



Premier ministre

**Agence nationale de la sécurité
des systèmes d'information (ANSSI)**

**Règles applicables en matière d'échantillonnage dans
le cadre de la qualification des prestataires de service
de certification électronique (PSCE) et d'horodatage
électronique (PSHE)**

version 1.0

Règles applicables en matière d'échantillonnage dans le cadre de la qualification des prestataires de service de certification électronique (PSCE) et d'horodatage électronique (PSHE)

Version	Date	Critère de diffusion	Page
1.0	23 avril 2014	Public	1/4

HISTORIQUE DES VERSIONS

DATE	VERSION	EVOLUTION DU DOCUMENT	REDACTEUR
23 avril 2014	1.0	<i>Règles applicables en matière d'échantillonnage dans le cadre de la qualification des prestataires de service de certification électronique (PSCE) et d'horodatage électronique (PSHE)</i>	ANSSI

La qualification des prestataires de services de confiance au sens du RGS est réalisée par un organisme accrédité par le COFRAC et habilité par l'ANSSI. Cet organisme doit effectuer les audits de qualification dans le respect du document [CERT CEPE REF 21 rev. 02 « Exigences spécifiques pour la qualification des prestataires de services de confiance »](#).

Le présent document, cité aux paragraphes 6.1.1.3 et 6.2.3 du document CEPEREF 21, précise les règles relatives à l'échantillonnage des sites à auditer dans le cadre de la qualification des prestataires de service de certification électronique (PSCE) et d'horodatage électronique (PSHE).

Les commentaires sur le présent document sont à adresser à :

**Agence nationale de la sécurité
des systèmes d'information**

SGDSN/ANSSI

51 boulevard de La Tour-Maubourg
75700 Paris 07 SP

rgs@ssi.gouv.fr

Règles applicables en matière d'échantillonnage dans le cadre de la qualification des prestataires de service de certification électronique (PSCE) et d'horodatage électronique (PSHE)

Version	Date	Critère de diffusion	Page
1.0	23 avril 2014	Public	2/4

1. Opportunité d'un audit par échantillon

Dans le cas où certaines fonctions de sécurité du PSCE ou du PSHE sont assurées sur plusieurs sites géographiques, l'audit des fonctions concernées peut être réalisé sur la base d'un échantillon. L'organisme de qualification décide, après avis de l'entité auditée, des fonctions qui seront auditées selon cette méthode.

Cette procédure est indiquée dans le paragraphe 6.1.1.3 du CERT CEPE REF 21. Elle est rappelée pour mémoire, mais ne sera pas modifiée.

2. Élaboration des profils

Les PSCE et PSHE réalisent une typologie de profils des périmètres à auditer, c'est-à-dire des sites géographiques sur lesquels sont opérées les fonctions de sécurité. Cette typologie peut être définie selon plusieurs critères : fonctions remplies (notamment l'enregistrement), mode d'organisation, procédures définies, population concernée, taille du site, etc.

Chaque site appartenant au périmètre général de l'audit indiqué par l'organisme de certification doit être classé dans un profil et un seul.

Les PSCE et PSHE fournissent à l'organisme de certification la méthode de réalisation des profils, ainsi que le classement des sites dans cette typologie. Ils en demeurent responsables et garantissent à l'organisme de qualification l'exhaustivité des profils et leur pertinence par rapport au périmètre de l'audit de qualification.

3. Constitution des échantillons

L'organisme de qualification retient deux sites à auditer pour chaque profil. Au moins l'un des deux sites doit être choisi de manière aléatoire, par exemple par tirage au sort. Le cas échéant, le site restant peut être désigné par l'organisme de certification. Dans ce cas, l'organisme de certification produit un avis motivé quant à ce choix.

4. Conclusions de l'audit

a. Conformité des échantillons

En cas de conformité de l'ensemble des sites audités, l'organisme de qualification produit une attestation de conformité dont le périmètre couvre l'ensemble de la prestation de services du PSCE/PSHE.

b. Non-conformité d'un ou plusieurs éléments de l'échantillon

En cas de non-conformité d'un site, l'organisme de qualification produit une fiche d'écart.

Les PSCE et PSHE réalisent les modifications nécessaires à la mise en conformité sur l'ensemble des sites associés au profil de l'échantillon défaillant. Ils fournissent ensuite à l'organisme de qualification les preuves (rapport interne, procédure, etc.) que chaque site associé au profil ne fait plus l'objet d'un écart et est conforme au référentiel d'audit.

En cas d'écart majeur ou de doute quant à la régularisation de la fiche d'écart, l'organisme de qualification peut procéder à un audit complémentaire sur deux autres sites associés au profil ayant fait l'objet de la fiche d'écart et ne faisant pas partie de l'échantillon.

Règles applicables en matière d'échantillonnage dans le cadre de la qualification des prestataires de service de certification électronique (PSCE) et d'horodatage électronique (PSHE)

Version	Date	Critère de diffusion	Page
1.0	23 avril 2014	Public	3/4

La qualification du PSCE ou du PSHE ne peut être accordée ou ne peut être maintenue qu'en l'absence d'écart majeur ou de doute.

Si le PSCE ou le PSHE disposait déjà d'une qualification au titre du décret n° 2010-112 pour la fonction concernée par l'écart, cette qualification est suspendue ou retirée.

5. Publicité

Ces règles sont reproduites dans les documents de procédures relatifs aux audits de qualification.

Les sites qui ont été audités sont mentionnés :

- dans le rapport d'audit ;
- sur le site de l'organisme de certification ;
- si nécessaire, sur le certificat.

6. Audits ultérieurs

Les audits ultérieurs (audit de surveillance, audit complémentaire, etc.) doivent être effectués sur des sites de même profil, différents de ceux audités précédemment avec une méthode et des critères identiques à ceux précédemment utilisés.

Règles applicables en matière d'échantillonnage dans le cadre de la qualification des prestataires de service de certification électronique (PSCE) et d'horodatage électronique (PSHE)

Version	Date	Critère de diffusion	Page
1.0	23 avril 2014	Public	4/4