Hardware-based Cryptography

Smart cards, YubiKeys & more

Karol Babioch
Security Engineer
kbabioch@suse.de

Rationale

- Computers running general purpose software can be compromised
  → “hacked”
  → Offline-access, etc.

- Hardware-based cryptography is much more limited
  – Only simple interfaces
  – Only specific operations
  – Cannot be copied / cloned
  – Tamper resistant

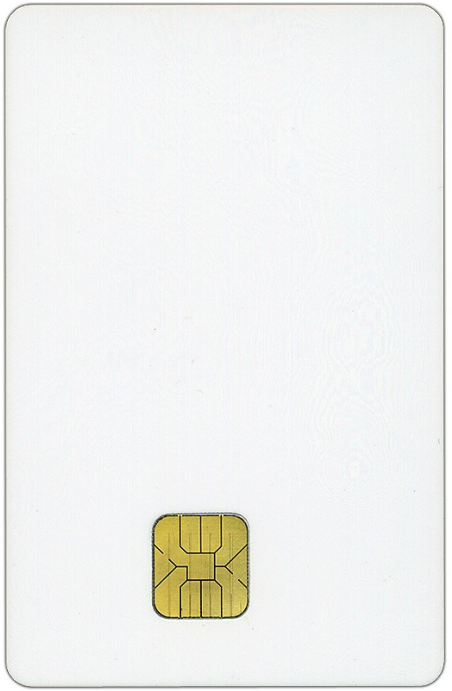
  → Difficult to “hack”
  → Won’t reveal the secret

Examples


gemalto


übertragung
aktiviert
1 2 3 TAN
4 5 6 C
7 8 9 F
0 OK
0987654321
12/12


RSA
SecurID®
032 848
Powered by RSA




Y
Yubico

YubiKey as example

Functions	YubiKey 4	YubiKey 4 Nano	YubiKey 4C	YubiKey 4C Nano	YubiKey NEO	Security Key by Yubico
Secure Static Passwords	●	●	●	●	●	
Yubico OTP	●	●	●	●	●	
OATH – HOTP (Event)	●	●	●	●	●	
OATH – TOTP (Time)	?	?	?	?	?	
Smart Card (PIV-Compatible)	●	●	●	●	●	
OpenPGP	●	●	●	●	●	
FIDO U2F (Universal Second Factor)	●	●	●	●	●	●
FIDO2						●
Secure Element	●	●	●	●	●	●

U2F

Karol Babioch
Security Engineer
kbabioch@suse.de

U2F

- Universal 2nd Factor
- Initially developed by Yubico & Google
- Contributed to FIDO alliance → FIDO U2F

Features:

- Challenge-response protocol
- Phishing protection → “Origin Binding”
- Man-in-the-Middle protection
- Application-specific keys
- Device cloning detection
- Device attestation

U2F

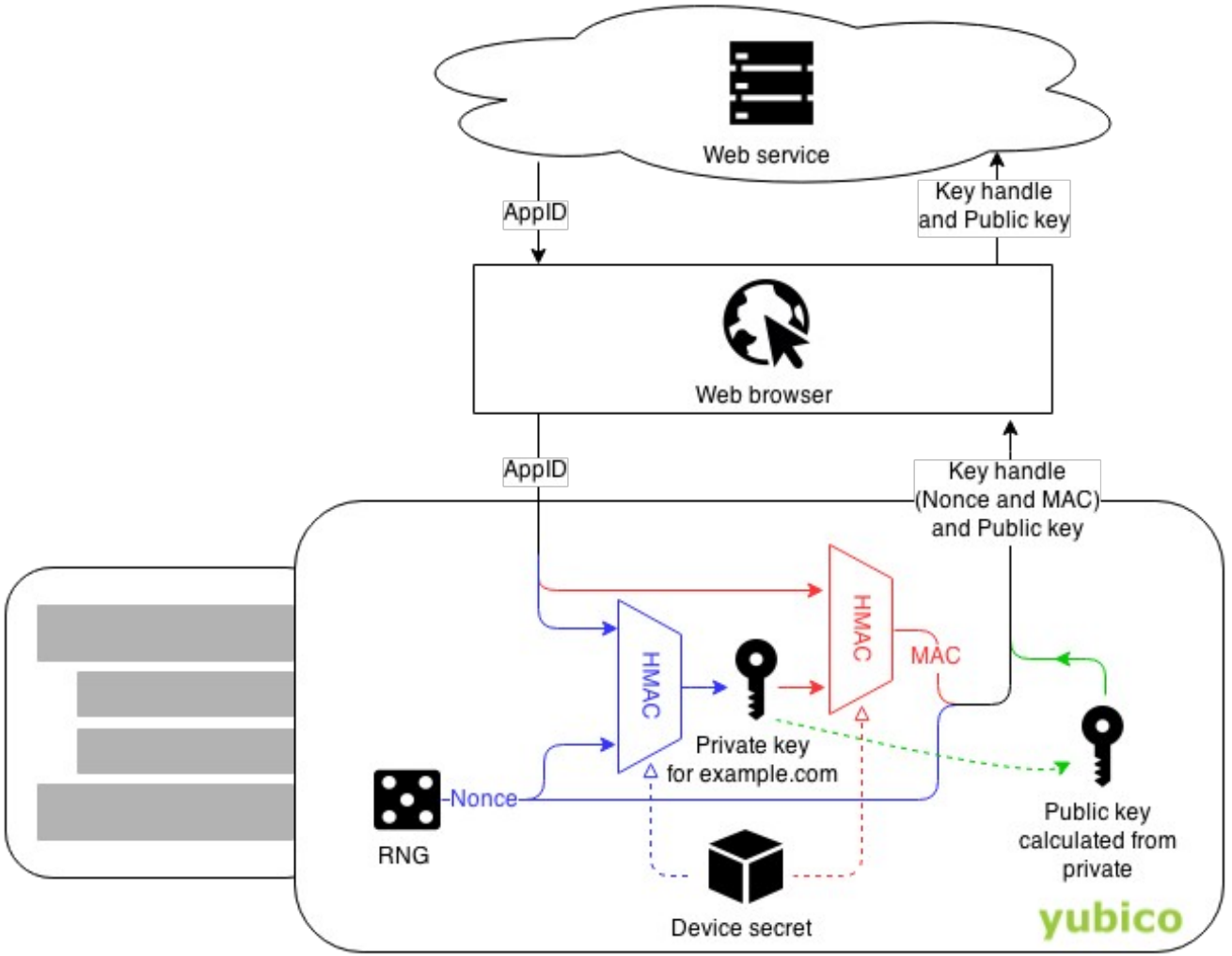
- Requires browser support

- Similar to WebAuthn, mostly compatible

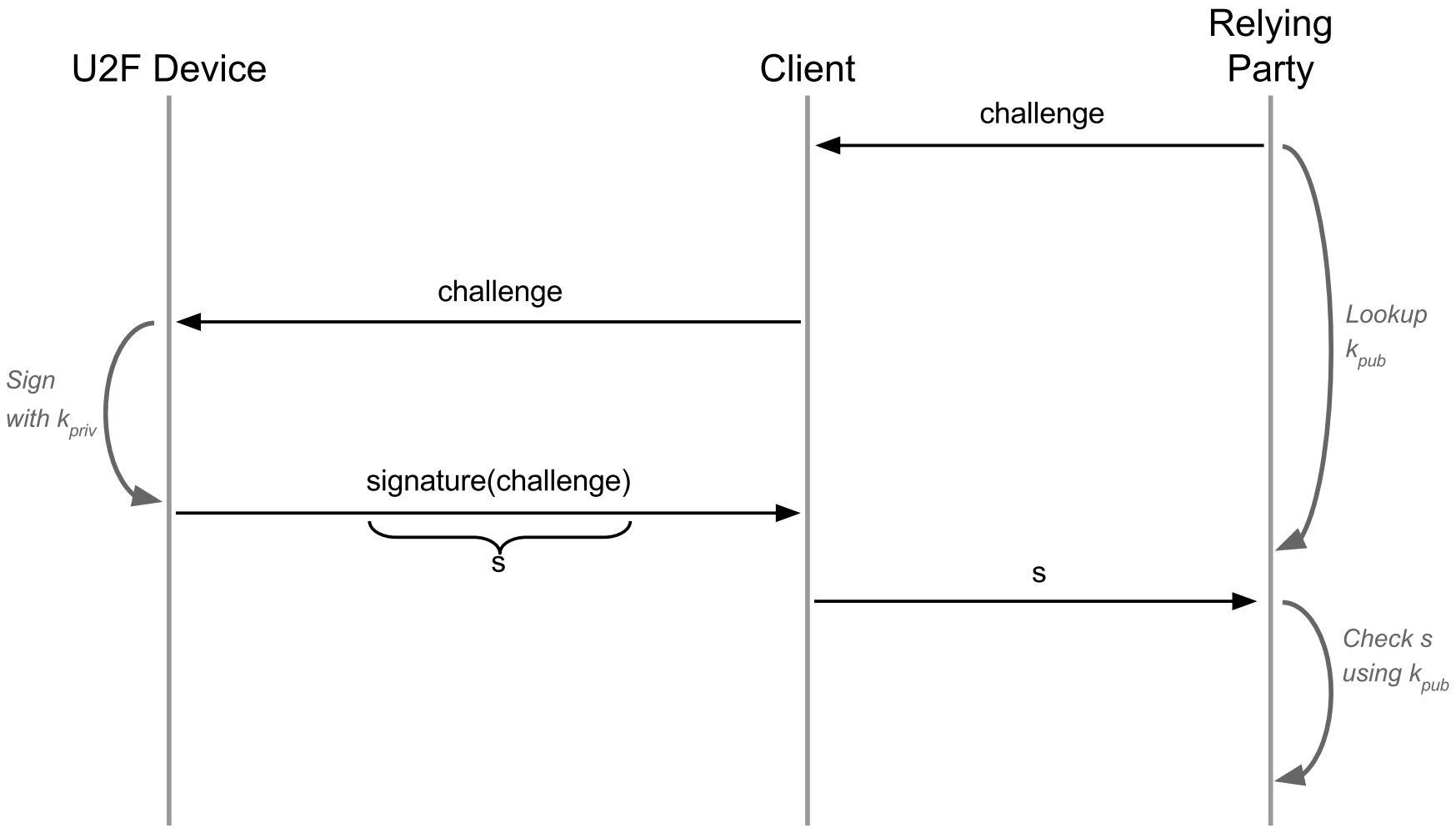
- Two flows:

1.) Registration
2.) Authentication

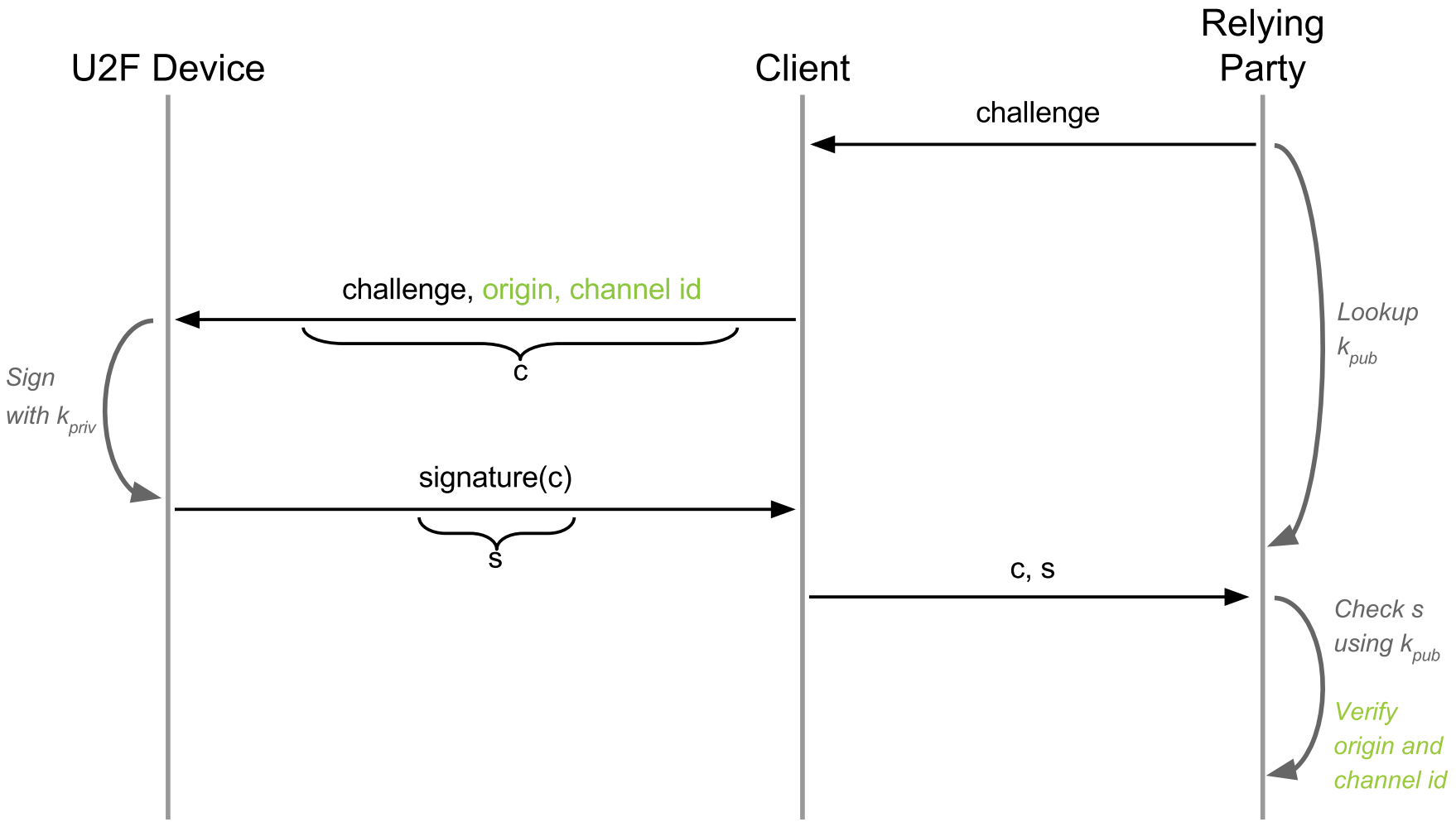
U2F on-the-fly key generation



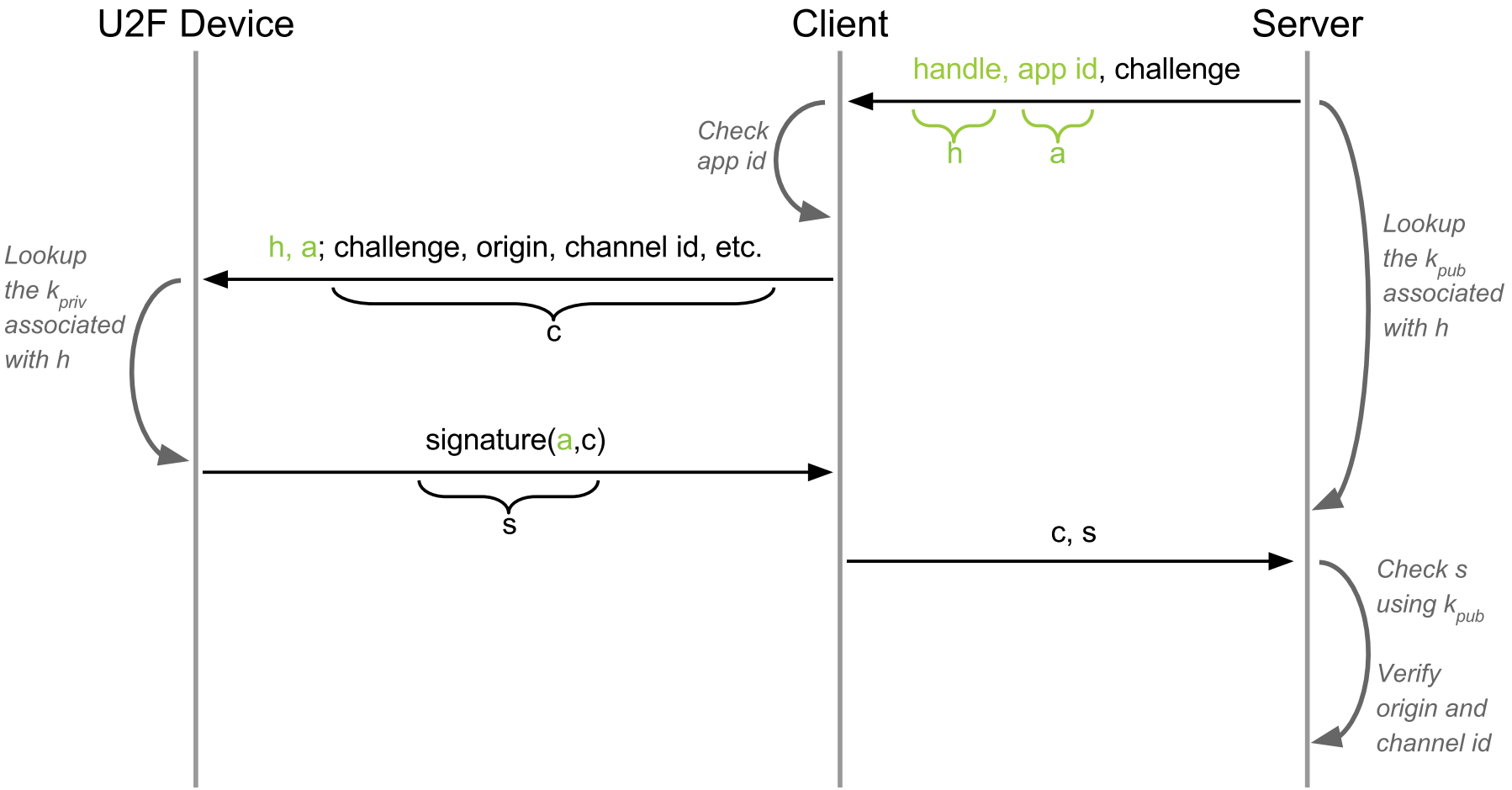
U2F challenge-response



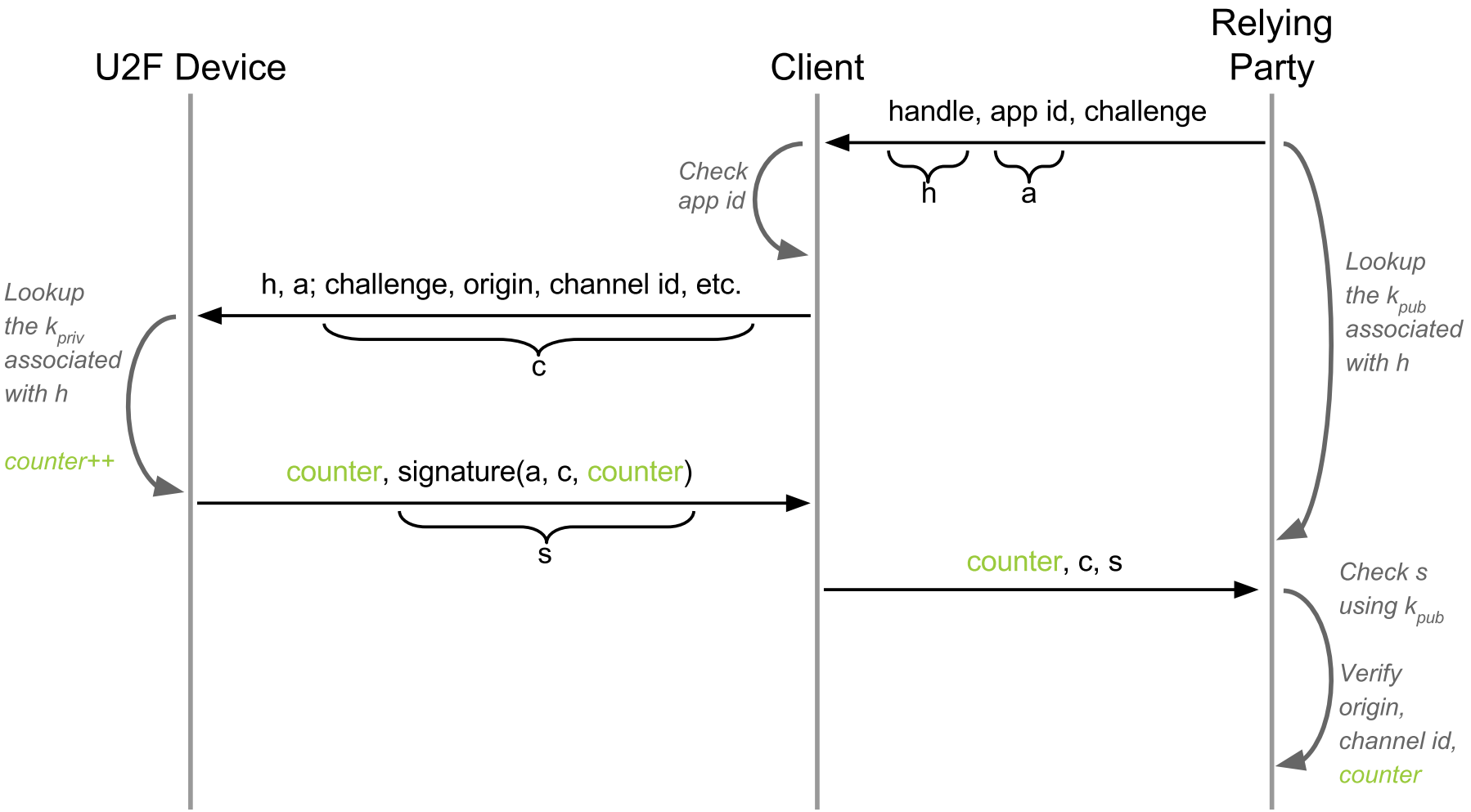
U2F phishing and MitM protection



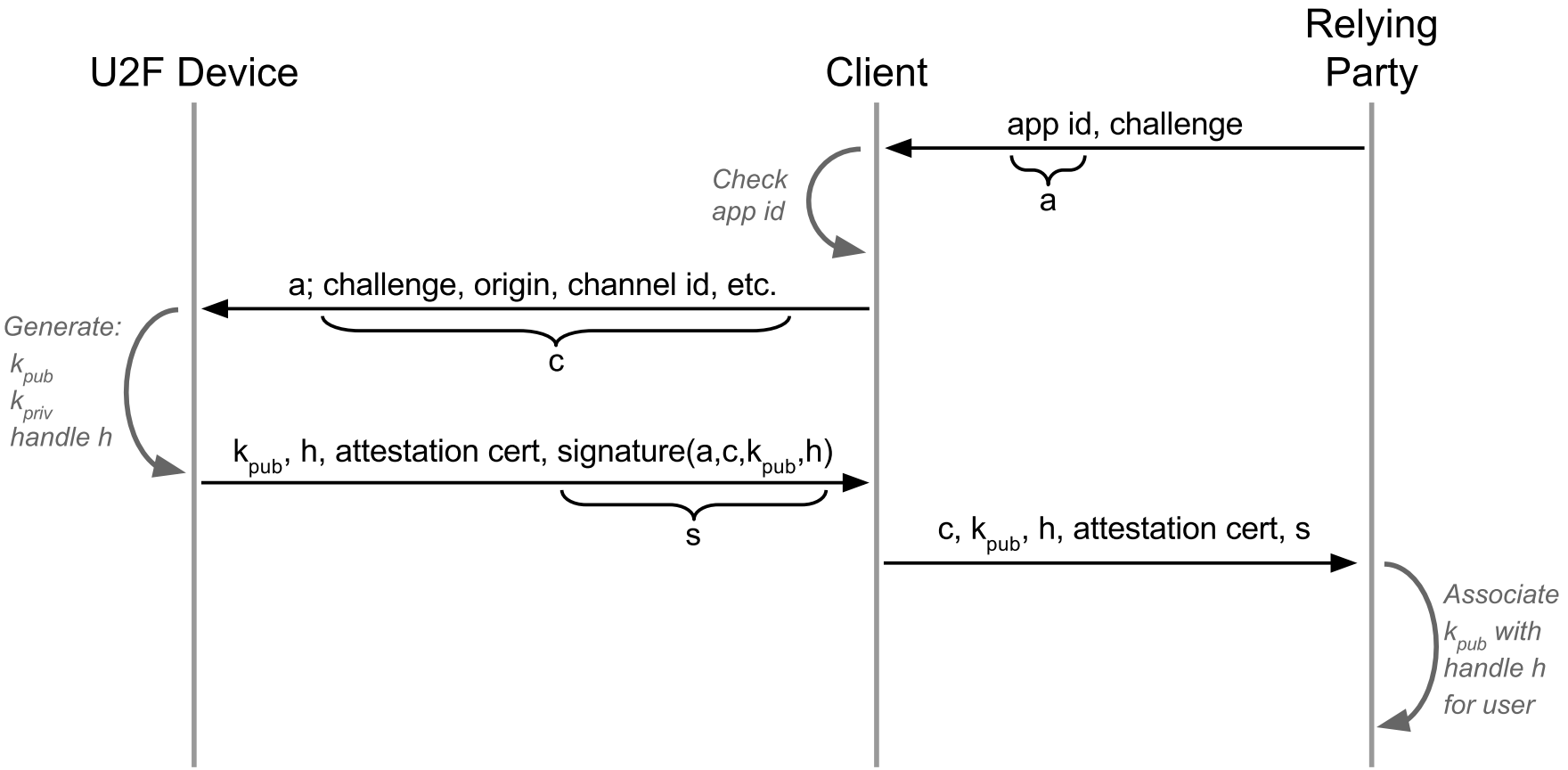
U2F application-specific keys



U2F device cloning detection



U2F device attestation



FIDO2 / U2F / WebAuthn

Karol Babioch
Security Engineer
kbabioch@suse.de

FIDO2 / U2F / WebAuthn

- FIDO2 is evolution of U2F → passwordless login flows
- FIDO2 is mostly compatible with U2F
- WebAuthn supports both FIDO2 as well as U2F
- U2F client-side protocol → CTAP1
- New extensible client-to-authenticator protocol CTAP2 developed
  - Allows for external authenticators (tokens, phones, smart cards, etc.)
- FIDO2 requires WebAuthn and CTAP2
- WebAuthn also suports U2F via CTAP1

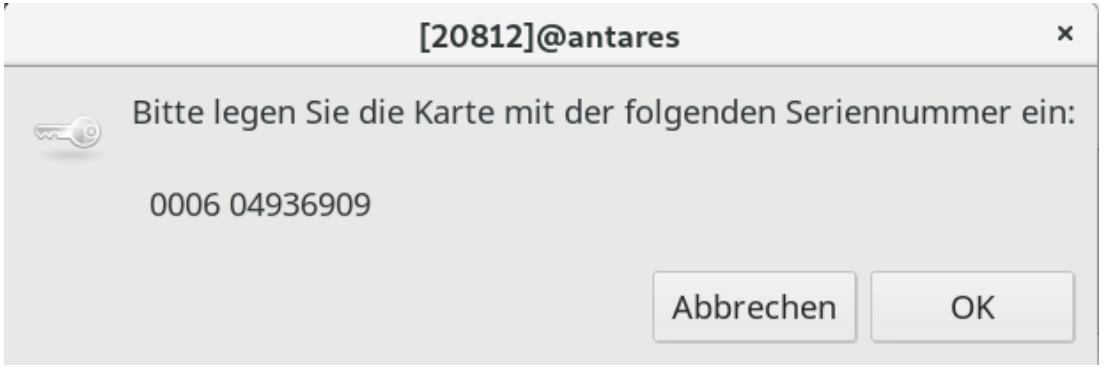
OpenPGP smart card

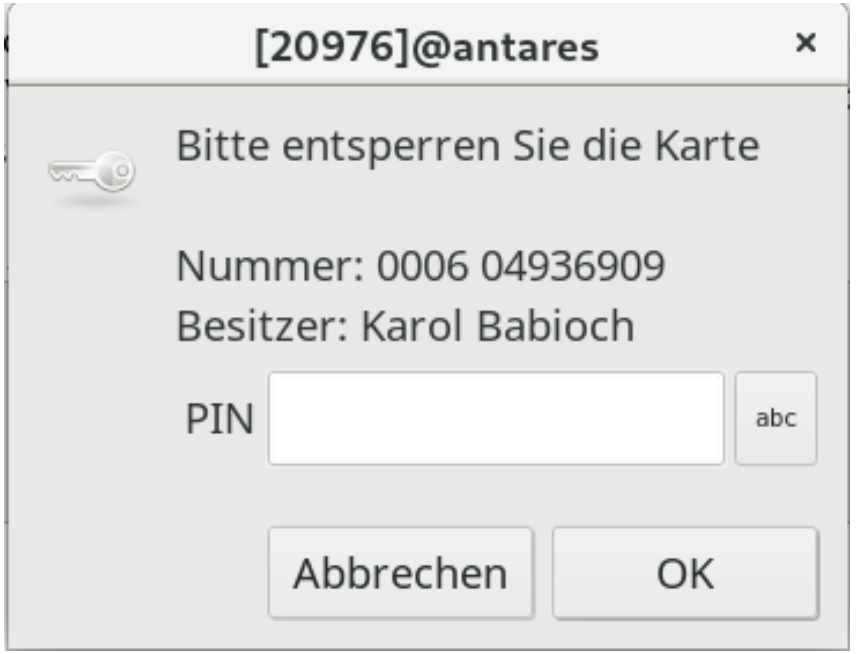
Karol Babioch
Security Engineer
kbabioch@suse.de

OpenPGP smart card

- Specific application for OpenPGP
- GnuPG supports this out of the box
  – Stores a reference to smart card in keyring
- Up to three private keys are stored in hardware
  → Useful for subkeys
- Can be imported into the smart card
- Can be generated on the smart card
- Stores some metadata
  - Name of card holder
  - PIN retry counter → Will be blocked after three unsuccessful attemps
  - URL of public key
  - Signature counter
- Signature PIN (optional)

OpenPGP smart card example





Smart card (PIV)

Karol Babioch
Security Engineer
kbabioch@suse.de

Smart card (PIV)

- RSA / ECC sign/encrypt/decrypt operations
- Private key stored on smart card
- Requires PIN to unlock
- PIN will be blocked after three unsuccessful attempts → PUK
- PUK will be blocked after three unsuccessful attempts → Reset
- Multiple key slots (e.g. Yubikey supports up to 12)
  - Slot 9a: PIV Authentication
  - Slot 9c: Digital Signature
  - Slot 9d: Key Management
  - Slot 9e: Card Authentication
  - Slot 82-95: Retired Key Management
  - Slot f9: Attestation

Smart card (PIV)

- Access via standardized interface (PKCS11)
  - Supported on all major operating systems

- Many applications
  - OS login
  - SSH
  - Browser
  - Code signing
  - OpenSSL

→ In theory every application that can deal with certificates

Problems with hardware-based crypto

Karol Babioch
Security Engineer
kbabioch@suse.de

General problems with hardware crypto

- Historically speaking: Inconvenient → FIDO2?
- Can be lost / stolen / destroyed

- “Software” running in hardware can still be broken
  – e.g. Infineon RSA key generation → Also affected YubiKeys

- Interfaces between hardware and software can be vulnerable
  – e.g. X41 security announcements → fuzzing

- Host can still be compromised → Session hijacking, phishing, MitM, etc.

- User consent vs. transactional awareness (e.g. no display, etc.)

Demos & discussion

Karol Babioch
Security Engineer
kbabioch@suse.de

Demos & discussion

- Yubico OTP
- Yubico HOTP
- Yubico U2F
- WebAuthn
- OpenPGP smart card


SUSE
We adapt. You succeed.