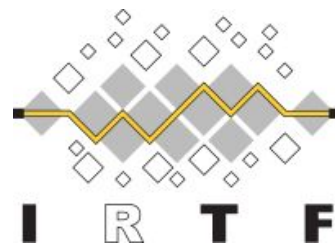


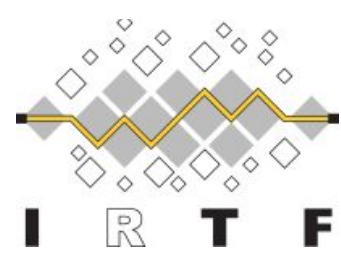
draft-bradleylundberg-cfrg-arkg

The Asynchronous Remote Key Generation (ARKG) algorithm

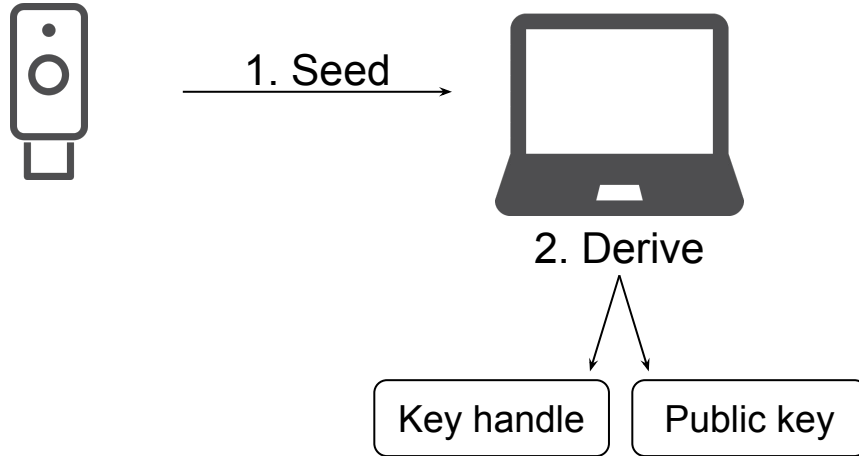
Emil Lundberg
IETF 125, Shenzhen
March 17, 2026



Summary



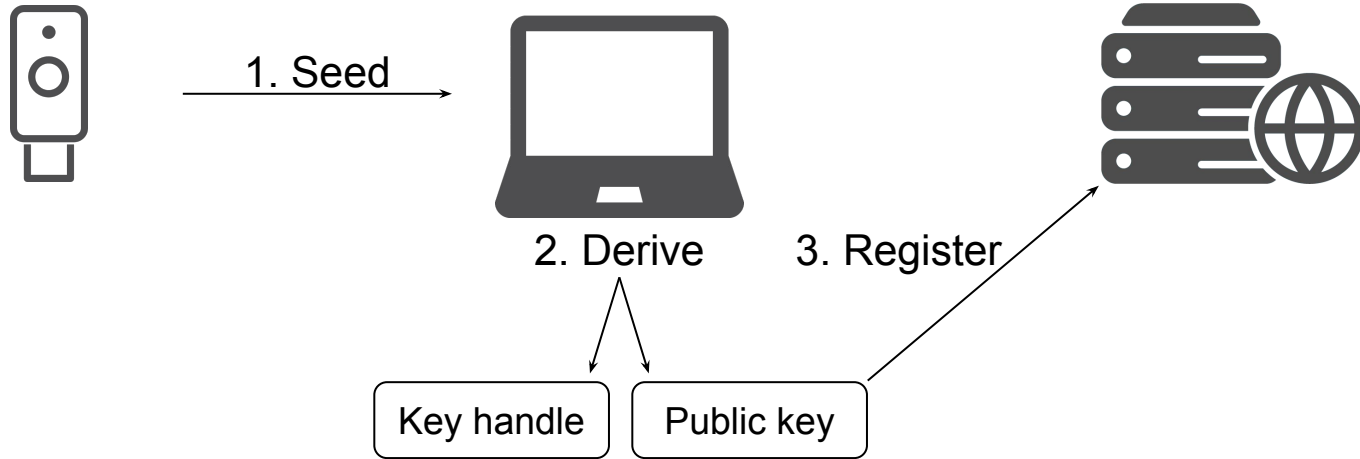
Delegate public key creation without private key access



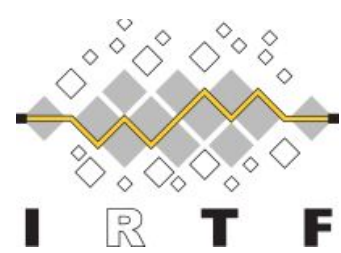
Summary



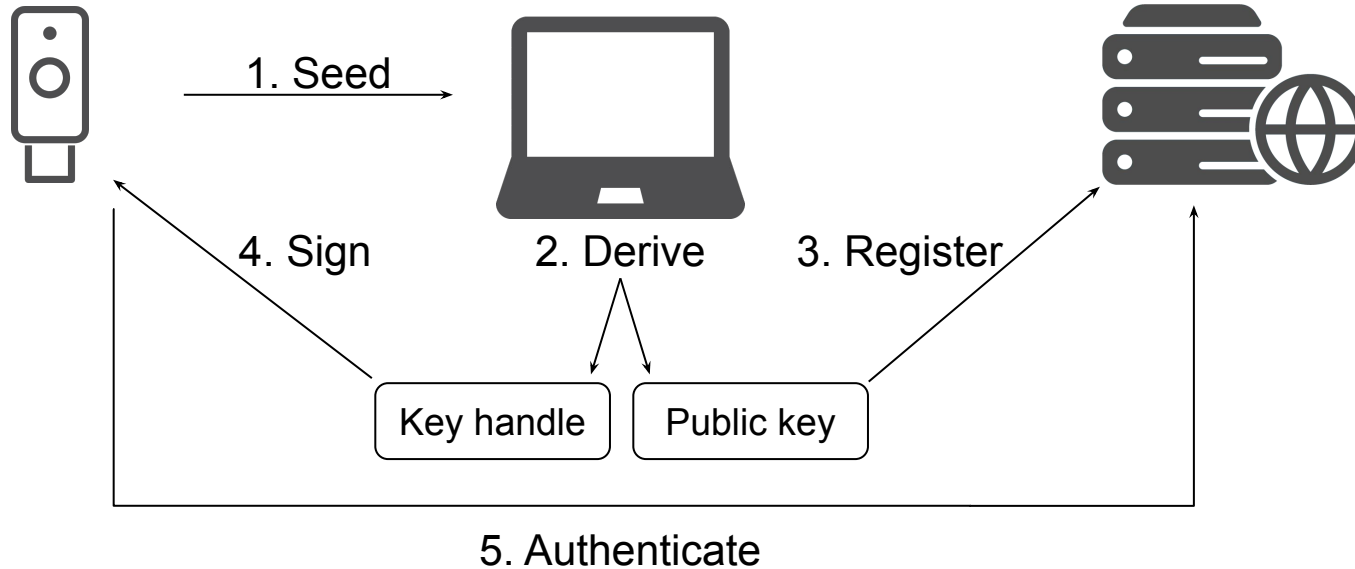
Delegate public key creation without private key access



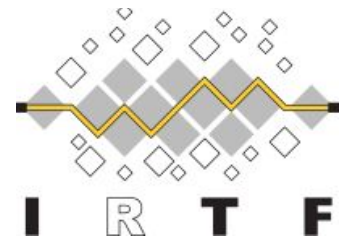
Summary



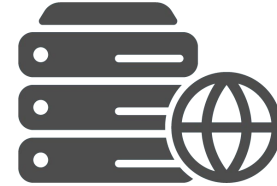
Delegate public key creation without private key access



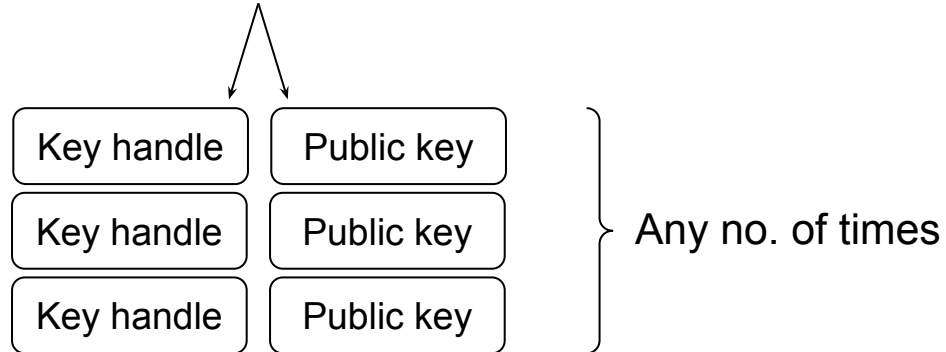
Summary



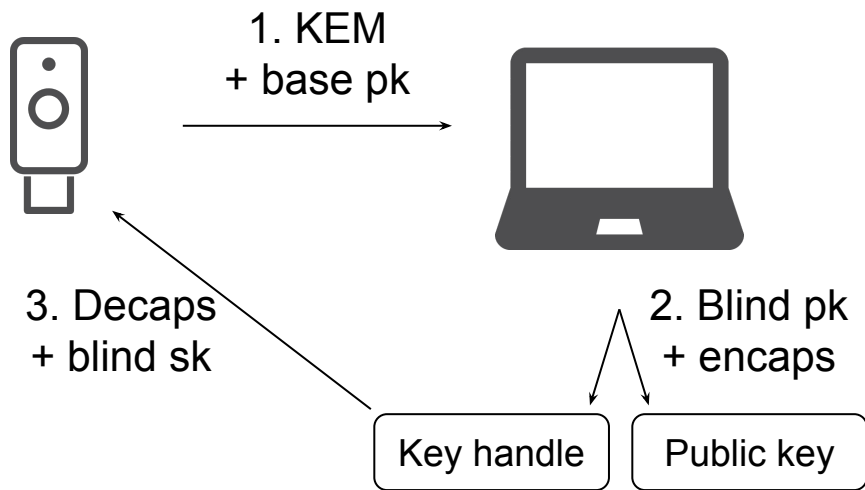
Delegate public key creation without private key access



2. Derive



How it works: KEM + key blinding



Background



- 2012 Wuille “BIP 32 Hierarchical Deterministic Wallets”
 - <https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki>
- 2019 Lundberg and Nilsson “WebAuthn recovery extension: Asynchronous delegated key generation without shared secrets”
 - <https://github.com/Yubico/webauthn-recovery-extension>
- 2020 Frymann et al. “Asynchronous Remote Key Generation: An Analysis of Yubico's Proposal for W3C WebAuthn”
 - Formal security proof
 - <https://eprint.iacr.org/2020/1004>
- 2023 Wilson “Post-Quantum Account Recovery for Passwordless Authentication”
 - PQC construction
 - <https://uwspace.uwaterloo.ca/items/d1f73f71-e3b2-438c-b261-11632becdbb2>
 - Similar concurrent publications linked in draft

Use cases



- Efficient hardware binding
 - Batch-issued single-use digital ID
 - Single-use keys for privacy
- Backup keys
 - Offline backup device delegates public key generation
- Implementation status:
 - Tech preview in YubiKey 5.8
 - wwWallet/Siros ID (EUDI) likely to integrate with Longfellow ZK

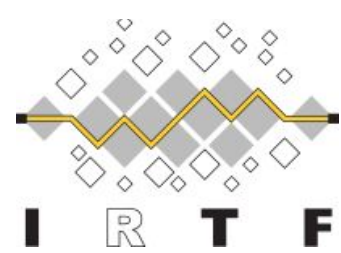
Contributions

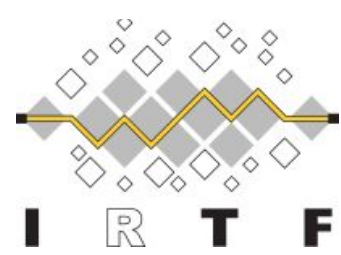


- Concrete ARKG construction and instances
 - General-purpose keygen primitive
 - NIST curves & X25519/X448
 - Test vectors for P-256
- Modular construction [Wilson]
 - PQC ready
 - “Just” add alg IDs

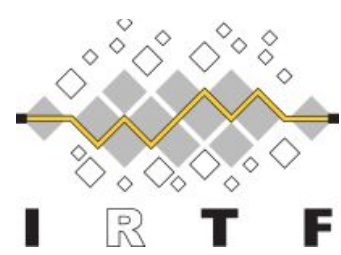
Next Steps

Time for Research Group Call for Adoption?



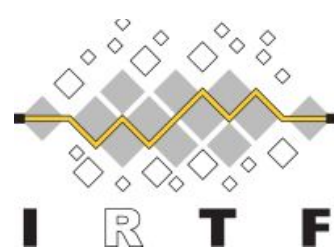


Questions!



spare slides

Terms



- **Delegating party** (e.g., hardware security device)
 - Generates seed
 - Holds **private seed**
 - Shares **public seed**
 - Derives and uses private keys
- **Subordinate party** (e.g., userspace app)
 - Holds public seed
 - Derives public keys
 - Submits public keys to 3rd parties