

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.

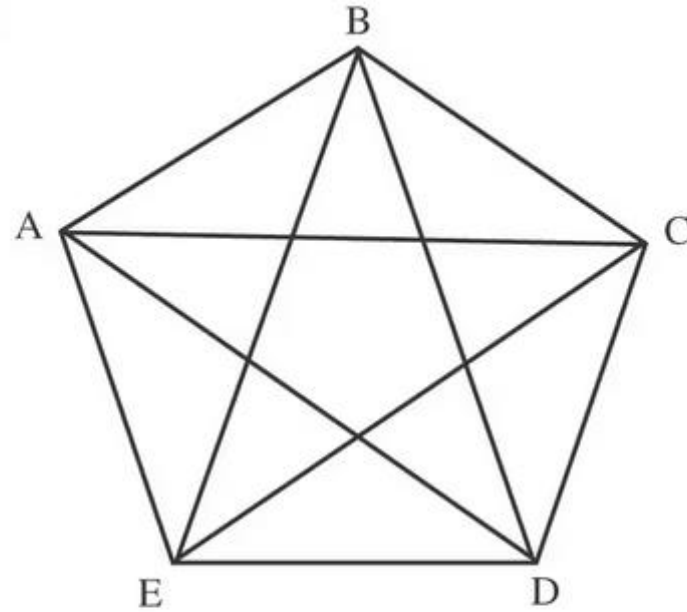
How do we solve the identity problem?

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

Approach scales poorly

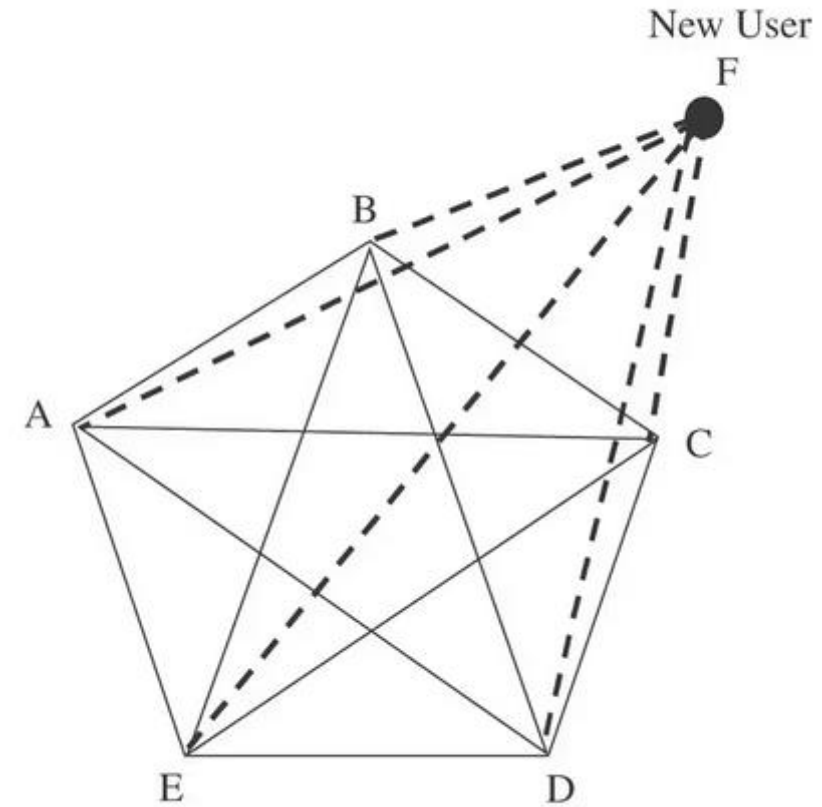
An n user system requires $n * (n-1)/2$ keys

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



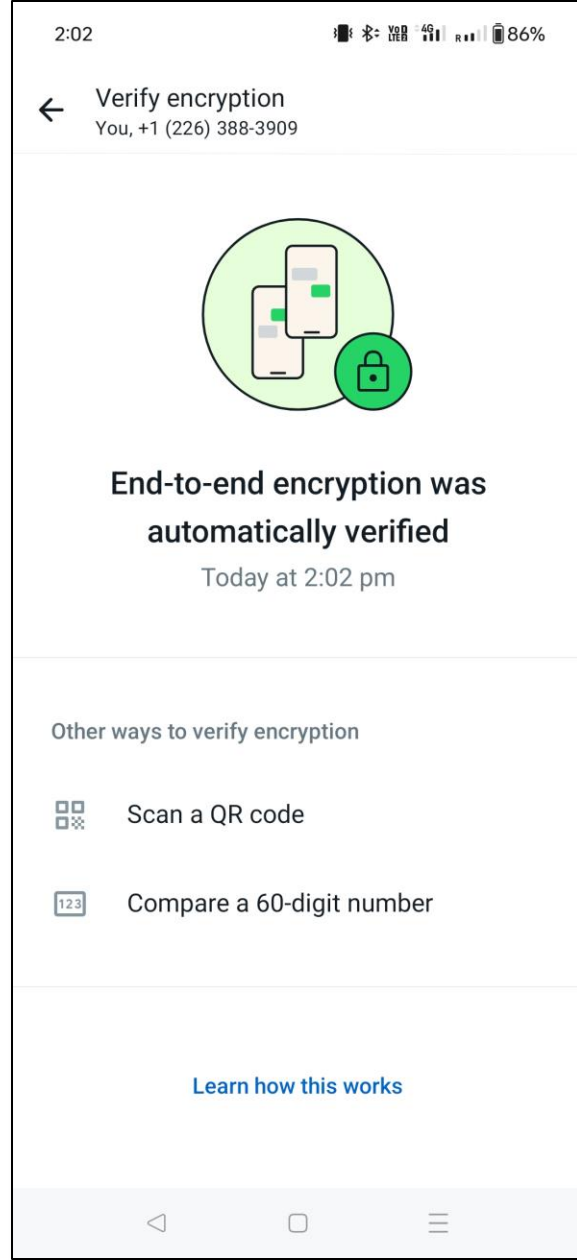
Existing Users

New Keys to Be Added - - - - -

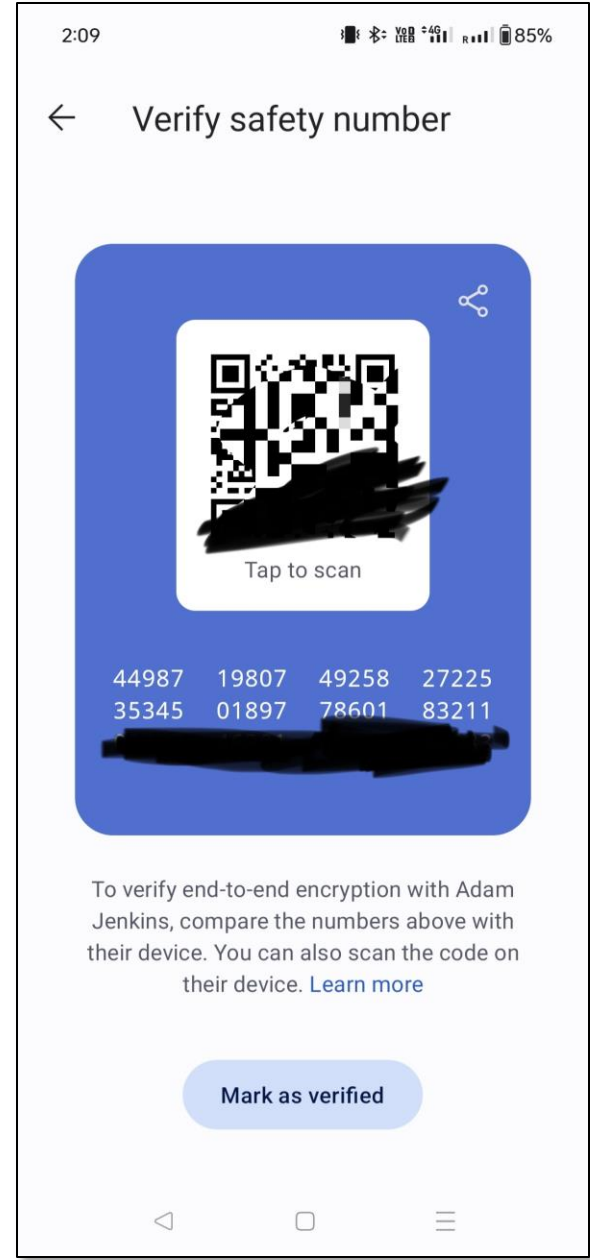


User comparing of keys is still used for verification today by common apps like WhatsApp and Signal.

WhatsApp



Signal



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

PSIRT PGP Key (0x33E9E596) x

Secure | https://blogs.adobe.com/psirt/?page_id=146

blogs.adobe.com Search Blogs

Adobe Product Security Incident Response Team (PSIRT) Blog

Working to help protect customers from vulnerabilities in Adobe software. Contact us at [PSIRT\(at\)adobe\(dot\)com](mailto:PSIRT(at)adobe(dot)com).

PSIRT PGP Key (0x33E9E596)

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: Mailvelope v1.8.0
Comment: https://www.mailvelope.com

xsFNBfM/2KMBEADbwToJM3BCVE1OeC22HgVEqNEDppXzuD2dgfKuy0M4tx2L
De7GkPjo6AOsw4yi8bakLiidpw5B0J/AR1VtIjIDeMs0F9MRZicV0UKyA5qV
c9BafZnAicY7nezkIJUmyLcIVMC60pqSHzo0Ewy2PZjxzcI4vDGhHmcgfV5X
R+duYld3LtVI+A/5jv326LB16bCNTs/tOhW2T0LraMPOctdH84Z4tPcyp335
s8/dZ2C+eOMD4iX1kIymZ1kqEfZNVcs1sRUXy27sL01VHCyMi6UNWCeeHOu2
2yJxMiBCniozBKZUwcR6ysg97nng633dN9mf7V30PS3zAjhe0Hvmzg3B/Nfo
qzy2dAEU/JDUBhiAo+xr9VF3ZPOoC8JySORgyUm/2t3TTBaH+DnfsUBiqo5U
2T0n8x2R1FWxyZYNCTku5JOvPqRBft13DSyJD7LDDps62nqhpavb34eprwuk
qIk0TMRu9mB4EQc+cNFR3ZpN1AKj+HOb/TUJwCJpVju2/3g0wgdqHh+OQ1vC
Nm8vIGnQZwQ30WqnH/UFoh3RPJ+WqnDq88NmQbq8I4aNV4u8MgoObd/zrtVX
kAwYHbIZLo925NjFyPuuxhWiCotKen18dZefB8aB81RjyUMnCJ0GQus+JG8
TJyEesNdK/q8HD5h1kCRSzMHD1+Ra3z/1+FFIwARAQABzR1BZG9iZSBQU01S
VCA8cHNpcnRAYWRvYmUuY29tPslBewQQAQgALwUCWb/YrWUJAEZgAYLCQgH
AwIJEIbAD8Kvh3YWBbUIAgoDFgIBAhkBAhsDAh4BAADk2A//f+6PFzg4VmLI
PzstZPoqPR/1X1Z7RIYbQosHvsFwyW0WWX1uIlsEeD5Qo7HQ6NNMAOW51Js
wFvFOWIa9U6SHRoU1kGTSESReOq5HnXe4DcBubsKmoMS68PuiZ88wYOIM4Up
9V9PUuaue0U4oSrYHnH5qBOqurtv8wO5Cq4uTwnfnjN7n4OH0++2910PJ68B
6+kMuQyG4swmxsZh1j1qGMHcs0c/BuI3W+n5w+xLM7N5jjCTjNXR+tGmstdm
RPEoLW0so+ZFwfNW0CLKjYUahp3p6H9x8R13wrp2re0GhqKRgt3D4UcAgsPs
```

CATEGORIES

- Alert
- Security Bulletins and Advisories
- Uncategorized

ARCHIVES

- September 2017
- August 2017
- July 2017
- June 2017
- May 2017
- April 2017
- March 2017
- February 2017
- January 2017
- December 2016
- November 2016
- October 2016
- September 2016
- August 2016
- July 2016
- June 2016
- May 2016
- April 2016
- March 2016
- February 2016
- January 2016
- December 2015

Photo credit: Juho Nurminen @jupenur

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

```
xsFNBFm/2KMBEADbwToJM3BCVE1OeC22HgVEqNEDppXzuD2dgfKuy0M4tx2L
De7GkPjo6AOsw4yi8bakLiidpw5B0J/AR1VtIjIDeMS0F9MRZicV0UKyA5qV
c9BafZnAicY7nezkJJUmYlCIVMC60pqSHzo0Ewy2PZjxzcI4vDGhHmcgfV5X
R+duYld3LtVI+A/5jv326LB16bcNts/tOhW2T0LraMPoCtdH84Z4tPcyp335
s8/dZ2C+eOMD4iX1kIymZ1kqEfZNVcs1sRUXy27sL01VHCYmi6UNWCeeHOu2
2yJxMiBCniozBKZUwcr6ysg97nnq633dN9mf7V30PS3zAjhE0Hvmzg3B/Nfo
qzy2dAEU/JDUBhiAo+xr9VF3ZPOoC8JySORgyUm/2t3TTBaH+DnfsUBiqo5U
2T0n8x2R1FWxyZYNCTku5JOvPqRBft13DSyJD7LDDps62nqhpaVb34eprwuk
qIk0TMRu9mB4EQc+cNFR3ZpN1AKj+HOb/TUJwCJpVju2/3g0wgdqHh+OQ1vC
Nm8vIGnQZwQ30WqnH/UFoh3RPJ+WqnDq88NmQBq8I4aNV4u8MgoObd/zrtVX
kAwYHbIZLo925NjFyPuuxhWiCotKen18dZefB8aB81RjYuImnCJ0GQus+JG8
TJyEesNdK/q8HD5h1kCRSzMHD1+Ra3z/1+FFIwARAQABzR1BZG9iZSBQU01S
VCA8cHNpcnRAYWRvYmUuY29tPslBewQQAQgALwUCWb/YrWUJAeEzqAYLCQgH
AwIJEIbAD8Kvh3YWBUIAgoDFgIBAhkBAhsDAH4BAADk2A//f+6PFzg4VmLI
PzsTZPoqPR/lXlZ7RIYbQosHvsFwyW0WwX1uIlsEeD5Qo7HQ6NNMAOW51Js
wFvFOWIa9U6SHRoU1kGTSESReOq5HnXe4DcBubsKmoMS68PuiZ88wYOIM4Up
9V9PUuaue0U4oSrYHnH5qB0qurtv8wO5Cq4uTwnfnjN7n4OH0++2910PJ68B
6+kMuQyG4swmxsZhlj1qGMHcs0c/BuI3W+n5w+xLM7N5jjCTjNXR+tGmstdm
RPEoLW0so+ZFwfNW0CLKjYUahp3p6H9x8R13wrp2re0GhqKRGt3D4UcAqsPs
```

Photo credit: Juho Nurminen @jupenur

PSIRT PGP Key (0x33E9E596)

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: Mailvelope v1.8.0
Comment: https://www.mailvelope.com

xsFNBFm/2KMBEADbwToJM3BCVE1OeC22HgVEqNEDppXzuD2dgfKuy0M4tx2L
De7GkPjo6AOsw4yi8bakLiidpw5B0J/AR1VtIjIDeMS0F9MRZicV0UKyA5qV
c9BafZnAicY7nezkJJUmYlCIVMC60pqSHzo0Ewy2PZjxzcI4vDGhHmcgfV5X
R+duYld3LtVI+A/5jv326LB16bcNts/tOhW2T0LraMPoCtdH84Z4tPcyp335
s8/dZ2C+eOMD4iX1kIymZ1kqEfZNVcs1sRUXy27sL01VHCYmi6UNWCeeHOu2
2yJxMiBCniozBKZUwcr6ysg97nnq633dN9mf7V30PS3zAjhE0Hvmzg3B/Nfo
qzy2dAEU/JDUBhiAo+xr9VF3ZPOoC8JySORgyUm/2t3TTBaH+DnfsUBiqo5U
2T0n8x2R1FWxyZYNCTku5JOvPqRBft13DSyJD7LDDps62nqhpaVb34eprwuk
qIk0TMRu9mB4EQc+cNFR3ZpN1AKj+HOb/TUJwCJpVju2/3g0wgdqHh+OQ1vC
Nm8vIGnQZwQ30WqnH/UFoh3RPJ+WqnDq88NmQBq8I4aNV4u8MgoObd/zrtVX
kAwYHbIZLo925NjFyPuuxhWiCotKen18dZefB8aB81RjYuImnCJ0GQus+JG8
TJyEesNdK/q8HD5h1kCRSzMHD1+Ra3z/1+FFIwARAQABzR1BZG9iZSBQU01S
VCA8cHNpcnRAYWRvYmUuY29tPslBewQQAQgALwUCWb/YrWUJAeEzqAYLCQgH
AwIJEIbAD8Kvh3YWBUIAgoDFgIBAhkBAhsDAH4BAADk2A//f+6PFzg4VmLI
PzsTZPoqPR/lXlZ7RIYbQosHvsFwyW0WwX1uIlsEeD5Qo7HQ6NNMAOW51Js
wFvFOWIa9U6SHRoU1kGTSESReOq5HnXe4DcBubsKmoMS68PuiZ88wYOIM4Up
9V9PUuaue0U4oSrYHnH5qB0qurtv8wO5Cq4uTwnfnjN7n4OH0++2910PJ68B
6+kMuQyG4swmxsZhlj1qGMHcs0c/BuI3W+n5w+xLM7N5jjCTjNXR+tGmstdm
RPEoLW0so+ZFwfNW0CLKjYUahp3p6H9x8R13wrp2re0GhqKRGt3D4UcAqsPs

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

The screenshot shows a web browser window with the address bar displaying "Secure | https://blogs.adobe.com/psirt/?page_id=146". The main content area contains a PGP key block. The public key section is visible, ending with "-----END PGP PUBLIC KEY BLOCK-----". Below it, the private key section begins with "-----BEGIN PGP PRIVATE KEY BLOCK-----". A purple arrow points from the right side of the image towards the private key section, with the text "Do not do this" written inside the arrow. The browser's address bar and the page's URL are visible at the top. The right side of the browser shows a navigation menu with a list of months and years from April 2014 down to December 2010.

```
GAEIABkFAlm/2LAFQCQHhM4AJEibAD8Kvh3YWAHsMAACz+g/+KmbnChEUZXdo
ZIVpZp3KvZQHWCY+5qGqdoxNkfkUSKkzC0M51Kq7emVpVXYrMRdJRHxFP
83HIahA5UiufsDt7QlMwVRgtJYxhH+TNZBBbDBVQ1JQxuC3mH7F/tFhb9N1G
kURUwa2fdDBPw2+DOWa2+iVhcPhfB2iy9exs2txXjgPx67aZi70Jw44ixvpY
TWs/M5I6SXQsyuB5Qw0jtXKioQyTOLmeUFmJR2Ui5FK+t5SXus44mRCuJEUn
YDqDmxKDNhssEvnwz4Kws2uvNXNwlnZcHVSyXukf3F1CwP0TESCOecdqbl0
Cs+vLivixsh33xqZwNd78xv92t2Ggp2a41gBOaaCjx2irqZ9RHiv0YzNfQz
yz5XYEGI2iCrvdStrbZfX1Dqslrqs/pZRbV48KfbuDvGZuNR3hrsfmfsgR
zkESOQmpuKhj/Es3CKjdafLDc8HOyVhJ+n4tvWXYRyEhuDh/tzeDuuB9vfG
QA9TNhSpAp5lHFJklmd9knWbExJ0srUbK2QVmvn9CZx/sdUfwdWp1GeANLsO
MRNlr3Irk1bZ0bFH+nrcJQZ5+sDzHGNe4P9Dt30yvFHoyS1BkrndLuawSlqh
LJyYLUvFjL3i3jbiNT1NKldwqaL2i9OuRAuHthoFGOKIqr6hmtOYzUem/cl+
ZlRwd77Vmfc=
=QOc7
-----END PGP PUBLIC KEY BLOCK-----

-----BEGIN PGP PRIVATE KEY BLOCK-----
Version: Mailvelope v1.8.0
Comment: https://www.mailvelope.com

xcaGBFm/2KMBEADbwToJM3BCVE1OeC22HgVEqNEDppXzuD2dgfKuy0M4tx2L
De7GkPjo6Aosw4yi8bakLiidpw5B0J/AR1VtIjIDeMS0F9MRZicV0UKyA5qV
c9BafZnAicY7nezkiJUmyLcIVMC60pqSHzo0Ewy2PZjxzcI4vDGHmcgfV5X
R+duYld3LtVI+A/5jv326LB16bcNts/tOhW2T0LraMPoCtdH84Z4tPcyp335
s8/dZ2C+EoMD4ix1kiymZ1kqEfZNVcs1sRUXy27sL01VhcYmi6UNWCeeHOu2
2yJxMiBCniozBKZUwcr6ysg97nnq633dN9mf7V30PS3zAjhe0Hvmzg3B/Nfo
qzy2dAEU/JDUBhiAo+xr9VF3ZPOoC8JySORgyUm/2t3TTBaH+DnfsUBiqo5U
2T0n8x2R1FWxyZYNCTku5JOvPqRBft13DSyJD7LDDps62nqhpavb34eprwuk
qIk0TMRu9mB4EQc+cNFR3ZpN1AKj+HOb/TUJwCJpVju2/3g0wgdqHh+OQ1vC
Nm8vIGnQZwQ30WqnH/UFoh3RPJ+WqnDq88NmQBq8I4aNV4u8MqoObd/zrtVX
kAwYHbIZLo925NjFyPuuxhWiCotKenl8dZefB8aB81RjYuIMnCJ0GQus+JG8
TJyEesNdK/q8HD5h1kCRSzMHD1+Ra3z/1+FFIwARAQAB/gkDCA7HXpjNu7yW
YBVIglTandp2qwxLZTA0Jm3YMOwvBoje4ZDL41VZBh2sBphQ15CLulx7MUrD
```

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


My public key

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

```
mQENBFHMcgABCAC9WrYDO6K2L3VHy14eHN6suHLqMpJ+SO+IUTuLEVNuzIoXAUXH
KozHejV/9XoG8j933ZtszXKCog3aMESeoEoz6fNGfolvaCe5B4jwqoJt8NHwb5L
B2dnqoCplgXcN2GJxFeHHUaf27COsObCjXpMESHU4ZHKke+g6DatmiEtBpVp41Ot
1zxdmQkgb2H2xw28RYfYkdDoueteIkOrFLrCy9ZF9KdMhA1eBH94KnwI QshdiZR
QYEX25+M8cKCb++Rc9H6an7EG9WHOFrW4oUSy52OfveOyfQPzkkRto7u12339hvHo
B/h+7xLM6FQbOUZQ9BD5w7IQHgytXJVsUjodABEBAAgOIkthbWkgVmFuaVWvHIDxr
dmFuaWVhQGluZi5jZC5hYy51az6JAT8EEwELACKfAlYKYvECCGyMFCQlMAYAHcWkI
BwMCAQYVCAIJCgsEFgIDAQIEAQIXgAAKCRCTdsxl9/HZffG+ CACShuKxje3QAqew
GWh8K4gCdiYoxDqJwq3PHxmyhZmQeN/1a1KcOrIj12b+Q75/5t+EgXOHpRoP IxfG
LZ6zOEpf6A18iFXX3JgQZdwPD0jtBiWNpOyMeBGTgIvEYg3so2VueQoeXcq3dbYp
5vstVxtD+TKHQ5CioIT75P2bzYq/XLT5aIbNqHQPcTooDgbRH+FvqsRXr7yeaef
JaPnxXo+1L33t2QY9zctiGyebwrvHMriPBj2VYCDzQk7JuQ5eFh4ZhsMgOmzLQD4
YiGr5weIMFwAvxZOaRxEagVf48jiWvrXuJ8YfHWSohESeNOCYC2P8q2olwwE26T
lpdtrwCqtB1LYW1pIFZhbmllySA8a2FtaUB2YW5pZWEuY29tPokBQgQTAQIALAIB
IwUJCWYBgaAcLCQgHAWIBBhULAgkKCwQWAgMBAh4BAheABQJWCmMeAhkBAaOJEJN2
zGX38dl9JJAIAIWorxIYsrmKS6CbW8MgTxxTDOXA Ct1b7FoWoQZHskIUQhEcE+a
XBYibiA5uHaatLfyjeXaD3qMEoZnQHoYMGEoGku00wWsbhfoQzHPgwzRLkDii75M
BibaWwoKWoVB9e4AkMakXJcNf5BXe06AHL2v15V205DikVnlCRXocKtu8b7LnmK
eLn7oLobr1deIuyKoNzbSnO/vpKDjPo/EY5yUeV9oIypZy/6wFQBehg1sXye6znO
9wb9uUsu9+/P8pz4JILMDSevjfT7zSRSl/YP3fOfZ6N4bc+K0dWPM7u5Iyoeuqzh
pzibv3ge7VhH2xIWz8vYZ/2xT1345tWRRMOJAhwEEwECAAyFALTnSpEACgkQjyxM
p99tBt2B8A/+OpIzOsQbQJB8yxti4I7PpD1weJdf3a81Vhm7JyXE/Xy66ypfdt3w
XmFRUulrwezYiNebWNCrQHzQvRv/VJwjbTUx+Q3HsjIkKlHbE7iCiQXxtTRkoEny
2nuDcJGI2vo3C3B2JCucEw6esF1x79PI/IPv2+6tgUBKmDfOpsB2vbtqrHnmAYKL
4lQBfH1YSJgnzwo2JkhhocHdF9oZem1eMeiDeeVkh63893N8Swk5fBKdJt+SKZ/L
rQElBBlpMR9BmeY6bPvWRuyevKonIMR8oG9iFABxjTpWBL8aGk6EeVK5EqYDgVkd
ZlarK84r+KU1KD5IfgOCN7nhwgy7VI me68caZHSRiPWZP1fVVMhydiRjv8WsoUs6
InFVU3nxH+ZythPbYot86leGSchBT5k/fBQvbjhrRTbTfWvzSifb9efWylDi994
nzP6cN0rir3GIpsT8gPGBB2/NjxaWiM6y3X1az1vRnsunQHuyKkFWPZwnEvDJYaC
NN/3jWcbhLFwKBDSaHps2+1meFpooJFvNetz2bjT9a9pD4Q6KhOm05DnhLcaV97
bFBpsUuBGaYzTSSo5x1RdXHQpEbgap8dtuHhVvJw9YDQBjroK4aKyG9qqMD8cta
Pl/FAdyAqwH8Nw9efqAK+RQxSVUae9BYEnbIRpsDK6MkP3YMFmu5ki5AQoEUcxy
AAEIALyXYy8G2ZaTdJpdGcRhmIqOOSUlzPV7/5E5BbYKBNu4KU3nX+JLvcF5jxPQ
42c7i/WRVxE1BJTiarKGSvEvCig94TTXSIUKAt3T1oGBtXmGvqbGBq8ljSGl1UTwdJ
5yu5oJyRSf2fQRND6P/2eHNXejDUtdvhUXIUt8h9MuUO/ipDoDnwIvMnAATJHA+R
Zqw6oNpyjRGzvr3i uWUwe4PtyJDI3ELAFkbp/NAc5TIuVHRHNOwNpldJhM5zHuB
QQb3G/EsCn2PQZ5w5SDzavF2SpvQfDqxYpDaTLAXiF+wsJL5iaUjxwRgJPodbCZf
2Tozd7h9MXtGJDlPKJ8eLG8ogcMAEQEAAYkBJQYQAIA DWuCUcxyAAIBDAUJCWYB
gAAKCRCTdsxl9/HZfs+hB/9BJqSmIgcOHFXnb1PVIKxekzL8+WVm5Pk/EgMQSLZ2
HX4p3ial5PEPcYgUw9YnaG4ioodwJGw5/daTWrrTzcnKd8YqoP+DUOt96HZDSu3m
mCzE9NVAQYboFbVmGOx0eo627UBSvFqaXvAxBDYkoR8BoTnKhrQFwXkZVb3ohKwD
TgAFjOGIziE6uAdST231tFaqobizYfe5AVXRqro2oxBqNbaJNqs3SWoD83iSyvdv
lloBx83/Rogg7hUk16F2vzXicWmUwFSXRggCSbLosHsP6isBWwvIHeRmna/aQab
YKG3gbV9iyzAS31gbogVLAZqNSWhp8vVIEE28Fyf/Ed
=x5FK
```

-----END PGP PUBLIC KEY BLOCK-----

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 

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 Hierarchy

▾ QuoVadis Root CA 2

▾ QuoVadis EV SSL ICA G1

www.ease.ed.ac.uk

Certificate Fields

Issuer

▾ Validity

Not Before

Not After

Subject

▾ Subject Public Key Info

Subject Public Key Algorithm

Subject's Public Key

Field Value

Modulus (2048 bits):

```
9d 6b 8a 90 ff 2a c7 ad 11 f0 5f 95 ff 34 f5 c1
fa 9b d6 38 9c d6 90 49 8f b5 2c 9c 8b 51 ec 74
9b 69 17 ed b7 25 8c c0 8c ac 90 28 55 97 00 0b
d2 e4 88 c5 4b 03 ae 3d 73 d6 92 ac 25 06 99 39
b1 13 c8 2a 56 9d 6d 89 47 b0 eb 8b e8 c8 17 25
fd 60 1c b6 f5 62 fb 5f 82 33 cb a5 5d 0f 24 92
25 04 c2 16 4a 35 66 a6 66 b3 c5 75 ff 5e cb 94
31 c6 e6 a5 aa f4 3a 40 72 42 e4 93 43 b2 a6 0e
```

Export...

Certificate Authorities are used by browsers to verify identity

Online Banking, CDs, Mo x +

Ally Financial Inc. (US) https://www.a Search

Ally Financial Inc.
Secure Connection

You are securely connected to this site, owned by:

Ally Financial Inc.
Detroit
Michigan, US

Verified by: Entrust, Inc.

More Information

Whether it's banking, credit card, home loans or auto finance, nothing stops us from doing right by you.

View Ally Bank Auto Online Banking on the Why Choose Ally

You can see lots of details about any encrypted connection.

Page Info — https://uwaterloo.ca/

General Media Permissions **Security**

Website Identity

Website: uwaterloo.ca

Owner: This website does not supply ownership information.

Verified by: Certainly

[View Certificate](#)

Privacy & History

| | | |
|---|--------------------------------------|---|
| Have I visited this website prior to today? | Yes, 10,451 times | |
| Is this website storing information on my computer? | Yes, cookies and 1.7 MB of site data | Clear Cookies and Site Data |
| Have I saved any passwords for this website? | Yes | View Saved Passwords |

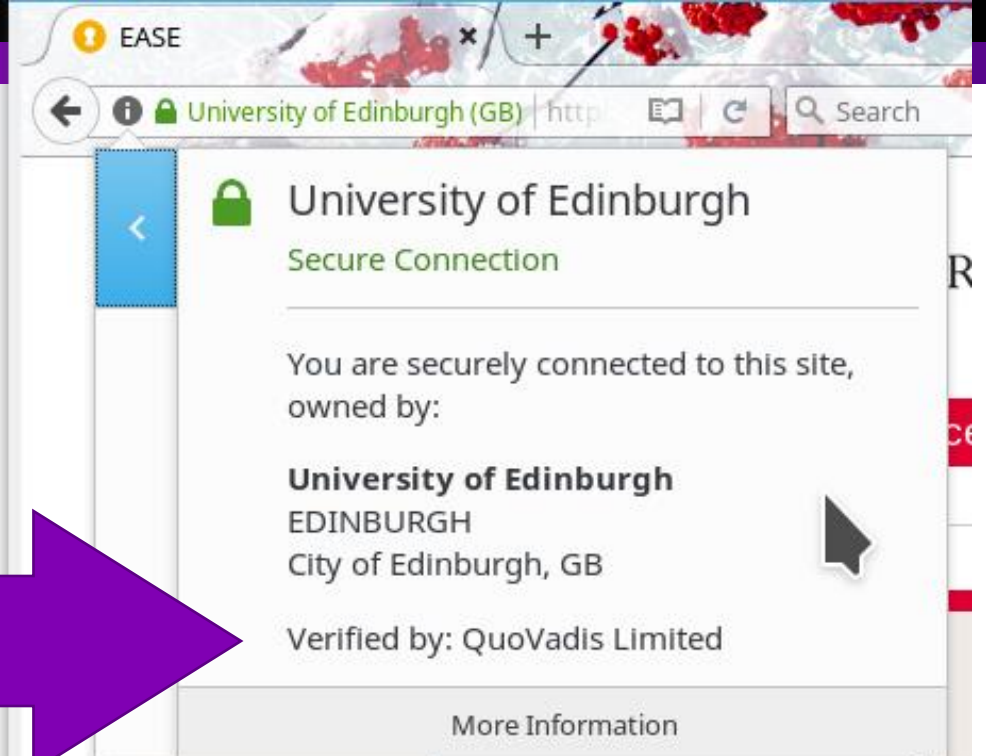
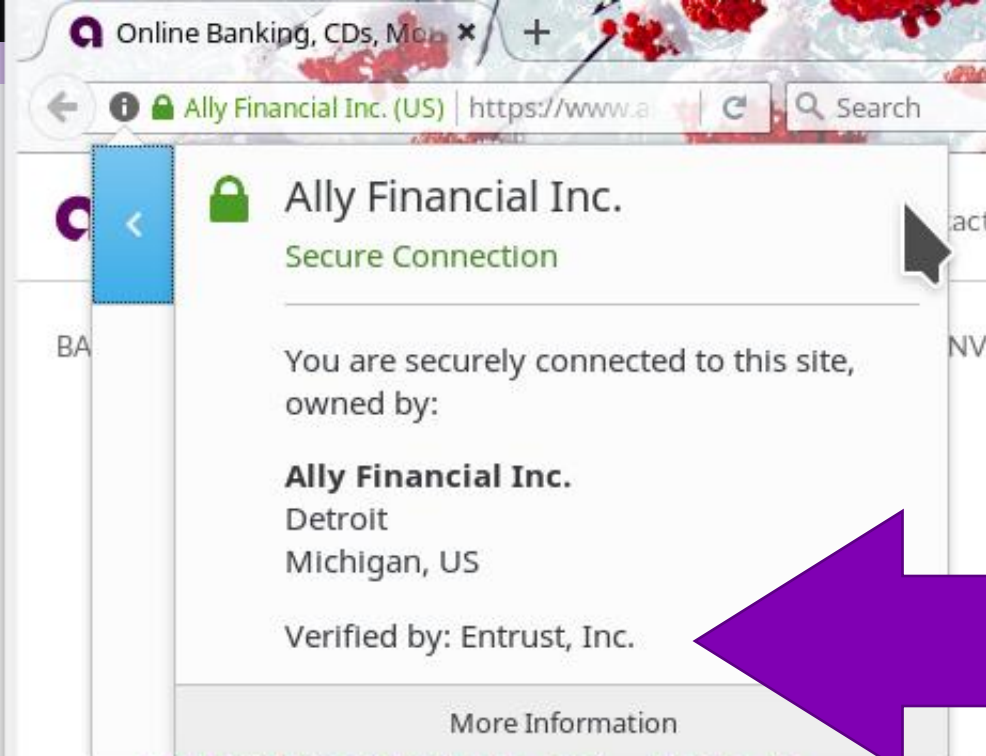
Technical Details

Connection Encrypted (TLS_AES_128_GCM_SHA256, 128 bit keys, TLS 1.3)

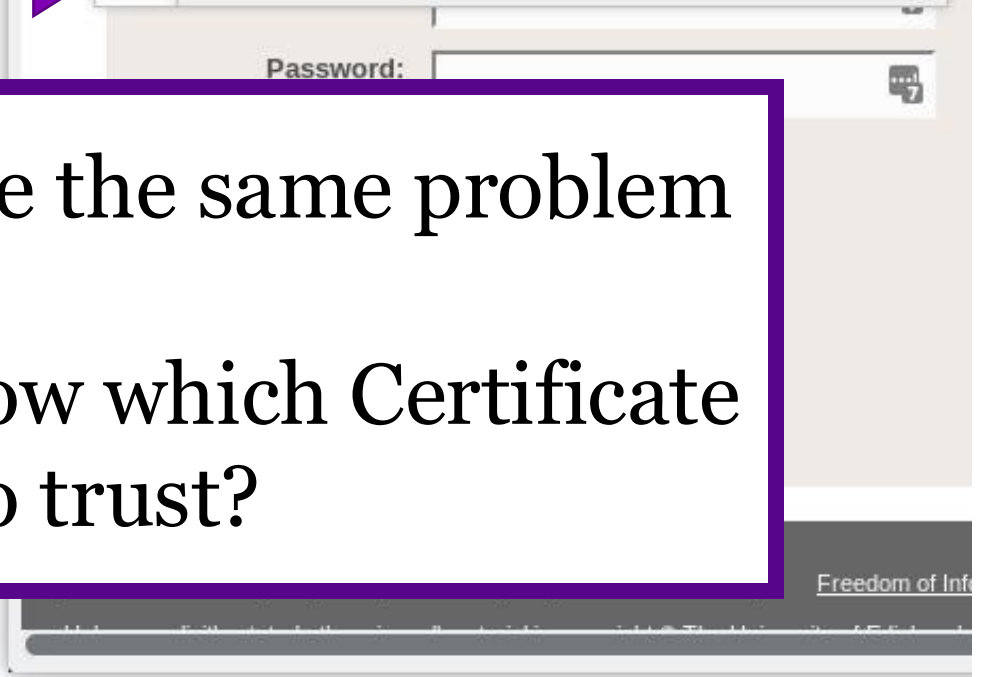
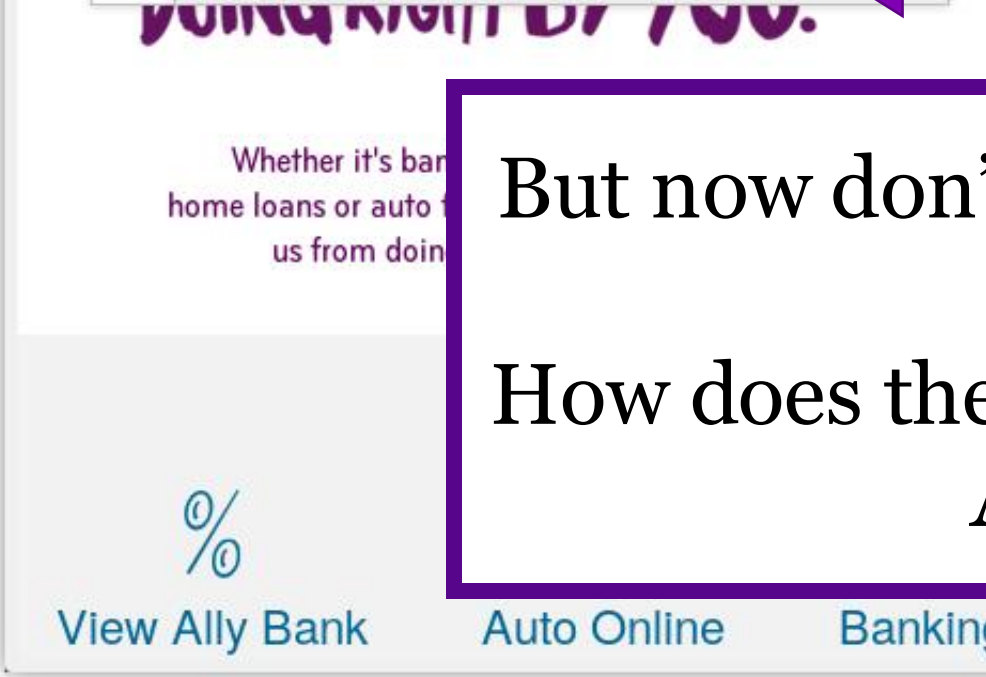
The page you are viewing was encrypted before being transmitted over the Internet. Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

This website complies with the Certificate Transparency policy.

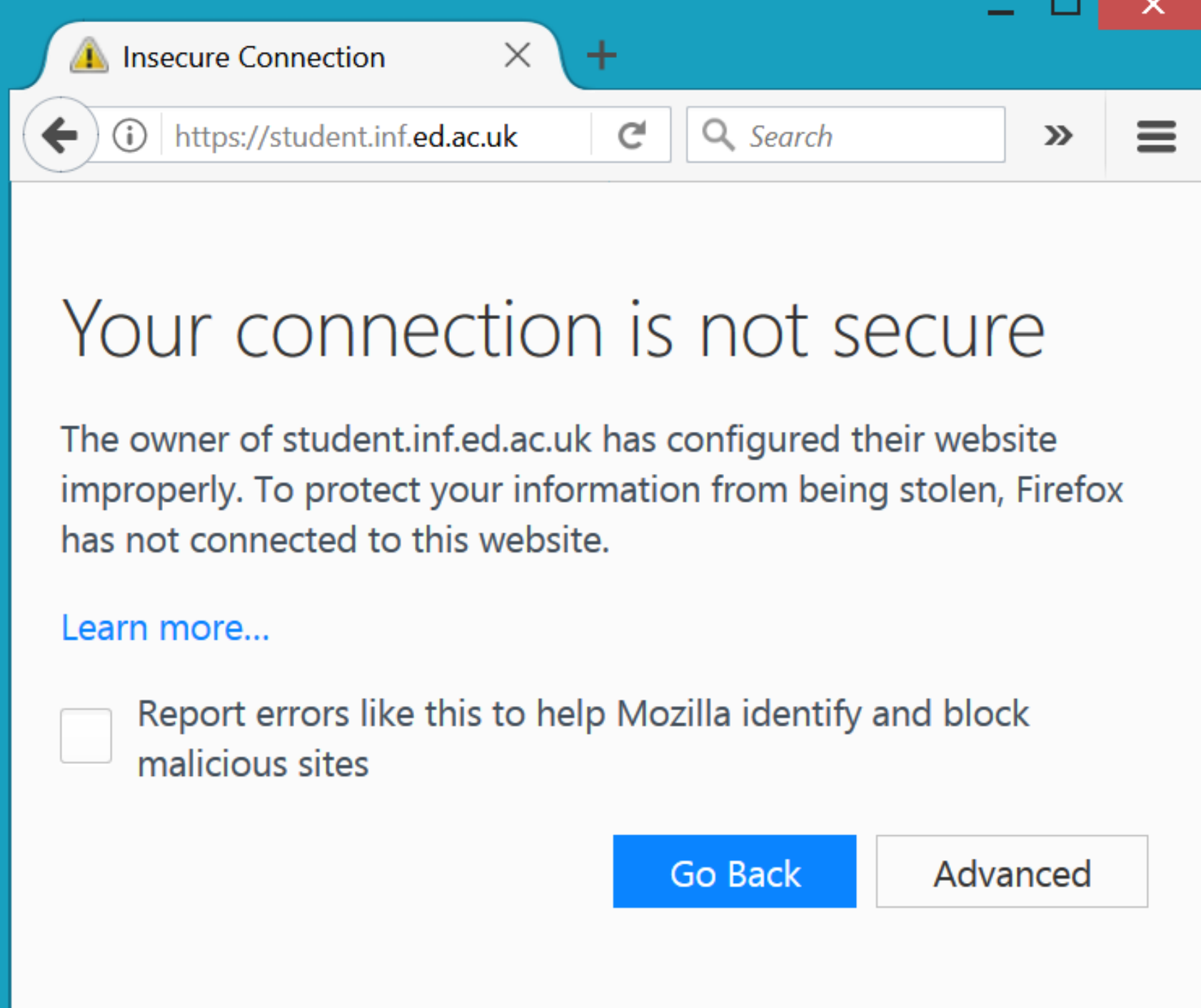
[Help](#)



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.**



The image shows a Firefox browser window with a teal title bar. The address bar displays a warning icon, an information icon, the URL 'https://student.inf.ed.ac.uk', a refresh icon, a search box with the text 'Search', and a menu icon. The main content area has a white background with the heading 'Your connection is not secure'. Below this, a paragraph explains that the website owner has configured it improperly and that Firefox has not connected. A blue link 'Learn more...' is provided. At the bottom, there is a checkbox for reporting errors and two buttons: 'Go Back' (highlighted in blue) and 'Advanced'.

Insecure Connection

https://student.inf.ed.ac.uk

Your connection is not secure

The owner of student.inf.ed.ac.uk has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

[Learn more...](#)

Report errors like this to help Mozilla identify and block malicious sites

[Go Back](#) [Advanced](#)

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

Page Info - https://student.inf.ed.ac.uk/

General Media **Security**

Web Site Identity

Web site: student.inf.ed.ac.uk

Owner: **This web site does not supply ownership information.**

Verified by: **Not specified**

Privacy & History

Have I visited this web site before today? **No**

Is this web site storing information (cookies) on my computer? **No** [View Cookies](#)

Have I saved any passwords for this web site? **No** [View Saved Passwords](#)

Technical Details

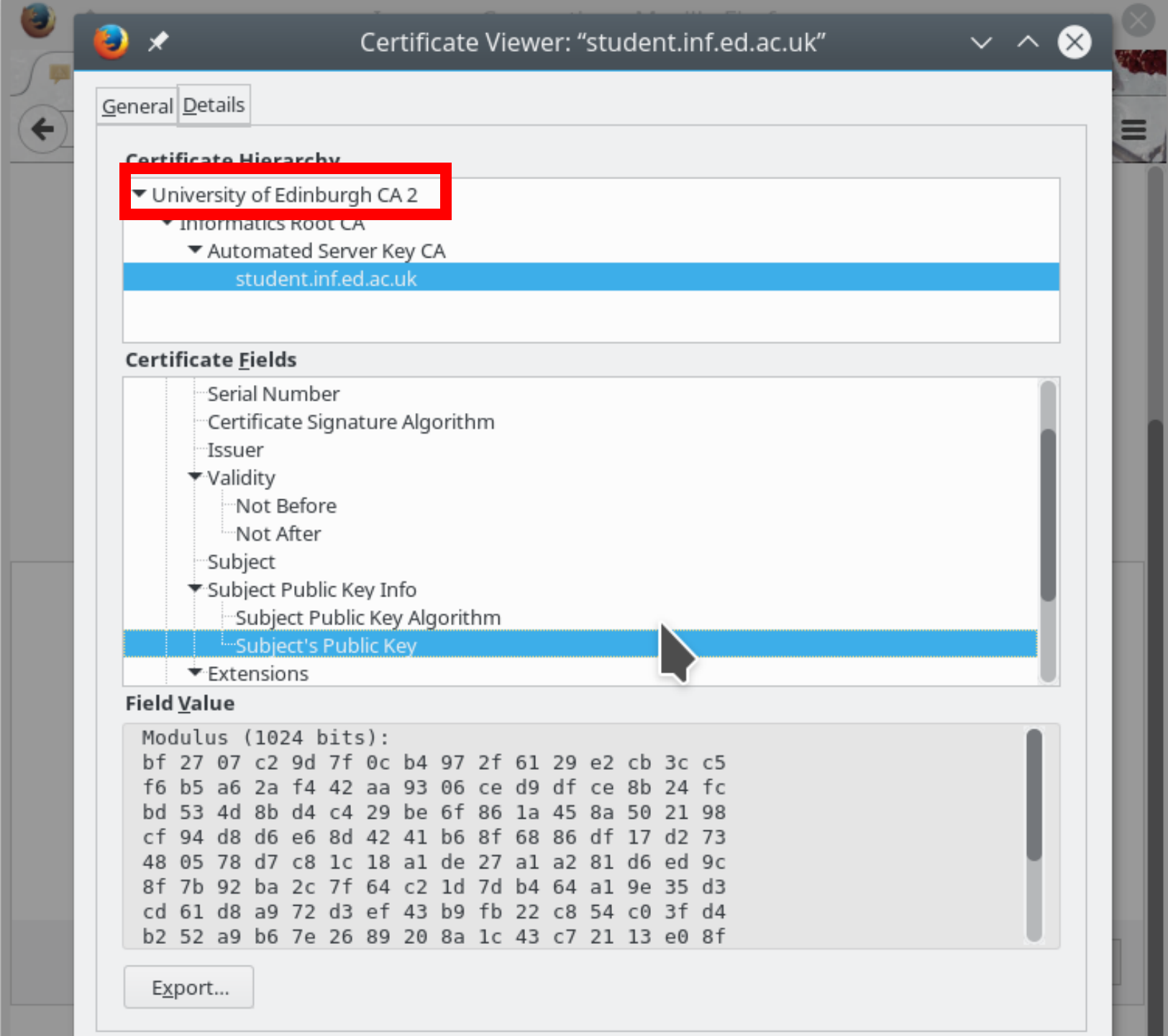
Connection Not Encrypted

The web site student.inf.ed.ac.uk does not support encryption for the page you are viewing. Information sent over the Internet without encryption can be seen by other people while it is in transit.

[Help](#)

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

About |

Informed news analysis every weekday

Google to Symantec: We don't trust you anymore

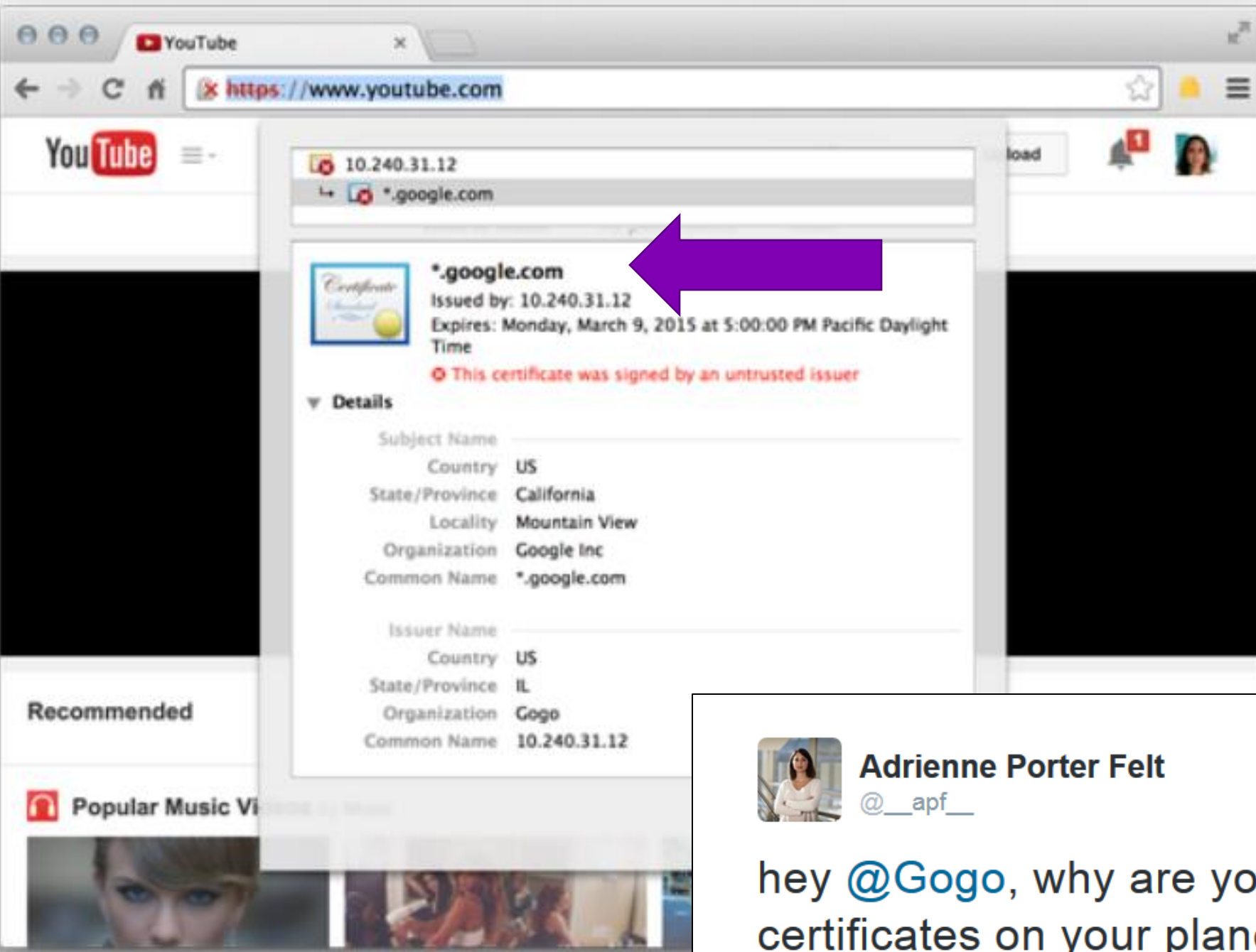
Admins need to consider whether they still want to use Symantec after its repeated mistakes with issuing TLS certificates



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



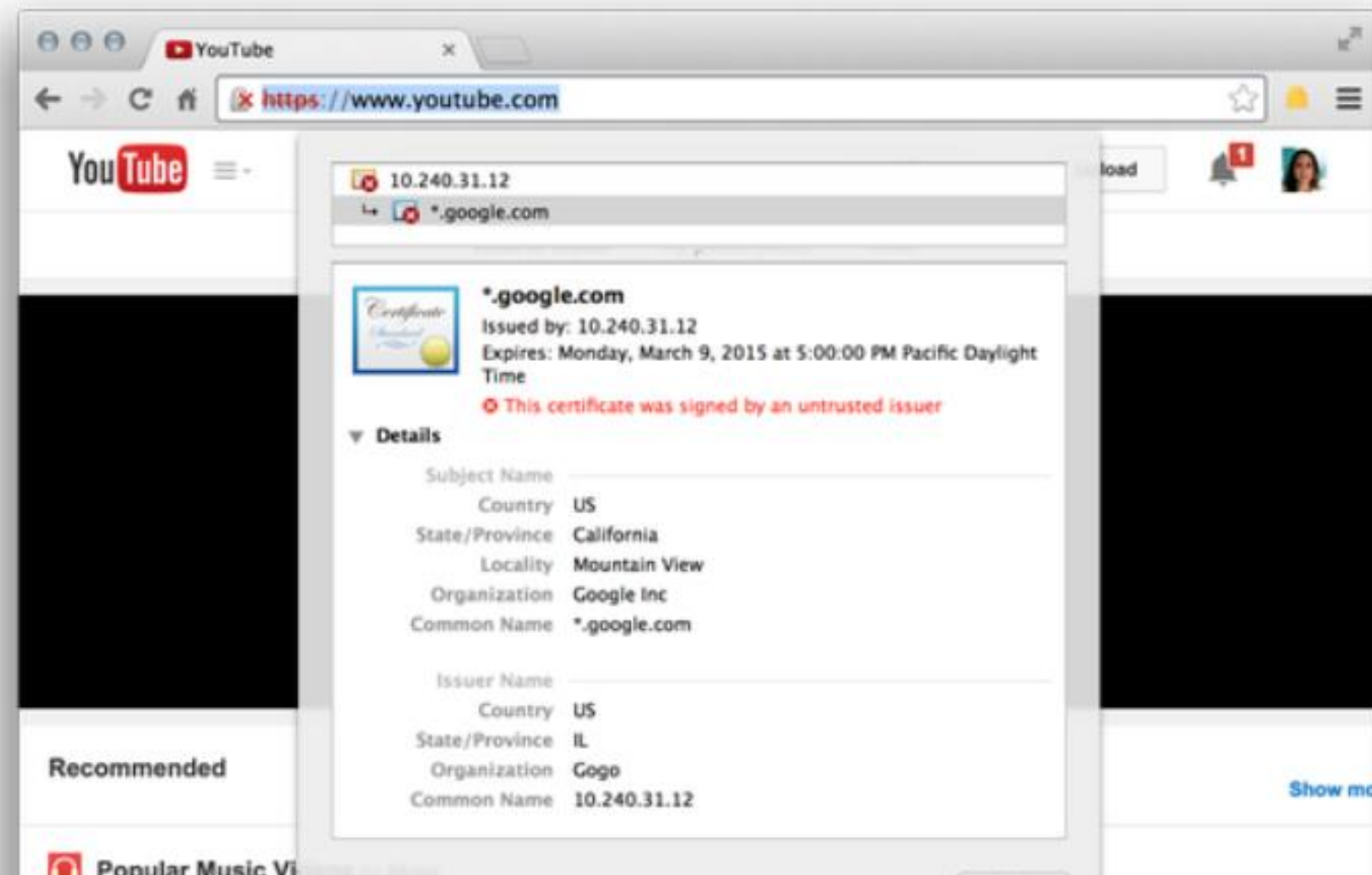
Adrienne Porter Felt
@__apf__



Following

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

Think-pair-share

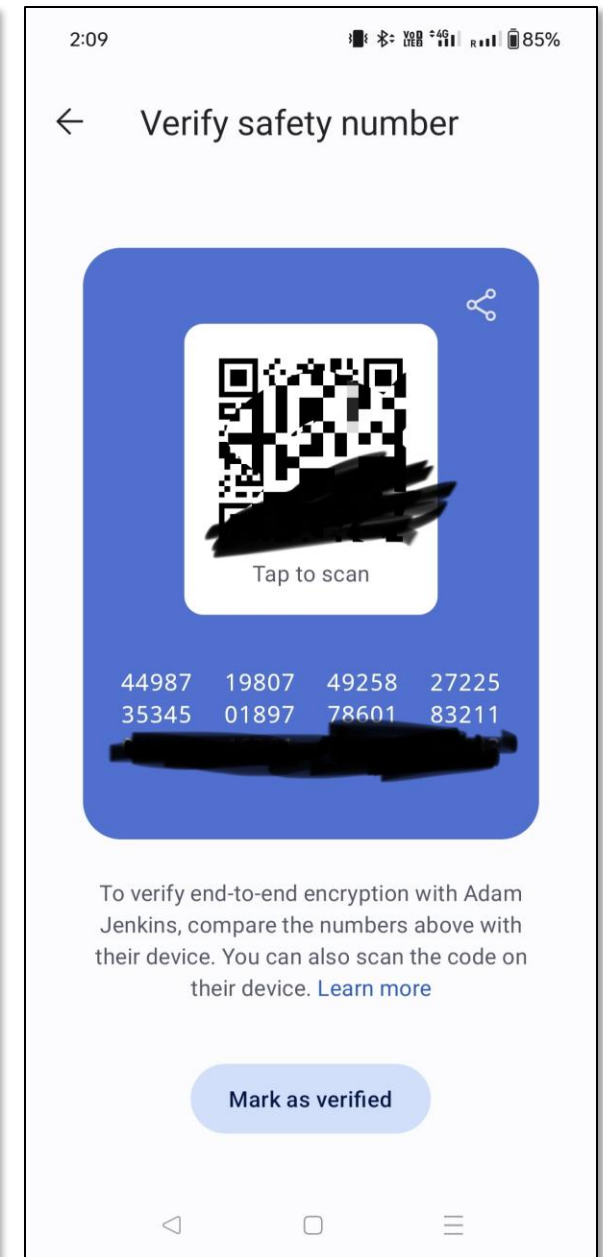
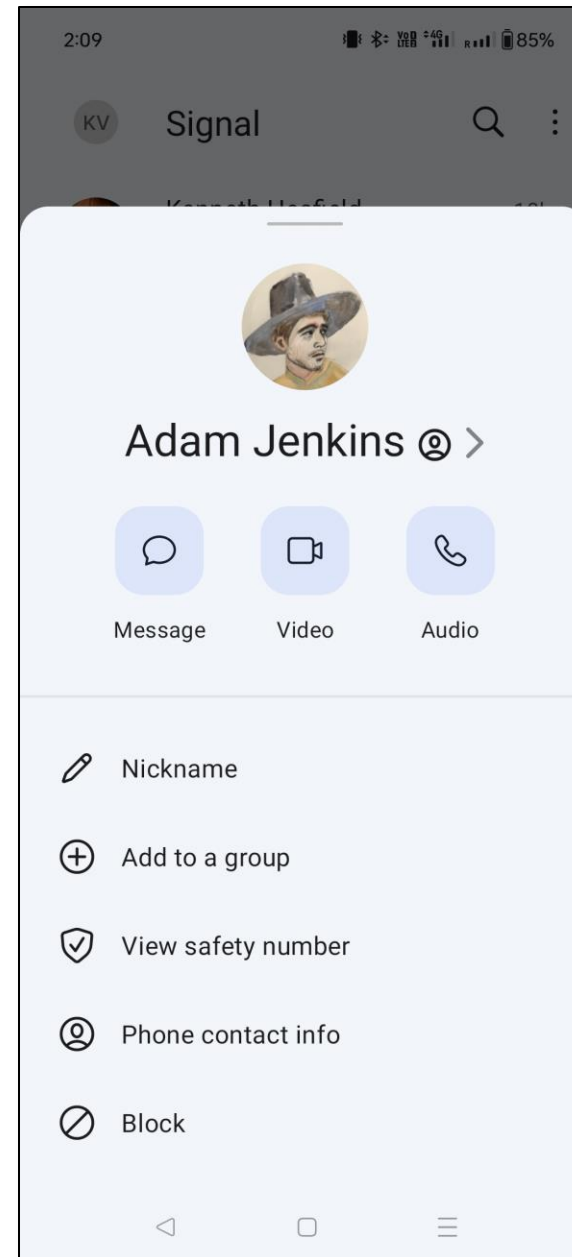


- A Firefox user would (theoretically) have seen no error in this case.
- How was Gogo able to successfully load a Google page with no errors on some browsers?

END-TO-END MESSAGING

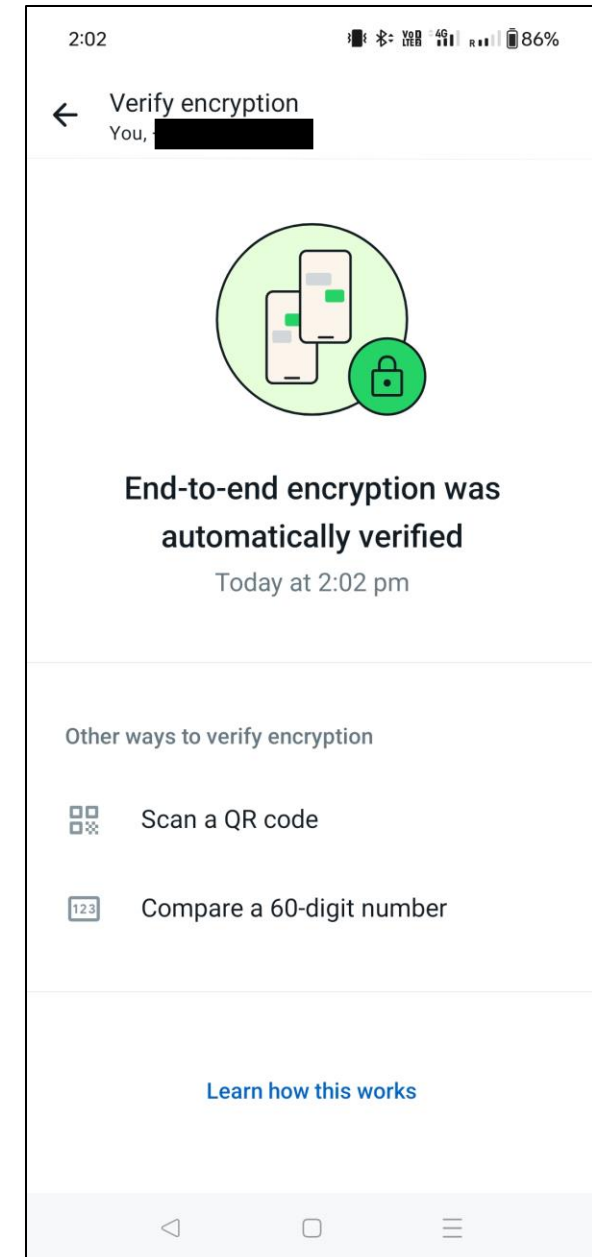
Signal

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



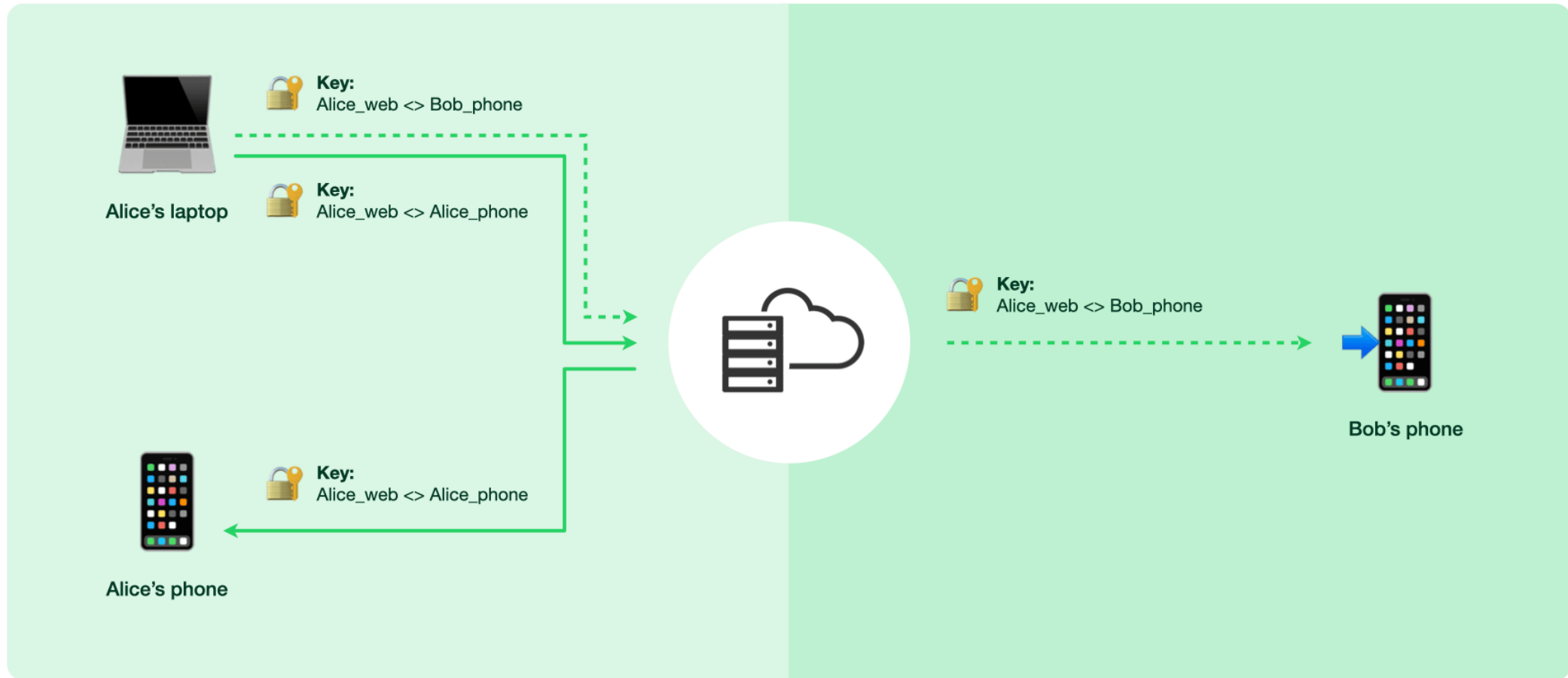
WhatsApp

- 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



→ - - - → End-to-end encrypted channels

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

FIDO: PASSWORDLESS AUTHENTICATION

PassKeys

Idea:
Use public/private keys instead of passwords.

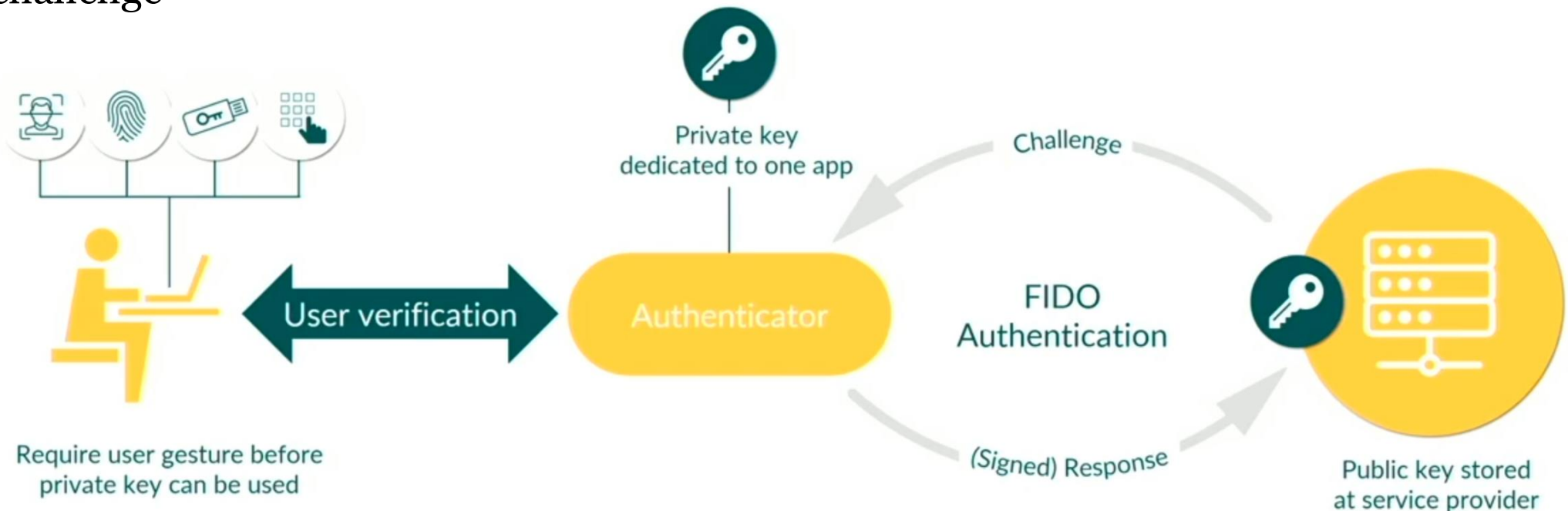
PassKeys: Registration

- 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

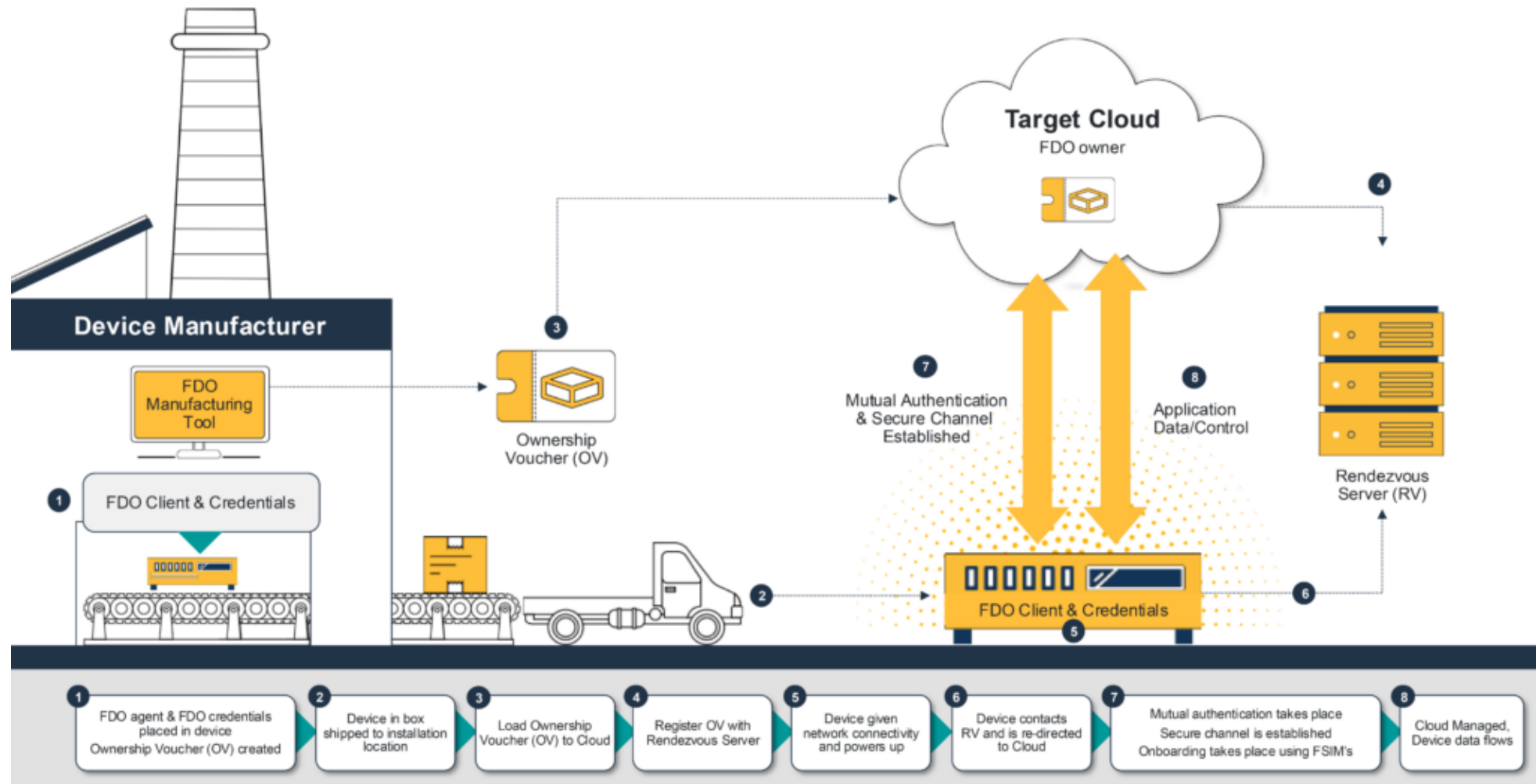
PassKeys: Authentication

- 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

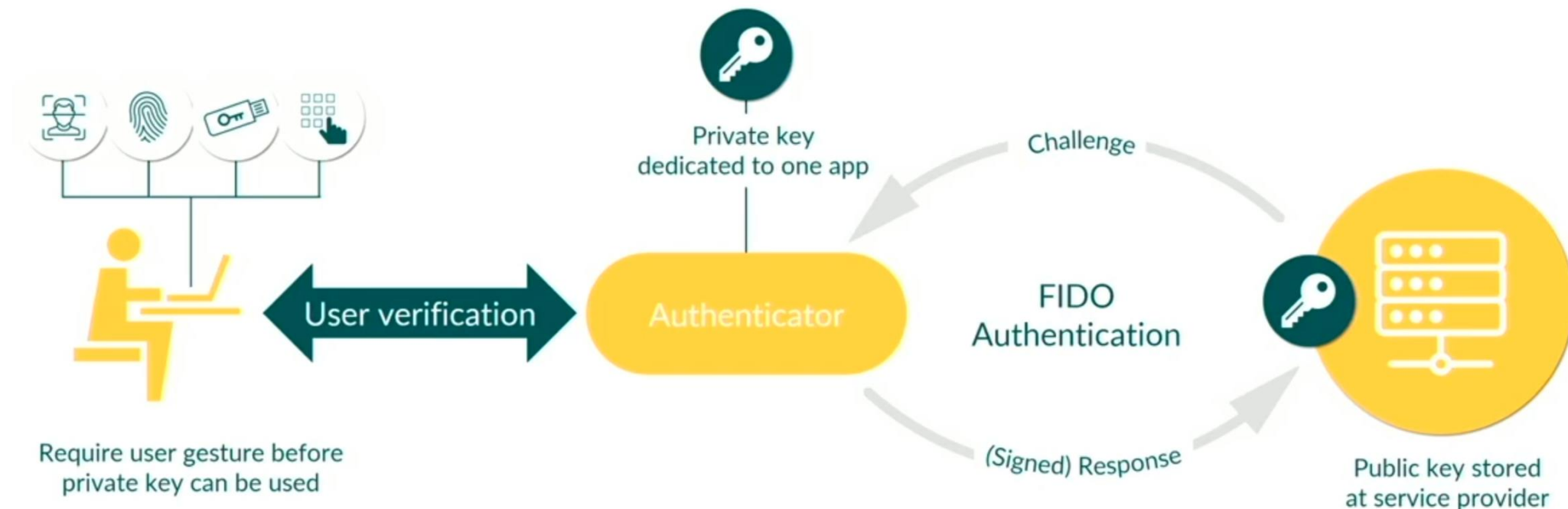


Hardware matters: device need to be trusted

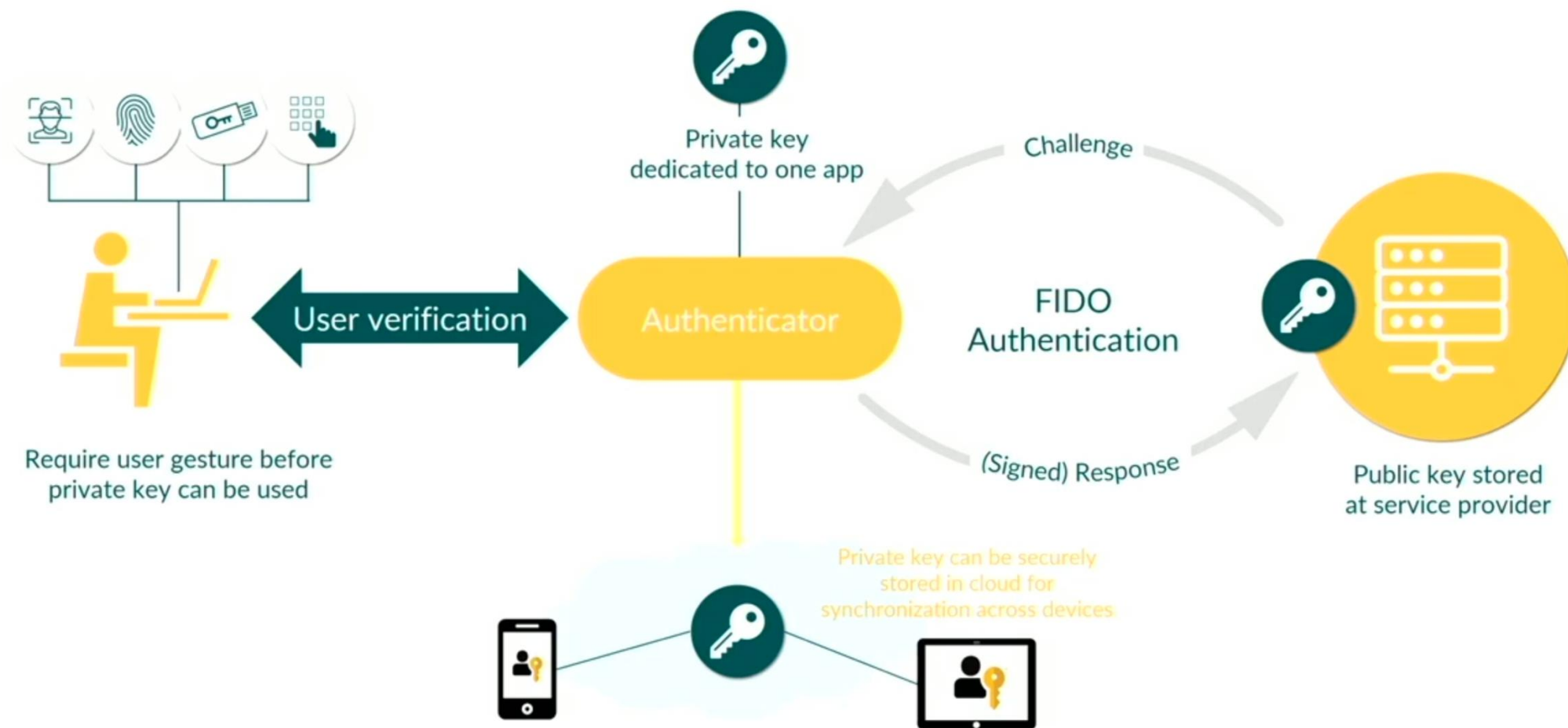


Think-pair-share

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



What about multiple devices: key syncing



QUESTIONS