : Journalisation des événements
Origine : PC² 4.5.6	**Critère :** Systèmes de collecte des journaux (interne ou externe)
ETSI : 7.4.11	

Exigences minimales pour le référentiel de sécurité du PSC :

- Les moyens et procédures utilisés afin de collecter les événements durant toute la période d'activité du système informatique.
- Les mesures de protection.
- L'administration de la sécurité.
- Les procédures et moyens permettant d'apporter des garanties quant à son contrôle d'accès

Contrôles :		**Réponses**
Q1	Les procédures de journalisation sont-elles formalisées, documentées et mises à jour ?	
Q2	Existe-t-il des mécanismes de protection pour éviter le contournement ou la mise hors service de la journalisation des événements audités ?	
Q3	Y a-t-il des garanties suffisantes quant à la séparation des pouvoirs, notamment quant à ce qui concerne la journalisation de toutes les opérations d'administration et les possibilités d'audit ?	
Q4	Les méthodes et procédures d'évolution, de mise à jour et de gestion en configuration des moyens et procédures de journalisation des événements audités et d'accès aux journaux sont-ils conformes à la DPC ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 62	**Chapitre** : **BESOINS OPÉRATIONNELS**
	Titre : Journalisation des événements
Origine : PC² 4.5.7	**Critère :** Imputabilité
ETSI : 7.4.11	

Exigences minimales pour le référentiel de sécurité du PSC :

- Le fonctionnement du mécanisme logiciel assurant l'authentification et la non-répudiation possible de l'exécutant, garantissant ainsi l'imputabilité des actions.
- La liste détaillée du contenu des différentes traces d'événements enregistrables.

Contrôles :		**Réponses**
Q1	La liste des événements audités est-elle conforme à celle spécifiée dans la DPC ?	
Q2	Pour chaque événement audité les informations enregistrées correspondent-elles à celles spécifiées dans la DPC ?	
Q3	Compte tenu des événements spécifiés peut-on garantir que tout événement est imputable à une personne individuellement identifiée et authentifiée ?	
Q4	Le contenu des informations enregistrées est-il conforme aux spécifications de la DPC (sur le système) ?	
Q5	Consulter le journal des événements correspondant aux dernières périodes afin de s'assurer du bon fonctionnement de la fonction de journalisation (par exemple : pas d'interruption prolongée dans les enregistrements ; dispersion satisfaisante des événements enregistrés, ...).	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 63	**Chapitre** : **BESOINS OPÉRATIONNELS**
	Titre : Journalisation des événements
Origine : PC² 4.5.8	**Critère :** Analyse des vulnérabilités
ETSI : 7.4.11	

Exigences minimales pour le référentiel de sécurité du PSC :

- Définir les procédures d'analyse des tentatives d'attaque, de traitement des tentatives d'attaque des systèmes, de remontée des incidents et de traitement de l'alerte, d'identification d'une vulnérabilité globale ou d'une attaque de grande dimension, et de réaction face aux différents incidents de sécurité.
- Définir les incidents nécessitant la rédaction de rapports.
- Définir le format des rapports.

Contrôles :		**Réponses**
Q1	Existe-t-il une procédure formalisée, documentée et mise à jour d'analyse des tentatives d'attaque du système, à partir des journaux d'événements et d'accès?	
Q2	Existe-t-il une procédure formalisée, documentée et mise à jour de traitement des tentatives d'attaque des systèmes permettant de mettre en évidence des tentatives organisées?	
Q3	Existe-t-il une procédure formalisée, documentée et mise à jour de remontée des incidents et de traitement de l'alerte?	
Q4	Existe-t-il une procédure formalisée, documentée et mise à jour permettant d'identifier, au travers d'incidents individuels, une vulnérabilité globale ou une attaque de grande dimension?	
Q5	Existe-t-il une procédure formalisée, documentée et mise à jour de réaction face à la mise en évidence d'une tentative d'attaque organisée ou d'une vulnérabilité particulière?	
Q6	Les procédures de détection d'attaque, de remontée de l'incident, de déclenchement de l'alerte et de réaction face à une attaque détectée ou supposée sont-elles formalisées, documentées et mises à jour?	
Q7	Se faire communiquer les rapports concernant les derniers incidents constatés et les suites données. Apprécier la qualité des suites données (efficacité, rapidité, ...).	
Q8	Les tests de relecture des journaux sont-ils effectués de manière régulière ? Vérifier par sondage qu'ils sont régulièrement effectués, conformément aux procédures et qu'ils donnent lieu à un Procès Verbal formel.	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n : 64	**Chapitre** : **BESOINS OPÉRATIONNELS**
	Titre : Archives
Origine : PC² 4.6.1	**Critère :** Types de données à archiver
ETSI : 7.3.1.g, h, k, 7.4.11, a, c, g, i	

Exigences minimales pour le référentiel de sécurité du PSC :

- La politique de protection doit être précisée, en particulier si différents niveaux de protection sont définis et gérés. Dans ce cas, les règles de protection associées à chaque niveau doivent être précisées.
- Les conditions de conservation des archives
- Pour chaque type d'archives, le lieu d'archivage.
- Le rôle et les responsabilités des personnes participant à l'archivage des données.
- Pour chaque type de donnée, la fréquence d'archivage doit être précisée.
- La DPC doit préciser les autres données non mentionnées dans la PC devant être archivées.
- Les moyens et les procédures de protection de l'intégrité des archives.

Contrôles :	**Réponses**
Q1 Vérifier que les informations suivantes sont archivées : ✓ Accords contractuels ou conventions avec d'autre PSC ✓ Certificats du signataire et de composantes ✓ CRL ✓ Demande de révocation et leurs résultats ✓ Données collectées lors de la phase d'enregistrement du signataire (y compris quand cela est utilisé le lien entre un signataire et son certificat qualifié) dont le numéro de référence et les limitations de validité et d'usage des pièces d'identité officielles utilisées lors de l'enregistrement. ✓ Journaux d'événements des entités du PSC en relation avec les opérations propres aux certificats et le cas échant aux clés privée et publique ✓ Logiciels et fichiers de configuration des différentes composantes ✓ Ensemble des éléments utiles à l'enregistrement des signataires. ✓ Documents présentés par le demandeur. ✓ Emplacement où sont conservées les copies des formulaires remplis par le demandeur, y compris le document manifestant l'adhésion et l'acceptation du signataire aux conditions d'utilisation du contenu du certificat. ✓ Tout choix spécifique effectué par le signataire lors de son adhésion aux conditions d'utilisation du certificat (par exemple, acceptation ou refus de publication du certificat dans un annuaire). ✓ Identité de la personne morale au nom de laquelle a lieu la demande. ✓ Méthode utilisée pour valider les documents d'identité.	
Q2 Vérifier que les conditions et modalités d'archivages sont cohérentes avec les exigences découlant de la PC et avec les obligations découlant de la DPC.	
Q3 S'assurer par sondage au cours des dernières périodes que ces exigences sont effectivement appliquées.	
Q4 Le rôle et les responsabilités des personnes participant à l'archivage des données sont-ils bien définis ?	
Q5 Les droits d'accès aux archives sont-ils cohérents avec les droits d'accès attribués aux	

	informations avant archivage ?	
Q6	Les procédures concernant les conditions de conservation des archives, en particulier quant à leur protection physique et à la protection de leur confidentialité sont-elles formalisées, documentées et à mises à jour ?	
Q7	Les conditions de sécurité physique assurent-elles un niveau de sécurité conforme aux règles de protection correspondant au niveau de sensibilité (ou classification des archives) ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 65	**Chapitre** : **BESOINS OPÉRATIONNELS**
	Titre : Archives
Origine : PC² 4.6.2	**Critère :** Période de rétention des archives
ETSI : 7.4.11.e, notes 4 et 5	

Exigences minimales pour le référentiel de sécurité du PSC :

- Le respect de la durée minimale de conservation.
- La destruction effective des archives au terme de leur période de rétention, et la méthode utilisée par rapport à leur niveau de classification / sensibilité.

Contrôles :	**Réponses**
Q1 La durée minimale de conservation spécifiée par la DPC répond-elle aux exigences de la PC ?	
Q2 Les procédures de destruction des archives sont-elles conformes à leur niveau de sensibilité / classification ?	
Q3 Vérifier par sondage la durée de conservation des archives [*]	
Q4 Se faire communiquer et vérifier par sondage des PV de destruction d'archive [*]	
[*] Ce type de contrôle ne pourra être effectué que lorsque la durée d'existence du PSC sera suffisante.	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 66	**Chapitre** : **BESOINS OPÉRATIONNELS**
	Titre : Archives
Origine : PC² 4.6.3	**Critère :** Protection des archives
ETSI : 7.4.11.a, b	

Exigences minimales pour le référentiel de sécurité du PSC :

- La politique de protection doit être précisée, en particulier si différents niveaux de protection sont définis et gérés. Dans ce cas, les règles de protection associées à chaque niveau doivent être précisées.
- Les moyens et les procédures de protection de l'intégrité et de la disponibilité des archives.
- Les conditions de conservation des archives.
- Selon la sensibilité des archives, les moyens (techniques et humains) et procédures assurant la confidentialité des archives, notamment des clés privées de confidentialité ou de transport de clés.

Contrôles :		**Réponses**
Q1	Les moyens et les procédures mis en œuvre pour la protection en intégrité des archives sont-ils conformes à la DPC ?	
Q2	Les niveaux de protection associés aux archives et les règles de protection associées sont-ils conformes à la DPC ou à la Politique de Sécurité Interne sur ce point ?	
Q3	Les moyens et les procédures mis en œuvre pour la protection de la confidentialité des archives sont-ils conformes à la DPC ?	
Q4	Vérifier que les droits d'accès physique définis sont spécifiés et qu'ils sont conformes à la PC et aux règles de séparation des pouvoirs.	
Q5	Se faire communiquer la liste des utilisateurs autorisés à accéder aux archives et vérifier sa conformité par rapport aux règles, et s'assurer qu'elle est à jour.	
Q6	Demander copie de l'avis favorable de l'AC quant à la définition de la sensibilité des archives. Apprécier son caractère conforme.	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 67	**Chapitre** : **BESOINS OPÉRATIONNELS**
	Titre : Archives
Origine : PC² 4.6.5	**Critère :** Besoin de datation des enregistrements
ETSI : 7.4.11.note 3	

Exigences minimales pour le référentiel de sécurité du PSC :

- Préciser les modalités de datation concernant le traitement des archives.

Contrôles :	**Réponses**
Q1 Les moyens et les procédures mis en œuvre pour la datation des événements journalisés sont-ils conformes aux spécifications de la DPC ?	
Q2 Porter une appréciation sur l'adéquation des moyens et procédures mis en œuvre par rapport aux engagements de la PC quant à la datation des événements journalisés.	
Q3 Les moyens et procédures mis en œuvre pour la datation des enregistrements et la synchronisation des horloges sont-ils conformes aux spécifications de la DPC ?	
Q4 La précision de l'horloge servant à la datation des enregistrements du PSC est-elle de plus ou moins une seconde par rapport au temps UTC ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 68	**Chapitre** : **BESOINS OPÉRATIONNELS**
	Titre : Archives
Origine : PC² 4.6.6	**Critère :** Système de collecte des archives (interne ou externe)
ETSI : 7.4.11	

Exigences minimales pour le référentiel de sécurité du PSC :

- Les mécanismes de collecte et de protection des archives mis en œuvre.
- Les méthodes et procédures d'évolution, de mise à jour et de gestion en configuration des moyens et procédures de collecte des archives.

Contrôles :		**Réponses**
Q1	Les mécanismes de collecte des archives mis en œuvre sont-ils conformes aux spécifications de la DPC ?.	
Q2	Les mécanismes mis en œuvre pour éviter le contournement de la collecte des archives sont-ils conformes aux spécifications de la DPC ?	
Q3	Les méthodes et procédures d'évolution, de mise à jour et de gestion en configuration des moyens et procédures de collecte des archives sont-elles conformes aux spécifications de la DPC ?.	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°:.69	**Chapitre** : **BESOINS OPÉRATIONNELS**
	Titre : Archives
Origine : PC² 4.6.7	**Critère :** Procédures de récupération des archives
ETSI : 7.4.11	

Exigences minimales pour le référentiel de sécurité du PSC :

- Le processus de récupération doit faire l'objet d'une procédure interne ou doit être détaillé
- La DPC doit préciser les garanties permettant de s'assurer que chaque composante n'a accès qu'à ses propres archives.
- Détailler les moyens permettant de s'assurer de la récupération d'archives sous un délai maximum.
- Lister les cas où il existe une possibilité de consulter les archives d'une autre composante.

Contrôles :		**Réponses**
Q1	Existe-t-il une procédure interne concernant la récupération des archives ?	
Q2	Se faire communiquer la procédure de récupération des archives et vérifier qu'elle remplit les exigences de la PC.	
Q3	Les conditions de conservation et les moyens de récupération des archives permettent-ils de garantir que seules les personnes autorisées au sein de la composante peuvent avoir accès aux archives, et que cet accès est possible sous un délai maximum conforme aux engagements de la PC ?	
Q4	Dans le cas où d'autres entités du PSC pourraient avoir accès aux archives, les moyens et procédures mis en place garantissent-ils que seules les personnes autorisées peuvent avoir accès aux archives ?	
Q5	Vérifier que ces procédures sont régulièrement testées ; se faire communiquer les comptes rendus des tests ; vérifier qu'ils démontrent le caractère opérationnel de la procédure et des moyens.	
Q6	Si besoin, et notamment en cas de doute, procéder au test direct de la procédure.	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 70	**Chapitre** : **BESOINS OPÉRATIONNELS**
	Titre : Changement de clé d'une composante
Origine : PC² 4.7	**Critère :** néant

Exigences minimales pour le référentiel de sécurité du PSC :

- Les procédures et les moyens permettant d'informer les utilisateurs et l'AC du PSC du changement de clé utilisée pour les besoins externes.
- Le rôle et les responsabilités des personnes chargées de la diffusion de l'information concernant un changement de clé.

Contrôles :		**Réponses**
Q1	La procédure de mise à disposition d'information des utilisateurs concernant le changement de clé d'AC est-elle formalisée, documentée et mise à jour ?	
Q2	S'assurer que la procédure et les moyens mis en œuvre garantissent que l'AC et tous les utilisateurs seront informés dans le délai maximal stipulé dans la PC.	
Q2	Les rôles et les responsabilités des personnes chargées de la diffusion de l'information concernant un changement de clé sont-ils clairement définis ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 71	**Chapitre** : **BESOINS OPÉRATIONNELS**
	Titre : Compromission et plan anti-sinistre
Origine : PC² 4.8	**Critère** : néant
ETSI : 7.4.4.b, c, d, 7.4.5.g	

Exigences minimales pour le référentiel de sécurité du PSC :

- Indiquer la liste des risques couverts par un plan anti-sinistre.
- Préciser les services couverts par le plan anti-sinistre.
- Décrire les moyens mis en œuvre ou prévus pour les cas de sinistre.
- Préciser l'organisation mise en place pour assurer la gestion et la maintenance du plan anti-sinistre.
- Préciser l'organisation de Cellule de Crise prévue.
- Expliquer les procédures, les moyens et l'organisation mis en place pour la réalisation des tests, pour leur suivi et pour le traitement des incidents constatés.

Contrôles :		**Réponses**
Q1	Existe-t-il un plan anti-sinistre qui permet de s'assurer contre toute perte, dommage ou compromission des biens du PSC ainsi que contre toute interruption de service ?	
Q2	Ce plan anti-sinistre indique-t-il les modalités de déclenchement, de création de rapports d'incidents et les personnes responsables ?	
Q3	Ce plan est-il régulièrement testé ?	
Q4	Le PSC dispose-t-il d'un plan de reprise d'activité en cas de sinistre qui prend en compte les paramètres suivants : • Délai minimum de recouvrement de ces services ? • Politique de sécurité et de protection des secrets ? • Procédures de secours ? • Tests pratiques, formation et entraînement des personnels ?	
Q5	Les services de génération de certificat, de génération des clés et de révocation sont-ils pris en compte dans le plan de continuité et le plan anti-sinistre ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 72	**Chapitre** : **BESOINS OPÉRATIONNELS**
	Titre : Compromission et plan anti-sinistre
Origine : PC² 4.8.1	**Critère :** Corruption des ressources informatiques, logicielles et / ou des données
ETSI : 7.4.4.b, c, 7.4.5.f	

Exigences minimales pour le référentiel de sécurité du PSC :

- Le plan anti-sinistre mis en œuvre permettant l'utilisation des sauvegardes et des archives en cas de corruption des ressources informatiques, logicielles et / ou des données.
- La fréquence et le déroulement de tests de vérification de l'efficacité du plan anti-sinistre.

Contrôles :		**Réponses**
Q1	Existe-t-il un plan anti-sinistre formalisé, documenté et à jour qui porte notamment sur les ressources informatiques, logicielles et/ou données ?	
Q2	Existe-t-il des procédures de secours et de reprise pour les systèmes et les activités opérationnelles ?	
Q3	Le plan anti-sinistre est-il l'objet de tests réguliers, avec établissement de comptes-rendus formels ?	
Q4	Se faire communiquer et contrôler les comptes-rendus des tests récents, par échantillonnage au cours des dernières années ?	
Q5	Vérifier que les tests donnent lieu à l'établissement de fiches d'incident et à des actions correctives.	
Q6	Vérifier qu'il existe une organisation et des procédures adaptées pour le suivi de la réalisation du plan anti-sinistre.	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 73	**Chapitre** : **BESOINS OPÉRATIONNELS**
	Titre : Compromission et plan anti-sinistre
Origine : PC² 4.8.3	**Critère :** Compromission de clé d'une composante
ETSI : 7.4.8.a, b	

Exigences minimales pour le référentiel de sécurité du PSC :

Pour les cas de révocation de la clé publique d'une AC pour compromission ou la suspicion de compromission de clé, la perte ou le vol, préciser :

- Les procédures permettant de garantir la révocation des certificats émis au moins depuis la date de connaissance de la compromission de clé.
- Les procédures et moyens permettant de garantir la mise hors service du PSC.

Contrôles :		**Réponses**
Q1	Les procédures permettant de garantir la révocation des certificats émis au moins depuis la date de connaissance de la compromission de clé de l'AC sont-elles formalisées, documentées et mises à jour ?	
Q2	Les moyens nécessaires à l'application de la procédure visée ci-dessus sont-ils en place ?	
Q3	Les procédures permettant de garantir la mise hors service du PSC en cas de compromission de clé d'une composante sont-elles formalisées, documentées et mises à jour ?	
Q4	Les moyens nécessaires à l'application de la procédure visée ci-dessus sont-ils en place ?	
Q5	Vérifier que les moyens mis en œuvre sont testés régulièrement ; se faire communiquer le compte rendu des tests ; vérifier que les comptes rendus démontrent le caractère opérationnel de la procédure et des moyens, ou qu'un plan d'actions correctives est en cours de réalisation : dans ce dernier cas, s'assurer du caractère réaliste du plan d'actions.	
Q6	La procédure permettant, lorsque l'AC est informée de la compromission des clés privées d'un autre PSC, avec lequel des accords ou des conventions existent de révoquer sans délai tout certificat émis pour ce PSC suivant les clauses contractuelles les liants est-elle formalisée, documentée et mise à jour ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 74	**Chapitre** : **BESOINS OPÉRATIONNELS**
	Titre : Compromission et plan anti-sinistre
Origine : PC² 4.8.4	**Critère :** Mesures de sécurité en cas de sinistre
ETSI : 7.4.8.a	

Exigences minimales pour le référentiel de sécurité du PSC :

La DPC doit préciser :

- Le plan anti-sinistre mis en œuvre assurant le respect des mesures de sécurité.
- La fréquence et le déroulement de tests de vérification de l'efficacité du plan anti-sinistre.

Contrôles :		**Réponses**
Q1	Existe t-il un plan anti-sinistre qui porte notamment sur les mesures de sécurité en cas de sinistre ?	
Q2	Les principes généraux et les règles de sécurité en cas de sinistre sont-ils formalisés ?	
Q3	Le plan anti-sinistre fait-il l'objet de tests réguliers, avec établissement de comptes-rendus formels ?	
Q5	Lorsque cela s'applique, se faire communiquer et contrôler les comptes-rendus des tests récents, par échantillonnage au cours des dernières années ?	
Q6	Vérifier que les tests donnent lieu à l'établissement de fiches d'incident et à des actions correctives.	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 75	**Chapitre** : **BESOINS OPÉRATIONNELS**
	Titre : Fin de vie d'une composante
Origine : PC² 4.9	**Critère** : néant
ETSI : 7.4.9, a, b, c	

Exigences minimales pour le référentiel de sécurité du PSC :

Décrire les procédures et moyens :

- De remise à l'AC des archives, des clés privées de confidentialité.
- Permettant d'informer ses partenaires de la fin de vie d'une entité du PSC.
- S'il existe d'autres spécificités concernant certaines entités du PSC, celles-ci doivent être détaillées.
- Les dispositions de transfert d'obligations et de déblocage de fond.

Contrôles :		**Réponses**
Q1	Dans le cas d'une fin de vie d'une entité du PSC la procédure concernant l'information des partenaires (les signataires, autres entités, autres PSC...) est-elle formalisée, documentée et à jour ?	
Q2	Pour le cas d'une fin de vie d'une entité du PSC, la procédure concernant la remise des archives et des clés à l'AC est-elle formalisée, documentée et à jour?	
Q3	Dans le cas ou la révocation du certificat d'une entité du PSC par une AC extérieure au PSC est prévue, la procédure est-elle formalisée, documentée et à jour ?	
Pour le cas de cessation d'activité :		
Q4	Les procédures prévoient-elles une information avec un délai conforme aux engagements de la PC ?	
Q5	Les moyens prévus pour la mise en œuvre des procédures visées ci-dessus sont-ils suffisants et sont-ils effectivement opérationnels.	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 76	**Chapitre : CONTRÔLES DE SÉCURITÉ PHYSIQUE, CONTRÔLES DES PROCÉDURES, CONTRÔLES DU PERSONNEL**
	Titre : Contrôles physiques
Origine : PC² 5.1.1	**Critère :** Situation géographique et construction de sites
ETSI : 7.4.4.f, note 2	

Exigences minimales pour le référentiel de sécurité du PSC :

- Si l'analyse de risque spécifie des exigences de sécurité, s'assurer que la DPC apporte les garanties d'assurance correspondantes.

Contrôles :		**Réponses**
Q1	La situation géographique et la construction des sites sont-elles conformes aux besoins exprimés par l'analyse de risque ?	
Q2	La procédure prévoyant que tous nouveaux services de l'AC en liaison avec la certification ou la validation est sécurisée avec un même degré d'assurance est-elle formalisée, documentée et à jour ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 77	**Chapitre** : **CONTRÔLES DE SÉCURITÉ PHYSIQUE, CONTRÔLES DES PROCÉDURES, CONTRÔLES DU PERSONNEL**
	Titre : Contrôles physiques
Origine : PC² 5.1.2	**Critère :** Accès physique
ETSI : 7.2.5 b, 7.4.4.a, e, f, g, 7.4.6.h, i, j	

Exigences minimales pour le référentiel de sécurité du PSC :

- Les mesures prises en vue de protéger l'accès physique à une composante et aux ressources du PSC de manière à détecter, enregistrer et réagir contre tout accès non autorisé doivent être précisées.
- Les procédures et les moyens permettant de garantir la sécurité du site en dehors des heures ouvrées doivent être décrites.
- La DPC doit préciser l'organisation des locaux du PSC en différentes zones dont les accès ne seront possibles qu'avec les habilitations nécessaires. Les catégories d'habilitations du personnel doivent être précisées dans la DPC ; elles correspondent aux besoins liés à la fonction.
- La fréquence et la méthode de contrôle des enregistrements des accès physiques doivent être établies.

Contrôles :		**Réponses**
Q1	Les règles et procédures d'accès sont-elles formalisées, documentées, à jour et conforme à l'analyse de risque ?	
Q2	Ont-elles été communiquées et sont-elles connues de l'ensemble du personnel, en fonction du besoin d'en connaître ?	
Q3	Les règles de contrôle d'accès précisées dans la DPC sont-elles appliquées par la mise en œuvre de moyens de contrôle d'accès appropriés ?	
Q4	Vérifier que les enregistrements des accès physiques sont régulièrement contrôlées et auditées (se faire communiquer les rapports).	
Q5	Par sondage, vérifier la cohérence des enregistrements d'accès avec les droits d'accès.	
Q6	Les *équipements sensibles* sont-ils situés dans une zone de sécurité renforcée, à accès strictement limité et contrôlé ?	
Q7	Si le PSC partage une partie de ses locaux avec un autre organisme : Vérifier que les personnels (des locaux communs) n'appartenant pas au PSC ne peuvent pas accéder aux fonctions et équipements définis comme sensibles par l'analyse de risque.	
Q8	Des moyens et procédures existent-ils pour garantir une continuité de sécurité du site en dehors des heures ouvrées ?	
Q9	Des contrats de maintenance existent-ils pour les systèmes de sécurité physique de contrôle d'accès.	
Q10	Les droits d'accès sont-ils régulièrement revus et mis à jour ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 78	**Chapitre** : **CONTRÔLES DE SÉCURITÉ PHYSIQUE, CONTRÔLES DES PROCÉDURES, CONTRÔLES DU PERSONNEL**
	Titre : Contrôles physiques
Origine : PC² 5.1.3	**Critère :** Électricité et air conditionné
ETSI : 7.4.4.f	

Exigences minimales pour le référentiel de sécurité du PSC :

La prévention physique contre des incidents matériels doit être précisée notamment sur certains points essentiels :

- Les équipements vitaux doivent être protégés contre les risques de panne d'alimentation électrique ou de toute anomalie d'énergie électrique.
- Les équipements vitaux doivent être placés dans des locaux équipés d'installation d'air conditionné.
- Les câbles d'alimentation doivent être protégés contre les dommages matériels.

Contrôles :		**Réponses**
Q1	Les équipements vitaux sont-ils au minimum équipés d'un onduleur ?	
Q2	Les équipements vitaux dont le fonctionnement ne doit pas être interrompu disposent-ils d'une alimentation électrique secourue (Groupe électrogène) ?	
Q3	Le groupe électrogène fait-il l'objet de tests réguliers (fonctionnement en conditions réelles) et de l'existence d'un contrat de maintenance : vérifier les PVs ?	
Q4	Les locaux dans lesquels sont situés les équipements vitaux sont-ils équipés d'une installation d'air conditionné garantissant des conditions de température satisfaisante dans les locaux ? [*]	
Q5	Les équipements d'air conditionné présentent-ils une redondance suffisante ? [*]	
Q6	Les équipements de conditionnement de l'air font-ils l'objet d'une maintenance régulière : vérifier les PVs d'intervention de la maintenance ?	
Q7	Dans les faux planchers et les chemins de câbles, les câbles d'alimentation électriques et les câbles de communication de données sont-ils séparés dans des chemins de câbles différents et isolés du sol ? (problème de CEM)	
Q8	Les armoires électriques sont-elles maintenues fermées à clef?	
Q9	Des contrats de maintenance existent-ils pour les équipements d'air conditionné et les équipements de secours d'alimentation électrique ?	
Q10	Des contrats de maintenance existent-ils pour les moyens d'infrastructure ?	
Q11	Les équipements de production d'électricité présentent-ils une redondance suffisante?	
[*] si les équipements, dans leur environnement d'exploitation, nécessitent une installation de conditionnement de l'air.		

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 79	**Chapitre** : **CONTRÔLES DE SÉCURITÉ PHYSIQUE, CONTRÔLES DES PROCÉDURES, CONTRÔLES DU PERSONNEL**
	Titre : Contrôles physiques
Origine : PC² 5.1.4	**Critère :** Expositions à l'eau
ETSI : 7.4.4.f	

Exigences minimales pour le référentiel de sécurité du PSC :

Les équipements vitaux doivent être protégés contre l'exposition à l'eau.

Contrôles :		**Réponses**
Q1	Les équipements vitaux sont-ils protégés contre l'exposition à l'eau ?	
Q2	Vérifier que les systèmes de protection contre l'exposition à l'eau font l'objet d'une maintenance régulière : vérifier les PVs d'intervention de la maintenance.	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 80	**Chapitre** : **CONTRÔLES DE SÉCURITÉ PHYSIQUE, CONTRÔLES DES PROCÉDURES, CONTRÔLES DU PERSONNEL**
	Titre : Contrôles physiques
Origine : PC² 5.1.5	**Critère :** Prévention et protection contre le feu
ETSI : 7.4.4.f	

Exigences minimales pour le référentiel de sécurité du PSC :

- Les équipements vitaux doivent être placés dans des locaux équipés pour la protection contre les incendies.

Contrôles :		**Réponses**
Q1	Les entités du PSC respectent-elles les normes en matière de sécurité incendie, en détection et extinction ?	
Q2	Vérifier que les systèmes de détection et d'extinction d'incendie font l'objet d'une maintenance régulière : vérifier les PVs d'intervention de la maintenance.	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 81	**Chapitre** : **CONTRÔLES DE SÉCURITÉ PHYSIQUE, CONTRÔLES DES PROCÉDURES, CONTRÔLES DU PERSONNEL**
	Titre : Contrôles physiques
Origine : PC² 5.1.6	**Critère :** Conservation des médias
ETSI : 7.4.5.e	

Exigences minimales pour le référentiel de sécurité du PSC :

- Préciser les procédures de contrôle d'accès au média.
- Apporter les garanties quant à l'application de ces contrôles.
- Apporter les garanties quant à l'efficacité des enceintes sécurisées.
- Le lieu de conservation des médias classés sensibles ne doit pas être précisé.

Contrôles :		**Réponses**
Q1	Existe-t-il une procédure, formalisée, documentée et à jour contre le vol, l'atteinte à l'intégrité et à la confidentialité des médias ?	
Q2	Vérifier par l'examen de la main courante et les comptes-rendus d'exécution que les procédures d'accès aux médias sont appliquées de manière conforme.	
Q3	Se faire communiquer la liste des utilisateurs ayant un droit d'accès aux médias. Vérifier la cohérence des profils attribués avec les fonctions.	
Q4	La procédure permettant d'identifier les supports de données et leur niveau de protection associé est-elle formalisée, documentée et à jour ?	
Q5	Les supports contenant des données sensibles sont-ils détruits lorsqu'ils sont retirés du service (dont les disques durs des équipements informatiques) ?	
Q6	Les médias font-ils l'objet d'une classification en fonction de la sensibilité des données qu'ils contiennent ?	
Q7	Avant réutilisation, les médias font-ils l'objet d'une vérification de la sensibilité des informations qu'ils contiennent ?	
Q8	Vérifier que les équipements, les informations et les logiciels du PSC ne peuvent pas quitter le site sans autorisation ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 82	**Chapitre** : **CONTRÔLES DE SÉCURITÉ PHYSIQUE, CONTRÔLES DES PROCÉDURES, CONTRÔLES DU PERSONNEL**
	Titre : Contrôles physiques
Origine : PC² 5.1.7	**Critère :** Traitement des déchets
ETSI : 7.4.5.e, 7.4.6.g	

Exigences minimales pour le référentiel de sécurité du PSC :

- Les supports d'information papiers et magnétiques ne présentant plus d'utilité doivent être détruits selon des procédures sécuritaires.
- Les procédures de destruction des informations sensibles doivent être écrites et garantir que les informations enregistrées sur ces supports ne peuvent pas être lues ou réutilisées. Ces procédures doivent prévoir une destruction physique des supports d'information, ou au moins trois réécritures dans le cas d'un effacement logique.
- Dans le cas d'informations sensibles, la destruction du support ou l'effacement doit être constaté par un P.V. formel signé de deux personnes (normalement l'utilisateur normal et l'opérateur ayant procédé à la destruction, à défaut un témoin).

Contrôles :		**Réponses**
Q1	Existe t-il une procédure formalisée, documentée et à jour pour la destruction des supports contenant des informations sensibles et prévoit-elle les précautions et mesures adaptées ?	
Q2	Existe t-il une procédure formalisée, documentée et à jour pour la réutilisation des supports contenant des informations sensibles et prévoient-elles les précautions et mesures adaptées ?	
Q3	Dans le cas d'informations sensibles, la destruction du support ou l'effacement est-il constaté par un P.V. formel signé de deux personnes ?	
Q4	Vérifier par sondage des PVs pour des destructions récentes.	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 83	**Chapitre** : **CONTRÔLES DE SÉCURITÉ PHYSIQUE, CONTRÔLES DES PROCÉDURES, CONTRÔLES DU PERSONNEL**
	Titre : Contrôle des procédures
Origine : PC² 5.2.1	**Critère :** Rôle de confiance
ETSI : 7.4.3.b et g, 7.4.5 note 1	

Exigences minimales pour le référentiel de sécurité du PSC :

- Les attributions associées à chaque rôle doivent être précisées.
- Définir les procédures permettant d'identifier les différents rôles.
- La DPC doit apporter les garanties concernant la conformité de la distribution des rôles au sein des entités du PSC avec l'annexe "Rôles" de la DPC.

Contrôles :	**Réponses**
Q1 Vérifier par sondage (tâches sensibles et quelques fonctions au hasard) que les définitions de poste incluent une définition claire des responsabilités en matière de sécurité.	
Q2 Éventuellement, vérifier également par enquête auprès de quelques agents (tâches sensibles et au hasard) de la connaissance qu'ils ont de leur mission et de leur responsabilité en matière de sécurité.	
Q3 Se faire communiquer la procédure et les modalités de vérifications préalables à l'embauche (extrait de casier judiciaire) ; sont-ils formalisés, documentés et à jour ?	
Q4 Vérifier que les agents employés à des tâches sensibles font l'objet d'enquête de renouvellement périodique (typiquement tous les 2/3 ans).	
Q5 L'autorité a-t-elle clairement identifiées et définies les responsabilités décrites ci-dessous : • *Responsable sécurité* : Il est responsable de l'application de la politique de sécurité physique et fonctionnelle d'une composante du PSC et de son environnement. Il gère les contrôles d'accès physiques à la plate-forme de la composante, et est chargé de mettre en œuvre la politique de sécurité régissant la composante. • *Contrôleur* : 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 politiques de certification, des déclarations des pratiques de certification et des services effectivement fournis par la composante du PSC. • *Administrateur* : Un administrateur met en œuvre les politiques de certification et déclarations des pratiques de certification du PSC au sein de la composante qu'il administre. Il est responsable de l'ensemble des services rendus par cette composante. • *Ingénieur système* : Il est chargé de la mise en route, de la configuration et de la maintenance technique de la plate-forme informatique de la composante. Il assure l'administration du système et du réseau de cette plate-forme. • *Opérateur* : L'opérateur d'une composante (autorité de certification (AC), autorité d'enregistrement (AE), une tierce partie de confiance TPC, une autorité d'horodatage (AH),) réalise l'exploitation des services offerts par la composante, dans le cadre de ses attributions. Il est chargé de lancer	

l'exécution des fonctions cryptographiques.	
Justification des réponses négatives :	
Solutions envisagées ou proposées :	

Fiche n°: 84	**Chapitre** : **CONTRÔLES DE SÉCURITÉ PHYSIQUE, CONTRÔLES DES PROCÉDURES, CONTRÔLES DU PERSONNEL**
	Titre : Contrôle des procédures
Origine : PC² 5.2.2	**Critère :** Nombre de personnes nécessaires à chaque tâche
ETSI : 7.4.3.b, 7.4.5.d, h	

Exigences minimales pour le référentiel de sécurité du PSC :

- Le nombre d'exploitants prévus par type d'opérations doit être précisé.
- Apporter des garanties quant à la conformité du nombre de personnes nécessaire à chaque tâche, avec l'annexe "Rôles".

Contrôles :		**Réponses**
Q1	Vérifier qu'un document formalisé précise le nombre d'exploitants minimum nécessaires par type d'opérations.	
Q2	Contrôler la conformité de ce document avec le document "Rôles".	
Q3	Analyser les journaux d'événements et les PVs afin de contrôler l'application stricte du document précisant le nombre d'exploitants minimum nécessaires par type d'opérations.	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 85	**Chapitre** : **CONTRÔLES DE SÉCURITÉ PHYSIQUE, CONTRÔLES DES PROCÉDURES, CONTRÔLES DU PERSONNEL**
	Titre : Contrôle des procédures
Origine : PC² 5.2.3	**Critère :** Identification et authentification des rôles
ETSI : 7.4.3.c, 7.4.6.d, e	

Exigences minimales pour le référentiel de sécurité du PSC :

- La création, la modification ou la suppression d'identifiant, de droits d'accès et d'autorisation sur tous les systèmes d'informations et services multi-utilisateurs doivent être effectués selon une procédure formalisée, documentée et à jour par les administrateurs dûment habilités.
- La création, la modification ou la suppression de privilèges d'administration ou d'exploitation doivent être effectués par l'administrateur selon une procédure rigoureuse.
- Les droits d'accès attribués aux utilisateurs en fonction de leurs rôles doivent faire régulièrement l'objet d'une revue, sur la base de procédures référencées.

Contrôles :		**Réponses**
Q1	Les procédures de demande d'attribution de profils utilisateurs, de modification de privilèges d'administration et de modification de droits d'accès sont-elles formalisées, documentées et mises à jour ?	
Q2	Vérifier, par sondage, les traces formelles (notes, fax, e-mail, …) des demandes d'attribution des droits d'accès.	
Q3	La liste des utilisateurs habilités et de leurs droits existe-t-elle ? Vérifier la cohérence des profils attribués avec les fonctions.	
Q4	Vérifier par sondage les traces des créations de profils utilisateurs : elles doivent être affectées à un administrateur habilité.	
Q5	L'attribution et le contrôle des droits d'accès font-ils l'objet d'audits réguliers ? Se faire communiquer et examiner les rapports.	
Q6	Existe-t-il des mécanismes de sécurité permettant de séparer les différentes fonctions de confiance ?	
Q7	Les procédures d'attribution de profil d'accès aux utilisateurs font-elles l'objet d'audits réguliers ? Se faire communiquer et examiner les rapports.	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 86	**Chapitre** : **CONTRÔLES DE SÉCURITÉ PHYSIQUE, CONTRÔLES DES PROCÉDURES, CONTRÔLES DU PERSONNEL**
	Titre : Contrôles du personnel
Origine : PC² 5.3.1	**Critère :** Compétences, qualifications et antécédents requis
ETSI : 7.4.3.a, e	

Exigences minimales pour le référentiel de sécurité du PSC :

- Les compétences nécessaires du personnel pour chaque poste.
- Les méthodes de vérifications des compétences professionnelles.
- Les vérifications à effectuer avant l'embauche définitive.
- La procédure d'embauche doit être adaptée en fonction de la sensibilité de chaque poste. La procédure doit être précisée, validée par la Direction et appliquée pour toute embauche.

Contrôles :		**Réponses**
Q1	Vérifier par sondage les compétences professionnelles de certains agents employés, afin de les comparer aux pré-requis de leur poste.	
Q2	Le nom et la fonction de tous les employés sont-ils explicitement précisés dans un document ?	
Q3	Le personnel d'encadrement possède-t-il l'expertise appropriée à son rôle et est-il familier aux procédures de sécurité en vigueur au sein du PSC ?	
Q4	Vérifier par sondage (tâches sensibles et par sondage) que les procédures sont effectivement appliquées.	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 87	**Chapitre** : **CONTRÔLES DE SÉCURITÉ PHYSIQUE, CONTRÔLES DES PROCÉDURES, CONTRÔLES DU PERSONNEL**
	Titre : Contrôles du personnel
Origine : PC² 5.3.2	**Critère :** Procédures préalables de contrôle
ETSI : 7.4.3.i, f	

Exigences minimales pour le référentiel de sécurité du PSC :

- La procédure décrivant les modalités de l'enquête conduite auprès du personnel (appelé à remettre ou mettre en œuvre des conventions secrètes).
- La procédure d'embauche doit être adaptée en fonction de la sensibilité de chaque poste. La procédure doit être précisée, validée par la Direction Générale et appliquée pour toute embauche de chacune des composantes.

Contrôles :		**Réponses**
Q1	La procédure d'embauche est-elle adaptée en fonction de la sensibilité de chaque poste défini par l'analyse de risque de l'AC ?	
Q2	Vérifier par sondage (tâches sensibles et par sondage) que les procédures sont effectivement appliquées.	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 88	**Chapitre** : **CONTRÔLES DE SÉCURITÉ PHYSIQUE, CONTRÔLES DES PROCÉDURES, CONTRÔLES DU PERSONNEL**
	Titre : Contrôles du personnel
Origine : PC² 5.3.3	**Critère :** Exigences de formation initiale
ETSI : 7.4.3.d	

Exigences minimales pour le référentiel de sécurité du PSC :

- La procédure de vérification des compétences du personnel
- Les moyens de s'assurer de l'adéquation entre les compétences du personnel et le niveau de formation nécessaire.

Contrôles :	**Réponses**
Q1 La procédure de vérification des compétences du personnel est-elle formalisée, documentée et à jour ?	
Q2 Les nouveaux arrivants et les stagiaires reçoivent-ils une sensibilisation à la sécurité des systèmes d'information ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 89	**Chapitre** : **CONTRÔLES DE SÉCURITÉ PHYSIQUE, CONTRÔLES DES PROCÉDURES, CONTRÔLES DU PERSONNEL**
	Titre : Contrôles du personnel
Origine : PC² 5.3.4	**Critère :** Exigences et fréquence des formations
ETSI : 7.4.3.d	

Exigences minimales pour le référentiel de sécurité du PSC :

- Préciser le contenu et l'évolution des contenus des formations du personnel.

Contrôles :	**Réponses**
Formation initiale : couverte par la Fiche précédente **Formation permanente** : **Q1** Existe-t-il un plan de formation permettant aux personnels du PSC en poste d'avoir le niveau de compétence requis pour les tâches qu'ils réalisent ? **Q2** Le personnel participe-t-il régulièrement à des exercices (mise en œuvre des secours, alerte d'attaque d'intrusion,…) ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 90	**Chapitre** : **CONTRÔLES DE SÉCURITÉ PHYSIQUE, CONTRÔLES DES PROCÉDURES, CONTRÔLES DU PERSONNEL**
	Titre : Contrôles du personnel
Origine : PC² 5.3.5	**Critère :** Gestion des métiers
ETSI : 7.4.3. a, e, h	

Exigences minimales pour le référentiel de sécurité du PSC :

- Le PSC doit s'assurer que tout le personnel habilité à exercer une fonction de confiance le soit par un personnel de direction responsable de la sécurité.
- La clause de confidentialité peut être séparée ou rédigée comme une clause particulière du contrat d'embauche.

Contrôles :		**Réponses**
Q1	Les personnels exerçant une fonction de confiance sont-ils autorisés par un personnel identifié de la direction du PSC ou de ses entités ?	
Q2	Les personnels du PSC signent-ils une clause de confidentialité avec leur employeur?	
Q3	Vérifier la rédaction des clauses de confidentialité, s'assurer qu'elles sont limitées dans le temps et l'espace.	
Q4	Vérifier par sondage l'application effective de la procédure.	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 91	**Chapitre** : **CONTRÔLES DE SÉCURITÉ PHYSIQUE, CONTRÔLES DES PROCÉDURES, CONTRÔLES DU PERSONNEL**
	Titre : Contrôles du personnel
Origine : PC² 5.3.6	**Critère :** Sanctions pour des actions non autorisées

Exigences minimales pour le référentiel de sécurité du PSC :

- Pour chaque abus ou opération non-conforme (ex : manquement à la politique, aux règles et aux procédures de sécurité), les sanctions applicables, en s'assurant du respect avec la législation du travail.
- Les modalités de vérification de l'application rigoureuse des sanctions.

Contrôles :		**Réponses**
Q1	Le PSC a-t-il définit des actions en cas de non-respect ou de manquement à la politique, aux règles ou procédures de sécurité ?	
Q2	Sont-elles formalisées dans un document ?	
Q3	Ont-elles déjà été mises en œuvre ?	
Q4	La PSSI rappelle-t-elle les dispositions du règlement intérieur concernant les manquements aux règles de sécurité ?	
NON OBLIGATOIRE		

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 92	**Chapitre** : **CONTRÔLES DE SÉCURITÉ PHYSIQUE, CONTRÔLES DES PROCÉDURES, CONTRÔLES DU PERSONNEL**
	Titre : Contrôles du personnel
Origine : PC² 5.3.7	**Critère :** Contrôle du personnel contractant
ETSI : 7.5.i	

Exigences minimales pour le référentiel de sécurité du PSC :

- Des Cahiers de Prescriptions de Sécurité des Systèmes d'Information (CPSSI) doivent être systématiquement annexés aux contrats de sous-traitance ou de prestation de service.
- Les Cahiers de Prescriptions de Sécurité des Systèmes d'Information (CPSSI) doivent respecter des modèles établis pour chaque nature de prestation (ex. : développement de logiciel, exploitation de systèmes, mise à disposition de personnel,…)

Contrôles :	**Réponses**
Se faire communiquer le modèle de contrat type correspondant à chaque nature de prestation (développement de logiciel, exploitation de systèmes, mise à disposition de logiciel,…). **Q1** Vérifier que les contrats type incluent les clauses de sécurité requises et qu'ils renvoient à des CPSSI (ou équivalents) pour les modalités techniques.	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 93	**Chapitre** : **CONTRÔLES DE SÉCURITÉ PHYSIQUE, CONTRÔLES DES PROCÉDURES, CONTRÔLES DU PERSONNEL**
	Titre : Contrôles du personnel
Origine : PC² 5.3.8	**Critère :** Documentation fournie au personnel
ETSI : 7.4.1.c, 7.4.3.d	

Exigences minimales pour le référentiel de sécurité du PSC :

- Détailler les moyens mis en œuvre pour s'assurer que la documentation nécessaire au personnel est bien disponible.
- Si d'autres documents devaient être nécessaires au personnel, ils doivent être précisés dans la DPC.
- Les rôles et responsabilités de la personne en charge de la diffusion de la documentation.

Contrôles :		**Réponses**
Q1	Existe-t-il un système de gestion de la documentation à disposition du personnel ?	
Q2	La documentation à la disposition du personnel couvre-t-elle l'ensemble des activités et chaque agent y-a–t-il accès en fonction de son besoin d'en connaître ?	
Q3	La diffusion ou l'accès à la documentation sont-ils gérés en fonction du besoin d'en connaître ?	
Q4	Les versions et mises à jour successives de la documentation font-elles l'objet d'une gestion adaptée (gestion en configuration) ?	
Q5	Le suivi de la mise à jour de la documentation est-il confié à une personne bien désignée ?	
Q6	Se faire communiquer les éléments de suivi de la mise à jour et de la diffusion de la documentation. Apprécier s'ils respectent les engagements de la PC et les spécifications de la DPC.	
Q6	Les documents suivants sont-ils à la disposition du personnel (en fonction du besoin d'en connaître) : • DPC propre au domaine de certification • Documents constructeurs des matériels et logiciels utilisés • Politiques de certification supportée par la composante à laquelle il appartient • Procédures internes de fonctionnement	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 94	**Chapitre : CONTRÔLES TECHNIQUES DE SÉCURITÉ**
	Titre : Génération et installation de bi-clé
Origine : PC² 6.1.1	**Critère :** Génération de bi-clé de signataires
ETSI : 7.2.1.b, 7.2.8.a, b, c, d, 7.2.9.b	

Exigences minimales pour le référentiel de sécurité du PSC :

- Décrire le matériel cryptographique.
- Apporter des garanties quant à la conformité du matériel cryptographique au exigences de l'article 3.I du décret 2001-272 : certificat de conformité pour la fonction de génération des clés de signature.
- Rappeler les points concernant la génération de bi-clé.

Contrôles :		**Réponses**
Q1	Vérifier que le matériel cryptographique a reçu la certification de la DCSSI ou d'un organisme étranger désigné par un Etat membre de l'Union européenne.	
Q2	Les clés privée et publique sont-elles conservées de telles sorte à garantir leur confidentialité et leur intégrité avant d'être délivrées au signataire ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 95	**Chapitre** : **CONTRÔLES TECHNIQUES DE SÉCURITÉ**
	Titre : Génération et installation de bi-clé
Origine : PC² 6.1.1	**Critère :** Génération de bi-clé Initialisation d'une AC
ETSI : 7.2.1, 7.2.1.b	

Exigences minimales pour le référentiel de sécurité du PSC :

- Détailler la procédure de sécurité particulière permettant l'initialisation d'une AC.
- Apporter des garanties quant à la conformité du matériel cryptographique aux exigences de l'annexe de l'arrêté relatif à la qualification des PSC.

Contrôles :		**Réponses**
Q1	Vérifier que le matériel cryptographique a été certifié conforme par la DCSSI aux exigences de l'annexe de l'arrêté relatif à la qualification des PSC.	
Q2	Se faire communiquer les procédures d'initialisation de l'AC, de génération et d'enregistrement de clés. Vérifier qu'elles sont conformes aux exigences de la PC.	
Q3	Se faire communiquer la main courante et les procès verbaux correspondant aux séances de génération de clés et d'initialisation de l'AC. Vérifier qu'ils confirment le respect de la procédure et l'absence d'incident.	
Q4	En cas d'incident constaté lors d'une séance de génération de clés ou d'initialisation de l'AC, s'assurer que les éléments suspects ont été détruits.	
Q5	L'AC génère-t-elle ses propres clés privées dans un environnement physique sécurisé?	
Q7	La génération se fait-elle par un personnel de confiance, autorisé à effectuer cette opération, et au moins sous un double contrôle ?	
Q8	Les moyens et procédures permettent-ils de s'assurer qu'il y a unicité des clés privée et publique?	
Q9	Les moyens et procédures permettent-ils de garantir qu'il y a correspondance entre la clé privée et la clé publique portée dans le certificat ?	
Q10	L'initialisation de l'AC se déroule-t-elle sous le contrôle d'au moins un témoin externe au PSC (éventuellement tiers assermenté) ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 96	**Chapitre** : **CONTRÔLES TECHNIQUES DE SÉCURITÉ**
	Titre : Génération et installation de bi-clé
Origine : PC² 6.1.2	**Critère :** Soumission de clé privée à un signataire ou une composante
ETSI : 7.2.8.c, d, 7.2.9.b, d, note 2, 7.3.3.c	

Exigences minimales pour le référentiel de sécurité du PSC :

- Préciser les procédures de remise de clé privée.
- Spécifier les canaux de la soumission de clé protégés en confidentialité et en intégrité de bout en bout, par la description de ses méthodes.
- Préciser les moyens de stockage des clés avant leur remise à un signataire.

NB : La DPC ne doit pas livrer d'informations secrètes, c'est à dire directement exploitable pour une attaque contre le système.

Contrôles :		**Réponses**
Q1	Les moyens et procédures mis en place pour la délivrance des clés privées au signataire permettent-ils de garantir leur intégrité et confidentialité ?	
Q2	Les moyens et procédures mis en place permettent-ils de garantir que la clé privée n'est délivrée qu'au signataire concerné ?	
Q3	Les procédures et les moyens mis en oeuvre correspondent-ils aux exigences formulées dans la PC ?	
Q4	Vérifier par sondage que des procédures spécifiées sont effectivement appliquées (voir les comptes rendus, etc ...).	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 97	**Chapitre** : **CONTRÔLES TECHNIQUES DE SÉCURITÉ**
	Titre : Génération et installation de bi-clé
Origine : PC² 6.1.3	**Critère :** Délivrance de clé publique à une AC
ETSI : 7.2.3, a	

Exigences minimales pour le référentiel de sécurité du PSC :

- Lister les méthodes autorisées de remise de clé publique.
- Apporter des garanties quant à l'utilisation de canaux de délivrance de clé protégés en intégrité de bout en bout, par la description de ses méthodes.

Contrôles :		**Réponses**
Q1	La délivrance de la donnée de vérification de signature d'un signataire à l'AC s'effectue-t-elle de telle sorte à garantir l'intégrité de bout en bout et à en authentifier l'origine ?	
Q2	Les procédures et les moyens mis en oeuvre correspondent-ils aux exigences formulées dans la DPC ?	
Q3	Le signataire fournit-il la preuve de la possession de la clé privée à l'AC lors de l'enregistrement ?	
Q4	Vérifier par sondage que des procédures spécifiées sont effectivement appliquées (voir les comptes rendus, etc ...).	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 98	**Chapitre** : **CONTRÔLES TECHNIQUES DE SÉCURITÉ**
	Titre : Génération et installation de bi-clé
Origine : PC² 6.1.4	**Critère :** Délivrance de la clé publique d'une AC aux utilisateurs
ETSI : 7.2.3, a	

Exigences minimales pour le référentiel de sécurité du PSC :

- Préciser les moyens utilisés pour la protection en intégrité (de bout en bout) de la clé publique de l'AC à l'occasion de sa distribution à ses partenaires.

Contrôles :	**Réponses**
Q1 La délivrance de la clé publique de l'AC aux vérificateurs est-elle réalisée selon une méthode sécurisée en intégrité et permettant d'en authentifier l'origine ?	
Q2 Les procédures et moyens mis en oeuvre correspondent-ils aux exigences formulées dans la DPC ?	
Q3 Le certificat de l'AC ne pouvant être considéré à lui seul comme un élément de confiance, vérifier qu'il est soit : ➢ Signé par une autre autorité. ➢ Accompagné d'une déclaration signalant qu'il s'agit de la bonne clé publique. ➢ Procédé à la délivrance d'un condensat par une source de confiance.	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 99	**Chapitre** : **CONTRÔLES TECHNIQUES DE SÉCURITÉ**
	Titre : Génération et installation de bi-clé
Origine : PC² 6.1.5	**Critère :** Taille des clés
ETSI : 7.2.1 d notes 1 et 2, 7.2.8 a, b	

Exigences minimales pour le référentiel de sécurité du PSC :

- Préciser la longueur des clés utilisées.

Contrôles :	**Réponses**
Q1 L'algorithme et l'ensemble des paramètres cryptographiques connexes sont-ils au minimum conformes aux recommandations du guide de l'ETSI SR 002176 sur les algorithmes recommandés pour la signature électronique sécurisée et prennent-ils en compte le type d'application auquel ils sont destinés ?	
Q2 Les modules cryptographiques utilisés par l'AC ont-ils fait l'objet d'une analyse de leurs mécanismes cryptographiques lors de l'évaluation en vue de leur certification ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 100	**Chapitre** : **CONTRÔLES TECHNIQUES DE SÉCURITÉ**
	Titre : Génération et installation de bi-clé
Origine : PC² 6.1.7	**Critère :** Contrôle de la qualité des paramètres
ETSI : 7.2.1.c, d note 2, 7.2.8 a	

Exigences minimales pour le référentiel de sécurité du PSC :

- Préciser les standards reconnus de contrôle de qualité des paramètres cryptographiques et spécifier celui(ceux) qui est (sont) utilisé(s).

Contrôles :	**Réponses**
Q1 L'entité qui génère les clés respecte-t-elle les conditions de génération des clés de signature à l'aide d'un algorithme recommandé dans le guide de l'ETSI SR 002176 ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 101	**Chapitre** : **CONTRÔLES TECHNIQUES DE SÉCURITÉ**
	Titre : Génération et installation de bi-clé
Origine : PC² 6.1.8	**Critère :** Mode de génération de clé
ETSI : 7.2.1.b, c, 7.2.9 d note 3	

Exigences minimales pour le référentiel de sécurité du PSC :

- Décrire la ressource cryptographique.
- Apporter des garanties quant à la conformité des ressources cryptographiques.

Contrôles :		**Réponses**
Q1	Pour l'AC, le module cryptographique, dans lequel sont générées ses clés privée et publique, est-il conforme aux exigences de l'annexe de l'arrêté relatif à la qualification des PSC ?	
Q2	La procédure permettant de s'assurer que pour générer ses clés, le signataire utilise un module cryptographique certifié par la DCSSI ou par un organisme étranger désigné par un Etat membre de l'Union européenne est-elle formalisée, documentée et à jour ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 102	**Chapitre** : **CONTRÔLES TECHNIQUES DE SÉCURITÉ**
	Titre : Génération et installation de bi-clé
Origine : PC² 6.1.9	**Critère :** Usage de la clé
ETSI : 7.2.1 b Note 1, c, d note 2, 7.2.5.a, 7.2.8 a	

Exigences minimales pour le référentiel de sécurité du PSC :
Néant

Contrôles :	**Réponses**
Usage de la clé de signature de l'AC : **Q1** L'AC s'engage-t-elle sur le fait que ses clés privées ne peuvent être utilisées qu'à des fins de signature de certificat d'un signataire et de CRL ? **Usage de la clé de signature du signataire :** **Q1** Le signataire doit être informé que ses clés doivent être utilisées à des fins de signature et mises en œuvre à l'aide d'un SSCD évalué certifié conformément à la procédure SIG/P/01.1 .	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°:.103	**Chapitre** : **CONTRÔLES TECHNIQUES DE SÉCURITÉ**
	Titre : Protection de clé privée d'AC
Origine : PC² 6.2.2	**Critère :** Contrôle de clés privées d'AC par plusieurs personnes
ETSI : 7.2.2, a, 7.2.7.c	

Exigences minimales pour le référentiel de sécurité du PSC :

- Préciser les termes du contrôle des clés privées par plusieurs personnes.
- Apporter des garanties quant à l'application du contrôle des clés privées.
- Détailler les modalités du contrôle des clés privées par plusieurs personnes.

Contrôles :		**Réponses**
Q1	Les procédures de contrôle des clés font-elles appel à au moins deux personnes habilitées ?	
Q2	Y-a-t-il un contrôle des clés de n parmi m (avec n≥3) ?	
Q3	Quels sont les noms des personnes porteurs des parts de secret dans l'entreprise, vérifier la cohérence avec les procès verbaux et les tâches qu'ils réalisent ?	
Q4	Se faire communiquer les Procès Verbaux de chargement de clés de composantes du PSC au cours d'une période récente et vérifier : • Que les procédures spécifiées ont été respectées ? • Que les chargements de clé ont donnés lieu à un PV formel, approuvé par l'AC ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 104	**Chapitre** : **CONTRÔLES TECHNIQUES DE SÉCURITÉ**
	Titre : Protection de clé privée
Origine : PC² 6.2.3	**Critère :** Séquestre de clé privée
ETSI : 7.2.4, 7.2.7 c	

Exigences minimales pour le référentiel de sécurité du PSC :

Contrôles :	**Réponses**
Q1 Vérifier que les clés des signataires et des entités du PSC ne sont pas séquestrées par le PSC ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 105	**Chapitre** : **CONTRÔLES TECHNIQUES DE SÉCURITÉ**
	Titre : Protection de clé privée
Origine : PC² 6.2.4	**Critère :** Copie de secours de clé privée de l'AC
ETSI : 7.2.2.c, d, e7.2.7 c	

Exigences minimales pour le référentiel de sécurité du PSC :

- Préciser la méthode de sauvegarde applicable.
- Apporter des garanties permettant d'assurer que la copie de la clé privée de signature est conservée avec autant de garanties d'intégrité et de confidentialité que la clé privée originale.

Contrôles :		**Réponses**
Q1	La DPC apporte-t-elle les précisions requises quant aux conditions de conservation des clés privées ?	
Q2	Quel est le niveau de sécurité du dispositif qui conserve les copies de secours de la clé privée ?	
Q3	Ce niveau de sécurité est-il supérieur ou égal à celui des clés privées en cours d'utilisation ?	
Q4	Après la période de fin de validité, toutes les copies des clés privées de l'AC sont-elles détruites ou conservées de telle sorte à ne pas pouvoir être remises en usage ?	
Q5	Si l'AC, utilise un module cryptographique, pour copier ses clés privée et publique, est-il conforme aux exigences de l'annexe de l'arrêté du (A COMPLETER) ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 106	**Chapitre** : **CONTRÔLES TECHNIQUES DE SÉCURITÉ**
	Titre : Protection de clé privée
Origine : PC² 6.2.5	**Critère :** Archivage de clé privée
ETSI : 7.2.2.c, 7.2.7 c, 7.2.6 a	

Exigences minimales pour le référentiel de sécurité du PSC :

- Définir les méthodes d'archivage des clés privées de l'AC.

Contrôles :		**Réponses**
Q1	Les clés privées de l'AC sont-elles archivées de telle sorte qu'elles ne puissent plus être réutilisées qu'à des fins de preuve ?	
Q2	Le niveau de sécurité garanti pour les clés archivées est-il équivalent à la protection garantie pour les clés en cours d'utilisation ?	
Q3	Quand les clés de l'AC sont contenues dans une ressource matérielle dédiée, un contrôle d'accès existe-t-il pour rendre les clés inaccessibles en dehors du module ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 107	**Chapitre** : **CONTRÔLES TECHNIQUES DE SÉCURITÉ**
	Titre : Protection de clé privée
Origine : PC² 6.2.6	**Critère :** Mise à la clé du module cryptographique du signataire et de l'AC
ETSI : 7.2.2.b, 7.2.9.a, c	

Exigences minimales pour le référentiel de sécurité du PSC :

- La méthode de mise à la clé de la ressource cryptographique doit être détaillée si elle n'est pas confidentielle.

Contrôles :	**Réponses**
Q1 Se faire communiquer la(les) procédure(s) de mise à la clé de la ressource cryptographique.	
Q2 La procédure de mise à la clé de la ressource cryptographique, prévoit-elle, qu'en cas d'incident lors de la mise à la clé, les éléments suspects ne sont pas été utilisés en phase opérationnelle ?	
Q6 Lorsque la clé privée de l'AC est en dehors du dispositif de création de signature de l'AC, est-elle chiffrée à l'aide d'un algorithme et d'une taille de clé, conformes aux recommandations du guide de l'ETSI SR 002176 ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 108	**Chapitre** : **CONTRÔLES TECHNIQUES DE SÉCURITÉ**
	Titre : Protection de clé privée
Origine : PC² 6.2.7	**Critère :** Méthode d'activation de clé privée
ETSI : 7.2.1.a, b, 7.2.7. c	

Exigences minimales pour le référentiel de sécurité du PSC :

- Préciser la liste des méthodes d'activation des clés ou les inclure en annexe.
- Apporter des garanties quant à l'utilisation d'une ou plusieurs méthodes d'activation des clés éprouvée.

Contrôles :		**Réponses**
Q1	La procédure d'activation des clés est-elle conforme à la DPC ?	
Q2	Se faire communiquer les rapports relatifs à la dernière activation des clés, et s'assurer du respect de la procédure.	
Q3	La mise en œuvre des clés est-elle toujours réalisée par au moins deux personnes ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 109	**Chapitre** : **CONTRÔLES TECHNIQUES DE SÉCURITÉ**
	Titre : Protection de clé privée
Origine : PC² 6.2.8	**Critère :** Méthode de désactivation de clé privée
ETSI : 7.2.7	

Exigences minimales pour le référentiel de sécurité du PSC :

- Préciser la période d'inactivité au bout de laquelle la clé est désactivée.
- Décrire les cas particuliers de désactivation de la clé privée dans le module cryptographique.
- Préciser la ou les méthodes éprouvée(s) de désactivation de la clé privée utilisée(s).

Contrôles :		**Réponses**
Q1	La procédure de désactivation de la clé privée est-elle formalisée, documentée et à jour ?	
Q2	Après sa désactivation, le module cryptographique est-il conservé dans un lieu protégé ?	
Q3	La désactivation de la clé privée s'effectue-t-elle à la déconnexion de l'utilisateur ou après une certaine période d'inactivité ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 110	**Chapitre** : **CONTRÔLES TECHNIQUES DE SÉCURITÉ**
	Titre : Protection de clé privée
Origine : PC² 6.2.9	**Critère :** Méthode de destruction de clé privée
ETSI : 7.2.6.a, 7.2.7.c, e, 7.2.9.c	

Exigences minimales pour le référentiel de sécurité du PSC :

- Préciser la ou les méthodes de destruction de la clé privée qui est(sont) utilisée(s).

Contrôles :		**Réponses**
Q1	La procédure de destruction des clés privées et des supports associés prévoit-elle leur destruction physique, assortie d'un PV de destruction signé par au moins deux témoins ?	
Q2	Ce traitement rend-il leur réutilisation impossible ?	
Q3	La personne responsable de ce traitement est-elle clairement identifiée ?	
Q4	Se faire communiquer des PV de destruction récents (s'il y en a). La procédure est-elle correctement appliquée ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 111	**Chapitre** : **CONTRÔLES TECHNIQUES DE SÉCURITÉ**
	Titre : Autres aspects de la gestion des bi-clés
Origine : PC² 6.3.1	**Critère :** Archivage des clés publiques
ETSI : 7.4.11	

Exigences minimales pour le référentiel de sécurité du PSC :

- Préciser les procédures et méthodes d'archivage utilisées pour les certificats.

Contrôles :		**Réponses**
Q1	Les procédures de destruction des archives des clés publiques sont-elles conformes à leur niveau de sensibilité / classification ?	
Q2	Vérifier par sondage la durée de conservation des archives des clés publiques, est-elle conforme à la DPC ?	
Q3	Se faire communiquer et vérifier par sondage des PV de destruction d'archives des clés publiques, sont-ils conformes ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 112	**Chapitre** : **CONTRÔLES TECHNIQUES DE SÉCURITÉ**
	Titre : Données d'activation
Origine : PC² 6.4.1 **ETSI :** 7.2.2 a, 7.2.9.d, note2	**Critère :** Génération et installation des données d'activation de l'AC et du signataire

Exigences minimales pour le référentiel de sécurité du PSC :

- Lister les méthodes existantes pour la génération et l'installation des clés.
- Préciser la ou les méthodes utilisée(s) pour la génération et l'installation des clés

Contrôles :	**Réponses**
Q1 La procédure pour la génération et l'installation des données d'activation est-elle conforme à la DPC ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 113	**Chapitre** : **CONTRÔLES TECHNIQUES DE SÉCURITÉ**
	Titre : Données d'activation
Origine : PC² 6.4.2	**Critère :** Protection des données d'activation de l'AC et du signataire
ETSI : 7.2.2 a, 7.2.9.d	

Exigences minimales pour le référentiel de sécurité du PSC :

- Préciser le niveau de protection en confidentialité et en intégrité dont bénéficient les données d'activation sans pour autant divulguer les matériels et méthodes utilisé à ces fins.

Contrôles :		**Réponses**
Q1	Les moyens de protection mis en œuvre pour les données d'activation sont-ils conforme à la DPC ?	
Q2	Les moyens de protection spécifiés pour les données d'activation permettent-ils de garantir un niveau de protection suffisant en confidentialité et en intégrité ?	
Q3	Lorsque l'AC génère la donnée d'activation du signataire, la protège-t-elle en confidentialité et en intégrité jusqu'à sa distribution au signataire ?	
Q4	Le signataire est-il informé des mesures à prendre pour protéger ses données d'activation ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 114	**Chapitre** : **CONTRÔLES TECHNIQUES DE SÉCURITÉ**
	Titre : Données d'activation
Origine : PC² 6.4.3	**Critère :** Autres aspects concernant les données d'activation de l'AC et du signataire

Exigences minimales pour le référentiel de sécurité du PSC :

- Préciser le type de logiciel utilisé permettant de contrôler la consistance des mots de passe (avec des exemples) ainsi que ceux permettant la génération de mots de passe.
- Les mécanismes bloquant le module après plusieurs tentatives infructueuses de connexion doivent rester confidentiels.

Contrôles :	**Réponses**
Q1 Les règles de composition et de gestion des mots de passe nécessaires à l'activation des modules cryptographiques sont-ils conformes à la DPC ?	
Q2 Les moyens utilisés pour contrôler la composition et la robustesse des mots de passe nécessaires à l'activation des modules cryptographiques sont-ils conformes à la DPC?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 115	**Chapitre** : **CONTRÔLES TECHNIQUES DE SÉCURITÉ**
	Titre : Contrôles de la sécurité des postes de travail
Origine : PC² 6.5.1 **ETSI :** 7.4.5.a, b, 7.4.6.c, d, e, f, g, 7.4.11. note 2, f	**Critère :** Besoins de sécurité spécifiques sur les postes de travail des entités du PSC

Exigences minimales pour le référentiel de sécurité du PSC :

- La méthode de gestion en configuration des systèmes informatiques
- La gestion des mots de passe
- La fréquence de renouvellement des logiciels de protection (anti-virus, scanners, etc..)

Contrôles :		**Réponses**
Q1	Existe-t-il une procédure définissant les moyens de composition et de gestion des mots de passe ?	
Q2	La procédure de mise à jour des logiciels de protection est-elle formalisée, documentée et à jour ?	
Q3	La procédure de contrôle des postes de travail du PSC est-elle formalisée, documentée et à jour ?	
Q4	Les accès aux fonctions d'information et aux applications du système sont-ils effectivement restreints conformément à la politique de contrôle d'accès ?	
Q5	Vérifier que les mesures de sécurité suivantes sont mises en œuvre : • Journalisation (imputabilité et nature des actions effectuées) des évènements en fonction des rôles et des opérations • Gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'utilisateur). • Gestion des comptes des utilisateurs, notamment la modification et la suppression rapides des droits d'accès • Identification et authentification des utilisateurs du poste de travail • Protection contre les virus informatiques et toutes formes de logiciels compromettant ou non-autorisé et mise à jour des logiciels • Protection des supports d'informations contre les dommages, le vol et la compromission même par réutilisation et l'usurpation • Filtrage des entrées/sorties réseau • Mise en gestion de la configuration du système d'information	
Q6	La mise en œuvre des programmes utilitaires du système est-elle restreinte et strictement contrôlée ?	
Q7	Vérifier par sondage la bonne administration des postes de travail.	
Q8	Les équipements de développement et de test sont-ils séparés des équipements de production ?	
Q9	Les équipements identifiés comme sensibles, par les fonctions et les applications qu'ils mettent en œuvre, sont-ils isolés des autres postes de travail ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°:.116	**Chapitre** : **CONTRÔLES TECHNIQUES DE SÉCURITÉ**
	Titre : Contrôles de la sécurité des postes de travail
Origine : PC² 6.5.2	**Critère :** Niveau de sécurité du poste de travail des entités du PSC
ETSI : 7.4.7	

Exigences minimales pour le référentiel de sécurité du PSC :

- Un niveau minimal d'assurance dans la sécurité offerte doit être défini concernant le traitement des informations sensibles.
- Les composantes du PSC doivent justifier leurs choix quant aux systèmes informatiques utilisés (robustesse, fiabilité, sécurité, etc..)

Contrôles :		**Réponses**
Q1	Les systèmes informatiques utilisés dans le cadre du PSC sont-ils des systèmes répondant aux objectifs de l'analyse de risque ? (S'assurer que la DPC fournit des éléments suffisants pour le garantir).	
Q2	Des procédures d'installation des postes de travail prenant en compte les aspects sécurité sont-elles formalisées, documentées et à jour ?	
Q3	Des procédures d'utilisation des postes de travail prenant en compte les aspects sécurité sont-elles formalisées, documentées et à jour ?	
Q4	Le cas échéant, réaliser des tests pour s'assurer que les systèmes informatiques opérationnels sont conformes aux spécifications (vérification des paramétrages, etc.).	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 117	**Chapitre** : **CONTRÔLES TECHNIQUES DE SÉCURITÉ**
	Titre : Contrôles techniques du système durant son cycle de vie
Origine : PC² 6.6.1	**Critère :** Contrôles des développements des systèmes
ETSI : 7.4.7.a	

Exigences minimales pour le référentiel de sécurité du PSC :

- Fournir la référence de la procédure à mettre en œuvre lorsqu'un système doit évoluer.
- Elle doit identifier la méthode utilisée pour spécifier et développer le système notamment les étapes normales (expression des besoins, spécification des exigences fonctionnelles, spécifications techniques, développement, tests, recettes formelles). Toutes ces étapes doivent être détaillées.

Contrôles :		**Réponses**
Q1	Une analyse de risque est-elle menée avant tout développement de système de façon à prendre en considération les objectifs de sécurité dès la phase de spécification ?	
Q2	L'AC s'assure-t-elle que chacune de ses entités satisfait aux exigences de sécurité correspondantes en utilisant, par exemple, des systèmes et/ou des matériels conformes à un ou plusieurs profils de protection appropriés, définis dans le cadre de la norme ISO 15408 ou une norme équivalente ?	
Q3	Les procédures prévoient-elles que tout développement et toute évolution significative d'une application sur les systèmes opérationnels fassent l'objet d'une recette ?	
Q4	Vérifier, sur des projets récents et significatifs, l'application des règles ci-dessus et contrôler les documents produits (existence et qualité).	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 118	**Chapitre** : **CONTRÔLES TECHNIQUES DE SÉCURITÉ**
	Titre : Contrôles techniques du système durant son cycle de vie
Origine : PC² 6.6.2	**Critère :** Contrôles de la gestion de la sécurité
ETSI : 7.2.7.a, b, d, 7.4.1.d, 7.4.5.f, 7.4.7.b	

Exigences minimales pour le référentiel de sécurité du PSC :

- Toute évolution majeure du système doit faire l'objet d'une autorisation de l'AC.
- La procédure à mettre en œuvre lorsqu'un produit ou un système doit évoluer.

Contrôles :	**Réponses**
Q1 Les procédures prévoient-elles que tout développement et toute évolution significative d'une application sur les systèmes opérationnels fasse l'objet d'une recette et d'une acceptation formelle ?	
Q2 S'assurer que : • Des procédures de contrôle portant sur les modifications (mise à jour, correction, patch,…) existent et soient formalisées, documentées et à jour. • La sécurité du dispositif matériel n'est pas altérée par un tiers ou de toute autre manière lors de son transport. • La sécurité du dispositif matériel n'est pas altérée par un tiers ou de toute autre manière pendant la durée de son utilisation ou de sa conservation éventuelle. • La capacité de traitements et de stockage répond au besoin des signataires.	
Q3 Ces procédures permettent-elles des évolutions pour lesquelles le PSC reste opérationnel en permanence ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 119	**Chapitre** : **CONTRÔLES TECHNIQUES DE SÉCURITÉ**
	Titre : Contrôles de sécurité réseau
Origine : PC² 6.7	**Critère :** néant
ETSI : 7.4.6.a, note 1, b et h	

Exigences minimales pour le référentiel de sécurité du PSC :

- Justifier les choix de configuration des passerelles selon les applications et les systèmes installés.
- Ces configurations doivent rester strictement confidentielles.

Contrôles :		**Réponses**
Q1	Les moyens de protection des interconnexions vers des réseaux publics sont-ils conformes aux spécifications de la DPC ?	
Q2	Les moyens utilisés offrent-ils la qualité, la robustesse et la fiabilité suffisante ?	
Q3	Le PSC protège-t-il ses systèmes informatiques et ses données contre les virus, les chevaux de Troie et les autres formes de logiciels pernicieux ou non autorisés ?	
Q4	Cette protection s'étend-elle à l'ensemble de ses systèmes informatiques ?	
Q5	Le PSC protège-t-il les données sensibles, notamment les informations liées à l'enregistrement du signataire, lorsqu'elles sont communiquées par le biais d'un réseau non sécurisé ?	
Q6	Existe-t-il des procédures formalisées, documentées et à jour de rapport d'incidents ?	
Q7	Existe-t-il des procédures formalisées, documentées et à jour de réponse aux incidents ?	
Q8	La configuration des composants du réseau locale fait-elle l'objet d'audits réguliers par le contrôleur ?	
Q9	Y–a-t-il un suivi de la montée en charge et un maintien du système à niveau ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 120	**Chapitre : PROFILS DES CERTIFICATS ET CRL**
	Titre : Profil du certificat qualifié
Origine : PC² 7.1	**Critère** : néant
ETSI : 7.3.3.a	

Exigences minimales pour le référentiel de sécurité du PSC :

- Les champs de base définis dans la recommandation X.509 v3 spécifiés dans le document ETSI TS 101 862 "Qualified certificate profile" et l'article 6.2 du décret 2001-272.

Contrôles :		**Réponses**
Q1	Les formats des certificats spécifiés dans la PC et la DPC sont-ils conformes aux champs de base définis dans la recommandation X.509 v3 spécifiés dans le document ETSI TS 101 862 et dans l'article 6.2 du décret 2001-272 ?	
Q2	S'assurer (par sondage) que les certificats émis respectent les spécifications de la norme.	
Q3	Les limites fixées à l'utilisation du certificat ou la valeur des transactions pour lesquelles il peut être utilisé figurent-elles dans le certificat ?	
Q4	Est-ce que le certificat porte une mention relative à la qualification ?	
Q5	L'OID inclut dans les certificats fait-il référence à la PC de l'AC qui gère ce certificat ?	
Q6	Le PSC permet-il au signataire de choisir pour le champ KeyUsage du certificat entre "signature" et "non-répudiation" ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 121	**Chapitre** : **PROFILS DES CERTIFICATS ET CRL**
	Titre : Profil des CRLs
Origine : PC² 7.2.1	**Critère :** Néant
ETSI : 7.3.3.a	

Exigences minimales pour le référentiel de sécurité du PSC :

- Rappeler les éléments de la version 2 du format des CRL ou l'inclure en annexe.

Contrôles :	**Réponses**
Q1 Si les CRL et delta-CRL sont utilisés : • L'heure prévue de la prochaine CRL est-elle indiquée ? • Les publication de la CRL suivante sont-elles faites avant l'heure limite ? • La CRL est-elle signée par l'AC ou une autorité désignée par l'AC ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 122	**Chapitre : ADMINISTRATION DES SPÉCIFICATIONS**
	Titre : Procédures de modification de ces spécifications
Origine : PC² 8.1	**Critère** : Néant
ETSI : 7.1.h, 7.4.1.d	

Exigences minimales pour le référentiel de sécurité du PSC :

- Les procédures d'approbation par l'AC d'une modification de spécifications d'un certificat.
- Spécifier les procédures et moyens de communication avec les entités du PSC.

Contrôles :		**Réponses**
Q1	Les procédures d'approbation par l'AC sont-elles conformes à la DPC ?	
Q2	Les procédures de communication pour prévenir les entités du PSC ainsi que les signataires et les vérificateurs, de même que les PSC avec lesquels des accords de reconnaissance ont été conclus, (dans la mesure où ces modifications peuvent affecter ces accords ou le niveau de sécurité offert par le PSC) sont-elles formalisées, documentées et à jour ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 123	**Chapitre** : **ADMINISTRATION DES SPÉCIFICATIONS**
	Titre : Politiques de publication et de notification
Origine : PC² 8.2	**Critère** : Néant
ETSI : 7.1.c, d et note 2	

Exigences minimales pour le référentiel de sécurité du PSC :

- Décrire le processus de publication et de notification par l'AC.

Contrôles :		**Réponses**
Q1	Les procédures de diffusion des informations provenant de la PC et de la DPC aux personnels sont-elles formalisées, documentées et mises à jour ?	
Q2	Les procédures de diffusion des éléments de sa DPC aux signataires et aux vérificateurs sont-elles formalisées, documentées et mises à jour ?	
Q3	La publication des documents devant être publiés concernant le PSC est-elle mise à jour suite à toute modification ?	
Q4	Le PSC a-t-il mis en place un processus de gestion de la documentation ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

Fiche n°: 124	**Chapitre** : **ADMINISTRATION DES SPÉCIFICATIONS**
	Titre : Procédures d'approbation des DPC
Origine : PC² 8.3	**Critère** : Néant
ETSI : 7.1.e, f	

Exigences minimales pour le référentiel de sécurité du PSC :

- Décrire le processus formel d'approbation de la DPC par le responsable identifié par la Direction de l'AC.

Contrôles :	**Réponses**
Q1 Le processus d'approbation de la DPC est-il documenté et à jour ?	
Q2 Ce processus fait-il appel à un responsable identifié au sein de la direction du PSC pour l'approbation de la DPC et de sa mise en œuvre ?	

Justification des réponses négatives :

Solutions envisagées ou proposées :

ANNEXES

Glossaire

Accord entre domaines
Accord portant sur les échanges entre deux domaines distincts. Les termes de l'accord portent sur l'interopérabilité des IGC et des applications communicantes.

Accord de reconnaissance entre IGC
Accord par lequel une IGC d'un domaine reconnaît la totalité ou une partie préalablement identifiée des certificats d'un autre domaine.

Accréditation
Autorisation et approbation délivrées par une instance désignée par arrêté du ministre chargé de l'industrie à une organisation ou à un individu, et permettant à ceux-ci de réaliser une évaluation en vue de la qualification des PSC.

Autorité Administrative (AA)
Autorité responsable de l'IGC et possédant un pouvoir décisionnaire au sein de l'IGC. Elle est garante de l'application de la politique de sécurité du domaine d'application qui régit l'IGC. Cette politique de sécurité englobe la ou les politiques de certification des IGC du domaine d'application. Elle valide les pratiques de certification respectées par les différentes composantes de l'IGC : AC, AE, SP, OC. Elle peut éventuellement être confondue avec l'AC.

Autorité de certification (AC)
Autorité chargée par un ou plusieurs utilisateurs de créer et d'attribuer les certificats. Cette autorité peut, facultativement, créer les clés d'utilisateur. [9594-8]
L'AC est l'entité responsable du PSC. Elle peut sous-traiter uen partie de ses activités à d'autres entités du PSC.
Elle peut demander à être qualifiée.

Autorité de certification racine (ACR)
Autorité de certification (AC) prise comme référence par une communauté d'utilisateurs et les AC d'une IGC. Elle est un élément essentiel de la confiance qui peut être accordée à l'IGC dans un contexte donné.

Autorité compétente
Responsable hiérarchique du signataire ou du correspondant local de sécurité du domaine d'application.

Autorité d'Enregistrement (AE)
Entité dont le but est de soutenir localement un ensemble d'entités d'extrémités physiquement éloignées de l'autorité de certification à laquelle elles sont subordonnées. Une autorité d'enregistrement remplit en partie des fonctions de l'administrateur de l'autorité de certification directement responsable d'un ensemble d'entités d'extrémité subordonnées. Ces fonctions comprennent :
l'enregistrement, l'annulation de l'enregistrement et la modification des attributs des entités d'extrémité subordonnées ;
l'autorisation des demandes de récupération des certificats ;
l'approbation et l'autorisation des demandes de révocation de certificats ;
la remise physique des jetons individuels au personnel autorisé à les détenir ;
l'enregistrement, l'annulation de l'enregistrement et l'attribution de privilèges au personnel de l'autorité d'enregistrement locale.

Une autorité d'enregistrement n'est généralement pas habilitée à émettre des certificats ou des liste des certificats révoqués ni à connaître les clés privées des entités d'extrémité.

L'expression générique « autorité d'enregistrement » peut être modifiée pour les IGC individuelles (par exemple autorité locale d'enregistrement, autorité d'enregistrement d'organisation) et chacune de ces IGC peut mettre en œuvre un ensemble modifié des fonctions décrites ci-dessus.

Autorité Responsable d'Application (ARA)

L'autorité responsable d'application est responsable du domaine d'application. La garantie de l'autorité responsable d'application vis à vis des signataires et des utilisateurs de certificats par rapport à l'application concernée vient de la qualité de la technologie mise en œuvre et du cadre réglementaire et contractuel qu'elle définit dans une politique régissant l'application et qu'elle s'engage à respecter. L'élaboration et la mise en œuvre de la politique de sécurité, qui est un volet de la politique régissant l'application, du domaine d'application est confié à l'autorité administrative. Elle délègue la responsabilité de l'authentification des utilisateurs finaux à l'autorité administrative (AA).

Bi-clé

Un bi-clé est un couple composé d'une clé privée (devant être conservée secrète) et d'une clé publique, nécessaire à la mise en œuvre d'une prestation de cryptologie basée sur des algorithmes asymétriques. Quatre types de bi-clés interviennent dans une infrastructure de gestion de clés :
Les bi-clés d'intégrité, dont la clé privée est utilisée à des fins de contrôle d'accès, de non-répudiation et de signature et la clé publique à des fins de vérification,
les bi-clés de certification, sont nécessaires au fonctionnement d'une IGC ;
les bi-clés de confidentialité, grâce auxquels des messages ou des données sont protégés en confidentialité ;
les bi-clés d'échange de clés qui permettent de transporter les clés (symétriques ou asymétriques).

Centre d'élaboration de clés (CEC)

Plate-forme technique offrant des services de génération de clés et paramètres cryptographiques pour le compte de signataires ou de composantes de l'IGC.

Certificat

Clé publique d'un utilisateur, ainsi que certaines autres informations rendues infalsifiables par chiffrement avec la clé privée d'une autorité de certification (AC) qui l'a délivré. [9594-8]
Un certificat contient des informations telles que :

- l'identité du porteur de certificat,
- la clé publique du porteur de certificat,
- la durée de vie du certificat,
- l'identité de l'autorité de certification qui l'a émis,
- la signature de l'AC qui l'a émis.

Un format standard de certificat est normalisé dans la recommandation X509 v3[3].

Certificat d'AC

Certificat d'une autorité de certification fournit par une autre autorité de certification. [9594-8]

Certificat auto-signé

Certificat d'une autorité de certification signé par cette même autorité de certification. [RFC 2459]

Certificat électronique qualifié

Un certificat électronique répondant aux exigences définies à l'article 6 du [D2001-272].

Certificat feuille

Certificat terminal du chemin de certification (opposé au certificat de l'AC racine).

Chaîne de certification

Voir Chemin de certification.

Chemin de certification

Suite ordonnée de certificats liés les uns aux autres.

Généralement, le chemin relie un certificat feuille à un certificat auto-signé.

Clé publique
Clé composante d'un bi-clé asymétrique d'une entité qui peut être rendue publique. [ISO/IEC 9798-1]

Clé privée
Clé composante d'un bi-clé asymétrique d'une entité qui doit uniquement être utilisée par cette entité. [ISO/IEC 9798-1]

Composante
Plate-forme constituée d'au moins un poste informatique, une application, un moyen de cryptologie et jouant un rôle déterminé au sein de l'IGC. Une composante peut être l'autorité de certification (AC), une autorité d'enregistrement (AE), etc.

Contremarque de temps
Ensemble de données qui associe une représentation d'une donnée à un instant particulier, dans le but d'établir une preuve indiquant une date à laquelle la donnée existait.

Contrôle de conformité
Action qui consiste à réaliser un examen le plus exhaustif possible afin de vérifier l'application et le maintient des Déclarations des Pratiques de Certification et de la réglementation au sein d'un organisme conformément aux Politiques de Certification mises en œuvre par l'autorité de certification (AC).

Croisement de certificat
Action de reconnaître et garantir les certificats émis par une autre IGC. Le croisement de certificat consiste aujourd'hui à certifier la clé publique de l'autorité de certification (AC), appartenant à l'autre IGC.

Condensat, Condensé
Voir haché.

Déclaration des Pratiques de Certification (DPC)
Déclaration des pratiques mises en œuvre par une autorité de certification pour émettre et gérer des certificats. [RFC 2527]
Il peut comporter des parties confidentielles.

Délivrance de clé privée
Dans le cas où un centre de génération de clés est utilisé pour la génération du bi-clé de confidentialité d'un signataire, la remise de la clé privée à son porteur doit être protégée en intégrité et en confidentialité.

Domaine
Groupe d'entités assujetties à la même politique de sécurité et relevant d'une même autorité chargée de mettre en œuvre cette politique.

Domaine d'application
Ensemble constitué de personnels, de systèmes d'information (IGC, applications, réseaux,…) et de moyens. Par exemple : ministère, direction d'un ministère, sociétés, opérateurs de certification.

Domaine de certification
Périmètre d'application de la politique de certification de l'IGC.

Données d'activation
Données privées associées à un signataire permettant de mettre en œuvre sa clé privée.

Données de création de signature électronique
Les éléments propres au signataire, tels que des clés cryptographiques privées, utilisés par lui pour créer une signature électronique. [D2001-272]

Données de vérification de signature électronique
Les éléments, tels que des clés cryptographiques publiques, utilisés pour vérifier la signature électronique. [D2001-272]

Données d'identifications personnelles
Informations relatives à une personne et permettant de connaître avec précision et sans ambiguïté son identité.

Dispositif de vérification de signature électronique
Un matériel ou un logiciel destiné à mettre en application les données de vérification de signature électronique. [D2001-272]

Dispositif de création de signature électronique
Un matériel ou un logiciel destiné à mettre en application les données de création de signature électronique. [D2001-272]

Dispositif sécurisé de création de signature électronique
Un dispositif de création de signature électronique qui satisfait aux exigences définies au I de l'article 3 du [D2001-272].

Édition d'un gabarit de certificat
Opération effectuée par une autorité d'enregistrement (AE) et qui consiste à rassembler un ensemble d'informations publiques sur une entité (son nom, la valeur de sa clé publique, l'algorithme asymétrique mis en œuvre, etc.) ainsi que des données propres au type du certificat désiré (politique de certification, nom de l'autorité de certification). Cette action est le résultat de l'acte d'enregistrement d'un demandeur auprès de l'AE.

Émission d'un certificat
Délivrance par une AC d'un certificat à un signataire ou à une composante de l'IGC.

Enregistrement
Action qui consiste pour une autorité d'enregistrement à renseigner le profil d'un demandeur de certificat et à en vérifier la véracité, conformément à une politique de certification.

Entité
Utilisateur, processus ou système faisant partie de l'infrastructure de gestion des clés ou de l'application utilisateur. Les exemples donnés ici comprennent les systèmes et applications d'extrémité (désignés comme entités d'extrémité) et des composantes de l'infrastructure comme les autorités de certification et les autorités d'enregistrement.

Exploitant
Personne travaillant pour le compte de l'IGC et disposant de droits d'accès à une autorité associés aux rôles qui lui sont attribués.

Génération d'un certificat
Processus de création d'un certificat à partir d'éléments spécifiques à l'application et au signataire. Action réalisée au moyen d'une signature du certificat par une autorité de certification (AC).

Haché, condensat, condensé
Résultat d'une fonction de hachage à sens unique (on ne peut pas revenir au message initial), c'est-à-dire d'une fonction calculant une empreinte d'un message de telle sorte qu'une modification même infime du message entraîne la modification de l'empreinte.

Infrastructure de gestion de clés (IGC)
Ensemble organisé de composantes fournissant des services de gestion des clés cryptographiques et de certificats de clés publiques au profit d'une communauté d'utilisateurs (signataires, vérificateurs…).

Interopérabilité
Capacité de deux IGC à constituer un domaine de confiance partagée.

Journalisation
Fait d'enregistrer dans un fichier dédié à cet effet certains types d'événements provenant d'une application ou du système d'exploitation d'un poste informatique. Le fichier résultant rend possible la traçabilité et l'imputabilité des opérations effectuées.

Liste des Certificats Révoqués (CRL)
Liste contenant les identifiants des certificats révoqués ou invalides. Lors d'une révocation, l'AC ajoute l'identifiant du certificat à révoquer dans la CRL, la signe et la transmet au service de publication. Il appartient à l'utilisateur qui souhaite connaître l'état d'un certificat de vérifier la présence de l'identifiant correspondant dans la liste.

Liste des Autorités de certification Révoquées (ARL)
Une ARL est une CRL qui ne contient que des identifiants de certificats d'AC révoqués et pas de certificats feuilles.

Opérateur de Certification (OC)
L'opérateur de certification assure les prestations techniques pour le compte de l'AC. La responsabilité de l'OC est d'exécuter les actions demandées par l'AE et de répondre aux exigences définies par l'AC. Sa responsabilité se limite au respect des procédures établies dans la DPC.

Opérateur de prestation d'externalisation (OPE)
L'OPE assure des prestations techniques, entre autre cryptographiques, nécessaires au processus de gestion de certificat (enregistrement, certification, révocation, publication,…) conformément à une PC. Dans le cas de l'AC, l'OPE est un OC.
Sa responsabilité se limite au respect des procédures établies dans la DPC.

Paramètres de clés publiques
Données publiques relatives à la mise en œuvre de l'algorithme asymétrique de cryptographie.

Politique de certification (PC)
Ensemble de règles, identifié par un nom, relatives à l'applicabilité d'un certificat à une communauté particulière et/ou à une classe d'applications ayant des besoins de sécurité communs. [9594-8]

Prestataire de service de certification (PSC)
Toute personne ou entité qui délivre des certificats au public ou lui fournit d'autres services liés aux signatures électroniques.
C'est une IGC qui délivre des certificats, elle peut être composée d'une AC, d'une AE et d'un SP.

Publication d'un certificat
Fait de rendre disponible un certificat via un média (par ex. annuaire, serveur d'information, support amovible,…)

Qualification des prestataires de services de certification électronique
L'acte par lequel un tiers, dit organisme de qualification, atteste qu'un prestataire de services de certification électronique fournit des prestations conformes à des exigences particulières de qualité. [D2001-272]

La qualification vaut présomption de conformité aux exigences de l'article 6 du décret 2001-272.

Rapport facial
Action de se présenter en personne auprès d'une composante de l'IGC dans le but de prouver son identité ou son accord.

Renouvellement de certificat
Action effectuée à la demande d'un signataire et en fin de période de validité d'un certificat et qui consiste à générer un nouveau certificat pour un porteur. La re-génération de certificat après révocation n'est pas un renouvellement.

Révocation de certificat
Processus consistant à indiquer qu'un certificat est devenu invalide. Cette action peut être la conséquence de différents types d'événements tels que le changement de nom de l'entité, le changement de l'association entre l'entité et l'AC, la compromission ou la suspicion de compromission de la clé privée.
Action demandée par une AC, une AE, le porteur de certificat ou son AA.

Service de publication
Le service de publication rend disponible les certificats de clés publiques émis par une AC, à l'ensemble des utilisateurs potentiels de ces certificats. Il publie une liste de certificats reconnus comme valides et une liste de certificats révoqués (CRL). Ce service peut être rendu par un annuaire (par exemple, de type X500), un serveur d'information (Web), une délivrance de la main à la main, une application de messagerie, etc.

Signataire
Toute personne physique, agissant pour son propre compte ou pour celui de la personne physique ou morale qu'elle représente, qui met en oeuvre un dispositif de création de signature électronique. [D2001-272]
Le signataire est appelé demandeur de certificat lorsqu'il effectue une demande de certificat auprès d'une AE. Il est appelé porteur de certificat dès l'instant où il dispose d'un certificat émis par l'IGC. Un signataire ne peut émettre de certificat pour le compte d'autrui.

Signature électronique
Une donnée qui résulte de l'usage d'un procédé répondant aux conditions définies à la première phrase du second alinéa de l'article 1316-4 du code civil : « Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. ». [D2001-272]

Signature électronique sécurisée
Une signature électronique qui satisfait, en outre, aux exigences suivantes :
- être propre au signataire ;
- être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ;
- garantir avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable. [D2001-272]

Suspension de certificat
Action demandée par une AC, une AE, le porteur de certificat ou son Autorité administrative (AA) et dont le résultat est la suspension de la validité d'un certificat pour une période donnée.

Tampon d'horodatage
Voir contremarque de temps.

Technique cryptographique asymétrique
Technique cryptographique utilisant deux transformations connexes, une transformation publique (définie par la clé publique) et une transformation secrète (définie par la clé privée). Ces deux

transformations ont pour propriété de rendre impossible de déduire par ordinateur la transformation secrète, en raison de la transformation publique. [ISO/IEC 11770-1]

Tierce Partie de Confiance (TPC)

Organisme gérant pour le compte d'autrui des conventions secrètes de moyens ou de prestations de cryptologie permettant d'assurer des fonctions de confidentialité. **Erreur ! Source du renvoi introuvable.**

Validation de certificat

Service offrant l'assurance que les informations contenues dans le certificat ont été validées par une autorité de confiance. La validation d'un certificat inclut entre autres la vérification de sa période de validité, de son état (révoqué ou non), et la vérification de la signature de l'AC génératrice. Elle inclut également la validation du certificat de l'AC génératrice.

Vérificateur

Toute entité (utilisateur humain, organisme ou entité des technologies de l'information) utilisant un certificat de clé publique. Synonyme : utilisateur de certificat.

Vérification de signature

La vérification d'une signature consiste à déchiffrer la signature d'un message, en mettant en œuvre la clé publique de l'émetteur. Si le clair obtenu est identique au haché calculé à partir du message reçu, alors il est garanti que le message est intègre et qu'il a été signé par le porteur de la clé privée correspondante à la clé publique utilisée pour la vérification.

La vérification d'une information signée nécessite des vérifications supplémentaires notamment la datation de l'information, le rôle du signataire, les conditions éventuelles de non-répudiation.

Rôles

Responsable sécurité :
Il est responsable de l'application de la politique de sécurité physique et fonctionnelle d'une ou plusieurs composantes du PSC et de son environnement. Il gère les contrôles d'accès physiques aux plates-formes des composantes, et est chargé de mettre en œuvre la politique de sécurité régissant la ou les composante(s).

Contrôleur :
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 politiques de certification, des déclarations des pratiques de certification et des services effectivement fournis par la composante du PSC.

Administrateur :
Un administrateur met en œuvre les politiques de certification et déclarations des pratiques de certification du PSC au sein de la composante qu'il administre. Il est responsable de l'ensemble des services rendus par cette composante.

Ingénieur système :
Il est chargé de la mise en route, de la configuration et de la maintenance technique de la plate-forme informatique de la composante. Il assure l'administration du système et du réseau de cette plate-forme.

Opérateur :
L'opérateur d'une composante (autorité de certification (AC), autorité d'enregistrement (AE), une tierce partie de confiance (TPC), une autorité d'horodatage (AH),) réalise l'exploitation des services offerts par la composante, dans le cadre de ses attributions. Il est chargé de lancer l'exécution des fonctions cryptographiques.

Acronymes

AA	Autorité administrative
AC	Autorité de certification
AE	Autorité d'enregistrement
ARL	Liste des Autorités de certification Révoquées
CEC	Centre d'élaboration de clés
CNIL	Commission Nationale de l'Informatique et des Libertés
CPSSI	Cahiers de Prescriptions de Sécurité des Systèmes d'Information
CRL	Certificate Revocation List (Liste des Certificats Révoqués)
DCSSI	Direction Centrale de la Sécurité des Systèmes d'Information
DN	Distinguish Name
DPC	Déclaration des Pratiques de Certification
DSCS	Dispositif sécurisé de création de signature électronique
IGC	Infrastructure de Gestion de clé
ISO	International Organization for Standardization
ITU	International Telecommunications Union
OC	Opérateur de Certification
OID	Object IDentifier
OPE	Opérateur de Préstation d'Externalisation
PC	Politique de certification
PKIX	Public Key Infrastructure Working Group (Groupe de travail de l'IETF)
PSSI	Politique de Sécurité des Systèmes d'Information
PSC	Prestataire de Services de Certification
PV	Procés Verbal
SP	Service de Publication
SSCD	Secure Signature Creation Divice
TPC	Tierce Partie de Confiance
UTC	Coordinated Universal Time

Documents de références

Lois et Réglements	
[DES]	Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques – (JOCE du 19 janvier 2000).
[L00-230]	Loi n 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique (JO du 14 mars 2000).
[L90-1170]	Article 28 de la loi n 90-1170 du 29 décembre 1990 sur la réglementation des télécommunications modifié par l'article 17 de la loi 96-659 du 26 Juillet 1996.
[LEN]	No 991 PROJET DE LOI modifié par le sénat pour la confiance dans l'économie numérique. Enregistré à la Présidence de l'Assemblée nationale le 26 juin 2003.
[L78-19]	Loi n 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (Art. 323-1 à 323-3 du Code pénal).
[D2002-535]	Décret du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.
[D2001-272]	Décret n°2001-272 du 30 mars 2001 pris pour application de l'article 1316 du code civil et relatif à la signature électronique
[D98-102]	Décret 98-102 du 24 Février 1998 précisant l'article [L90-1170] relatif aux conditions dans lesquelles sont agréés les organismes gérant pour le compte d'autrui les conventions secrètes de cryptologie.
[A02]	Arrêté du 31 mai 2002 relatif à la reconnaissance de la qualification des prestataires de certification électronique et à l'accréditation des organismes chargés de l'évaluation.
Documentations Internationales	
[TS 101 456]	ETSI TS 101 456 V1.2.1 (2002-04) - « Policy requirements for certification authorities issuing qualified certificates »
[SR 002 176]	ETSI SR 002 176 V1.1.1 (2003-03) - « Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures »
[TS 101 862]	ETSI TS 101 862 V1.2.1 (2001-06) – « Qualified certificate profile»
[9594-1]	ISO/IEC 9594-1 (1995) - « Information Technology – Open Systems Interconnection : The Directory : Overview of concepts, Models and Services » (Egalement Recommandation ITU-T X.500).
[9594-8]	ISO/IEC 9594-8 (1995) - « Information Technology – Open Systems Interconnection : The Directory : Authentication Framework » (Egalement Recommandation ITU-T X.509 (1997)). NF ISO/CEI 9594-8 (1996) – « Technologies de l'information – Interconnexions de systèmes ouverts (OSI) – L'annuaire : Cadre d'authentification ».
[ISO/IEC 11770-1]	ISO/IEC 11770-1: 1996, *Information technology - Security techniques - Key management - Part 1: Framework.*
[ISO/IEC 9798-1]	ISO/IEC 9798-1 (2nd edition): 1997, « *Information technology - Security techniques - Entity authentication - Part 1: General* ».
[ALGO]	Algorithms and Parameters for Secure Electronic Signatures v2.1 (19 Octobre 2001)

[RFC 2527]	« Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practises Framework » (Mars 1999) - IETF - Network Working Group.
[RFC 3280]	« Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile » (avril 2002) - Internet Engineering Task Force (IETF) - Network Working Group.
[RFC 3039]	« Internet X.509 Public Key Infrastructure Qualified Certificates Profile » (Janvier 2001) - Internet Engineering Task Force (IETF) - Network Working Group.
[CWA 14169]	European Committee for Standardization CEN/ISS : Security Requirements of Secure Signature Creation Devices (SSCD) – SSCD-PP
[CWA 14167-1]	Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements. November 2001
[CWA 14167-2]	Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2: Cryptographic Module for CSP Signing Operations - Protection Profile (MCSO-PP). March 2002
[GOC]	Digital Signature and Confidentiality - Certificate Policies - Government of Canada Public Key Infrastructure - Version 2.0 - Août 1998.
[AFNOR NF Z74-400]	Exigences concernant la politique mise en œuvre par les autorités de certification délivrant des certificats qualifiés.
Documents Interministériels	
[IGI1300]	Instruction générale interministérielle sur la protection du secret et des informations concernant la défense nationale et la sûreté de l'état n 1300/SGDN/SSD du 12 mars 1982 (document en diffusion restreinte).
[IGI910]	Instruction interministérielle sur les articles contrôlés de la sécurité des systèmes d'information n 910/SGDN/SSD/DR, n 910/DISSI/SCSSI/DR du 19 décembre 1994 (document en diffusion restreinte).
[IGI900]	Instruction générale interministérielle sur la sécurité des systèmes d'information qui font l'objet d'une classification de défense pour eux-mêmes ou pour les informations traitées n 900/SGDN/SSD/DR n 900 /DISSI/SCSSI/DR du 20 juillet 1993 (document en diffusion restreinte).
[R901]	Recommandation pour la protection des systèmes d'information traitant des informations sensibles non classifiées de défense n 901/DISSI/SCSSI du 2 mars 1994.
[CERTIFICAT_IGC]	Format des certificats utilisés dans les infrastructures de gestion de clés – Groupe Ad Hoc Messagerie Sécurisée de la Sous-Commission Chiffre de la CISSI.
[SIG/P/01.1]	PROCEDURE SIG/P/01.1 "CERTIFICATION DE CONFORMITE DES DISPOSITIFS DE CREATION DE SIGNATURE ELECTRONIQUE" 7 avril 2003
[DECOUPAGE_IGC]	Découpage fonctionnel des autorités d'une IGC - Groupe Ad Hoc Messagerie Sécurisée de la Sous-Commission Chiffre de la CISSI.
[ROLES_IGC]	Rôles des exploitants d'une infrastructure de gestion de clés – Groupe Ad Hoc Messagerie Sécurisée de la Sous-Commission Chiffre de la CISSI.
[PP_AC]	Profil de protection pour une autorité de certification – Groupe Ad

	Hoc Messagerie Sécurisée de la Sous-Commission Chiffre de la CISSI.
[PP_AE]	Profil de protection autorité d'enregistrement – Groupe Ad Hoc Messagerie Sécurisée de la Sous-Commission Chiffre de la CISSI.
[PP_IGC]	Profil de protection infrastructures de gestion des clés – Groupe Ad Hoc Messagerie Sécurisée de la Sous-Commission Chiffre de la CISSI.
[PP_OSM]	Profil de protection sur les outils de sécurisation de message version 1.5 du 24 juin 1998 (PP/9804) – Groupe Ad Hoc Messagerie Sécurisée de la Sous-Commission Chiffre de la CISSI.
[PP_RCIGC]	Profil de protection ressource cryptographique pour une infrastructure de gestion des clés – Groupe Ad Hoc Messagerie Sécurisée de la Sous-Commission Chiffre de la CISSI.
[VAR_TEMPS]	Définition des variables de temps intervenant dans une infrastructure de gestion de clés – Groupe Ad Hoc Messagerie Sécurisée de la Sous-Commission Chiffre de la CISSI.

Site de la DCSSI – volet sur la signature électronique :
www.ssi.gouv.fr/fr/sigelec/index.html

Types d'informations considérées comme confidentielles

A titre indicatif :

- Archives de journaux d'événements
- Archives des conventions cryptographiques utilisées (paramètres, valeurs d'initialisations)
- Clés privées propres à l'AC
- Clés privées des signataires
- Données d'identification d'un utilisateur (identifiants nominatifs)
- Journaux d'audit
- Données d'activation de la clé privée du signataire

Documents à fournir pour l'audit

- **POLITIQUE DE CERTIFICATION DE L'AC**
- **DECLARATION DES PRATIQUES DE CERTIFICATION DE L'AC**
- **DECLARATION DES PRATIQUES DE CERTIFICATION PUBLIABLE**
- **ROLES ET RESPONSABILITES**

  Le document précise les principes de séparation de fonctions. Ce document établit les rôles et responsabilités de chacun des intervenants ainsi que les droits particuliers affectés à chaque fonction.

- **PROCEDURE DE « GENERATION DES CLEFS»**

  (Key ceremony)

  elle définit les pré-requis, les actions de préparation et les étapes qui seront suivies lors de la génération des clés de l'AC.

- **SCHEMA DE L'ARCHITECTURE TECHNIQUE**

  Il est constitué d'un ensemble de schémas permettant d'avoir aussi bien une vision générale qu'une vision détaillée de l'architecture technique du PSC et des liaisons entre les différents composants.

- **POLITIQUE DE SECURITE ADAPTEE A L'AC.**

  Elle définit les règles de sécurité physique et logique couvrant l'ensemble du périmètre de l'AC. Elle intègre les éléments relatifs à l'architecture des systèmes et aux procédures rédigées.

- **PLAN QUALITE**

  Il définit les normes de qualité que l'organisation responsable mettra en oeuvre et précise de quelle façon elle compte y parvenir.

- **PLAN DE REPRISE D'ACTIVITE**

  Il définit les procédures de reprise en cas de sinistre d'un ou plusieurs composants.

  Ce document énumère les procédures à suivre en fonction du type d'incident susceptible de survenir et identifie les personnes qui devront être contactées. Ces procédures pourront être présentées sous la forme de plans d'actions détaillant les étapes qui devront être suivies pour remettre le PSC dans un état opérationnel.

- **PROCEDURES DE FONCTIONNEMENT EN MODE DEGRADE**

  Le document doit récapituler l'ensemble des procédures permettant au PSC de continuer à fonctionner dans un mode dégradé en attendant que l'application du plan de reprise d'activité ait permis de rendre le PSC opérationnel.

- **PLAN D'AUDIT INTERNE**

  Le document détaille les contrôles qui seront effectués, leur fréquence et les thèmes sur lesquels ils porteront.

- **PROCEDURE DE SUIVI DES RECOMMANDATIONS FAITES A L'ISSUE DES AUDITS**

  Le document définit la procédure permettant de bâtir les plans d'actions qui seront mis en œuvre après les audits.

- **PROCEDURES DE JOURNALISATION DES EVENEMENTS**

Le document définit les procédures de journalisation des informations. Ce document fixe les objectifs de journalisation des événements, d'analyses d'anomalies ainsi que des rapprochements entre journaux.

- **PROCEDURES DE SAUVEGARDE**

  Le document détaille les moyens mis en œuvre pour réaliser les sauvegardes ainsi que la gestion et la restauration de ces sauvegardes.

- **PROCEDURE D'ARCHIVAGE**

  Le document détaille les moyens mis en œuvre pour réaliser l'archivage ainsi que la gestion et la consultation de ces archives.

- **CHARTE SECURITE DES PERSONNELS DU PSC**

  Le document définit les règles de sécurité applicables aux personnels gestionnaires et exploitants du PSC. Cette charte de sécurité, signée par les personnels du PSC, les engage à porter une attention particulière aux contrôles et aux tâches sensibles et met l'accent sur l'importance des conséquences induites par des erreurs de manipulation.

- **PROCEDURE DE BACK-UP DE L'AE**

  Le document détaille les moyens mis en œuvre afin d'assurer la continuité et la disponibilité de l'Autorité d'Enregistrement.

- **PROCEDURE DE GESTION DES DROITS**

  Ce document définit la procédure de gestions des droits de chacun des acteurs du PSC (utilisateurs, AE, AC, Etc).

- **PROCEDURE DE CLASSIFICATION DE L'INFORMATION**

  Ce document détaille les différents niveaux de classification de l'information au sein de l'organisation. Il définit les règles et modalités de gestion des documents sensibles.

- **PROCEDURE DE PROTECTION DE L'INFORMATION**

  Ce document définit les règles de protection physique et logique de l'information véhiculée ou hébergée par les systèmes de l'organisation suivant leur classification.

- **PROCEDURE DE GESTION DES CLES CRYPTOGRAPHIQUES**

  Le document :

  - définit les règles de gestion des secrets d'AC et identifie les possesseurs de secrets,

  - détaille la gestion du boîtier cryptographique contenant le bi-clé de l'AC ainsi que la procédure de reconstruction du bi-clé.

- **PROCEDURE DE DEMANDE DE CERTIFICAT**

  Le document définit l'ensemble des actions à entreprendre pour l'enregistrement d'un signataire.

- **PROCEDURE DE REVOCATION D'UN CERTIFICAT**

  Le document définit les actions à entreprendre pour révoquer un certificat suivant l'origine de la demande.

- **PROCEDURE DE GESTION DES INCIDENTS**

  Le document définit les actions à entreprendre lors de la détection d'un incident. Il doit décrire les fiches de suivi d'incident qui devront être remplies lors de leur survenue et les étapes d'évolution de ces fiches.

- **CESSATION D'ACTIVITE OU CHANGEMENT DE COMPOSANTS DE L'AC**

Le document définit les procédures à suivre dans les différents cas de cessation d'activité ou de changement de l'une ou de plusieurs composantes de l'AC.

- **PROCEDURE DE MISE A JOUR DE LA PLATE-FORME TECHNIQUE**

  Le document définit les étapes de mise à jour de la plate-forme sous la forme de plans d'actions.

- **PROCEDURE DE MISE A JOUR DES PC ET DPC**

  Le document définit les étapes de mise à jour des PC et DPC.

- **REFERENTIEL DOCUMENTAIRE**

  Le document identifie l'ensemble des documents, leur version, les auteurs, les valideurs et leur statut. Ce référentiel peut être le point d'entrée de consultation des procédures.

Couverture ETSI TS 101 456– Guide d'audit

Cette annexe présente la matrice de couverture des exigences de l'ETSI TS 101 456 et des fiches du guide d'audit.

ETSI		Guide d'audit
1	**Champ d'application**	1.1
4.1	**Service de certification**	1.3.1
5.2	**Identification**	1.2
7.1	**Déclaration des pratiques et politique**	2.1(AC)
7.1.a		2.1 (AC) ; 8.3
note 1		2.1 (AC)
7.1.b		2.1 (AC)
7.1.c		8.2
Note 2		8.2
7.1.d		2,1 (AC) ; 8.2
7.1.e		8.3
7.1.f		8.3
7.1.g		2.7.1 ; 2.7.2 ; 2.7.3 ; 2.7.4 ; 2.7.5
7.1.h		2.1 (AC) ; 8.1
7.2	**Signature électronique sécurisée de l'OSC**	
7.2.1	**Génération des données de création de signature du PSC**	2.1 (AC) ; 6.1.1
7.2.1.a		6.2.7
7.2.1.b		6.1.1 ; 6.1.8 ; 6.1.9 ; 6.2.7
note 1		6.1.5 ; 6.1.9 ; 6.2.1
7.2.1.c		6.1.7 ; 6.1.8 ; 6.1.9
7.2.1.d		6.1.5 ; 6.1.7 ; 6.1.9
note 2		6.1.5 ; 6.1.6 ; 6.1.7 ; 6.1.9
7.2.2	**Conservation des données de création de signature**	2.1 (AC) ; 6.2.2
7.2.2.a		6.2.2 ; 6.4.1 ; 6.4.2
7.2.2.b		6.2.6
7.2.2.c		6.2.4 ; 6.2.5
7.2.2.d		6.2.4
7.2.2.e		6.2.4
7.2.3	**Distribution des données de vérification de signature du PSC**	2.1 (AC)
7.2.3.a		6.1.4 ; 6.1.3
Note		6.1.4
7.2.4	**Dépôt des clés privées du titulaire**	6.2.3
7.2.5	**Données de création de signature du PSC**	6.1.9
7.2.5.a		6.1.9
7.2.5.b		5.1.2
7.2.6	**Fin du cycle de vie des données de création de signature du PSC**	2.1 (AC)

ETSI		Guide d'audit
7.2.6.a		6.2.5 ; 6.2.9
7.2.7	**Cycle de vie du dispositif sécurisé de création de signature**	2.1 (AC)
7.2.7.a		6.6.2
7.2.7.b		6.6.2
7.2.7.c		6.2.2 ; 6.2.3 ; 6.2.4 ; 6.2.5 ; 6.2.7 ; 6.2.9
7.2.7.d		6.6.2
7.2.7.e		6.2.9
7.2.8	**Service de gestion des données de signature du titulaire**	2.1 (AC)
7.2.8.a		6.1.1 ; 6.1.5 ; 6.1.7 ; 6.1.9 ; 6.2.1
7.2.8.b		6.1.1 ; 6.1.5
note		6.1.5
7.2.8.c		6.1.1 ; 6.1.2
7.2.8.d		6.1.1 ; 6.1.2
7.2.9	**Preparation des équipements de création de signature**	2.1 (AC)
7.2.9 a		6.2.6
7.2.9 b		6.1.1 ; 6.1.2
7.2.9 c		6.2.6(react) 6.2.9 (desac)
7.2.9 d		6.1.2 ; 6.1.8 ; 6.4.1 ; 6.4.2
Note 2		6.1.2 ; 6.4.1
Note 3		6.1.8
7.3	**Cycle de vie du certificat électronique**	
7.3.1	**Enregistrement de la demande de certificat**	2.1 (AE)
note 1		3.1.8 ; 3.1.9
7.3.1.a		2.1.6 ; 2.6.1 ; 4.1
7.3.1.b		4.1 ; 2.6.1
note 2		2.6.1 ; 2.1.6
7.3.1.c		3.1.9 ; 3.1.8
note 3		3.1.9
note 4		1.3.2
7.3.1.d		3.1.9 ; 4.1
note 5		4.1
Note 6		2.1 (AC)
7.3.1.e		4.1
7.3.1.f		4.1
7.3.1.g		4.6.1
7.3.1.h		4.6.1; 4.3
note 8		4.3
note 9		4.3
note 10		4.3
7.3.1.i		2.6.1
7.3.1.j		3.1.7
note 11		3.1.7
7.3.1.k		2.1 (AE) ; 3.1.7 ; 4.1 ; 4.6.1

ETSI		Guide d'audit
7.3.2	**Renouvellement du certificat**	2.1 (AE)
7.3.2.a		3.2
7.3.2.b		4.1
7.3.2.c		4.1 ; 3.2
7.3.2.d		3.2 ; 3.3
7.3.3	**Création du certificat**	2.1 (AC)
7.3.3.a		3.1.1 ; 3.1.2 ; 3.1.3 ; 7.1 ; 7.1.1 ; 7.1.2 ; 7.1.3 ; 7.1.4 ; 7.1.5 ; 7.1.6 ; 7.1.7 ; 7.1.8 ; 7.2 ; 7.2.1; 7.2.2 ;
7.3.3.b		4.2
7.3.3.c		6.1.2 ; 4.2
7.3.3.d		3.1.4
7.3.3.e		4.2
7.3.3.f		4.2
7.3.4	**Distribution des conditions d'utilisation**	2.1(AC)
7.3.4.a		2.6.1 ; 4.4.10
7.3.4.b		2.6.1 ; 2.6.2
note		Traité dans 2.6.1
7.3.5	**Distribution du certificat**	2.1 (SP)
7.3.5.a		2.6.4
7.3.5.b		2.6.4
7.3.5.c		2.6.4
7.3.5.d		2.6.4
7.3.5.e		2.6.2
7.3.5.f		2.6.2
7.3.6	**Révocation et suspension du certificat**	2.1 (AC) ; 4.4.6 ; 4.4.7 ; 4.4.10 ; 4.4.14
7.3.6.a		3.4 ; 4.4.1 ; 4.4.2 ; 4.4.3 ; 4.4.5
note 1		4.4.3
7.3.6.b		4.4.3 ; 4.4.4
7.3.6.c		4.4.3
7.3.6.d		4.4.8 ; 4.4.3
note 2		2.1 (AC) optionel
7.3.6.e		4.4.3
7.3.6.f		4.4.3
7.3.6.g		4.4.9
7.3.6.h		4.4.4 ; 4.4.12
7.3.6.i		4.4.9 ; 4.4.14
note 3		4.4.12 ; 4.4.13 ; 4.4.14
7.3.6.j		4.4.3
7.3.6.k		4.4.12
7.4	**Organisation et fonctionnement du PSC**	
7.4.1	**Gestion de la sécurité**	2.1 (AC)
7.4.1.a		2.1 (AC)
7.4.1.b		2.1 (AC)

ETSI	Guide d'audit
7.4.1.c	2.1 (AC) ; 5.3.8
7.4.1.d	8.1 ; 6.6.2
7.4.1.e	mis dans 2.1 (AC)
7.4.1.f	2.1 (AC)
7.4.2 Inventaire et gestion des biens	2.1 (obligation générale)
7.4.2.a	2.8.1 ; 2.8.2
7.4.3 Sécurité liée au personnel	2.1 (AC)
7.4.3.a	5.3.1 ; 5.3.5 ; 5.3.7
note 1	Traité dans 5.3
7.4.3.b	5.2.1 ; 5.2.2
7.4.3.c	5.2.3
7.4.3.d	5.3.3 ; 5.3.4 ; 5.3.8
7.4.3.e	5.3.1 ; 5.3.5
7.4.3.f	5.3.2
7.4.3.g	7.4.3.g
7.4.3.h	5.3.5
7.4.3.i	5.3.2
7.4.4 Sécurité physique et environnementale	2.1 (obligation générale)
7.4.4.a	5.1.2
7.4.4.b	4.8 ; 4.8.1
7.4.4.c	4.8 ; 4.8.1
7.4.4.d	4.8
7.4.4.e	5.1.2
7.4.4.f	5.1.1 ; 5.1.2 ; 5.1.3 ; 5.1.4 ; 5.1.5
7.4.4.g	5.1.2
7.4.5 Gestion des opérations	2.1 (obligation générale)
7.4.5.a	6.5.1
7.4.5.b	6.5.1
7.4.5.c	2.8.1 ; 2.8.2
note 1	5.2.1
7.4.5.d	5.2.2
7.4.5.e	2.8.1 ; 5.1.7
7.4.5.f	6.6.2 ; 4.8.1
7.4.5.g	4.8
7.4.5.h	5.2.2
7.4.6 Accès au système informatique	2.1 (obligation générale)
7.4.6.a	6.7
note 1	6.7
7.4.6.b	6.7
7.4.6.c	6.5.1
7.4.6.d	5.2.3 ; 6.5.1
7.4.6.e	6.5.1 ; 5.2.3
7.4.6.f	6.5.1
7.4.6.g	6.5.1 ; 5.1.7
7.4.6.h	5.1.2 ; 6.7
7.4.6.i	5.1.2
7.4.6.l	2.6.3 ; 2.6.3

ETSI	Guide d'audit
7.4.6.k	2.6.3
7.4.6.l	2.6.3
7.4.7 Installation et maintenance des systèmes sécurisés	2.1 (obligation générale) ; 6.6.1 ; 6.5.2
7.4.7.a	6.6.1
7.4.7.b	6.6.2
7.4.8 Plan de continuité et reprise sur incident	2.1 (obligation générale)
7.4.8.a	4.8 ; 4.8.4
7.4.8.b	4.8.3
note	4.8.3
7.4.9 Cessation de l'activité du PSC	2.1 (AC) 4.9
7.4.9.a	4.9
7.4.9.b	4.9
7.4.9.c	4.9
7.4.10 Conformité aux exigences légales	2.1 (obligation générale)
7.4.10.a	4.5.4
7.4.10.b	2.1 (AE) ; 2.4.1
7.4.10.c	2.1 (obligation générale)
7.4.10.d	2.1 (AC) ; 2.8.4 ; 2.8.5 ; 2.8.6
7.4.11 Conservation des informations concernant les certificats qualifiés	2.1(obligation générale) 4.5 ; 4.6.1 ; 6.3.1
7.4.11.a	4.5.1 ; 4.6.1 ; 4.6.3
7.4.11.b	4.6.3
7.4.11.c	4.6.1
note 2	6.5.1
7.4.11.d	4.5.1
note 3	4.6.5
7.4.11.e	2.1 (obligation générale) ; 4.6.2 ; 4.5.3
note 4	4.6.2
note 5	4.6.2
7.4.11.f	6.5.1
7.4.11.g	4.6.1
7.4.11.h	4.5.1
7.4.11.i	4.6.1
7.4.11.j	2.1 (obligation générale)
7.4.11.k	4.5.1
7.4.11.l	4.5.1
7.4.11.m	4.5.1
7.4.11.n	4.5.1
7.4.11.o	4.5.1
7.5 Organisation générale	
7.5.a	2.1 (AC)
7.5.b	2.1 (obligation générale)
7.5.c	2.1 (obligation générale)
7.5.d	2.1 (obligation générale)
7.5.e	2.1 (obligation générale)
7.5.f	2.3 ; 2.3.1 ; 2.3.2 ; 2.3.3 ; 2.1 (AC)
7.5.g	2.1 (obligation générale)
7.5.h	2.4.2 ; 3.1.5 ; 2.1 (AC)

ETSI	Guide d'audit
7.5.i	2.1 (AC) ; 5.3.7
7.5.j	2.1 (obligation générale)
7.5.k	2.1 (obligation générale)

Formulaire de recueil de commentaires

Ce formulaire peut être envoyé à l'adresse suivante :

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP
conseil.dcssi@sgdn.pm.gouv.fr

Identification de la contribution
Nom et organisme (facultatif) : .....
Adresse électronique : .....
Date : .....

Remarques générales sur le document
Le document répond-il à vos besoins ? Oui ☐ Non ☐

Si oui :

Pensez-vous qu'il puisse être amélioré dans son fond ? Oui ☐ Non ☐

Si oui :

Qu'auriez-vous souhaité y trouver d'autre ?
.....
.....

Quelles parties du document vous paraissent-elles inutiles ou mal adaptées ?
.....
.....

Pensez-vous qu'il puisse être amélioré dans sa forme ? Oui ☐ Non ☐

Si oui :

Dans quel domaine peut-on l'améliorer ?
- lisibilité, compréhension ☐
- présentation ☐
- autre ☐

Précisez vos souhaits quant à la forme :
.....
.....

Si non :

Précisez le domaine pour lequel il ne vous convient pas et définissez ce qui vous aurait convenu :
.....
.....

Quels autres sujets souhaiteriez-vous voir traiter ?
.....
.....

Remarques particulières sur le document
Des commentaires détaillés peuvent être formulés à l'aide du tableau suivant.
"N°" indique un numéro d'ordre.

"Type" est composé de deux lettres :

La première lettre précise la catégorie de remarque :

- O Faute d'orthographe ou de grammaire
- E Manque d'explications ou de clarification d'un point existant
- I Texte incomplet ou manquant
- R Erreur

La seconde lettre précise son caractère :

- m mineur
- M Majeur

"Référence" indique la localisation précise dans le texte (numéro de paragraphe, ligne…).
"Énoncé de la remarque" permet de formaliser le commentaire.
"Solution proposée" permet de soumettre le moyen de résoudre le problème énoncé.

N°	Type	Référence	Énoncé de la remarque	Solution proposée
1				
2				
3				
4				
5				

Merci de votre contribution