PGP Email

Using PGP encrypted email for medical correspondence

PGP Email

PGP
=
“Pretty Good Privacy”

PGP Email

Patient confidentiality. Why do we care?

- Obligation to protect confidential and sensitive patient information
- College requirements and legal exposure with confidentiality breaches
- “The relationship between doctor and patient is based on trust. Trust requires privacy.”

Concept of “circle of care”

PGP Email

Yet we need to communicate within the circle of care to provide effective care

Fax Machines

Why do people still use paper faxes in the 21st century?

- Dead easy to use and easy basic setup
- Unilateral, simple setup (all you need is someone's fax number to send them a fax)
- Relatively cheap
- Toner on paper is an “open” format. Nobody owns it (no license fees to use it)
- Direct point-to-point communication
- Secure(ish)

Fax Machines

What's bad about paper fax machines?

- Machine, paper and toner cost (financial. environmental)
- Increase in office workload. Print-scan-shred on both sender and recipient side
- Lost faxes, sent to wrong number, transmission errors, ran out of paper, machine malfunction, misfiled faxes
- Poor image resolution once scanned into EMR
- Scanned images don't contain electronic text (not electronically search-able or selectable)

Electronic Fax

PROs

- No printing and scanning (on sender's side)
- Fast and convenient to use right from the OSCAR user desktop once set up
- Can integrate into EMR
- Can communicate with paper fax machines (unilateral setup)

CONs

- Fiddly and technologically complicated
- Cost (if using third party provider)
- Confidentiality issues (if using third party provider)
- Fax is old analog tech from last century. Are its days numbered?

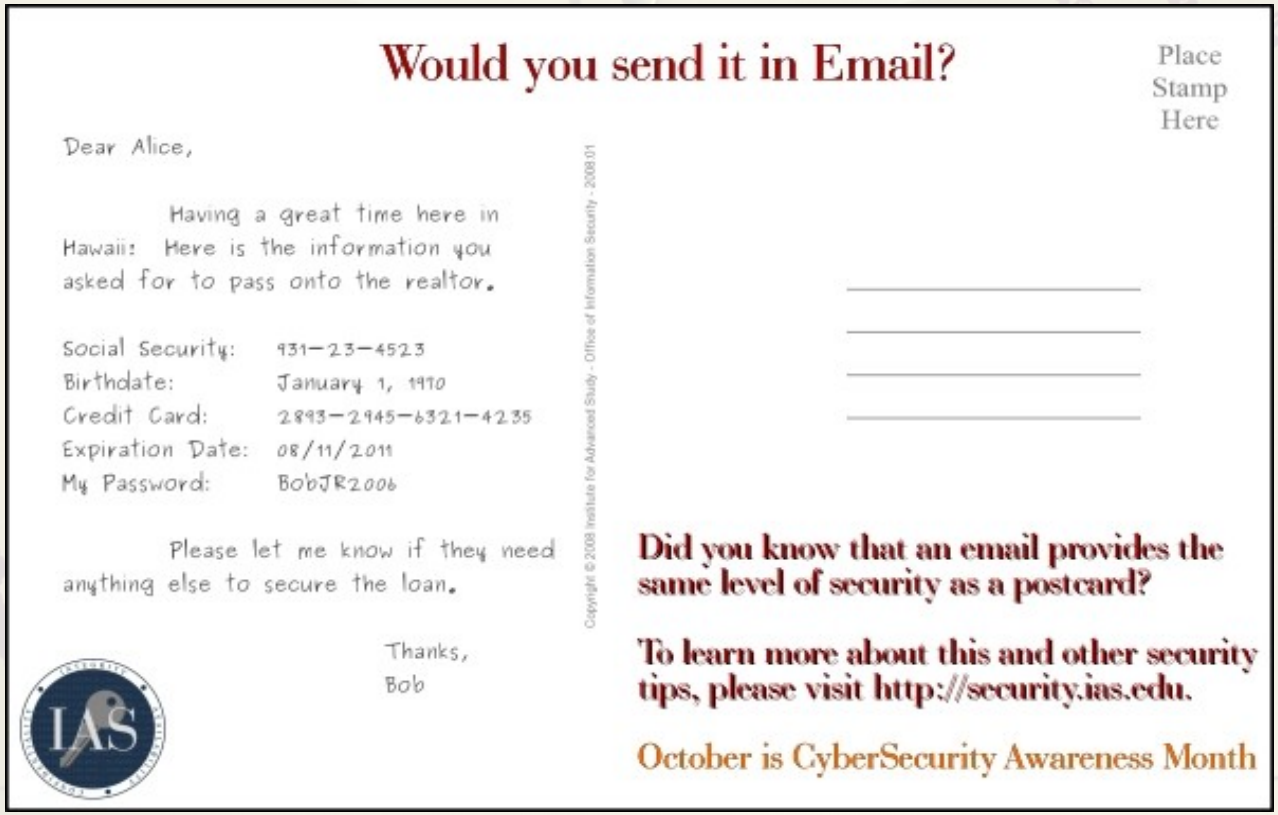
Regular Open Email

Why do people use email?

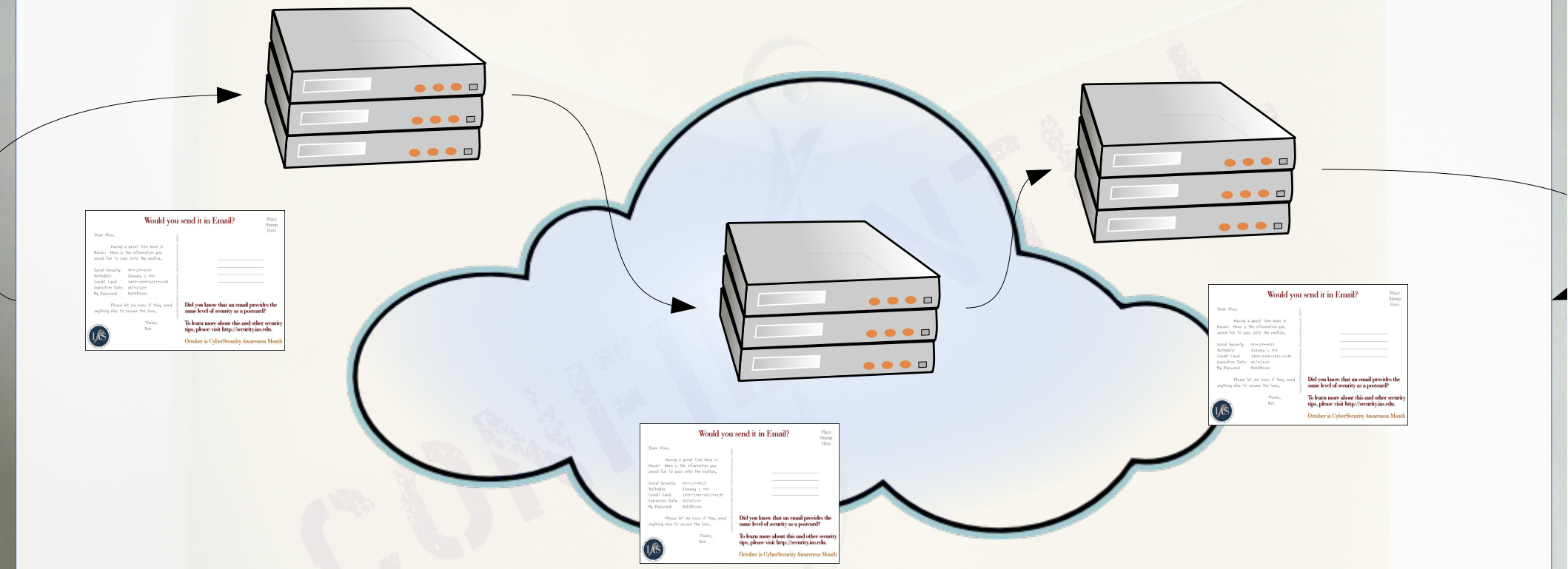
- Dead easy and convenient
- Super fast
- Super quality – digital transmission
- Everybody has it and is already using it (these days arguably more people have access to email than to fax machines)
- Accessible from multiple locations and on mobile
- All electronic. No printing and scanning
- Free (or very low cost)

Regular Open Email

But the security issues...



Regular Open Email



Encrypting the Email

Encrypting the Email

Plain text

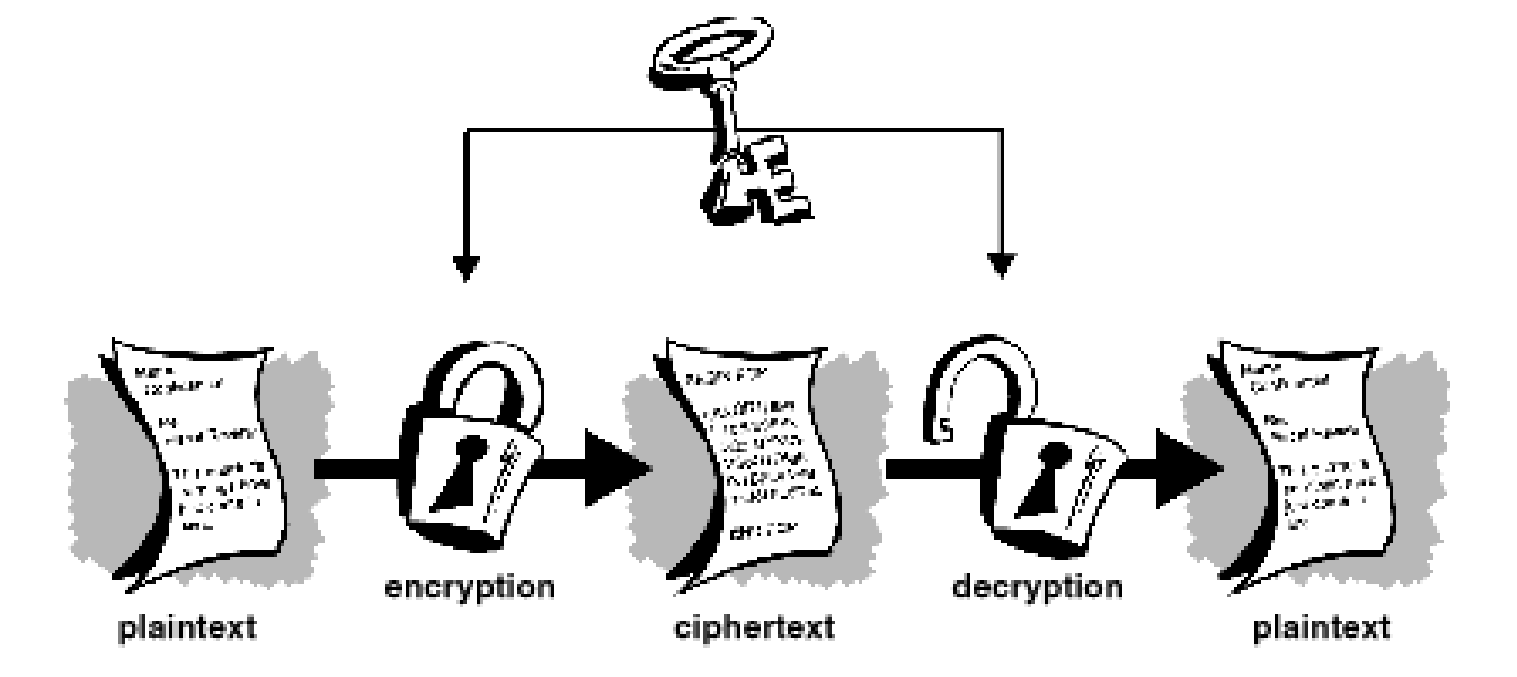
The quick brown fox jumps over the lazy dog

Cyphertext

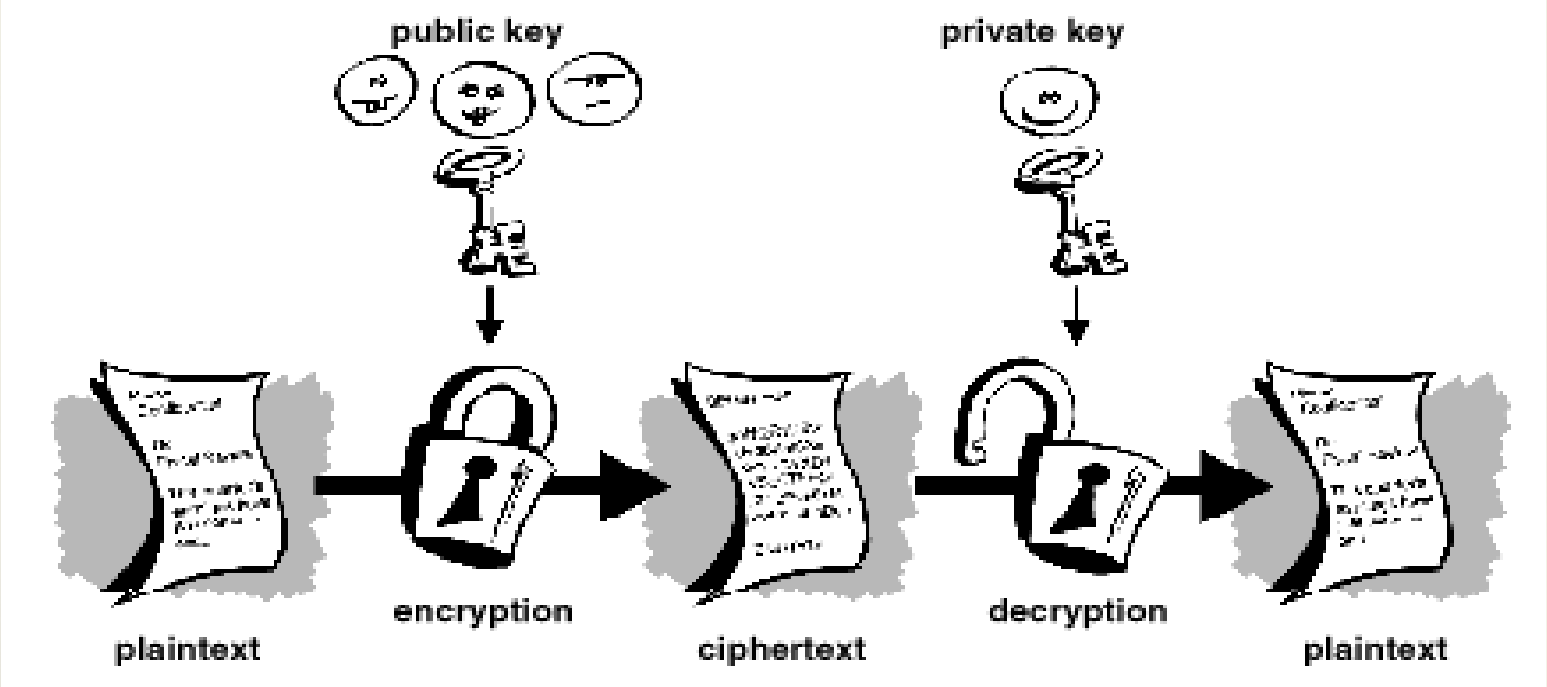
```
-----BEGIN PGP MESSAGE-----
Charset: ISO-8859-1
Version: GnuPG v1
Comment: Using GnuPG with Thunderbird - http://www.enigmail.net/

hQEMA0G3B7ZWQQLyAQf8D/fFBkGD+WUeTbqq02Yy4ewNuTcHHwozvKWJ1GzF+3Fm
3OebziGt27U2jYTWqz6k8IN0DOAXTvDaAhx+4OI7/DBoOftSavWp31a9WzioueMm
1P613z7a9I+u5ZsFCt1UzXD7rRONUKmjkbk1//e2ifMeaF2jhMJ9DJV7XZlfSE3y
VmU2Y61JyykzzazNe5KDuMCYY0f/ksRihbsO68iap+iC93l7CYrJ+cTdI+EMxIz5
a2Dp1n9uJn+86MMuoMA5ulI5qyHvMehdMyViwoKDYblq2PHlK/6wA1XuNvuT3cKx
55jT8xvc4j+gbqef0bALFI3pBvMSWYDTM1BOpQShpdLA2QGpa3v+bb1fCGqkB5Pl
RcDNJuwW/qkzX0tkGUpS4wzgpqwXHgVHtMaqZx7lTnkk5UYS4Kf+8kopQBO8P2+c
0Xe/m/ZIgJqaS4Y8aqXV6x0XSsPhn6x5Bh/VvdkBn1h0ad1YKyh4ZYAgKy7pvQqN
uRMK5RBcI6IiMV1ErdYcCc8erFVxLDapzZ84sS1WcCZ5z63xuE0i30TijZsDfYDF
nEsZmFMJ1vzALNDSHs7CDjCstIe+06WN04aJuyR7isOrbBwOmJMMqlxN4om1BKwI
aQO52k8qUTmgmEMwSQ2iKTDgUzab0EbOoJJApEyG5SUH1BujKH/X2ct3+M/AObM7
1TQSIlTlWc5lrq55jBGFw1okxlDWo2ZMjyyRv/dKxmrQ6diWl+ghO6Sy+vb/JVg1
4zmG7cuuFBVp5ABh3TWwTNn+vZGj+ZHzW0usgmLTs2h2KwVxoE+eGnt8csveVyaK
7mVjm5C1MH6WefrRUJrBrjn0GP1TDsQBQql5ukunfilQKsXgO48SMLo2Ok5ua69f
b8oNTSfB09Nj9aY=
=DBEO
-----END PGP MESSAGE-----
```

Conventional Cryptography

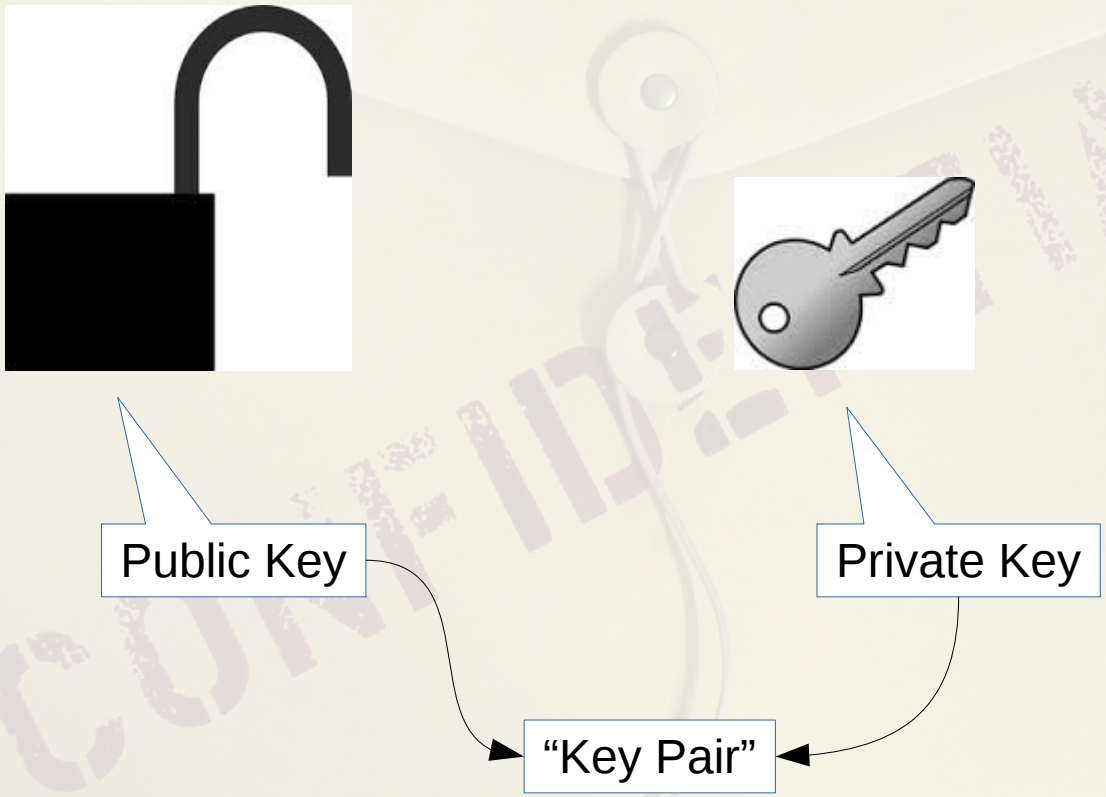


Public Key Cryptography



Public Key Cryptography

Public Key Cryptography

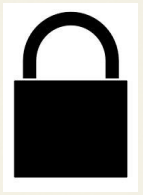


PGP Email

Your Friends & Colleagues

You

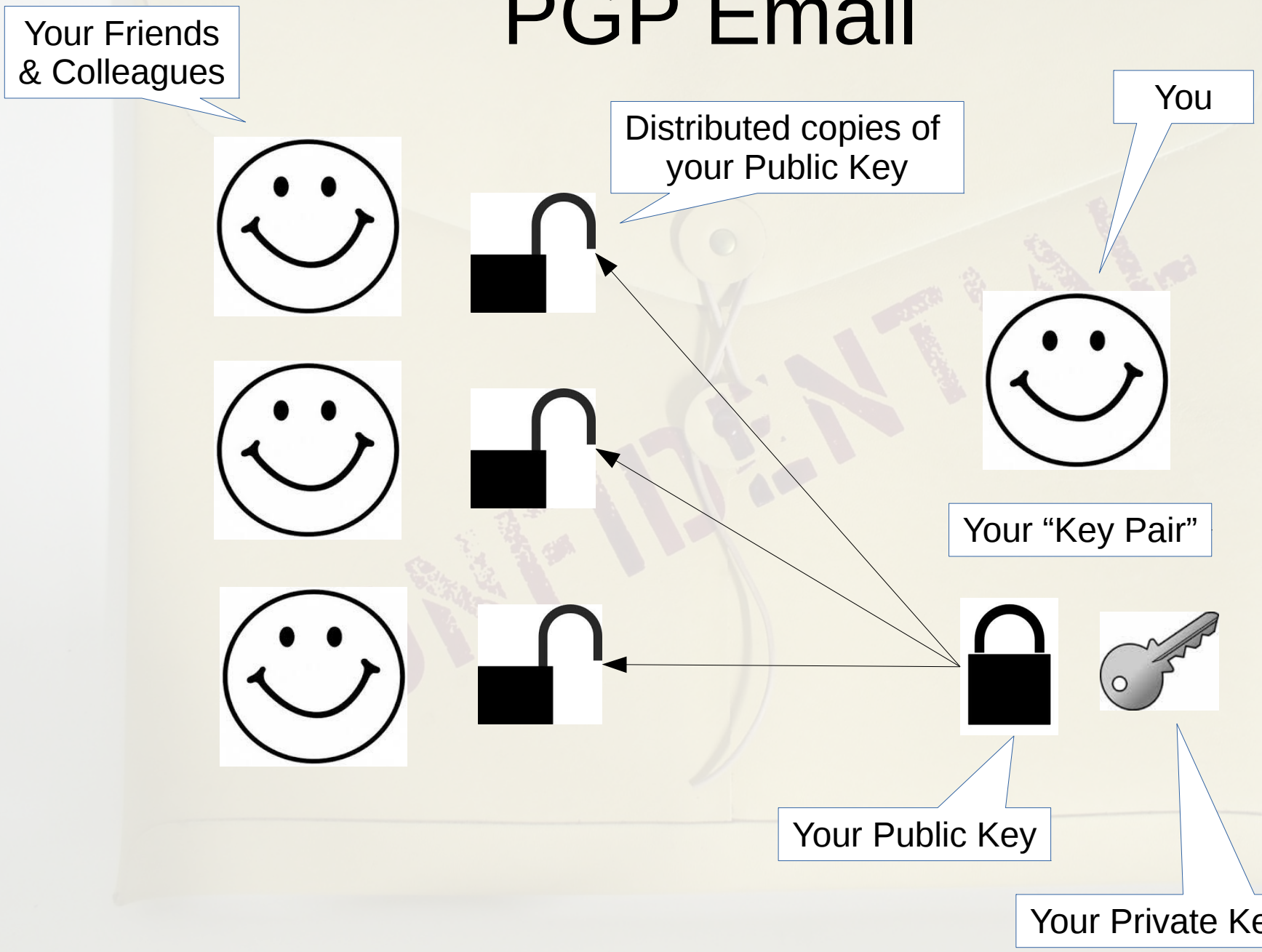
Your “Key Pair”



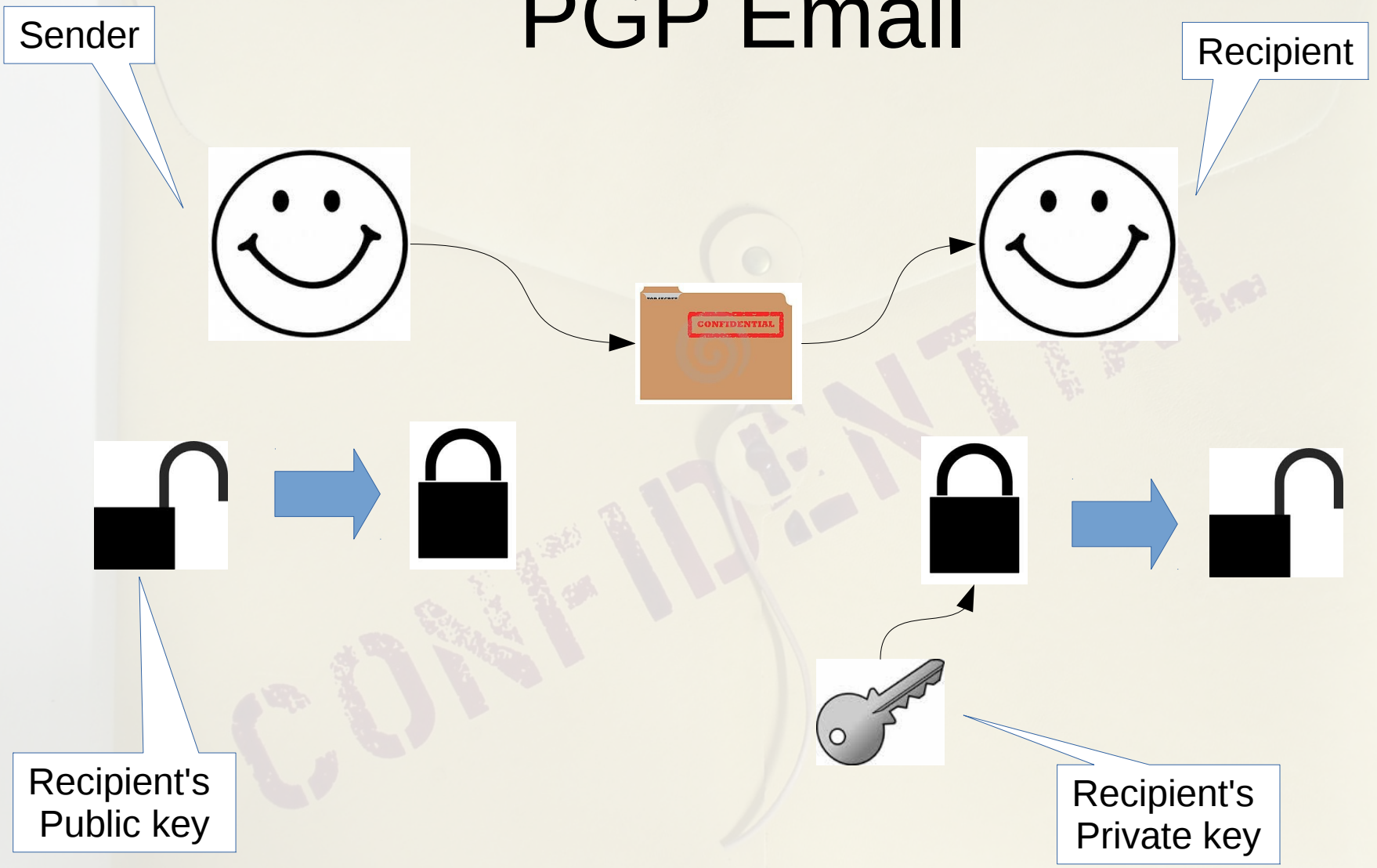
Your Public Key

Your Private Key

PGP Email


Your Friends & Colleagues
Distributed copies of your Public Key
You
Your “Key Pair”
Your Public Key
Your Private Key

PGP Email


Sender
Recipient
CONFIDENTIAL
Recipient's
Public key
Recipient's
Private key

PGP Email

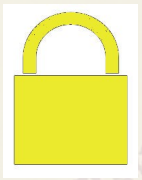
Your Friends & Colleagues

What about the other way around?

You

PGP Email

Your Friends & Colleagues



You

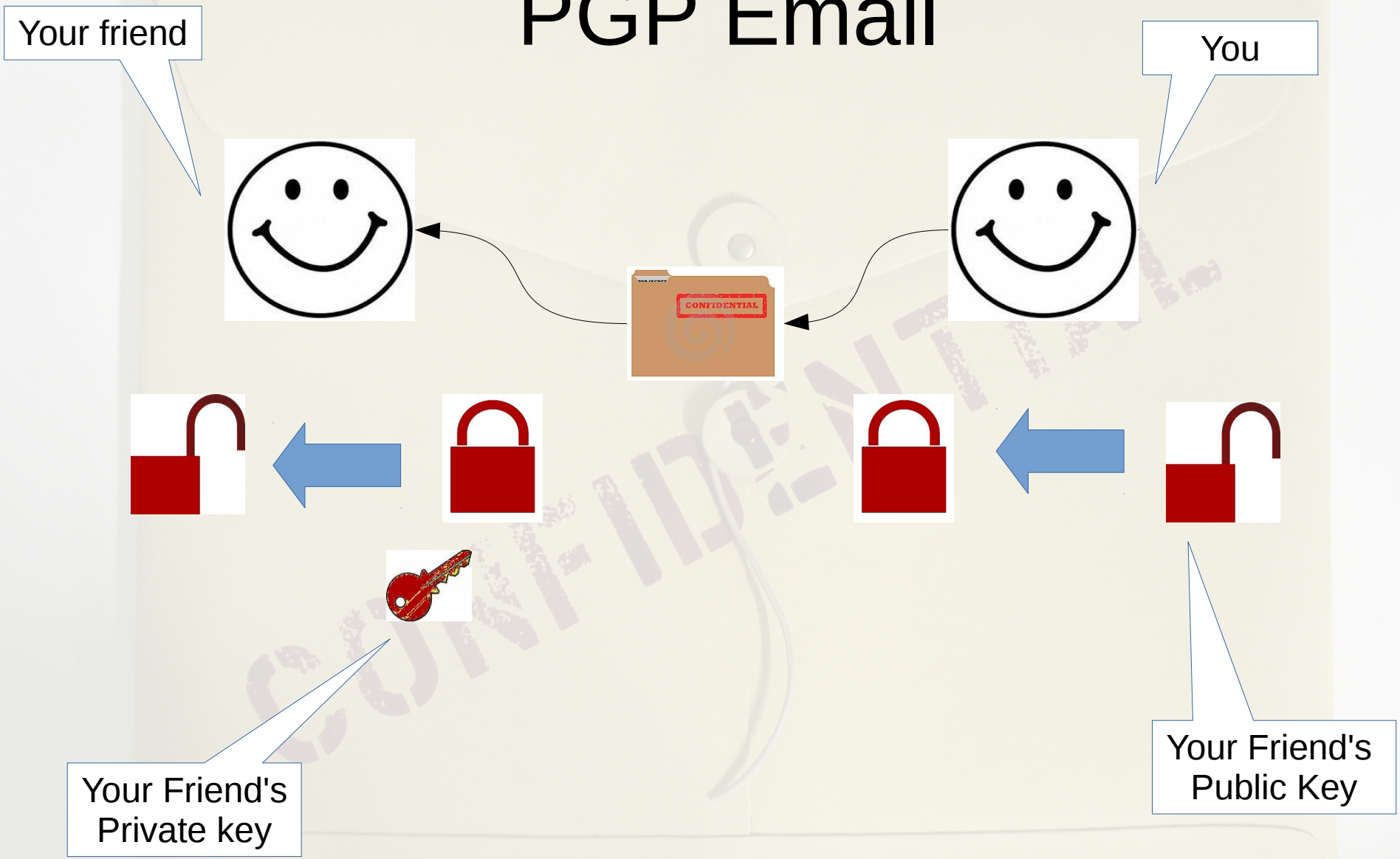
Your Friend's Public Key

Your Friend's Private Key

PGP Email


Your Friends & Colleagues
All your friends give you copies of their public keys
You
Your Friend's Public Key
Your Friend's Private Key

PGP Email


Your friend
You
CONFIDENTIAL
Your Friend's Private key
Your Friend's Public Key

PGP Public Key (Example)

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: SKS 1.1.4
Comment: Hostname: pgp.rediris.es

mQENBFJ8iiEBCACxPavt1+Kpc1O4mzE4HfIF3APzJBzgV6iAIvbiCz1X4ZU3RDLiIs5nyLyd
v2VagHk5VsAcFLev7djb9hPhqgJAP5zrXwn/pQxwxLDHmisTgh2I6HpwtXsGTYoOsosli+P+
KkL/d9VW/AsFJpuW2c/U2sFKAgte6h4YUo7VRpcUm7scp2PLLWugsn4FgJ5m/6eYi3TEphSk
HA9UZyx0zo+BGuk5fZ7pgXI9PcAaGN7XZ+1IuSrI5Rro5uIg3ylWoH0KBLD+giHIkv8CKpwA
icKVHhe8CIKIJBM3S5eoA/aig7t08I56tTNU22lyrnusgsgxRssIXg5Q3fyDsnfTD+R/ABEB
AAG0M1JpdmVyIENpdHkgRnJvbnQgRGVzayAxIDxyaXZlcmNpdHljbGluaWNAdGVsdXMubmV0
PokBPgQTAQIAKAUCUnyKIQIbIwUJCWYBgAYLCQgHAwIGFQgCCQoLBBYCAwECHgECF4AACgkQ
US4fll0NJHOd1wf7Bhza7hHK70RZ1yvjaBrvm909kwcf7gdIaIoLcIaw/pjuk8aB1NbCAjuB
x/C9b8+9Xycc7rF7AkQ7DESVjaSIL8Mk6iyUYZwTd6PMONFfZvhCfwugTA2RkSkVm+zoi+eq
EN8X7xXH4bRWnJBrwIcP/3zYQY7ynzZWPrlMROf35I4+a/zj+ZHcHf+fgRZslE30bQ+P3oNu
cHHYWWQKUzwzNBKxIQXogiEYG+LpbwoyaSP2HQtxIqa1lxzcnkyXDdYApG2BdrslPBO/qYzn
Z4Hq27g3M9ZK4Z2Md5reiTzFN3fZSSFhA/nmaKPDMcDv4EgR6YHqyrceBZVrOly4DE1obLkB
DQRSfIohAQgAx3/vLQda+YhXcuGGNe81egYt8LC8AONhj0rZ2XZM7V0z2i2XZJ/CevtKjarK
MNFTfTjQuUbokXb0u9QjYANJlGvZVY1P/YzORJwEc2tm/2+ZyFh2iPFjnTKF7ANkjxKsWfbw
Y/g/saU8FwyddaMHWXLp0BpTTeAlbFvUjqDJlZoen33Gu2aqF7GGHoDV0tkDpMY4M0VybvOe
oqrNAbukujuq/b80XIhIb644hhRrArufGRVR+6LoRXewAHAmWFBydUgTkpuyIzar36NE25EX
M2Unz12F3EY7L9E4HSPFRRwc0nojcKydLETs5lHB4sR2SyoyMWH0iSi/SmTMSDBpFwARAQAB
iQElBBgBAgAPBQJSfIohAhsMBQkJZgGAAAoJEFEuH5ZdDSRzT8sH/i5l1+56naAHMvT3GAeY
kz1rWWJbpUHeyFEA/0VfemzZaz+N4aqPB2Lv6ejwL9AqRpcl/XS8oxQFmpNaZ3n8sGBwgfEu
naCzTANqnazhVEfOxfSH5EPHXI1hFXJDh9nYNKJ4gpfSD6DifxY4ZtAbXIYA4HlD4qskwr27
NdMmeeZ+B7qFU2HUO24wZ+7Sh+otD1CulXsCcRuAhsKViBmk68rKdBk3vIZW0BE57CHmpw93
lQgGGab5ylkNb/L0UUzV0BvzHO2YKyK/ylDnkVUsKpz7wrO1Bm1VWLMXfehIRVRbzdQL8Rfe
aQbvLi6haofons03qtXzn3OChmzjw5XbOlk=
=EbZT
-----END PGP PUBLIC KEY BLOCK-----
```

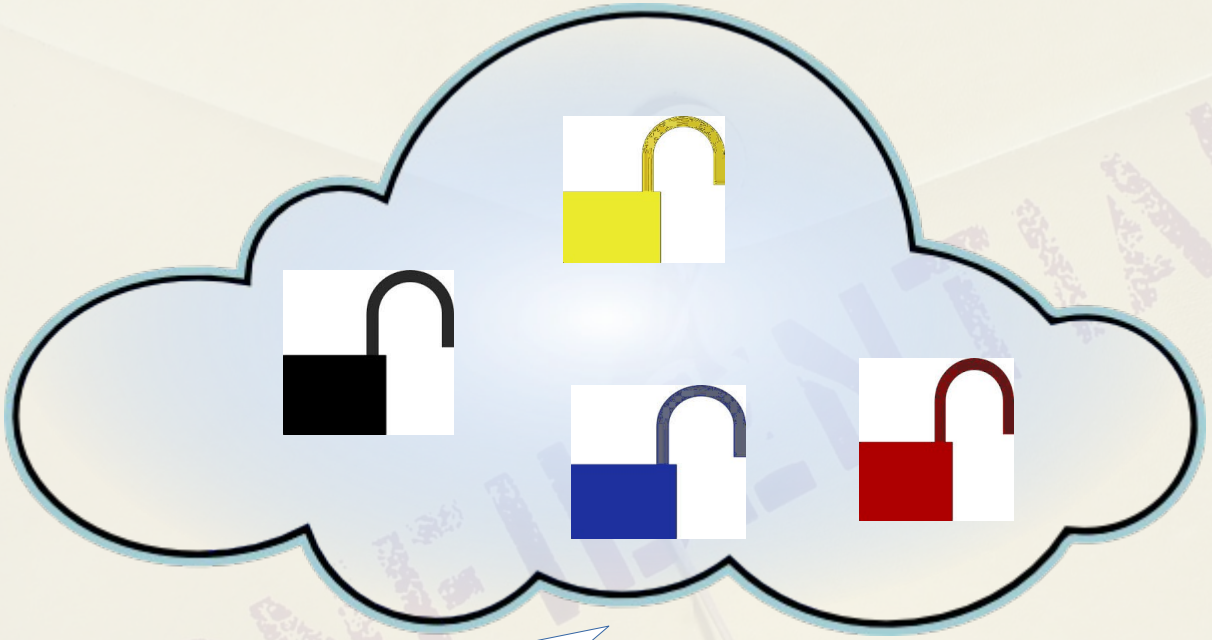
PGP Public Key (Example)

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: SKS 1.1.4
Comment: Hostname: pgp.rediris.es

mQENBFJ8iiEBCACxPavt1+Kpc1O4mzE4HfIF3APzJBzgV6iAIvbiCz1X4ZU3RDLiIs5nyLyd
v2VagHk5VsAcFLev7djb9hPhqgJAP5zrXwn/pQxwxLDHmisTgh2I6HpwtXsGTYoOsosli+P+
KkL/d9VW/AsFJpuW2c/U2sFKAgte6h4YUo7VRpcUm7scp2PLLWugsn4FgJ5m/6eYi3TEphSk
HA9UZyx0zo+BGuk5fZ7pgXI9PcAaGN7XZ+1IuSrI5Rro5uIg3ylWoH0KBLD+giHIkv8CKpwA
icKVHhe8CIKIJBM3S5eoA/aig7t08I56tTNU22lyrnusgsgxRssIXq5Q3fyDsnfTD+R/ABEB
AAG0M1JpdmVyIENpdHkgRnJvbnQgRGVzayAxIDxyaXZlcmN[illegible]GluaWNAdGVsdXMubmV0
PokBPgQTAQIAKA[illegible]HgECF4AACgkQ
US4fll0NJHOd1w[illegible]k8aB1NbCAjuB
x/C9b8+9Xycc7r[illegible]kSkVm+zoi+eq
EN8X7xXH4bRWnJ[illegible]lE30bQ+P3oNu
cHHYWWQKUzwzNB[illegible]drslPBO/qYzn
Z4Hq27g3M9ZK4Z[illegible]Oly4DE1obLkB
DQRSfIohAQgAx3[illegible]ZJ/CevtKjarK
MNFTfTjQuUbokX[illegible]7ANkjxKsWfbw
Y/g/saU8FwyddaMHWXLp0BpTTeAlbFVUjqDJlZoen33GuZaqF7GGHoDV0tkDpMY4M0VybvOe
oqrNAbukujuq/b80XIhIb644hhRrArufGRVR+6LoRXewAHAmWFBydUgTkpuyIzar36NE25EX
M2Unz12F3EY7L9E4HSPFRRwc0nojcKydLETs5lHB4sR2SyoyMWH0iSi/SmTMSDBpFwARAQAB
iQElBBgBAgAPBQJSfIohAhsMBQkJZgGAAAoJEFEuH5ZdDSRzT8sH/i5l1+56naAHMvT3GAeY
kz1rWWJbpUHeyFEA/0VfemzZaz+N4aqPB2Lv6ejwL9AqRpcl/XS8oxQFmpNaZ3n8sGBwgfEu
naCzTANqnazhVEfOxfSH5EPHXI1hFXJDh9nYNKJ4gpfSD6DifxY4ZtAbXIYA4HlD4qskwr27
NdMmeeZ+B7qFU2HUO24wZ+7Sh+otD1CulXsCcRuAhsKViBmk68rKdBk3vIZW0BE57CHmpw93
lQgGGab5ylkNb/L0UUzV0BvzHO2YKyK/ylDnkVUsKpz7wrO1Bm1VWLMXfehIRVRbzdQL8Rfe
aQbvLi6haofons03qtXzn3OChmzjw5XbOlk=
=EbZT
-----END PGP PUBLIC KEY BLOCK-----
```

Send your public key to your friends
By email

PGP Email



Just post public keys in “the cloud” (a.k.a cyperspace) Everyone's public keys can be uploaded to a selection of “Public Key Servers” on the Internet, e.g.

pool.sks-keyservers.net

PGP Email

One practical PGP implementation:

- GnuPG (Gpg4win)

+

- Mozilla Thunderbird Email

+

- Enigmail Add-on

PGP Email

Why this combination?

- Open source in all its components (open source encryption tools are generally considered more secure than proprietary/closed ones)
- Free – no cost
- Cross platform for Windows, Mac and Linux (consistent user interface makes support and troubleshooting much easier)
- Easy to set up. Very easy to use

PGP Email

Early experience in a small community:

- Used by office **MOAs**, rather than the doctors themselves. Not that useful as a workstation desktop utility for doctors.
- Does not replace fax machine, or snailmail, but supplements it and cuts down on fax and mail traffic, and substantially reduces scanning and faxing workload in some offices
- Doctors like the prefect text resolution. MOAs like the instant speed and convenience of use and transmission.
- Things occasionally do go wrong, usually key mixup issues, so it is a good idea to ask for email return receipts to confirm delivery of the document
- PGP email is a good fit for small general practice groups or for solo specialist offices where MOAs tend to multitask (the same MOA doing front desk as well as back office tasks, e.g. scanning, dealing with incoming and outgoing correspondence)
- Most MOAs seem to be able to use it, but some find the initial setup daunting and are scared off when things go wrong (learning curve).

PGP Email

Troubleshooting:

- PGP configuration issues
- Email configuration issues
- Complicated “message rules”
- Incorrect key selection
- Defunct / obsolete keys - “revoking” keys
- Hard drive crashes, new computers, reformatted OS, lost keys

- It helps to have a “PGP champion” MOA in each office, who knows how to tweak the setup and configuration.

PGP Email

Demonstration and walk-through

PGP Email

Useful Online Resources:

- How-to on the Mozilla Thunderbird site: https://support.mozilla.org/en-US/kb/digitally-signing-and-encrypting-messages
- How PGP works: http://www.pgpi.org/doc/pgpintro/
- To add a Gmail IMAP account to Mozilla Thunderbird: http://email.about.com/od/mozillathunderbirdtips/qt/et_get_gmail.htm

PGP Email

Need for dedicated email address?

Concomitant use of other email clients?

Office policy decision

PGP Email

Questions?