



**Die Sicherheitsarchitektur für höchste Ansprüche
designed by Crypto AG**



Die Sicherheitsarchitektur der Crypto AG – elegant und effektiv

Seit 1952 sorgt Crypto AG stets mit den modernsten Mitteln der Kryptographie dafür, dass Sie Ihre vitalen und sensiblen Informationen vor unberechtigtem Zugriff schützen können. Bis heute durchdringt diese Zielsetzung die gesamte Philosophie des Unternehmens. Die Essenz der Sicherheitsphilosophie bildet dabei unsere – in ihrer Art einzigartige und über Jahrzehnte weiterentwickelte – Sicherheitsarchitektur.

Das Konzept der Architektur erlaubt Crypto AG gleichzeitig die Übergabe einer für jeden Kunden spezifizierbaren Algorithmusbasis, die Sicherstellung perfekten kryptografischen Schutzes und damit eine optimale Unterstützung der Security Policy der Kunden. Ihnen gewährt die Sicherheitsarchitektur im Gegenzug – durch Ihre Einflussnahme – vollständige Unabhängigkeit Ihrer Verschlüsselungslösung, Selbstbestimmung aller kryptographischen Bereiche und Verifikation der Funktionsweise Ihres Algorithmus.

Das Fundament der Sicherheitsarchitektur bildet der originäre Basisalgorithmus von Crypto AG. Dessen Design repräsentiert kryptographisch höchstes Niveau und bildet die Grundlage für Lösungen einzigartiger Sicher-

heitsqualität. Mit dem Algorithmus sind mehrere interdependent agierende Kernfunktionen der Architektur verknüpft, die zusammen einen äusserst resistenten und stabil funktionierenden kryptologischen Nukleus bilden. Dessen Funktionalität wird durch hardwarebasierte Chiffrierung in einem separaten und vom Informatik-Netz (ICT-Netz) getrennten Sicherheitsmodul unterstützt. Die Flexibilität der Architektur ist im Chiffrieralltag mit dem effizienten und bequem zu bedienenden Security- und Key-Management nutzbar. Dieses arbeitet nahtlos mit Ihrem eigenen Network-Management zusammen. Insgesamt erfüllt die Sicherheitsarchitektur von Crypto AG somit Ihre Anforderungen an die hohe Verfügbarkeit Ihrer Chiffrierlösung.



Die Kernfunktionen des Algorithmus machen Sie unabhängig

Vom geheimen Basisalgorithmus (Secret Proprietary Algorithm) von Crypto AG erhalten Sie eine eigene Ausprägung. Mit dieser jeweils eigenständigen Ausgangslage schützt Sie Crypto AG vor dem Mitwissen anderer Kunden. Damit Sie vollkommen von Crypto AG unabhängig werden und in der Lage sind, Ihre Sicherheit selbst zu kontrollieren, erlaubt Ihnen das Design des Algorithmus, wesentliche Funktionen des Algorithmus selbst zu bestimmen. Mit Ihrer nunmehr selbst-vorgenommenen spezifischen Profilierung übernehmen Sie den Algorithmus vollständig in Ihren Besitz. Das trägt Ihren Bedürfnissen nach Autonomie und Separation Rechnung. Sie verfügen nun über einen weltweit absolut singulären Algorithmus, der jetzt weder Crypto AG noch Dritten bekannt oder zugänglich ist. Einzig Sie selbst kennen und kontrollieren Ihre Sicherheit.

Der Algorithmus orientiert sich dabei am symmetrischen Verschlüsselungsverfahren, in dem für Chiffrierung und Dechiffrierung derselbe Schlüssel verwendet wird. Der (digitale) Schlüssel muss vor allem höchsten Anforderungen an seine Zufälligkeit genügen. Dafür sorgt ein hardwarebasierter, separater und höchstwertiger Generator von Zufallszahlen. Auf dieser Basis garantiert die Schlüssellänge von minimal 128 Bit, im Zusammenspiel mit der Komplexität Ihres geheimen Chiffrieralgorithmus, die Aussichtslosigkeit von Attacken auf Ihr System.

Resistente kryptographische Protokolle erlauben das Definieren von Schlüsseln auf mehrfachen hierarchischen Ebenen (Multi-hierarchical Key Grouping). Das verschafft Ihrem Sicherheitsmanagement eine hohe Flexibilität. In der praktischen Anwendung der Geräte von Crypto AG können Sie deshalb Ihre Security Policy gezielt unterstützen, beispielsweise indem Sie –

je nach Anwendungsszenario – kryptografische Kommunikationsgruppen unterschiedlicher Hierarchiestufen und mit gegenseitiger Überlappung festlegen. Kooperation und Separation lassen sich dabei jederzeit veränderten Organisationsbedürfnissen anpassen. Die Anzahl Teilnehmer ist unbeschränkt. Damit Sie als Kunde und Inhaber Ihres eigenen Algorithmus absolute Gewissheit über die Struktur und die Funktionsweise Ihres Algorithmus haben, verschafft Ihnen die Algorithmusbeschreibung von Crypto AG Transparenz in der Evaluation. Zusammen mit dem einzigartigen Acceptance Cipher Check (ACC) steht Ihnen auf Wunsch ausserdem ein leistungsfähiges Werkzeug zur Verfügung, um selbständig jederzeit und überall die korrekte Implementation und Funktionsweise Ihres Algorithmus zu überprüfen. Die Verifikation der kryptographischen Vorgänge schafft Verständnis und Vertrauen in die Lösungen von Crypto AG.



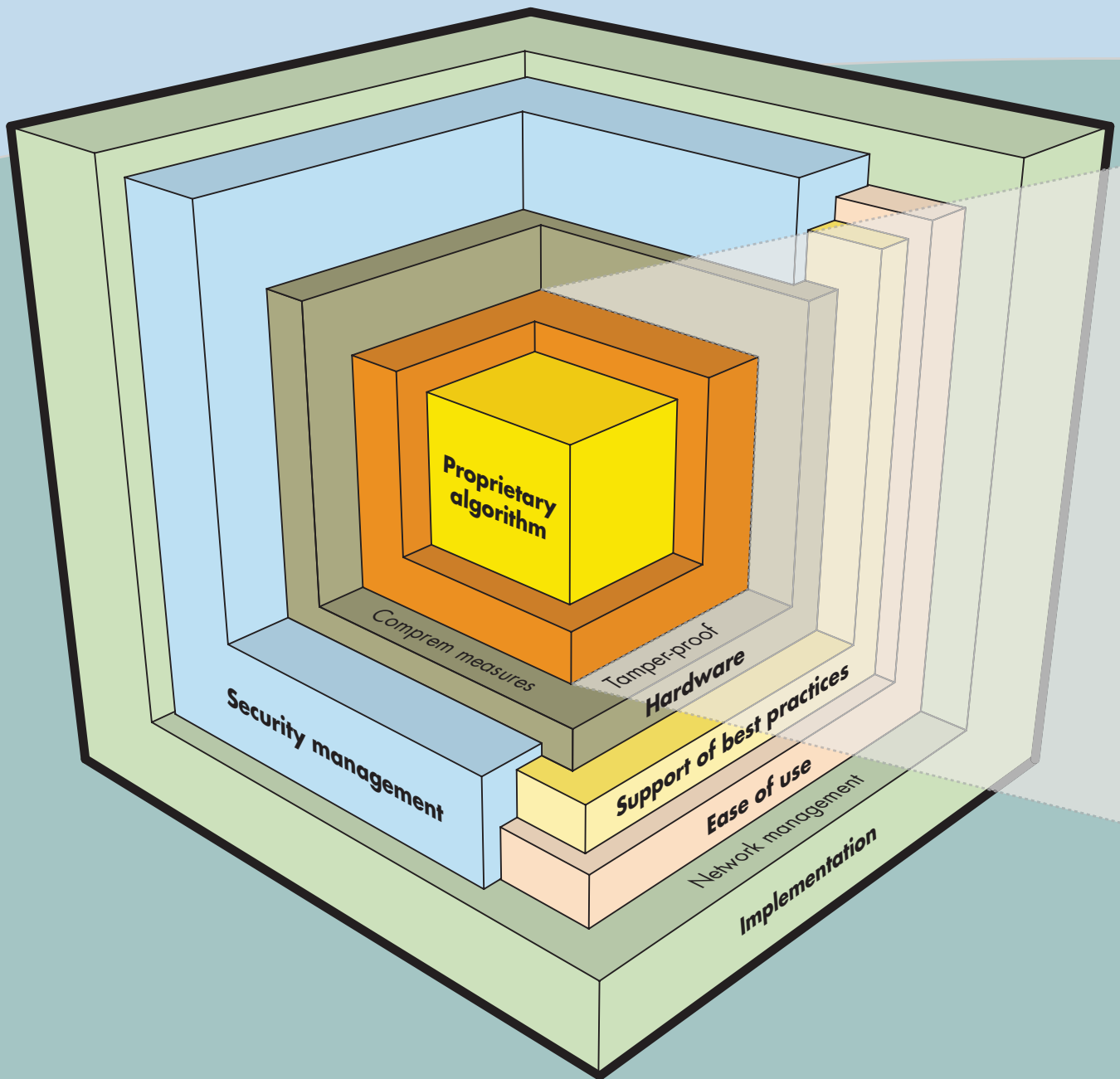
Hardware komplettiert die Sicherheit

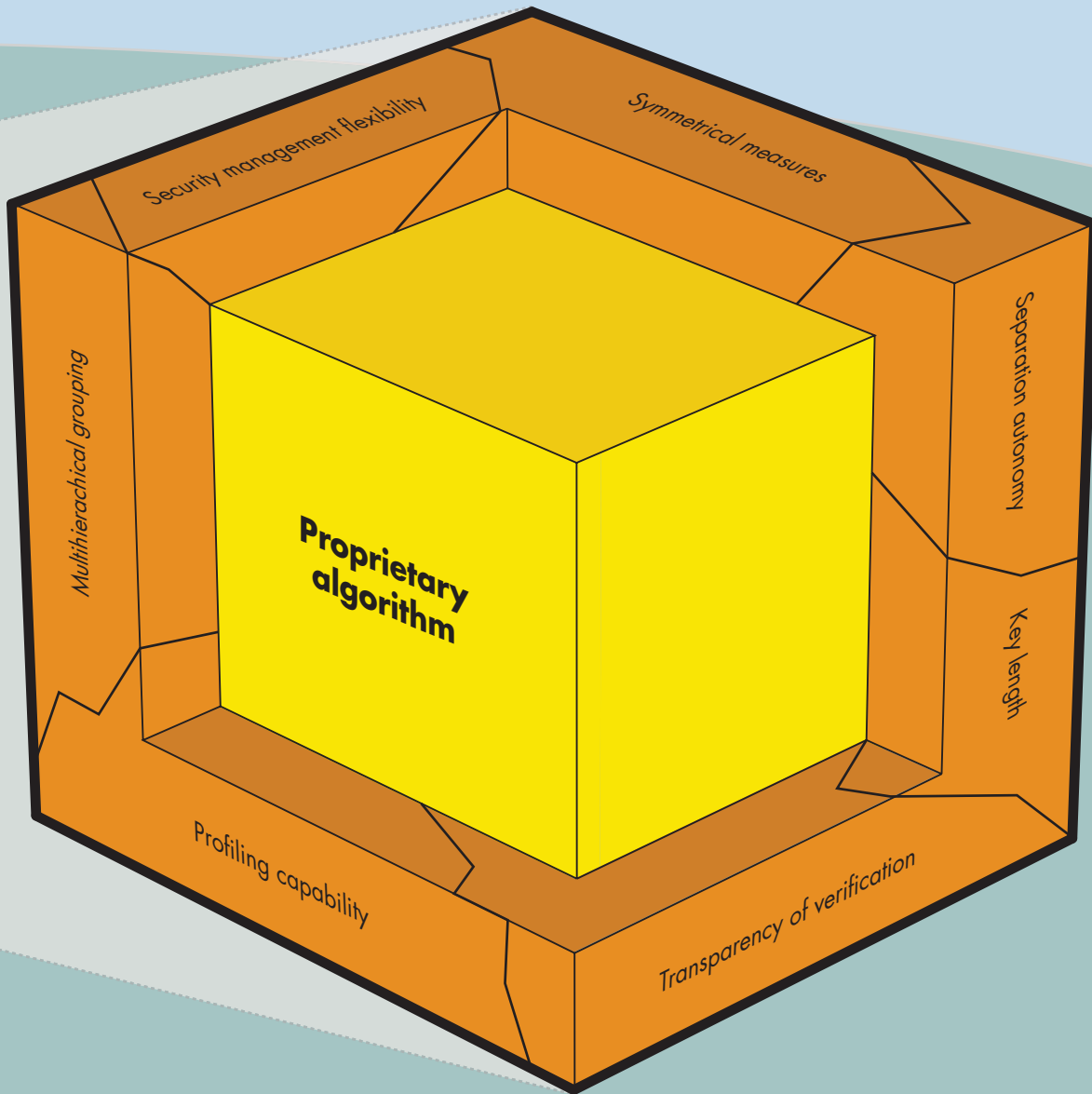
Die Kernfunktionen des Algorithmus werden von der Konstruktion der Prozessoren der Verschlüsselungsgeräte von Crypto AG unterstützt. Diese umfasst sowohl das Design des Sicherheitsmoduls (Security Module), in dem die kryptologisch relevanten Funktionen ablaufen, als auch die Konstruktion der Gerätegehäuse. Im Sicherheitsmodul der Chiffriergeräte sind Ihre Sicherheitsparameter (Master Keys) ihrerseits verschlüsselt abgelegt. Alle Chiffrierprozesse laufen somit geschützt vor Einflüssen und Gefahren der Kommunikationsnetze ab. Darüber hinaus sorgt der ins Hardwaredesign integrierte Manipulationsschutz (tamper-proof Hardware) des Moduls für einen effektiven Schutz Ihrer lo-

gischen Sicherheitselemente vor unbefugtem Zugriff.

Das Chiffriergerätedesign ist auf eine konsequente Trennung chiffrierter und unchiffrierter Datenströme (Red/Black-Separation) ausgelegt. Gleichzeitig gewährleisten – von Beginn der Entwicklung eines Geräts an – strengste Auflagen an Konstruktion und Materialauswahl die Abschirmung verätherischer Abstrahlung (Comprem Measures: Massnahmen gegen kompromittierende Abstrahlung, die an sich jedem elektronischen Gerät eigen sind). Im Prüflabor der Crypto AG werden die Geräte umfassend auf ihre Einstrahlungsfestigkeit und Vermeidung von Ausstrahlung geprüft.

Your information is surrounded by different layers of Security Architecture





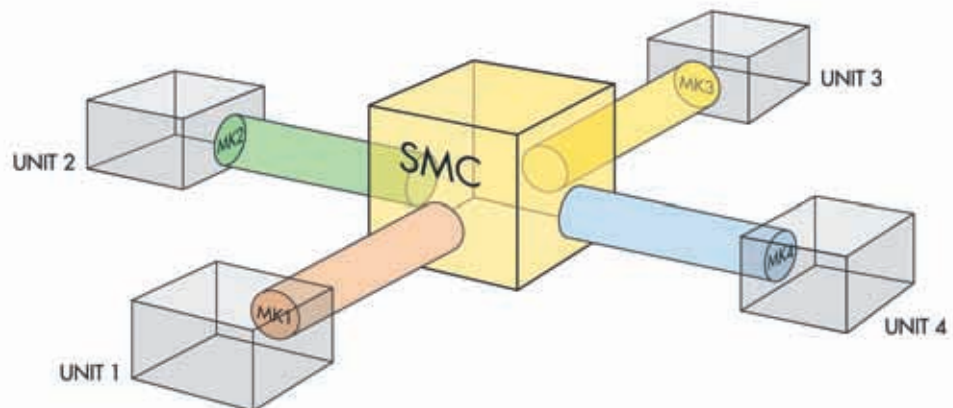


Das Security Management: zentral, effizient und komfortabel

Ein bedienerfreundliches, individualisierbares Management der Sicherheitsfunktionen ist für lückenlose Sicherheit mitentscheidend und erhöht die Effizienz Ihres Kommunikationssystems wesentlich. Dank der ausgereiften Sicherheitsarchitektur von Crypto AG können Sie alle Management-Aufgaben über ein computerbasiertes Security Management Centre (SMC) von Crypto AG schnell und bequem am Bildschirm erledigen. Das erlaubt unter anderem chiffrierte Online- und/oder Offline-Schlüsselverteilung, Bildung kryptologischer Gruppen, das Verwalten autorisierter Beziehungen

unter Netzwerk-Teilnehmern und Teilnehmer-Gruppen, sowie den Einbezug oder Ausschluss von Geräten in Ihre Sicherheitsdisposition. Selbst verloren gegangene oder entwendete Chiffriergeräte sind für Sie deshalb kein Problem. Schlüssel können automatisch und terminierbar ausgewechselt werden. Der unterbrechungsfreie Betrieb Ihrer Kommunikationsinfrastruktur bleibt dank des ausgefeilten Schlüsselsystems der Geräte selbst während des Schlüsselaustauschs gewährleistet. Hohe Verfügbarkeit Ihrer Chiffrierlösung ist somit garantiert.

Dank der Verschlüsselung gespeicherter Sicherheitsparameter (Local Security), dem chiffrierten Schlüsselaustausch und der Trennung von SMC und dem öffentlichen Netzwerk durch den Message Scheduler, ist ein umfassender Schutz Ihrer Daten auf dem SMC garantiert. Mit dem Security Management Centre von Crypto AG verwalten Sie Ihre Netzwerksicherheit deshalb auf demselben Sicherheitsniveau, auf dem die Chiffriergeräte von Crypto AG – dank der Sicherheitsarchitektur – Ihre Kommunikation an sich schützen.





Das Hardware-Sicherheitsmodul

Chiffriergeräte von Crypto AG haben die Chiffrierung in einem separaten Sicherheitsmodul implementiert und schützen Ihre Informationen gegen alle Risiken äusseren Zugriffs. Dank der manipulationsgeschützten (tamper-proof) Hardware ist auch der Chiffrierprozess selbst vor unbefugtem Zugriff und Manipulation geschützt. Ausserdem trennt das Modul damit den Chiffrierprozess vollständig von der ICT-Umgebung, in deren Rahmen er abläuft, ab. Das bedeutet zugleich einen wirksamen Schutz vor Viren und Angriffen aus dem Netz. Ausserdem erhöht diese Trennung die Geschwindigkeit des Chiffrierprozesses.

Ein Aufbrechen der Hardware hat das automatische Löschen aller Sicherheitsparameter zur Folge. Hardwarebasierte Chiffrierung, wie sie Crypto AG offeriert, ist deshalb die beste Garantie für höchste Sicherheit. Dank der Chiffrierung im separaten Sicherheitsmodul wird die Leistungsfähigkeit des Netzwerks nicht beeinträchtigt. So verlieren Sie in Ihrer Kommunikation nicht unnötig Zeit.



Support von Best Practices

Die Sicherheitsarchitektur von Crypto AG ist so ausgelegt, dass sie anerkannte Praktiken zur Festigung Ihrer Sicherheit unterstützt und nahtlos in Ihre Security Policy integrierbar ist. Dies betrifft vor allem den periodischen Schlüsselwechsel, den Sie durch die Schlüsselhierarchie und das Konzept des Security Managements von Crypto AG einfach, automatisiert, terminierbar und verschlüsselt vollziehen können. In diesem Prozess verwenden Chiffriergeräte von Crypto AG nur einmal und nur kurze Zeit gültige Schlüssel. Gemäss dem Prinzip der Geheimnisaufteilung, ist das Manage-

ment des Algorithmus (Profilierung) vom Schlüsselmanagement abgekoppelt. Demselben Grundsatz entsprechend, zielt die Sicherheitsarchitektur darauf ab, Management und chiffrierte Kommunikations-Anwendung der Geräte (kryptographisch) auseinander zu halten. Diese Separation ist auch für die Zugriffskontrolle auf die Sicherheitsparameter wichtig. Hierbei werden verschiedenen Rolleninhabern (z.B. Security Manager, Network Manager, Operator) unterschiedliche Zugriffsrechte gewährt.



www.crypto.ch

Crypto AG – To Remain Sovereign

Crypto AG ist Ihr kompetenter Partner, wenn Sie effizient und sicher mit Informationen arbeiten wollen.

Als juristisch und wirtschaftlich unabhängiges Schweizer Unternehmen sind wir keinen Exportrestriktionen unterworfen. Seit über 50 Jahren konzentrieren wir uns auf die Entwicklung, Produktion und Implementati- on von individuellen Sicherheitslösungen.

Unser Angebotspaket enthält modernste Technologie und umfassende Dienstleistun- gen. Während der gesamten Systemlebens- dauer stellen wir Ihnen After-Sales-Support und Produktraining zur Verfügung, die einen autonomen Betrieb und hohe Verfügbarkeit in jeder Anwenderumgebung garantieren.

Vertrauen deshalb auch Sie auf die Kompe- tenz und Leistungsfähigkeit von Crypto AG, genau so wie unsere Kunden aus über 150 Ländern.

Crypto AG, Hauptsitz

Crypto AG
Postfach 460
CH-6301 Zug
Schweiz
Tel. +41 41 749 77 22
Fax +41 41 741 22 72
crypto@crypto.ch
www.crypto.ch

Crypto AG, regionale Büros

Abidjan

Crypto AG
01 B.P. 5852
Abidjan 01
Elfenbeinküste
Tel. +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
Vereinigte Arabische Emirate
Tel. +971 2 64 22 228
Fax +971 2 64 22 118

Buenos Aires

Crypto AG
Maipu 1256 PB «A»
1006 Buenos Aires
Argentinien
Tel. +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
Malaysia
Tel. +60 3 7872 2150
Fax +60 3 7872 2140

Muscat

Crypto AG
Regional Office
Seeb PC 111
Sultanat Oman
Tel. +968 2449 4966
Fax +968 2449 8929