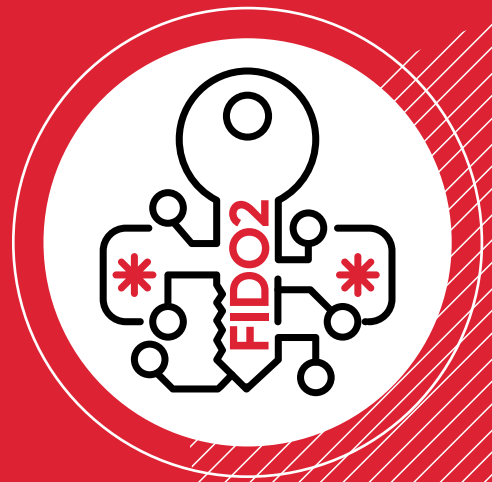
РУТОКЕН

конференция РусКрипто

Возможности применения российских криптографических алгоритмов в стандарте FIDO2

Мироненко Евгений, руководитель отдела исследований
Скоробогатова Марина, младший аналитик
Сабиров Эдуард, младший аналитик

Компания «Актив»



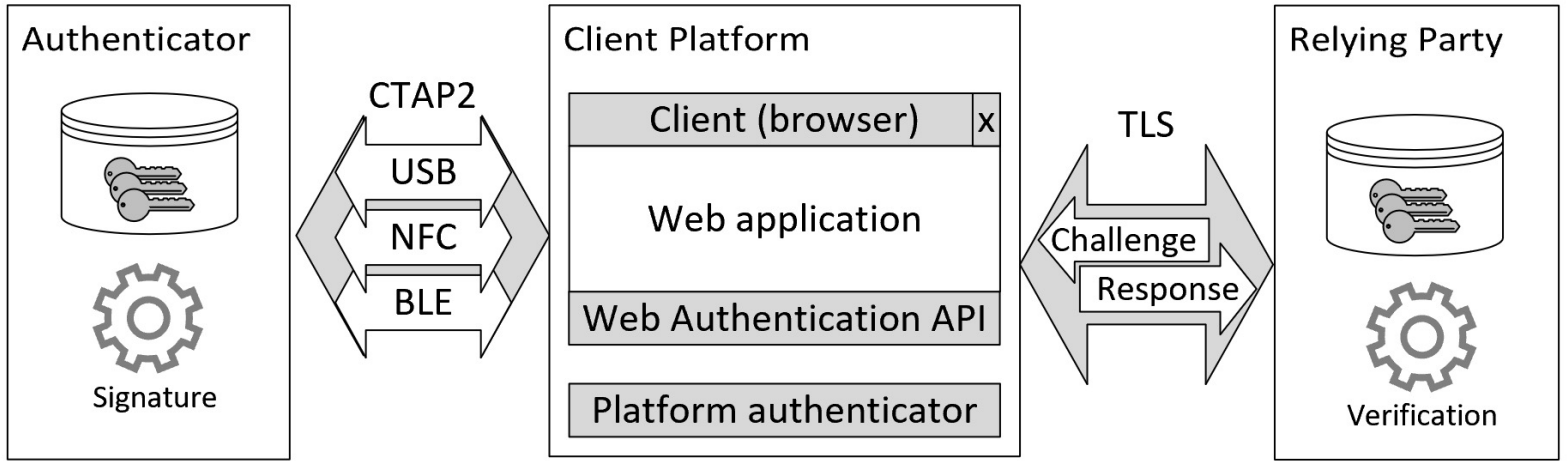
FIDO2 — аутентификация в Web

Двухфакторная беспарольная аутентификация

- Фактор владения криптографическим устройством
- Локальная аутентификация в устройство:
  - Пин-код
  - Пароль
  - Биометрия

Спецификации:

- W3C Web Authentication API (Webauthn)
- CTAP2 (Client to Authenticator Protocol)



Почему FIDO2?

Поддержка браузером

Это не криптографический плагин

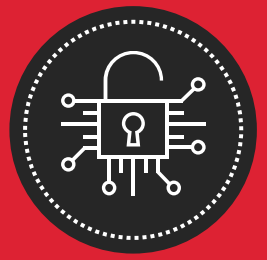
Свойства безопасности

- Противодействие фишингу, replay-атакам
- Сохранение приватности пользователя
  - Информирование пользователя о выполняемых операциях
  - Независимые учетные данные в различных системах
  - Пользователя нельзя отследить по аутентификатору

Гибкость

- Многообразие аутентификаторов
- Управление параметрами процесса аутентификации:
  - тип аутентификатора
  - тип локального фактора аутентификации
  - криптографический механизм
- Допускает расширения (например, авторизация транзакций)

Предмет исследования



Существующие интеграции FIDO2 используют зарубежную криптографию

Тренд в российской стандартизации:

- Международный технический стандарт
- Отечественные криптографические примитивы

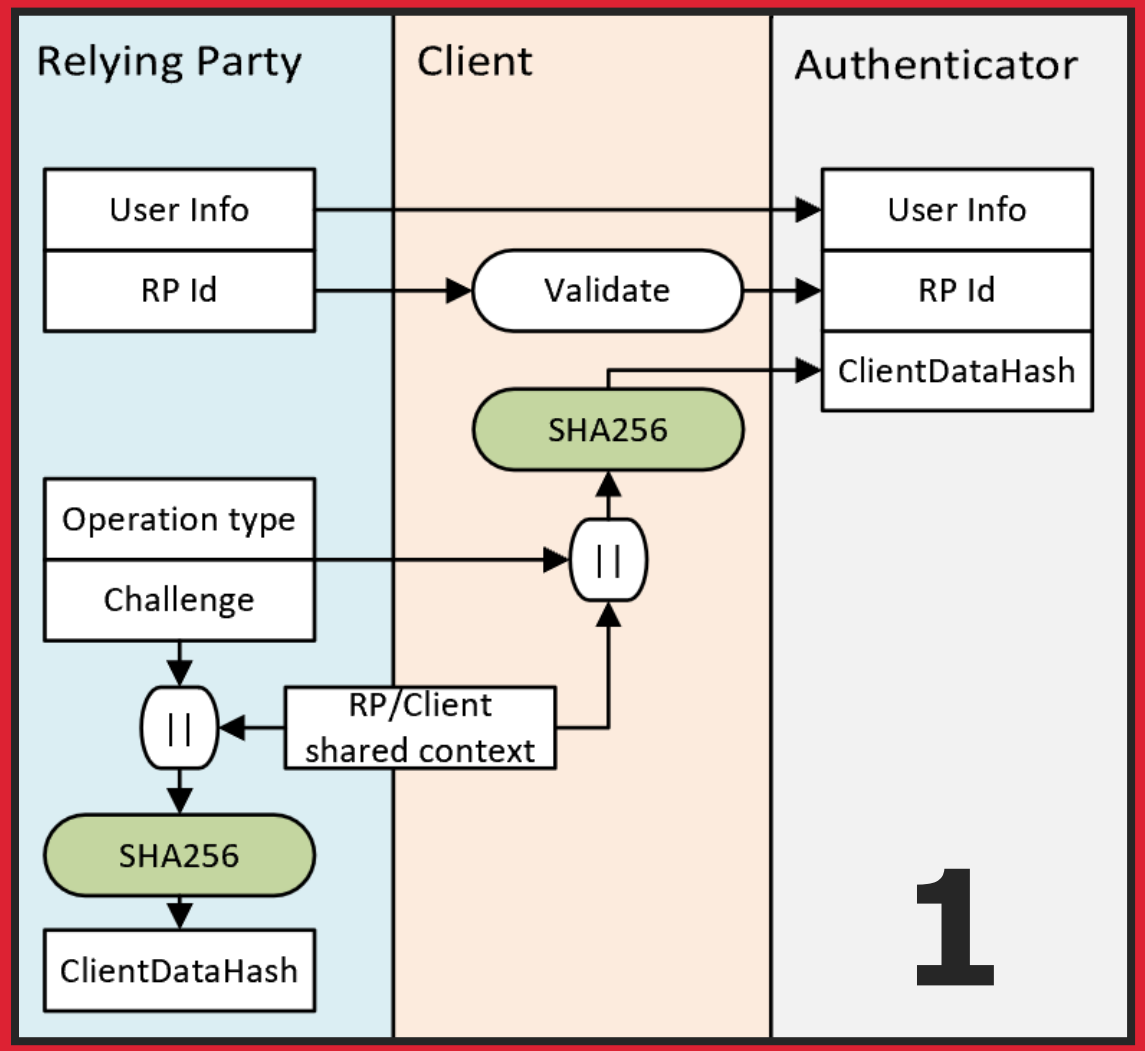
Применителен ли подход к FIDO2?

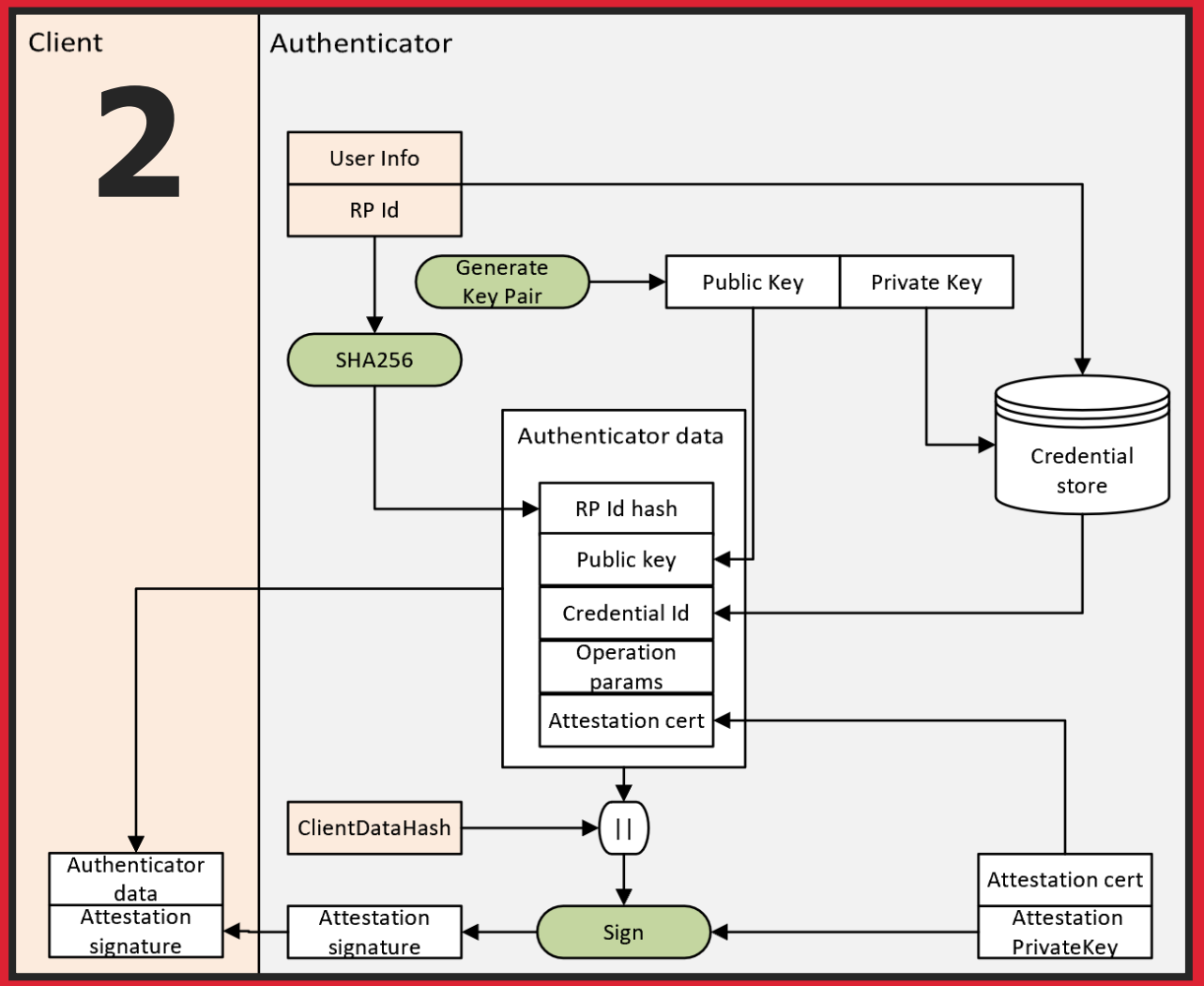
Можно ли не модифицировать браузер?

Использование российских криптографических алгоритмов…

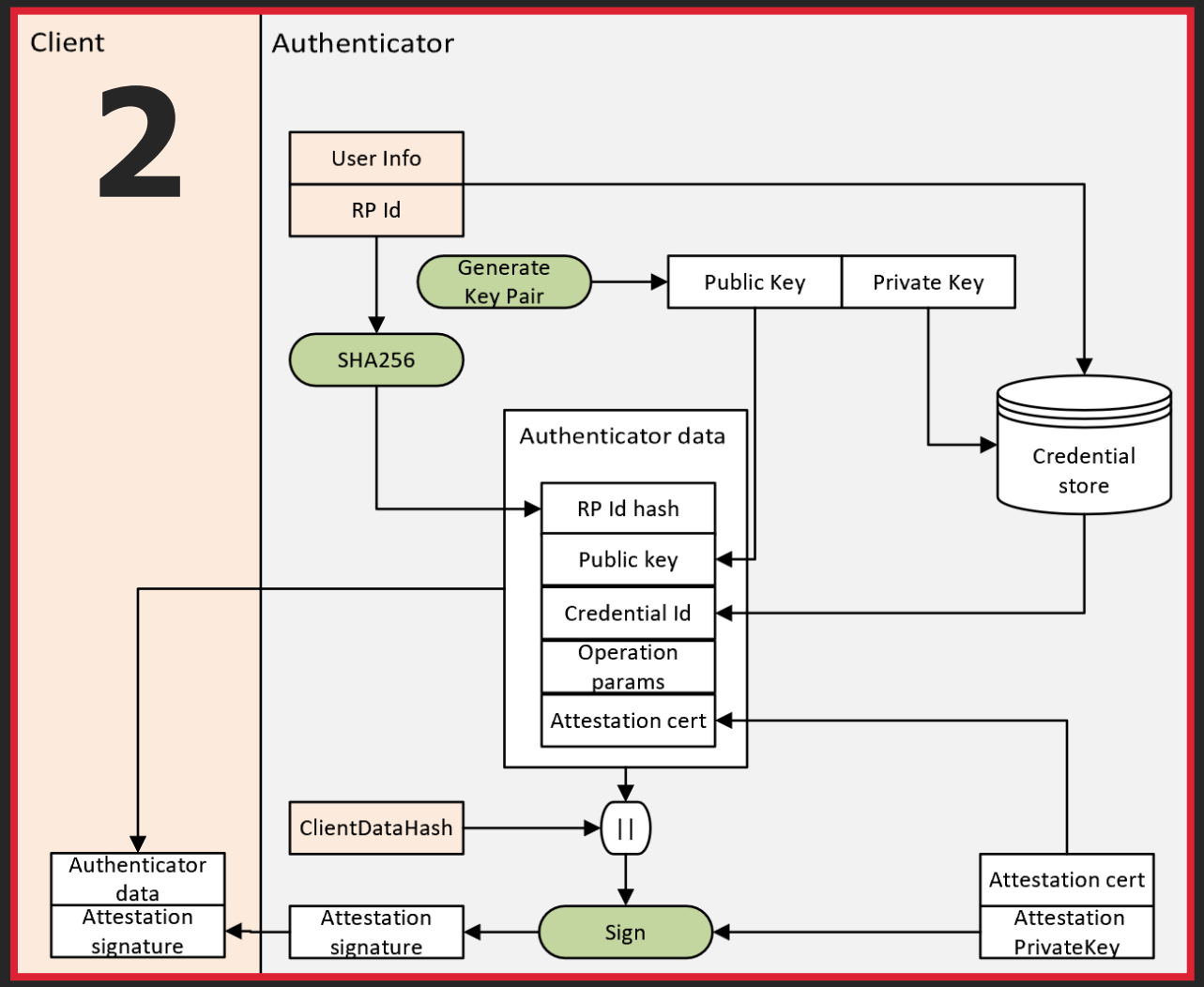
- в протоколе безопасности транспортного уровня (TLS 1.2)
- в сообщениях формата CMS
- в сертификате, списке аннулированных сертификатов (CRL) и запросе на сертификат PKCS #10 инфраструктуры открытых ключей X.509
- для реализации обмена данными по протоколу DLMS
- в протоколе обмена ключами в сети Интернет версии 2 (IKEv2)
- в протоколе защиты информации ESP
- в протоколах и форматах сообщений на основе XML
- в протоколе штампов времени (TSP)
- в протоколе безопасности транспортного уровня (TLS 1.3)
- …

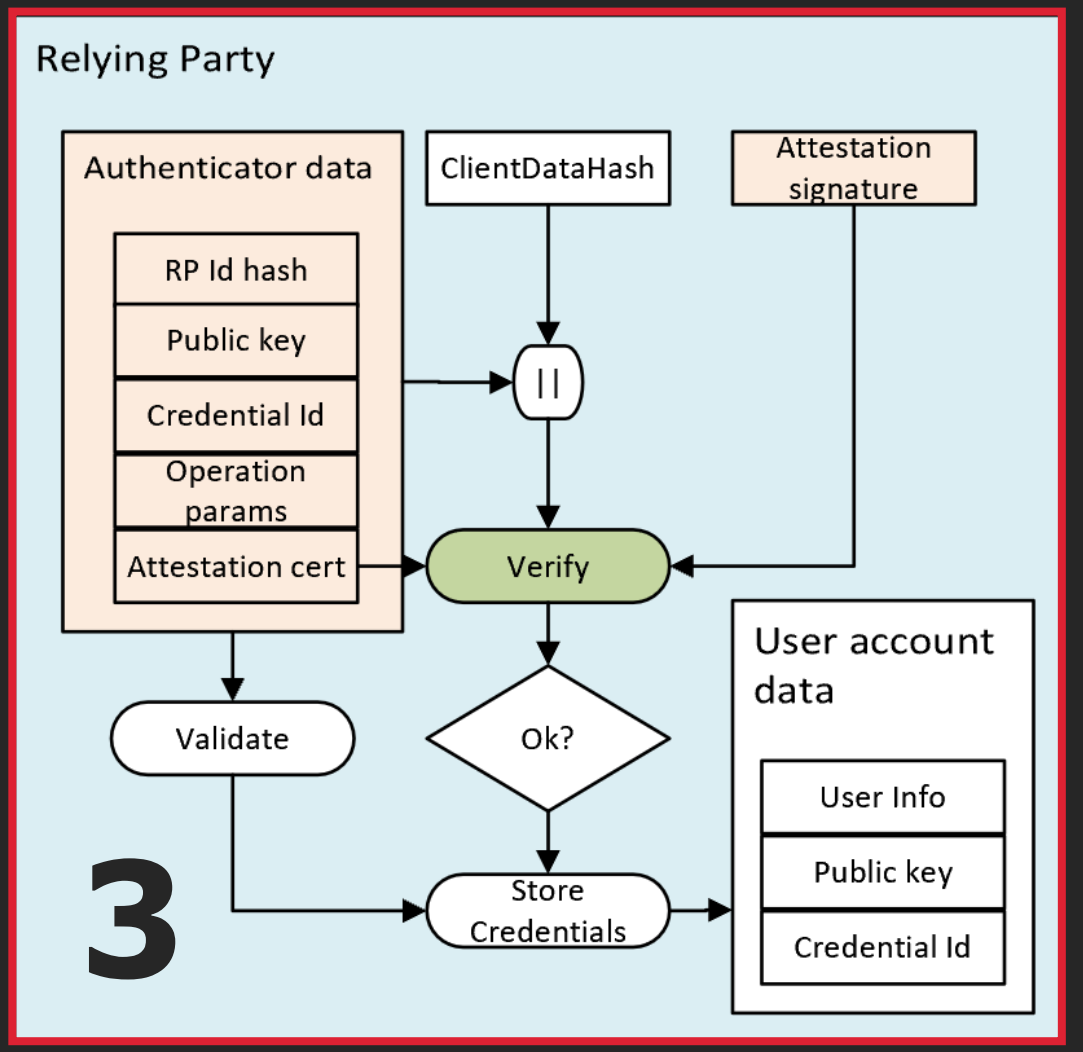
FIDO2: регистрация



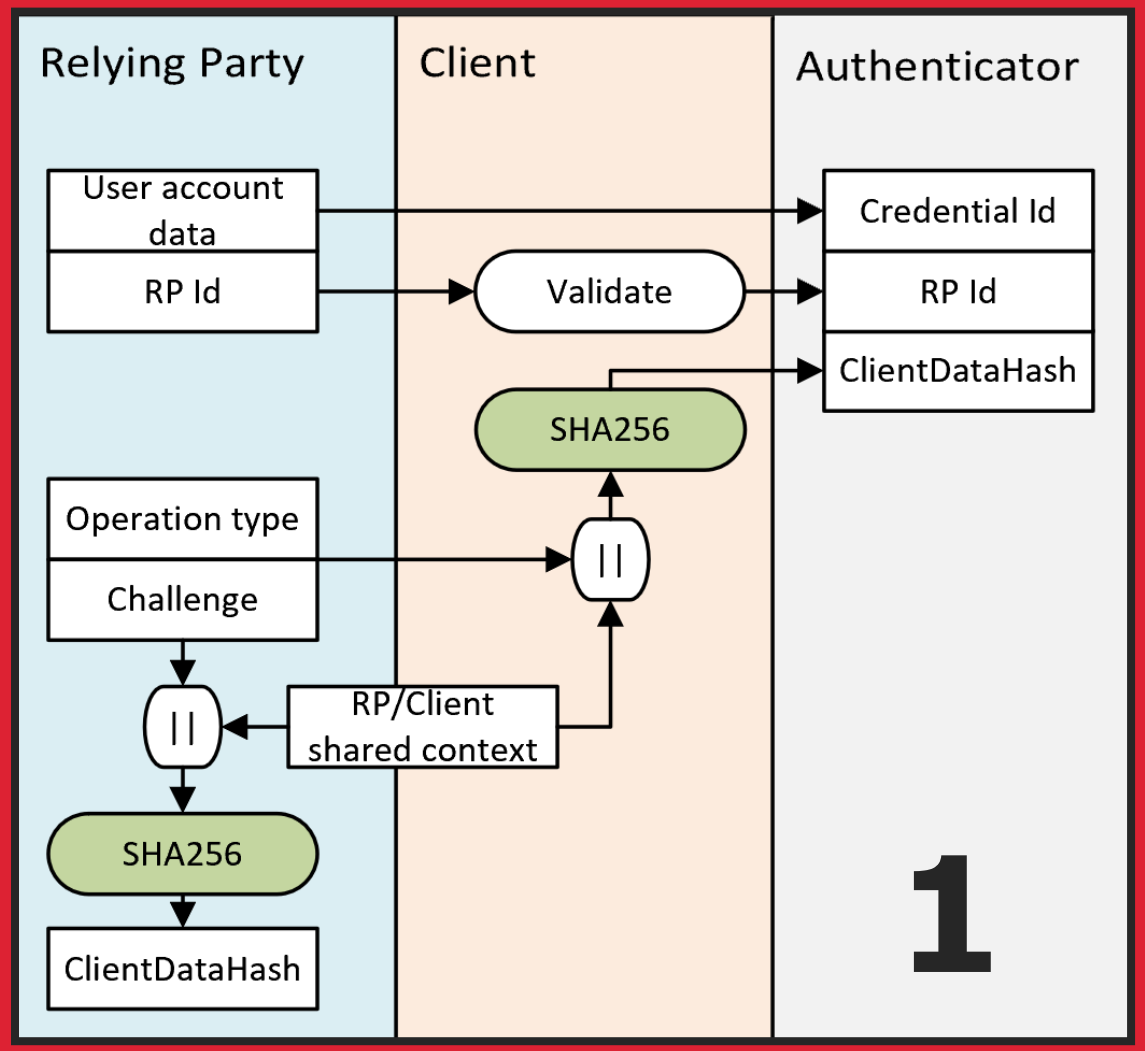


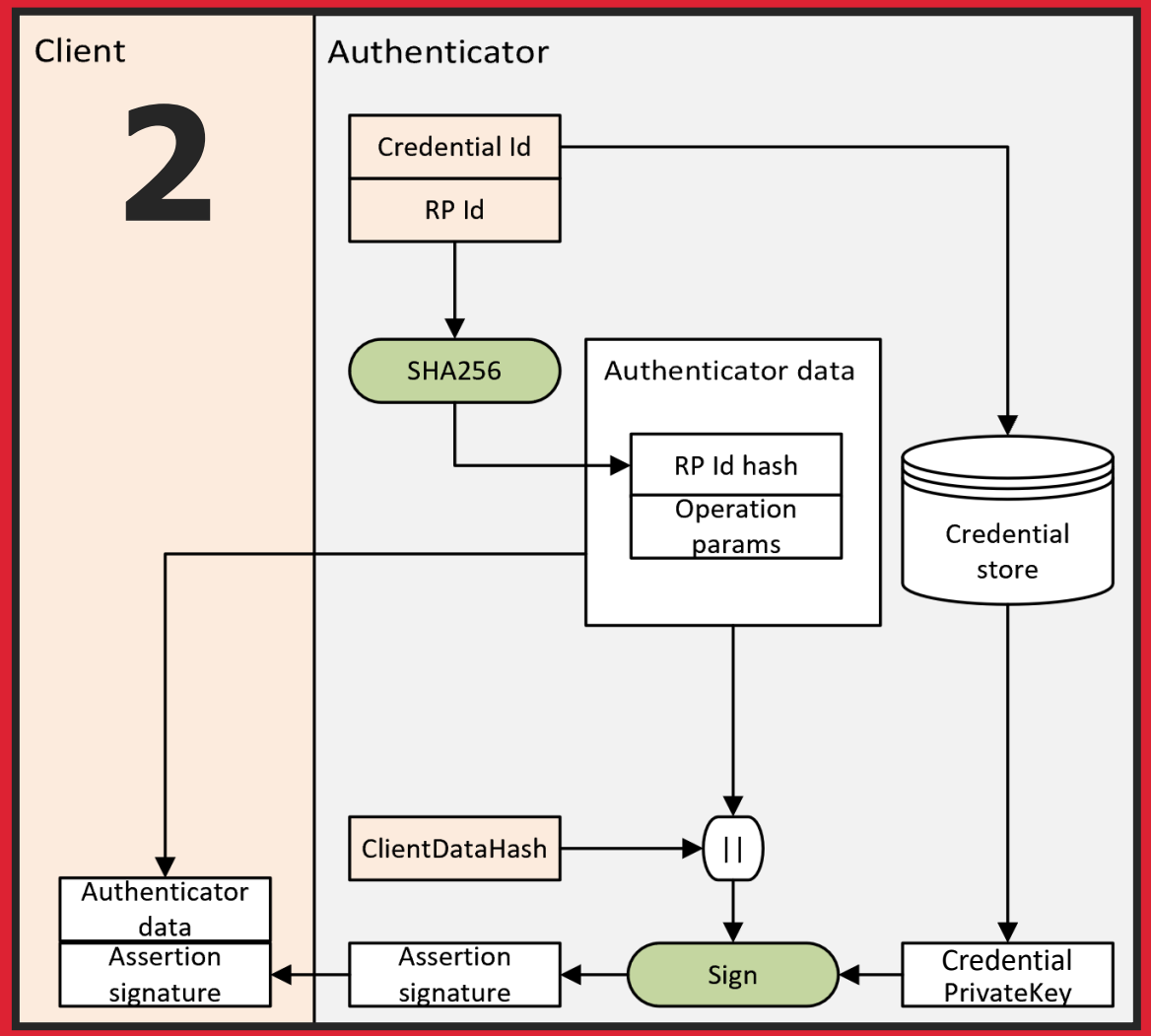
FIDO2: регистрация



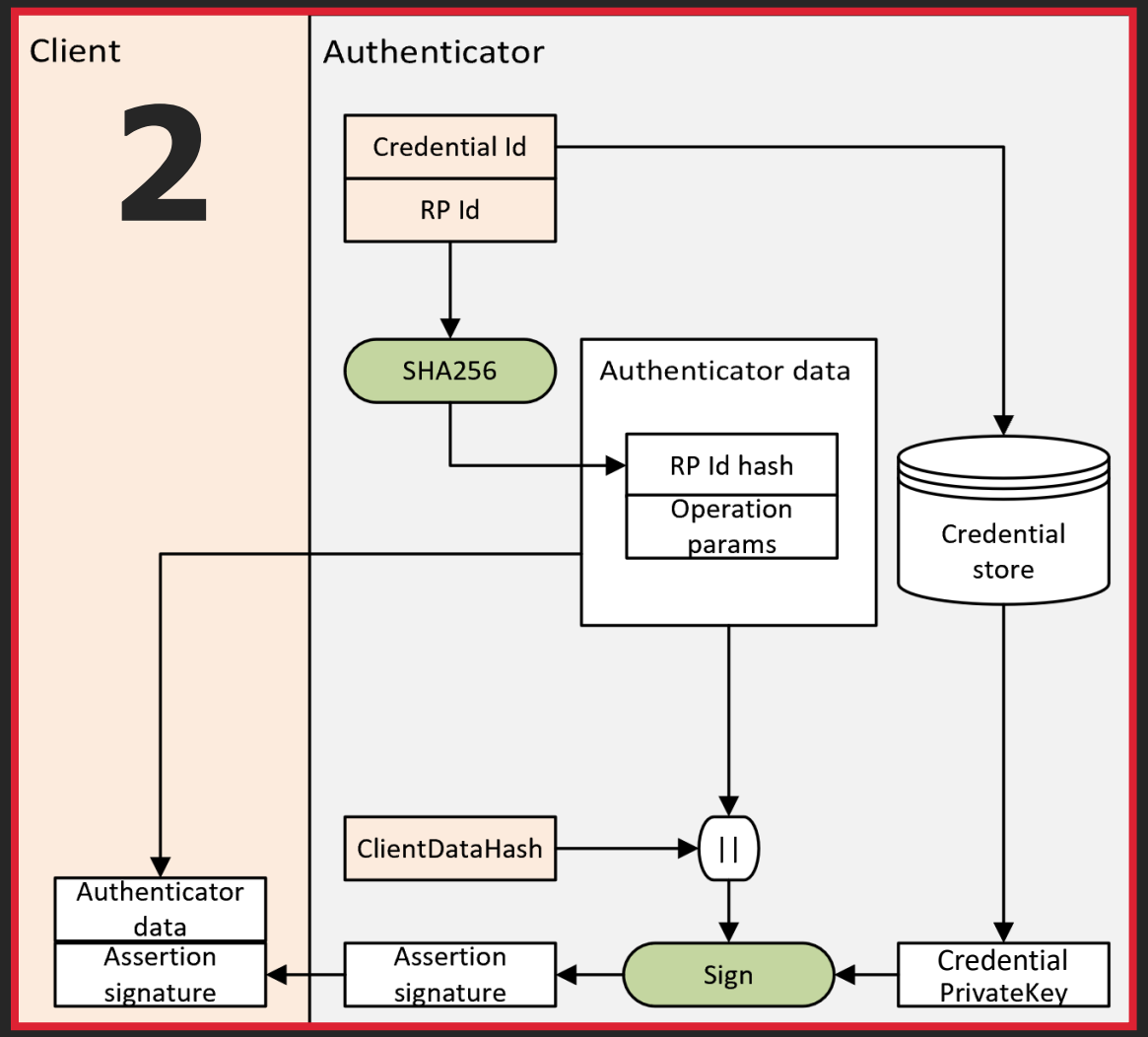


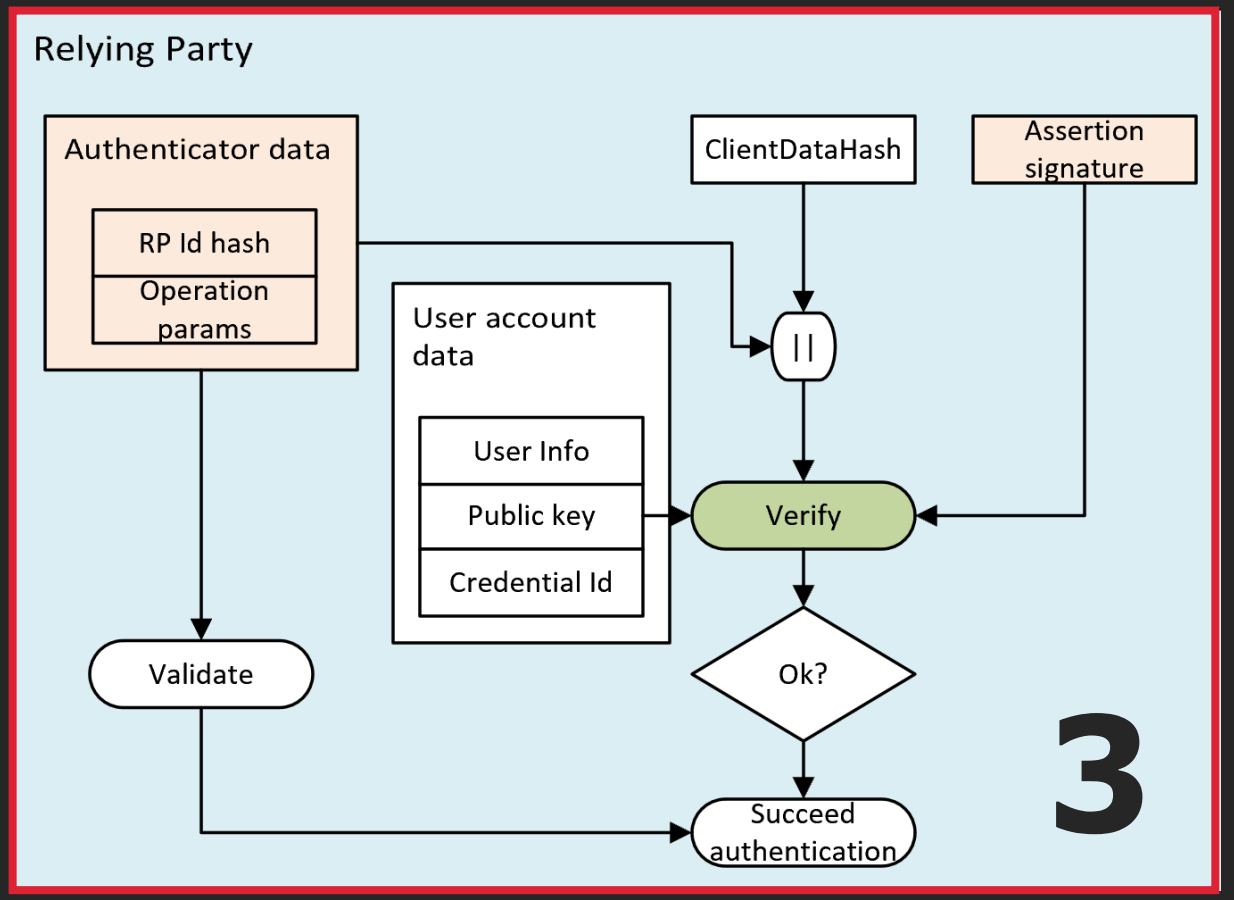
FIDO2: аутентификация





FIDO2: аутентификация





Подпись и проверка подписи

Обмен данными с аутентификатором в формате CBOR

Представление криптографических объектов в формате COSE

RFC7049 Concise Binary Object Representation (CBOR)

- Компактное представление данных
- Компактная кодовая база для парсинга
- Парсинг не требователен к ресурсам
- Конвертируемость из/в JSON

RFC8152 CBOR Object Signing and Encryption (COSE)

- Семантические тэги для криптографических объектов
- Представление криптографических сообщений
- Представление ключей и параметров криптоалгоритмов

COSE в FIDO2

Идентификация криптоалгоритма

A **COSEAlgorithmIdentifier's** value is a number identifying a cryptographic algorithm. The algorithm identifiers **SHOULD** be values registered in the **IANA COSE Algorithms registry** [IANA-COSE-ALGS-REG]

Передача публичного ключа

The credential public key encoded in **COSE_Key** format, as defined in Section 7 of [**RFC8152**], using the CTAP2 canonical CBOR encoding form. The COSE_Key-encoded credential public key MUST contain the "alg" parameter and MUST NOT contain any other OPTIONAL parameters.

Подпись при регистрации и аутентификации

It is **RECOMMENDED** that any new attestation formats defined **not use ASN.1 encodings**, but **instead represent** signatures as equivalent fixed-length byte arrays without internal structure, using the same representations **as used by COSE signatures** as defined in [RFC8152] and [RFC8230].

Российские криптоалгоритмы в FIDO2

Идентификация криптоалгоритма

Name	Value	Description
GOST-3410-2012-256	-261	GOST R 34.10-2012, 256-bit key
GOST-3410-2012-512	-262	GOST R 34.10-2012, 512-bit key

Параметры эллиптических кривых

Name	Value	Key Type	Description
TC26-GOST-3410-2012-256-A	-257	EC2	...
TC26-GOST-3410-2012-256-B	-258	EC2	...
TC26-GOST-3410-2012-256-C	-259	EC2	...
TC26-GOST-3410-2012-256-D	-260	EC2	...
TC26-GOST-3410-2012-512-A	-261	EC2	...
TC26-GOST-3410-2012-512-B	-262	EC2	...
TC26-GOST-3410-2012-512-C	-263	EC2	...

Российские криптоалгоритмы в FIDO2

Сериализация публичного ключа

```
{
  1:   2,    ; kty: EC2 key type
  3:   -261, ; alg: GOST-3410-2012-256 signature algorithm
 -1:   -257, ; crv: TC26-GOST-3410-2012-256-A curve
 -2:   x,    ; x-coordinate as byte string 32 bytes in length;
             ; e.g., in hex: 65eda5a12577c2bae829437fe338701a10aaa...
 -3:   y     ; y-coordinate as byte string 32 bytes in length;
             ; e.g., in hex: 1e52ed75701163f7f9e40ddf9f341b3dc9ba8...
}
```

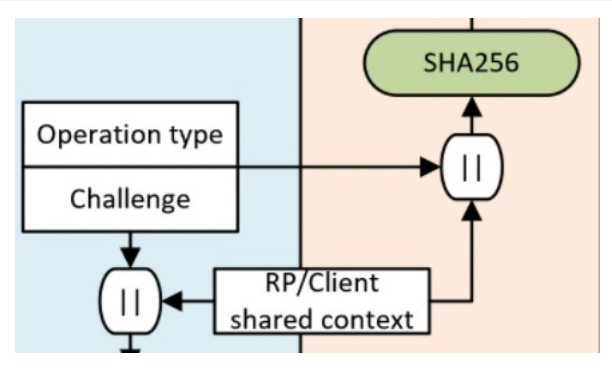
Подпись при регистрации и аутентификации

При использовании алгоритма ГОСТ Р 34.10-2012 с длиной ключа 256 бит поле signature задается байтовой строкой (bstr) длины 64 байта, при этом первые 32 байта содержат число s в представлении big-endian (старший бит записывается первым), а вторые 32 байта содержат число r в представлении big-endian.

SHA256 в FIDO2

Угроза:
возможность нахождения первого/второго прообраза или коллизии.

ClientDataHash

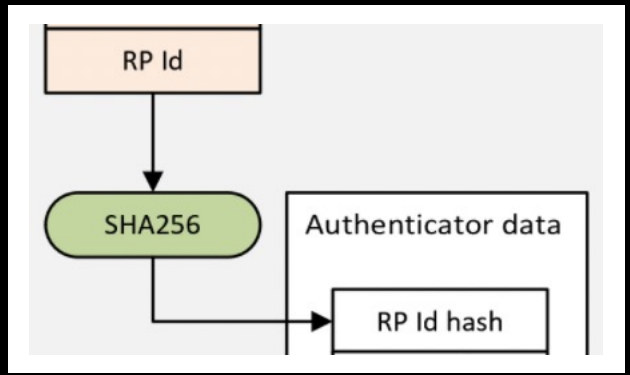


Непосредственно не приводит к уязвимости

Требуется дополнительный анализ

- Совпадение ClientDataHash для разных RP допустимо
- Клиент и аутентификатор контролируют RP Id
- Митигация против подписи навязанных данных: extensions

AuthenticatorData: rpIdHash



- Корректность rpIdHash проверяется клиентом

Угроза: SHA256(Malicious_RP_Id) == SHA256(RP_Id)

- Аутентификатор может обнаружить коллизию, если ассоциирует ключ подписи с RP Id, а не с RP Id hash.
- Может быть решено добавлением "Security considerations" для аутентификаторов

Результаты исследования

- Есть техническая возможность замены криптоалгоритмов в FIDO2 на отечественные
- Для «незаменимых» международных криптографических примитивов есть способы снижения рисков от их использования

- Намечен путь для перехода на отечественные криптоалгоритмы
- Заинтересованность сообщества
- От стандартизации выиграют все участники рынка

Вопросы

Контактная информация

Евгений Мироненко

mironenko@rutoken.ru
info@rutoken.ru

www.rutoken.ru
www.aktiv-company.ru

+7 495 925-77-90

РУТОКЕН