РАЗВИТИЕ КРИПТОГРАФИЧЕСКОЙ ИНФРАСТРУКТУРЫ В РЕСПУБЛИКЕ БЕЛАРУСЬ

Шибков Александр Владимирович.
Оперативно-аналитический центр при Президенте Республики Беларусь
+375 17 309 23 88
e-mail shav@oac.gov.by

КРИПТОГРАФИЧЕСКАЯ ИНФРАСТРУКТУРА РЕСПУБЛИКИ БЕЛАРУСЬ (1994 – 2017)

ТЕХНИЧЕСКИЕ НОРМАТИВНЫЕ ПРАВОВЫЕ АКТЫ

I. Требования к криптографическим алгоритмам.

II. Требования к криптографическим протоколам.

III. Требования к форматам криптографических данных.

IV. Требования к средствам криптографической защиты информации.

V. Требования к взаимодействию с криптографическими токенами.

VI. Требования к инфраструктуре открытых ключей, в том числе к сервисам доверия.

КРИПТОГРАФИЧЕСКАЯ ИНФРАСТРУКТУРА РЕСПУБЛИКИ БЕЛАРУСЬ (1994 – 2017)

I. КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ.

ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».

СТБ 34.101.31-2011 «Информационные технологии. Защита информации. Криптографические алгоритмы шифрования и контроля целостности».

СТБ 34.101.45-2013 **«**Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых».

СТБ 34.101.47-2017 **«**Информационные технологии и безопасность. Криптографические алгоритмы генерации псевдослучайных чисел».

СТБ 34.101.60-2014 **«**Информационные технологии и безопасность. Алгоритмы разделения секрета».

КРИПТОГРАФИЧЕСКАЯ ИНФРАСТРУКТУРА РЕСПУБЛИКИ БЕЛАРУСЬ (1994 – 2017)

II. КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ.

СТБ 34.101.65-2014 «Информационные технологии и безопасность. Протокол защиты транспортного уровня (TLS)»

СТБ 34.101.66-2014 «Информационные технологии и безопасность. Протоколы аутентификации и выработки общего ключа на основе эллиптических кривых»

OpenID, OAuth

КРИПТОГРАФИЧЕСКАЯ ИНФРАСТРУКТУРА РЕСПУБЛИКИ БЕЛАРУСЬ (1994 – 2017)

III. ФОРМАТЫ КРИПТОГРАФИЧЕСКИХ ДАННЫХ.

СТБ 34.101.17-2012 «Информационные технологии и безопасность. Синтаксис запроса на получение сертификата». (PKCS#10).

СТБ 34.101.19-2012 «Информационные технологии и безопасность. Форматы сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей». (rfc5280:2008).

СТБ 34.101.18-2009 «Информационные технологии. Синтаксис обмена персональной информацией» (PKC#12).

СТБ 34.101.23-2012 «Информационные технологии и безопасность. Синтаксис криптографических сообщений». (CMS).

СТБ 34.101.26-2012 «Информационные технологии и безопасность. Онлайновый протокол проверки статуса сертификата (OCSP)».

КРИПТОГРАФИЧЕСКАЯ ИНФРАСТРУКТУРА РЕСПУБЛИКИ БЕЛАРУСЬ (1994 – 2017)

IV. СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ.

ПРОГРАММНЫЕ

СТБ 34.101.27-2011 «Информационные технологии и безопасность. Требования безопасности к программным средствам криптографической защиты информации»

ПРОГРАММНО-АППАРАТНЫЕ

СТБ 34.101.1-2014 «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель».

СТБ 34.101.2-2014 «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности».

СТБ 34.101.3-2014 «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 3. Гарантийные требования безопасности».

КРИПТОГРАФИЧЕСКАЯ ИНФРАСТРУКТУРА РЕСПУБЛИКИ БЕЛАРУСЬ (1994 – 2017)

V. КРИПТОГРАФИЧЕСКИЕ ТОКЕНЫ.

СТБ 34.101.20-2009 «Информационные технологии. Синтаксис криптографической информации для токенов». (PKCS#15).

СТБ 34.101.21-2009 «Информационные технологии. Интерфейс обмена информацией с аппаратно-программным носителем криптографической информации (токеном)». (PKCS#11).

КРИПТОГРАФИЧЕСКАЯ ИНФРАСТРУКТУРА РЕСПУБЛИКИ БЕЛАРУСЬ (1994 – 2017)

VI. ИНФРАСТРУКТУРА ОТКРЫТЫХ КЛЮЧЕЙ.

СТБ 34.101.48-2012 «Информационные технологии и безопасность. Требования к политике применения сертификатов удостоверяющих центров».

СТБ 34.101.49-2012 «Информационные технологии и безопасность. Формат карточки открытого ключа».

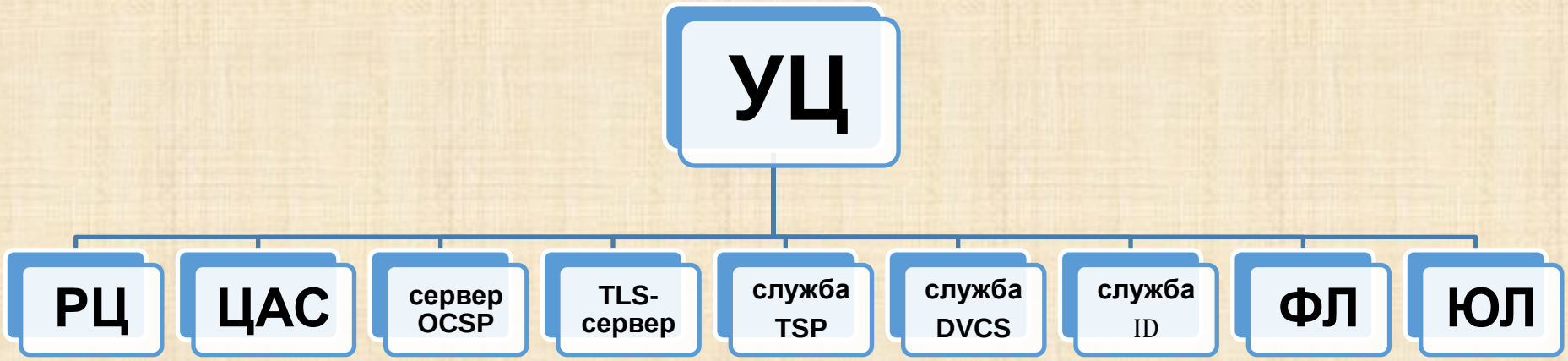
ЗАДАЧИ ПО РАЗВИТИЮ НАЦИОНАЛЬНОЙ PKI (ГОСУДАРСТВЕННАЯ СИСТЕМА УПРАВЛЕНИЯ ОТКРЫТЫМИ КЛЮЧАМИ ПРОВЕРКИ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ РЕСПУБЛИКИ БЕЛАРУСЬ

1. Конкретизировать стороны инфраструктуры открытых ключей.
2. Определить типовые процедуры взаимодействия;.
3. Разработать форматы данных при обмене между сторонами.
4. Разработать прикладные интерфейсы взаимодействия между сторонами ГосСУОК, а также сторон ГосСУОК с прикладными системами.
5. Определить требования к формату ключевого контейнера программных криптографических токенов.
6. Разработать высокоуровневые интерфейсы взаимодействия криптографического программного обеспечения средств электронной цифровой подписи с аппаратными криптографическими токенами (USB-токены, токены на смарт-картах).

СТБ 34.101.78

«Информационные технологии и безопасность. Профиль инфраструктуры открытых ключей» (https://github.com/bcrypto/bpki/releases - СТБ 34.101.bpki v1.00)

СТОРОНЫ ВЗАИМОДЕЙСТВИЯ



СТБ 34.101.78

«Информационные технологии и безопасность. Профиль инфраструктуры открытых ключей»

ПРОЦЕССЫ УПРАВЛЕНИЯ СЕРТИФИКАТАМИ

1 **Enroll** — выпуск сертификата для стороны, которая располагает действительным удостоверением, но не обязательно действительным сертификатом.

2 **Reenroll** — обновление действительного сертификата.

3 **Spawn** — выпуск нового сертификата для стороны, которая располагает действительным сертификатом.

4 **Retrieve** — получение сертификата, который был запрошен в процессах Enroll, Reenroll, Spawn и выпуск которого задерживается.

5 **Chpwd** — установка (изменение) пароля отзыва сертификата.

6 **Revoke** — отзыв сертификата.

СТБ 34.101.78
«Информационные технологии и безопасность. Профиль инфраструктуры открытых ключей»

РЕШЕНИЕ ИНЫХ ЗАДАЧ

ФОРМАТЫ ДАННЫХ

ПРОГРАММНЫЙ КЛЮЧЕВОЙ КОНТЕЙНЕР

ПРОГРАММНЫЙ ИНТЕРФЕЙС

ТРАНСПОРТ

СТБ 34.101.79
«Информационные технологии и безопасность. Криптографические токены»
(https://github.com/bcrypto/btok/releases - СТБ 34.101_btok v0.05)

КРИПТОГРАФИЧЕСКИЙ ТОКЕН АУТЕНТИФИКАЦИИ (e-Sign, e-ID)

- внутренние объекты токена (криптографические ключи, сертификаты, идентификационные данные владельца);
- криптографические алгоритмы;
- криптографические протоколы;
- компоновка алгоритмов в прикладные программы;
- схема аутентификации (использование токенов для аутентификации в информационных системах);
- командный интерфейс взаимодействия КТА с клиентской программой и терминал посредством APDU-команд.

e-IDAS

Регламент Европейского парламента и Совета (ЕС) от 23 июля 2014 года № 910/2014

Об электронных идентификационных и доверительных услугах для электронных транзакций на внутреннем рынке.

- СЕРВИС КВАЛИФИЦИРОВАННОЙ ЭЛЕКТРОННОЙ ПОДПИСИ
- СЕРВИС ДОСТОВЕРНОГО ПОДТВЕРЖДЕНИЯ ПОДЛИННОСТИ ЭЛЕКТРОННОЙ ПОДПИСИ
- СЕРВИС ЭЛЕКТРОННОЙ ПЕЧАТИ
- СЕРВИС ШТАМПА ВРЕМЕНИ
- СЕРВИС ГАРАНТИРОВАННОЙ ДОСТАВКИ
- СЕРВИС АУТЕНТИФИКАЦИИ WEB-SITE

НАЦИОНАЛЬНАЯ ИНФРАСТРУКТУРА ОТКРЫТЫХ КЛЮЧЕЙ. СЕРВИСЫ ДОВЕРИЯ

РАСШИРЕННАЯ ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ

проект **СТБ 34.101.80**
«Информационные технологии и безопасность.
Расширенные электронные цифровые подписи»
https://github.com/bcrypto/stb/tree/master/34.101.80

ETSI EN 319 132-1 V1.1.1. Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures.

ETSI EN 319 132-2 V1.1.1. Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures.

ETSI TS 319 122-1 V1.1.1. Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures.

ETSI TS 319 122-2 V1.1.1. Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures.

ETSI TS 102 778-1 V1.1.1. Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview - a framework document for PAdES.

ETSI TS 102 778-2 V1.2.1. Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 2: PAdES Basic - Profile based on ISO 32000-1.

ETSI TS 102 778-3 V1.1.2. Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles.

ETSI TS 102 778-4 V1.1.1. Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 4: PAdES Long Term - PAdES-LTV Profile.

ETSI TS 102 778-5 V1.1.1. Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 5: PAdES for XML Content - Profiles for XAdES signatures.

РАСШИРЕННАЯ ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ

Электронная цифровая подпись документа и атрибутов (подписанных) вместе с дополнительными атрибутами (неподписанными), которые касаются подписанного документа и подписавшей его стороны

ФОРМАТЫ РЭЦП:

CAdES является уточнением формата подписанных данных, определенного в СТБ 34.101.23. Подпись CAdES описывается на языке АСН.1 и задается типом SignedData. Подписываемый документ может иметь произвольный формат.

XAdES (от англ. XML Advanced Electronic Signature) является уточнением формата XML-DSig. Подпись XAdES описывается на языке XML. Подписываются части (элементы) XML-документа или весь XML-документ целиком.

PAdES (от англ. PDF Advanced Electronic Signature) встраивается в документы формата PDF. Подпись представляется либо в формате CAdES, либо в формате XAdES.

РАСШИРЕННАЯ ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ

ПОСТАВЩИКИ УСЛУГ ДОВЕРИЯ

- удостоверяющий центр
- издатель списков отозванных сертификатов
- регистрационный центр
- сервер OCSP
- служба хранения
- служба простановки штампов времени
- служба рапортов времени
- издатель политики подписи
- центры атрибутных сертификатов
- службы заверения данных

РАСШИРЕННАЯ ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ

ПРОФИЛИ АТРИБУТОВ
(базовые B-B B-T B-LT B-LTA
+
расширенные)

БАЗОВЫЕ АТРИБУТЫ
(подписант, подписываемые данные, подпись)

АТРИБУТЫ,
содержащие штамп времени подписи

АТРИБУТЫ,
содержащие проверочные данные

АТРИБУТЫ,
содержащие данные для архивной проверки

сервис OCSP
онлайновая проверка статуса сертификата

СТБ 34.101.26-2012

«Информационные технологии и безопасность. Онлайновый протокол проверки статуса сертификата (OCSP)»

СООБРАЖЕНИЯ БЕЗОПАСНОСТИ

обязательное подключение систем к поставщику OCSP;

«отказ в обслуживании»;

использование заранее вычисленных ответов;

запросы не содержат информацию о службе, в которую они направляются;

надежность механизмов кэширования HTTP.

ИНФРАСТРУКТУРА АТРИБУТНЫХ СЕРТИФИКАТОВ

СТБ 34.101.67-2014

«Информационные технологии и безопасность. Инфраструктура атрибутных сертификатов».

форматы атрибутных сертификатов, классы атрибутов, маршруты атрибутных сертификатов;

отношения между УЦ и ЦАС, а также привилегии в АС и СОК;

модели инфраструктуры управления привилегиями;

расширения сертификатов, связанные с управлением привилегиями (отзыв, источники привилегий, роли, делегирование, управление доменами);

процедуры обработки маршрутов АС;

схема директории ИУП (классы объектов, атрибуты ДИУП, общие правила соответствия.

ИНФРАСТРУКТУРА АТРИБУТНЫХ СЕРТИФИКАТОВ

общая модель (объект, заявитель привилегии, инспектор привилегии);

модель системы управления доступом (заявитель привилегии (прав доступа), инспектор привилегии, объект, политика применения привилегий, параметры среды);

модель делегирования привилегий (источник привилегий, инспектор привилегий, другие ЦАС, заявитель привилегий);

модель назначения привилегий группе субъектов (через групповой АС – прямое наименование группы либо ролевое наименование группы – определяется компонентом holder);

модель ролей;

модель взаимодействия доменов (локальная ИУП и удаленная ИУП) – статическая либо динамическая модель;

СЛУЖБА ПРОСТАНОВКИ ШТАМПА ВРЕМЕНИ

проект **СТБ.ПР.34.101.82**
«Информационные технологии и безопасность. Протокол постановки штампа времени»
https://github.com/bcrypto/stb/blob/master/34.101.82/t
(rfc3161 Internet X.509 Public Key Infrastructure. Time-Stamp Protocol (TSP))

СЛУЖБА ПРОСТАНОВКИ ШТАМПОВ ВРЕМЕНИ

поставщик услуг доверия, который создает штампы времени для подтверждения соответствия данных к определенному моменту времени.

ШТАМП ВРЕМЕНИ

(time-stamp token)

информационный объект, который связывает представление данных (как правило, значение хэш-функции) с определенным моментом времени, тем самым удостоверяя существование данных к этому времени.

СЛУЖБА ЗАВЕРЕНИЯ ДАННЫХ

проект СТБ 34.101.81 «Информационные технологии и безопасность. Протоколы службы заверения данных»
(rfc3029 Internet X.509 Public Key Infrastructure. Data Validation and Certification Server Protocols (DVCS))

СЛУЖБА ЗАВЕРЕНИЯ ДАННЫХ

поставщик услуг доверия, который подтверждает факты владения данными, существования данных, действительности электронных документов и сертификатов открытых ключей, выпуская аттестаты заверения

СЕРВИСЫ СЛУЖБЫ ЗАВЕРЕНИЯ ДАННЫХ

заверение факта владения данными (cpd – Certificate of Procession of Data);

заверение факта существования данных (ccpd – Certification of Claim of Procession of Data);

проверка действительности электронных документов (vsd – Validation of Signed Document);

проверка действительности сертификата открытого ключа (vpkc – Validation of Public key Certificate).

СЛУЖБА ЗАВЕРЕНИЯ ДАННЫХ (DVCS)

ОБЯЗАТЕЛЬНЫЕ УСЛОВИЯ

служба должна обрабатывать запросы на заверение – результат аттестат (квитанция) либо сообщение об ошибке

в аттестате должны быть указаны заверенные факты либо сообщение о причине отказа от заверения;

должна применяться политика заверения данных;

аттестаты должны нумероваться, используя монотонно возрастающий номер; который должен содержаться в выпускаемом аттестате;

в аттестат должна быть включена отметка времени либо штамп времени;

для личного ключа службы, который используется для подписи аттестата выпускается отдельный СОК (в KeyUsage – биты digitalSignature, nonRepudiation, keyCertSign, cRLSign, кроме того в СОК расширение ExtKeyUsageSyntax с идентификатором службы);

аттестат должен содержать ссылку на СОК службы, которая определяется значением типа ESSCertIDv2 в подписанном атрибуте SigningCertificatev2;

перед выпуском аттестата службы должна проверять действительность собственного СОК и заверяемых СОК.

СЛУЖБА ЗАВЕРЕНИЯ ДАННЫХ (DVCS)

ЗАПРОС описывается типом – DVCSRequest ::= SEQUENCE

ОТВЕТ описывается типом DVCSResponse ::= SEQUENCE
ФОРМАТ ОТВЕТА представляет собой подписанные данные типа SignetData, которые инкапсулируются в ContentInfo

вспомогательные типы данных

DigestInfo – описывает хэш-значение;
DVCSTime – описывает метку времени;
PKIStatusInfo – описывает результат выполненной проверки;
PathProcInput – описывает политики;
CertEtcToken – описывает аттестат, который требуется проверить или который уже проверен, и результат проверки;
TargetEtcChain- описывает сертификат, который требуется проверить или который уже проверен, результаты проверки, политики проверки;
DVCSRequestInformation – описывает общие, не относящиеся к заверяемым фактам, данные запроса;
Data – описывает заверяемые данных;
DVCSCertInfo – описывает содержание аттестата заверения/

СПАСИБО ЗА ВНИМАНИЕ !

Шибков Александр Владимирович.
Оперативно-аналитический центр при
Президенте Республики Беларусь
+375 17 309 23 88
e-mail shav@oac.gov.by