

HTTPS Explained

DR KAMI VANIEA

http versus https

A screenshot of a web browser window. The address bar shows the URL www.ally.com. A blue arrow points from the left towards the address bar. The page content includes the Ally logo, navigation links for Ally Bank, Auto Financing, About Ally, and various banking products like Savings, CDs, IRAs, Checking, and Banking with Ally. Contact information for the bank and auto financing is also present.

A screenshot of a web browser window showing a secure connection. The address bar displays the URL <https://www.ally.com>, preceded by a green lock icon. A blue arrow points from the right towards the address bar. The page content is identical to the first screenshot, featuring the Ally logo and various banking product sections.

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.

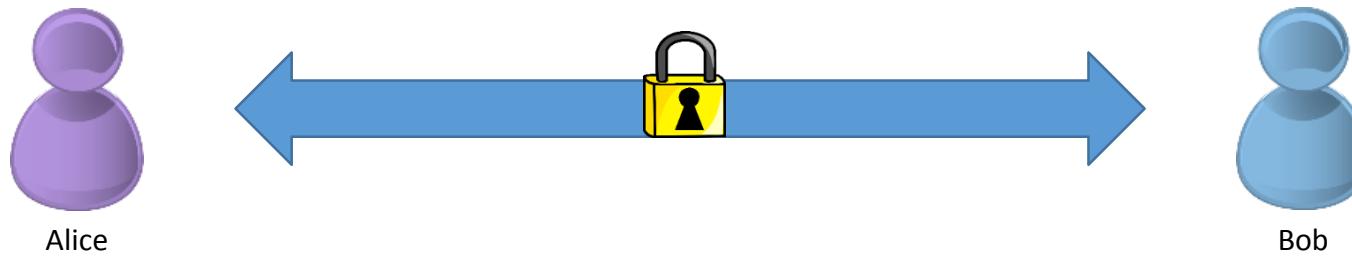
2. **Knowing who** you are communicating with

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

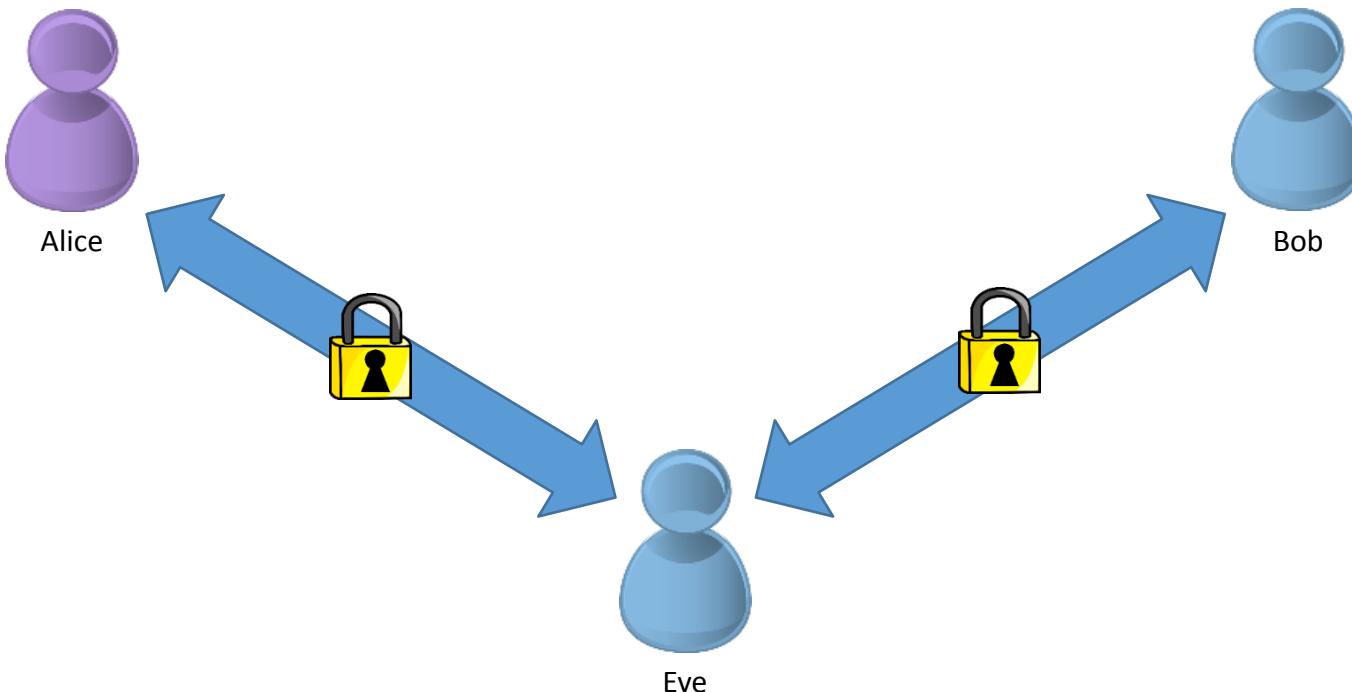
Alice wants to talk securely with Bob



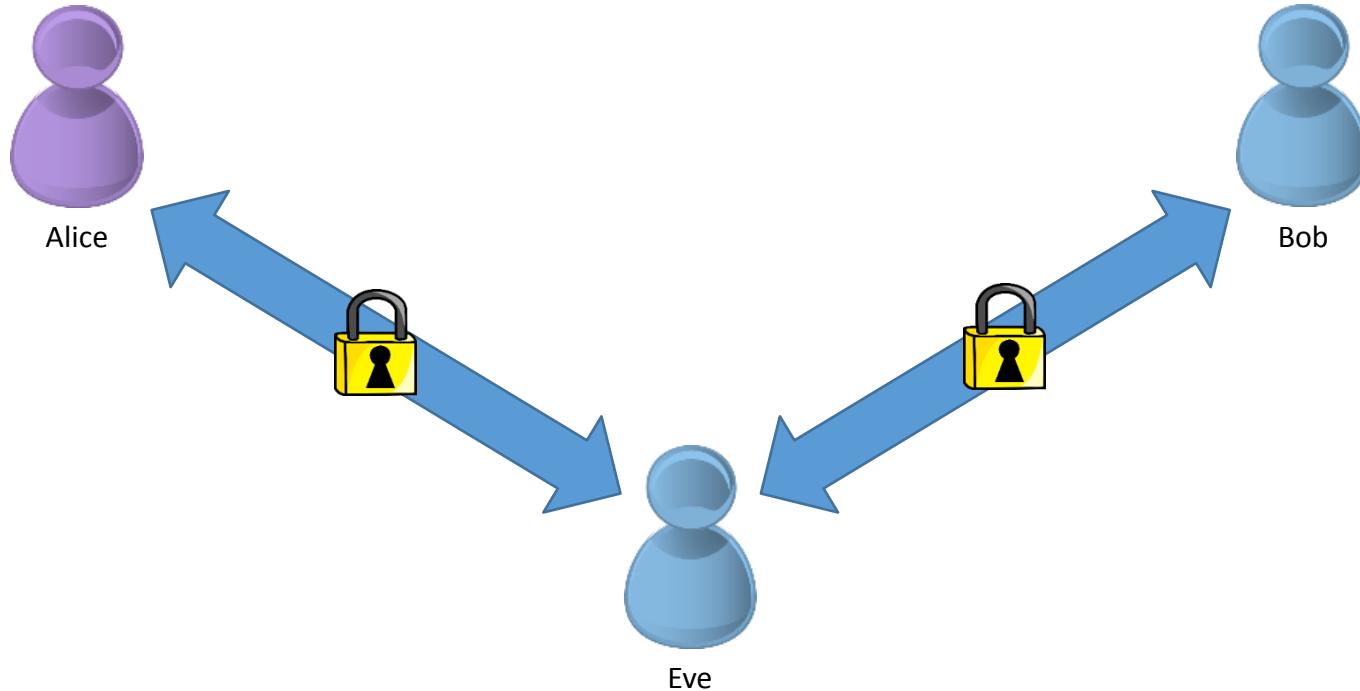
She can encrypt the connection (1)



**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

mQENBFHMcgABCAC9WrYDO6K2L3VHyi4eHN6suHLqMpJ+SO+IUTuLEVnUzloXAUXH
KozHejfV/9XoG8j933ZtszKCCog3aMESe0E026fNGfolvaCe5B4jwqoJt8NHwb5L
B2dnq0CplgXcN2GjxfEHHUaf27COSobCxPMeshUh4ZHke+g6DatmiEtBpVp41Ot
1zgxdMQkgb2H2xw28RYfYkdDoutelkOrLrC9ZKdMhA1eBH94KnwlQshdiZR
QEYEX25+M8cCb++Rc9H6an7EG9WHOFRW40Usy520fveOyfQPzkkRto7u2339hvH0
B/h+7xLM6FQbOUZQ9BD5w7IQHgTjXJVsUj0dABEBAAG0IkthbWkgVmFuawVhIdxr
dmFuaWvhQGluzi5lZC5hYy51az6JAT8EEwEIACkFAIYKyvECGyMFCQImAYAHcwkl
BwMCAQYVCAIJCgsEFgIDAQleAQXgAAKCRCTdsxI9/HZffG+CACShuKxje3QAqew
GWh8K4gCdi6A18FX3jQzdwPDojtBiWNPoYMeBGTglvEYQ3so2VueQoeXcq3dbp
5vstVxtb+TKHQ5CioltT75P2bzYq/XLT5albNQhQDPCTo0DgbRH+FvqsRx7yeaef
JaPnxX0+1L33t2QY9zctiGyebwrvHMrIPBJ2VYCdZQkJ7uQ5eFh4ZhsMgOmzLQD4
YiGr5weIMFwAvxZoArxEa9Vf48jWvxru8YfHW50hEscNOcyC2P8q20JuwvE26T
lpdrwCqtB1LYW1pIFZhbmllUSA2aFtaUBZWy5pZWEUy29tPokBQgQTAQIALAlb
IwUJCWYBgAcLQgHAWlBBhUIAgkCwQAgMBAh4BAheABQJWCmMeAhkBAAGjeJN2
zGx38d19JJAIW0rxrlYsrmKS6CbW8MgTxTDoxA Ct1b70W0QZHSkluQhEc+a
XBYib1A5uHaatlFyjeXaD3qMeEznQHoYMG0GKu00wWsbhfoQzHPgwzRLkD1i75M
B1baww0KWoVB9e4AkMakXJcnF5Bxeo6AHRL2v15V205DikVnICRXocKtu8b7LnkM
cln7oLbr1de1uyKoNbzSn0/vpKDjp0/EV5yUev90lypZy/6wFQBBehglsXye6znO
9wb9uUsu9+/P8pz4JILMDSevitT7zSRS/YP3ofZ6N4bc+KODwPM7u5lyoeu9zh
pzibv3ge7vhH2xlWz8vYZ/2xT1345tWRRMOJAhweEwECAAyFAITnSpEAcgkQjyxM
p99tBt2B8A/+OpIzOsQbQJB8yxti4I7PpD1weJDf3a81Vhm7jyXE/Xy66ypfdt3w
XmFRUlrwezY1NebWNCRQHzQvRv/VjwjbTUx+Q3HsjlkIHbE7iCiQXXtTRk0Eny
2nudcjGl2v03C3B2jCucEw6esF1x79PI/Pv2+6tgUBKmDfOpsB2vbtrqrHnmAYKL
4IQBFH1YSJgnzw02Jkh0hcHdf90Zem1eMeIDeVhK63893N8Swk5fBKdTj-SKZ/L
rQEIBBlpMR9BmeY6bPvWRuycvK0nIMR80G9iFABxjTpWBL8aGk6EeVK5EqYDGvd
ZiarK84r+KU1KD5fgOCN7nhwgY7VmE68caZHSRIPWZP1fVMMhydiRJv8WsoUs6
INFVU3nxH+ZYthPbY0T86leGSchBT5K/fBQbjhrRTfwvzSifb9efWylD1994
nzP6cNorir3GipsT8gPgBB2/NjxaWiM6y3X1az1vRnsunQHuyKKFWPZwnEvDJYaC
NN/3jWcbhLFwKBDSaHps2+1meFP00JFvNetzp2bjt9a9pxQa6KhOMo5DnhLcaV97
bFBpsUuBGAyZTSS05x1RdXhqEbgap8dtuHhVv9WQYDQBJr0K4aKyG9qqMD8cta
Pl/FAdyAqwH8N9efqAK+RQxSVUaae9BYEnblRpzDK6MkP3YMFmu5ki5AQOEYDGV
AAEIALyXYgG2zaTDJpdGcRhmlqOOSULzPv7/5E5BbYKBNU4KU3nX+JLvcF5jPQ
42c7i/WRVx1EBTiarKGsEvCi94TTXSIUKAt3T1oGBtXmGvqbGBq8ljSGI1UTwdF
5yu50JyRSf2fqRND6P/2eHNxejdUtdvhUXIUt8h9MuUO/tpD0DnwlvMnAATJHA+R
Zqw6oNpyjRGzvriiuWUwe4PtyjDI3ELAFkbp/NAc5TluVHRHNOWNplclJhM5zHuB
QQb3G/EsCn2PQZ5w5SDzavF2SpvQfDqxYpDaTLAXtF+wsJL5iaUjxwRgjPOdbCzf
2Tozd7h9MXtGJdIPK8jeLG8qgcMAEQEAAyKbQQYQAQIAdwUCUcxxyAAlbDAUICWYB
gAAKCRC7dsxI9/HZfs+hB/9BjQsMlgcoHFxnb1PVIKxekzL8+WVm5Pk/EgMQSL22
HX4p3ial5PEPCygyUw9YnaG4i00dWJGw5/daTWRrTzcnKd8YqoP+DU0t96HZDSu3m
mCzE9NVNAQYboFbVmGOxeo627UBsvFqaXvAxBDYkoR8B0TnKhrQfwXkZVb30hKwD
TgAfjOGiZiE6uAdST231tFaQobizYfe5AVXRqro20xBqNbajNqs3SW0D831Sydv
IIObx83/R0gg7hUkL6F2vzXicWmUwFSXRRggCsBlosHsP6isBWhwvIHeRmna/aQab
YKG3gbV9iyczAS31gbogVLAZqNSWhp8vIEE28Fyf/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

```
mQENBFHMcgABCAC9WrYDO6K2L3VHyi4eHN6suHLqMpJ+SO+IUTuLEVnUzloXAUXH  
KozHejFv/9XoG8j933ZtszKCog3aMESe0E026fNGfolvaCe5B4jwqoJt8NHwb5L  
B2dnq0CplgXcN2GjxfEHUuaF27COSobCxPMeshUh4ZHke+g6DatmiEtBpVp41Ot  
1zgxdMQkgb2H2xw28RYfYkdDoutelkOrLrC9Z9KdMhA1eBH94KnwlQshdiZR  
QYEX25+M8cCb++Rc9H6an7EG9WHOFRW40UsY520fveOyfQPzkkRto7u2339hvHO  
B/h+7xLM6FQbOUZQ9BD5w7IQHgYtXJVsUj0dABEBAAG0IkthbWkgVmFuawVhIDxr  
dmFuawVhQGluzi5IZC5hYy51az6JAT8EEwEIACKAYKyvECGyMFCQImAYAHcwkl  
BwMCAQYVCAIJCgsEFgIDAQleAQIxgAAKCRCTdsx9/HZffG+CACShuKxje3Qaqew  
GWh8K4gCdi6A18FX3jgQzdwPD0jtBiWNpOyMeBG7tgIeyG3so2VueQoeXcq3dbYp  
5vstVxtb+TKHQ5CioltT75P2bzYq/XLTsalbNQhQDPCTo0DgbRH+FvqsRx7yeaef  
JaPnxX0+1L33t2QY9zctiGyebwrvHMrlPBj2VYCDzQkj7uQ5eFh4ZhsMgOmzLQD4  
YiGr5weIMFwAvxZoArxEa9Vf48jiWvruxu8YFHWS0hEscNOcYC2P8q20JwwE26T  
lpdtrwCqtB1LYW1pIFZhbmllUSA2FtaUB2YW5pZWEmY29tPokBQgQTAQIALAlb  
lwUJCWYBgAcLQgHAwIBbhUIAgkKCQgKwAgMBAh4BAheABQJWCmMeAhkBAAjOEJN2  
zGx38d19JJAIAlW0rxlYsrmKS6CbW8MgTxzTDXaCt1b70W0QZhsklUQhEc+a  
XBYib1A5uHaatlFyjeXaD3qMEoZnQHoYMG0GKu00wWsbhfoQzHPgwzRLkD1i75M  
Blbaww0KWoVB9e4AkMakXJcnF5Bxeo6AHRL2v15V205DikVnlCRXocKtu8b7LnkM  
cln7oLbr1de1uyKoNzbSn0/vpkDjp0/EV5yUeV9olypZy/6wFQBBehglsXye6znO  
9wb9Usu9+/P8pz4JILMDSevjtT7zsRS/YP3f0zC64bcKODwPM7u5lyoeu9zh  
pzibv3ge7vhH2xlWz8vYZ/2xT1345tWRRMOJAhweEwECAAyFAITnSpEACgkQjyxM  
p99tBt2B8A/+OpIzOsQbQJB8yxti4I7PpD1weJDf3a81Vhm7jyXE/Xy66ypfdt3w  
XmrFUlrwezY1NebWNCRQHzQvRv/VjwjbTUx+Q3HsjlkIHbE7iCiQXXtTRk0Eny  
2nudcjGl2v03C3B2jCucEw6esF1x79PI/Pv2+6tgbUKmDfOpsB2vtqrhNmAYKL  
4IQBFH1YSJgnzw02Jkh0hcHdf90Zem1MeIDeEvkH63893N8Swk5fBKdTj-SKZ/L  
rQEIBB1pMR9BmeY6bPwRuyCn0nlMR80G9iFABxjTpWBL8aGk6EeV5EqYDGvd  
Zlark84+rKU1KD5IfgOCN7nhwgY7VlmE68caZHSRIPWZP1fVMMhydiRJv8WsoUs6  
INFU3nxH+ZythPbY0T86leGSchBT5K/fBQvjhrRTbTFwvjzSifb9efWylDi994  
nzP6cNorir3GipsT8gPgBB2/NjxaWiM6y3X1az1vRnsunQHuyKKFWPZwnEvDJYaC  
NN/3jWcbhLFWKBDSAHPs2+1meFP0oJFvNetzp2bjT9a9pxaQ6KhOMo5DnhLcaV97  
bFBpsUuBGAyZTSS05x1RdXhqpEbgap8dtuHhVvJw9QYDQBJr0K4aKyG9qqMD8cta  
Pl/FAdyAqwH8Nw9efqAK+RQxSVUaae9BYEnblRpzDK6MkP3YMFmu5ki5AQOEUCxy  
AAEIALyXYg8G2zaTDJpdGcRhmlqOOSUlzPV7/5E5BbYKBNU4KU3nX+JLvcF5jxPQ  
42c7i/WRVx1EBTiarKGsEvCi94TTXSIUKAt3T1oGBtXmGvqbGBq8ljSGI1UTwdF  
5yu50JyRSF2fqRND6P/2eHNxejdUtdvhUXIUt8h9MuUO/tpD0DnwlvMnAATJHA+R  
Zqw6oNpyjRGzvri3iuWUwe4PtyjDI3ELAFkbP/NaC5TluVHRHNOWNplclJhM5zHuB  
QQb3G/EsCn2PQZ5w5SDzavF2SpvQfDqxYpDaTLAXtF+wsJL5iaUjxwRgjPOdbCzf  
2Tozd7h9MXtGJdIPKj8eLG8ogcMAEQEAAYkBQQYAQIAdwUCUcxxyA1lbdAUJCWYB  
gAAKCRCTdsx9/HZfs+hB/9BjQSmIgcoHFXnb1PVIKxekzL8+WVm5Pk/EgMQSL22  
HX4p3ial5PEPCygUw9YnaG4i00dWJGw5/daTWRrtTzcnKd8YqoP+DU0t96HZDSu3m  
mCzE9NVNAQYboFbVmGOx0eo627UBsvFqaXvAxBDYkoR8B0TnKhrQFwXkZVb30hKwD  
TgAfjOGIZiE6uAdST231tFaQ0bizYfe5AVXRqro20xBqNbajNs3SW0D831Syvdv  
IIObx83/R0gg7hUk16F2vzXicWmUwFSXRsrggCsblLosHsP6isBWwvIHeRmna/aQab  
YKG3gbV9iyyczAS31gbogVLAZqNSWhp8vIEE28Fyf/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

```
mQENBFHMcgABCAC9WrYDO6K2L3VH yi4eHN6suHLqMpJ+SO+IUTuLEVnUzloXAUXH  
KozHejfV/9XoG8j933ZtszKCog3aMESe0E0z6fNGfolvaCe5B4jwqoJt8NHwb5L  
B2dnq0CplgXcN2GjxfEHUuaF27COSobCjxPMeshUh4ZHke+g6DatmiEtBpVp41Ot  
1zgxdMQkgb2H2xw8RYfYkdDoutelkOrLrCy9ZF9KdMhA1eBH94KnwlQshdiZR  
QEYEX25+M8cCb++Rc9H6an7EG9WHOFRW40UsY520fveOyfQPzkkRto7u2339hvH0  
B/+h7xLM6FQbOUZQ9BD5w7IQHgTjXVsUj0dABEBAAG0IkthbWkgVmFuawVhIdxr  
dmFuawVhWQGluzi5lZC5hYy51az6JAT8EEwEIACkFAIYKyvECGyMFCQImAYAHcwkl  
BwMCAQYVCAIJCgsEFgIDAQleAQIxgAAKCRCTdsx9/HZffG+CACShuKxe3Qaqew  
GWh8K4gCdiY0zDqJwq3PHxmyhZmQeN/1a1KcOrlj12b+Q75/5t+EgXOHpRPlxfG  
IZ6zOEpfGA18FX3jgQzdwPD0jtBiVNpOyMeBGTglvEYG3so2VueQoeXcq3db5  
5vstVxtb+TKHQ5Ciolt75P2bzYq/XLTsalbNQhQDPCTo0DgbRH+FvqsRx7yeaeF  
JaPnxXo+1L33t2QY9zctiGyebwrvHMrIPBJ2VYCdZQkj7uQ5eFh4ZhsMgOmzLQD4  
YiGr5weIMFwAvxZOaRx Ea9Vf48jWvxu8YFHWS0hEscNOcyC2P8q20JwwE26T  
lpdtrwCqtB1LYW1pIFzhbmllYSA8a2FtaUB2YW5pZWUeY29tPokBQgQTAQIALAlb  
lwUJCWYBgAcLQgHAwIBbhUIAgkCQwAgMba4BAheABQJWCmMeAhkBAAljeJN2  
zGx38d19JJAIAlW0rxlYsrmKS6CbW8MgTxTDoxA Ct1b70W0QZhsklUQhEc+a  
XBYib1A5uHaatlFyjeXaD3qMEoZnQHoYMG0EGKu00wWsbhfoQzHPgwzRLkD1i75M  
B1baww0KWoVB9e4AkMakXJcnF5Bxeo6AHLR2v15V205DikVnICRXocKtu8b7LnkM  
cln7oLobr1de1uKoNbzSn0/vpKDjp0/EV5yUev9olpzy/6wFQBBehglsXye6znO  
9wb9uUsu+/P8pz4JILMDSevit7zSRSL/YP3f0zFZ64bc/KOdwPM7u5lyoeu9zh  
pzibv3ge7vhH2xlWz8YZ/2xT1345tWRRMOJAhwEEwECAAyFAITnSpEACgkQyxM  
p99tBt2B8A/+OpIzOsQbQB8yxti4I7PpD1weJdf3a81Vhm7jyXE/Xy66ypfdt3w  
XmfRUlrlwezY1NebWNCRQHzQvRv/VjwjbTUx+Q3HsjlkIHbE7iCiQXXtTRk0Eny  
2nudcjGl2v03C3B2jCucEw6esF1x79PI/Pv2+6tgUBKmDfOpsB2vbtrhNmAYKL  
4IQBFH1YSJgnwo2Jkh0hcHdf90Zem1eMeIDeVkh63893N8Swk5fBKdTj+SKZ/L  
rQEIBBlpMR9BmeY6bpWVuycVK0nIMR80G9iFABxjTpWBL8aGk6EeVK5EqYDGvkD  
ZiarK84+rKU1KD5fgOCN7nhwgY7VmE68caZHSRIPWZP1fVMMhydiRJv8WsoUs6  
INFVU3nxH+ZyThPbY0T86leGSchBT5K/fBQvjhrRTfwvzSifb9efWylDi994  
nzP6cNorir3GipsT8gPgBB2/NjxaWiM6y3X1az1vRnsunQHuyKKFWPZwnEvDJyA  
NN/3jWcbhLFwKBDSaHps2+1meFP0ojFNetzp2bjt9a9pxaQ6Kh0mo5DnhLcaV97  
bFBpsUuBGAyZTSS05x1RdXhqgap8dtuHhVvJw9QYDQBJr0K4aKyG9qqMD8cta  
Pl/FAdyAqwH8Nw9efqAK+RQxSVUaae9BYEnblRpzDK6MkP3YMFmu5ki5AQOEUCxy  
AAEIALyXYg8G2zaTDJpdGcRhmlqOOSULzPV7/5E5BbYKBNU4KU3nX+JLvcF5jxPQ  
42c7i/WRVx1EBTiarKGsEvCi94TTXSIUKAt3T1oGbtXmGvqbGBq8ljSGI1UTwdF  
5yu50JyRSF2fqRND6P/2eHNxejdUtdvhUXIUt8h9MuUO/tpD0DnwlvMnAATJHA+R  
Zqw6oNpyjRGzvriiuWUwe4PtyjDI3ELAFkbp/NAc5TluVHRHNOWNplclJhM5zHuB  
QQb3G/EsCn2PQZ5w5SDzavF2SpvQfDqxYpDaTLAXtF+wsJL5iaUjxwRgjPOdbCzf  
2Tozd7h9MXtGJdIPK8eLG8ogcMAEQEAAYkBQQYAQIAdwUCUcxxyAAlbDAUJCWYB  
gAAKCRCTdsx9/HFzS+hB/9BjQsMlgcoHFXnb1PVIKxekzL8+WVm5Pk/EgMQSL22  
HX4p3ial5PEPCygUw9YnaG4i00dWJGw5/daTWRrtZcnKd8YqoP+DU0t96HZDSu3m  
mCzE9NVAQYboFbVmGOx0eo627UBsvFqaXvAxBDYkoR8B0TnKhrQFwXkZVb30hKwD  
TgAfjOGIZiE6uAdST231tFaQobizYfe5AVXRqro20xBqNbajNs3SW0D831Syvdv  
IIObx83/R0gg7hUk16F2vzXicWmUwFSXRsrggCsblLosHsP6isBWwvIHeRmna/aQab  
YKG3gbV9iyyczAS31gbogVLAZqNSWhp8vIEE28Fyf/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

```
mQENBFHMcgABCAC9WrYDO6K2L3VHyi4eHN6suHLqMpJ+SO+IUTuLEVnUzloXAUXH
KozHejfV/9XoG8j933ZtszKCo3g3aMESe0E02f6fNGfolvaCe5B4jwqoJt8NHwb5L
B2dnq0CplgXcN2GjxfEHUuaF27COSobCxPMeshUh4ZHke+g6DatmiEtBpVp41Ot
1zgxdMQkgb2H2xw72RyfYkdDoubetelkOrLrC9Z9KdMhA1eBH94KnwlQshdiZR
QYEX25+M8cCb++Rc9H6an7EG9WHOFRW40UsY520fveOyfQPzkkRto7u2339hvHO
B/+h7xLM6FQbOUZQ9BD5w7IQHgTjXVsUj0dABEBAAG0IkthbWkgVmFuavVhIdxr
dmFuavVhQGluzi5lZC5hYy51az6JAT8EEwEIACkFAIYKyvECGyMFCQImAYAHcwkl
BwMCAQYVCAIJCgsEFgIDAQleAQIxgAAKCRCTdsxI/HZffG+CACShuKxje3Qaqew
GWh8K4gCdiY0zJwq3PHxmyhZmQeN/1a1KcOrlj12b+Q75/5t+EgXOHpR0PlxfG
IZ6zOEpf6A18FX3jgQzdwpD0jtBiVWnpOyMeBGTglvEYg3so2VueQoeXcq3dbp
5vstVxtb+TKHQ5Ciolt75P2bzYq/XLTsalbNQhQDPCTo0DgbRH+FvqsRx7yeaef
JaPnxX0+1L33t2QY9zctiGyebwrvHMrlPBj2VYCdZQk7uQ5eFh4ZhsMgOmzLQD4
YiGr5weIMFwAvxZoArxEa9Vf48jWvrxu8YfHWs0hEscNOcYC2P8q20JwwE26T
lpdtrwCqtB1LYW1pIFZhbmllUSA8a2FtaUB2YW5pZWEuY29tPokBQgQTAQIALAlb
lwUJCWYBgAcLcQgHAwIBbhUIAgkCkwQWaMBAh4BAheABQJWCmMeAhkBAAlOEJN2
zGx38d19JJAA1W0rrlYsrmKS6CbW8MgTxtdoxaCt1b7f0W0QZhsklUQhEc+a
XBYib1A5uHaatlFyjeXaD3qMEoZnQHoYMG0EGKu00wWsbhfoQzHPgwzRLkD1i75M
B1baww0KWoVB9e4AkMakXJcnF5Bxeo6AHRL2v15V205DikVnlCRXocKtu8b7LnkM
cln7oLbr1de1uyKoNzbSn0/vpkDjp0/EV5yUeV9olypZy/6wFQBBehglsXye6znO
9wb9uUsu+/P8pz4JILMDSevit7zSRS/YP3f0zN4bc/KodwPM7u5lyoeu9zh
pzibv3ge7vhH2xlWz8vYZ/2xT1345tWRRMOJAhweEwECAAyFAITnSpEACgkQjyxM
p99tBt2B8A/+OpIzOsQbQJB8yxti4I7PpD1weJdf3a81Vhm7jyXE/Xy66ypfdt3w
XmrFRUlrwezY1NebWNCRQHzQvRv/VjwjbTUx+Q3HsjlkIHbE7iCiQXXtTRk0Eny
2nudcjGl2v03C3B2jCucEw6esF1x79Pi/IpV2+6tgUBKmDfOpsB2vbtqrhNmAYKL
4IQBFH1YSJgnzw02Jkh0hcHdf90Zem1eMeIDeEvkH63893N8Swk5fBKdTj+SKZ/L
rQEIBBlpMR9BmeY6bPwVRuyCVk0nIMR80G9iFABxjTpWBL8aGk6EeVK5EqYDGvd
Zlark84r+KU1KD5IfgOCM7nhwgY7VlmE68caZHSRIPWZP1fVMMhydiRJv8WsoUs6
INFU3nxH+ZYthPbY0T86leGSchBT5K/fBQvjhrRTbTFwvjzSifb9efWylDi994
nzP6cNorir3GipsT8gPgBB2/NjxaWiM6y3X1az1vRnsunQHuyKKFWPZwnEvDJYaC
NN/3jWcbhLFwkBDsaHps2+1meFP0oJFvNetzp2bjT9a9pxQa6KhOMo5DnhLcaV97
bFBpsUuBGAyZTSS05x1RdXhqpEbgap8dtuHhVvJw9QYDQBJr0K4aKyG9qqMD8cta
PI/FAdyAqwH8Nw9efqAK+RQxSVUaae9BYEnblRpDK6MkP3YMFmu5ki5AQOEUCxy
AAEiALyXYg8G2zaTDJpdGcRhmlqOOSUlzPV7/5E5BbYKBNU4KU3nX+JLvcF5jxPQ
42c7i/WRVx1EBTiarKGsEvCi94TTXSIUKAt3T1oGBtXmGvqbGBq8ljSGI1UTwdF
5yu50JyRSF2fqRND6P/2eHNxejdUtdvhUXIUt8h9MuUO/tpD0DnwlvMnAAJtJHA+R
Zqw6oNpyjRGzvriiuWUwe4PtyjDI3ELAFkbp/NaC5TluVHRHNOWNplclJhM5zHuB
QQb3G/EsCn2PQZ5w5SDzavF2SpvQfDqxYpDaTLAXtF+wsJL5iaUjxwRgjPOdbCzf
2Tozd7h9MXtGJdIPK8eLG8ogcMAEQEAAYkBQQYAQIAdwUCUcxxyA1lbdAUICWYB
gAAKCRC7dsxI9/HfZs+hB/9BjQsMlgcoHFXnb1PVIKxekzL8+WVm5Pk/EgMQSL22
HX4p3ial5PEPCygUw9YnaG4i00dWjGw5/daTWRrtTzcnKd8YqoP+DU0t96HZDSu3m
mCzE9NVAQYboFbVmGOx0eo627UBsvFqaXvAxBDYkoR8B0TnKhrQfwXkZVb30hKwD
TgAfOGIZiE6uAdST231tFaQobizYfe5AVXRqro20xBqNbaJnqs3SW0D831Syvdv
IIObx83/R0gg7hUk16F2vzXicWmUwFSXrRggCsblLosHsP6isBWwvIHeRmna/aQab
YKG3gbV9iyyczAS31gbogVLAZqNSWhp8vIEE28Fyf/Ed
=x5FK
-----END PGP PUBLIC KEY BLOCK-----
```

My public key

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

Version: GnuPG v2

```
mQENBFHMcgABCAC9WrYDO6K2L3VHyi4eHN6suHLqMpJ+SO+IUTuLEVnUzloXAUXH  
KozHejfV/9XoG8j933ZtszKCog3aMESe0Eo26fNGfolvaCe5B4jwqoJt8NHwb5L  
B2dnq0CplgXcN2GjxfEHUuaF27COSobCxPMeshU4ZHke+g6DatmiEtBpVp41Ot  
1zgxdM0kgb2H2xw28RYfYkdDoutelkOrLrCy9ZF9KdMhA1eBH94KnwlQshdiZR  
QEYEX25+M8cCb++Rc9H6an7EG9WHOFRW40UsY520fveOyfQPzkkRto7u2339hvHO  
B/h+7xLM6FQbOUZQ9BD5w7IQHgYtXJVsUj0dABEBAAG0IkthbWkgVmFuaWVhIDxr  
dmFuaWVhQGluzi5lZC5hYy51az6JAT8EEwEIACKAYKyvECGyMFCQImAYAHcwkl  
BwMCAQYVCAIJCgsEFgIDAQleAQIxgAAKCRCTdsxI9/HZffG+CACShuKjxe3QAew  
GWh8K4gCdiY0xQDjwq3PHxmyhZmQeN/1a1KcOrlj12b+Q75/5t+EgXOHP0PlxfG  
IZ6zOEpfGA18FX3JgQZdwPD0jtBiVNpOyMeBGTglvEYg3so2VueQoeXcq3dbYp  
5vstVxtb+TKHQ5CioltT75P2bzYq/XLTsalbNQhQDPCTo0DgbRH+FvqsRx7yeaef  
JaPnxXo+1L33t2QY9zctiGyebwrvHMrlPBj2VYCdZQkJ7uQ5eFh4ZhsMgOmzLQD4  
YiGr5weIMFwAvxZOaRx Ea9Vf48jWvr xu8YfHWs0hEscNOcYc2P8q20JwwE26T  
lpdtrwCqtB1LYW1pIFzhbmllYSA8a2FtaUB2YW5pZWEmY29tPokBQgQTAQIALAlb  
lwUJCWYBgAcLQgHAwIBbhUIAgkCQwAgMBAh4BAheABQJWCmMeAhkBAAljeJN2  
zGx38d19JJAIAlW0rxlYsrmKS6CbW8MgTxzTDOxaCt1b7f0W0QZHsklUQhEc+a  
XBYib1A5uHaatlFyjeXaD3qMEoZnQHoYMG0GKu00wWsbhfoQzHPgwzRLkD1i75M  
B1baww0KWoVB9e4AkMakXJcnF5Bxeo6AHRL2v15V205DikVnlCRXocKtu8b7LnkM  
cln7oLobr1de1uyKoNzbSn0/vpkDjp0/EV5yUev9olypZy/6wFQBBehglsXye6znO  
9wb9uUsu+/P8pz4JILMDSevit7zRSY/YP3ofZ6N4bc+KodwPM7u5lyoeu9zh  
pzibv3ge7vhH2xlWz8vYZ/2xT1345tWRMOMJAhwEEwECAAyFAITnSpEACgkQyxM  
p99tBt2B8A/+OpIzOsQbQJB8yxti4I7PpD1weJdf3a81Vhm7jyXE/Xy66ypfdt3w  
XmfRUlrlwezY1NebWNCRQHzQvRv/VjwjbTUx+Q3HsjlkIHbE7iCiQXXtTrk0Eny  
2nudcjGl2v03C3B2JcuCeW6esF1x79PI/Pv2+6tgUBKmDfOpsB2vtbqrHnmAYKL  
4IQBFH1YSJgnzw2Jkh0hHdf90Zem1eMeIDeVkh63893N8Swk5fBKdTj-SKZ/L  
rQEIBBlpMR9BmeY6bPwVRuyCvK0nIMR80G9iFABxjTpWBL8aGk6EeVK5EqYDGvd  
ZlarK84+rKU1KD5fgOCN7nhwgY7VmE6caZHSRIPWZP1fVMMhydiRJv8WsoUs6  
INFU3nxH+ZyThPbY0T86leGSchBT5K/fBQvjhRTfwvzjsifb9efWylDi994  
nzP6cNorir3GipsT8gPgBB2/NjxaWiM6y3X1az1vRnsunQHuyKKFWPZwnEvDJYaC  
NN/3jWcbhLFWKBDSaHps2+1meP00JFNetzp2bjT9a9pxA6KhOMo5DnhLcaV97  
bFBpsUuBgaYZTSS05x1RdXHqpEbgap8dtuHhVvJw9QYDQBJr0K4aKyG9qqMD8cta  
Pl/FAdyAqwH8N9efqAK+RQxSVUaa9BYEnblRpzDK6MkP3YMFmu5ki5AQOEUCxy  
AAEIALyXYgG2zaTDJpdGcRhmlqOOSULzPv7/5E5BbYKBNU4KU3nX+JLvcF5jxPQ  
42c7i/WRVx1EBTiarKGsEvCi94TTXSIUKAt3T1oGbtXmGvqbGBq8ljSGI1UTwdF  
5yu50JyRSf2fqRND6P/2eHNxejdUtdvhUXIUt8h9MuUO/tpD0DnwlvMnAATJHA+R  
Zqw6oNpyjRGzr3iuWUwe4PtyJDI3ELAFkbp/NaC5TluVHRHNOWNplclJhM5zHuB  
QQb3G/EsCn2PQZ5w5SDzav2SpvQfDqxYpDaTLAXtF+wsJL5iaUjxwRgjPOdbCzf  
2Tozd7h9MXtGJdIPK8eLG8ogcMAEQEAAYkBQQYAQIAdwUCUcxxyA1bDAUJCWYB  
gAAKCRCTdsxI9/HZfs+hB/9BjQSmIgcoHFxnb1PVIKxekzL8+WVm5Pk/EgMQSL22  
HX4p3ial5PEPcYgUw9YnaG4i00dWJGw5/daTWRrtZcnKd8YqoP+DU0t96HZDSu3m  
mCzE9NVAQYboFbVmGOx0eo627UBsvFqaXvAxBDYkoR8B0TnKhrQfwXkZVb30hKwD  
TgAfjOGIZiE6uAdST231tFaQobizYfe5AVXRqro20xBqNbaJnqs3SW0D831Svvdv  
IIObx83/R0gg7hUk16F2vzXicWmUwFSXRsrggCsblLosHsP6isBWwvIHeRmna/aQab  
YKG3gbV9iyyczAS31gbogVLAZqNSWhp8vIEE28Fyf/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.**

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.

PSIRT PGP Key (0x33E9E596)

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

```
xsFNBFm/2KMBEAbwToJM3BCVE1OeC22HgVEqNEDppXzuD2dgfKuy0M4tx2L
De7GkPjo6AOsw4yi8bakLiidpw5B0J/AR1VtIjIDEmS0F9MRZIcV0UKyA5qv
c9BafZnAicY7nezkIJUmyLcIVMC60pqSHzo0Ewy2PZjxzci4vDGhHmcgfV5X
R+duYld3LtVI+A/5jv326LB16bCNts/tOhW2T0LraMPoCtdH84Z4tPcyp335
s8/dz2C+EoMD4iX1kIymZ1kqEfZNvcs1sRUXy27sL01VHcYmi6UNWCeeHou2
2yJxMiBCnizBKZUwcR6ysg97nnq633dN9mf7V30PS3zAjhE0Hvmzg3B/Nfo
qzy2dAEU/JDUBhiAo+xr9VF3ZPOoC8JySORgyUm/2t3TTBaH+DnfsUBiqo5U
2T0n8x2R1FWxyZYINCTku5JOvPqRBft13DSyJD7LDDps62nqhpaVb34eprwuk
qIk0TMRu9mB4EQc+cNFR3ZpN1AKj+HOb/TUJwCJpVju2/3g0wgdqHh+OQlvC
Nm8vIGnQZWQ30WqnH/UFoh3RPJ+WqnDq88NmqBq8I4aNv4u8MqoObd/zrtVX
kAwYHbIZLo925NjFyPuuxhWiCotKen18dZefB8aB81RjYuIMnCJ0GQus+JG8
TJyEesNdK/q8HD5h1kCRSzMDl+Ra3z/1+FFIwARAQABzR1BZG9iZSBQU01s
VCA8cHNpcnRAYWRvYmUuY29tPsLBewQQAQgALwUCWb/YrwUJAeEzgAYLCQgH
AwIJEIbAD8Kvh3YWBBUIAgoDFgIBAhkBAhsDAh4BAADk2A//f+6PFzg4VmLI
PzsTZPoqPR/lXlZ7RIYbQosHvsFwyW0WWX1uIl1sEeD5Qo7HQt6NNMAOW51Js
wFvFOWIa9U6SHRoU1kGTSESReOq5HnXe4DcBubsKmoMS68PuiZ88wYOIM4Up
9V9PUuaue0U4oSrYHnH5qB0qurtv8wO5Cq4uTwnfnjN7n4OH0++2910PJ68B
6+kMuQyG4swmxsZh1jlqGMHcs0c/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

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

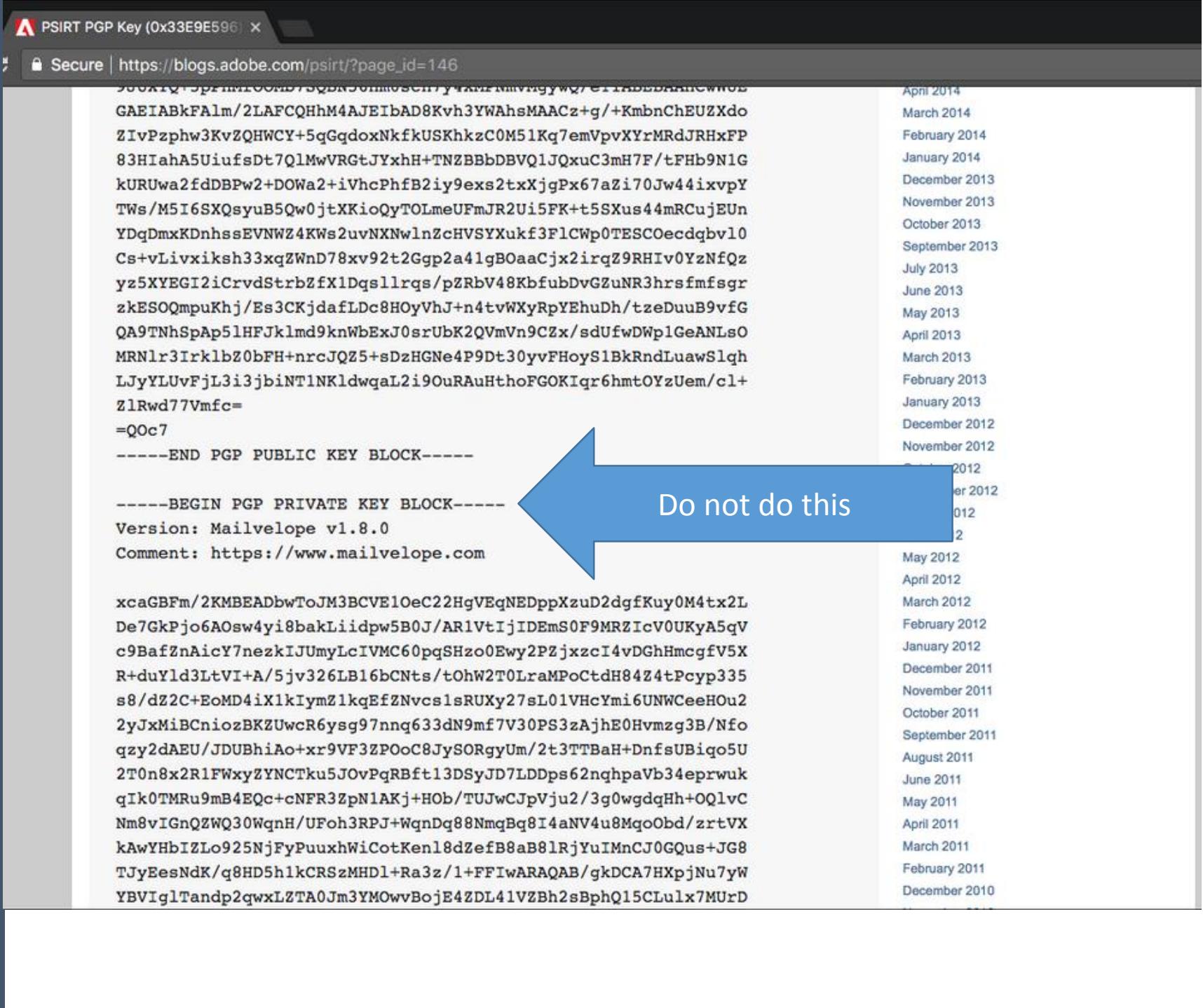
The screenshot shows a web browser window with the following details:

- Title Bar:** PSIRT PGP Key (0x33E9E596) X
- Address Bar:** Secure | https://blogs.adobe.com/psirt/?page_id=146
- Header:** blogs.adobe.com (with a red lock icon) and a search bar labeled "Search Blogs".
- Page Content:**
 - Section Header:** Adobe Product Security Incident Response Team (PSIRT) Blog
 - Text:** Working to help protect customers from vulnerabilities in Adobe software. Contact us at PSIRT(at)adobe(dot)com.
 - Section Header:** PSIRT PGP Key (0x33E9E596)
 - Text:** -----BEGIN PGP PUBLIC KEY BLOCK-----
Version: Mailvelope v1.8.0
Comment: https://www.mailvelope.com
 - Text:** A large block of PGP public key data is displayed below the comment line.
- Right Sidebar:**
 - CATEGORIES:** Alert, Security Bulletins and Advisories, Uncategorized
 - ARCHIVES:** A list of months from September 2017 down to December 2015.

```
xsFNBFm/2KMBEADbwToJM3BCVE1OeC22HgVEqNEDppXzuD2dgfKuy0M4tx2L
De7GkPjo6AOsw4yi8bakLiidpw5B0J/AR1VtIjIDEms0F9MRZIcV0UKyA5qv
c9BafZnAicY7nezkIJUmyLcIVMC60pqSHzo0Ewy2PZjxzci4vDGhHmcgfV5X
R+duYld3LtVI+A/5jv326LB16bCNts/tOhW2T0LraMPoCtdH84Z4tPcyp335
s8/dz2C+EoMD4iX1kIymZ1kqEfZNvcs1sRUXy27sL01VHcYmi6UNWCeeHou2
2yJxMiBCnizozBKZUwcR6ysg97nnq633dN9mf7V30PS3zAjhE0Hvmzg3B/Nfo
qzy2dAEU/JDUBhiAo+xr9VF3ZPOoC8JySORgyUm/2t3TTBaH+DnfsUBiqo5U
2T0n8x2R1FWxyZYINCTku5J0vPqRBft13DSyJD7LDDps62nqhpavb34eprwuk
qIk0TMRu9mB4EQc+cNFR3ZpN1AKj+HOb/TUJwCJpVju2/3g0wgdqHh+OQlvC
Nm8vIGnQZWQ30WqnH/UFoh3RPJ+WqnDq88NmqBq8I4aNV4u8MqoObd/zrtVX
kAwYHbIZLo925NjFyPuuxhWiCotKen18dZefB8aB81RjYuIMnCJ0GQus+JG8
TJyEesNdK/q8HD5h1kCRSzMDH1+Ra3z/1+FFIwARAQABzR1BZG9iZSBQU01S
VCA8cHNpcnRAYWRvYmUuY29tPsLBewQQAQgALwUCWb/YrwUJAeEzgAYLCQgH
AwIJEibAD8Kvh3YWBBUIAgoDFgIBAhkBAhsDAh4BAADk2A//f+6PFzg4VmLI
PzsTZPoqPR/lX1Z7RIYbQosHvsFwyW0WWX1uI1sEeD5Qo7HQt6NNMAOW51Js
wFvFOWIa9U6SHRoU1kGTSESReOq5HnXe4DcBubsKmoMS68PuiZ88wYOIM4Up
9V9PUuaue0U4oSrYHnH5qBOqurtv8w05Cq4uTwnfnjN7n4OH0++2910PJ68B
6+kMuQyG4swmxsZh1jlqGMHcs0c/BuI3W+n5w+xLM7N5jjCTjNXR+tGmstdm
RPEoLWoso+ZFwfNW0CLKjYUahp3p6H9x8R13wrp2re0GhqKRgt3D4UcAqsPs
```

Photo credit: Juho Nurminen
@jupenur

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



Do not do this

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: 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

```
mQENBFHMcgABCAC9WrYDO6K2L3VHyi4eHN6suHLqMpJ+SO+IUTuLEVnUzloXAUXH  
KozHejfV/9XoG8j933ZtszKCog3aMESe0E02f6fNGfolvaCe5B4jwqoJt8NHwb5L  
B2dnq0CplgXcN2GjxfEHUaf27COSobCxjPMeshUh4ZHke+g6DatmiEtBpVp41Ot  
1zgxdMqkzb2H2xw7RyfYkdouetelkOrLrCy9Zf9KdMhA1eBH94KnwlQshdiZR  
QYEX25+M8cCb++Rc9H6an7EG9WHOFRW40Usy520fveOyfQPzkkRto7u2339hvH0  
B/h+7xLM6FQbOUZQ9BD5w7IQHgYtXJVsUj0dABEBAAG0IkthbWkgVmFuawVhIDxr  
dmFuawVhQGluzi5lZC5hYy51az6JAT8EEwEIACKAYKyvECGyMFCQImAYAHcwkl  
BwMCAQYVCAIJCgsEFgIDAQleAQIxgAAKCRCTdsx9/HZffG+CACShuKxje3Qaqew  
GWh8K4gCdiY0dQjwq3PHxmhzQmNeN/1KcOrlj12b+Q75/5t+EgXOHpR0PlxfG  
IZ6zOEpfGA18FX3jgQZdwPDojtBiWNpOyMeBG7glvYG3so2VqeOoeXcq3dbp  
5vstVxtb+TKHQ5Ciolt75P2bzYq/XLTsalbNQhQDPCTo0DgbRH+FvqsRx7yeaef  
JaPnx0+1L33t2QY9zctiGyebwrvHMrIPBJ2VYCDzQkj7uQ5eFh4ZhsMgOmzLQD4  
YiGr5weIMFwAvxZOaRx Ea9Vf48jiWvrxu8YfHWs0hEscNOcyC2P8q20JwwE26T  
lpdrwCqtB1LYW1pIFZhbmIIYSA8a2FtaUBZYW5pZWEmY29tPokBQgQTAQIALAlb  
lwUJCWYBgAcLQgHAwIBbhAagKQwAgMBAh4BAheABQJWCmMeAhkBAAljeJN2  
zGx38d19JJAlAIW0rrlYsrmKS6CbW8MgTxzTDOxaCt1b7F0W0QZHsklUQhEc+a  
XBYib1A5uHaatLfjeXaD3qMEoZnQHoYMG0EGKu00wWsbhfoQzHPgwzRLkD1i75M  
B1baaw0KWoVB9e4AkMakXJcnF5Bxeo6AHRL2v15V205DikVnICRXocKtu8b7LnkM  
cln7oLbr1de1uyKoNzbSn0/vpKDjp/EV5yUeV9olypZy/6wFQBBehglsXye6znO  
9wb9uUsu9+/P8pz4JILMDSevit7zSRS/YP3ofZ6N4bc+kOdwrPM7u5lyoeu9zh  
pzibv3ge7vhH2xlWz8YZ/2xT1345tWRRMOJAhweEwECAAyFAITnSpEACgkQjyxM  
p99tBt2B8A/+OpIzOsQbQB8yxti4I7PpD1weJdf3a81Vhm7JyXE/Xy66ypfdt3w  
XmrFUlrwezY1NebWNCRQHzQvRv/VjwjbTUx+Q3HsjlkIHbE7iCiQXXtTRk0Eny  
2nudcjGl2v03C3B2jCucEw6esF1x79PI/Pv2+6tgUBKmDfOpsB2vbtrqrHnmAYKL  
4IQBFH1YSJgnzw2Jkh0hcHdf90Zem1eMeIDeVkh63893N8Swk5fBKdTj-SKZ/L  
rQEIBBlpMR9BmeY6bPwVRuyckV0nIMR80G9iFABxjTpWBL8aGk6EeVK5EqYDGvk  
ZiarK84r+KU1KD5fgOCN7nhwgY7VmE68caZHSRIPWZP1fVMMhydiRJv8WsoUs6  
INFU3nxH+ZyThPbY0T86leGSchBT5K/fBQvjhrRTfwvzjsfB9efWylDi994  
nzP6cNorir3GipsT8gPgBB2/NjxaWiM6y3X1az1vRnsunQHuyKKFWPZwnEvDJYaC  
NN/3jWcbhLFwKBDSaHps2+1meFP0oJfVNetzp2bjT9a9pxA6KhOMo5DnhLcaV97  
bFBpsUuBGaYZTSS05x1RdXHqpb8dtuHhVv9QYDQBJr0K4aKyG9qqMD8cta  
Pl/FAdyAqwH8Nw9efqAK+RQxSVUaae9BYEnblRpzDK6MkP3YMFmu5ki5AQOEUCxy  
AAEIALyXYg8G2zaTDJpdGcRhmlqOOSULzPV7/5E5BbYKBNU4KU3nX+JLvcF5jxPQ  
42c7i/WRVx1EBTiarKGsEvCi94TTXSIUKAt3T1oGBtXmGvqbGBq8ljSGI1UTwdF  
5yu50JyRSF2fqRND6P/2eHNxejdUtdvhUXIUt8h9MuUO/tpD0DnwlvMnAATJHA+R  
Zqw6oNpyjRGzr3iuWUwe4PtyJDI3ELAFkbp/NaC5TluVHRHNOWNplclJhM5zHuB  
QQb3G/EsCn2PQZ5w5SDzavF2SpvQfDqxYpDaTLAXtF+wsJL5iaUjxwRgjPOdbCzf  
2Tozd7h9MXtGJdIPKj8eLG8ogcMAEQEAAyKbQQYQAQIAdwUCUcxxyA1bDAUJCWYB  
gAAKCRCTdsx9/HfZs+hB/9Bj9SmIgcoHFXnb1PVIKxekzL8+WVm5Pk/EgMQSL22  
HX4p3ial5PEPCygUw9YnaG4i00dWJGw5/daTWRrtZcnKd8YqoP+DU0t96HZDSu3m  
mCzE9NVNAQYboFbVmGOx0eo627UBsvFqaXvAxBDYkoR8B0TnKhrQfwXkZvB30hKwD  
TgAfjOGIZiE6uAdST231tFaQ0bizYfe5AVXRqro20xBqNbajNs3SW0D831Syvdv  
IIObx83/R0gg7hUk16F2vzXicWmUwFSXRsrggCsblLosHsP6isBWwvIHeRmna/aQab  
YKG3gbV9iyczAS31gbogVLAZqNSWhp8vIEE28Fyf/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

A screenshot of a web browser displaying the Ally Financial Inc. website. The address bar shows the URL <https://www.ally.com>. The page content includes a green lock icon and the text "Ally Financial Inc. Secure Connection". It states, "You are securely connected to this site, owned by: Ally Financial Inc., Detroit, Michigan, US. Verified by: Entrust, Inc." A blue arrow points from the text "Verified by: Entrust, Inc." to another blue arrow pointing towards the bottom left of the page, which contains the text "Whether it's banking, credit card, home loans or auto finance, nothing stops us from doing right by you." To the right of the text is a photograph of a woman with long brown hair, wearing a red jacket, looking slightly to the side. At the bottom of the page are icons for a percentage sign, a computer monitor, a smartphone, and a ribbon, with corresponding text links: "View Ally Bank", "Auto Online", "Banking on the", and "Why Choose Ally".

Online Banking, CDs, Mo... +

Ally Financial Inc. (US) | https://www.ally.com C 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://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](#)

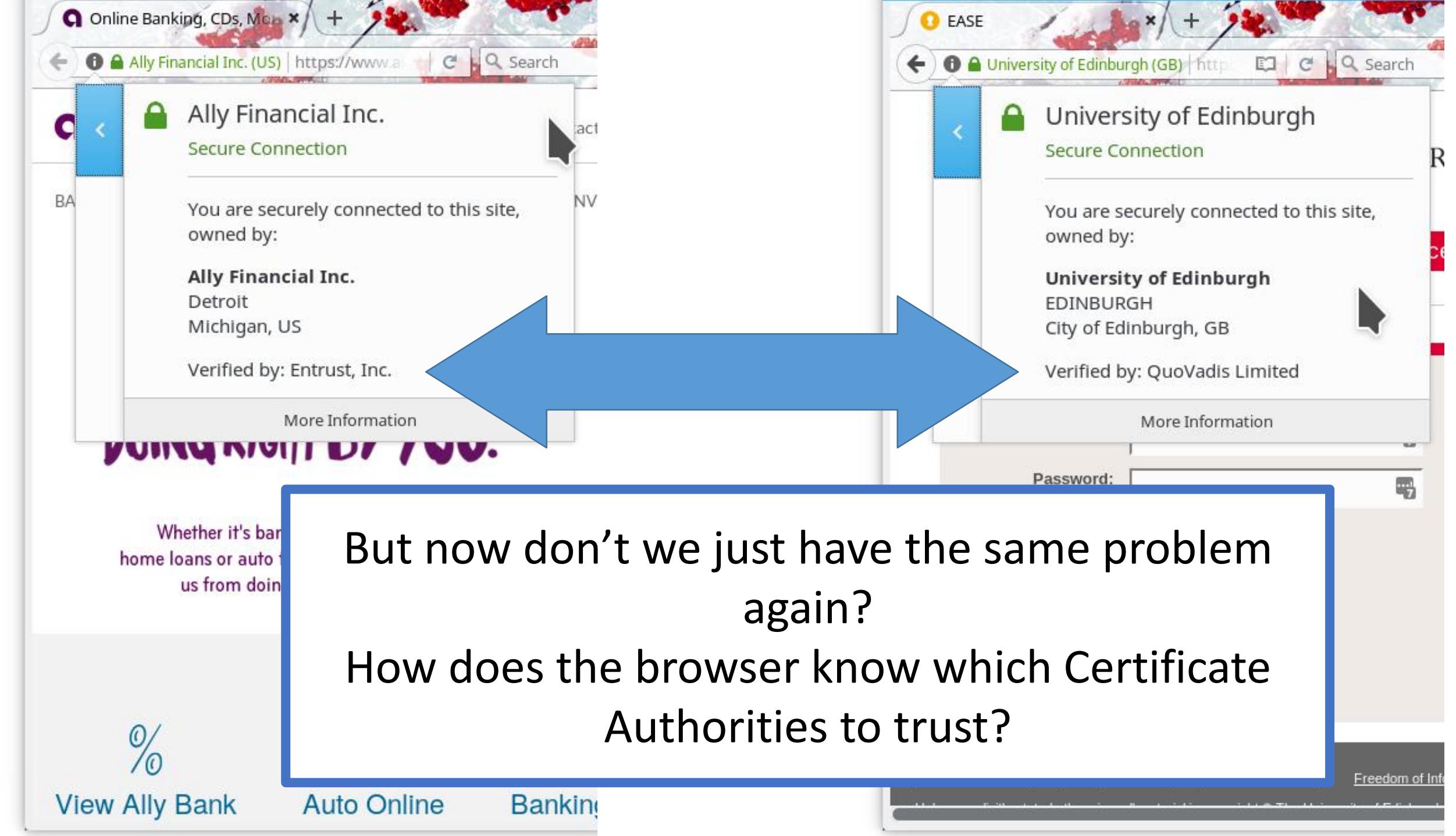
Privacy & History

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.

Insecure Connection X +

< i | https://student.inf.ed.ac.uk ↻ Search » ≡

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

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.

Certificate Viewer: "student.inf.ed.ac.uk"

General Details

Certificate Hierarchy

- ▼ University of Edinburgh CA 2
- └ Informatics Root CA
- └ Automated Server Key CA
- └ student.inf.ed.ac.uk

Certificate Fields

- Serial Number
- Certificate Signature Algorithm
- Issuer
- ▼ Validity
 - Not Before
 - Not After
- Subject
- ▼ Subject Public Key Info
 - Subject Public Key Algorithm
 - Subject's Public Key
- ▼ Extensions

Field Value

Modulus (1024 bits):

```
bf 27 07 c2 9d 7f 0c b4 97 2f 61 29 e2 cb 3c c5  
f6 b5 a6 2a f4 42 aa 93 06 ce d9 df ce 8b 24 fc  
bd 53 4d 8b d4 c4 29 be 6f 86 1a 45 8a 50 21 98  
cf 94 d8 d6 e6 8d 42 41 b6 8f 68 86 df 17 d2 73  
48 05 78 d7 c8 1c 18 a1 de 27 a1 a2 81 d6 ed 9c  
8f 7b 92 ba 2c 7f 64 c2 1d 7d b4 64 a1 9e 35 d3  
cd 61 d8 a9 72 d3 ef 43 b9 fb 22 c8 54 c0 3f d4  
b2 52 a9 b6 7e 26 89 20 8a 1c 43 c7 21 13 e0 8f
```

Export...

The screenshot shows a Firefox Certificate Viewer window for the URL "student.inf.ed.ac.uk". The title bar says "Certificate Viewer: 'student.inf.ed.ac.uk'". The main area has two tabs: "General" and "Details", with "General" selected. Under "Certificate Hierarchy", it shows a tree structure: "University of Edinburgh CA 2" (highlighted with a red box), which has "Informatics Root CA" as a child, which in turn has "Automated Server Key CA" as a child, which finally has "student.inf.ed.ac.uk" as a child. Under "Certificate Fields", there is a list of items like "Serial Number", "Issuer", "Validity", "Subject", etc. The "Subject's Public Key" item is highlighted with a blue bar and has a black cursor arrow pointing to its value. Below the fields, the "Modulus (1024 bits)" is listed in hex format: bf 27 07 c2 9d 7f 0c b4 97 2f 61 29 e2 cb 3c c5, followed by several more lines of hex digits. At the bottom of the window is a "Export..." button.

**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

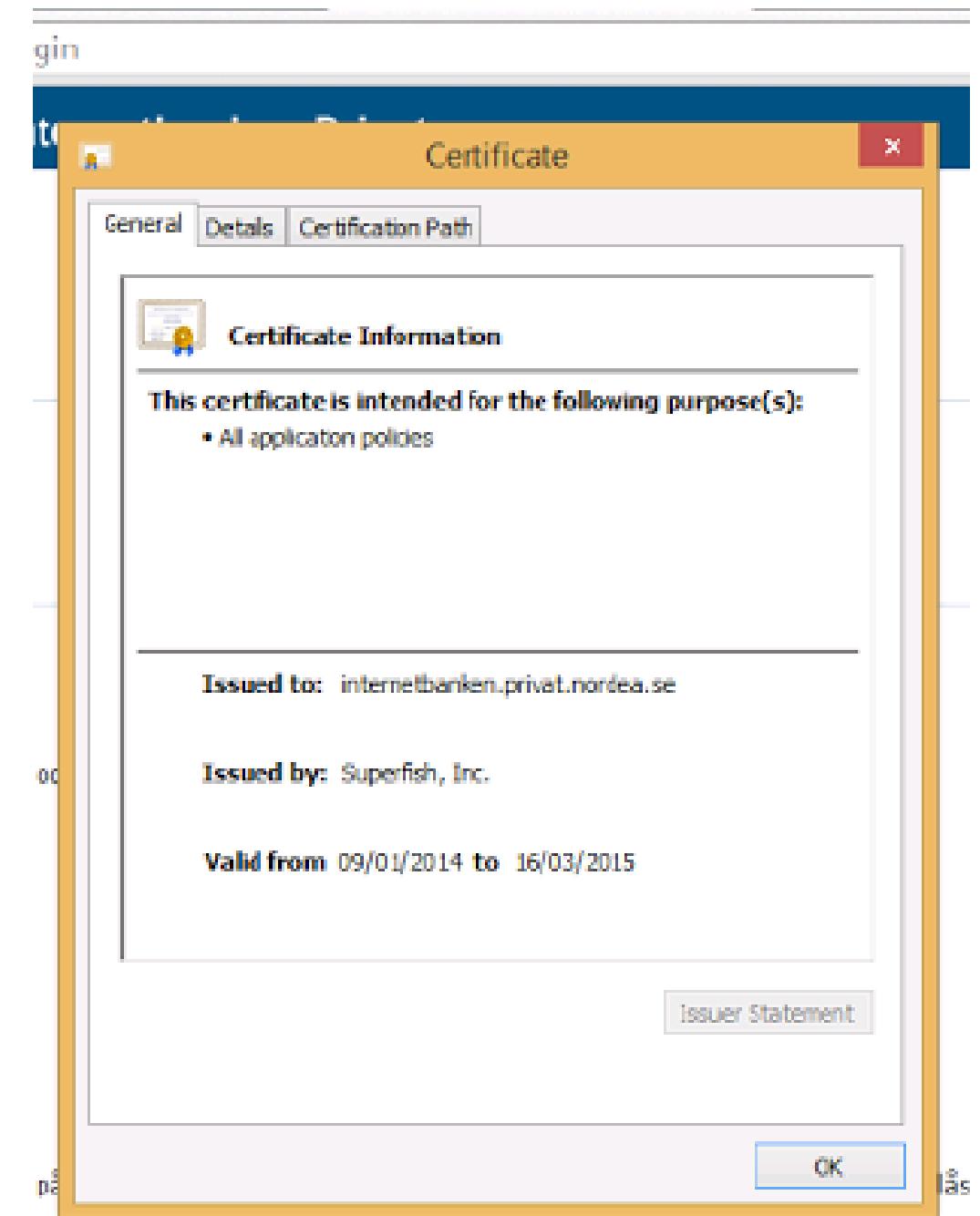
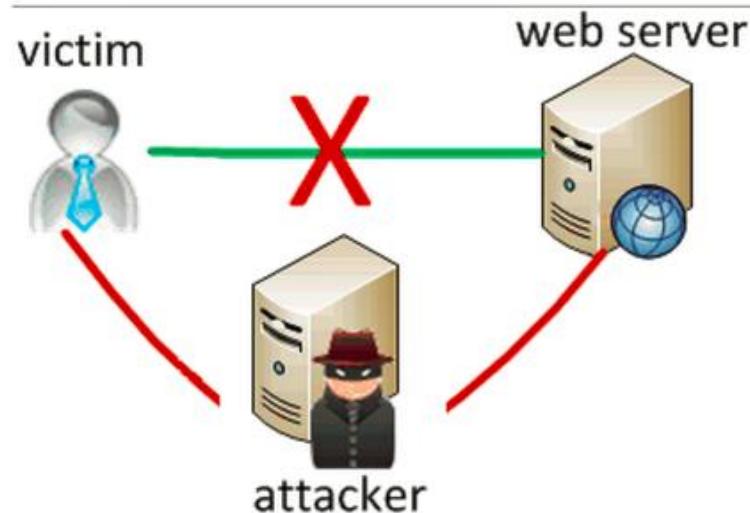
RISK ASSESSMENT / SECURITY & HACKTIVISM

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

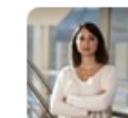
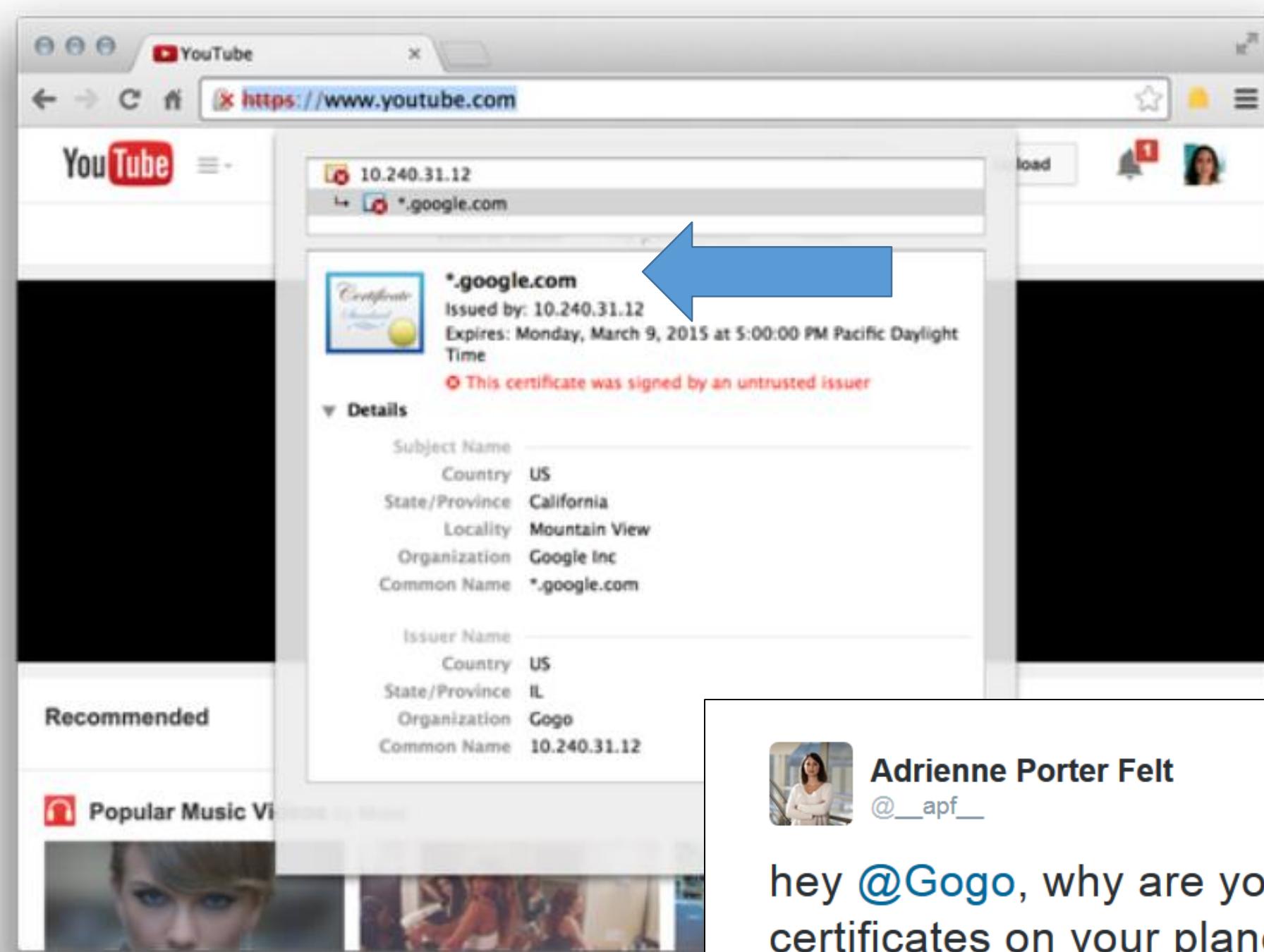
10.240.31.12
*.google.com

***.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: *.google.com
Country: US
State/Province: California
Locality: Mountain View
Organization: Google Inc
Common Name: *.google.com

Issuer Name: Gogo
Country: US
State/Province: IL
Organization: Gogo
Common Name: 10.240.31.12



Adrienne Porter Felt

@__apf__



Following

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

Questions?