TF-CSIRT

TRANSITS I
SCM – Secure Communication Module

Authors: Olivier Caleff, Jeffeny Hoogervorst, Don Stikvoort and Nicole Harris

Version: 7.2 release

Presenter Ideas- DELETE

TF-CSIRT

- **Discussions**
  - There are four group discussions in this material.
  - Group Discussion 1: how do we trust secure comms / do this as a group and have a matrix of technical, people, legal, other on a flipchart to note down ideas.
  - Group Discussion 2: standards for secure communication. have the group do this in small groups and feedback to the main group.
  - Group Discussion 3: What tools do we use and how do we secure? Group Discussion.
  - Group Discussion 4: Is PGP still relevant? You might want to move this / not do based on the experience of the group with PGP. See right.

- PGP
  - There are three sections on PGP. An advanced group would probably only need section 5a. A less advanced group would need section 5b as well to go into further detail.
  - Section 5c is for a PGP keysigning party. Do not use if you are not going to do this with the group.

Learning Objectives

Gain an overview of elements to communicate securely

Discuss when and how a CSIRT needs to communicate securely

Know how to get started

Understand key reference documents to help you

Session Plan

- How can communications be secured?
- Tools and standards
- PGP/GPG
- Usage in the CSIRT communities
- Wrap-up

TF-CSIRT

Why Secure Communication ?

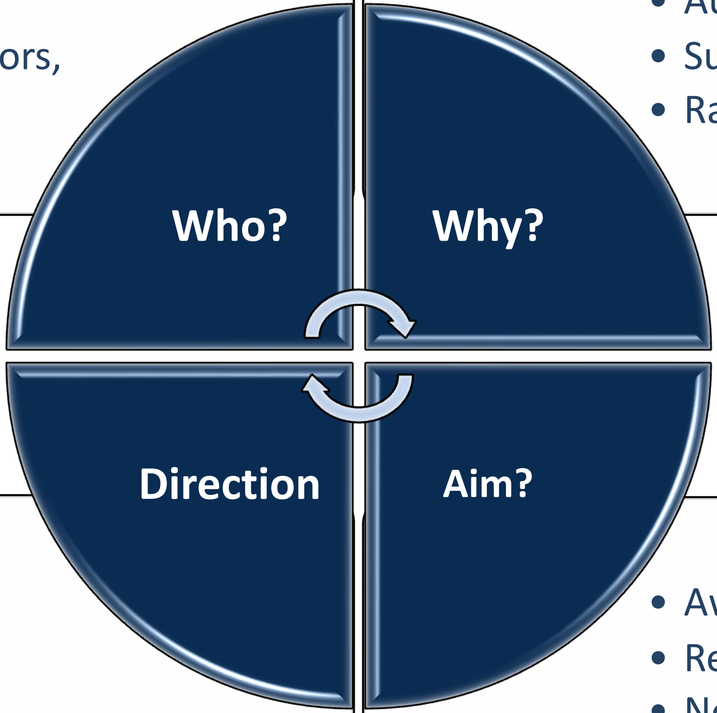
Introduction – Concepts, techniques and trust – What is “secure” ?

When it comes to communication… (1/2)

TF-CSIRT

- Stakeholders, Level of trust
- Constituents, Partners, Editors, Authorities …

- Authoritative
- Supportive
- Rationale …



Who?

Why?

Direction

Aim?

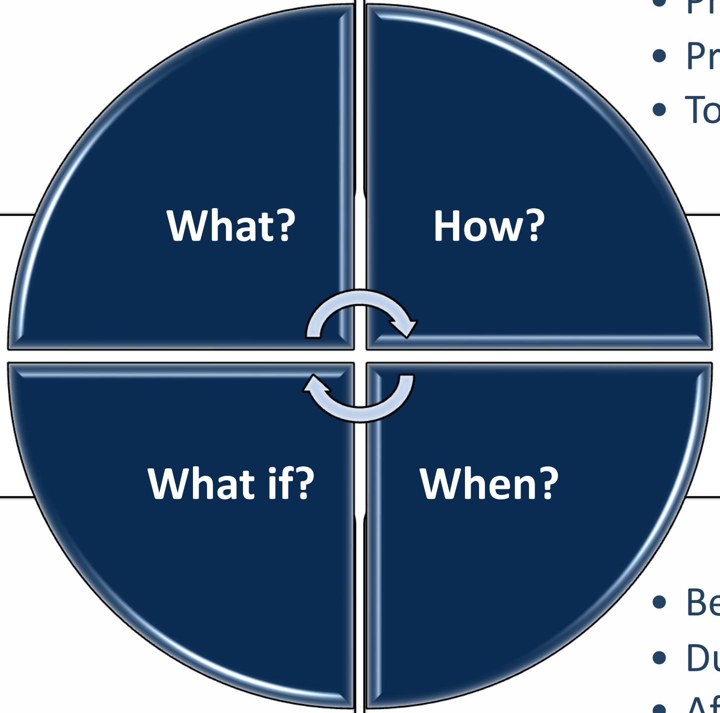
- Incoming
- Outgoing
- Disseminating…

- Awareness, Information
- Request
- Notification, Alert…

When it comes to communication… (2/2)

- Context,
- Sharing policy
- Content…

- Processes
- Practices
- Tools…



- Sample use cases
- Scenario
- Potential risks…

- Before
- During
- After…

Share Your Ideas

TF-CSIRT

How do we trust / secure any communication?

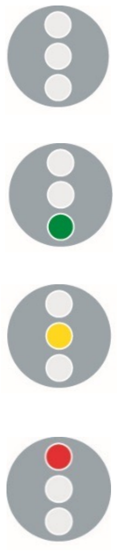
(technical, human, policy / process, combined?)

TF-CSIRT

Communication Standards and Processes

TLP Traffic Light Protocol

- **TLP CLEAR**
  Unlimited – no restrictions
- **TLP GREEN**
  Community-wide, not public
- **TLP AMBER**
  In-house (organization + clients), need-to-know distribution
- **TLP AMBER+STRICT**
  In-house (organization ONLY), need-to-know distribution
- **TLP RED**
  Personal, for named! recipients! only!



More information: https://www.first.org/tlp

NDAS and CSIRTS

TF-CSIRT

NDA = Non Disclosure Agreement

Pre-agreed process for information sharing

Legal contract (must be able to sign)

Does not preclude use of TLP

Group Discussion

TF-CSIRT

What problems might exist with using either of the standards for secure communication presented here (NDA / TLP)?

4 – Secure Information Handling Process

Information must be received securely

Information must be shared securely

Receiver must know the rules of sharing

Information must be stored securely

Does your team have a process on how to handle information securely?

TF-CSIRT

Technical Tools

Context and technical aspects

Tools

TF-CSIRT

Voice

- Phone/mobile with VoIP/Chat apps

Messaging

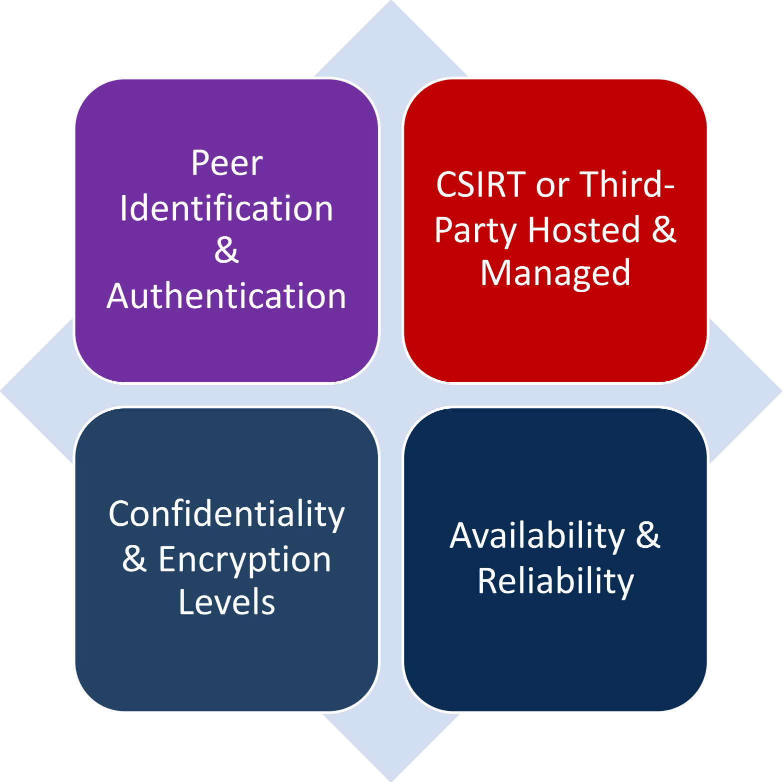
- Email, Instant Messaging

Web site or workspaces

- Web portal with form(s)

Sharing resources

- File repository, File shares



Peer Identification & Authentication

CSIRT or Third-Party Hosted & Managed

Confidentiality & Encryption Levels

Availability & Reliability

Share YourIdeas

TF-CSIRT

What tools do you use, and how secure are they?

"Secure" tools, really?

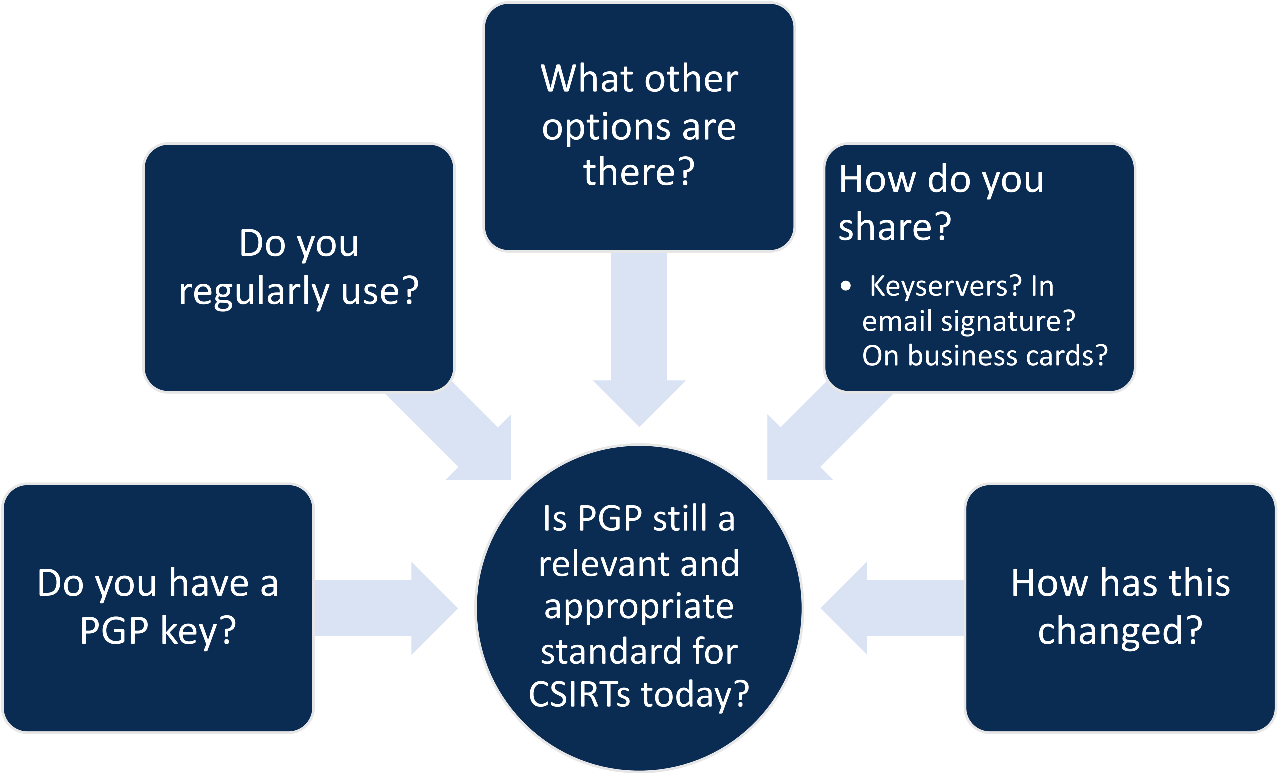
- Which ones are "secure"? What & who can you trust? Which criteria?
- Can you ever trust a "free" product? Better with a "paid" product?
- Can you trust XXX a very popular app/ecosystem?
- What about reliability and sustainability?
- What are the underlying infrastructure dependencies?

TF-CSIRT

Secure e-mail and Cryptography

Group Discussion

TF-CSIRT



Is PGP still a relevant and appropriate standard for CSIRTs today?

Do you have a PGP key?

Do you regularly use?

What other options are there?

How do you share?

- Keyservers? In email signature? On business cards?

How has this changed?

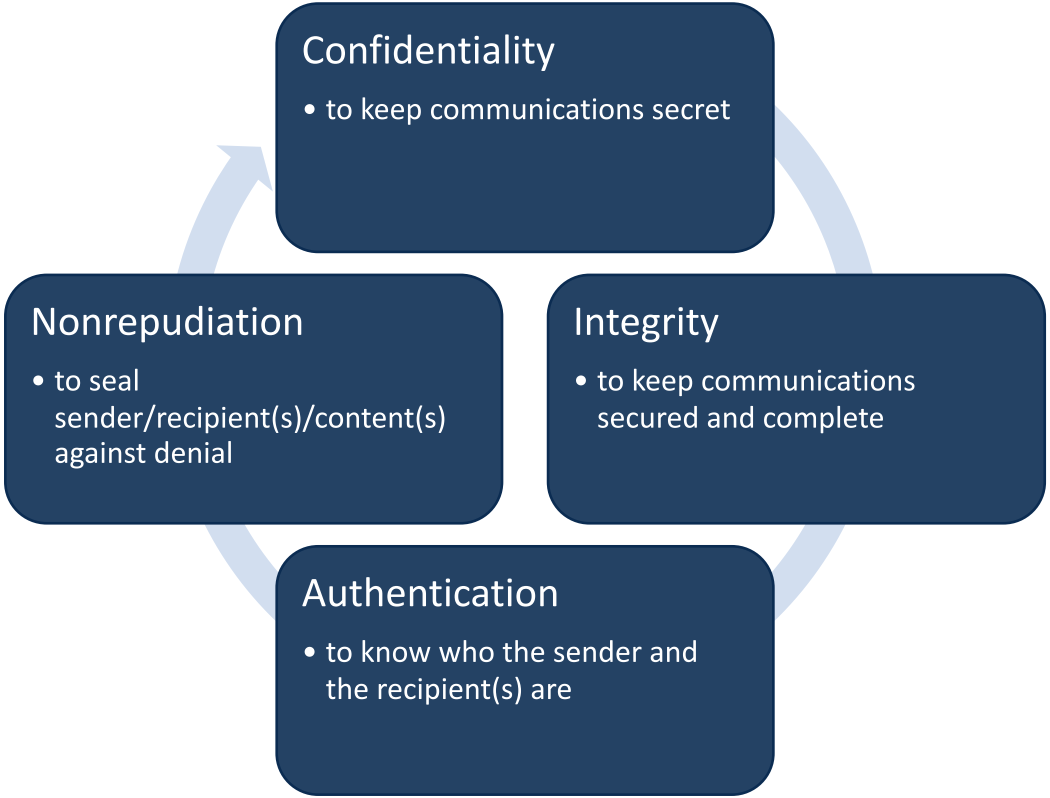
Cryptography

- **Cryptography**
  - Using algorithms to encrypt and decrypt data

- **Symmetric cryptography (Signal, file encryption, bitlocker)**
  - Symmetric encryption uses a shared secret
  - Same key/password/code used to encrypt and decrypt data
  - Faster

- **Asymmetric cryptography (PGP, Adobe Sign, TLS)**
  - Asymmetric encryption is based on secrets that are kept private and corresponding public keys
  - Different key used to encrypt and decrypt data
  - Easier to share

Security Requirements



Confidentiality

- to keep communications secret

Integrity

- to keep communications secured and complete

Authentication

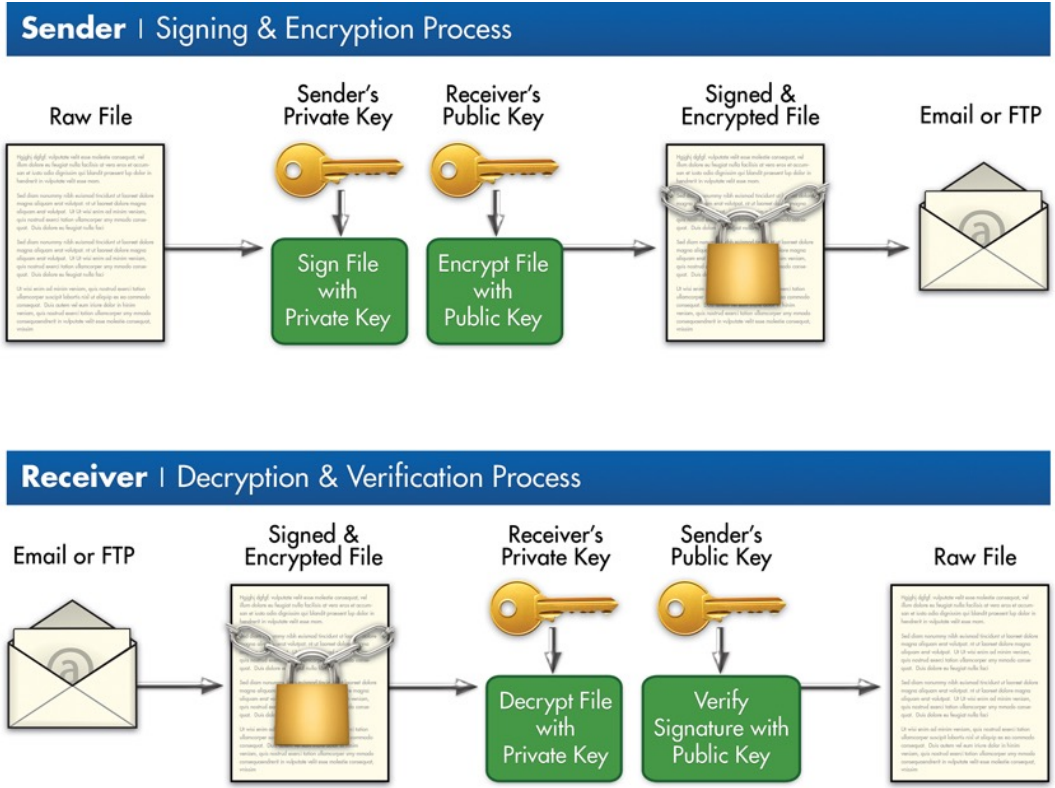
- to know who the sender and the recipient(s) are

Nonrepudiation

- to seal sender/recipient(s)/content(s) against denial

Asymmetric process

TF-CSIRT



Sender | Signing & Encryption Process
Raw File
Sender's Private Key
Receiver's Public Key
Signed & Encrypted File
Email or FTP
Sign File with Private Key
Encrypt File with Public Key
Receiver | Decryption & Verification Process
Email or FTP
Signed & Encrypted File
Receiver's Private Key
Sender's Public Key
Raw File
Decrypt File with Private Key
Verify Signature with Public Key

image source: https://www.andretimokhin.com/wp-content/uploads/2013/07/OpenPGP.jpg

Relationship between identity(ies) and key(s)

- **Identity = email address ≠ a real person**
- A direct association between an identity and a keypair
- It’s not a one-to-one relationship
  - A keypair can be related to multiple email addresses

Example

```
pub  4096R/40009346 2018-01-12 Olivier Caleff <security@caleff.com>
                    Olivier Caleff (OPS-T) <opst@caleff.com>
                    Olivier Caleff (CSIRT) <csirt@caleff.com>
                    Olivier Caleff (FIRST) <first@caleff.com>
                    Olivier Caleff (TF-CSIRT) <tfcsirt@caleff.com>
                    Olivier Caleff (TRANSITS) <transits@caleff.com>
                    Olivier Caleff (OpenCSIRT) <opencsirt@caleff.com>
Fingerprint=3D75 29D8 0593 8153 5FC6  55C9 6BFC B595 4000 9346
```

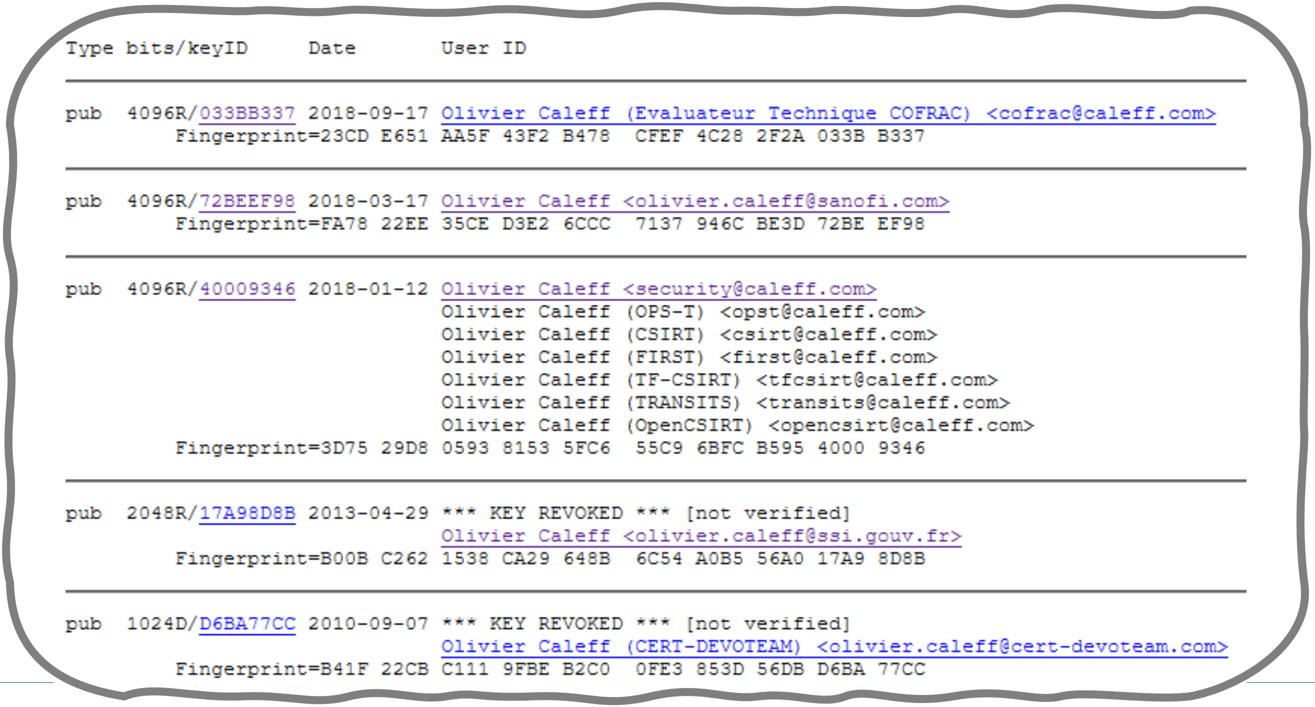
  - An email address can be related to multiple keypairs… but is it wise?

Relationship between identity(ies) and humans

TF-CSIRT

- A human can have multiple employers over his career, and different roles at any given time
- A human can have multiple valid and obsolete email addresses

Example



```
Type bits/keyID     Date       User ID

pub  4096R/033BB337 2018-09-17 Olivier Caleff (Evaluateur Technique COFRAC) <cofrac@caleff.com>
         Fingerprint=23CD E651 AA5F 43F2 B478  CFEF 4C28 2F2A 033B B337

pub  4096R/72BEEF98 2018-03-17 Olivier Caleff <olivier.caleff@sanofi.com>
         Fingerprint=FA78 22EE 35CE D3E2 6CCC  7137 946C BE3D 72BE EF98

pub  4096R/40009346 2018-01-12 Olivier Caleff <security@caleff.com>
                               Olivier Caleff (OPS-T) <opst@caleff.com>
                               Olivier Caleff (CSIRT) <csirt@caleff.com>
                               Olivier Caleff (FIRST) <first@caleff.com>
                               Olivier Caleff (TF-CSIRT) <tfcsirt@caleff.com>
                               Olivier Caleff (TRANSITS) <transits@caleff.com>
                               Olivier Caleff (OpenCSIRT) <opencsirt@caleff.com>
         Fingerprint=3D75 29D8 0593 8153 5FC6  55C9 6BFC B595 4000 9346

pub  2048R/17A98D8B 2013-04-29 *** KEY REVOKED *** [not verified]
                               Olivier Caleff <olivier.caleff@ssi.gouv.fr>
         Fingerprint=B00B C262 1538 CA29 648B  6C54 A0B5 56A0 17A9 8D8B

pub  1024D/D6BA77CC 2010-09-07 *** KEY REVOKED *** [not verified]
                               Olivier Caleff (CERT-DEVOTEAM) <olivier.caleff@cert-devoteam.com>
         Fingerprint=B41F 22CB C111 9FBE B2C0  0FE3 853D 56DB D6BA 77CC
```

How to Manage Keys?

Single Key, Single Person

- Pros: easier to manage to easier find you
- Cons: anyone can see your identities, your life can tracked via roles, might not meet company policy

Multiple Keys, Single Person

- Pros: easier to split identities
- Cons: people may use the wrong key

Shared Team Key

- Pros: simple approach
  Cons: against authentication principle, issues when people leave

Main Key with Subkeys for Team

- Pros: Easier to manage people joining and leaving
- Cons: Needs active management, might not fit with other personal communication

History and Acronyms

TF-CSIRT

PGP = Pretty Good Privacy

- 1991 - Phil Zimmerman
- Now commercial
- RFC1991

OpenPGP

- 1997, IETF WG
- Non-proprietary
- RFC2440 / 4880

GPG = GnuPG

- 1999, Werner Koch
- Implementation of RFC4880

S/MIME

- 1995, RSA Data Security
- RFC2045 (MIME)
- RFC3850/1

TF-CSIRT

External Communication

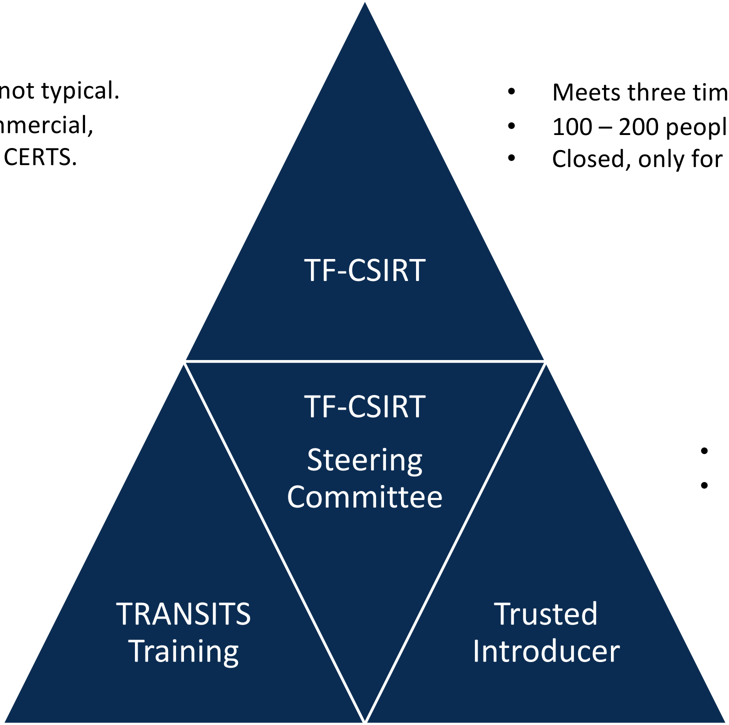
Build your Network

TF-CSIRT, Trusted Introducer and TRANSITS

TF-CSIRT

- GÉANT Task Force but not typical.
- Even mix of NREN, commercial, government / national CERTS.

- Meets three times a year.
- 100 – 200 people per meeting.
- Closed, only for teams in TI.



- Provides both taught courses and licenses materials for general use.

- Procured service.
- Supports listing, accreditation and certification of teams.

What is Trusted Introducer?

TF-CSIRT

- A process for CSIRT teams to get to know each other and build trust.
- A registry of CSIRT teams.
- A set of tools that can be used by the teams for incident response.
- An accreditation and certification process to help teams express their trustworthiness.
- Traditionally Europe + surrounding regions but now accepts all teams.

Three Processes of TI

TF-CSIRT

Listing

- Free service
- Simple team listing in registry
- Must be supported by 2 existing teams
- Can attend TF-CSIRT general sessions

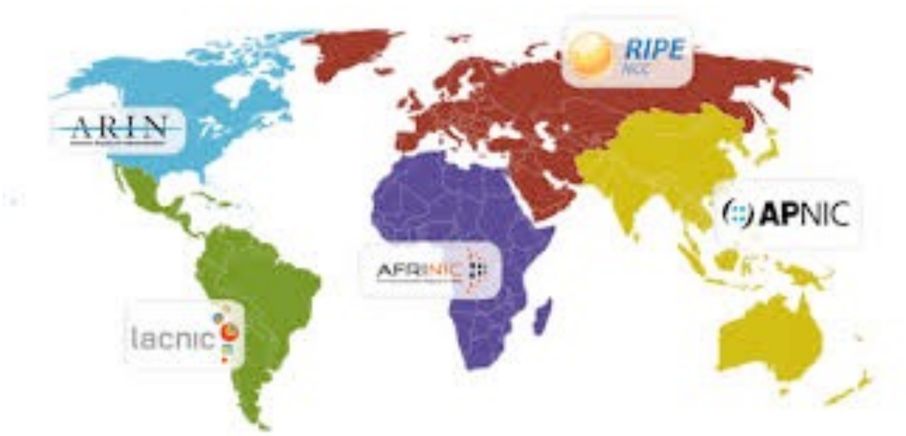
Accreditation

- Cost of 1,200 euros per year, plus one time fee (800 euros)
- Supported self-assessment against a set of criteria
- Can attend closed meetings, be on closed lists, access closed area of website

Certification

- Cost of 2,400 euros (in Europe, more outside)
- Full audited certification

Partners



We align with the Regional Internet Regions

- APCERT,
- AfricaCERT,
- AMPARO,
- FIRST,
- ENISA,
- RIPE.

Mission

The mission of TF-CSIRT is to facilitate and improve the collaboration within the European CSIRT community to make cyber space a better place

Why Us?

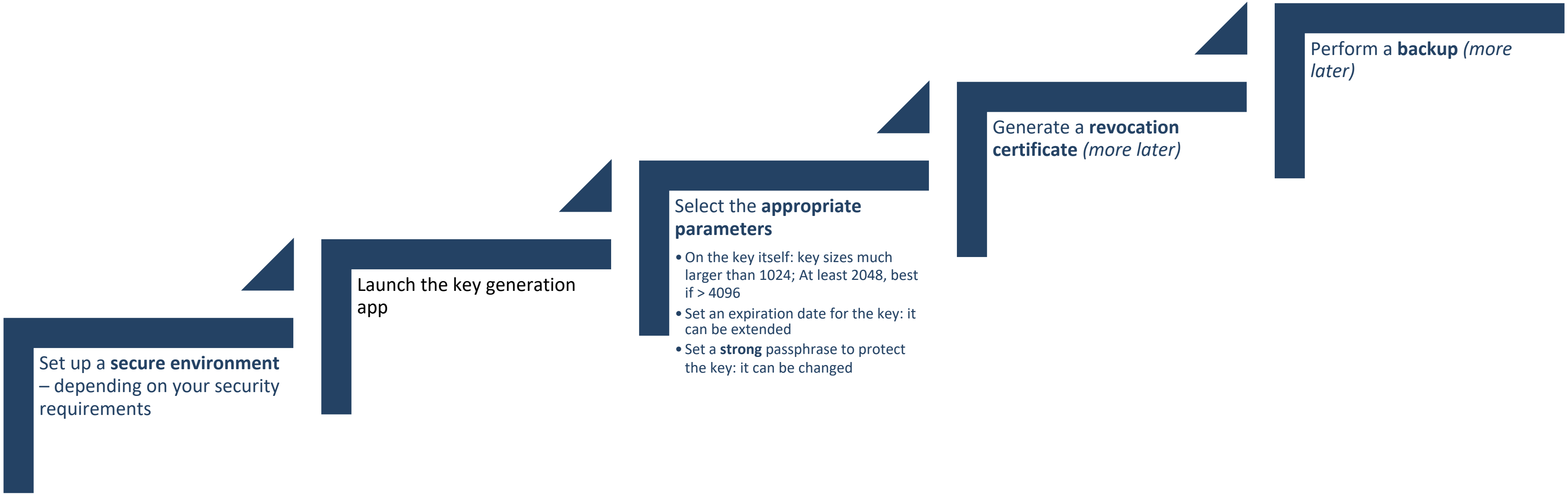
TF-CSIRT

"TF-CSIRT operates with a European mindset, and strives to make it services and meetings inclusive, accessible, easy-to-reach, and affordable for all CSIRTS in Europe – regardless of sector. Through the Trusted Introducer service, TF-CSIRT can offer well-maintained and up-to-date information and provide teams with recognition status via its differentiated listing, accreditation and certification processes."

TF-CSIRT

Getting started with PGP / GPG

Key generation



Set up a **secure environment** – depending on your security requirements

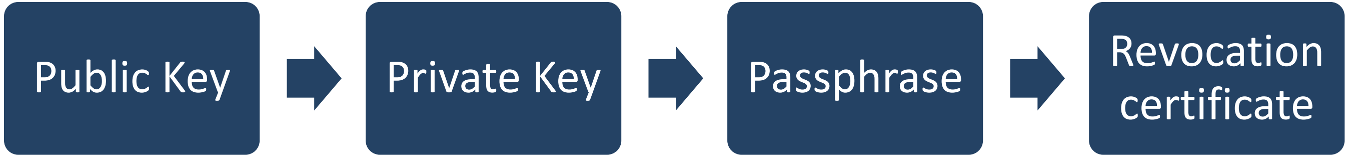
Launch the key generation app

Select the **appropriate parameters**

- On the key itself: key sizes much larger than 1024; At least 2048, best if > 4096
- Set an expiration date for the key: it can be extended
- Set a **strong** passphrase to protect the key: it can be changed

Generate a **revocation certificate** *(more later)*

Perform a **backup** *(more later)*



Key generation

- **Fingerprint** - a recognisable 128-bit hash value, in hexadecimals like
  - 3D75 29D8 0593 8153 5FC6 55C9 6BFC B595 4000 9346

- **KeyID** is identical to last 8 or 16 hexadecimal positions → '0x40009346' or '0x*6BFCB595*40009346’

- Check fingerprint **and** name/e-mail
  - The fingerprint is not guaranteed unique

Key storages and sharing

- **Key storage**
  - Export the private key and keep it in a secured and controlled location
  - Export the revocation certificate
  - Keep the passphrase in a safe location

- **Key sharing**
  - Public announcement
  - Upload on major publicly available servers
    - https://pgp.mit.edu/ – http://pgp.circl.lu/ – https://pgp.surfnet.nl/
    - http://pool.sks-keyservers.net/
    - Others: https://keys.openpgp.org/ – https://keyserver.pgp.com/
  - Sharing with a CSIRT community
  - Next step: Ensuring of authenticity of the shared key

Key updates and revocation

- **Key update**
  - Adding an email address
  - Extending the duration of the validity

- **Key revocation**
  - When the key becomes useless
  - When there are some risks that it has been compromised

- Do not think about modifying or deleting
- **Revocation is the only way**
  - What do you need to revocate a key?

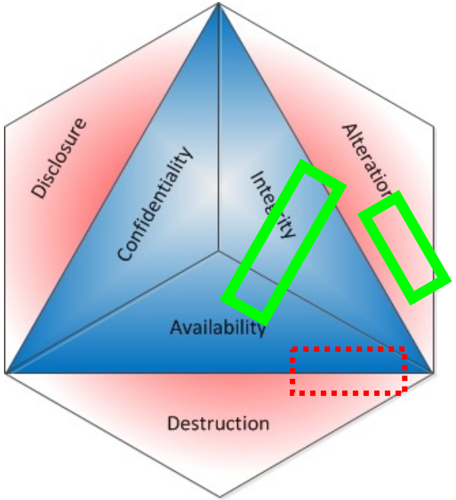
Key Signing Party

- Gathering to cross-sign the keys of participants
- Participants print their key-data (email, fingerprint) and bring their ID ready
- For each **individual** key presented, verify individual’s identity (against passport or national ID with photo)
- Do this effectively by rotating like the track of a tank
- Sign all the keys that you verified (this is best practice – but you decide based on your policy)
- Need electronic copy of public key from keyservers
- Add signed keys to keyservers in order to have your signature visible to the world

Wrap-up

TF-CSIRT

- **Public key cryptography with a keypair**
  - **PUBLIC** key to be **shared** over key servers
  - **PRIVATE** key to be protected and **kept PRIVATE**
- **Encryption/DEcyption**
  - ENcrypted with the recipient's public key
  - DEcrypted with the recipient's private key
  - Encryption enforces Confidentiality and Integrity,
    - Availability is not covered
  - Encrypted information can be sent over insecure communication links
- **Signing with a PRIVATE key**
  - Makes recipients know you are the author of a message



TF-CSIRT

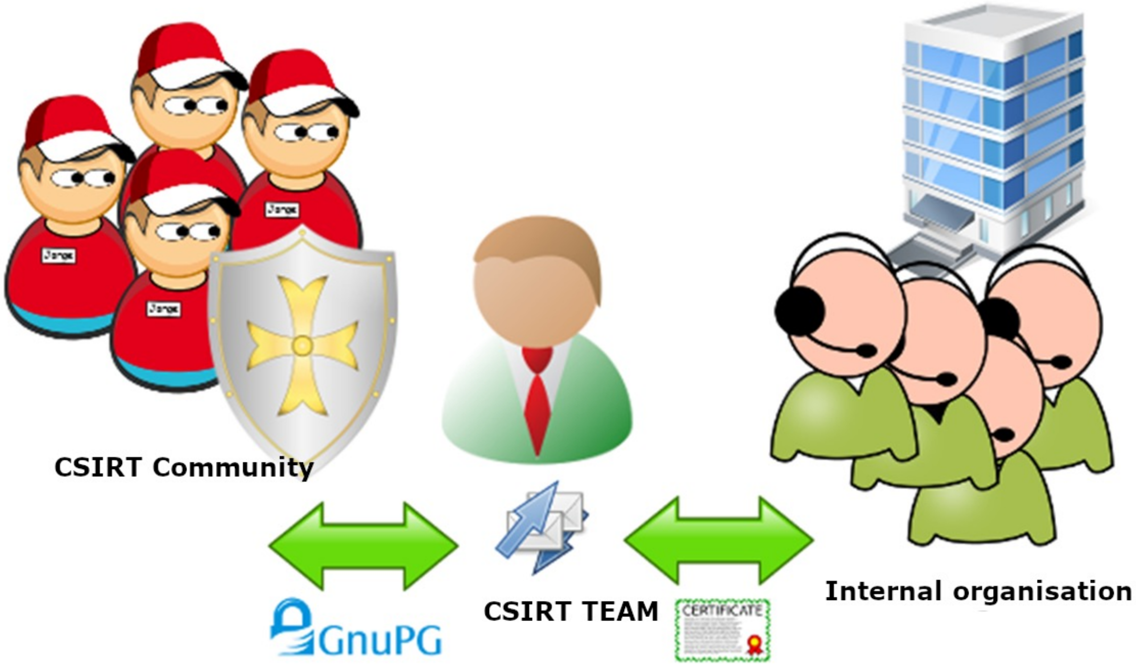
PGP Usage in CSIRT communities

Usage in the CSIRT Community

TF-CSIRT

- **A team GPG key is a MUST-HAVE**
- **The team managers (main + alternate) MUST HAVE their own GPG keypairs**
- The communication basis for tools such as MISP
- Key Sharing parties are organized at most CSIRT conferences and at all on-site TRANSITS trainings

PGP/MIME versus S/MIME



Cryptographic basis of S/MIME and PGP/MIME

Symmetric encryption uses a shared secret

- A password/code to encrypt/decrypt on both sides
- Does not scale for bigger groups or communities

S/MIME and PGP/MIME both based on:

Asymmetric encryption is based on secrets that are kept private
and corresponding public keys

- Keypair: **private/secret** and **public** keys
- Secret key unlocked by passphrase - remember that the chain is as strong as its weakest link ....
- Items encrypted with your PUBLIC key can only be decrypted using your SECRET key
- Items signed with your SECRET key can be recognized using your PUBLIC key
- Additionally, the signing process is used to ensure integrity

TF-CSIRT

PGP Keysigning Party

Key Signing Party

TF-CSIRT

- Gathering to cross-sign the keys of participants
- We’ve printed participant key-data (email, fingerprint)
- Bring your ID ready
- For each **individual** key presented, verify individual’s identity (against passport or national ID with photo)
- Do this effectively by rotating like the track of a tank
- Sign all the keys that you verified (this is best practice – but you decide based on your policy)
- Need electronic copy of public key from keyservers
- Add signed keys to keyservers in order to have your signature visible to the world

TF-CSIRT

TRANSITS I
SCM – Secure Communication Module

Authors: Olivier Caleff, Jeffeny Hoogervorst & Don Stikvoort

Version: experimental