fido™ alliance | simpler stronger authentication

The FIDO Alliance & Security:

A conversation with expert information security firm iSEC Partners, part of NCC Group

21 January 2015 | Webinar

Introduction to FIDO Alliance and FIDO Security

Who is FIDO Alliance?

fido™ alliance | simpler stronger authentication

A non-profit consortium of over 150 companies with a mission to change the nature of online authentication security, led by this diverse group of Board Members

DISCOVER® Bank of America. Google QUALCOMM®

lenovo. FOR THOSE WHO DO.™ PayPal™ ARM® oberthur TECHNOLOGIES THE M COMPANY

Synaptics® IdentityX® Nok Nok LABS SAMSUNG

NXP Microsoft CrucialTec MasterCard

yubico Trust the Net. VISA Alibaba Group RSA®

What problem are we solving?

Data breaches are common-place and costly

- $3.5M per data breach (Ponemon Institute)
- Target, Home Depot, Chase, …

Passwords are expensive for providers to support

- $420 annual productivity loss per employee (Widmeyer Survey)

Russian criminals steal 1.2 billion passwords

By James O'Toole and Jose Paglier

Russian hackers know y

NEW YORK (CNNMoney)

Posted August 27, 2014

Chase Bank Customer Attack

By Hal M. Bundrick

NEW
attac
camp
mass
Augu
atten
shelf
disre
multi-
the th

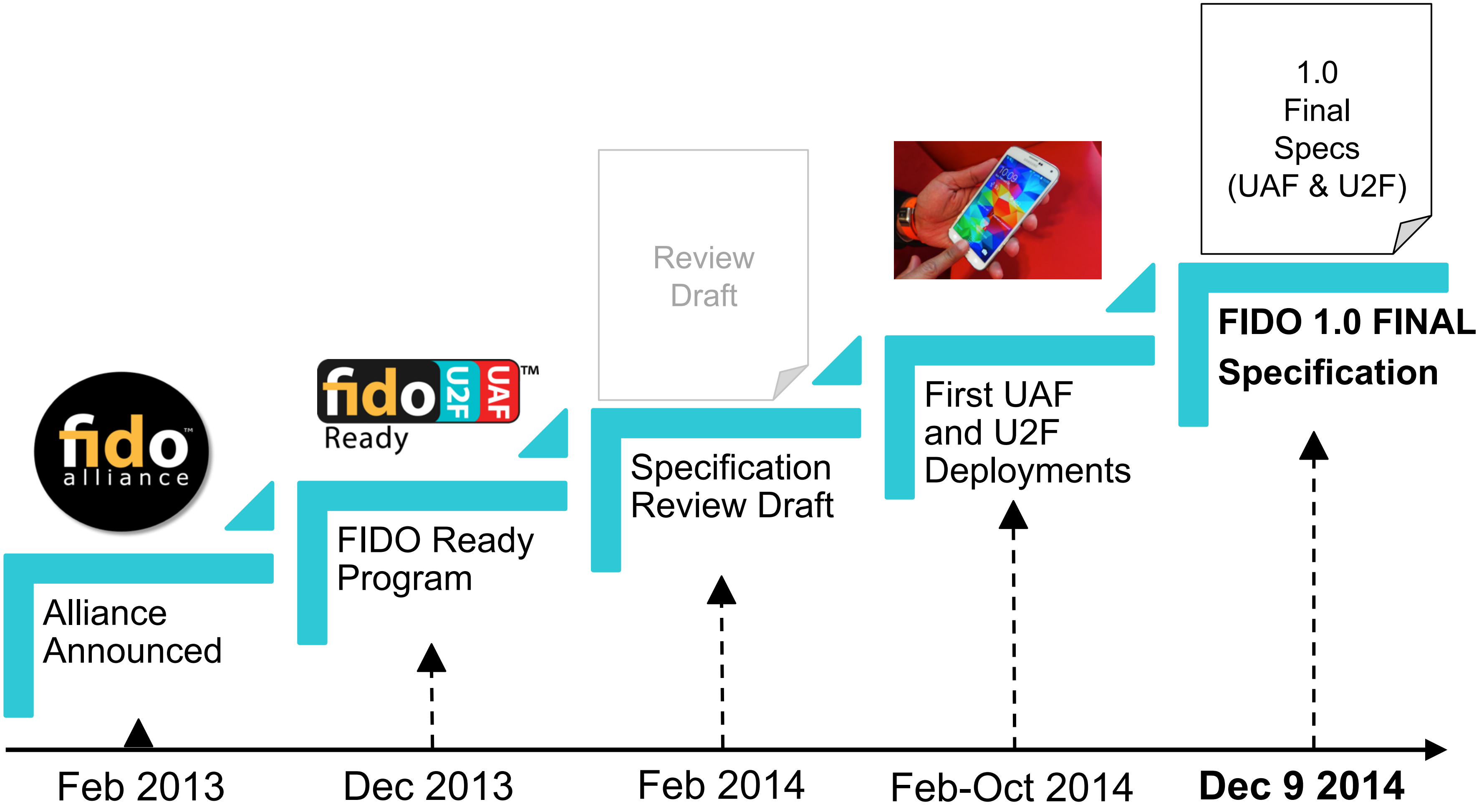
How the Eurograbber attack stole 36 million euros

Posted on 05.12.2012

Check Point has revealed how a sophisticated malware attack was used to steal an estimated €36 million from over 30,000 customers of over 30 banks in Italy, Spain, Germany and Holland over summer this year.

The theft used malware to target the PCs and mobile devices of banking customers. The attack also took advantage of SMS messages used by banks as part of customers' secure login and authentication process.

What have we done so far?



Alliance Announced
Feb 2013

FIDO Ready Program
Dec 2013

Specification Review Draft
Feb 2014

First UAF and U2F Deployments
Feb-Oct 2014

1.0
Final
Specs
(UAF & U2F)

FIDO 1.0 FINAL Specification
Dec 9 2014

FIDO design principles?

- No 3rd Party in the Protocol
- No Secrets on the Server side
- Biometric data (if used) never leaves device
- No link-ability between Services
- No link-ability between Accounts

Who benefits from FIDO?

fido alliance simpler stronger authentication

Online Service Providers

- Exceptional user experience
- Stronger security
- Cost containment

Enterprises

- Reduced cost and complexity
- Strong asset protection
- Effective BYOD support

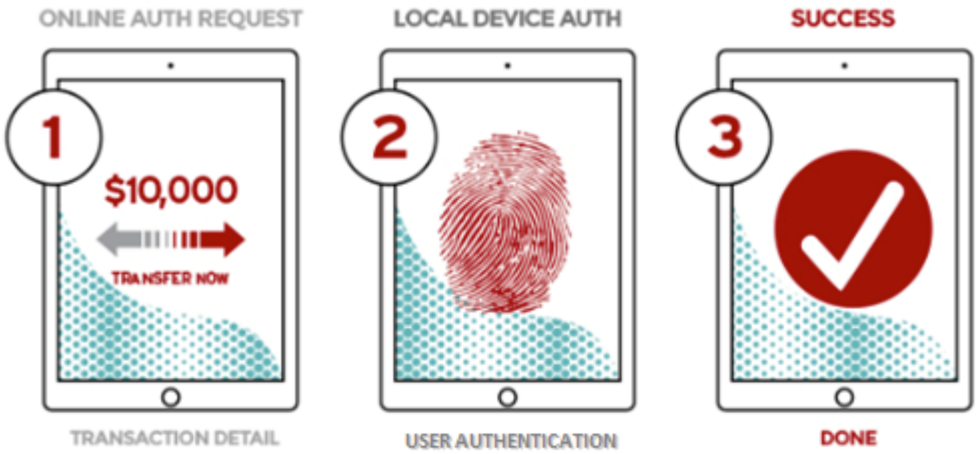
Consumers

- Ease of use
- Interoperability (one device for many services)
- Security and Privacy

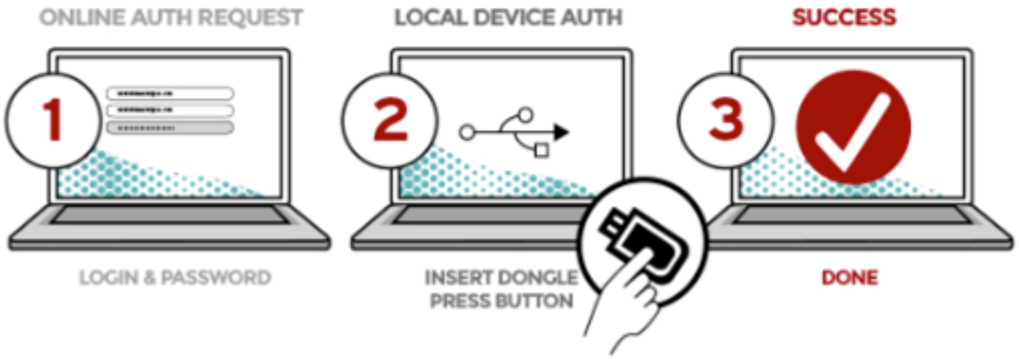
How does FIDO work?

simpler
stronger
authentication

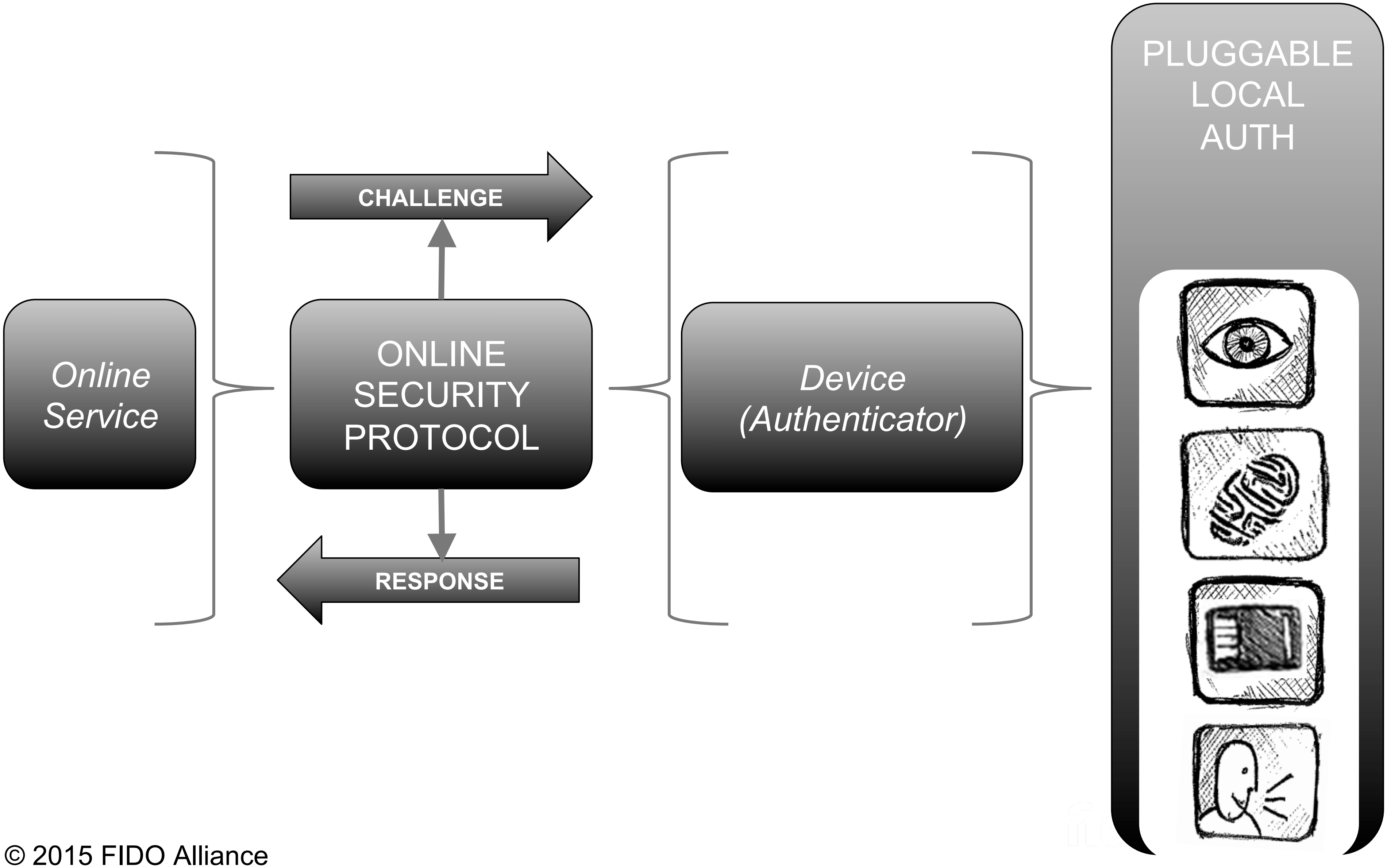
PASSWORDLESS EXPERIENCE (UAF standards)



SECOND FACTOR EXPERIENCE (U2F standards)



FIDO Standardization



Online Service

CHALLENGE

ONLINE SECURITY PROTOCOL

RESPONSE

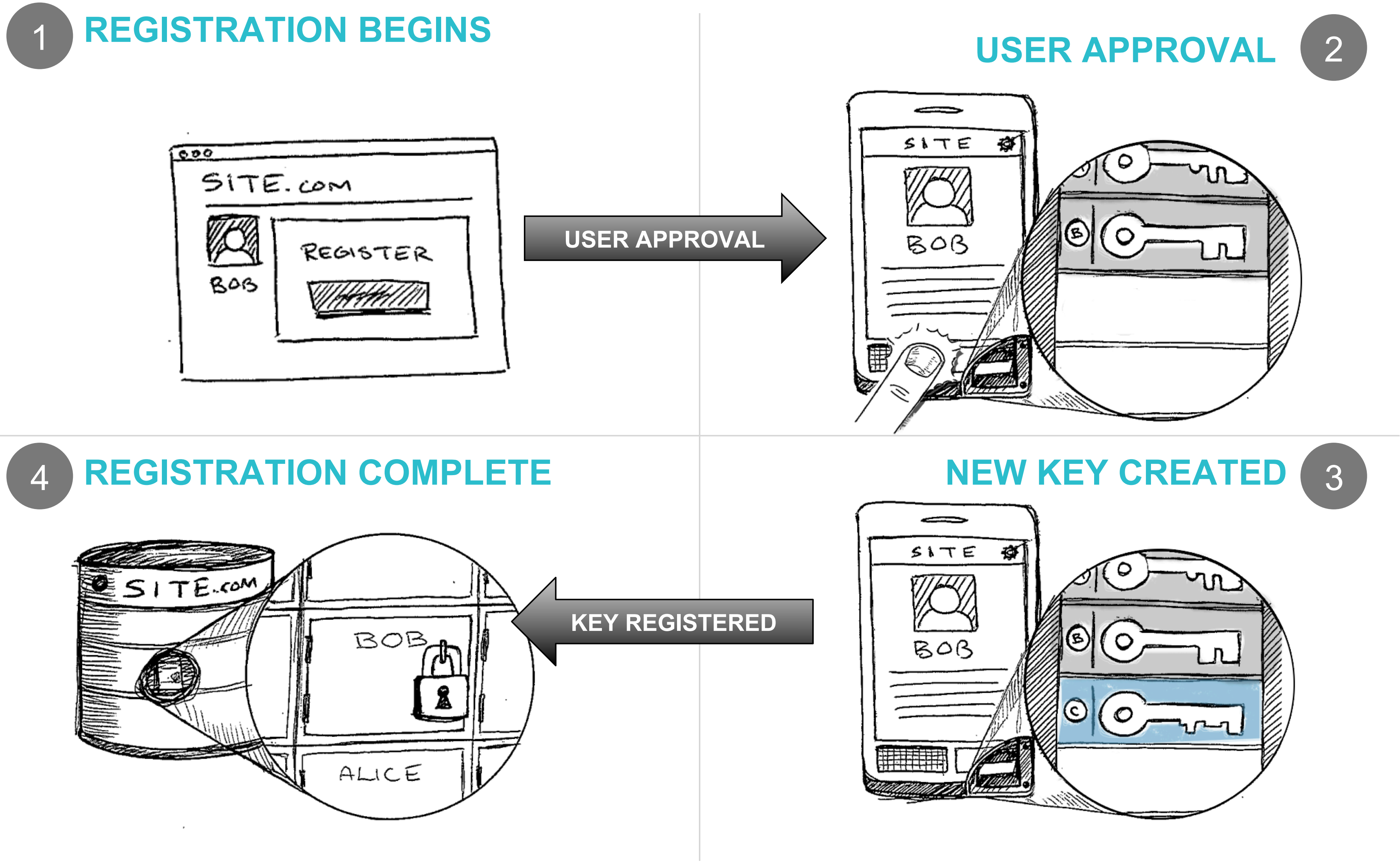
Device (Authenticator)

PLUGGABLE LOCAL AUTH

FIDO Registration & Login

taking a closer look

FIDO Registration Overview



1 REGISTRATION BEGINS

USER APPROVAL

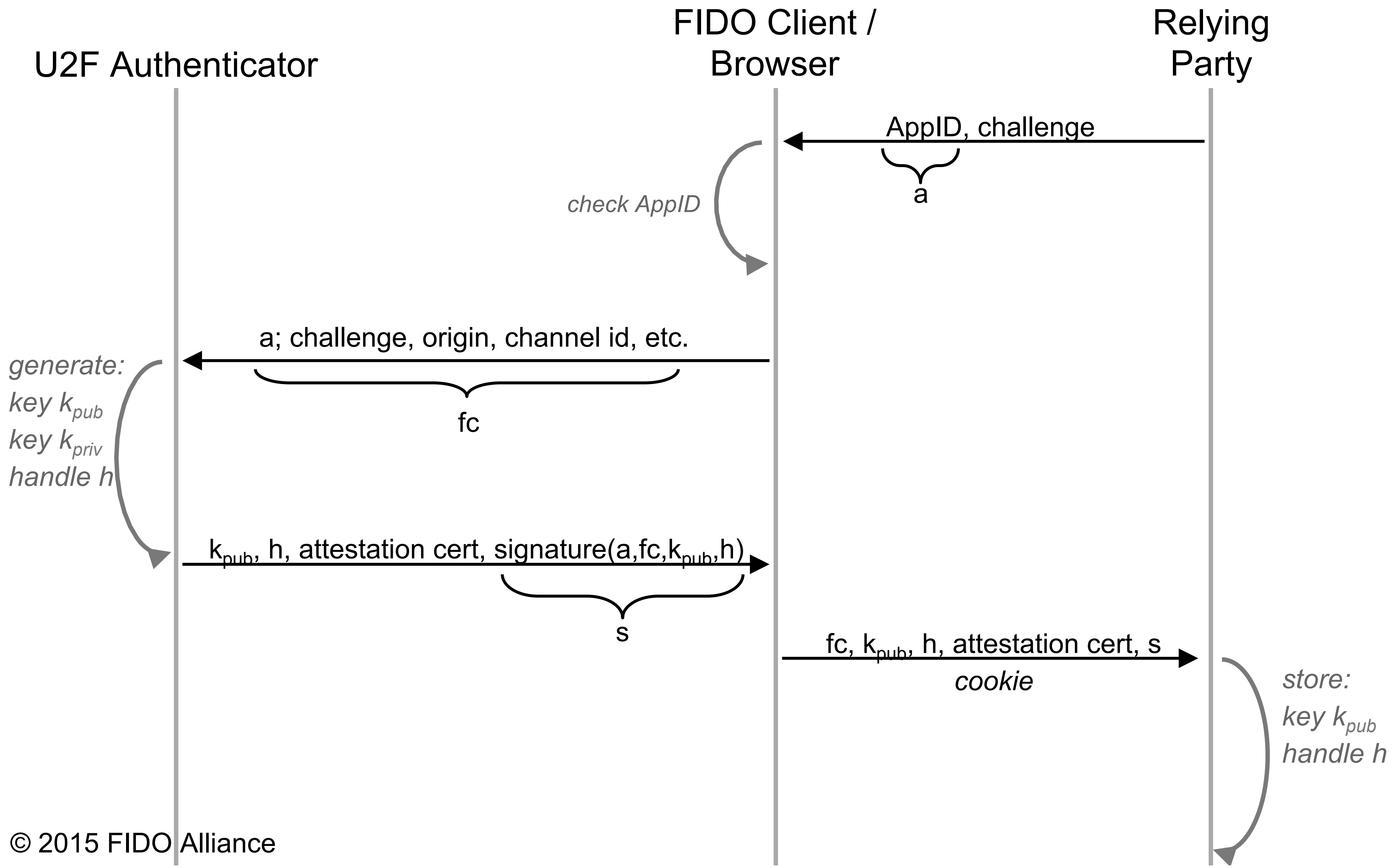
USER APPROVAL 2

NEW KEY CREATED 3

KEY REGISTERED

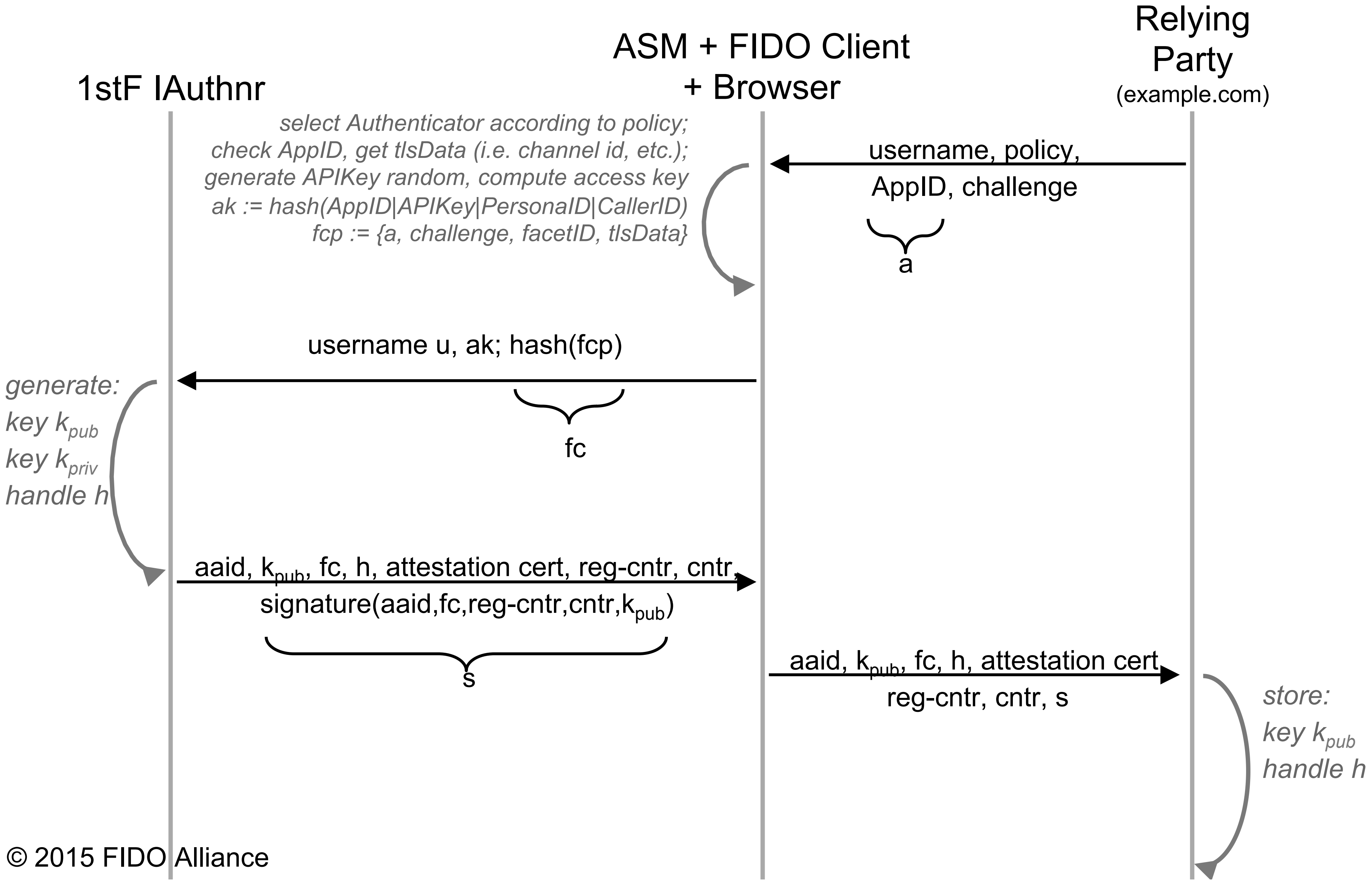
4 REGISTRATION COMPLETE

U2F Registration Flow



UAF Registration Flow

fido alliance
simpler
stronger
authentication



1stF IAuthnr

ASM + FIDO Client + Browser

Relying Party (example.com)

username, policy, AppID, challenge

a

select Authenticator according to policy;
check AppID, get tlsData (i.e. channel id, etc.);
generate APIKey random, compute access key
ak := hash(AppID|APIKey|PersonalID|CallerID)
fcp := {a, challenge, facetID, tlsData}

username u, ak; hash(fcp)

fc

generate:
key k_{pub}
key k_{priv}
handle h

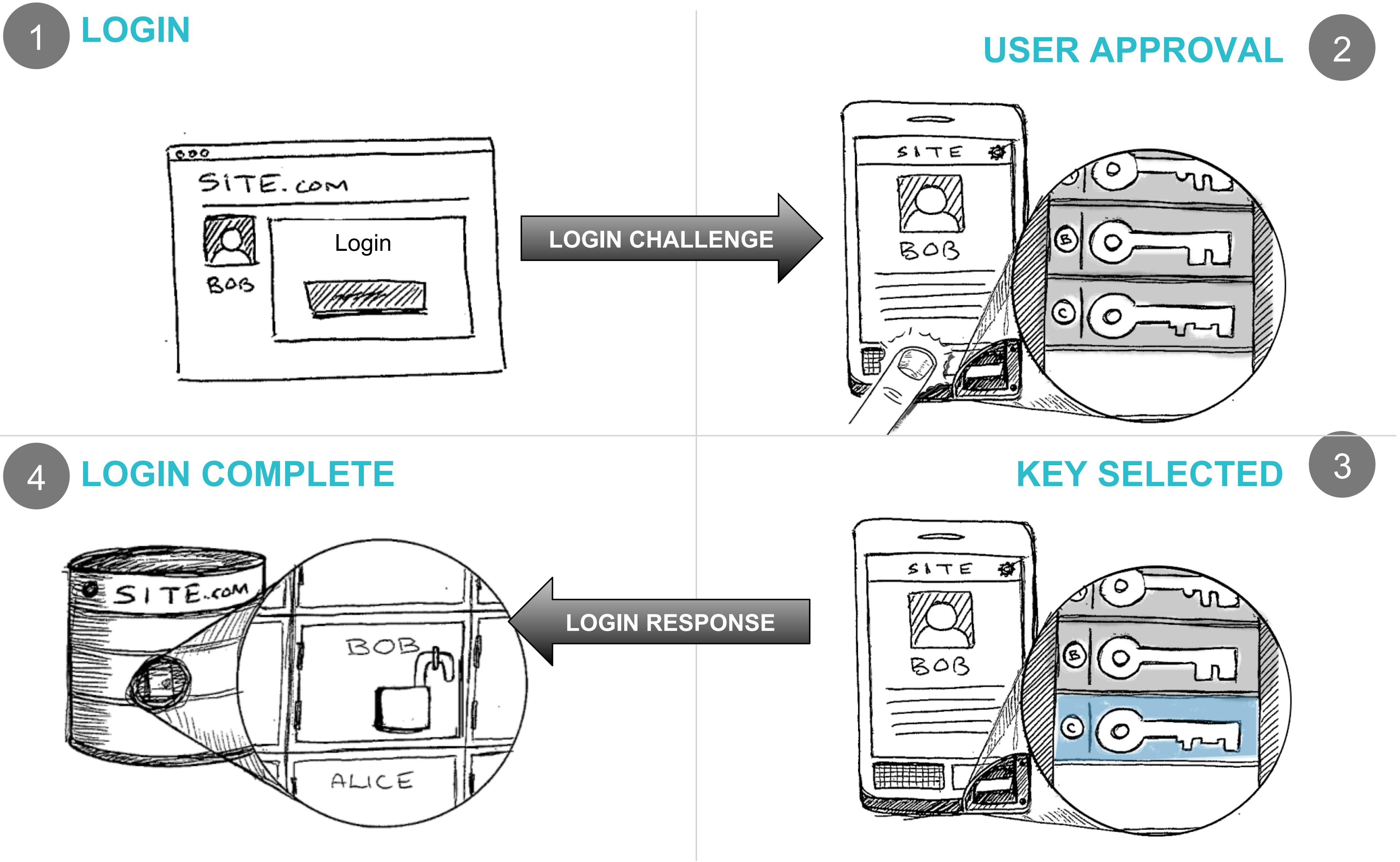
aaid, k_{pub}, fc, h, attestation cert, reg-cntr, cntr, signature(aaid,fc,reg-cntr,cntr,k_{pub})

s

aaid, k_{pub}, fc, h, attestation cert reg-cntr, cntr, s

store:
key k_{pub}
handle h

FIDO Login Overview



1 LOGIN

LOGIN CHALLENGE

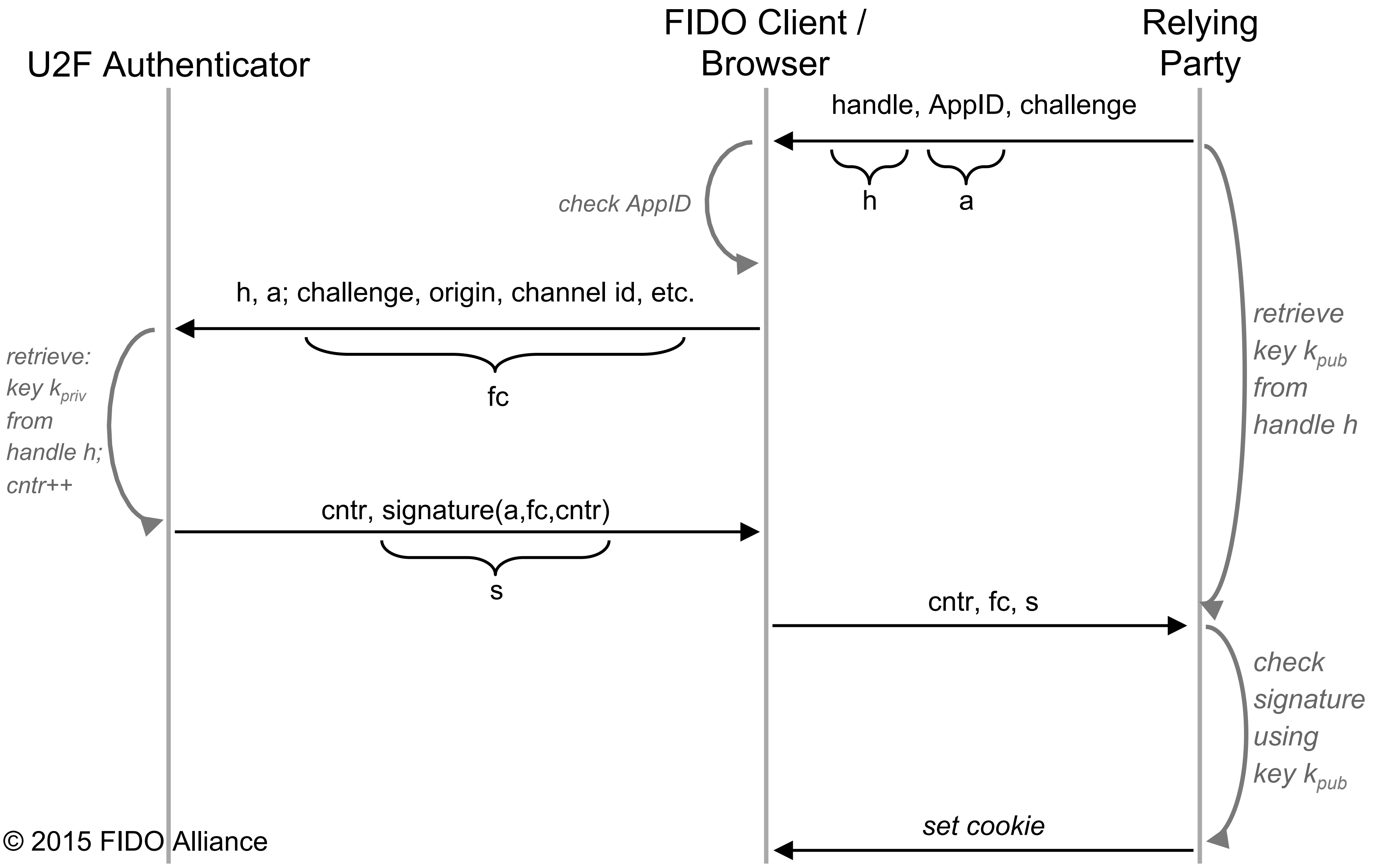
USER APPROVAL 2

KEY SELECTED 3

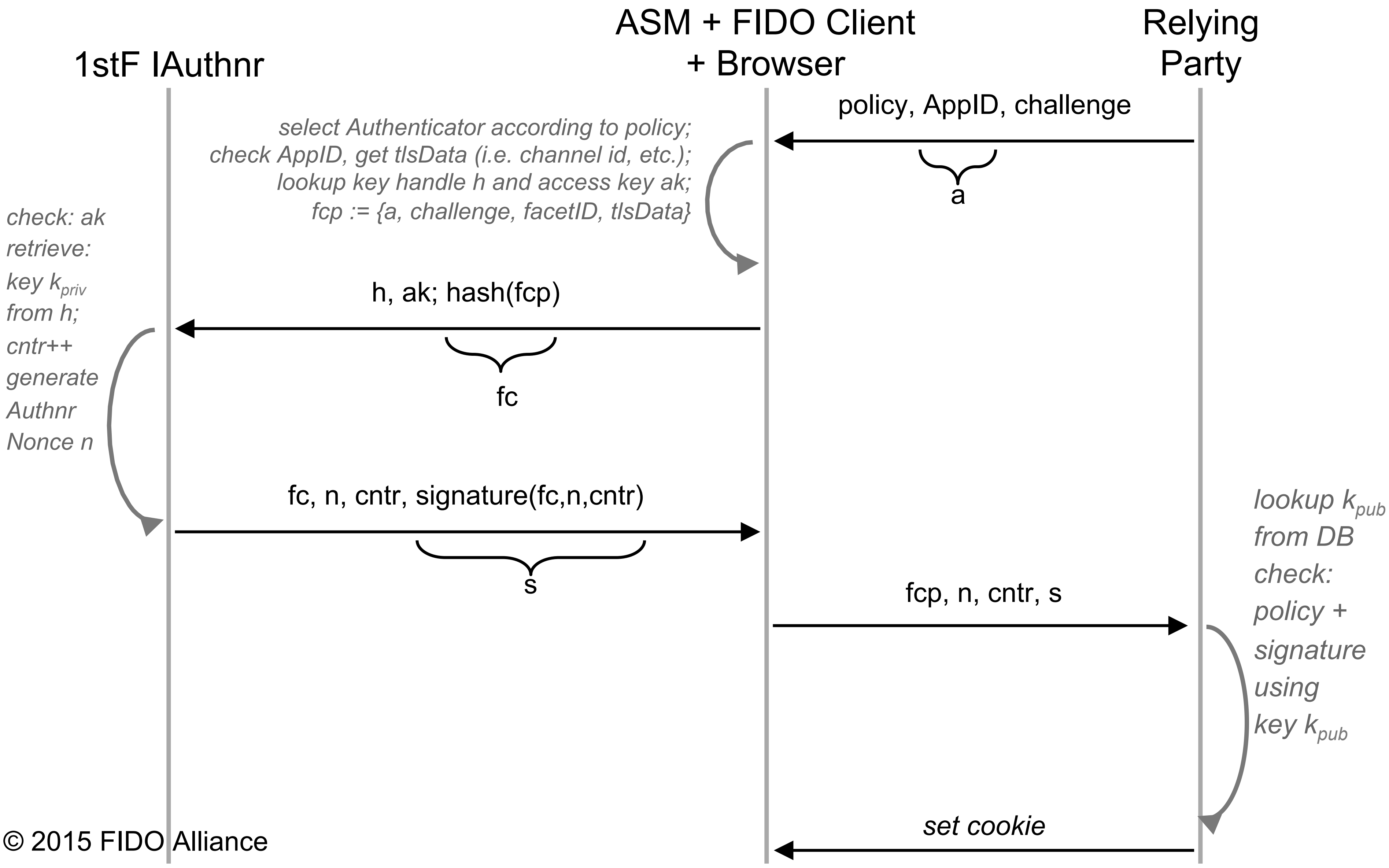
LOGIN RESPONSE

4 LOGIN COMPLETE

U2F Authentication Flow


U2F Authenticator
FIDO Client / Browser
Relying Party
handle, AppID, challenge
h
a
check AppID
h, a; challenge, origin, channel id, etc.
fc
retrieve: key k_{priv} from handle h; cntr++
cntr, signature(a,fc,cntr)
s
retrieve key k_{pub} from handle h
cntr, fc, s
check signature using key k_{pub}
set cookie

UAF Authentication Flow



1stF IAuthnr

ASM + FIDO Client + Browser

Relying Party

policy, AppID, challenge

a

select Authenticator according to policy;
check AppID, get tlsData (i.e. channel id, etc.);
lookup key handle h and access key ak;
fcp := {a, challenge, facetID, tlsData}

h, ak; hash(fcp)

fc

check: ak
retrieve:
key k_{priv}
from h;
cntr++
generate
Authnr
Nonce n

fc, n, cntr, signature(fc,n,cntr)

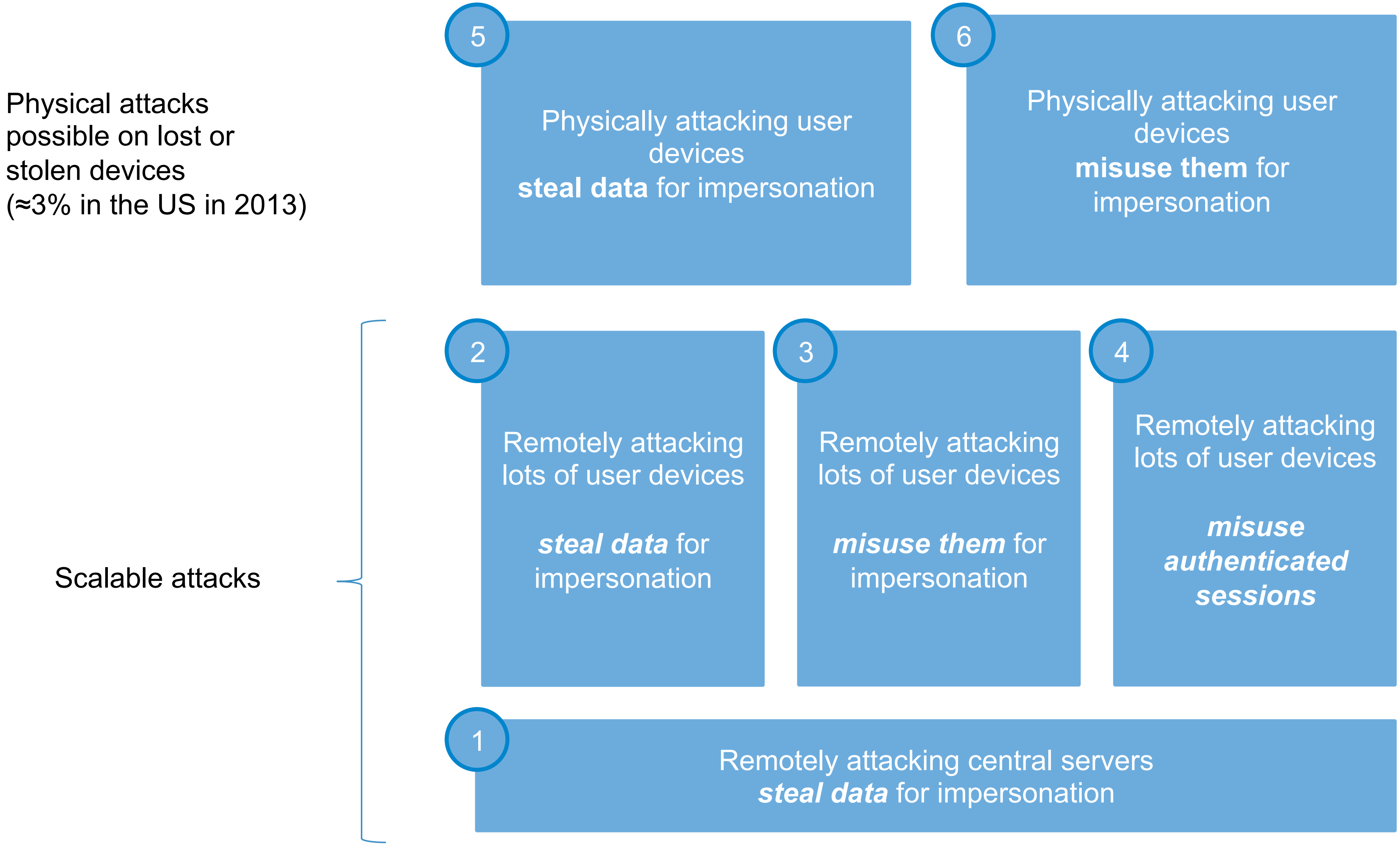
s

fcp, n, cntr, s

lookup k_{pub}
from DB
check:
policy +
signature
using
key k_{pub}

set cookie

Security Considerations



Physical attacks possible on lost or stolen devices (≈3% in the US in 2013)

Scalable attacks

5 Physically attacking user devices **steal data** for impersonation

6 Physically attacking user devices **misuse them** for impersonation

2 Remotely attacking lots of user devices

steal data for impersonation

3 Remotely attacking lots of user devices

misuse them for impersonation

4 Remotely attacking lots of user devices

misuse authenticated sessions

1 Remotely attacking central servers ***steal data*** for impersonation

Security Review & iSEC Partners

The FIDO Alliance and Security

A conversation with expert information security firm, iSEC Partners, part of NCC Group

Tom Ritter, Practice Director, Cryptography Services
iSEC Partners, Part of NCC Group

About NCC Group

iSECpartners
part of nccgroup

Who we are

- Total information assurance solution – unique offering in the marketplace
- £100m business – publically listed on LSE
- 1,000+ Employees worldwide
- Client base of over 15,000 customers worldwide and growing rapidly
- Making the internet a safer place

What we do

- Escrow & Verification
- Security Consulting
- Website Performance
- Software Testing
- Domain Services

Cryptography Services

- Started in 2014, and spans iSEC Partners, Matasano Security, Intrepidus Group and NCC Group
- With this wealth of combined experience building, breaking, fixing and deploying cryptographic solutions, NCC Group has distinguished itself as a leading provider of Cryptographic Security Assessments including:
  - Testing implementations and modifications of SSL/TLS
  - Cryptographic algorithm and protocol implementations
  - Custom protocol design and review

Why We're Doing This

- Very uncommon for us to do a webinar like this.
- We, like FIDO, believe that the Web needs stronger authentication
- We don't like walled gardens: we like open standards and specifications
- We've worked with FIDO reviewing the specs for some time.

Scope of FIDO Review

- UAF and U2F as of November Drafts
- Protocols and APIs of UAF and U2F, for
  - Choice of crypto primitives, invalid state transitions, cross protocol attacks, strong authentication, replay, DoS and similar concerns
- Document adequately
  - Guided implementers away from security flaws
  - Documented risks and their mitigations

Findings

- Didn’t identify protocol weaknesses
- Protocol & the Metadata regarding devices together give a strong understanding of device behavior
- Some nit-picky concerns with documentation
- Enumerated a few additional attack scenarios

Disclaimer: We, like you, are not perfect.

iSECpartners
part of nccgroup

Europe

Manchester - Head Office
Cheltenham
Edinburgh
Leatherhead
London
Munich
Amsterdam
Zurich

North America

Austin
Atlanta
Chicago
New York
San Francisco
Seattle
Sunnyvale

Australia

Sydney

fido™ alliance | simpler stronger authentication

Q&A

21 January 2015 | Webinar