Создание организационно-правовых и технологических механизмов «инфраструктуры доверия» в органах исполнительной власти Томской области

по Государственному контракту №600 от «19» декабря 2008 г.

Мещеряков Роман Валерьевич

к.т.н., доцент,
Заведующий лабораторией Систем Безопасности Центра Технологий Безопасности ТУСУР

Цель реализации «инфраструктуры доверия»: создание специализированных сервисов доверенной третьей стороны – **Службы «Доверенная третья сторона»** в составе узла среды электронного взаимодействия органов исполнительной власти Томской области для обеспечения юридической значимости информационного взаимодействия электронными документами в рамках административных процессов исполнения государственных функций и предоставления государственных услуг.

Исполнитель – ТУСУР, Центр Технологий Безопасности.

Центр Технологий Безопасности ТУСУР является системным интегратором в области построения комплексных систем защиты информации.

На базе Центра Технологий Безопасности ТУСУР функционирует Удостоверяющий Центр Сибири.

Приоритетными направлениями деятельности Центра технологий безопасности являются:

- программно-аппаратные средства защиты информации;

- средства криптографической защиты информации;

- обеспечение защищенного электронного документооборота;

- проведение аудита информационной безопасности;

- подготовка и переподготовка кадров в области информационной безопасности.

Для достижения поставленной цели были решены следующие задачи:

1. Поставка программно-технических средств, реализующих функции Службы «Доверенная третья сторона».

2. Ввод в эксплуатацию функционально-технологического комплекса Службы «Доверенная третья сторона» на базе информационно-технической инфраструктуры Администрации Томской области.

3. Проведена опытная эксплуатация «инфраструктуры доверия» на пилотных задачах информационного взаимодействия в рамках реализации административных процессов исполнения государственных функций и предоставления государственных услуг.

Для достижения поставленной цели были решены следующие задачи:

4. Разработана концепция, функционально-технологическая архитектура «инфраструктуры доверия» в исполнительных органах государственной власти Томской области и комплект организационно-правовой и нормативно технической документации Службы «Доверенная третья сторона».

При обмене информацией между двумя субъектами должен создаваться элемент доверия между получателем и отправителем информации. Получатель должен признавать идентичность отправителя, что он в действительности является отправителем, а отправитель - признавать идентичность получателя, что он является получателем, которому направлена информация. Определенные условия доверия между получателем и отправителем обеспечиваются информационными системами, основанными на применение современных информационных технологий.

В условиях осуществления деловой деятельности, связанной с коммерческой деятельностью или деятельностью государства с использованием информационных технологий, требуются все более надежные элементы доверия для достижения адекватных уровней защищенности информационного взаимодействия. Эти предполагаемые элементы доверия между участниками информационного взаимодействия в недостаточной степени обеспечиваются информационными системами и могут потребовать участие «доверенной третьей стороны», чтобы способствовать надежному обмену информацией.

В настоящее время сервисы «Доверенной третьей стороны» являются основной платформой для развертывания различных высокотехнологичных сервисов и услуг, в том числе относящихся к «**электронному правительству**». За последние десять лет данная технология прошла путь «с нуля» до законодательно обоснованного инструмента, позволяющего строить защищенные информационные системы в масштабах страны.

МЕМОРАНДУМ седьмой международной научно-практической конференции «PKI-Форум 2009»

«…Поддержать инициативы деловых кругов в применении технологий трансграничного, межрегионального, межведомственного электронного документооборота на сервисах доверенной третьей стороны в интересах трансграничных бизнес-процессов»

В роль Доверенной третьей стороны (ДТС) входит предоставление гарантий участникам взаимодействия, что сообщения и сделки своевременно и точно передаются предполагаемому получателю с обеспечением целостности, подлинности и авторства, и что в случае возникновения любых споров существуют определенные методы для создания и предоставления необходимых фактов, подтверждающих совершение действий и ход событий.

Создание ДТС должно основываться на международных стандартах и рекомендациях.

В соответствии с рекомендациями Международного союза телекоммуникаций ITU-T серии X.842 «Информационные технологии. Методы защиты. Рекомендации по использованию и управлению услугами третьей доверенной стороны», в соответствии с которыми выполнены работы:

Доверенная третья сторона (ДТС, Trusted Third Party, TTP) — это организация или её агент, предоставляющий один или более сервисов в области безопасности, которому доверяют другие объекты как поставщику данных услуг.

Также в рекомендациях определены службы и услуги ДТС, представлены указания по использования и управлению ДТС и определены роли и обязательства ДТС и лиц, пользующихся этими услугами.

Сервисы доверенной третьей стороны могут включать управление ключами и сертификатами, поддержку идентификации и аутентификации, фиксацию времени (time stamping), электронные нотариальные службы и другие сервисы.

В исполнительных органах государственной власти Томской области были реализованы следующие **основные элементы функционально-технологической архитектуры Службы «Доверенная третья сторона»**.

1. Служба атрибутирования.
2. Служба фиксации времени.
3. Службы электронного нотариата.
4. Службы идентификации, аутентификации и контроля доступа.

Роль службы управления ключами и сертификатами выполняет сторонняя организация - **Удостоверяющий Центр Сибири ТУСУР**.

В основе средств, реализующих функции Службы «Доверенная третья сторона», лежит серверное программное обеспечение, разработанное ООО «Топ Кросс» и состоящее из следующих компонентов.

1. Автоматизированная Система Служба «Заверения электронных сообщений» (Служба «Электронного Нотариата»).

2. Автоматизированная Система «Служба атрибутирования».

3. Модуль разграничения доступа для протокола http.

Служба «Электронного Нотариата» предоставляет сервисы всевозможных проверок, подтверждений и выработки «штампа времени» (в соответствии с международными рекомендациями RFC 3029, RFC 2560, RFC 3161).

Сервис DVCS (Data Validation and Certification Server) в соответствии с RFC 3029 (Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols) реализует следующие функции.

1. Декларирование наличия данных (CPD).

2. Декларирование признака наличия данных, без их предоставления сервису (CCPD).

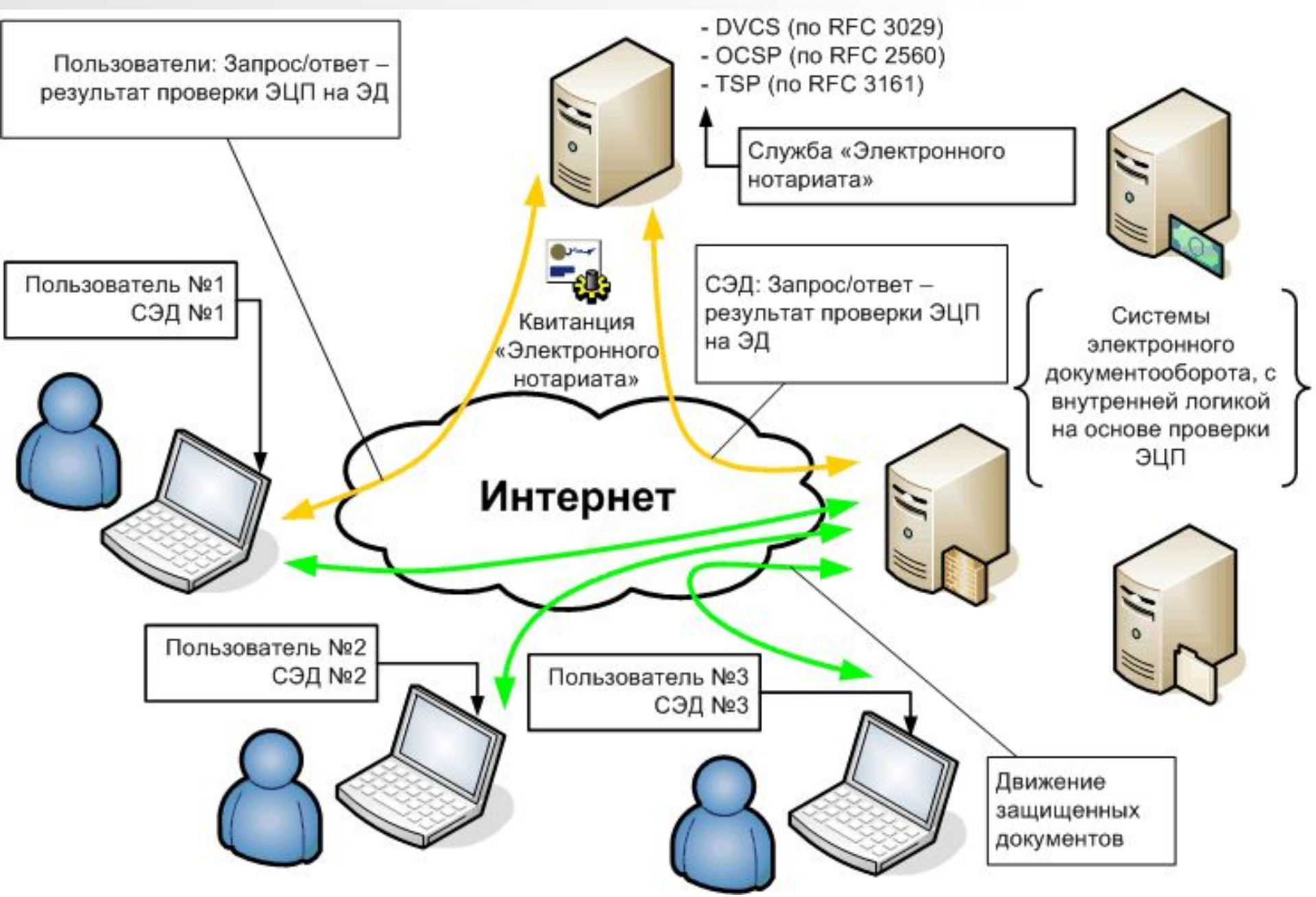
3. Проверка действительности подписи на документах (VSD).

4. Проверка действительности сертификатов открытых ключей (VPKC).

Результатом выполнения той или иной функции сервисом DVCS Службы «Электронного Нотариата» служит **DVC квитанция** – подписанный ЭЦП документ, содержащий результаты проверки и данные о времени выполнения проверки.

Сервис OCSP (Online Certificate Status Protocol) в соответствии с RFC 2560 реализует функцию online определения статуса сертификатов открытого ключа. Результатом работы службы OCSP являются сформированные в соответствии с протоколом OCSP-ответы (соответствующие OCSP-запросам), содержащие информацию о статусе запрашиваемых к проверке сертификатов открытых ключей.

Сервис TSP (Time-Stamp Protocol) в соответствии с RFC 3161 реализует функцию выработки «штампа времени». Результатом работы службы TSP являются сформированные в соответствии с протоколом TSP-ответы (соответствующие TSP-запросам), содержащие заверенный «штамп времени» с использованием эталонного источника времени информационной системы.


Пользователи: Запрос/ответ – результат проверки ЭЦП на ЭД
- DVCS (по RFC 3029)
- OCSP (по RFC 2560)
- TSP (по RFC 3161)
Служба «Электронного нотариата»
Пользователь №1
СЭД №1
Квитанция «Электронного нотариата»
СЭД: Запрос/ответ – результат проверки ЭЦП на ЭД
Системы электронного документооборота, с внутренней логикой на основе проверки ЭЦП
Интернет
Пользователь №2
СЭД №2
Пользователь №3
СЭД №3
Движение защищенных документов

Задачами, в которых может быть использована Служба «Электронного нотариата», являются следующие.

1. Создание единого домена защищенного электронного документооборота для разнородных программно-аппаратных и технологических платформ.

2. Получение «штампа времени» на заверенном документе для систем электронного документооборота. Служба «Электронного нотариата» как независимая «третья» сторона может использоваться для фиксации определенных этапов (стадий) в технологической цепочке документооборота.

3. Длительное архивное хранение электронных документов. ЭЦП на электронном документе имеет срок действия, который определяется периодом действительности сертификата подписавшей стороны. Срок действия сертификата на практике обычно не превышает 1 года.

Согласно ст.4 ФЗ «Об электронной цифровой подписи», условия признания равнозначности электронной цифровой подписи и собственноручной подписи:

«…сертификат ключа подписи, относящийся к этой электронной цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания».

Наличие DVC квитанций о результатах проверки ЭЦП позволяет делать выводы о действительности ЭЦП уже **после истечения срока действительности сертификата**. Данное свойство объясняется наличием механизмов пролонгации квитанций (выпуска квитанций на квитанцию).

4. Организация проверки ЭЦП «третьей» стороной для пользователей, что позволяет пользователям уйти от самостоятельного принятия решения о действительности ЭЦП и использования криптографических вычислений на сертифицированных СКЗИ.

5. Организация проверки сертификатов открытых ключей «третьей стороной», например, при прохождении процедуры аутентификации в системе.

6. Подтверждение факта обладания информацией без ее предоставления. Например, по регламенту открытых аукционов до процедуры «вскрытия конвертов» никто не должен иметь доступ к конкурсному материалу. Для таких систем участники могут предоставить квитанции об истинности ЭЦП конкурсного материала до процедуры «вскрытия конвертов». Истинность впоследствии предоставленного материала подтверждается ЭЦП из состава квитанции.

В рамках опытной эксплуатации «инфраструктуры доверия» было отработано использование сервисов Службы «Электронного нотариата» **Автоматизированной информационной системой «Государственные услуги Томской области»**.

1. ЭЦП электронных документов перед публикацией на сайте Портала Государственных услуг проверяется в Службе «Электронного нотариата».

2. На сайте Портала вместе с электронным документом размещается также квитанция Службы «Электронного нотариата». Квитанция содержит дату проверки и подтверждает момент времени публикации информации на сайте Портала.

3. Все запросы ведомственных и платежных систем на изменение статуса оказываемой гражданину услуги подписываются ЭЦП и проверяются получателем в Службе «Электронного нотариата»

4. Все подтверждения Портала об изменении статуса оказываемой гражданину услуги подписываются ЭЦП и проверяются получателем в Службе «Электронного нотариата».

В предлагаемой схеме взаимодействия со Службой «Электронного нотариата» квитанции результатов проверки ЭЦП являются электронными документами однозначной трактовки, которые подписаны ЭЦП соответствующего уполномоченного лица, что в совокупности придает им юридическую силу.

Квитанции предоставляют доказательную базу по фактам взаимодействия участников для выполнения государственных услуг. Таким образом, данный подход позволяет **противодействовать коррупции**.

Дополнительно в рамках опытной эксплуатации «инфраструктуры доверия» было отработано использование сервисов Службы «Электронного нотариата» Автоматизированной информационной системой документационного обеспечения управления.

1. При подписании электронных документов в системе ЭЦП проверяется в Службе «Электронного нотариата».

2. В системе вместе с электронным документом размещается также квитанция Службы «Электронного нотариата». Квитанция содержит дату проверки и подтверждает момент времени подписания электронного документа.

В предлагаемой схеме взаимодействия со Службой «Электронного нотариата» квитанции подтверждают время подписания электронных документов, а механизм автоматической пролонгации квитанций обеспечивает юридически значимое архивное хранение электронных документов.

Модуль разграничения доступа для протокола HTTP – внешний модуль к серверу HTTP, обеспечивающий поддержку TLS (RFC 2246, Transport Layer Security) и предоставляющий инструментарий для управления доступом к отдельным частям ресурса.

Модуль обеспечивает следующие технические возможности:

- защищенный доступ для пользователей сертифицированных СКЗИ;

- гибкие механизмы задания политики разграничения доступа;

- разграничение доступа на основе любых элементов X.509 сертификатов;

- разграничение доступа на основе атрибутных сертификатов и любых их элементов;

- настраиваемые механизмы проверки сертификатов, включая поддержку протокола OCSP и самостоятельное построение цепочки сертификации. Поддерживается также использование сетевого справочника (LDAP) и точек распространения списков отозванных сертификатов и обновлений к ним.

Автоматизированная Система «Служба атрибутирования» в соответствии с RFC 3281 (An Internet Attribute Certificate. Profile for Authorization) обеспечивает привязку внешне изданных сертификатов через механизм атрибутных сертификатов к частным дополнительным атрибутам пользователя, которые могут быть использованы как источник ролевой, дополнительной информации о пользователе и т.п., а также позволяет осуществить криптографическую связь между абстрактным блоком данных и дополнительной информацией (метаданными).

«Служба атрибутирования» является программным комплексом, выполняющим функции формирования и обслуживания атрибутного сертификата и ведения актуального реестра атрибутных сертификатов.

Задачи, решаемые с помощью атрибутных сертификатов.

Задача 1. Разграничить доступ и определение условий обработки информации согласно собственным правилам, где идентификационным элементом выступает сертификат открытого ключа из другого домена.

Отсутствие возможности внести в состав личного сертификата, при его создании, всю информацию, которая впоследствии будет требоваться на обрабатываемой стороне.

Данные задачи решаются путем указания дополнительной информации об участниках информационного обмена в атрибутных сертификатах, связанных с сертификатом автора запроса.


Удостоверяющий Центр сертификатов ключей подписи
Удаленный доступ
Персональный Сертификат участвующий при образовании TLS
Прикладная автоматизированная система
Модуль разграничения доступа для протокола HTTP
Сертификат ключа подписи
TLS
Интернет
Клиентское ПО на основе ИОК
Атрибутный Сертификат однозначно соответствующий персональному сертификату
Персональный Сертификат извлечен из ЭЦП
Приложения пользователей взаимодействующих с ресурсом по защищенному протоколу TLS, формирование защищенного ЭЦП электронных документов
Электронный Документ защищенный ЭЦП
CallBack на Запрос по поиску соответствующего атрибутного сертификата
Сервер атрибутных сертификатов (по RFC 3281)

Использование атрибутных сертификатов для данных целей позволяет не нагружать сертификат открытого ключа персональной информацией, которая чаще меняется чем Ф.И.О, а при изменении необходимо отзывать сертификат с последующим выпуском нового.

Основное логическое отличие:

Сертификат открытого ключа – это аналог «электронного паспорта» - идентификационный элемент.

Атрибутный Сертификат – «электронный пропуск» с указанием достоверной ролевой информации ранее идентифицированного субъекта. Размещение - не публичное.

Задача 2: Обеспечение актуальности информации

Исходящая и соответственно входящая информация для информационных систем организаций представляет собой более сложную структуру, нежели просто электронный документ, пусть даже с ЭЦП. В соответствии с действующим ГОСТ Р ИСО 15489-1-2007, помимо содержания документ должен иметь соотнесенные с контентом метаданные, отражающие операции деловой деятельности, и быть постоянно связанным или объединенным с ними. Такого рода метаданные, сопровождающие документ, должны содержать указания, обеспечивающие пригодность документа для последующего его использования, отражающие возможность локализации и поиска документа, воспроизводимости электронного документа техническими средствами визуализации.

В ряде случаев документ имеет период действительности, то есть информация, содержащаяся в документе, может потерять свою актуальность, к тому же часто возникает потребность, вызванная спецификой деловой активности, в преждевременном отзыве документа. Наиболее яркий пример таких документов - различного рода разрешения.

Реализация информационного контейнера электронного документа с использованием механизма атрибутных сертификатов придает следующие свойства:

1. Контейнер имеет механизмы защиты целостности данных и идентификации источника данных.

2. Язык описания и правил кодирования контейнера универсален и позволяет описывать сложные структуры и типы данных.

3. Наличие признака, по которому информацию (включая и метаданные) содержащуюся в контейнере можно ассоциировать с событием или информацией в СЭД.

4. Обеспечены условия определения в любой момент времени актуальности информации помещённой в контейнер.

Структура атрибутного сертификата :

Владелец (Holder)

1. Хэш-функция от ЭД
2. Идентификатор ЭД в пространстве документов поддерживаемых СЭД организации

Атрибуты и метаданные

1. ЭД или ссылка на него
2. Метаданные, определяющиеся спецификой СЭД и по своему качеству соответствующие ГОСТ Р ИСО 15489-1-2007 для задач обеспечения создания Надежных (доверенных) документов, обладающих следующими характеристиками:
   I. *Аутентичность*
   II. *Достоверность*
   III. *Целостность*
   IV. *Пригодность для использования*

Продолжительность действительности контейнера

Интервал времени в течении которого информация инкапсулированая в контейнер считается действительной по правилам СЭД

Механизм отзыва контейнера

Указание ресурса со списком отозванных контейнеров в рамках СЭД или признак того, что такой контейнер не может быть отозван

ЭЦП издателя контейнера

Обеспечивает доверие и целостность содержащейся в контейнере информации

Техническая реализация ЭЦП (привычный всем формат ЭЦП в виде CMS (PKCS#7), или «подпись с расширенными данными для проверки» по ETSI TS 101 733) не предоставляет механизмов обеспечить актуальность документа.

Возможными областями использования атрибутных сертификатов являются следующие.

1. Бизнес-процессы, в которых исходящие документы имеют функции разрешения или лицензии на что либо, выдаваемые на определенный срок и с возможностью преждевременного отзыва.

2. Различного рода выписки из Реестров, Кадастров и т.п., наиболее яркий например, выписка из Единого Реестра Юридических Лиц. Например: выписка из ЕГРЮЛ на бумажном носителе имеет ограниченный срок действия. С помощью механизма атрибутных сертификатов можно реализовать выписку из ЕГРЮЛ действительную всю время, пока не изменятся сведения о юридическом лице или не истечет срок действия атрибутного сертификата (который может быть несколько лет).

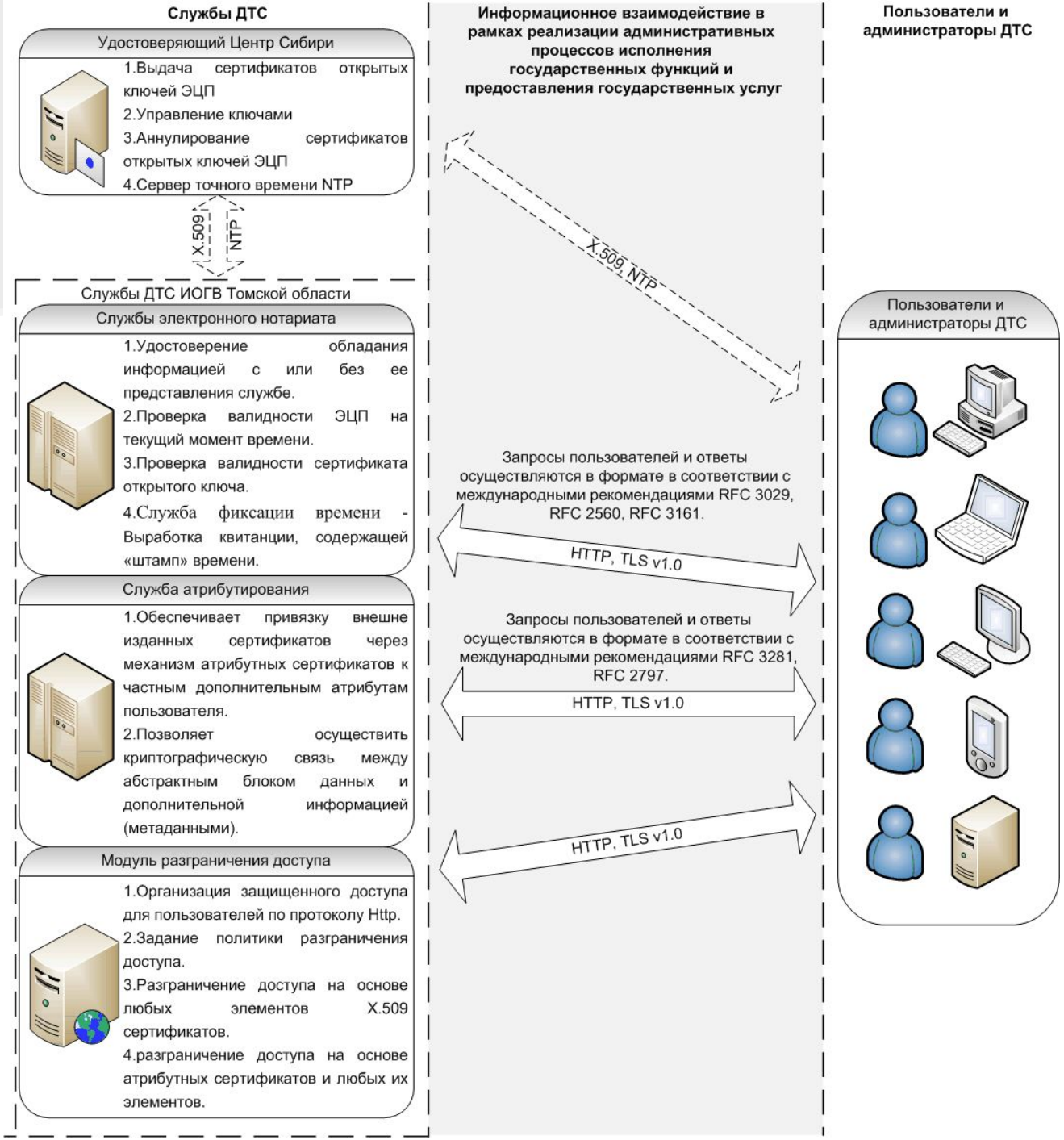
3. Электронная лицензия на программное обеспечение или иную информацию (дополнительно автоматически решается задача контроля целостности и неизменности программного обеспечения или иной информации).

4. Контейнеры (метки целостности и актуальности) защищенных электронных документов содержащие метаданные и имеющие технологию управления актуальностью контента самого ЭД, без отзыва сертификатов авторов ЭЦП.

Разработан комплект организационно-правовой и нормативно технической документации Службы «Доверенная третья сторона», в который входит следующее.

1. Концепция и функционально-технологическая архитектура ДТС.

Целью концепции является формирование методологических основ реализации «инфраструктуры доверия» в исполнительных органах государственной власти Томской области и предложение функционально-технологической архитектуры.


Службы ДТС
Удостоверяющий Центр Сибири
1.Выдача сертификатов открытых ключей ЭЦП
2.Управление ключами
3.Аннулирование сертификатов открытых ключей ЭЦП
4.Сервер точного времени NTP
X.509
NTP
Службы ДТС ИОГВ Томской области
Службы электронного нотариата
1.Удостоверение обладания информацией с или без ее представления службе.
2.Проверка валидности ЭЦП на текущий момент времени.
3.Проверка валидности сертификата открытого ключа.
4.Служба фиксации времени - Выработка квитанции, содержащей «штамп» времени.
Служба атрибутирования
1.Обеспечивает привязку внешне изданных сертификатов через механизм атрибутных сертификатов к частным дополнительным атрибутам пользователя.
2.Позволяет осуществить криптографическую связь между абстрактным блоком данных и дополнительной информацией (метаданными).
Модуль разграничения доступа
1.Организация защищенного доступа для пользователей по протоколу Http.
2.Задание политики разграничения доступа.
3.Разграничение доступа на основе любых элементов X.509 сертификатов.
4.разграничение доступа на основе атрибутных сертификатов и любых их элементов.
Информационное взаимодействие в рамках реализации административных процессов исполнения государственных функций и предоставления государственных услуг
X.509, NTP
Запросы пользователей и ответы осуществляются в формате в соответствии с международными рекомендациями RFC 3029, RFC 2560, RFC 3161.
HTTP, TLS v1.0
Запросы пользователей и ответы осуществляются в формате в соответствии с международными рекомендациями RFC 3281, RFC 2797.
HTTP, TLS v1.0
HTTP, TLS v1.0
Пользователи и администраторы ДТС
Пользователи и администраторы ДТС

2. Комплект нормативно-технических документов стандартизующих, регламентирующих и специфицирующих механизмы взаимодействия информационных систем с сервисами Службы «Доверенная третья сторона».

2.1.Проект интерфейса защищенного доступа для пользователей к веб-серверу с установленным модулем разграничения доступа для протокола HTTP.

2.2.Проект интерфейса по осуществлению защищенного доступа и взаимодействия пользователей со Службой «Электронного нотариата».

2.3.Проект интерфейса по осуществлению защищенного доступа и взаимодействия пользователей с «Служба атрибутирования».

2. Комплект нормативно-технических документов стандартизующих, регламентирующих и специфицирующих механизмы взаимодействия информационных систем с сервисами Службы «Доверенная третья сторона».

2.1.Проект интерфейса защищенного доступа для пользователей к веб-серверу с установленным модулем разграничения доступа для протокола HTTP.

2.2.Проект интерфейса по осуществлению защищенного доступа и взаимодействия пользователей со Службой «Электронного нотариата».

2.3.Проект интерфейса по осуществлению защищенного доступа и взаимодействия пользователей с «Служба атрибутирования».

3. Комплект организационно-правовой документации Службы «Доверенная третья сторона».

3.1.Проект положения о Службе «Доверенная третья сторона».

3.2.Общие требования к критериям подтверждения подлинности ЭЦП.

3.3.Проект договора с федеральными службами ДТС в процессах общероссийского информационного обмена.

3.4.Проект соглашения о порядке признания юридического значения документов, подготовленных в электронном виде с учетом технологического регламента функционирования и эксплуатации Службы «Доверенная третья сторона».

3.5.Проекты организационно-правовых документов, регулирующих вопросы функционирования Службы «Доверенная третья сторона».

В процессе выполнения работ по Государственному контракту №600 от «19» декабря 2008 г. получены следующие результаты.

Разработана концепция и функционально-технологическая архитектура «инфраструктуры доверия» в исполнительных органах государственной власти Томской области.

Осуществлена поставка программно-технических средств, реализующих функции Службы «Доверенная третья сторона» и осуществлен ввод в действие функционально-технологического комплекса Службы «Доверенная третья сторона» на базе информационно-технической инфраструктуры Администрации Томской области.

Разработан комплект нормативно-технических документов стандартизующих, регламентирующих и специфицирующих механизмы взаимодействия информационных систем Заказчика с сервисами Службы «Доверенная третья сторона».

Разработан комплект организационно-правовой документации Службы «Доверенная третья сторона».

Проведена опытная эксплуатация «инфраструктуры доверия» на пилотных задачах информационного взаимодействия в рамках реализации административных процессов исполнения государственных функций и предоставления государственных услуг.

Функциональный комплекс Службы «Доверенная третья сторона» реализован на основе следующих международных рекомендаций:

- RFC 3029 Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols (DVCS);

- RFC 2560. Online Certificate Status Protocol – OCSP;

- RFC 3161. Time-Stamp Protocol (TSP);

- RFC 3281. An Internet Attribute Certificate. Profile for Authorization.

Осуществлен ввод технологий Службы «Доверенная третья сторона» в промышленную эксплуатацию.

Проведенный комплекс работ полностью соответствуют положениям рекомендаций ITU-T серии X.842 и требованиям, указанным в Техническом задании, в том числе по выполнению базовых функций, поддержке необходимых механизмов разграничения доступа, приему и обработке электронных сообщений, по составу функционального комплекса и требованиям к компонентам, по требованиям к клиентскому специальному программному обеспечению, по поддержке криптографических средств с реализацией отечественных алгоритмов (в соответствии с RFC 4357, 4490, 4491).

В части стандартизации были унифицированы требования к взаимодействию ДТС между собой, т.е. определен интерфейс и формат взаимодействия, для того, чтобы субъекты одного ДТС могли надежно связываться с субъектами другой ДТС возможности, а также создать взаимоувязанную сеть ДТС.

В случае взаимодействия ДТС и пользователя установлены единые требования запроса услуг ДТС и предоставления данных для проверки, а также форматы результатов проверки, получаемые пользователем. В качестве средств формирования и проверки электронной цифровой подписи используются сертифицированные средства криптографической защиты информации.

Перспективным направлением развития Службы «Доверенная третья сторона» является Служба документирования, которая основана на требованиях ГОСТ Р ИСО 15489-1-2007 к документированию деловой активности.

Служба документирования является программным комплексом, выполняющим функции факто фиксирующей системы для внешних событий или информации и ведения их актуальной базы данных.

Внесение информации в систему может осуществляться как внешними средствами по отношению к комплексу на соответствующем программном обеспечении пользователя или СЭД, например, с использованием утилиты командной строки, так и средствами графического интерфейса Службы.

Служба документирования выполняет следующие функции:

1) регистрацию событий и связанной с ними информации;

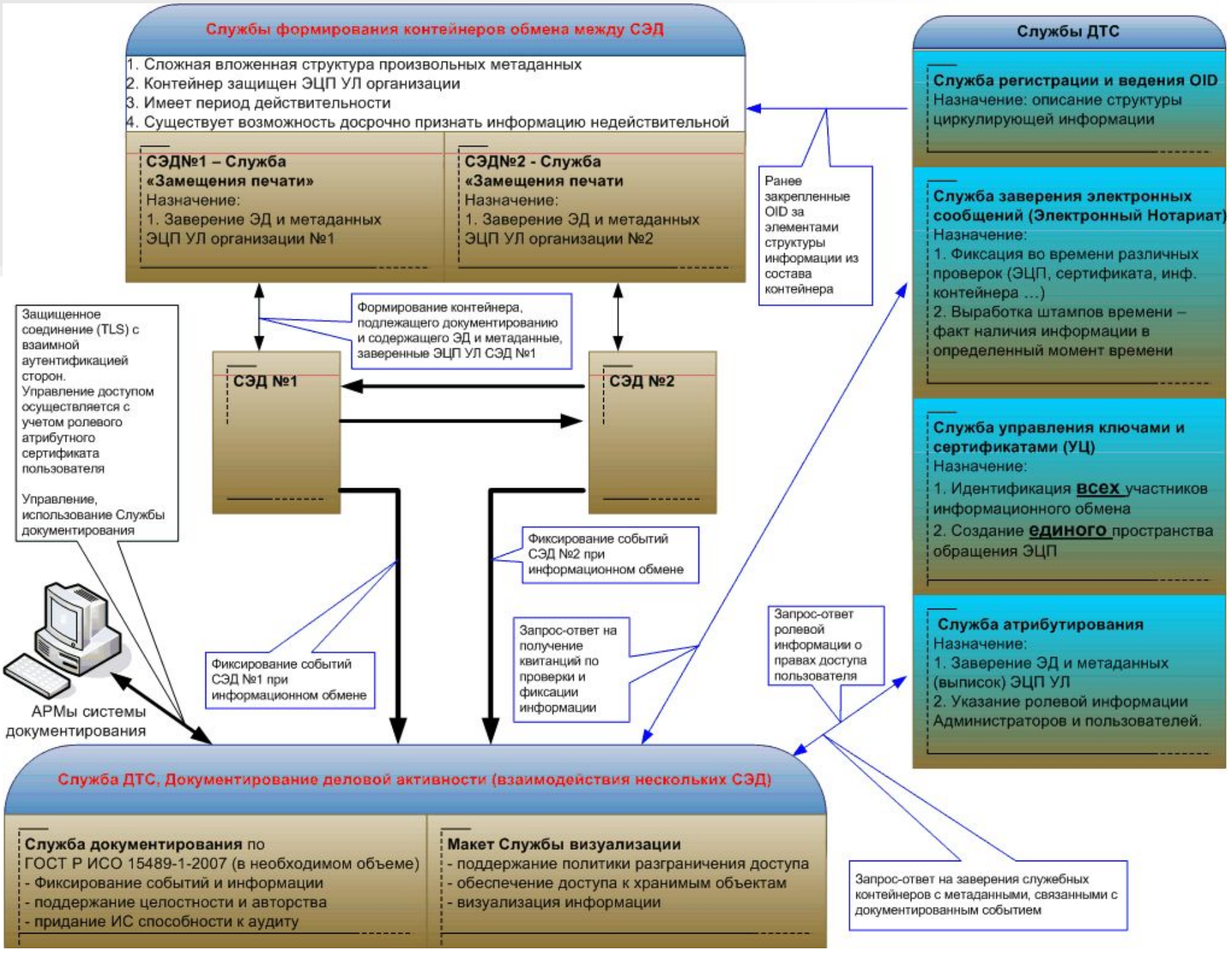
2) осуществление проверки принимаемой к документированию информации с использованием внешней Службы «Электронного нотариата»

3) взаимодействие со Службой атрибутирования

4) предоставление интерфейса для визуализации, навигации и поиска информации, связанной с определенными внешними событиями;

5) формирование выписок конкретных документов в виде защищенного контейнера (атрибутного сертификата).

Для более наглядной иллюстрации роли и места Службы, на рисунке изображена структурная схема абстрактного бизнес-процесса, в которым происходит взаимодействие двух СЭД с документированием событий и информации их сопровождающей в Службе документирования. Процесс происходит во взаимодействии с другими Службами ДТС.


Службы формирования контейнеров обмена между СЭД
1. Сложная вложенная структура произвольных метаданных
2. Контейнер защищен ЭЦП УЛ организации
3. Имеет период действительности
4. Существует возможность досрочно признать информацию недействительной
СЭД№1 – Служба «Замещения печати»
Назначение:
1. Заверение ЭД и метаданных ЭЦП УЛ организации №1
СЭД№2 - Служба «Замещения печати
Назначение:
1. Заверение ЭД и метаданных ЭЦП УЛ организации №2
Службы ДТС
Служба регистрации и ведения OID
Назначение: описание структуры циркулирующей информации
Ранее закрепленные OID за элементами структуры информации из состава контейнера
Служба заверения электронных сообщений (Электронный Нотариат)
Назначение:
1. Фиксация во времени различных проверок (ЭЦП, сертификата, инф. контейнера …)
2. Выработка штампов времени – факт наличия информации в определенный момент времени
Служба управления ключами и сертификатами (УЦ)
Назначение:
1. Идентификация всех участников информационного обмена
2. Создание единого пространства обращения ЭЦП
Служба атрибутирования
Назначение:
1. Заверение ЭД и метаданных (выписок) ЭЦП УЛ
2. Указание ролевой информации Администраторов и пользователей.
Формирование контейнера, подлежащего документированию и содержащего ЭД и метаданные, заверенные ЭЦП УЛ СЭД №1
Защищенное соединение (TLS) с взаимной аутентификацией сторон.
Управление доступом осуществляется с учетом ролевого атрибутного сертификата пользователя
Управление, использование Службы документирования
СЭД №1
СЭД №2
Фиксирование событий СЭД №2 при информационном обмене
Фиксирование событий СЭД №1 при информационном обмене
Запрос-ответ на получение квитанций по проверки и фиксации информации
Запрос-ответ ролевой информации о правах доступа пользователя
АРМы системы документирования
Служба ДТС, Документирование деловой активности (взаимодействия нескольких СЭД)
Служба документирования по ГОСТ Р ИСО 15489-1-2007 (в необходимом объеме)
- Фиксирование событий и информации
- поддержание целостности и авторства
- придание ИС способности к аудиту
Макет Службы визуализации
- поддержание политики разграничения доступа
- обеспечение доступа к хранимым объектам
- визуализация информации
Запрос-ответ на заверения служебных контейнеров с метаданными, связанными с документированным событием

Спасибо за внимание!
Пожалуйста, вопросы.