«PKI - FORUM Украина 2012»
www.pki-forum.com.ua
16-18 мая, г.Киев, Украина

ГАЗИНФОРМСЕРВИС

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

PKI FORUM UKRAINE 2012

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 PKI

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

Характеристики современной PKI

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

Характеристики современной PKI

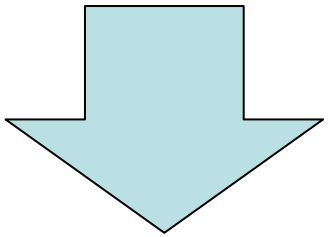
3. Популярность использования PKI растет, применение становится массовым

Характеристики современной PKI

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 **<u>есть положительная динамика:</u>**

- 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

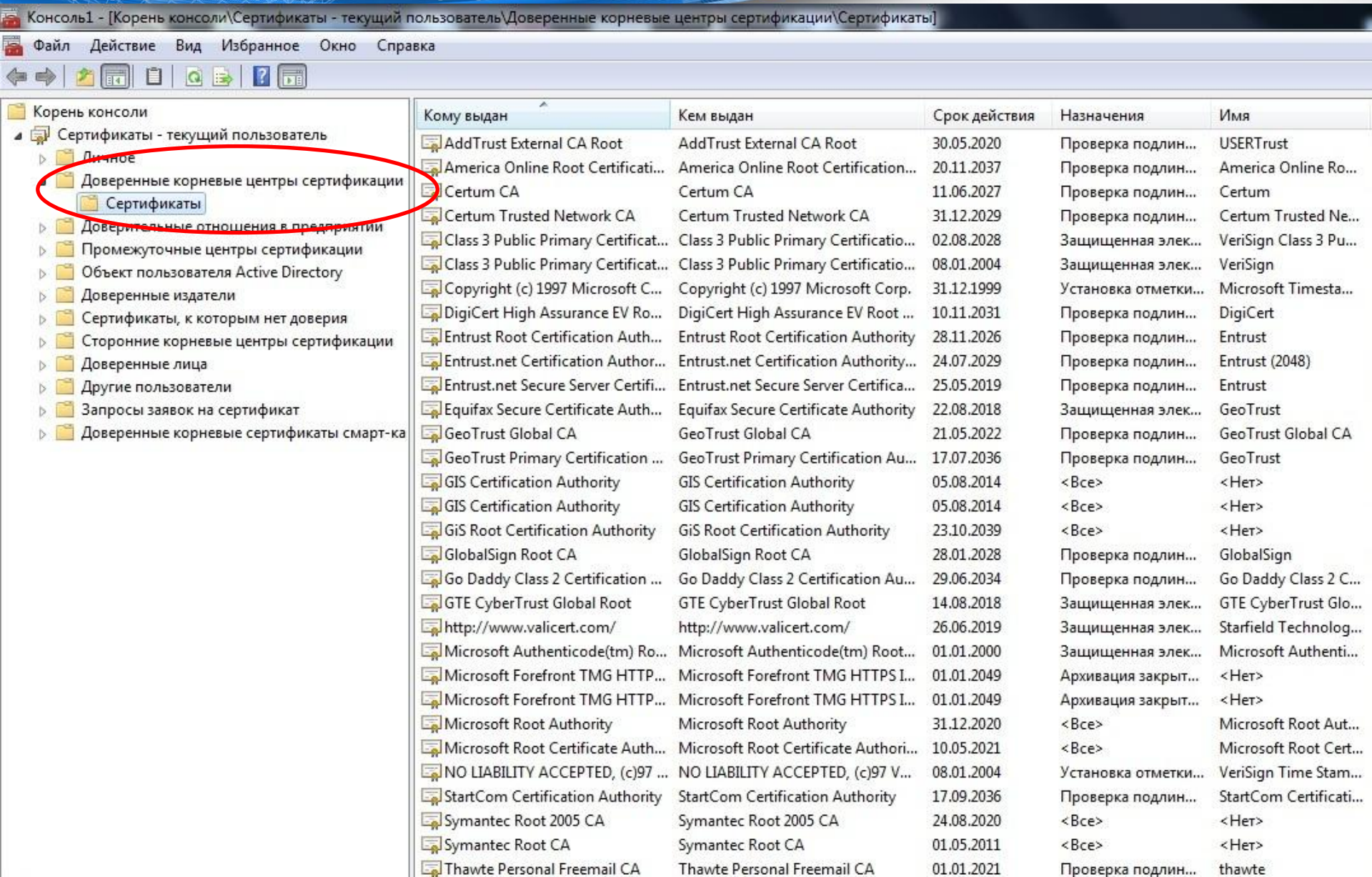
Базовые принципы программы:

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

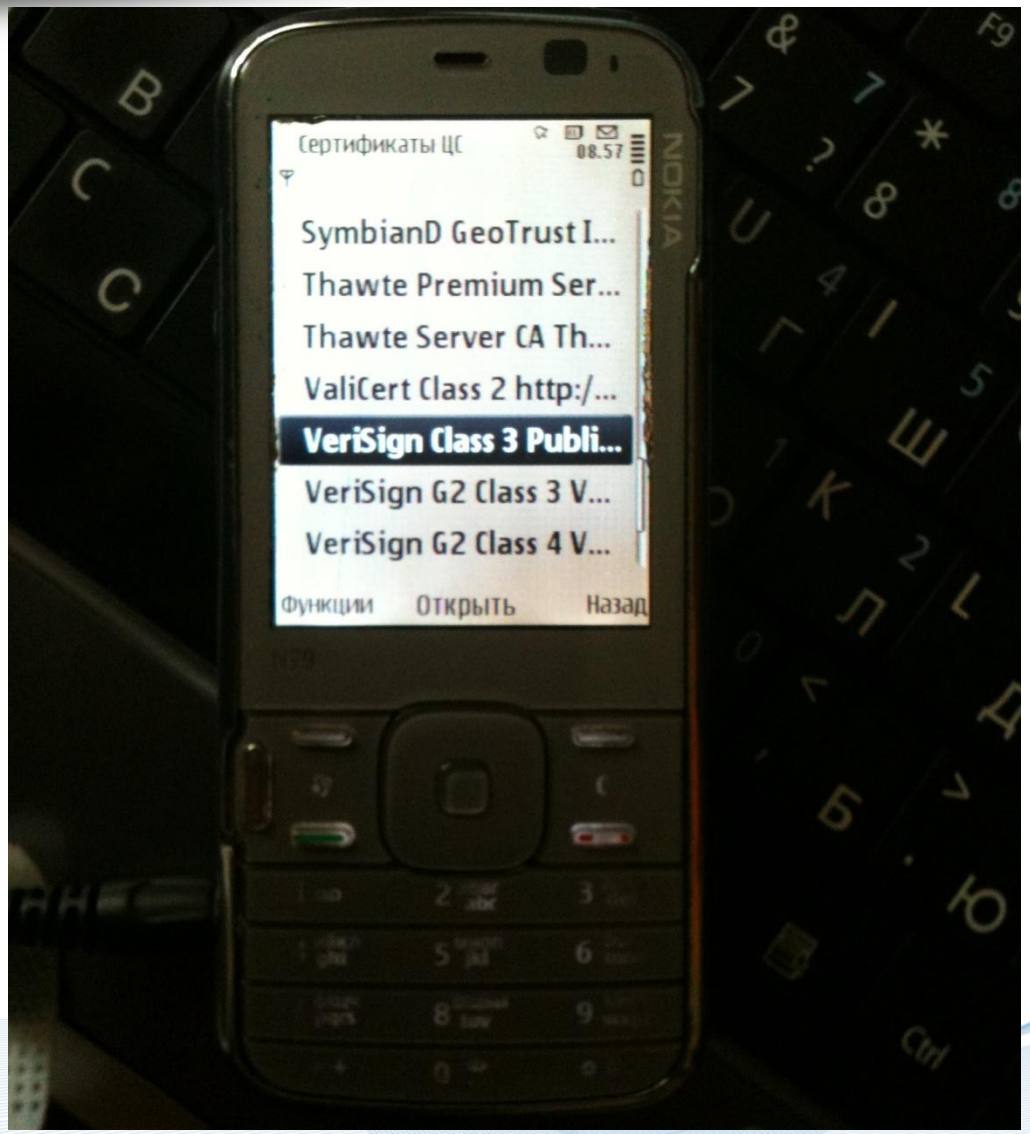
Программы сертификации root-ов (RCP)

- 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



Попробуем найти Украинский или Российский root



Принципиальное препятствие…

…было

NIST Special Publication 800-57

March, 2007

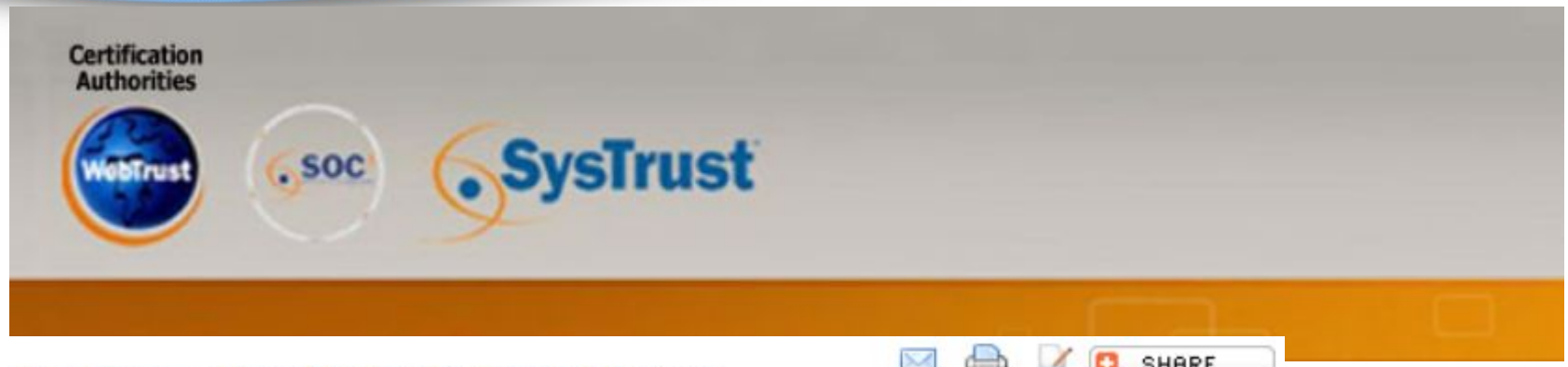
Recommendation for Key Management – Part 1: General (Revised)

NIST

National Institute of Standards and Technology

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

Осталось аудитора найти...



Trust Services > Licensed WebTrust Practitioners : International

SHARE

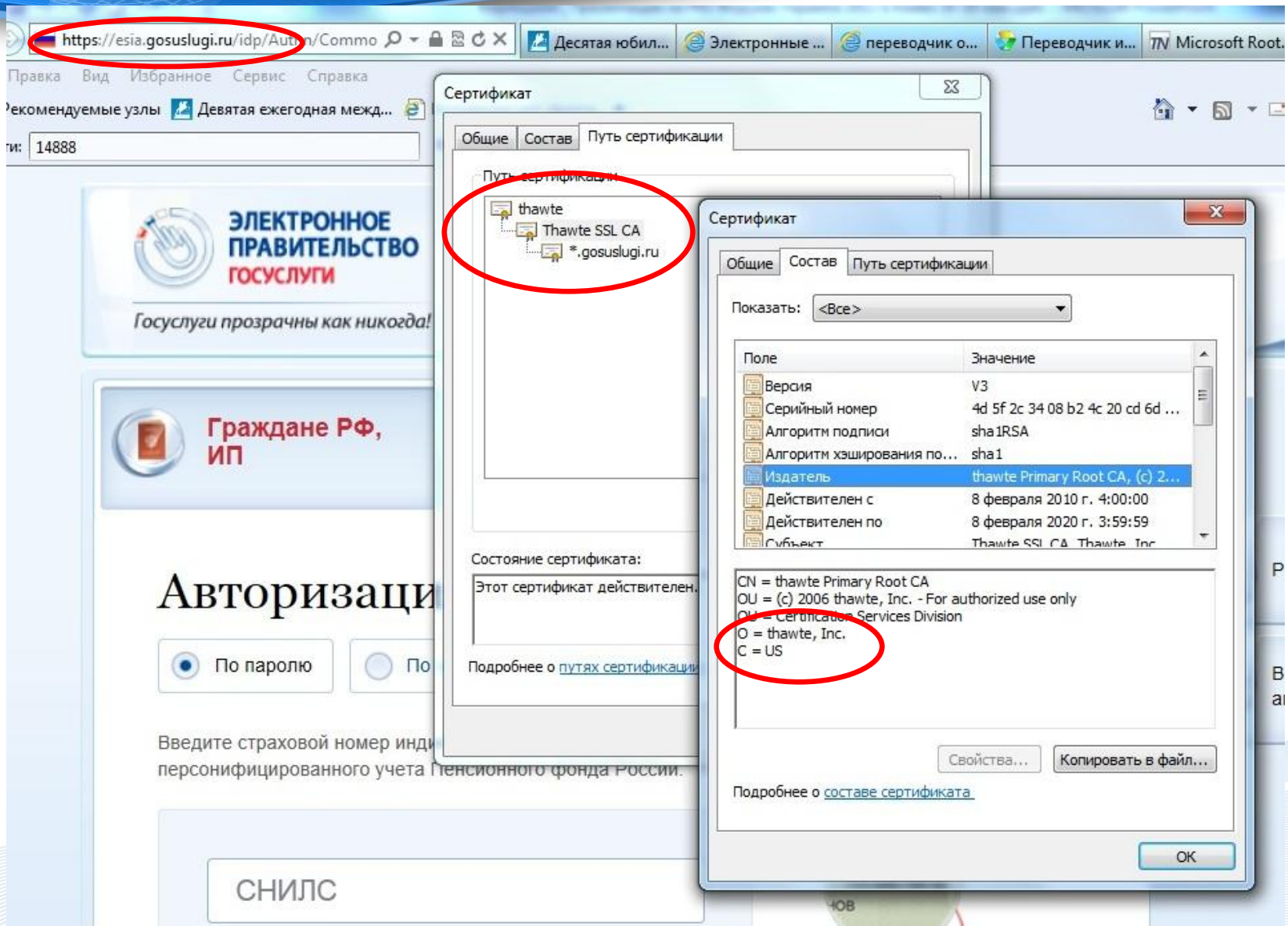
Licensed WebTrust Practitioners : International

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



Штрих к вопросу о востребованности

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

Вопрос к экспертам – участникам Форума

- Необходимы ли для развития PKI как массового инструмента, обладающего в том числе трансграничной интероперабельностью, национальные издатели в предустановленных 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!
Dziękujemy 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