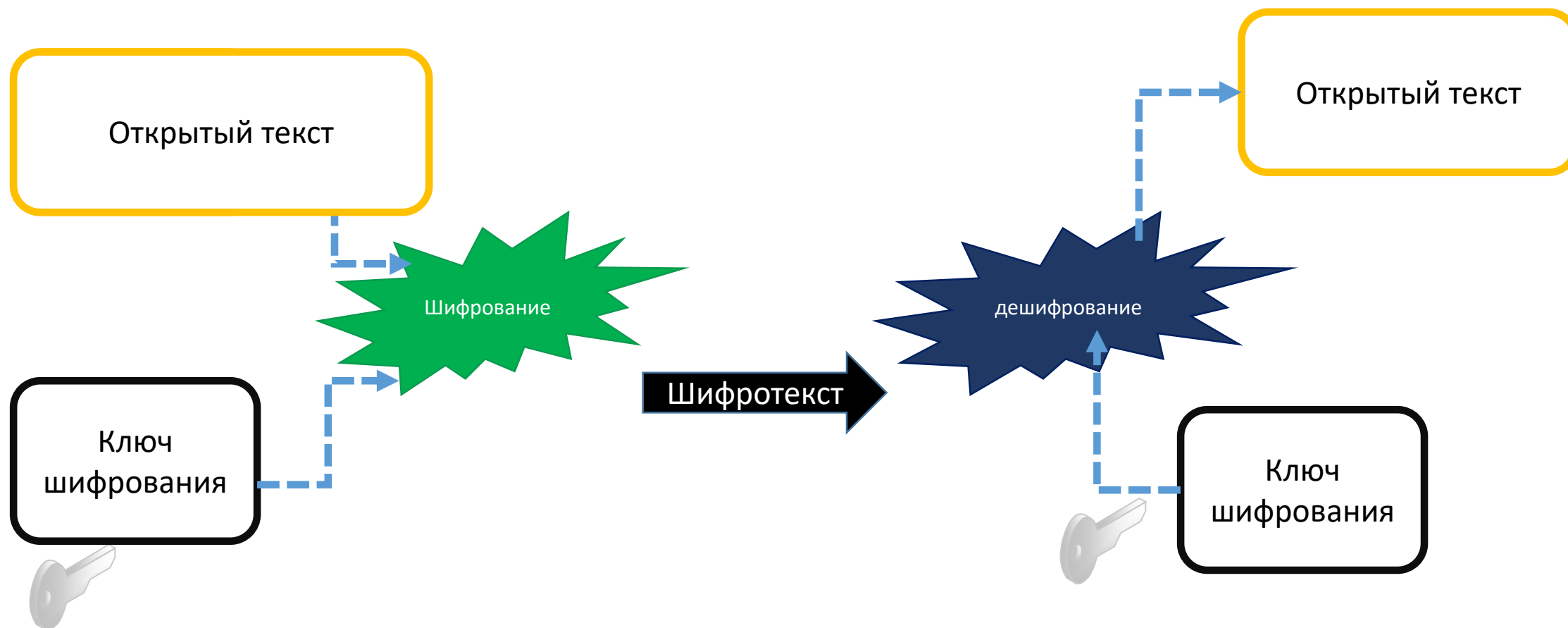
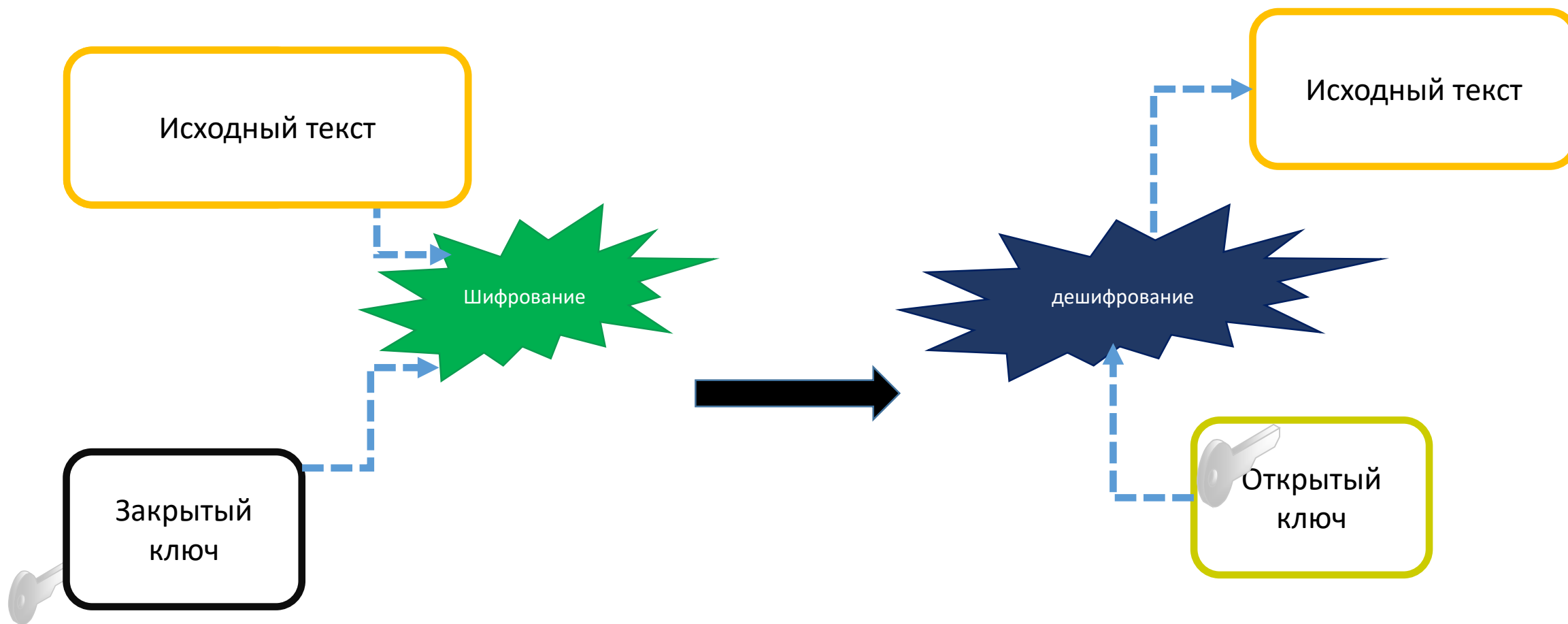


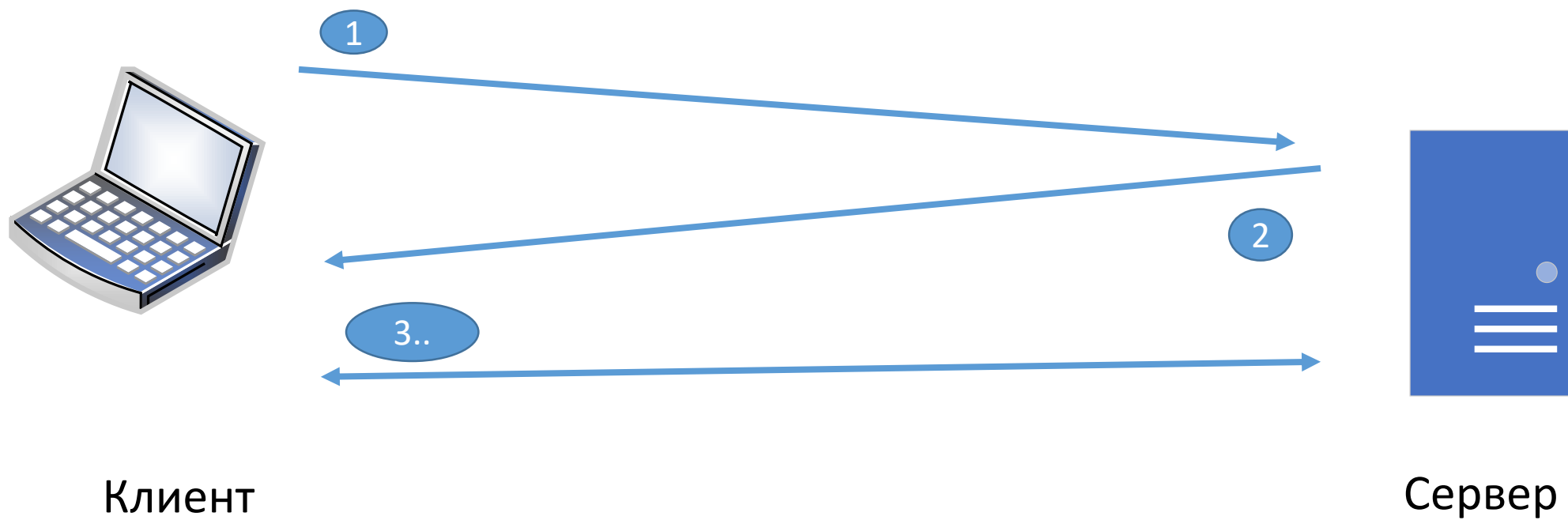


24.07.2024

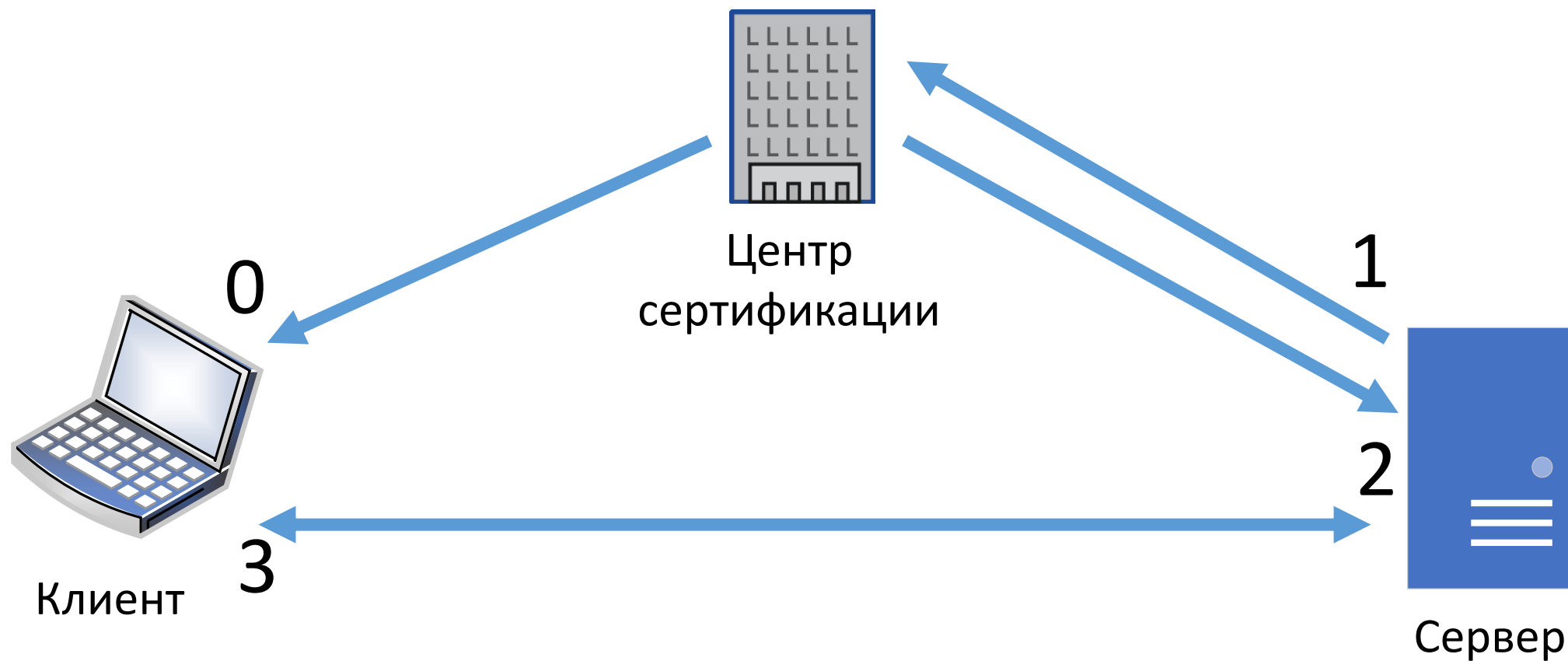
Протокол SSL/TLS, сертификаты и др











Сертификат есть зашифрованный на приватном ключе СА
хеш из публичного ключа сервера + метаданных



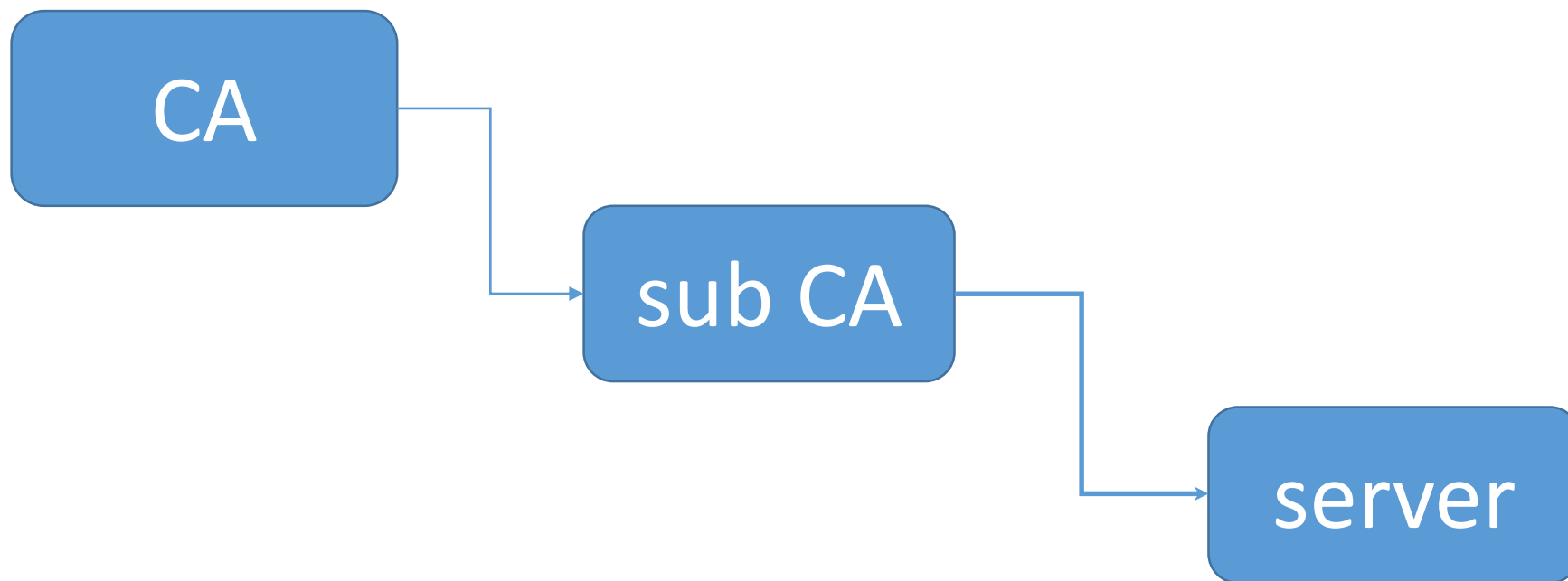
1. Создание ключевой пары (приватный+публичный ключи)
2. Из публичного ключа + метаданных создаётся CSR – запрос на сертификат
3. CSR отправляется в CA
4. Из CA получается сертификат
5. Приватный ключ и сертификат добавляется в конфигурацию сервера



1. Сертификат подписан доверенным центром сертификации
2. Выписан на верное имя DNS (DN и SubjectAltName)
3. Время актуальное



- Сертификат выписан СА из списка
- СА не из списка
- Самоподписанный / selfsigned





Log in



MENU

ericss

Troubleshooting TechNotes /

Hon

Identify vEdge Certificate Expired on May 9, 2023



Save



Translations



Download



Print

Updated: May 24, 2023

Document ID: 220448

[Bias-Free Language](#)

Contents

[Introduction](#)[Background Information](#)[Precautions to Avoid Service Disruption](#)[Remediation Process](#)[Fixed Software Versions](#)[Upgrade Recommendation Matrix](#)

taken immediate action to minimize impact and support the restoration of services.

TAC

Contributed by Cisco Engineers

Amanda Nava Zarate

Cisco TAC Technical Leader

Kendra J Dodson

Cisco TAC Technical Leader

Ryan Ratliff

Cisco TAC Manager



Следить за сроком действия



Technical Advisories:

- ~~Смарт-замки~~
- Подключаются по Wifi
- Управляются с приложения смартфона

Lack of Certificate Validation on TLS Communications (CVE-2022-32509)

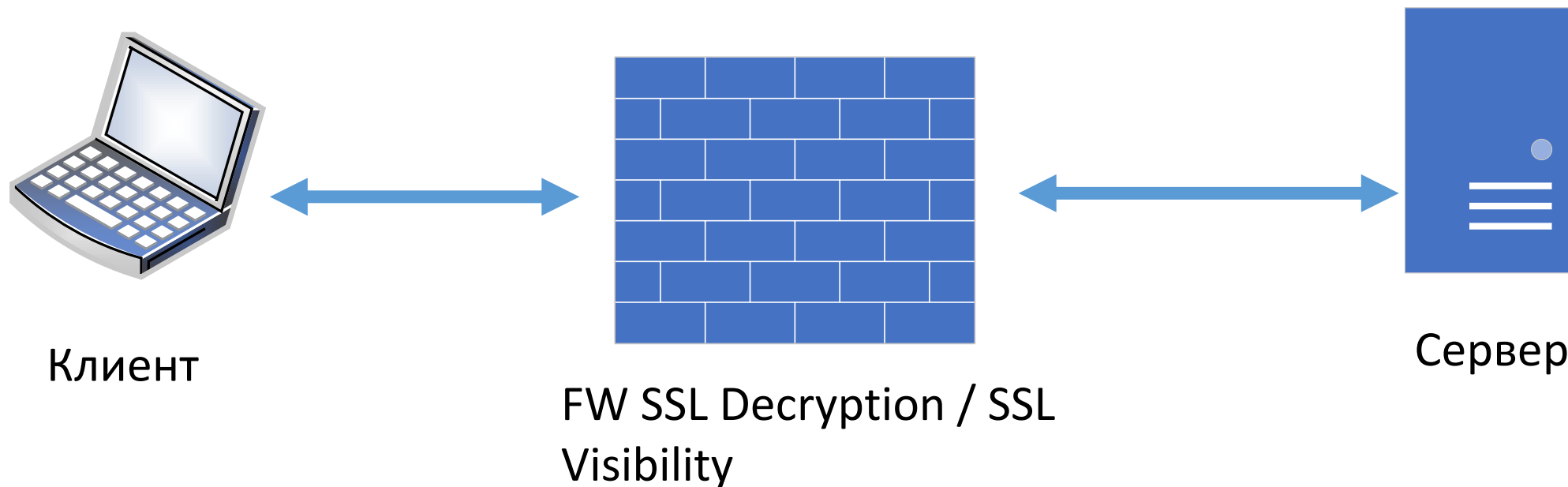
Vendor: Nuki (<https://nuki.io>)

Systems and Versions affected:

- Nuki Smart Lock 3.0 (<3.3.5)
- Nuki Bridge v1 (<1.22.0)



- Аутентифицируют клиента на сервере
- Часто применяются внутри систем когда несколько устройств взаимодействуют между собой (M2M) вместо логинов и паролей
- Проверяется аналогично: у сервера список доверенных СА и он разрешает доступ клиентам с сертификатами оттуда
- Популярно в OpenVPN, используется на сайтах ЭТП
- Тоже надо следить за сроком действия, проверять сертификаты и ограничить список доверенных СА



- Дополнительная защита от MITM хозяином клиентского устройства
- При подключении к серверу проверяет не только список доверенных CA, но и явно его публичный ключ
- Расстраивает софт в ситуации SSL Decryption на брандмауэрах



- *.example.com
- Только на домены одного уровня: ✓ www.example.com и lab.example.com,
✗ uc.lab.example.com
- Усиливаются риски для приватного ключа
- Особо внимательно следить за расползанием и везде за сроком действия
- Можно через Shodan и Censys

TOTAL RESULTS

15

TOP COUNTRIES



United States	7
Germany	3
Netherlands	2
France	1
Taiwan	1



View Report



Download Results



Historical Trend



View on Map



Advanced Search

Partner Spotlight: Looking for a Splunk alternative to store all the Shodan data? Check out [Gravwell](#)

404 - Not Found ↗

2024-07-28T12:24:41.104742

93.184.216.34

www.example.org

www.example.com

example.org

example.net

example.com

NETBLK-03-EU-93-
184-216-0-24United
States, Secaucus

cdn



SSL Certificate

Issued By:

|- Common Name:

DigiCert Global G2

TLS RSA SHA256

2020 CA1

|- Organization:

DigiCert Inc

Issued To:

|- Common Name:

www.example.org

|- Organization:

Internet Corporation for Assigned Names and Numbers

Supported SSL

Versions:

HTTP/1.1 404 Not Found

Content-Type: text/html

Date: Sun, 28 Jul 2024 12:24:41 GMT

Server: ECS (nyd/D16B)

Content-Length: 345



- Let's Encrypt и аналоги
- Короткий срок действия, всего 90 дней
- Полный автомат
- Могут быть wildcard



- DER
- PEM (*.crt, *.csr, *.key, etc)
- PFX/PKCS#12
- Java Keystore (JKS)
- и др





1. Версии SSL 2.0, TLS1.0, TLS1.1, 1.2 и 1.3
2. Алгоритмы шифрования, цифровой подписи, хеш-функции, ...

Проблема только для активных атак MITM

ECDHE-RSA-AES128-GCM-SHA256

TLS_AES_128_GCM_SHA256

ARIA256-GCM-SHA384

ECDHE-RSA-CHACHA20-POLY1305

[...]

Сейчас должно быть разрешены только TLS1.2 и 1.3

DES/3DES, RC4, MD5/SHA1 – точно запрещено



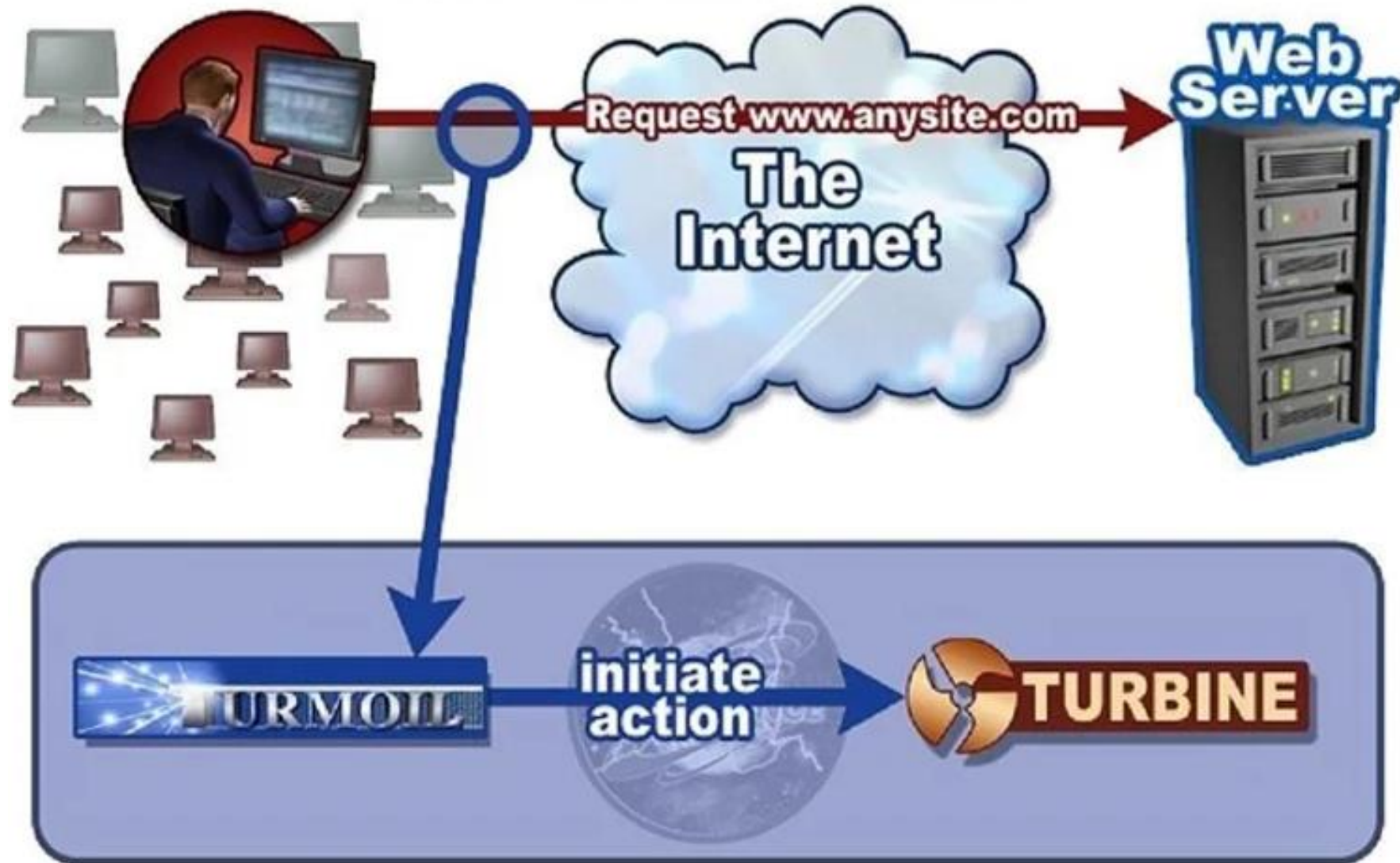
Firefox

about:config

Firefox ESR

- security.tls.version.enable-deprecated: true
- security.tls.version.min: 1

- софты типа stunnel, haproxy, nginx
- Риски старого ПО остаются





- Сертификат X.509, не SSL
- Применяется также в подписи файлов, IPsec, электронной почте S/MIME, загрузчиках ОС, WiFi, OpenVPN и тп

<https://habr.com/ru/news/470539/>

Моя лента Все потоки Разработка Администрирование Дизайн Менеджмент Маркетинг Научпоп



marks 7 окт 2019 в 21:46

Россиянину, у которого украли квартиру при помощи поддельной электронной подписи, удалось вернуть недвижимость

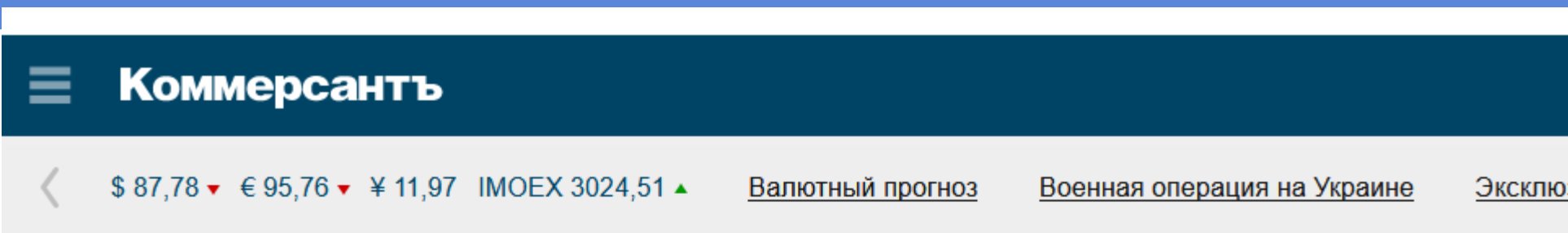


4 мин



22K

Информационная безопасность*, Законодательство в IT, Облачные сервисы*, Финансы в IT



[Телекоммуникации](#)

18.07.2024, 14:14



5K



1 мин.





9



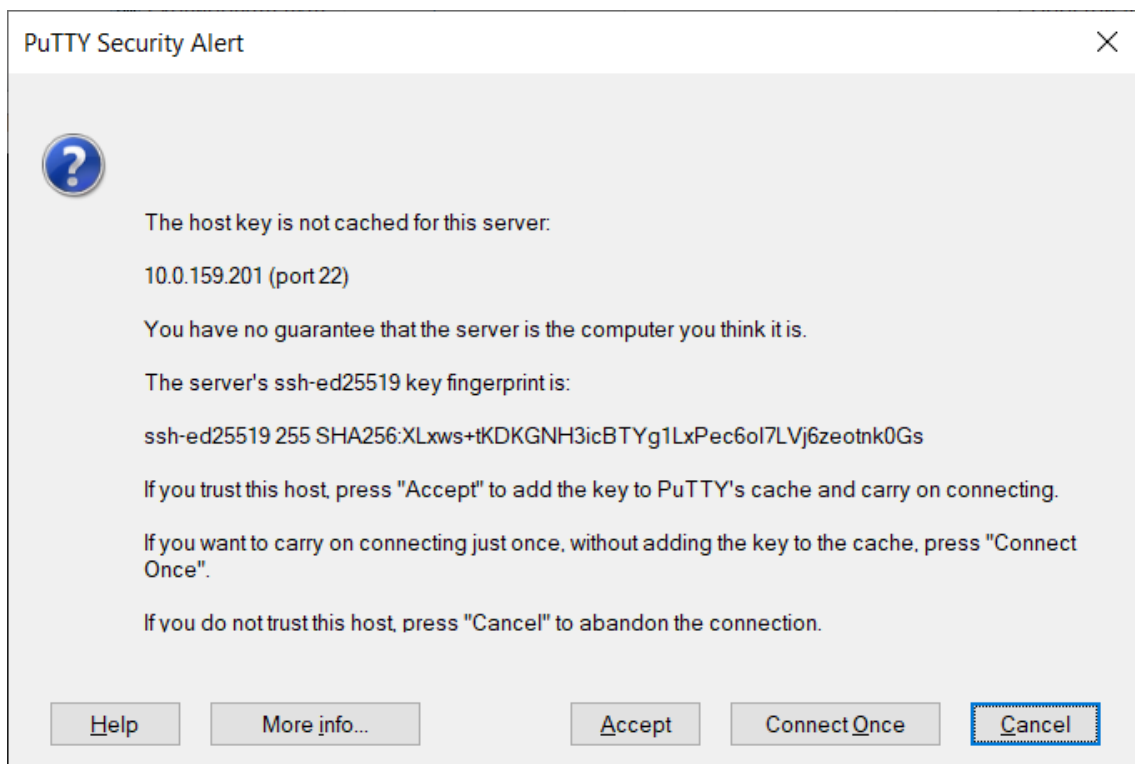
Минцифры: мошенники не могут приобрести чужую недвижимость через «Госуслуги»

Мошенники не могут завладеть чужой квартирой через «Госуслуги», поскольку на портале нет функции, позволяющей купить или продать недвижимость, сообщило Минцифры. Ранее «Газета.ру» писала о случаях сделок с недвижимостью с помощью поддельной цифровой подписи.



<div>  Identity Search  Group by Issuer </div>							
Criteria Type: Identity Match: ILIKE Search: 'sberbank.ru'							
Certificates	crt.sh ID	Logged At ↑	Not Before	Not After	Common Name	Matching Identities	Issuer Name
	13713601256	2024-07-12	2024-07-12	2025-07-12	clickstream.sberbank.ru	clickstream.sberbank.ru	C=IT, ST=Bergamo, L=Ponte San Pietro, O=Actalis S.p.A., CN=Actalis Domain Validation Server CA G3
	13651052293	2024-07-07	2024-07-07	2025-07-07	*.online.sberbank.ru	*.online.sberbank.ru online.sberbank.ru	C=GR, O=Hellenic Academic and Research Institutions CA, CN=HARICA DV TLS RSA
	13468598269	2024-06-21	2024-06-21	2025-06-21	chatnc.csc.sberbank.ru	chatnc.csc.sberbank.ru	C=IT, ST=Bergamo, L=Ponte San Pietro, O=Actalis S.p.A., CN=Actalis Domain Validation Server CA G3
	13288041709	2024-06-04	2024-06-04	2025-06-04	www.osago.sberbank.ru	osago.sberbank.ru www.osago.sberbank.ru	C=IT, ST=Bergamo, L=Ponte San Pietro, O=Actalis S.p.A., CN=Actalis Domain

<https://crt.sh/?q=sberbank.ru>



```
$ ssh 10.0.159.201
The authenticity of host '10.0.159.201 (10.0.159.201)' can't be established.
ED25519 key fingerprint is SHA256:XLxws+tKDKGNH3icBTYg1LxPec6oI7LVj6zeotnk0Gs.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? █
```



```
$ ls -l /etc/ssh/ssh_host*_key*  
-rw----- 1 root root 505 Jul 6 2022 /etc/ssh/ssh_host_ecdsa_key  
-rw-r--r-- 1 root root 176 Jul 6 2022 /etc/ssh/ssh_host_ecdsa_key.pub  
-rw----- 1 root root 411 Jul 6 2022 /etc/ssh/ssh_host_ed25519_key  
-rw-r--r-- 1 root root 96 Jul 6 2022 /etc/ssh/ssh_host_ed25519_key.pub  
-rw----- 1 root root 2602 Jul 6 2022 /etc/ssh/ssh_host_rsa_key  
-rw-r--r-- 1 root root 568 Jul 6 2022 /etc/ssh/ssh_host_rsa_key.pub
```

```
$ ssh-keygen -l -f /etc/ssh/ssh_host_ed25519_key.pub  
256 SHA256:wt8Hn/e+3HTLfux/vJj9WEKQNDcZd1TYvmmNbrRKgWI root@hyperbole (ED25519)
```

```
$ ssh localhost  
The authenticity of host 'localhost (:::1)' can't be established.  
ED25519 key fingerprint is SHA256:wt8Hn/e+3HTLfux/vJj9WEKQNDcZd1TYvmmNbrRKgWI.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? ^C  
$
```



- Протокол: всегда версии 2
- Алгоритмы шифрования
- Хеш-функции, etc



Apply a display filter ... <Ctrl-/> → + no-junk1 no-junk2 no-junk3

No.	Time	Source	Destination	Protocol	Length	Info
3	2024-07-12 22:19:10.080366	10.0.10.10	172.16.34.11	TCP	66	42404 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=
4	2024-07-12 22:19:10.080905	10.0.10.10	172.16.34.11	SSHv2	106	Client: Protocol (SSH-2.0-OpenSSH_9.2p1 Debian-2+de
5	2024-07-12 22:19:10.080919	172.16.34.11	10.0.10.10	TCP	66	22 → 42404 [ACK] Seq=1 Ack=41 Win=65152 Len=0 TSval
6	2024-07-12 22:19:10.088395	172.16.34.11	10.0.10.10	SSHv2	106	Server: Protocol (SSH-2.0-OpenSSH_9.2p1 Debian-2+de
7	2024-07-12 22:19:10.088840	10.0.10.10	172.16.34.11	TCP	66	42404 → 22 [ACK] Seq=41 Ack=41 Win=64256 Len=0 TSval
8	2024-07-12 22:19:10.089239	172.16.34.11	10.0.10.10	SSHv2	1178	Server: Key Exchange Init
9	2024-07-12 22:19:10.097043	10.0.10.10	172.16.34.11	TCP	154	[TCP Previous segment not captured] 42404 → 22 [PSH
10	2024-07-12 22:19:10.097053	172.16.34.11	10.0.10.10	TCP	78	[TCP Dup ACK 5#1] 22 → 42404 [ACK] Seq=1153 Ack=41
11	2024-07-12 22:19:10.296488	172.16.34.11	10.0.10.10	TCP	1190	[TCP Retransmission] 22 → 42404 [PSH, ACK] Seq=41 A
12	2024-07-12 22:19:10.504568	172.16.34.11	10.0.10.10	TCP	1190	[TCP Retransmission] 22 → 42404 [PSH, ACK] Seq=41 A
13	2024-07-12 22:19:10.928745	172.16.34.11	10.0.10.10	TCP	1190	[TCP Retransmission] 22 → 42404 [PSH, ACK] Seq=41 A
14	2024-07-12 22:19:11.760578	172.16.34.11	10.0.10.10	TCP	1190	[TCP Retransmission] 22 → 42404 [PSH, ACK] Seq=41 A
15	2024-07-12 22:19:13.424336	172.16.34.11	10.0.10.10	TCP	1190	[TCP Retransmission] 22 → 42404 [PSH, ACK] Seq=41 A
16	2024-07-12 22:19:15.112088	PcsCompu_01:52:	PcsCompu_6c:fd:	ARP	60	Who has 172.16.34.11? Tell 172.16.34.12

▶ Frame 11: 1190 bytes on wire (9520 bits), 1190
▶ Ethernet II, Src: PcsCompu_6c:fd:f8 (08:00:27:04:98:fc), Dst: 08:00:00:00:00:00
▶ Internet Protocol Version 4, Src: 172.16.34.11, Dst: 10.0.10.10
▶ Transmission Control Protocol, Src Port: 22, Dst Port: 42404

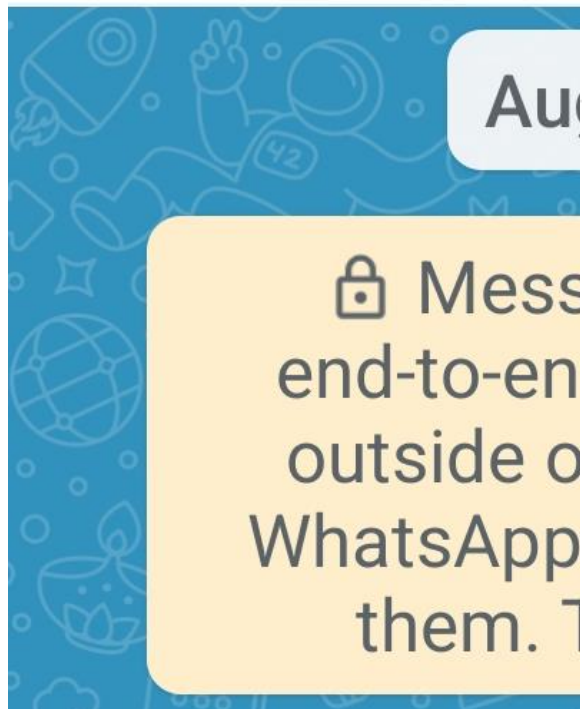
Offset	Hex	ASCII
0000	08 00 27 01 52 ef 08 00 27 6c fd f8 08 00 45 00	..'.R... 'l...E.
0010	04 98 fc 8b 40 00 40 06 57 af ac 10 22 0b 0a 00@.@. W..."
0020	0a 0a 00 16 a5 a4 63 57 ce 8d fa df 91 7a b0 18cWz..
0030	03 fa e6 af 00 00 01 01 08 0a c7 cc 4a 5d fc 71J].q
0040	30 28 01 01 05 0a fa df 97 22 fa df 97 7a 00 00	0(....."....z..
0050	04 54 0a 14 63 b7 3b 6b 27 b9 8d d7 23 2c 4f 48	.T..c.;k '...#,0H
0060	7a 5f 1f 37 00 00 01 26 73 6e 74 72 75 70 37 36	z_.7...& sntrup76
0070	31 78 32 35 35 31 39 2d 73 68 61 35 31 32 40 6f	1x25519- sha512@o
0080	70 65 6e 73 73 68 2e 63 6f 6d 2c 63 75 72 76 65	penssh.c om,curve
0090	32 35 35 31 39 2d 73 68 61 32 35 36 2c 63 75 72	25519-sh a256,cur
00a0	76 65 32 35 35 31 39 2d 73 68 61 32 35 36 40 6c	ve25519- sha256@l



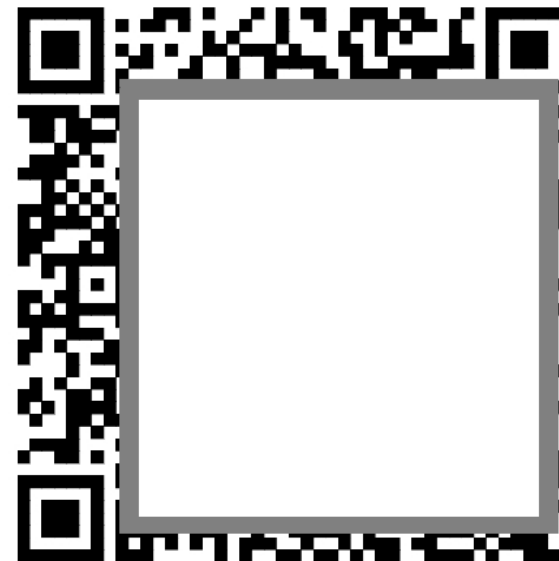
← Scan QR code
You, Бабушка



end-to-end encryption, scan the QR code
on their device or ask them to scan your QR code.

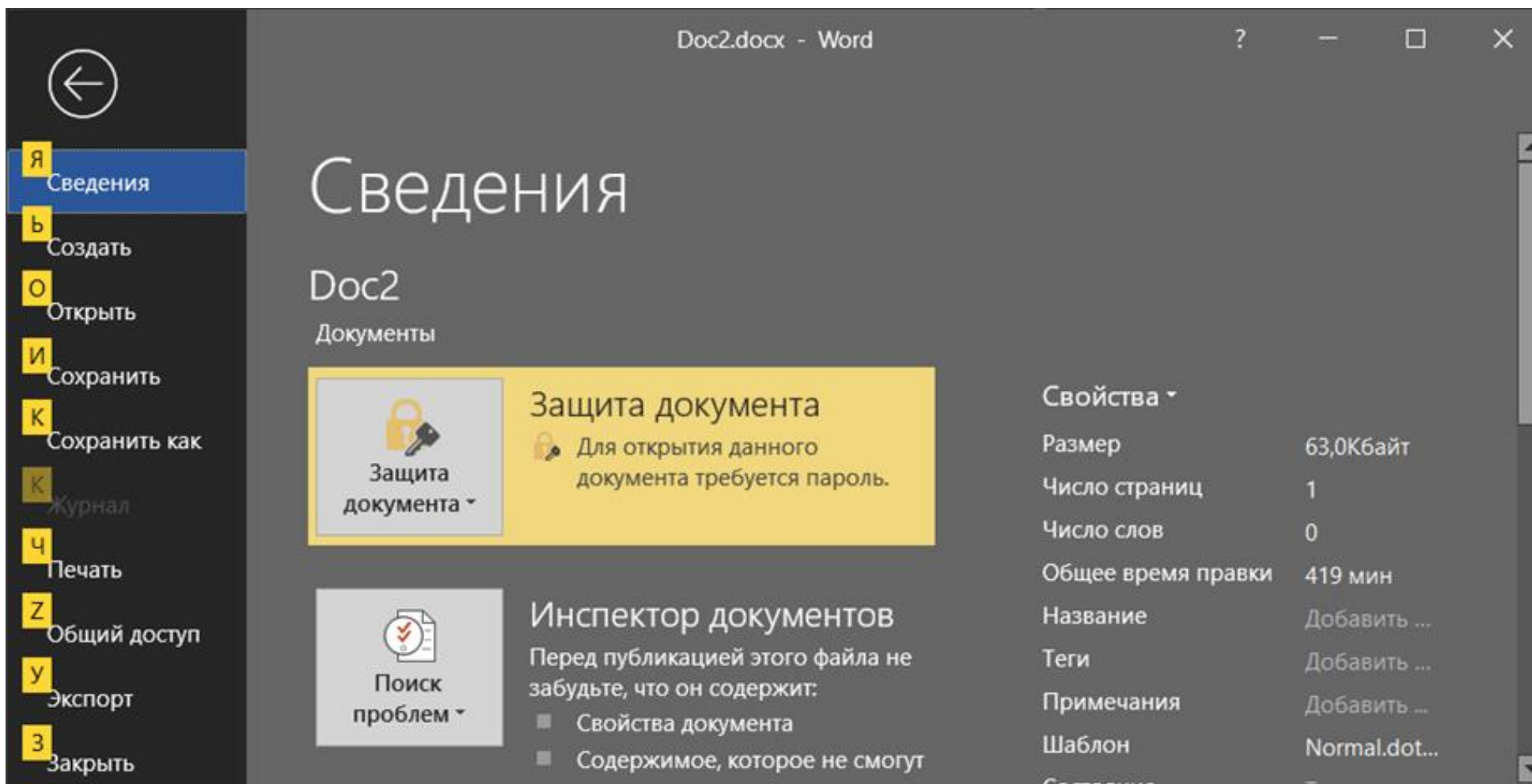


Your QR Code





Файлы drag'n'drop в Word и сохранить с паролем





DigiCert® SSL/TLS Best Practice Workshop Student Guide

<https://www.digicert.com/content/dam/digicert/pdfs/ssl-tls-best-practice-workshop-student-guide-en.pdf>



🔗 The Illustrated TLS 1.3 Connection 🔗

Every byte explained and reproduced

In this demonstration a client connects to a server, negotiates a TLS 1.3 session, sends "ping", receives "pong", and then terminates the session. Click below to begin exploring.

<https://tls13.xargs.org>

Open All

± Client Key Exchange Generation

› Client Hello

± Server Key Exchange Generation



S. A. X. X. @_SaxX_ · 6h ...
This morning, I began another #pentest for a client. After some google-fu dorking combine with the major search engines, I found the id_rsa key that gave me access to the server and a bunch of others 🤖
another mistake under their radar...

```
-----BEGIN RSA PRIVATE KEY-----  
MIIEKQIBAAKCAgEApRVJnLLaLV07zNZPbqW4xYZtZpxPpQs3Io3JauefRg+UP5ye  
INAZ0whZV7vmo0uidzItwjPXVNLRTOWQ1Vzp720xJ9F5WcBsxwWx9AhkBGyNtGYC  
i3UDlfx9ut3vXIiZN1v3lk6KIOEwJmFNiVh50yMpnY44DUYYsjDUiwlCjKWagn0  
PGpEANxZMqG0Ber7uWI0iLta4Wq0G88wzz08nW5V326Xh8Xn/oIASyV8JjRCPRb  
3uBL6KE2q28lqBwk8k8l+HDhZptq0z5h4lCmUp13aiaDXJypLoG70LoHq7yy/jd3  
9E3R9jldze3p099154Yp1+deT8EH9CusRluVZ7i4npUT691xWtL6W5IvYD1GzeUS  
[REDACTED]
```

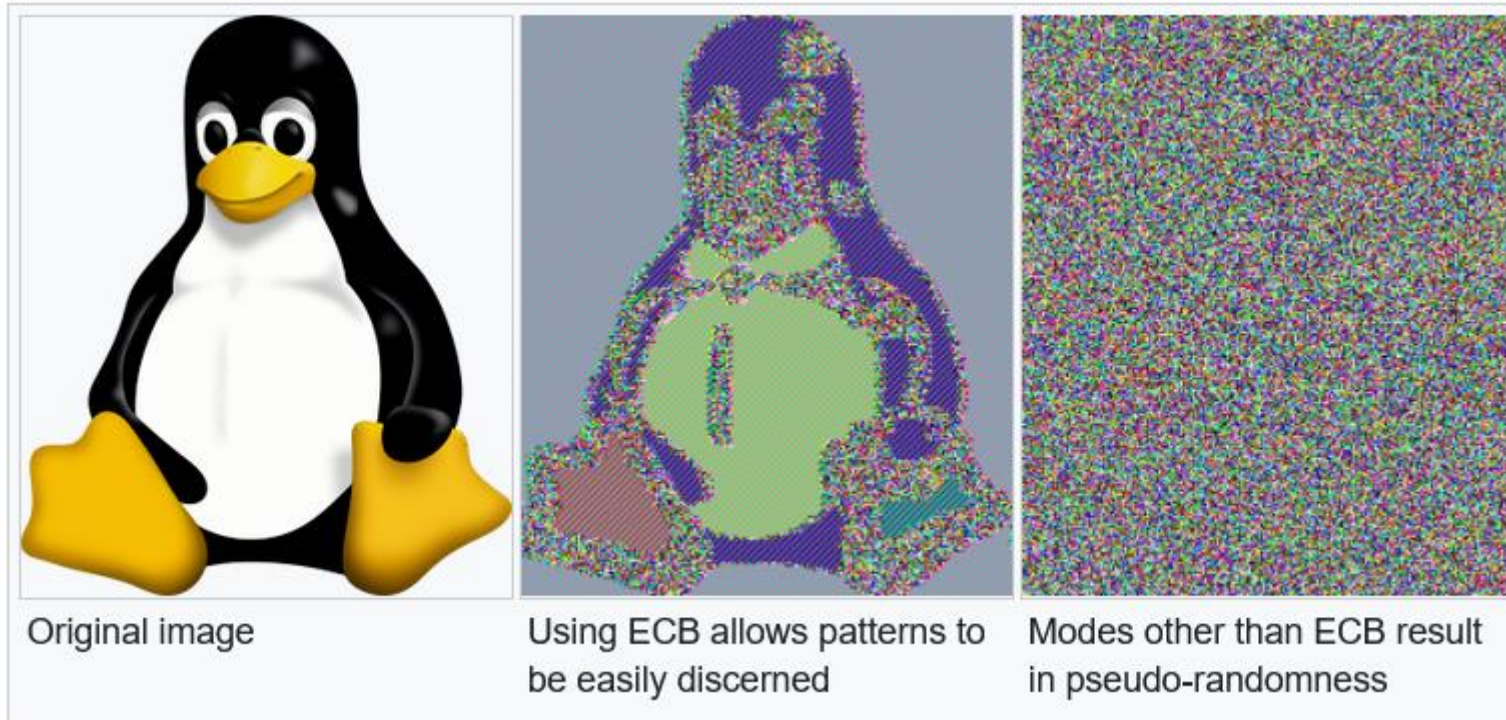
9 1 23

Florian Picca @ENOENT_ · 4h ...
Recovery the full private key based on the infos you just leaked looks a lot like a CTF challenge and might be doable (cc @CryptoHack_)

1 21

- Показал в социальной сети кусочек приватного ключа
- Многие отретушировал, но оставшегося хватило для получения полных данных

<https://blog.cryptohack.org/twitter-secrets>



[https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation#Electronic_codebook_\(ECB\)](https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation#Electronic_codebook_(ECB))

- Вопросы
- Слайды
- Видео