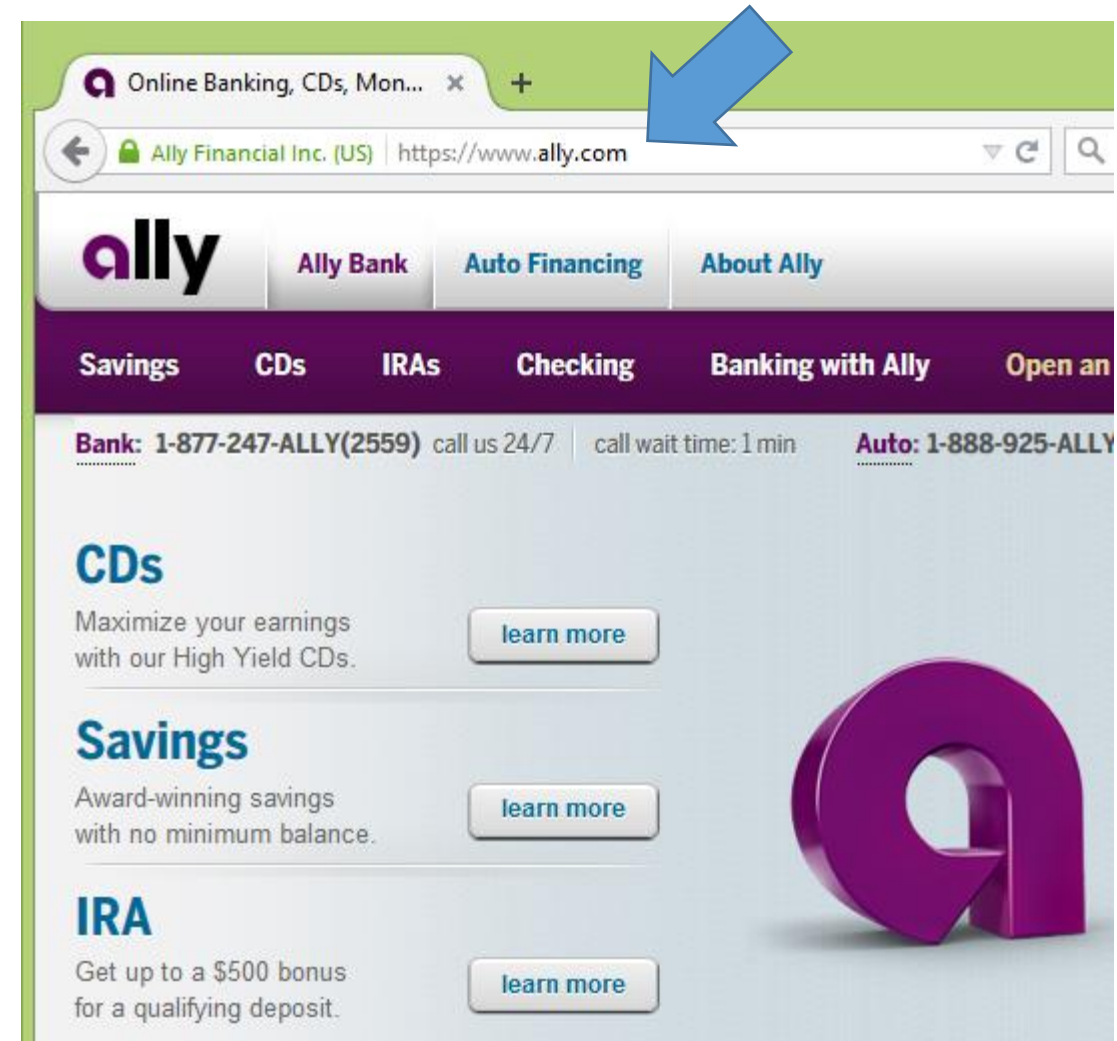
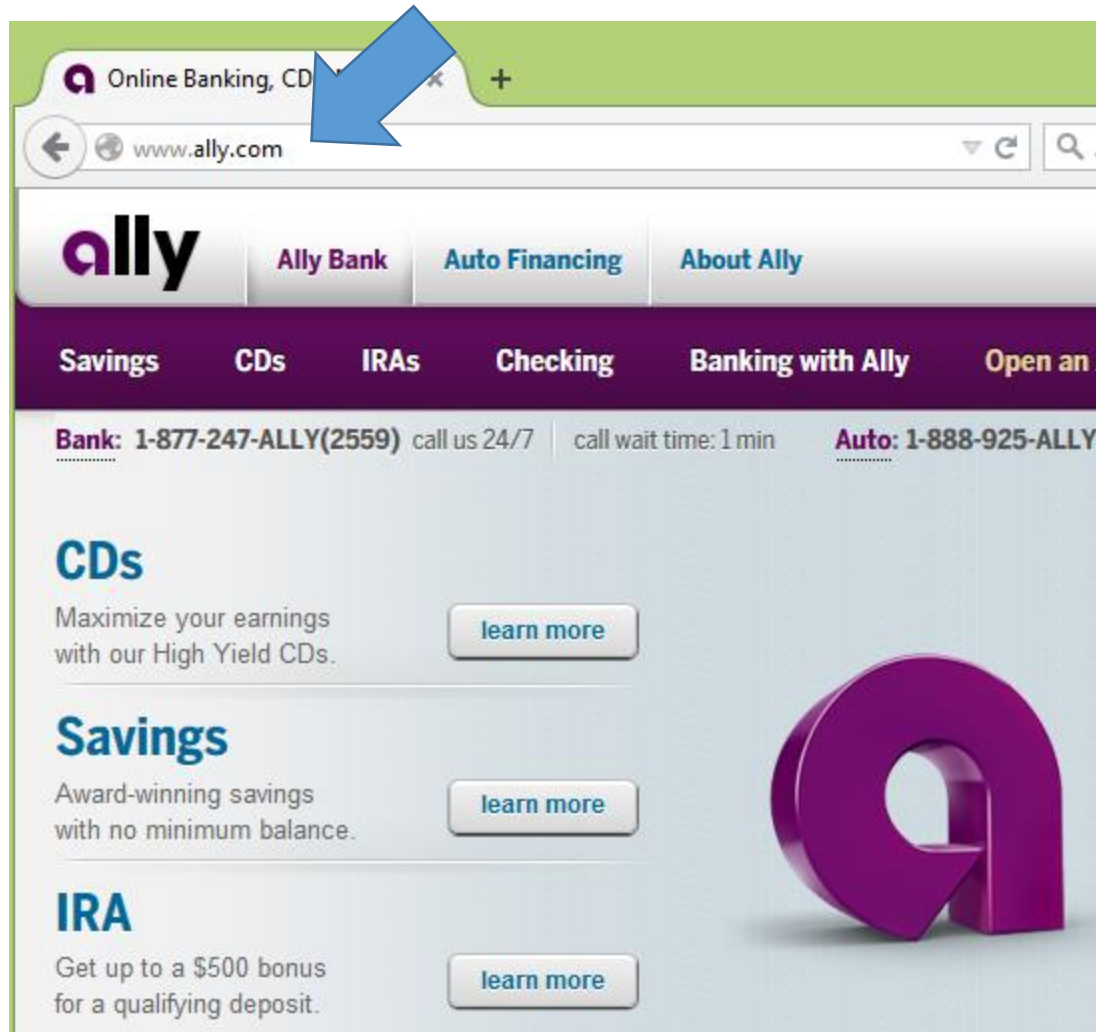


HTTPS Explained

DR KAMI VANIEA

http versus https





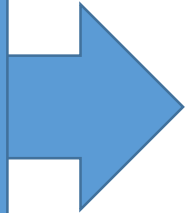
https://ally.com

versus

http://ally.com

Encryption properties we want:

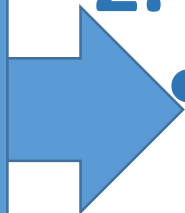
Cryptography magic sorts this one out for us: Confidentiality, Integrity.



1. The communication between you and the other party is **confidential** and has **not been changed**

- No one can read what you sent
- No one can change what you sent

This one is a bit harder.
Cryptography can verify you are speaking to the same person, but not identity.



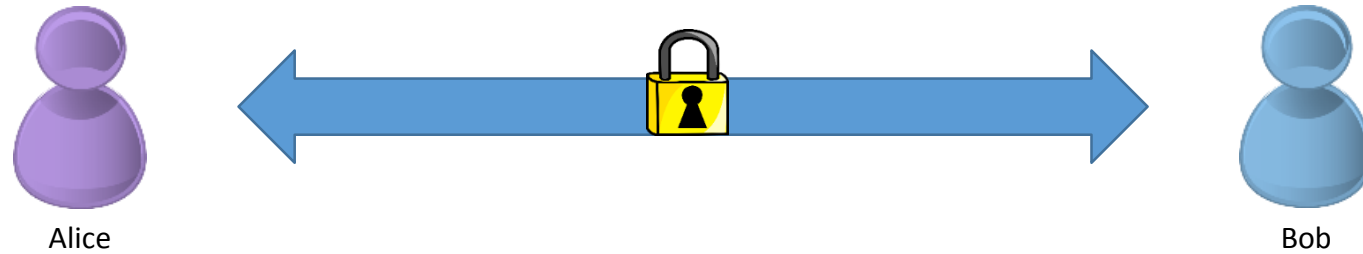
2. **Knowing who** you are communicating with

- You are talking to who you think you are talking to and not someone else

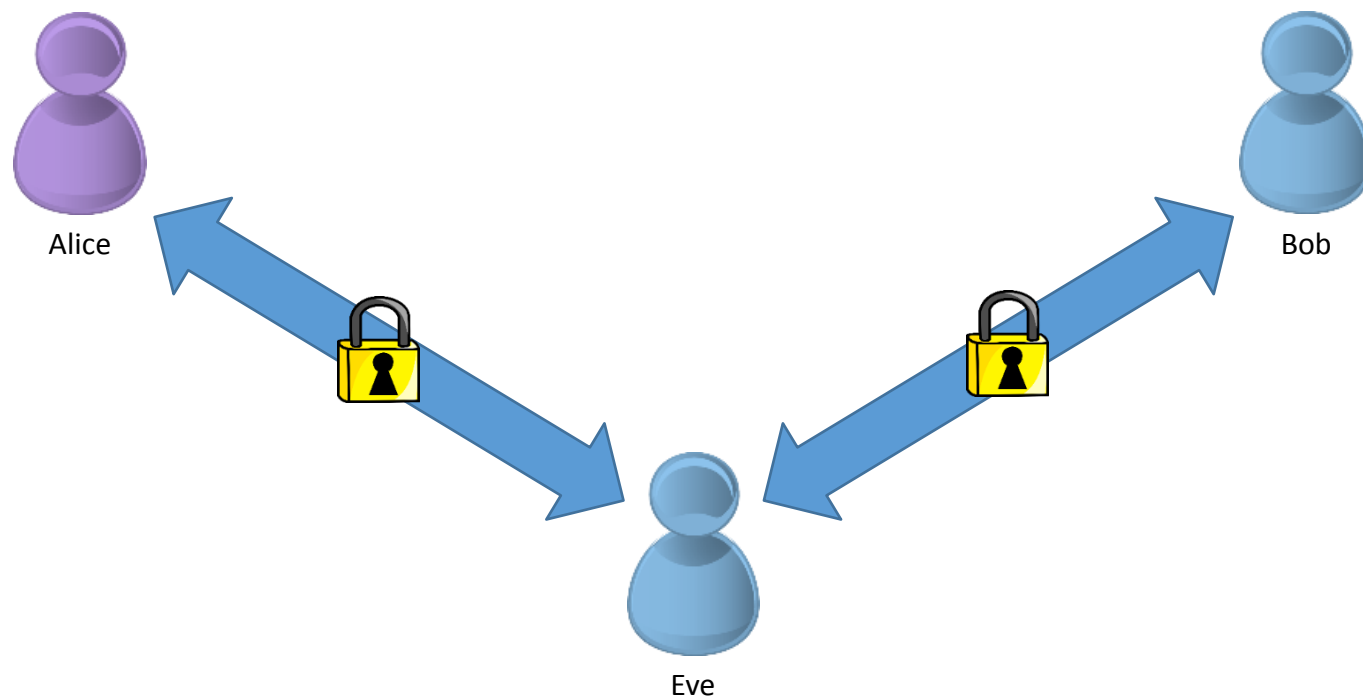
Alice wants to talk securely with Bob



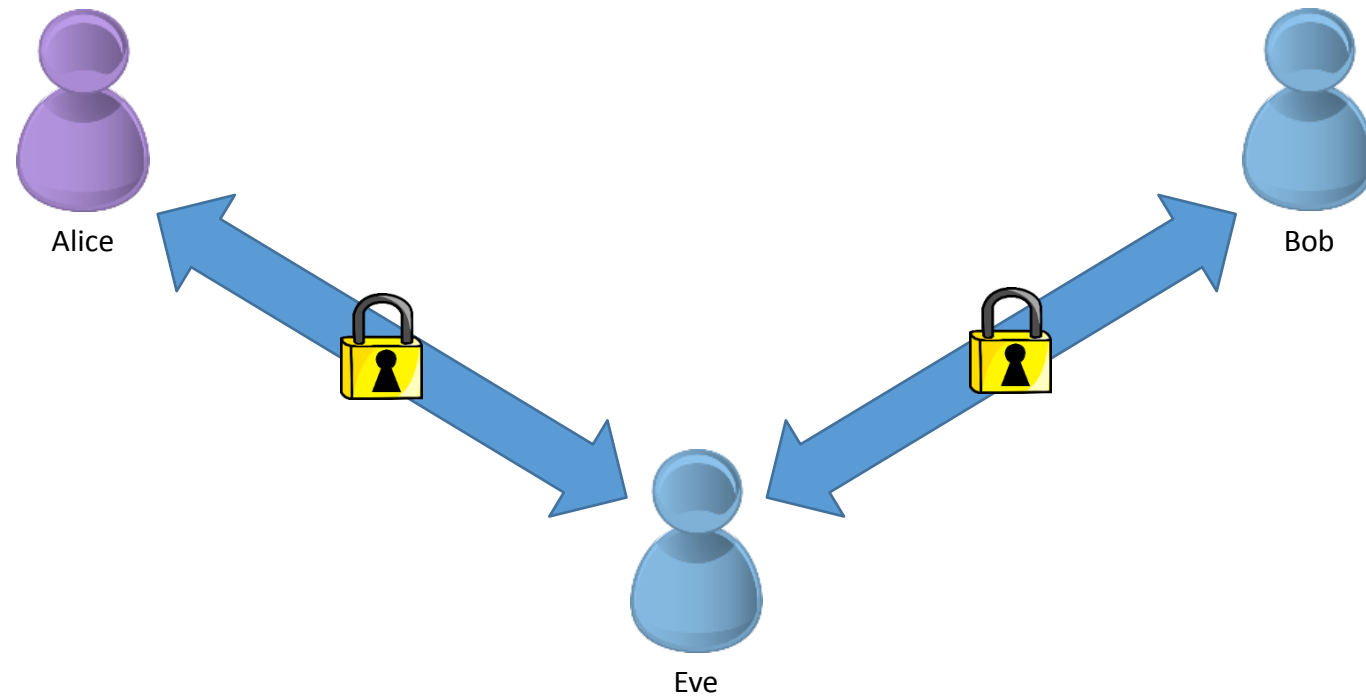
She can encrypt the connection (1)



**But how can Alice know she is
talking to Bob and not talking to
Eve? (2)**



Man in the middle attack



Encryption properties we want:

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

First, a short primer on encryption.

You will need to understand this eventually, but for now you mostly need to get the general idea of it.

Link identity to keys

- Encryption often depends on keys like the one on the right
- These keys are used with a whole pile of math to encrypt and decrypt a file.

Overly simple example:

Message	C	R	Y	P	T	O
Key	A	Y	S	Y	I	F
Encrypted	C	P	Q	N	B	T

My public key

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

mQENBFHMcgABCAC9WrYDO6K2L3VHyi4eHN6suHLqMpl+SO+IUTuLEVNuzIoXAUXH
KozHejFV/9XoG8j933ZtszXKCog3aMESe0E0z6fNGfolvaCe5B4jwq0t8NHwb5L
B2dnq0CplgXcN2GJxfEHUaf27COSobCJxPMeshUh4ZHke+g6DatmiEtBpVp41Ot
1zgxDMQkgb2H2xw28RyFYkdDouetelkOrFLrCy9ZF9KdMhA1eBH94KnnwIQshdiZR
QYEX25+M8cKCb++Rc9H6an7EG9WHOFRW40UsY52OfveOyfQPzkkRto7u2339hvH0
B/h+7xLM6FQbOUZQ9BD5w7IQHgYtXJVsUj0dABEBAAG0IktbWkgVmfuaWVhIDxr
dmFuaWVhQGluZi5lZC5hYy51az6JAT8EEwEIAckFAIYKYvECGyMFCQlMAYAHcwkI
BwMCAQYVCAIJCsEFglDAQleAQIXgAAKCRCTdsxl9/HZffG+CACShuKxje3QAqew
GWh8K4gCdiY0xDqJwq3PHxmyhZmQeN/1a1KcOrljl2b+Q75/5t+EgXOHpR0PlxfG
IZ6zOEpf6A18iFxx3JgQZdwPD0jtBiWNpOyMeBGTglvEYG3so2VueQoeXcq3dbYp
5vstVxtD+TKHQ5CiolT75P2bzYq/XLT5albNqhQDPcTo0DgbRH+FvqsRXr7yeaef
JaPnxX0+1L33t2QY9zctiGyebwrvHMrIPBJ2VYCDzQk7uQ5eFh42hsMgOmzLQD4
YiGr5weIMFwAvxZOaRxEa9Vf48jiWvrXuJ8YfHWS0hEScNocC2P8q20JjwwE26T
lpdtrwCqtB1LYW1plFZhbmlIYSA8a2FtaUB2YW5pZWUyY29tPobKbQgQTAQIALAib
lwUJCWYBgAcLQgHAWIBBHUIAgkKCwQWAgMBAh4BAheABQJWCmMeAhkBAaOJEJN2
zGX38dl9JIAIAIW0rxrlysrnKS6CbW8MgTxxTDOXA Ct1b7F0W0QZHSklUQHecE+a
XBYib1A5uHaatLfyeXaD3qMEoZnQHoYMGE0Gku00wWsbhfoQzHPgwrLkD1i75M
Bibaww0KWoVB9e4AkMakXJCnF5BXeo6AHLR2v15V205DikVnICRXCocKti8b7LnkM
cLn7oLobr1de1uyKoNzbSnO/vpKDjp0/EY5yUeV9olypZy/6wFQBehg1sXye6znO
9wb9uUsu9+/P8pz4JILMDSevjfT7zSRSl/YP3fofZ6N4bc+kOdWPM7u5Iyoeu9zh
pzibv3ge7VhH2xlWz8vYZ/2xt1345tWRRMOJAhwEEwECAAYFAITnSpEACgkQjyxM
p99tBt2B8A/+OplzOsQbQJB8yxti4l7PpD1weJdf3a81Vhm7JyXE/Xy66ypfdt3w
XmFRUulrwezY1NebWNCRCQHqZvRv/VJwjbTux+Q3HsjikIhB7iCiQXXtTRk0Eny
2nudcG12v03C3B2JCucEw6esF1x79Pl/IPv2+6tgUBKmdfOpsB2vbtqrHnmAYKL
4lQBFH1YSJgnzwo2Jkh0hcHdF90Zem1eMeiDEeVkh63893N8Swk5fBkdTj+SKZ/L
rQEIBBlpMR9BmeY6bPvWruycVK0nIMR80G9iFABxjTpWBL8aGk6EeVK5EqYDGvkd
ZlarK84r+KU1KD5IfgOCN7nhwgy7VImE68caZHSRiPWZP1fvVMyhdiRjW8WsoU56
InfVU3nxH+ZYthPbY0T86leGSchBT5K/fBQvbjhrRTbTFwvjzSifb9efWylDi994
nzP6cNorir3GlpsT8gPgBB2/NjxaWiM6y3X1az1vRnsunQHuyKkFWPZwnEvDJYaC
NN/3jWcbhLfwKBDsaHps2+1meFP0oJFvNetzp2bjT9a9pXaQ6KhOmo5DnhLcaV97
bFBpsUuBGaYzTSS05x1RdXHqpEbgap8dtuHhVvjw9QYDQBJr0K4aKyG9qqMD8cta
Pl/FAdyAqwH8Nw9efqAK+RQxSVUaue9BYEnbIRpsDK6MkP3YMFmu5ki5AQOEucxy
AAEIALyXyY8G2ZaTDJpdGcRhmlqOOSUlzPV7/5E5BbYKBNu4KU3nX+JLVcF5jxPQ
42c7i/WRVxE1BJTiarKGsEvCi94TTXSIUKat3T1oGbtXmGvqbGBq8JSGl1UTwdf
5yu50JyRSf2fqRND6P/2eHNXejDutdvHUXiUt8h9MuUO/ipD0DnwlVmnAATJHA+R
Zqw60NpyjRGzvr3iuWUwe4PtyJDl3ELAFkbp/Nac5TluVHRHNOwNpIcJhM5zHuB
QQb3G/EsCn2PQZ5wSSDzavF2SpvQfdqxYpDaTLAXtF+wsJL5iaUjxwRgJPodbCZf
2Tozd7h9MXtGJDIPK8eLg8ogcMAEQEAAyKBJQYQAQIADwUCUcxyAAlbDAUJCWYB
gAAKCRCTdsxl9/HZf5+hB/9BJqSmlgcoHFxnblPVIKxekzL8+VVm5Pk/EgMSQLZ2
HX4p3ial5PEPcYUw9YnaG4i00dwJGw5/daTWRrTzcnKd8YqoP+DU0t96HZDSu3m
mCzE9NVAQYboFbVmGQX0eo627UBSvFqaXvAXBDYkoR8B0TnKhrQFwxkZVb30hKwD
TgAFjOGIZi6uAdSt231tFaq0bizYfe5AVXRqro20xBqNbaJNqs3SW0D831Syvdv
lIOBx83/R0gg7hUkI6F2vzXicWmUwFSXRrggCSbLosHsP6isBWwwlHeRmna/aQab
YKG3gbV9iycZAS31gbogVLAZqNSWWhp8vVIEE28Fyf/Ed
=x5FK
-----END PGP PUBLIC KEY BLOCK-----

Public/private key cryptography

- Generate two “keys” that are paired
- **Whatever one key locks only the other key can unlock**
- Public keys are given out to everybody
- Private keys are kept private

My public key

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

```
mQENBFHMmcgABCAC9WrYDO6K2L3VHYi4eHN6suHLqMpl+SO+IUTuLEVnUzIoXAUXH
KozHejFV/9XoG8j933ZtszXKCog3aMESe0E0z6fNGfolvaCe5B4jwqJt8NHwb5L
B2dnq0CplgXcN2GJxfEHUaf27COSobCJxPMeshUh4ZHke+g6DatmiEtBpVp41Ot
1zgxdlMQkgb2H2xw28RyYfkdDouetelkOrFLrCy9ZF9KdMhA1eBh94KnnwIQshdiZR
QYEX25+M8cKCb++Rc9H6an7EG9WHOFRW40UsY52OfveOyfQPzkkRto7u2339hvH0
B/h+7xLM6FQbOUZQ9BD5w7IQHgYtXJVsUj0dABEBAAG0IkthbWkgVmFuaWVhIDxr
dmFuaWVhQGluzi5lZC5hYy51az6JAT8EEwEIAcKFAIYKYvECGyMFCQImAYAHcWkl
BwMCAQYQYCAIJCsEFgIDAQIeAQIXgAAKCRCTdsxl9/HZfFG+CACShuKxje3QAqew
GWh8K4gCdiY0xDqJwq3PHxmyhZmQeN/1a1KcOrljl2b+Q75/5t+EgXOHpR0PlxfG
IZ6zOEpf6A18iFxx3JgQZdwPD0JtBiWNPoOyMeBGTglvEYG3so2VueQoeXcq3dbYp
5vstVxtD+TKHQ5CiolT75P2bzYq/XLT5albNqHQDPcTo0DgbRH+fvqsRr7yeaef
JaPnxX0+1L33t2QY9zctiGyebwrvHMrIPBJ2VYCDzQk7uQ5eFh42hsMgOmzLQD4
YiGr5weIMFwAvxZOaRxEa9Vf48jiWvruxJ8YfHWS0hEScNocYC2P8q20JjwwE26T
lpdtrwCqtB1LYW1plFZhbmlIYSA8a2FtaUB2YVW5pZWUuY29tPokBQgQTAQIALAIB
lwUJCWYBgAcLCOgHAWIBBhUIAgkKCwQWAgMBAh4BAheABQJWCmMeAhkBAaOJEJN2
zGX38d9JIAIAIW0rxrlysmKS6CbW8MgTxxTD0XaCt1b7F0W0QZHSklUQHecE+a
XBYib1A5uHaatlFyjeXaD3qMEoZnQHoYMGEOGku00wWsbhfoQzHPgwrLkD1i75M
Blbaww0KWoVB9e4AkMakXJCnF5BXeo6AHLRL2v15V205DikVnICRXCocKtu8b7LnkM
cLn7oLobr1de1uyKoNzbSnO/vpKDJp0/EY5yUeV9olypZy/6wFQBehg1sXye6znO
9wb9uUsu9+/P8pz4JILMDSevjft7zSRSl/YP3fOfZ6N4bc+KodwPM7u5lyoeu9zh
pzibv3ge7VhH2xlWz8vYZ/2xT1345tWRRMOJAhwEEwECAAYFAITnSpEACgkQjyxM
p99tBt2B8A/+OplzOsQbQJB8yxti4l7PpD1weJdf3a81Vhm7JyXc/Xy66ypfdt3w
XmFRUulrwezY1NebWNCRQHqZvRv/VJwjbTux+Q3HsjikIHbE7iCiQXXtTRk0Eny
2nudcJGI2v03C3B2JCucEw6esF1x79PI/IPv2+6tgUBKmdfOpsB2vbtqrHnmAYKL
4lQBfH1YSJgnzwo2Jkh0hcHdF90Zem1eMeiDEeVkh63893N8Swk5fBKdTj+SKZ/L
rQEIBBlpMR9BmeY6bPvWruycVK0nIMR80G9iFABxjTpWBL8aGk6EeVK5EqYDGvkd
ZlarK84r+KU1KD5IfgOCN7nhwgy7VImE68caZHSRiPWZP1fvVMyhydiRjv8WsoS6
INFVU3nxH+ZYthPbY0T86leGSchBT5K/fBQvbjhrRTbTFwvjzSifb9efWylDi994
nzP6cNorir3GlpsT8gPgBB2/NjxaWiM6y3X1az1vRnsunQHuyKkFWPZwnEvDJYaC
NN/3jWcbhLFwKBDsaHps2+1meFP0oJFvNetzp2bjT9a9pXaQ6KhOmo5DnhLcaV97
bFBpsUuBGaYZTSS05x1RdXHqpEbgap8dtuHhVvJw9QYDQBJR0K4aKyG9qqMD8cta
PI/FAdyAqwH8Nw9efqAK+RQxSVUaue9BYEnbIRpsDK6MKp3YMFmu5k15AQOEucxy
AAEIALyXyY8G2ZaTDJpdGcRhmlqOOSUlzPV7/5E5BbYKBNu4KU3nX+JLVcF5jxPQ
42c7i/WRVxE1BJTiarKGsEvCi94TTXSIUKAt3T1oGBtXmGvqbGBq8JlSGl1UTwdf
5yu50JyRSf2fqRND6P/2eHNXejDutdvHUXiUt8h9MuUO/ipD0DnwlVmnAATJHA+R
Zqw60NpyjRGzvr3iuWUwe4PtyJDI3ELAFkbp/Nac5TiuVHRHNOwnPlclJhM5zHuB
QQb3G/EsCn2PQZ5w5SDzavF2SpvQfdqxYpDaTLAXtF+wsJL5iaUjxwRgJPodbCZf
2Tozd7h9MxTgDIPKJ8eLG8ogcMAEQEAAyKBJQYAQIADwUCUcxyAAlbDAUJCWYB
gAAKCRCTdsxl9/HZf5+hB/9BJqSmlgcoHFxnb1PVIKxekzL8+VWm5Pk/EgMQSLZ2
HX4p3ial5PEPcYgUw9YnaG4i00dwJGw5/daTWRrTzcnKd8YqoP+DU0t96HZDSu3m
mCzE9NVAQYboFbVmGOxo0e627UBSvFqaXvAXBDYkoR8B0TnKhrQFwxkZvB30hKwD
TgAFjOGIZi6uadSt231tFaq0bizYfe5AVXRqro20xBqNbaJNqs3SWOD831Syvdu
lIOBx83/R0gg7hUkl6F2vzXicWmUwFSXRggCSbLosHsP6isBWwwlHeRmna/aQab
YKG3gbV9iyczAS31gbogVLAZqNSWWhp8vVIEE28Fyf/Ed
=x5FK
```

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

I want to prove a message is from me

- I encrypt (lock) the message with my private key
- Anyone with the public key can use it to decrypt (unlock) the file. If it decrypts (unlocks), then it must have been encrypted (locked) by my private key and no other.

My public key

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

```
mQENBFHMCGABCAC9WrYDO6K2L3VHyi4eHN6suHLqMpl+SO+IUTuLEVnUzIoXAUXH
KozHejFV/9XoG8j933ZtszXKCog3aMESe0E0z6fNGfolvaCe5B4jwqJt8NHwb5L
B2dnq0CplgXcN2GJxfEHUaf27COSobCJxPMeshUh4ZHke+g6DatmiEtBpVp41Ot
1zgxDMQkgb2H2xw28RyFYkdDouetelkOrFLrCy9ZF9KdMhA1eBH94KnnwIQshdiZR
QYEX25+M8cKCb++Rc9H6an7EG9WHOFRW40UsY52OfveOyfQPzkkRto7u2339hvH0
B/h+7xLM6FQbOUZQ9BD5w7IQHgYtXJVsUj0dABEBAAAG0IkthbWkgVmFuaVWVhIDxr
dmFuaVWVhQGlUzi5lZC5hYy51az6JAT8EEwEIAckFAIYKYvECGyMFCQlMAYAHcWkl
BwMCAQYQYCAIJGcsEFfIDAQIeAQIXgAAKCRCTdsxl9/HZffG+CACShuKxje3QAqew
GWh8K4gCdiY0xDqJwq3PHxmyhZmQeN/1a1KcOrljl2b+Q75/5t+EgXOHpR0PlxfG
IZ6zOEpf6A18iFxx3JgQZdwPD0jtBiWNpOyMeBGTglvEYG3so2VueQoeXcq3dbYp
5vstVxtD+TKHQ5CiolT75P2bzYq/XLT5albNqHQDPcToODgbrRH+Fvq5Rr7yeaef
JaPnxX0+1L33t2QY9zctiGyebwrvHMrlPBj2VYCDzQk7uQ5eFh42hsMgOmzLQD4
YiGr5weIMFwAvxZOaRxEa9Vf48jiWvrXuJ8YfHWS0hE5cNocYC2P8q20JjwwE26T
lpdtrwCqtB1LYW1plFZhbmlIYSA8a2FtaUB2Yw5pZWUyY29tPobKQgQTQAIALAib
lwUJCWYBgAcLCQgHAWIBBHUIAgkKcWQWAgMBaH4BAheABQJWCmMeAhkBAaOJEJN2
zGX38dI9JIAIw0rxrlysmKS6CbW8MgTxxTDOXA Ct1b7F0W0QZHSklUQH EcE+a
XBYib1A5uHaatlFyjeXaD3qMEoZnQHoYMGE0Gku00wWsbhfoQzHPgwrLkD1i75M
Bibaww0KWoVB9e4AkMakXJCnF5BXeo6AHLR2v15V205DikVnICRXCocKtu8b7LnkM
cLn7oLobr1de1uyKozNbSnO/vpKDJp0/EY5yUeV9olypZy/6wFQBehg1sXye6znO
9wb9uU9u9+/P8pz4JILMDSevjft7zSRSl/YP3fOfZ6N4bc+kOdWPM7u5lyoeu9zh
pzibv3ge7VhH2xiWz8vYZ/2xT1345tWRRMOJAhwEEwECAAyFAITnSpEACgkQjyxM
p99tBt2B8A/+OplzOsQbQJB8yxti4l7PpD1weJdF3a81Vhm7JyXe/Xy66ypfdt3w
XmFRUulrwezY1NebWNCROHzQvRv/VJwjbTux+Q3HsjikIhB7iCiQXXtTRk0Eny
2nudcJG12v03C3B2JCucEw6esF1x79Pl/Pv2+6tgUBKMDfOpsB2vbtqrHnmAYKL
4lQBfH1YSJgnzwo2Jkh0hcHdF90Zem1eMeiDEeVkh63893N8Swk5fBKdTj+SKZ/L
rQEIBBlpMR9BmeY6bPvWruycVK0nIMR80G9iFABxjTpWBL8aGk6EeVK5EqYDGvkd
ZlarK84r+KU1KD5IfgOCN7nhwgy7VImE68caZHSRiPWZP1fvVMyhdiRjWsoU56
INfVU3nxH+ZYthPbY0T86leGSchBT5K/fBQvbjhrRTbTFwvjzSifb9efWylD1994
nzP6cNorir3GlpsT8gPgBB2/NjxaWiM6y3X1az1vRnsunQHuyKkFWPZwnEvDJYaC
NN/3jWcbhLfwKBDsaHps2+1meFP0oJFvNetzp2bjT9a9pXaQ6KhOmo5DnhLcaV97
bFBpsUuBGaYZTSS05x1RdXHqpEbgap8dtuHhVvJw9QYDQBJR0K4aKyG9qqMD8cta
Pl/FAdyAqwH8Nw9efqAK+RQxSVUaue9BYEnbIRpsDK6MKp3YMFmu5ki5AQOEucxy
AAEIALyXyY8G2ZaTDJpdGcRhmlqOOSUlzPV7/5E5BbYKBNu4KU3nX+JLVcF5jxPQ
42c7i/WRVxE1BJTiarKGsEvCi94TTXSIUKat3T1oGBtXmGvqbGBq8JlSGl1UTwdf
5yu50JyRSf2fqRND6P/2eHNXejDutdvHUXiUt8h9MuUO/ipD0DnwlVmnAATJHA+R
Zqw60NpyjRGzvr3iuWUwe4PtyJDI3ELAFkbp/Nac5TiuVHRHNOwNpIcJhM5zHuB
QQb3G/EsCn2PQZ5w5SDzavF2SpvQfDqxYpDaTLAXtF+wsJL5iaUjxwRgJPodbCZf
2Tozd7h9MxTgtDIPKJ8eLG8ogcMAEQEAAYkBJQYQAQIADwUCUcxyAAlbDAUJCWYB
gAAKCRCTdsxl9/HZf5+hB/9BJqSmlgcoHFxnb1PVIKxekzL8+WVm5Pk/EgMQSLZ2
HX4p3ial5PEPcYgUw9YnaG4i00dwJGw5/daTWRrTzcnKd8YqoP+DU0t96HZDSu3m
mCzE9NVAQYbOfbVmGOxo0e627UBSvFqaXvAXBDYkoR8B0TnKhrQFwxkZVb30hKwD
TgAFJOGIZiE6uAdSt231tFaq0bizYfe5AVXRqro20xBqNbaJNqs3SWOD831Syvdv
lIOBx83/R0gg7hUkl6F2vzXicWmUwFSXRggCSbLosHsP6isBWwwlHeRmna/aQab
YKG3gbV9iyczAS31gbogVLAZqNSWhp8vVIEE28Fyf/Ed
=x5FK
```

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

I want to send Bob a message that no one else can read

- I encrypt (lock) the message with Bob's public key.
- Only Bob has his private key, so only Bob can decrypt (unlock) the message.

My public key

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

```
mQENBFHMcgABCAC9WrYDO6K2L3VHYi4eHN6suHLqMpl+SO+IUTuLEVNzUoXAUXH
KozHejFV/9XoG8j933ZtsXKCog3aMESe0E0z6fNGfolvaCe5B4jwqJt8NHwb5L
B2dnq0CplgXcN2GJxfEHUaf27COSobCJxPMeshUh4ZHke+g6DatmiEtBpVp41Ot
1zgxDMQkgb2H2xw28RYfYkdDouetelkOrFLrCy9ZF9KdMhA1eBH94KnwIQshdiZR
QYEX25+M8cKCb++Rc9H6an7EG9WHOFRW40UsY52OfveOyfQPzkkRto7u2339hvH0
B/h+7xLM6FQbOUZQ9BD5w7IQHgYtXJVsUj0dABEBAAAG0IkthbWkgVmFuaWVhIDxr
dmFuaWVhQGluzi5lZC5hYy51az6JAT8EEwEIAcKFAIYKYvECGyMFCQlMAYAHcwkI
BwMCAQYVCAIJCsEFgIDAQIeAQIXgAAKCRCTdsxl9/HZfFG+CACSShuKxje3QAqew
GWh8K4gCdiY0xDqJwq3PHxmyhZmQeN/1a1KcOrljl2b+Q75/5t+EgXOHpR0PlxfG
IZ6zOEpf6A18iFxx3JgQZdwPD0jtBiWNpOyMeBGTglvEYG3so2VueQoeXcq3dbYp
5vstVxtD+TKHQ5CiolT75P2bzYq/XLT5albNqHQDPcToODgbRH+FvqsRXr7yeaef
JaPnxX0+1L33t2QY9zctiGyebwrvHMrlPBj2VYCDzQk7uQ5eFh42hsMgOmlQD4
YiGr5weIMFVAvxZOaRxEa9Vf48jiWvrXuJ8YfHWS0hEScNOcYC2P8q20JjwwE26T
lPdtwCqtB1LYW1plFZhbmlIYSA8a2FtaUB2YVW5pZWUyY29tPokBQgQTQIAIAIb
lwUJCWYBgAcLCQgHAWlBBhUIAgkKCwQWAgMBAh4BAheABQJWCmMeAhkBAaOJEJN2
zGX38d9JIAIAIW0rxrlysmKS6CbW8MgTxxTDOXA Ct1b7F0W0QZHSklUQH EcE+a
XBYib1A5uHaatlFyjeXaD3qMEoZnQHoYMGE0Gku00wWsbhfoQzHPgwrLkD1i75M
Blbaww0KWoVB9e4AkMakXJCnF5BXeo6AHLR2v15V205DikVnICRXocKtu8b7LnkM
cLn7oLobr1de1uyKoNzbSnO/vpKDJp0/EY5yUeV9olypZy/6wFQBehg1sXye6znO
9wb9uUusu9+/P8pz4JILMDSevjfT7zSRSl/YP3fOfZ6N4bc+kOdWPM7u5lyoeu9zh
pzibv3ge7VhH2xiWz8vYZ/2xT1345tWRRMOJAhwEEwECAAyFAITnSpEACgkQjyxM
p99tBt2B8A/+OplzOsQbQJB8yxti4l7PpD1weJdF3a81Vhm7JyXe/Xy66ypfdt3w
XmFRUulrwezY1NebWNCRQHqZvRv/VJwjbTux+Q3HsjlKIhBE7iCiQXXtTRk0Eny
2nudcJGI2v03C3B2JCucEw6esF1x79Pl/IPv2+6tgUBKmdfOpsB2vbtqrHnmAYKL
4lQBfH1YSJgnzwo2Jkh0hcHdF90Zem1eMeiDEeVkh63893N8Swk5fBKdTj+SKZ/L
rQEIBBlpMR9BmeY6bPvWRuycVK0nIMR80G9iFABxjTpWBL8aGk6EeVK5EqYDGvkd
ZlarK84r+KU1KD5IfgOCN7nhwgy7VImE68caZHSRiPWZP1fVvMhydiRjv8WsoU56
INFvU3nxH+ZYthPbY0T86leGSchBT5K/fBQvbjhrRTbTFwvjzSifb9efWylDi994
nzP6cNorir3GlpsT8gPgBB2/NjxaWiM6y3X1az1vRnsunQHuyKKFWPZwnEvDJYaC
NN/3jWcbhLFwKBDsaHps2+1meFP0oJFvNetzp2bjT9a9pXaQ6KhOmo5DnhLcaV97
bFBpsUuBGaYZTSS05x1RdXHqpEbgap8dtuHhVvJw9QYDQBJr0K4aKyG9qqMD8cta
PI/FAdyAqwH8Nw9efqAK+RQxSVUaue9BYEnblRpsDK6MKp3YMFmu5k15AQOEucxy
AAEIALyXYy8G2ZaTDJpdGcRhmlqOOSUlzPV7/5E5BbYKBNu4KU3nX+JLVcF5jxPQ
42c7i/WRVxE1BJTiarKGsEvCi94TTXSIUKAt3T1oGBtXmGvqbGBq8JlSGl1UTwdf
5yu50JyRSf2fqRND6P/2eHNXejDutdvHUXiUt8h9MuUO/ipD0DnwlVmnAATJHA+R
Zqw60NpyjRGzvr3iuWUwe4PtyJDI3ELAFkbp/Nac5TluVHRHNOWNpIclJhM5zHuB
QQb3G/EsCn2PQZ5w5SDzavF2SpvQfdqxYpDaTLAXtF+wsJL5iaUjxwRgJPodbCZf
2Tozd7h9MxTgDIPKJ8eLG8ogcMAEQEAAYkBJQYAQAIAQWUUCyXAAIbDAUJCWYB
gAAKCRCTdsxl9/HZf5+hB/9BJqSmlgcoHFxnb1PVIKxekzL8+VWm5Pk/EgMQSLZ2
HX4p3ial5PEPcYgUw9YnaG4i00dwJGw5/daTWRrTzcnKd8YqoP+DU0t96HZDSu3m
mCzE9NVAQYboFbVmGOxo0e627UBSvFqaXvAxBDYkoR8B0TnKhrQFwxkZVb30hKwD
TgAFjOGIZiE6uAdSt231tFaq0bizYfe5AVXRqro20xBqNbaJNqs3SWOD831Syvdu
lIOBx83/R0gg7hUkl6F2vzXicWmUwFSXRggCSbLosHsP6isBWwwlHeRmna/aQab
YKG3gbV9iyczAS31gbogVLAZqNSWWhp8vVIEE28Fyf/Ed
=x5FK
-----END PGP PUBLIC KEY BLOCK-----
```

If I do both of those at the
same time I can prove that only
I could have sent the message
and that only Bob can read it.

My public key

-----BEGIN PGP PUBLIC KEY BLOCK-----

Version: GnuPG v2

```
mQENBFHMcgABCAC9WrYDO6K2L3VHYi4eHN6suHLqMpJ+SO+IUTuLEVnUzIoXAUXH
KozHejFV/9XoG8j933ZtszXKCog3aMESe0E0z6fNGfolvaCe5B4jwqJt8NHwb5L
B2dnq0CplgXcN2GJxfEHHUaf27COSobCJxPMeshUh4ZHke+g6DatmiEtBpVp41Ot
1zgxDMQkgb2H2xw28RyFYkdDouetelkOrFLrCy9ZF9KdMhA1eBH94KnnwIQshdiZR
QYEX25+M8cKCb++Rc9H6an7EG9WHOFRW40UsY52OfveOyfQPzkkRto7u2339hvH0
B/h+7xLM6FQbOUZQ9BD5w7IQHgYtXJVsUj0dABEBAAG0IktbWkgVmfuaWVhIDxr
dmFuaWVhQGluZi5lZC5hYy51az6JAT8EEwEIAcKFAIYKYvECGyMFCQlmaYAHcWkl
BwMCAQYVCAIJCgsEFglDAQIeAQIXgAAKCRCTdsxl9/HZffG+CACShuKxje3QAqew
GWh8K4gCdiY0xDqJwq3PHxmyhZmQeN/1a1KcOrljl2b+Q75/5t+EgXOHpR0PlxfG
IZ6zOEpf6A18iFXx3JgQZdwPD0jtBiWNPoYMeBGTglvEYG3so2VueQoeXcq3dbYp
5vstVxtD+TKHQ5CiolT75P2bzYq/XLT5albNqHQDPcToODgbRH+FvqsRXr7yeaef
JaPnxX0+1L33t2QY9zctiGyebwrvHMrIPBJ2VYCDzQk7uQ5eFh42hsMgOmlZQD4
YiGr5weIMFwAvxZOaRxEa9Vf48jiWvrXuJ8YfHWS0hEScNocYC2P8q20JjwwE26T
lpdtrwCqtB1LYW1plfZhbmlYSA8a2FtaUB2YW5pZWUyY29tPokBQgQTAQIALAIB
lwUJCWYBgAcLCQgHAwIBBhUIAgkKCwQWAgMBAh4BAheABQJWCmMeAhkBAaOJEJN2
zGX38dl9JIAIAIW0rxrlySrmKS6CbW8MgTxxTDOXaCt1b7F0W0QZHSklUQHecE+a
XBYib1A5uHaatLfyeXaD3qMEoZnQHoYMGE0Gku00wWsbhfoQzHPgwrLkD1i75M
Blbaww0KW0VB9e4AkMakXJCnF5BXeo6AHLR2v15V205DikVnlCRXocKtu8b7LnkM
cLn7oLobr1de1uyKoNzbSnO/vpKDJp0/EY5yUeV9olypZy/6wFQBehg1sXye6znO
9wb9uUsu9+/P8pz4JILMDSevjfT7zSRSl/YP3fOfZ6N4bc+kOdWPM7u5lyoeu9zh
pzibv3ge7VhH2xiWz8vYZ/2xT1345tWRRMOJAhwEEwECAAYFAITnSpEACgkQjyxM
p99tBt2B8A/+OplzOsQbQJB8yxti4l7PpD1weJdf3a81Vhm7JyX/Xy66ypfdt3w
XmFRUulrwezY1NebWNCROHQzQvRv/VJwjbtUx+Q3HsjikIHbE7iCiQXXtTRk0Eny
2nudcGj2v03C3B2JCucEw6esF1x79Pl/IPv2+6tgUBKmdFopsB2vbtqrHnmAYKL
4lQBfH1YSJgnzwo2Jkh0hcHdF90Zem1eMeiDEeVkh63893N8Swk5fBKdTj+SKZ/L
rQEIBBlpMR9BmeY6bPvWruycVK0nIMR80G9iFABxjTpWBL8aGk6EeVK5EqYDGvkd
ZlarK84r+KU1KD5IfgOCN7nhwgy7VImE68caZHSRiPWZP1fvVMhydiRjv8WsoU56
InfvU3nxH+ZYthPbY0T86leGSchBT5K/fBQvbjhrRTbTFwvj2Sifb9efWylDi994
nzP6cNorir3GlpsT8gPgBB2/NjxaWiM6y3X1az1vRnsunQHuyKkFWPZwnEvDJYaC
NN/3jWcbhLFwKBDsaHps2+1meFP0oJFvNetzp2bjT9a9pXaQ6KhOmo5DnhLcaV97
bFBpsUuBGaYZTSS05x1RdXHqpEbgap8dtuHhVvJw9QYDQBJr0K4aKyG9qqMD8cta
Pl/FadyAqwH8Nw9efqAK+RQxSVUaue9BYEnblRpsDK6MKp3YMFmu5ki5AQOEucxy
AAEIALyXYy8G2ZaTDJpdGcRhmlqOOSUlzPV7/5E5BbYKBNu4KU3nX+JLVcF5jxPQ
42c7i/WRVxE1BJTiarKGsEvCi94TTXSIUKat3T1oGBtXmGvqbGBq8JlSGl1UTwdf
5yu50JyRSf2fqRND6P/2eHNXejDUtdvhUXiUt8h9MuUO/ipD0DnwlVmnAATJHA+R
Zqw60NpyjRGzvr3iuWUwe4PtyJDI3ELAFkbp/Nac5TluVHRHNOwnPlclJhM5zHuB
QQb3G/EsCn2PQZ5w5SDzavF2SpvQfDqxYpDaTLAXtF+wsJL5iaUjxwRgJPodbCZf
2Tozd7h9MXtGtDIPKJ8eLG8ogcMAEQEAAyKBJQYAQAQIADwUCucyAAIbDAUJCWYB
gAAKCRCTdsxl9/HZf5+hB/9BJqSmlgcoHFxb1PVIKxekzL8+wwm5Pk/EgMQLSZ2
HX4p3ial5PEPcYUw9YnaG4i00dwJGw5/daTWRrTcnKd8YqoP+DU0t96HZDSu3m
mCzE9NVAQYboFbVmGQx0eo627UBSvFqaXvABDYkoR8B0TnKhrQFwxkZVb30hKwD
TgAFjOGIZi6uadSt231tFaq0bizYfe5AVXRqro20xBqNbaJNqs3SWOD831Syvdv
lIOBx83/R0gg7hUkl6F2vzXicWmUwFSXRggCSbLosHsP6isBWwwlHeRmna/aQab
YKG3gbV9iyzcAS31gbogVLAZqNSWWhp8vVIEE28Fyf/Ed
```

=x5FK

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

But we still have a problem:

All that assumes that we know which key goes with which person (2).

How do we solve the identity problem?

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

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/ARlVtIjIDEmS0F9MRZicV0UKyA5qV
c9BafZnAicY7nezkIJUmyLcIVMC60pqSHzo0Ewy2PZjxzcI4vDGhHmcgfV5X
R+duYld3LtVI+A/5jv326LB16bCNts/tOhW2T0LraMPOctdH84Z4tPcyp335
s8/dZ2C+EoMD4iX1kIymZ1kqEfZNvcs1sRUXy27sL01VHcYmi6UNWCeeHOu2
2yJxMiBCniozBKZUwcr6ysg97nnq633dn9mf7V30PS3zAjhe0Hvmzg3B/Nfo
qzy2dAEU/JDUBhiAo+xr9VF3ZPOoC8JySORgyUm/2t3TTBaH+DnfsUBiqo5U
2T0n8x2R1FWxyZYNCTku5JOvPqRBft13DSyJD7LDDps62nqhpVb34eprwuk
qIk0TMRu9mB4EQc+cNFR3ZpN1AKj+HOb/TUJwCJpVju2/3g0wgdqHh+OQlvC
Nm8vIGnQZWQ30WqnH/UFoh3RPJ+WqnDq88NmQBq8I4aNV4u8MgoObd/zrtVX
kAwYHbIZLo925NjFyPuuxhWiCotKen18dZefB8aB81RjYUIMnCJ0GQus+JG8
TJyEesNdK/q8HD5h1kCRSzMHD1+Ra3z/1+FFIwARAQABzR1BZG9iZSBQU01S
VCA8cHNpcnRAYWRvYmUuY29tPsLBewQQAQgALwUCWb/YrWUJAEezgAYLCQgH
AwIJEIbAD8Kvh3YWBBUIAgoDFgIBAhkBAhsDAh4BAADk2A//f+6PFzg4VmLI
PzstTZPoqPR/lXlZ7RIYbQosHvsFwyW0WWXluIlsEeD5Qo7HQ6NNMAOW51Js
wFvFOWIa9U6SHRoU1kGTSESReOq5HnXe4DcBubsKmoMS68PuiZ88wYOIM4Up
9V9PUuaue0U4oSrYHnH5qBOqurtv8wO5Cq4uTwnfnjN7n4OH0++2910PJ68B
6+kMuQyG4swmxsZhljlqGMHcs0c/BuI3W+n5w+xLM7N5jjCTjNXR+tGmstdm
RPEoLWOso+ZFwfNW0CLKjYUahp3p6H9x8R13wrp2re0GhqKRgt3D4UcAqsPs
```

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
c9BafZnAicY7nezkiJUmYlCIVMC60pgSHzo0Ewy2PZjxzcI4vDGhHmcgfV5X
R+duYld3LtVI+A/5jv326LB16bCNts/tOhW2T0LraMPoCtdH84Z4tPcyp335
s8/dZ2C+EOmd4iX1kIymZ1kqEfZNvcs1sRUXy27sL01VHcYmi6UNWCeeHOu2
2yJxMiBCniozBKZUwCR6ysg97nnq633dN9mf7V30PS3zAjhE0Hvmzg3B/Nfo
qzy2dAEU/JDUBhiAo+xr9VF3ZPOoC8JySORgyUm/2t3TTBaH+DnfsUBiqo5U
2T0n8x2R1FWxyZYnCTku5JOvPqRBft13DSyJD7LDDps62nqhpaVb34eprwuk
qIk0TMRu9mB4EQc+cNFR3ZpN1AKj+HOb/TUJwCJpVju2/3g0wgdcHh+OQlvC
Nm8vIGnQZwQ30WqnH/UFoh3RPJ+WqnDq88NmQbq8I4aNV4u8MgoObd/zrtVX
kAwYHbIZLo925NjFyPuuxhWiCotKenl8dZefB8aB81rjYuIMnCJ0GQus+JG8
TJyEesNdK/q8HD5h1kCRSzMHD1+Ra3z/1+FFIwARAQABzR1BZG9iZSBQU01S
VCA8CHNpcnRAYWRvYmUuY29tPSLBewQQAQgALwUCWb/YrWUJAeEzgAYLCQgH
AwIJEIbAD8Kvh3YWBbUIAgoDFgIBAhkBAhsDAh4BAADk2A//f+6PFzg4VmLI
PzsTZPoqPR/lXlZ7RIYbQosHvsFwyW0WWX1uIlsEeD5Qo7HQ6NNMAOW51Js
wFvFOWIa9U6SHRoU1kGTSESReOq5HnXe4DcBubsKmoMS68PuiZ88wYOIM4Up
9V9PUuaue0U4oSrYHnH5qBOqurtv8wO5Cq4uTwnfnjN7n4OH0++2910PJ68B
6+kMuQyG4swmxsZhlj1qGMHcs0c/BuI3W+n5w+xLM7N5jjCTjNXR+tGmstdm
RPEoLWOso+ZFwfNW0CLKjYUahp3p6H9x8R13wrp2re0GhqKRgt3D4UCaQsPs
```

Photo credit: Juho Nurminen
@jupenur

PSIRT PGP Key (0x33E9E596) x

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



blogs.adobe.com

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
c9BafZnAicY7nezkiJUmYlCIVMC60pgSHzo0Ewy2PZjxzcI4vDGhHmcgfV5X
R+duYld3LtVI+A/5jv326LB16bCNts/tOhW2T0LraMPoCtdH84Z4tPcyp335
s8/dZ2C+EOmd4iX1kIymZ1kqEfZNvcs1sRUXy27sL01VHcYmi6UNWCeeHOu2
2yJxMiBCniozBKZUwCR6ysg97nnq633dN9mf7V30PS3zAjhE0Hvmzg3B/Nfo
qzy2dAEU/JDUBhiAo+xr9VF3ZPOoC8JySORgyUm/2t3TTBaH+DnfsUBiqo5U
2T0n8x2R1FWxyZYnCTku5JOvPqRBft13DSyJD7LDDps62nqhpaVb34eprwuk
qIk0TMRu9mB4EQc+cNFR3ZpN1AKj+HOb/TUJwCJpVju2/3g0wgdcHh+OQlvC
Nm8vIGnQZwQ30WqnH/UFoh3RPJ+WqnDq88NmQbq8I4aNV4u8MgoObd/zrtVX
kAwYHbIZLo925NjFyPuuxhWiCotKenl8dZefB8aB81rjYuIMnCJ0GQus+JG8
TJyEesNdK/q8HD5h1kCRSzMHD1+Ra3z/1+FFIwARAQABzR1BZG9iZSBQU01S
VCA8CHNpcnRAYWRvYmUuY29tPSLBewQQAQgALwUCWb/YrWUJAeEzgAYLCQgH
AwIJEIbAD8Kvh3YWBbUIAgoDFgIBAhkBAhsDAh4BAADk2A//f+6PFzg4VmLI
PzsTZPoqPR/lXlZ7RIYbQosHvsFwyW0WWX1uIlsEeD5Qo7HQ6NNMAOW51Js
wFvFOWIa9U6SHRoU1kGTSESReOq5HnXe4DcBubsKmoMS68PuiZ88wYOIM4Up
9V9PUuaue0U4oSrYHnH5qBOqurtv8wO5Cq4uTwnfnjN7n4OH0++2910PJ68B
6+kMuQyG4swmxsZhlj1qGMHcs0c/BuI3W+n5w+xLM7N5jjCTjNXR+tGmstdm
RPEoLWOso+ZFwfNW0CLKjYUahp3p6H9x8R13wrp2re0GhqKRgt3D4UCaQsPs

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](#)

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

```
-----BEGIN PGP PUBLIC 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+OQlvC
Nm8vIGnQZWQ30WqnH/UFoh3RPJ+WqnDq88NmQBq8I4aNV4u8MqoObd/zrtVX
kAwYHbIZLo925NjFyPuuxhWiCotKenl8dZefB8aB81RjYuIMnCJ0GQus+JG8
TJyEesNdK/q8HD5h1kCRSzMHD1+Ra3z/1+FFIwARAQAB/gkDCA7HXpjNu7yW
YBVIglTandp2qwxLZTA0Jm3YMOwvBojE4ZDL41VZBh2sBphQ15CLulx7MUrD
=QOc7
```

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

-----BEGIN PGP PRIVATE KEY BLOCK-----

Version: Mailvelope v1.8.0

Comment: https://www.mailvelope.com

```
-----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+OQlvC
Nm8vIGnQZWQ30WqnH/UFoh3RPJ+WqnDq88NmQBq8I4aNV4u8MqoObd/zrtVX
kAwYHbIZLo925NjFyPuuxhWiCotKenl8dZefB8aB81RjYuIMnCJ0GQus+JG8
TJyEesNdK/q8HD5h1kCRSzMHD1+Ra3z/1+FFIwARAQAB/gkDCA7HXpjNu7yW
YBVIglTandp2qwxLZTA0Jm3YMOwvBojE4ZDL41VZBh2sBphQ15CLulx7MUrD
=QOc7
```

Do not do this

April 2014
March 2014
February 2014
January 2014
December 2013
November 2013
October 2013
September 2013
July 2013
June 2013
May 2013
April 2013
March 2013
February 2013
January 2013
December 2012
November 2012
October 2012
September 2012
August 2012
July 2012
June 2012
May 2012
April 2012
March 2012
February 2012
January 2012
December 2011
November 2011
October 2011
September 2011
August 2011
July 2011
June 2011
May 2011
April 2011
March 2011
February 2011
December 2010

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: What if everyone did a few verifications. 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).

My public key

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

```
mQENBFHMmcgABCAC9WrYDO6K2L3VHYi4eHN6suHLqMpl+SO+IUTuLEVnUzIoXAUXH
KozHejfv/9XoG8j933ZtszXKCog3aMESe0E0z6fNGfolvaCe5B4jwqJt8NHwb5L
B2dnq0CplgXcN2GJxfEHUaf27COSobCJxPMeshUh4ZHke+g6DatmiEtBpVp41Ot
1zgxdlMQkgb2H2xw28RYfYkdDouetelkOrFLrCy9ZF9KdMhA1eBh94KnwIQshdiZR
QYEX25+M8cKCb++Rc9H6an7EG9WHOFRW40UsY52OfveOyfQPzkkRto7u2339hvH0
B/h+7xLM6FQbOUZQ9BD5w7IQHgYtXJVsuJ0dABEBAAG0IktbWkgVmfuaVWVhIDxr
dmFuaVWVhQGluzi5lZC5hYy51az6JAT8EEwEIAckFAIYKYvECGyMFCQlMAYAHcWkl
BwMCAQYQYCAIJGsfEgIDAQIeAQIXgAAKCRCTdsxl9/HZffG+CACShuKxje3QAqew
GWh8K4gCdiY0xDqJwq3PHxmyhZmQeN/1a1KcOrljl2b+Q75/5t+EgXOHpR0PlxfG
Iz6zOEpf6A18iFxx3JgQZdwPD0jtBiWNPoYMeBGTglvEYG3so2VueQoeXcq3dbYp
5vstVxtD+TKHQ5CiolT75P2bzYq/XLT5albNqHqQDPcToODgbRH+fvqsRr7yeaef
JaPnxX0+1L33t2QY9zctiGyebwrvHMRlPBj2VYCDzQk7uQ5eFh42hsMgOmzLQD4
YiGr5weIMfWAvxZOaRxEa9Vf48jiWvrXuJ8YfHWS0hEScNocYC2P8q20JjwwE26T
lpdtrwCqtB1LYW1plFZhbmlIYSA8a2FtaUB2YVW5pZWUuY29tPokBQgQTAQIALb
IwUJCWYBgAcLQgHAWlBBhUIAgkKcWQWAgMBAh4BAheABQJWCmMeAhkBAaOJEJN2
zGX38dl9JIAIAIW0rxrlYsrnKS6CbW8MgTxxTDOXA Ct1b7F0W0QZHSklUQHcE+a
XBYib1A5uHaatLfyeXaD3qMEoZnQHoYMGE0GKu00wWsbhfoQzHPgwrLkD1i75M
Blbaww0KW0Vb9e4AkMakXJCnF5BXeo6AHLR2v15V205DikVnCRXocKtu8b7LnkM
cLn7oLobr1de1uyKoNzbSnO/vpKDJp0/EY5yUeV9olypZy/6wFQBehg1sXye6znO
9wb9uUusu9+/P8pz4JILMDSevjft7zSRSl/YP3fOfZ6N4bc+KodwPM7u5lyoeu9zh
pzibv3ge7VhH2xlWz8vYZ/2xt1345tWRRMOJAhwEEwECAAYFAITnSpEACgkQjyxM
p99tBt2B8A/+OplzOsQbQJB8yxti4l7PpD1weJdf3a81Vhm7JyX/XY66ypfdt3w
XmFRUuIrwzY1NebWNCRQHzQvRv/VJwjbTux+Q3HsjikIHbE7iCiQXXtTRk0Eny
2nudcJG12v03C3B2JCucEw6esF1x79Pl/Pv2+6tgUBKMDfOpsB2vbtqrHnmAYKL
4lQBfH1YSJgnzwo2Jkh0hcHdF90Zem1eMeiDEeVkh63893N8Swk5fBKdTj+SKZ/L
rQEIBBlpMR9BmeY6bPvWruycVK0nIMR80G9iFABxjTpWBL8aGk6EeVK5EqYDGvkd
ZlarK84r+KU1KD5IfgOCN7nhwgy7VImE68caZHSRiPWZP1fvVMhydiRjWsoU56
InfVU3nxH+ZYthPbY0T86leGSchBT5K/fBQvbjhrRTbTFwvjSifb9efWylD1994
nzP6cNorir3GlpsT8gPgBB2/NjxaWiM6y3X1az1vRnsunQHuyKkFWPZwnEvDJYaC
NN/3jWcbhLFwKBDsaHps2+1meFP0oJFvNetzp2bjT9a9pXaQ6KhOmo5DnhLcaV97
bFBpsUuBGaYZTSS05x1RdXHqpEbgap8dtuHhVvJw9QYDQBJr0K4aKyG9qqMD8cta
PI/FadyAqwH8Nw9efqAK+RQxSVUaue9BYEnbIRpsDK6MKp3YMFmu5ki5AQOEucxy
AAEIALyXyY8G2ZaTJdpdGcRhmlqOOSUlzPV7/5E5BbYKBNu4KU3nX+JLVcF5jxPQ
42c7i/WRVxE1BJTiarKGsEvCi94TTXSIUKAt3T1oGBtXmGvqbGBq8lSGl1UTwdf
5yu50JyRSf2fqRND6P/2eHNXejDutdvHUXiUt8h9MuUO/ipD0DnwlVmnAATJHA+R
Zqw60NpyjRGzvr3iuWUwe4PtyJDI3ELAFkbp/Nac5TluVHRNOWNpIclJhM5zHuB
QQb3G/EsCn2PQZ5w5SDzavF2SpvQfdqxYpDaTLAXtF+wsJL5iaUjxwRgJPodbCZf
2Tozd7h9MxTgDIPKJ8eLG8ogcMAEQEAAyKBJQYAQAIDwUCUcxyAAlbDAUJCWYB
gAAKCRCTdsxl9/HZf5+hB/9BJqSmlgcoHFxb1PVIKxekzL8+WVm5Pk/EgMSQLZ2
HX4p3ial5PEPcYgUw9YnaG4i00dwJGw5/daTWRrTzcnKd8YqoP+DU0t96HZDSu3m
mCzE9NVAQYboFbVmGOx0eo627UBSvFqaXvABDYkoR8B0TnKhrQFwxkZVb30hKwD
TgAFjOGIZiE6uAdSt231tFaq0bizYfe5AVXRqro20xBqNbaJNqs3SW0D831Syvdu
lIOBx83/R0gg7hUkl6F2vzXicWmUwFSXRggCSbLosHsP6isBWwwlHeRmna/aQab
YKG3gbV9iycZAS31gbogVLAZqNSWWhp8vVIEE28Fyf/Ed
=x5FK
```

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

Wonderful idea in theory. But verifying those long keys is hard... also I don't actually trust most of you 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

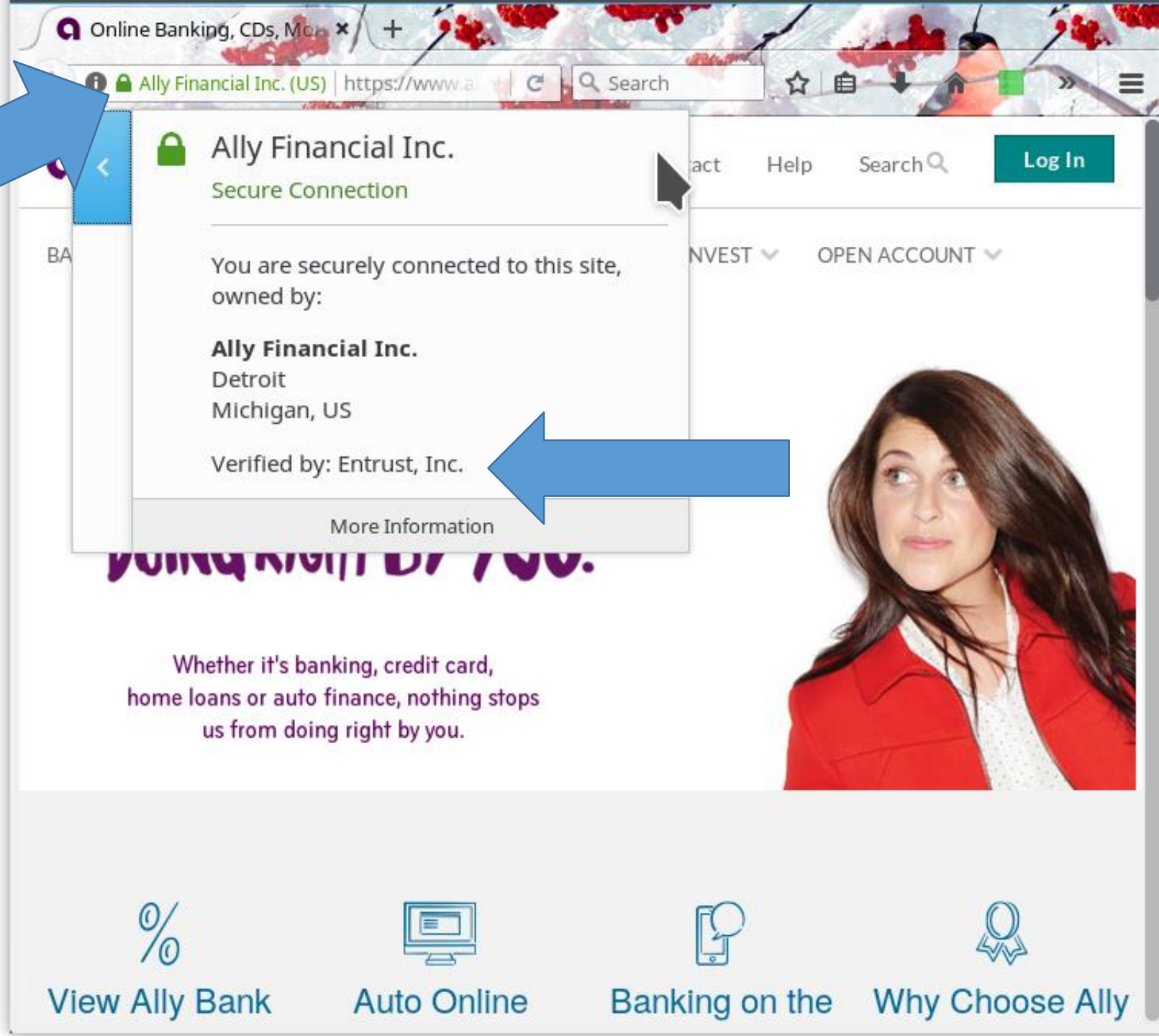
Field Value

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



You can see
lots of
details
about any
encrypted
connection.

Page Info - https://www.ally.com/

General Media Permissions **Security**

Web Site Identity

Web site: **www.ally.com**
Owner: **Ally Financial Inc.**
Verified by: **Entrust, Inc.**

[View Certificate](#)

Privacy & History

Have I visited this web site before today?	Yes, 10 times	
Is this web site storing information (cookies) on my computer?	Yes	View Cookies
Have I saved any passwords for this web site?	No	View Saved Passwords

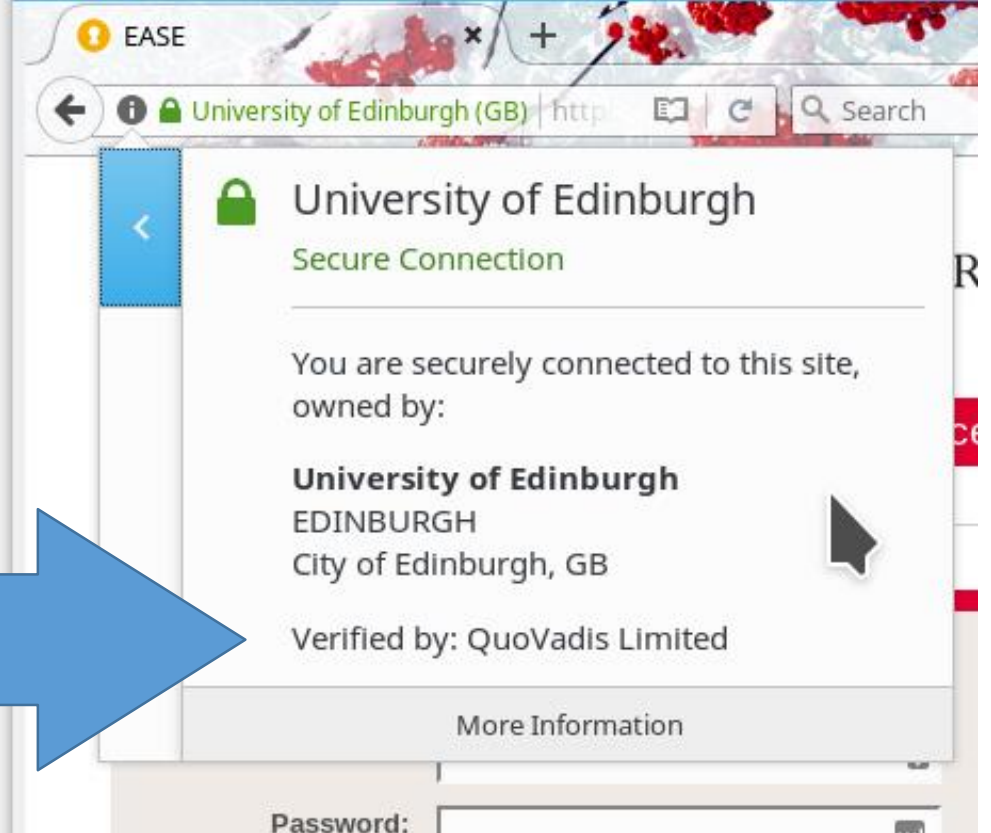
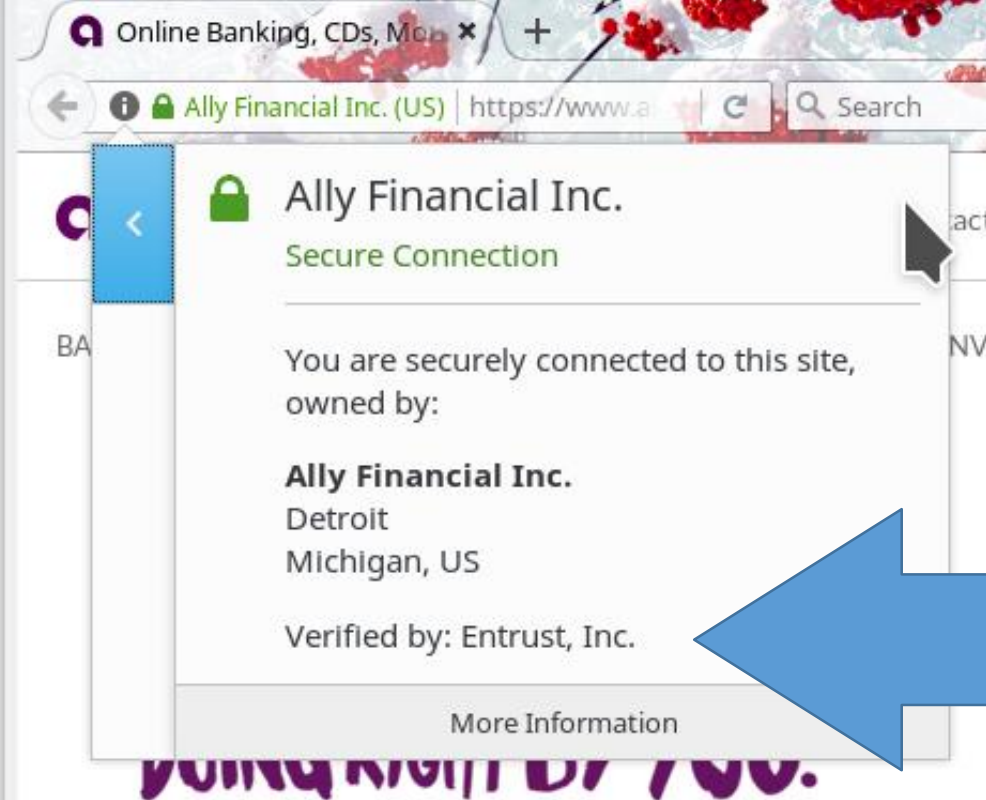
Technical Details

Connection Encrypted (TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, 256 bit keys, TLS 1.2)

The page you are viewing was encrypted before being transmitted over the Internet.

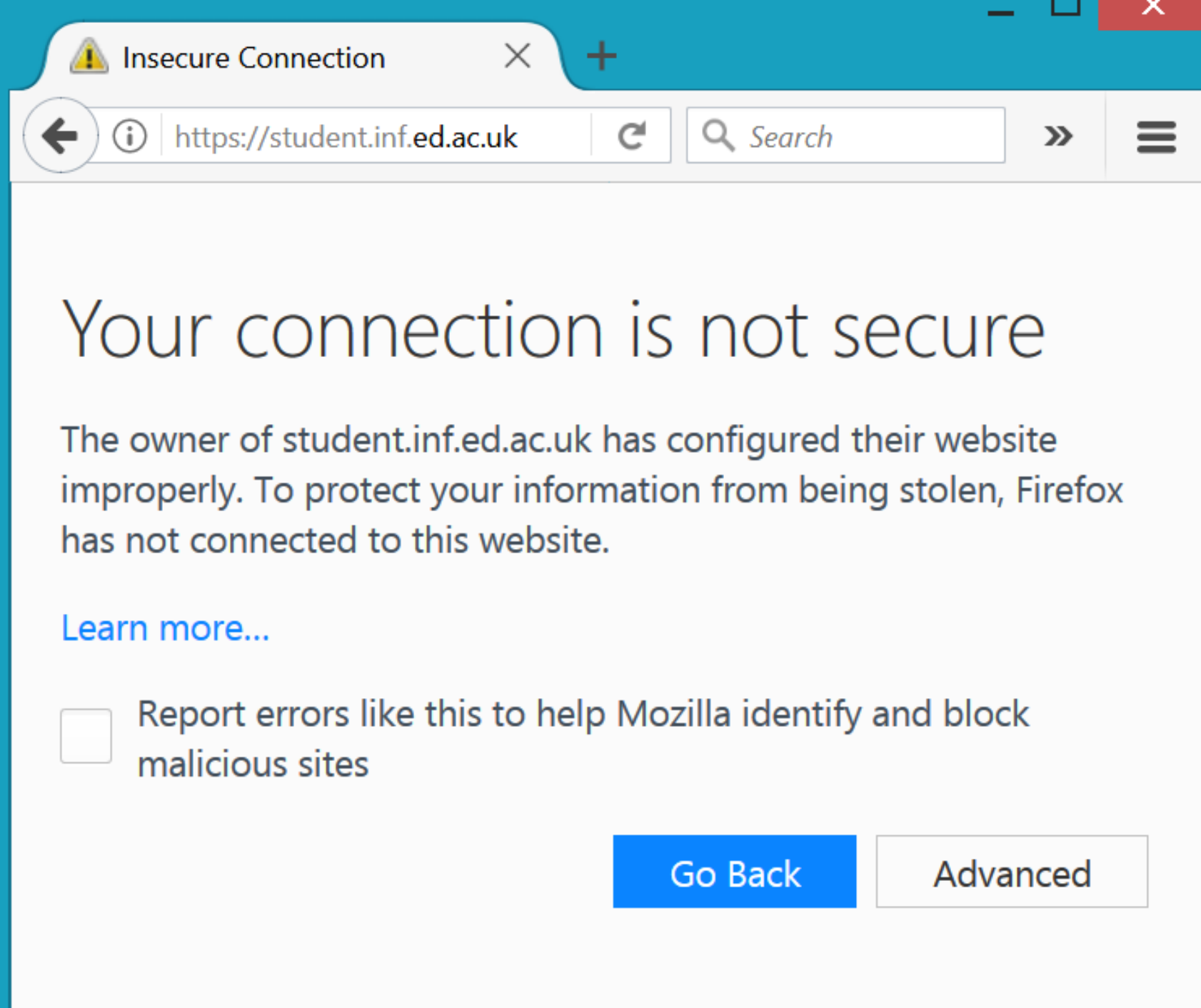
Encryption makes it difficult for unauthorised people to view information travelling between computers. It is therefore unlikely that anyone read this page as it travelled across the network.

[Help](#)

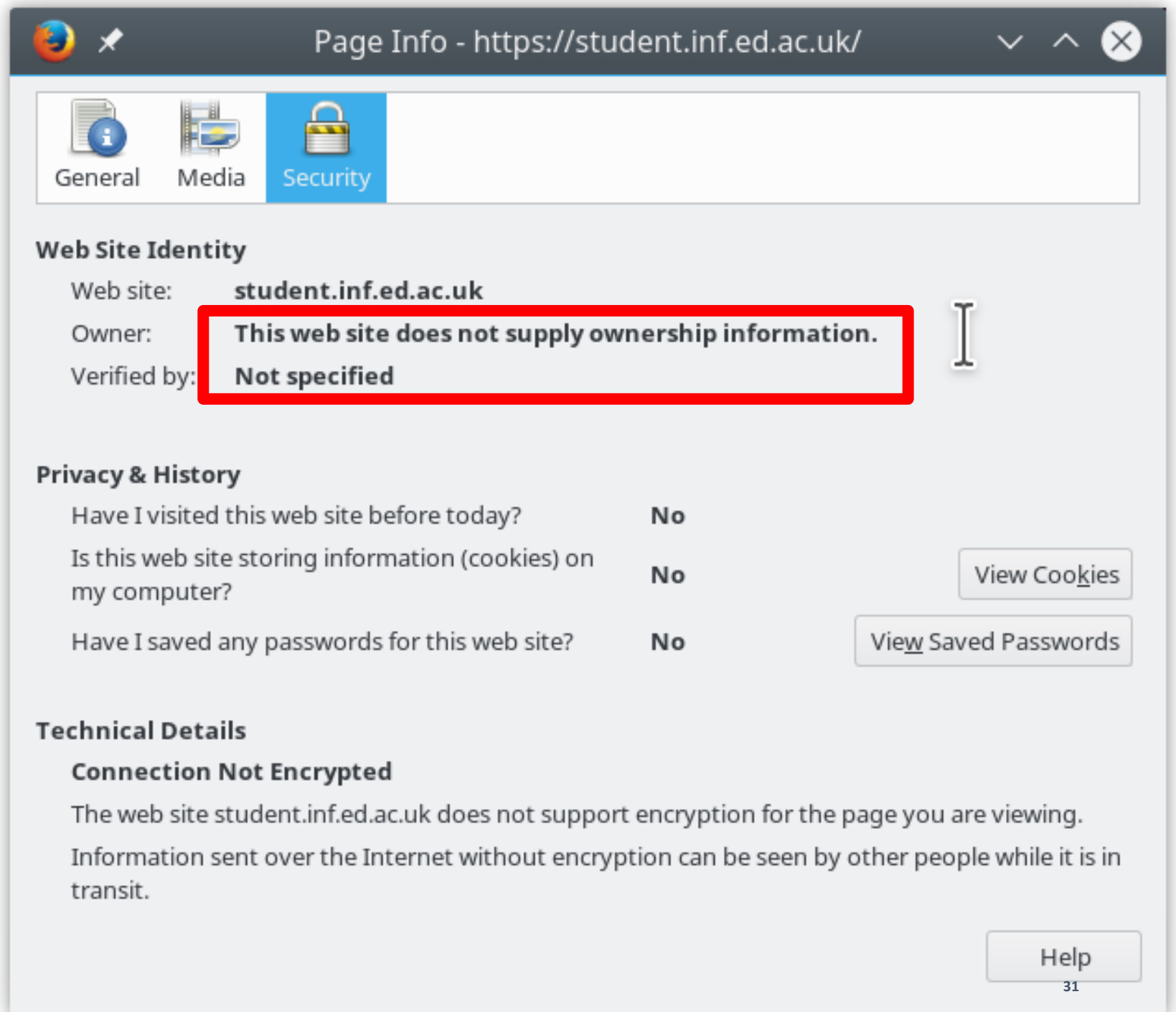


But now don't we just have the same problem again?
How does the browser know which Certificate Authorities to trust?

Clearly some
Certificate
Authorities are
trusted and some
are not.

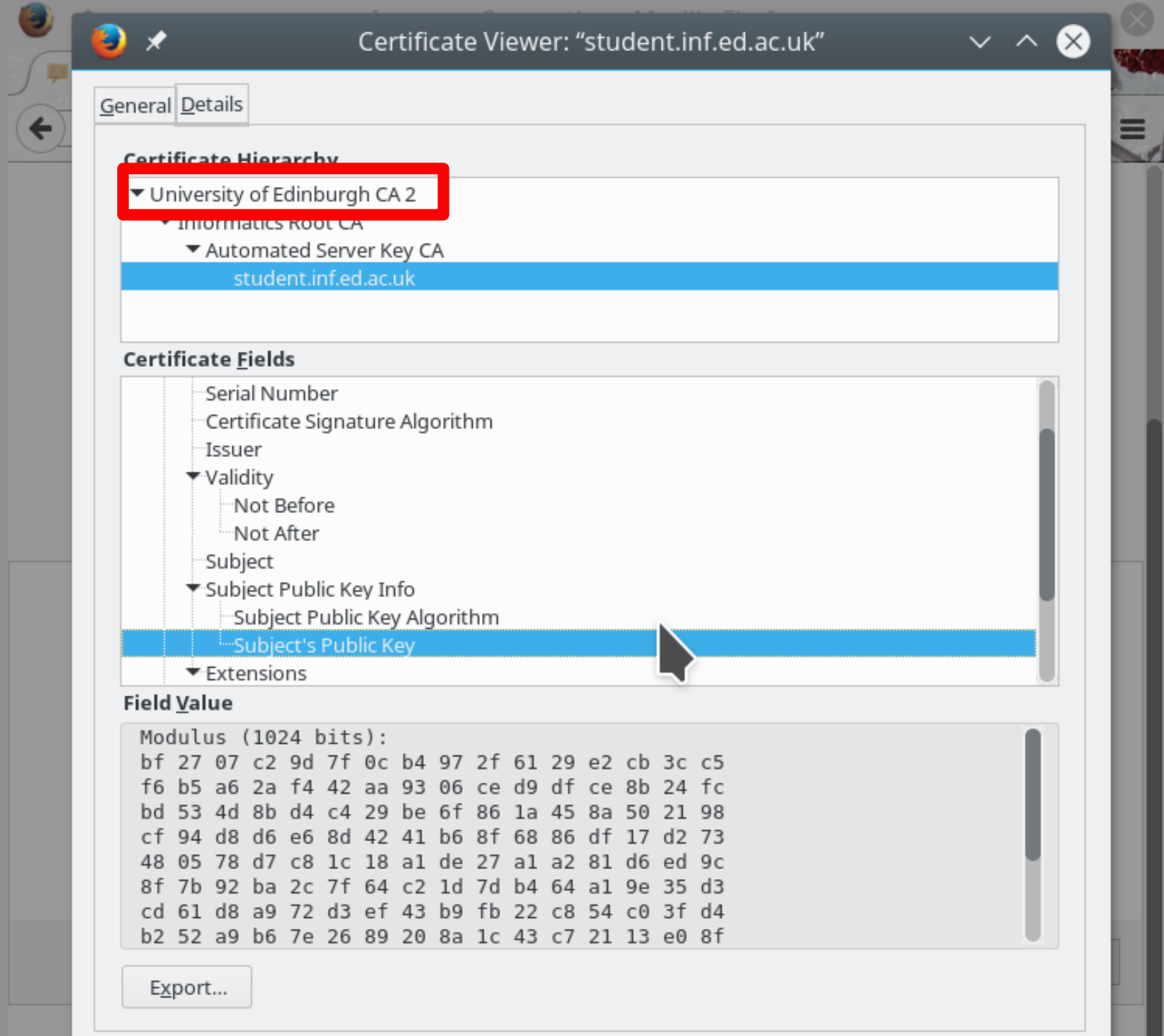


Errors on
student.inf.ed.ac.uk
are a bit easier to
understand though,
identity information
is missing...



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.



**DICE machines will never give you an error on
student.inf.ed.ac.uk but your personal laptop will.**

What is the difference?

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

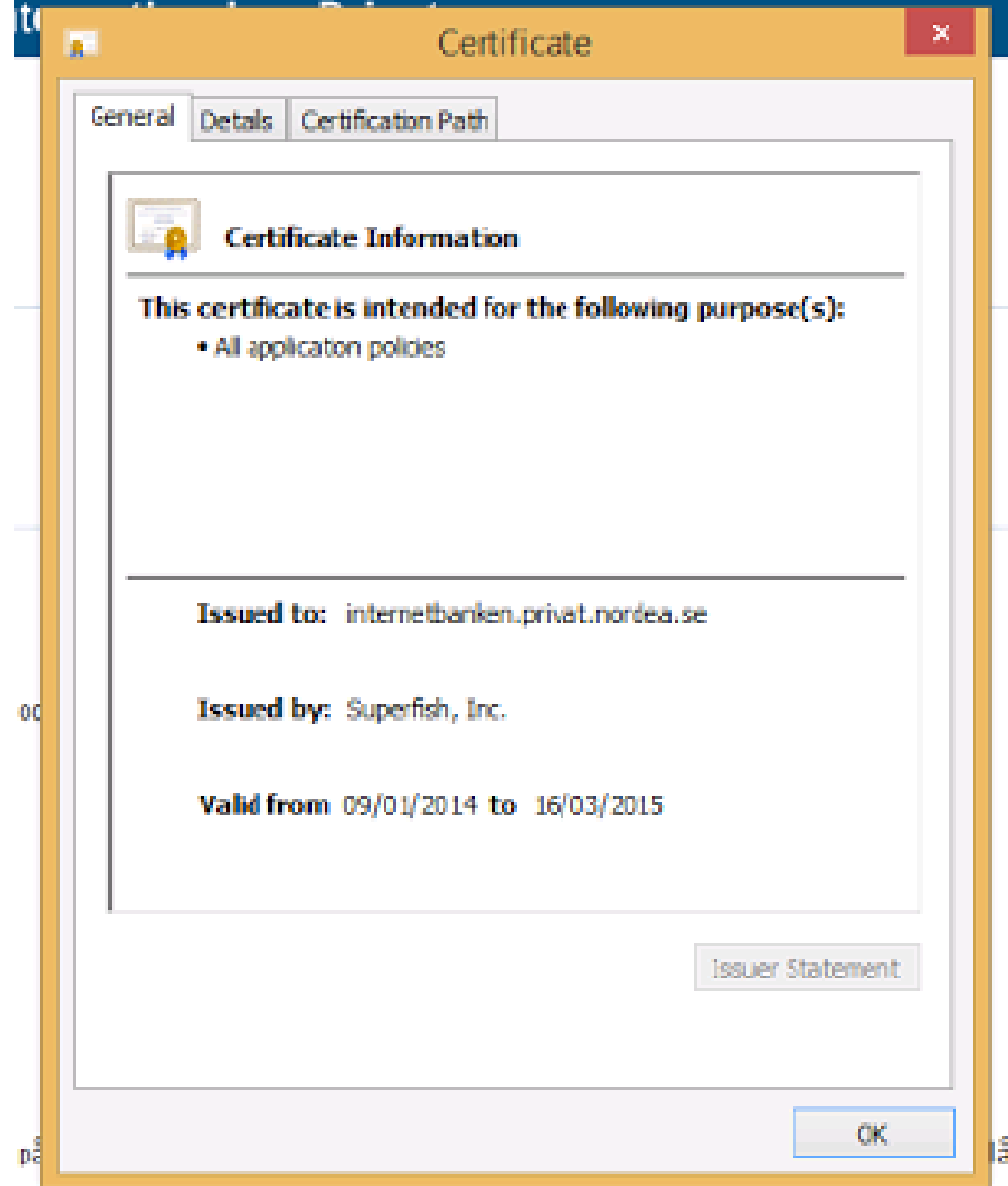
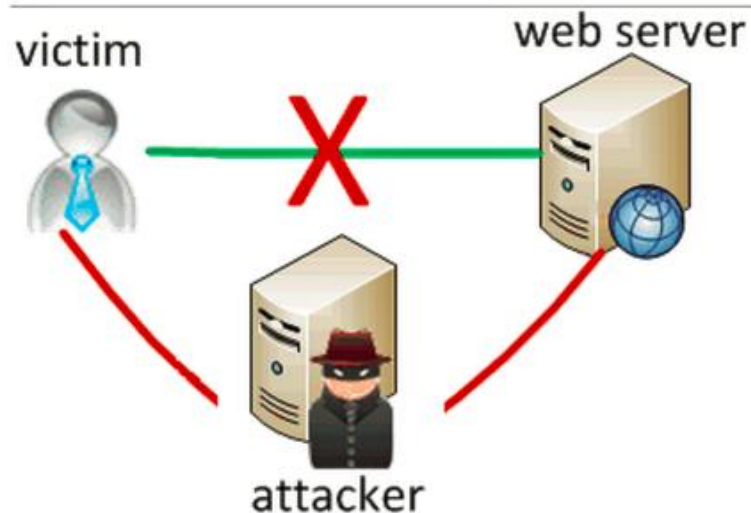
RISK ASSESSMENT / SECURITY & HACKTIVISM

Lenovo PCs ship with man-in-the-middle adware that breaks HTTPS connections [Updated]

Superfish may make it trivial for attackers to spoof any HTTPS website.

by Dan Goodin - Feb 19, 2015 11:36am EST

[Share](#)
[Tweet](#)
[333](#)



YouTube

https://www.youtube.com

10.240.31.12
*.google.com

 *.google.com
Issued by: 10.240.31.12
Expires: Monday, March 9, 2015 at 5:00:00 PM Pacific Daylight Time
This certificate was signed by an untrusted issuer

Details

Subject Name	
Country	US
State/Province	California
Locality	Mountain View
Organization	Google Inc
Common Name	*.google.com
Issuer Name	
Country	US
State/Province	IL
Organization	Gogo
Common Name	10.240.31.12

Recommended

Popular Music V



Adrienne Porter Felt

@__apf__



Following

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

Questions?