Российская криптографическая ассоциация
Конференция РусКрипто'2011

Проблемы построения и функционирования больших систем защиты информации

Попов Владимир Олегович
к.ф.-м.н.
Совет директоров ассоциации РусКрипто
МГУ им М.В. Ломоносова, факультет ВМК
ООО Крипто Про

Общие представления о больших системах

- Под большими системами защиты информации понимаются:

- ведомственные системы сбора и обработки конфиденциальной информации и персональных данных

- системы обслуживания населения с передачей персональных данных.

- ***Основные черты больших систем защиты информации:***

- территориальная распределённость пользователей системы, пользователи могут находиться в малых населённых пунктах (до 200 человек), где нерентабельно содержать лицензированные органы распространения и сопровождения СКЗИ, а также службы нотариата и пр.;

- использование Интернет в качестве сети связи и оказания сетевых услуг;

- использование в качестве АРМ СКЗИ общедоступных ЭВМ с различными ОС, как правило под управлением ОС Windows (концепция слабо защищённых АРМ СКЗИ);

- используются СКЗИ различных производителей;

- слабая подготовка пользователей в обеспечении безопасности СКЗИ;

- пользователь самостоятельно получает, устанавливает, эксплуатирует СКЗИ;

- пользователь не имеет возможности регистрироваться на УЦ непосредственно, присутствуя лично;

- пользователь самостоятельно выполняет роль администратора органа криптозащиты;

- как правило отсутствует возможность очного обучения по использованию СКЗИ и инструктажа по правилам безопасности;

- ЭД и правила работы на СКЗИ пользователь получает по каналу с сайта разработчика (организатора системы);

- высокие риски информационной безопасности.

Общая модель безопасности информации

- ***Классы защищаемой информации:***

- персональные данные;
- конфиденциальная информация;

- ***Модель нарушителя для больших систем.***

- В сети присутствуют нарушители Н1 – Н5. Нарушители всех типов имеют доступ к ресурсам системы (АРМ'ам пользователей и серверам доступа) только по каналам связи. Нарушители Н4 – Н5 осуществляют атаку только на сетевые ресурсы системы. Нарушители Н1 – Н3 осуществляют атаки на все ресурсы системы в рамках протоколов доступа к ресурсам.
- Нарушители Н1 – Н3 не имеют возможность нарушать деятельность зарубежных удостоверяющих центров, имеющих традиционно высокое доверие, таких как УЦ VeriSign. Нарушители Н4 – Н5 не ставят цели по нарушению деятельности таких центров.

- Сетевые ресурсы по нормам РФ должны быть защищены от Н5.
- АРМ пользователя может быть защищён от Н1 (Н1 – Н3).
- Модель нарушителя требует построения неоднородных по уровню защиты систем связи.

PKI сеть

Подсеть сети общего доступа, характеризующаяся единым корневым сертификатом

Также характеризуется:

- Иерархической системой УЦ
- Системой регистрации пользователей
- Системами управления:
  - Удостоверяющими центрами и центрами регистрации
  - Сертификатами пользователей
  - СКЗИ пользователей (распространение , учёт, контроль)
- Организатор PKI сети и оператор сети в соответствии с документом «**Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных**»

Современное состояние нормативной базы

Законы о защите конфиденциальной информации и персональных данных:

- Закон об ЭЦП;
- Закон об информационных технологиях и о защите информации;
- Законы о Тайне:
  - Служебной,
  - Коммерческой;
- Федеральный Закон о персональных данных.

Инструкции (ведомственные), ФСБ:

- Типовые требования к защите персональных данных;
- Методические рекомендации к защите персональных данных.

Нормативная база и структуры сети

Законы и указы
Инструкции
Правила безопасности
Правила Пользования

Требования ФСБ

Требования ФСТЭК

«Типовые требования …»
«Методические рекомендации …»
по защите персональных данных.
Требуется распространить на конфиденциальную информацию

- **Разработчики СКЗИ**
  - **Политика учета СКЗИ**
  - **Политика распространения СКЗИ**
  - **Политика лицензирования СКЗИ**
- **Разработчики системы (PKI сети)**
  - **Создание ЭДО с использованием и средств защиты и СКЗИ**
  - **Создание АРМ ЭДО**
- **Операторы сети**
  - **Поддержка УЦ**
  - **Регистрация пользователей**
  - **Управление УЦ, сертификатами, ЭЦП**
  - **Распространение АРМ СКЗИ и АРМ ЭДО**
- **Пользователи PKI сети**
  - **Установка АРМ пользователя**
  - **Регистрация в ЦР**
  - **Управление личными закрытыми ключами**
  - **Управление сертификатами**

Особенности

В настоящее время используются СКЗИ многих производителей.

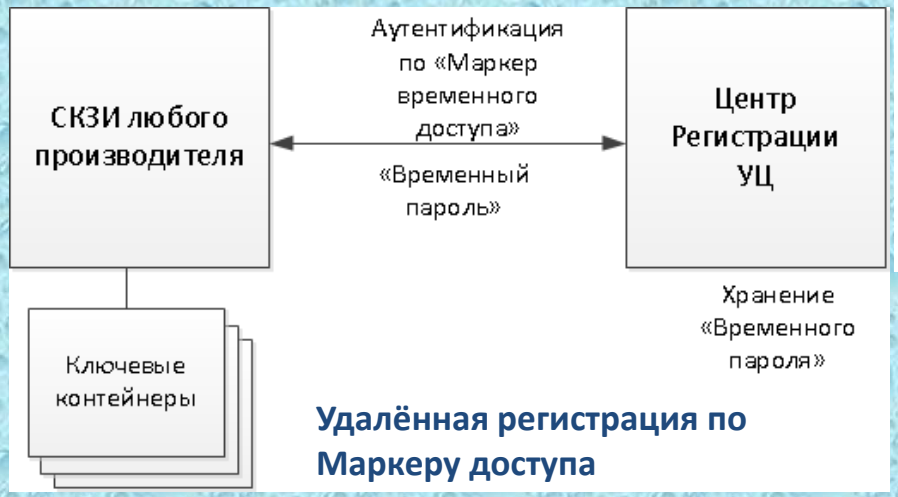
Существует множество:

- Разработчиков ЭДО;
- PKI сетей.

- Нет полноты и гармонизации требований и стандартов, определяющих PKI в достаточно полном объеме;
- Не сформулировано понятие АРМ пользователя;
- Не согласованы способы доставки АРМ.
- …
- Не сформированы понятие и требования к Единому пространству доверия

Регистрация пользователя в PKI сети

Удалённая регистрация по доверенному каналу (TLS)



Удалённая регистрация по Маркеру доступа

Регистрация с использованием СКЗИ иного разработчика

АРМ пользователя:

АРМ пользователя:

- аппаратная составляющая - широкий спектр бытовых ПС
- ОС Windows
- Приложения плохо определены
- Средства защиты (СКЗИ, МЗ, антивирус, …)
- документация по безопасности.

- Доставка не СКЗИ, а защищенного АРМ'а пользователям.
- Концепция слабозащищенной системы.
- Разработка и внедрение политики безопасности ПК и ОС.
- Создание «простых» средств контроля среды и СКЗИ (средств доверенной загрузки).

Вопросы доставки АРМ пользователям:

- Доставка дистрибутива по сети.
-

- Взаимодействие с использованием предустановленного PKI, например VeriSign, для обеспечения доверенной доставки дистрибутива.

Проблемы и недостатки

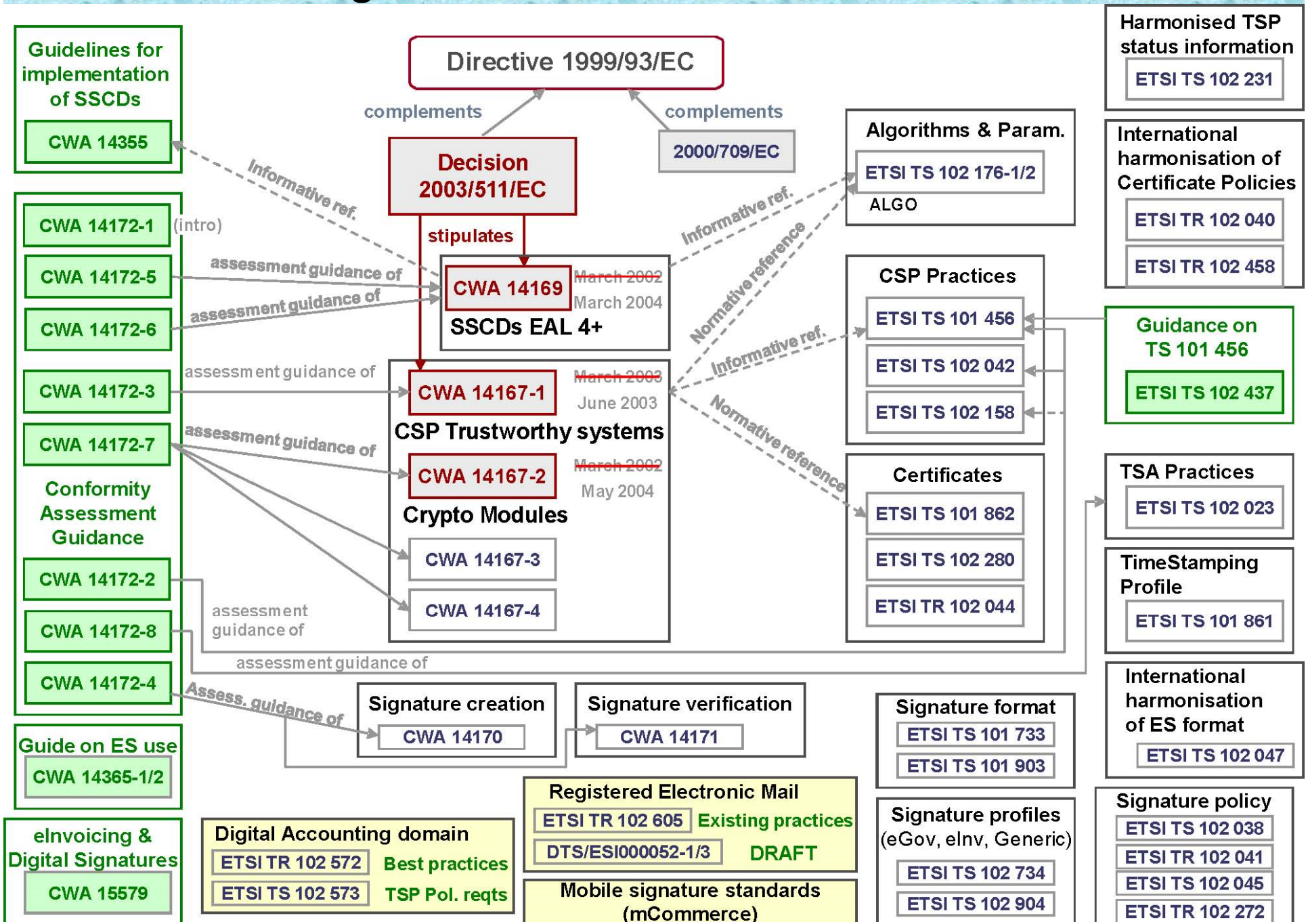
Закон об ЭЦП описывает:

- Advanced Signature;
- Qualified Signature = Advanced Signature + CMS Advanced Electronic Signature (основанная на qualified certificate и созданная с помощью SSCD - secure-signature-creation device).

Требования и рекомендации как правило используют модель защиты ключей симметричной криптографии.

Потребность: создать базовые нормативы управления сертификатами и ЭЦП.

EU eSignature Standardisation Work overview



Директива 1999/93/ES

Правило об отсутствии дискриминации подписи:

- Собственноручной
- Простой ЭП
- Advanced ЭП (аккредитованная ЭП, улучшенная ЭП)
- Квалифицированной ЭП

Квалифицированная ЭП:

1. Определяет правила квалифицированной ЭП

   НО:

   - Квалифицированная ЭП не синоним юридически значимой подписи (приравненной к собственноручной подписи).
   - Невыполнение требований к квалифицированной ЭП не означает отказ от принятия подписи к рассмотрению ее юридической значимости.
   - Выполнение требований к квалифицированной ЭП является одним из требований, но не единственным требованием, дающим возможность приравнять ЭП к собственноручной подписи.
2. Директива определяет: подпись (ЭП) должна быть защищена

Приложения к директиве:
Требование к квалифицированной ЭП

Требования к квалифицированной ЭП не должны прописываться на уровне закона, но прописываются на уровне технических стандартов

PKI applications Standards

- **1. "Implementing" the directive (1999/93/EC)**
- European Electronic Signature Standardization Initiative (EESSI)
  - CEN (Comité Européen de Normalisation) / ISSS (Information Society Standardization System) E-sign workshop
  - CWA – CEN (EUROPEAN COMMITTEE FOR STANDARDIZATION) workshop agreement
  - ETSI (European Telecommunications Standards Institute) TC (Technical Committee) / ESI (Electronic Signatures and Infrastructures)
- **"Implementing" the directive (1999/93/EC)**
- European Commission
  - Annex II of Directive 1999/93/EC (*Requirements for certification-service-providers issuing qualified certificates*):
    - CWA 14167-1 (March 2003): security requirements for trustworthy systems managing certificates for electronic signatures — Part 1: System Security Requirements
    - CWA 14167-2 (March 2002): security requirements for trustworthy systems managing certificates for electronic signatures — Part 2: cryptographic module for CSP signing operations — Protection Profile (MCSO-PP)
  - Annex III of Directive 1999/93/EC (*Requirements for secure signature-creation devices*):
    - CWA 14169 (March 2002): secure signature-creation devices
- **1.1. CEN/ISSS E-sign workshop**
- CWA 14167 (Multipart) - Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures
- CWA 14169 - **Secure Signature-creation devices "EAL 4+"**
- CWA 14170 - Security requirements for signature creation applications
- CWA 14171 - General guidelines for electronic signature verification
- CWA 14172 (Multipart) - EESSI Conformity Assessment Guidance
- CWA 14355 - Guidelines for the implementation of Secure Signature-Creation Devices
- CWA 14365 (Multipart) - Guide on the Use of Electronic Signatures
- CWA 14890 (Multipart) - Application Interface for smart cards used as Secure Signature Creation Devices
- **1.2. ETSI TC/ESI**
- ETSI TS 101 733 V1.7.3 - **CMS Advanced Electronic Signatures (CAdES)**
- ETSI TS 101 862 V1.3.3 - **Qualified Certificate profile**
- ETSI TS 101 456 V1.4.3 - Policy requirements for certification authorities issuing qualified certificates
- ETSI TS 102 042 V1.3.4 - Policy requirements for certification authorities issuing public key certificates
- ETSI TS 101 861 V1.3.1 - Time stamping profile
- ETSI TS 101 903 V1.3.2 - XML Advanced Electronic Signatures (XAdES)
- ETSI TR 102 605 V1.1.1 - Registered E-Mail

Предложения ООО Крипто Про по развитию нормативной базы PKI

Необходимо разработать проектные решения по информационным технологиям, методам, техническим средствам и системам, требованиям и стандартам, обеспечивающим единообразное применение ЭЦП в процессе предоставления государственных услуг и межведомственного взаимодействия, которые должны включать:

- Требования к составу и содержанию сертификатов, используемых в ЕПД ЭЦП;
- Требования к представлению ЭЦП в форматах криптографических сообщений XAdES (на основе XML), CAdES (на основе CMS), PAdES (на основе PDF) с учетом национальных стандартов;
- Требования к представлению ЭЦП цифровая подпись в формате XML (XMLDSIG) с учетом национальных стандартов
- Требования к представлению ЭЦП в списках поставщиков доверенных услуг (TSL);
- Требования к реализации протоколов служб штампов времени (TSP), онлайн проверки сертификатов (OCSP), протокола безопасного транспортного уровня (TLS) с учетом национальных стандартов.

Выводы и заключение

- В условиях подготовки нового закона «Об электронной подписи» необходимо провести анализ нормативной базы российской PKI на предмет полноты и достаточности с точки зрения применения в системах межведомственного взаимодействия и в процессе представления государственных услуг.
- Рассмотреть предложения ООО Крипто Про по развитию нормативной базы PKI.

- Вопросы.