Проблемы долговременного хранения действующих и исторических документов, подписанных электронно – цифровой подписью

Храмцовская Наталья Александровна

к.и.н., ведущий эксперт по управлению документацией
компании «Электронные Офисные Системы»,
член Гильдии Управляющих Документацией и ARMA International

Вопросы, которые придется решать при долговременном хранения документов с ЭЦП

- Как обеспечить проверку ЭЦП на протяжении длительного периода времени, и нужно ли это?
- Как доказывать аутентичность, целостность и т.д. соответствующих электронных документов?
- Что делать с подписанными электронным образом документами постоянного срока хранения?
- ЭЦП не неуязвима, и со временем может быть скомпрометирована и/или подделана. Что делать?

Практика

- Уже шесть лет работают полноценные государственные электронные архивы. ЭЦП проверяется в момент поступления документов на архивное хранение.
- Лет десять говорят о возможности переподписания документов. Реально работающей, признанной законодательством России технологии до сих пор нет. Скандал в Германии при попытке такую технологию ввести.

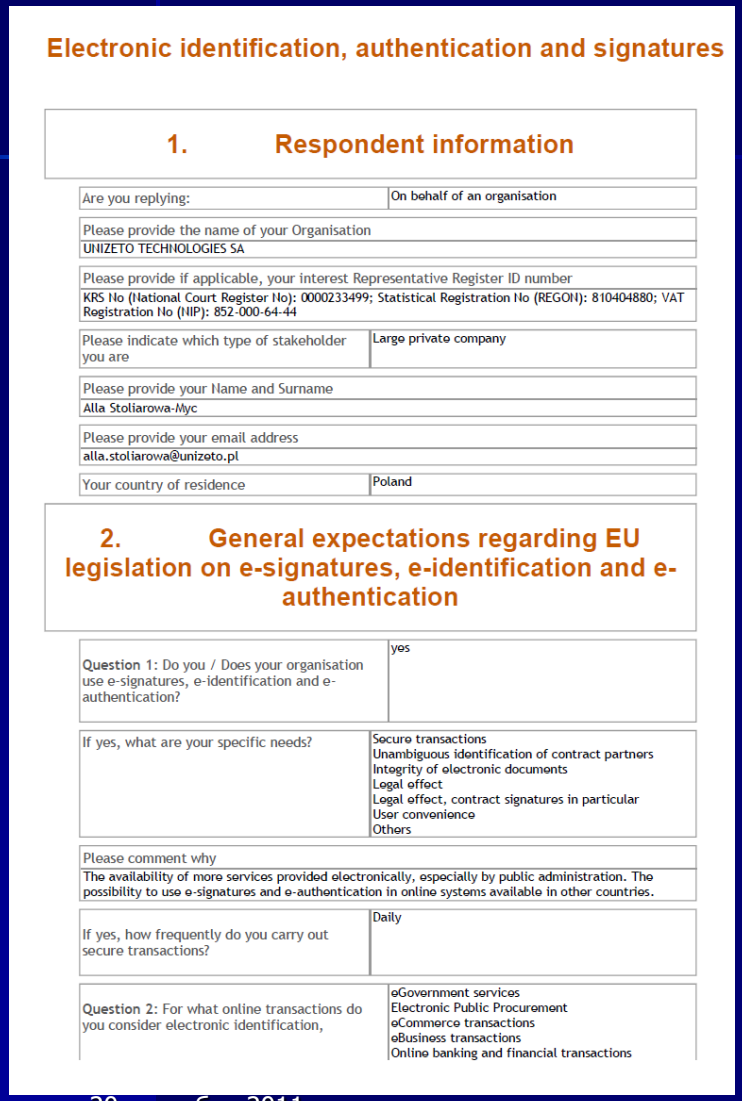
Отчет UNCITRAL о правовых проблемах при использовании средств электронной идентификации и подписи, 2009 г.

- **Проблемы при практическом использовании инфраструктуры открытых ключей**

  «...Долговременная сохранность ЭЦП обычно проблематична. ...Фактически, ЭЦП были задуманы скорее для обеспечения безопасности при передаче информации, чем для обеспечения долговременной сохранности информации. Попытки решить эту проблему пока что не дали каких-то реальных результатов.» (п.51 стр.25-26)

  http://www.uncitral.org/pdf/english/texts/electcom/08-55698_Ebook.pdf

Еврокомиссия провела онлайн-консультации с общественностью об ЭП



Electronic identification, authentication and signatures

1. Respondent information

Are you replying:	On behalf of an organisation
Please provide the name of your Organisation	
UNIZETO TECHNOLOGIES SA	
Please provide if applicable, your interest Representative Register ID number	
KRS No (National Court Register No): 0000233499; Statistical Registration No (REGON): 810404880; VAT Registration No (NIP): 852-000-64-44	
Please indicate which type of stakeholder you are	Large private company
Please provide your Name and Surname	
Alla Stoliarowa-Myc	
Please provide your email address	
alla.stoliarowa@unizeto.pl	
Your country of residence	Poland

2. General expectations regarding EU legislation on e-signatures, e-identification and e-authentication

Question 1: Do you / Does your organisation use e-signatures, e-identification and e-authentication?	yes
If yes, what are your specific needs?	Secure transactions Unambiguous identification of contract partners Integrity of electronic documents Legal effect Legal effect, contract signatures in particular User convenience Others
Please comment why	
The availability of more services provided electronically, especially by public administration. The possibility to use e-signatures and e-authentication in online systems available in other countries.	
If yes, how frequently do you carry out secure transactions?	Daily
Question 2: For what online transactions do you consider electronic identification,	eGovernment services Electronic Public Procurement eCommerce transactions eBusiness transactions Online banking and financial transactions

- Опрос общественного мнения по поводу электронных подписей и электронной идентификации личности (29 вопросов) проходил в феврале -апреле 2011 г.
- Получено 434 отзыва, из них 417 – через сайт, и ещё 17 – по электронной почте
- 45% респондентов считают вопрос долговременного хранения важным

Германия: сокращение использования УКЭП, 2011 год

- Закрытие системы ELENA для сдачи работодателями электронной отчетности о выплачиваемой сотрудникам зарплате
- С 1 июля 2011 года электронные счета и счета-фактуры не обязательно подписывать квалифицированной электронной подписью
- Скандал вокруг Технического руководства 03125 «Сохранение доказательной силы документов, подписанных с использованием криптографических методов» (TR-ESOR)

Методика организации долговременного хранения

- Первый метод: Организация может предпочесть сохранять возможность перепроверять цифровые подписи
- Второй метод: Регулярное переподписание документов уполномоченным лицом или органом
- Третий метод: Сохраняется документация, подтверждающая подлинность документа, собранная во время или вскоре после подписания документа

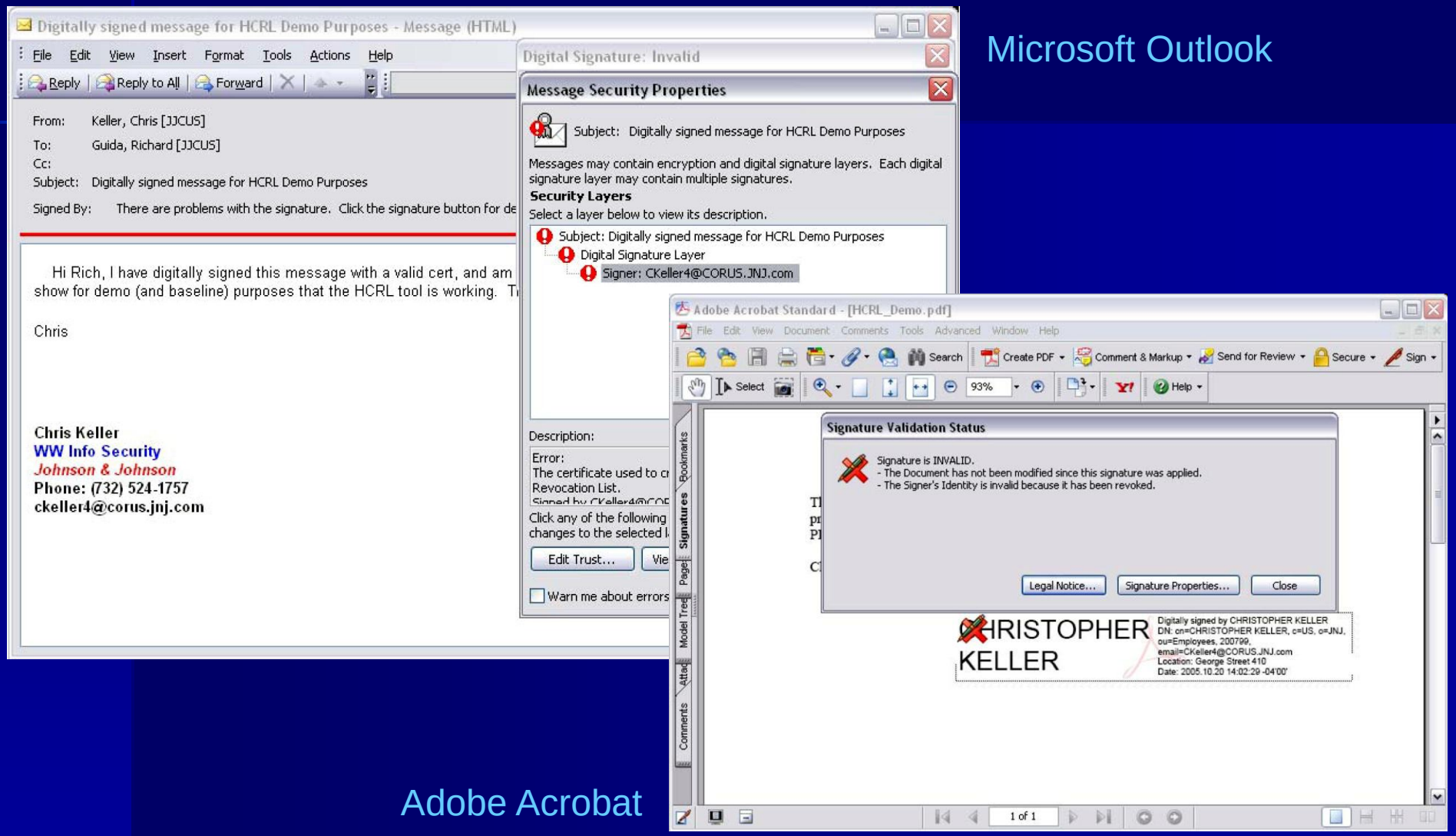
Какие проблемы могут возникнуть

- Возможность взлома алгоритма цифровой подписи через 10-15 лет и компрометации ЭЦП
- Необходимость организовать долговременное хранения не только самого документа, но и всех поддерживающих его документов на протяжении всего срока хранения
- Необходимость сохранения, причем в рабочем состоянии всех технических и программных средств, использовавшихся при подписании документа

Защита на случай компрометации ЭЦП в будущем

- Документирование факта успешной проверки подписи в период времени, когда она заведомо не была взломана или скомпрометирована
- Предоставление доказательств, что документ постоянно хранился в защищённой системе, гарантирующей его целостность и аутентичность
- Ведение учёта документов, подписанных ЭЦП. На основании этих данных в ряде случаев можно будет доказать или опровергнуть подлинность документов

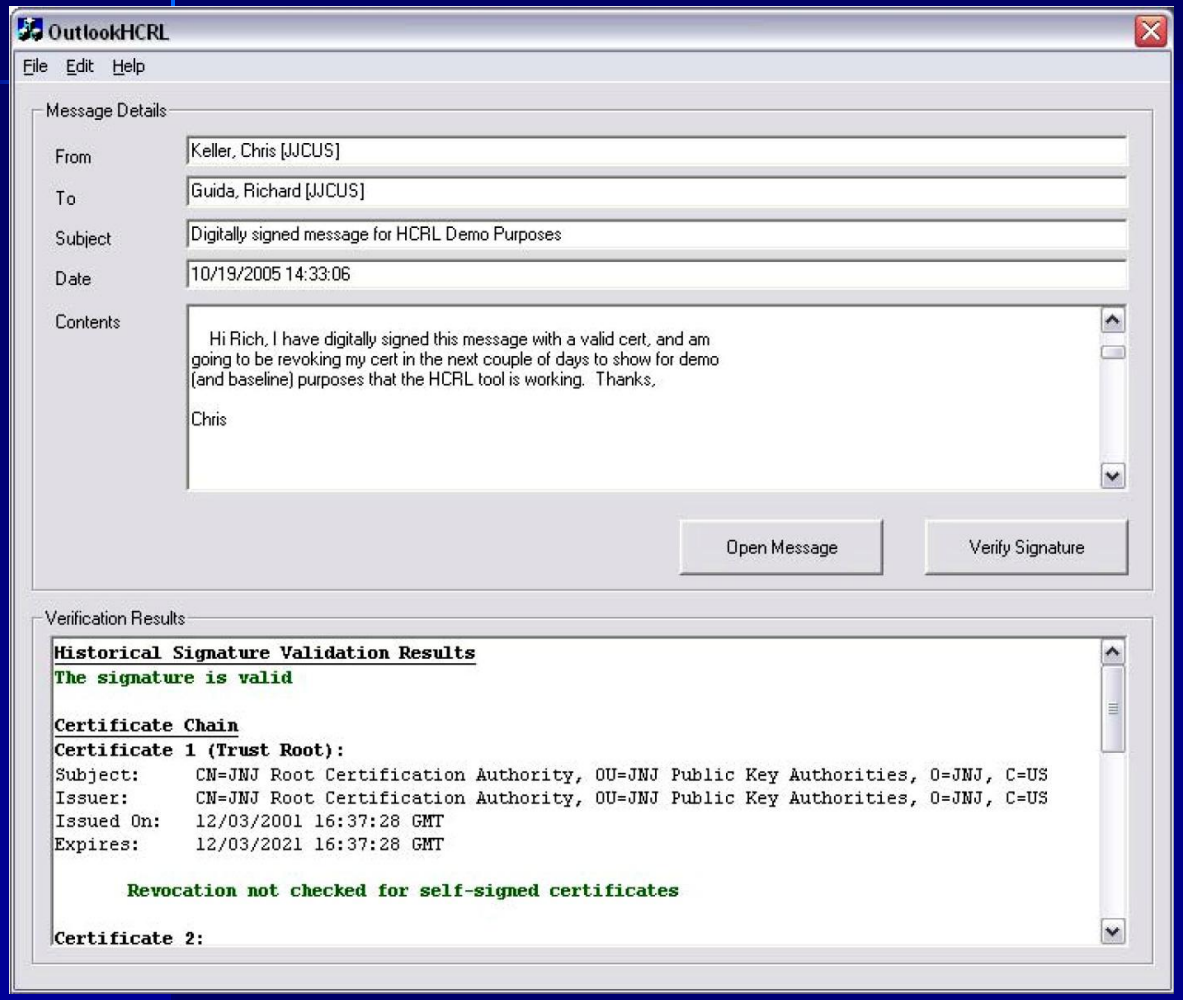
По истечении срока действия сертификатов, «обычные» приложения ведут себя вот так:



Microsoft Outlook

Adobe Acrobat

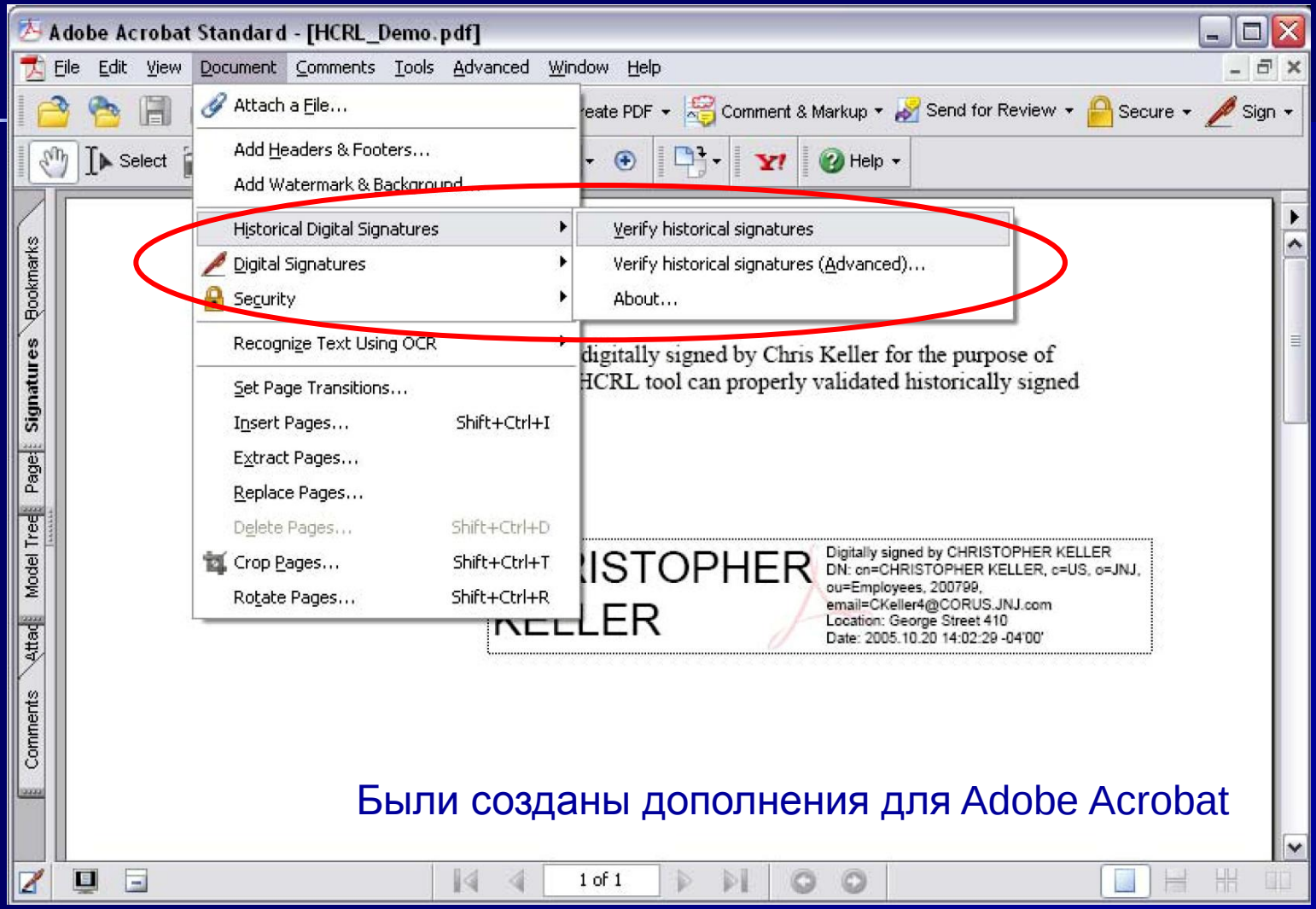
Для проверки «исторических» подписей приходится делать заказные доработки



Microsoft Outlook

- Фирма «Johnson & Johnson» создала собственную систему проверки исторических подписей (Outlook, Acrobat)
- Для этого создано хранилище CRL-списков и сертификатов
- Решение прошло сертификацию у контролирующего органа (FDA)

Для проверки «исторических» подписей приходится делать заказные доработки



Были созданы дополнения для Adobe Acrobat

Опыт фирмы «Johnson & Johnson» (свыше 75 тыс. действующих ЭЦП)

- Использованы два решения:
  - Создана БД списков отозванных сертификатов и разработаны средства проверки ЭЦП, созданных в недавнем прошлом
  - Создан долговременный архив и служба «электронного нотариата» для сохранения объектов PKI даже после устаревания криптоалгоритмов
- «В подобных возможностях уже сегодня остро нуждаются многие компании – хотя пока еще не осознают этого»

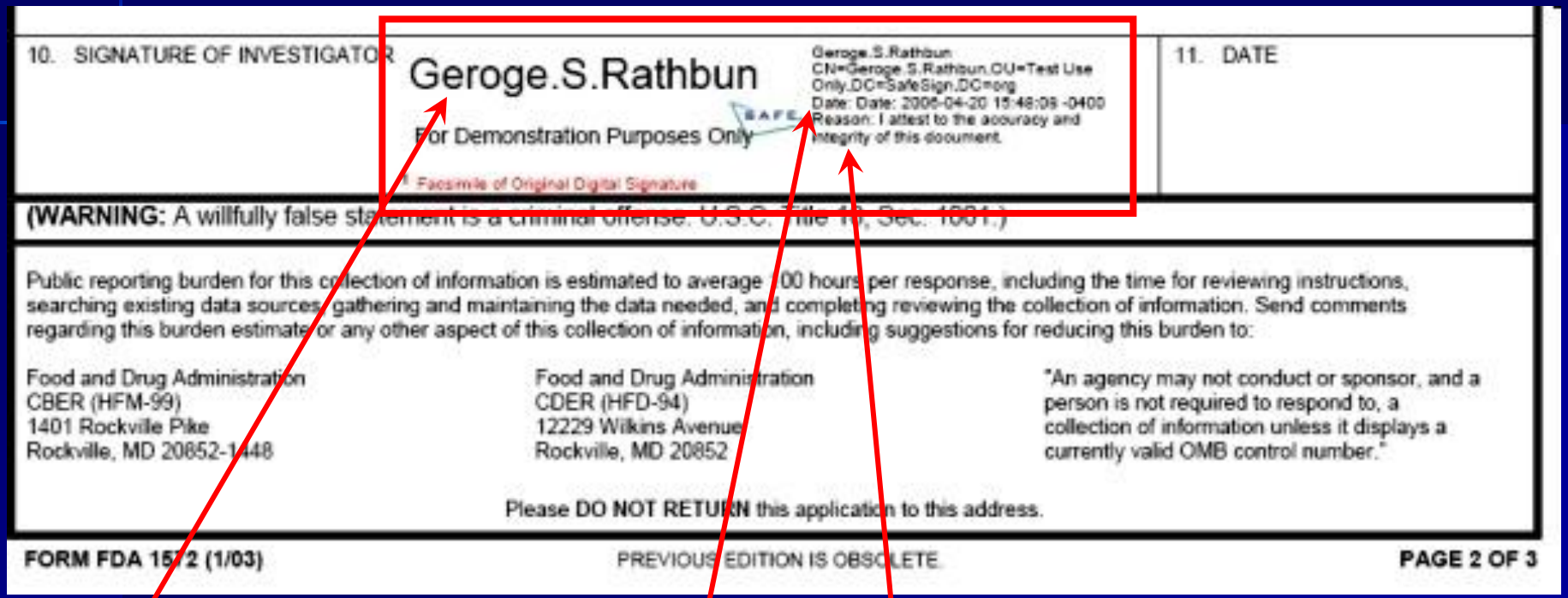
Rich Guida, Peter Hesse, Carl Wallace
«Digital Signatures Over Time» (презентация на конференции RSA-2007),
http://geminisecurity.com/wp-content/uploads//ASEC-302%20Guida,Hesse,Wallace.pdf

Рекомендации FDA - Агентства по контролю за пищевыми продуктами и лекарственными препаратами (США)

- Формы FDA (например, 356h) и документы должны быть подписаны. FDA допускает следующие методы подписания:
  - Отсканированные подписи
  - Электронные цифровые подписи (рекомендуется использовать средства подписания Adobe Acrobat)
  - Расшифрованные ЭЦП (Flattened digital signatures)
- Агентство не проверяет электронные/цифровые подписи, за исключением случаев целевых проверок, охватывающих подачу документов

  http://www.fda.gov/cder/regulatory/ersr/Gateway-and-Validation-Duggan.pdf
  октябрь 2008 года

Пример допускаемой FDA «расшифрованной ЭЦП»



10. SIGNATURE OF INVESTIGATOR

Geroge.S.Rathbun

For Demonstration Purposes Only

Facsimile of Original Digital Signature

Geroge.S.Rathbun
CN=Geroge.S.Rathbun,OU=Test Use Only,DC=SafeSign,DC=org
Date: Date: 2006-04-20 15:46:06 -0400
Reason: I attest to the accuracy and integrity of this document.

11. DATE

(WARNING: A willfully false statement is a criminal offense. U.S.C. Title 18, Sec. 1001.)

Public reporting burden for this collection of information is estimated to average 100 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to:

Food and Drug Administration
CBER (HFM-99)
1401 Rockville Pike
Rockville, MD 20852-1448

Food and Drug Administration
CDER (HFD-94)
12229 Wilkins Avenue
Rockville, MD 20852

"An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid OMB control number."

Please DO NOT RETURN this application to this address.

FORM FDA 1572 (1/03) PREVIOUS EDITION IS OBSOLETE PAGE 2 OF 3

- «Расшифрованная» ЭЦП должна содержать
  1. Имя подписанта
  2. Дату и время подписания
  3. Намерение

http://www.fda.gov/esg/userguide/webhelp/Digital_Signatures.htm

Интересный подход к архивации документов с ЭЦП, 2009 г.

1.5.5. ЭЦП и архивные документы

Документы, зарегистрированные в системе **ЕВФРАТ**, после выведения из активного документооборота могут быть списаны в электронный архив. Для этих целей служит специальный модуль системы **ЕВФРАТ** — программа **Архивариус**. Архивные документы не подлежат никаким изменениям. Поэтому все ЭЦП, которыми подписан тот или иной электронный документ, уничтожаются при списании документа в электронный архив.

- http://www.evfrat.ru/file/docs/evfrat_ecp.pdf

ЭЦП - полезное средство для оперативной работы, но:

- Создает массу проблем при необходимости долговременного хранения документов
- Существующая законодательно-нормативная база не содержит норм, допускающих переподписание документов
- Существующая законодательно-нормативная база не содержит норм, необходимых для работы электронных архивов
- Проблема долговременного хранения документов, подписанных ЭЦП даже более актуальна, чем проблема интероперабельности, и ею нужно заниматься


Вопросы?