Comment choisir une clé USB inviolable pour vos données sensibles

Certifications et normes de cryptage

• Vérifiez la certification FIPS 140-2 ou 140-3 (niveau 3 recommandé) pour garantir la résistance physique du module cryptographique.

• Exigez un chiffrement matériel AES 256 bits XTS pour éviter toute exposition des clés de chiffrement au système hôte.

• Privilégiez les modèles certifiés Common Criteria EAL4+ pour une conception sécurisée validée contre les attaques complexes.

Protection contre les intrusions physiques

• Optez pour une clé avec clavier physique ou interface d'authentification embarquée afin de contrer les attaques par keyloggers.

• Assurez-vous que le dispositif intègre une fonction d'auto-destruction ou de blocage définitif après 10 tentatives de code PIN infructueuses.

• Recherchez une fabrication robuste (coque en aluminium anodisé, remplissage en résine époxy) pour prévenir l'extraction physique des données.

Fonctionnalités de sécurité opérationnelle

• Utilisez le mode 'Read-Only' (lecture seule) commutable matériellement pour protéger vos fichiers contre les logiciels malveillants.

• Privilégiez des modèles 'OS-agnostic' (driverless) pour éliminer le besoin d'installer des pilotes tiers et réduire la surface d'attaque.

• Vérifiez la présence d'un verrouillage automatique immédiat dès le retrait du port USB.

• Favorisez les dispositifs supportant l'authentification à deux facteurs (ex: FIDO2) pour une gestion d'accès renforcée.