

ANNEXE - Sécurité applicative

Modalités d'établissement d'une connexion TLS

Ci-dessous le tableau récapitule des algorithmes et protocoles autorisés dans le cadre de l'établissement des connexions sécurisées HTTPS

Eléments	Protocoles/Algorithmes
Protocole	>TLS V1.2 minimum
Algorithme de chiffrement	>AES >Camelia
Taille de bloc	>A minima 2048 bits pour les chiffrements asymétriques >A minima 128 bits pour les chiffrements symétriques symétriques en Privilégiant le 256 bits
Mode opératoire (pour les chiffrements par bloc)	>CBC >Combiné
Algorithme d'intégrité	>Algorithme de chiffrement par bloc combiné >HMAC-SHA256 >HMAC-SHA384 >HMAC-SHA512

Une négociation TLS avec authentification mutuelle sera demandée au titulaire si ce dernier accède à un service présent dans le système d'information du pouvoir adjudicateur (Cnaf).