

Актуальные вопросы применения международной системы аудита удостоверяющих центров в странах с национальной криптографией



Кирюшкин Сергей Анатольевич, к.т.н.
Советник генерального директора
ООО "Газинформсервис",
Санкт-Петербург, Россия
Kiryushkin-S@gaz-is.ru

www.gaz-is.ru

Тел. +7(812)305-20-50

Цели доклада

1. Затронуть вопрос;
2. Поделиться мнением относительно его актуальности;
3. Обменяться мнениями с экспертным сообществом по **необходимости** решения данного вопроса.

Характеристики современной РКІ

1. РКІ – эффективная основа комплексных решений в области информационной безопасности и юридической силы электронных документов;

Характеристики современной РКІ

2. В некоторых случаях интересы национальной безопасности определяют необходимость национальных решений в области РКІ

Характеристики современной РКІ

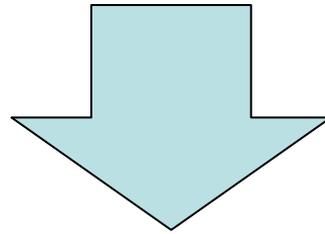
3. Популярность использования РКІ растет, применение становится массовым

Характеристики современной РКІ

4. Процессы международной интеграции предполагают применение технологий, обладающих трансграничной интероперабельностью

Основные тренды

- Массовое применение
- Трансграничная интероперабельность



Прозрачная для пользователя
применимость в наиболее
распространенных платформах,
приложениях, технологиях

В наиболее распространенных...

- Microsoft Internet Explorer
- Mozilla Firefox
- Opera
- Google Chrome
- Apple Safari 4.0, Apple iPhone, iPod Safari 3.0, Apple Mail
- Microsoft Windows
- Apple MacOS
- Linux (OpenSSL)
- Microsoft Outlook
- Mozilla Thunderbird
- Microsoft Office (Word, Excel, Powerpoint, Access, InfoPath)
- Microsoft Authenticodes & Visual Basic Applications (VBA)
- ...

Применимость прозрачная для пользователя

- СКЗИ встроенное в платформу
- Доверие к сертификатам “на лету”

СКЗИ встроенное в платформу

Можно констатировать, что в РФ и в Украине **есть** **положительная динамика:**

- В РФ – ФЗ-63, неквалифицированная электронная подпись
- Публикация 4 июня 2010 г. стандарта ISO/IEC 14888-3:2006/Amd 1:2010 «Elliptic Curve Russian Digital Signature Algorithm...»
- В Украине – криптографические стандарты ETSI, в том числе на государственном уровне

WebTrust for Certification Authorities

Название программы:

WebTrust^{SM/TM} Program for Certification Authorities

Инициатива принадлежит:

- American Institute of Certified Public Accountants, Inc.
- Canadian Institute of Chartered Accountants.

Исполнитель:

AICPA/CICA Electronic Commerce Assurance Task Force

WebTrust for Certification Authorities

Программа служит основой для аудиторов WebTrust®, позволяющей оценить соответствие и эффективность средств управления, используемых провайдерами сертификационных услуг (центрами сертификации, удостоверяющими центрами)

WebTrust for Certification Authorities

Базовые принципы программы:

- 1) Открытость бизнес-практики СА
- 2) Интегральный подход к предоставлению сервисов
- 3) Контроль среды функционирования

Программы сертификации root-ов (RCP)

- Apple Root Certificate Program
- Microsoft Root Certificate Program
- Mozilla CA Certificate Policy
- Specification for X.509 root certificates to be included in the Opera browser
- ...

Попробуем найти Украинский или Российский root

Консоль1 - [Корень консоли\Сертификаты - текущий пользователь\Доверенные корневые центры сертификации\Сертификаты]

Файл Действие Вид Избранное Окно Справка

Корень консоли

- Сертификаты - текущий пользователь
 - Личное
 - Доверенные корневые центры сертификации**
 - Сертификаты**
 - Доверительные отношения в предприятии
 - Промежуточные центры сертификации
 - Объект пользователя Active Directory
 - Доверенные издатели
 - Сертификаты, к которым нет доверия
 - Сторонние корневые центры сертификации
 - Доверенные лица
 - Другие пользователи
 - Запросы заявок на сертификат
 - Доверенные корневые сертификаты смарт-ка

Кому выдан	Кем выдан	Срок действия	Назначения	Имя
AddTrust External CA Root	AddTrust External CA Root	30.05.2020	Проверка подлин...	USERTrust
America Online Root Certificati...	America Online Root Certification...	20.11.2037	Проверка подлин...	America Online Ro...
Certum CA	Certum CA	11.06.2027	Проверка подлин...	Certum
Certum Trusted Network CA	Certum Trusted Network CA	31.12.2029	Проверка подлин...	Certum Trusted Ne...
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	02.08.2028	Защищенная элек...	VeriSign Class 3 Pu...
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	08.01.2004	Защищенная элек...	VeriSign
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	31.12.1999	Установка отметки...	Microsoft Timesta...
DigiCert High Assurance EV Ro...	DigiCert High Assurance EV Root ...	10.11.2031	Проверка подлин...	DigiCert
Entrust Root Certification Auth...	Entrust Root Certification Authority	28.11.2026	Проверка подлин...	Entrust
Entrust.net Certification Author...	Entrust.net Certification Authority...	24.07.2029	Проверка подлин...	Entrust (2048)
Entrust.net Secure Server Certifi...	Entrust.net Secure Server Certifica...	25.05.2019	Проверка подлин...	Entrust
Equifax Secure Certificate Auth...	Equifax Secure Certificate Authority	22.08.2018	Защищенная элек...	GeoTrust
GeoTrust Global CA	GeoTrust Global CA	21.05.2022	Проверка подлин...	GeoTrust Global CA
GeoTrust Primary Certification ...	GeoTrust Primary Certification Au...	17.07.2036	Проверка подлин...	GeoTrust
GIS Certification Authority	GIS Certification Authority	05.08.2014	<Все>	<Нет>
GIS Certification Authority	GIS Certification Authority	05.08.2014	<Все>	<Нет>
GiS Root Certification Authority	GiS Root Certification Authority	23.10.2039	<Все>	<Нет>
GlobalSign Root CA	GlobalSign Root CA	28.01.2028	Проверка подлин...	GlobalSign
Go Daddy Class 2 Certification ...	Go Daddy Class 2 Certification Au...	29.06.2034	Проверка подлин...	Go Daddy Class 2 C...
GTE CyberTrust Global Root	GTE CyberTrust Global Root	14.08.2018	Защищенная элек...	GTE CyberTrust Glo...
http://www.valicert.com/	http://www.valicert.com/	26.06.2019	Защищенная элек...	Starfield Technolog...
Microsoft Authenticode(tm) Ro...	Microsoft Authenticode(tm) Root...	01.01.2000	Защищенная элек...	Microsoft Authent...
Microsoft Forefront TMG HTTP...	Microsoft Forefront TMG HTTPS I...	01.01.2049	Архивация закрыт...	<Нет>
Microsoft Forefront TMG HTTP...	Microsoft Forefront TMG HTTPS I...	01.01.2049	Архивация закрыт...	<Нет>
Microsoft Root Authority	Microsoft Root Authority	31.12.2020	<Все>	Microsoft Root Aut...
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	10.05.2021	<Все>	Microsoft Root Cert...
NO LIABILITY ACCEPTED, (c)97 ...	NO LIABILITY ACCEPTED, (c)97 V...	08.01.2004	Установка отметки...	VeriSign Time Stam...
StartCom Certification Authority	StartCom Certification Authority	17.09.2036	Проверка подлин...	StartCom Certificati...
Symantec Root 2005 CA	Symantec Root 2005 CA	24.08.2020	<Все>	<Нет>
Symantec Root CA	Symantec Root CA	01.05.2011	<Все>	<Нет>
Thawte Personal Freemail CA	Thawte Personal Freemail CA	01.01.2021	Проверка подлин...	thawte

Попробуем найти Украинский или Российский root



Принципиальное препятствие... ...было

NIST Special Publication 800-57

March, 2007

NIST

**National Institute of
Standards and Technology**

Recommendation for Key
Management – Part 1: General
(Revised)

**Elaine Barker, William Barker, William Burr,
William Polk, and Miles Smid**

Осталось аудитора найти....



Licensed WebTrust Practitioners : International

Below is a list of global practitioners. For contact information, click on the name of the firm you wish to contact and Christina Herwig will provide you with the information you require

Australia
Belgium
Brazil
Canada
China
Colombia
Denmark

Hong Kong
Germany
Israel
Japan
Malaysia
Mexico
Middle East

Netherlands
Poland
Spain
Taiwan
United States
United Kingdom

И ДЕНЬГИ...



Штрих к вопросу о востребованности

https://esia.gosuslugi.ru/idp/Authn/Commo

Правка Вид Избранное Сервис Справка

Рекомендуемые узлы Девятая ежегодная межд...

ти: 14888

ЭЛЕКТРОННОЕ ПРАВИТЕЛЬСТВО ГОСУСЛУГИ
Госуслуги прозрачны как никогда!

Граждане РФ, ИП

Авторизация

По паролю По...

Введите страховой номер индивидуального лицевого счёта (СНИЛС) и номер персонализированного учётного записи Пенсионного фонда России.

СНИЛС

Сертификат

Общие Состав Путь сертификации

Путь сертификации

- thawte
 - Thawte SSL CA
 - *.gosuslugi.ru

Состояние сертификата:
Этот сертификат действителен.

Подробнее о [путях сертификации](#)

Сертификат

Общие Состав Путь сертификации

Показать: <Все>

Поле	Значение
Версия	V3
Серийный номер	4d 5f 2c 34 08 b2 4c 20 cd 6d ...
Алгоритм подписи	sha1RSA
Алгоритм хэширования по...	sha1
Издатель	thawte Primary Root CA, (c) 2...
Действителен с	8 февраля 2010 г. 4:00:00
Действителен по	8 февраля 2020 г. 3:59:59
Субъект	Thawte SSL CA Thawte, Inc

CN = thawte Primary Root CA
OU = (c) 2006 thawte, Inc. - For authorized use only
OU = Certification Services Division
O = thawte, Inc.
C = US

Свойства... Копировать в файл...

Подробнее о [составе сертификата](#)

ОК

Штрих к вопросу о востребованности



Сейчас, внучек, вот только устанавливаю самоподписанный сертификат в хранилище “доверенные корневые”

Вопрос к экспертам – участникам Форума

- Необходимы ли для развития РКІ как массового инструмента, обладающего в том числе трансграничной интероперабельностью, национальные издатели в предусмотренных траст-листах наиболее популярного ПО?

PKI-Форум Россия

ДЕСЯТАЯ ЮБИЛЕЙНАЯ

**ЕЖЕГОДНАЯ МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ ПО ПРОБЛЕМАТИКЕ
ИНФРАСТРУКТУРЫ ОТКРЫТЫХ КЛЮЧЕЙ И ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ**

«PKI-FORUM РОССИЯ 2012»



Место проведения: г. Санкт-Петербург,
гостиница «Прибалтийская»

Даты проведения: 18 – 20 сентября 2012 г.

Организатор: Минкомсвязи России

При участии: ФСБ России, ФСТЭК России

Организационная поддержка:
«Авангард Центр», МОО «АЗИ»

<http://www.pki-forum.ru/>

Дякую за увагу!
Dziękuję za uwagę!
Рақмет соң көңілді !
Спасибо за внимание!



Кирюшкин Сергей Анатольевич, к.т.н.
Советник генерального директора
ООО "Газинформсервис",
Санкт-Петербург, Россия
Kiryushkin-S@gaz-is.ru

www.gaz-is.ru
Тел. +7(812)305-20-50