Brochure produit

SecurityServer - Sécurisez les ressources les plus précieuses de votre organisation

SecurityServer - La garantie confiance pour les applications professionnelles

HSM

Utimaco
SecurityServer

Creating Trust in the Digital Society

40 utimaco® YEARS

SecurityServer en quelques mots

Génération, stockage et utilisation sécurisés de clés pour de nombreuses applications professionnelles

Aujourd'hui, toutes les entreprises, institutions et organisations sont entrées dans l'ère numérique, et ce dans tous les secteurs. Le déploiement à grande échelle des systèmes numériques conduit également à un accroissement de la quantité de données générées. Les entreprises recherchent des solutions pour sécuriser leurs données confidentielles, leurs processus, leur propriété intellectuelle et les données des utilisateurs et des clients. L'arrivée de nouveaux appareils et composants connectés nécessite également de protéger leur identité.

La protection des données et des identités augmente la demande en applications d'authentification, de signature de documents, de délivrance de certificats, d'injection de clés, etc. Certaines compagnies recherchent des applications très performantes, tandis que d'autres ont besoin d'une sécurité physique maximale pour se protéger des attaques virtuelles et physiques.

La sécurité de ces applications n'est garantie que si les clés utilisées pour les exécuter sont elles-mêmes sécurisées. En résumé, si les clés sont sécurisées, votre entreprise l'est aussi.

L'offre **SecurityServer** d'Utimaco ajoute une couche supplémentaire de sécurité à vos applications professionnelles. SecurityServer fournit un environnement inviolable pour le chiffrement des données, la signature de documents, l'émission de certificats et de nombreuses autres applications nécessitant une sécurité maximale.

Avantages de SecurityServer

SÉCURITÉ
de la génération et du stockage de clés

UTILISATION DES CLÉS
dans un environnement inviolable

HAUTE QUALITÉ
de la génération de nombres aléatoires pour garantir l'unicité des clés

Utimaco SecurityServer

SecurityServer combine 30 ans d'expérience dans le domaine du chiffrement et de la technologie HSM (module de sécurité matériel) au sein d'une offre unique qui constitue une garantie confiance en matière de sécurité et de conformité des applications professionnelles. Les ressources les plus précieuses de votre organisation bénéficient ainsi d'une couche supplémentaire de sécurité. Prenant en charge une large gamme de plateformes matérielles, SecurityServer répond aux exigences de performance et de sécurité des petites entreprises comme des grandes infrastructures de chiffrement et propose toujours le meilleur rapport qualité-prix dans différents scénarios de déploiement.

Caractéristiques principales

Matériel

- **Environnement inviolable** pour des opérations sécurisées sur les clés

Administration

- **Gestion à distance** complète

Simulateur de logiciel gratuit

- Simulateur HSM **doté de toutes les fonctionnalités de SecurityServer**

Intégration facile

- Intégration facile avec les **applications tierces**

Logiciel

- Microprogramme **personnalisable**

Pour les applications et les segments de marché à forte sécurité physique.

Intégration plug-and-play avec de nombreuses applications professionnelles.

Solution SecurityServer

Les excellentes caractéristiques et fonctionnalités de SecurityServer sont applicables à divers cas d'utilisation et secteurs d'activité.

Environnement inviolable pour des opérations sécurisées sur les clés

SecurityServer assure la génération, le stockage et l'utilisation sécurisés de clés au sein d'un HSM inviolable. En fonction des exigences du marché, SecurityServer permet de générer des clés en grande quantité et assure une génération de nombres aléatoires de haute qualité afin de garantir l'unicité des clés.

Gestion à distance complète

SecurityServer permet une gestion efficace des clés et des mises à jour du microprogramme via un accès à distance. Notre solution prend en charge l'automatisation du diagnostic à distance via le protocole SNMP (protocole de gestion de réseau simple).

Simulateur de logiciel gratuit

Le simulateur de SecurityServer permet d'essayer facilement SecurityServer et de tester son intégration avec des applications professionnelles avant de procéder à son déploiement.

Intégration facile avec des applications tierces

SecurityServer prend en charge toutes les API de chiffrement courantes telles que PKCS #11, JCE, OpenSSL, Microsoft CNG et SQLEKM. De plus, son intégration plug-and-play avec de nombreuses applications professionnelles garantit la sécurisation de vos systèmes en un tournemain.

Microprogramme personnalisable

Lorsque les API de chiffrement courantes ne répondent pas à vos besoins, par exemple lorsqu'elles ne prennent pas en charge un algorithme gouvernemental spécifique ou une nouvelle méthode de dérivation de clé, ou lorsqu'elles sont inefficaces car il est nécessaire d'enchaîner plusieurs commandes, notre kit de développement de microprogramme HSM vous permet d'affiner et d'optimiser les fonctionnalités et les performances de vos HSM.

Cas d'utilisation

- **Chiffrement des données**
- **Signature de documents**
- **Signature de code**
- **Délivrance de certificats**
- **Infrastructure à clés publiques**
- **Personnalisation de puces et d'appareils**
- **Authentification d'utilisateurs et d'appareils**
- **Et plus encore**

Secteurs

- **IdO et fabrication**
- **Services financiers**
- **Cloud/fournisseurs de services cloud**
- **Gouvernement**
- **Vente au détail**
- **Télécommunications**
- **Et plus encore**

Fonctionnalités HSM

Fonctionnalités

- **Gestion étendue des clés**
- **Stockage sécurisé des clés à l'intérieur d'un HSM,** sous forme de blobs de clés chiffrés dans le système de fichiers ou dans une base de données d'entreprise.
- **Authentification à 2 facteurs** avec cartes à puce
- **Authentification de type « m sur n »** (par exemple, 3 sur 5)
- Contrôle d'accès configurable **basé sur des rôles** et séparation des fonctions
- Prise en charge de **plusieurs clients**
- **Systèmes d'exploitation** pris en charge : **Windows** et **Linux**
- **Multiples intégrations** avec les applications PKI, le chiffrement des bases de données, etc.
- **Toutes les fonctionnalités sont incluses** dans le prix du produit

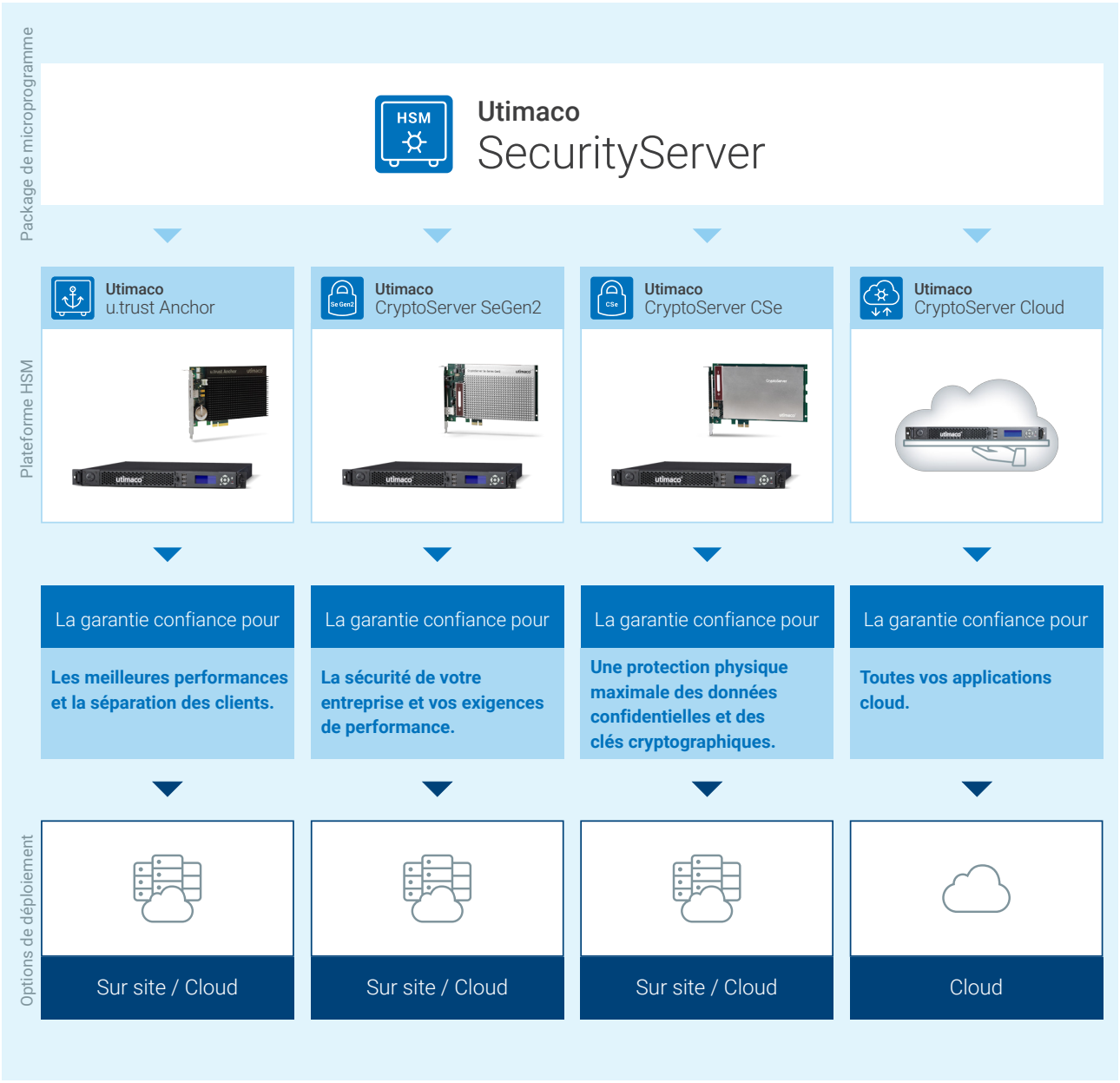
Algorithmes de chiffrement

- **RSA, DSA, ECDSA** avec courbes NIST, Brainpool et FRP256v1, EdDSA
- **DH, ECDH** avec courbes NIST, Brainpool, FRP256v1 et Montgomery
- **AES, Triple-DES, DES**
- **MAC, CMAC, HMAC**
- **SHA-1, SHA2-Family, SHA3, RIPEMD**
- **SM2, SM3 et SM4 (Chine)**
- Compatible **5G, blockchain** et **PQC**
- **Générateur déterministe de nombres aléatoires basé sur le hachage** (DRG.4 acc. AIS 31/ NIST SP800-90B)
- **Générateur de nombres aléatoires** (PTG.2 acc. AIS 31)
- **Tous les algorithmes sont inclus** dans le prix du produit

Interfaces de programmation d'applications (API)

- **PKCS #11**
- **Extension de chiffrement Java** (JCE)
- **API Microsoft Crypto** (CSP) et **Cryptography Next Generation** (CNG)
- **Microsoft SQL Extensible Key Management** (SQLEKM)
- **OpenSSL**
- **Cryptographic eXtended services Interface** (CXI) - L'interface haute performance d'Utimaco permet d'intégrer facilement des fonctionnalités de chiffrement dans les applications clients.

Plateforme SecurityServer et options de déploiement



Spécifications techniques

Utimaco
u.trust Anchor

Appareil réseau

Dimensions

- **Dimensions :** 19" 1U
- **Poids** : 22,05 lb (10 kg)
- **Largeur :** 17,56 in (446 mm) sans les supports
- **Profondeur :** 21,79 in (533,4 mm) sans les poignées
- **Hauteur :** 1,73 in (44 mm)

Connectivité

- **Interfaces :** 2 RJ45, 1 Gb/s
- 2 interfaces réseau SFP+ 10 Gb/s ou 2 interfaces réseau RJ45 1 Gb/s en option

Caractéristiques électriques

- **Alimentation :** Démontable, 2 x 100 ~ 240 V AC, 50 ~ 60 Hertz, 300 W
- **Consommation électrique :** usage normal 55 W / 78 VA, max. 65 W / 90 VA
- **Dissipation de la chaleur :** max. 222 Btu/h

Environnement opérationnel

- **Température de fonctionnement :** De 50 °F à 122 °F (de 10 °C à 50 °C)
- **Humidité relative de fonctionnement :** De 10 % à 95 %, en l'absence de condensation
- **Température de stockage :** De 14 °F à 131 °F (de -10 °C à 55 °C)
- **MTBF :** 134 250 heures d'après Telcordia Issue 3, température 30 °C, à terre, environnement protégé

Certification / Conformité

- **Sécurité et conformité électromagnétique :** IEC/EN 60950-1, IEC/EN 62368-1, UL, Certificats CB, CE, FCC Classe B
- **Environnemental :** RoHS II, REACH
- **Sécurité :** FIPS 140-2 niveau 3

Horloge

- DCF-77 ou récepteur GPS en option

Carte PCIe

Caractéristiques physiques

- **Dimensions :** Demi-longueur, pleine hauteur 4 voies, Carte PCI Express
- **Compatibilité :** Emplacements PCIe 1.1, PCIe 2.0 et PCIe 3.0
- **Hauteur :** 0,74 po (18,6 mm)
- **Largeur :** 4,38 po (111,15 mm)
- **Profondeur :** 6,60 po (167,65 mm) sans les supports
- **Poids :** 0,88 lb (0,4 kg)

Connectivité

- **Interface :** PCIe x4

Caractéristiques électriques

- **Alimentation :** 3,3 V fournis par le connecteur PCIe
- **Consommation électrique :** max. 25 W
- **Batterie de secours :** Pile au lithium 3 V, type CR2447

Environnement opérationnel

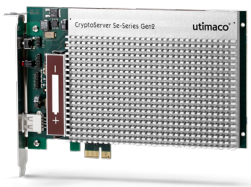
- **Température de fonctionnement :** De 50 °F à 113 °F (de 10 °C à 45 °C)
- **Humidité relative de fonctionnement :** De 10 % à 95 %, en l'absence de condensation
- **Température de stockage :** De 14 °F à 131 °F (de -10 °C à 55 °C)
- **MTBF :** 389 797 heures, d'après Telcordia Issue 3, température 30 °C, à terre, installation fixe, température 50 °C pour les pièces dans le matériau de remplissage

Certification / Conformité

- **Sécurité et conformité électromagnétique :** IEC/EN 60950-1, IEC/EN 62368-1, UL, Certificats CB, CE, FCC Classe B
- **Environnemental :** RoHS II, REACH
- **Sécurité :** FIPS 140-2 niveau 3

Utimaco

CryptoServer SeGen2



Appareil réseau

Caractéristiques physiques

- **Dimensions :** 19" 1U
- **Poids** : 22,05 lb (10 kg)
- **Largeur :** 17,56 in (446 mm) sans les supports
- **Profondeur :** 21,79 in (533,4 mm) sans les poignées
- **Hauteur :** 1,73 in (44 mm)

Connectivité

- **Interfaces :** 2 RJ45, 1 Gb/s
- 2 interfaces réseau SFP+ 10 Gb/s ou 2 interfaces réseau RJ45 1 Gb/s en option

Caractéristiques électriques

- **Alimentation :** Démontable, 2 x 100 ~ 240 V AC, 50 ~ 60 Hertz, 300 W
- **Consommation électrique :** usage normal 45 W / 66 VA, max. 50 W / 70 VA
- **Dissipation de la chaleur :** max. 171 Btu/h

Environnement opérationnel

- **Température de fonctionnement :** De 50 °F à 122 °F (de 10 °C à 50 °C)
- **Humidité relative de fonctionnement :** De 10 % à 95 %, en l'absence de condensation
- **Température de stockage :** De 14 °F à 131 °F (de -10 °C à 55 °C)
- **MTBF :** 125 322 heures à 25 °C / 77 °F, à terre, environnement protégé et contrôlé

Certification / Conformité

- **Sécurité et conformité électromagnétique :** IEC/EN 60950-1, IEC/EN 62368-1, UL, Certificats CB, CE, FCC Classe B, BIS, KC
- **Environnemental :** RoHS II, WEEE
- **Sécurité :** FIPS 140-2 niveau 3

Horloge

- DCF-77 ou récepteur GPS en option

Carte PCIe

Caractéristiques physiques

- **Dimensions :** Demi-longueur, pleine hauteur, une seule voie, Carte PCI Express
- **Compatibilité :** Emplacements PCIe 1.1, PCIe 2.0 et PCIe 3.0
- **Hauteur :** 4,38 po (111,15 mm) « pleine » hauteur
- **Poids :** 0,88 lb (0,4 kg)

Connectivité

- **Interface :** PCIe x1

Caractéristiques électriques

- **Alimentation :** 3,3 V fournis par le connecteur PCIe
- **Consommation électrique :** max. 9,9 W
- **Batterie de secours :** Pile au lithium 3 V, Ø 12 mm, longueur 60 mm, FDK CR12600SE-T1 ou VARTA CR2NP-T1

Environnement opérationnel

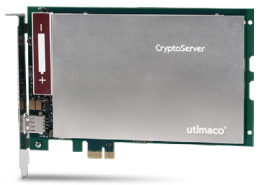
- **Température de fonctionnement :** De 50 °F à 113 °F (de 10 °C à 45 °C)
- **Humidité relative de fonctionnement :** De 10 % à 95 %, en l'absence de condensation
- **Température de stockage :** De 14 °F à 131 °F (de -10 °C à 55 °C)
- **MTBF :** 360 000 heures à 25 °C / 77 °F, à terre, environnement protégé et contrôlé

Certification / Conformité

- **Sécurité et conformité électromagnétique :** IEC/EN 60950-1, IEC/EN 62368-1, UL, Certificats CB, CE, FCC Classe B
- **Environnemental :** RoHS II, WEEE
- **Sécurité :** FIPS 140-2 niveau 3

Utimaco

CryptoServer CSe



Appareil réseau

Caractéristiques physiques

- **Dimensions :** 19" 1U
- **Poids** : 22,05 lb (10 kg)
- **Largeur :** 17,56 in (446 mm) sans les supports
- **Profondeur :** 21,79 in (533,4 mm) sans les poignées
- **Hauteur :** 1,73 in (44 mm)

Connectivité

- **Interfaces :** 2 RJ45, 1 Gb/s
- 2 interfaces réseau SFP+ 10 Gb/s ou 2 interfaces réseau RJ45 1 Gb/s en option

Caractéristiques électriques

- **Alimentation :** Démontable, 2 x 100 ~ 240 V AC, 50 ~ 60 Hertz, 300 W
- **Consommation électrique :** usage normal 45 W / 66 VA, max. 50 W / 70 VA
- **Dissipation de la chaleur :** max. 171 Btu/h

Environnement opérationnel

- **Température de fonctionnement :** De 50 °F à 104 °F (de 10 °C à 40 °C)
- **Humidité relative de fonctionnement :** De 10 % à 95 %, en l'absence de condensation
- **Température de stockage :** De 14 °F à 131 °F (de -10 °C à 55 °C)
- **MTBF :** 98 244 heures à 25 °C / 77 °F, à terre, environnement protégé et contrôlé

Certification / Conformité

- **Sécurité et conformité électromagnétique :** IEC/EN 60950-1, IEC/EN 62368-1, UL, Certificats CB, CE, FCC Classe B, BIS, KC
- **Environnemental :** RoHS II, WEEE
- **Sécurité :** FIPS 140-2 niveau 3, Sécurité physique FIPS 140-2 niveau 4

Horloge

- DCF-77 ou récepteur GPS en option

Carte PCIe

Dimensions

- **Dimensions :** Demi-longueur, pleine hauteur, une seule voie, Carte PCI Express
- **Compatibilité :** Emplacements PCIe 1.1, PCIe 2.0 et PCIe 3.0
- **Hauteur :** 4,38 po (111,15 mm) « pleine » hauteur
- **Poids :** 0,88 lb (0,4 kg)

Connectivité

- **Interface :** PCIe x1

Caractéristiques électriques

- **Alimentation :** 3,3 V fournis par le connecteur PCIe
- **Consommation électrique :** max. 6 W
- **Batterie de secours :** Pile au lithium 3 V, Ø 12 mm, longueur 60 mm, FDK CR12600SE-T1 ou VARTA CR2NP-T1

Environnement opérationnel

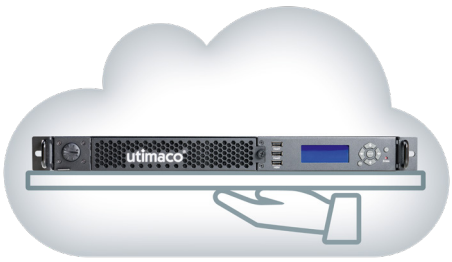
- **Température de fonctionnement :** De 50 °F à 95 °F (de 10 °C à 35 °C)
- **Humidité relative de fonctionnement :** De 10 % à 95 %, en l'absence de condensation
- **Température de stockage :** De 14 °F à 131 °F (de -10 °C à 55 °C)
- **MTBF :** 360 000 heures à 25 °C / 77 °F, à terre, environnement protégé et contrôlé

Certification / Conformité

- **Sécurité et conformité électromagnétique :** IEC/EN 60950-1, IEC/EN 62368-1, UL, Certificats CB, CE, FCC Classe B
- **Environnemental :** RoHS II, WEEE
- **Sécurité :** FIPS 140-2 niveau 3, Sécurité physique FIPS niveau 4

Utimaco

CryptoServer Cloud



HSM en tant que service

Disponibilité

- 99 % avec un seul HSM dans un seul centre de données
- 99,9 % avec deux HSM dans deux centres de données chacun

Certification / Conformité

- **Sécurité :** HSM certifié FIPS 140-2 niveau 3
- Hébergé dans un centre de données conforme aux normes ISO/IEC 27001, PCI et HIPAA (États-Unis uniquement)

Hébergement

- Entièrement hébergé par Utimaco - aucun effort de votre part

Service

- Surveillance, maintenance, mise à jour du microprogramme de l'environnement HSM

Gestion

- Gestion à distance possible

Assistance

- Assistance 24/7 incluse

À propos d'Utimaco

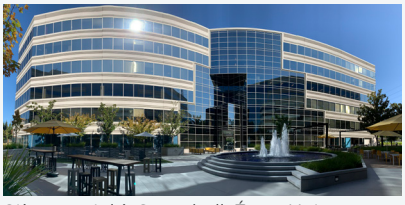
Utimaco est un fournisseur mondial reconnu de solutions et de services en matière de cybersécurité et de conformité, dont les sièges sont situés à Aix-la-Chapelle (Allemagne) et à Campbell, CA (États-Unis).

Utimaco développe des modules de sécurité matériels (HSM) sur site et dans le cloud, des solutions pour la gestion de clés, la protection des données et la gestion d'identités, ainsi que des solutions d'analyse des données pour les infrastructures critiques réglementées et les systèmes d'alerte publique. Utimaco est l'un des premiers fabricants mondiaux dans ses principaux segments de marché.

Plus de 550 employés dans le monde entier créent des solutions et des services innovants pour protéger les données, les identités et les réseaux de communication afin de répondre de façon responsable aux besoins de clients et de citoyens du monde entier. Des clients et partenaires de nombreux secteurs différents apprécient la fiabilité et la sécurité à long terme offertes par les produits et les solutions de haute sécurité d'Utimaco.

Pour en savoir plus, rendez-vous sur utimaco.com

Siège social à Aix-la-Chapelle, Allemagne



Siège social à Campbell, États-Unis

Prenez contact

EMEA

Utimaco IS GmbH

Germanusstrasse 4
52080 Aix-la-Chapelle,
Allemagne

+49 241 1696 200

hsm@utimaco.com

Amériques

Utimaco Inc.

900 E Hamilton Ave., Suite 400
Campbell, CA 95008,
ÉTATS-UNIS

+1 844 Utimaco

hsm@utimaco.com

APAC

Utimaco IS Pte Limited

6 Temasek Boulevard
#23-04 Suntec Tower Four
Singapore 038986

+65 6993 8918

hsm@utimaco.com

Pour plus d'informations sur les produits Utimaco® HSM, veuillez consulter le site suivant :

utimaco.com

Creating Trust in the **Digital Society**

utimaco®