

СЕТИ. БЕЗОПАСНОСТЬ

Урок 37

RSA, сертификаты и мандаты

Вспоминаем RSA

1. У каждого участника есть закрытый ключ d , открытый ключ e и модуль n
2. Закрытый ключ держится в секрете, открытый публикуется для всех участников
3. Шифровка: $C = M^e \bmod n$, где C – зашифрованное сообщение
4. Расшифровка: $M = C^d \bmod n$, где M – расшифрованное сообщение

d e n

Публичный ключ

e n

$$M^e \bmod n = Se$$

Приватный ключ

d n

$$Se^d \bmod n = M$$

Схема RSA

Общеизвестны

e_p	n_p
-------	-------

e_s	n_s
-------	-------

Пользователь

d_p	e_p	n_p
-------	-------	-------

$$S = M^{e_s} \bmod n_s$$

Шифруем
публичным ключом получателя

$\{ S \}$

Сайт

d_s	e_s	n_s
-------	-------	-------

$$M = S^{d_s} \bmod n_s$$

Расшифровываем
приватным ключом получателя

Схема ЭЦП

Общеизвестны

e_p	n_p
-------	-------

e_s	n_s
-------	-------

Пользователь

d_p	e_p	n_p
-------	-------	-------

$$E = M^{d_p} \bmod n_p$$

Шифруем
приватным ключом отправителя

E

Сайт

d_s	e_s	n_s
-------	-------	-------

$$M = E^{e_p} \bmod n_p$$

Расшифровываем
публичным ключом отправителя

Схема ЭЦП

Общеизвестны

e_p	n_p
-------	-------

e_s	n_s
-------	-------

Пользователь

d_p	e_p	n_p
-------	-------	-------

$\left\{ \begin{array}{l} hm = \text{Hash}(M) \\ E = hm^{d_p} \bmod n_p \end{array} \right\}$

Шифруем
приватным ключом отправителя

$\{ M, E \}$

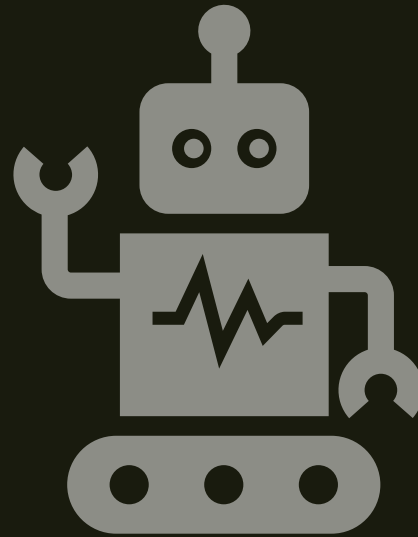
Сайт

d_s	e_s	n_s
-------	-------	-------

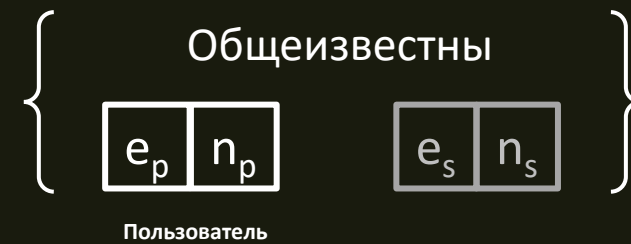
$\left\{ \begin{array}{l} hm = \text{Hash}(M) \\ hm' = E^{e_p} \bmod n_p \\ \text{hm} == \text{hm}' \end{array} \right\}$

Расшифровываем
публичным ключом отправителя

Практика



Подмена



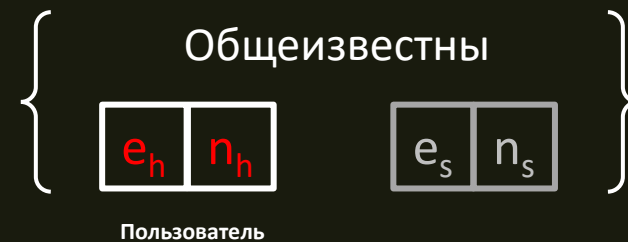
Пользователь



Сайт



Подмена



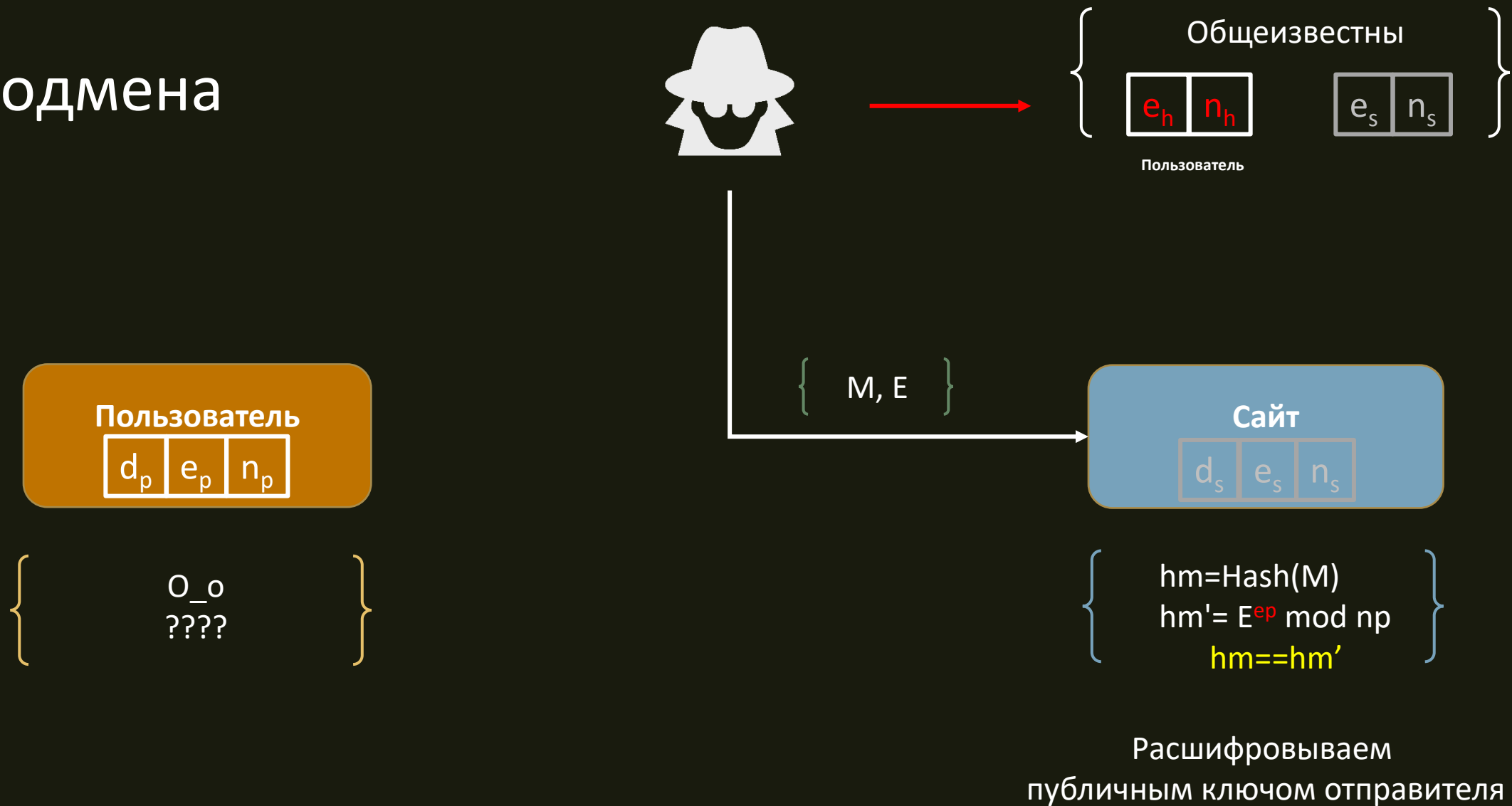
Пользователь



Сайт



Подмена



Сертификаты



Пользователь

d_p	e_p	n_p
-------	-------	-------

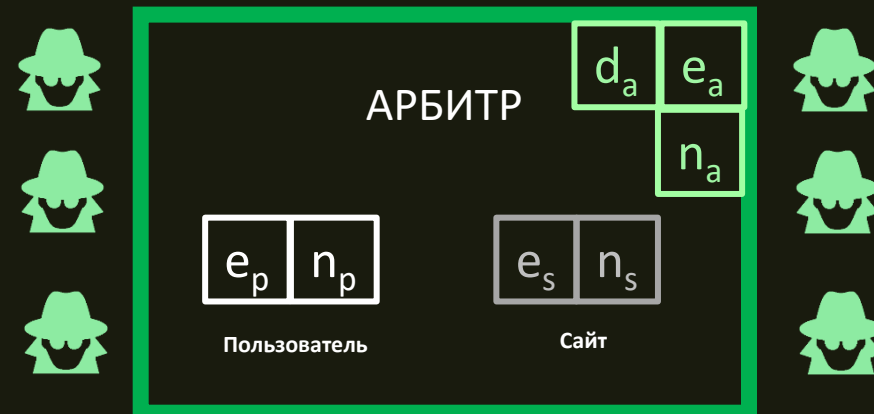
Сайт

d_s	e_s	n_s	e_a	n_a
-------	-------	-------	-------	-------

Сертификаты

Пользователь

d_p	e_p	n_p
-------	-------	-------



Сайт

d_s	e_s	n_s	e_a	n_a
-------	-------	-------	-------	-------

$$\left\{ Z = (\text{Пользователь})^{e_a} \bmod n_a \right\}$$

Сертификаты

Пользователь

d_p e_p n_p

$$\left\{ \begin{array}{l} ZE = [e_p]^{d_a} \bmod n_a \\ ZN = [n_p]^{d_a} \bmod n_a \end{array} \right\}$$



ZE, ZN

Z

Сайт

d_s e_s n_s e_a n_a

$$Z = (\text{Пользователь})^{e_a} \bmod n_a$$

Сертификаты

$$\left\{ \begin{array}{l} ZE = [e_p]^{d_a} \bmod n_a \\ ZN = [n_p]^{d_a} \bmod n_a \end{array} \right\}$$



ZE, ZN

Z

Пользователь



Сайт

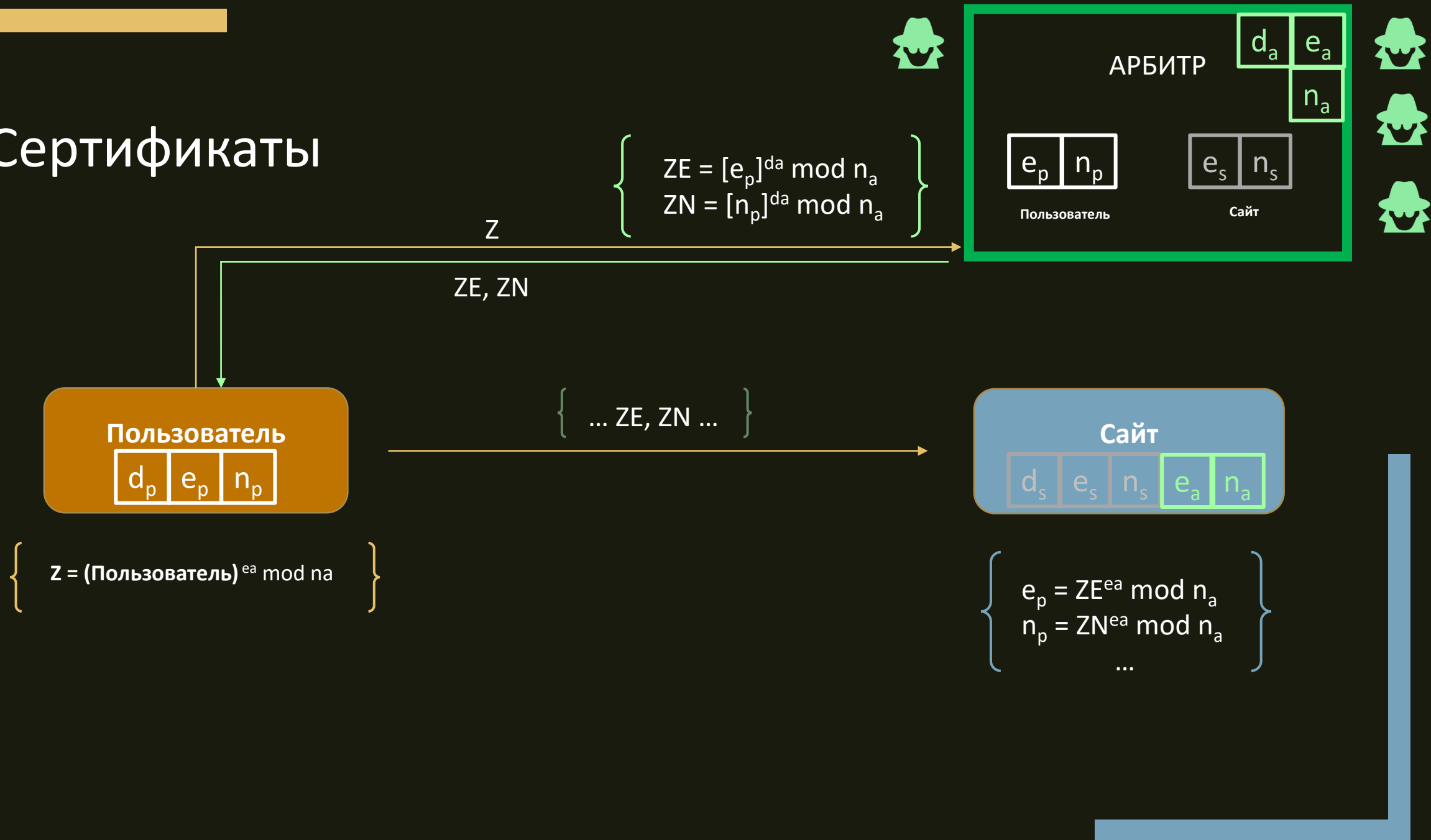


RSA, ЭЦП...

$$Z = (\text{Пользователь})^{e_a} \bmod n_a$$

$$\left\{ \begin{array}{l} e_p = ZE^{e_a} \bmod n_a \\ n_p = ZN^{e_a} \bmod n_a \end{array} \right\}$$

Сертификаты



Сертификаты

- Подтверждает **подлинность** ключей
- Подтверждает **подлинность** собеседника/сайта
- Требуется наличие **доверенного арбитра**
- Бывают **самоподписанными**

Доверенные корневые центры сертификации				Доверенные издатели	Издатели, не
Кому выдан	Кем выдан	Срок де...	Понятное имя		
AAA Certificate Ser...	AAA Certificate Services	01.01.2029	Sectigo (AAA)		
Actalis Authenticati...	Actalis Authentication...	22.09.2030	Actalis Authentic...		
AddTrust External ...	AddTrust External CA...	30.05.2020	Sectigo (AddTrust)		
AffirmTrust Comme...	AffirmTrust Commercial	31.12.2030	AffirmTrust Com...		
Baltimore CyberTru...	Baltimore CyberTrust ...	13.05.2025	DigiCert Baltimor...		
Blizzard Battle.net ...	Blizzard Battle.net Loc...	20.12.2027	<нет>		
Certification Author...	Certification Authority...	08.08.2039	WoSign		
Certum CA	Certum CA	11.06.2027	Certum		
Certum Trusted Ne...	Certum Trusted Netw...	31.12.2029	Certum Trusted ...		

Практика

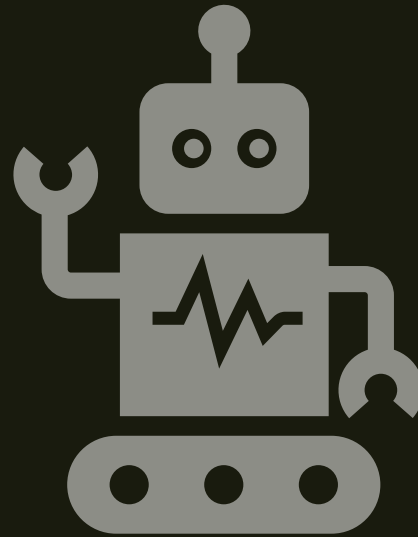


Схема мандата

Арбитр-секретарь

e_s	n_s	e_a	d_a	n_a
-------	-------	-------	-------	-------

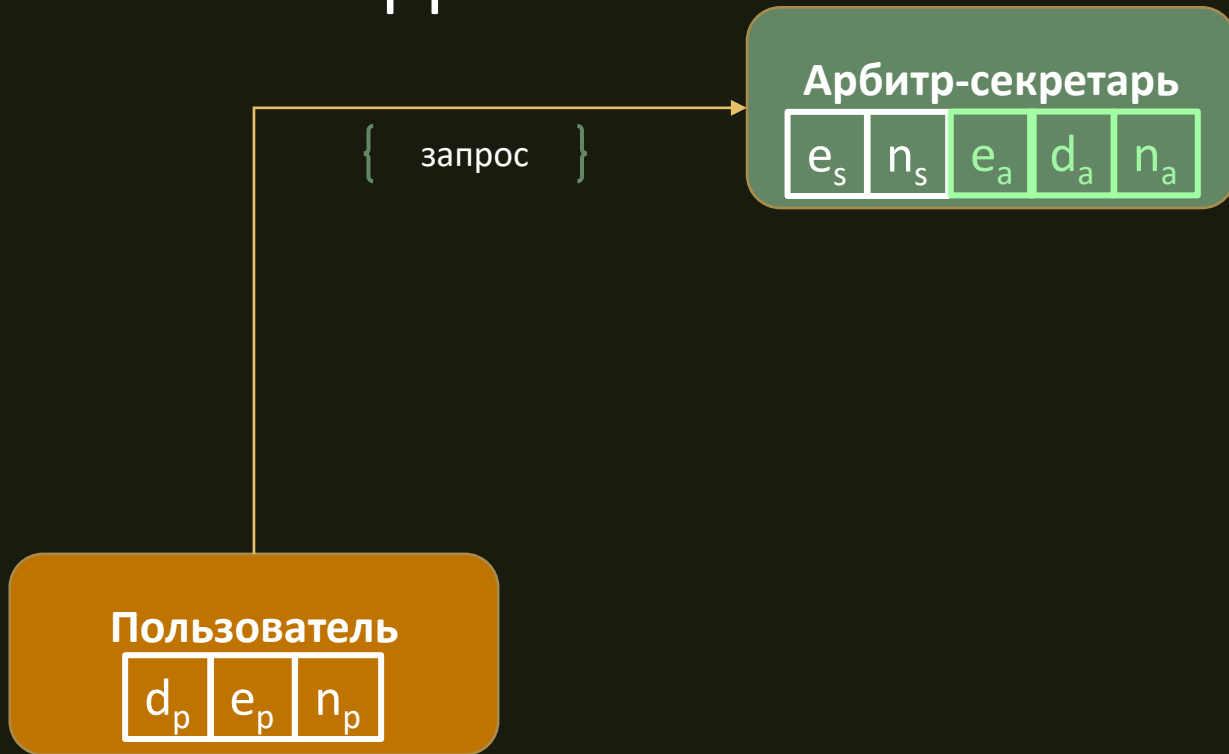
Пользователь

d_p	e_p	n_p
-------	-------	-------

Сайт

d_s	e_s	n_s	e_a	n_a
-------	-------	-------	-------	-------

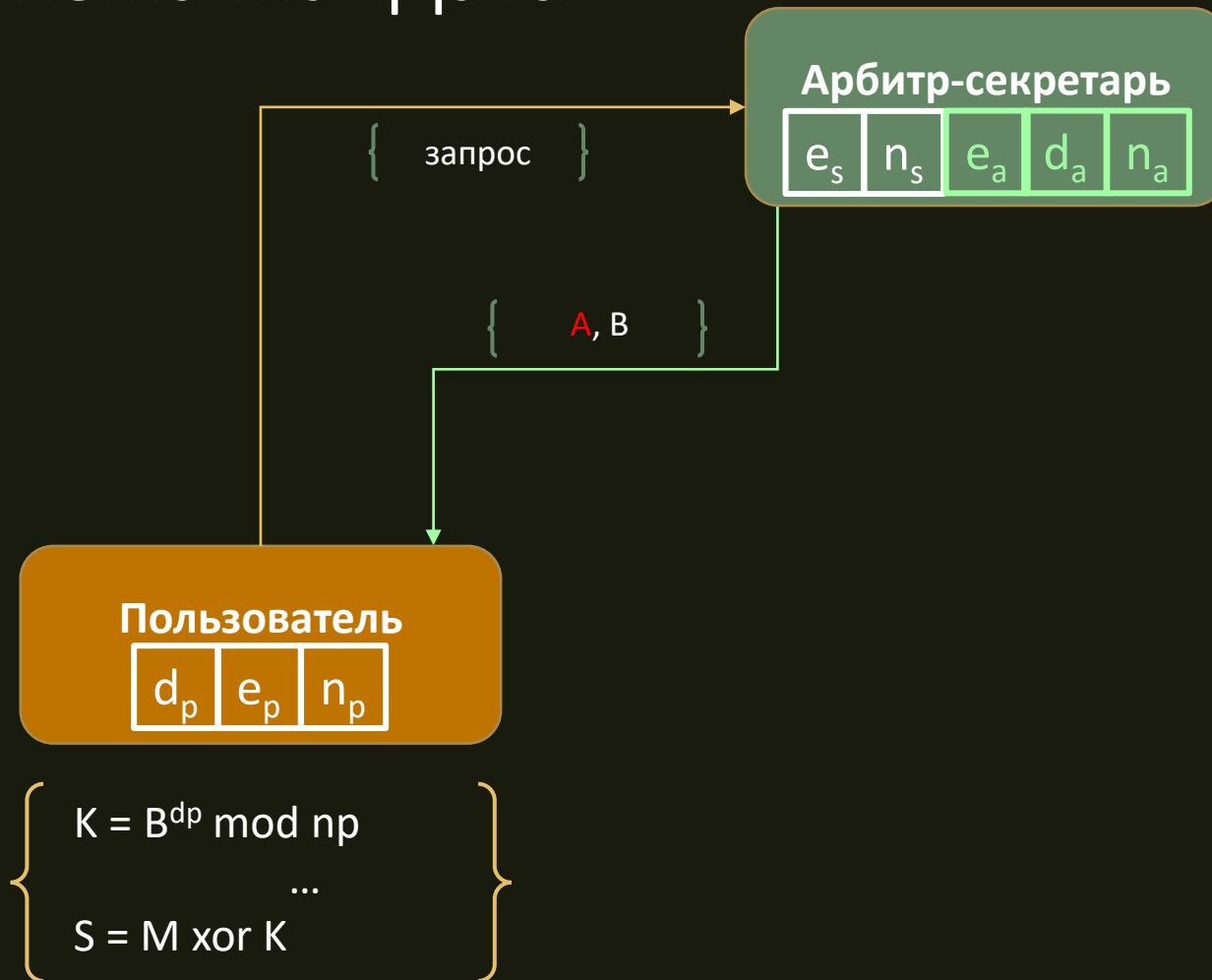
Схема мандата



Проверка сертификата
Проверка права и лимита
...
Генерация сеансового ключа K
...
 $A = (K^{e_s} \bmod n_s)^{d_a} \bmod n_a$
 $B = K^{e_p} \bmod n_p$



Схема мандата



Проверка сертификата
Проверка права и лимита

...

Генерация сеансового ключа K

...

$$A = (K^{e_s} \bmod n_s)^{d_a} \bmod n_a$$

$$B = K^{e_p} \bmod n_p$$

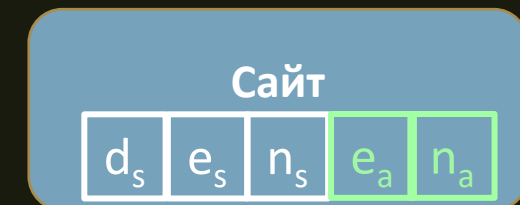
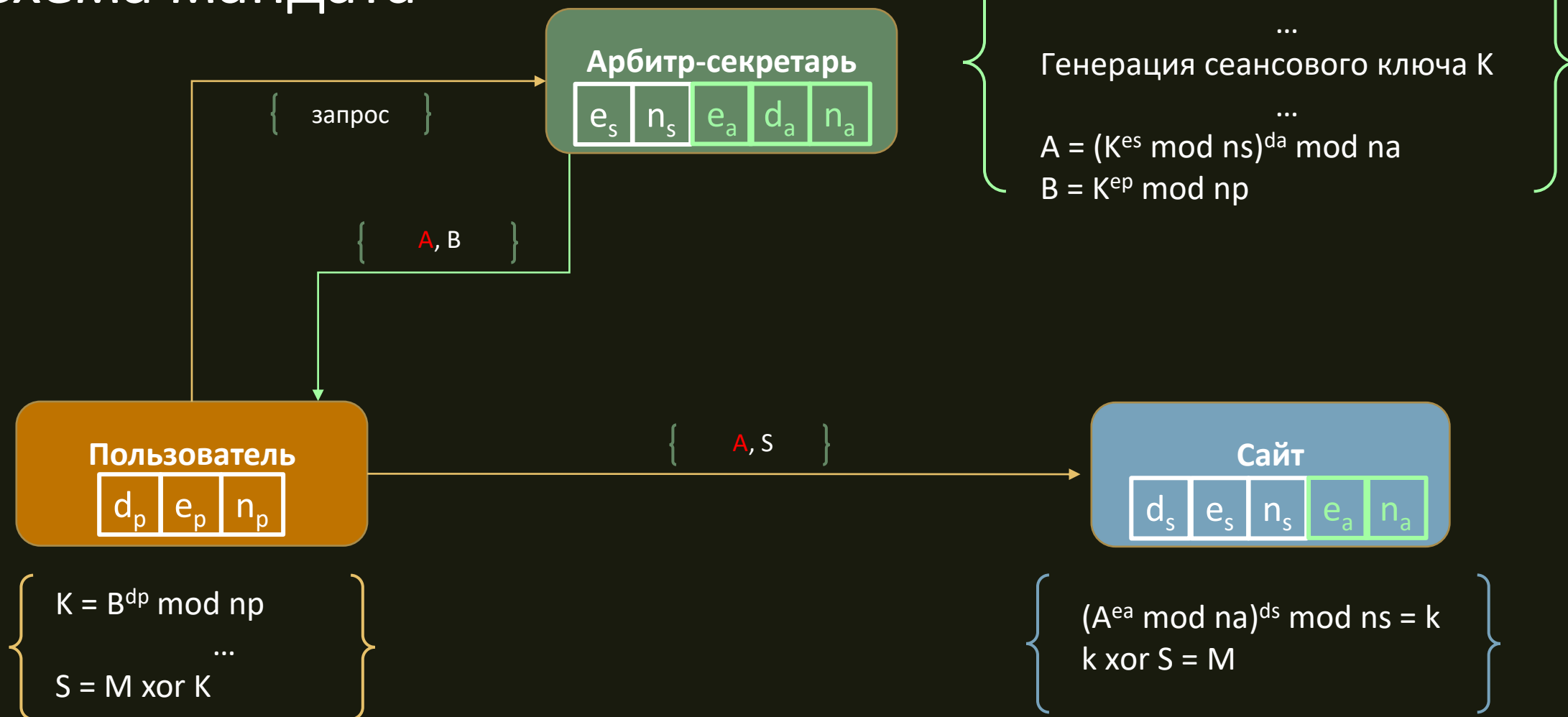


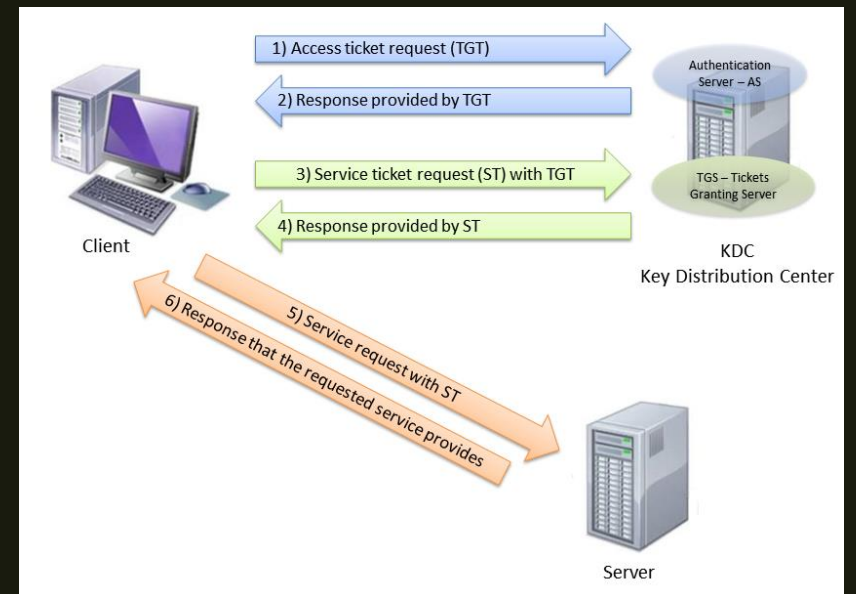
Схема мандата



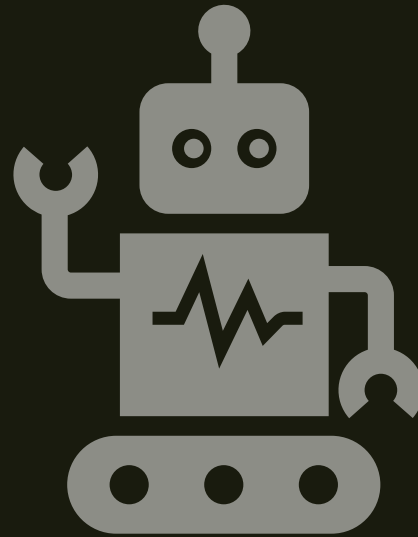
Мандаты

1. Подлинность отправителя
2. Подлинность получателя
3. Право и очередь отправителя на общение с получателем
4. Экономия времени и ресурсов основного сервера

KERBEROS (Network Authentication Protocol)



Практика



Рецепты

1. RSA открывается секретным ключом получателя
2. RSA закрывается публичным ключом получателя
3. ЭЦП открывается публичным ключом отправителя
4. ЭЦП ставится секретным ключом отправителя
5. Сертификат содержит публичный ключ третьего лица. Вскрывается публичным ключом арбитра.
6. Самоподписанный сертификат тождественен ЭЦП
7. Мандат для отправителя: второе число вскрывается своим секретным ключом
8. Мандат для получателя: вскрывать сначала публичным ключом арбитра, затем секретным своим

Общая схема

1. Подготовка сообщения и сеансового ключа шифрования
2. Запрос сертификата **Получателя** у Арбитра
3. Передача по **RSA** сеансового ключа К
4. Хеширование сообщения отправителем
5. Подпись Хеша
6. Шифрование сообщения и подписи
7. **Передача сообщения и подписи**
8. Запрос сертификата **Отправителя** у Арбитра
9. Открытие по **RSA** сеансового ключа К
10. Расшифрование сообщения и подписи
11. Хеширование сообщения
12. Верификация подписи
13. ...готово...

Отправка

Получение

Конкурс на лучший рисунок

