



Как установить подлинность медиа-контента и не облажаться

20 ноября 2023



Кузьмичева Ольга

Разработчик встраиваемых систем



Стародубцев Дмитрий

Разработчик встраиваемых систем

А причем тут мы?



Мы занимались

Настройкой библиотеки
для встраиваемых устройств



Нам было важно

Чтобы устройство могло фиксировать
подлинность произведенного контента

Подлинный медиаконтент (изображение, видео, аудио)

Можно доказать

- Авторство
- Дату и время создания
- Содержимое контента не менялось с момента создания

Дезинформация

Ложная или вводящая в заблуждение информация, которая распространяется с намерением обмануть, манипулировать или создать путаницу.



Пример 1

Сотрудник безопасности

Я хочу иметь доказательство
оригинальности видеозаписи
события.



Пример 2

Репортер

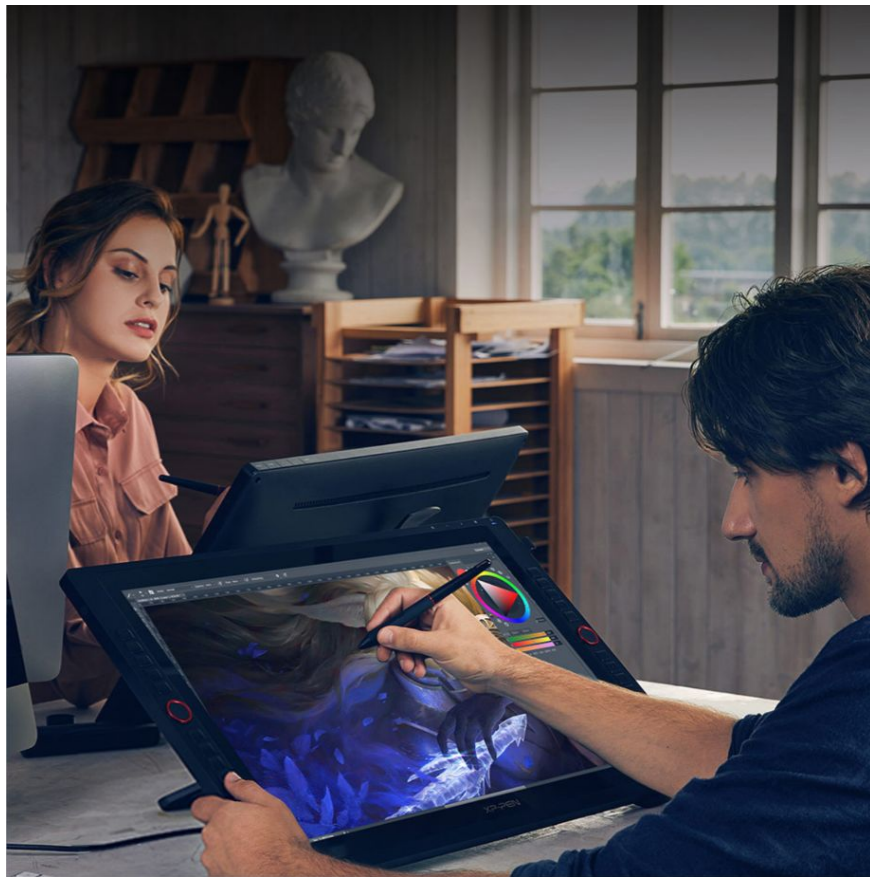
Мне важно доказать, что события, которые происходили у меня на глазах, были именно такими, какими я их видел.



Пример 3

Создатель контента

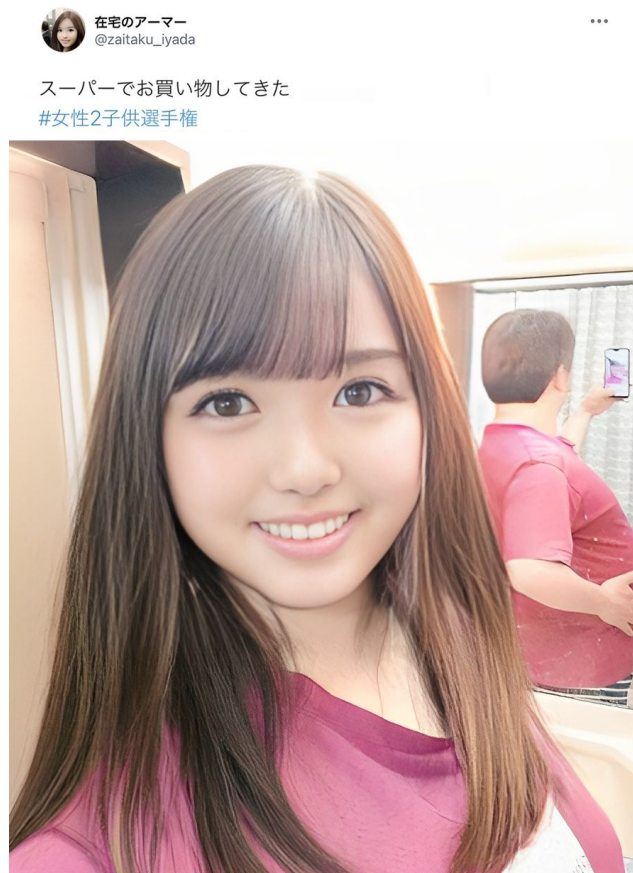
Я хочу делиться своей работой
с миром, при этом сохранив
за собой авторство.



Пример 4

Пользователь соц. сетей

Я хочу понимать, какая информация реальна, а какая – подделка.



Инструменты для обеспечения подлинности данных

Блокчейн

- NFT

Цифровой отпечаток

- Youtube Content ID
- Facebook Rights Manager
- Twitch Soundtrack

C2PA

- Content Credentials

Важные для нас критерии

1. Запуск на устройствах
2. Установление подлинности контента
3. Установление авторства
4. Поддержка различных форматов данных:
фото, видео, аудио
5. Возможность верифицировать изменения

Блокчейн

Децентрализованная и неизменяемая технология реестра, используемая для проверки подлинности контента.



Блокчейн

Плюсы

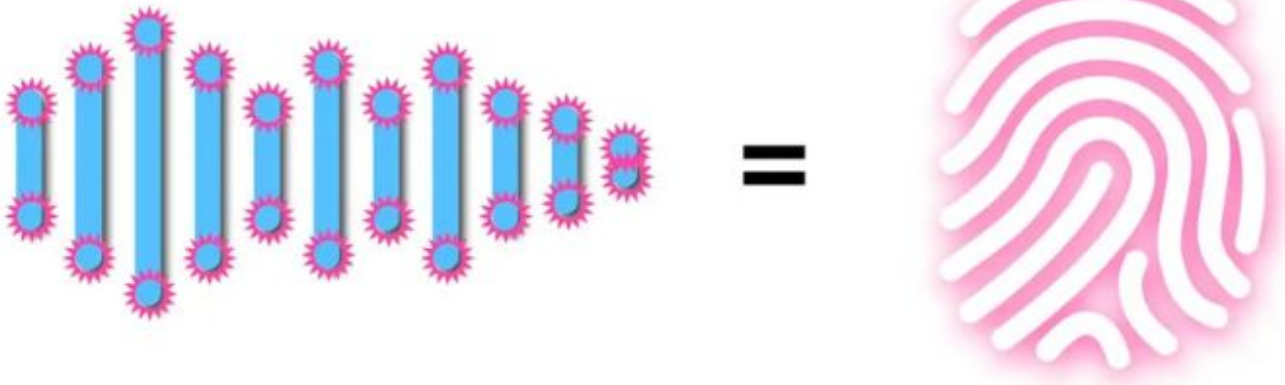
- Подтверждает подлинность и авторство
- Любой человек, обладающий крипто-кошельком, может использовать

Минусы

- Подпись при загрузке в сеть, а не при создании контента
- Платно

Цифровой отпечаток

Технология, создающая уникальный идентификатор или подпись, созданную на основе конкретных характеристик части цифрового контента.



Цифровой отпечаток

Плюсы

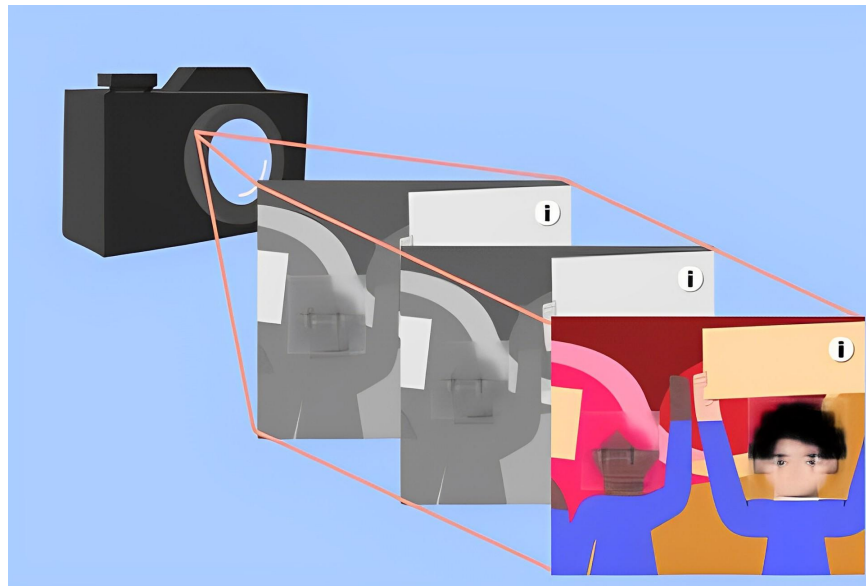
- Подтверждает подлинность и авторство
- Может находить похожий контент на основе оригинального

Минусы

- Нет поддержки верификации изменений
- Не общедоступно

C2PA

Стандарт, использующий метаданные и криптографические методы для предоставления проверяемой информации о происхождении, истории и модификациях части контента.



C2PA












Плюсы

- Открытый стандарт, имеющий opensource реализации
- Подтверждает подлинность и авторство
- Поддерживает верификацию изменений

Минусы

- Не распространен
- Только начинает развиваться (поддержка стримов)

ИТОГИ

	Блокчейн	Цифровой отпечаток	C2PA
Запуск на устройствах			
Установление подлинности контента			
Установление авторства			
Поддержка различных форматов данных: фото, видео, аудио			
Возможность верифицировать изменения			

Кто занимается созданием стандарта?

CAI (Content Authenticity Initiative) - коллаборация организаций, разработчиков, активистов.

в 2019 году

основана Adobe

>100

участников



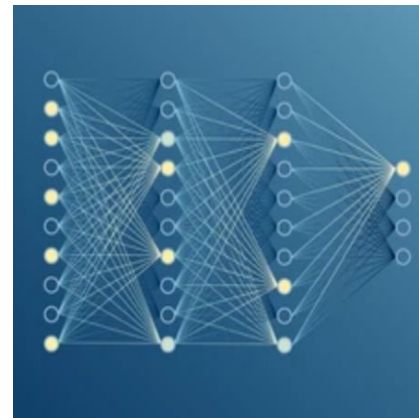
Каким разработчикам будет интересно?



Разработчики
фото/видео устройств



Разработчики
фото/видео редакторов



Разработчики
генеративных
нейронных сетей

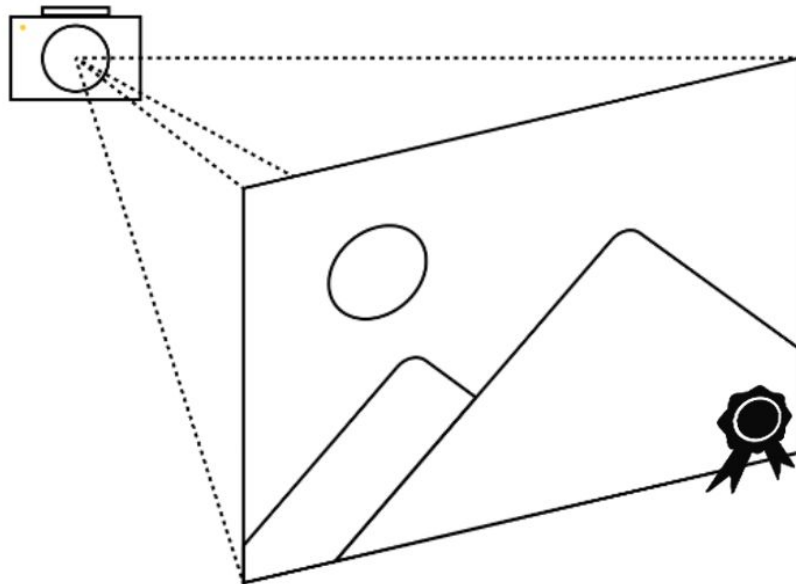
**суть
стандарта**

1

Создание

При создании медиаконтента через девайс или редактор, создаются метаданные об авторе, дате и времени создания.

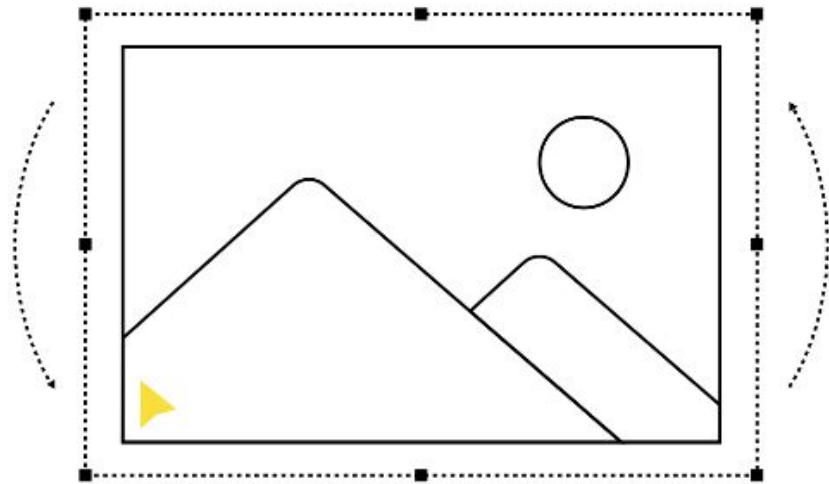
Далее, с помощью хэширования и цифровой подписи, контент “упаковывается и запечатывается”.



2

Изменение

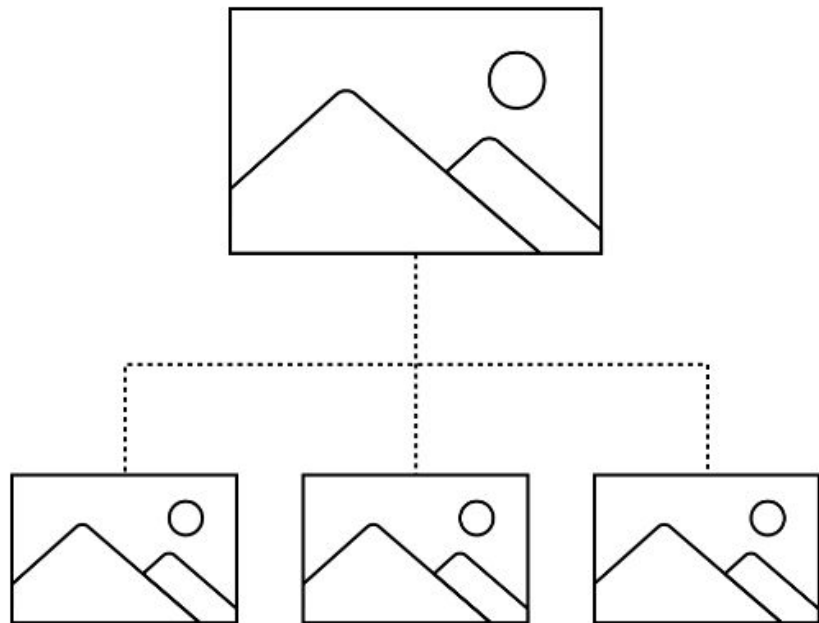
Редакторы (например, Photoshop),
позволяют внести достоверные
изменения.



3

Публикация

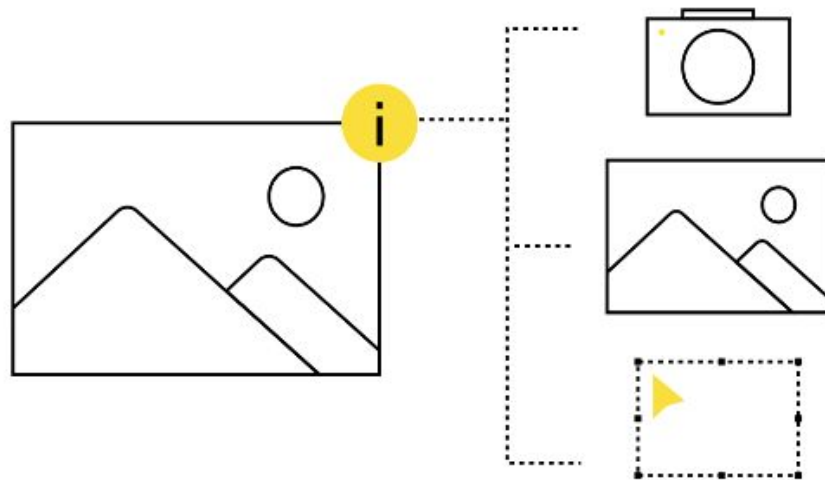
Социальные сети и публичные страницы, сохраняют информацию о достоверности контента при его передаче.



4

Просмотр

Верификаторы позволяют просмотреть информацию о достоверности контента, а также историю изменений.



Выберите другой файл на своем устройстве или перетащите куда угодно



Поиск возможных совпадений



Sep 24, 2023



Jun 18, 2023

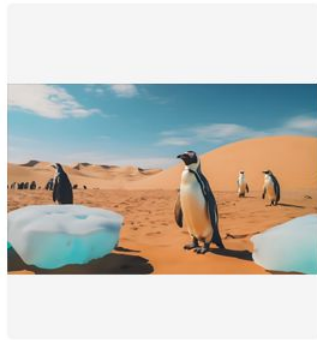


Oct 1, 2023



Oct 4, 2023

5 окт. 2023 г.



Сводная информация о контенте

Это изображение состоит из нескольких фрагментов контента, минимум один из которых сгенерирован с помощью инструмента или алгоритма на основе ИИ.

Благодарность и использование

Автор поделился следующей информацией:

Кем создано

obidigbo nzeribe

Учетные записи в социальных сетях

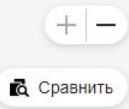
obidinzeribe
Instagram

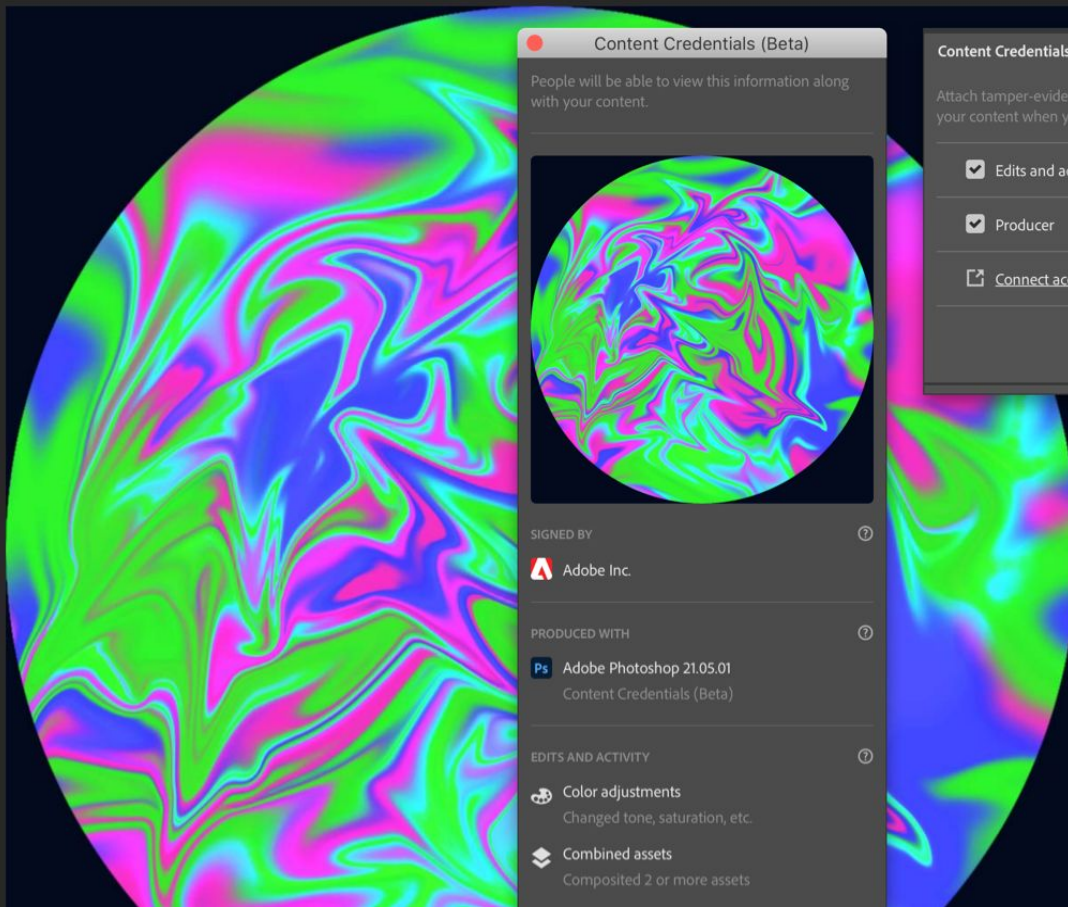
obidigbo nzeribe
Behance

25/64



<https://contentcredentials.org/verify>





Content Credentials (Beta)

People will be able to view this information along with your content.



SIGNED BY

 Adobe Inc.

PRODUCED WITH

 Adobe Photoshop 21.05.01
Content Credentials (Beta)

EDITS AND ACTIVITY

-  Color adjustments
Changed tone, saturation, etc.
-  Combined assets
Composited 2 or more assets

Content Credentials (Beta)

Attach tamper-evident attribution and history data to your content when you export it.

- Edits and activity
- Producer
- Connect accounts





Preview

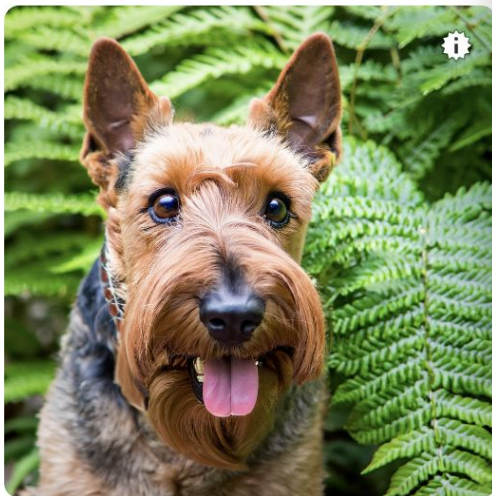
Color Swatches



Layers Channels Paths

Kind Normal Opacity: 100% Lock: Fill: 100%

-  Curves 1
-  Hue/Saturation 1
-  Color Fill 1
-  Background



Content Credentials



 Adobe Inc.
20/03/2023, 23:27

Content summary

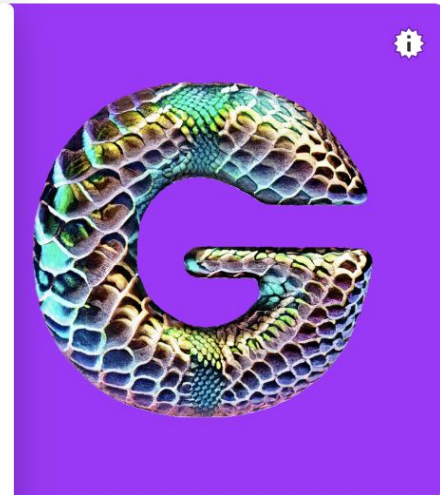
 This content was generated with an AI tool.

Process

PRODUCED WITH

 Adobe Firefly 1.0

View more





PREVIEW



a close-up photo for a new gaming avatar that is a spaceship pilot with brown hair putting on a helmet

Bing Image Creator | 1024 x 1024 png | Created now

- [Share](#)
- [Save](#)
- [Download](#)
- [Feedback](#)


Content credentials


Generated with AI · Sept 21, 2023 at 11:11am








Other people will be able to view this info with your content



SIGNED BY
 Adobe Inc.

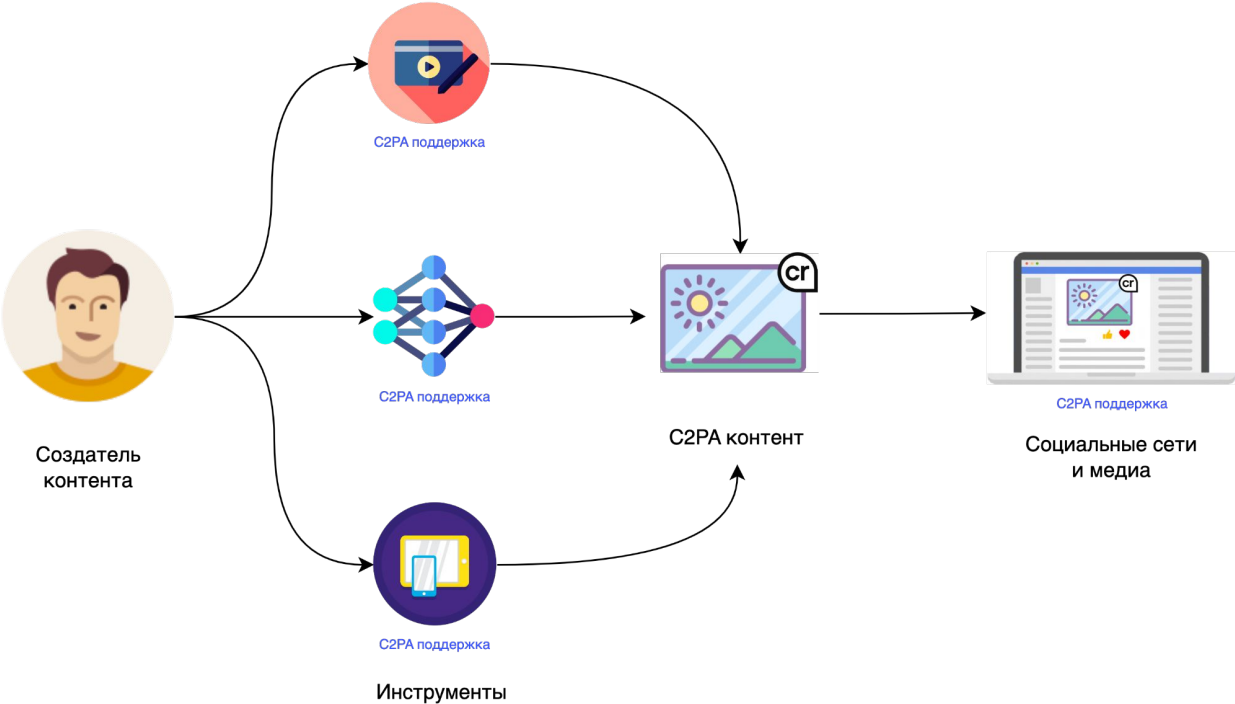
PRODUCED WITH
 Adobe Photoshop 23.51
Content Credentials (Beta)

EDITS AND ACTIVITY
 Imported assets
Added Images, videos, etc.

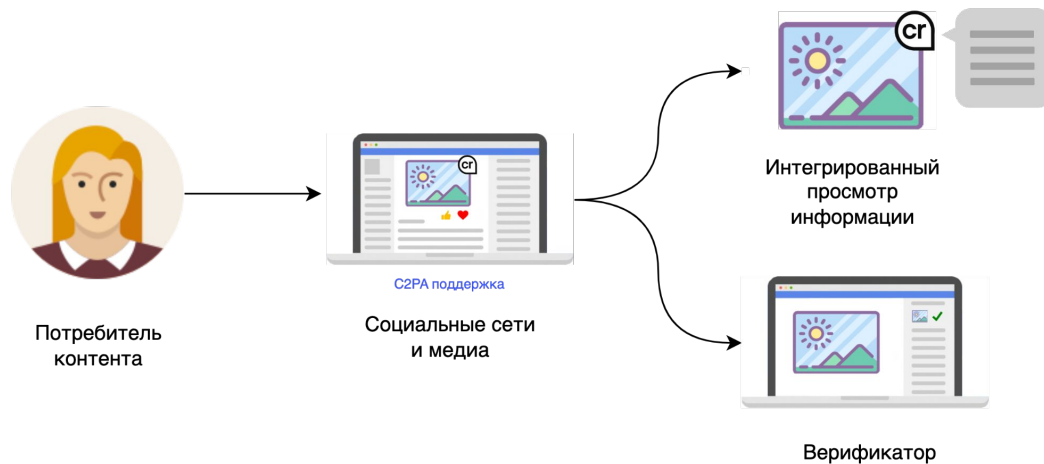
ASSETS USED


PRODUCED BY
Hannah Darby

C2PA глазами создателей контента



C2PA глазами потребителей контента



Open-source продукты

Библиотеки

c2pa-js

JavaScript библиотека для верификации

c2pa-node

Node.js библиотека для подписи
и верификации

c2pa-rs

Rust библиотека для подписи
и верификации

Приложения

Verify.contentauthenticity.org

Сайт для верификации

c2patool

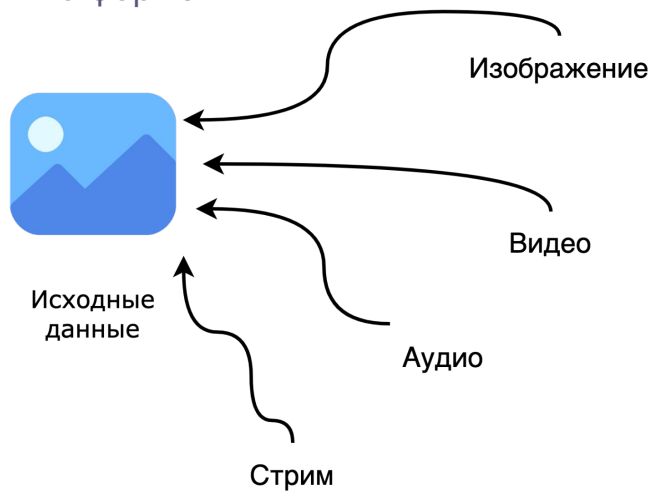
Консольное приложение
для подписи и верификации

Как C2PA защищает данные?

Исходные данные

Форматы метаданных

- 1) JUMBF
- 2) ISO-BMFF
- 3) Еще какой-то формат



Хэширование

Последовательность
шестнадцатеричных чисел
длиной в 32 - 64 байт



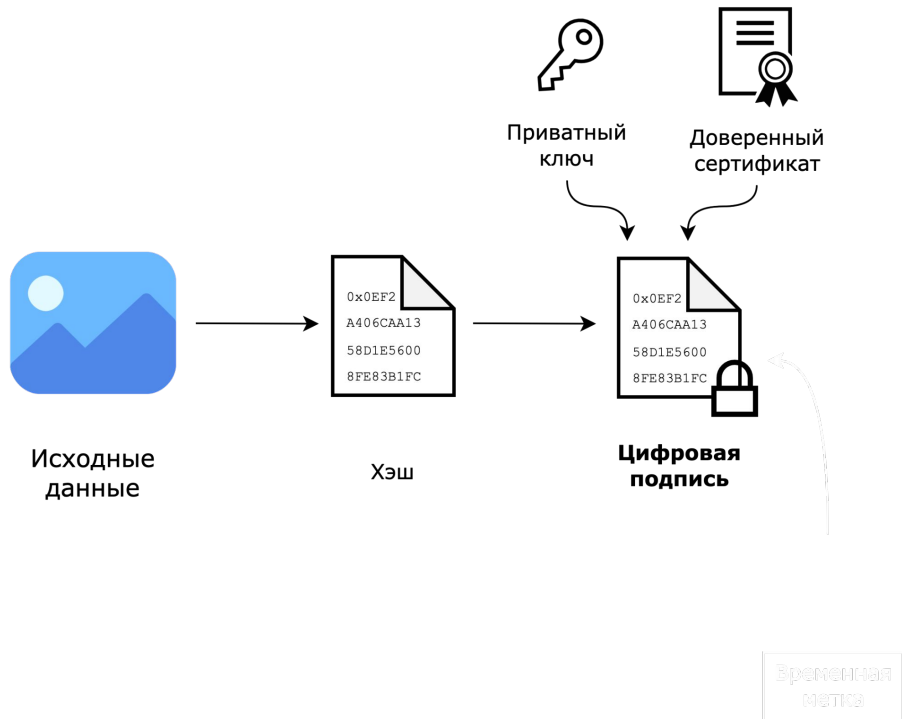
Исходные
данные



Хэш

Цифровая подпись

Подтверждает подлинность
данных



Приватный ключ и сертификат

Используется
для зашифровки данных

Хранится в **безопасном** месте

- Облако
- Персональный компьютер
- Устройство



Приватный
ключ



Доверенный
сертификат

Используется для
расшифровки данных

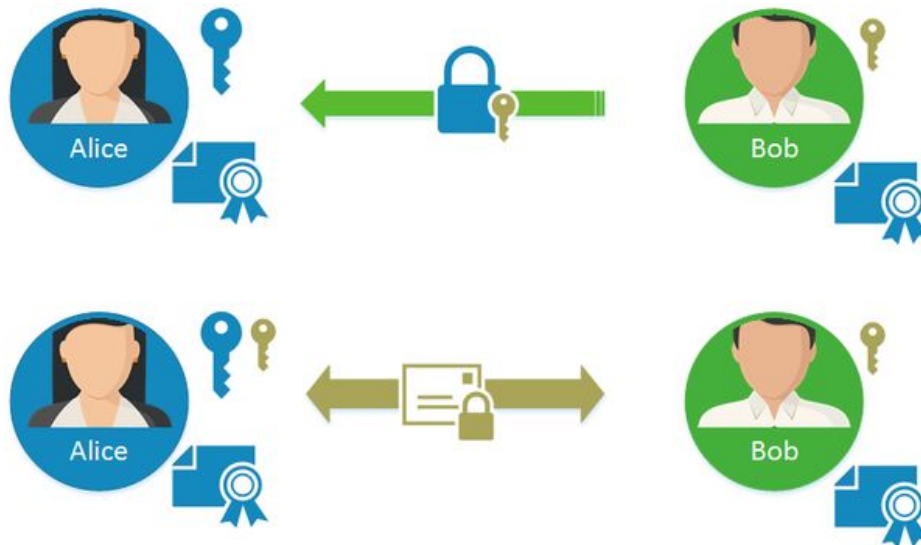
Публично доступный
документ

Выдается доверенным
источником

Асимметричное шифрование

Примеры использования

- Идентификация пользователей
- Установление защищенной сессии передачи данных (HTTPS)



Данным доверяют настолько, насколько доверяют сертификату

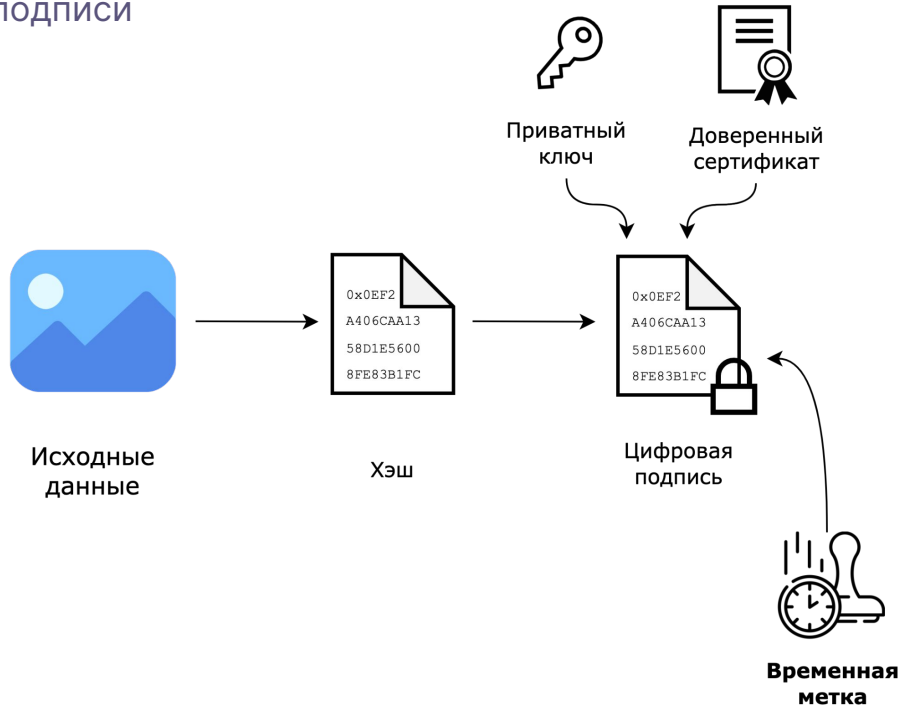
- Приватный ключ украден
- Изменились персональные данные
- Центр сертификации закрылся



Сертификат
отзывается

Временная метка

Подтверждает время создания
цифровой подписи

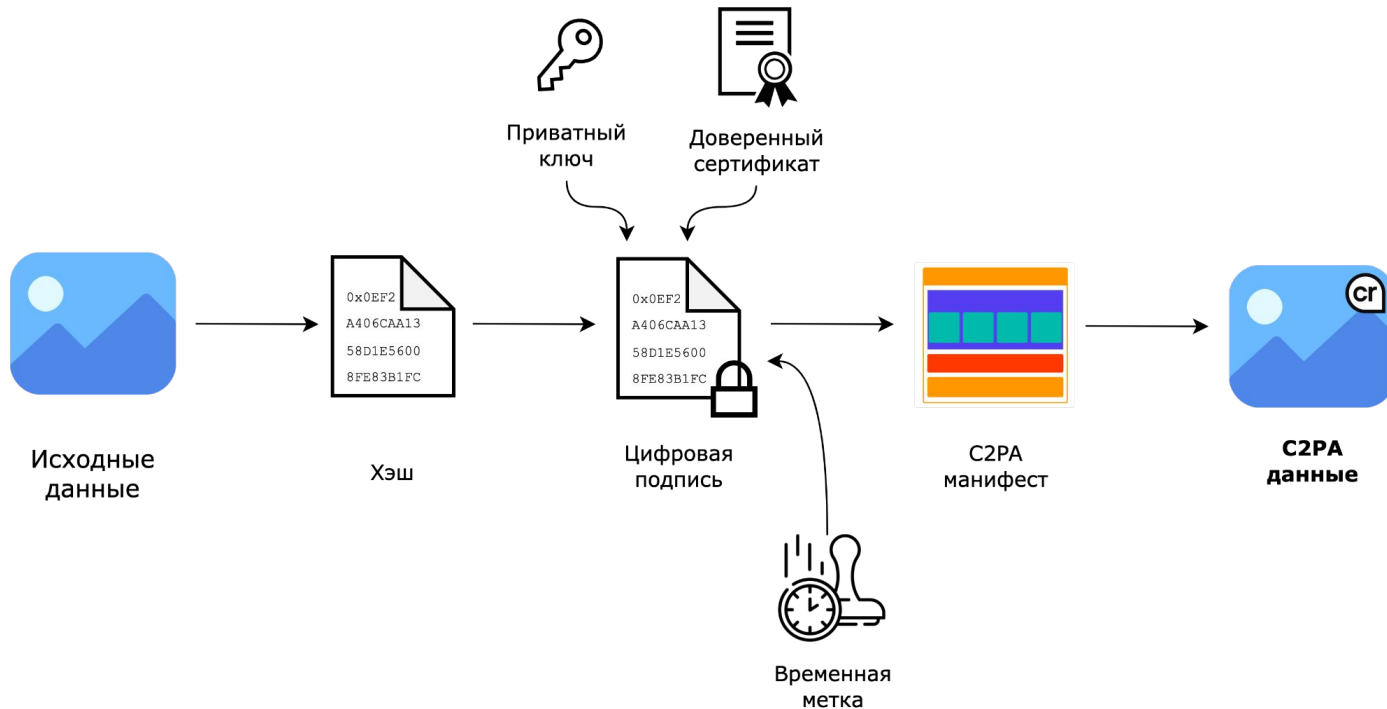


C2PA манифест

Объединяет в себе цифровую подпись и полезную информацию



Подлинный контент



Как C2PA хранит данные?

C2PA Manifest

Полный набор информации

Claim Signature

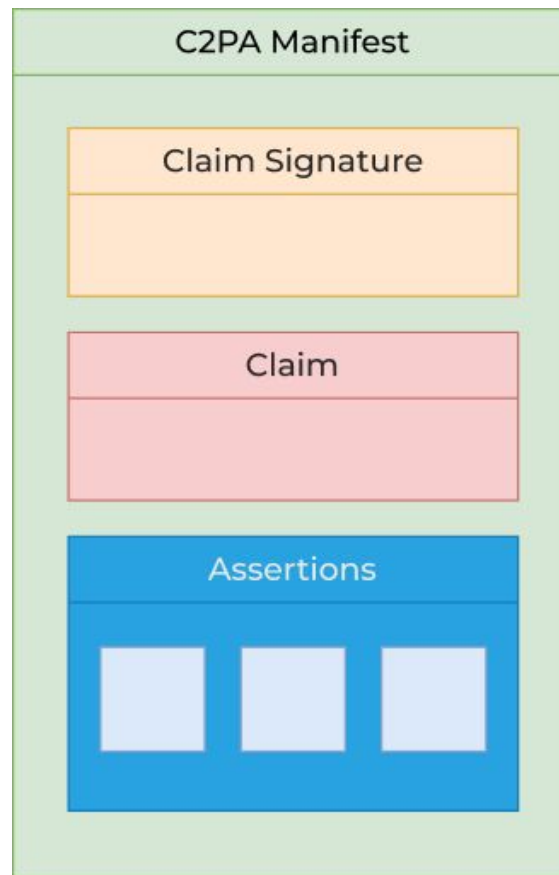
Цифровая подпись Claim

Claim

Детали полезной информации

Assertions

Полезная информация



Assertions

- Информация об авторе
- Метаданные
- Действия, совершенные над контентом
- Характеристики контента (хэш и пр.)

Copyright © 2017 Masha. All Rights Reserved

АНКЕТА

Друзья делают нашу жизнь лучше! У тебя есть лучший друг или лучшая подруга? Дай ему или ей заполнить эту анкету.

Имя: _____

Возраст: _____

Животные: _____

Хобби: _____

Таланты: _____

Ваши отличия: _____

Почему вы дружите? _____

Опиши себя одним словом: _____



3

razki-razki-razhki.blogspot.com

Claim

- алгоритм хеширования
- генератор Claim
- ссылка на цифровую подпись
- формат
- список Assertions



Claim Signature

- цепочка сертификации
- цифровая подпись
- временная метка



Manifest

Объединяет
всю информацию



Какие данные сейчас поддерживаются

- Текст (PDF)
- Изображения (JPEG, PNG, SVG, WebP, AVIF, HEIC, HEIF, TIFF, DNG)
- Видео (MP4, AVI, MOV)
- Аудио (MP3, M4A, WAV)
- Стримы

MPEG-4

Что подписывается?

- видео целиком
- группы кадров
- каждый кадр

Куда встраивается манифест?

- между заголовками видео (ftyp) и данными видео (mdat)
- хранится внешне

MPEG-4

```
00 00 00 20 66 74 79 70 69 73 6F 6D 00 00 02 00 ... ftypisom...
69 73 6F 6D 69 73 6F 32 61 76 63 31 6D 70 34 31 isomiso2avc1mp41
00 00 3A E8 75 75 69 64 D8 FE C3 D6 1B 0E 48 3C ...:æuuid+...H<
92 97 58 28 87 7E C4 81 00 00 00 00 6D 61 6E 69 ÅùX(ç~ü...mani
66 65 73 74 00 00 00 00 00 00 00 00 00 00 3A fest.....:
BB 6A 75 6D 62 00 00 00 1E 6A 75 6D 64 63 32 70 ¶jumb...jumdc2p
61 00 11 00 10 80 00 00 AA 00 38 9B 71 03 63 32 a....Ç..-.8çq.c2
70 61 00 00 00 3A 95 6A 75 6D 62 00 00 00 47 6A pa...:òjumb...Gj
75 6D 64 63 32 6D 61 00 11 00 10 80 00 00 AA 00 umdc2ma....Ç..-.
38 9B 71 03 75 72 6E 3A 75 75 69 64 3A 32 34 65 8çq.urn:uuid:24e
62 63 32 34 62 2D 64 39 33 30 2D 34 35 63 36 2D bc24b-d930-45c6-
..*
AD 03 58 87 F9 06 CA 2C 00 00 00 08 66 72 65 65 ¡.Xç.⌘,....free
00 3A 21 0D 6D 64 61 74 00 00 00 0B 06 00 07 81 .:!.mdat.....ü
3C 68 00 23 28 40 80 00 00 00 08 06 01 04 00 00 <h.#(@Ç.....
08 10 80 00 01 05 C6 65 B8 04 08 FF F7 81 2D 3C ..Ç...|eç.. zü-<
BB A8 CB 1B AF F7 78 8B EE BF 46 40 D5 44 CC B2 ¶¿¶.»xîε¶F@¶D¶¶
C4 B2 6D D2 00 00 03 00 00 03 00 00 0A F2 40 C7 -¶¶.....≥@|
4C 8A 9E 30 31 D1 A4 40 24 EE BB CB 9C 74 16 98 LèP01¶ñ@§ε¶¶ft.ÿ
EF 2C 22 6D E6 39 01 08 7F 4B 04 65 2C 07 B1 D9 ς,"μ9...αK.e,·¶¶
11 92 17 78 49 1C 96 73 30 58 B7 CE 05 FB FD 6D .Æ.xI.ûs0X¶.√²m
43 32 36 34 4B F9 A2 4B 20 06 CA EB BC 83 11 94 C264K·ók.⌘⌘â.ö
45 15 1A 07 40 CC FA 23 E3 EF EB A2 21 2E 1A C6 E...@|·#πñδó!...|
..*
```

ISO-BMFF заголовок

C2PA сегмент

Байты видео

Стримы

Рассмотрим стримы как фрагментированный MPEG-4 формат

Спорные моменты

- Передача данных с C2PA
- Затраты на создание C2PA манифеста

Очевидная уязвимость C2PA



Частичное решение уязвимости

Использование временной метки



Автор: **Петров**
Дата: **1 ноября**

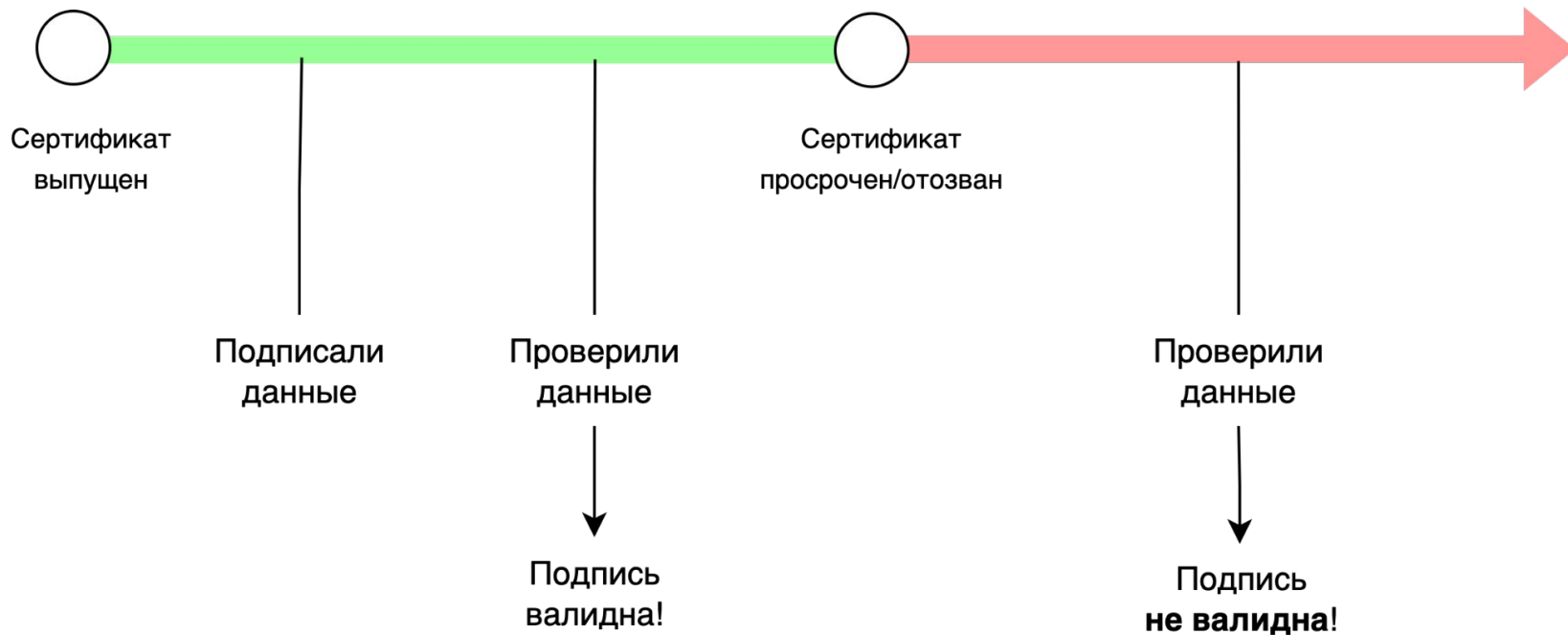
Оригинал



Автор: **Иванов**
Дата: **2 ноября**

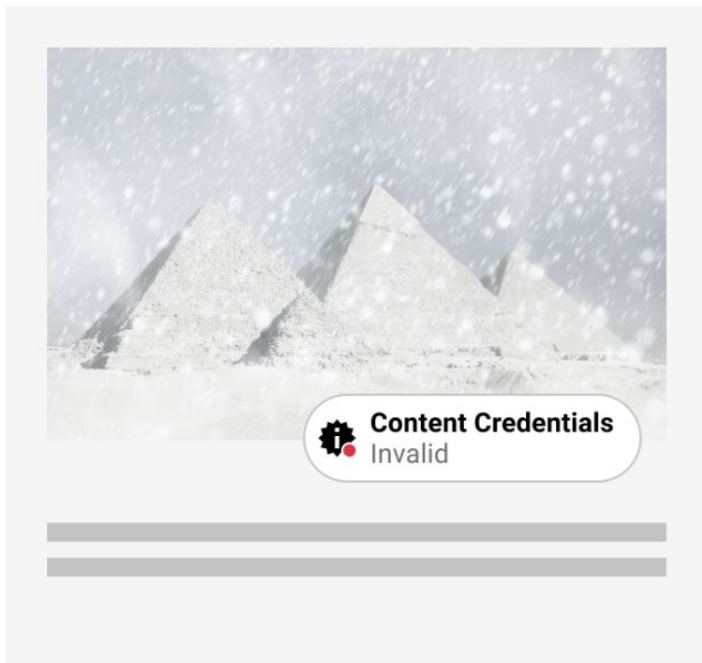
Подделка

Какие у нас были проблемы с С2РА

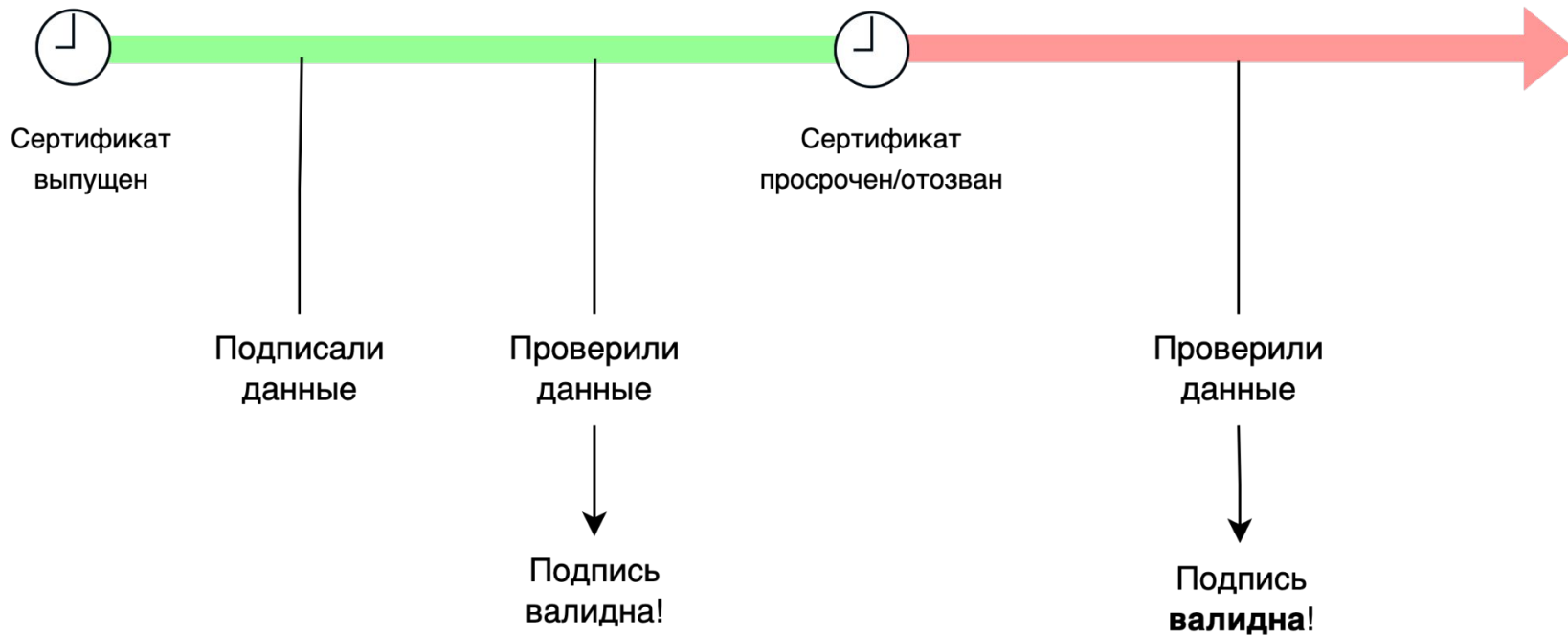


Последствие невалидной подписи

L1 with invalid active manifest



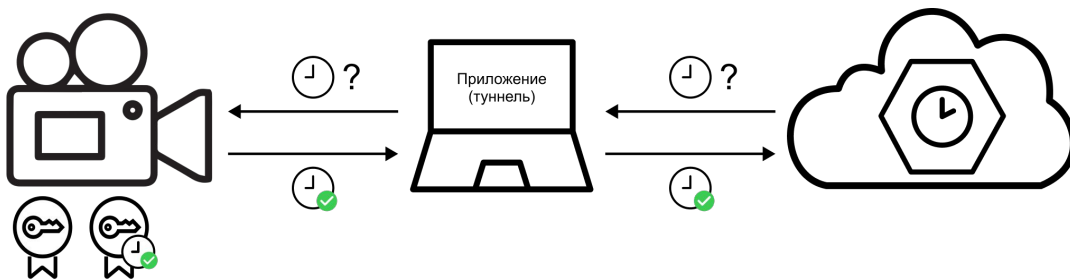
Добавим временную метку...



Временная метка на устройстве

Плюсы

- Не нужен доступ к Интернету во время создания контента
- Безопасно
- Можно проверять статус сертификата



Минусы

- Ответственность за достоверное время - на пользователе
- Ответственность за проверку статуса сертификатов на пользователе

Впечатления о работе с C2PA

- Рабочее решение
- Интересная технология
- Доступное общение с разработчиками

НО

- C2PA – это не панацея
- Есть много лазеек
- Требуется обширная поддержка сторонних приложений и сервисов

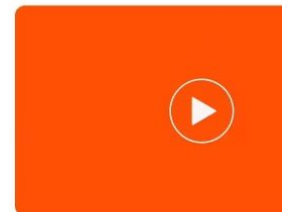
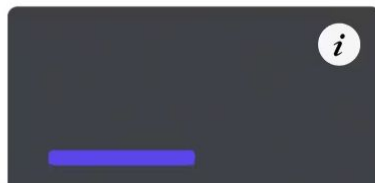
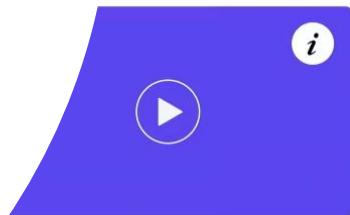
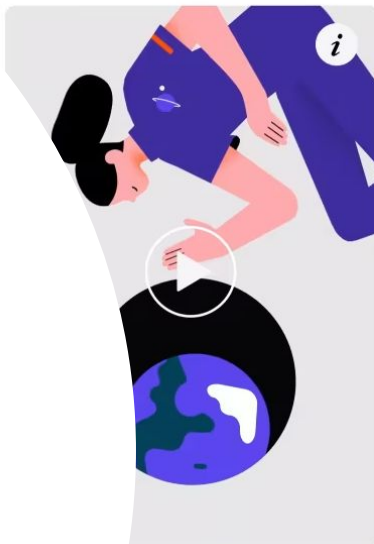
Какое будущее может быть у С2РА?

Основа защиты всего медиа пространства

C2PA используется повсеместно

- телефоны, камеры
- редакторы медиафайлов
- социальные сети

C2PA обеспечивает подлинность
медиафайлов в интернете.



Инструмент для установления авторства

C2PA используется точноно

- некоторые устройства
- популярность у создателей контента

C2PA – способ доказать авторство.



Будущее за вами!



<https://c2pa.org/>



<https://discord.gg/cai>



<https://github.com/c2pa-org>

Итоги

C2PA

Относительно
общедоступный

Относительно
универсальный

Относительно
безопасный :)

Но определенно интересный!

Спасибо за внимание!

Кузьмичева Ольга

✉ okuzmicheva@tourmalinecore.com

Стародубцев Дмитрий

✉ dstarodubtcev@tourmalinecore.com

