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
<table>
<thead>
<tr>
<th>Use key for...</th>
<th>PGP Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main Comm.</td>
<td>User ID: Klaus-Peter Kossakowski <a href="mailto:Klaus-Peter.Kossakowski@trusted-introducer.org">Klaus-Peter.Kossakowski@trusted-introducer.org</a></td>
</tr>
<tr>
<td></td>
<td>User ID: KPK <a href="mailto:kpk@pre-secure.de">kpk@pre-secure.de</a></td>
</tr>
<tr>
<td></td>
<td>User ID: KPK <a href="mailto:kpk@pre-secure.com">kpk@pre-secure.com</a></td>
</tr>
<tr>
<td></td>
<td>User ID: KPK <a href="mailto:klaus-peter@kossakowski.de">klaus-peter@kossakowski.de</a></td>
</tr>
<tr>
<td></td>
<td>User ID: Klaus-Peter Kossakowski, Germany</td>
</tr>
<tr>
<td></td>
<td>Fingerprint: 8F2F 5D1F F7DC 18EB 350C 99CA C115 2B57 6D1A 12C0</td>
</tr>
<tr>
<td></td>
<td>Key type: DSA/1024</td>
</tr>
<tr>
<td></td>
<td>Expires: never</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Visibility</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>public</td>
<td></td>
</tr>
</tbody>
</table>
### PGP Keys

<table>
<thead>
<tr>
<th>Use key for...</th>
<th>Main Comm.</th>
<th>Mailing List</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **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 9BDO D608 DB35 058E
- **Key type:** DSA/1024
- **Expires:** never
Upload Public PGP Key(s)

ASCII-armored encoded, including BEGIN and END markers

Or Upload a PGP File

Datei auswählen Keine Datei ausgewählt
Content must be ASCII-armored encoded, including BEGIN and END markers

Cancel Upload Key(s)
as of 30 April 2019
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?
Summary

Overall Rating

Certificate
Protocol Support
Key Exchange
Cipher Strength

Configuration

Protocols

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS 1.3</td>
<td>No</td>
</tr>
<tr>
<td>TLS 1.2</td>
<td>Yes</td>
</tr>
<tr>
<td>TLS 1.1</td>
<td>Yes</td>
</tr>
<tr>
<td>TLS 1.0</td>
<td>Yes</td>
</tr>
<tr>
<td>SSL 3</td>
<td>No</td>
</tr>
<tr>
<td>SSL 2</td>
<td>No</td>
</tr>
</tbody>
</table>

For TLS 1.3 tests, we only support RFC 8446.
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
Configuration B: Weaker ciphers, more clients

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

EDH+CAMELLIA:EDH+aRSA:EECDH+aRSA+AEGSOM:
EECDH+aRSA+SHA384:EECDH+aRSA+SHA256:EECDH:
+CAMELLIA256:+AES256:+CAMELLIA128:+AES128:+SSLv3:
!aNULL:!eNULL:!LOW:!3DES:!MD5:!EXP:!PSK:!SRP:!DSS:!RC4:!SEED:!ECDUA: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
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
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