

Assuming Responsibility For One'S Own Security

This is my agenda for establishing a personal digital security strategy.

Motivation

Risk Mitigation ¹

Mitigating Risks When Using PKI Processes.

The trust in processes described above hinges on the receiver's confidence that the public key they use to verify a signature actually belongs to the sender. This is where digital certificates and Certificate Authorities (CAs) come in.

Even when we can trust the public key, keys can be compromised, so although it does belong to the sender, when compromised someone other than the sender may be using it. That is where revocation comes in. The owner of the key pair must revoke the key as soon as possible when it may have been compromised (E.G. Stolen laptop). All receivers must be diligent about verifying that keys have not been revoked.

It is a sensible assumption that sooner or later every key will be compromised, in light of that our policy needs to concern itself with the lifespan that key pairs remain valid, thus reducing the extent of damage of a single compromise.

Interoperability

Since the range of platforms used by any community of interest is broad. The availability of functions we rely on to implement our security protocols must be equally broad.

Conclusion

Our policy needs to concern itself with the creation, distribution, revocation, and longevity of **PKI (Public Key Infrastructure)** key pairs. It needs to concern itself with mechanisms for discovering sender and receiver public keys.

Our policy needs to confine itself to what is reasonably available to all participants in our community of interest.

Policy

We mandate the use of the OpenPGP standard for our **PKI (Public Key Infrastructure)**. This standard has remained consistent, reliable and widespread for over a decade. However because of a recent **Schism** in the OpenPGP community two diverging standards (Crypto Refresh - RFC 9580 - and LibrePGP) have emerged.

So to avoid incompatibilities our policy will mandate only what their standards hold in common. They both descend from RFC 4880. That is the common ground. So we adopt the policy of limiting ourselves to only to RFC 4880 key formats until this rift is resolved one way or another and we are back to a single standard.

For the sake of interoperability, we confine ourselves to the *Compatibility Policy* outlined below.

Compatibility Policy.

Key type

- All parties generate RSA key types

Key length

- Minimum key length 3072, 4096 is a good choice.

Algorithms

- Symmetric Encryption use AES (e.g. AES-256)

- Hash use SHA-256 or SHA-512

Summary

- Use RSA keys with a length of 4096.
- Use AES-256 for symmetric encryption.
- Exchange and verify key fingerprints through a secure, out-of-band channel such as whatsapp.

1

Risk Mitigation:

Nowadays, we must interact electronically with the various financial, medical, governmental institutions, and with our community in general.

We need to guard against others maskering as ourselves, others gaining unauthorized access to our assets, others tampering with documents, media, software, data we share, others discovering our private information. In some cases we need to protect our anonymity.

If we do not address these issues we open ourselves to many risks.