Newsletter #28 – 6 février 2015

A l'attention des acteurs de la demande de logement social

Cette newsletter est diffusée par l'équipe projet nationale en charge du déploiement de la réforme de la demande unique de logement social.

LES CERTIFICATS ELECTRONIQUES : A QUOI SERVENT-ILS ?

Les guichets, dans le cadre des interfaces synchrone ou asynchrone de leur système informatique avec le SNE doivent utiliser des certificats électroniques qui leur permettent de **garantir leur identité** et de **sécuriser les échanges**. Ces certificats s'apparentent aux identifiant et mot de passe nécessaires à une connexion à l'application Web.
Les certificats utilisés sont des certificats conformes à la norme RGS.
Cependant les certificats répondant à la norme PRIS V1 présents actuellement sur le SNE restent supportés jusqu'à leur date de fin de validité.
Les certificats nécessaires répondent à trois usages différents : **chiffrement**, **signature**, **authentification**.
À l'origine, le chiffrement est utilisé pour garder des informations secrètes. Chiffrer un texte, c'est le rendre illisible pour qui ne possède pas la clé de déchiffrement, appelée clé privée. Un message chiffré par une clé publique n'est donc lisible que par le propriétaire de la clé privée correspondante.
La signature électronique assure l'identité de la personne ou de l'organisme qui a apposé sa signature et garantit que le document n'a pas été altéré entre l'instant où le document est signé et le moment où le document est consulté.
L'authentification est la procédure qui consiste, pour un système informatique, à vérifier l'identité d'une personne ou d'un ordinateur afin d'autoriser l'accès de cette entité à des ressources.
Pour plus de détail, vous pouvez regarder le Cahier des charges des Interfaces disponible sur le site du SNE
http://sne.info.application.territoires.gouv.fr/applications-interfacees-r48.html

COMMENT FONCTIONNENT LES ECHANGES ASYNCHRONES ?

Lors d'une communication entre le SNE et une application privative :

1) Le message contenant le fichier à transmettre est chiffré avec la **clé publique du Système National d'Enregistrement (SNE)** et est signé avec le **certificat de signature du service enregistreur**,
2) À la réception du message chiffré et signé, le SNE le déchiffre et en **vérifie la signature**,
3) Si le message est validé, le fichier est alors traité par le SNE,

- À la fin du traitement, le SNE génère un fichier de retour qui est joint dans un message **chiffré par la clé publique du service enregistreur** et **signé avec le certificat de signature du SNE**, puis envoyé au service enregistreur,
- Le service enregistreur reçoit le message contenant le fichier de retour qui est alors **déchiffré par sa clé privée.**

QUE DOIT INSTALLER UN SERVICE ENREGISTREUR ?

Le service enregistreur doit donc installer :

- le **certificat de chiffrement du SNE** : pour chiffrer les messages envoyés au SNE,
- la **chaîne de certification (autorités) du ministère** : pour utiliser le certificat de chiffrement du SNE et vérifier la signature électronique contenue dans les messages envoyés par le SNE,
- son **certificat de chiffrement** : pour déchiffrer les messages en provenance du SNE,
- son **certificat de signature** : pour signer les messages envoyés au SNE,
- son **certificat d'authentification** : uniquement si utilisation des web services,
- la **chaîne de certification de son fournisseur des certificats** : pour utiliser les certificats acquis par le guichet.

QUE DOIT TRANSMETTRE LE SERVICE ENREGISTREUR AU GESTIONNAIRE TERRITORIAL ?

Le service enregistreur doit extraire la clé publique du certificat de chiffrement et la transmettre au gestionnaire territorial.

QUELLES DONNEES SONT NECESSAIRES A L'ACHAT DES CERTIFICATS ?

Pour acheter ses certificats, le service enregistreur doit fournir :

- un **NOM**,
- un **N° SIREN** : cette donnée est importante car elle est exigée et vérifiée lors de l'installation du certificat dans le SNE, Le SIREN doit être identique à celui du guichet,
- une **adresse mail** : il est conseillé de donner l'**adresse mail technique d'échange** (les échanges doivent obligatoirement partir de l'adresse renseignée dans le certificat pour certains logiciels de messagerie)