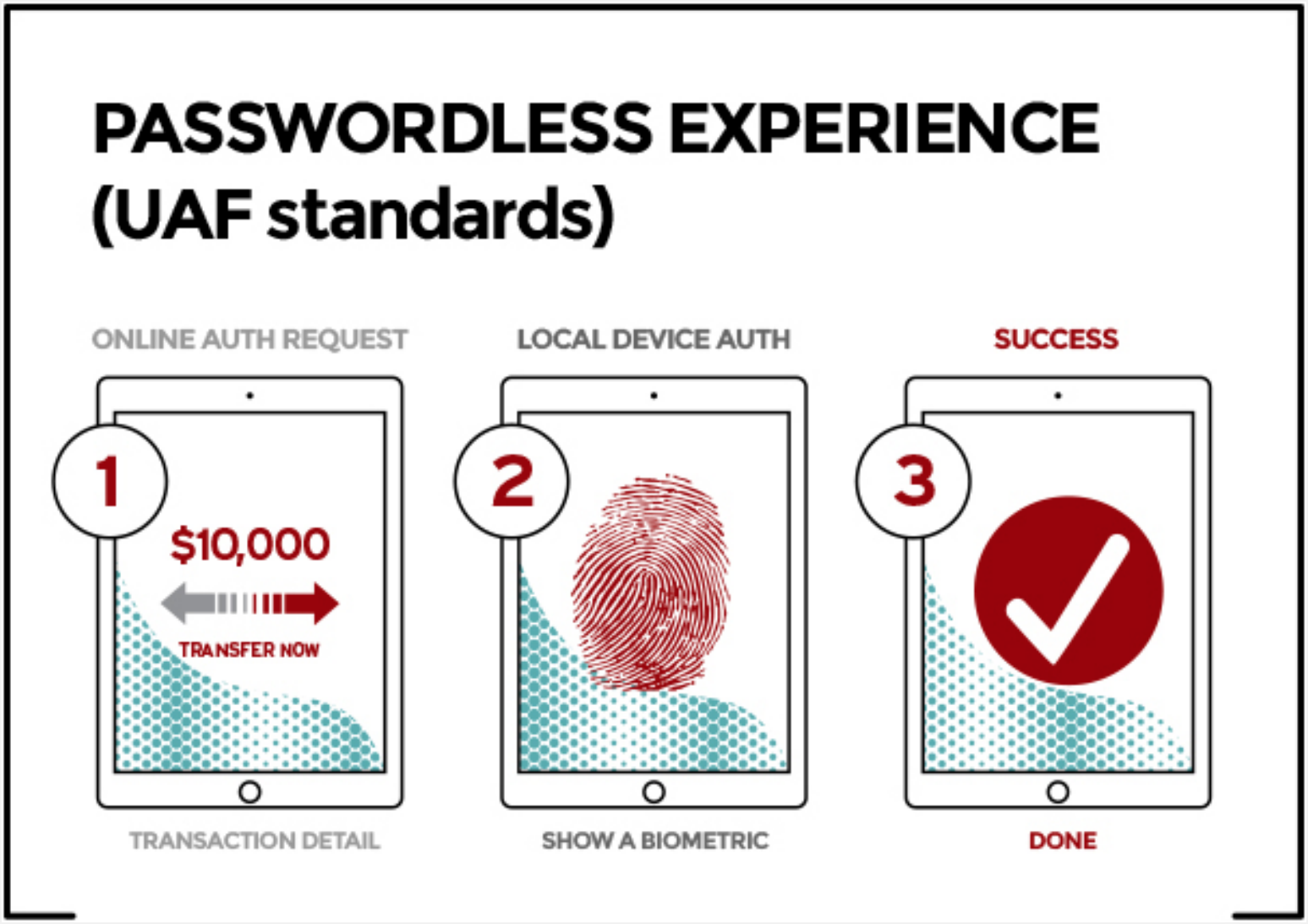
fido™ alliance | simpler stronger authentication

UAF Technical Overview

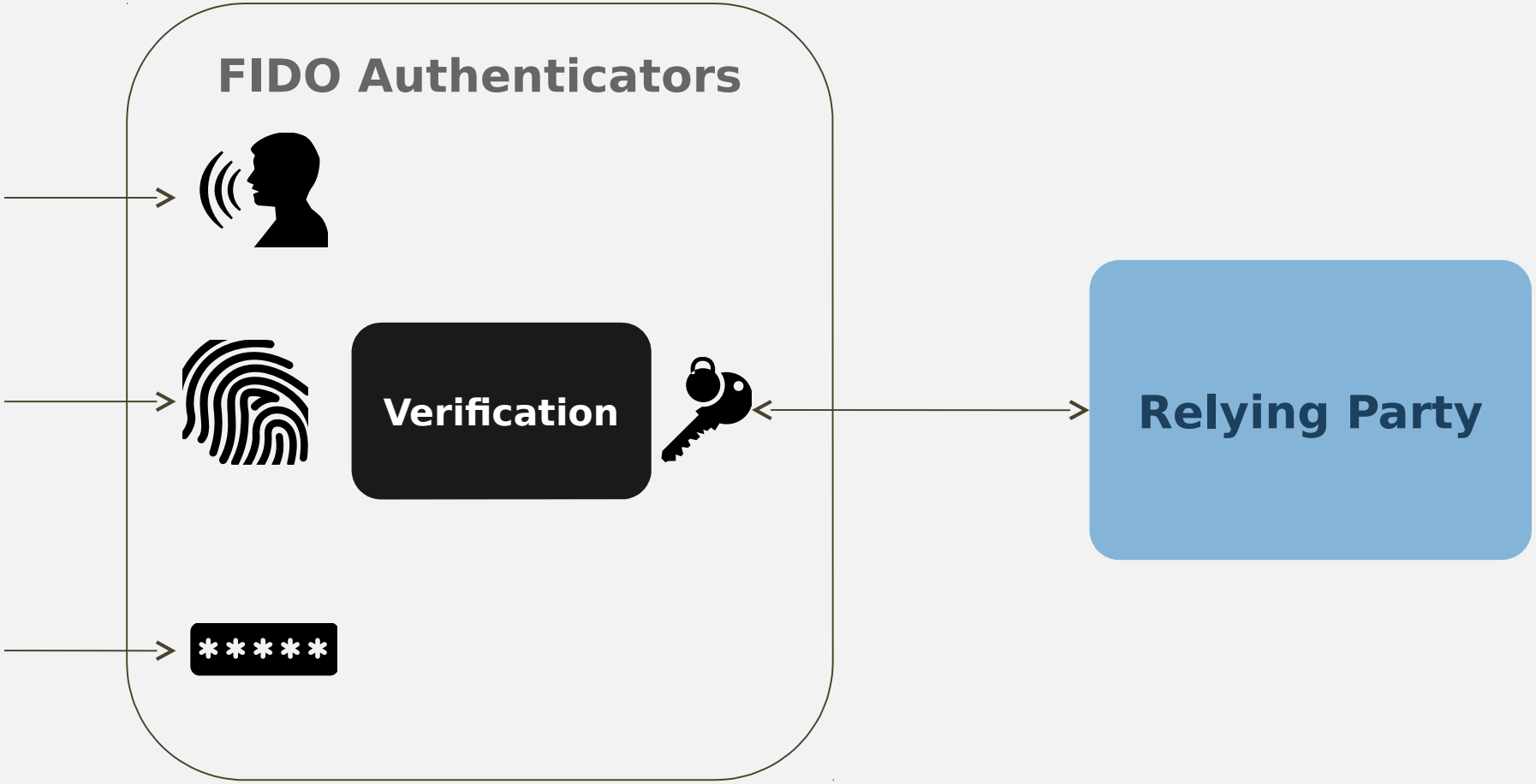
Davit Baghdasaryan – Nok Nok Labs

UAF



http://www.fidoalliance.org/specifications

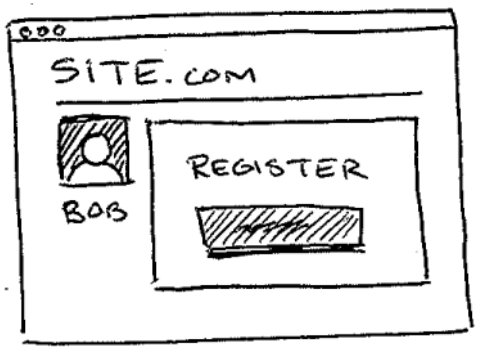
How does UAF work?



FIDO Registration

1

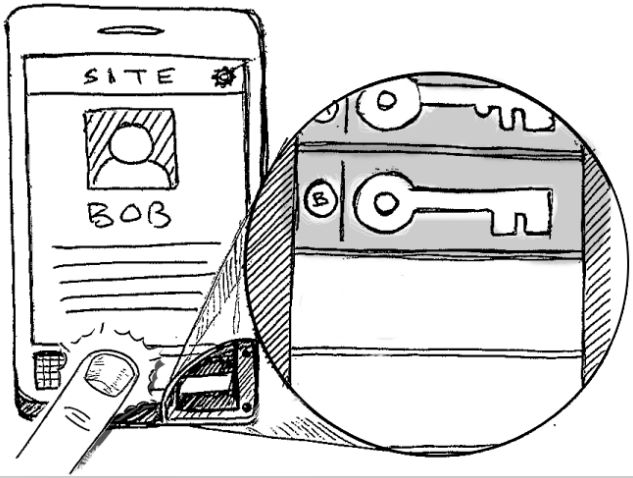
REGISTRATION BEGINS



USER APPROVAL

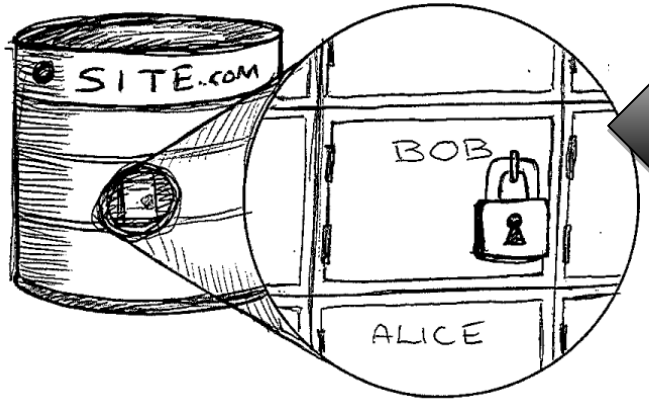
USER APPROVAL

2



4

REGISTRATION COMPLETE

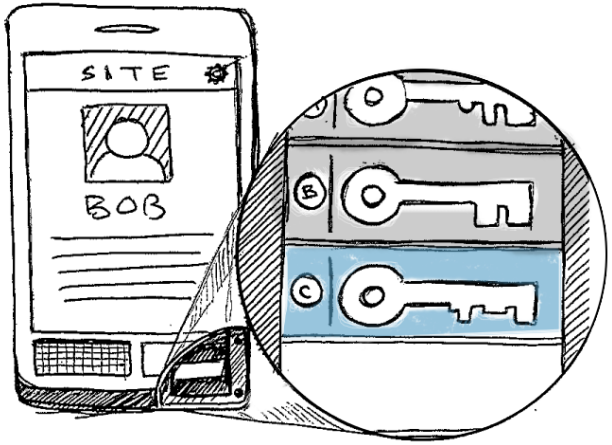


KEY REGISTERED

Using
Public key
Cryptography

NEW KEY CREATED

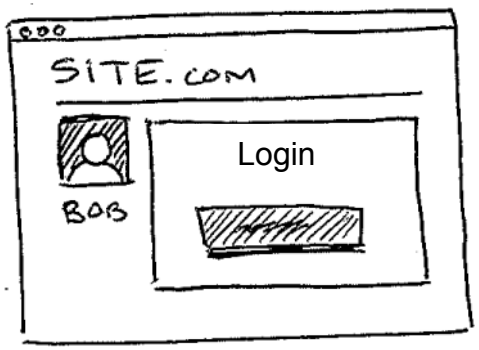
3



FIDO Login

1

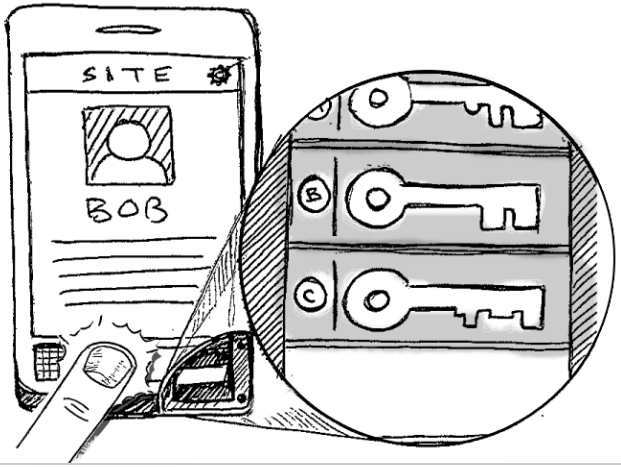
LOGIN



LOGIN CHALLENGE

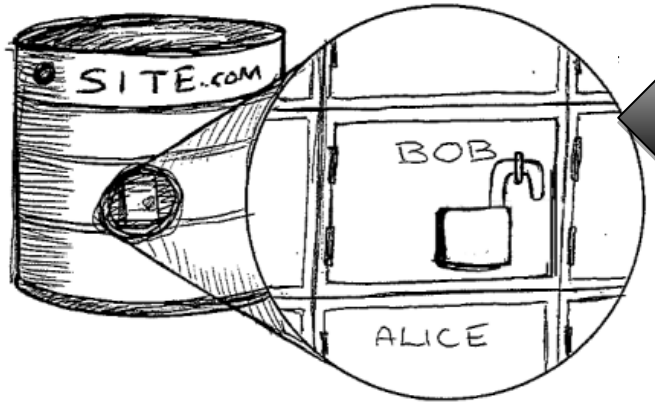
2

USER APPROVAL



4

LOGIN COMPLETE

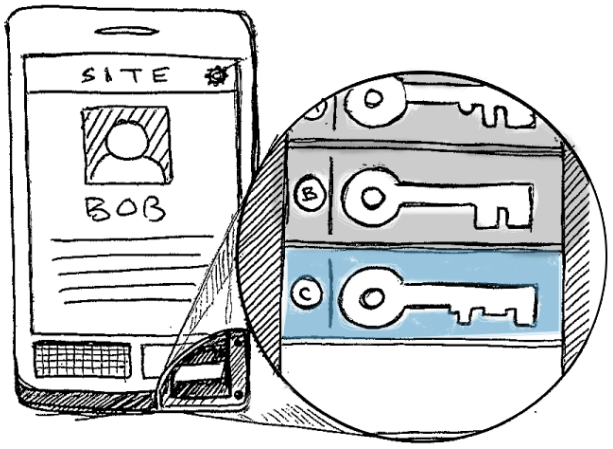


LOGIN RESPONSE

Using
Public key
Cryptography

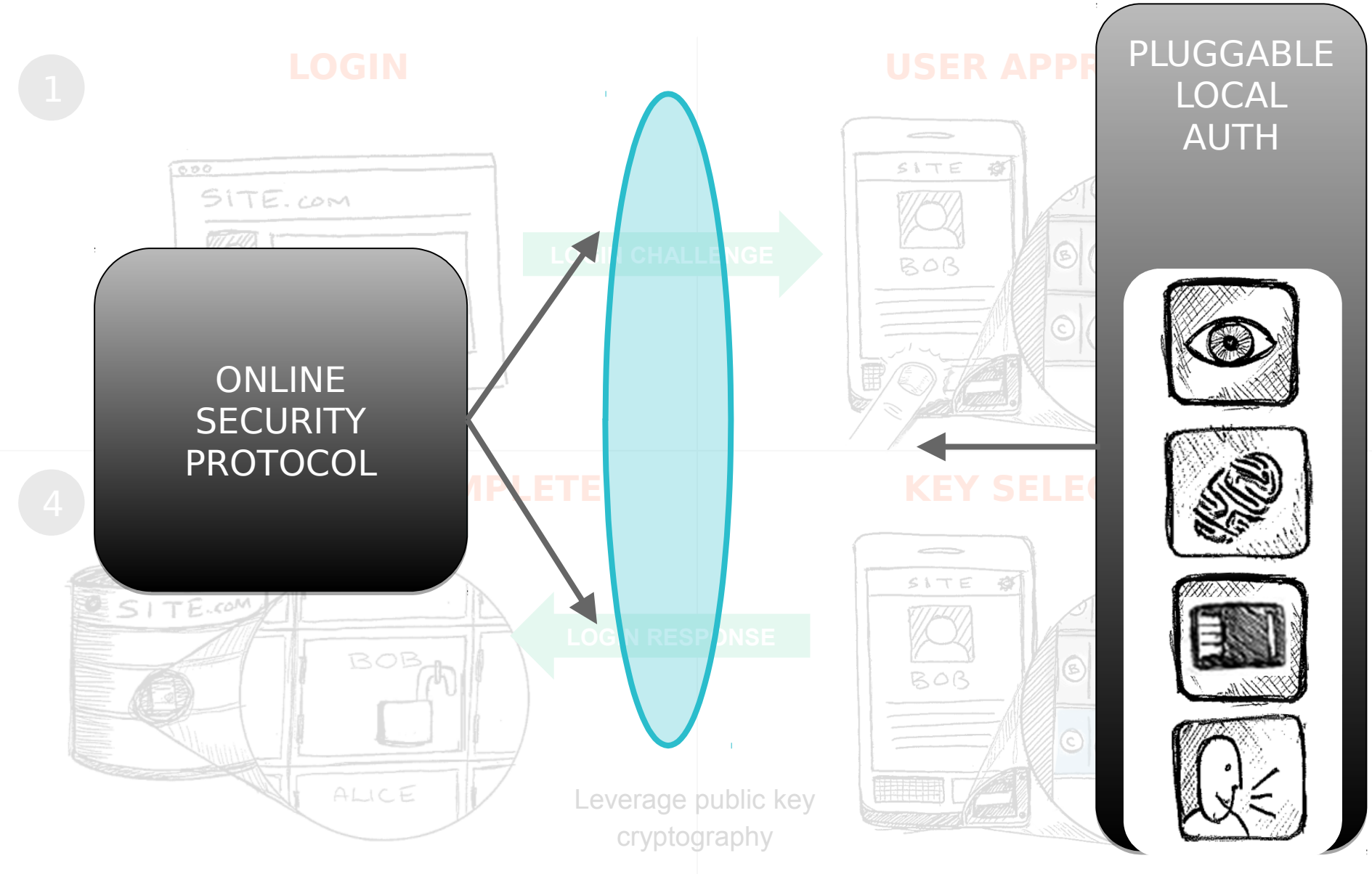
3

KEY SELECTED



UAF Design Considerations

Decouple User Verification Method from Authentication Protocol



No 3rd Party in the Protocol

No secrets on Server side

Focus on User Privacy

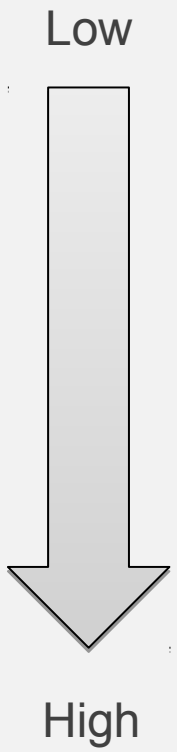
- Biometric data never leaves user’s device
- No linkability between RPs
- No linkability between RP accounts

Embrace all kinds of Authenticators

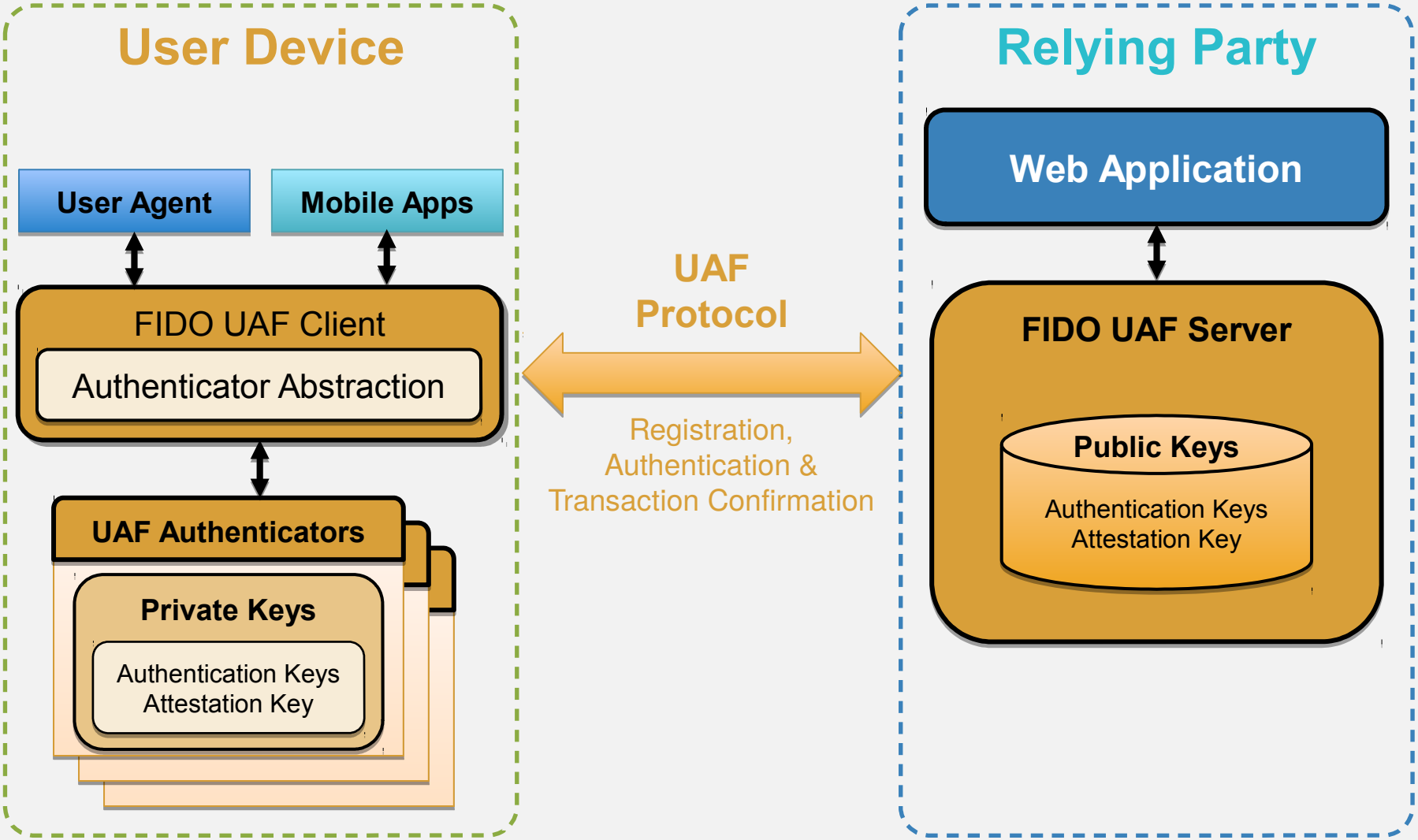
software, proprietary hardware, certified hardware, ...

Risk Based Authentication

- Login to online account
- Change shipping address
- Transfer $10.000



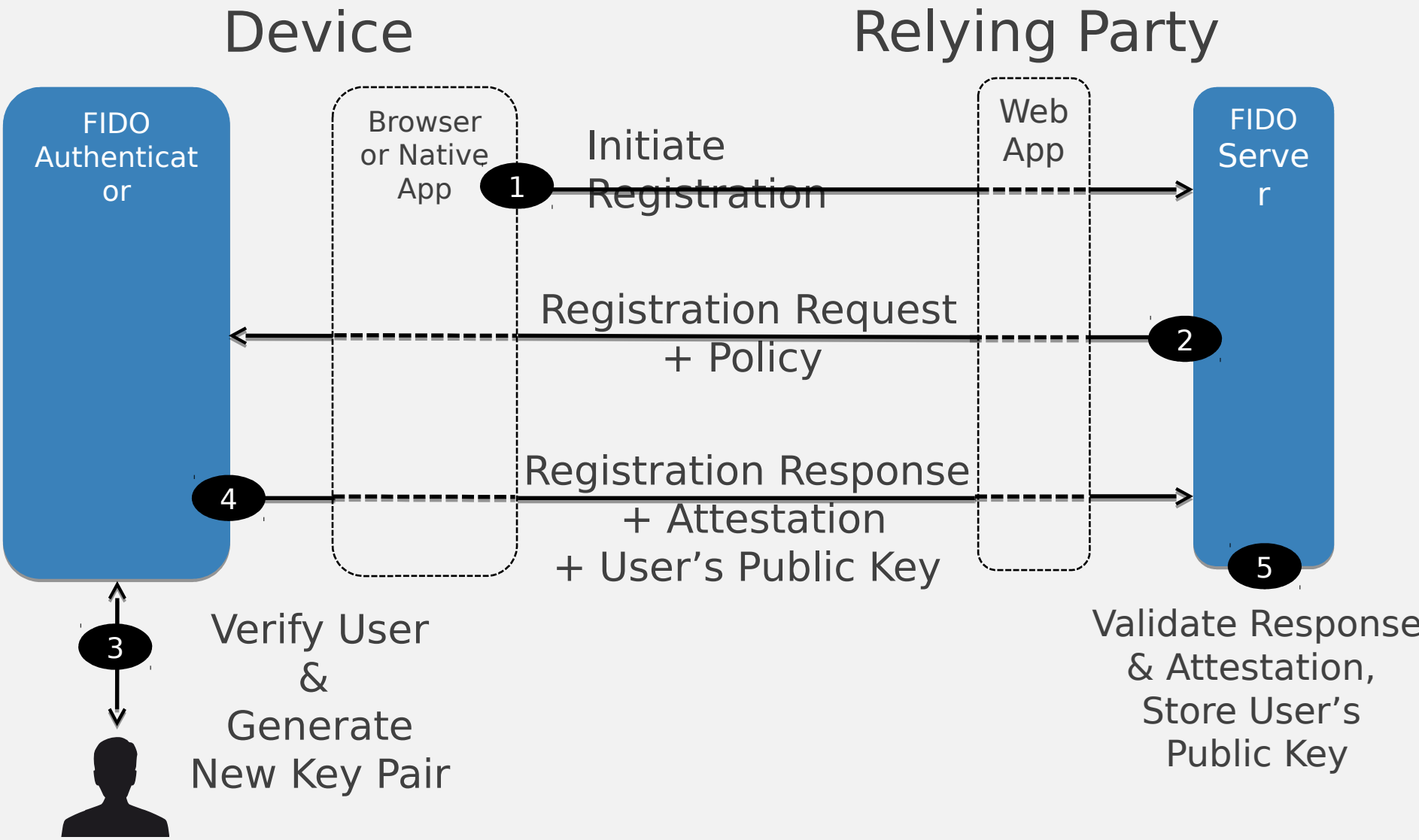
UAF Architecture


User Device
User Agent
Mobile Apps
FIDO UAF Client
Authenticator Abstraction
UAF Authenticators
Private Keys
Authentication Keys
Attestation Key
UAF
Protocol
Registration,
Authentication &
Transaction Confirmation
Relying Party
Web Application
FIDO UAF Server
Public Keys
Authentication Keys
Attestation Key

UAF Protocol

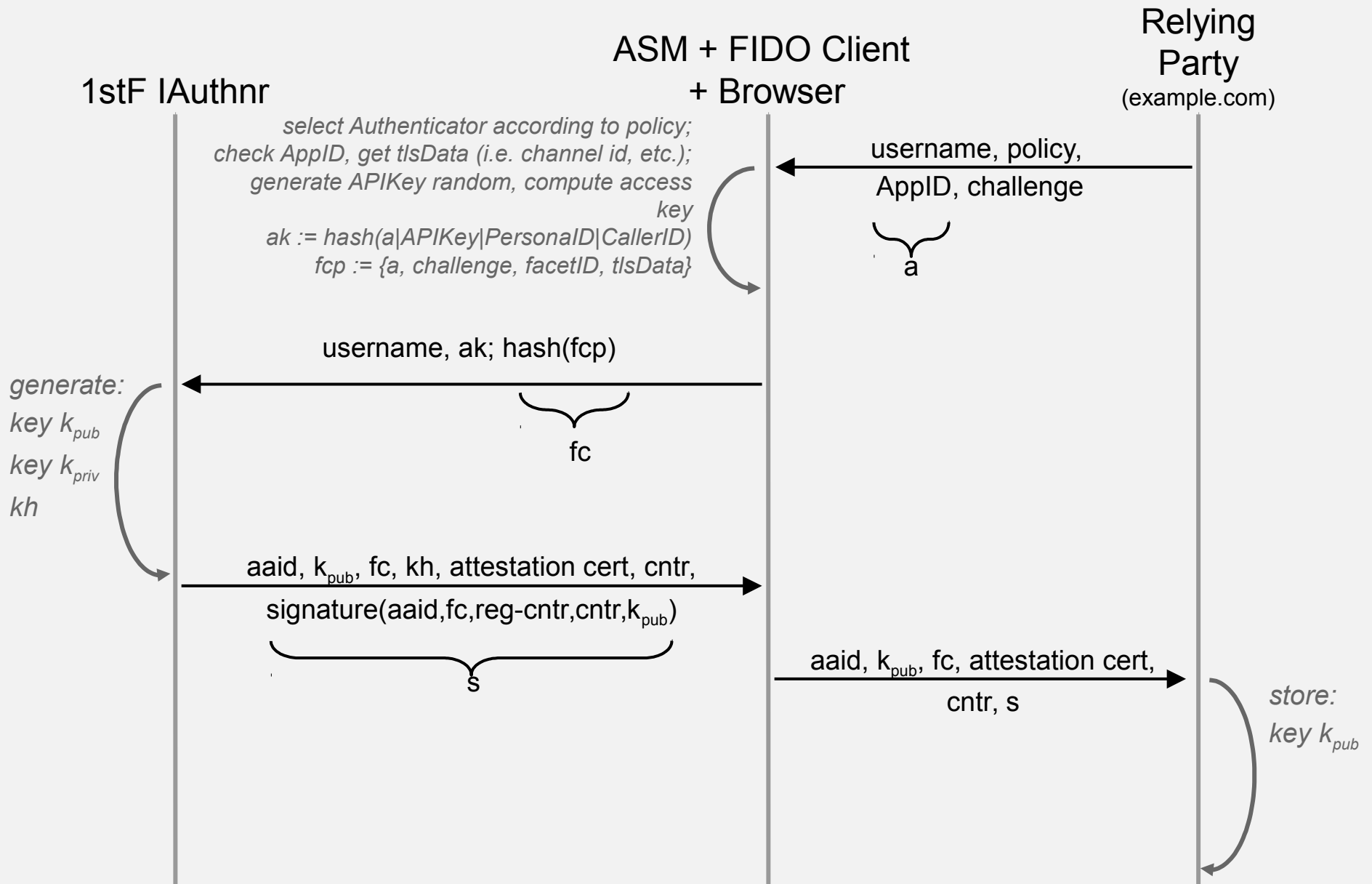
- Discovery of authenticators on the client
- Registration
- Authentication
- Transaction Confirmation
- Deregistration

Registration



UAF Registration

Note: This represents using a FIDO ***First-Factor Internal Authenticator*** -- it makes the differences to U2F more clear.

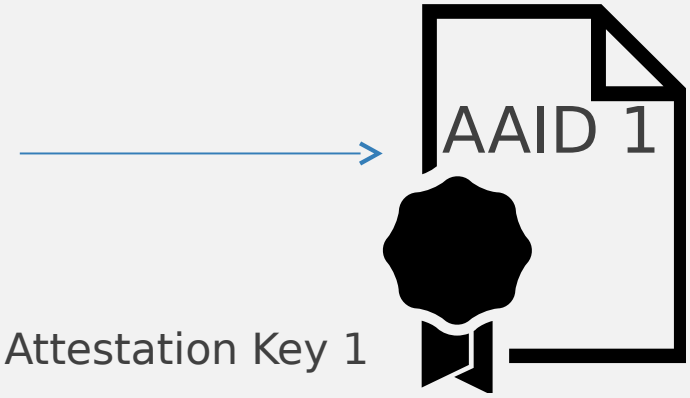


Attestation

FIDO Authenticator

Using HW based crypto

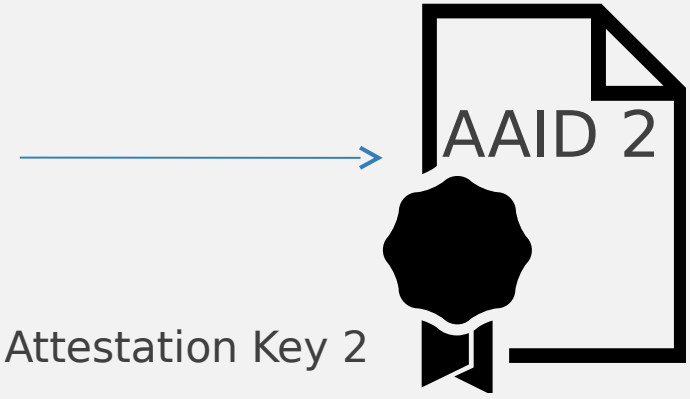
Based on FP Sensor X



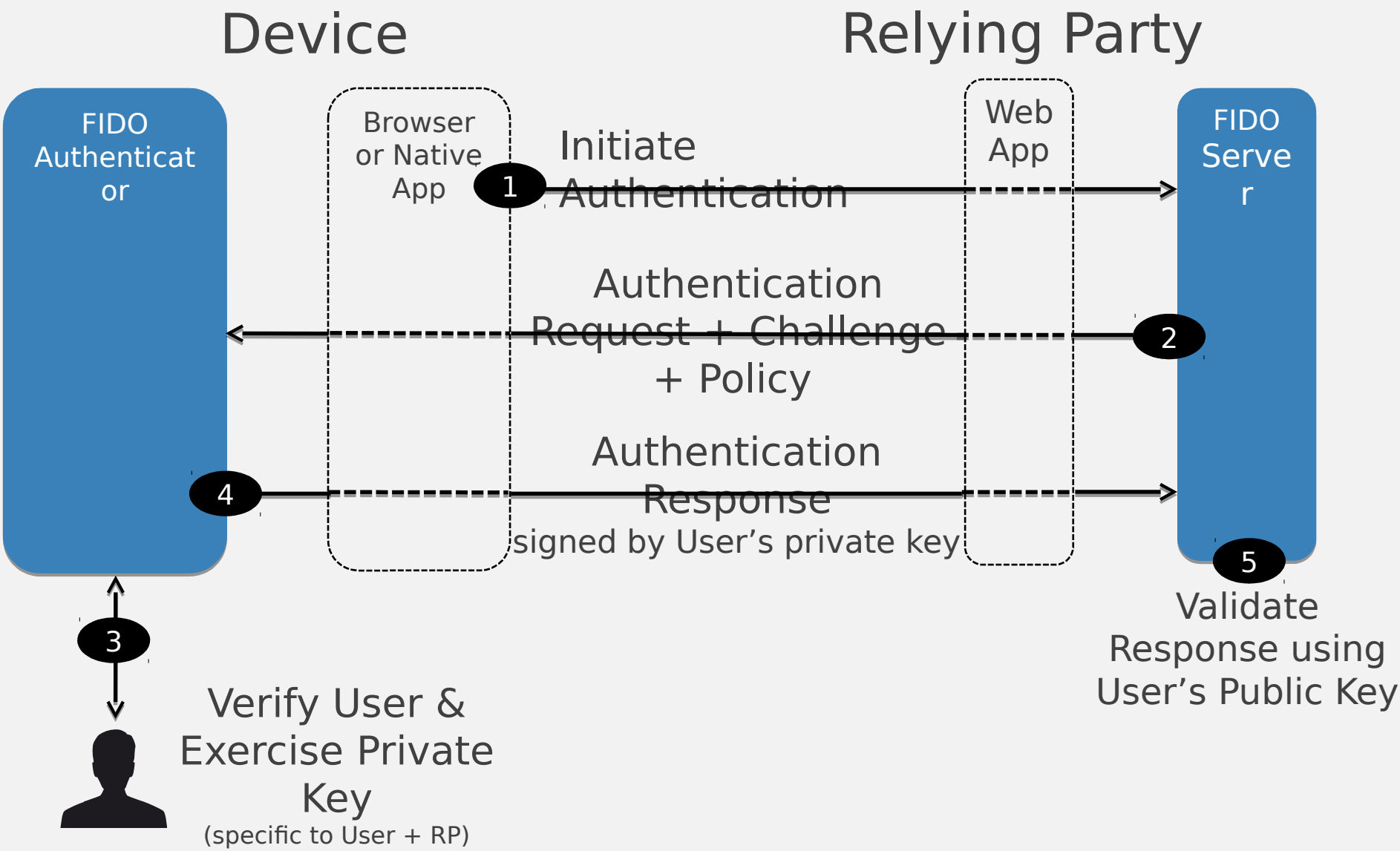
FIDO Authenticator

Pure SW based implementation

Based on Face Recognition alg. Y

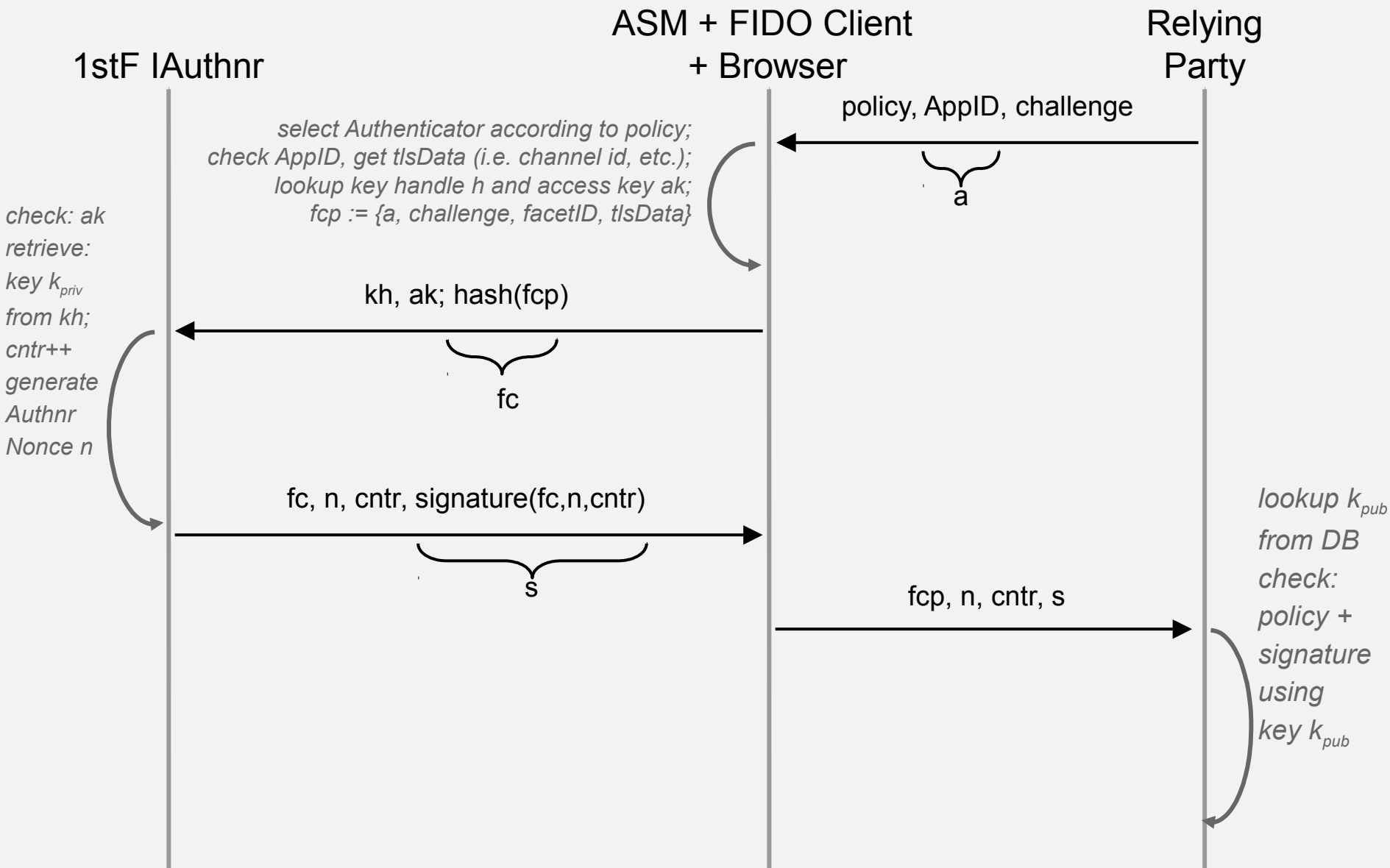


Authentication

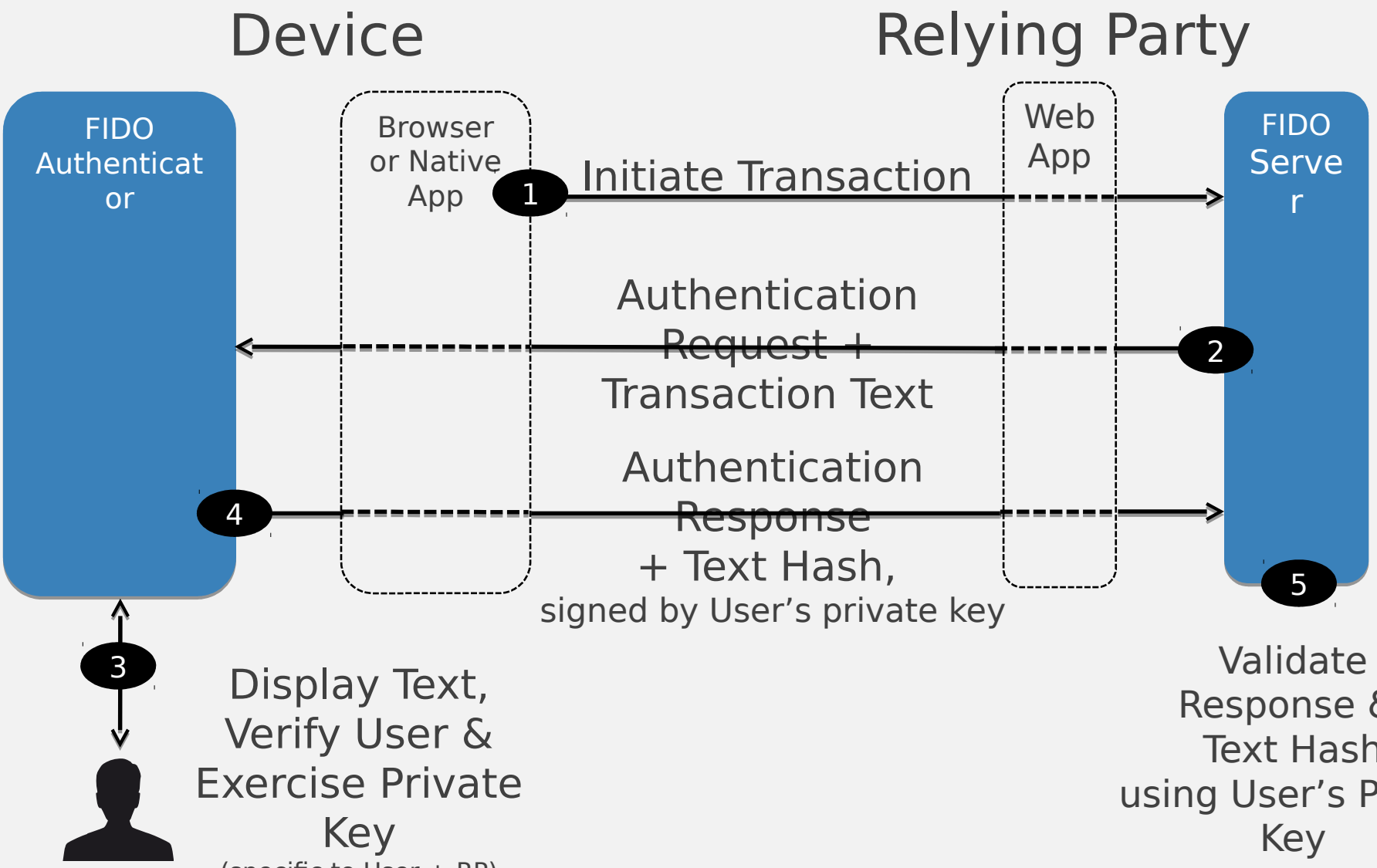


UAF Authentication

Note: NO username+Password login required before this sequence. Click on FIDO Button (or similar trigger) is sufficient.

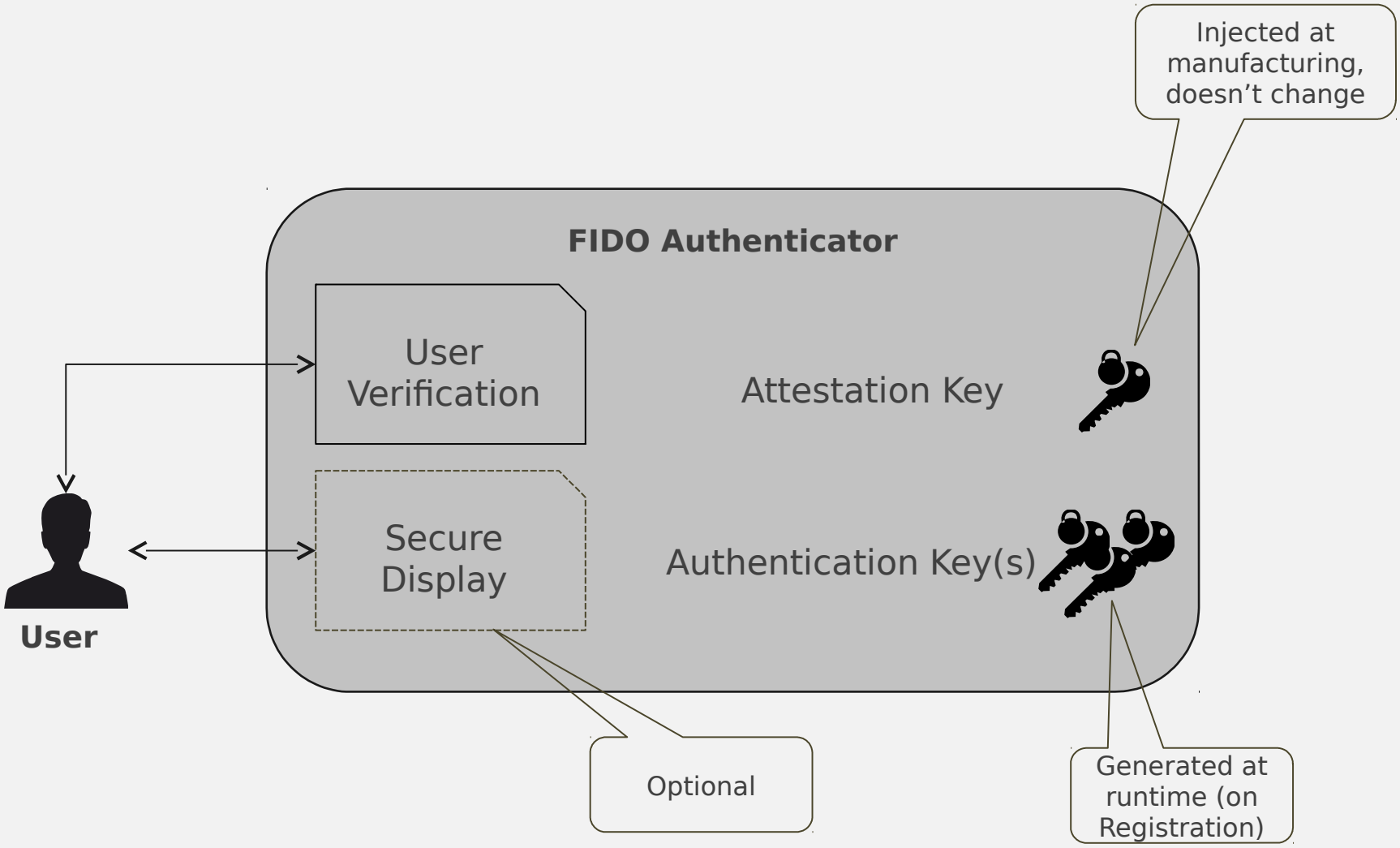


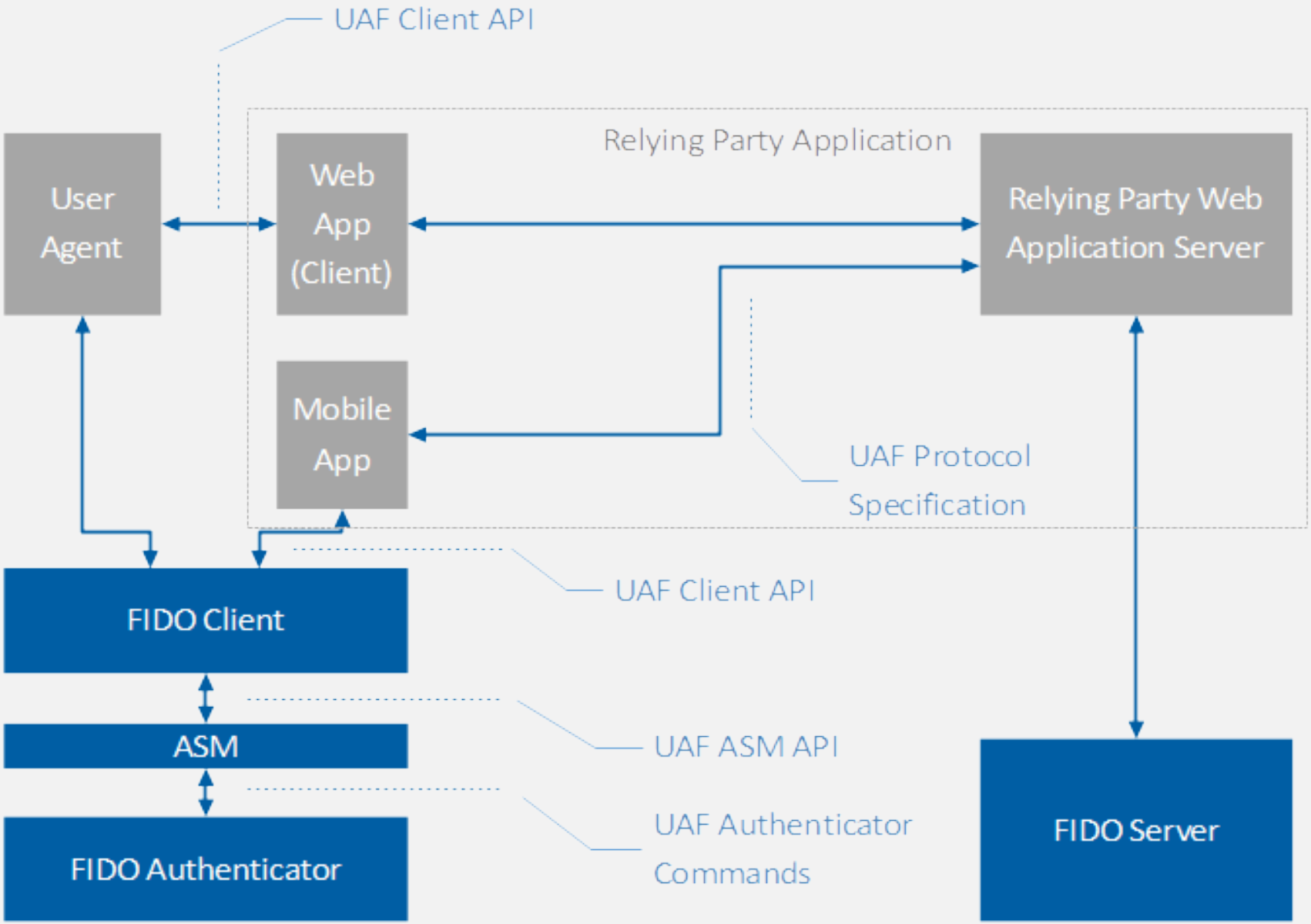
Transaction Confirmation



UAF Authenticator

- Bound Authenticator
- Roaming Authenticator
- Other metadata (verification method, key protection, secure display, …)


Injected at manufacturing, doesn't change
FIDO Authenticator
User Verification
Attestation Key
Secure Display
Authentication Key(s)
User
Optional
Generated at runtime (on Registration)


UAF Client API
Relying Party Application
User Agent
Web App (Client)
Relying Party Web Application Server
Mobile App
UAF Protocol Specification
UAF Client API
FIDO Client
ASM
UAF ASM API
UAF Authenticator Commands
FIDO Authenticator
FIDO Server

Thank you