Universal Two-Factor Authentication for the Web And The Mac

Thomas Westfeld
Cocaheads Aachen
2015-03-26

„Treat your password like your toothbrush.
Don't let anybody else use it, and get a
new one every six months.“

–Clifford Stoll

Who on earth does this?

Most Used Passwords in 2014

1. 123456
2. password
3. 12345
4. 12345678
5. qwerty
6. 123456789
7. 1234
8. baseball
9. dragon
10. football
11. 1234567
12. monkey
13. letmein
14. abc123

http://splashdata.com/press/worst-passwords-of-2014.htm

We are doomed !

Best Practices for Passwords

1. Choose long passwords (e.g. use Dicewords™)
2. Do not use keyboard patterns (qwerty, etc.)
3. Do not use consecutive number sequences (1234)
4. Do not reuse passwords along different sites.
5. Change password regularly.

Best Practices for Passwords

1. Choose long passwords (e.g. use Dicewords™
2. Do not use keyboard patterns (qwerty, etc.)
3. Do not use consecutive number sequences (1234)
4. Do not reuse passwords along different sites.
5. Change password regularly.

Almost impossible for every password.

Use an offline password manager !

Authentication Is All About Factors

****

Knowledge Factors

Something only

the user knows

Authentication Is All About Factors

****

Knowledge Factors

Something only

the user knows

Possession Factors

Something only

the user has

Authentication Is All About Factors

****

Knowledge Factors

Something only

the user knows

Possession Factors

Something only

the user has

Inherence Factors

Something only

the user is

Two-Factor Authentication (2F)

********** +

Time-based one time password
TOTP (RFC 6238)
Counter-based one time password
HOTP (RFC 4226), iTAN or SMS

Two-Factor Authentication (2F)

********** +

Time-based one time password
TOTP (RFC 6238)
Counter-based one time password
HOTP (RFC 4226), iTAN or SMS

Drawbacks of Two-Factor Authentication

- Need to be able to receive SMS
- Needs to have your authenticator handy
- Transfer received code to login form
- As a fallback application specific passwords may be generated.
- Backup codes have to be stored at a secure location

Drawbacks of Two-Factor Authentication

- Need to be able to receive SMS
- Needs to have your authenticator handy
- Transfer received code to login form
- As a fallback application specific passwords may be generated.
- Backup codes have to be stored at a secure location

You cannot login without the second factor.

The FIDO Alliance

- Founded in summer 2012
- Publicly launched in February of 2013
- Published their first standard 1.0 in 2014-12-09

Universal Second Factor Authentication U2F

FIDO Universal-Two-Factor (U2F)

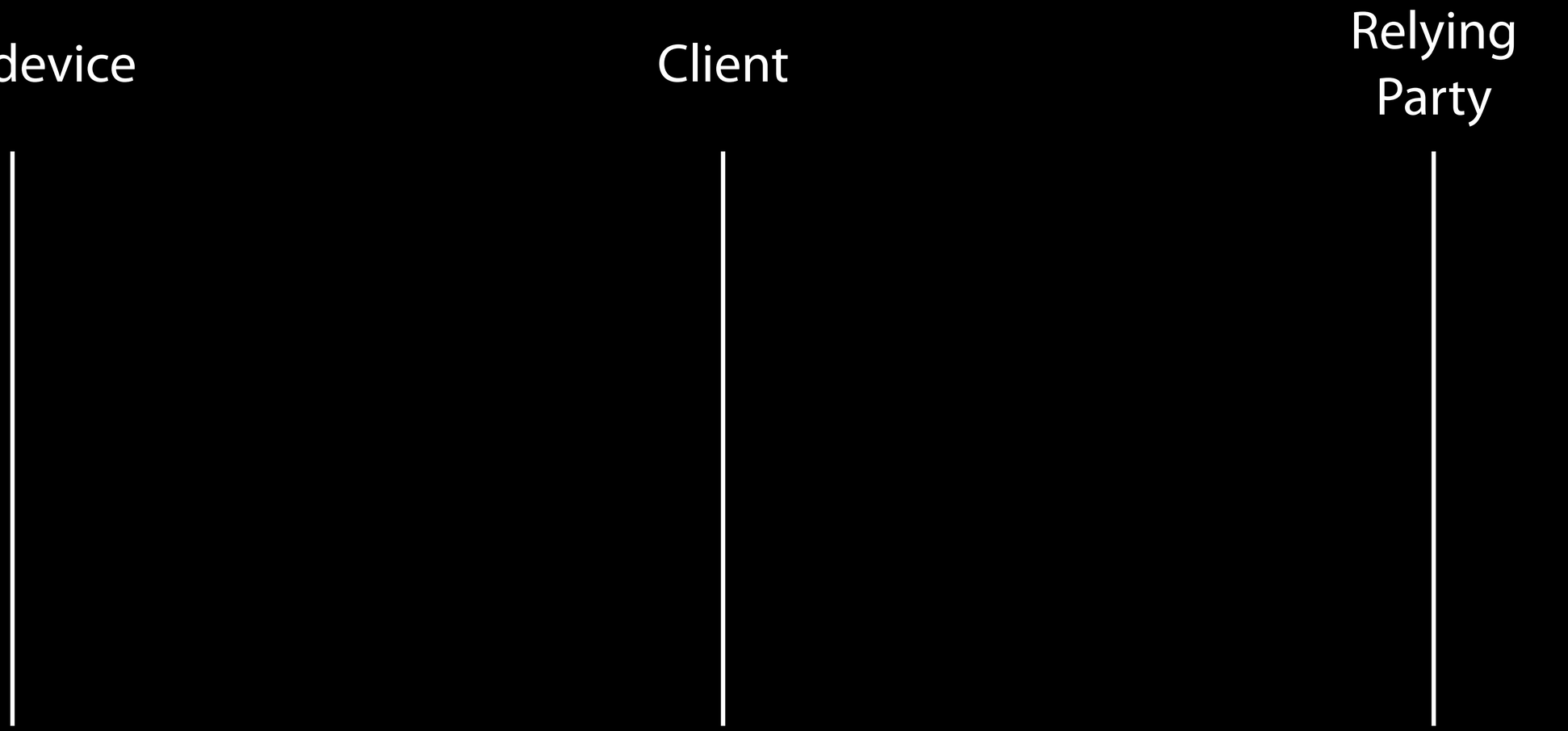
- Challenge-response public-private key cryptography
- Uses elliptic curve cryptography to minimize key-lengths
- Easy to use, just push a button

How to use U2F ?

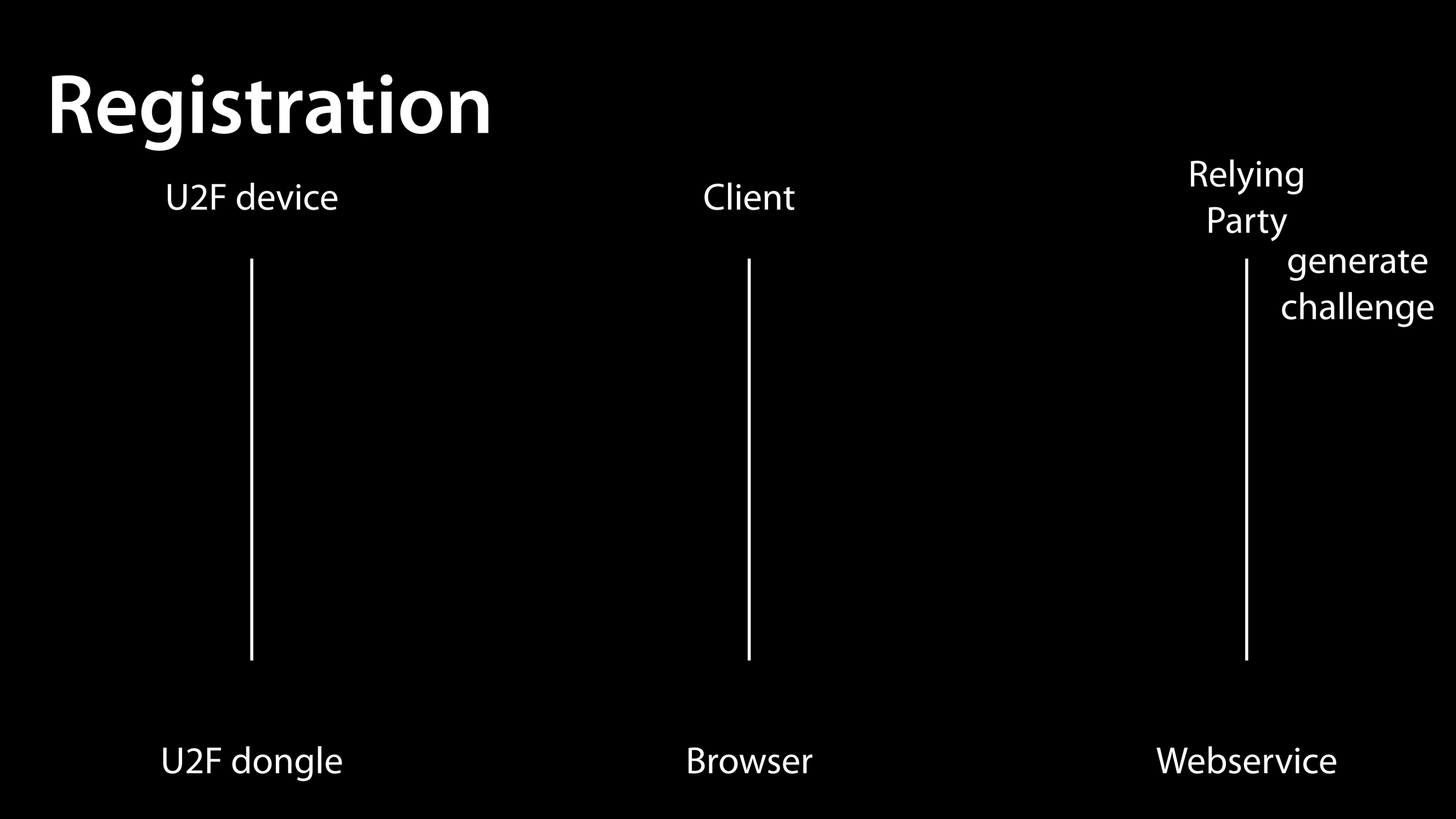
Register U2F device

Authenticate w/ U2F device

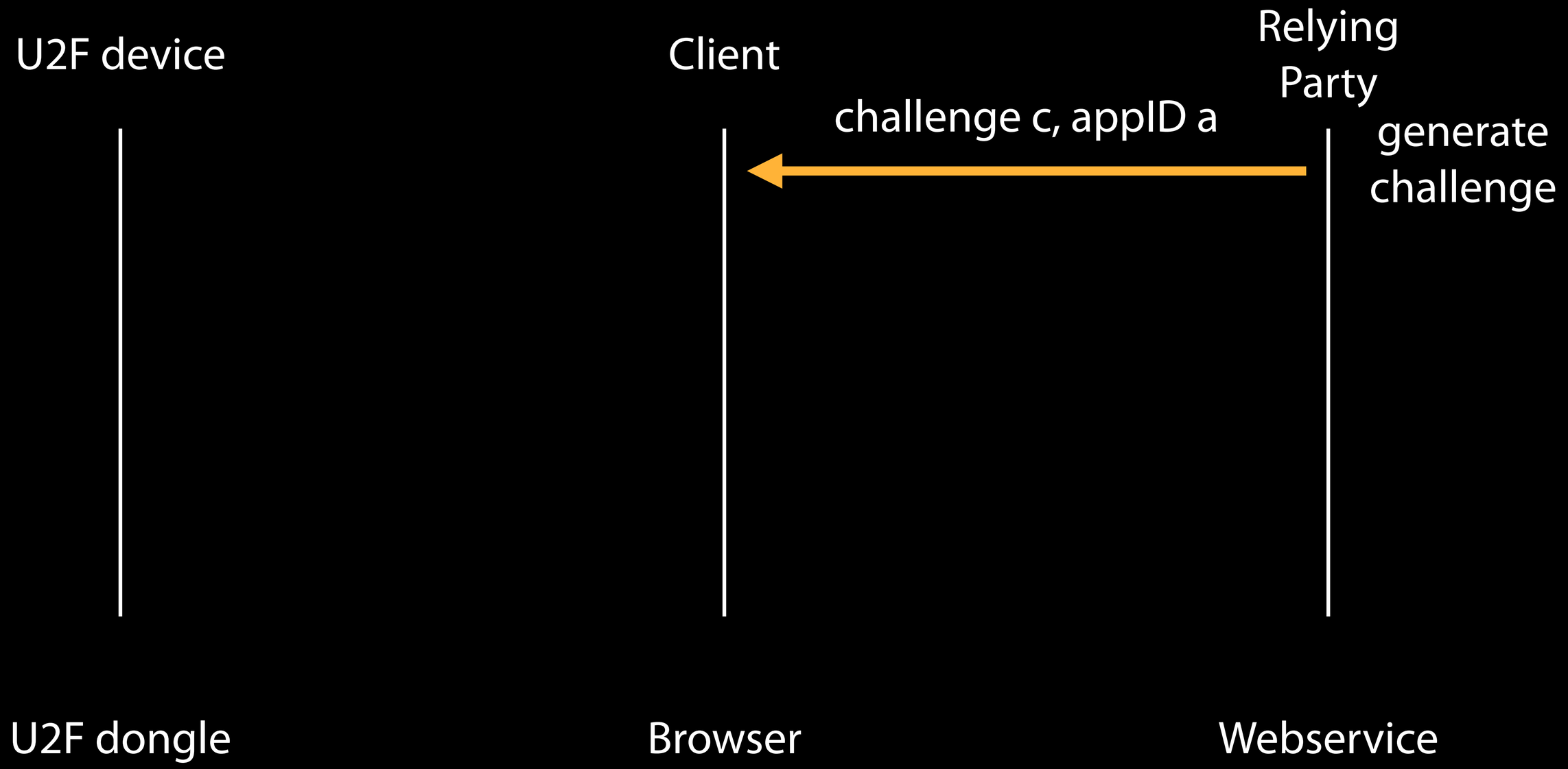
Registration



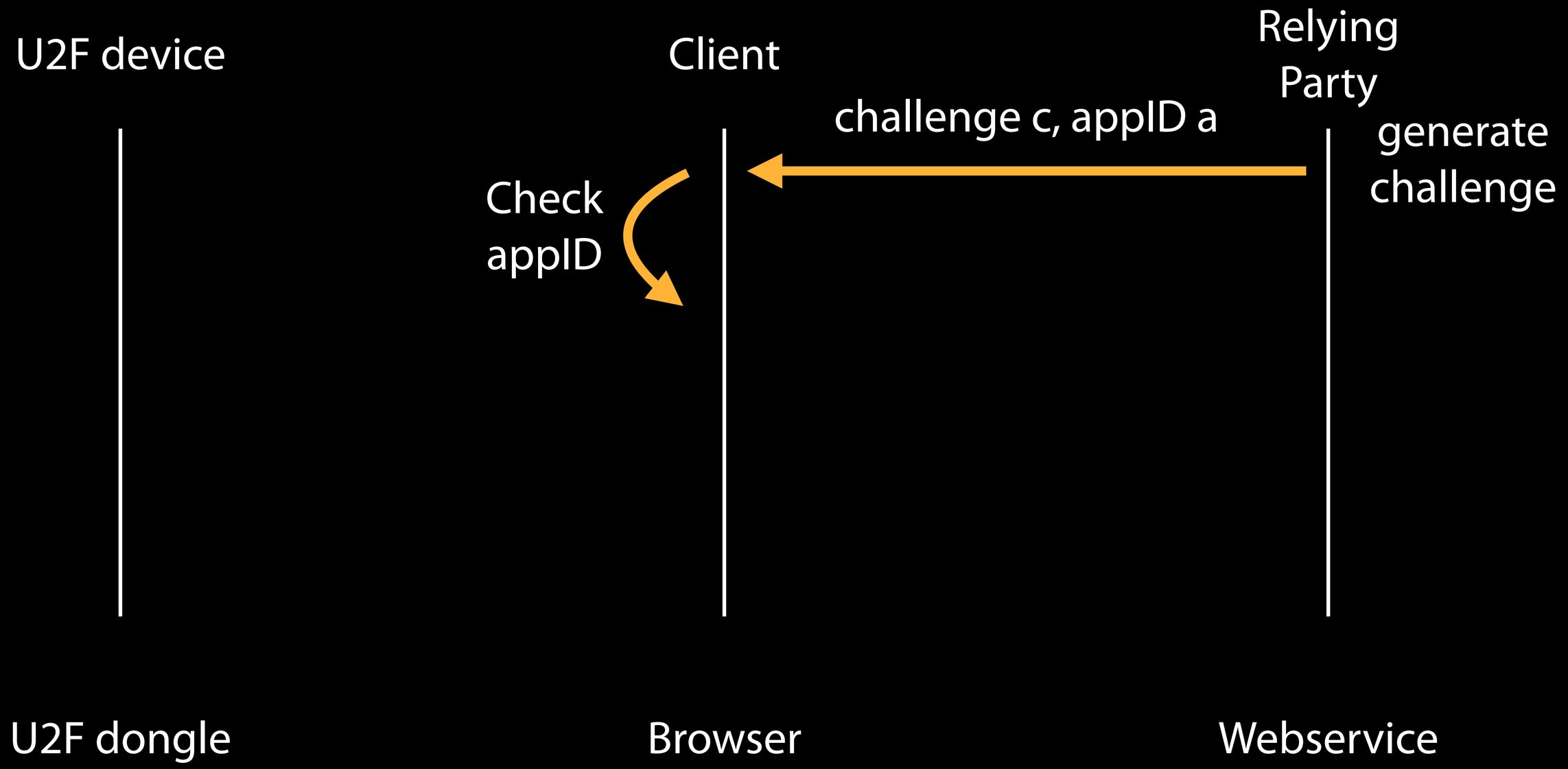
Registration



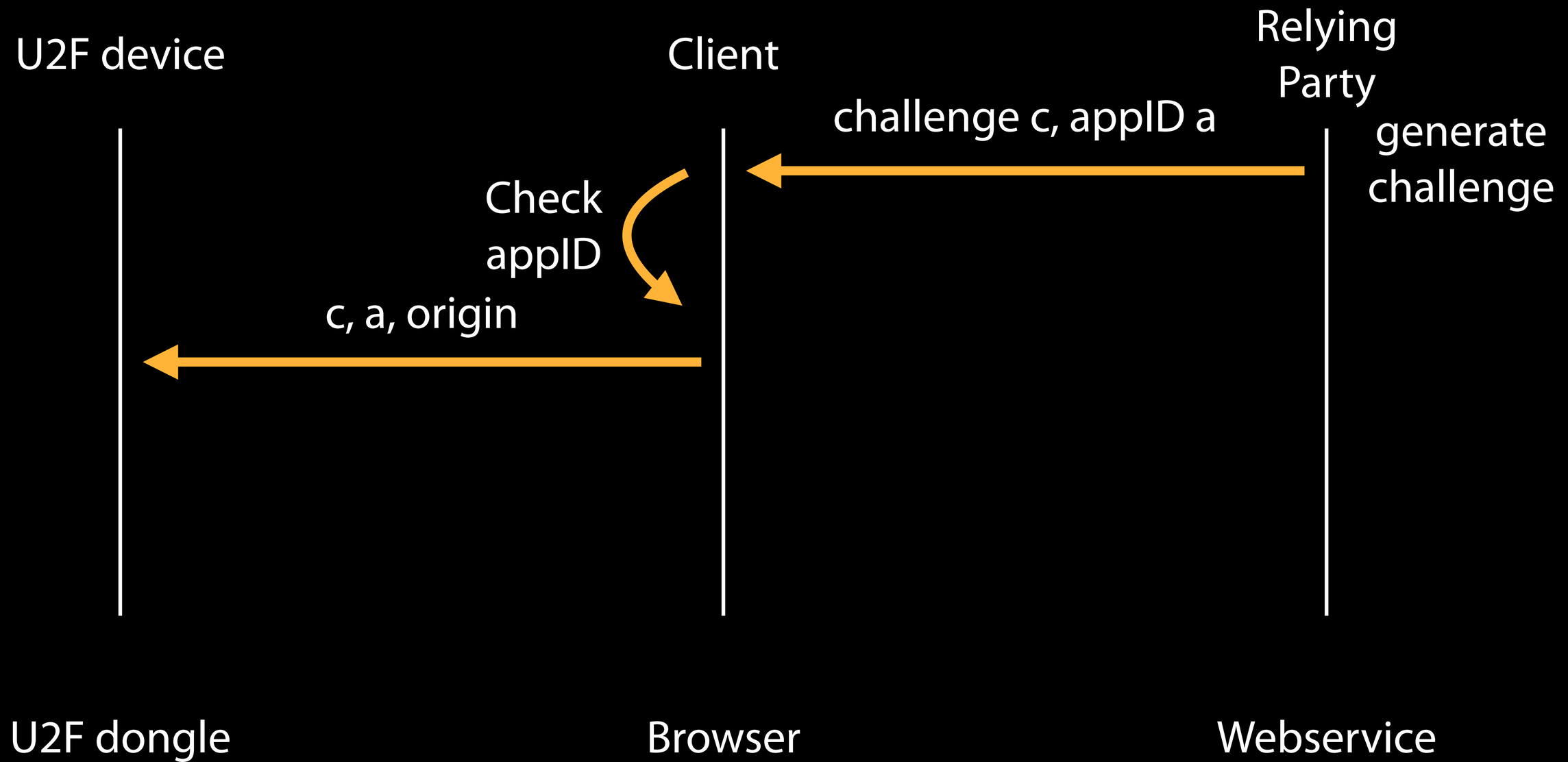
Registration



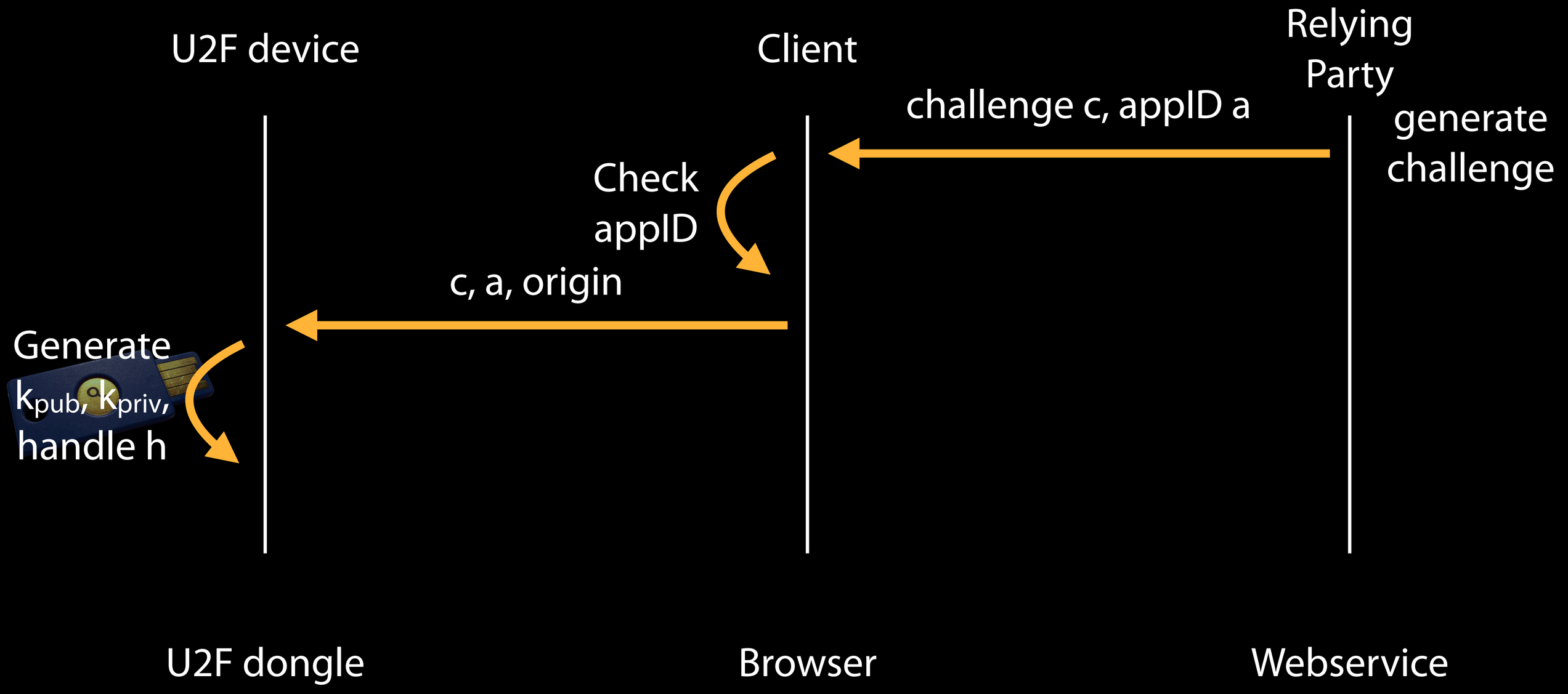
Registration



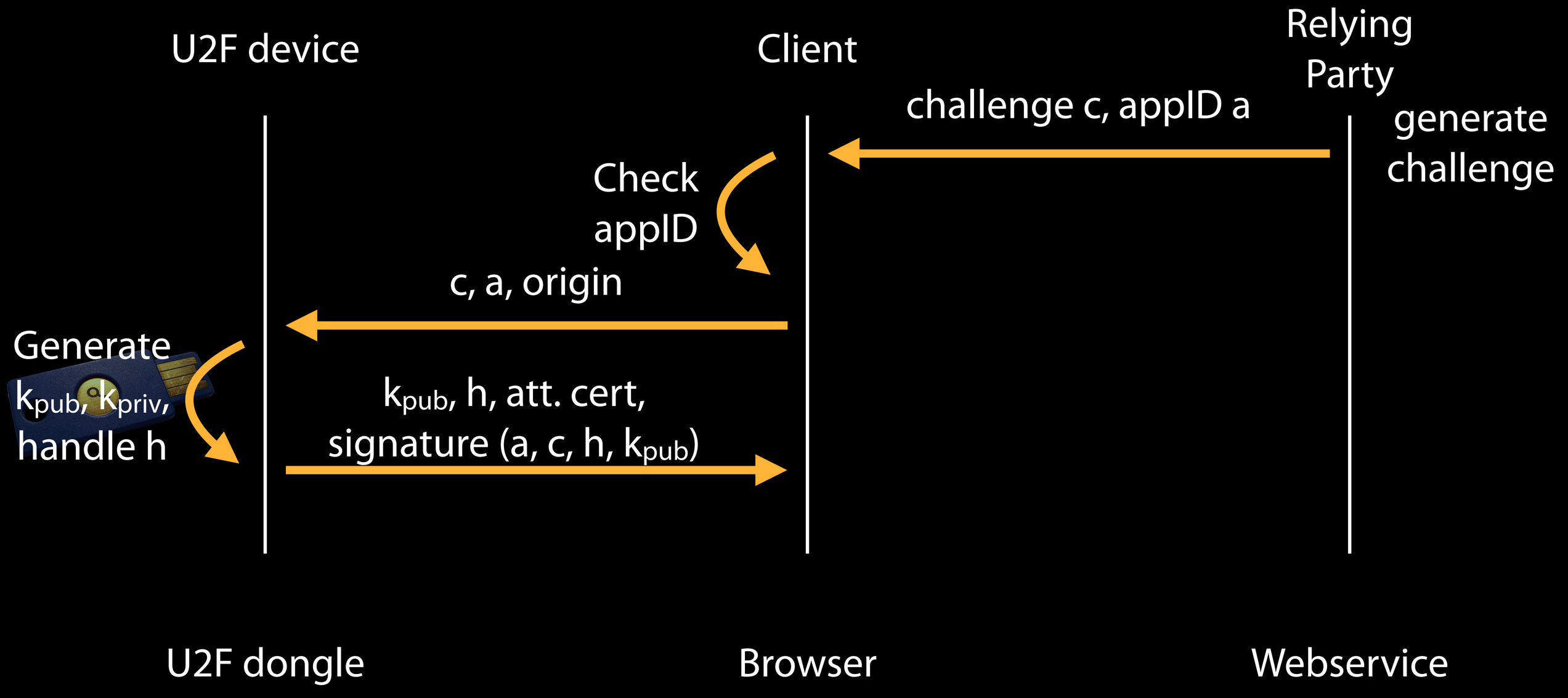
Registration



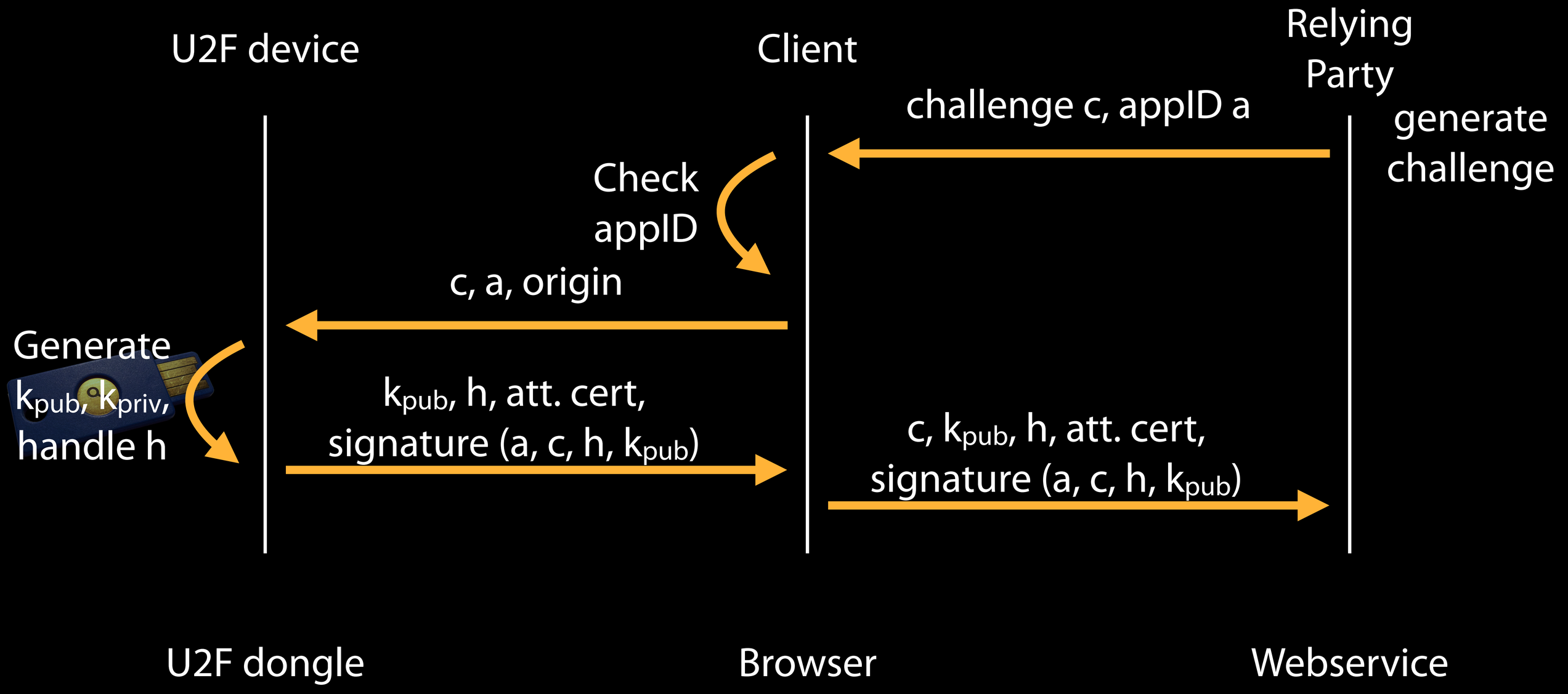
Registration



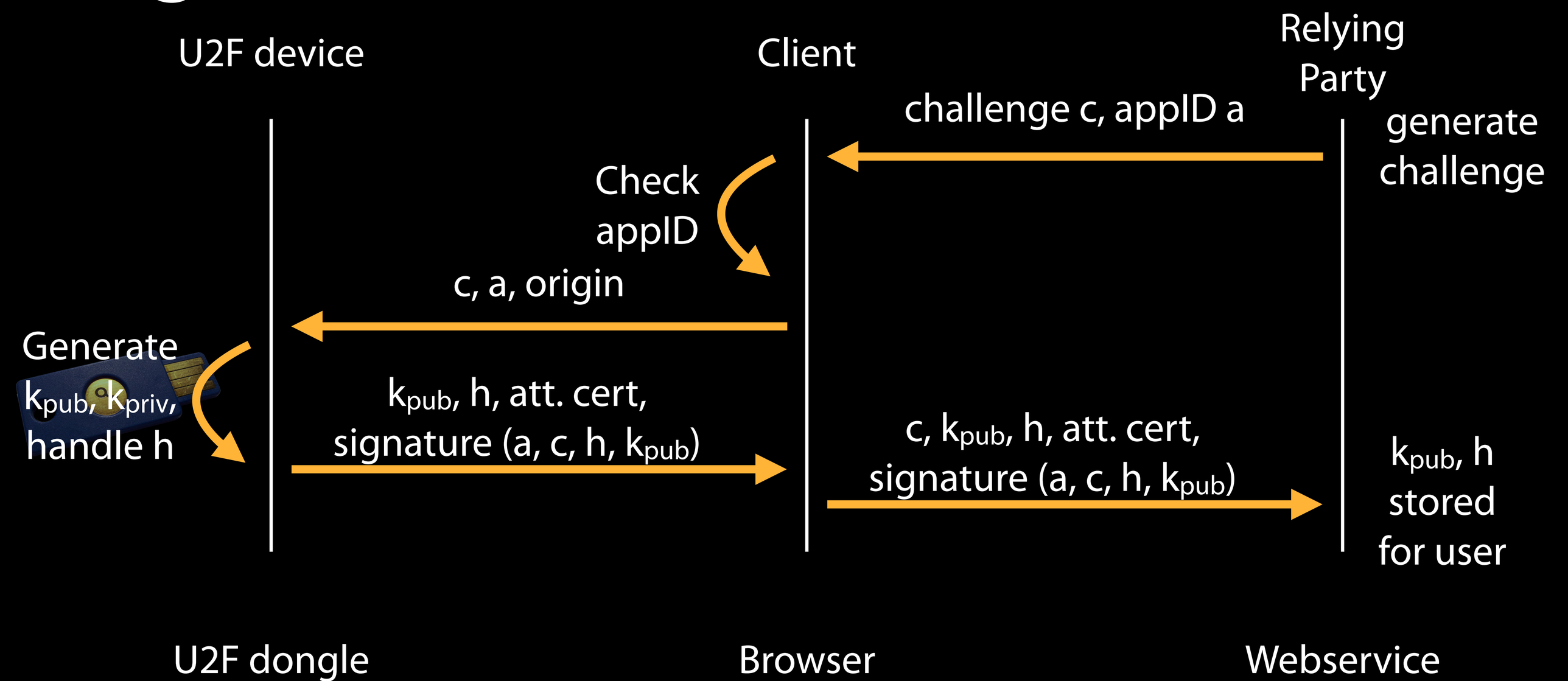
Registration



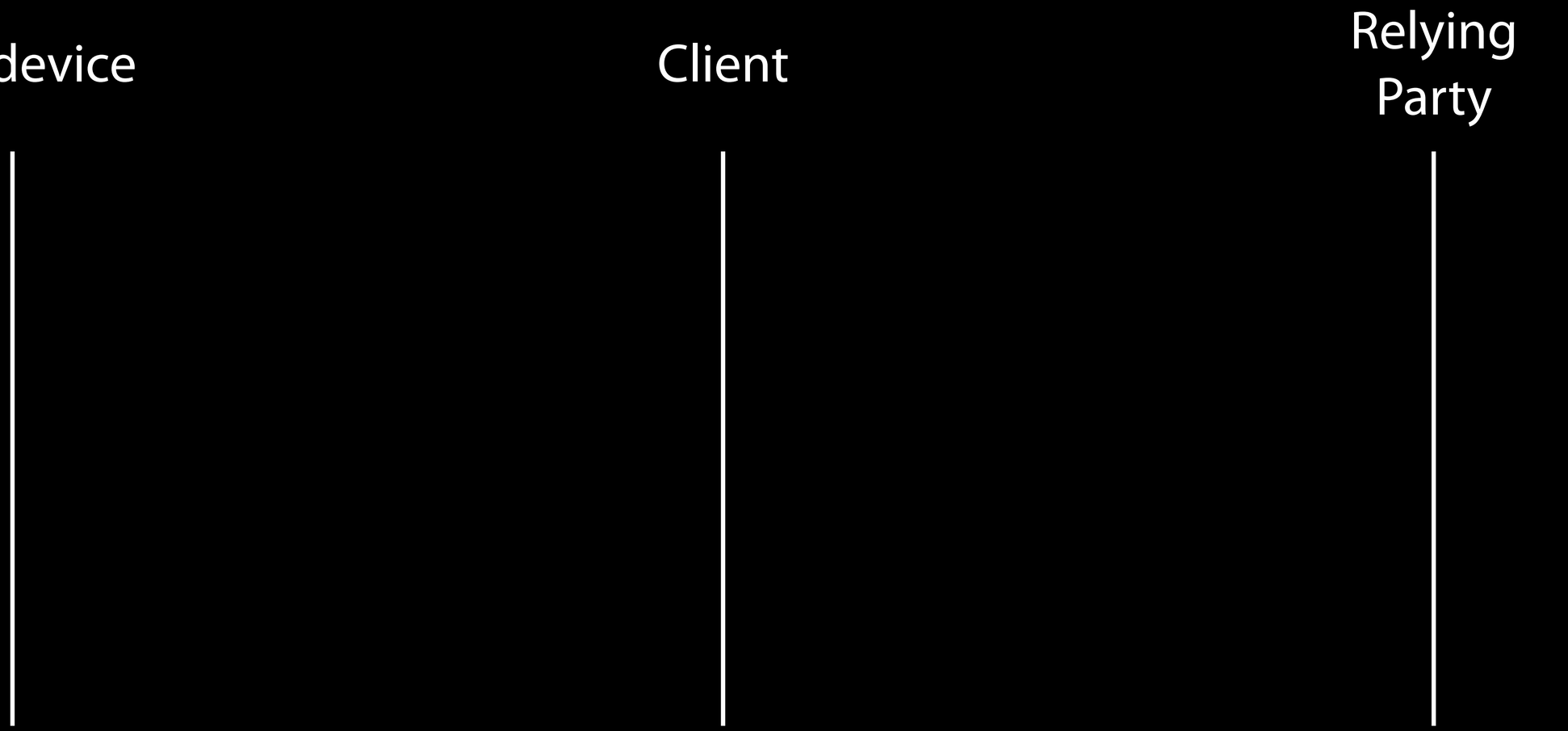
Registration



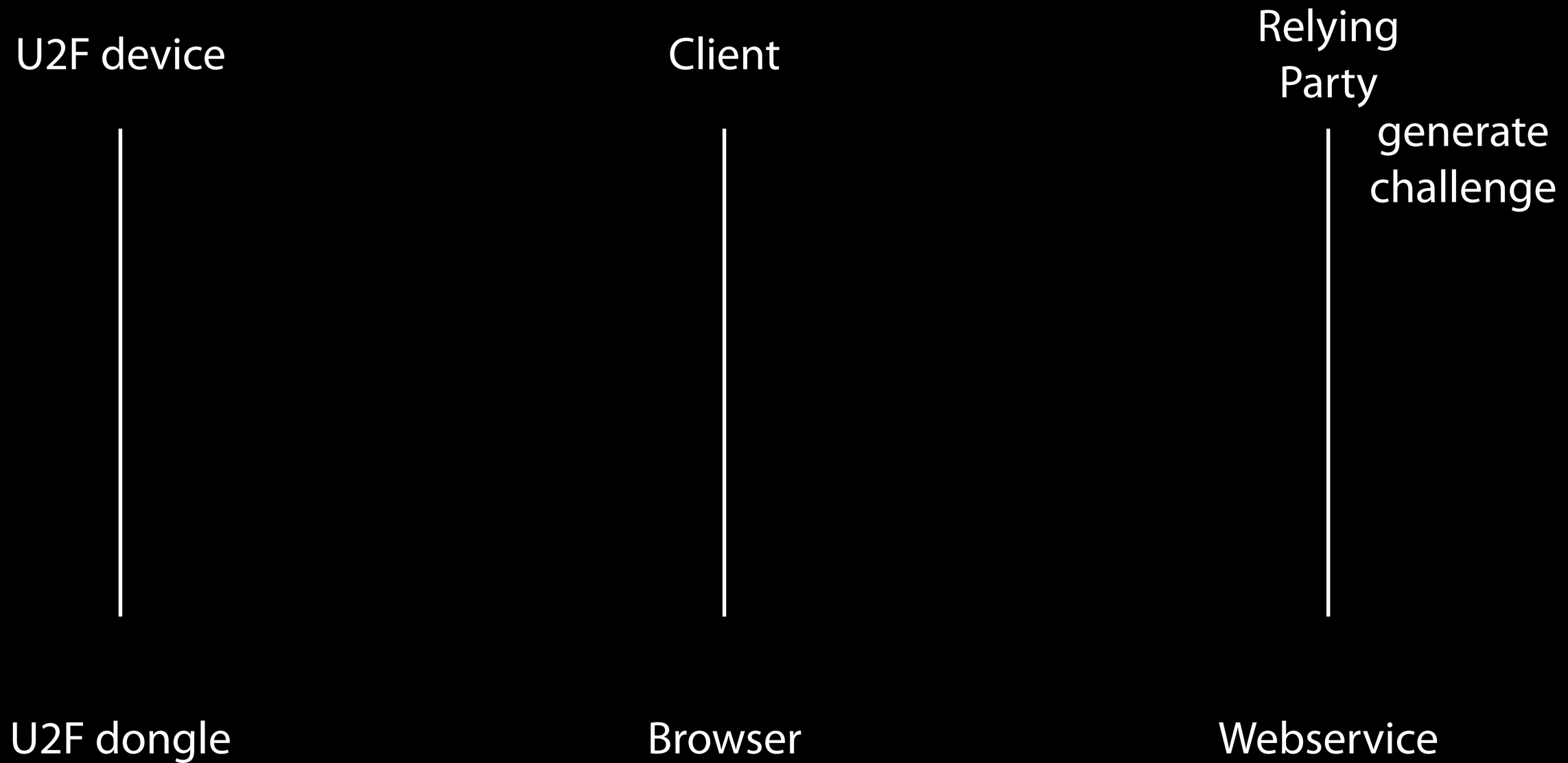
Registration



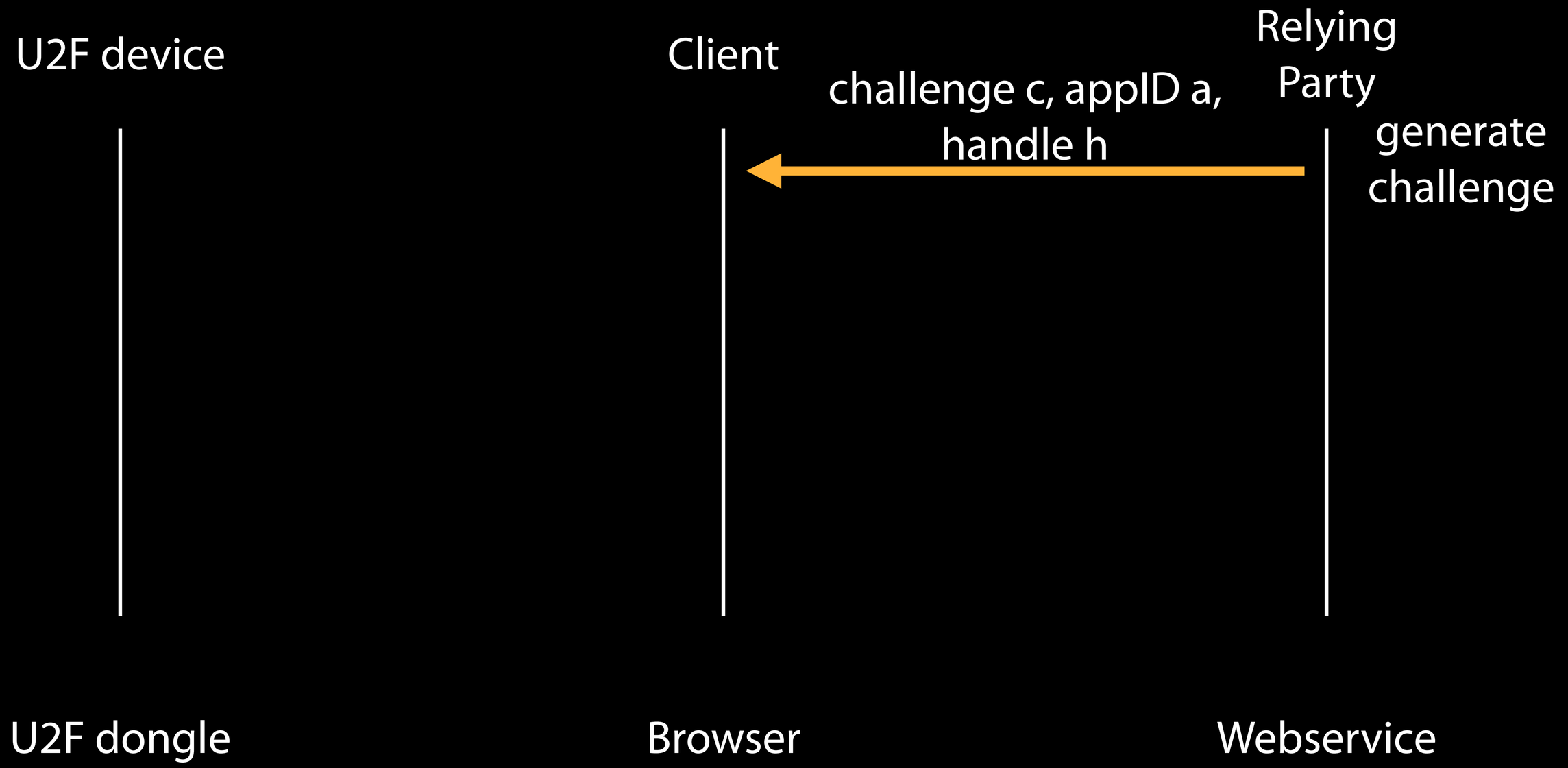
Authentication



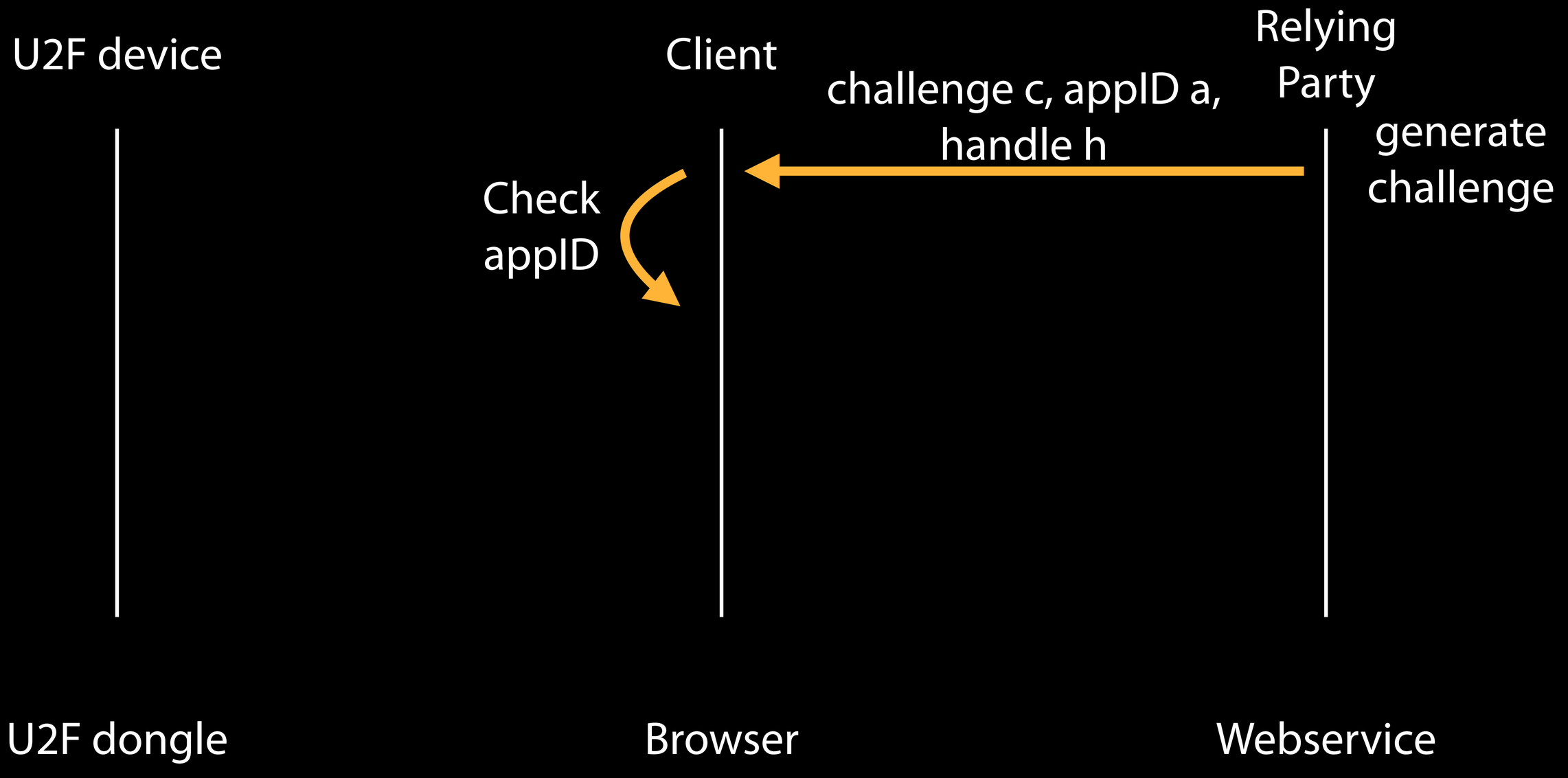
Authentication



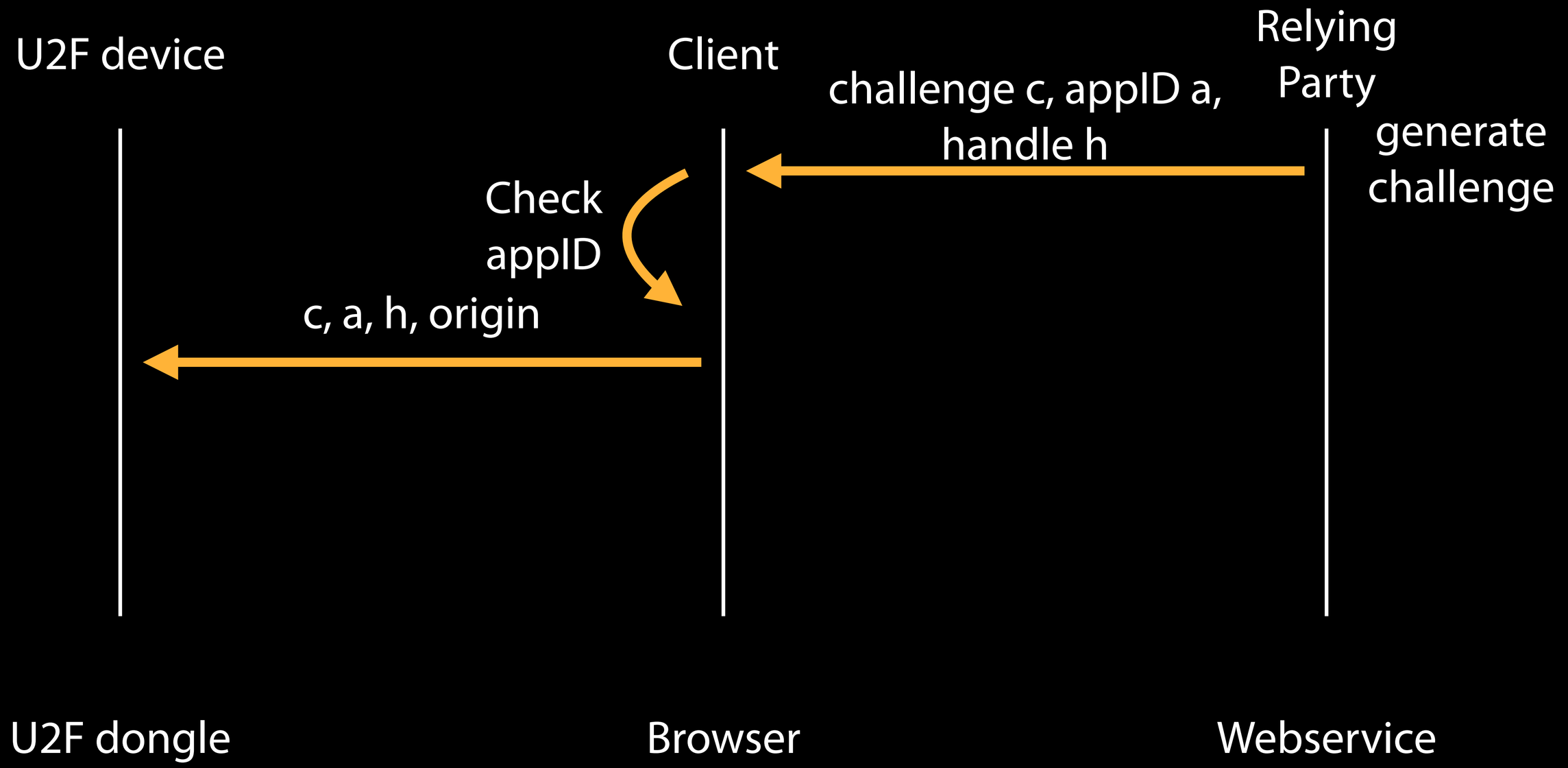
Authentication



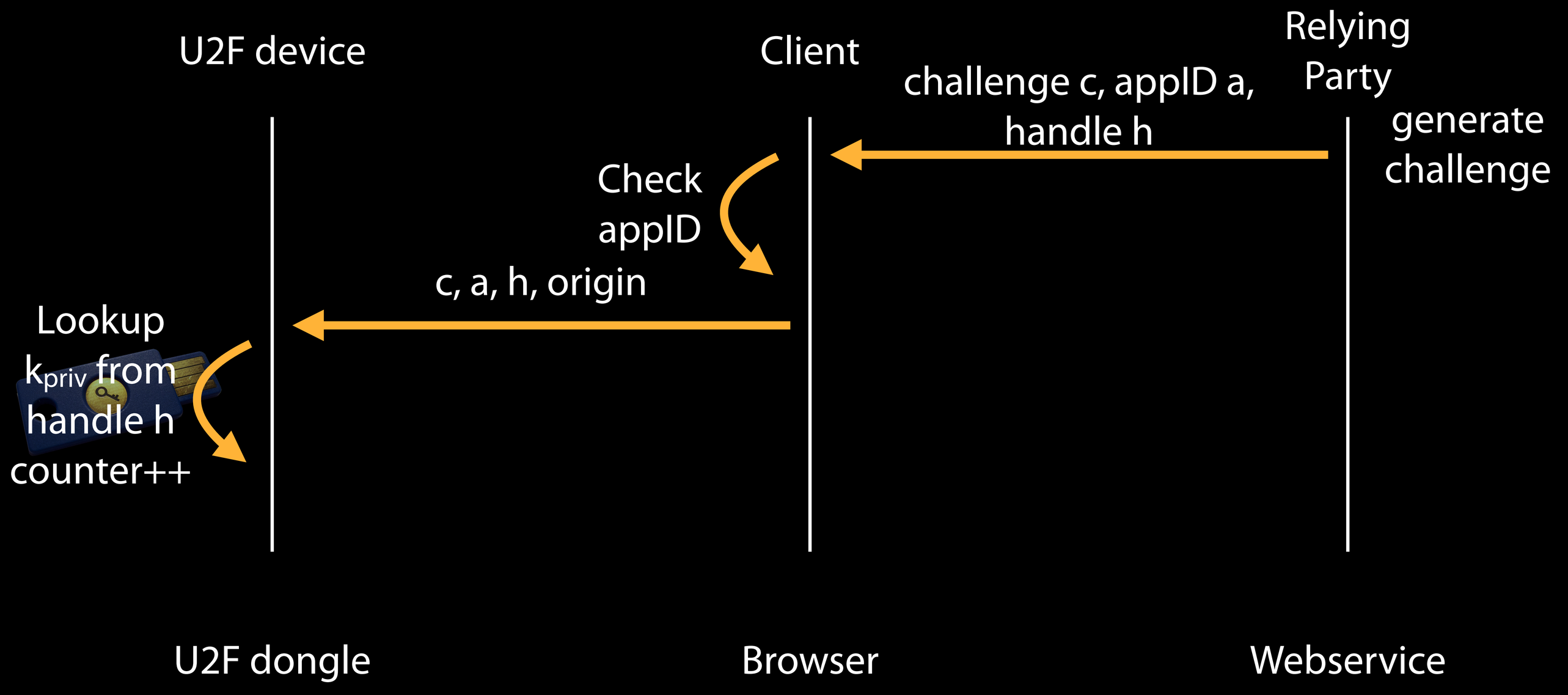
Authentication



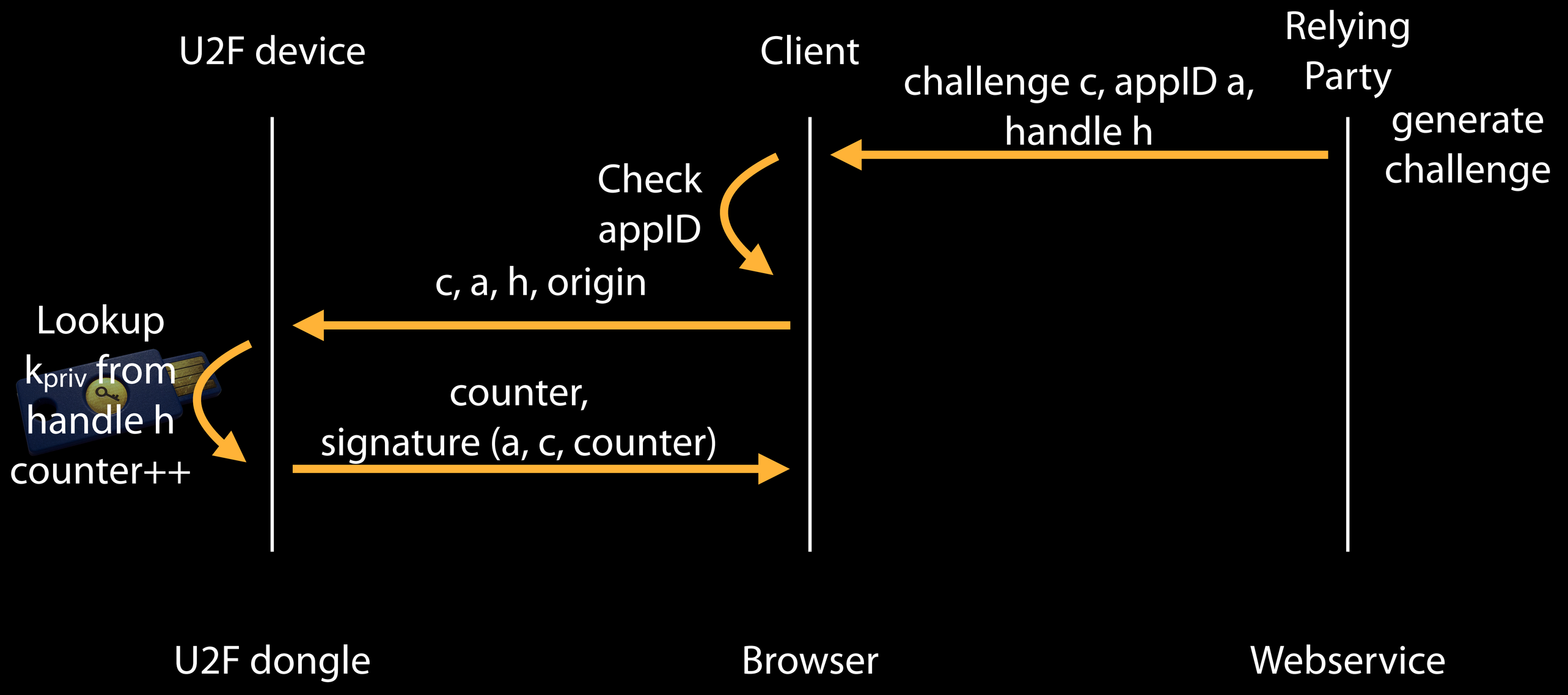
Authentication



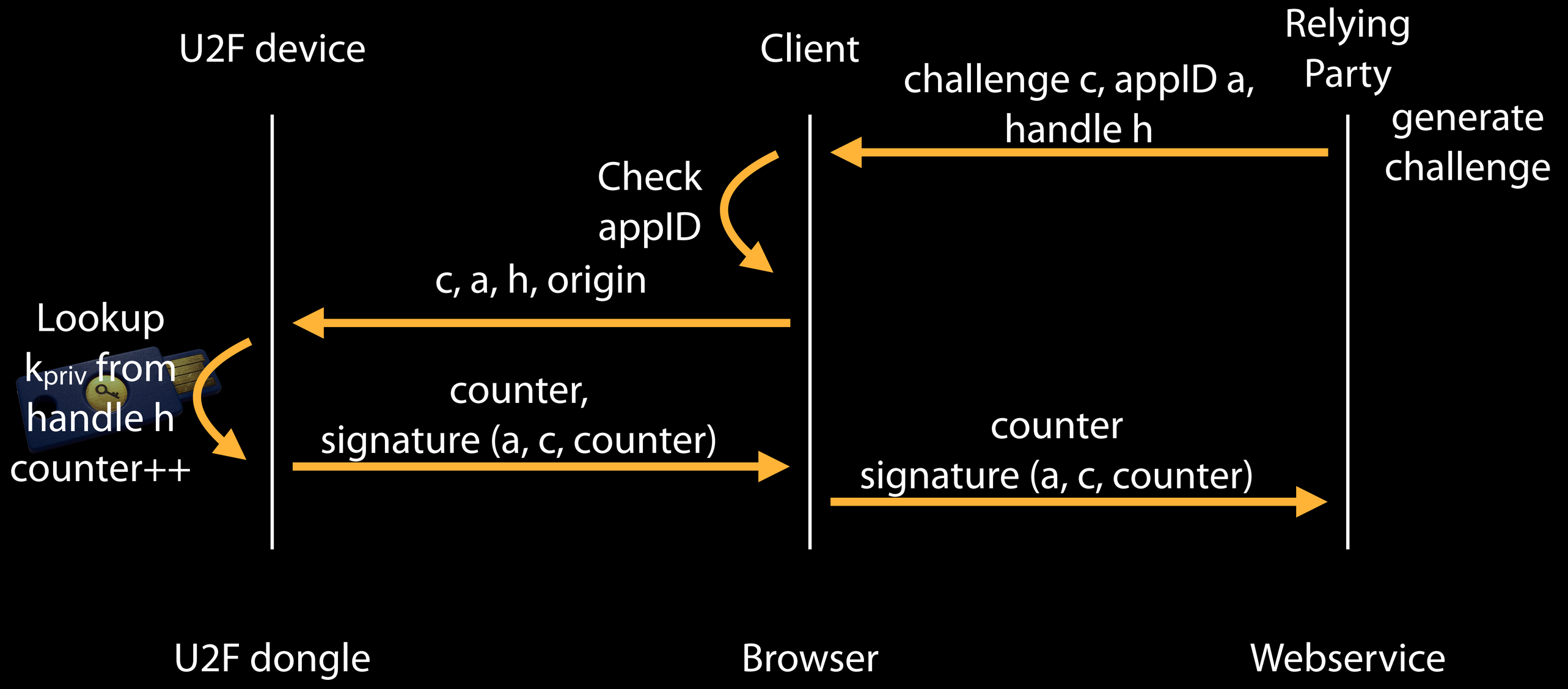
Authentication



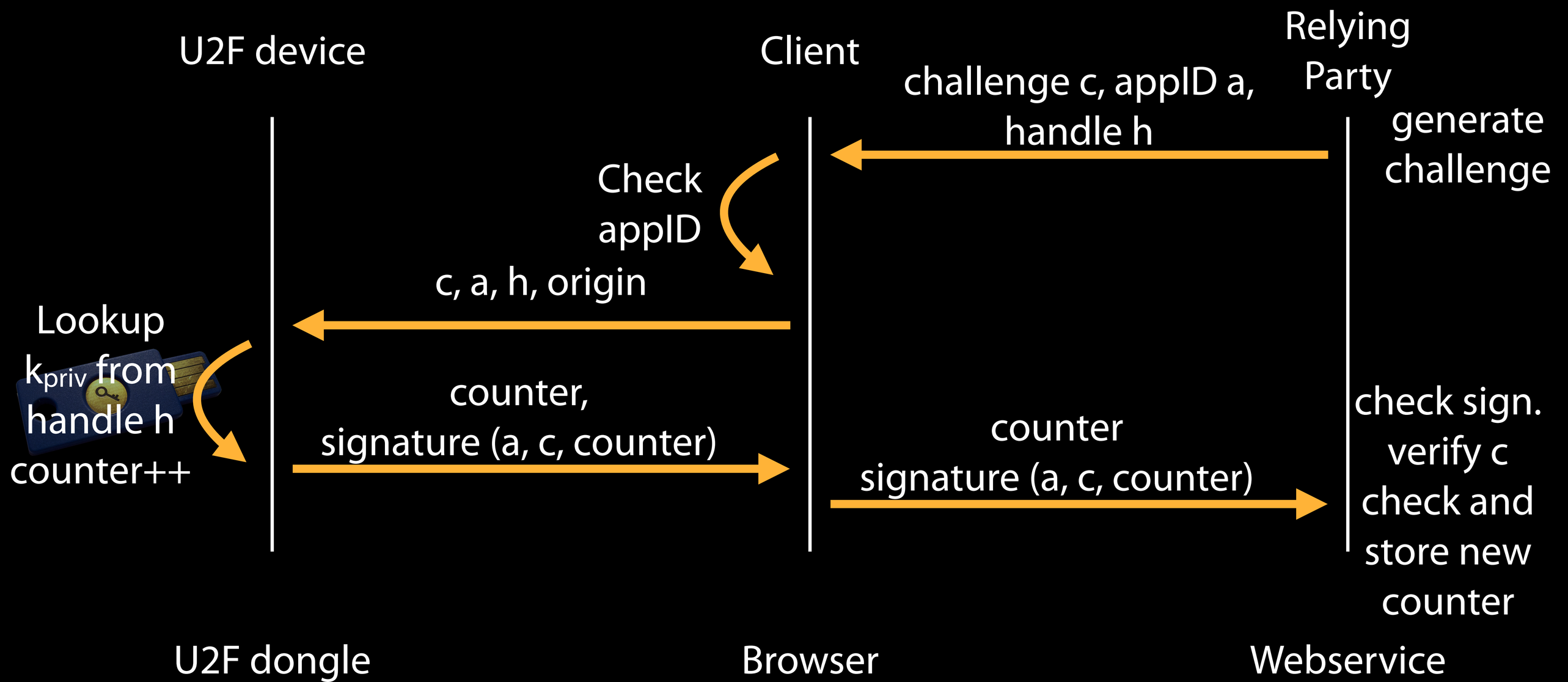
Authentication



Authentication



Authentication



How many accounts on the U2F dongle?

- As many as you like!
- The private key is NOT stored on the device in Yubico’s implementation. Instead it is encrypted with a 256bit AES key on the secure element on the dongle.

U2F Summary

- Every account on every website gets a new public-private key pair.
- The dongle has no UUID and cannot be tracked between different sites.
- No passcode has to be entered manually.
- No shared secret - even if key handle and public keys leaked one cannot copy the U2F dongle.

References

- Yubico U2F demo server https://demo.yubico.com/u2f
- The U2F specifications https://fidoalliance.org/specifications/download/
- Yubico developers for U2F https://developers.yubico.com/U2F/
- Yubico U2F C host library https://github.com/Yubico/libu2f-host