Asynchronous Remote Key Generation: An Analysis of Yubico's Proposal for W3C WebAuthn

Nick Frymann
n.frymann@surrey.ac.uk
Surrey Centre for Cyber Security
University of Surrey
Guildford, UK

Emil Lundberg
emil@yubico.com
Yubico AB
Stockholm, Sweden

Daniel Gardham
d.gardham@surrey.ac.uk
Surrey Centre for Cyber Security
University of Surrey
Guildford, UK

Mark Manulis
mark@manulis.eu
Surrey Centre for Cyber Security
University of Surrey
Guildford, UK

Franziskus Kiefer
mail@franziskuskiefer.de
Wire Swiss GmbH
Berlin, Germany

Dain Nilsson
dain@yubico.com
Yubico AB
Stockholm, Sweden

Asynchronous Remote Key Generation (ARKG)

- New cryptographic primitive
- Delegated, asynchronous public key generation

- Application: user friendly backup keys for W3C WebAuthn

yubico

Agenda

- Background issue
- Yubico's proposal
- The ARKG scheme
- WebAuthn implementation

WebAuthn

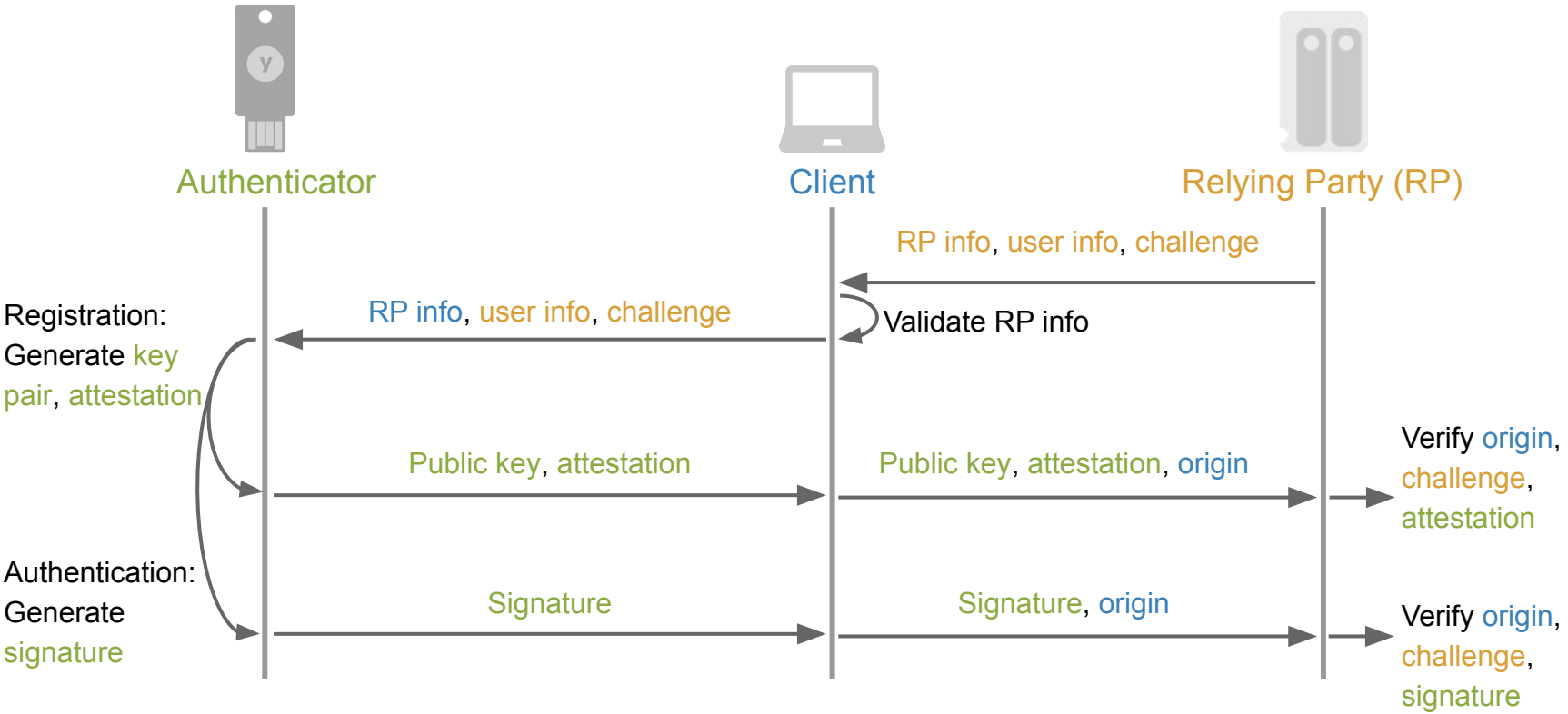
Web Authentication: An API for accessing Public Key Credentials

https://www.w3.org/TR/webauthn-2/

- **W3C standard, released 2019**
- **Phishing-resistant public key authentication**
- **JavaScript API**
- **Various hardware backends**
  - Dedicated hardware tokens (“Security keys”)
  - Mobile phones
  - Laptop TPMs
  - etc.

yubico

WebAuthn summary

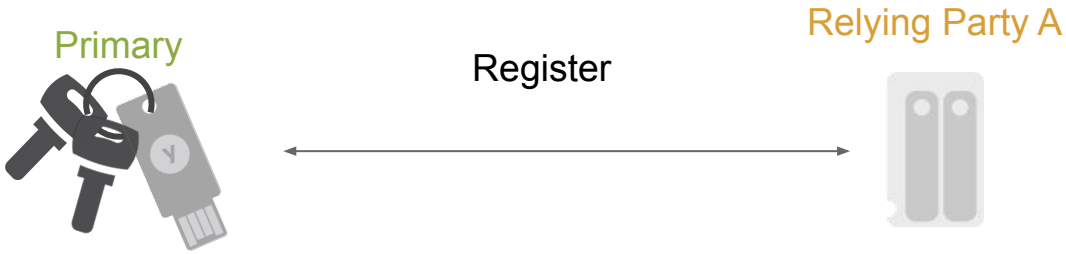


WebAuthn: Key properties

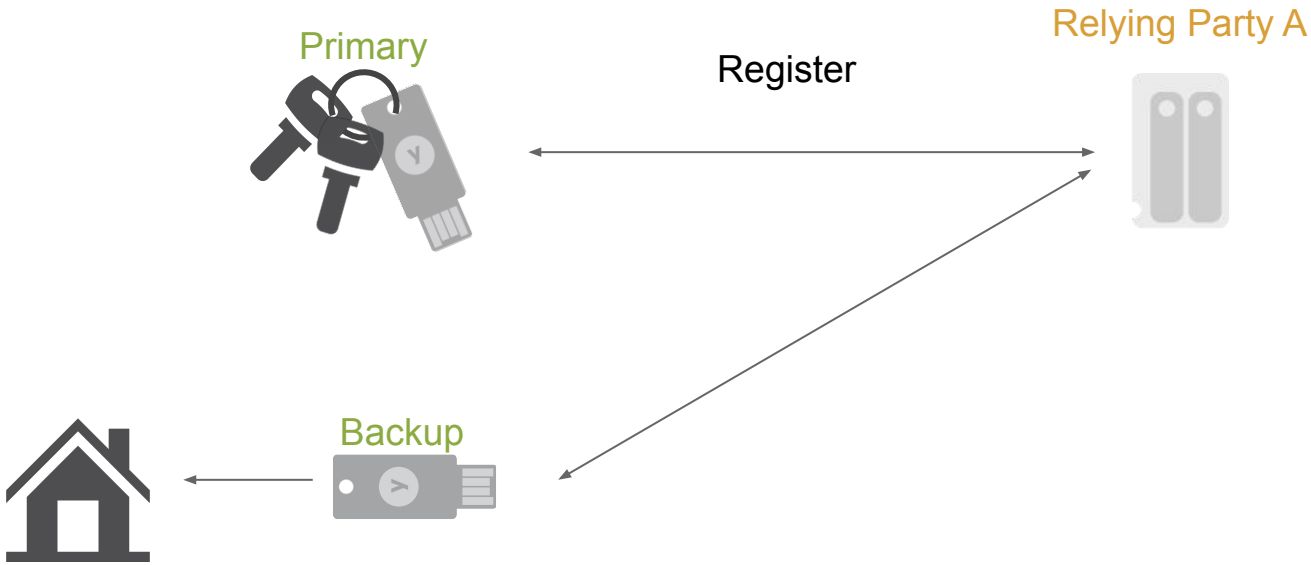
- **Unlinkable public keys**
  - Cannot determine whether two public keys were generated by the same authenticator

- **Authenticator attestation**
  - Authenticators can prove make and model
  - RP can trust certifications, security guarantees
    - Passwordless multi-factor authentication

WebAuthn backup keys

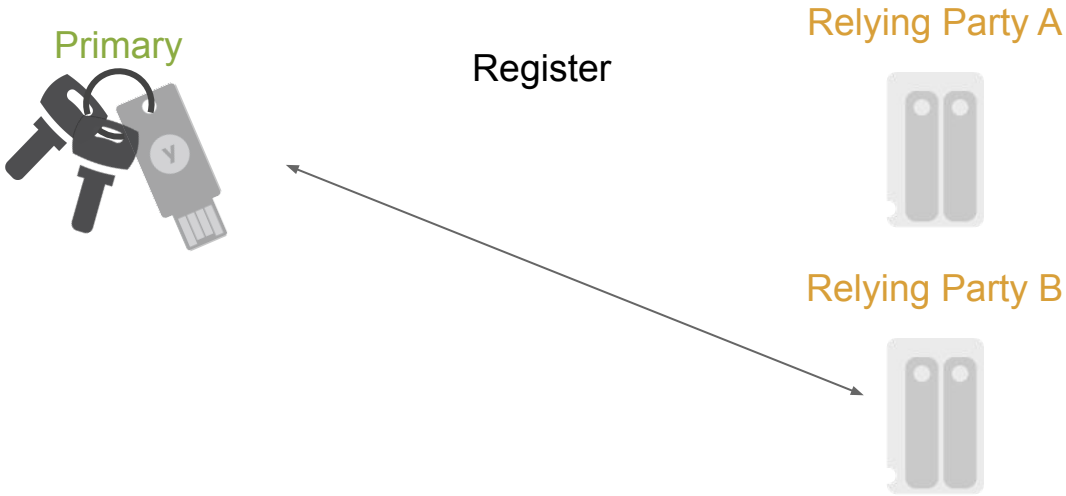


WebAuthn backup keys



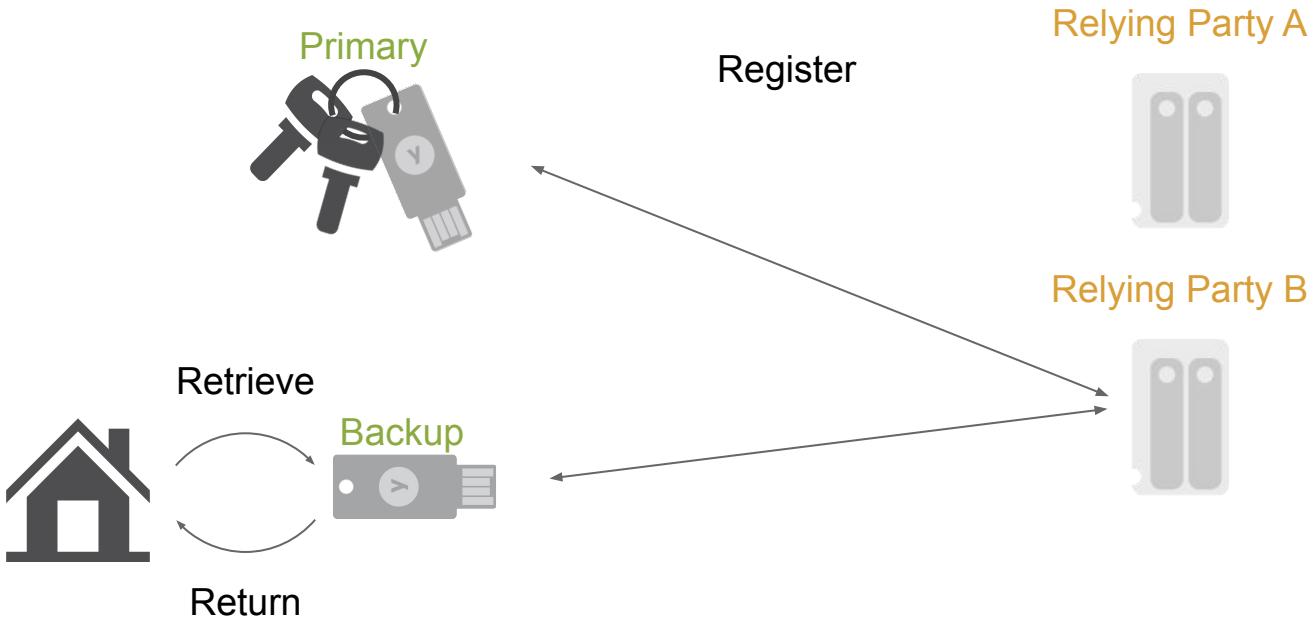
yubico

WebAuthn backup keys

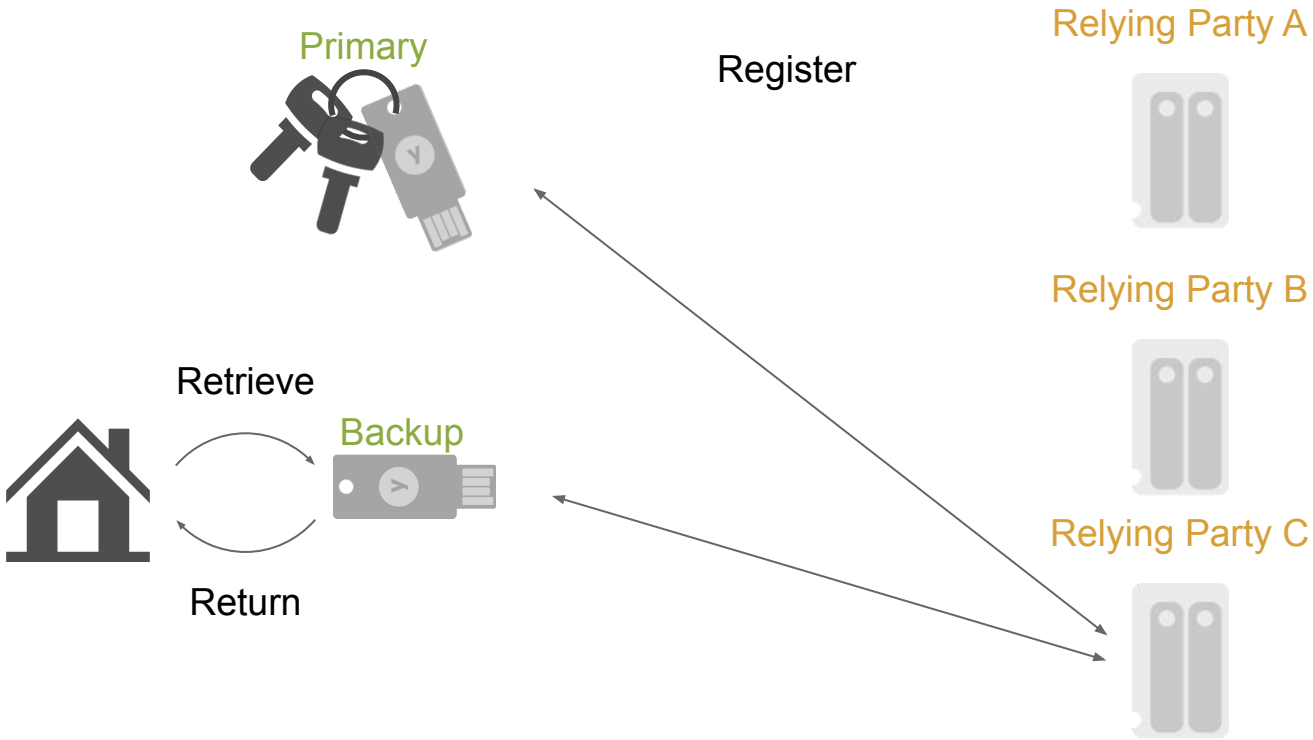


yubico

WebAuthn backup keys



WebAuthn backup keys



WebAuthn backup keys

Problems:

- Inconvenient
- Backup stashed away: risk forgetting to register it
- Backup easily accessible: risk losing it

WebAuthn backup keys

Problems:

- Inconvenient
- Backup stashed away: risk forgetting to register it
- Backup easily accessible: risk losing it

Design constraints:

- Unlinkable keys
- Maintain attestation integrity
- Vendor interoperability
- Ideally no 3rd party dependency

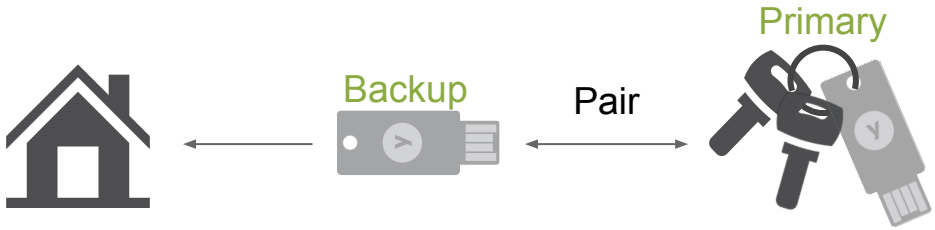
Other proposals

- **Shared private keys**
  - Problematic for attestation
  - Breaks signature counters
  - Possible(?) with mutual attestation, but likely not interoperable

- **Preemptively generated key pairs**
  - Too large for small hardware tokens
  - Alt. requires remote storage

- **Static backup public key**
  - Breaks unlinkability

Yubico’s proposal

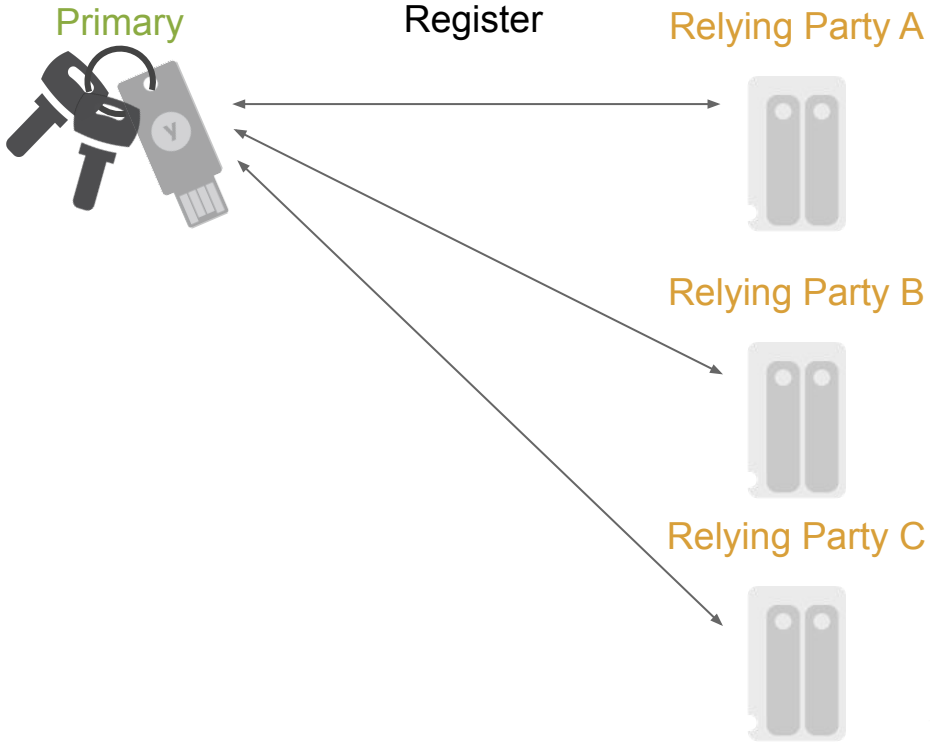


Yubico’s proposal

Primary

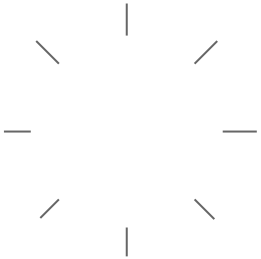
Backup

Yubico’s proposal



Yubico’s proposal

Backup

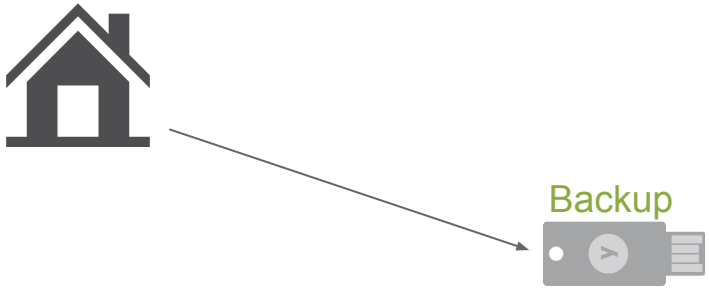


Relying Party A

Relying Party B

Relying Party C

Yubico’s proposal

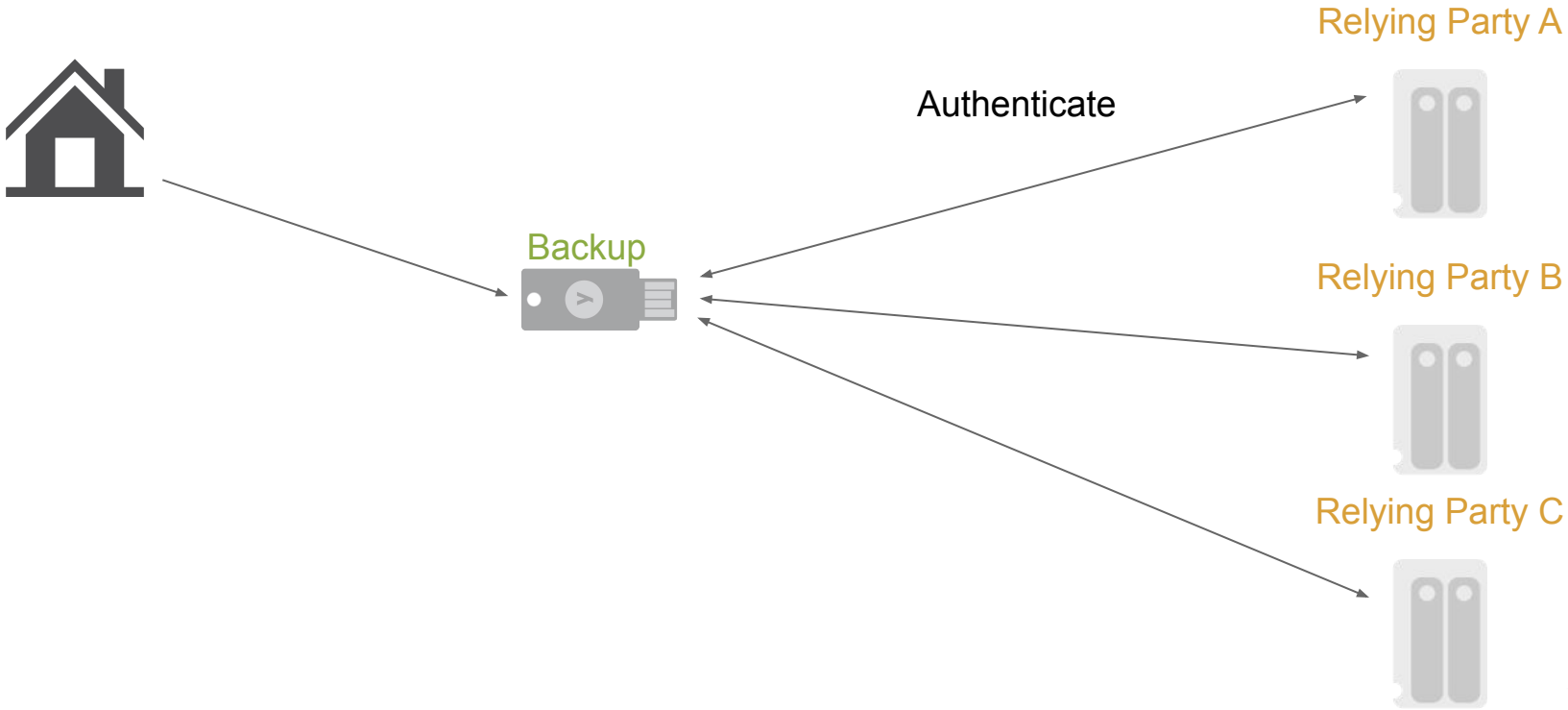


Relying Party A

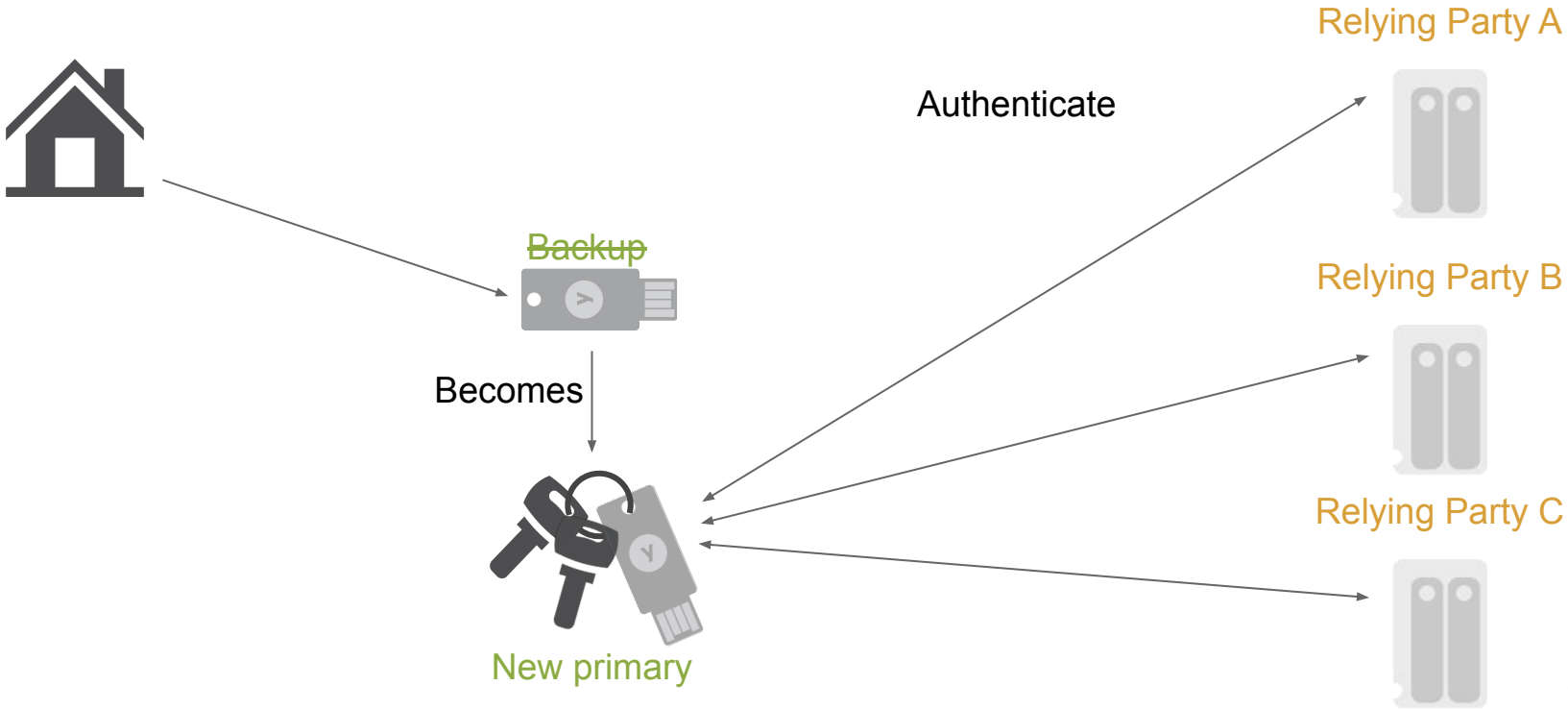
Relying Party B

Relying Party C

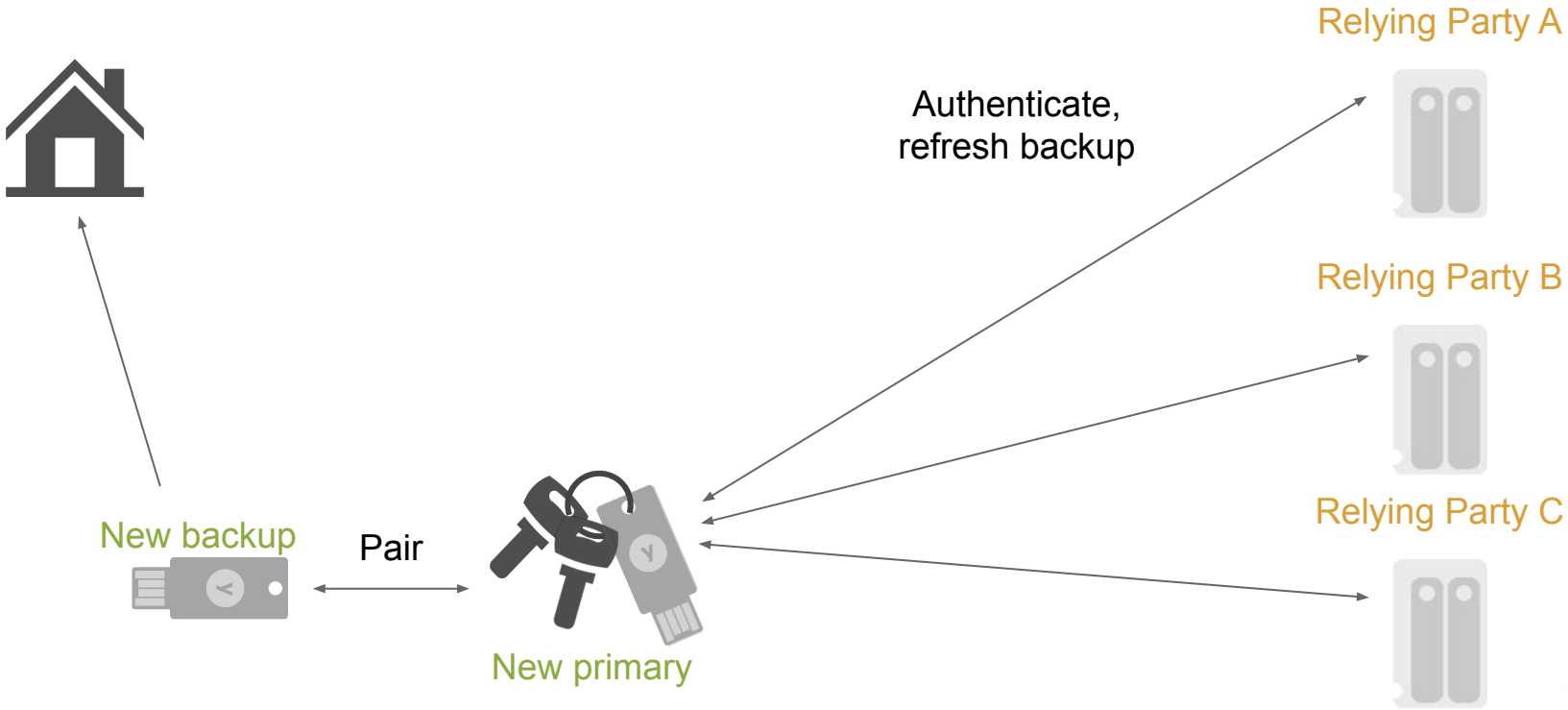
Yubico’s proposal



Yubico's proposal



Yubico’s proposal



Security analysis: ARKG

Asynchronous Remote Key Generation

ARKG

***G*, *n*:** Group generator, order

Participants:

- **PA(*S*): Primary authenticator**
  - *S*: Public key seed from backup authenticator
- **BA(*S*, *s*): Backup authenticator**
  - *S*, *s*: Backup seed key pair
- **RP(rpId, *P*, cred): Relying Party**
  - rpId: Relying Party ID
  - *P*: User's backup public key
  - cred: User's backup key handle

Phases:

1. **Setup**
   - Pair authenticators
   - Once per pair
2. **Registration**
   - PA generates public keys for BA
   - Continues until PA is lost
3. **Recovery**
   - BA derives private keys

ARKG: Setup

PA(S = ?)

BA(S, s)

1. S, s ←$ KGen

2. S

3. Store S

S, s: Backup seed key pair

ARKG: Registration

PA(S)

RP(rpId, P = ?, cred = ?)

1. rpId

2. E, e ←$ KGen
3. k_{cred} ← $KDF_1(S^e)$
4. k_{mac} ← $KDF_2(S^e)$
5. P ← (k_{cred} × G) + S
6. cred ← E || MAC(k_{mac}, E || rpId)

7. P, cred

8. Store P, cred

ARKG: Recovery

BA(S, s, G, n)

RP(rpId, P, cred)

1. Generate challenge

2. rpId, cred, challenge ⟵

3. E ⟵ cred
4. k_{cred} ⟵ $KDF_1(E^s)$
5. k_{mac} ⟵ $KDF_2(E^s)$
6. Verify cred = E || $MAC(k_{mac}, E \,||\, rpId)$
7. p ⟵ $k_{cred} + s \bmod n$
8. Sign challenge with p

9. Signature ⟶

10. Verify signature with P

Security analysis

Security properties:

- **PK-unlinkability**
  - Given public keys pk_1, pk_2, attacker cannot determine whether pk_1 and pk_2 were derived from the same seed key
- **SK-security**
  - Given derived public key, attacker cannot find corresponding secret key

- Satisfiability proven using PRF-ODH, by Brendel et al., and discrete logarithm assumptions
- Composability with arbitrary asymmetric protocols proven using composability framework by Brzuska et al.
- Opens for new instantiations, possibly beyond elliptic curves

WebAuthn implementation

- **Implementable as WebAuthn extension**
- **RP implementation required**
  - Library support possible

- **Attestation:**
  - Deferred until recovery phase
  - Preliminary (unsigned) attestation in registration phase

- **Performance:**
  - Expected 100% - 150% hardware runtime increase
  - Currently ~100 ms without extension
  - Most ceremonies unaffected

Summary

- **ARKG: new cryptographic primitive**
- **Enables WebAuthn backup key solution**
- **Security proved using PRF-ODH and DL assumptions**
- **Composable with arbitrary asymmetric protocols**

- **More details**
  - ARKG analysis: https://eprint.iacr.org/2020/1004
  - Yubico blog: https://www.yubico.com/blog/yubico-proposes-webauthn-protocol-extension-to-simplify-backup-security-keys/
  - Extension proposal: https://github.com/Yubico/webauthn-recovery-extension/
  - ACM CCS presentation: https://www.youtube.com/watch?v=urJ2DhpLAEk

Asynchronous Remote Key Generation: An Analysis of Yubico's Proposal for W3C WebAuthn

Nick Frymann
n.frymann@surrey.ac.uk
Surrey Centre for Cyber Security
University of Surrey
Guildford, UK

Emil Lundberg
emil@yubico.com
Yubico AB
Stockholm, Sweden

Daniel Gardham
d.gardham@surrey.ac.uk
Surrey Centre for Cyber Security
University of Surrey
Guildford, UK

Mark Manulis
mark@manulis.eu
Surrey Centre for Cyber Security
University of Surrey
Guildford, UK

Franziskus Kiefer
mail@franziskuskiefer.de
Wire Swiss GmbH
Berlin, Germany

Dain Nilsson
dain@yubico.com
Yubico AB
Stockholm, Sweden