En tant que FS, je dois garantir que la forme de stockage des secrets de sécurité utilisés lors de l'authentification des utilisateurs (personnes ou autres systèmes) interdise définitivement d'accéder à leur valeur en clair tout en permettant leur comparaison avec un secret à tester. Je peux avoir recours à des fonctions de hachage cryptographique à cette fin.

Si besoin, le haché du secret peut être utilisé comme index pour retrouver les informations contextuelles liées au secret mais qui ne constituent pas elles-mêmes des secrets de sécurité, et qui peuvent être nécessaires à des validations de sécurité (ex: date d'expiration de l'état d'authentification matérialisé par le secret, état de révocation ou non du secret, identifiant du système autorisé à utiliser le secret...) ou aux fonctions métiers assurées par le système (ex: informations relatives à l'utilisateur...).

|  |  |  |  |
| --- | --- | --- | --- |
| **EXI EDC 119** | | | |
|  | **Editeur de Logiciel Utilisateur** |  | **Editeur de Logiciel Proxy e-santé** |
| *[Il est attendu que le Fournisseur de Service décrive le paramétrage de la solution garantissant que toute information de raccordement éphémère ne soient stockées qu'en mémoire volatile ;*  *OU fasse référence à un extrait, clairement identifié, d’un document qu’il fournira*  *]* | | | |