



**L'Architecture de Sécurité à son plus haut niveau
designed by Crypto AG**



L'Architecture de Sécurité de Crypto AG – élégante et efficace

Depuis 1952, Crypto AG s'est fixé pour but de protéger systématiquement vos informations vitales et sensibles contre les accès non autorisés grâce aux systèmes de chiffrement les plus modernes. Aujourd'hui encore, cet objectif sous-tend toute la philosophie de l'entreprise. Fruit de plusieurs décennies de développement, notre Architecture de Sécurité unique constitue le cœur de notre philosophie de sécurité.

La conception de cette architecture permet à Crypto AG de remettre au client une base d'algorithme définissable tout en offrant un niveau de protection cryptographique optimal et donc un soutien exemplaire de sa politique de sécurité. Par ailleurs, du fait de votre intervention directe, elle garantit l'indépendance absolue de votre solution de chiffrement, l'autodétermination de tous les domaines cryptographiques et la vérification du mode de fonction de votre algorithme.

La base de l'Architecture de Sécurité est l'algorithme de base d'origine de Crypto AG dont la conception représente le plus haut niveau cryptographique existant et sur laquelle reposent des solutions offrant une qualité de sécurité unique. Plusieurs fonc-

tions centrales interdépendantes de l'architecture sont liées à l'algorithme, constituant avec celui-ci un noyau de chiffrement particulièrement résistant et au fonctionnement stable. Sa fonctionnalité est supportée par un chiffrement basé sur matériel qui a lieu dans un module de sécurité distinct, séparé du réseau informatique (réseau ICT). La flexibilité de l'architecture est un atout au quotidien grâce à une gestion efficace et conviviale de la sécurité et des clés. Cette dernière travaille main dans la main avec la gestion de réseau des utilisateurs. Résultat: l'Architecture de Sécurité de Crypto AG offre la disponibilité élevée que vous êtes en droit d'attendre de votre solution de chiffrement.



Les fonctions centrales de l'algorithme vous rendent indépendant

Vous recevez votre propre version de l'algorithme de base secret (secret proprietary algorithm) de Crypto AG. De cette manière, Crypto AG vous protège des autres clients utilisant un système similaire. Afin que vous soyez entièrement indépendant de Crypto AG et en mesure de contrôler vous-même votre système de sécurité, l'algorithme est conçu de manière à vous permettre de déterminer vous-même ses principales fonctions. Ayant donc paramétré vous-même un profil spécifique, vous prenez entièrement possession de l'algorithme, satisfaisant par là vos besoins en matière d'autonomie et de séparation. Vous disposez ainsi d'un algorithme absolument unique au monde, que ni Crypto AG ni aucun tiers ne connaissent, et auquel personne ne peut accéder. Vous êtes le seul à connaître et à contrôler votre sécurité.

Pour cela, l'algorithme s'appuie sur un procédé de chiffrement symétrique utilisant la même clé pour le chiffrement

et le déchiffrement. La clé (numérique) doit avant tout satisfaire à des exigences maximales en matière de caractère aléatoire, un critère garanti par un générateur de nombres aléatoires, séparé et de très haute qualité, basé sur matériel. Sur cette base, la longueur de clé d'au moins 128 bits, associée à la complexité de votre algorithme de chiffrement secret, vous toute attaque de votre système à l'échec.

Des protocoles de chiffrement résistants permettent de définir des clés sur plusieurs niveaux hiérarchiques (multi-hierarchical key grouping), conférant une grande souplesse à votre gestion de la sécurité. En pratique, lorsque vous utilisez des appareils de Crypto AG, vous soutenez votre politique de sécurité de manière ciblée, en déterminant par exemple – suivant le scénario d'application – des groupes de communication cryptographiques de niveaux hiérarchiques différents avec recouvrement réciproque. Dans

ce domaine, vous pouvez adapter la coopération et la séparation à vos besoins organisationnels variables quand vous le désirez. Le nombre d'utilisateurs est illimité.

La description fournie par Crypto AG vous procure, en tant que propriétaire d'un algorithme, la transparence nécessaire en matière d'évaluation pour vous permettre de disposer d'une certitude absolue quant à sa structure et à son mode de fonctionnement. Grâce à l'Acceptance Cipher Check (ACC), vous disposez de plus, si vous le souhaitez, d'un outil performant et unique vous permettant de vérifier par vous-même, à tout moment et en tout lieu, l'implémentation et le fonctionnement corrects de votre algorithme. La vérification des opérations cryptographiques assurant une excellente compréhension des solutions de Crypto AG, vous savez que vous pouvez vous y fier.

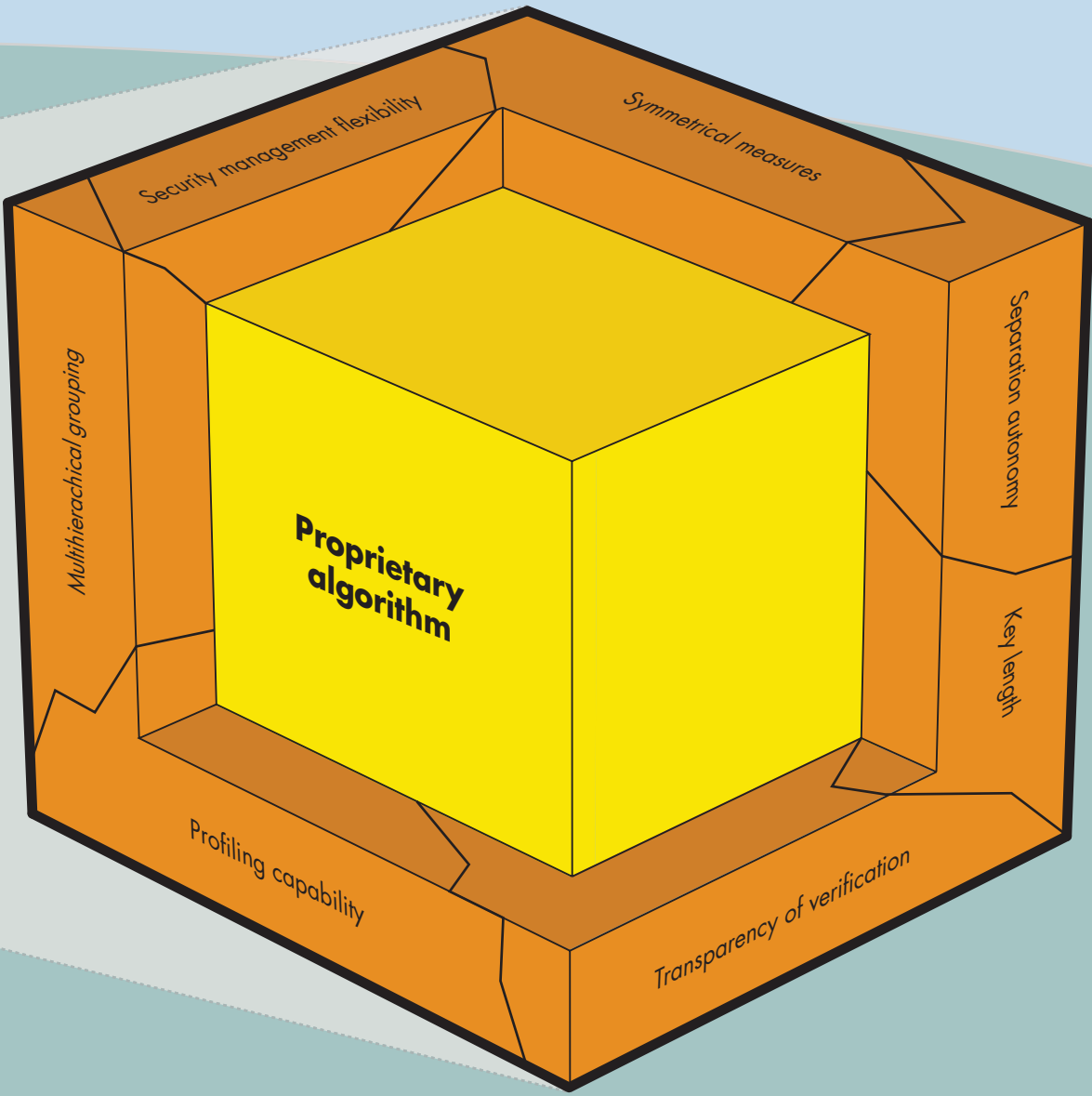


Le matériel, complément de sécurité

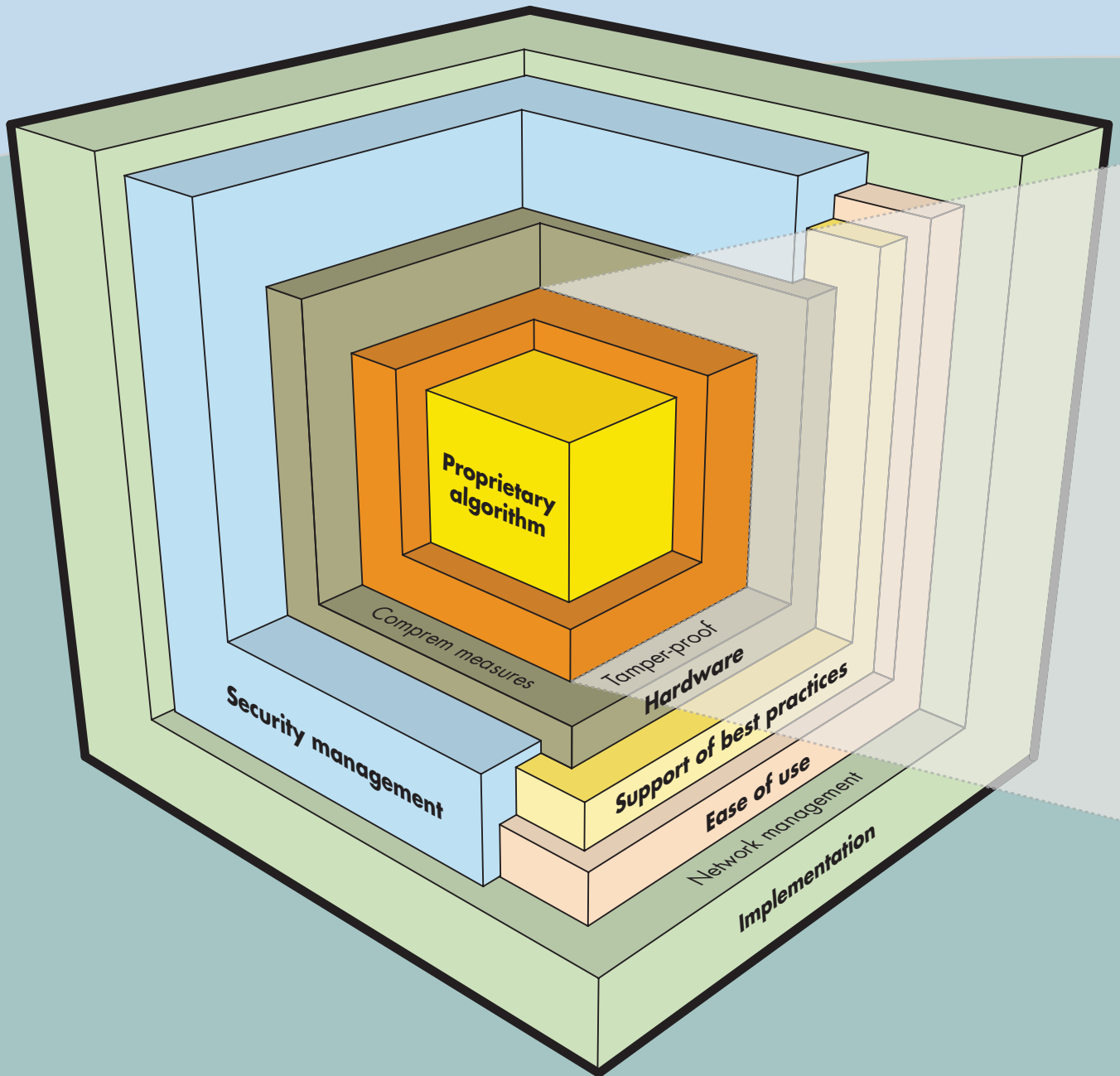
Les fonctions-clés de l'algorithme sont assistées par la construction des processeurs des appareils de chiffrement de Crypto AG. Il s'agit ici à la fois de la conception du module de sécurité (security module) à l'intérieur duquel sont exécutées les fonctions relatives au chiffrement, et de la construction des boîtiers des appareils. Vos paramètres de sécurité (master keys) sont mémorisés – eux-mêmes chiffrés – dans le module de sécurité des appareils de chiffrement. Tous les processus de chiffrement sont ainsi protégés des influences et dangers provenant des réseaux de communication. De plus, la protection contre les manipulations intégrée à la conception matérielle (matériel inviolable) du module assure une protection efficace de vos éléments de

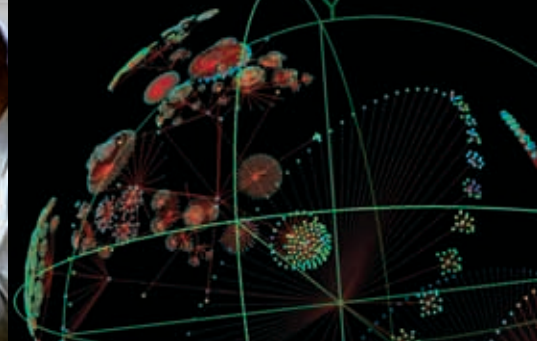
sécurité logiques contre les accès non autorisés.

La conception des appareils de chiffrement repose sur une séparation systématique des flux de données chiffrés et non chiffrés (séparation rouge-noir). Des exigences extrêmement strictes – appliquées depuis le début du développement de chaque appareil – sur la construction et le choix des matériaux, garantissent par ailleurs le blocage des rayonnements porteurs d'informations (comprenant mesures: mesures contre les émissions compromettantes) propres à tout appareil électronique. Les appareils sont soumis à des contrôles approfondis de résistance aux rayonnements et de prévention des rayonnements dans le laboratoire de tests de Crypto AG.



Your information is surrounded by different layers of Security Architecture



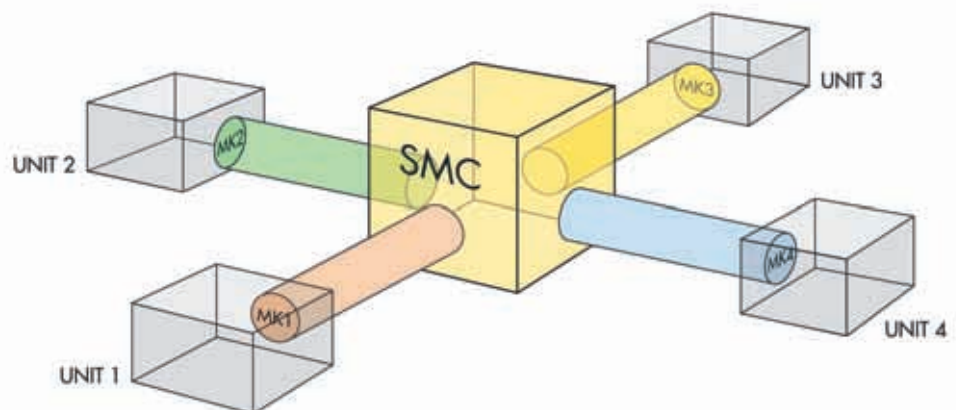


La gestion de sécurité: centralisée, efficace et confortable

Une gestion confortable et individualisable des fonctions de sécurité est décisive pour une sécurité sans faille, et accroît en outre considérablement l'efficacité de votre système de communication. Le niveau d'élaboration de l'Architecture de Sécurité de Crypto AG vous permet d'effectuer rapidement et confortablement toutes les tâches de gestion à l'écran au sein du Security Management Centre (SMC) sur ordinateur de Crypto AG, notamment la distribution chiffrée des clés en ligne ou hors ligne, la formation de groupes de chiffrement, la gestion de rela-

tions autorisées entre usagers du réseau et groupes d'utilisateurs, ainsi que l'ajout ou l'exclusion d'appareils au sein de votre programme de sécurité. Résultat: même la disparition ou le vol d'appareils de chiffrement ne constitue pas un problème. Les clés peuvent être remplacées automatiquement et à des moments définis. Le fonctionnement sans interruption de votre infrastructure de communication est assuré même pendant le changement de clé grâce à un système sophistiqué. Vous bénéficiez ainsi d'une solution de chiffrement dotée d'une haute disponibilité garantie.

Grâce au chiffrement des paramètres de sécurité enregistrés (local security), à l'échange de clé chiffré et à la séparation du SMC et du réseau public par le Message Scheduler, vous pouvez être certain que vos données sont entièrement protégées. Avec le Security Management Centre de Crypto AG, vous gérez donc votre sécurité de réseau à un niveau identique à celui avec lequel les appareils de chiffrement de Crypto AG protègent votre communication grâce à l'Architecture de Sécurité.





Le module de sécurité matériel

Les appareils de chiffrement de Crypto AG implémentent le chiffrement dans un module de sécurité séparé, protégeant vos informations contre tout risque d'accès venant de l'extérieur. Grâce au matériel protégé contre les manipulations (inviolable), le processus de chiffrement lui-même est protégé contre les accès et manipulations non autorisés. D'autre part, le module sépare entièrement le processus de chiffrement de l'environnement ICT dans lequel il a lieu. Cela signifie également une protection efficace contre les virus et les attaques en provenance

du réseau. Par ailleurs, cette séparation accroît la vitesse du processus de chiffrement.

Forcer le matériel entraîne l'effacement automatique de tous les paramètres de sécurité. Le chiffrement reposant sur matériel, tel que le propose Crypto AG, est donc la meilleure garantie d'une sécurité maximale.

Le chiffrement ayant lieu dans un module de sécurité séparé, les performances du réseau ne sont pas altérées, vous ne perdez donc pas de temps inutilement lors de vos communications.



Mise en œuvre des meilleures pratiques

L'Architecture de Sécurité de Crypto AG est conçue de manière à supporter les pratiques reconnues de consolidation de votre sécurité et à les intégrer directement au sein de votre politique de sécurité. Ceci concerne principalement le changement de clé périodique que vous pouvez réaliser simplement, de manière automatisée et chiffrée à dates fixes, grâce à la hiérarchie des clés et au concept de gestion de la sécurité de Crypto AG. Pour ce processus, les appareils de chiffrement de Crypto AG utilisent des clés valables une seule fois et brièvement. En application du

principe de la répartition du secret, la gestion de l'algorithme (paramétrage du profil) est séparée de la gestion des clés. Selon ce même principe, l'Architecture de Sécurité tient séparées la gestion et l'application de communication chiffrée des appareils (au niveau cryptographique). Cette séparation est également importante pour le contrôle des accès aux paramètres de sécurité. Dans ce cadre, les différents acteurs (p. ex. le security manager, le network manager, l'operator) possèdent des droits d'accès différents.



www.crypto.ch

Crypto AG – To Remain Sovereign

Crypto AG est le partenaire compétent des entreprises qui souhaitent manier des informations efficacement et en toute sécurité, En tant qu'entreprise suisse, indépendante aux niveaux juridique et économique, nous ne sommes soumis à aucune restriction d'exportation. Depuis plus de 50 ans, nous nous consacrons au développement, à la réalisation et à la mise en œuvre de solutions de sécurité individuelles. Pendant toute la durée de vie de nos systèmes, nous assurons un service après-vente et une formation garantissant une exploitation autonome et une grande disponibilité dans tous les environnements. Vous pouvez donc faire confiance à notre compétence et à notre savoir-faire. Des clients de plus de 130 pays nous ont déjà accordé leur confiance.

Crypto AG, siège principal

Crypto AG
Case postale 460
CH-6301 Zug
Suisse
Tél. +41 41 749 77 22
Fax +41 41 741 22 72
crypto@crypto.ch
www.crypto.ch

Crypto AG, bureaux régionaux

Abidjan

Crypto AG
01 B.P. 5852
Abidjan 01
République de Côte d'Ivoire
Tél. +225 22 41 17 71
Fax +225 22 41 17 73

Abu Dhabi

Crypto AG
Regional Office Middle East
P.O. Box 41076
Abu Dhabi
Emirats Arabes Unis
Tél. +971 2 64 22 228
Fax +971 2 64 22 118

Buenos Aires

Crypto AG
Maipu 1256 PB «A»
1006 Buenos Aires
Argentine
Tél. +54 11 4312 1812
Fax +54 11 4312 1812

Kuala Lumpur

Crypto AG
Regional Office Pacific Asia
No. 2 Jalan SS7/11 Kelana Jaya
47301 Petaling Jaya
Malaisie
Tél. +60 3 7872 2150
Fax +60 3 7872 2140

Muscat

Crypto AG Representative Office
P.O. Box 2911
Postal Code 111
Seeb
Sultanat de Oman
Tél. +968 2449 4966
Fax +968 2449 8929