Подходы к обеспечению дополнительных свойств электронной подписи

Герасимов Илья Юрьевич,
специалист-исследователь лаборатории криптографии, АО «НПК «Криптонит»

Бельский Владимир Сергеевич,
заместитель руководителя лаборатории криптографии, АО «НПК «Криптонит»

КРИПТОНИТ

Использование ЭП

КРИПТОНИТ

1 **Целостность**

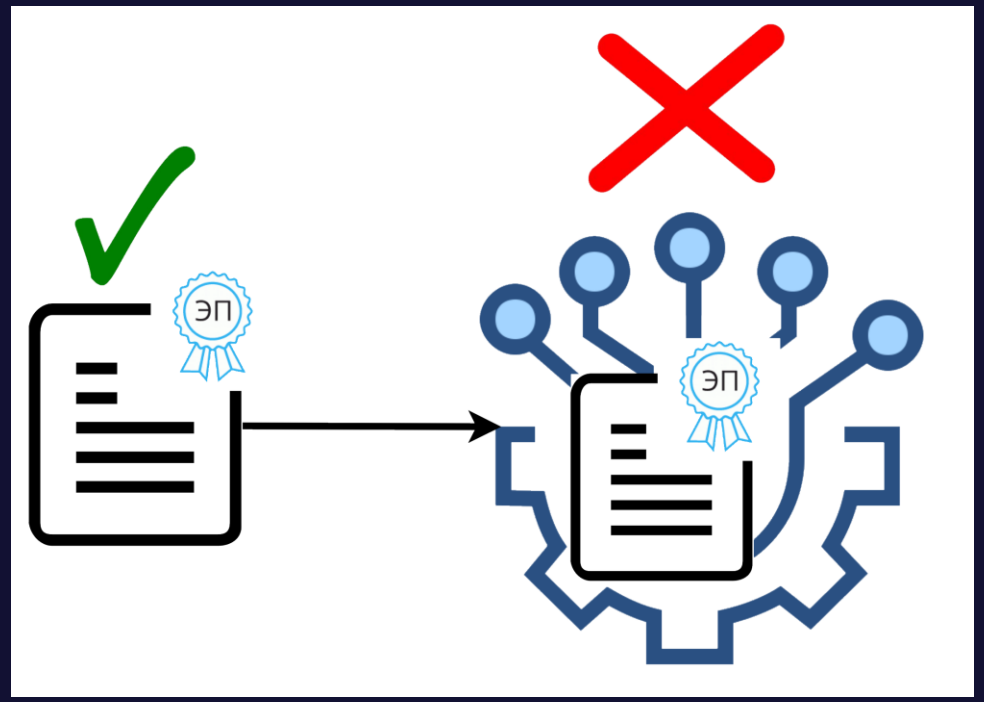
Осуществление контроля целостности передаваемого сообщения.

2 **Аутентификация**

Доказательное подтверждение авторства лица, подписавшего сообщение.

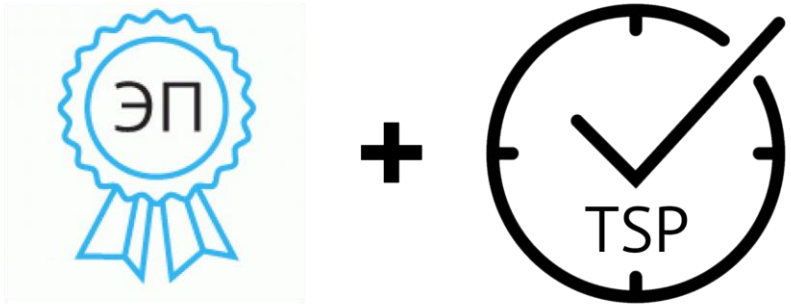
3 **Неподделываемость**

Защита сообщения от подделки.



Можно ли и каким образом систематизировать свойства и методы, которые необходимо учитывать при внедрении ЭП, составить решения, охватывающие наибольший спектр задач, в частности в рамках задачи аутентификации и идентификации (АИ)?

Существующие практики



Усовершенствованная ЭЦП (CAdES):

- Доказательство момента подписи,
- Доказательство действительности сертификата ключа подписи на момент подписи.

ПЦД ПД:

- Обеспечение конфиденциальности подписываемых данных,
- Доказательство корректности данных на момент подписи и в течение заранее определенного периода.

ПТК ДЭГ:

- Регистрация голосующего,
- Несвязываемость факта голосования с зарегистрированным голосующим.

Дополнительные требования в рамках АИ

КРИПТОНИТ

I. На взаимодействие участников накладываются дополнительные свойства и требования.

- Конфиденциальность,
- Несвязываемость,
- Наличие или отсутствие доверенных третьих сторон (ДТС),
- Количество участников.

W3C DID, VC
TSP, OCSP
ПДн

Аутентификационная информация уровня обмена

Аутентификационная информация уровня подтверждения

Аутентификационная информация верификации

II. Участники обладают атрибутами, значения которых определяют порядок действий.

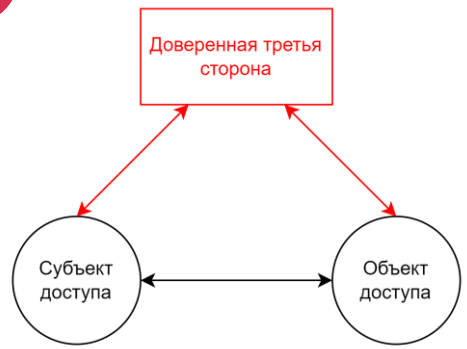
- Местоположение,
- Время,
- Количество обращений,
- Персональные данные участника,
- Характеристики аутентификационных данных.

Частные модели аутентификации и идентификации

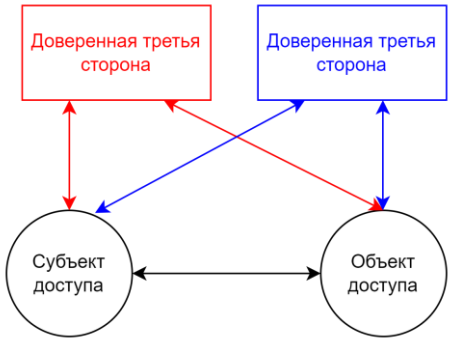
КРИПТОНИТ

1 Изолированная

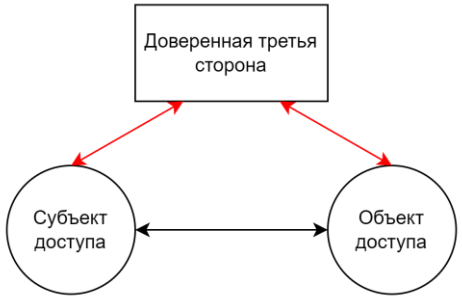
2 Централизованная



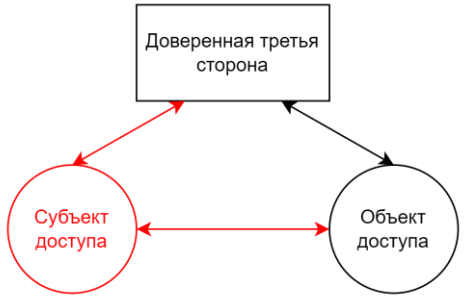
3 Федеративная



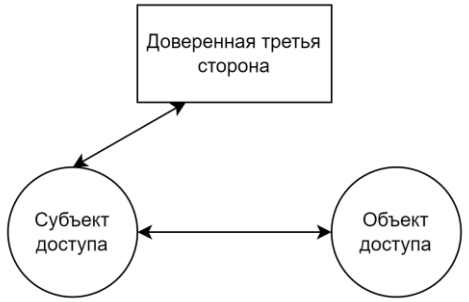
4 Сервисной аутентификации



5 Ориентированная на пользователя



6 Суверенная



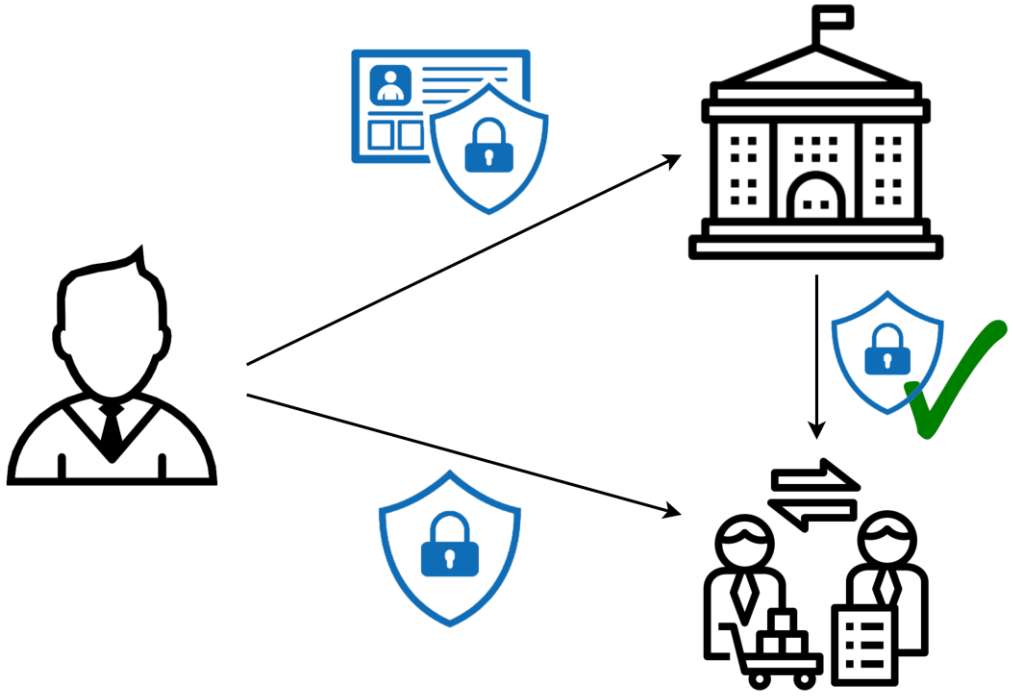
Бельский В. С., Герасимов И. Ю., Сабанов А. Г., Царегородцев К. Д. Анализ моделей идентификации и аутентификации // International Journal of Open Information Technologies. – 2024. – Т. 12. – №. 5. – С. 1-14.

I. Свойства информационного взаимодействия

КРИПТОНИТ

Конфиденциальность подписываемых данных

- Если на этапе аутентификации есть участник, отвечающий за обработку данных, подписываемые данные передаются в зашифрованном виде на ключе шифрования, полученном в результате процедуры согласования ключа подписывающего и дополнительного участника.
- Если такой участник отсутствует, используются протоколы с нулевым разглашением.

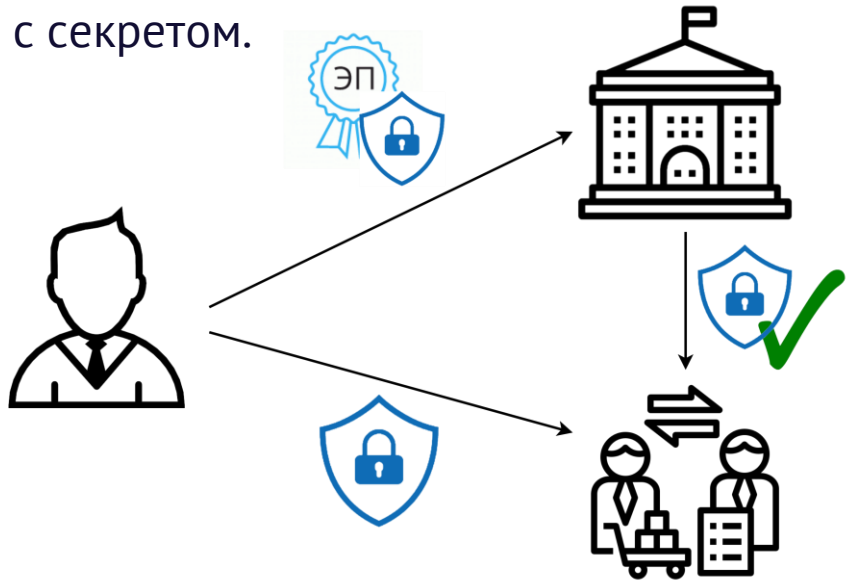


I. Свойства информационного взаимодействия

КРИПТОНИТ

Конфиденциальность подписи

- Если на этапе аутентификации есть участник, отвечающий за проверку подписи в зашифрованном виде, идея заключается в зашифровании подписи, основанной на сертификате ключа подписи участника, и добавлении одноразовой подписи, ключ для которой связан с ключом из сертификата. Связка может быть:
  - Декларативной: подписывающий создает одноразовую ключевую пару независимо от изначальной и регистрирует её у участника,
  - Криптографической: одноразовая ключевая пара формируется на основе изначальной посредством односторонней функции с секретом.

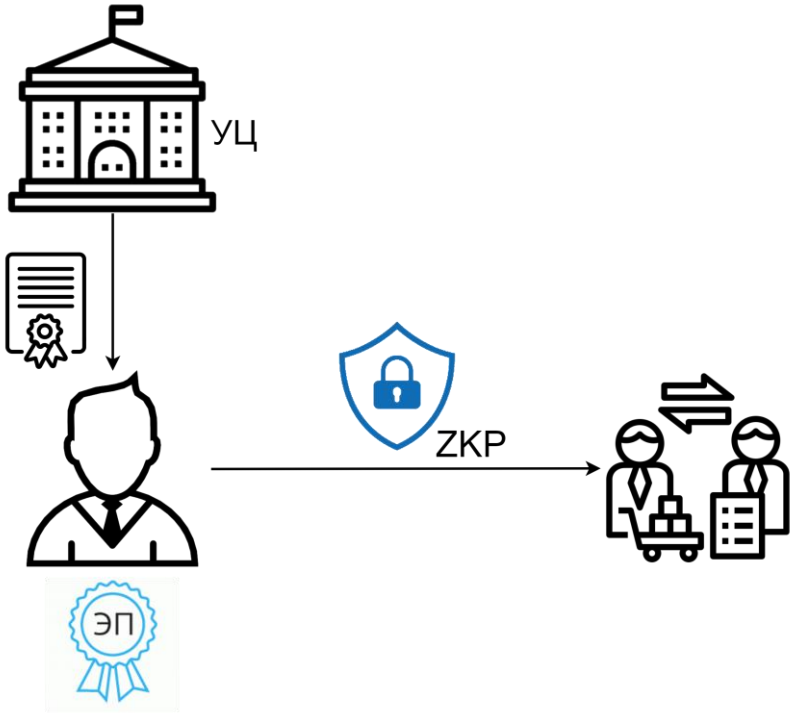


I. Свойства информационного взаимодействия

КРИПТОНИТ

Конфиденциальность подписи

- Если такого участника нет, в работах используется механизм доказательства знания подписи (Proof of Knowledge of Signature). ЭП выполняет роль аутентификационных данных, выдаваемых участникам с целью их последующей аутентификации. Для защиты от атак кражи личности, выдаваемая ЭП должна быть скрыта, её проверка осуществляется посредством протокола с нулевым разглашением.

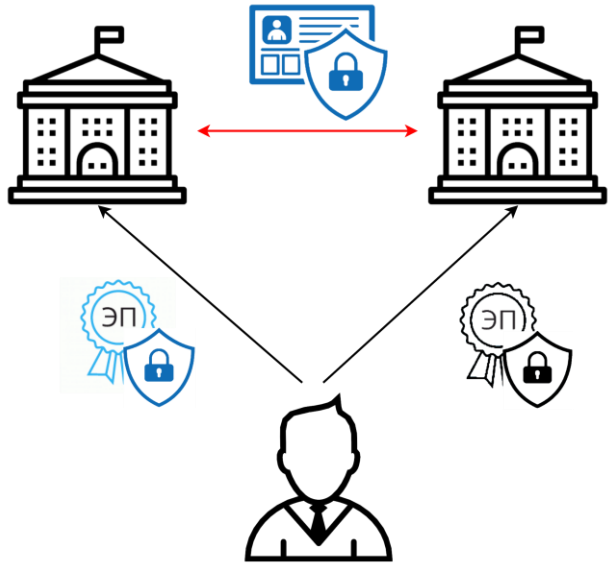


I. Свойства информационного взаимодействия

КРИПТОНИТ

Несвязываемость

- Обеспечение конфиденциальности подписи обеспечивает несвязываемость подписывающего со стороны проверяющего.
- При наличии на этапе аутентификации участника, получающего подпись в открытом виде, существуют решения только с предварительной регистрацией и последующим независимым от участника доказательством знания аутентификационных данных, полученных при регистрации. Участник не должен иметь возможности связывать факт регистрации с фактом аутентификации. Однако ему будет доступно связывание двух и более фактов аутентификации с одной неизвестной ему сущностью.



I. Свойства информационного взаимодействия

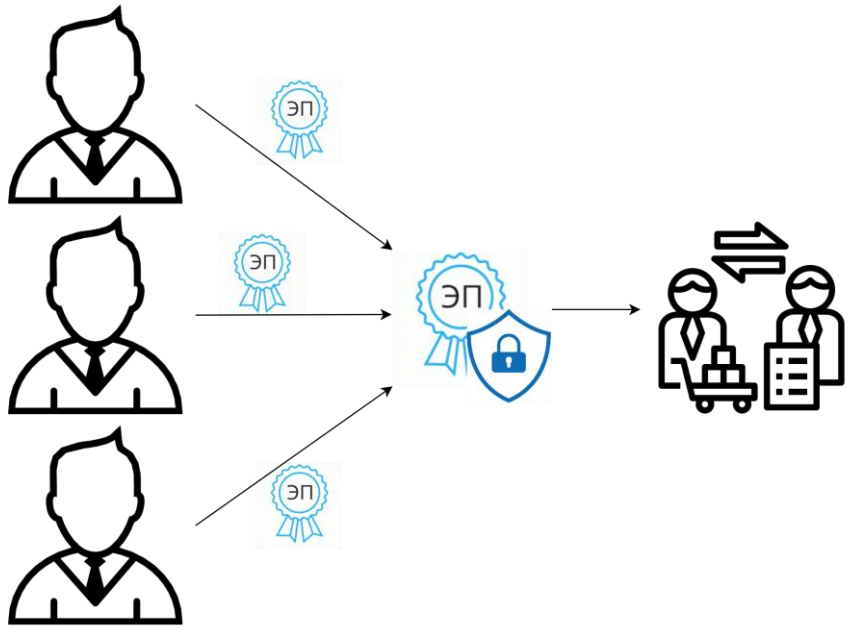
КРИПТОНИТ

Количество участников

Рассматривается ситуация, когда для одного сообщения требуется подпись от нескольких участников.

Можно выделить два основных подхода:

1. Каждый участник независимо подписывает сообщение, формируется массив ЭП.
2. Выполняется агрегация подписей. Формируется единая ЭП, которая проходит проверку только на заданном наборе сертификатов открытых ключей подписи.

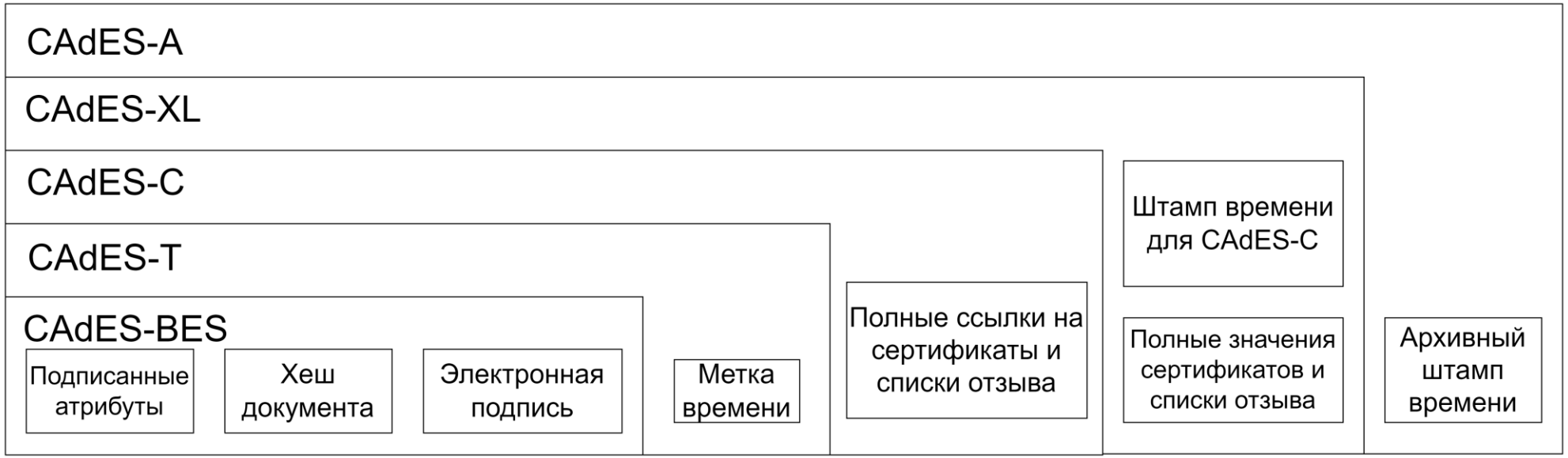


II. Свойства передаваемых данных

КРИПТОНИТ

Атрибут добавляется к подписываемому сообщению.

Если на этапе аутентификации есть участник, отвечающий за формирование и обработку атрибута, то подпись участника определяет корректность атрибута. Если подпись валидна, то атрибут корректен. Если подпись не валидна или отсутствует, значит атрибут не прошел проверку.



II. Свойства передаваемых данных

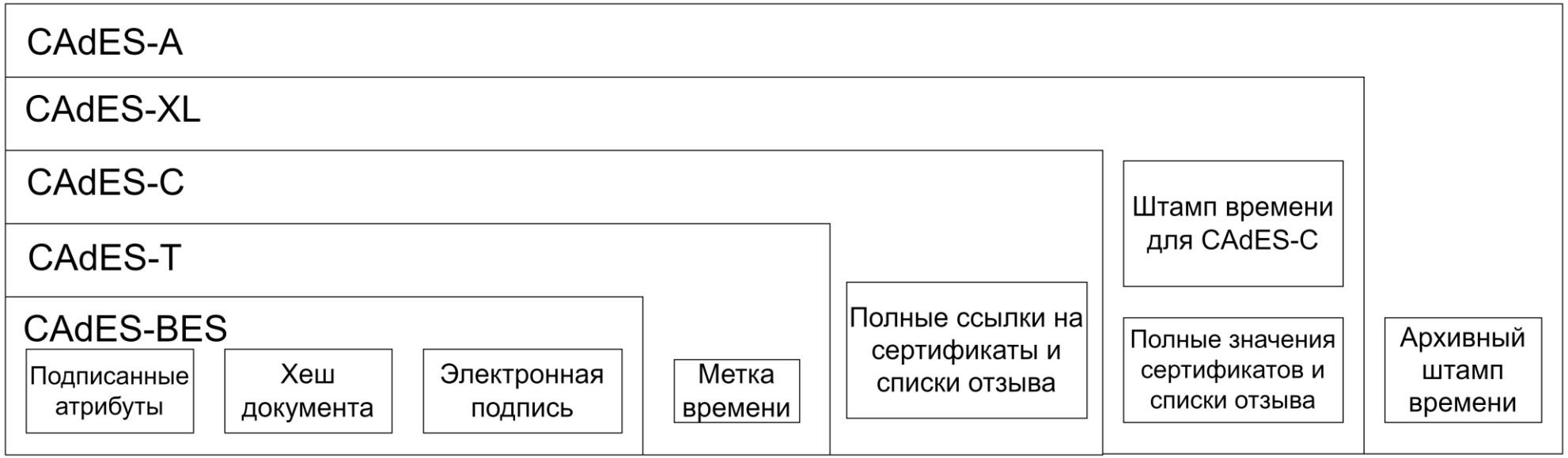
КРИПТОНИТ

Атрибут добавляется к подписываемому сообщению.

Если такой участник отсутствует, то подписывающий и проверяющий договариваются об алгоритме проверки атрибута. Информация об алгоритме проверки (его идентификатор) указывается вместе с атрибутом в подписываемом сообщении. В таком случае валидность атрибута определяется:

1. ЭП подписывающего участника, передающего сообщение,

2. ЭП проверяющего участника. Проверка ЭП проверяющего участника включается в выполнение алгоритма проверки корректности атрибута и проверки подписи ЭП.



Криптографические механизмы

КРИПТОНИТ

Свойство	Тип	Участие ДТС на этапе аутентификации	Дополнительные к ГОСТ 34.10 криптографические механизмы	Проработанность подхода
Добавление атрибута	II. Свойство передаваемых данных	Имеется	Р 50.1.113–2016	Реализовано в усовершенствованной ЭП*, ПЦД ПД**.
		Отсутствует	Внесение идентификатора алгоритма проверки атрибута в сообщение.	Реализовано в W3C VC*** пока что в статусе драфта.

*Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES). ETSI TS 101 733 V1.8.3 (2011-01). European Telecommunications Standards Institute. 2011. [электронный ресурс] URL: https://www.cryptopro.ru/sites/default/files/products/tsp/ts_101733v010803p.pdf

**Бельский, В. С., Герасимов, И. Ю., Царегородцев, К. Д., Чижов, И. В. Протокол обмена персональными данными: ИКС // International Journal of Open Information Technologies. – 2020. – Т. 8. – №. 6. – С. 1-23.

***Sporny M., Longley D., Chadwick D., Steele O. Verifiable Credentials Data Model v2.0 // White paper. – The World Wide Web Consortium. – 2024

Криптографические механизмы

КРИПТОНИТ

Свойство	Тип	Участие ДТС на этапе аутентификации	Дополнительные к ГОСТ 34.10 криптографические механизмы	Проработанность подхода
Конфиденциальность данных	I. Свойство информационного взаимодействия	Имеется	ГОСТ 34.12, Р 50.1.113–2016	Реализовано в ПЦД ПД.
		Отсутствует	Протокол с нулевым разглашением	Реализовано в ПТК ДЭГ. Требует стандартизации.
Конфиденциальность подписи	I. Свойство информационного взаимодействия	Имеется	ГОСТ 34.12, Р 50.1.113–2016, Механизм одноразовой подписи	Имеются решения, необходим полноценный криптоанализ. Уже существуют опубликованные результаты по анализу стойкости криптографической связки одноразовой пары ключей с изначальной.
		Отсутствует	Протокол с нулевым разглашением подписи	Требует криптографического анализа. Применяется в алгоритмах ЭП*, использующих билинейный невырожденный гомоморфизм.

*Camenisch J., Kiayias A., Yung M. On the portability of generalized schnorr proofs // Annual International Conference on the Theory and Applications of Cryptographic Techniques. – Berlin, Heidelberg : Springer Berlin Heidelberg, 2009. – С. 425-442.

Криптографические механизмы

КРИПТОНИТ

Свойство	Тип	Участие ДТС на этапе аутентификации	Дополнительные к ГОСТ 34.10 криптографические механизмы	Проработанность подхода
Несвязываемость	I. Свойство информационного взаимодействия	Имеется	Алгоритмы слепой подписи	Реализовано в ПТК ДЭГ в рамках регистрации субъекта. Открыта задача обеспечения несвязываемости со стороны ДТС обращений от одного неизвестного субъекта.
			Протокол с нулевым разглашением	Использует билинейный невырожденный гомоморфизм*, стойкость обращения которого имеет субэкспоненциальную сложность и основана на стойкости задачи DH на множестве эллиптических кривых специального вида**.
		Отсутствует	Не определены	Не имеет проработанного подхода.

*Au M. H., Susilo W., Mu Y. Constant-size dynamic k-TAA // Security and Cryptography for Networks: 5th International Conference, SCN 2006, Maiori, Italy, September 6-8, 2006. Proceedings 5. – Springer Berlin Heidelberg, 2006. – С. 111-125.

**Galbraith S., Hess F., Vercauteren F. Aspects of pairing inversion // IEEE Transactions on Information Theory. – 2008. – Т. 54. – №. 12. – С. 5719-5728.

Криптографические механизмы

КРИПТОНИТ

Свойство	Тип	Участие ДТС на этапе аутентификации	Дополнительные к ГОСТ 34.10 криптографические механизмы	Проработанность подхода
Агрегация подписей	I. Свойство информационного взаимодействия	Независимо	Последовательное добавление подписей	Реализовано в PKI.
			Гомоморфизм подписей	Агрегирование подписей посредством сложения открытого ключа в классической ЭП ГОСТ 34.10 не является стойким в модели угрозы подделки подписи для нового сообщения.
				Использует билинейный невырожденный гомоморфизм* **.

*Au M. H., Susilo W., Mu Y. Constant-size dynamic k-TAA // Security and Cryptography for Networks: 5th International Conference, SCN 2006, Maiori, Italy, September 6-8, 2006. Proceedings 5. – Springer Berlin Heidelberg, 2006. – С. 111-125.

**Galbraith S., Hess F., Vercauteren F. Aspects of pairing inversion // IEEE Transactions on Information Theory. – 2008. – Т. 54. – №. 12. – С. 5719-5728.

Итоговое обобщение подходов к обеспечению дополнительных свойств.

Необходимо продолжить стандартизацию таких механизмов как протоколы формирования и проверки электронной подписи вслепую

Начинать стандартизацию криптографических механизмов обеспечения анонимности, таких как протоколы с нулевым разглашением, с использованием отечественных криптографических механизмов и учетом наработанной практики в части многостороннего взаимодействия.

КРИПТОНИТ

Определить требования и возможности

Разбить требования на две составляющие:

1. Требования к взаимодействию,
2. Требования к передаваемым данным.

Определить модель

Выбрать частную модель АИ с учетом наличия ДТС, порядка взаимодействия и функционала.

Определить алгоритмы

ГОСТ 34.10 как основа ЭП.

ГОСТ 34.12, Р 50.1.113–2016 как средства обеспечения конфиденциальности и обработки атрибутов.

Методы обеспечения несвязываемости, а также свойств при отсутствии участия ДТС на этапе аутентификации требуют отдельного криптоанализа и проработки.

Спасибо за внимание!

Контактные данные:

i.gerasimov@kryptonite.ru
v.belsky@kryptonite.ru

КРИПТОНИТ