infotecs

Вопросы применения усиленной неквалифицированной подписи

Поташников А.

potashnikov@infotecs.ru

Интернет вещей (IoT)

«Пользователями» информационных систем являются устройства:

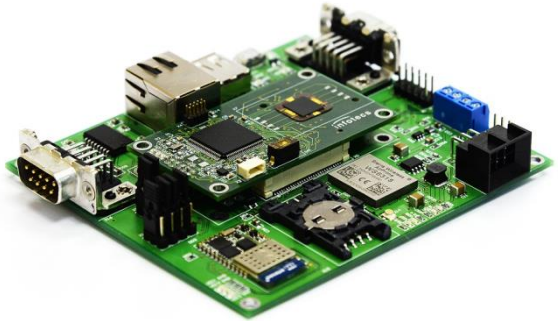
- Устройства управления промышленными и бытовыми объектами
- Сигнализации, датчики состояний, системы видеофиксации
- Счетчики продукции и услуг
- Банковские системы, терминалы, карты

Требования по безопасности

В зависимости от системы и модели нарушителя для нее необходимо обеспечивать следующие функции безопасности:

- Аутентификация
- Конфиденциальность
- Целостность
- Неотрекаемость

Особенности и ограничения индустриальных систем



- Ограниченные вычислительные возможности и объемы памяти
- Возможен ограниченный ресурс источника питания
- Возможна низкая пропускная способность каналов связи
- Ограничения на размеры передаваемых пакетов информации
- Жесткие требования на допустимое время задержки сигнала

Card Verifiable Certificates

Таблица 1. Формат CV-сертификата

Объект данных	Аббревиатура	Тэг	Тип	Наличие
CV сертификат	CV/C	0x7F21	Последовательность	m
Тело сертификата	CB	0x7F4E	Последовательность	m
Идентификатор версии формата сертификата	CPI	0x5F29	Беззнаковое целое	m
Идентификатор центра, выдающего сертификат	CAR	0x42	Символьная строка	m
Открытый ключ	PK	0x7F49	Последовательность	m
Идентификатор владельца сертификата	CHR	0x5F20	Символьная строка	m
Шаблон определения прав владельца сертификата	CHAT	0x7F4C	Последовательность	m
Дата начала действия сертификата	CED	0x5F25	Дата	m
Дата окончания действия	CExD	0x5F24	Дата	m

- ISO/IEC 7816-8 (описывается структура CV-сертификата, необходимая для обеспечения возможности его проверки смарт-картой);
- BSI TR-03110-3 (описывается PKI на основе CV-сертификатов, предназначенная для организации расширенного контроля доступа в ПВДНП);
- EN 14890-1 (описывается процедура проверки смарт-картой цепочки CV-сертификатов при использовании смарт-карты в качестве устройства для создания электронной подписи);
- ISO/IEC 18013-3, CEN/TS 15480-2 и др.

X.509 certificates

- Размер от 1 до 3 Кб
- Кодировка ASN.1
- Сложность проверки
- Высокая избыточность в структурах подписанных и зашифрованных данных CMS

CV certificates

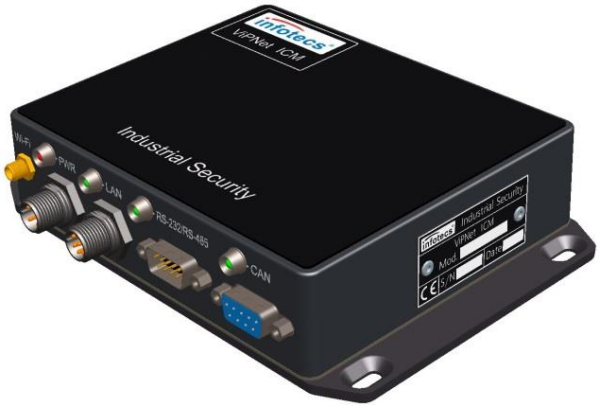
- Размер от 100 до 300 байт
- Кодировка TLV
- Примитивная проверка
- Минимальные размеры структур подписанных данных

CV-сертификаты с ГОСТ алгоритмами

Продукты для создания инфраструктуры CV-сертификатов и использования протоколов аутентификации с картами УЭК:

- ПО КриптоСФЕРА («АйТи Сфера»);
- СКЗИ КриптоПро УЭК CSP («Крипто-Про»)
- СКЗИ ViPNet CSP («ИнфоТеКС»)

Криптомодуль ViPNet ICM

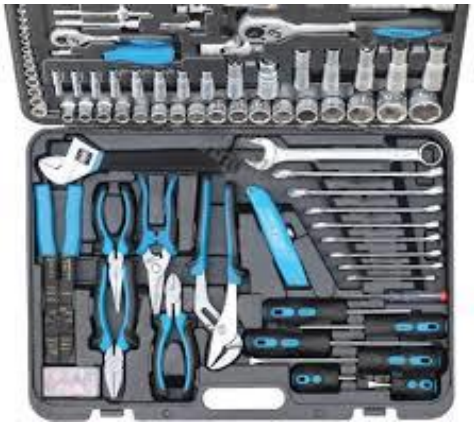


Предназначен для защиты данных в автоматизированных системах управления

Область применения ViPNet ICM

- Обеспечение целостности данных.
- Обеспечение конфиденциальности данных.
- Юридическая значимость информационного обмена за счет создания и проверки электронной подписи.
- Идентификация и аутентификация источника данных (machine identification).

Функциональность модулей

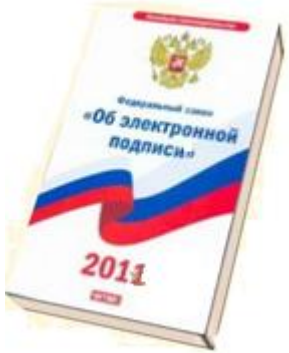


- Зашифрование/расширование, вычисление/проверка имитовставки по ГОСТ 28147-89.
- Создание/проверка ЭП по ГОСТ Р 34.10–2012.
- Хэширование по ГОСТ Р 34.11–2012.
- Ввод нормативной, справочной и ключевой информации с использованием локального порта управления и конфигурирования.
- Удаленное конфигурирование модуля через основной сетевой интерфейс.

Ключевая система

На основе асимметричных криптографических механизмов с поддерживающей инфраструктурой открытых ключей, предположительно CV-сертификаты.

Законы и требования



Электронная подпись при использовании CV-сертификата в терминологии 63-ФЗ является «усиленной неквалифицированной»

К средствам ЭП, использующим CV-сертификаты и средствам создания CV-сертификатов применимы требования ФСБ к средствам электронной подписи и Требований к средствам удостоверяющего центра (796 приказ от 27.12.2011)

К CV-сертификатам не применимы требования к форме квалифицированного сертификата ключа проверки электронной подписи.

Стандартизация

Материалы рабочей группы по использованию криптографических механизмов для идентификации граждан в электронной среде

- Использование алгоритмов ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012 в профиле сертификатов открытых ключей в формате CV
- Описание протокола защищенного обмена сообщениями SCP-F2 с использованием ГОСТ 28147-89, ГОСТ Р34.11-2012 и ГОСТ Р34.10-2012
- Методические рекомендации по использованию отечественных криптографических алгоритмов при организации расширенного контроля доступа к данным на бесконтактных микросхемах

infotecs

Спасибо за внимание.
Вопросы?

Поташников А.
potashnikov@infotecs.ru