redhat.

SMART CARD REMOTING

Daiki Ueno

AGENDA

- Smart cards?
- Remoting?
- Implementation
- Demo
- Future work

redhat.

Photo by Japanexperterna, CC-BY SA 2.0

SMART CARDS

- Card + card reader
- USB dongle
- Software implementation
- “Tokens”

redhat.

SMART CARDS

- Encryption & decryption
- Signature generation & verification
- Storage

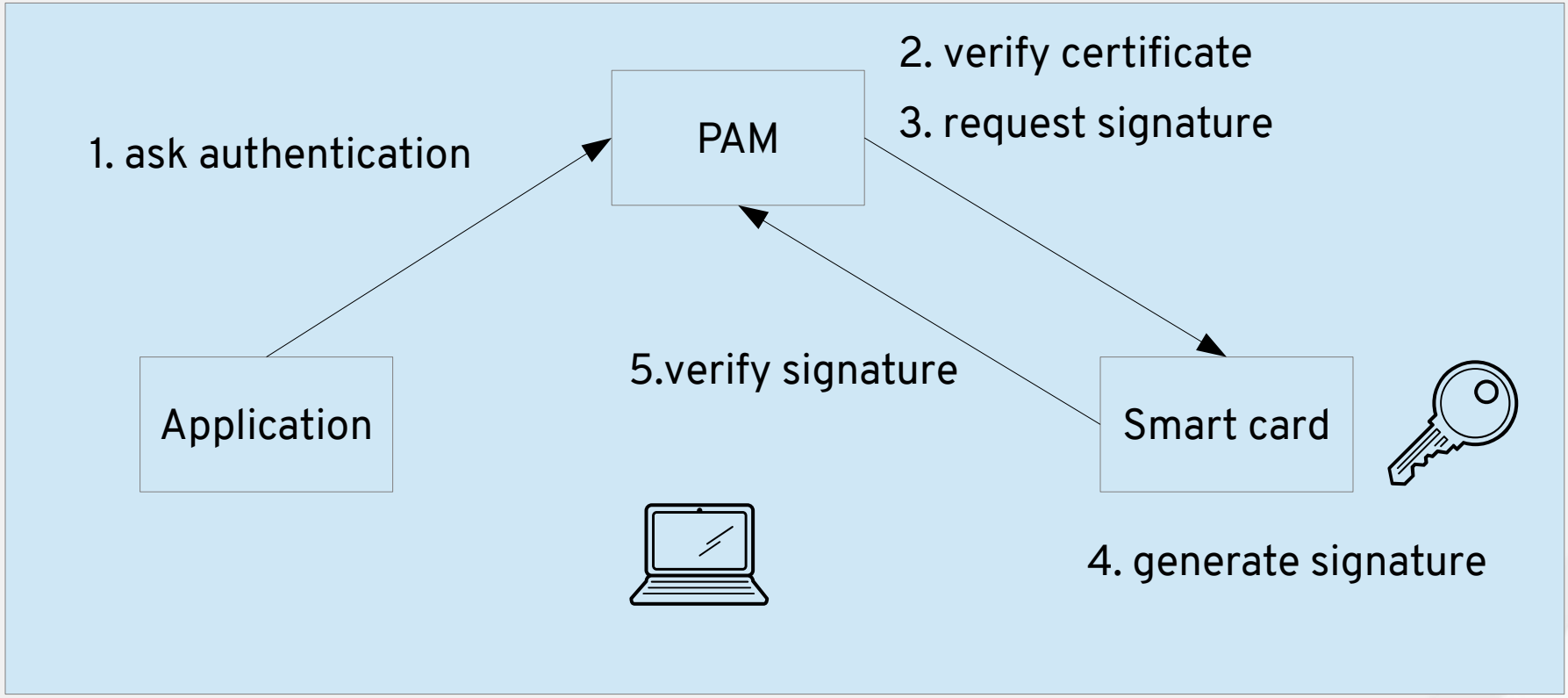
redhat.

WHY IMPORTANT?

- They can prevent leakage of private keys
  - Local filesystem, memory, ...
  - All private key operations happen in the card

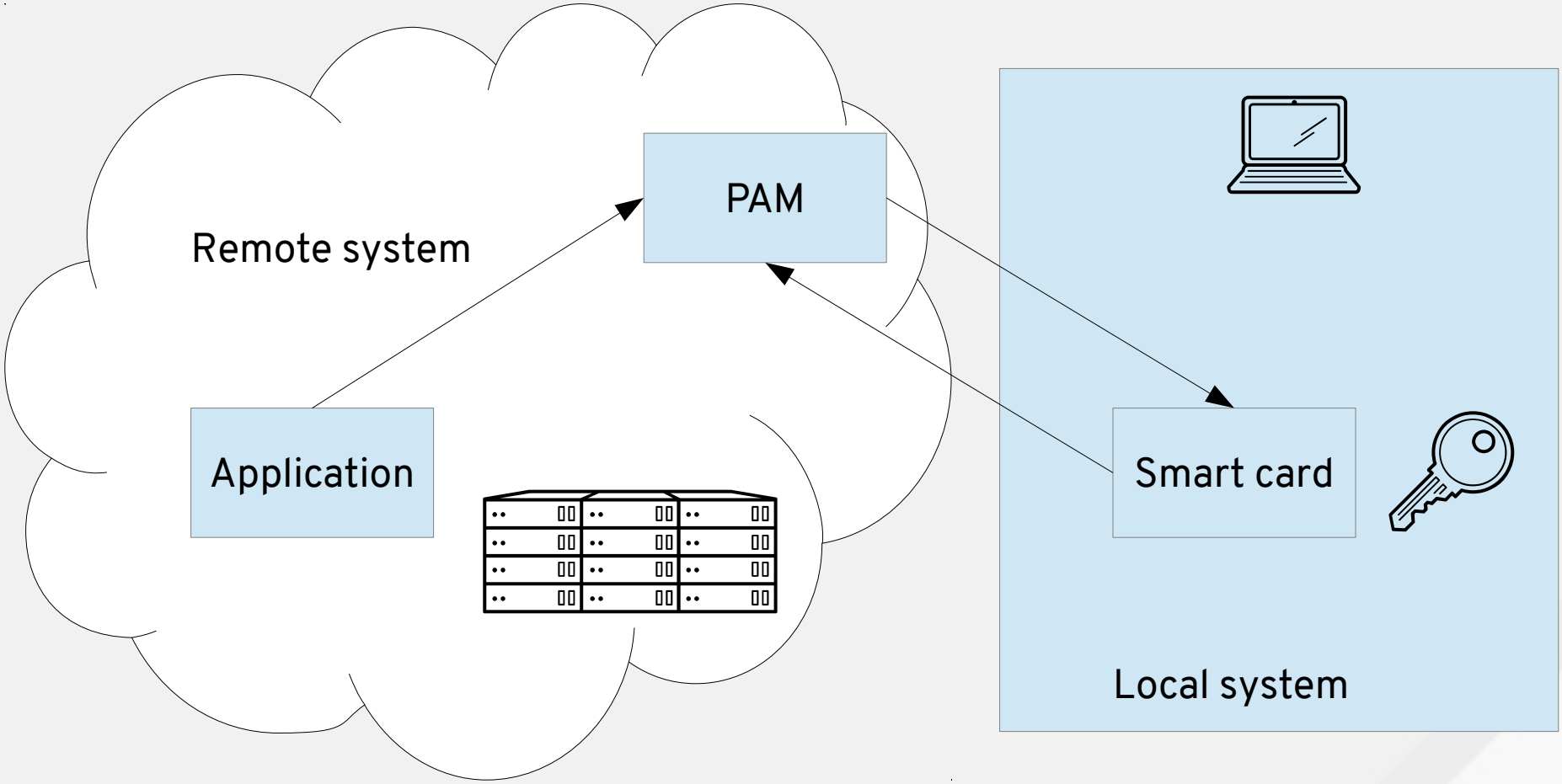
redhat.

LOCAL USE CASE: AUTHENTICATION



redhat.

REMOTE USE CASE



redhat.

POTENTIAL USES

- Protecting private keys for remote TLS server
- Signing packages/images on remote CI

redhat.

IMPLEMENTATION

- Define protocol that serializes smart card access
- Expose the protocol at a Unix domain socket
- Forward the socket with ssh

redhat.

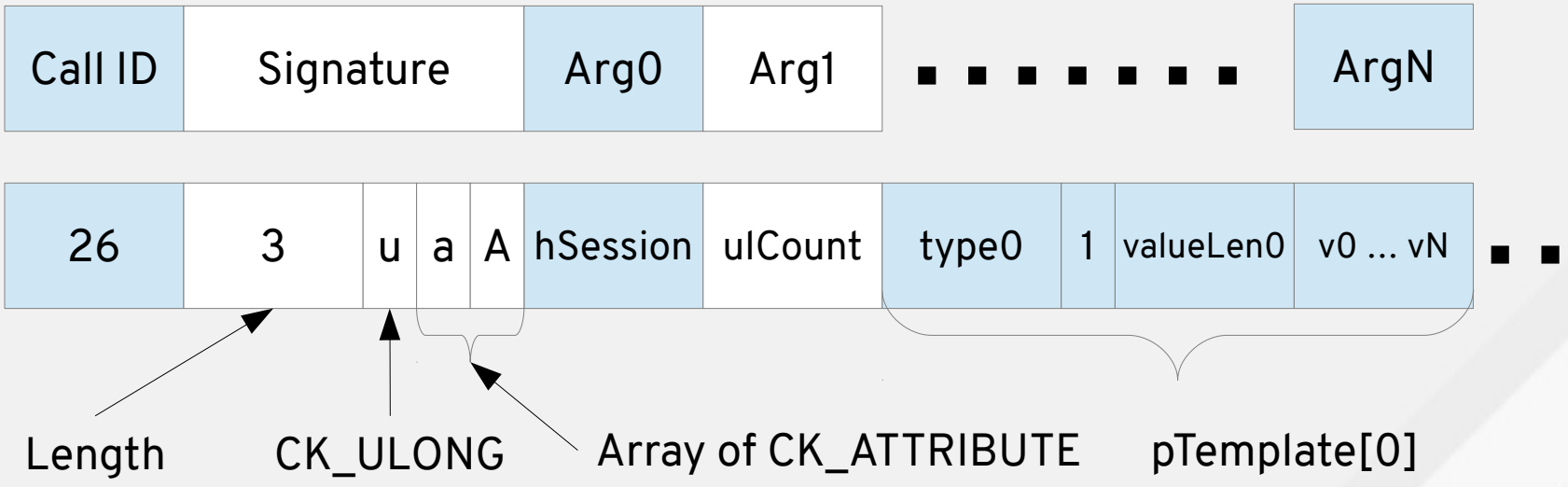
PROTOCOL: PKCS#11

- De-fact C API implemented by smart card drivers
  - OpenSC
  - Proprietary drivers
- The caller shall `dlopen()` the library

redhat.

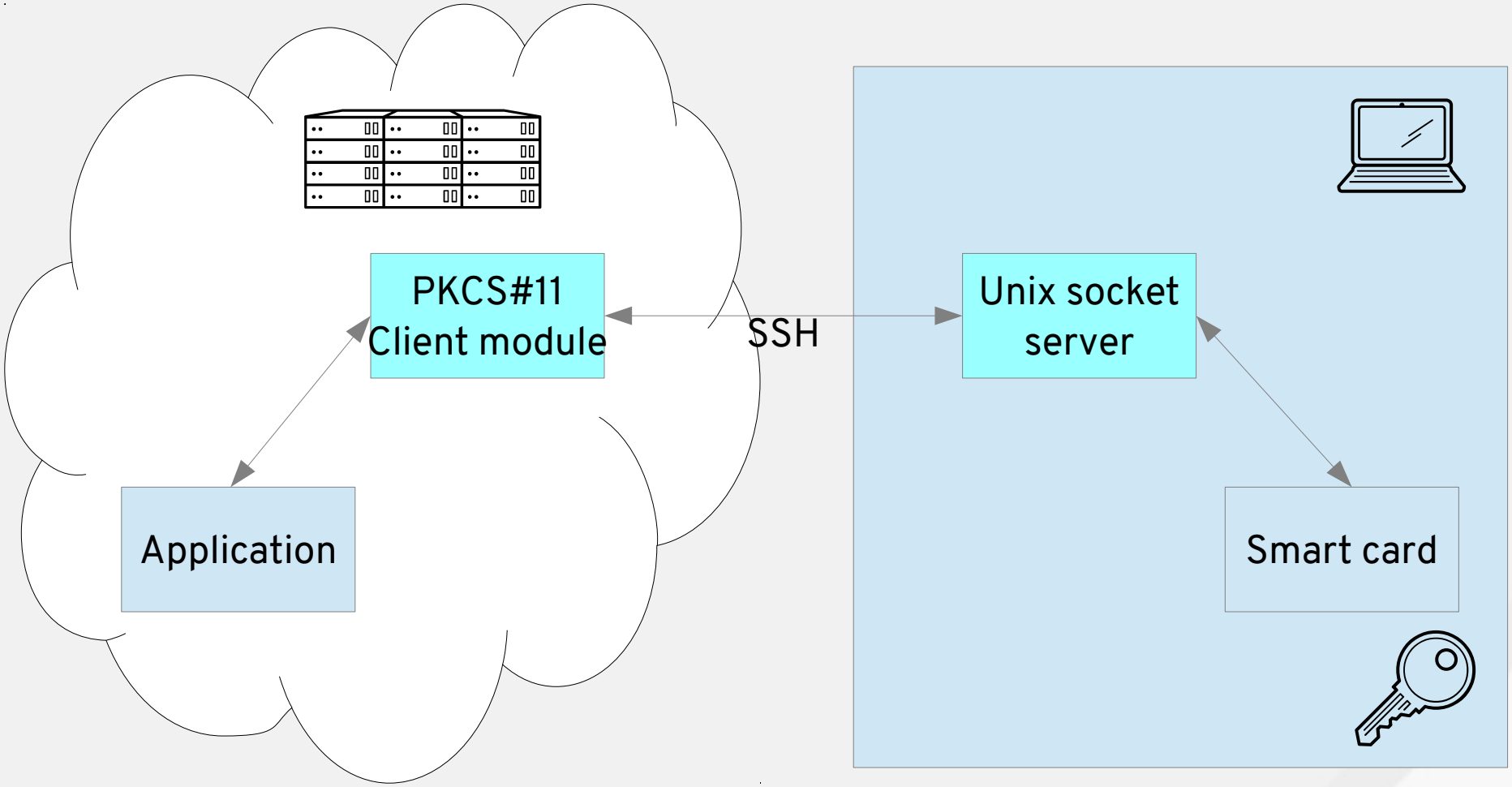
PROTOCOL: SERIALIZATION FORM

```
CK_RV
C_FindObjectsInit (CK_SESSION_HANDLE hSession,
                   CK_ATTRIBUTE_PTR  pTemplate,
                   CK_ULONG          ulCount);
```



redhat.

FORWARDING



redhat.

p11-kit

- Portable library to access PKCS#11 modules
  - Aggregation
  - Threading
  - PKCS#11 URI
- Consistent configuration for PKCS#11 modules

redhat.

DEMO

```
$ p11tool --list-tokens
Token 6:
    URL: pkcs11:model=SoftHSM%20v2;manufacturer=SoftHSM
%20project;serial=67060e945183d131;token=Daiki%27s%20token
    Label: Daiki's token
    Type: Generic token
    Manufacturer: SoftHSM project
    Model: SoftHSM v2
    Serial: 67060e945183d131
    Module: libsofthsm2.so

$ p11tool --list-all --login 'pkcs11:some-token'
$ p11tool --test-sign --login 'pkcs11:some-privkey'
```


redhat.

DEMO

```
$ p11-kit server 'pkcs11:some-token'
P11_KIT_SERVER_ADDRESS=unix:path=/run/user/500/p11-kit/pkcs11-12345
P11_KIT_SERVER_PID=12345

$ ssh -R .../p11-kit/pkcs11:/run/user/500/p11-kit/pkcs11-12345 \
remote-user@remote

[remote-user@remote ~]$ sudo id
Smartcard authentication starts
Smart card found.
Welcome SmartCard-HSM (UserPIN)!
Smart card PIN:
verifying certificate
uid=0(root) gid=0(root) groups=0(root)
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```


redhat.

FUTURE WORK

- Usability
  - OpenSSH / systemd integration
- Portability
  - Windows: PuTTY-CAC

redhat.

FUTURE WORK

- Access control
  - Make PKCS#11 objects invisible / read-only
  - Disallow certain operations
  - Redirect PIN input
- Protocol standardization

redhat.

QUESTIONS?

Git repo: https://github.com/p11-glue/p11-kit

Mailing list: p11-glue@lists.freedesktop.org

Contact: dueno@redhat.com

redhat.