Атрибутные сертификаты и ЭДО

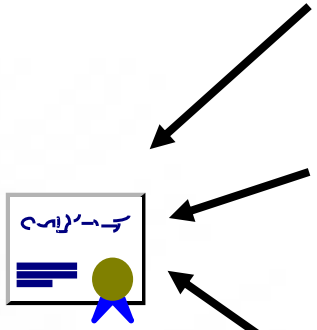
Конкурентоспособные отечественные разработки на основе международных стандартов

Что такое атрибутный сертификат? Правовой аспект

- Атрибутный сертификат (далее – АС) – стандартизованный электронный документ, созданный организацией и содержащий сведения о юридических фактах. АС создаются и изменяются в этих организациях.
- Создание АС инициируется уполномоченным должностным лицом организации (директором, начальником отдела кадров, руководителем делопроизводства и т.п.).
- АС содержит набор атрибутов, характеризующих: данную организацию, ее должностных лиц, членство в некоторой группе, роль, признаки безопасности, авторизационную информацию, электронные документы организации и их метаданные и др.
- Владелец АС – субъект (физическое или юридическое лицо) или объект (например, документ), сведения о котором содержатся в одном или нескольких АС.
- Связь АС и его владельца, а также связь АС и иных ЭД (например, СКП) производится с помощью идентификатора, включаемого в АС однозначно идентифицирующего владельца по уникальному имени (СНИЛС, ИНН ..., уникального имени ЭД в ЭДО) или свёртки от ЭД.
- АС позволяет реализовать в организации разный жизненный цикл для статичных или оперативно изменяющихся данных (редко или часто изменяющихся сведений), сохраняя между ними однозначную, автоматически проверяемую и юридически значимую связь.

Связь АС с сертификатом открытого ключа

Следует ли нагружать сертификат открытого ключа ролевой и иной информацией персонального или конфиденциального характера?



- Полномочия могут меняться чаще, чем идентифицирующая информация (ФИО, СНИЛС, ИНН).
- Полномочия могут действовать дольше, чем срок действительности СКП.
- Организационная граница «Отдел кадров» - «Отдел режима», каждый со своими регламентами.
- Явный конфликт с 152-ФЗ «О персональных данных». Все указанное в СКП становиться публичным. Реестр АС может не быть публичным.
- Часто НЕТ способов внести в состав СКП при его создании именно ту информацию, которая будет требоваться на обрабатываемой стороне. Авторизация – это функция принимающей стороны.

Что такое атрибутный сертификат? Технический аспект

- АС - двоичный блок данных в кодировке ASN.1 (такой же как и СКП), компиляторы для которой есть на рынке, в том числе с лицензиями Open Source.
- Связь АС с владельцем осуществляется через атрибут **holder**.
- Структура АС подобна сертификату X.509. Основное отличие – АС не содержит открытого ключа и не предполагает создание ключевой пары.
- Действительность АС ограничена только действительностью электронной подписи (ЭП) издателя АС, т.е. может иметь значительно более продолжительное время, чем сертификат ключа проверки (СКП) подписи. АС имеет инструменты досрочного аннулирования, приостановления и восстановления действительности.
- АС применяется параллельно с PKI и не требуют переделки средств подписи, УЦ и др. существующих компонент PKI-инфраструктуры.
- У АС очень длинная история как международного стандарта (с 2002 г.).

Области использования АС

- Для описания правовых статусов (полномочий) должностных лиц организации.
- Для управления разграничением доступа к сетевым ресурсам или процедурой обработки защищенных ЭП ЭД с учетом **полномочий, ролевых признаков** и иных характеристик автора или субъекта доступа.
- АС - **метка целостности и актуальности**, является «отзываемым» аналогом отсоединенной подписи. Используя механизмы управления временем действительности АС, позволяет технически обеспечить актуальность содержания документа. Бизнес-процессы, в которых ЭД имеют функции разрешения или лицензии на что-либо, выдаваемые на определенный срок и с возможностью отзыва, а также электронные выписки из различных реестров.
- АС - **защищенный контейнер**, идеально подходит при обмене структурированной информацией между ИС («сырыми» данными, не оформленными в документ, имеющий визуальное представление), максимально пригодными к последующей машинной обработке.

АС наиболее эффективны в публичном, межведомственном и трансграничном обмене, когда стороны не объединены единой системой ЭДО, и контрагентам для юридической значимости недостаточно получения ЭД и проверки ЭП

АС контейнер полномочий / доверенность

Требование	Реализация
Связка с владельцем	1. Различимое имя (ФИО+СНИЛС+ИНН) – возможность использования в «смешанном» документообороте 2. Свертка от данных (включая СКП)
Продолжительность действия	Абсолютные значения «от» … «до»
Возможность досрочного вывода АС из оборота Ссылка на информацию для автономной проверки статуса АС	Да. 1. CDP – ссылка на основной список ACRL 2. FreshestCRL – ссылка на обновления delta ACRL для real-time систем
Возможные статусы АС	Действительный, приостановленный, аннулированный.
Способ защиты АС	Электронная подпись издателя АС
Возможность указания атрибутов в машиночитаемом виде и комментарии	Да + очень гибкая структура атрибутов, включая возможность ввода человекочитаемых комментариев
Один субъект может иметь неограниченное число АС	Да
Сервис документирования процедуры проверки on-line статуса АС	Модернизированные стандартные протоколы OCSP и VPKC (из состава DVCS)

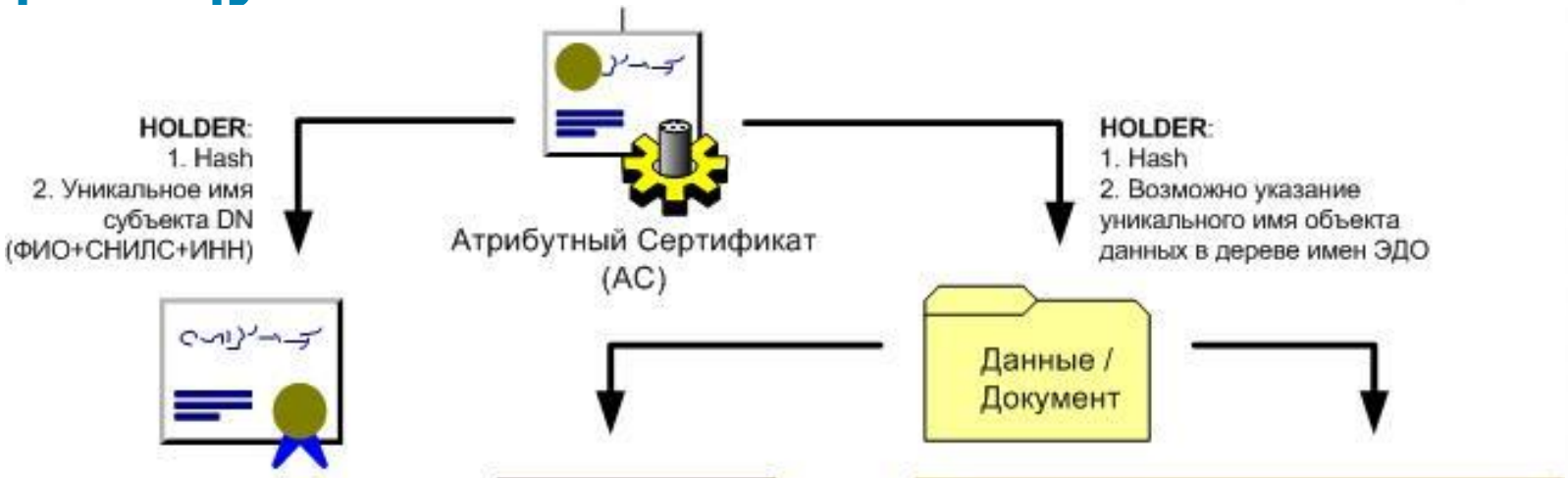
Стандарты и документы

- АС как стандартный технический инструментарий для указания дополнительной и ролевой информации, определён в RFC 5755, RFC 4476 и в X.842
- Использование АС в ЕС регламентируются рядом стандартов, например:
  - ETSI TR 102 044 (Требования к указанию ролевых признаков и атрибутов)
  - ETSI TS 102 158 (Требования к политикам сервисов по выпуску атрибутных сертификатов, предназначенных для использования с квалифицированными сертификатами.)
- «Атрибутные издатели» входят в европейский список доверенных сервисов и содержат квалифицированную (доверенную) информацию. Пример – список Польши https://www.nccert.pl/tsl/PL_TSL.xml:
  - <tsl:Name xml:lang="EN">Certification authority issuing Qualified Attribute Certificates</tsl:Name>
- ГОСТ Р ИСО/ТС 2260-1-2009 Информатизация здоровья. Управление полномочиями и контроль доступа. Часть 1 Общие сведения и управление политикой.
- Беларусь: ПОЛИТИКА ПРИМЕНЕНИЯ АТРИБУТНЫХ СЕРТИФИКАТОВ, изданных республиканским удостоверяющим центром Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь, Минск, 2016 год.

Препятствия для применения в РФ

- Слишком «общий» профиль СКП из Приказа ФСБ №795
- Неудачная ставка на фиксацию полномочий внутри СКП, что не противоречило первым редакциям 63-ФЗ. Привело к выпуску множества СКП разного назначения для одного и того же субъекта.
- В настоящий момент декларируется, что единый СКП может быть использован во всех ИС, но вопрос фиксации и проверки полномочий «повис в воздухе».
- Унаследованные ИС, особенно у регуляторов, где полномочия указываются в СКП или во внешних системах управления учётными данными (Idm - Identity management).
- Миф о том, что использование АС приведет к переделке средств подписи и УЦ, их пересертификации и т.д., т.е. что всё, якобы, сложно, долго и дорого.
- Игнорирование мирового опыта (например, Республики Беларусь, где с 2015 г. идет постепенное движение в сторону АС).

Классификация АС по принадлежности к владельцу

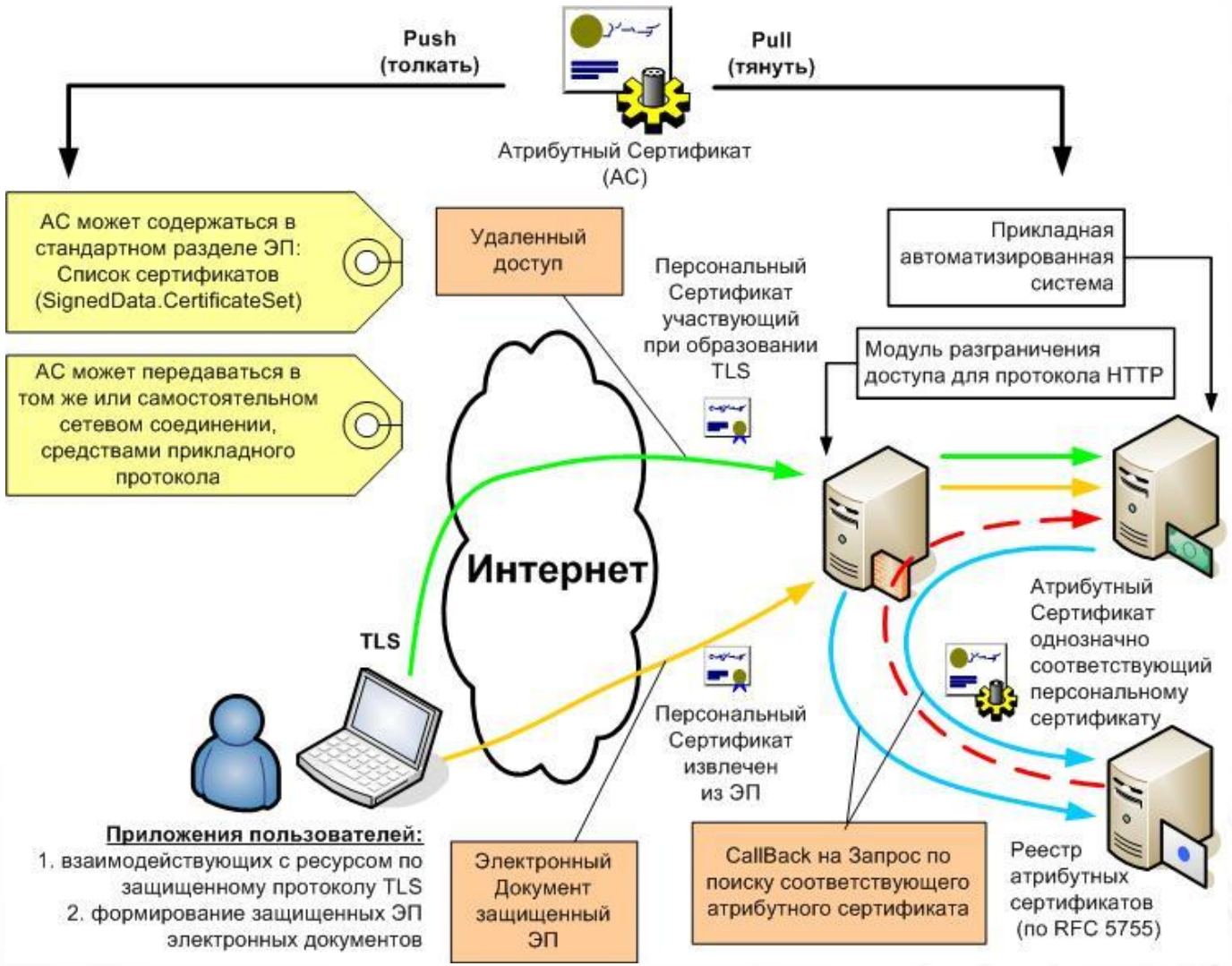


Применимость:
1. Указание дополнительной информации характеризующей автора ЭП (список АС)
2. Указание ролевой информации, используемой как признак разграничения доступа

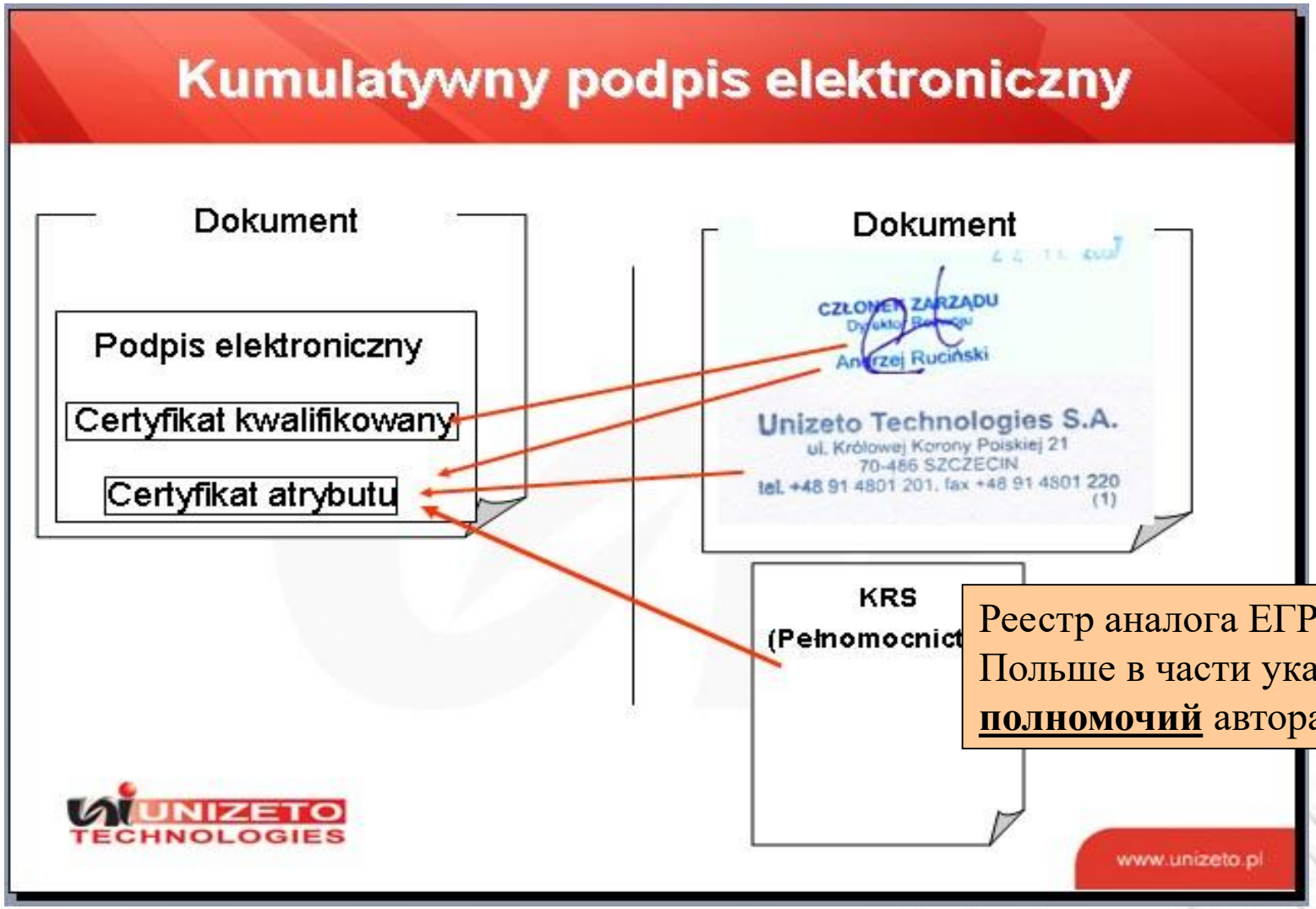
Применимость:
1. Обеспечение целостности данных (функциональный аналог отсоединённой подписи).
2. Обеспечение отзывности данных при потере их актуальности

Применимость:
1. Сам документ представляют из себя набор структурированных данных, легко обеспечивается машинная обработка.
2. Обеспечение отзывности данных при потере их актуальности

Классификация АС по способам доставки



Полномочия автора ЭД и АС



Реестр аналога ЕГРЮЛ в Польше в части указания **полномочий** автора ЭД

АС - структурированные данные на примере контейнера предварительного информирования

описание атрибута	тип атрибута	идентификатор атрибута
PERSON2	PERSON2	1.2.643.2.21.1.1.1.5.1.24
PERSON1	PERSON1	1.2.643.2.21.1.1.1.5.1.23
PERSON	PERSON	1.2.643.2.21.1.1.1.5.1.22
FINAL	FINAL	1.2.643.2.21.1.1.1.5.1.21
EXPENSES	EXPENSES	1.2.643.2.21.1.1.1.5.1.20
TOTAL	TOTAL	1.2.643.2.21.1.1.1.5.1.19
	ARTICLES	1.2.6
	ARTICLE	1.2.6
RENCY	ARTICLE_CURRENCY	1.2.6
D	RESERVE_FIELD	1.2.6
	VEHICLE_NRS	1.2.6
INVOICE_NRS	INVOICE_NRS	1.2.6
CURRENCY_CODE	CURRENCY_CODE	1.2.6
CONTRACT	CONTRACT	1.2.6
DELIVERY	DELIVERY	1.2.6
BANK_ACCOUNT	BANK_ACCOUNT	1.2.6
CONSIGNEE	CONSIGNEE	1.2.6
CONSIGNOR	CONSIGNOR	1.2.643.2.21.1.1.1.5.1.7
CCInfo	CCInfo	1.2.643.2.21.1.1.1.5.1.6
CUSTOMER	CUSTOMER	1.2.643.2.21.1.1.1.5.1.5
SELLER	SELLER	1.2.643.2.21.1.1.1.5.1.4
SCInfo	SCInfo	1.2.643.2.21.1.1.1.5.1.3
BILL	BILL	1.2.643.2.21.1.1.1.5.1.2
DOCUMENT	DOCUMENT	1.2.643.2.21.1.1.1.5.1.1

```
TOTAL ::= SEQUENCE {
    spots INTEGER,
    brutto          REAL,
    netto REAL,
    price  REAL
}
```

Комплект документов для таможенного оформления грузов является **структурированными данными**, которые легко представляются в формате АС, что позволяет их **автоматически обрабатывать в ИС**.
Могут быть **очень легко объявлены не актуальными** при отмене поставки груза.

Примеры внедрения АС

- 2010 г. ООО «Топ Кросс»

  Цель проекта - технология управления полномочиями на сервере обновлений ПО. АС имеет срок действия, равный договору сопровождения, и состав – перечень взятого ПО на сопровождение.

- 2010 г. ООО «Таможенно-Брокерский Центр»

  Внутренняя ЭДО. АС – структурированная информация по предварительному декларированию таможенных грузов с обеспечением актуальности структуры. Контейнер в виде АС максимально приспособлен к защищенной транспортировке и машинной обработке.

- 2013 г. ООО РТО и Ассоциация Электронных Торговых Площадок

  Цель – использовать указания полномочий при трансграничном ЭДО на ЭТП.

- 2017 г. Группа компаний «ФИННЕТ-СЕРВИС»

  Целью проекта является создание модуля к «1С-Кадры» для инфраструктуры управления полномочиями в ЭДО с использованием атрибутных сертификатов.

- 2016-2018 гг. Пенсионный Фонд Российской Федерации

  Цель проекта – обеспечение юридической значимости при длительном хранении ЭД. В АС упакованы процессные метаданные, необходимые для обеспечения аутентичности ЭД.

- 2017-2018 гг. - Группа компаний «Центр открытых систем и высоких технологий»

  Цель проекта – повышение эффективности работы сотрудников Федерального агентства по печати и массовым коммуникациям за счет создания системы управления полномочиями, использующих атрибутные сертификаты.

Вопросы?

Сергей Михайлович Муругов
ООО «Топ Кросс», Генеральный директор

Михаил Юрьевич Брауде-Золотарев,
РАНХиГС при Президенте РФ
Центр ИТ-исследований и экспертизы, директор