

yubico

Trust the Net

U2F Case Study

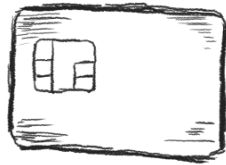
Examining the U2F paradox

yubico

What is Universal 2nd Factor (U2F)?

Simple, Secure, Scalable 2FA

Didn't We Solve This Already?



Smart Cards

- Readers/drivers
- Middleware
- Cost



SMS

- Coverage
- Delay
- Cost
- Battery
- Policy



OTP Devices

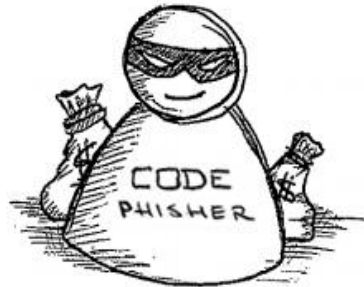
- One per site
- Provisioning costs
- Battery

And...



Bad User experience

Users find it hard to use



Still phishable

Successful attacks carried out today



MitM

Successful attacks carried out today

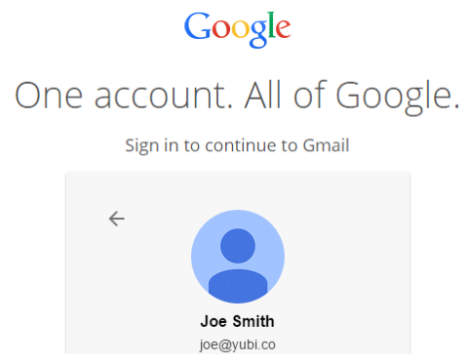
Why U2F?

- **Simple**
 - To register and authenticate -- a simple touch!
 - No drivers or client software to install
- **Secure**
 - Public key cryptography
 - Protects against phishing and man-in-the-middle
- **Scalable**
 - One U2F device, many services
- **Protects Privacy**
 - No secrets shared between service providers

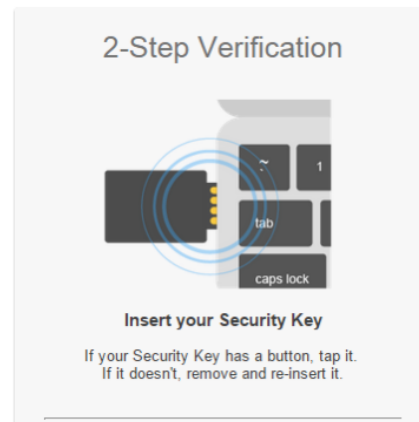


Google Login With U2F

1. Enter username/pwd



2. Insert U2F Key



3. Touch device



Dropbox Login With U2F

1. Enter username/pwd

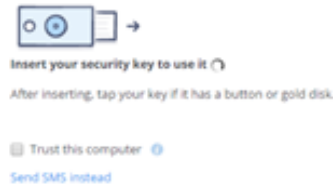


Sign in [or create an account](#)

Remember me

[Forgot your password?](#)

2. Insert U2F Key



3. Touch device



GitHub Login With U2F

1. Enter username/pwd

Sign in


Username or email address

Password (forgot password)

Sign in


2. Insert U2F Key

Two-factor authentication



Insert your security key

Press the button on your security key device to finish signing in. If it does not have a button, just re-insert it.

 Press the button on your security key...

3. Touch device



Your Login With U2F

1. Enter username/pwd

Welcome

User name *

Password *

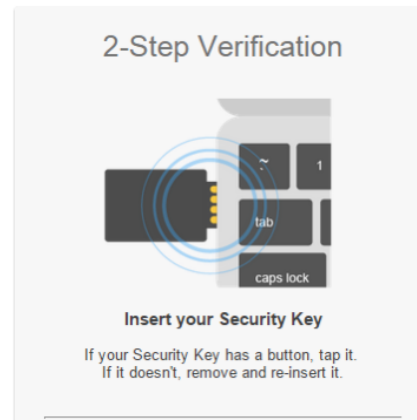
Remember me

[Sign in](#)

[Forgot user name/password? >](#)

[Not enrolled? Sign up now. >](#)

2. Insert U2F Key

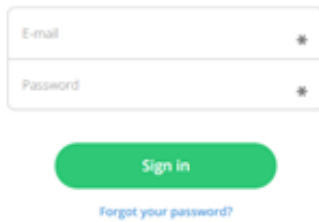


3. Touch device



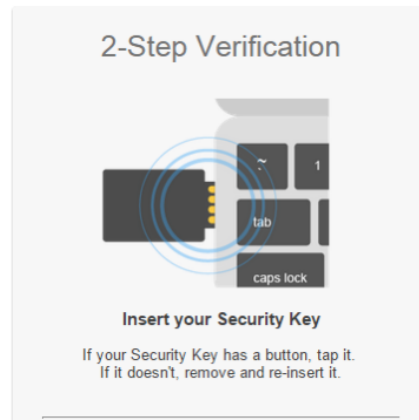
Your Login With U2F

1. Enter username/pwd



A login form with two input fields: "Email" and "Password", each with a small asterisk icon to its right. Below the fields is a green rounded button labeled "Sign in". Underneath the button is a blue link that says "Forgot your password?".

2. Insert U2F Key

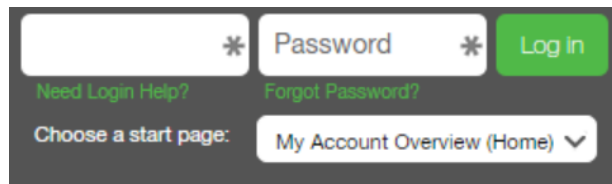


3. Touch device



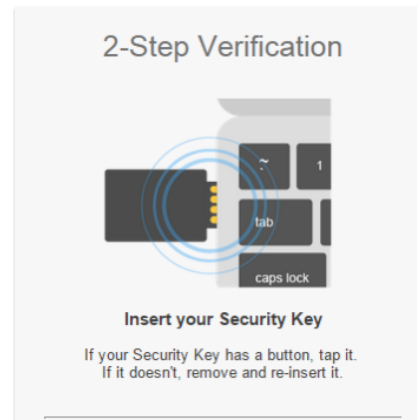
Your Login With U2F

1. Enter username/pwd



A screenshot of a login interface. It features a dark grey background with white text. On the left, there is a white input field for a username. To its right is a white input field for a password, marked with an asterisk on both sides. Further right is a green button with the text "Log In". Below the password field, there are two links: "Need Login Help?" and "Forgot Password?". At the bottom, there is a section labeled "Choose a start page:" followed by a dropdown menu showing "My Account Overview (Home)" with a downward arrow.

2. Insert U2F Key



3. Touch device



Protocol Overview

Registration

1 Server sends challenge

2 Device generates key pair

3 Device creates key handle

4 Device signs challenge + client info

5 Server receives and verifies device signature using attestation cert

6 Key handle and public key are stored in database

Authentication

1 Server sends challenge + key handle

2 Device unwraps/derives private key from key handle

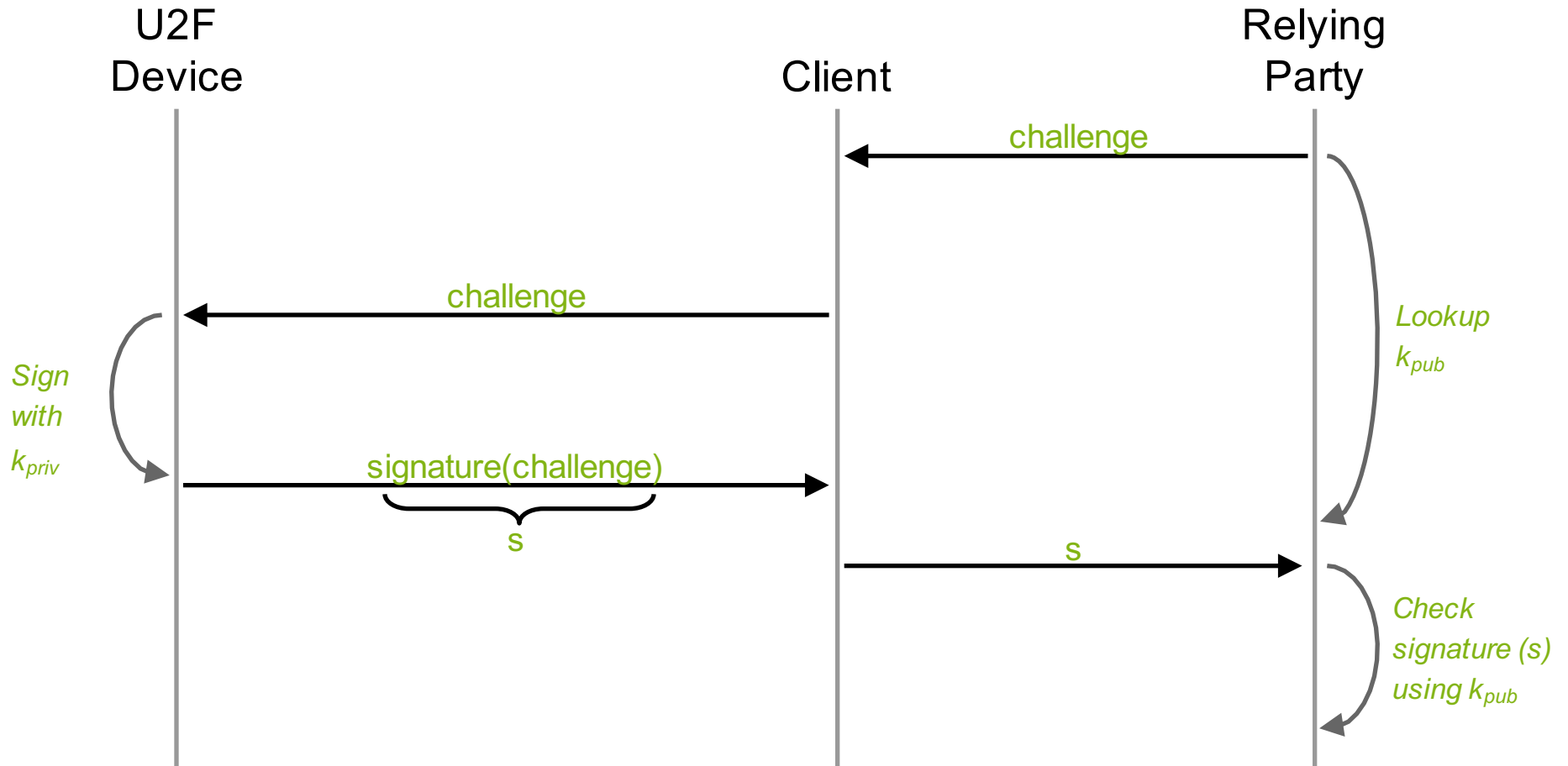
3 Device signs challenge + client info

4 Server receives and verifies using stored public key

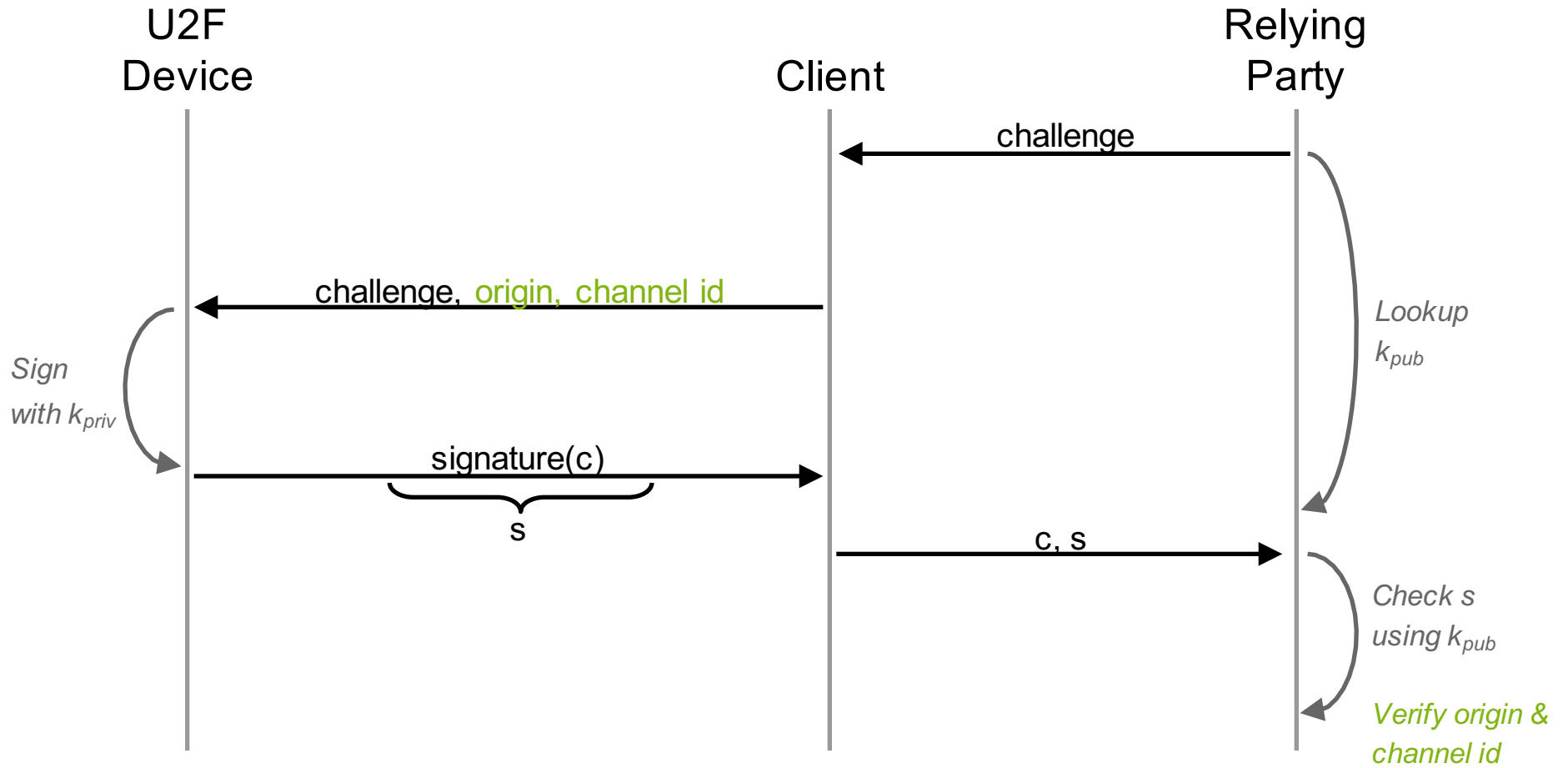
Protocol Design

Step-By-Step

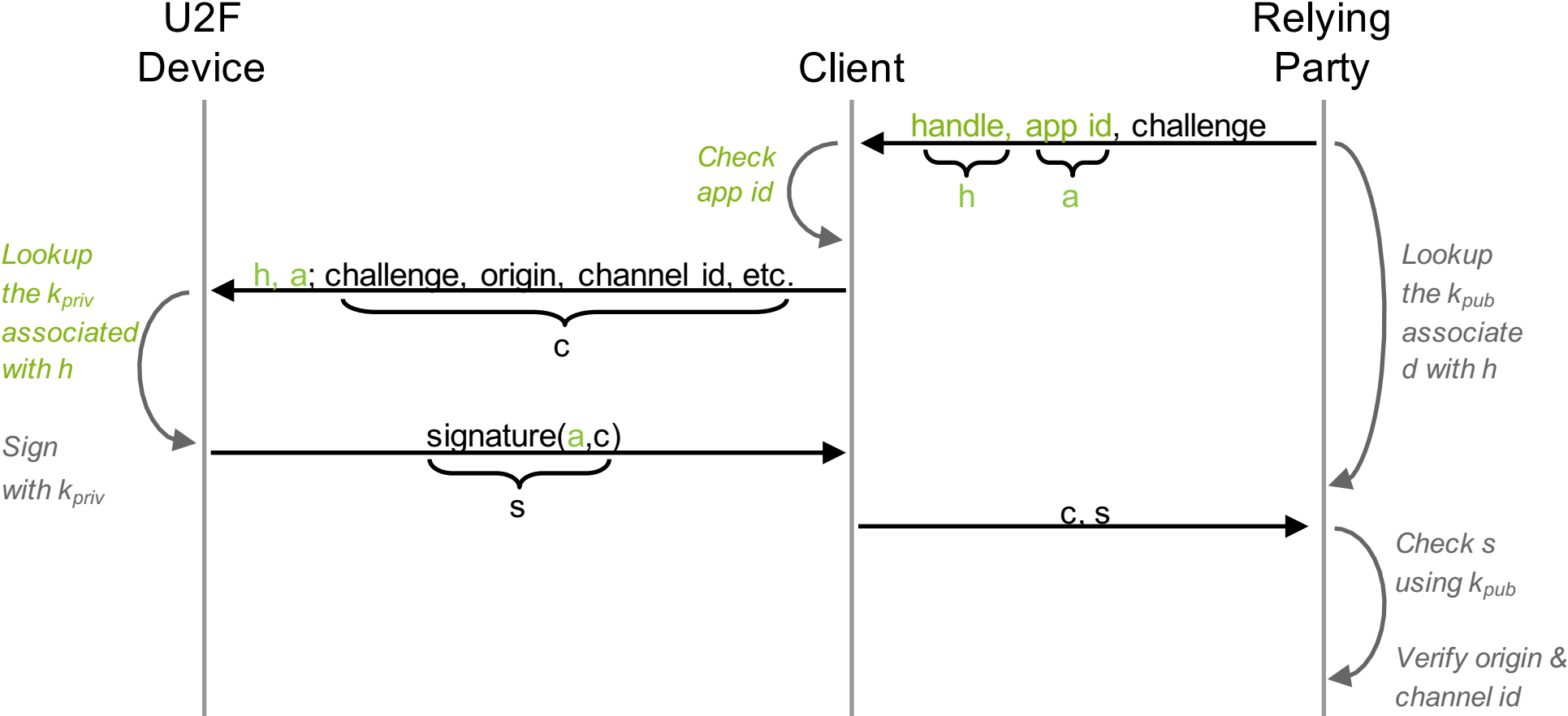
Authentication



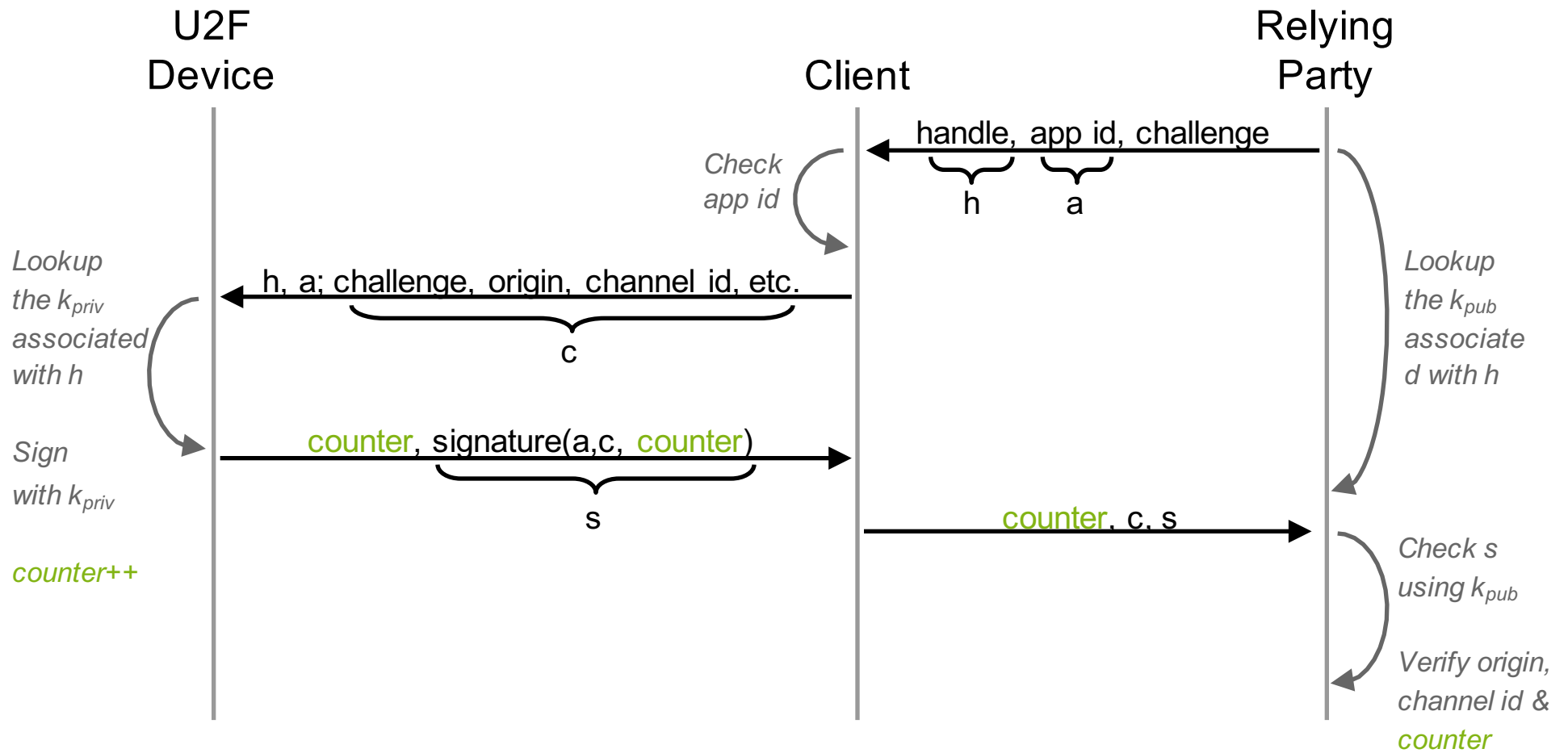
Phishing/MitM Protection



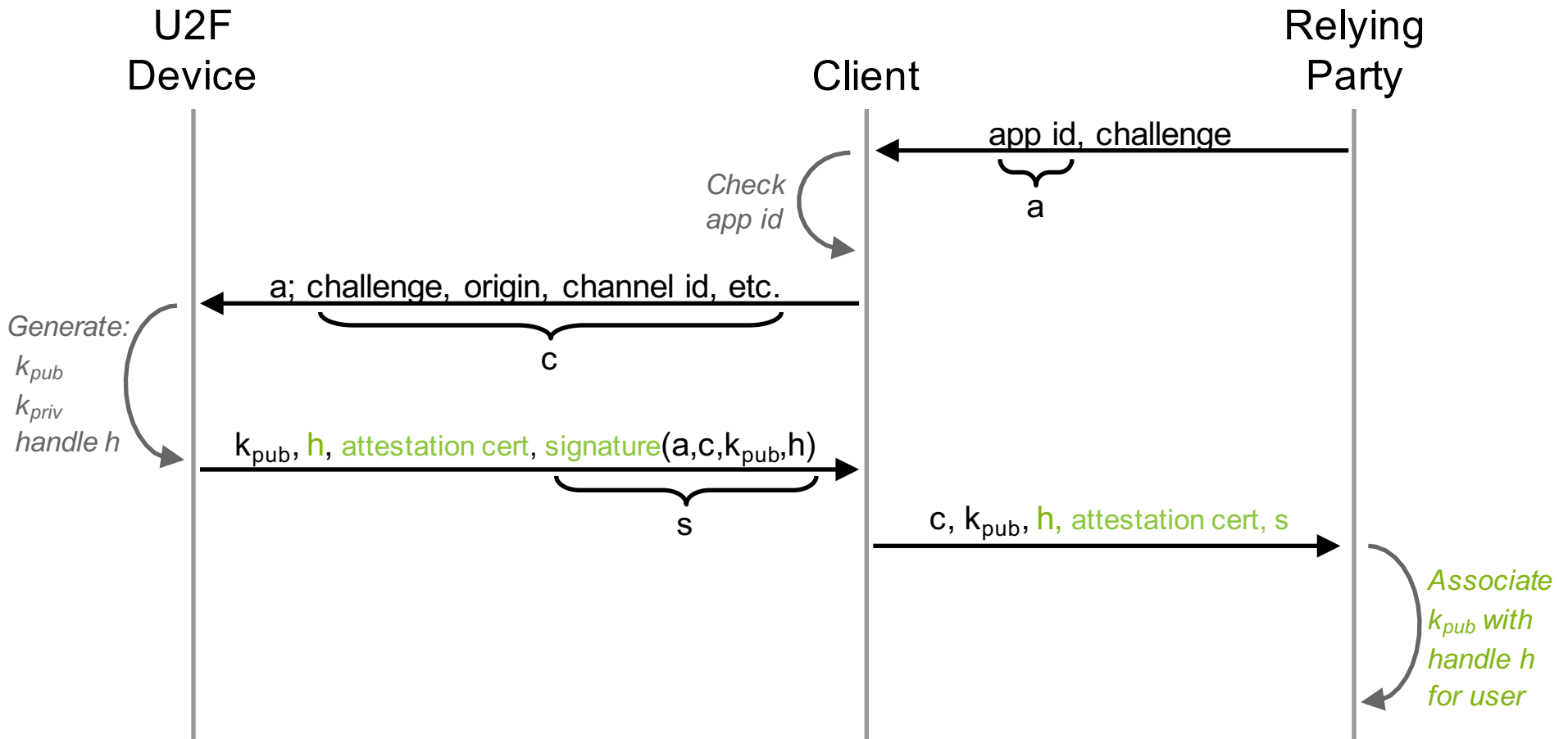
Application-Specific Keys



Device Cloning



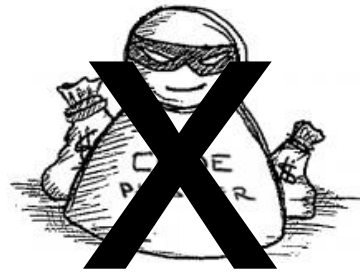
Registration + Device Attestation



So How Did We Do?



**Bad User
Experience**



**Still
Phishable**



MitM

Resources

Strengthen 2 step verification with Security Key

[Yubico Security Key](#)

[Yubico Libraries, Plugins, Sample Code, Documentation](#)

[FIDO U2F Protocol Specification](#)

[Yubico Demo Server - Test U2F](#)

[Yubico Demo Server - Test Yubico OTP](#)

[Google security blog](#)

yubico.com/security-key

developers.yubico.com

fidoalliance.org/specifications

demo.yubico.com/u2f

demo.yubico.com

Questions, Comments

Derek Hanson
derek@yubico.com
@derekhanson
@yubico

