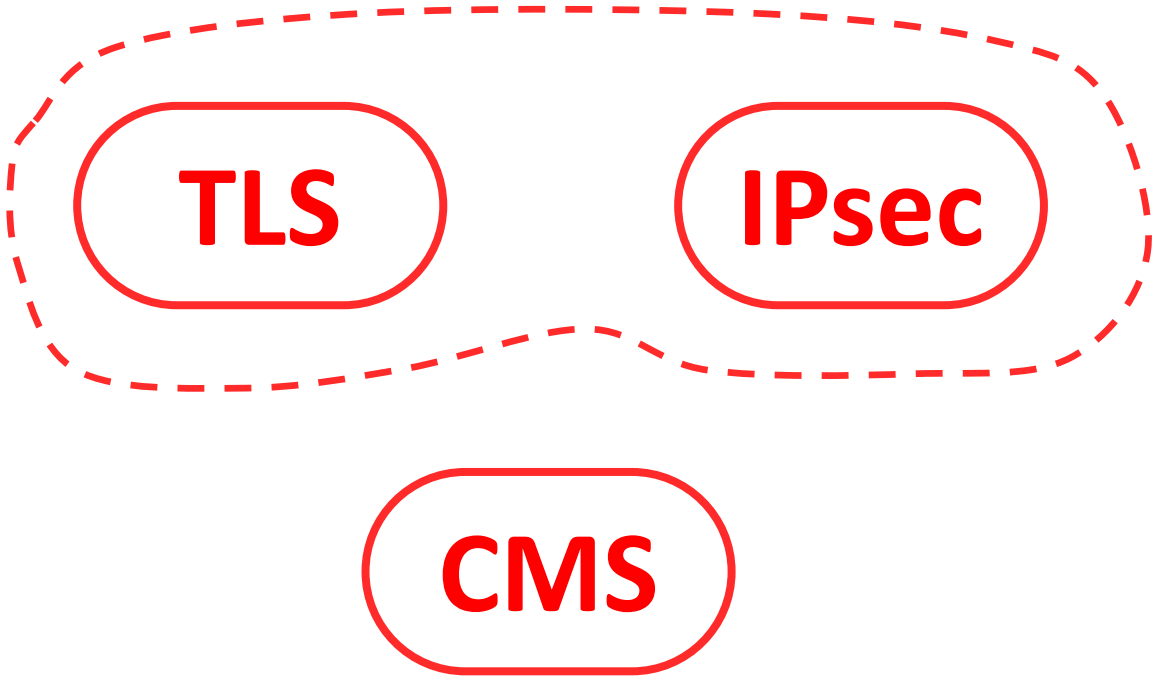
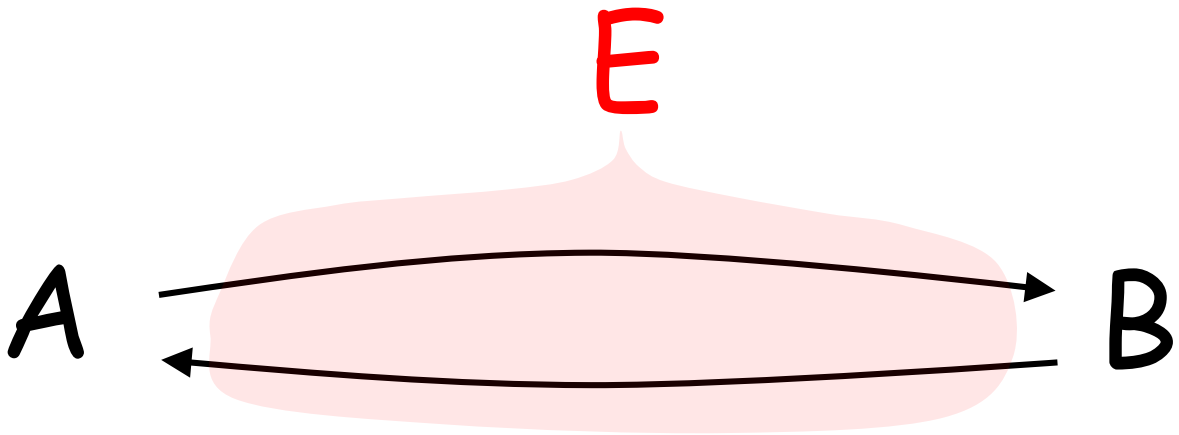
Всё, что вы хотели знать про TLS, IPsec и CMS, но стеснялись спросить

Смышляева Екатерина Сергеевна,
ess@cryptopro.ru

КРИПТОПРО

CTCrypt’2019

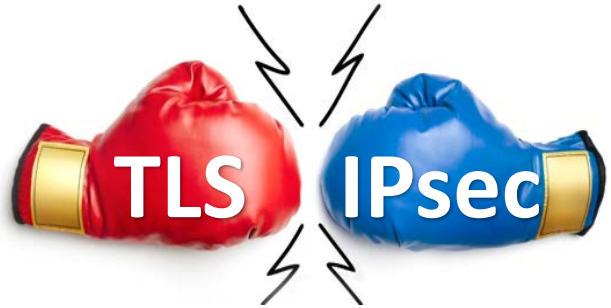

TLS
IPsec
CMS

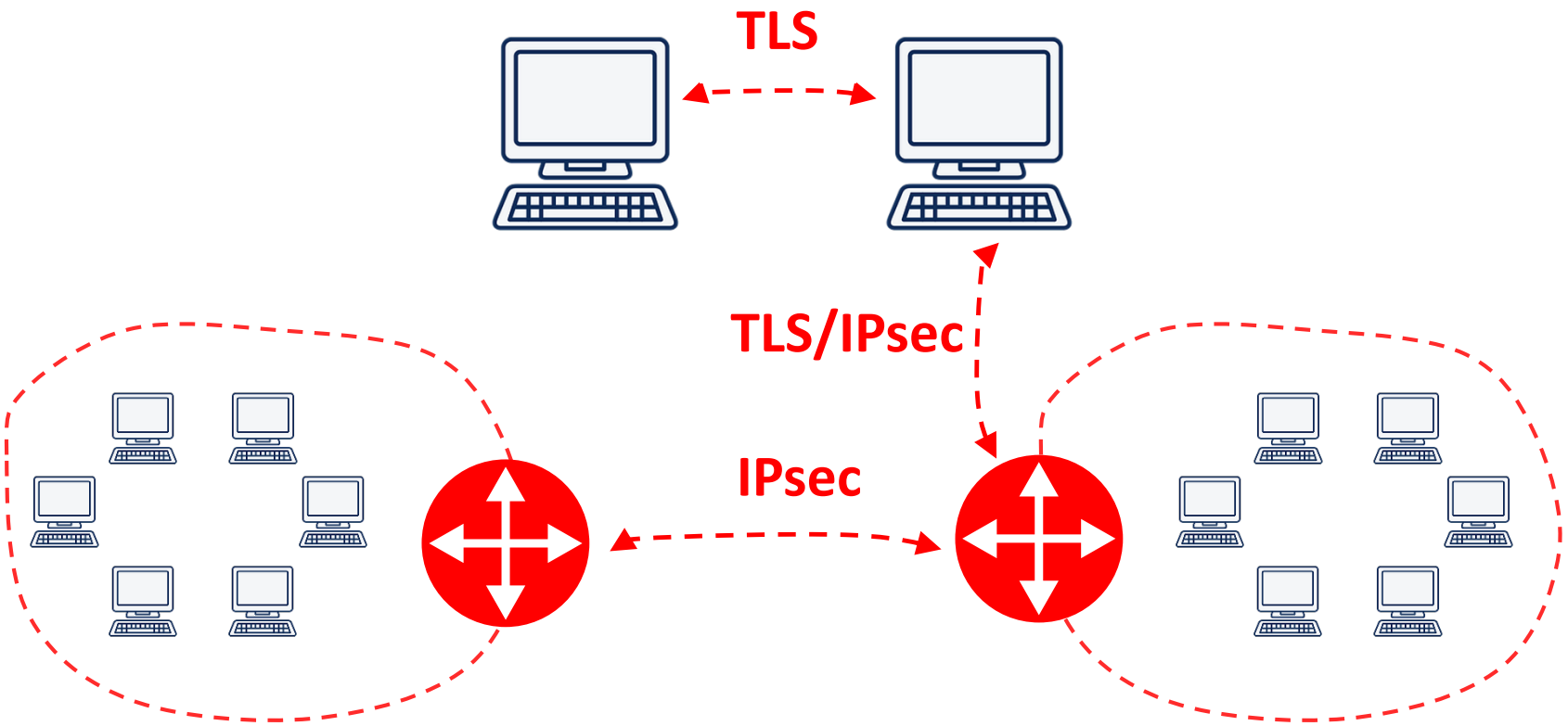

E
A
B

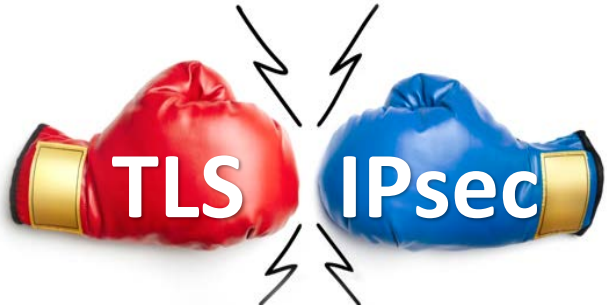
Два самых популярных протокола

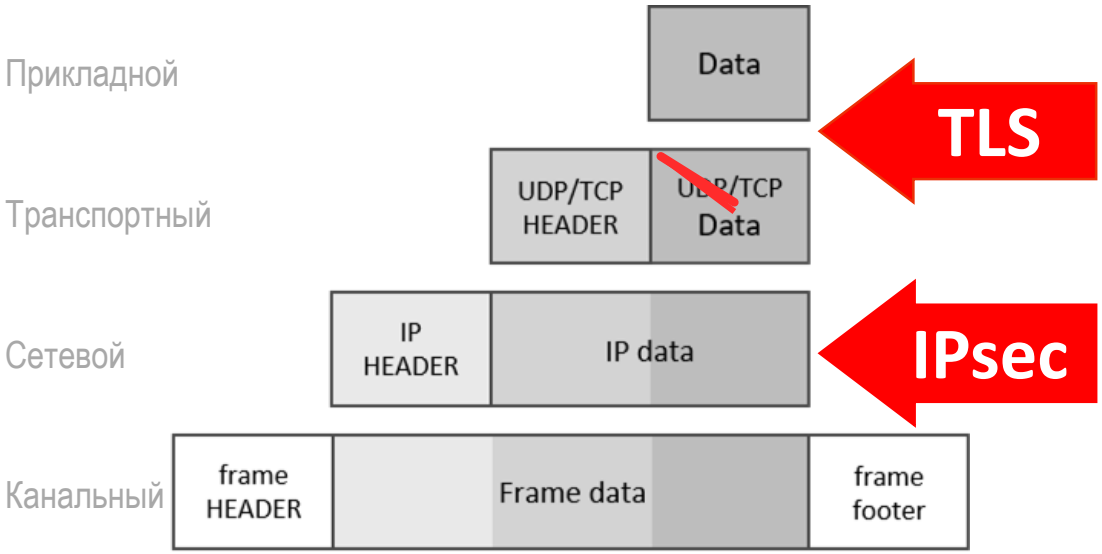
TLS IPsec

- Основные различия
- Принцип работы


TLS
IPsec

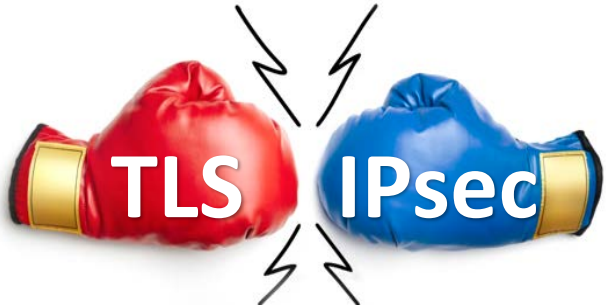

TLS
TLS/IPsec
IPsec

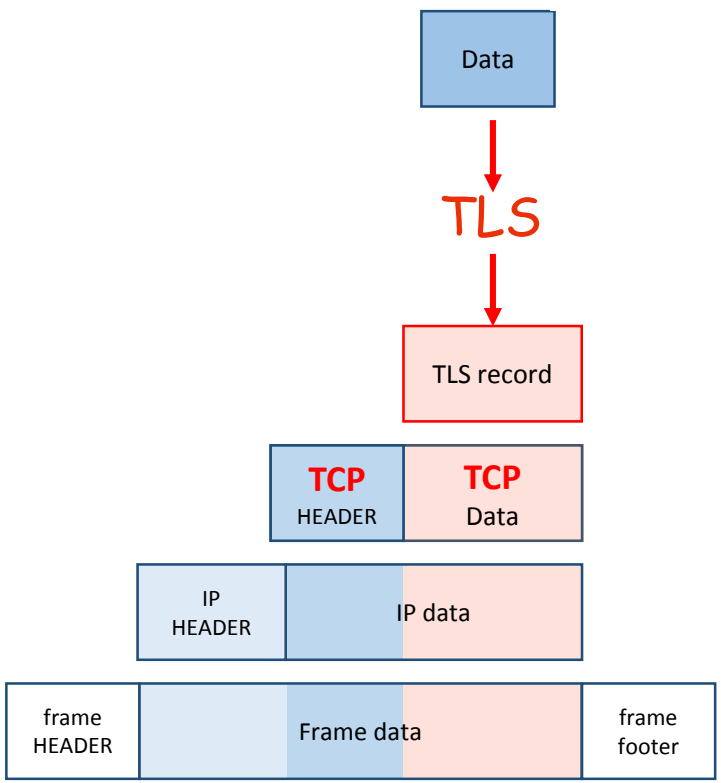


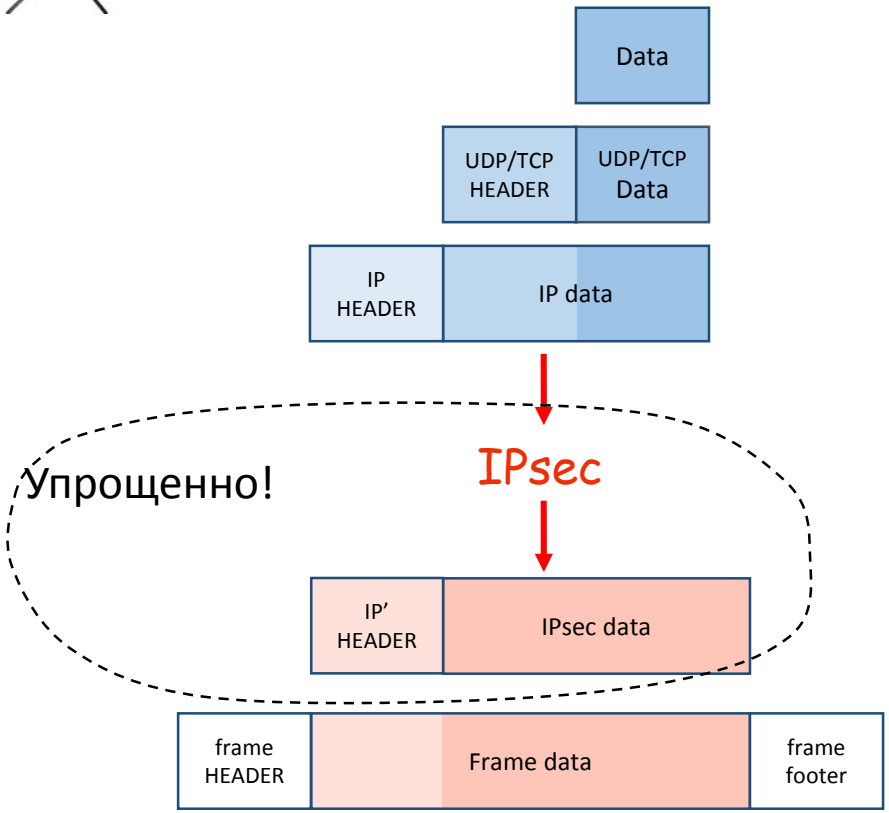


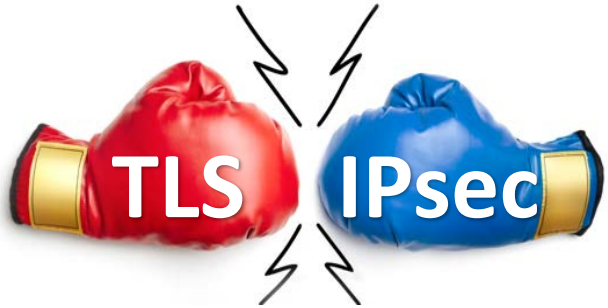
Конфиденциальность и целостность данных между двумя приложениями

Конфиденциальность и целостность данных в IP-пакете между двумя машинами

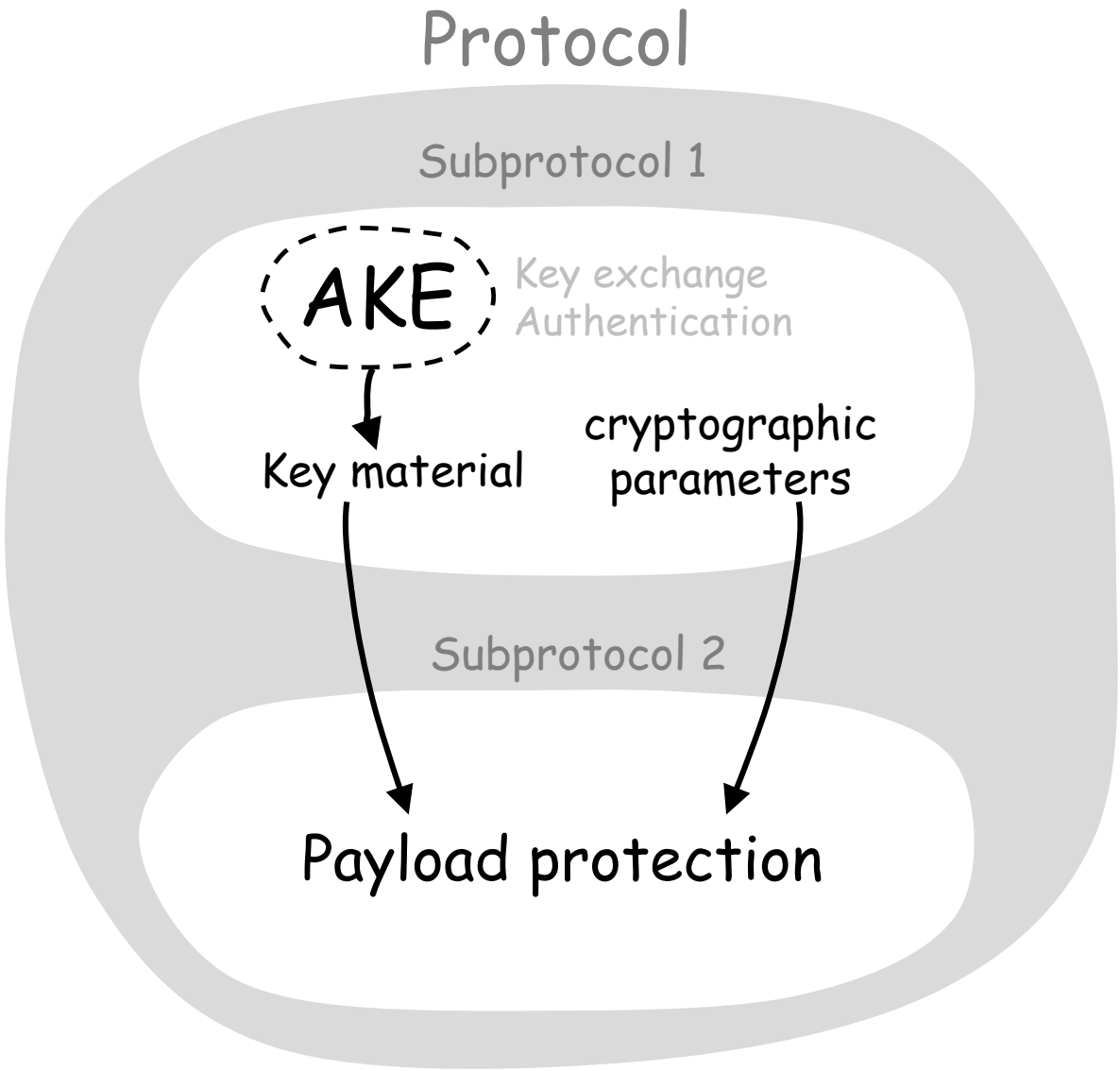

TLS
IPsec

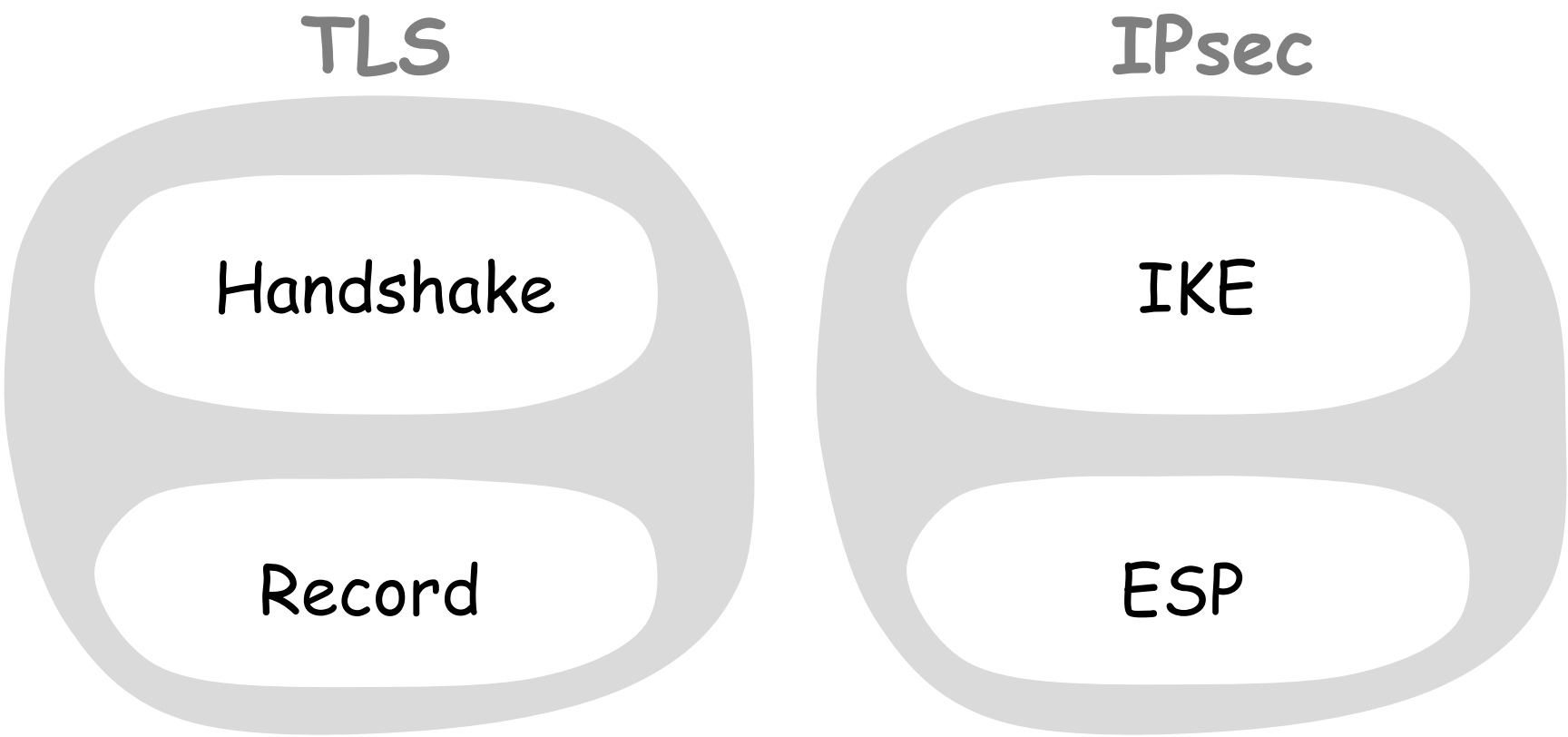

Data
TLS
TLS record
TCP HEADER
TCP Data
IP HEADER
IP data
frame HEADER
Frame data
frame footer

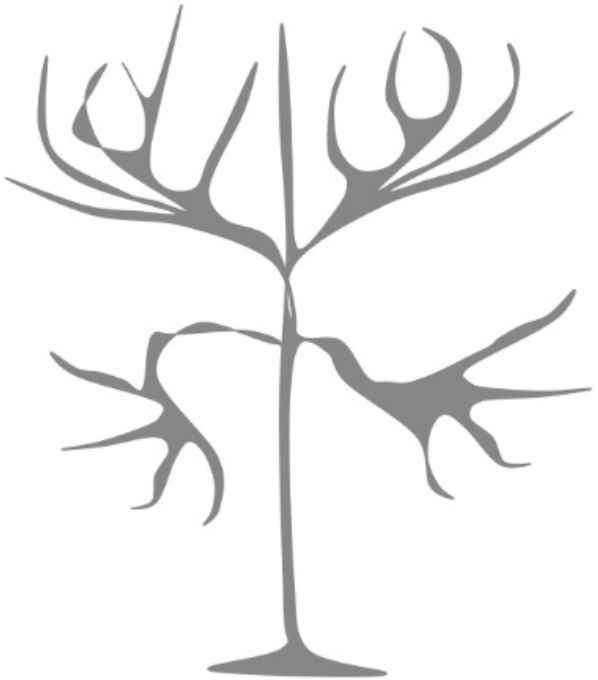

Data
UDP/TCP HEADER
UDP/TCP Data
IP HEADER
IP data
Упрощенно!
IPsec
IP' HEADER
IPsec data
frame HEADER
Frame data
frame footer



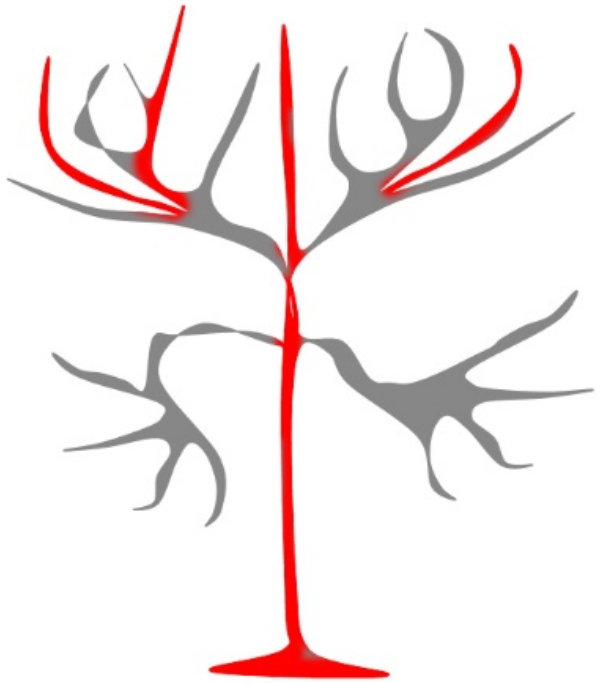
☺	Сложность реализации	☹
☹	Скрытие топологии сети (IP заголовков)	☺
☹	Скорость работы	☺
☹ только TCP	Поддержка UDP	☺ TCP и UDP
Одностороння/ двусторонняя	Аутентификация	Двусторонняя


Protocol
Subprotocol 1
AKE
Key exchange
Authentication
Key material
cryptographic
parameters
Subprotocol 2
Payload protection

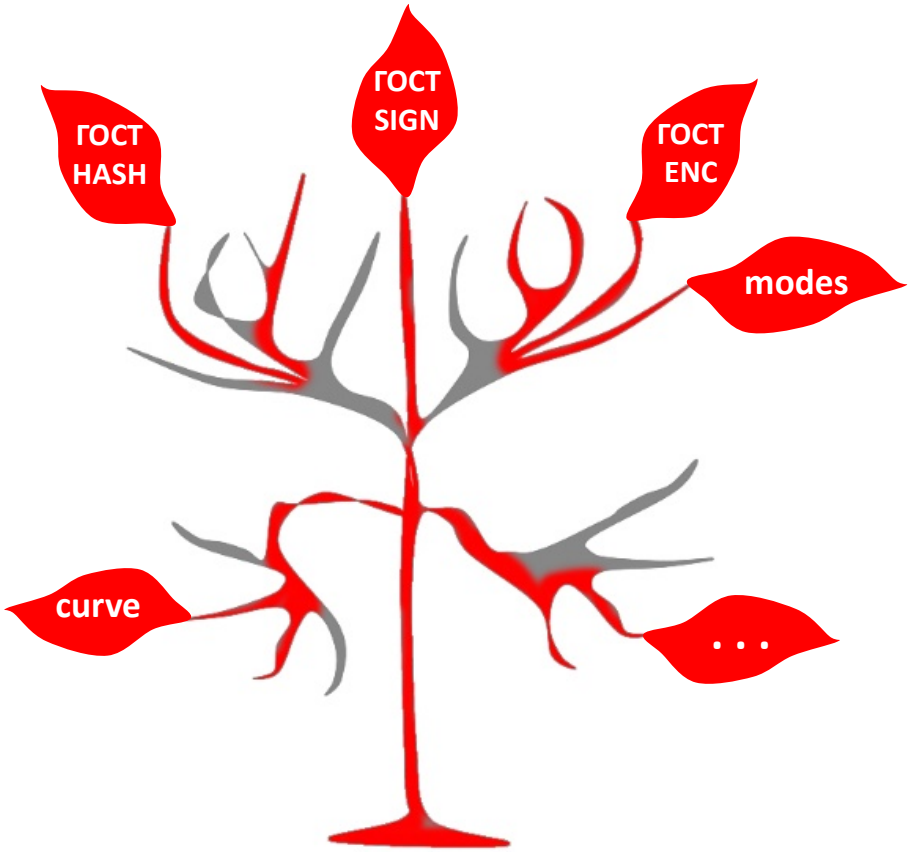

TLS
Handshake
Record
IPsec
IKE
ESP



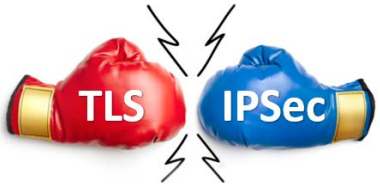
RFC



Обязательно / опционально

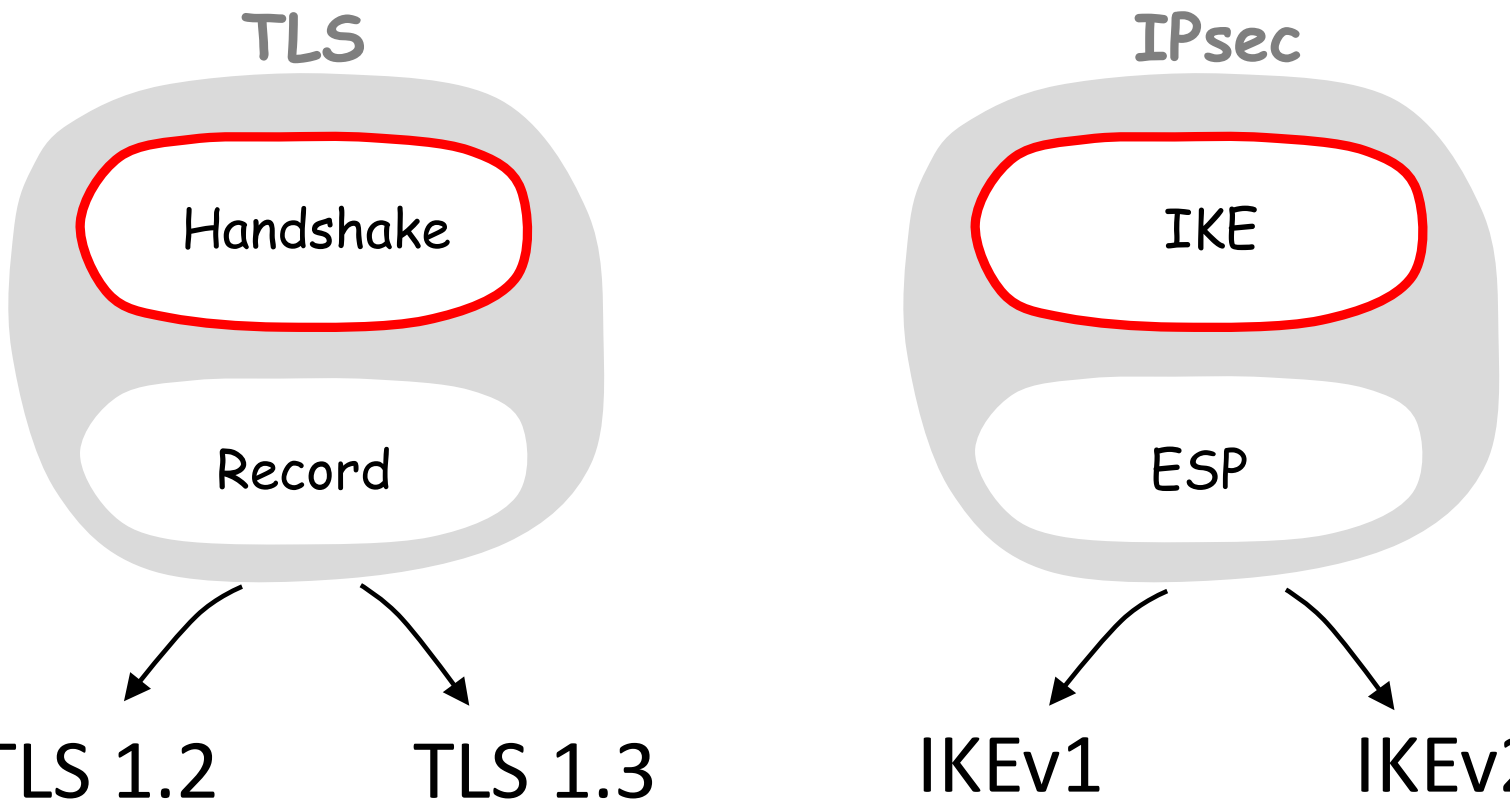


Криптонабор
cipher suite



Трансформы
transforms

Handshake / IKE



- ✓ Р 1323565.1.020-2018
- ✓ Драфт RFC
- ✓ Номера IANA

- ✓ Разработка рекомендаций

- ✓ ТС для ГОСТ 28147

- ✓ Разработка рекомендаций

Authenticated

1. SIGN
2. Факт обладания секретом

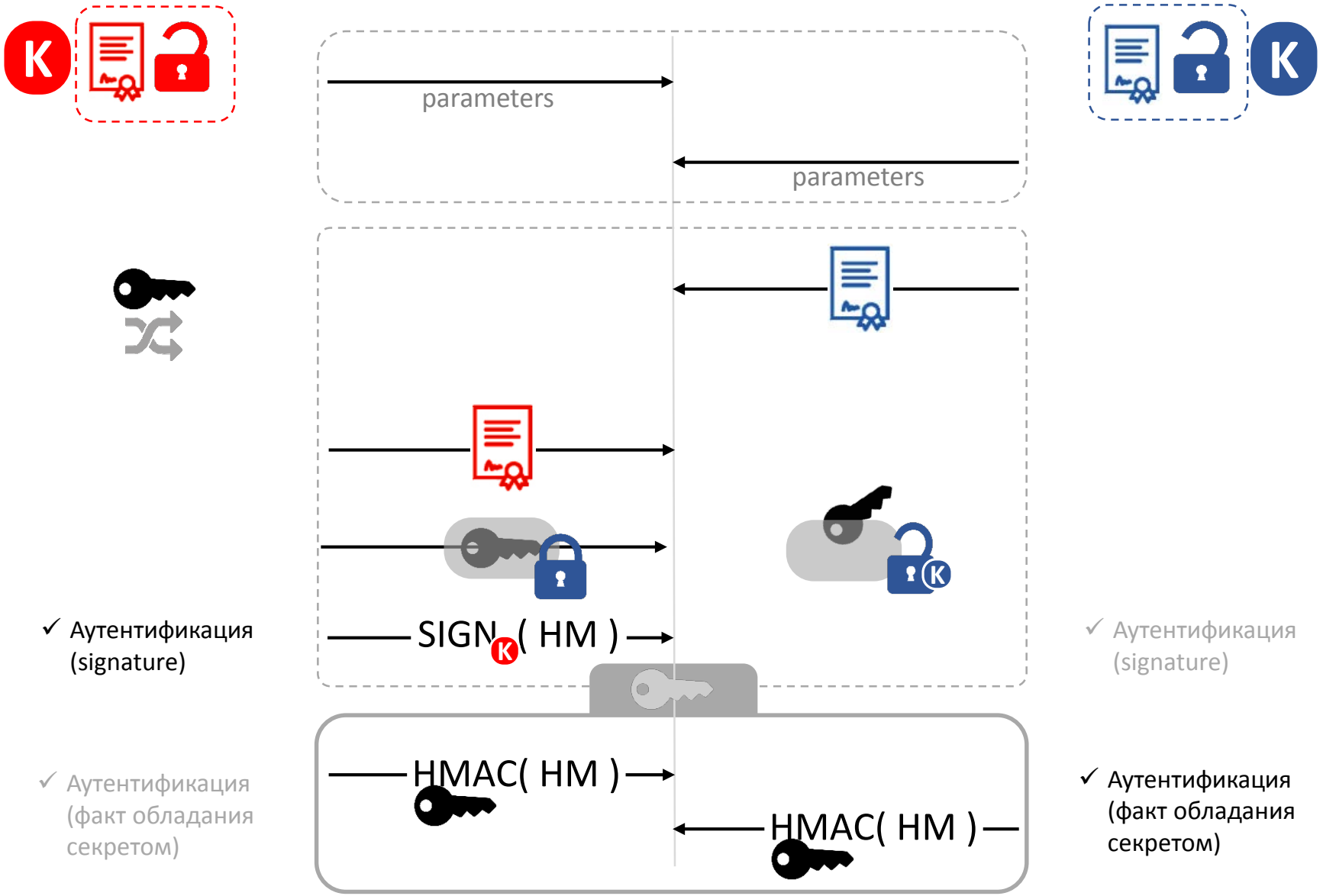
Key Exchange

1. ECDH
2. ECDHE
3. PSK

TLS 1.2 TLS 1.3 IKEv1 IKEv2

TLS 1.2

TLS 1.2



✓ Аутентификация (signature)

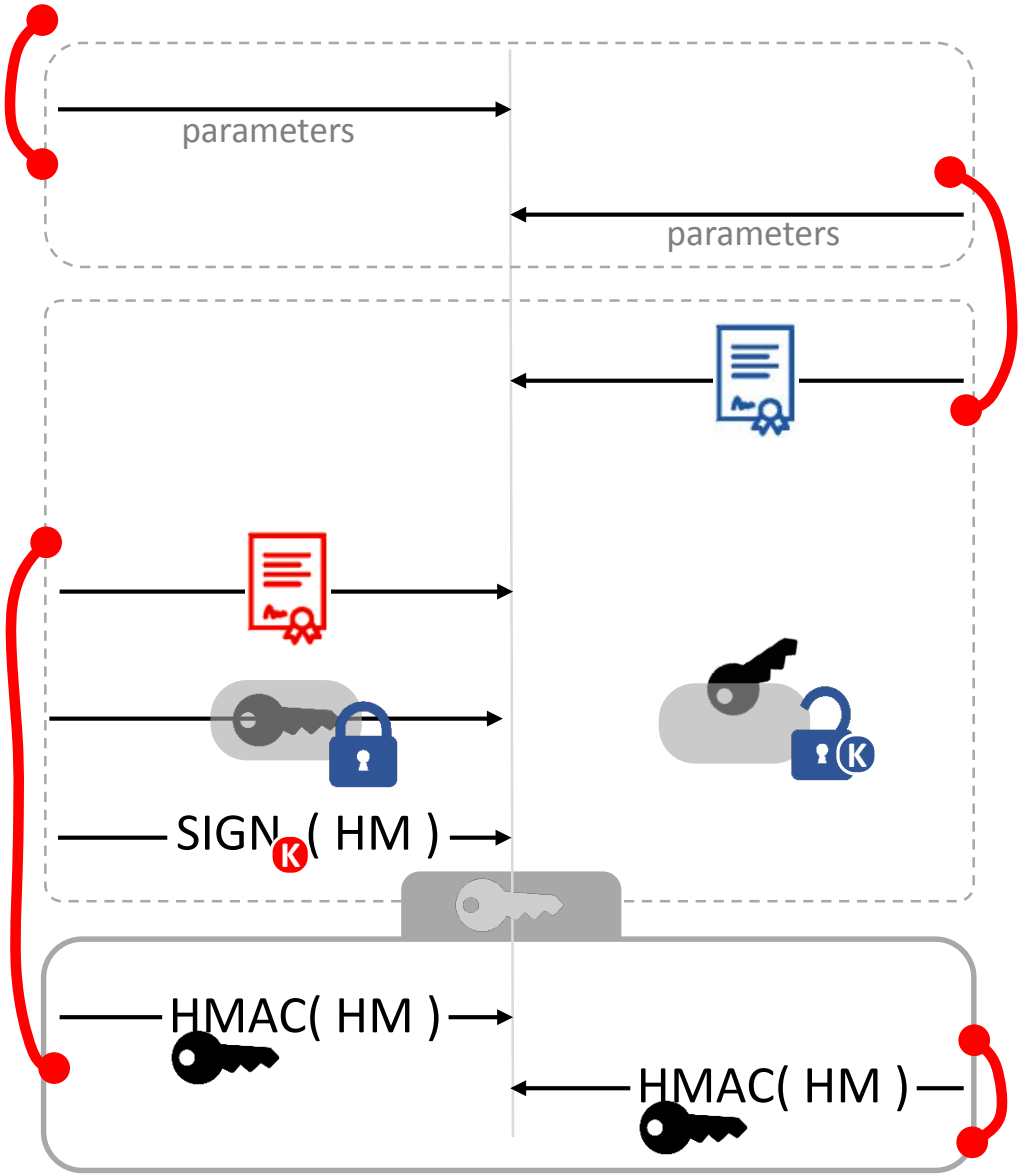
✓ Аутентификация (signature)

✓ Аутентификация (факт обладания секретом)

✓ Аутентификация (факт обладания секретом)

TLS 1.2

4



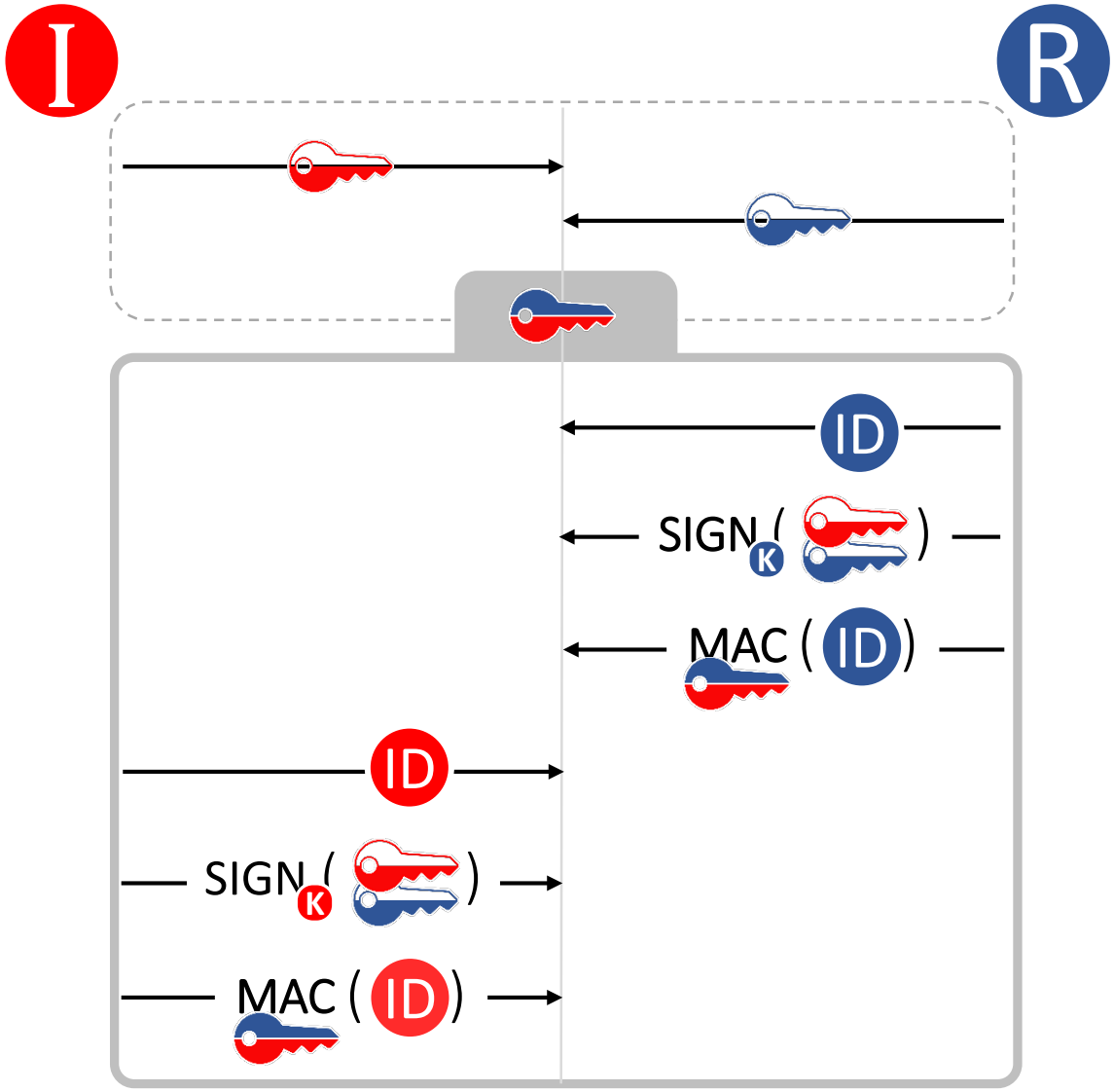
Authenticated Key Exchange

семейство протоколов

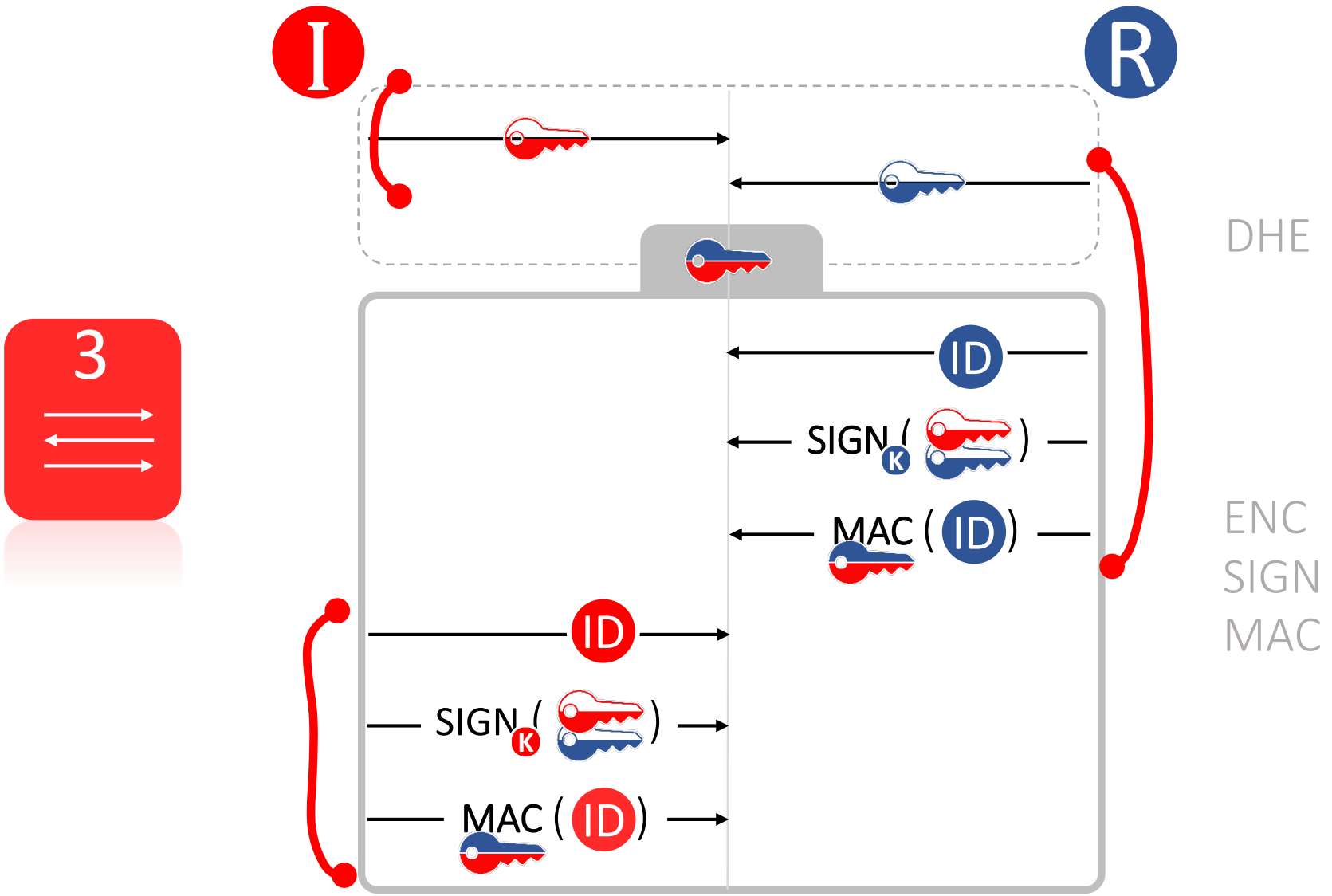
SigMa

TLS 1.2 | TLS 1.3 | IKEv1 | IKEv2

SigMa



SigMa



SigMa

DHE

✓Секретность итогового ключа

SIGN

✓Аутентификация (подпись своего открытого эфемерного ключа)

✓Защита в случае «утечки» закрытого эфемерного ключа (подпись случайных данных партнера)

MAC

✓Устойчивость к UKS атакам (подтверждение своего ID и знания итогового ключа)

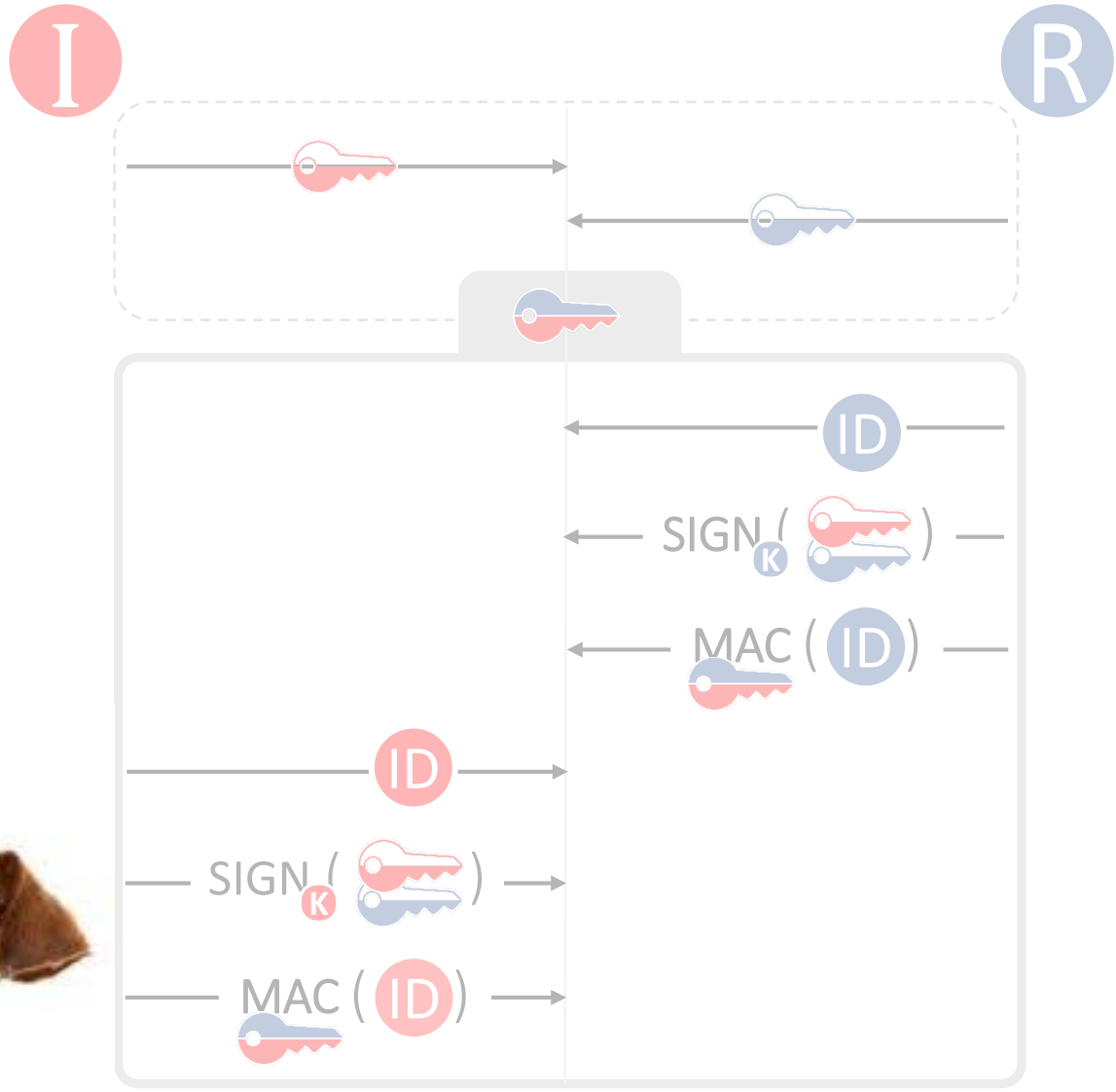
✓Устойчивость к KCI атакам

✓Свойство PFS

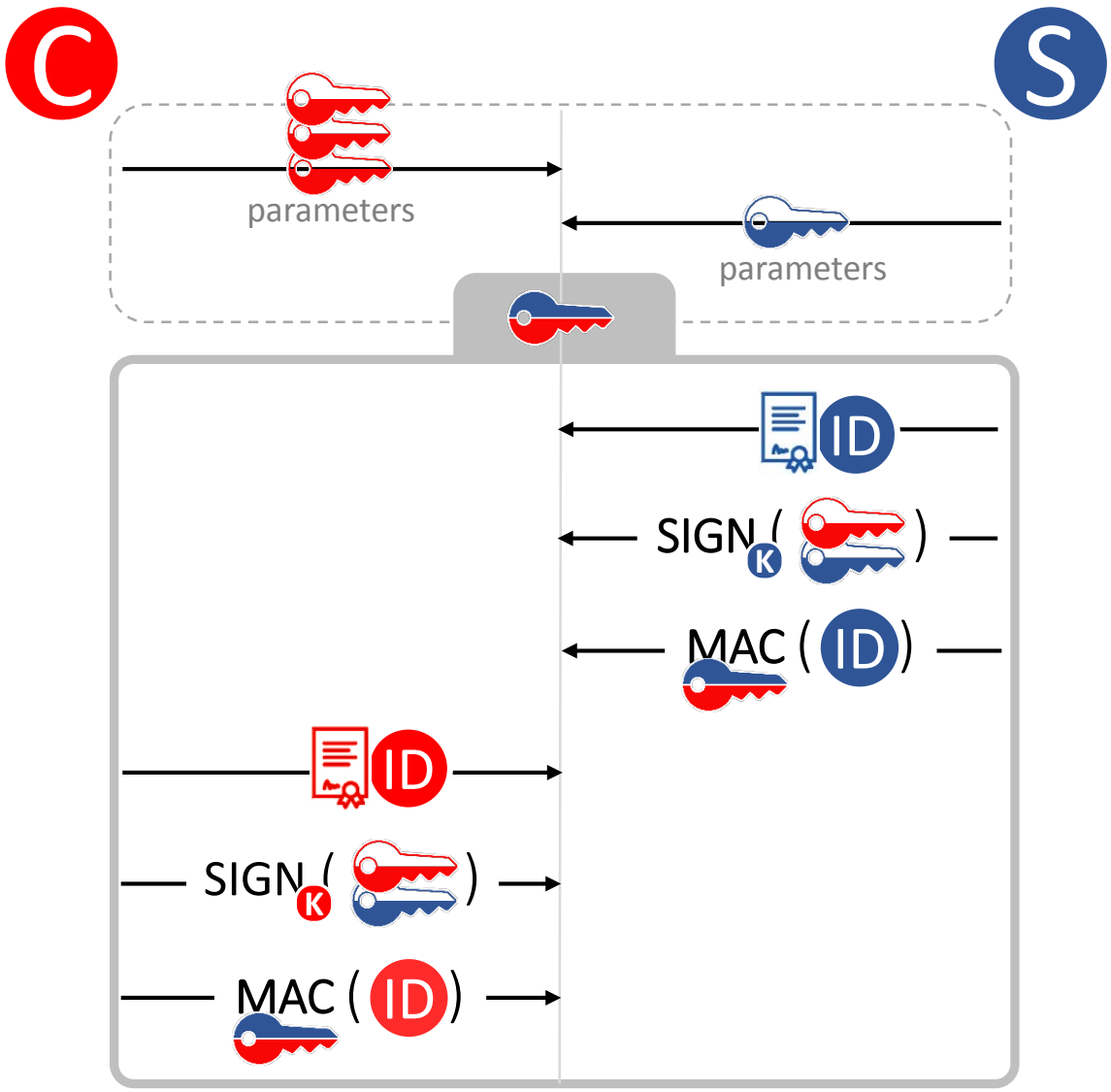
ENC

✓Анонимность (шифрование ID_i, ID_r)

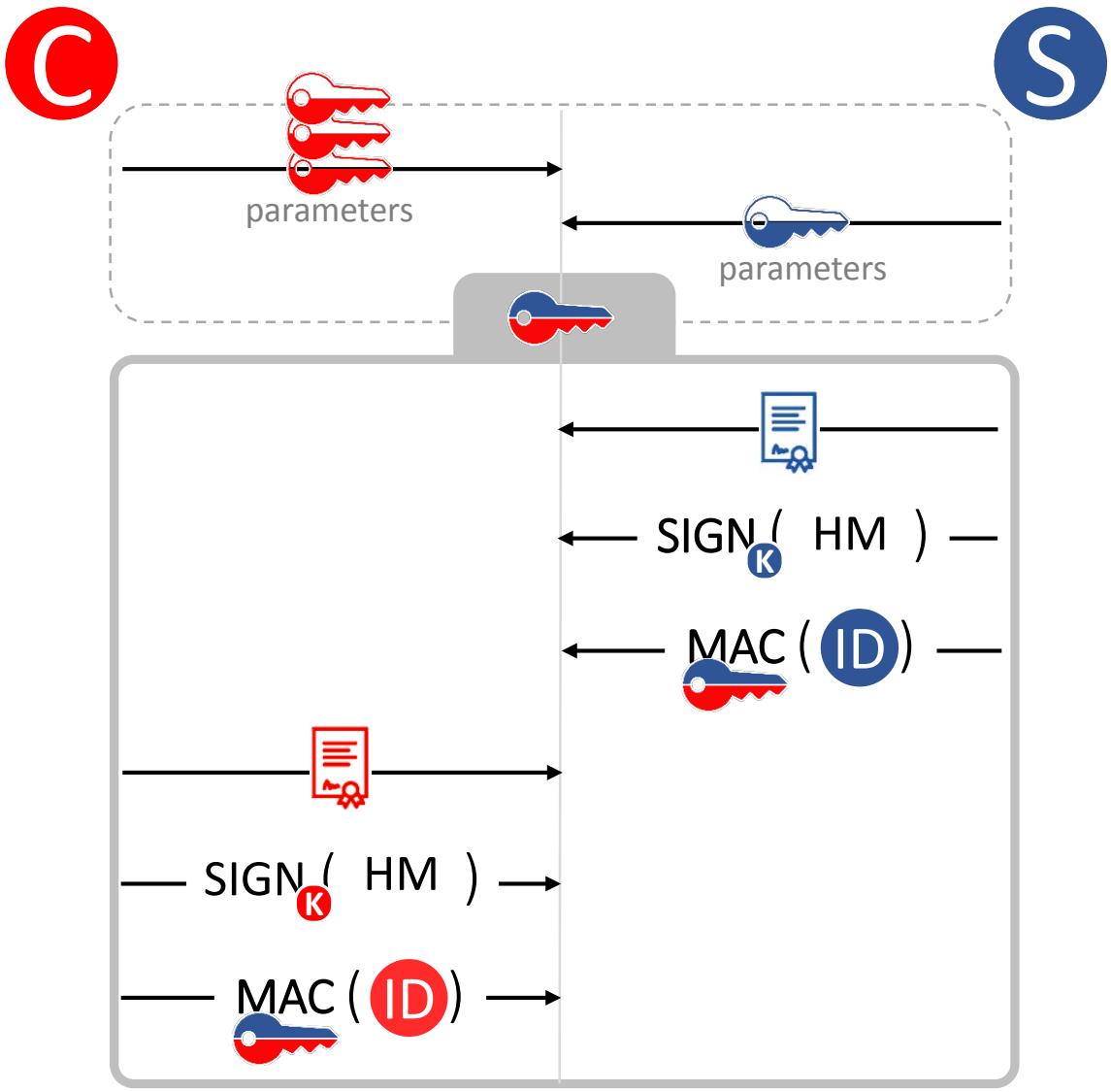
TLS 1.3



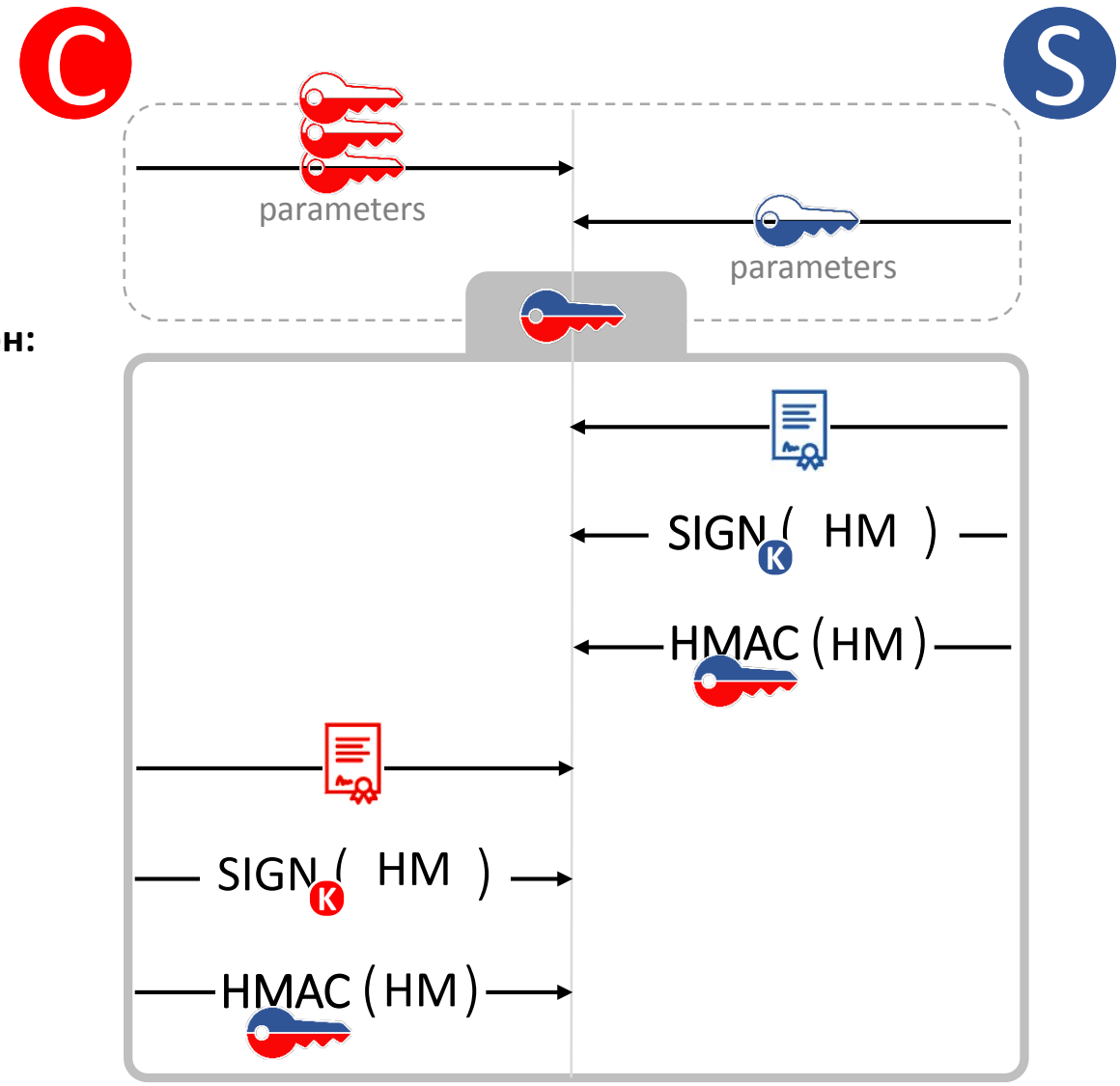
TLS 1.3...



TLS 1.3...



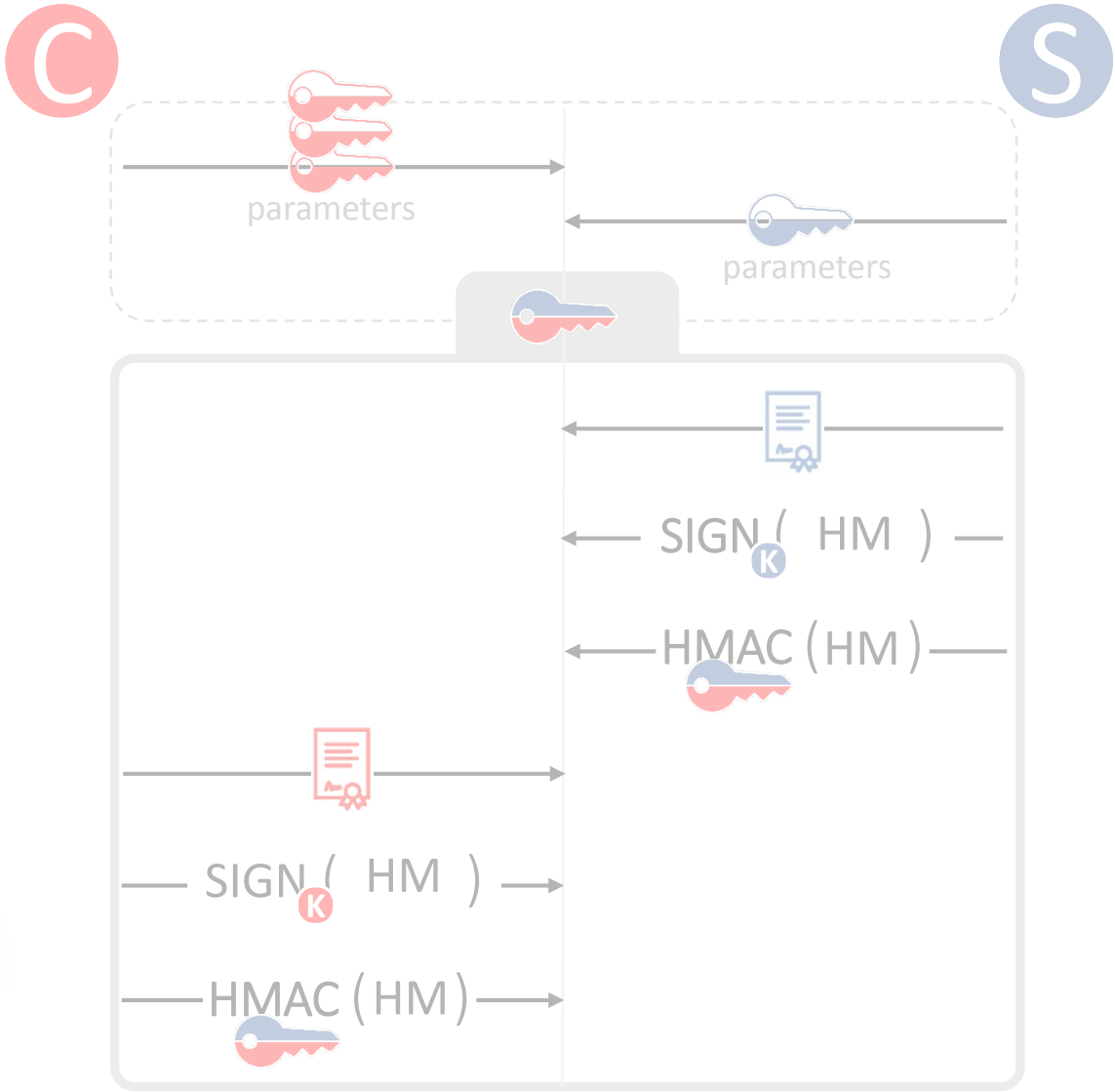
TLS 1.3



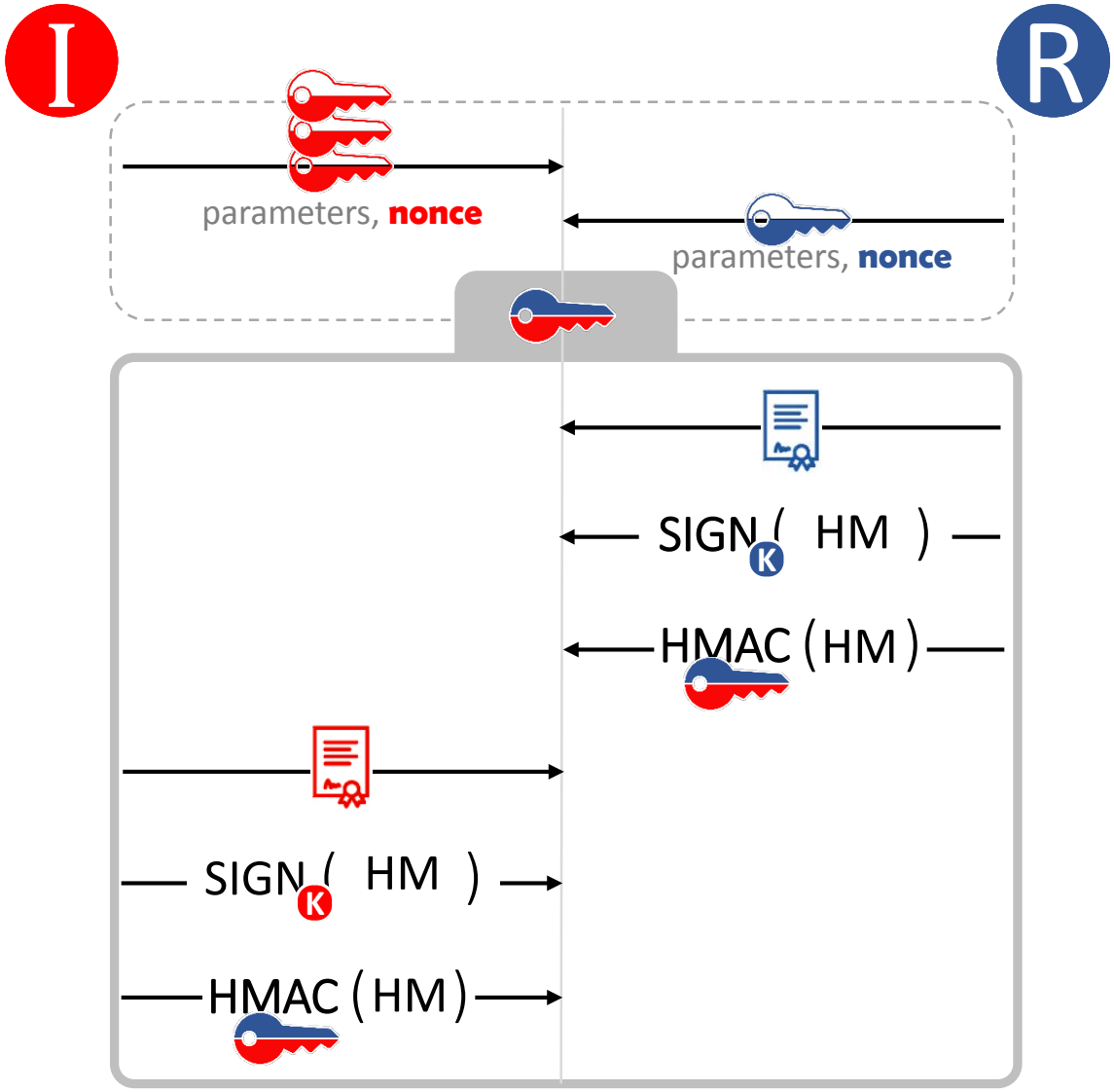
Анонимность сторон:

- Для клиента по отношению к *активному* противнику
- Для сервера по отношению к *пассивному* противнику

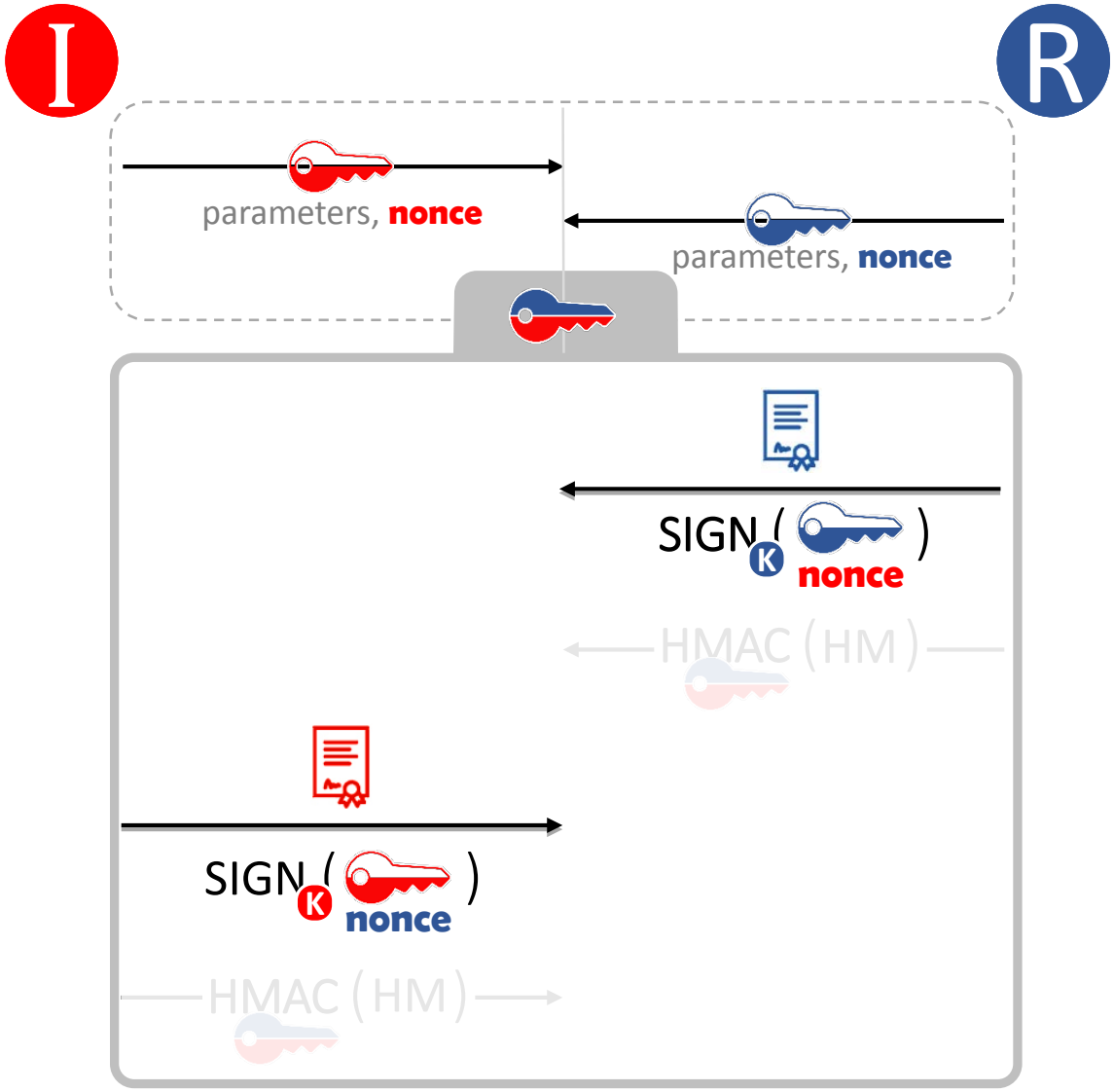
IKE v2



IKE v2...

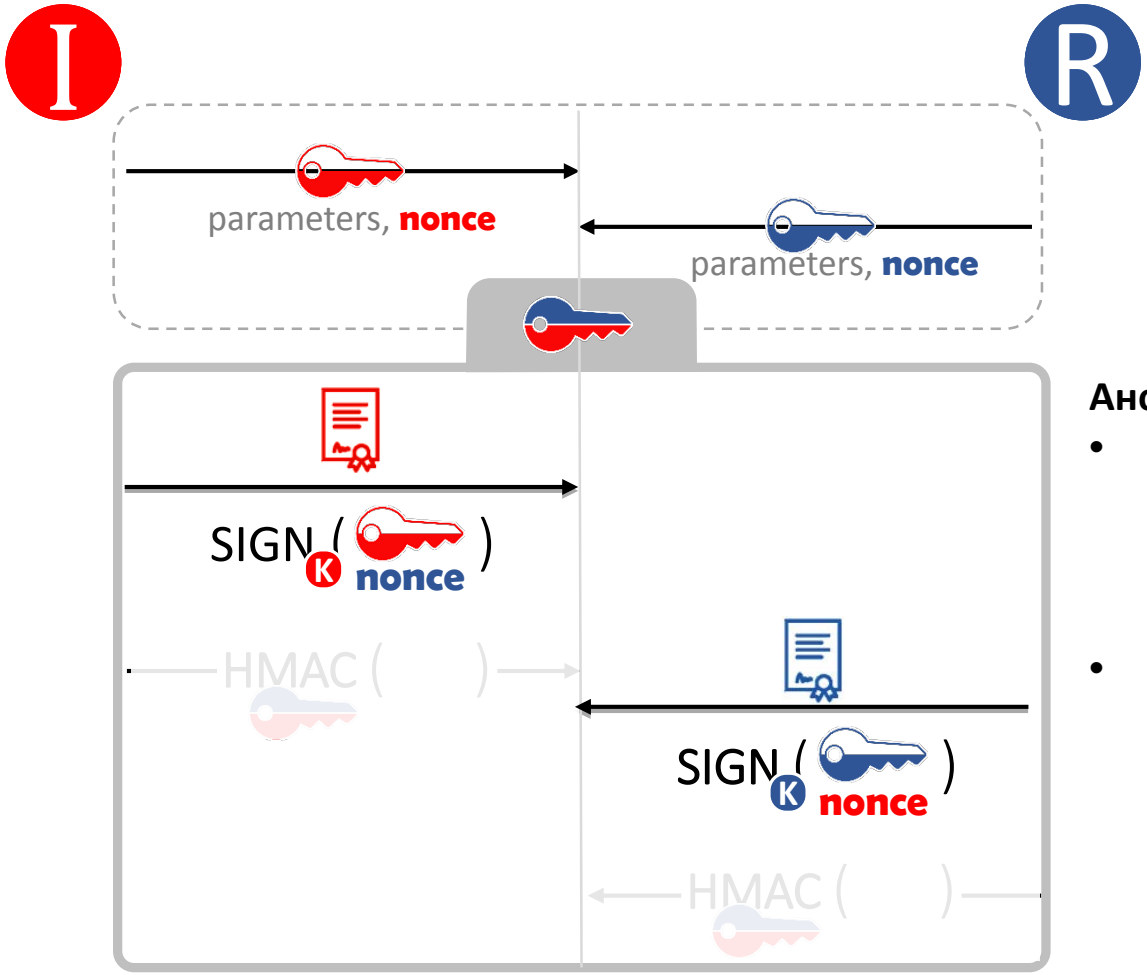

I
R
parameters, nonce
parameters, nonce
SIGN(HM)
HMAC (HM)
SIGN(HM)
HMAC (HM)

IKE v2...


I
R
parameters, nonce
parameters, nonce
SIGN (nonce)
HMAC (HM)
SIGN (nonce)
HMAC (HM)

IKE v2...

4



Анонимность сторон:

- Для инициатора по отношению к *пассивному* противнику
- Для получателя по отношению к *активному* противнику

IKE v2

I

R

parameters, **nonce**

parameters, **nonce**

MAC

SIGN (nonce)

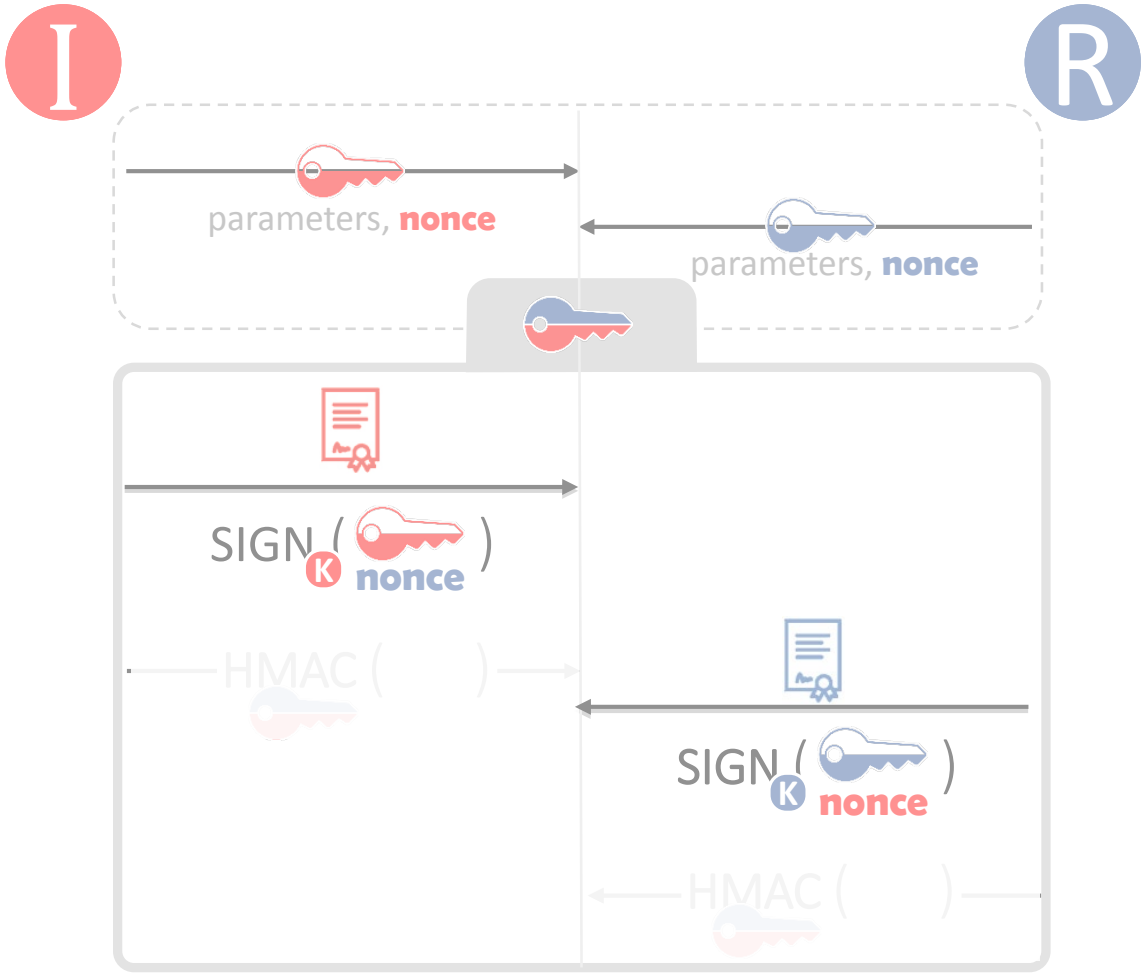
HMAC ( )

SIGN (nonce)

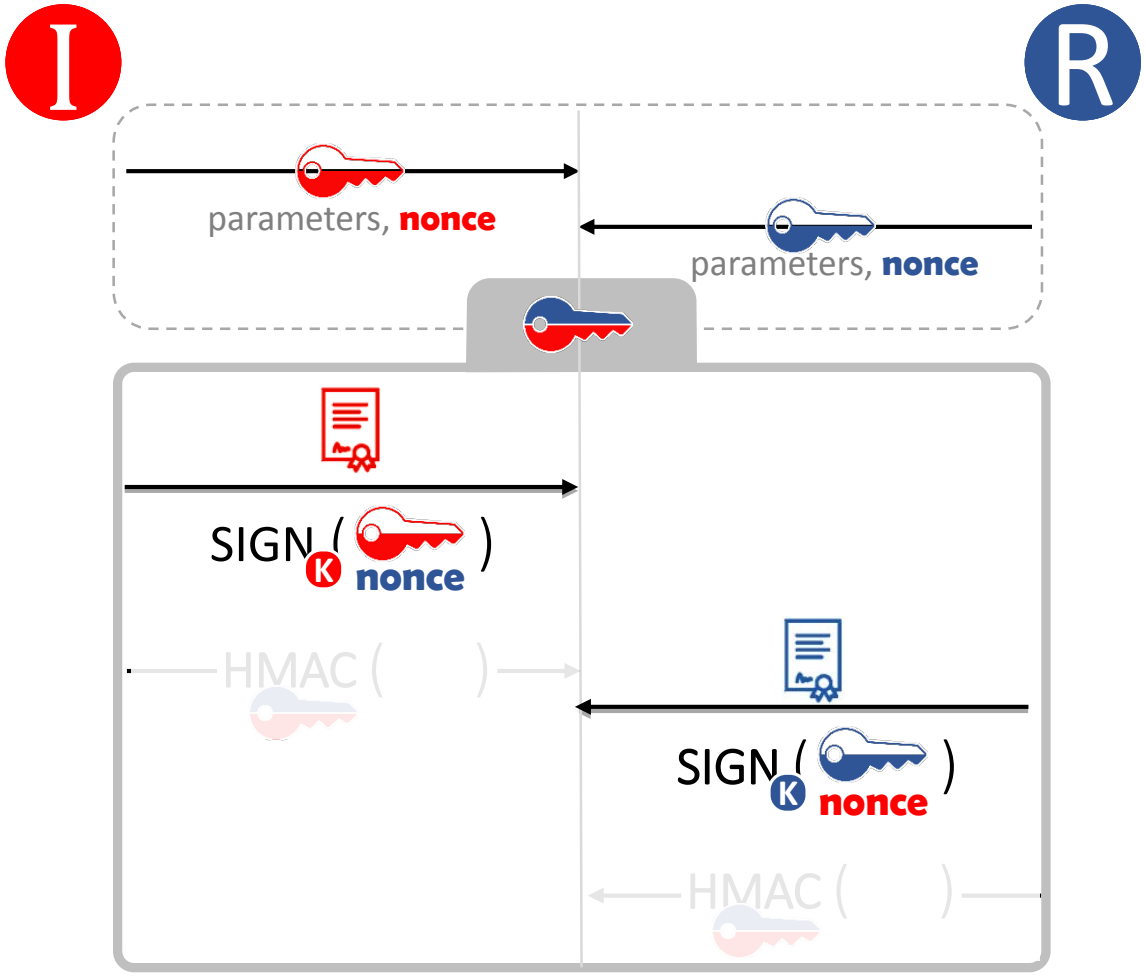
MAC

HMAC ( )

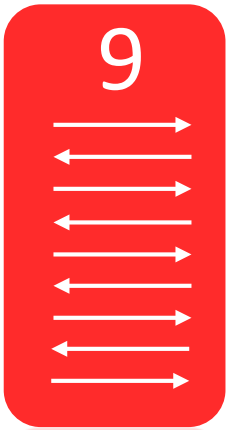
IKE v1

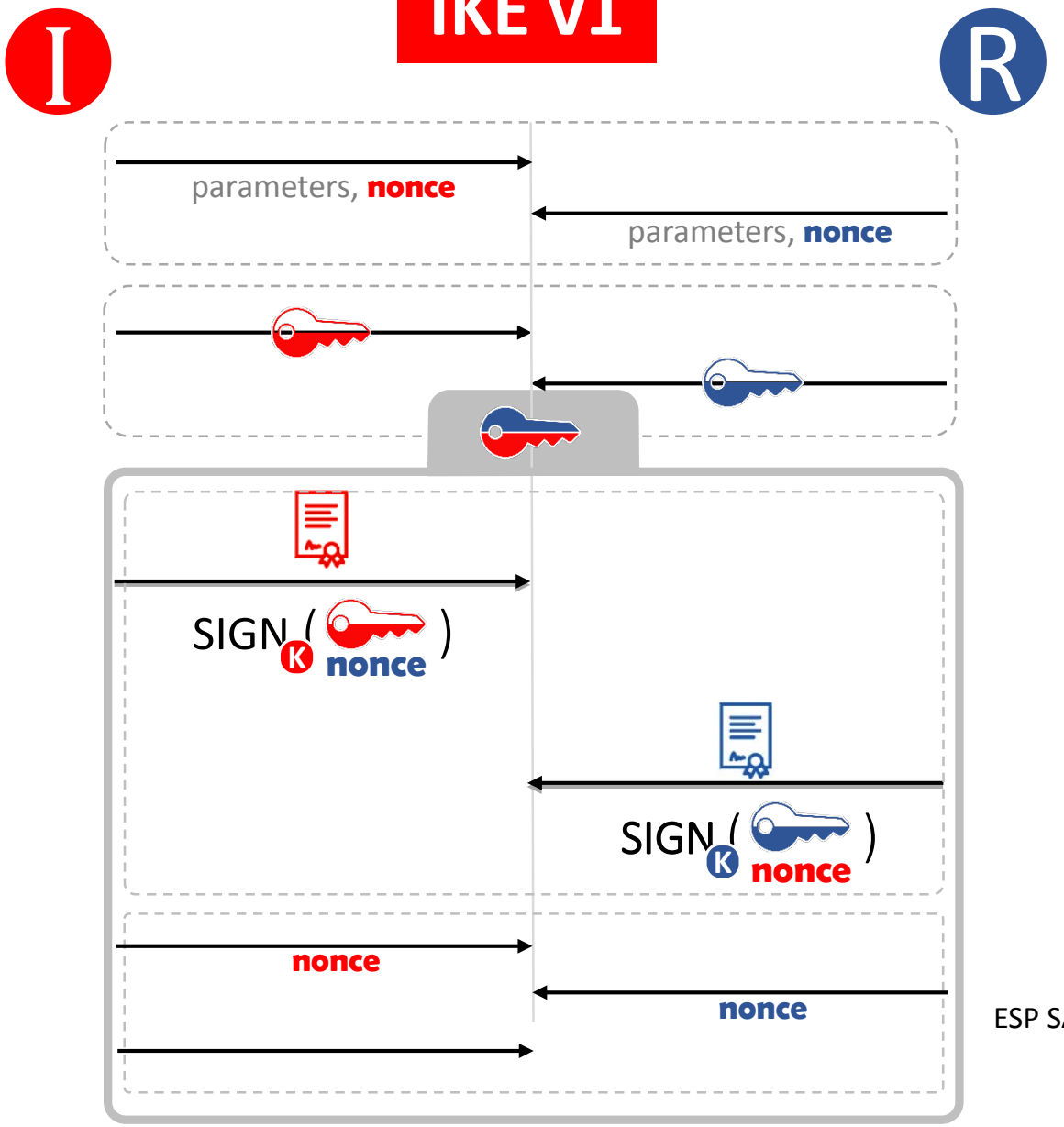

I
R
parameters, nonce
parameters, nonce
SIGN (nonce)
HMAC ( )
SIGN (nonce)
HMAC ( )

IKE v1...


I
R
parameters, nonce
parameters, nonce
SIGN (nonce)
HMAC ( )
SIGN (nonce)
HMAC ( )

IKE v1





ESP SA, ключи

Быстрые режимы создания соединения (без повторной аутентификации)

КРИПТОПРО

Екатерина Смышляева

TLS 1.2

Session resumption

Без DH

TLS 1.3

Internal PSK

[with DH]

IKEv1

Quick mode

[with DH]

IKEv2

CREATE_CHILD_SA

[with DH]

Защита данных

Екатерина Смышляева

TLS 1.2

AtE, EtA, AEAD

- ✓ только AtE
- ✓ TLSTREE
- ✓ CTR-ACPKM

TLS 1.3

AEAD

- ✓ MGM
- ✓ TLSTREE

IPsec ESP

EtA, AEAD

- ✓ MGM
- ✓ ESPTREE/IKETREE

PSK внешний

Екатерина Смышляева

TLS 1.2

Нет

TLS 1.3

ePSK

- ✓ Можно использовать только с DH

IPsec

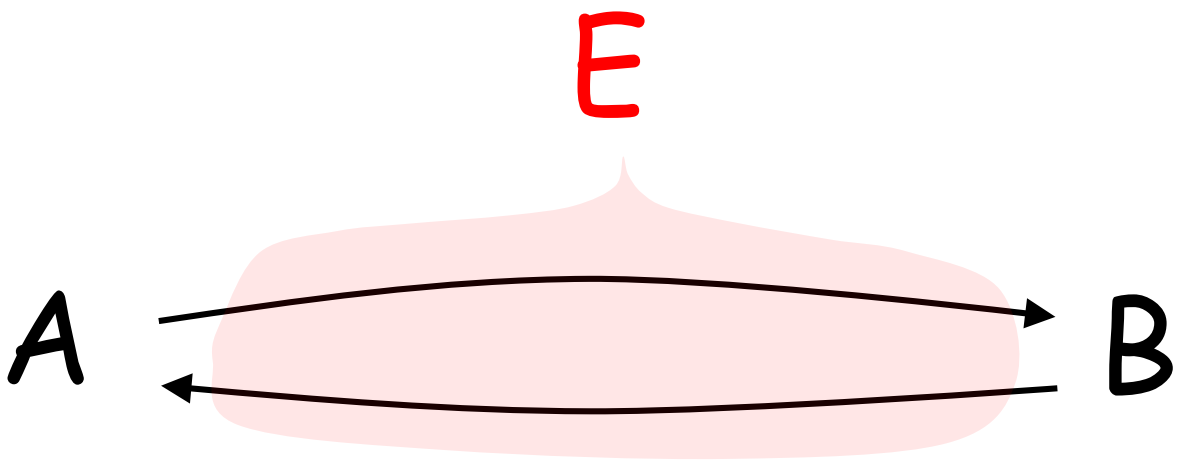
PSK

- ✓ В IKEv2 только для аутентификации

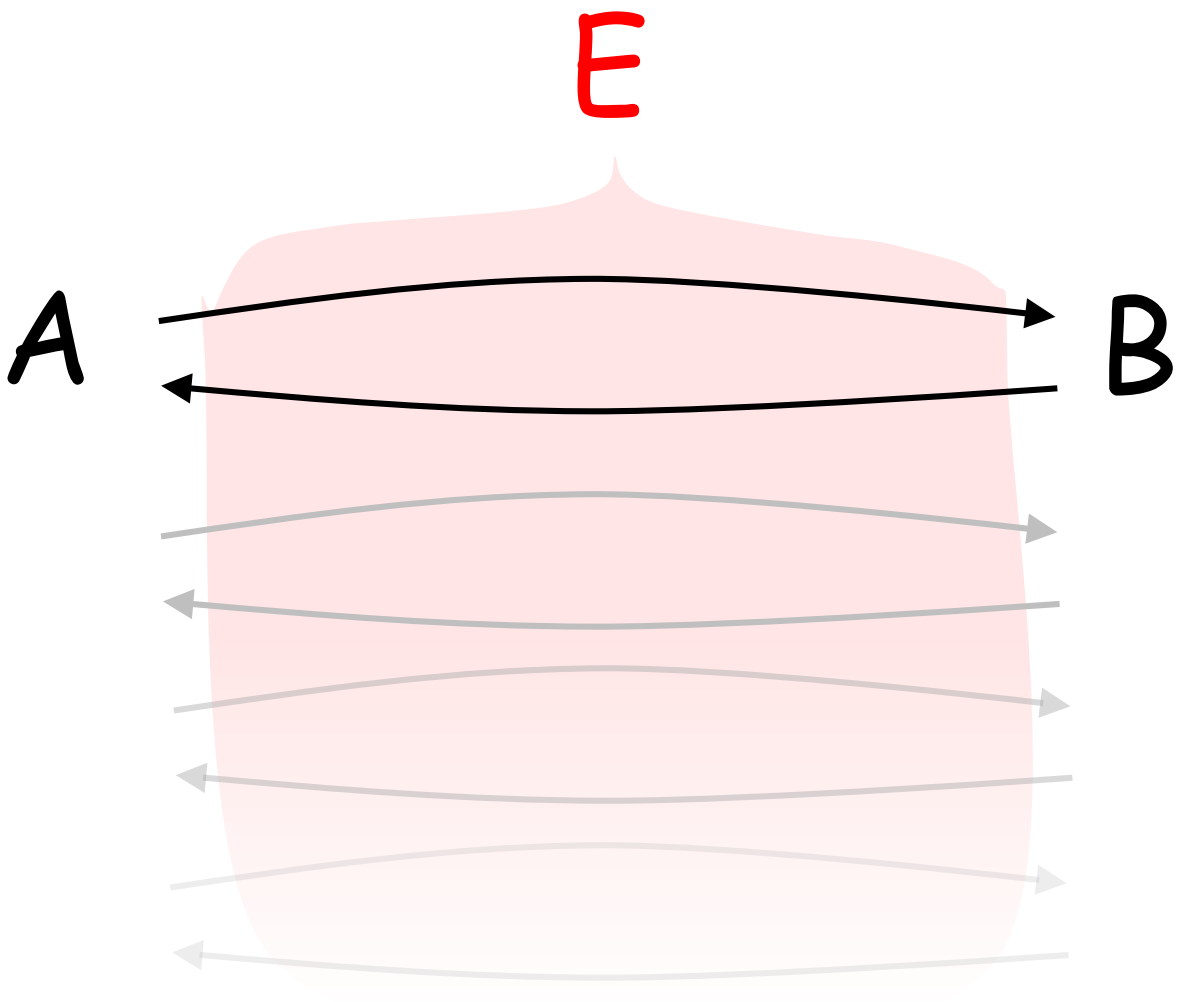
CMS

Cryptographic Message Syntax

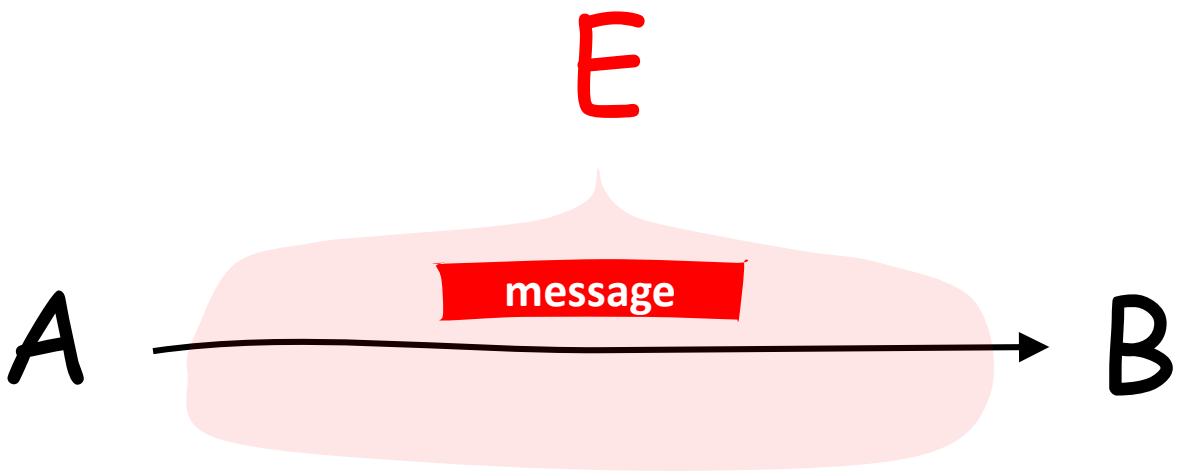
Форматы сообщений, защищенных криптографическими методами



TLS/IPSec



TLS/IPsec



Сообщения CMS являются ASN-структурами, которые хранятся и передаются в закодированном виде

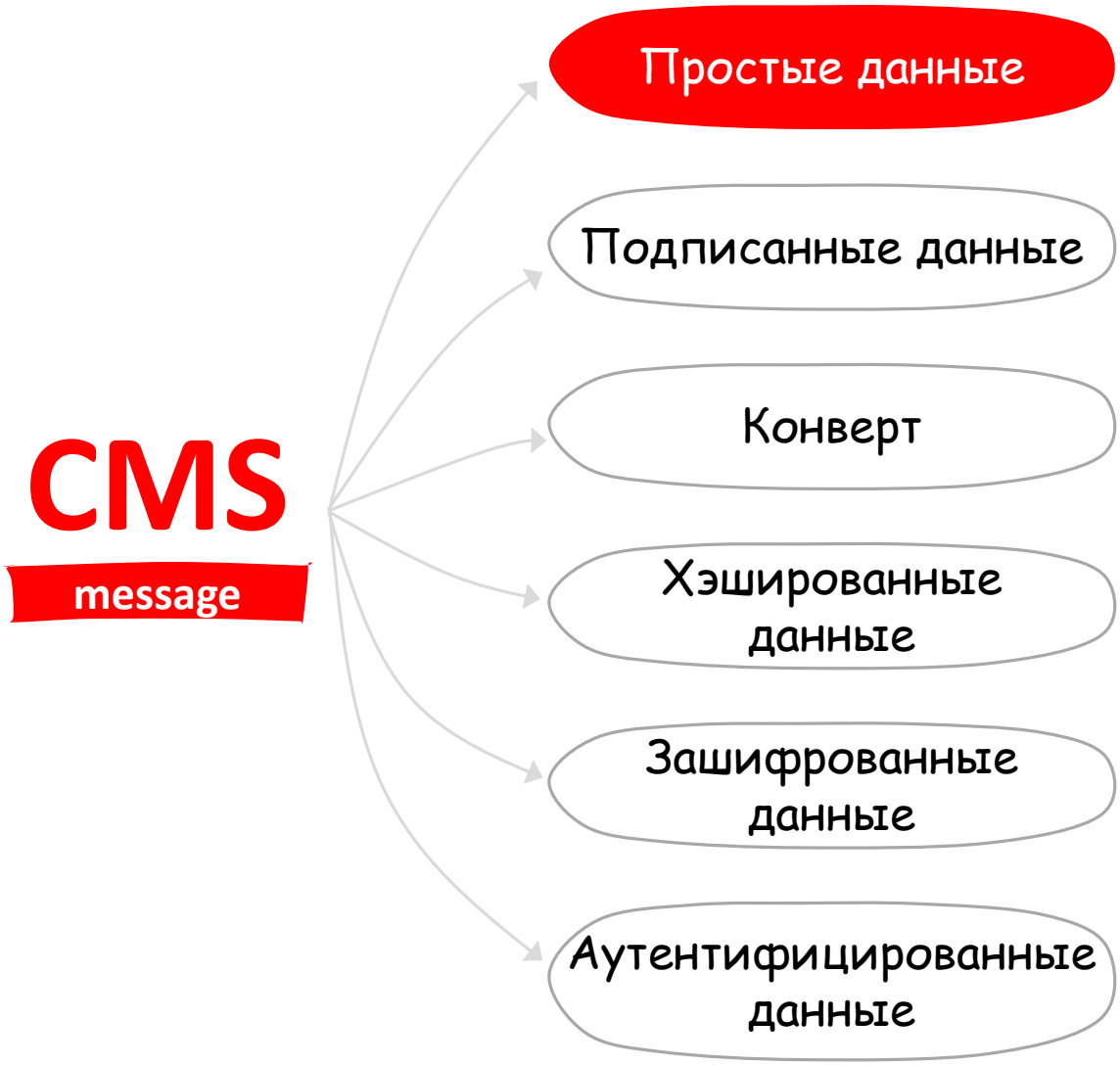
CMS

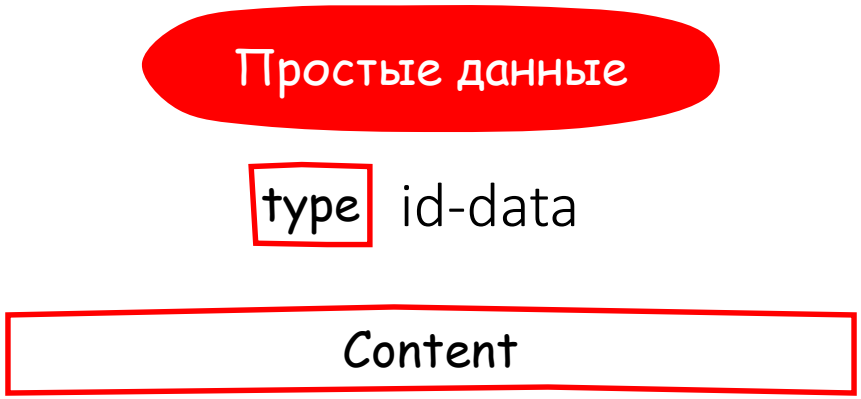
CMS

message

На верхнем уровне ASN-структура сообщения CMS состоит из двух полей:


CMS
message
Простые данные
Подписанные данные
Конверт
Хэшированные данные
Зашифрованные данные
Аутентифицированные данные


CMS
message
Простые данные
Подписанные данные
Конверт
Хэшированные данные
Зашифрованные данные
Аутентифицированные данные



- ✓ Строка байт, например, текстовые файлы ASCII.
- ✓ Не имеет никакой значимой для CMS (но может иметь собственные внутренние структуры)


CMS
message
Простые данные
Подписанные данные
Конверт
Хэшированные данные
Зашифрованные данные
Аутентифицированные данные

Подписанные данные

- ✓ Подпись может быть как с данными, так и без (отделённая)

Подписанные данные

Алгоритмы хэширования HASH

message *

Информация о сертификатах 

$SIGN_{K1}$ $SIGN_{K2}$ . . . $SIGN_{Ki}$

Подписанные данные

Алгоритм хэширования

Подписываемые атрибуты

HASH(message) + Attr

Алгоритм подписи

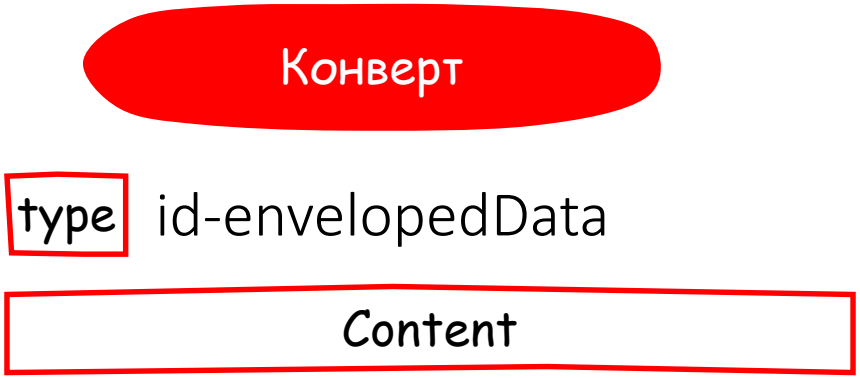
SIGN$_{Ki}$ (?)

message

HASH(message) + Atr

Неподписываемые атрибуты Attr


CMS
message
Простые данные
Подписанные данные
Конверт
Хэшированные данные
Зашифрованные данные
Аутентифицированные данные

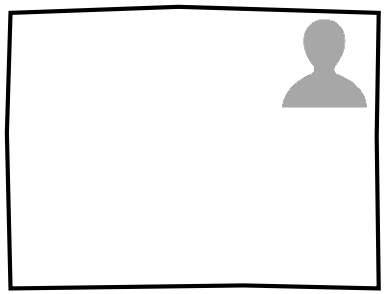


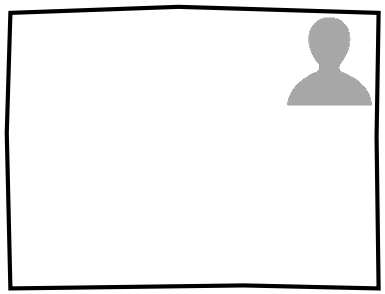
- ✓ Зашифрованные данные могут быть пустыми (используем для передачи ключевого материала)

Конверт

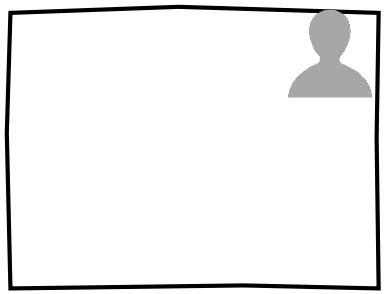
Content

Отправитель  *





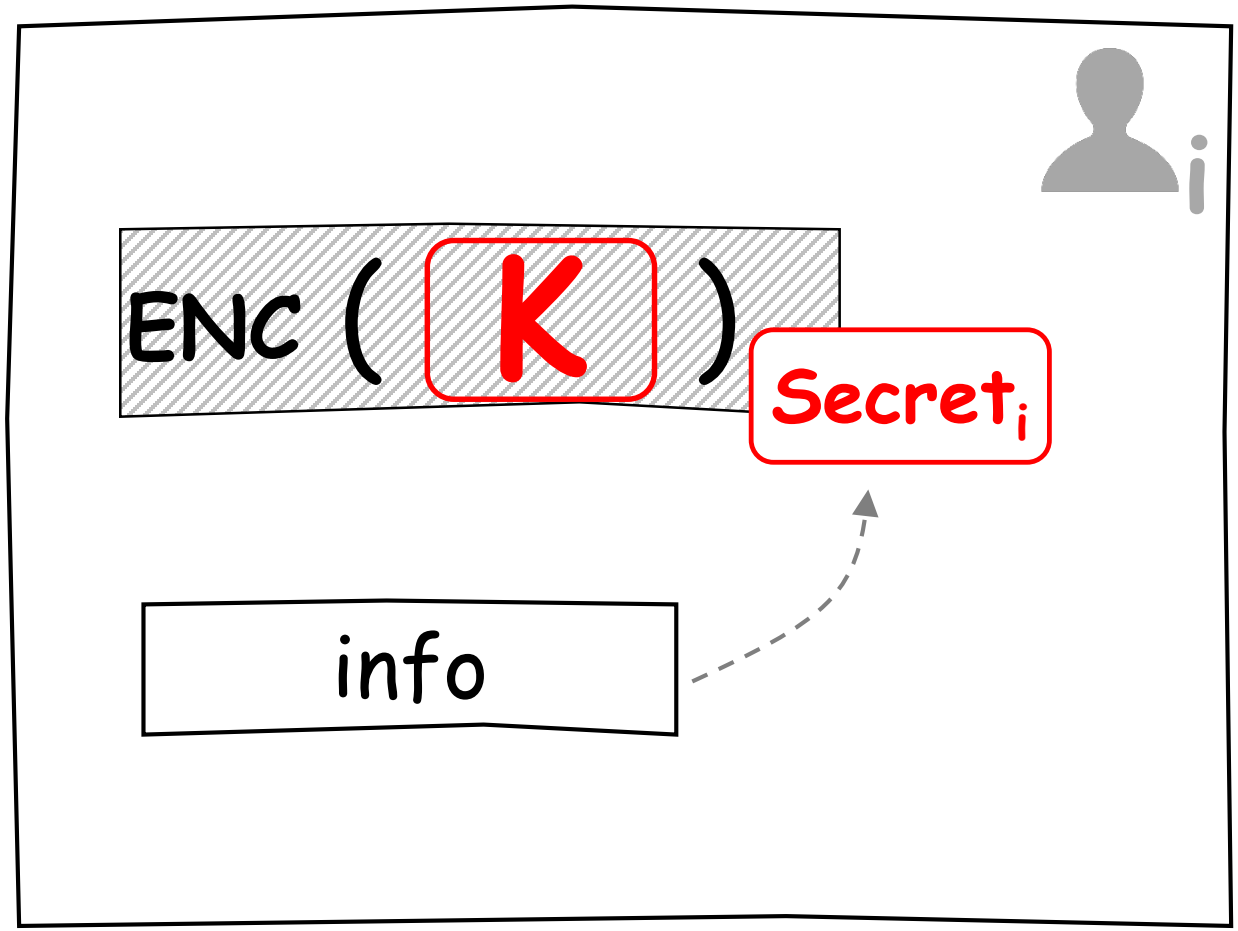
. . .



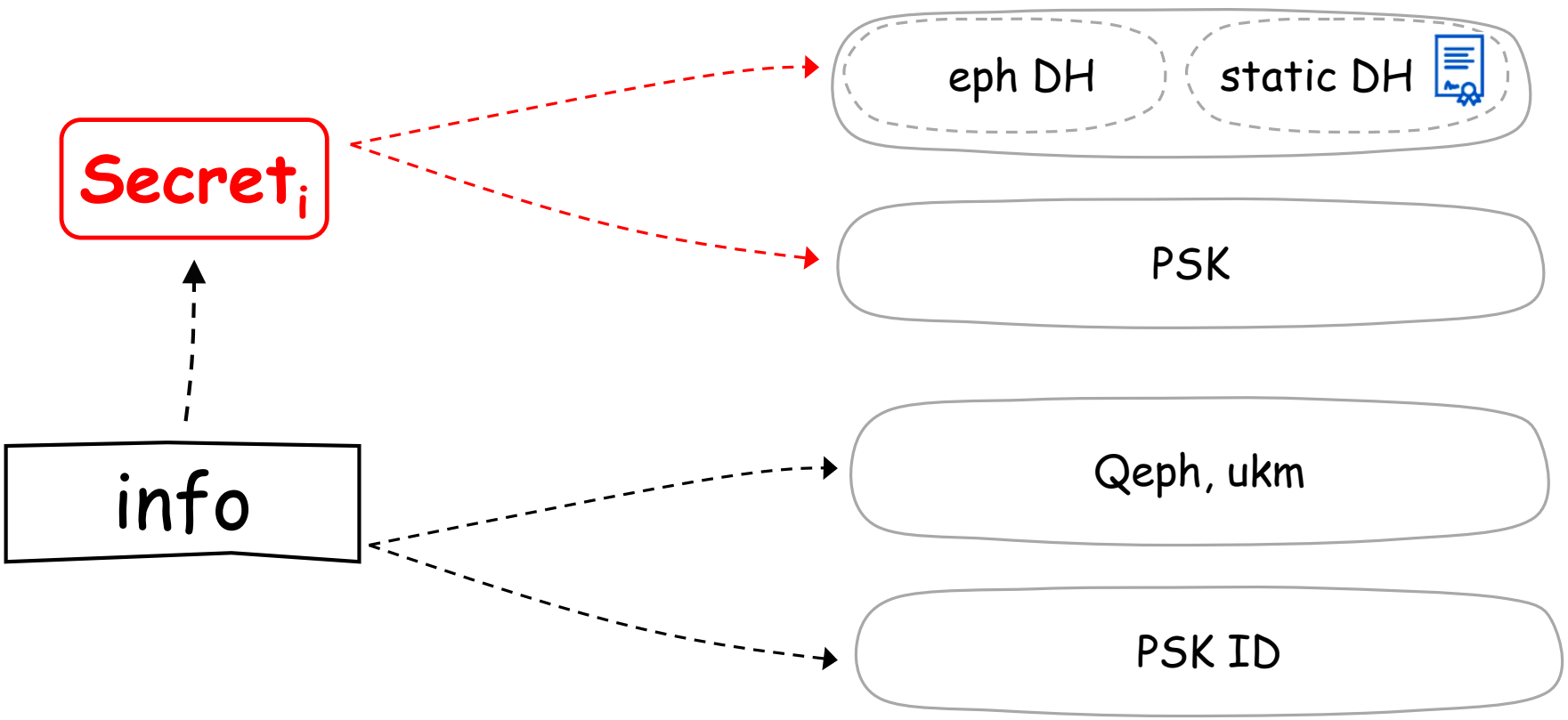
ENC (message) K

Незащищенные атрибуты 

Конверт



Конверт




CMS
message
Простые данные
Подписанные данные
Конверт
Хэшированные данные
Зашифрованные данные
Аутентифицированные данные

Хэшированные данные

type id-digestedData

Content

Алгоритмы хэширования HASH

message *

HASH(message)

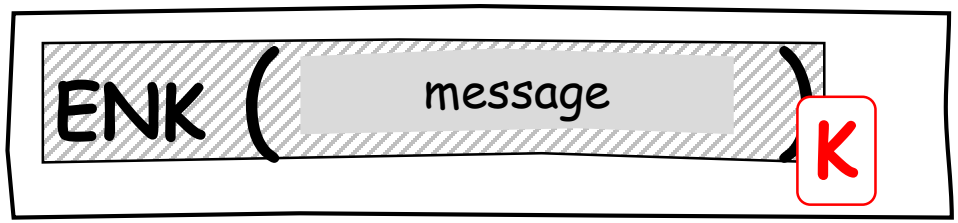
✓ Без получателя


CMS
message
Простые данные
Подписанные данные
Конверт
Хэшированные данные
Зашифрованные данные
Аутентифицированные данные

Зашифрованные данные

type id-encryptedData

Content



- ✓ Хранение шифрованных локальных данных
- ✓ Нет получателей
- ✓ Ключ K получен ранее

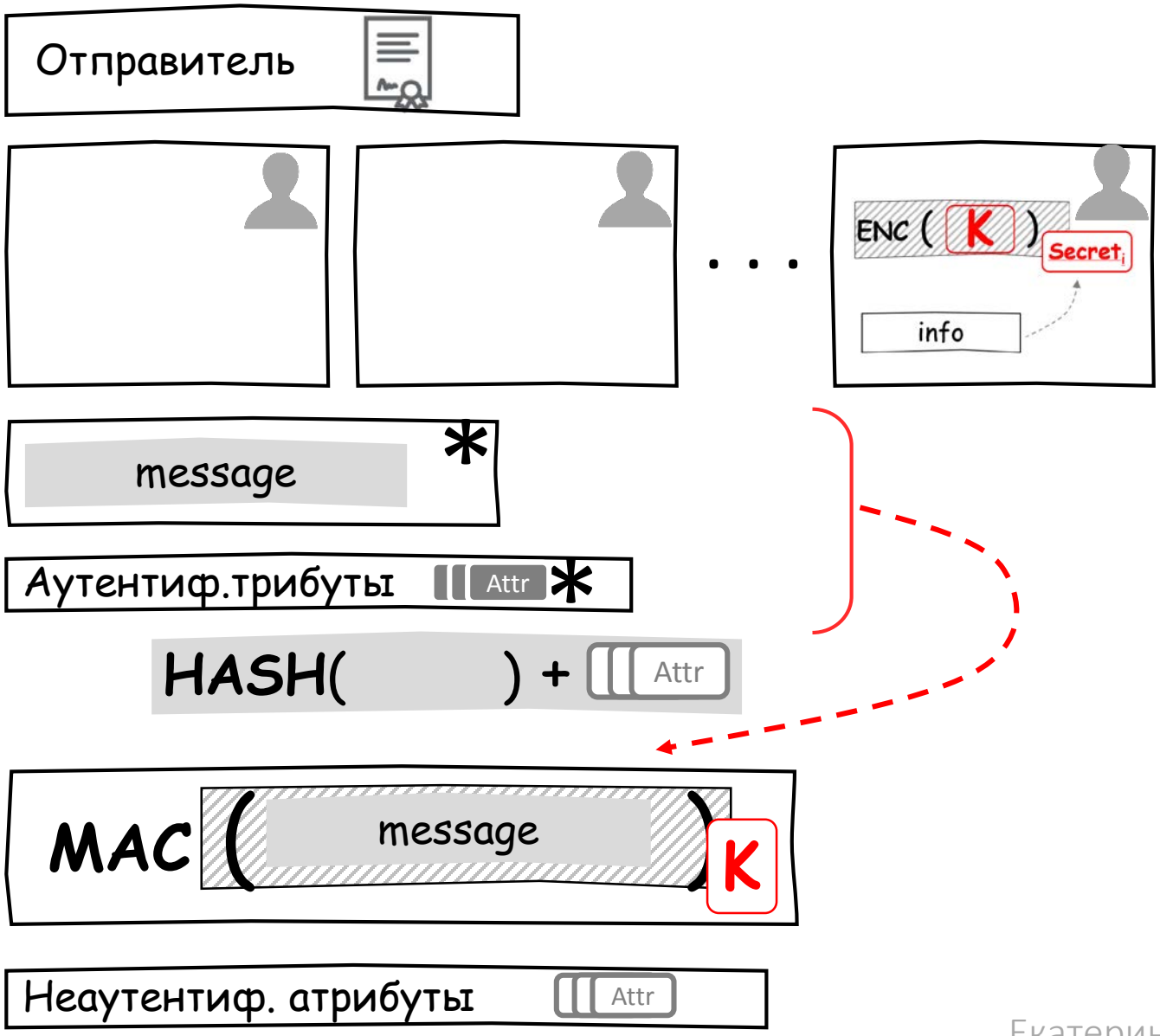

CMS
message
Простые данные
Подписанные данные
Конверт
Хэшированные данные
Зашифрованные данные
Аутентифицированные данные

Аутентифицированные данные

type id-ct-authData

Content

Аутентифицированные данные



Спасибо за внимание!

☺