Cert Security KZ

And what is wrong?

ЗаТелеком

ОЗИ

ОБЩЕСТВО ЗАЩИТЫ ИНТЕРНЕТА

Continuing to Protect our Users in Kazakhstan

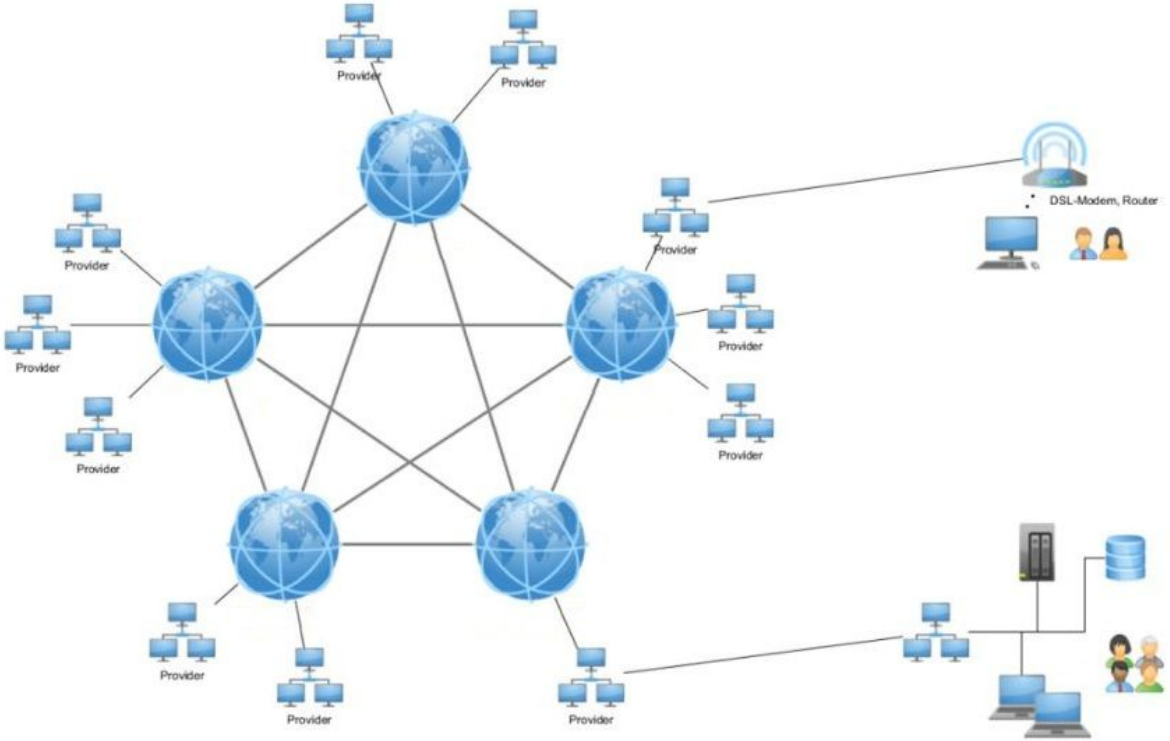
Marshall Erwin and Kathleen Wilson | December 18, 2020

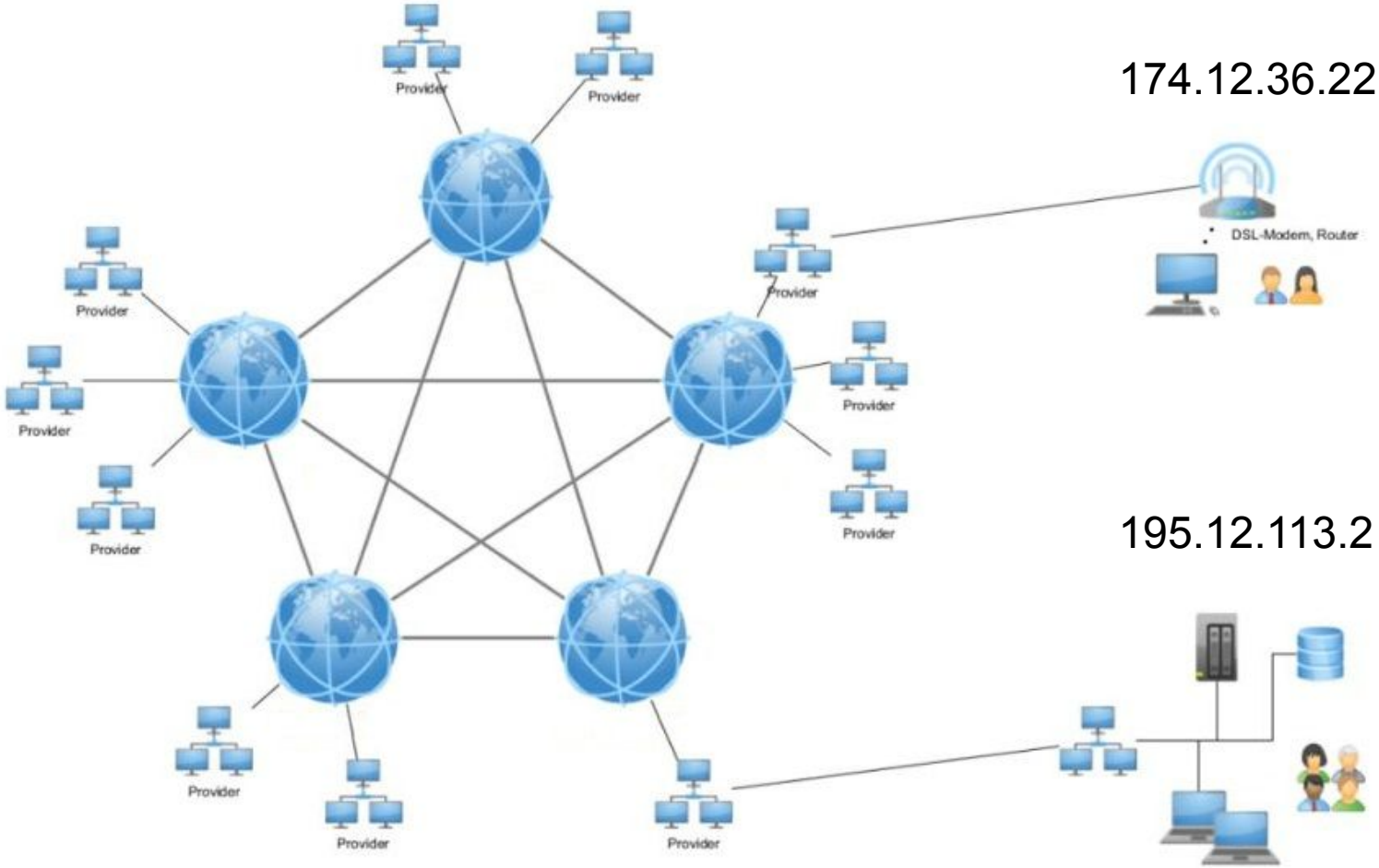
In a troubling rehash of events from July 2019, Mozilla was recently informed that Internet Service Providers (ISPs) in Kazakhstan have begun telling their customers that they must install a government-issued root certificate on their devices to access internet services. When a user in Kazakhstan installs the root certificate provided by their ISP, they are choosing to trust a Certificate Authority (CA) that enables the interception and decryption of network communications between Firefox and the website.

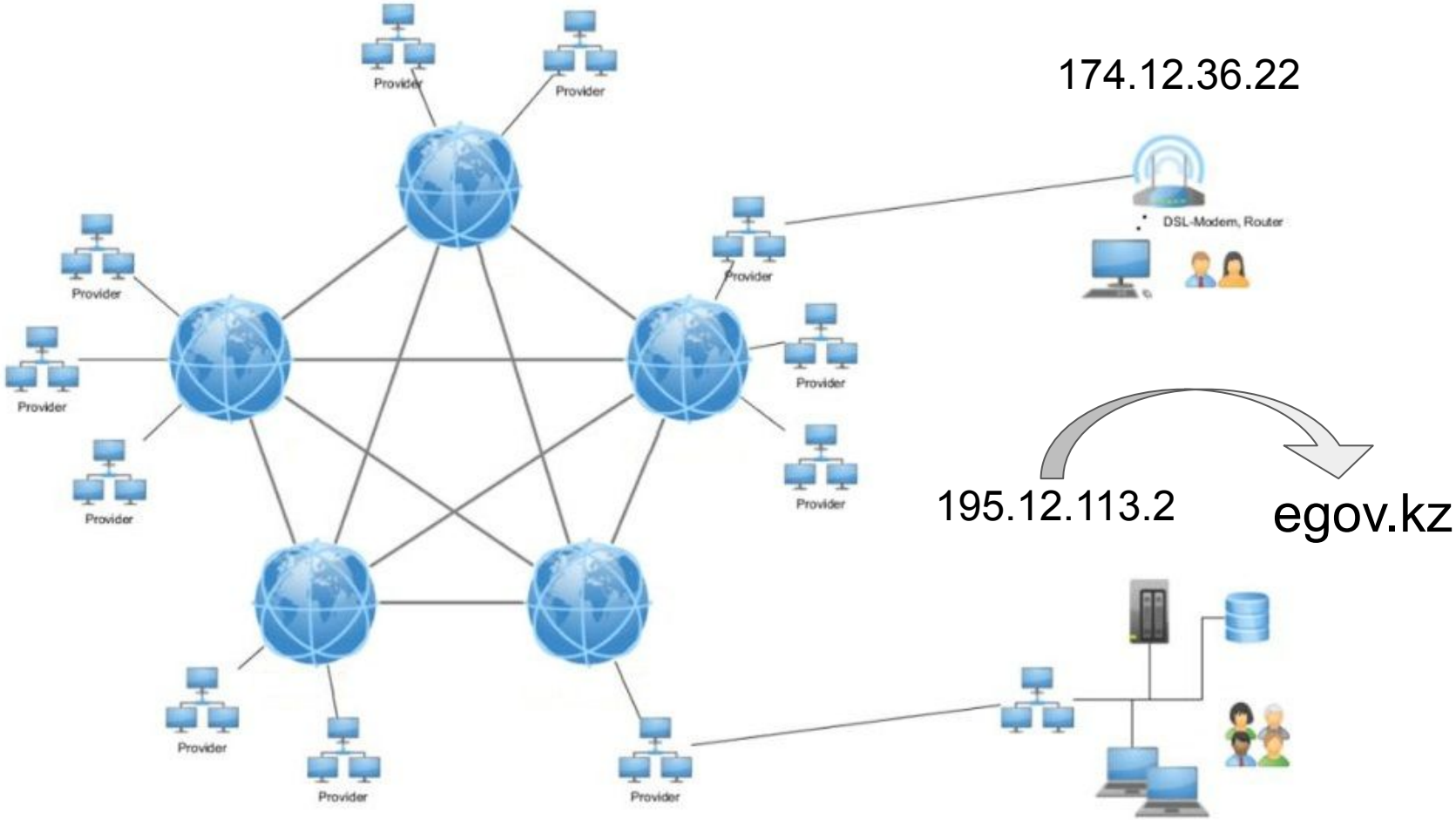
As we stated in 2019, we believe this act undermines the security of our users and the web, and it directly contradicts Principle 4 of the Mozilla Manifesto that states, "Individuals' security and privacy on the internet are fundamental and must not be treated as optional."

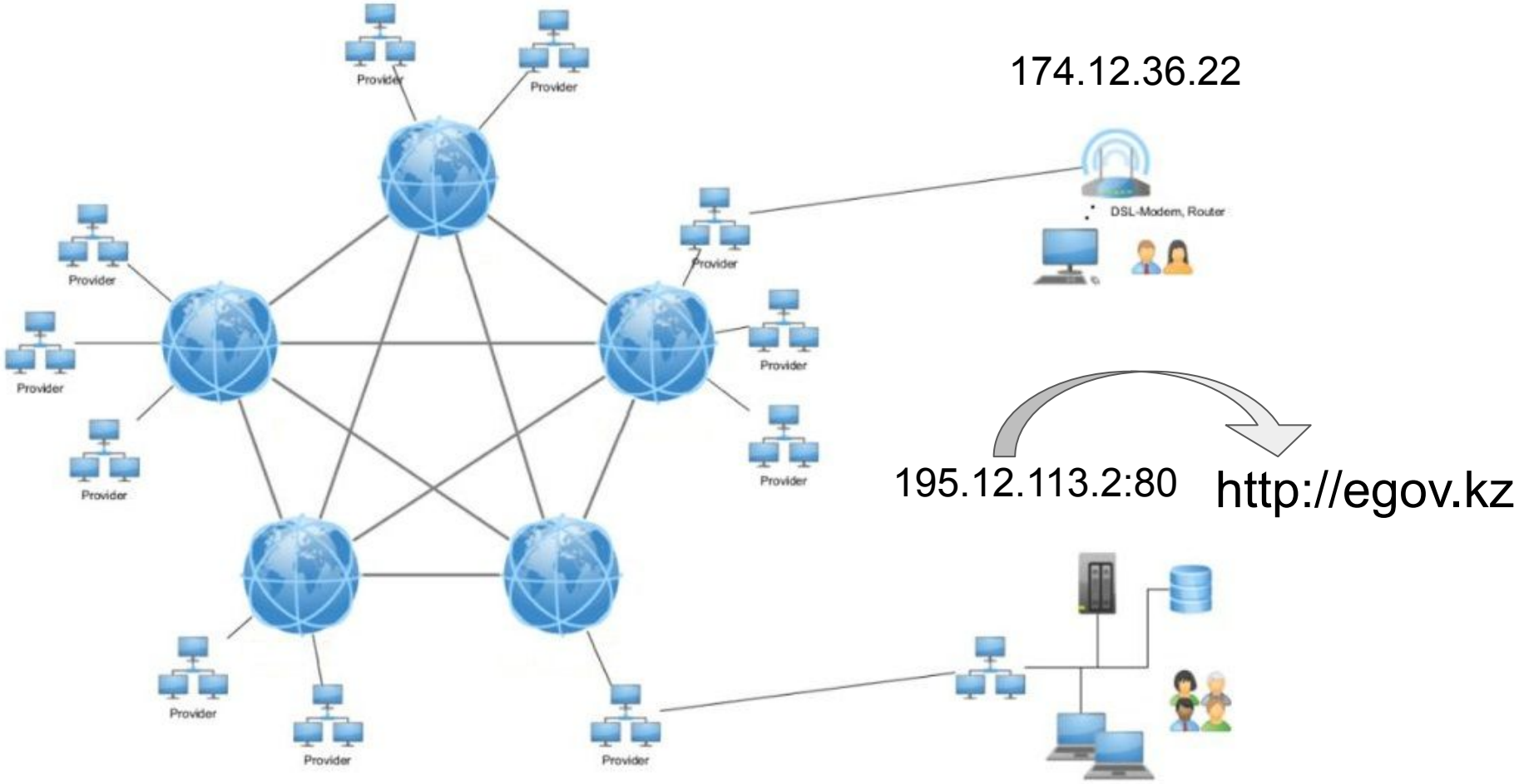
https://blog.mozilla.org/netpolicy/2020/12/18/kazakhstan-root-2020/

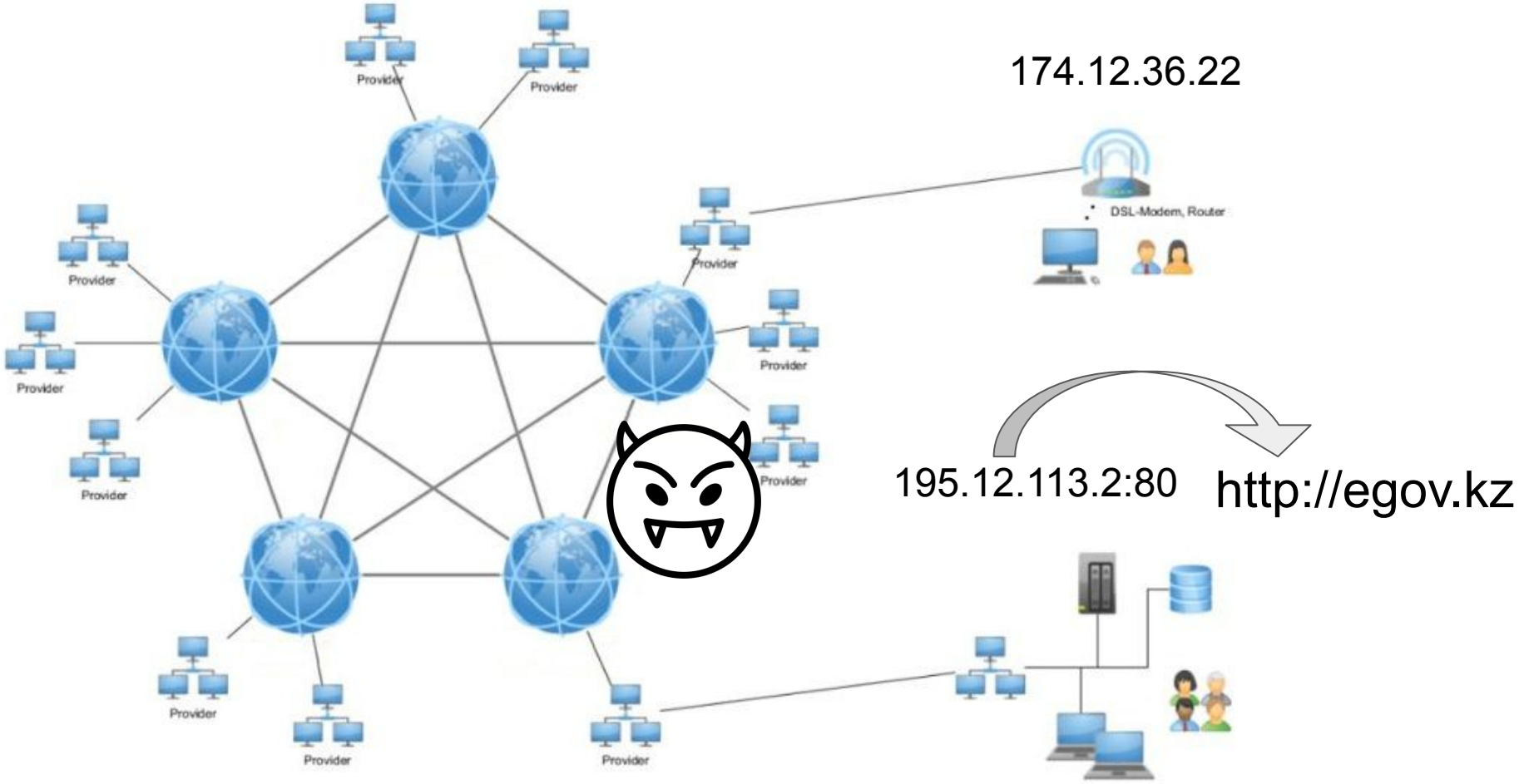
How it works?

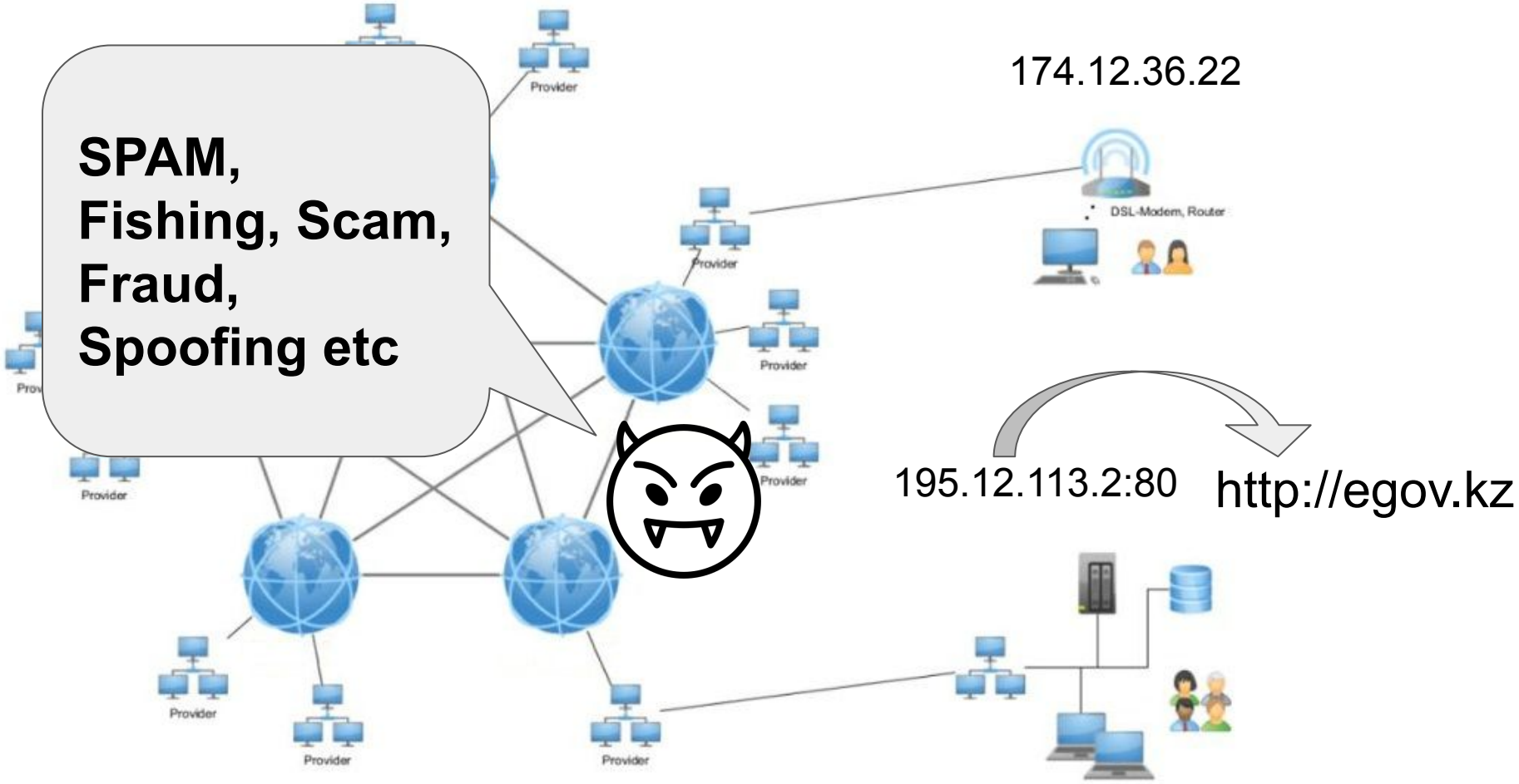

Provider
Provider
Provider
Provider
Provider
Provider
Provider
Provider
Provider
Provider
Provider
DSL-Modem, Router

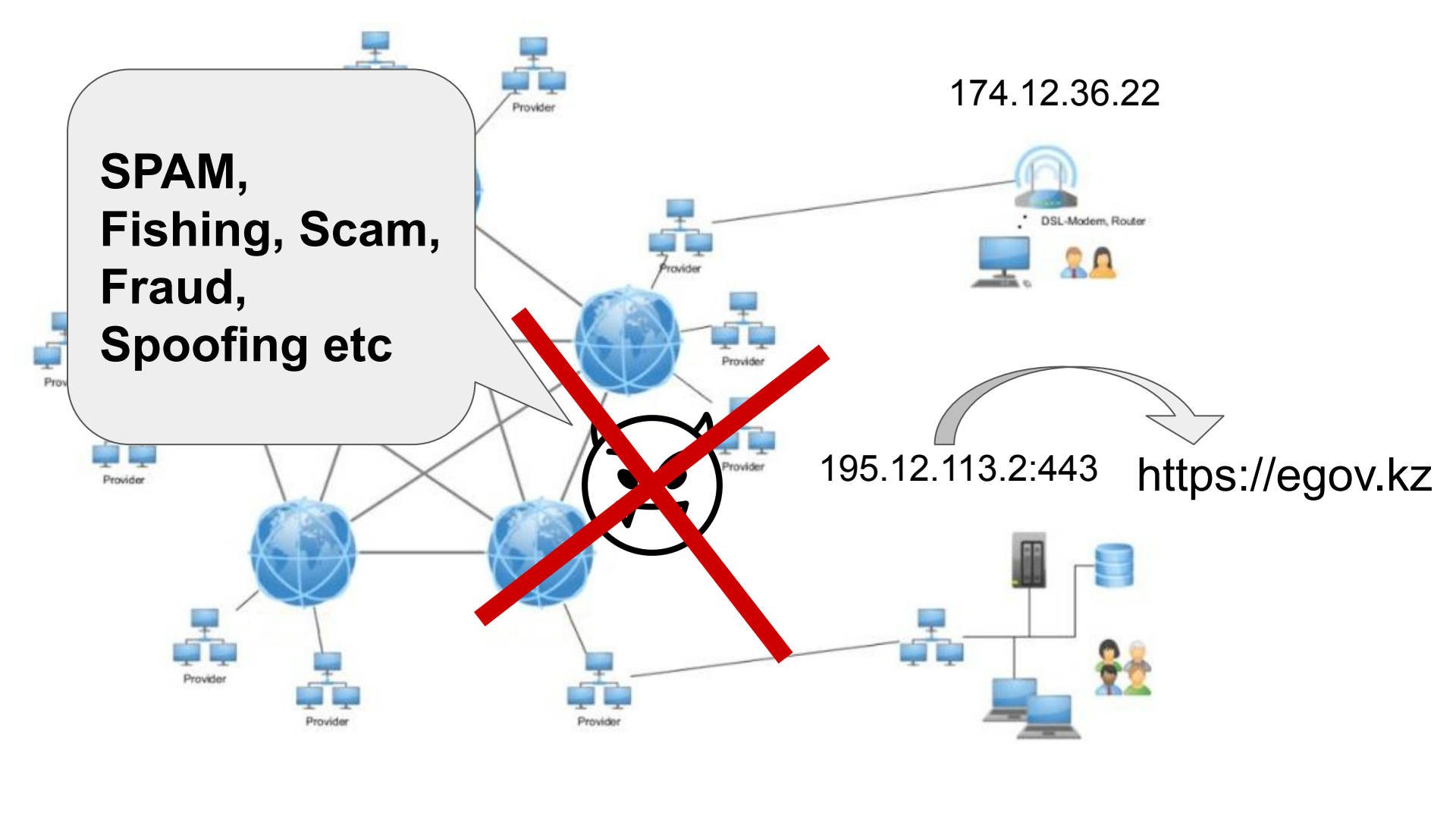

Provider
Provider
Provider
Provider
Provider
Provider
Provider
Provider
Provider
Provider
Provider
Provider
174.12.36.22
DSL-Modem, Router
195.12.113.2


Provider
Provider
Provider
Provider
Provider
Provider
Provider
Provider
Provider
Provider
Provider
174.12.36.22
DSL-Modem, Router
195.12.113.2
egov.kz

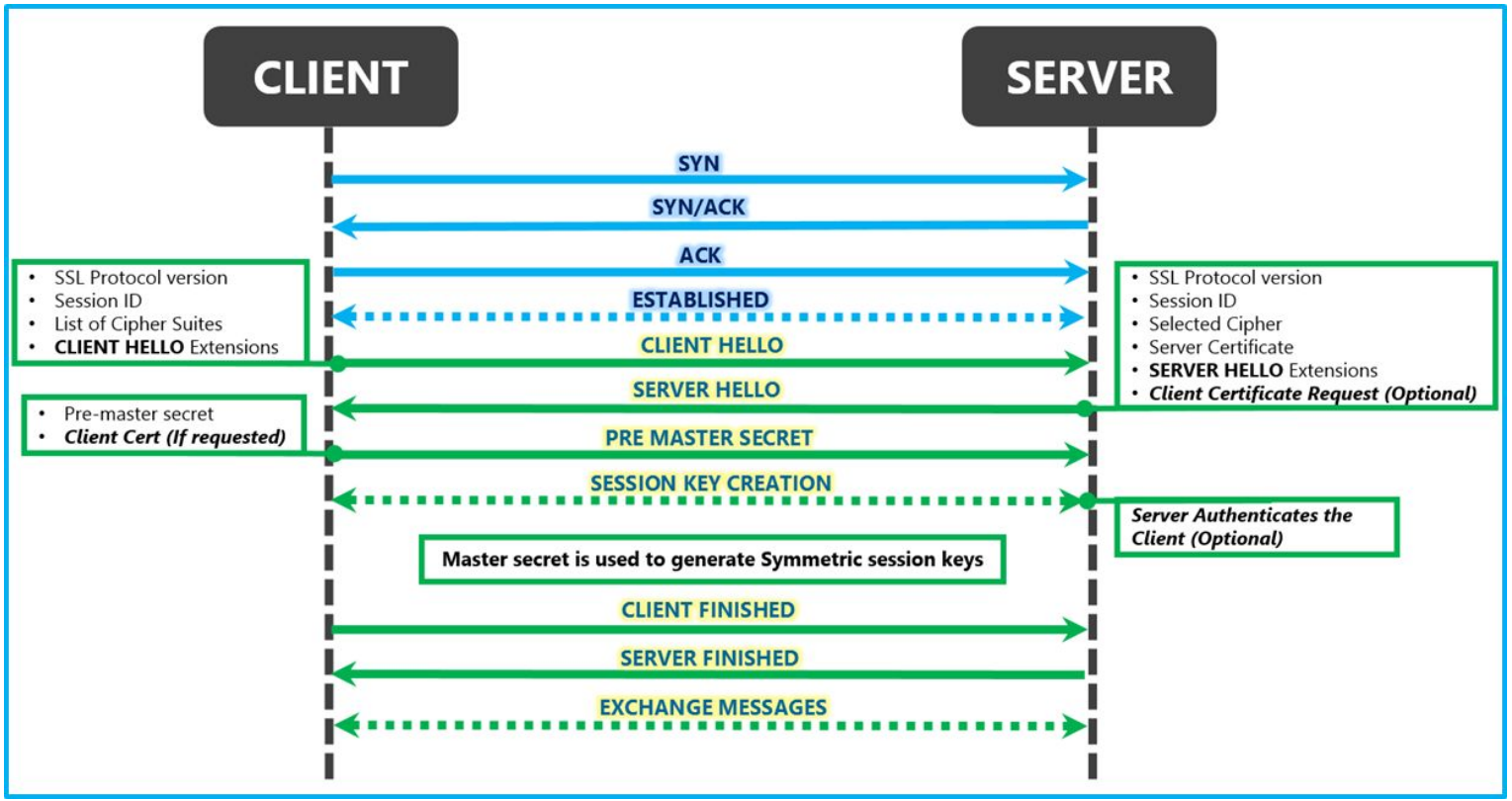

Provider
Provider
Provider
Provider
Provider
Provider
Provider
Provider
Provider
Provider
Provider
Provider
174.12.36.22
DSL-Modem, Router
195.12.113.2:80
http://egov.kz

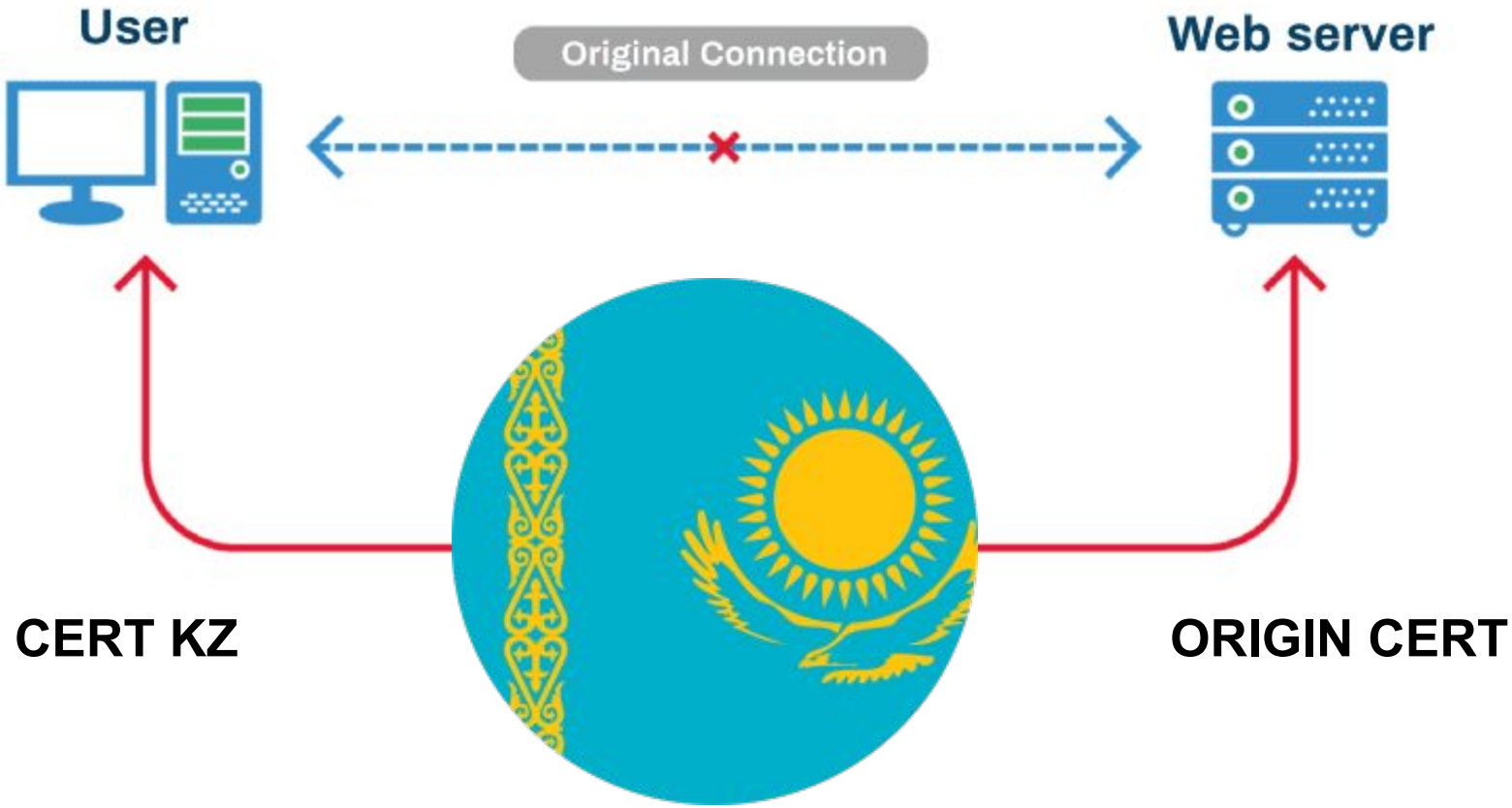

Provider
Provider
Provider
Provider
Provider
Provider
Provider
Provider
Provider
Provider
Provider
174.12.36.22
DSL-Modem, Router
195.12.113.2:80
http://egov.kz

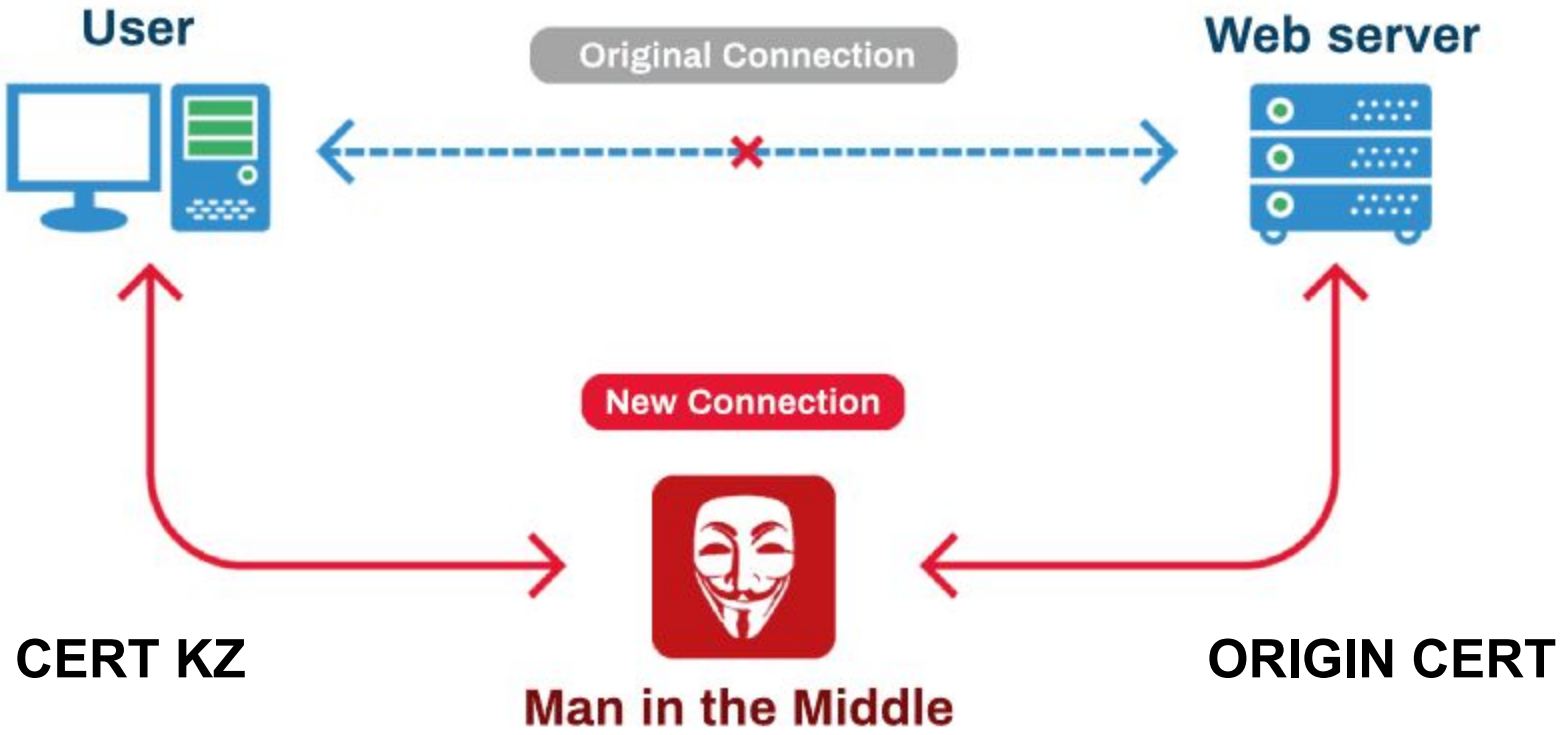

SPAM,
Fishing, Scam,
Fraud,
Spoofing etc
Provider
Provider
Provider
Provider
Provider
Provider
Provider
Provider
174.12.36.22
DSL-Modem, Router
195.12.113.2:80
http://egov.kz


SPAM,
Fishing, Scam,
Fraud,
Spoofing etc
Provider
Provider
Provider
Provider
Provider
Provider
Provider
Provider
Provider
174.12.36.22
DSL-Modem, Router
195.12.113.2:443
https://egov.kz

Cryptographic Protocols




User
Original Connection
Web server
CERT KZ
ORIGIN CERT


User
Original Connection
Web server
New Connection
CERT KZ
Man in the Middle
ORIGIN CERT

Information_Security_Certification_Authority_CA_pem.crt

Открыть в приложении «Связка ключей»

Information Security Certification Authority CA

Тема
- Общее имя Information Security Certification Authority CA
- Организация ISCA
- Страна или регион KZ

Кем выдан
- Общее имя Information Security Certification Authority CA
- Организация ISCA
- Страна или регион KZ

Серийный номер 28 7D CE 0C E3 C6 F7 AA A3 3F F9 65 E7 6E A9 8C 82 4A 59 DB
Версия 3
Алгоритм подписи SHA-256 с шифрованием RSA (1.2.840.113549.1.1.11)
- Параметры Нет

Действителен с пятница, 28 февраля 2020 г. в 09:08:03 Екатеринбург, стандартное время
Действителен до вторник, 28 февраля 2040 г. в 09:08:03 Екатеринбург, стандартное время

Свойства открытого ключа
- Алгоритм Шифрование RSA (1.2.840.113549.1.1.1)
- Параметры Нет
- Открытый ключ 512 Б : D9 0F 21 8D 84 FC F6 26 1F 0F E8 1D C6 26 8A C3 93 4D 46 AD 2C 7C A0 E3 D7 10 17 6E D9 A1 42 1F AD 03 90 E1 9D 53 DE 86 A1 72 6D 51 47 64 1B 32 33 09 8B F5 20 38 06 9F F6 CA D1 3B 0A 69 C3 79 FA A0 F7 17 D1 B8 D5 F6 A7 A4 73 52 0A EC 6A B6 1A 66 05 E0 68 F5 BE 83 F4 D9 FA 75 D4 B8 68 18 6F 52 34 D5 73 A0 E7 18 45 AF AE 5C 8C 83 39 0D 7E 4B F6 DA FD D2 DC D1 13 56 9F 8D E5 32 BD 3D 00 62 44 A8 75 0C C9 9B 07 90 1B 59 F3 59 0F 48 34 47 FF FE C9 90 7F A0 EF 82 EC 1E EA 90 99 C9 EF 11 73 06 DD 1F C3 FE D5 4E 6E 1E D9 88 28 64 96 55 1C D7 DF 8E CC D9 31 91 12 D3 9E 6A B0 1B 96 C7 E6 07 BE 6D FD E2 2B 69 C5 88 3F 4F A0 A1 04 9F F0 EF 78 D8 6A E1 06 9A A5 30 76 21 3D 89 F5 00 B6 29 80 95 53 A7 F9 A5 21 8B 65 1A D0 C3 11 EB BC 2C 76 C5 E7 3D 28 AC 40 4B A7 EC 79 68 06 EA 6F 02 14 5D DB C8 7A 37 A1 15 2E BA F4 CC 5B DA 9E 4A F5 70 DB 15 62 49 E6 8B 27 EA 90 0A 15 D4 F1 EE 8A 34 1E F1 90 3F AB D5 11 DB 07 93 36 4C 7A 78 63 F1 4E FA 8C 39 49 28 B0 19 8B 64 70 C3 75 2C 7F 2D 28 6E CB 0F 4F 52 2E 47 C2 4B 8E AA 55 83 05 F0 28 C6 9E 2E C1 9F E0 65 24 A8 12 CD B2 3E F6 7C D2 B9 34 60 89 59 E4 60 79 DD 06 FA 3A 9A 3F 6F CB 7F 65 02 6C CC 55 A4 09 A8 01 C8 8D 75 57 B1 63 DC AD 1F EC 0F 5C B2 CA 6C 63 C8 28 02 8F A9 EA 45 DE F8 57 E3 21 E8 2F 64 3E 81 1F 47 C7 5F 78 AF A8 51 75 F1 D5 00 A9 27 0E 81 BA FC C5 96 CD AA 84 89 E7 9C DB CA 17 08 D6 70 5D D9 0F 58 9C AC B1 AD 44 E9 6D 5F A2 32 FF C6 17 6F 9A 21 D4 15 47 91 DE B8 2C C6 23 0E 77 1B E1 16 EB 0A 6E E1 E3 62 91 B0 6F DF C3 EB E0 FB 85 44 06 95 26 7F F1 43 16 DE 17 D6 88 97
- Степень 65537
- Размер ключа 4 096 бит
- Применение проверка

Подпись 512 Б : 3D D0 C3 61 97 A8 E2 7C 05 4A 9D 37 7F 36 3B A2 B0 74 39 63 27 35 61 83 19 0E CD C0 BA 6A F7 E2 B2 86 7E 56 18 FB E1 DC BB AA 83 26 43 CE 0C FB 25 E7

ZDNet

Apple, Google, Microsoft, and Mozilla ban Kazakhstan's MitM HTTPS certificate

Today's ban also marks the second time the four browser makers banned a certificate issued by the Kazakh government for man-in-the-middle ...

Dec 18, 2020

Security Boulevard

Kazakhstan Spies on its People via Man-in-the-Middle Attack, Again

Kazakhstan Spies on its People via Man-in-the-Middle Attack, Again ... If you expand the row you can see the nation state MitM: notice the ...

Dec 7, 2020

ZDNet

Kazakhstan government is intercepting HTTPS traffic in its capital

Under the guise of a "cybersecurity exercise," the Kazakhstan ... made from users' devices via a technique called MitM (Man-in-the-Middle).

Dec 6, 2020