Портфель решений компании Crypto AG

Все, что необходимо для безопасной обработки информации

Содержание

1 Вступление

2 Архитектура безопасности / Управление безопасностью

3 Решения по безопасности сети

4 Решения по безопасности информационных технологий

5 Решения по офисной безопасности

6 Решения по безопасности для радиосвязи

7 Решения по безопасности для спутниковой связи

8 Услуги компании Crypto AG

Пионеры в шифровании на протяжении почти 60 лет

- Компанию основал в 1952 году в Швейцарии пионер в области шифрования Борис Хагелин
- Более 300 сотрудников
- Большой отдел исследований и разработки
- Собственные производственные мощности
- Имеются возможности для обучения (Академия Crypto)
- Заказчики в более чем 130 странах мира
- Отсутствие экспортных ограничений на технологии шифрования, надзора со стороны государства или обязательности депонирования ключей

Решение по индивидуальному сценарию заказчика

Безопасность сетей

Шифрование данных в сетях Ethernet, SONET / SDH и PDH на скоростях до10 Гбит/с

Центр управления безопасностью широкополосных сетей

Устройство для удаленного доступа

Безопасность информационных технологий

Мобильный клиент IP VPN компании Crypto

Шифрование IP VPN для малого офиса

Шифрование в сетях IP VPN предприятий, филиалов (Gigabit)

Ноутбук для использования в экстремальных условиях

Центр управления безопасностью сетей IP VPN

Офисная безопасность

Шифрование в ТфОП

Шифрование факсов

Защищенный GSM-телефон

Настольный компьютер компании Crypto

Центр обработки ключей

Безопасность радиосвязи

Шифрование радиосвязи MultiCom

Полевой терминал компании Crypto

Бортовая радиостанция SECOS

Multilink – оборудование для группового шифрования

Центр управления безопасностью MultiCom

Безопасность спутниковой связи

Развертываемые системы безопасной спутниковой связи

Шифрование Frame Relay

Центр управления безопасностью Frame Relay

Управление безопасностью от компании Crypto AG

- Комплексная архитектура безопасности компании Crypto охватывает все аспекты: оборудование, программное обеспечение, алгоритмы, управление ключами, внедрение и т.д.
- Управление безопасностью обеспечивает всесторонний контроль над всеми устройствами шифрования в сети в соответствии с политикой безопасности заказчика
- Управление устройствами шифрования возможно в любое время (в реальном времени или автономном режиме) и не влияет на процесс эксплуатации
- 128 битный шифрующий ключ, делающий практически невозможным подбор секретной комбинации
- Основной алгоритм шифрования уже встроен в оборудование
- Пользователь может сам определять параметры шифрования, генерировать и менять ключи

Управление безопасностью

Стойкость ключа

Длина ключа	Количество вариантов	Количество тестов в секунду	Количество компьютеров	Время поиска до расскрытия ключа
40 bit	1.1×10^{12}	10^9	10^3	1.1 секунды
56 bit	7.2×10^{16}	10^9	10^3	20 часов
90 bit	1.2×10^{27}	10^9	10^3	39'000'000 лет
128 bit	3.4×10^{38}	10^9	10^3	1.1×10^{19} лет
128 bit	3.4×10^{38}	10^9	6.5×10^9 *	1.7×10^{12} лет

Crypto AG

11' 000'000'000'000'000'000

Сравните с возрастом вселенной : 12'500'000'000

* общее количество компьютеров в мире

Центр управления безопасностью (для широкополосных сетей)

SMC-1100

Ручное управление

HC-84xx

HC-84xx

HC-85xx

Онлайновый канал

Сеть связи

Смарт-карта

HC-84xx

HC-85xx

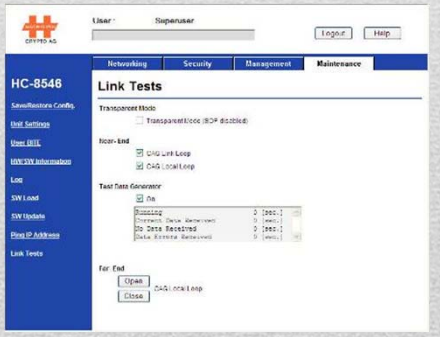
HC-84xx

HC-85xx

Централизованное управление безопасностью в реальном времени и автономном режиме

- Клавиатура и дисплей
- Доступ - аутентификация
- Ввод с помощью красной кнопки

- Безопасный носитель данных
- Информация по управлению
- Дублирование устройства



Локальный пользовательский интерфейс или удаленный доступ с помощью пользовательского веб-интерфейса

Безопасный удаленный доступ с помощью RAD

Типы сетей

- Сети C4ISTAR
- Сети командного управления (C2)
- Сети гражданского назначения
- Глобальные сети (WAN)
- Городские сети (MAN)
- Локальные сети (LAN)
- Сети хранения данных (SAN)
- Транспортные сети

Решения компании Crypto AG для шифрования в сетях Ethernet

Блок шифрования HC-8550 100M для многоточечных соединений в сетях Ethernet

Центр управления безопасностью SMC-1100 для широкополосных сетей

Блок шифрования HC-8552 1G для многоточечных соединений в сетях Ethernet

Блок шифрования HC-8556 10G для сетей Ethernet

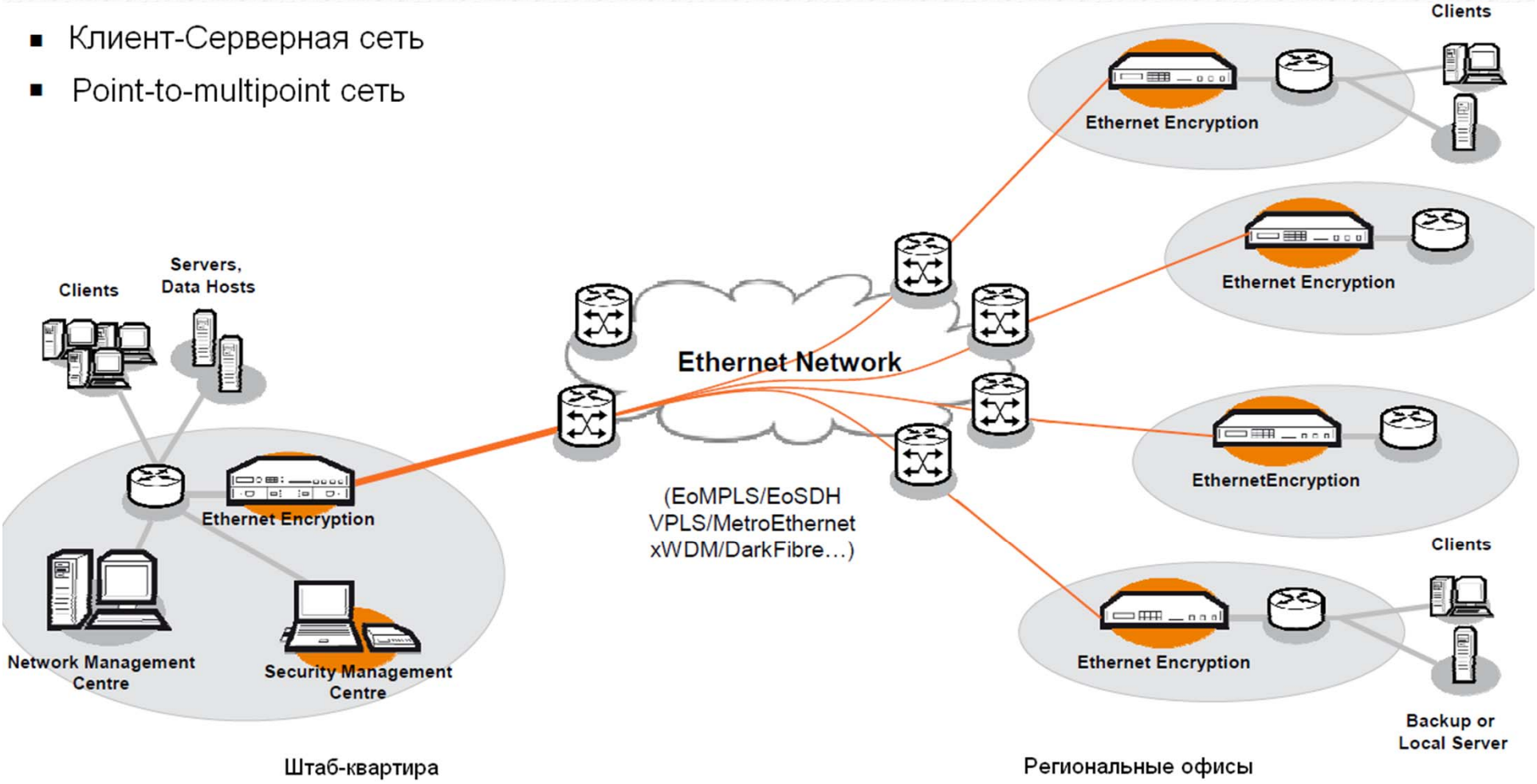
Устройство для удаленного доступа RAD-1100

Преимущества сетей Ethernet

- Сверхвысокая производительность передачи данных на скоростях до 10 Гбит/с
- Универсальный протокол для сетей уровня MAN / WAN
- Легко масштабируемая пропускная способность
- Нет необходимости изменения технологии для удовлетворения требований по полосе пропускания в будущем
- Обеспечение качества (QoS) и классов услуг (CoS) передачи данных
- Комплексные решения

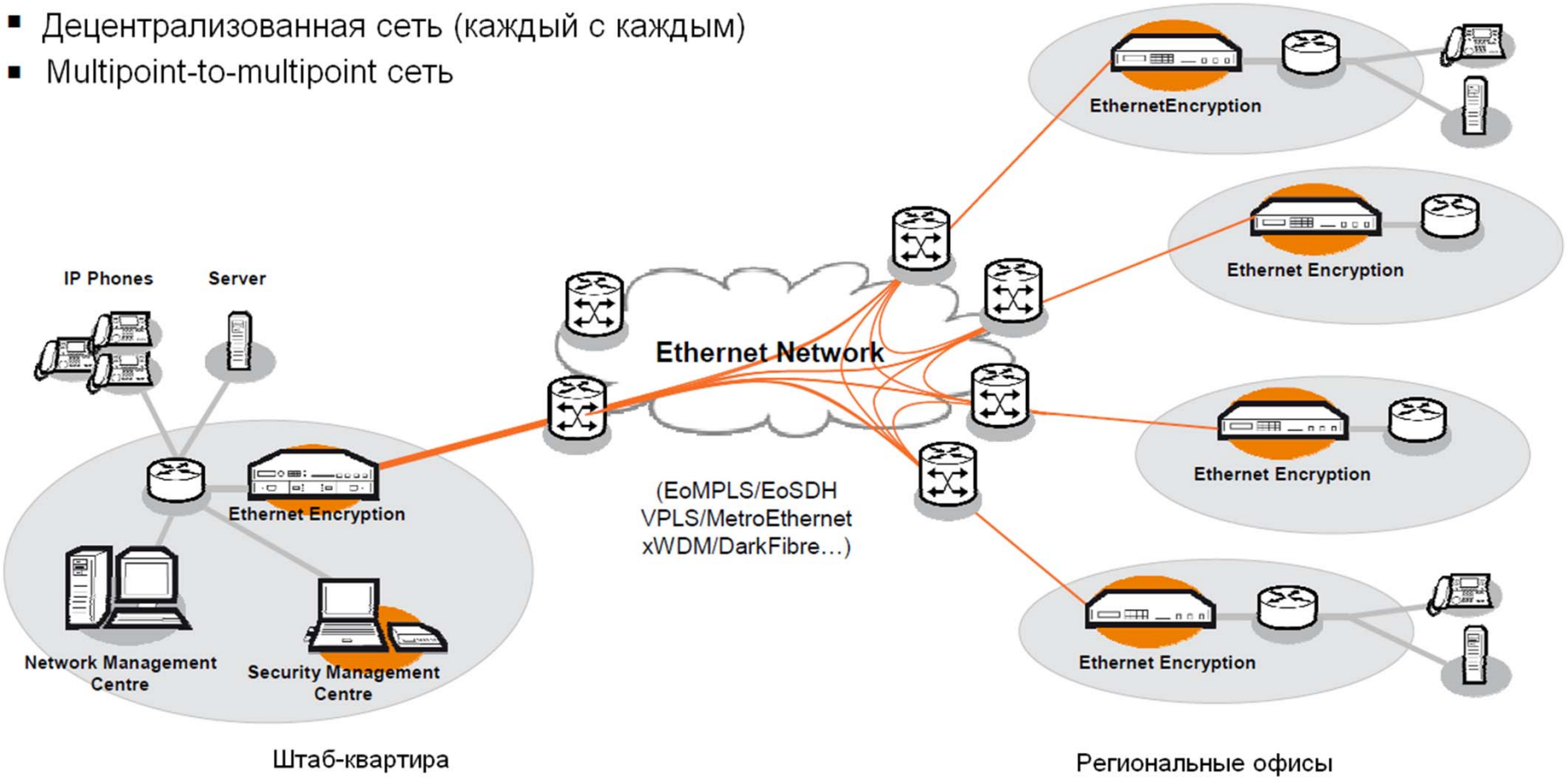
Ethernet-сценарий передачи зашифрованных данных

- Клиент-Серверная сеть
- Point-to-multipoint сеть



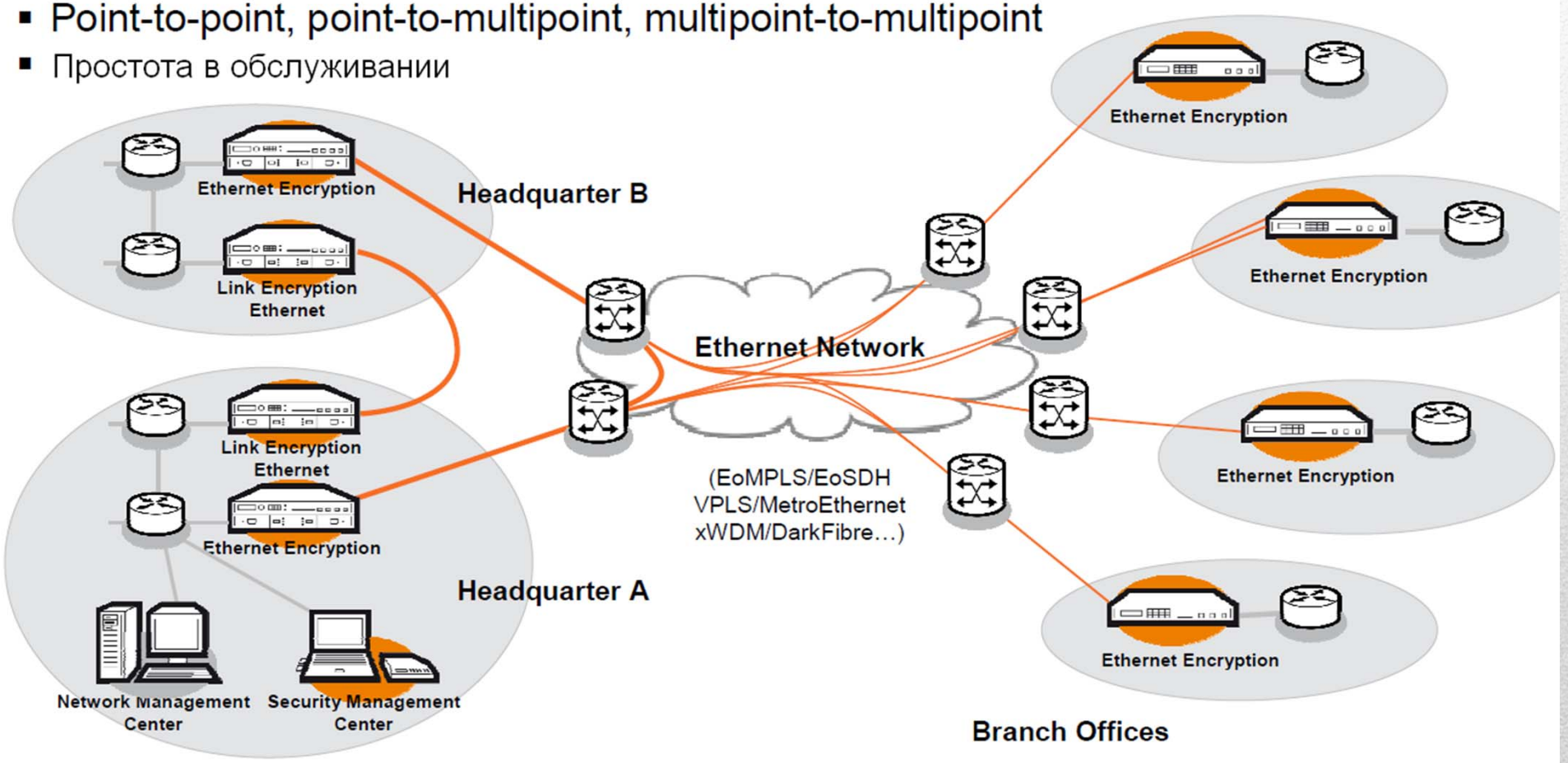
Ethernet-сценарий передачи зашифрованного голоса

- Децентрализованная сеть (каждый с каждым)
- Multipoint-to-multipoint сеть



Ethernet-сценарий с резервированием данных

- Отказоустойчивая система
- Point-to-point, point-to-multipoint, multipoint-to-multipoint
- Простота в обслуживании



Решения Crypto AG для сетей IP VPN

Мобильный клиент Crypto HC-7835 IP VPN 1/4/8M

Блок шифрования HC-7805 для сетей IP VPN малого офиса

Блок шифрования HC-7825 для сетей IP VPN предприятия / филиала

Блок шифрования радиосвязи MultiCom HC-2650 для сетей IP VPN

Центр управления безопасностью для сетей IP VPN

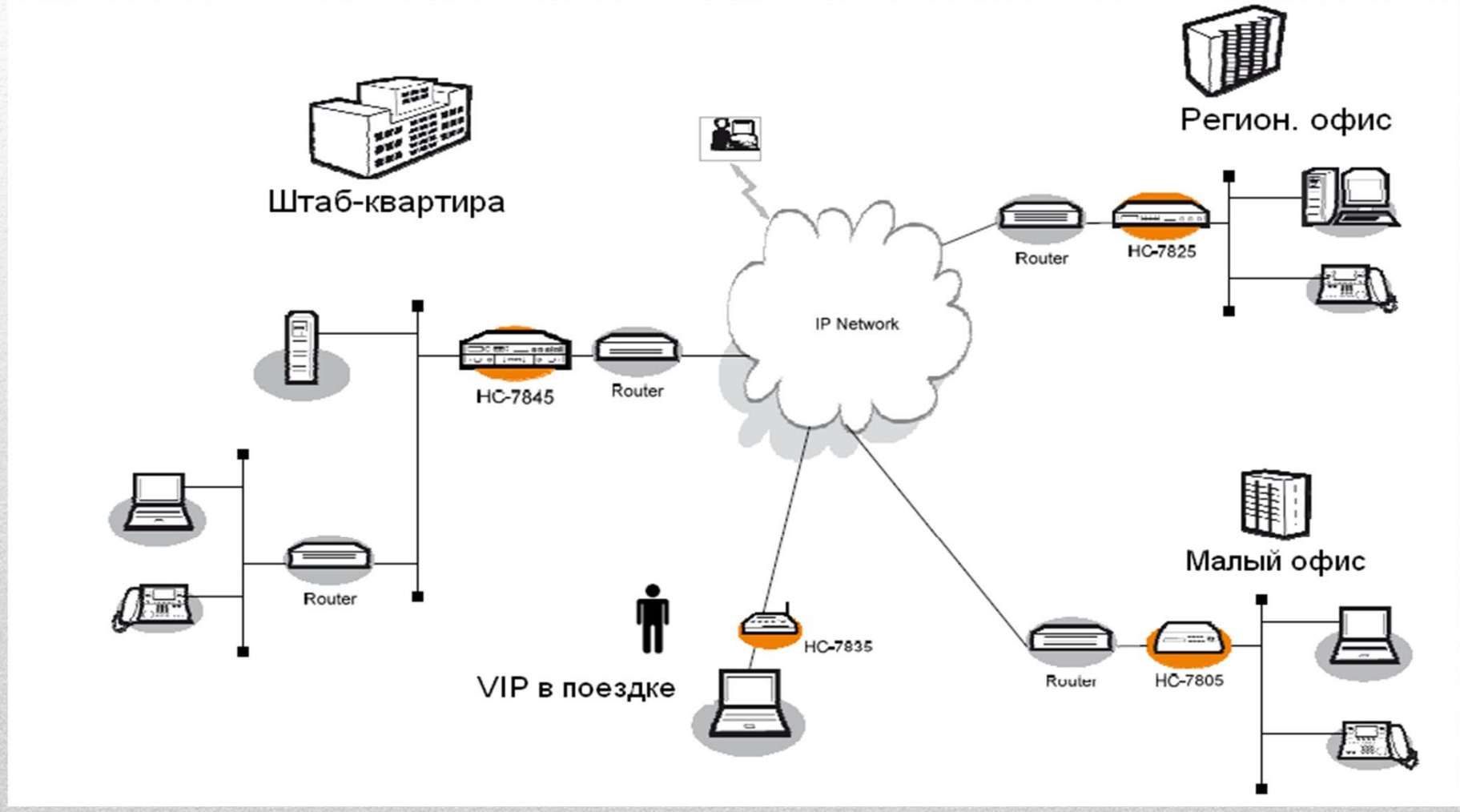
Устройство для удаленного доступа RAD-1100

Блок шифрования HC-7845 (гигабитная версия) для сетей IP VPN

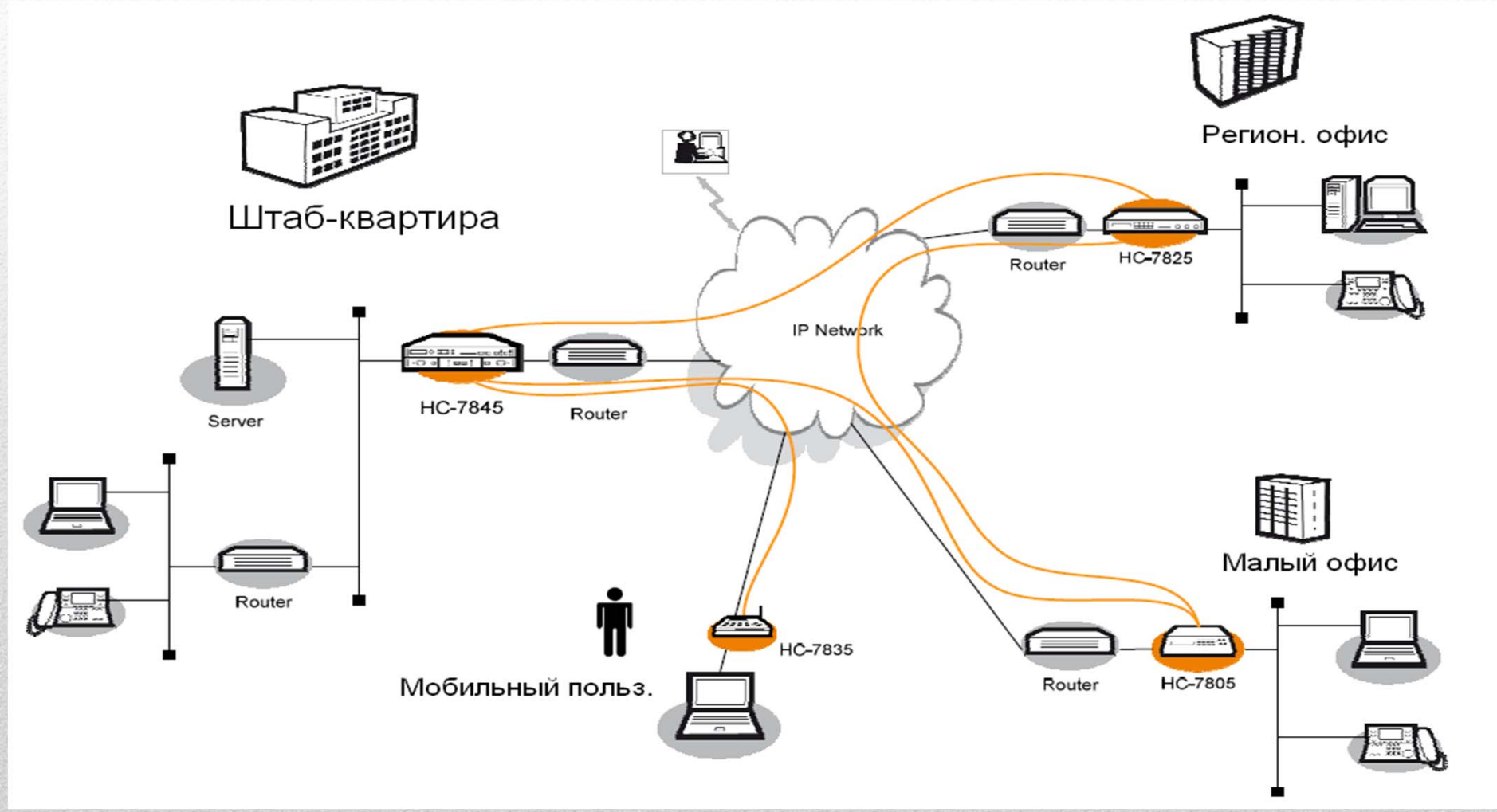
Основные характеристики

- Возможность одновременной передачи данных, голоса, видео (triple-play): все приложения защищены (передача данных, передача голоса по IP-протоколу, видеоконференция и т.д.)
- Низкая стоимость связи, инфраструктуры и технического обслуживания
- Совместимость с семейством сетей IP VPN
- Шифрование осуществляется в аппаратном модуле, устойчивом к внешним воздействиям
- Задаваемые пользователем алгоритмы на аппаратной базе
- Централизованное управление безопасностью
    - Локальное: клавиатура, дисплей
    - Локальное: SDC (последовательный контроллер данных)
    - Локальное / дистанционное: на базе веб
    - Дистанционное: блок SMC-1100 IP VPN

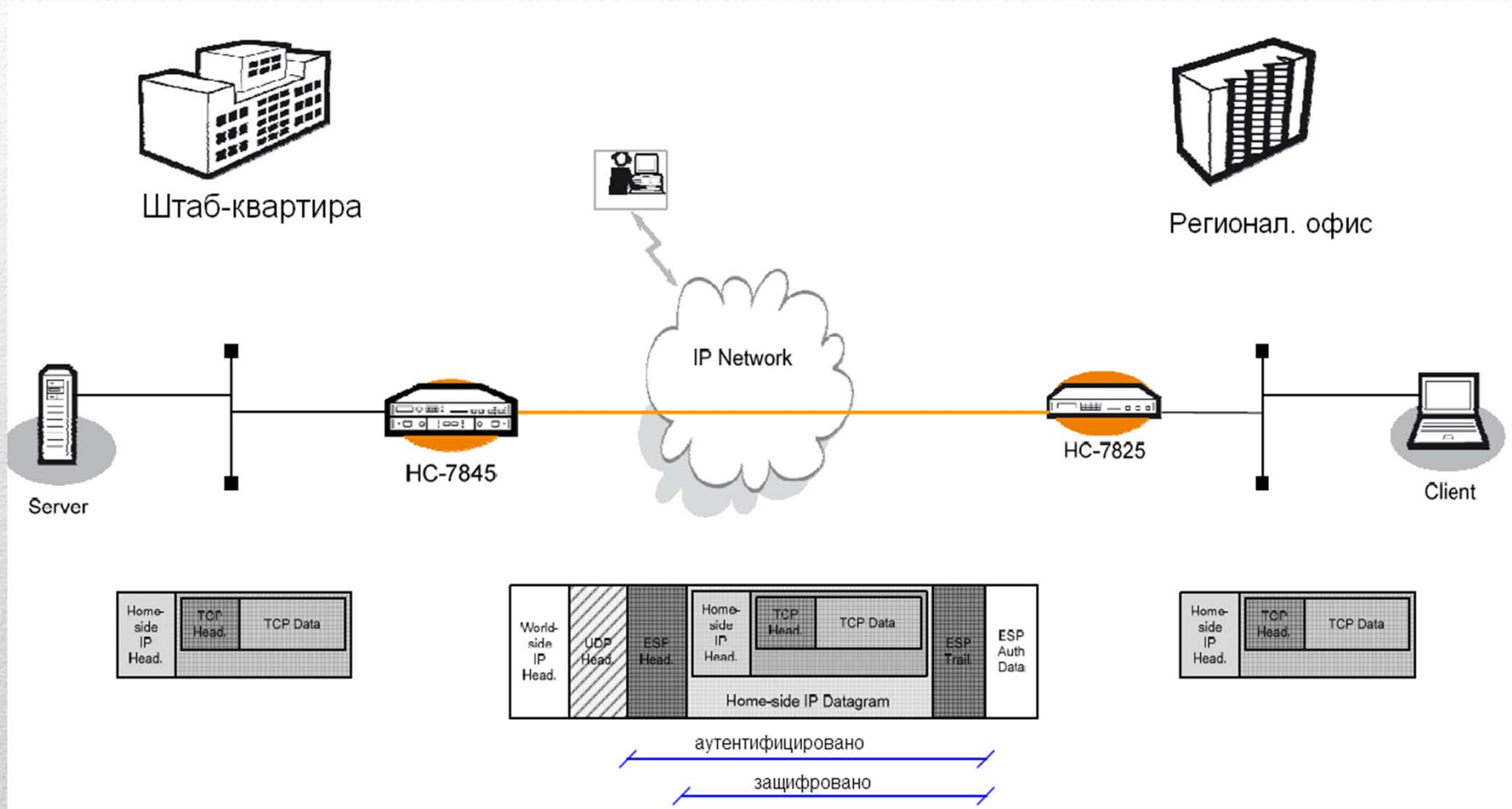
Инсталляция IP VPN устройств



Конфигурация тоннельных соединений между пунктами



Тоннельный режим



Режим мобильного клиента

Решения компании Crypto AG для обеспечения офисной безопасности

Блок шифрования факсов HC-4221

Центр обработки ключей KHC-1500 для факсимильных сетей

Настольный компьютер компании Crypto HC-9300

Настольный компьютер компании Crypto HC-9300

- Многофункциональная платформа шифрования для современных и перспективных офисных приложений
- Доступные приложения: шифрование факсов и файлов, защита голоса
- Совместимость с блоком HC-4221
- Шифрование факсов: классификация документов и защищенные почтовые ящики
- Опция передачи факса по электронной почте
- Простое интуитивное управление с помощью графического интерфейса пользователя (touchscreen)
- Телефонные интерфейсы (PSTN) для обработки факсов и Ethernet интерфейсы для VoIP и E-mail
- Полная защита от утечки информации путем ЭМ эмиссии (COMPREM)

Блок шифрования факсов HC-4221

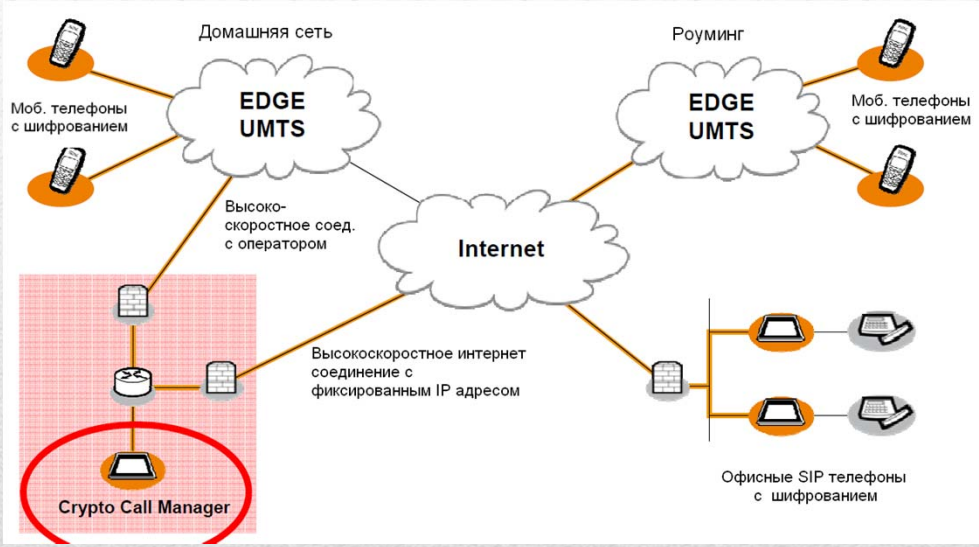
- Передача документов в цвете (при использовании факса для цветных изображений)
- Компактное и прочное настольное устройство, которое просто устанавливается между факсимильным аппаратом и настенной розеткой для подключения телефона / факса
- Блок совместим со всеми факсимильными устройствами, которые соответствуют стандартам G3 и Super G3
- Процесс шифрования автоматически приспосабливается к возможным скоростям передачи
- Архитектура безопасности компании Crypto: шифрование в аппаратном модуле, устойчивом к внешним воздействиям, задаваемые пользователем алгоритмы, централизованное управление безопасностью

Центр обработки ключей (KHC-1500)

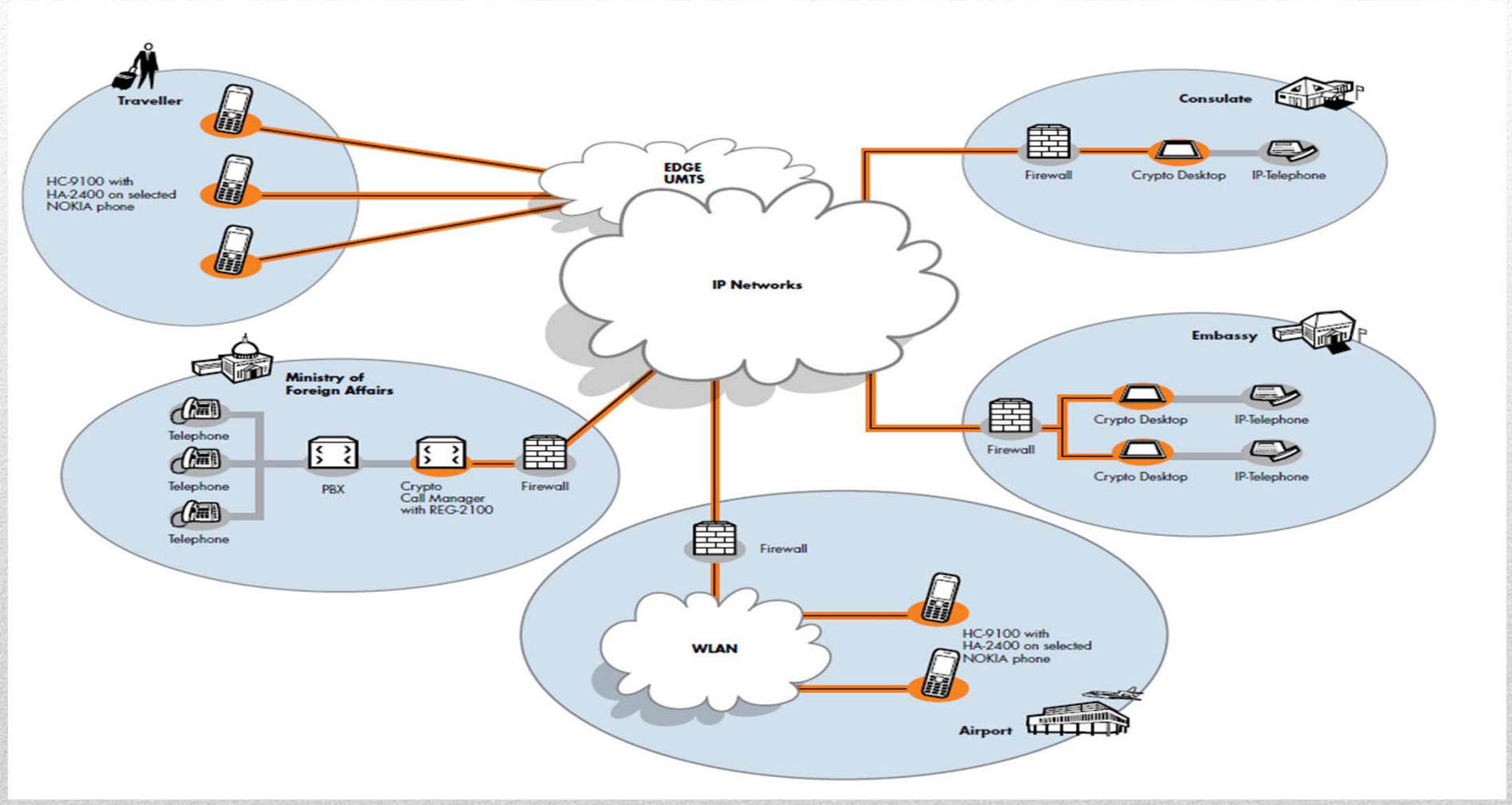
- Компьютерный центр безопасности и управления для безопасного управления и распространения секретной информации и ключей
- Централизованное управление безопасностью как для малых, так и для больших факсимильных сетей
- Базовому пользователю не требуется владение ноу-хау в области безопасности
- Случайная генерация ключей
- Криптографическая защита загрузки ключей и параметров по линии связи
- Криптографические данные и ключи хранятся в модуле безопасности компьютера, так чтобы они не были доступны посторонним лицам
- Независимое распространение ключей по кабелю (локально) или в зашифрованном виде на различных носителях информации, а также по обычной почте или с помощью курьера

Шифрование голоса

В большинстве случаев голосовая связь внутри организации содержит в себе много конфиденциальной информации. Это нормально, когда информация находится внутри организации, но при выходе ее за пределы компании она должна быть зашифрована. Для подобных сценариев компания Crypto AG предлагает уникальное ПО со специальным голосовым шлюзом – REG2100/HA2100. Это гарантирует, что все исходящие, посредством VoIP, телефонные звонки гарантированно зашифрованы. VIP персоны со своим собственным шифрующим устройством имеют возможность организовывать «закрытые соединения» из любых мест своего нахождения.



Шифрование голоса



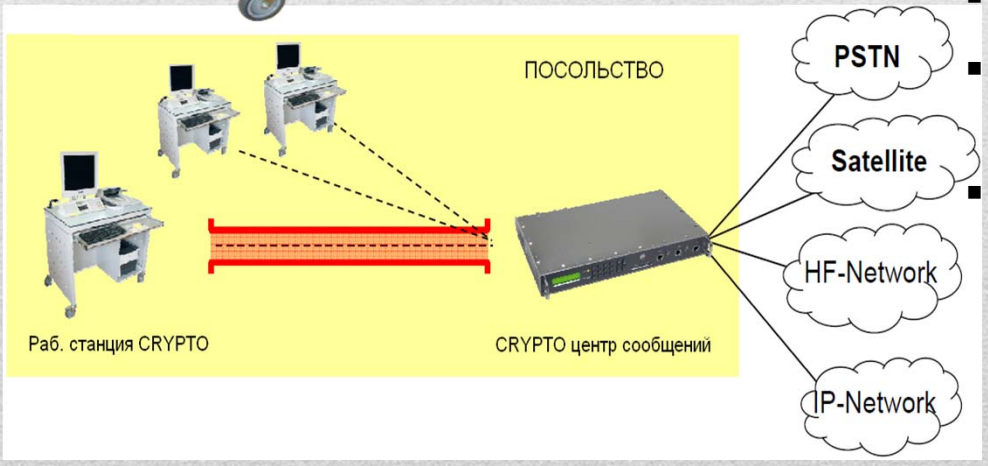
Шифрование голоса

HC-9100
HA-2400
Nokia

HC-9300
HA-2500
SIP Phone

HC-9300
HA-2100
REG-2100
VoIP PBX

Защищенная система обмена сообщениями для дипломатических служб



- Мобильная рабочая станция, с не имеющими излучения монитором, принтером и сканером
- Для формирования рабочей группы к локальному серверу подключается до четырех рабочих станций по защищенной беспроводной ЛВС
- В случае отключения рабочих станций все сообщения обрабатывает сервер
- Несколько степеней конфиденциальности
- Вся конфиденциальная информация хранится на защищенном сервере
- Доступ сотрудников к рабочим станциям на основе специальных карт (определяется количество защищенных п/я, степень конфиденциальности)

Безопасность радиосвязи

- Гражданские и военные условия эксплуатации
- Для стратегических и тактических каналов связи
- Возможны настройки для передачи голоса и данных в полудуплексном, дуплексном и симплексном режимах
- Соединения типа точка-точка, точка-многоточка
- Возможность обмена данными, передачи голоса и сообщений
- Полностью не зависима от сторонней аппаратуры и провайдеров

Решения компании Crypto AG по безопасности радиосвязи

Блок шифрования HC-2650 для радиосвязи MultiCom

Полевой терминал HC-6830 компании Crypto

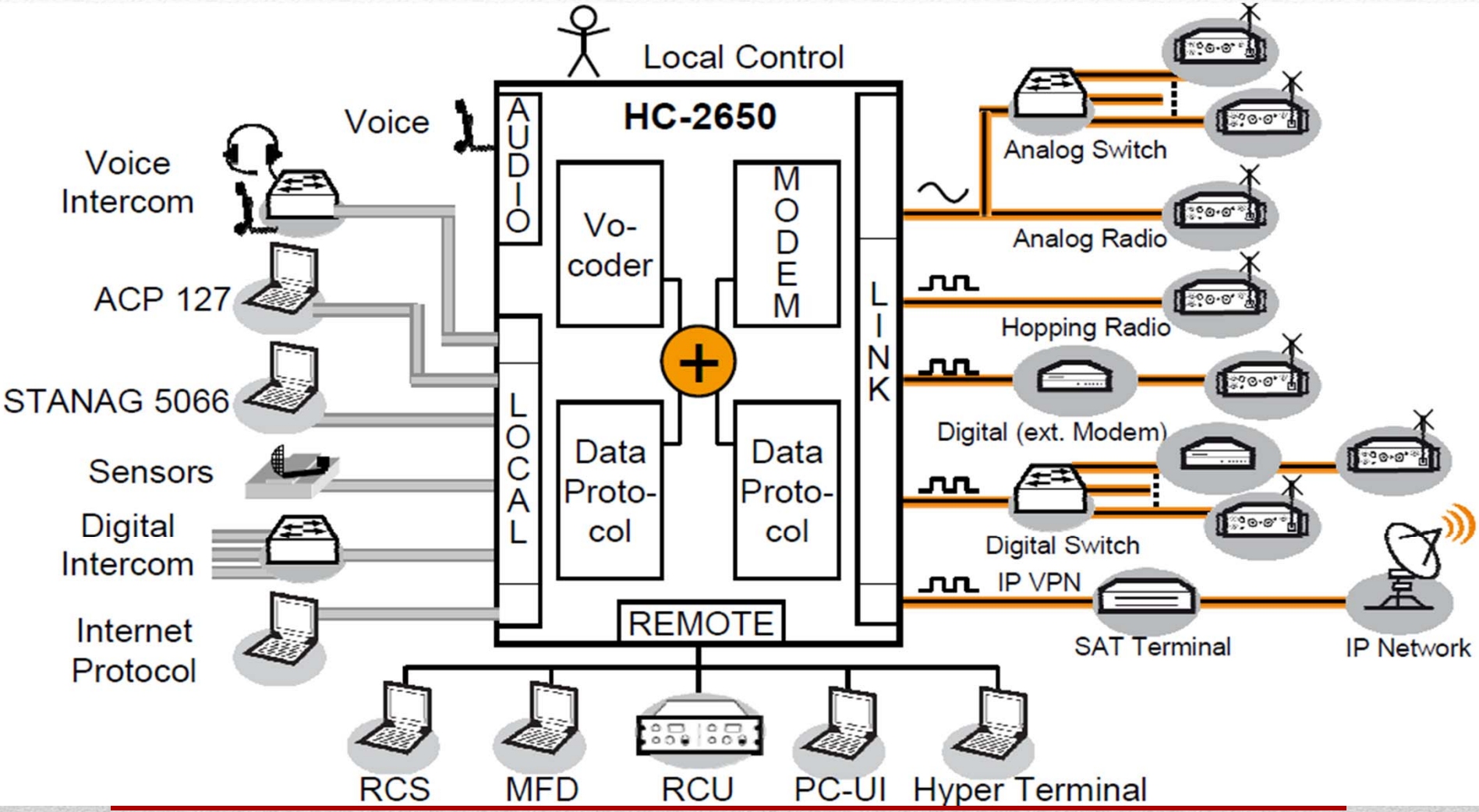
Блок группового шифрования HC-7550 для многозвенных соединений

Центр управления безопасностью SMC-1100 MultiCom

Бортовая радиостация SECOS

Решения компании Crypto AG по безопасности радиосвязи

Решения компании Crypto AG по безопасности радиосвязи



Решения компании Crypto AG для спутниковой связи

Приложения IP

Мобильный клиент HC-7835 компании Crypto для сетей IP VPN

Блок шифрования HC-7805 для сетей IP VPN (версия для малого офиса)

Блок шифрования HC-7825 для сетей IP VPN предприятия / филиала

Блок шифрования радиосвязи MultiCom HC-2650 для сетей IP VPN

Сети Frame Relay

Блок шифрования HC-7110 для сетей FR

Классические приложения

Блок шифрования HC-2203 для ТфОП

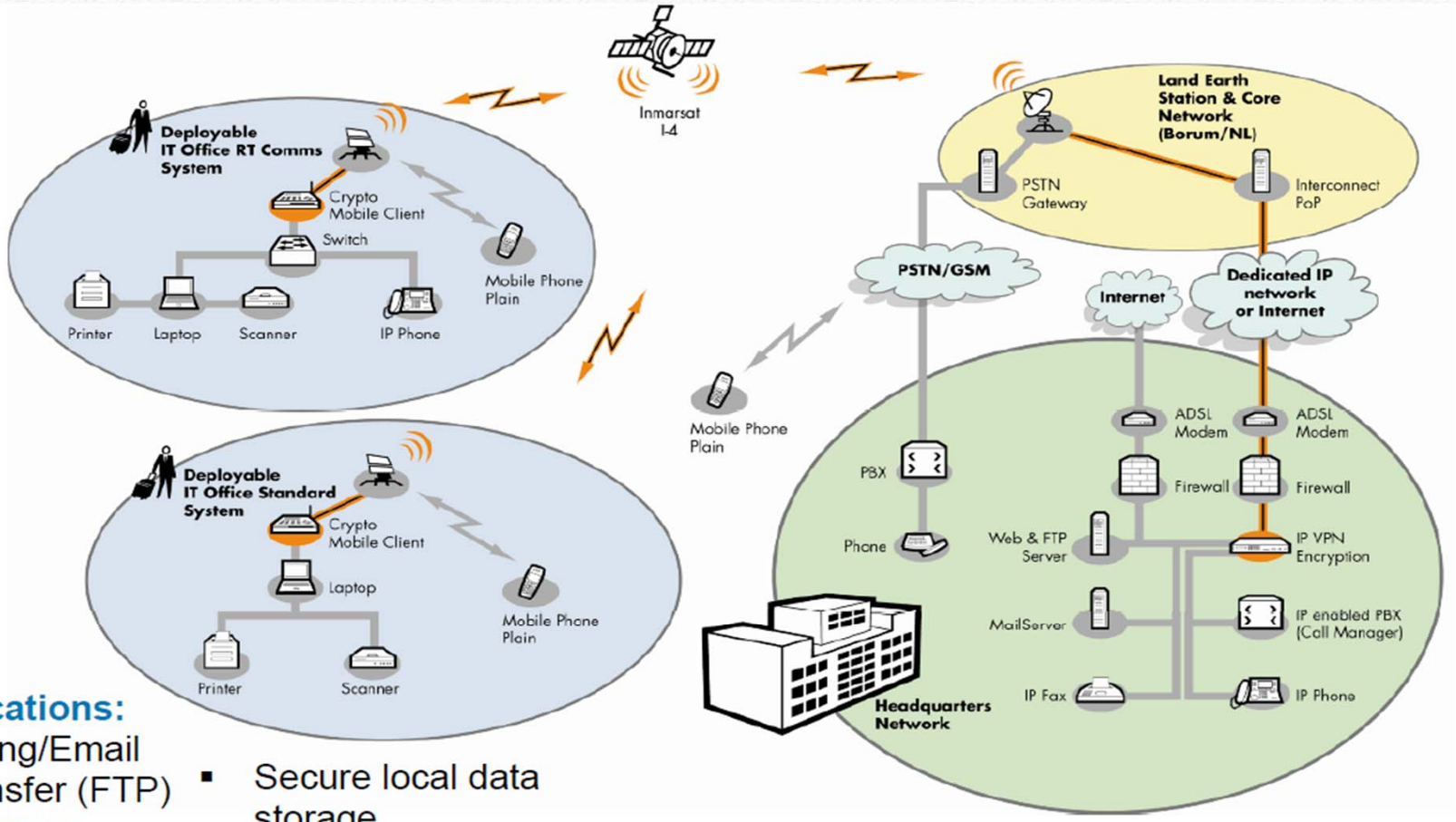
Блок шифрования факсов HC-4221

Обмен сообщениями

Полевой терминал HC-6830 компании Crypto

Надежный ноутбук HC-6835 компании Crypto

Решения компании Crypto AG для спутниковой связи



Main applications:

- Messaging/Email
- File Transfer (FTP)
- Client/Server
- Intranet etc.
- VoIP/FoIP*/Video
- Secure local data storage
- File/message encryption

* (FoIP reliable only over terrestrial networks)

Развертываемые защищенные спутниковые системы

- Антенна
- Сканер
- Netbook
- Принтер
- VoIP телефон
- Адаптер для подкл. Факса
- НС-7835 Мобильный клиент
- Телефон PBX
- Свитч

Развертываемые защищенные спутниковые системы

Пример “Компактной телефонной системы”

- **Модульная архитектура:** состав оборудования / приложений определяется заказчиком
- **Быстрое развертывание:** подключение к спутниковому терминалу, включение питания (или при наличии наземного доступа к Интернет – соответственно подключение к ТфОП)
- **Автономное питание:** улучшенная автономномность при использовании дополнительного контейнера с источником питания, состоящим из аккумуляторных батарей, входа для внешнего питания постоянного / переменного тока и панелей солнечных батарей для зарядки, выхода преобразователя постоянного тока в переменный синусоидальный ток (опция)

Развертываемые системы используются в тех случаях, когда:

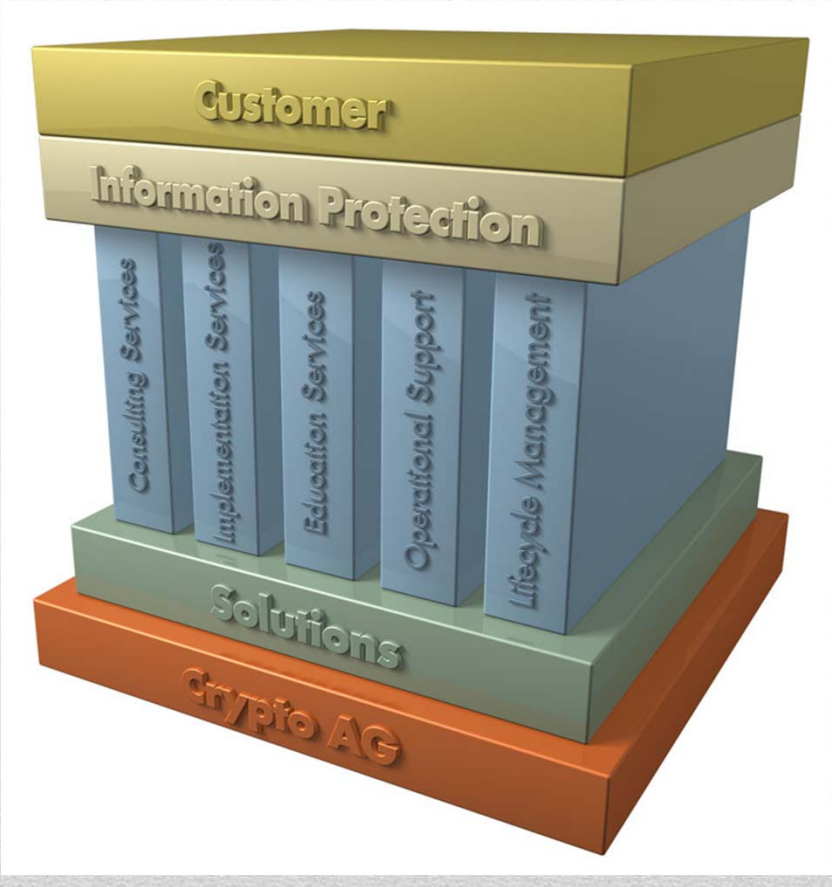
Пример “Модульной системы телефон/факс”

- пропускная способность наземных каналов связи недостаточна или отсутствует
- требуется независимость от наземной сети
- требуется избыточность связи, т.е. резервированная связь
- требуется мобильность
- невозможно или слишком дорого использовать VSAT

Потенциальные заказчики

- Министерства иностранных дел, миссии, небольшие посольства, находящиеся в дороге дипломаты, военные атташе
- Министерства внутренних дел больших стран с неравномерно и недостаточно развитой инфраструктурой связи, полиция, таможня, службы национальной безопасности и т.д.
- Президентские администрации
- Пограничный контроль
- Службы разведки

Услуги компании Crypto AG



Услуги компании CRYPTO AG дают Вам возможность самостоятельно делать все, что Вы хотите, для шифрования информации

И они освобождают Вас от тех задач, которые Вы не хотите выполнять сами

Услуги компании Crypto AG

Консультационные услуги

Ваша выгода:

Руководство для уточнения целей защиты информации и концепций для их достижения

Поставка:

Оценки информационной безопасности
Концепции по защите вашей информации
Схема обеспечения процесса информационной безопасности

Услуги по внедрению

Ваша выгода:

Вы получаете систему, в полном соответствии с поставленными целями

Поставка:

Интеграция вашего законченного информационно-коммуникационного решения;
Эксклюзивные отчеты, планы, диаграммы
Ваш собственный менеджер проекта

Образовательные услуги

Ваша выгода:

Вы получаете самые современные ноу-хау, навыки и опыт

Поставка:

Персонально разработанные курсы по криптографии, безопасности, управлению безопасностью, техобслуживанию/ремонту и эксплуатации системы

Услуги оперативной поддержки

Ваша выгода:

Вы получаете поддержку в части обеспечения высокой эксплуатационной готовности системы

Поставка:

Советы и поддержка по горячей линии
Техобслуживание экпертами в области криптографии и технологии

Услуги по управлению жизненным циклом

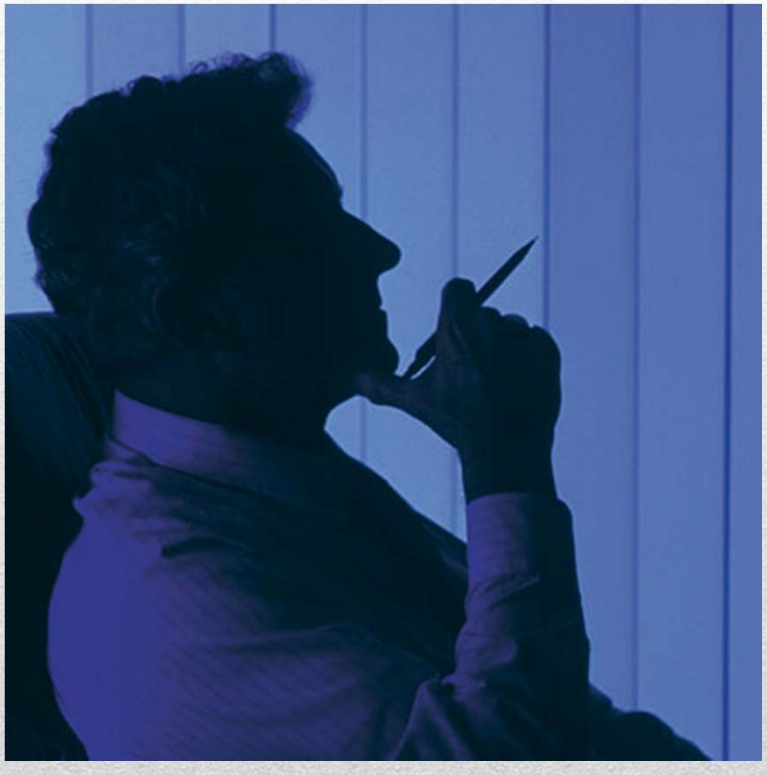
Ваша выгода:

Вы получаете пожизненную высокую готовность системы и защиту инвестиций

Поставка:

Программное Hardware-Upgrades
Концепция миграции
Модификация процесса для логистики

Консультационные услуги



Поставка:

- Оценка существующего уровня информационной безопасности с точки зрения технологии и организации
- Концепции и архитектура информационной безопасности, соответствующие вашим уникальным потребностям в области технологии и безопасности сегодня и в будущем
- Выполненная по индивидуальному заказу структура процесса безопасности для информационно-коммуникационных технологий, формализованный набор процедур

Услуги по внедрению

Поставка:

- Мы оказываем вам поддержку в оценке, планировании, анализе, разработке, совершенствовании, инсталляции и проверке качества вашего решения в области информационно-коммуникационных технологий
- Все технические схемы, планы, отчеты и рекомендации предоставляются исключительно для вашего уникального проекта
- Имеется только одна контактная точка

Образовательные услуги

Поставка:

- Мы предлагаем индивидуально подготовленные курсы по криптографии, информационной безопасности, управлению безопасностью, технологии связи, эксплуатации и обслуживанию системы
- Учебные курсы по принципу “быстрый старт” для основных ноу-хау в фазе запуска проекта

Услуги оперативной поддержки

Поддержка:

- Наша сервисная служба обеспечивает полную операционную поддержку, которая может вам понадобиться
- Поддержка опытными инженерами

Услуги по управлению жизненным циклом

Поставка:

- Аппаратные обновления, концепции миграции и модификация процессов логистики
- Детальные планы, соответствующие вашему уникальному набору целей по безопасности, конфигурациям системы и перемещениям персонала

Спасибо за внимание!

www.arustel.ru