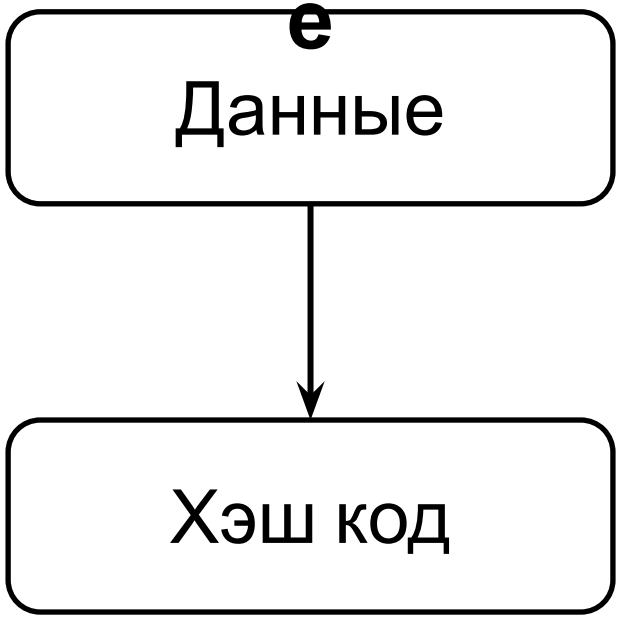
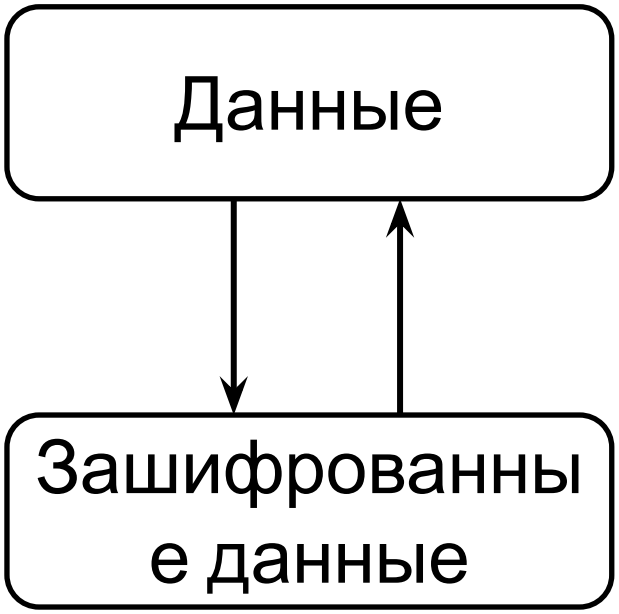
ОБЩИЕ ПРИНЦИПЫ ЦИФРОВОЙ ПОДПИСИ

Хэширование



Подпись



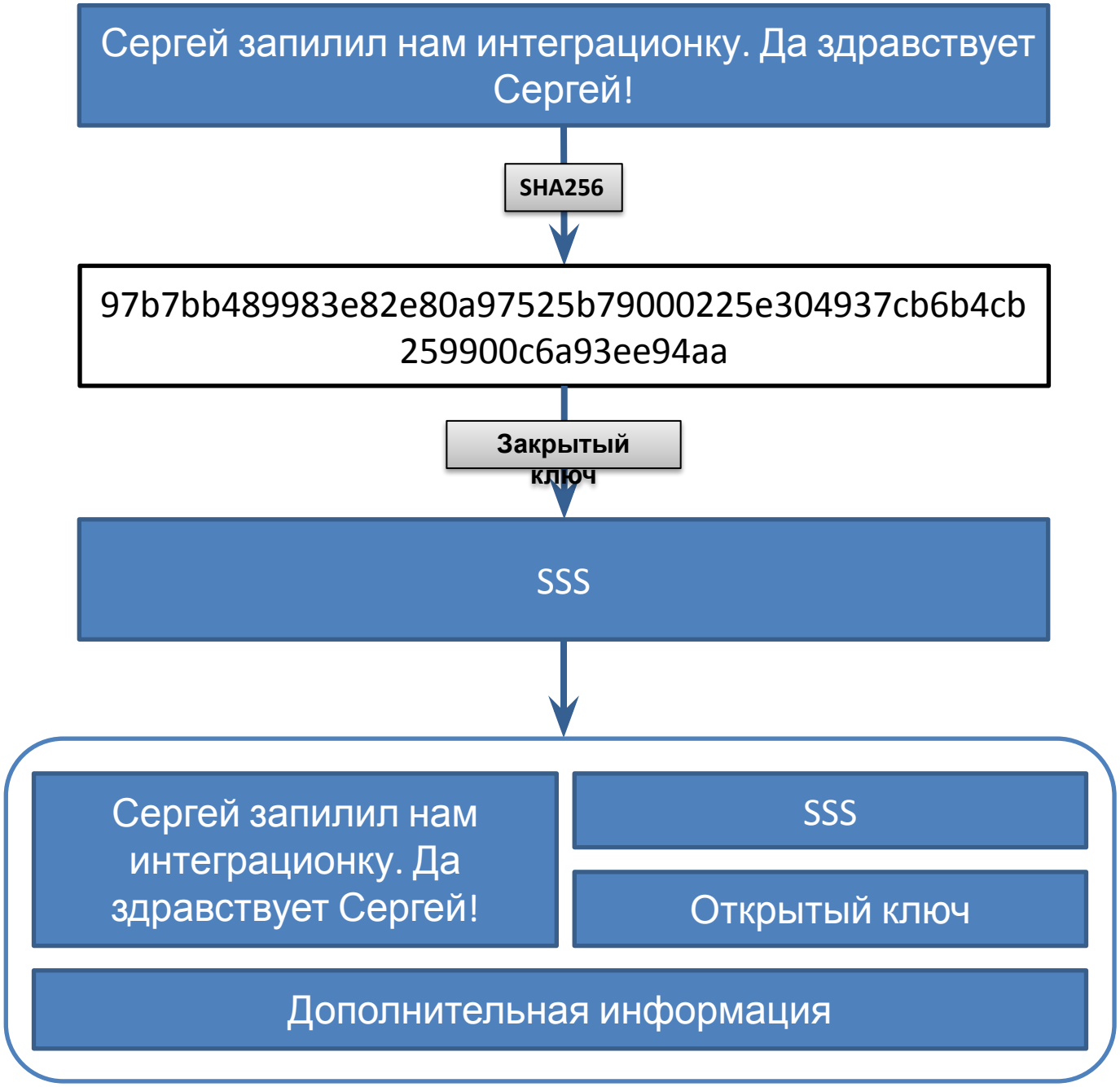
Ключи

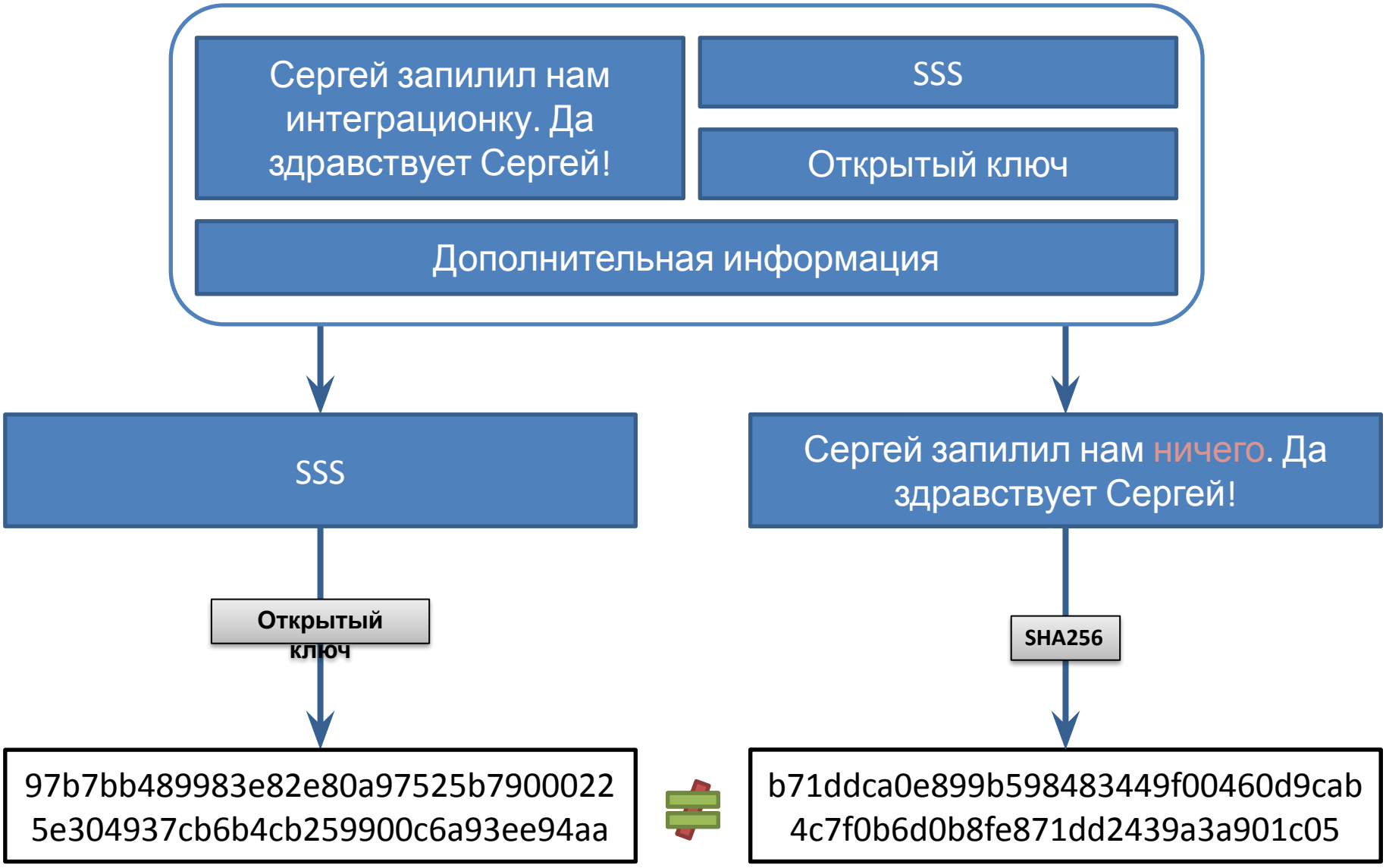
Закрытый (секретный)

- Зашифровывает (подписывает) данные
- Должен находиться только у подписывающего

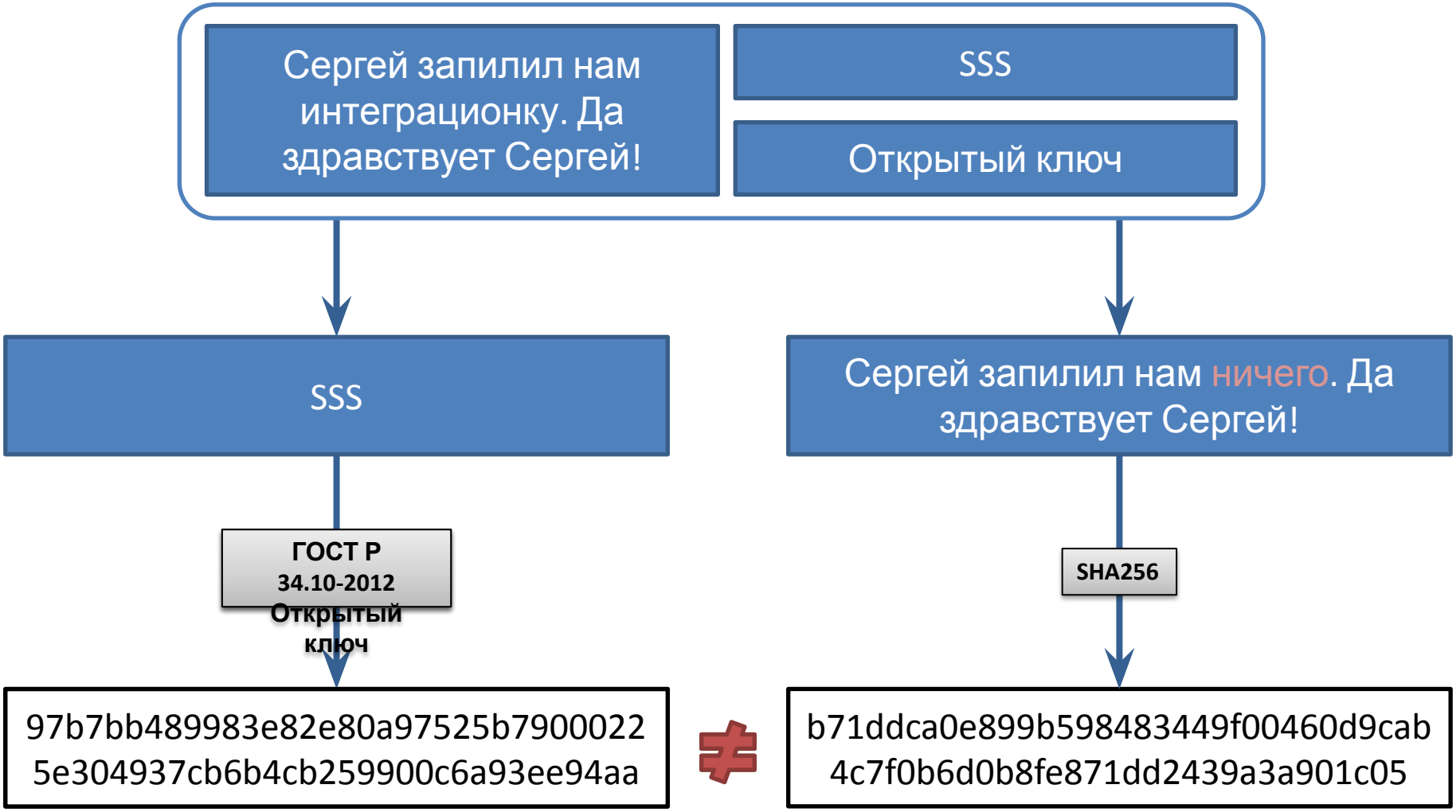
Открытый

- Расшифровывает подпись
- Доступен всем

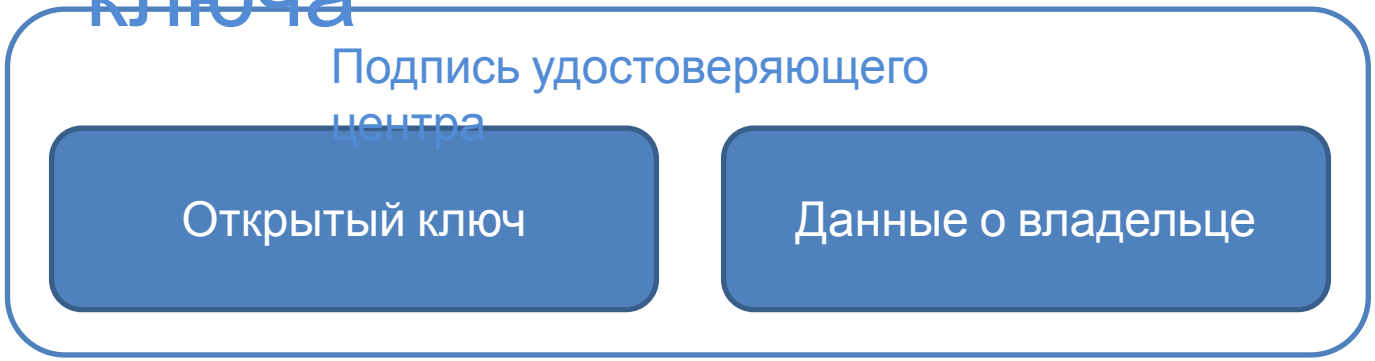

Сергей запилил нам интеграционку. Да здравствует Сергей!
SHA256
97b7bb489983e82e80a97525b79000225e304937cb6b4cb259900c6a93ee94aa
Закрытый ключ
SSS
Сергей запилил нам интеграционку. Да здравствует Сергей!
SSS
Открытый ключ
Дополнительная информация

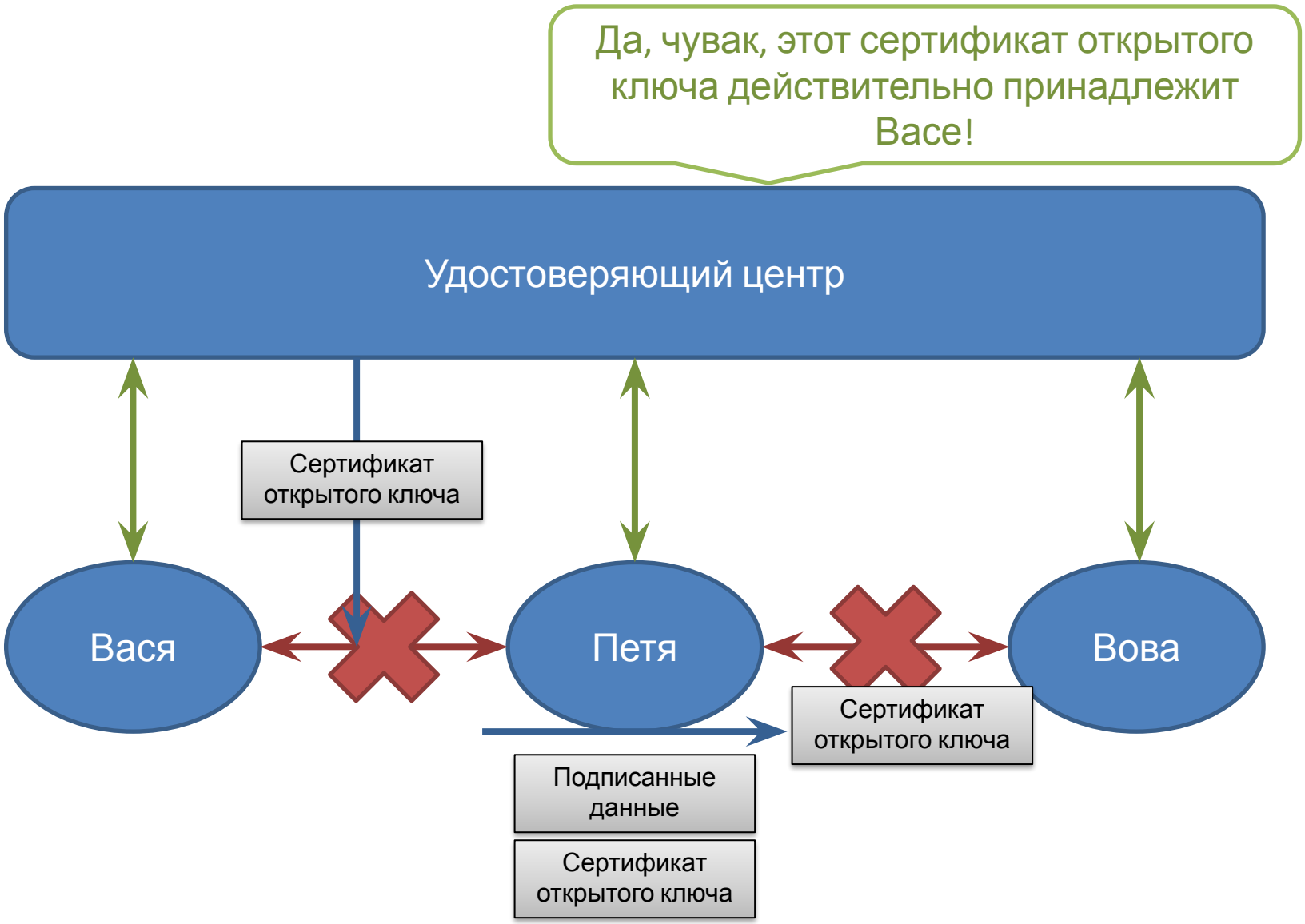

Сергей запилил нам интеграционку. Да здравствует Сергей!
SSS
Открытый ключ
Дополнительная информация
SSS
Сергей запилил нам ничего. Да здравствует Сергей!
Открытый ключ
SHA256
97b7bb489983e82e80a97525b7900022
5e304937cb6b4cb259900c6a93ee94aa
b71ddca0e899b598483449f00460d9cab
4c7f0b6d0b8fe871dd2439a3a901c05
Документ соответствует подписи!
Документ не соответствует подписи!

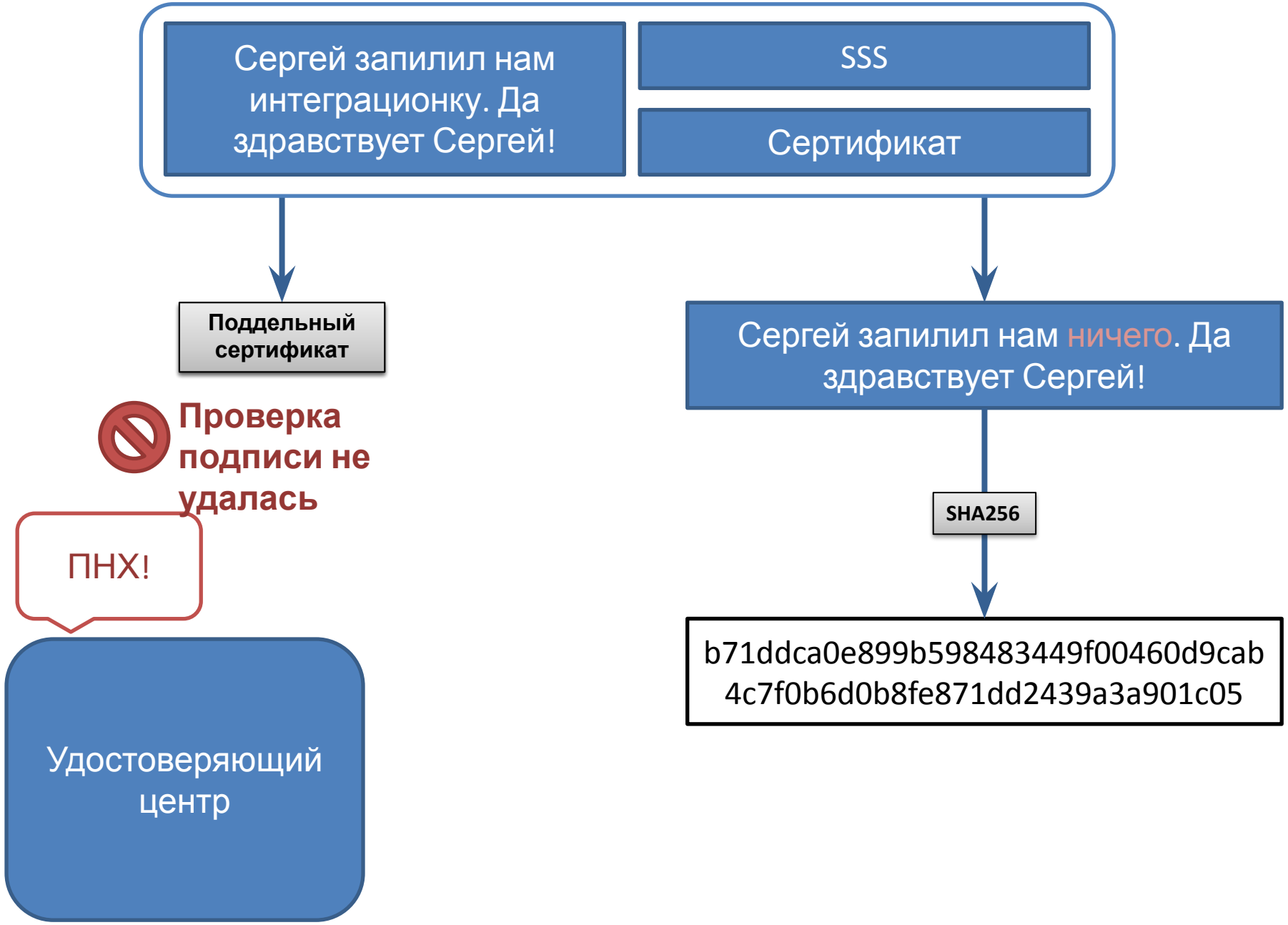
ИНФРАСТРУКТУРА ОТКРЫТЫХ КЛЮЧЕЙ


Сергей запилил нам интеграционку. Да здравствует Сергей!
SSS
Открытый ключ
SSS
Сергей запилил нам ничего. Да здравствует Сергей!
ГОСТ Р 34.10-2012 Открытый ключ
SHA256
97b7bb489983e82e80a97525b79000225e304937cb6b4cb259900c6a93ee94aa
≠
b71ddca0e899b598483449f00460d9cab4c7f0b6d0b8fe871dd2439a3a901c05
Документ не соответствует подписи!

Сертификат открытого ключа

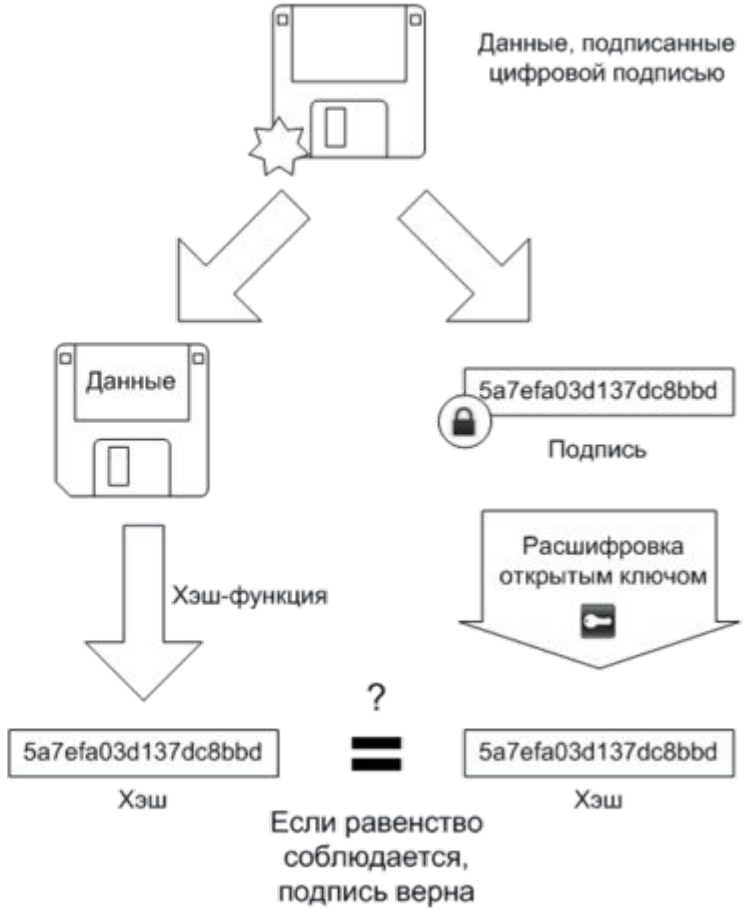



Да, чувак, этот сертификат открытого ключа действительно принадлежит Васе!
Удостоверяющий центр
Сертификат открытого ключа
Вася
Петя
Вова
Сертификат открытого ключа
Подписанные данные
Сертификат открытого ключа

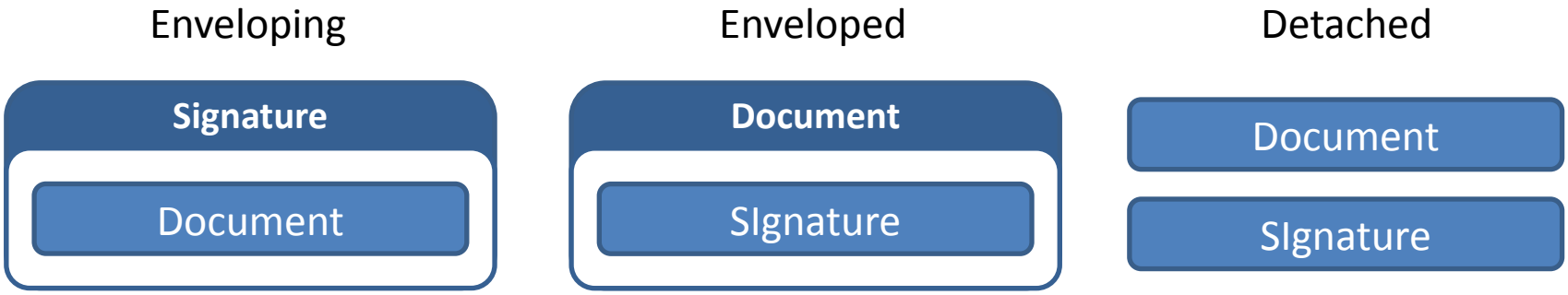

Сергей запилил нам интеграционку. Да здравствует Сергей!
SSS
Сертификат
Поддельный сертификат
Проверка подписи не удалась
ПНХ!
Удостоверяющий центр
Сергей запилил нам ничего. Да здравствует Сергей!
SHA256
b71ddca0e899b598483449f00460d9cab
4c7f0b6d0b8fe871dd2439a3a901c05

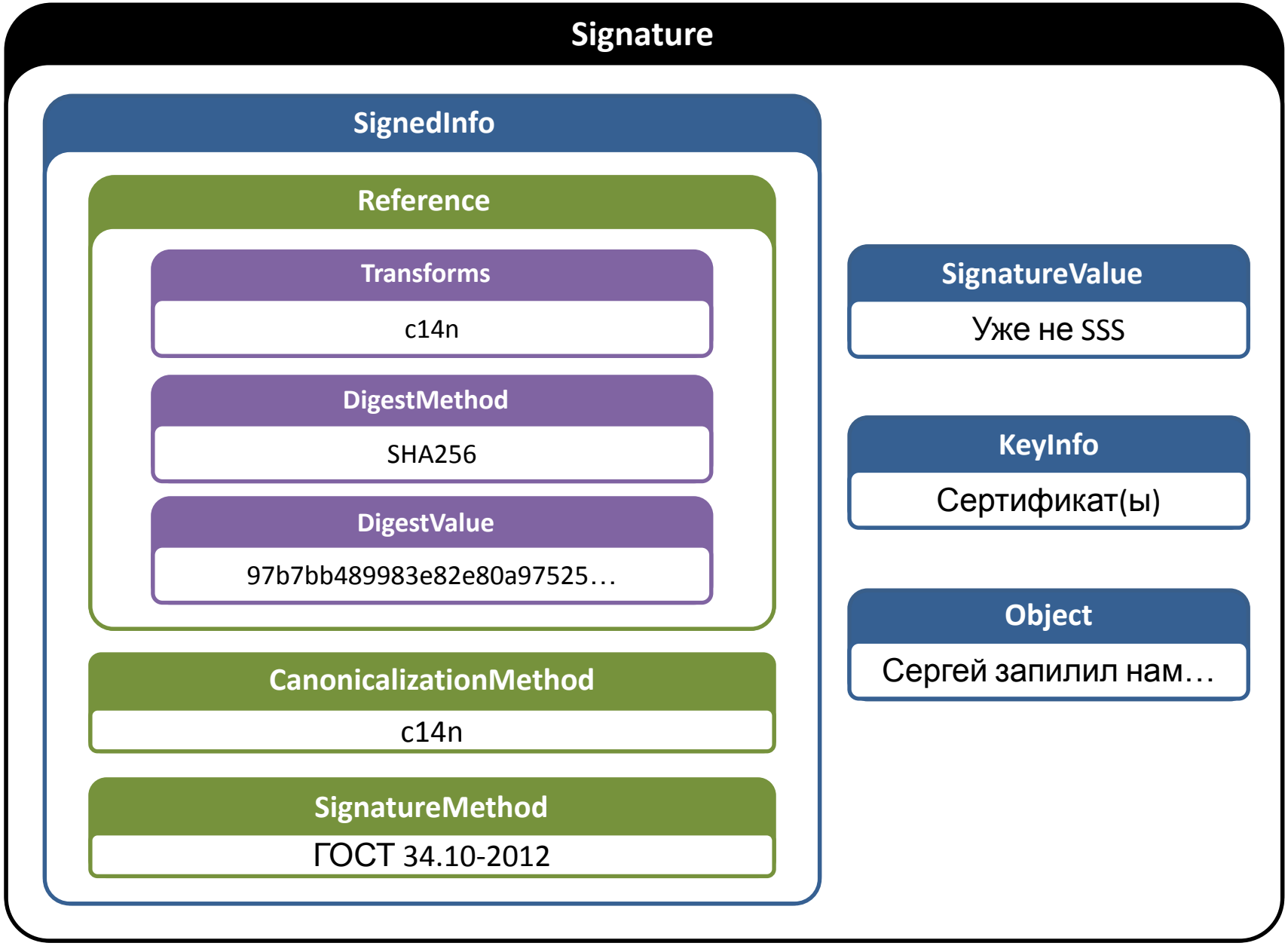
Подписывание

Проверка



XML SIGNATURE (XMLDSIG)


Enveloping
Signature
Document
Enveloped
Document
SIgnature
Detached
Document
SIgnature


Signature
SignedInfo
Reference
Transforms
c14n
DigestMethod
SHA256
DigestValue
97b7bb489983e82e80a97525…
CanonicalizationMethod
c14n
SignatureMethod
ГОСТ 34.10-2012
SignatureValue
Уже не SSS
KeyInfo
Сертификат(ы)
Object
Сергей запилил нам…

Core Validation

Валидация ссылок
(Reference Validation)

1. Канонизация SignedInfo
2. Для каждого Reference:
   a.) получение элемента по URL
   b.) его хеширование
   c.) сравнение полученного хеша со значением в DigestValue

Валидация подписи
(Signature Validation)

1. Получение открытого ключа из KeyInfo
2. Канонизация SignedInfo
3. Расшифровывается Signature Value
4. Полученные элементы SignedInfo сравниваются