ECE458/ECE750T27: Computer Security

Cryptography: Linking Keys and Identities

Dr. Kami Vaniea
Electrical and Computer Engineering
kami.vaniea@uwaterloo.ca

UNIVERSITY OF WATERLOO | FACULTY OF ENGINEERING

Last lecture:

- Symmetric vs Asymmetric Cryptography
- Diffie-Hellman key exchange (Symmetric key exchange)
- Public/Private key cryptography
  - Knapsack cryptosystem (Asymmetric key generation)

- These can create a shared secret key but….
  - Diffie-Hellman – key use only proves that communication partner same as when key was generated
  - Public/private – key use proves nothing about authentication

Encryption properties we want:

1. The communication between you and the other party is **confidential** and has **not been changed (integrity)**
   - No one can read what you sent
   - No one can change what you sent
2. **Knowing who** you are communicating with (authenticity)
   - You are talking to who you think you are talking to and not someone else

LINKING KEYS AND IDENTITIES

We still have a problem:

Public/Private still assumes that we know which key goes with which person/entity.

Linking keys to identities is one of the founding problems in Usable Security and Privacy.

Even now we have no good answer.

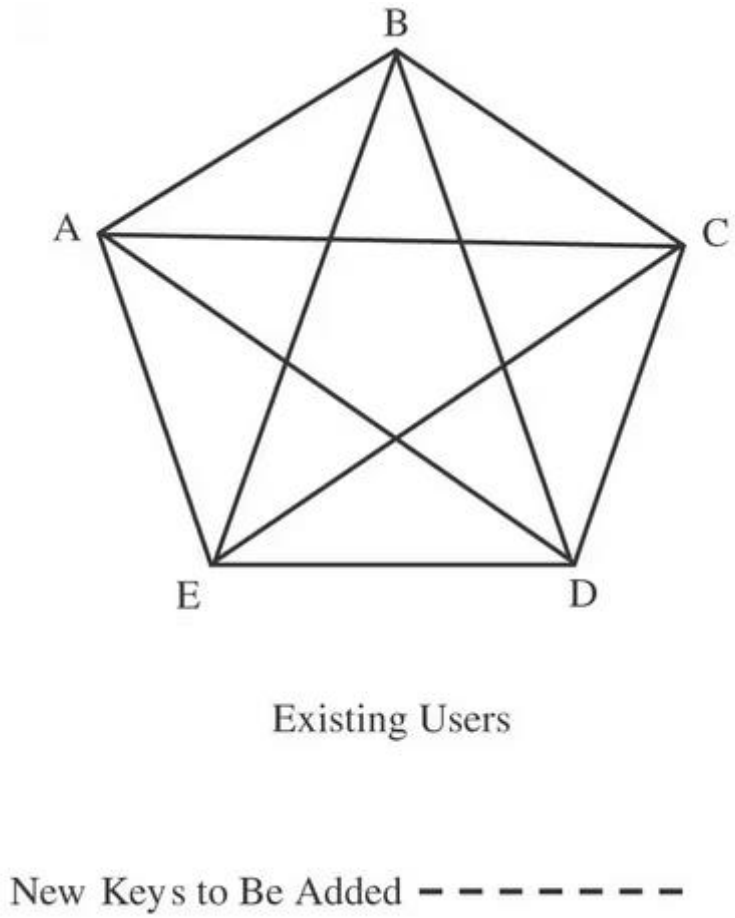
How do we solve the identity problem?

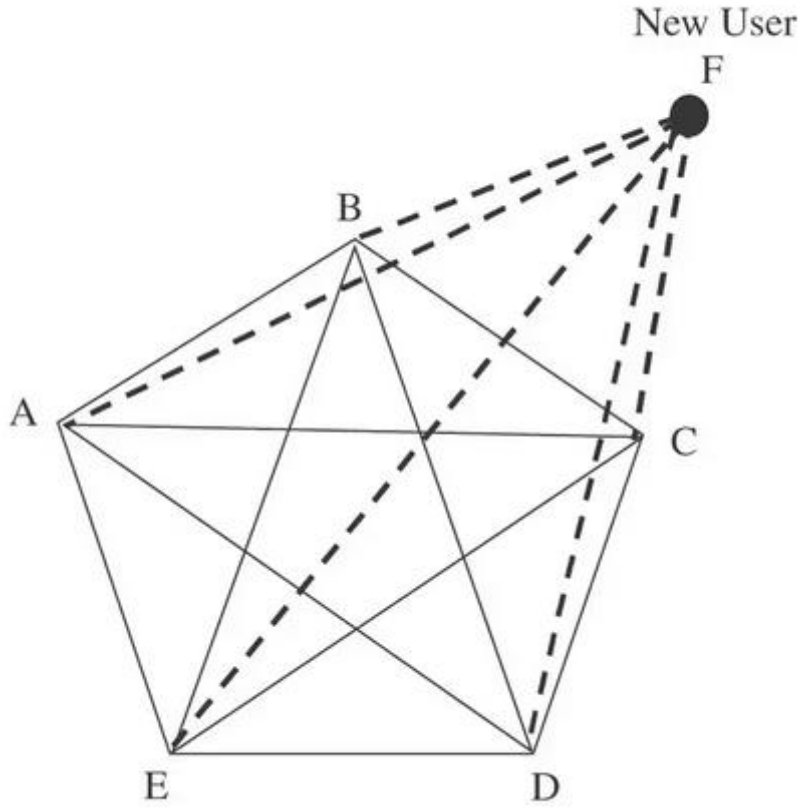
Idea: Have the humans do the linking of identity to cryptographic keys.

Approach scales poorly

An n user system requires n*(n-1)/2 keys

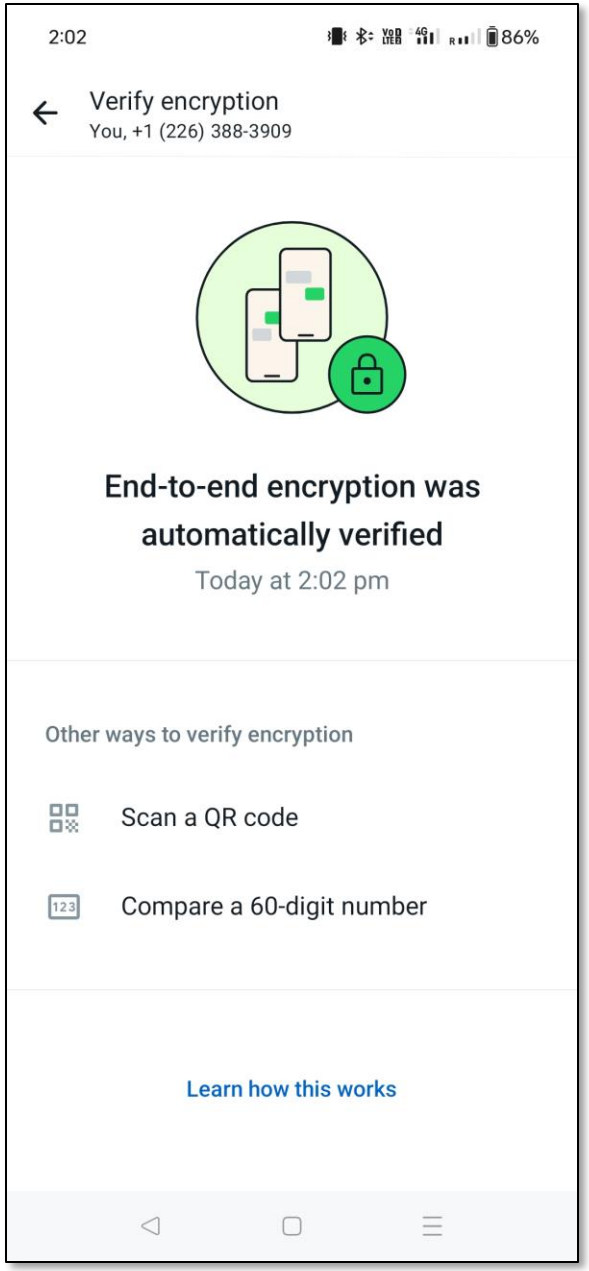
Expecting people to verify that many keys, as well as store and not loose them is unreasonable



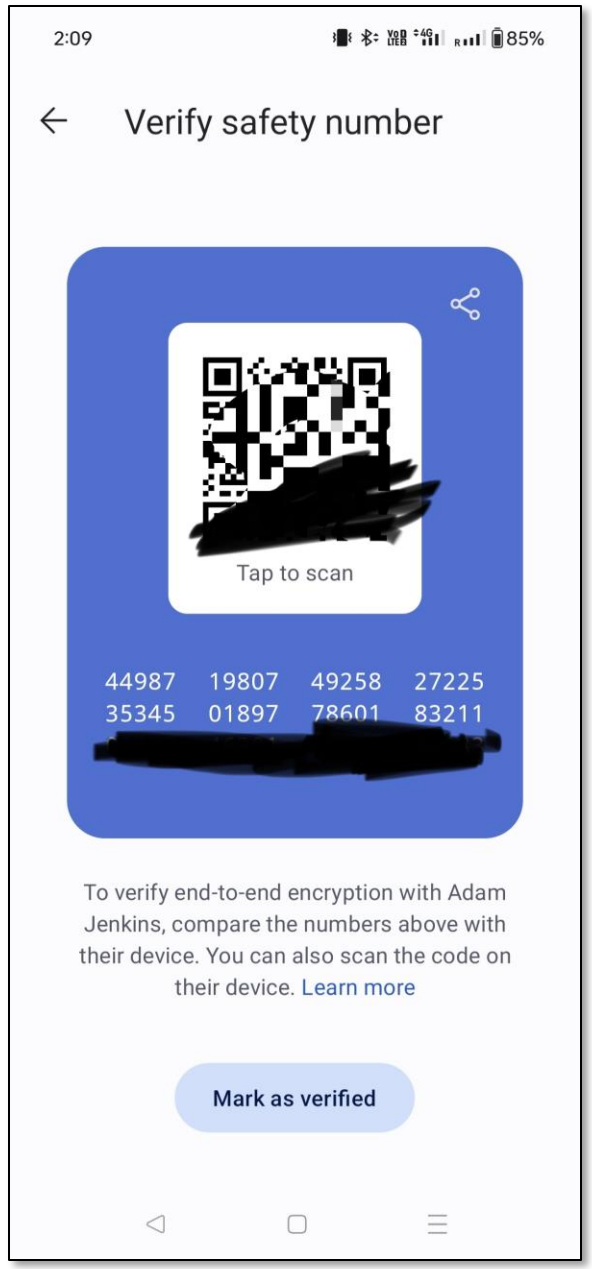


User comparing of keys is still used for verification today by common apps like WhatsApp and Signal.

WhatsApp



Signal



We could post the public key somewhere highly public and verifiable it came from us.

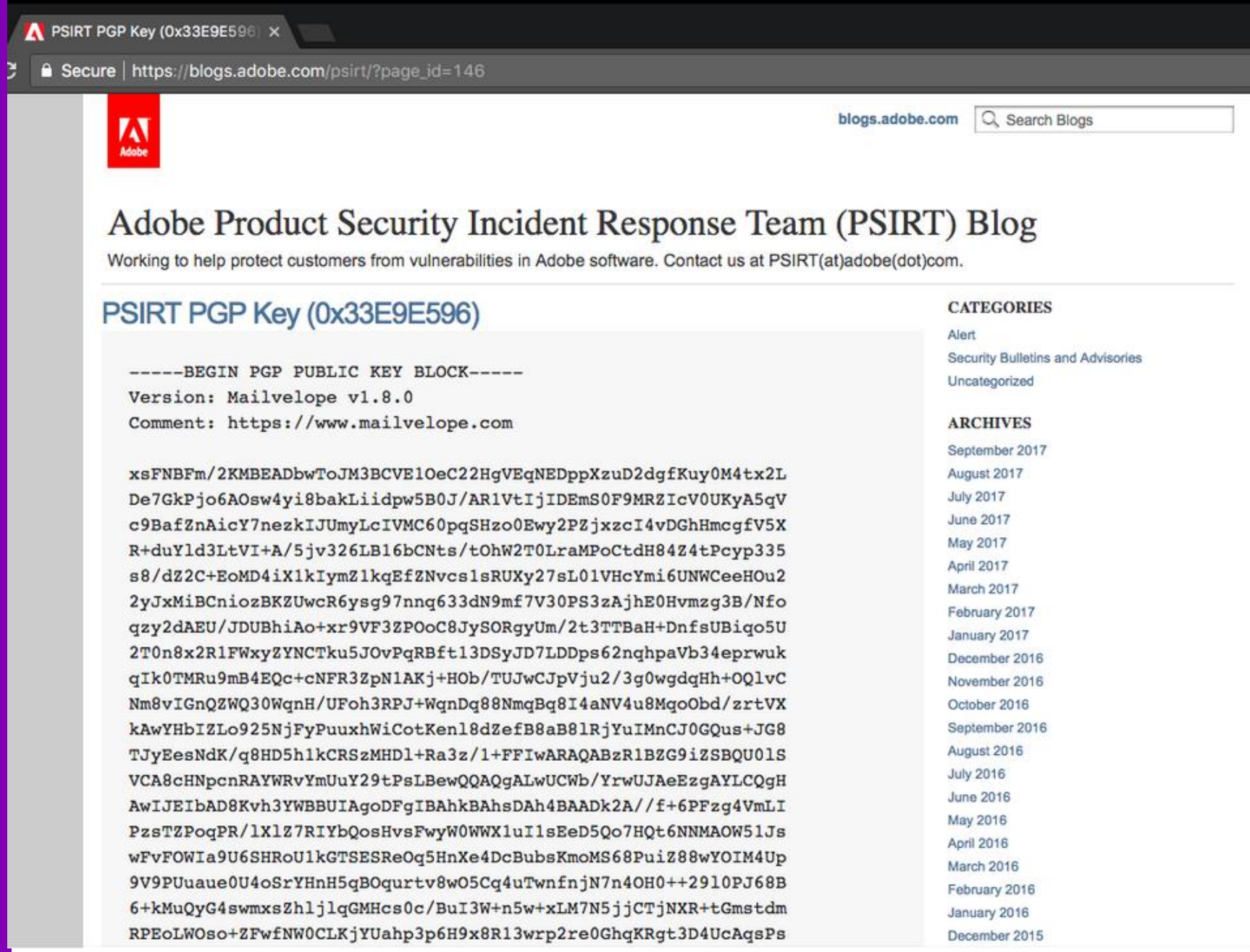


Photo credit: Juho Nurminen @jupenur

Other people can then compare the keys on their computers to the highly visible copy.

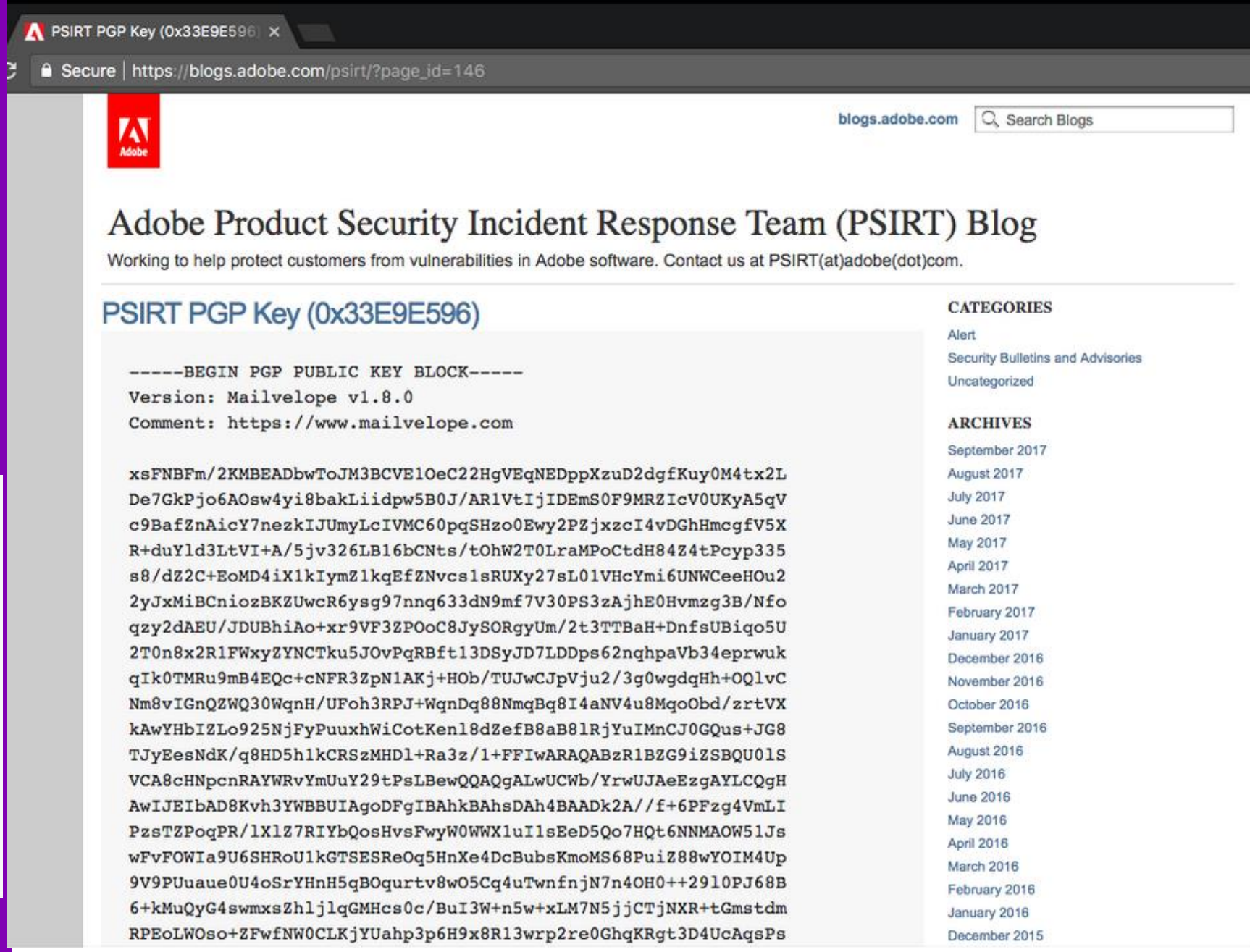


Photo credit: Juho Nurminen
@jupenur

Though we must be careful to post ONLY the public key…

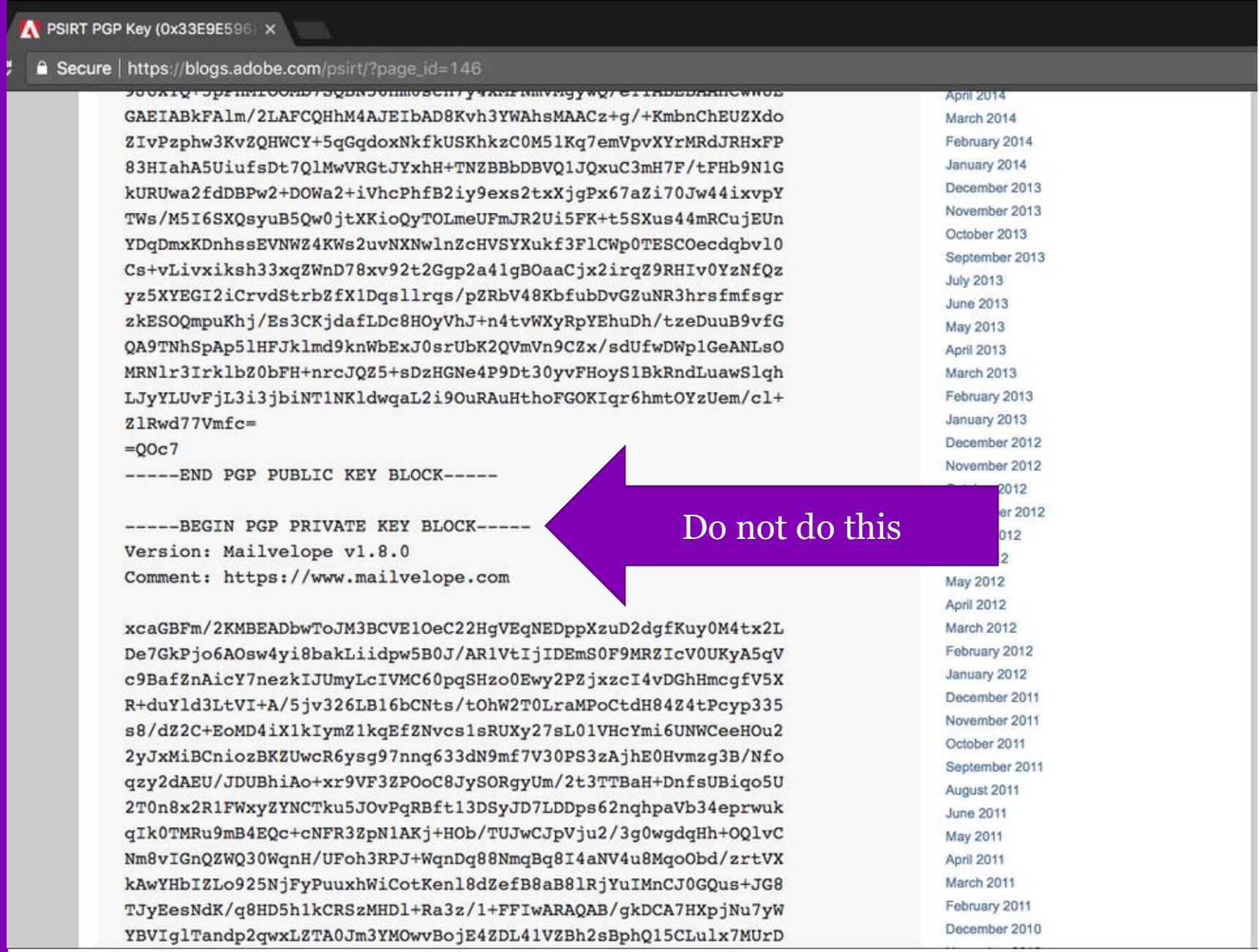


Photo credit: Juho Nurminen @jupenur

Nice idea, but it does not scale.

Also a chicken-and-egg problem. How do we find a place guaranteed to be from us without using cryptography?

Idea 2: Crowdsourcing!
We could slowly build a web of verifications like:

Alice verified Bob's key
Bob verified Charlie's key
so
Alice can trust Charlie's key

Web of trust

- Alice hand verifies that Bob's public key really does belong to Bob
- Then Alice "signs" the key by encrypting it with her private key.
- Now anyone that has hand verified Alice's key, can also trust Bob's key (if they trust Alice to do verifications).
- Key signing parties 

My public key

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2

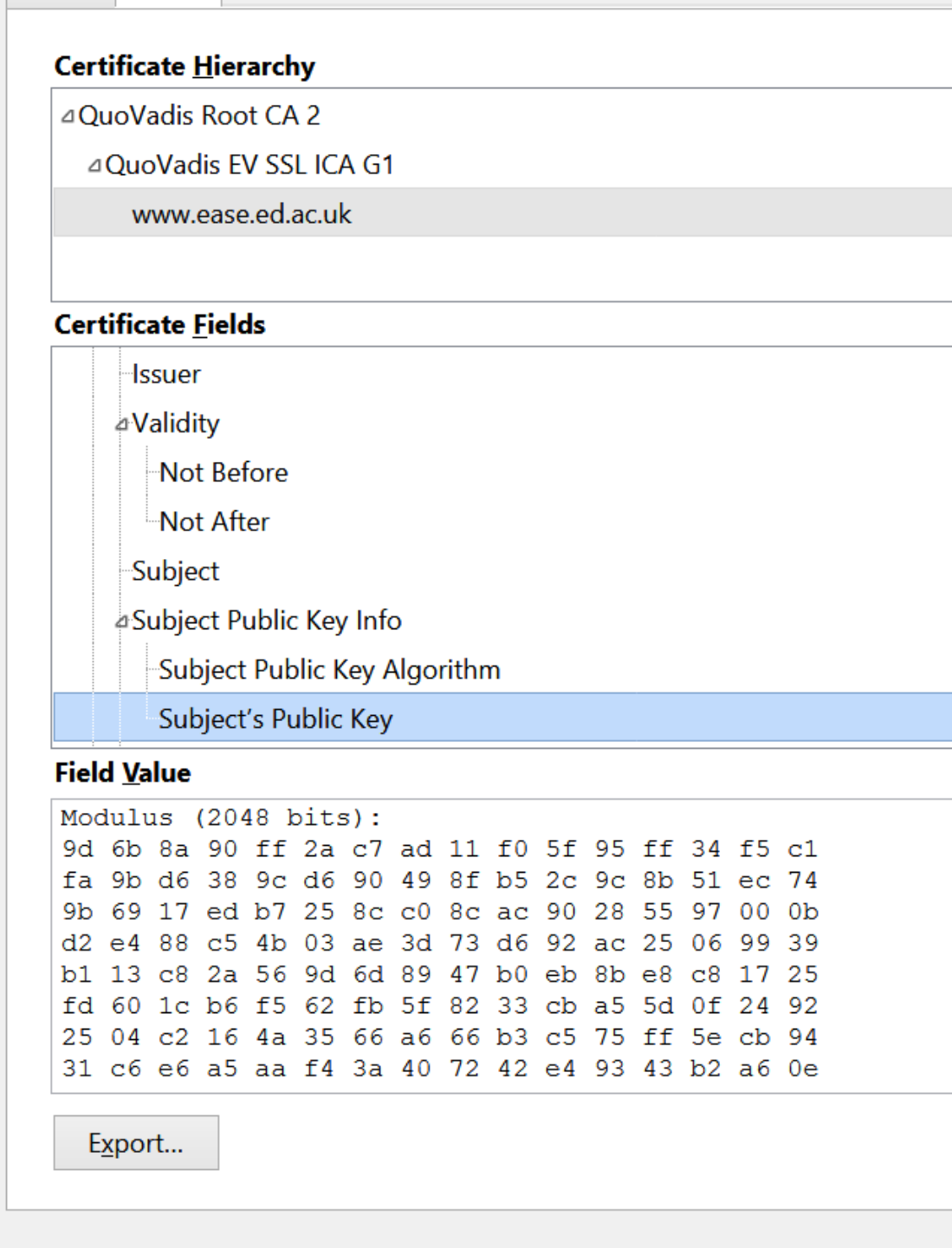
mQENBFHMcgABCAC9WrYDO6K2L3VHyi4eHN6suHLqMpJ+SO+IUTuLEVnUzIoXAUXH
KozHejfV/9XoG8j933ZtszXKCog3aMESe0E0z6fNGfolvaCe5B4jwq0Jt8NHwb5L
B2dnq0CplgXcN2GJxfEHHUaf27COSobCJxPMeshUh4ZHke+g6DatmiEtBpVp41Ot
1zgxdMQkgb2H2xw28RYfYkdDoueteIkOrFLrCy9ZF9KdMhA1eBH94KnwIQshdiZR
QYEX25+M8cKCb++Rc9H6an7EG9WHOFRW40UsY52OfveOyfQPzkkRto7u2339hvHo
B/h+7xLM6FQbOUZQ9BD5w7IQHgYtXJVsUjodABEBAAG0IkthbWkgVmFuaWVhIDxr
dmFuaWVhQGluZi5lZC5hYy51az6JAT8EEwEIACkFAlYKYvECGyMFCQlmAYAHCwkI
BwMCAQYVCAIJCgsEFgIDAQIeAQIXgAAKCRCTdsxl9/HZffG+CACShuKxje3QAqew
GWh8K4gCdiYoxDqJwq3PHxmyhZmQeN/1a1KcOrIjI2b+Q75/5t+EgXOHpR0PIxfG
lZ6zOEpf6A18iFXx3JgQZdwPD0jtBiWNpOyMeBGTgIvEYG3so2VueQoeXcq3dbYp
5vstVxtD+TKHQ5CioIT75P2bzYq/XLT5aIbNQhQDPcTo0DgbRH+FvqsRXr7yeaef
JaPnxX0+1L33t2QY9zctiGyebwrvHMrIPBJ2VYCDzQkJ7uQ5eFh4ZhsMgOmzLQD4
YiGr5weIMFwAvxZOaRxEa9Vf48jiWvrxuJ8YfHWS0hEScNOcYC2P8q20lJwwE26T
lpdtrwCqtB1LYW1pIFZhbmllYSA8a2FtaUB2YW5pZWEuY29tPokBQgQTAQIALAIb
IwUJCWYBgAcLCQgHAwIBBhUIAgkKCwQWAgMBAh4BAheABQJWCmMeAhkBAAoJEJN2
zGX38dl9JJAIAIW0rxrlYsrmKS6CbW8MgTxxTDOXaCt1b7F0W0QZHskIUQhEcE+a
XBYib1A5uHaatLfyjeXaD3qMEoZnQHoYMGE0GKu00wWsbhfoQzHPgwzRLkD1i75M
BIbaww0KW0VB9e4AkMakXJCnF5BXe06AHRL2v15V205DikVnlCRXocKtu8b7LnkM
cLn70Lobr1de1uyKoNzbSnO/vpKDJp0/EY5yUeV90IypZy/6wFQBehg1sXye6zn0
9wb9uUsu9+/P8pz4JILMDSevjfT7zSRSl/YP3fOfZ6N4bc+KOdwPM7u5Iyoeu9zh
pzibv3ge7VhH2xIWz8vYZ/2xT1345tWRRMOJAhwEEwECAAYFAlTnSpEACgkQjyxM
p99tBt2B8A/+OpIzOsQbQJB8yxti4I7PpD1weJDf3a81Vhm7JyXE/Xy66ypfdt3w
XmFRUuIrwezY1NebWNCRQHzQvRv/VJwjbTUx+Q3HsjIkKlHbE7iCiQXXtTRkoEny
2nudcjGI2v03C3B2JCucEw6esF1x79PI/lPv2+6tgUBKmDfOpsB2vbtqrHnmAYKL
4lQBFH1YSJgnzwo2Jkh0hcHdF90Zem1eMeiDEeVkH63893N8Swk5fBKdTj+SKZ/L
rQElBBlpMR9BmeY6bPvWRuycVKonIMR80G9iFABxjTpWBL8aGk6EeVK5EqYDGvkd
ZIarK84r+KU1KD5IfgOCN7nhwgy7VImE68caZHSRiPWZP1fVVMhydiRJv8WsoUs6
INfVU3nxH+ZYthPbY0T86leGSchBT5K/fBQvbjhrRTbTFwvjzSifb9efWylDi994
nzP6cNorir3GIpsT8gPgBB2/NjxaWiM6y3X1az1vRnsunQHuyKkFWPZwnEvDJYaC
NN/3jWcbhLFwKBDsaHps2+1meFP0oJFvNetzp2bjT9a9pXaQ6KhOmo5DnhLcaV97
bFBpsUuBGaYZTSS05x1RdXHqpEbgap8dtuHhVvJw9QYDQBJr0K4aKyG9qqMD8cta
Pl/FAdyAqwH8Nw9efqAK+RQxSVUaue9BYEnbIRpsDK6MkP3YMFmu5ki5AQ0EUcxy
AAEIALyXYy8G2ZaTDJpdGcRhmIqOOSUlzPV7/5E5BbYKBNu4KU3nX+JLVcF5jxPQ
42c7i/WRVxE1BJTiarKGsEvCi94TTXSIUKAt3T10GBtXmGvqbGBq8ljSGl1UTwdF
5yu50JyRSf2fqRND6P/2eHNXejDUtdvhUXIUt8h9MuUO/ipD0DnwIvMnAATJHA+R
Zqw60NpyjRGzvr3iuWUwe4PtyJDI3ELAFkbp/NAc5TIuVHRHNOWNplcIJhM5zHuB
QQb3G/EsCn2PQZ5w5SDzavF2SpvQfDqxYpDaTLAXtF+wsJL5iaUjxwRgJPOdbCZf
2Tozd7h9MXtGJDlPKJ8eLG80gcMAEQEAAYkBJQQYAQIADwUCUcxyAAIbDAUJCWYB
gAAKCRCTdsxl9/HZfS+hB/9BJqSmIgcoHFXnb1PVIKxekzL8+WVm5Pk/EgMQSLZ2
HX4p3ial5PEPcYgUw9YnaG4i00dwJGw5/daTWRrTzcnKd8Yq0P+DU0t96HZDSu3m
mCzE9NVAQYboFbVmGOx0eo627UBSvFqaXvAxBDYkoR8B0TnKhrQFwXkZVb30hKwD
TgAFjOGlZiE6uAdST231tFaq0bizYfe5AVXRqro20xBqNbaJNqs3SW0D831Syvdv
llOBx83/R0gg7hUkI6F2vzXicWmUwFSXRrggCSbLosHsP6isBWwvlHeRmna/aQab
YKG3gbV9iyczAS31gbogVLAZqNSWhp8vVIEE28Fyf/Ed
=x5FK
-----END PGP PUBLIC KEY BLOCK-----

Wonderful idea in theory. But verifying those long keys is hard… also I don’t trust most people to do a thorough job of it….

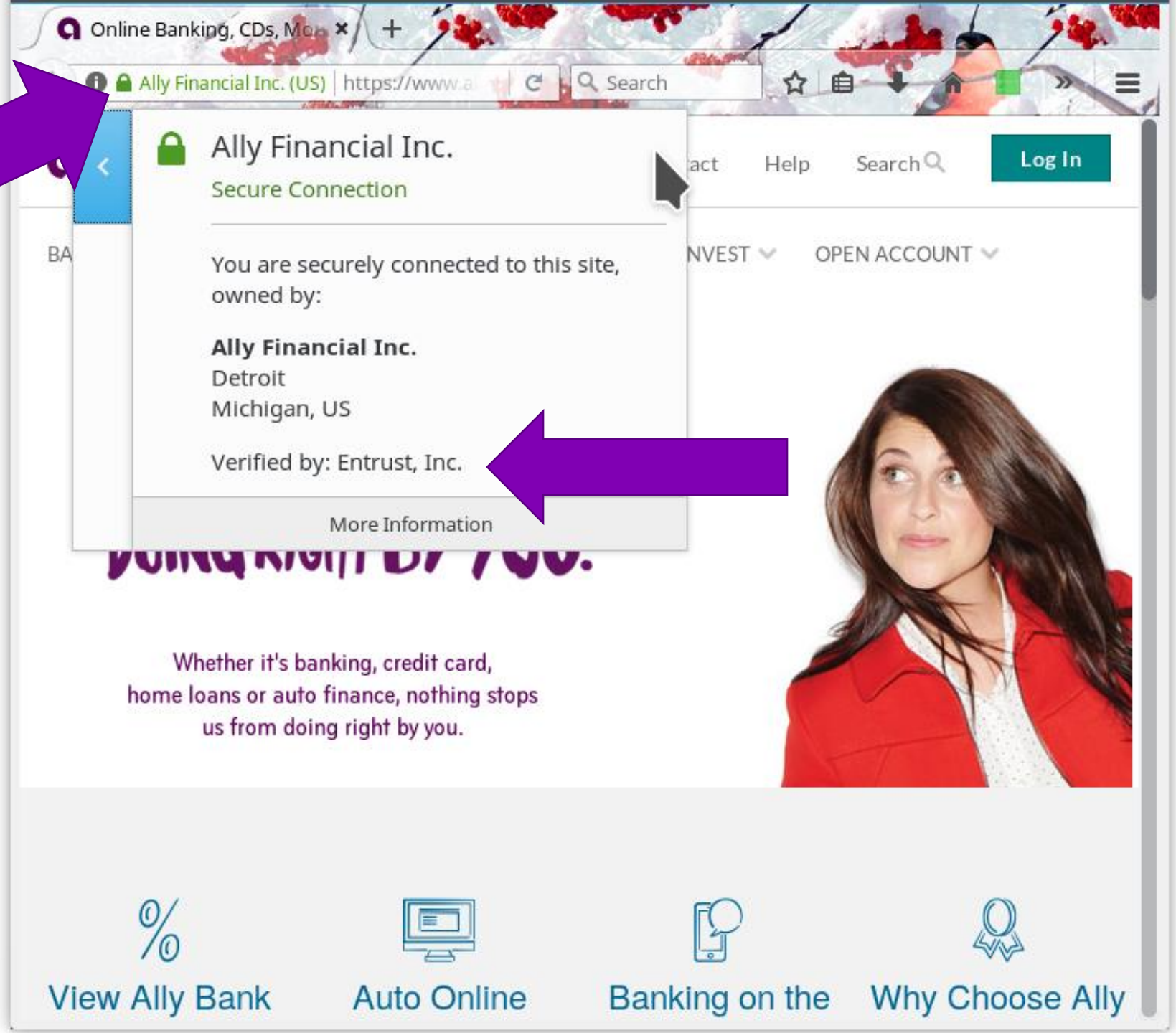
Idea 3: What if a couple of trusted groups did the verifications. Then they could have high standards and everyone could just trust them.

Certificate Authorities

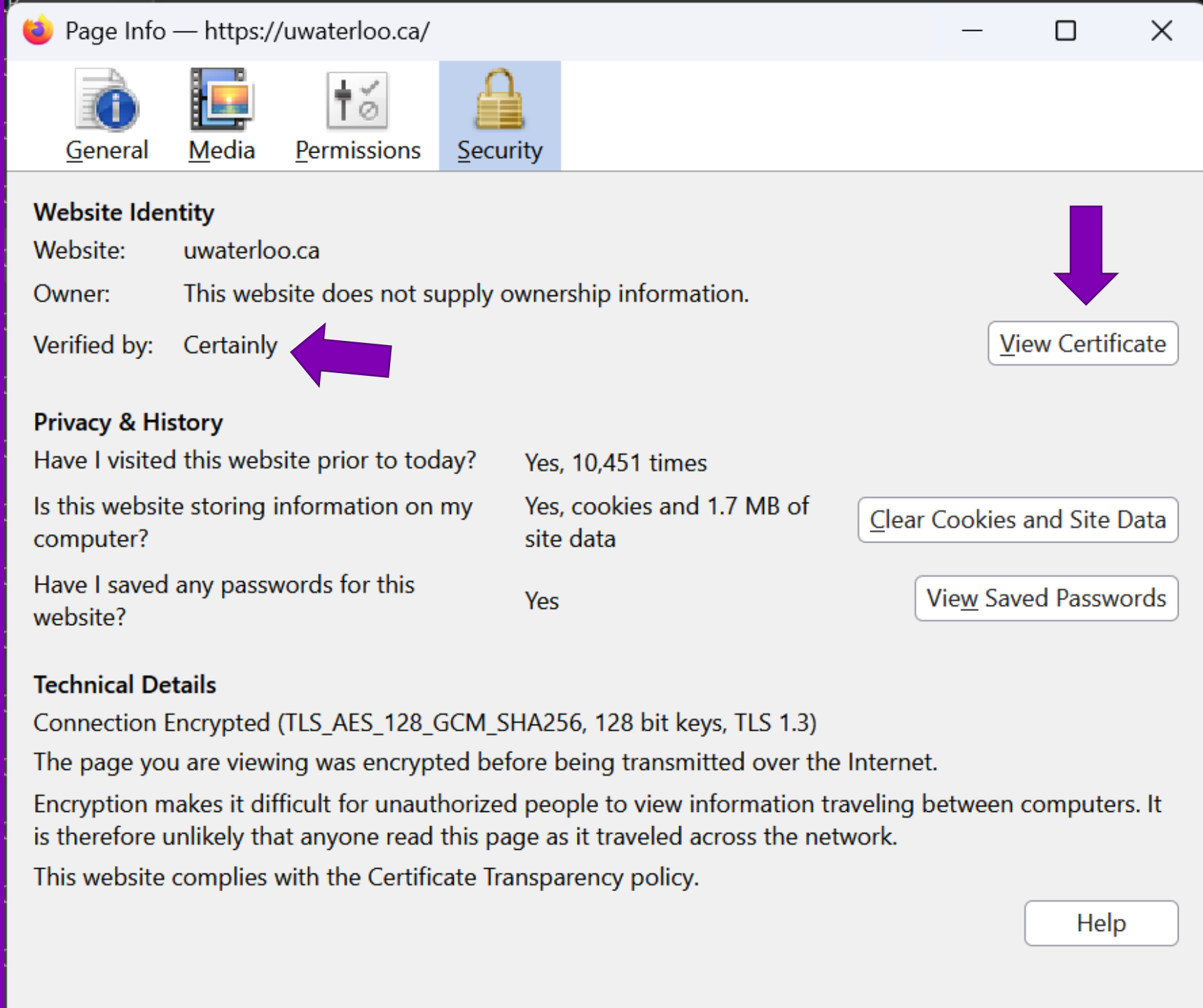
- A certificate authority verifies some properties of a person/organization and issues a “certificate” signed by their private key.
- Certificates can be quite detailed about what has been verified, and what they have been verified to do.

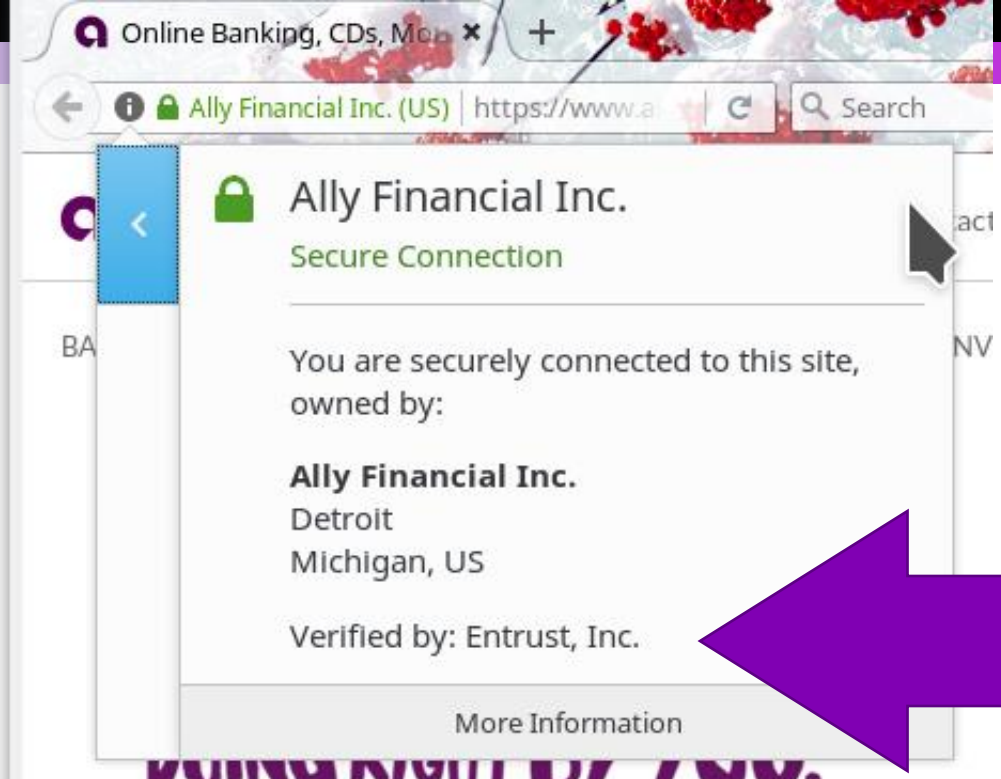


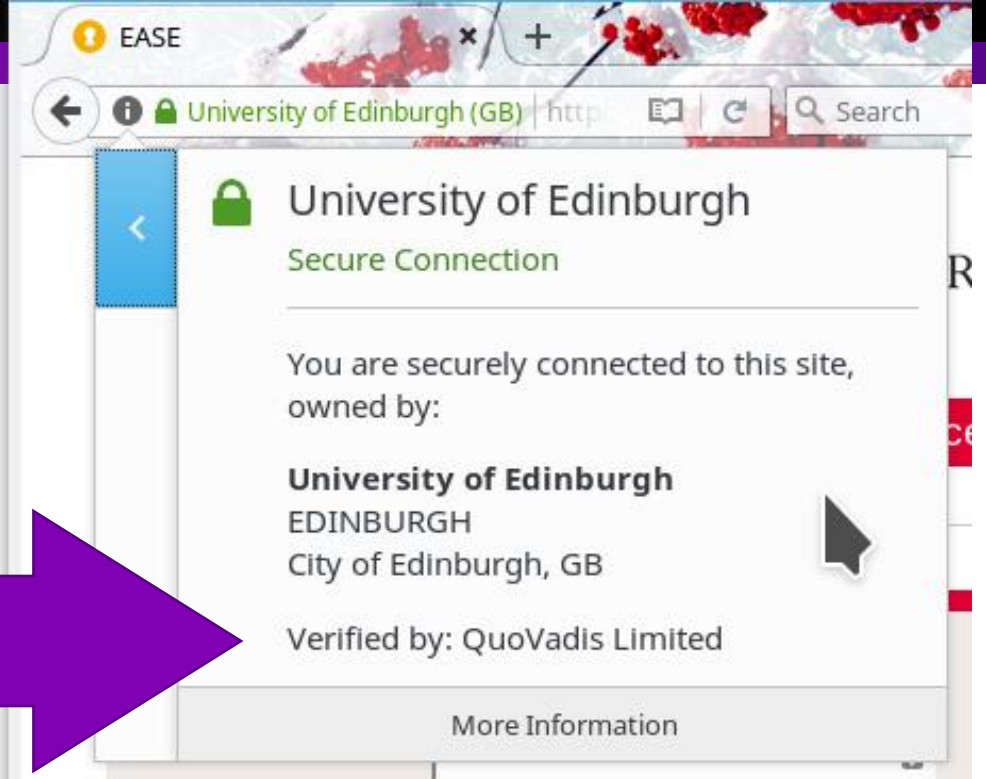
Certificate Authorities are used by browsers to verify identity



You can see lots of details about any encrypted connection.



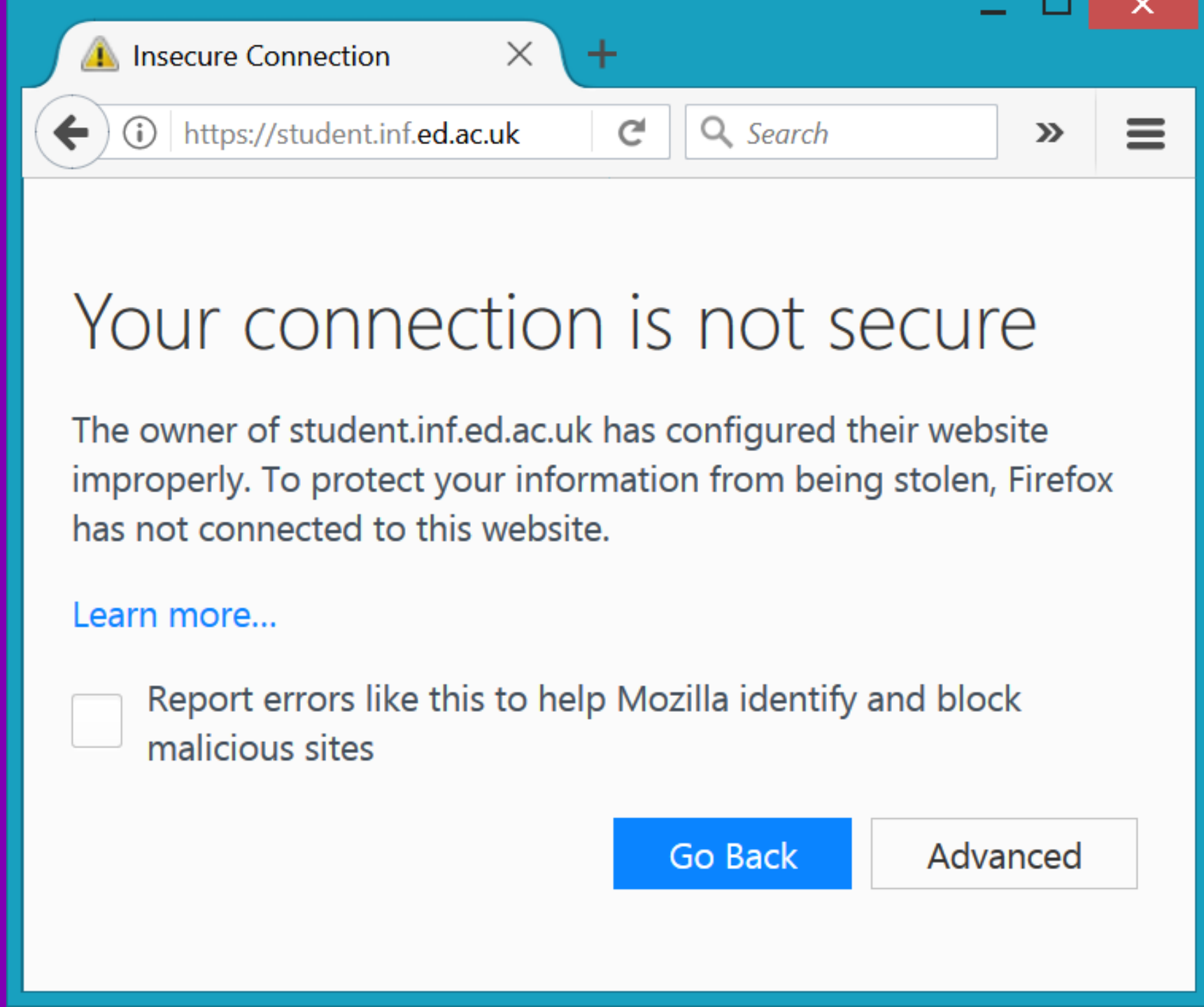




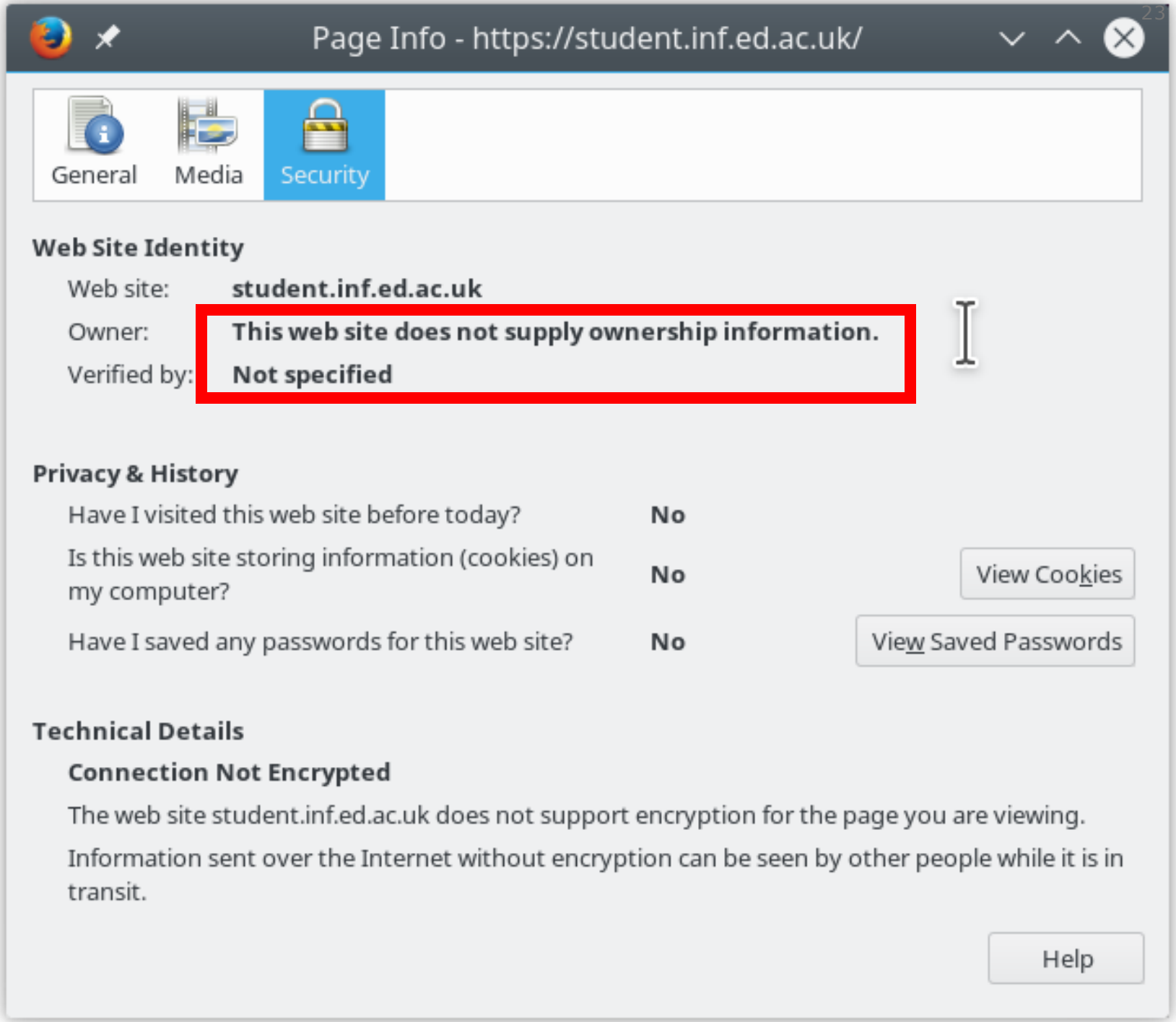
But now don't we just have the same problem again?

How does the browser know which Certificate Authorities to trust?

Clearly some Certificate Authorities are trusted and some are not.

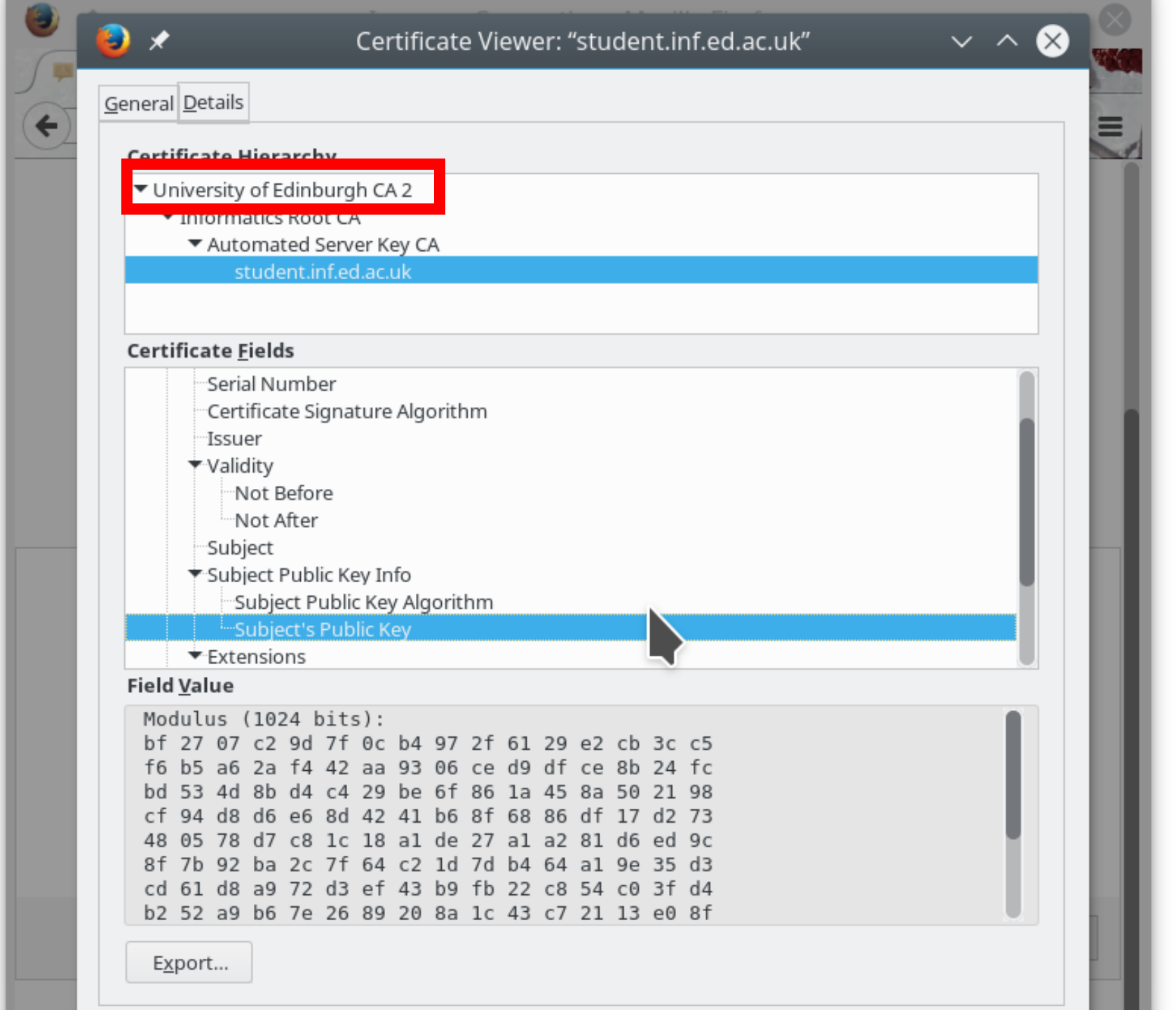


Errors like this one mean that a certificate exists but it is not signed by any organization this browser trusts.



This site is “self signed” which means that the University created its own Certificate Authority and used it to sign all the sites keys.

Why?
It costs money to get a signed certificate.



Your operating system and your browser both maintain lists of Certificate Authorities that they trust.

These lists differ between operating systems, browsers, and organizations.

Each organization makes its own trust decisions about Certificate Authorities

INFOWORLD TECH WATCH

By Fahmida Y. Rashid, Senior Writer, InfoWorld | MAR 24, 2017

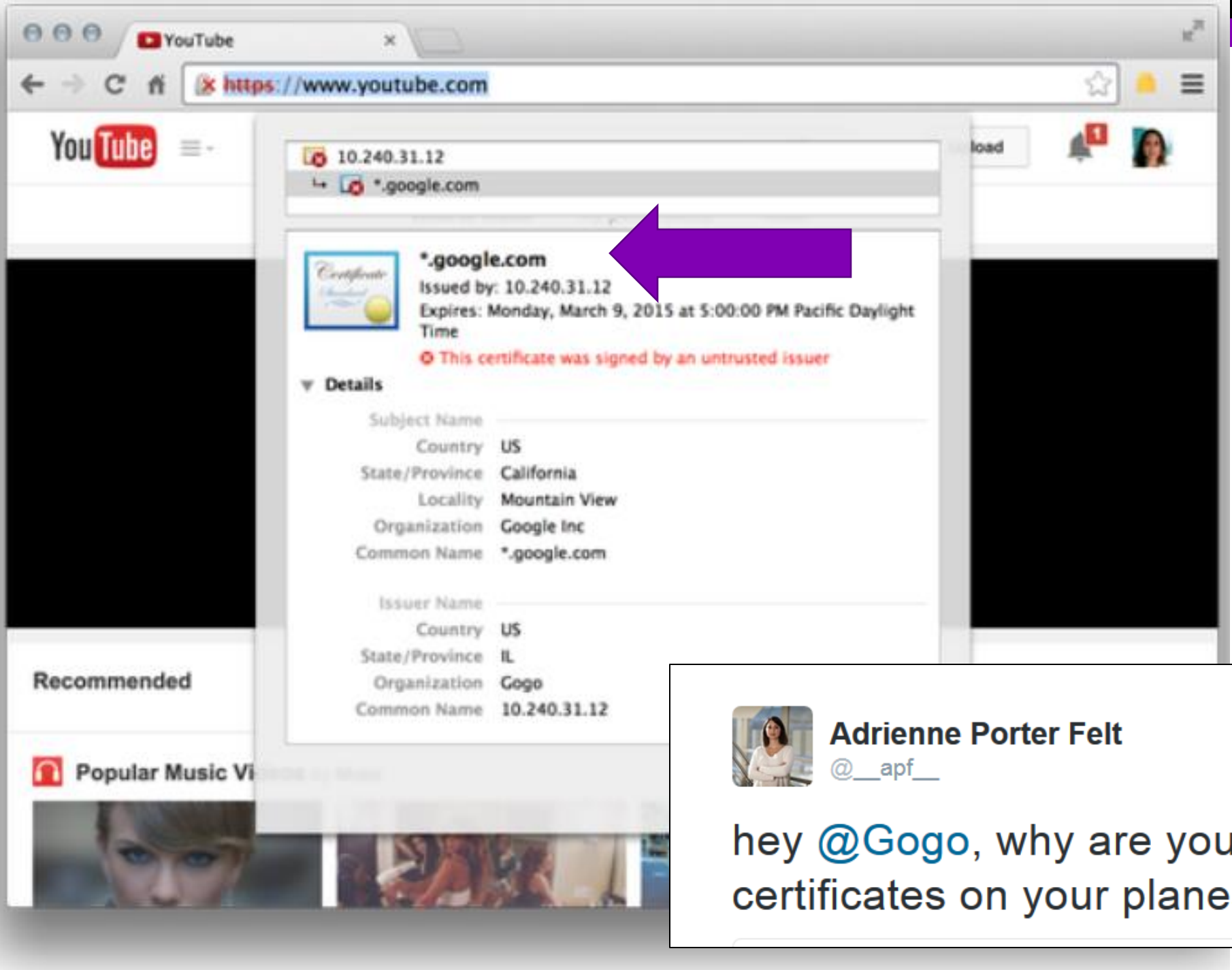
Google to Symantec: We don't trust you anymore

Admins need to consider whether they still want to use Symantec after its repeated mistakes with issuing TLS certificates

geralt via pixabay

Security teams, network administrators, and operations teams have busy days ahead. Google's Chrome development team is fed up with Symantec as a certificate authority and has announced plans to no longer trust current Symantec certificates.

In the past 18 months, Google has tangled repeatedly with Symantec over the way it issues transport layer security (TLS) certificates, with Symantec promising to do better. The latest incident—an investigation into 127 mis-issued certificates—ballooned into "at least 30,000, issued over a period spanning several years," Ravi Sleevi, a software engineer on the Google

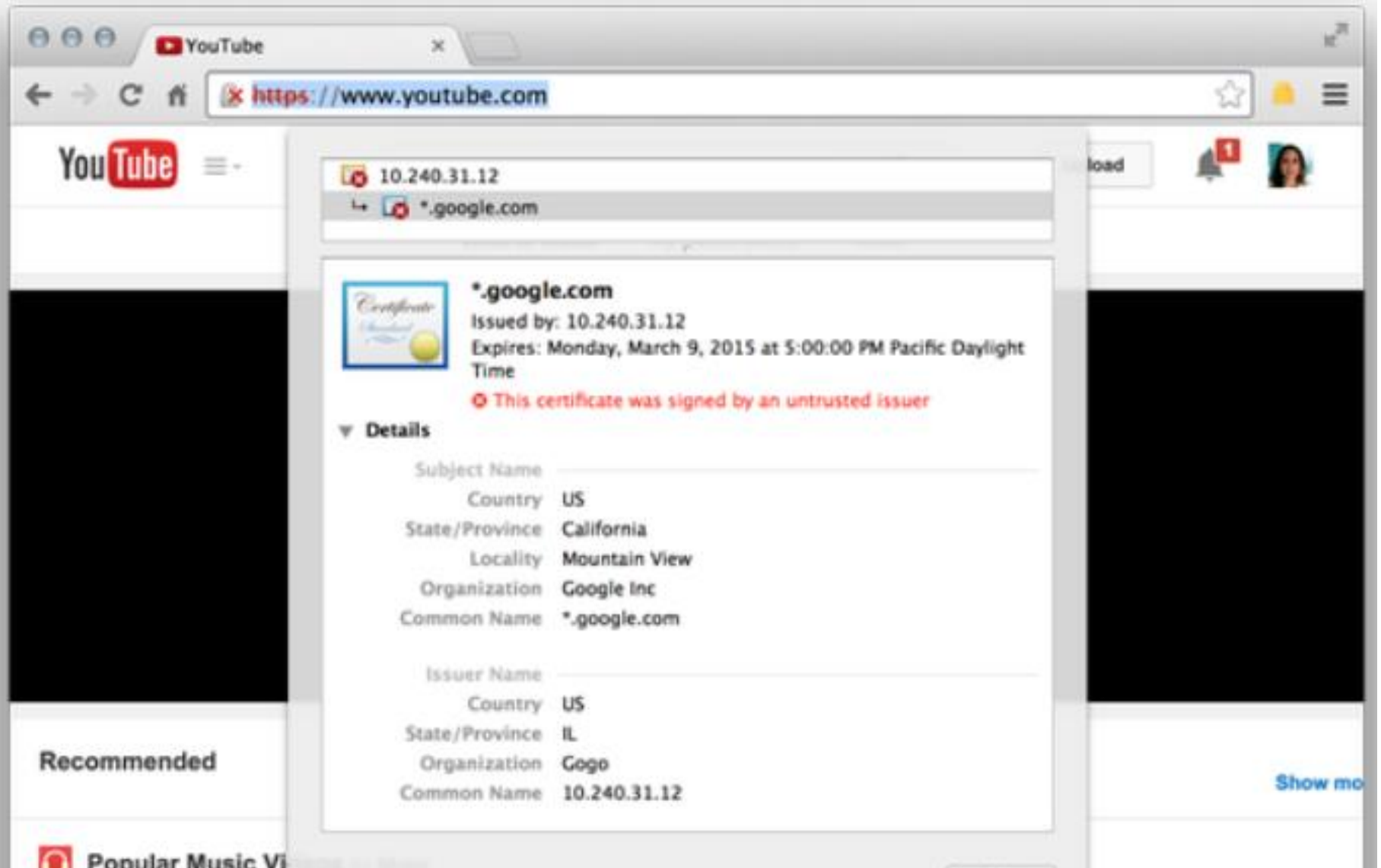


Adrienne Porter Felt
@__apf__

Following

hey @Gogo, why are you issuing *.google.com certificates on your planes?

Think-pair-share

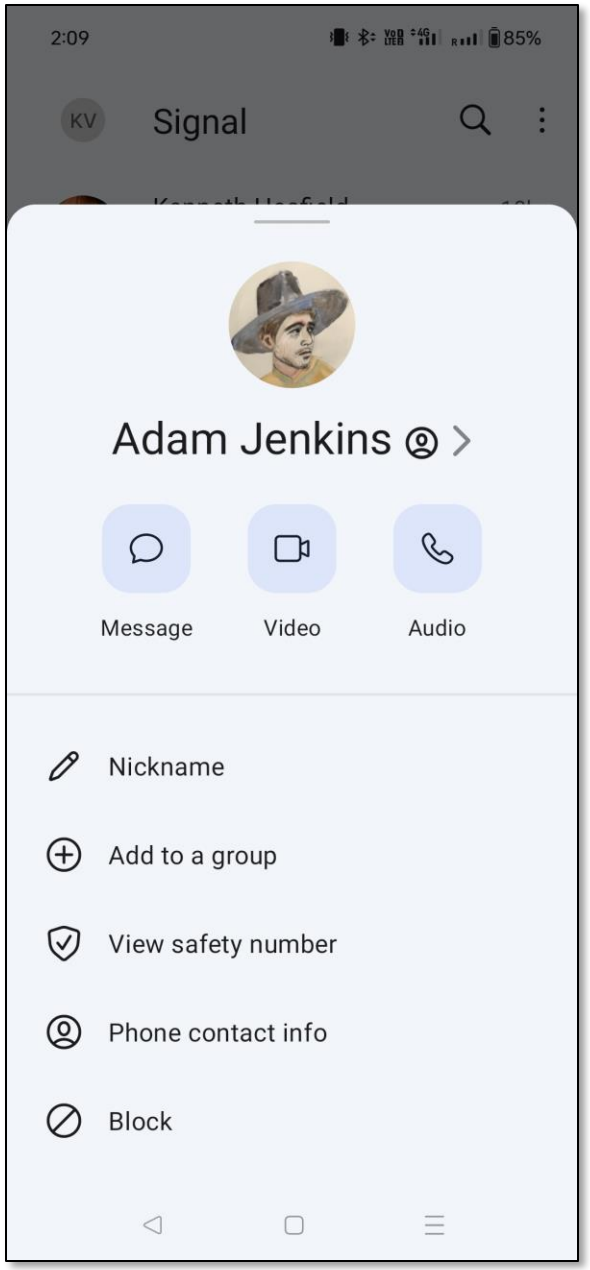


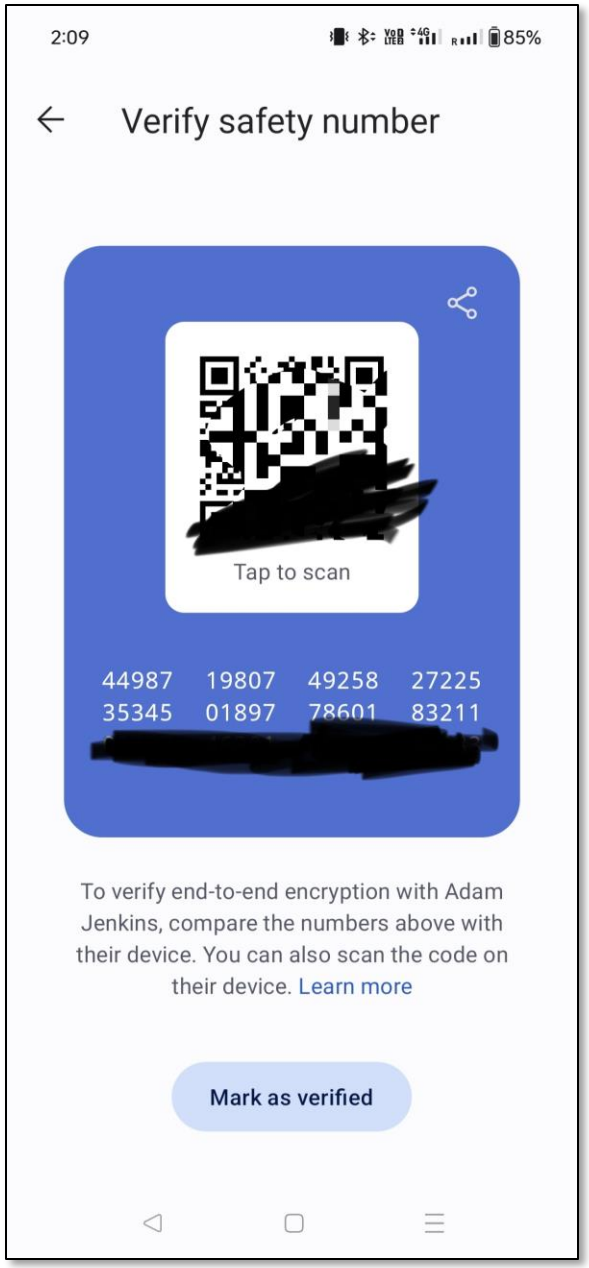
- A Firefox user would (theoretically) have seen no error in this case.
- How was Gogo able to successfully load a Google page with no errors on some browsers?

END-TO-END MESSAGING

Signal

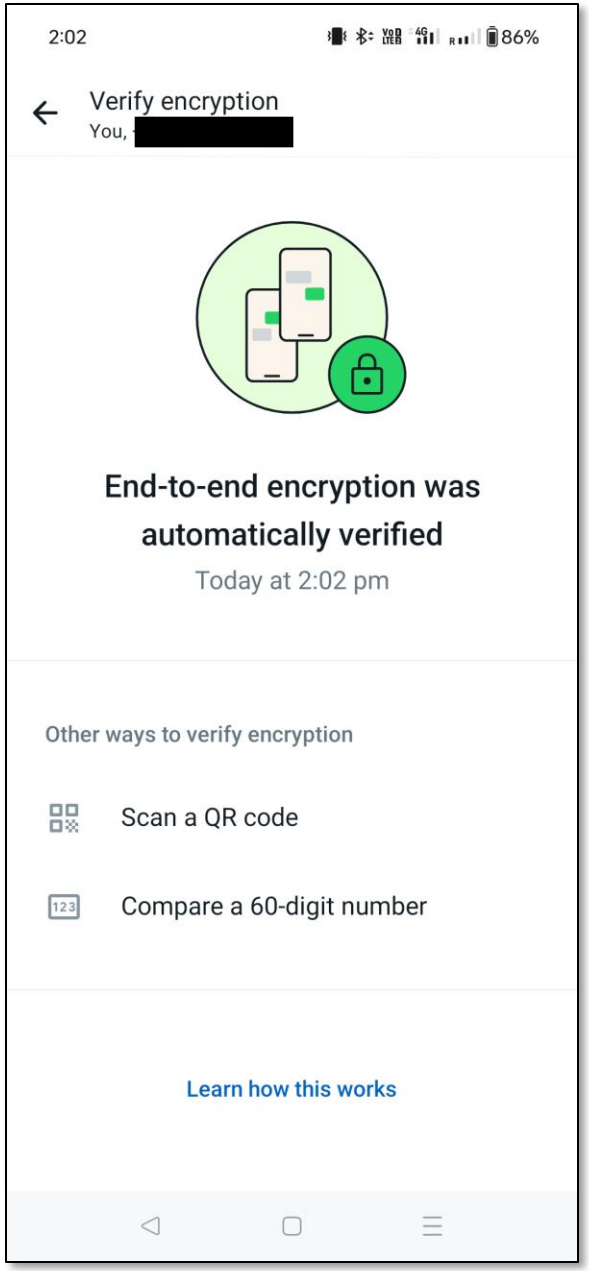
- End to end encrypted
- The “ends” are the apps on both sides





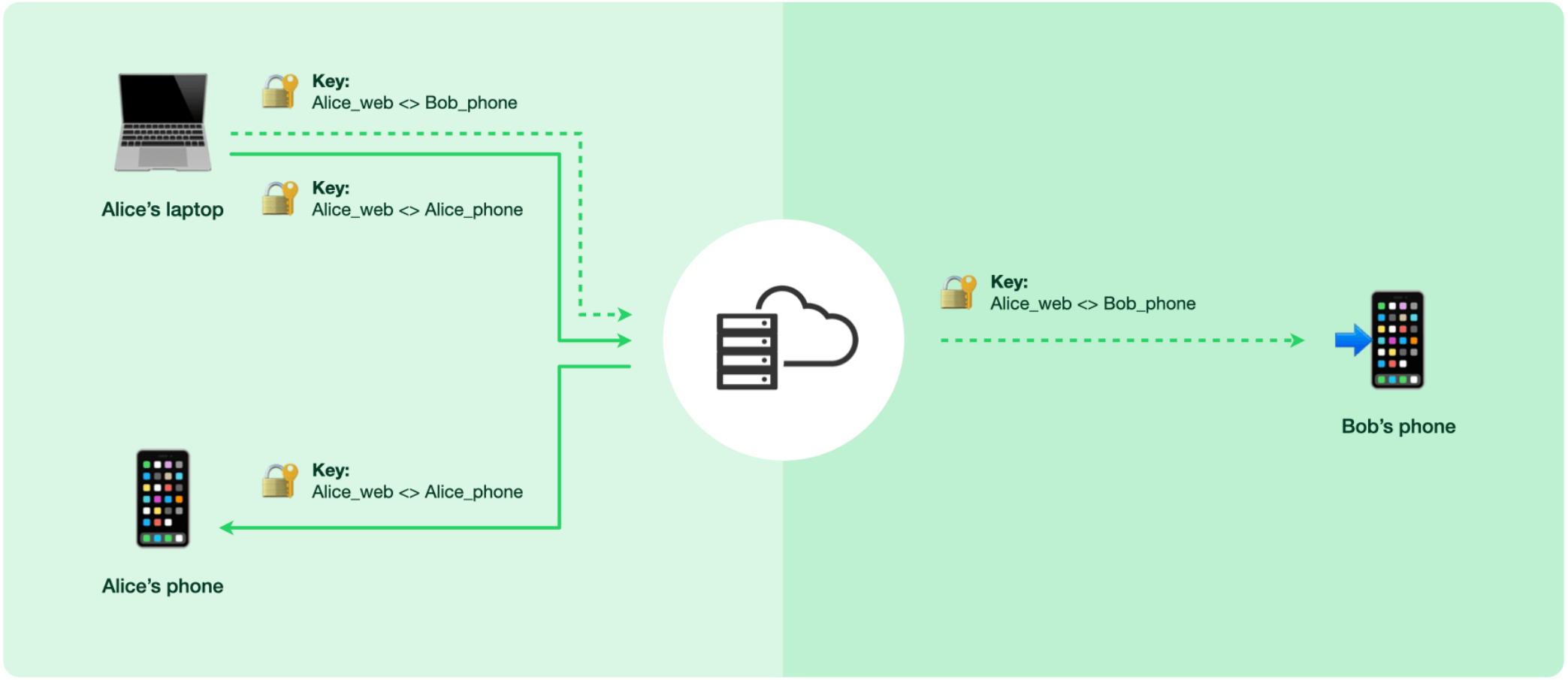
WhatsApp

- All messages, including group chats, are end-to-end encrypted
- The “ends” are the WhatsApp app on both devices
- Keys are managed by WhatsApp itself and shared with the devices as needed



WhatsApp: syncing chats

Life of a message



https://engineering.fb.com/2021/07/14/security/whatsapp-multi-device/

FIDO: PASSWORDLESS AUTHENTICATION

PassKeys

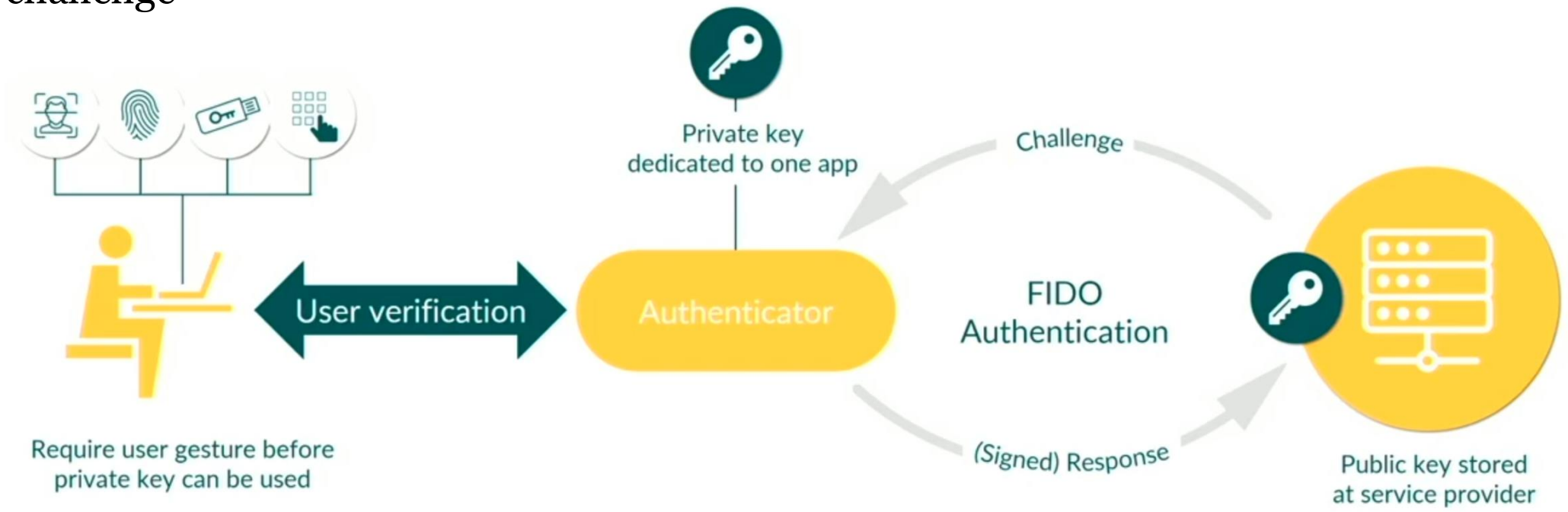
Idea:
Use public/private keys instead of passwords.

PassKeys: Registration

- A user is setting up a new account/relationship with a website
  - Device (phones, laptops, etc.) generates and stores a private/public key pair
  - Sends the public key to the website which stores it
  - Similar to a password, account authentication is now tied to the key not to the user identity

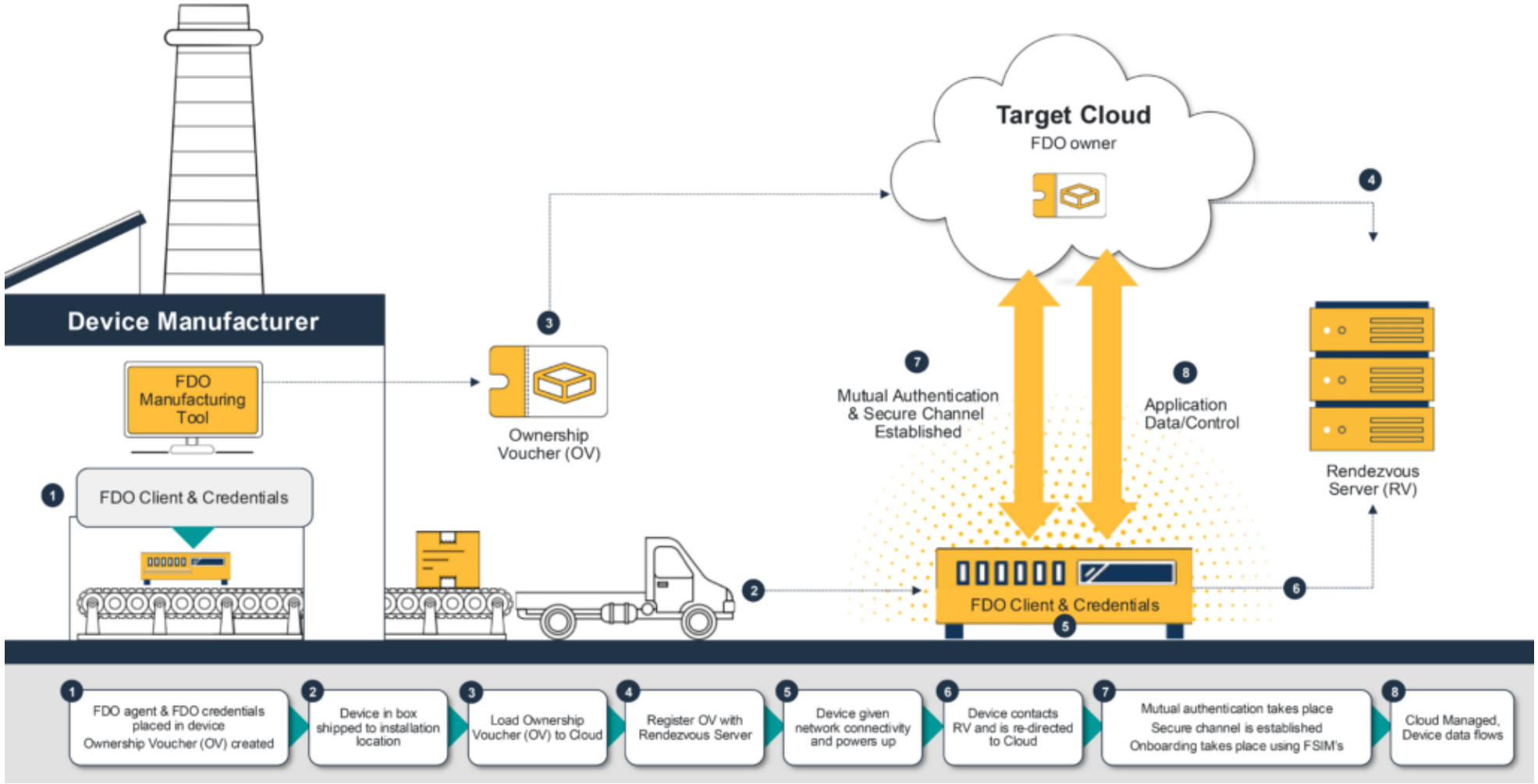
PassKeys: Authentication

- On login/authentication request
  - Server sends a challenge
  - Device verifies the user (e.g. fingerprint) and uses private key to sign the challenge
- Signature may also include facts about the device
- Website then uses their copy of the public key to verify the signature



David Turner, Authenticate Virtual Summit: Demystifying Passkey Implementations https://www.youtube.com/watch?v=Qiy_s-WpURc

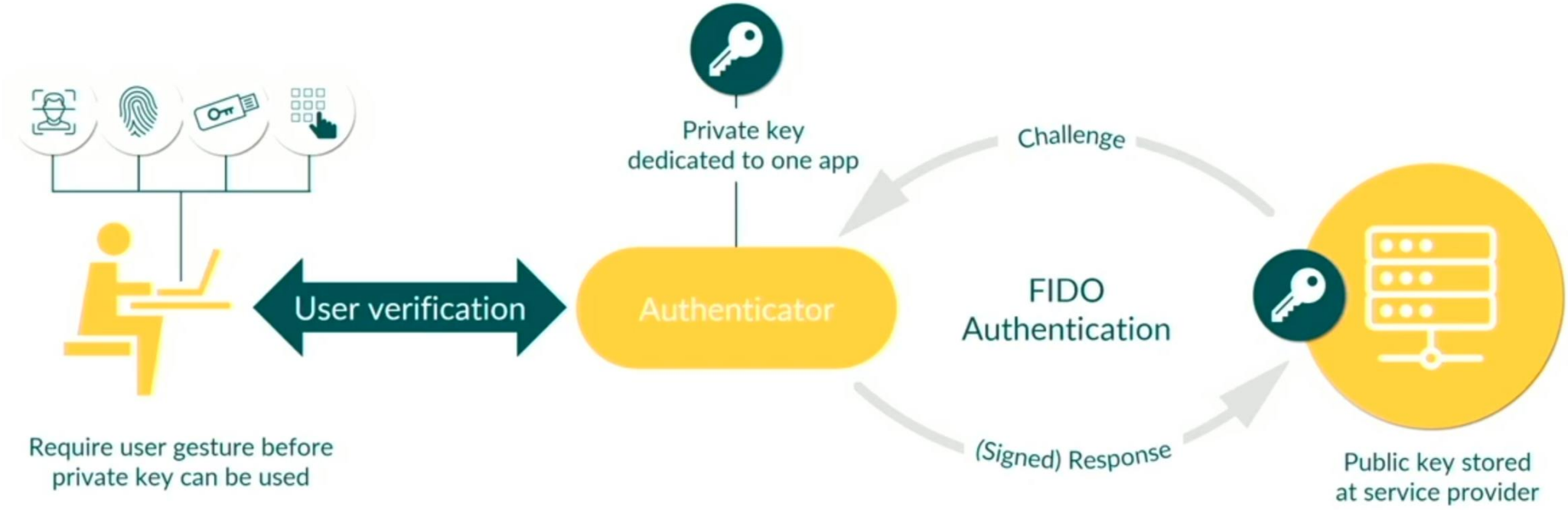
Hardware matters: device need to be trusted



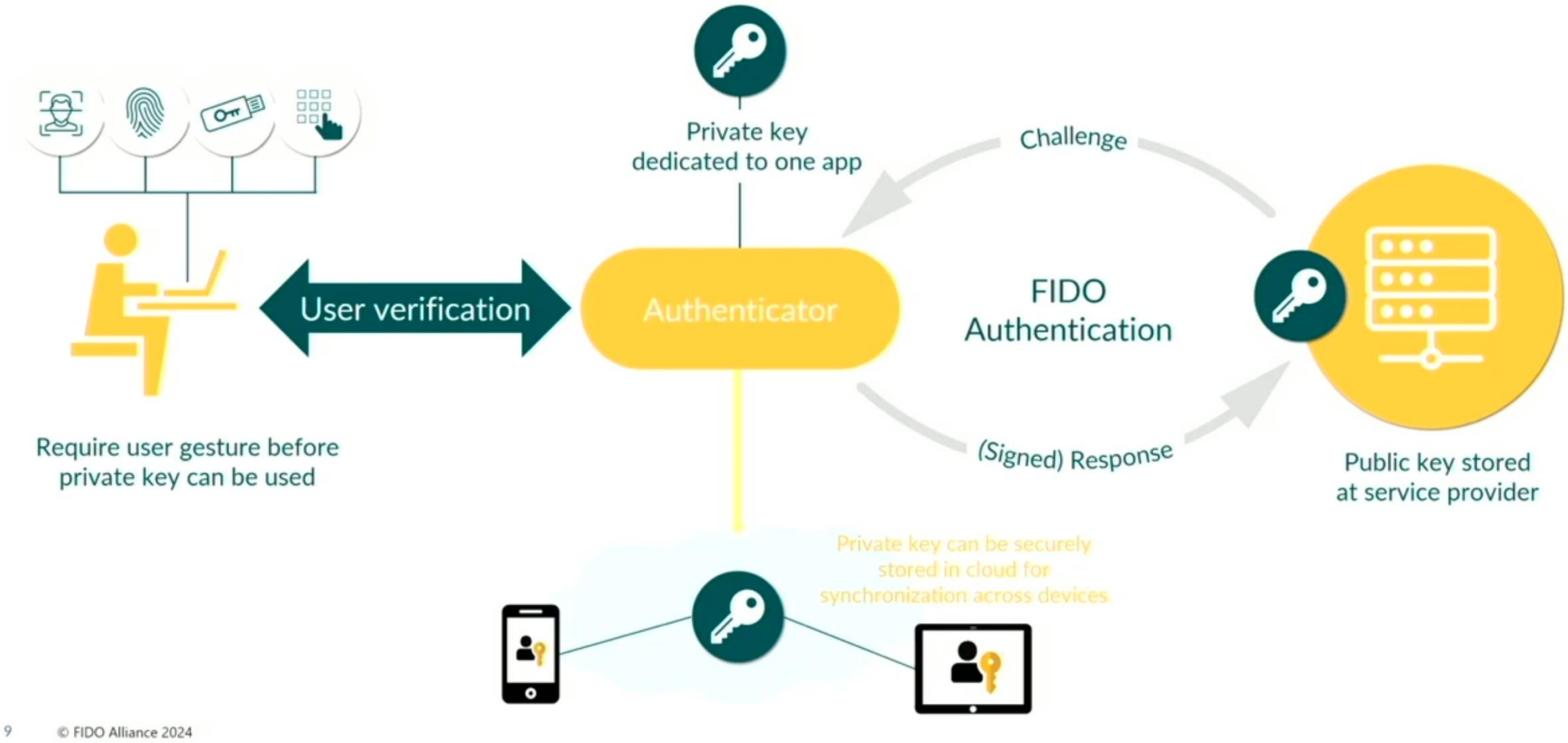
https://fidoalliance.org/device-onboarding-overview/

Think-pair-share

- What happens if the website gets hacked and they loose all the public keys?
- What type of capabilities/access would an attacker need to compromise this system?



What about multiple devices: key syncing



David Turner, Authenticate Virtual Summit: Demystifying Passkey Implementations https://www.youtube.com/watch?v=Qiy_s-WpURc

QUESTIONS