XII международная конференция по проблематике инфраструктуры открытых ключей и электронной подписи «PKI-Forum Россия 2014»

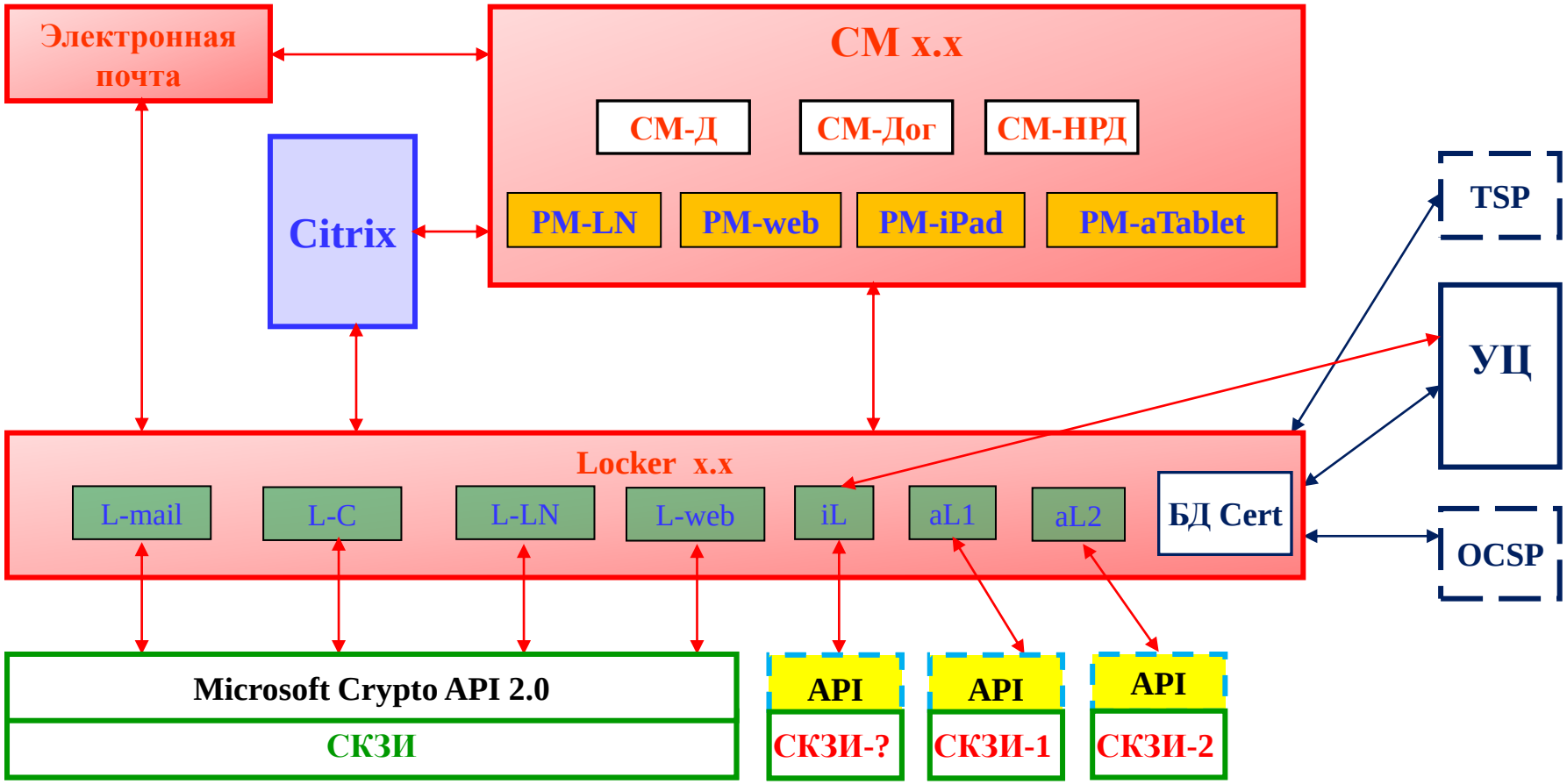
16 – 18 сентября 2014 г.

Что ждут пользователи и разработчики СЭД от разработчиков СКЗИ, удостоверяющих центров и регуляторов

Горностаев Владимир
Директор Центра компетенции по защите информации

Компания «ИнтерТраст»
+7 (495) 956-79-28, sales@inttrust.ru
http://www.intertrust.ru

Создание доверия в СЭД



Признание квалифицированной электронной подписи

Ст. 11 63-ФЗ «Об электронной подписи»

Квалифицированная ЭП признается действительной при одновременном соблюдении условий:

1) квалифицированный сертификат создан и выдан аккредитованным УЦ, аккредитация которого действительна на день выдачи указанного сертификата;

2) **квалифицированный сертификат действителен* на**

а). **момент подписания** ЭД (при наличии **достоверной информации о моменте подписания** ЭД) или

б). **день проверки** действительности указанного сертификата, если момент подписания ЭД не определен;

3) имеется положительный результат проверки принадлежности владельцу квалифицированного сертификата квалифицированной ЭП, с помощью которой подписан ЭД, и подтверждено отсутствие изменений, внесенных в этот документ после его подписания. При этом проверка осуществляется с использованием средств ЭП, получивших подтверждение соответствия требованиям, установленным в соответствии с настоящим ФЗ, и с использованием квалифицированного сертификата лица, подписавшего ЭД;

4) квалифицированная ЭП используется с учетом ограничений, содержащихся в квалифицированном сертификате лица, подписывающего ЭД (если такие ограничения установлены).

*** Не прекратил свое действие?????**

Правила использования квалифицированной электронной подписи

Утверждены ПП от 9 февраля 2012 г. № 111

5. Подписанный электронной подписью ЭД **должен иметь метку времени – достоверную информацию о моменте его подписания**, которая присоединена к указанному электронному документу или иным образом связана с ним.

9. В ИС участников межведомственного электронного взаимодействия обработке подлежат ЭД, которые подписаны ЭП, **признанной действительной.**

ЭП признается действительной при соблюдении условий п.1, 3 и 4 ст. 11 63-ФЗ, а также **при условии, что сертификат *не прекратил свое действие* и не был аннулирован на момент подписания электронного документа.***

*

п.6 ст. 14 63-ФЗ

6. Сертификат ключа проверки ЭП прекращает свое действие:

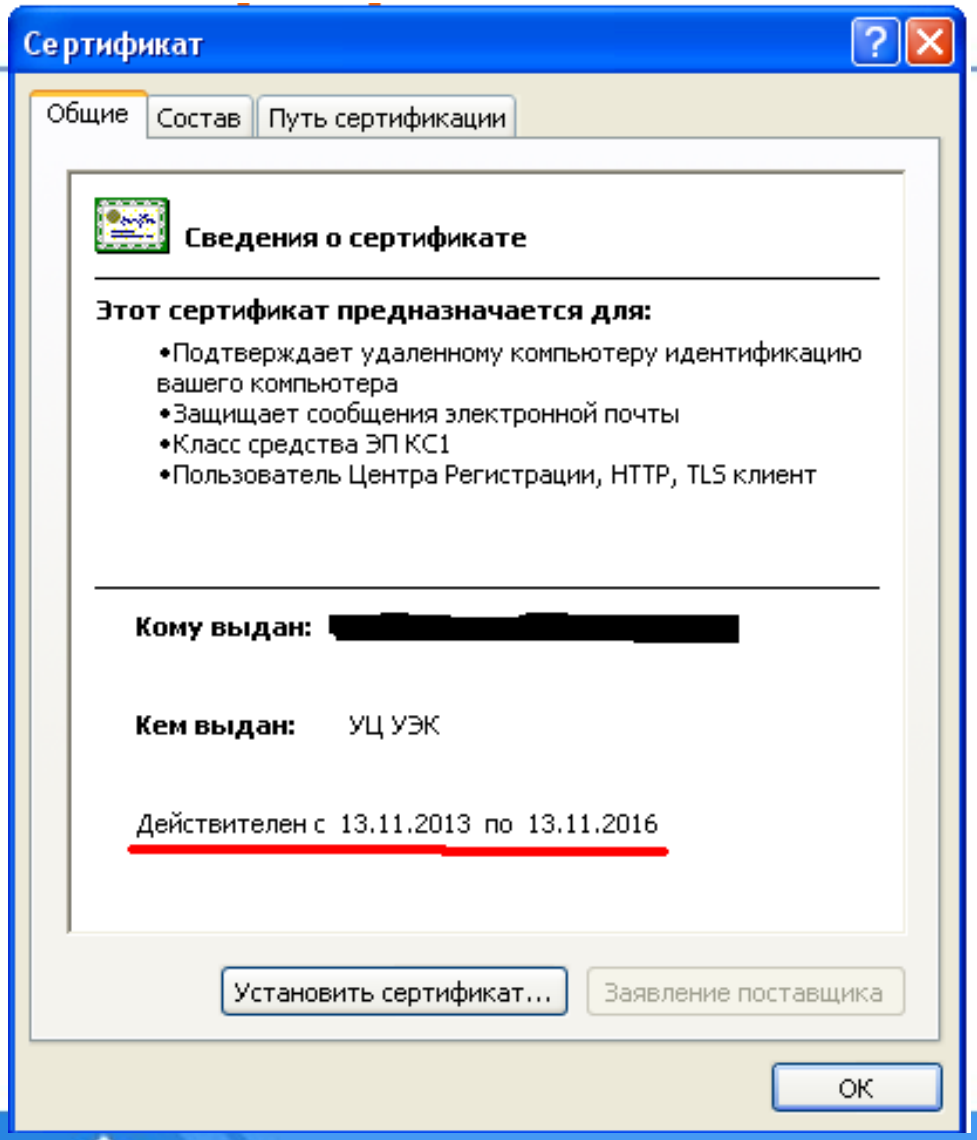
1) в связи с истечением установленного срока его действия;

2) на основании заявления владельца сертификата ключа проверки ЭП, подаваемого в форме документа на бумажном носителе или в форме ЭД;

3) в случае прекращения деятельности УЦ без перехода его функций другим лицам;

4) в иных случаях, установленных настоящим ФЗ, другими ФЗ, принимаемыми в соответствии с ними НПА или соглашением между УЦ и владельцем сертификата ключа проверки ЭП.

Действительный сертификат?



Действительный сертификат на момент проверки

Сертификат признается действительным на момент проверки, если:

- дата и время проверки находятся в интервале времени действия сертификата;
- проверяемый сертификат является **доверенным (подлинным);**
- сертификат отсутствует в актуальном списке отозванных сертификатов.

Сертификат признается **доверенным (подлинным)** на момент проверки, если:

- возможно построить цепочку сертификатов до доверенного УЦ;
- для проверяемого и каждого сертификата в цепочке успешно выполнена проверка электронной подписи уполномоченного лица УЦ (электронная подпись верна);
- дата и время проверки находятся в интервале времени действия всей цепочки сертификатов до доверенного УЦ (включая).

Актуальный список отозванных сертификатов является актуальным на момент проверки, если:

- дата и время проверки находятся в интервале времени действия СОС;
- для СОС успешно выполнена проверка электронной подписи уполномоченного лица УЦ (электронная подпись верна).

Действительный сертификат на момент подписания

Сертификат признается действительным на момент подписания, если в момент подписания:

- дата и время находились в интервале времени действия сертификата;
- проверяемый сертификат был **доверенным (подлинным);**
- сертификат отсутствовал в актуальном на момент подписания списке отозванных сертификатов.

Сертификат признается **доверенным (подлинным)** на момент подписания, если в момент подписания:

- было возможно построить цепочку сертификатов до доверенного УЦ;
- для проверяемого и каждого сертификата в цепочке успешно выполнена проверка электронной подписи уполномоченного лица УЦ (электронная подпись верна);
- дата и время находились в интервале времени действия всей цепочки сертификатов до доверенного УЦ (включая).

Актуальный список отозванных сертификатов является актуальным на момент подписания, если в момент подписания:

- дата и время находились в интервале времени действия СОС;
- для СОС успешно выполнена проверка электронной подписи уполномоченного лица УЦ (электронная подпись верна).

Усовершенствованная ЭП

XML Advanced Electronic Signatures (XAdES)
http://www.w3.org/TR/XAdES/

CMS Advanced Electronic Signature (CAdES), RFC 5126

PDF Advanced Electronic Signature (PAdES), ETSI TS 102 778

XML Advanced Electronic Signature

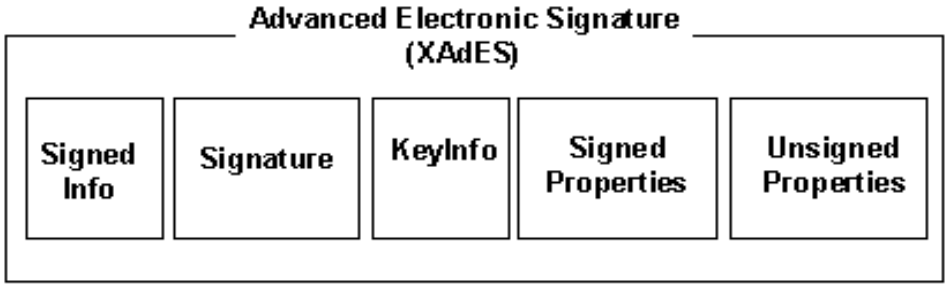


Figure 1. Illustration of a XAdES

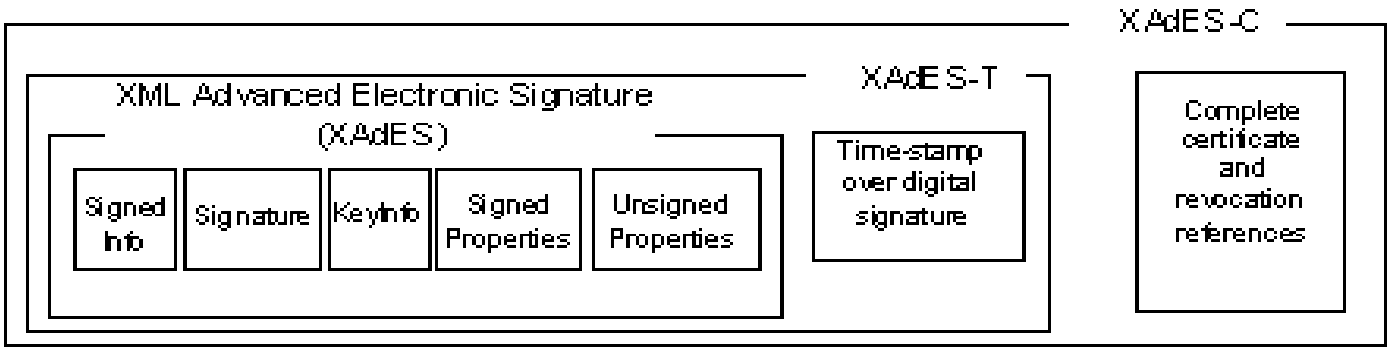


Figure 2. Illustration of a XAdES, XAdES-T and XAdES-C

XML Advanced Electronic Signature

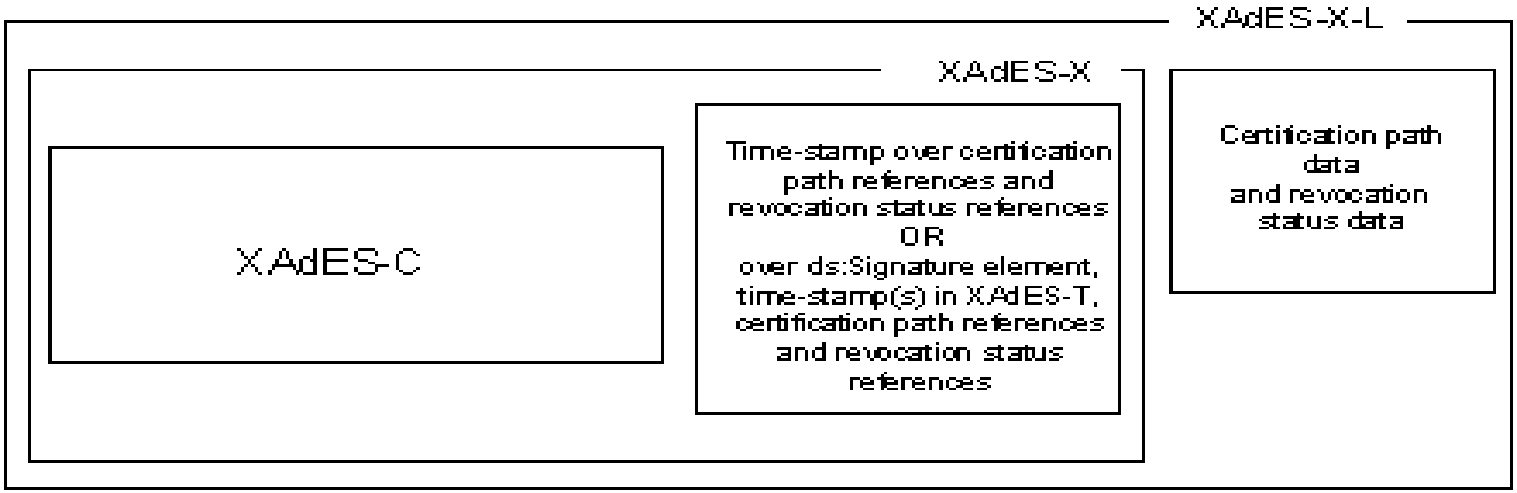


Figure 3. Illustration of XAdES-X andXAdES-X-L

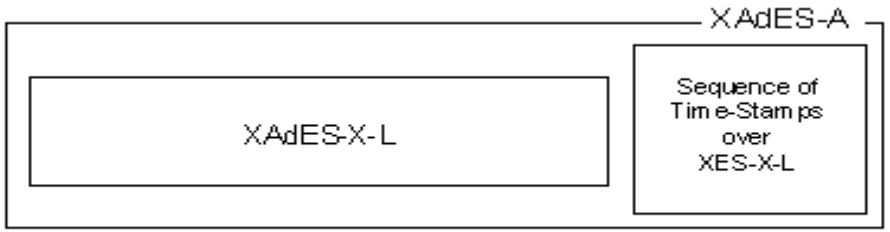
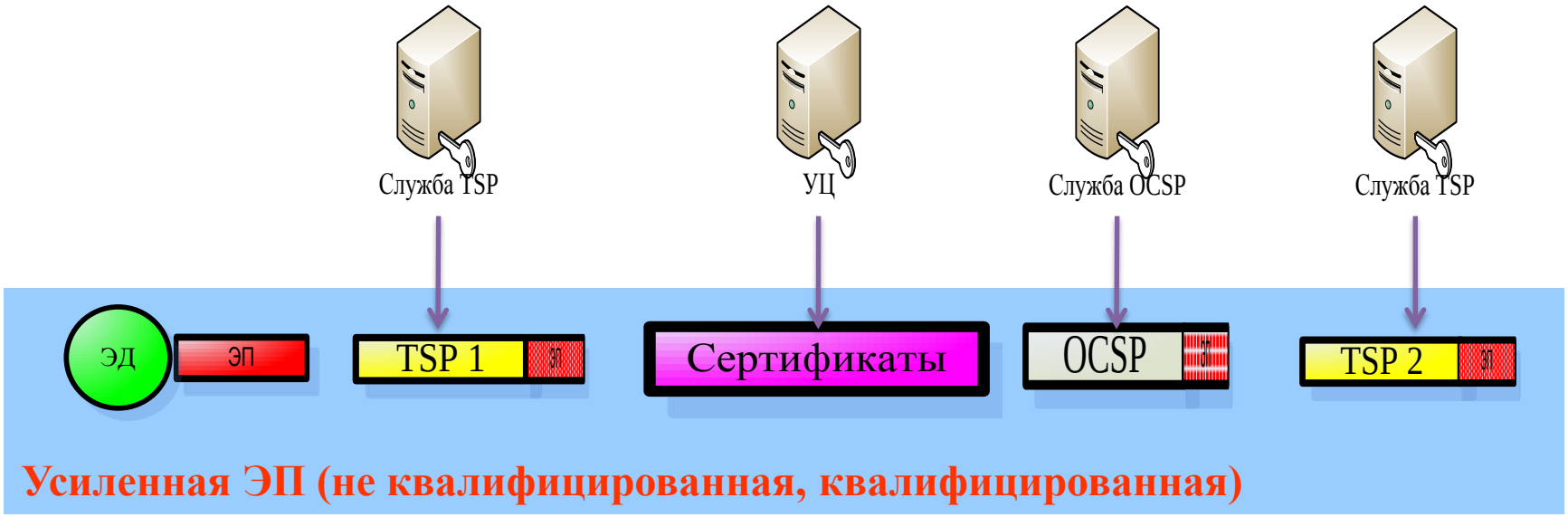


Figure 4. Illustration of XAdES-A

Advanced Electronic Signature



Усиленная ЭП (не квалифицированная, квалифицированная)

Начиналось ….

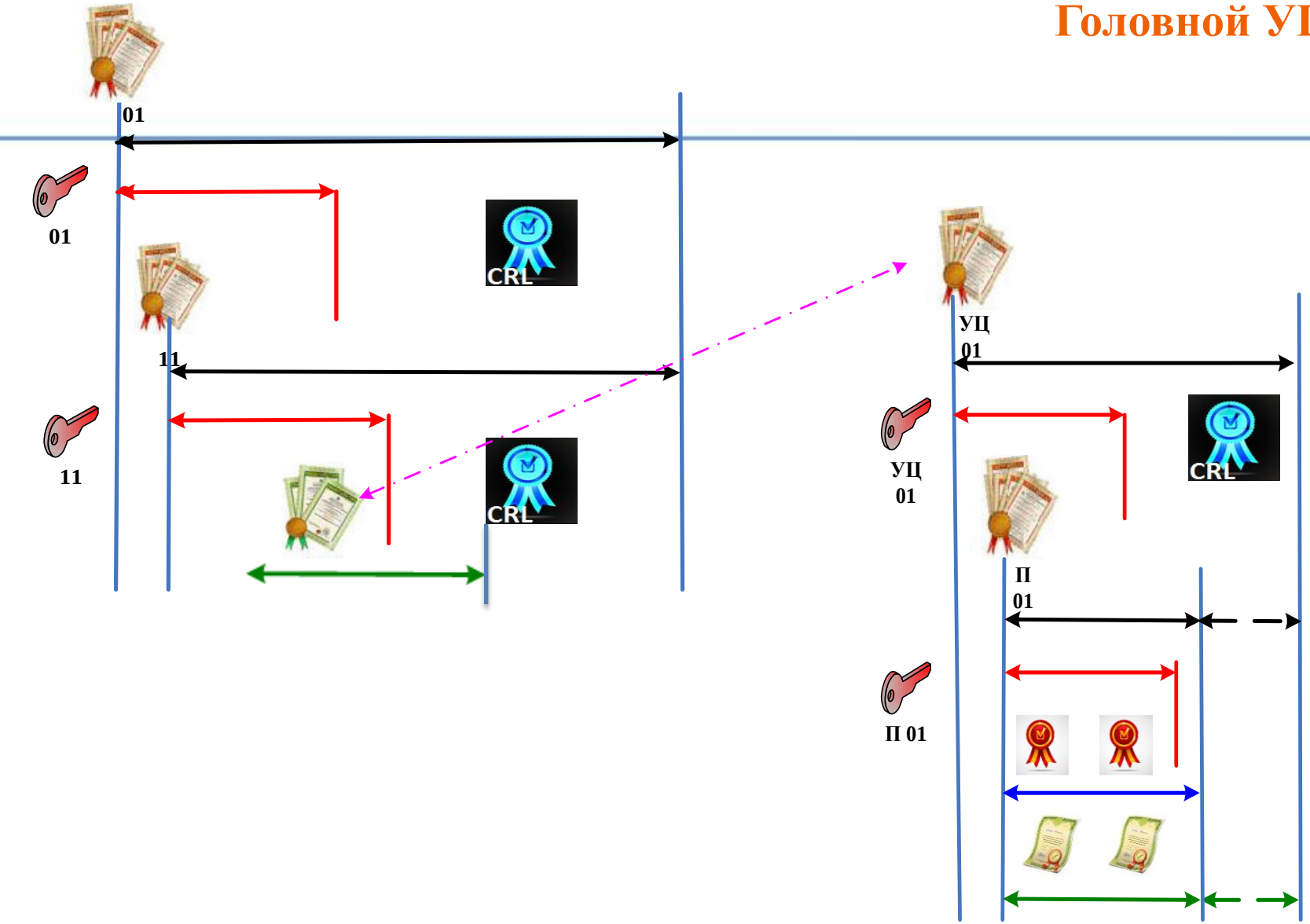
12.08.2014 г. Прошу прокомментировать ситуацию.

На Портале уполномоченного федерального органа в области использования электронной подписи (http://e-trust.gosuslugi.ru/) в реестре сертификаты УФО выводится следующая информация.

Кому выдан «ЗАО «Национальный удостоверяющий центр»
Кем выдан УЦ 1 ИС ГУЦ
Серийный номер: 15087D84000000000009
Действует с : 20.07.2012
Действует до: **20.07.2013**
Статус: **Действует**

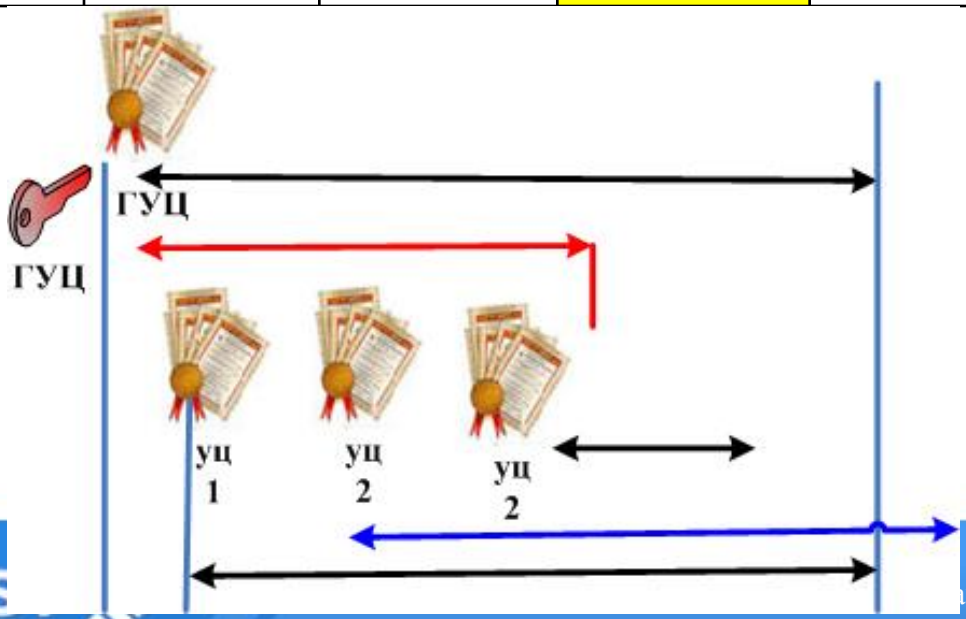
Кому выдан «ООО «КРИПТО-ПРО»
Кем выдан УЦ 1 ИС ГУЦ
Серийный номер: 6B69507000000000022
Действует с : 09.08.2012
Действует до: **09.08.2013**
Статус: **Действует**

Головной УЦ



Анализ «Доверия»

УЦ (поставщик/субъект), самоподписанный/ /субъект	Сроки действия сертификата ключа проверки ЭП			Серийный номер
	ключа ЭП			
	с	по	по	
ГУЦ	20.07.2012		17.07.2027	34 68 1e 40 cb 41 ef 33 a9 a0 b7 c8 76 92 9a 29
УЦ 1 ИС ГУЦ-1	20.07.2012		17.07.2027	00 d5 c9 e8 e3 00 00 00 00 00 0c
УЦ 2 ИС ГУЦ-1	28.12.2012		25.12.2027	00 eb 32 f7 ff 00 00 00 00 00 10
УЦ 2 ИС ГУЦ-2	23.07.2013		22.07.2017	3c 82 25 19 00 00 00 00 00 18



Анализ «Доверия»

Аккредитация УЦ с 7.08.2012 г. по 6.08.2017 г.

ГУЦ	**20.07.2012**		**17.07.2027**
УЦ 1 ИС ГУЦ-1	**20.07.2012**		**17.07.2027**
УЦ 2 ИС ГУЦ-1	**28.12.2012**		**25.12.2027**
УЦ 2 ИС ГУЦ-2	**23.07.2013**		**22.07.2017**
http://q.cryptopro.ru/			Нельзя выпуст
УЦ 2 "КРИПТО-ПРО"	***06.08.2013***	***06.02.2015***	***06.02.2015***
УЦ 1 "КРИПТО-ПРО"	***09.08.2012***	***09.08.2013***	***09.08.2013***
УЦ "КРИПТО-ПРО" 1	**09.08.2012**		**09.08.2027**
Ген. директор ФИО	11.	**Сертификат отозван**	11.10.2014
Зам.Кд. ФИО	06.12.2012		06.12.2013
			Нел
УЦ 2 "КРИПТО-ПРО"	***13.11.2013***	***13.05.2015***	***13.05.2015***
УЦ 1 "КРИПТО-ПРО"	***13.11.2013***	***13.05.2015***	***13.05.2015***
УЦ "КРИПТО-ПРО" 2	**08.11.2013**		**07.11.2028**

Подлинность сертификата НЕ ПОДТВЕРЖДЕНА

Статус сертификата, использованного для подтверждения подлинности ЭП: **Один из сертификатов цепочки аннулирован**

Статусы использованных сертификатов

Владелец : *Чернова ...., Генеральный директор, "ул. Сущевский вал, д. 18", ООО «КРИПТО-ПРО», info@cryptopro.ru,*

Издатель: *"ООО ""КРИПТО-ПРО""", г. Москва, RU, qca@cryptopro.ru, "ул. Сущёвский вал, д.16, стр.5",*

Действителен: **с 2013.10.11 по 2014.10.11**

Статус: ***Сертификат был отозван***

Уполномоченное лицо УЦ: *ООО «КРИПТО-ПРО», г.Москва, RU, qca@cryptopro.ru, "ул. Сущёвский вал, д.16,*

Издатель: *УЦ 2 ИС ГУЦ, RU, 77 г.Москва, Минкомсвязь России, 125375 г. Москва ул. Тверская д.7, dit@minsvyaz.ru,*

Действителен: **с 2013.08.06 по 2015.02.06**

Уполномоченное лицо УЦ: *УЦ 2 ИС ГУЦ, RU, 77 г.Москва, Минкомсвязь России, 125375 г. Москва ул. Тверская д.7, dit@minsvyaz.ru,*

Издатель: *ГУЦ, Минкомсвязь России, "125375 г. Москва, ул. Тверская, д. 7", dit@minsvyaz.ru*

Действителен: *с* **2013.07.23 по 2017.07.22**

Уполномоченное лицо УЦ: *ГУЦ, Минкомсвязь России, "125375 г. Москва, ул. Тверская, д. 7, dit@minsvyaz.ru*

Издатель: *ГУЦ, Минкомсвязь России, "125375 г. Москва, ул. Тверская, д. 7", dit@minsvyaz.ru*

Действителен: **с 2012.07.20 по 2027.07.17**

Анализ «Доверия»

Аккредитация УЦ с 7.08.2012 г. по 6.08.2017 г.

ГУЦ	20.07.2012		**17.07.2027**
УЦ 1 ИС ГУЦ-1	20.07.2012		**17.07.2027**
УЦ 2 ИС ГУЦ-1	28.12.2012		**25.12.2027**
УЦ 2 ИС ГУЦ-2	23.07.2013		**22.07.2017**
Адрес ???			**Нельзя выпус**
УЦ 2 УЭК	***19.11.2013***	***19.05.2015***	***19.05.2015***
УЦ 1 УЭК	***20.11.2012***	***20.11.2013***	***20.11.2013***
УЦ УЭК 1	**16.11.2012**		**16.11.2027**
УЭК ФИО	**13.11.2013**	**13.11.2016**	**13.11.2016**
			Нельзя выпу
УЦ 2 УЭК	***03.02.2014***	***03.02.2018***	***22.07.2017***
УЦ 1 УЭК	***03.02.2014***	***03.02.2018***	***04.12.2017***
УЦ УЭК 2	**30.01.2014**		**29.01.2029**

Подлинность сертификата ПОДТВЕРЖДЕНА

Статус сертификата, использованного для подтверждения подлинности ЭП: ДЕЙСТВИТЕЛЕН, сертификат выдан аккредитованным удостоверяющим центром

Статусы использованных сертификатов

Владелец : Горностаев, …….

Издатель: УЦ УЭК, "ООО ""КРИПТО-ПРО""", Москва, uecard@cryptopro.ru, "ул. Сущёвский вал, д. 16, стр. 5",

Действителен: с 2013.11.13 **по 2016.11.13**

Уполномоченное лицо УЦ: УЦ УЭК, "ООО ""КРИПТО-ПРО""", Москва, г. Москва, RU, uecard@cryptopro.ru, "ул. Сущёвский вал, д. 16, стр. 5",

Издатель: УЦ 2 ИС ГУЦ, RU, 77 Москва, Минкомсвязь России, 125375 г. Москва ул. Тверская д.7, dit@minsvyaz.ru, 1047702026701, 007710474375

Действителен: с 2013.11.19 **по 2015.05.19**

Уполномоченное лицо УЦ: УЦ 2 ИС ГУЦ, RU, 77 г. Москва, Минкомсвязь России, 125375 г. Москва ул. Тверская д.7, dit@minsvyaz.ru, 1047702026701, 007710474375

Издатель: ГУЦ, Минкомсвязь России, "125375 г. Москва, ул. Тверская, д. 7", Москва, 77 г. Москва, RU, dit@minsvyaz.ru

Действителен: с 2013.07.23 **по 2017.07.22**

Уполномоченное лицо УЦ: ГУЦ, Минкомсвязь России, "125375 г. Москва, ул. Тверская, д. 7", Москва, 77 г. Москва, RU, dit@minsvyaz.ru

Издатель: ГУЦ, Минкомсвязь России, "125375 г. Москва, ул. Тверская, д. 7", Москва, 77 г. Москва, RU, dit@minsvyaz.ru

Действителен: с 2012.07.20 **по 2027.07.17**

Анализ «Доверия»

Аккредитация УЦ с 30.06.2012 г. по 29.06.2017 г.

ГУЦ	**20.07.2012**		**17.07.2027**
УЦ 1 ИС ГУЦ-1	**20.07.2012**		**17.07.2027**
УЦ 2 ИС ГУЦ-1	**28.12.2012**		**25.12.2027**
УЦ 2 ИС ГУЦ-2	**23.07.2013**		**22.07.2017**
http://www.nucrf.ru	**Два одинаковых одним УЦ**		
УЦ 2 НУЦ	***23.07.2013***	***23.01.2015***	***23.01.2015***
УЦ 2 НУЦ	***19.07.2013***	***19.01.2015***	***19.01.2015***
УЦ 1 НУЦ	***20.07.2012***	***20.07.2013***	***20.07.2013***
УЦ НУЦ 1	**05.07.2012**		**05.07.2015**
УЦ 2 НУЦ	***02.07.2014***	***02.07.2018***	***22.07.2017***
УЦ 1 НУЦ	***02.07.2014***	***02.07.2018***	***04.12.2017***
УЦ НУЦ 2	**27.06.2014**		**26.06.2017**

Подлинность сертификата НЕ ПОДТВЕРЖДЕНА
Статус сертификата, использованного для подтверждения подлинности ЭП: Не удалось проверить на аннулированность один или несколько сертификатов цепочки ***(11.09.2014 18.14)***

Статусы использованных сертификатов
Владелец : *"ЗАО ""Национальный удостоверяющий центр""", УЦ, Москва, Москва, RU, ул.Авиамоторная д.8А стр.5, 007722766598,*
Издатель: *УЦ 2 ИС ГУЦ, Минкомсвязь России, 125375 г. Москва ул. Тверская д.7, dit@minsvyaz.ru,*
Действителен: **с 2013.07.19 по 2015.01.19**
Статус: Функция отзыва не смогла произвести проверку отзыва для сертификата. Невозможно проверить функцию отзыва, т.к. сервер отзыва сертификатов недоступен .

Уполномоченное лицо УЦ: *УЦ 2 ИС ГУЦ, RU, 77 г.Москва, Москва, Минкомсвязь России, 125375 г. Москва ул. Тверская д.7, dit@minsvyaz.ru, 1047702026701, 007710474375*
Издатель: *Головной удостоверяющий центр, 007710474375, 1047702026701, Минкомсвязь России, "125375 г. Москва, ул. Тверская, д. 7", dit@minsvyaz.ru*
Действителен: ***с 2012.12.28 по 2027.12.25***

Уполномоченное лицо УЦ: *Головной удостоверяющий центр, 007710474375, 1047702026701, Минкомсвязь России, "125375 г. Москва, ул. Тверская, д. 7", Москва, 77 г. Москва, RU, dit@minsvyaz.ru*
Издатель: *Головной удостоверяющий центр, 007710474375, 1047702026701, Минкомсвязь России, "125375 г. Москва, ул. Тверская, д. 7", Москва, 77 г. Москва, RU, dit@minsvyaz.ru*
Действителен: **с 2012.07.20 по 2027.07.17**

Анализ «Доверия»

Аккредитация УЦ с 7.08.2012 г. по 6.08.2017 г.

ГУЦ	**20.07.2012**		**17.07.2027**	**34 68 1e 40 cb 41 ef 33 a9 a0 b7 c8 76 92 9a 29**
УЦ 1 ИС ГУЦ-1	**20.07.2012**		**17.07.2027**	**00 d5 c9 e8 e3 00 00 00 00 00 0c**
УЦ 2 ИС ГУЦ-1	**28.12.2012**		**25.12.2027**	**00 eb 32 f7 ff 00 00 00 00 00 10**
УЦ 2 ИС ГУЦ-2	**23.07.2013**		**22.07.2017**	**3c 82 25 19 00 00 00 00 00 18**
http://rostelecom.ru/ нет информации об УЦ				**Нельзя выпустить сертификат**
УЦ 2 RTK	***05.08.2013***	***05.02.2015***	***05.02.2015***	***44 1f e2 e6 00 00 00 00 00 43***
УЦ 1 RTK	***08.08.2012***	***08.08.2013***	***08.08.2013***	***65 e8 7f d2 00 00 00 00 00 1d***
УЦ RTK 1				
				Нельзя выпустить сертификат
УЦ 2 RTK	***21.11.2013***	***21.05.2015***	***21.05.2015***	***71 b2 b7 67 00 00 00 00 01 61***
УЦ 1 RTK	***21.11.2013***	***21.05.2015***	***21.05.2015***	***6b 58 54 0e 00 00 00 00 02 28***
УЦ RTK 2	**21.11.2013**		**21.11.2018**	**65 82 52 0b f2 24 6f 96 4e 1b 54 d6 49 db fc 6c**
УЦ RTK 2 ФИО	**10.07.2014**	**10.07.2015**	**10.07.2015**	72 81 03 d6 00 02 00 00 58 02

Анализ «Доверия»

Аккредитация УЦ с 8 августа 2012 г. по 7 августа 2017 г.

ГУЦ	20.07.2012		17.07.2027	34 68 1e 40 cb 41 ef 33 a9 a0 b7 c8 76 92 9a 29
УЦ 1 ИС ГУЦ-1	20.07.2012		17.07.2027	00 d5 c9 e8 e3 00 00 00 00 00 0c
УЦ 2 ИС ГУЦ-1	28.12.2012		25.12.2027	00 eb 32 f7 ff 00 00 00 00 00 10
УЦ 2 ИС ГУЦ-2	23.07.2013		22.07.2017	3c 82 25 19 00 00 00 00 00 18
http://iitrust.ru				Нельзя выпустить сертификат
УЦ 2 ИИТ (К3)	*14.08.2013*	*24.08.2013*	*14.02.2015*	*72 64 0d 49 00 00 00 00 00 7b*
УЦ 1 ИИТ (К3)	*27.08.2012*	*27.08.2013*	*27.08.2013*	*47 ed a0 08 00 00 00 00 00 32*
УЦ ИИТ (К3) 1	24.08.2012	24.08.2013	24.08.2018	01 cd 81 cc 7b ae 14 90 00 00 00 00 00 06 00 02
				Нельзя выпустить сертификат
УЦ 2 ИИТ (К3)	*08.08.2013*	*08.08.2015*	*08.08.2015*	*54 05 45 2b 00 00 00 00 00 56*
УЦ 1 ИИТ (К3)	*08.08.2013*	*08.08.2015*	*08.08.2015*	*4d a3 37 3c 00 00 00 00 01 8d*
УЦ ИИТ (К3) 2	29.08.2013		29.08.2019	01 ce 8c 7e a0 10 8c 10 00 00 00 1b 00 06 00 02
				Нельзя выпустить сертификат
УЦ 2 ИИТ (К3)	*18.07.2014*	*18.07.2018*	*22.07.2017*	*3f 83 0f 5c 00 00 00 00 02 aa*
УЦ 1 ИИТ (К3)	*21.07.2014*	*21.07.2018*	*04.12.2017*	*61 02 cc 2f 00 01 00 00 02 ef*
УЦ ИИТ (К3) 3	18.07.2014		18.07.2020	01 cf a2 68 e4 66 1e b0 00 00 00 33 00 00 00 02

Что ждут пользователи и разработчики СЭД?

Предложения по решению некоторых проблем:

- законодательное и/или нормативное закрепление доп. требований, предъявляемые к УЦ (в части документации, срокам действия сертификатов, расширения прав пользователей в части выпуска сертификатов – сроки, OID);
- разработать и утвердить требования к перечню и содержанию документов, регламентирующих деятельность УЦ;
- определить понятия «Действительность ключа ЭП», «Действительный сертификат ключа проверки ЭП»;
- определить требования (рекомендации) к срокам действия сертификатов, выпускаемых Головным, подчиненными и аккредитованными УЦ;
- определение и законодательное или нормативное закрепление условий и «параметров» действительности квалифицированного сертификата ключа проверки ЭП;
- определение требований к сервису проверки подлинности ЭП (в части отчета);
- определение требований (рекомендаций) к формату усовершенствованной ЭП (лучше в виде российского стандарта, ТК 26);
- обеспечение возможности регистрации и получения объектных идентификаторов в российском сегменте (орган и процедура регистрации);
- обеспечение совместимости программных интерфейсов java провайдера (ТК 26).

БЛАГОДАРЮ ЗА ВНИМАНИЕ!

© ЗАО «Компания «ИнтерТраст»

+7 (495) 956-79-28 http://www.intertrust.ru