Firearms & Freedom

OFFICIAL NAPFN NEWSLETTER

Firearms & Freedom Official Newsletter of the North American Patriots Free Network	PGP empowers people to take their privacy into their own hands. There has been a growing social need for it. That's why I wrote it. – **Philip R. Zimmermann**

Vol.21, No.08 - - - - 6 Aug 2018

AUTHENTICATING DIGITAL DOCUMENTS

"Back in the Day" documents were signed with Pen and Ink. While skilled handwriting analysts were pretty good at authenticating signatures – particularly originals – critical documents would also be notarized or witnessed.

This doesn't work in a digital world.

Here's my pen & ink signature – signed on a digital device

Obviously you can cut and paste it,-- it's trivial to do so – on a computer.

So – how do we authenticate documents in a digital age?

The first part is simple: using PGP or GnuPG you can sign the document, digitally.

Let's work through an example to see how this is done

Here is the Test Message:

```
This has been a test.
Had it been an actual alert
you would not have received this message.
```

To sign the message DIGITALLY – I use PGP or GnuPG. Here we are dealing with Digital Authentications so we will look at the affect of the digital signature.

Firearms & Freedom

OFFICIAL NAPFN NEWSLETTER

Firearms & Freedom
Official Newsletter of the North American Patriots Free Network

PGP empowers people to take their privacy into their own hands. There has been a growing social need for it. That's why I wrote it. – **Philip R. Zimmermann**

Vol.21, No.08 - - - - 6 Aug 2018

The signed message can have different formats. Here is the Basic form:

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

This has been a test.
Had it been an actual alert
you would not have received this message.

-----BEGIN PGP SIGNATURE-----

iQIzBAEBCAAdFiEE6xdFHcvTCJ+AlVAO9ulBsU3qDa0FAltoPBYACgkQ9ulBsU3q
Da0UXA/9GoysIsU3vf9RVrejmvEB80geZihEw7GP0NFJmCE0ROASusMuutdf4DDf
Gr2f6YWuhR9dxKCPCigjAFBvuFgQqbbn/8PZa9og9qB8bmYxdXJ3RqhTQcIv6oBA
Px8TGjQtUzNluCA+z45ruuNjghUJoe+tAtYSSbC25t5UzuSq5AUFC4aA+HdoF91r
SZl0lz73v3NGq3fJpKiOzGsyhg+DumkZufcE/mTgHNtVSX7pgh9fHW6kTRz8kyGS
Ygs+FqDvWgKUYGRLJXUlC/IKTkiS4RdK2F3dh4prXd4XBr4LFYKM7qCZjV1zoZ7D
ZZwFtbnTWs9ADyoqZEzo9ZgbYX1L7Ks9iY0vQFurST3g4aVwucRLa4pWPqXANwZc
o5LiP7CkbblIwqEAQ8vhRXcit1M3OnFkrXgWYGEQxYLfo1kCJV/uQvkngnnpGGpL
T2dVufJLRd/sEfaZD6LfCCC/Mz6lUJFT4ofb+2jwCTkKc7Jtc2DoywNAYPNg7Cek
+lO6CkpMaWmSD9GFzrhdUSe4IjfMn7IWlWCFNcz61ZI0OQ6X6BNjFPtVfv1EFwrR
11WwNF+zAc+WZZn8iib+54BJzsXDXb6hL8nqIOhghSqwvXiFJ7xkDYYQwQCbh3kz
1h4N6gkeBbr+ZKN4rsS9IFESVwSpCmMHRJbmS+GWNS5Mrf2SLR8=
=aEto
-----END PGP SIGNATURE-----
```

On receipt of a PGP/GnuPG signed message you can verify authenticity:

```
$ gpg --verify test.txt.asc

gpg: Signature made Mon 06 Aug 2018 08:16:22 AM EDT
gpg: key EB17451DCBD3089F8095500EF6E941B14DEA0DAD
gpg: Good signature from "Mike Acker”
```

Firearms & Freedom

OFFICIAL NAPFN NEWSLETTER

Firearms & Freedom
Official Newsletter of the North American Patriots Free Network

PGP empowers people to take their privacy into their own hands. There has been a growing social need for it. That's why I wrote it. – **Philip R. Zimmermann**

Vol.21, No.08 - - - - 6 Aug 2018

Thus far we know three things:

1. The message is from someone who calls himself “Mike Acker” and is using key EB17 451D CBD3 089F 8095 500E F6E9 41B1 4DEA 0DAD
2. The plain text of the message has not been altered in transit.
3. Encyrption was not used.

The question then is : is this a fake? Or is it from Mike Acker? Just using PGP is not enough: you have to do your part. Call Mike and ask him for the “fingerprint” on his PGP key

He should respond:

EB17 451D CBD3 089F 8095 500E F6E9 41B1 4DEA 0DAD

If you are satisfied that you’re talking to Mike and he gives the right fingerprint, then you can go ahead and sign his key. This is the step that closes and locks the door. And it is the step that is generally not understood and then skipped.

The digital signature does you no good until you have validated/authenticated the sender’s key.

When you have validated the sender’s key you sign his key using your key. This makes his key VALID with respect to your system. When you receive a message from Mike you can now validate it and thus be assured that the message is actually from Mike and that it was not altered in transit by a third party.

Encryption is optional and can also be used when needed. PGP is mainly about authentication. Encryption products are a separate topic. PGP/GnuPG will typically use AES256 encryption – after Public Key Encryption is used to establish authenticity and to create the session key.

Firearms & Freedom

OFFICIAL NAPFN NEWSLETTER

Firearms & Freedom
Official Newsletter of the North American Patriots Free Network

PGP empowers people to take their privacy into their own hands. There has been a growing social need for it. That's why I wrote it. – **Philip R. Zimmermann**

Vol.21, No.08 - - - - 6 Aug 2018

Generally this data will be “internal and automatic” – particularly when an e/Mail client that supports PGP/GnuPG is used. I’m explaining the process here so that there may be a better understanding of its significance and implications.

One of the things that is confusing about PGP/GnuPG is the meaning of VALID|Not Valid as opposed to Trust as pertaining to keys.

When you have satisfied yourself that you know a key belongs to the person you think it should belong to then – and only then – can you consider the key VALID. To show this on PGP you sign the key with your own key. This will make the other person’s key VALID as far as PGP/GnuPG is concerned.

Trust is another matter altogether.

You may choose to trust a third party key as a valid introducer.

This would occur in an office environment. A designated person in your security department would be authorized to validate keys for everyone in the office – as well as for people in other offices that you need to communicate with.

In this case you would set the TRUST level on the key from your IT security as FULL TRUST so that keys sent to you which are signed by IT Security – would then be considered VALID in your system.

Note here that you will still need to sign the key for IT Security AND set it to Fully Trusted before the keys sent to you by your IT Security will be considered Valid. Remember: Valid means: Identity of owner has been verified and authenticated.

This is a complex topic. Every IT Department or Security Department that wants to implement PGP/GnuPG security will need to provide User Training and Help Desk Functions.

Firearms & Freedom

OFFICIAL NAPFN NEWSLETTER

Firearms & Freedom
Official Newsletter of the North American Patriots Free Network

PGP empowers people to take their privacy into their own hands. There has been a growing social need for it. That's why I wrote it. – **Philip R. Zimmermann**

Vol.21, No.08 - - - - 6 Aug 2018

Yuk? It's better than getting phished.
One more thing. In your Internet Browser you'll find a list of x.509 certificates and Certificate Authorities.

These x.509 certificates contain the public keys for the related web pages. And they are all "validated" – by one of the numerous "Certificate Authorities" – which are also listed in your browser – and none of which you have validated or set trust for.

What this means: SSL/TLS "Security" on web pages is just so much Snake Oil. A giant Linus blanket.

Anyone can get a x.509 certificate.

Security is something we all need to participate in. No one is going to give it out for free and it sure doesn't happen by itself.

NAPFN Homepage

NAPFN: Firearms and Freedom Index