TF-CSIRT
Trusted Introducer

Use of Crypto by CSIRTs

Luxembourg, 23 May 2019

HAW Hamburg
Prof. Dr. Klaus-Peter Kossakowski

Topics

- TI Self-Service
- GPG/PGP for TI usage
  => authenticating Team Representative
- TLS for TI usage
  => authenticating TI services
- How to proceed?

TI Self-Service: What was done?

- PGP/GPG
  - Fingerprints instead of short key ids
  - **Refreshing existing keys instead of demanding new (sub-) key submissions**
  - Self-Management for team and person entries

PGP Keys

Upload PGP Key(s)... or Add existing key...

Use key for...		PGP Key	Visibility	Delete
Main Comm.	Mailing Lists			
◉	◉	User ID: Klaus-Peter Kossakowski <Klaus-Peter.Kossakowski@trusted-introducer.org> User ID: KPK <kpk@pre-secure.de> User ID: KPK <kpk@pre-secure.com> User ID: KPK <klaus-peter@kossakowski.de> User ID: Klaus-Peter Kossakowski, Germany Fingerprint: 8F2F 5D1F F7DC 18EB 350C A9CA C115 2857 6B1A 12C0 Key type: DSA/1024 Expires: never	public	☐

PGP Keys

Upload PGP Key(s)... or Add existing key...

Use key for...

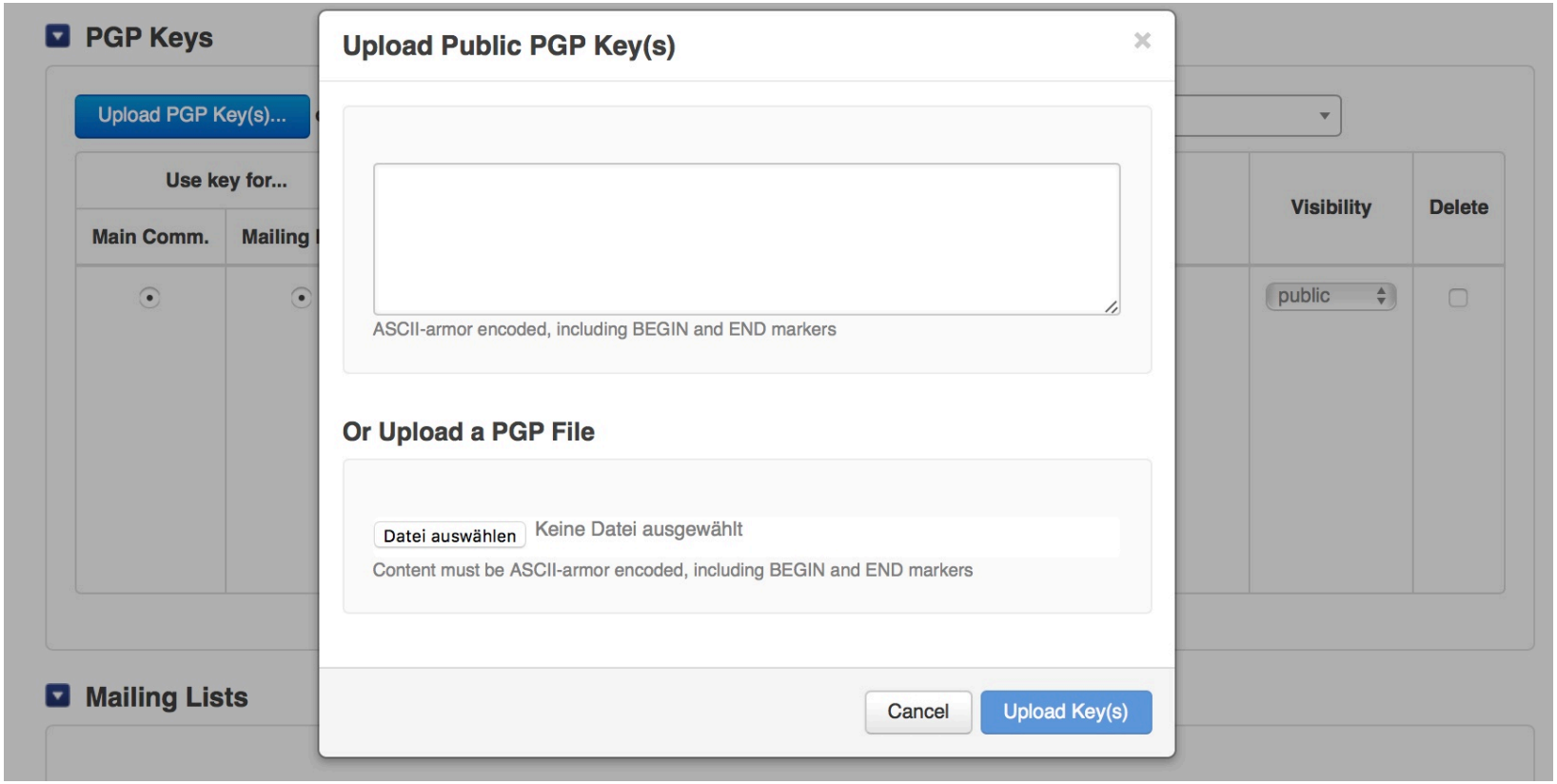
Main Comm.	Mailing Lis	ility	Delete

Expires: never

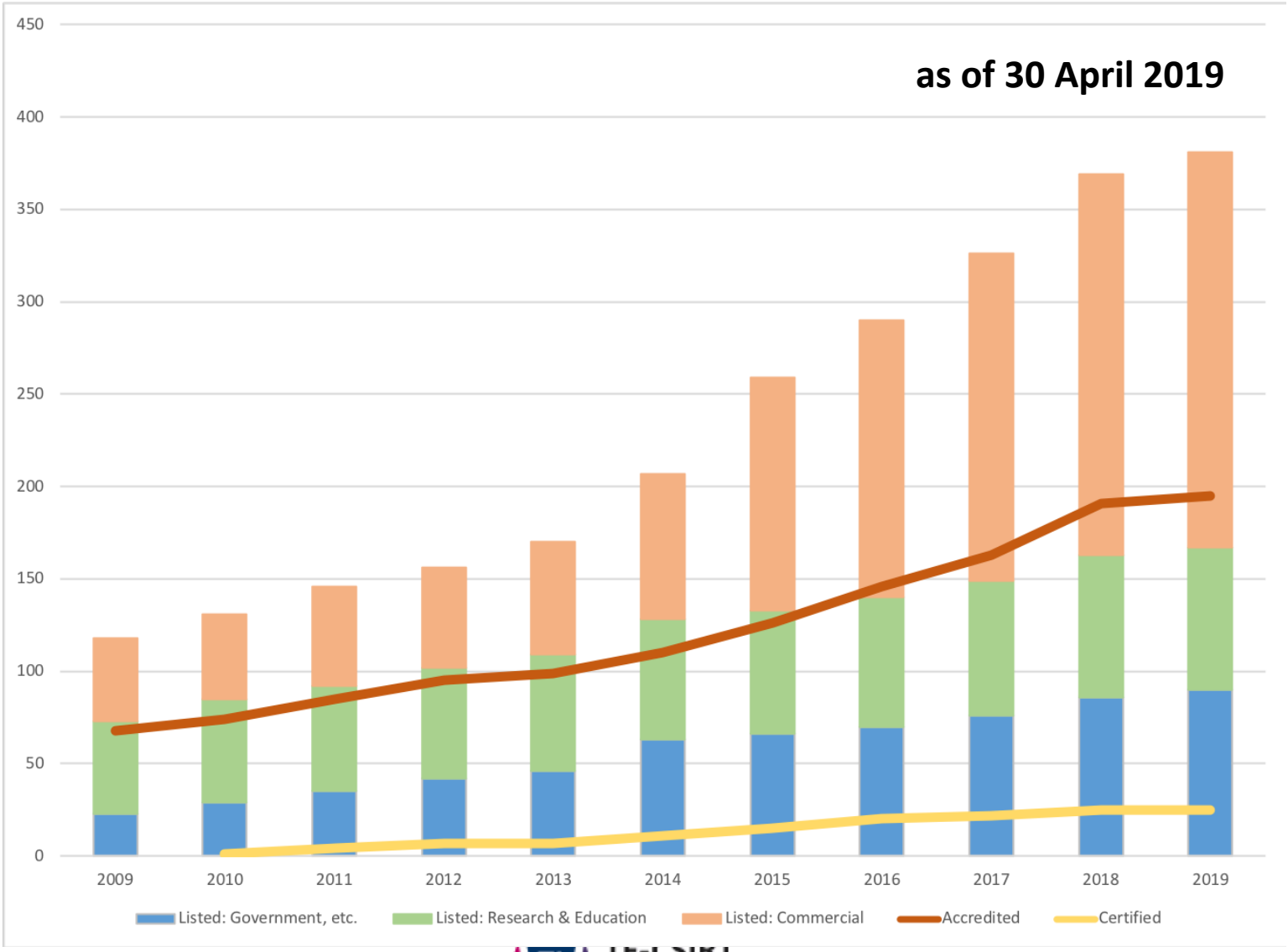
User ID: Till Doerges <doerges@pre-sense.de>
Fingerprint: F95B 5EBE 9DFC 3B30 1800 9492 2901 BAED 37FC 5954
Key type: DSA/1024
Expires: never

User ID: Juergen Sander <sander@pre-sense.de>
Fingerprint: 109B 4471 8788 BC71 A3F8 1466 9BD0 D608 DB35 058E
Key type: DSA/1024
Expires: never

Key type: DSA/1024
Expires: never



TF-CSIRT
Trusted Introducer


as of 30 April 2019
450
400
350
300
250
200
150
100
50
0
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
Listed: Government, etc.
Listed: Research & Education
Listed: Commercial
Accredited
Certified

Couldn‘t do without the Self-Service

- Interactions
  - Within 12 month: 41 listings, 28 accreditations
  - Within last 4 month: 54 re-listings, 11 listings, ...
- In the future new features like
  - Dashboard with all „issues“ (2019)
  - Assigning Proxies for votes (2019)
  - Voting on TI Associates (2019)
  - One-click registration for TF-CSIRT events (2020)

Scaling using Technology

- It all depends on the AUTHENTICATION of those allowed to change the data or to vote or ...
- Bootstrap:
  You need a trust anchor!

=> we build upon the reps GPG/PGP keys!

What if a team does

not support GPG/PGP?

What if a team is

forbidden to use GPG/PGP?

=> we build upon the reps GPG/PGP keys?

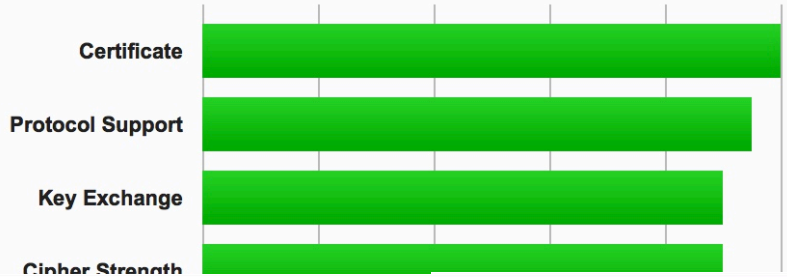
How can we?

TF-CSIRT
Trusted Introducer

Summary

Overall Rating

A



Visit our d

Configuration

Protocols

TLS 1.3	No
TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3	No
SSL 2	No

For TLS 1.3 tests, we only support RFC 8446.

BetterCrypto.ORG // December 2018

Configuration A: Strong ciphers, fewer clients

- TLS 1.2
- Perfect forward secrecy / ephemeral Diffie Hellman
- strong MACs (SHA-2) or
  GCM as Authenticated Encryption scheme

EDH+aRSA+AES256:EECDH+aRSA+AES256:!SSLv3

BetterCrypto.ORG // December 2018

Configuration B: Weaker ciphers, more clients

- TLS 1.2, TLS 1.1, TLS 1.0
- Allowing SHA-1

EDH+CAMELLIA:EDH+aRSA:EECDH+aRSA+AESGCM:
EECDH+aRSA+SHA384:EECDH+aRSA+SHA256:EECDH:
+CAMELLIA256:+AES256:+CAMELLIA128:+AES128:+SSLv3:
!aNULL:!eNULL:!LOW:!3DES:!MD5:!EXP:!PSK:!SRP:!DSS:!RC4:!S
EED:!ECDSA:CAMELLIA256-SHA:AES256-SHA:
CAMELLIA128-SHA:AES128-SHA

Proposal: Crypto Usage by/for us!

- We need to collect intelligence and check the status quo
- **We need to establish new baselines and adjust our MUST/SHOULD criteria!**

⇒ **if you have a practical interest in this, please send email to ti@trusted-introducer.org**

TF-CSIRT
Trusted Introducer

What will we do in the future?

If you have a feature request

please use email to

ti@trusted-introducer.org

or https://tib.trusted-introducer.org/wiki

TF-CSIRT
Trusted Introducer

Thank you very much for your kind attention !

https://tiw.trusted-introducer.org

mailto:ti@trusted-introducer.org

HAW Hamburg

Prof. Dr. Klaus-Peter Kossakowski

Klaus-Peter.Kossakowski@haw-hamburg.de

TF-CSIRT
Trusted Introducer