



**Удовлетворяющая самым высоким запросам
архитектура безопасности от фирмы Crypto AG**



Архитектура безопасности от фирмы Crypto AG – элегантность и эффективность

Уже с 1952 г. фирма Crypto AG, используя самые современные средства криптографии, стремится защищать Вашу жизненно важную и конфиденциальную информацию от несанкционированного доступа. И до сих пор этой задаче подчинена вся без остатка философия фирмы. Квинтэссенцией этой философии является наша совершенствуемая в продолжение десятилетий и единственная в своем роде архитектура безопасности.

Концепция архитектуры дает Crypto AG возможность предоставлять настраиваемую под требования каждого конкретного заказчика алгоритмическую базу и обеспечивать совершенную криптографическую защиту, оказывая тем самым оптимальную поддержку стратегии защиты пользователя. В свою очередь и Вам – благодаря Вашему собственному участию – архитектура безопасности гарантирует полную автономность Ваших криптографических решений, независимое определение все криптографических зон и верификацию Вашего алгоритма.

Основу архитектуры безопасности образует оригинальный базовый алгоритм от фирмы Crypto AG. Его структура отражает высший уровень криптографии и является основой для обеспечения уникального уровня безопасности. С ал-

горитмом связано несколько согласованно взаимодействующих стержневых функций архитектуры, которые совместно образуют в высшей степени устойчивое к взлому и стабильно функционирующее криптографическое ядро. Такая функциональность поддерживается осуществляемым аппаратными средствами шифрованием в отдельном и отделенном от информационной сети (ИСТ-сети) модуле безопасности. Гибкость архитектуры успешно используется в повседневной практике шифрования с ее эффективным и удобным менеджментом безопасности и распределения ключей. Последний вплотную стыкуется с Вашей собственной организацией работы сети. В итоге архитектура безопасности от Crypto AG способна удовлетворить всем требованиям к высокой функциональной готовности Ваших шифровальных решений.



Стержневые функции алгоритма делают Вас полностью независимым

От фирмы Crypto AG Вы получаете индивидуальный вариант секретного базового алгоритма (Secret Proprietary Algorithm). Таким индивидуальным в каждом конкретном случае подходом Crypto AG предотвращает возможность того, что касающиеся Вас сведения станут доступными для других клиентов фирмы. Чтобы Вы стали полностью независимыми от фирмы Crypto AG и были в состоянии сами контролировать свою безопасность, алгоритм устроен таким образом, что его существенные функции Вы определяете сами. Произведя своими силами своего рода специфическое профилирование, Вы становитесь полным хозяином алгоритма. Такое положение вещей отвечает Вашему стремлению к автономности и раздельности. В Вашем распоряжении не имеющий аналогов во всем мире алгоритм, который отныне недоступен и незнаком ни фирме Crypto AG, ни какой-либо третьей стороне. Только Вы сами располагаете всеми нужными сведениями и контролируете собственную безопасность.

Сам алгоритм основан на методе симметричного кодирования, при котором для шифрования и дешифрования используется один и тот же ключ. Такой (цифровой) ключ должен, в первую очередь, отвечать строжайшим требованиям к природе его случайности. Последнее обеспечивает высокосовременный автономный аппаратный генератор случайных чисел. Получаемая при этом длина ключа не менее 128 бит в сочетании со сложной структурой вашего секретного алгоритма шифрования гарантирует безуспешность любых атак на Вашу систему.

Устойчивые к взлому криптографические протоколы позволяют создавать ключи для многоуровневых иерархических систем (так наз. многоуровневые групповые ключи). Это придает особой гибкости Вашему менеджменту безопасности. Поэтому аппараты фирмы Crypto AG на практике позволят Вам целенаправленно поддерживать Вашу стратегию защиты, например, задавая – в рамках Вашей концепции реализации – криптографические коммуникационные

группы разных уровней иерархии с взаимным наложением. Кооперирование и разделение при этом каждый раз осуществляются согласно непрерывно изменяющимся организационным потребностям. Число участников обмена данными не ограничено.

Вам как заказчику и владельцу собственного алгоритма нужно полное понимание его структуры и принципа действия – и Crypto AG обеспечивает это за счет прозрачности описания алгоритма на этапе его оценки. В сочетании с таким уникальным средством контроля, как Acceptance Cipher Check (ACC), дополнительно и при желании Вам предоставляется мощный инструмент для самостоятельной проверки правильности реализации и функционирования алгоритма в различных приложениях – в любое время и в любом месте. Верификация криптографических процедур обеспечит понимание решений от фирмы Crypto AG и повысит доверие к ним.



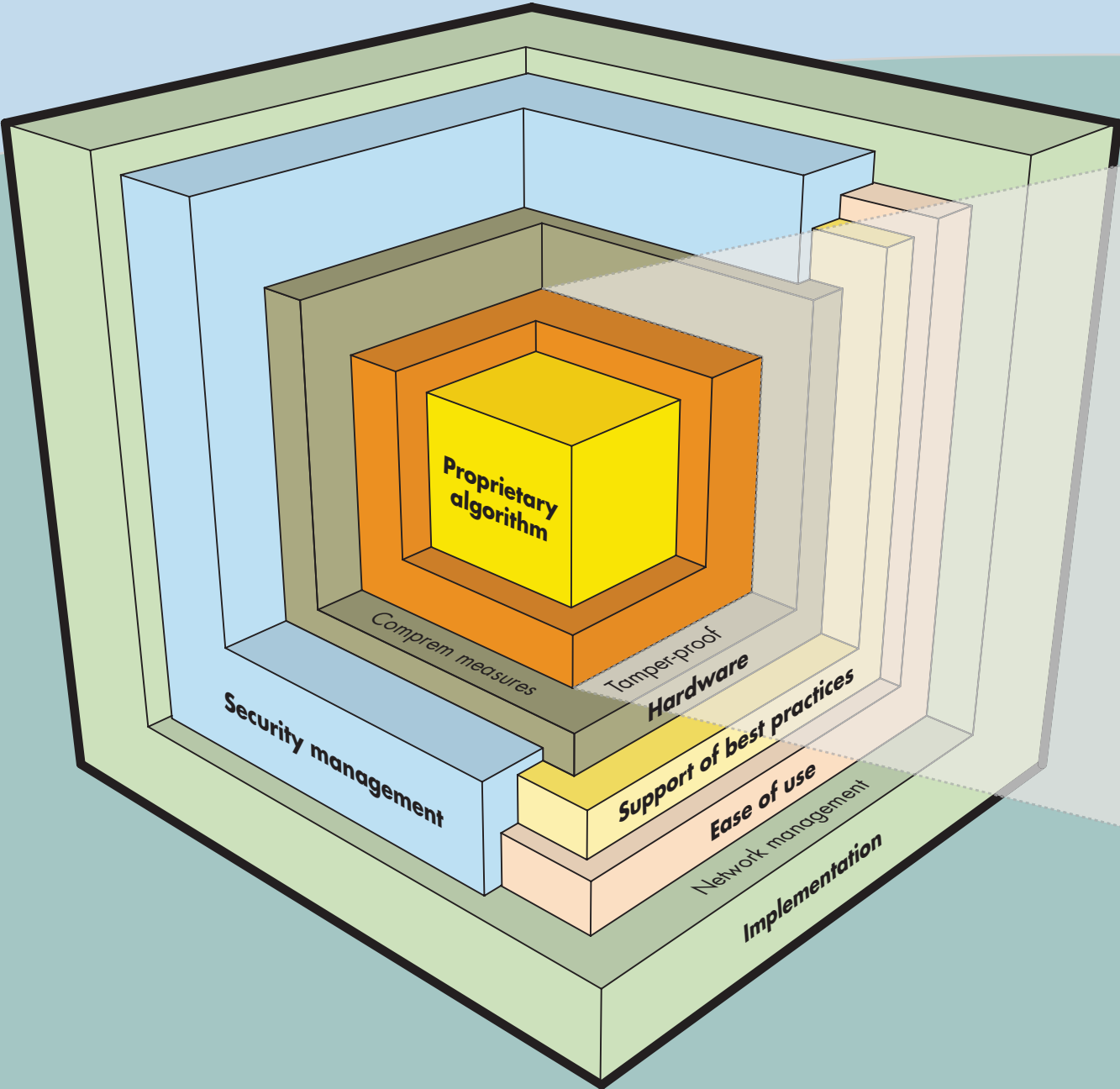
Аппаратное обеспечение – на службу безопасности

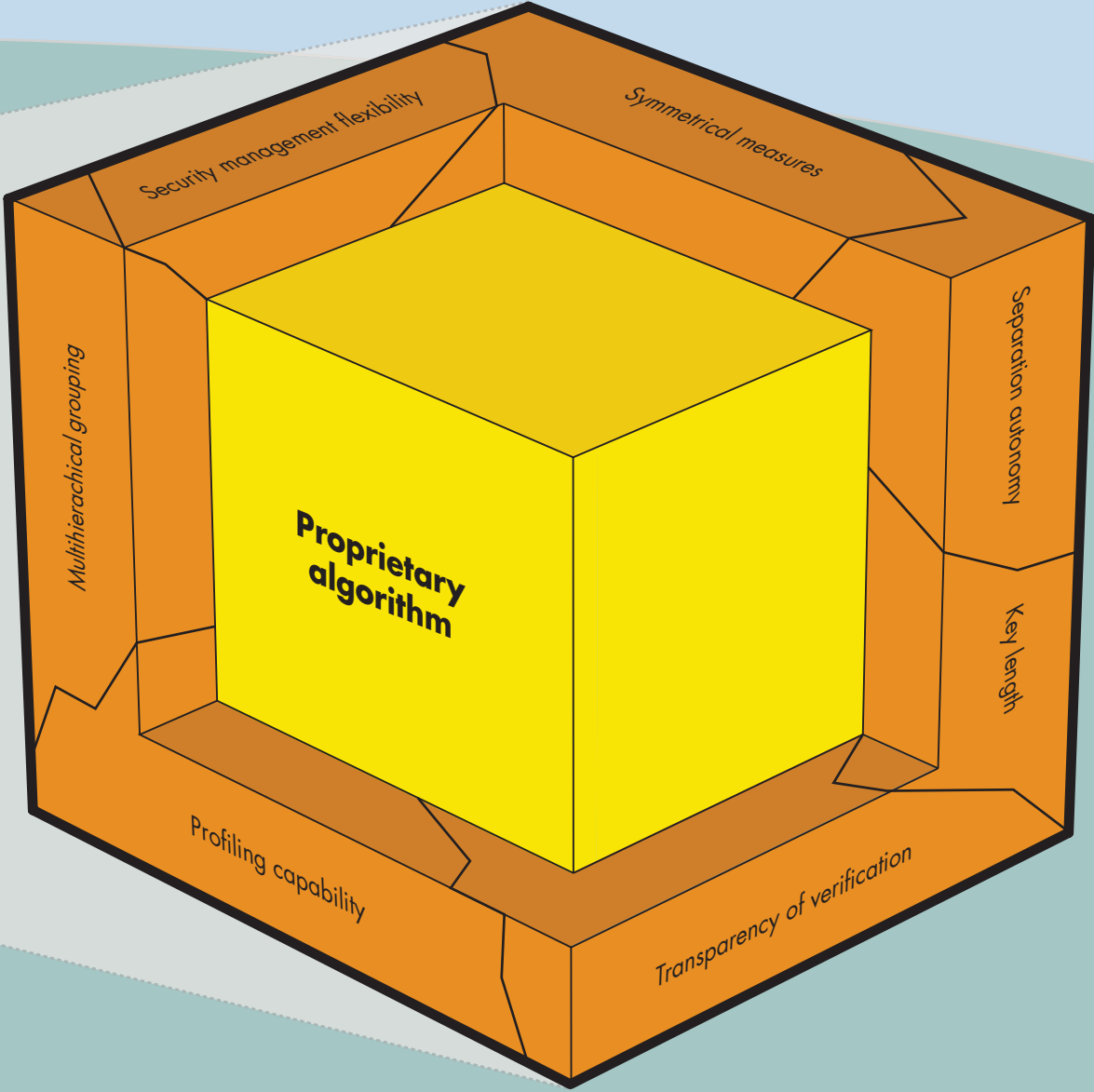
Стержневые функции алгоритма поддерживаются конструкцией процессоров шифровальных аппаратов фирмы Crypto AG. Сюда относится как строение модуля безопасности (Security Module), в котором выполняются криптологически важные функции, так и конструкция корпуса самого аппарата. В модуле безопасности шифровальных аппаратов сохранены – опять-таки в зашифрованном Вами виде – параметры безопасности (Master Keys). Таким образом, все процедуры шифрования защищены от вмешательства и угрозы взлома со стороны сетей передачи данных. Более того, встроенная на аппаратном уровне защита модуля от манипуляций (tamper-proof Hardware) обеспечивает эффективную защиту Ваших логических элементов безопасности от несанкционированного доступа к ним.

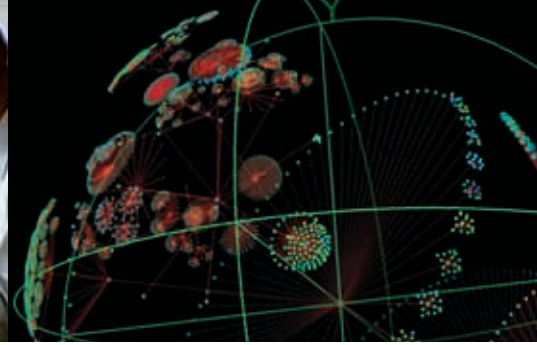
Архитектура шифровальных аппаратов предусматривает последовательное разделение зашифрованных и незашифрованных потоков данных (Red/Black-Separation). Предъявляемые с самого начала создания прибора строжайшие требования в отношении конструктивных решений и материалов гарантируют экранирование «предательских» излучений (Comprem Measures: меры против утечки информации через излучения, которые, собственно говоря, присущи любому электронному прибору).

Испытательная лаборатория фирмы Crypto AG всесторонне проверяет аппараты на стойкость к внешнему облучению и на предотвращение собственных излучений.

Your information is surrounded by different layers of Security Architecture





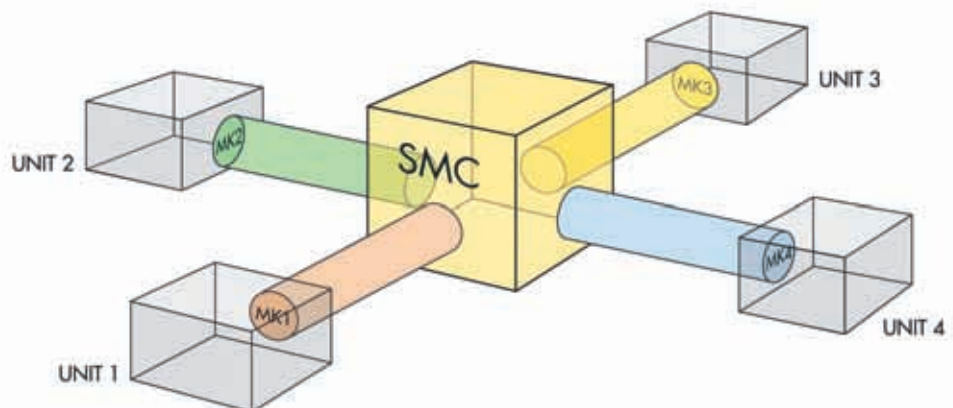


Менеджмент безопасности: централизованный, эффективный и удобный

Дружественный к пользователю и индивидуально настраиваемый менеджмент функций защиты – одно из условий полной безопасности и высокой эффективности системы передачи информации. Благодаря отработанной архитектуре безопасности от фирмы Crypto AG все задачи менеджмента можно быстро и удобно решать через экран компьютеризованного Центра менеджмента безопасности (Security Management Centre SMC) от Crypto AG. В числе прочего, он позволяет шифрованное распределение ключей в онлайн-овом или офлайн-овом режиме, создание криптологических групп, управление авторизован-

ными взаимоотношениями между участниками и группами участников сети, а также активирование и деактивирование аппаратуры для обеспечения безопасности обмена информацией. Поэтому даже в случае кражи или утери шифровальных аппаратов проблем у Вас не возникает. Ключи можно менять автоматически в заданные сроки. Бесперебойность функционирования Вашей инфраструктуры обмена информацией обеспечена благодаря выверенной системе управления ключами даже во время их замены. Таким образом, Ваши шифровальные системы постоянно находятся в состоянии готовности к эксплуатации.

Благодаря шифрованию сохраненных параметров безопасности (Local Security), шифрованной замене ключей и разделению SMC и открытой сети посредством диспетчера сообщений (Message Scheduler), достигается полная защищенность Ваших данных на SMC. Через Центр менеджмента безопасности от фирмы Crypto AG Вы управляете безопасностью сети на том же уровне, на котором шифровальные аппараты фирмы Crypto AG защищают – передаваемую Вами информацию.





Аппаратный модуль безопасности

Шифровальные аппараты от Crypto AG производят шифрование в отдельном модуле безопасности, что защищает Ваши данные от какого-либо риска вторжений извне. Благодаря защищенным от манипуляций (tamper-proof) аппаратным средствам и сам процесс шифрования защищен от несанкционированного доступа и манипуляций. Кроме того, модуль полностью разделяет процесс шифрования и ИСТ-среду, в рамках которой этот процесс протекает. Одновременно обеспечивается действенная защита от вирусов и атак из сети. К тому же такое разделение повышает скорость процесса шифрования.

Взлом корпуса аппаратного устройства автоматически приводит к уничтожению всех параметров безопасности. Поэтому аппаратное шифрование, предлагаемое фирмой Crypto AG, является наилучшей гарантией максимальной безопасности. Благодаря шифрованию в автономном модуле безопасности не снижается пропускная способность сети. Предотвращается также ненужная трата времени на установление связи.



Учтены новейшие достижения

Архитектура безопасности фирмы Scurto AG благодаря своей структуре способна поддерживать общепризнанные практические приемы по повышению Вашей безопасности и практически без зазора встраивается в Вашу стратегию защиты. Сказанное касается, прежде всего, периодического изменения ключей, которые Вы, благодаря иерархии ключей и концепции менеджмента безопасности от фирмы Scurto AG, можете производить просто, в автоматическом режиме, в заданные сроки и скрытно. В этом процессе шифровальные аппараты фирмы Scurto AG используют ключи, действующие только однократно и в течение непродолжительного времени. Следуя принципу

распределения секретности, менеджмент для алгоритма (профилирование) отделен от менеджмента ключей. Этому же принципу отвечает и направленность архитектуры безопасности на то, чтобы развести (криптографически) врозь менеджмент и зашифрованное задействование аппаратов. Такое разнесение важно также для контроля доступа к параметрам безопасности. При этом сотрудники – в зависимости от их должностных полномочий (например, менеджер по безопасности, сетевой администратор, оператор) – имеют разные права доступа.



www.crypto.ch

Crypto AG – To Remain Sovereign

Crypto AG – это Ваш компетентный партнер, если для Вас важно работать с информацией эффективно и надежно.

Являясь юридически и экономически независимым швейцарским предприятием, мы свободны от каких-либо ограничений на экспорт продукции. Уже в течение свыше 50 лет мы концентрируем свои усилия на разработке, создании и внедрении индивидуальных систем криптозащиты.

Наш пакет предложений содержит самую современную технологию и всесторонние услуги. Мы предоставляем на весь срок эксплуатации систем услуги по послепродажной поддержке продукции и по обучению работы с нею, что является гарантией автономной работы и высокой операционной готовности в каждой пользовательской среде.

Поэтому доверьтесь и Вы компетенции и возможностям Crypto AG. До Вас это уже сделали заказчики из более чем 130 стран.

Crypto AG, головное предприятие

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

Crypto AG, региональные бюро

Abidjan

Crypto AG
01 B.P. 5852
Abidjan 01
Республика Берега Слоновой Кости
Tel. +225/22 41 17 71
Fax +225/22 41 17 73

Abu Dhabi

Crypto AG
Региональное бюро по Ближнему Востоку
P.O. Box 41076
Abu Dhabi
Объединенные Арабские Эмираты
Tel. +971 2/64 22 228
Fax +971 2/64 22 118

Buenos Aires

Crypto AG
Maipu 1256 PB «A»
1006 Buenos Aires
Аргентина
Tel. +54 11/4312 1812
Fax +54 11/4312 1812

Kuala Lumpur

Crypto AG
Региональное бюро по тихоокеанскому азиатскому региону
No. 2 Jalan S57/11 Kelana Jaya
47301 Petaling Jaya
Малайзия
Tel. +60 3/7872 2150
Fax +60 3/7872 2140

Muscat

Crypto AG
Региональное бюро
Seeb PC 111
Султанат Оман
Tel. +968 2449 4966
Fax +968 2449 8929