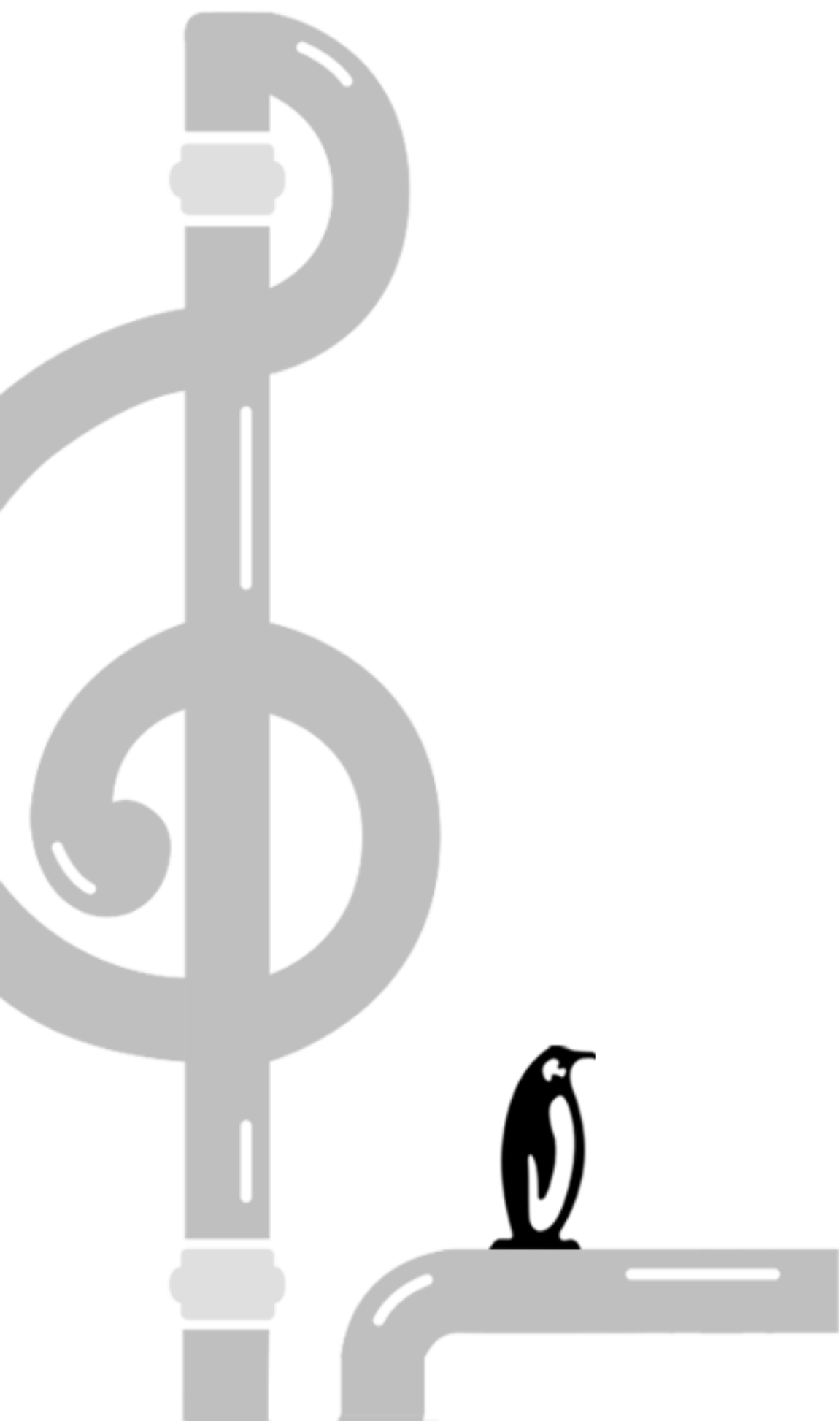


Linux Plumbers Conference

Vienna, Austria | September 18-20, 2024

PCI device authentication and encryption



LINUX PLUMBERS CONFERENCE | Vienna, Austria
Sept. 18-20, 2024

Reaching alignment on sysfs interface

1. “authenticated” attribute
2. “certificates/” directory
3. “signatures/” directory
4. “measurements/” directory



Reaching alignment on sysfs interface

- “authenticated” attribute
- read “1” or “0”
- write “re” to reauthenticate
(e.g. after adding trusted root certs to “.cma” keyring)



Reaching alignment on sysfs interface

“certificates/” directory

- contains “slot0” ... “slot7” bin_attributes
- read to see X.509 cert chain in slot
- write to provision slot with X.509 cert chain (TBD)



Reaching alignment on sysfs interface

“signatures/” directory

- log of signatures received from device
- for re-verification by remote attestation services
- if kernel not trusted or to apply custom policy
- set of attributes for each signature, prefixed by u32



Reaching alignment on sysfs interface

“signatures/” directory

- set of attributes for each signature:

“0_signature”

“0_transcript”

“0_hash_algorithm”

“0_combined_spdm_prefix”

“0_certificate_chain”



Reaching alignment on sysfs interface

“signatures/” directory

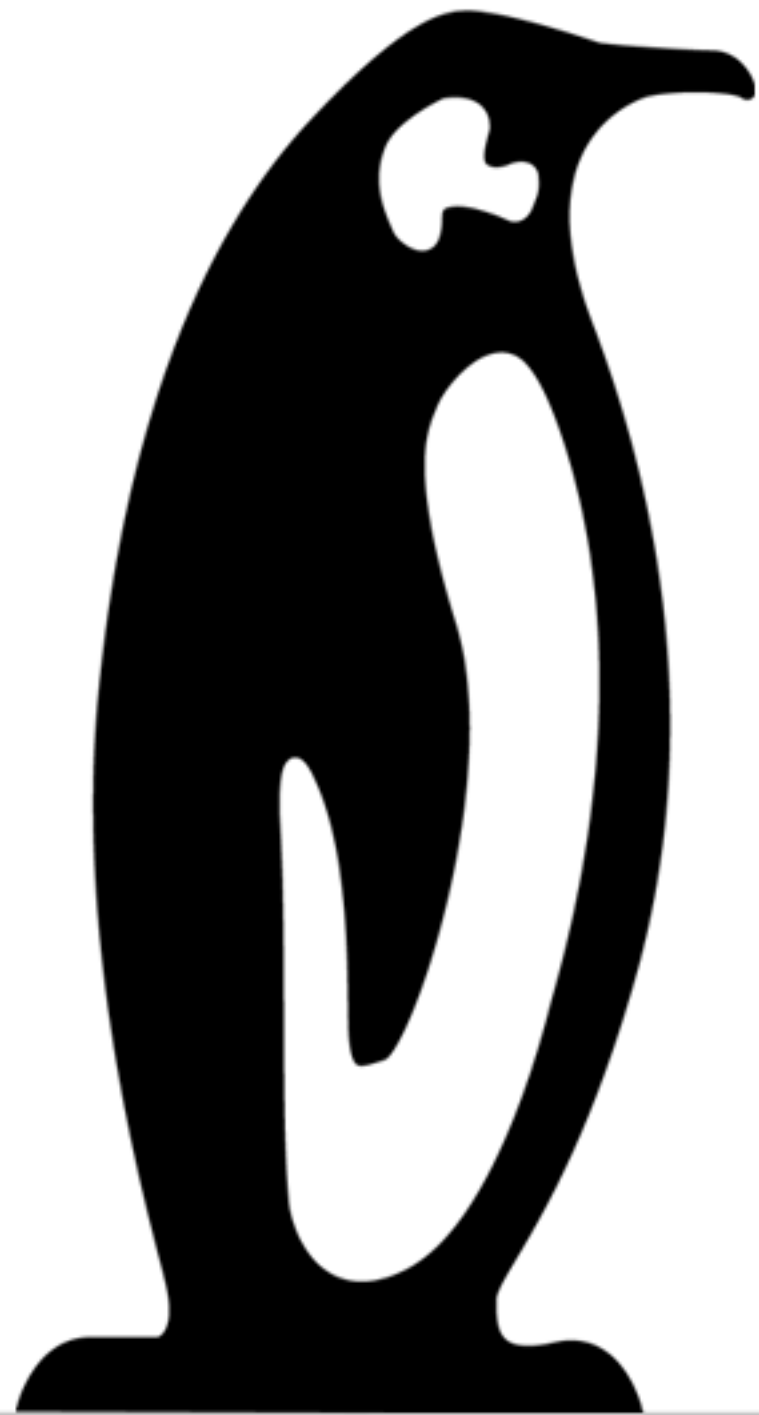
- read to see nonces used for a signature:
“0_requester_nonce”
“0_responder_nonce”
- write to control next requester nonce:
“next_requester_nonce”



Reaching alignment on sysfs interface

- “measurements/” directory (TBD)
- expose the up to 254 measurement indices:
 - “0xab_type”
 - “0xab_digest”
 - “0xab_bitstream”
- retrieve on-demand for freshness





Linux Plumbers Conference

Vienna, Austria | September 18-20, 2024

