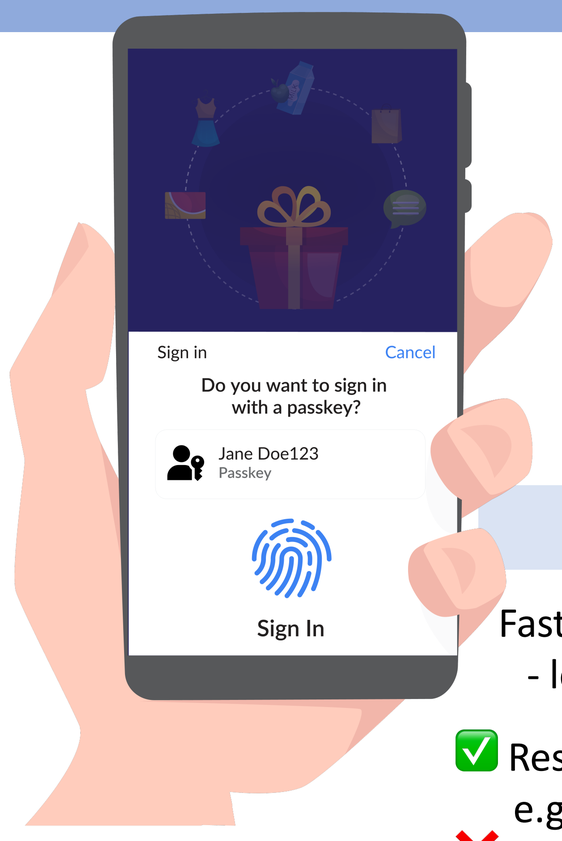
Toward Cloud-based FIDO Authentication with Secure Credentials Recovery

Momoko Shiraishi
The University of Tokyo
shiraishi@os.ecc.u-tokyo.ac.jp

Takahiro Shinagawa
The University of Tokyo
shina@ecc.u-tokyo.ac.jp



1 Background

Fast IDentity Online (FIDO) is emerging
- leverages public key authentication

✅ Resistant to attacks
e.g., phishing and man-in-the-middle

❌ **Account recovery**
when authentication devices are lost

2 Challenges & Previous Work

Challenge 1. Credential availability
Loss of (all) auth. devices does not lead to loss of credentials
<--> 😐 A backup token dedicated to recovery [1, 2]
<--> 😐 A group signature for multiple devices [3]

Challenge 2. Credential security
Credentials (private keys) never leave hardware devices
<--> 😐 Passkeys (multi-device FIDO credential)

Challenge 3. Recovery scalability
Recovery of web access does not take much time and effort [4]

3 Proposal: Cloudauthn

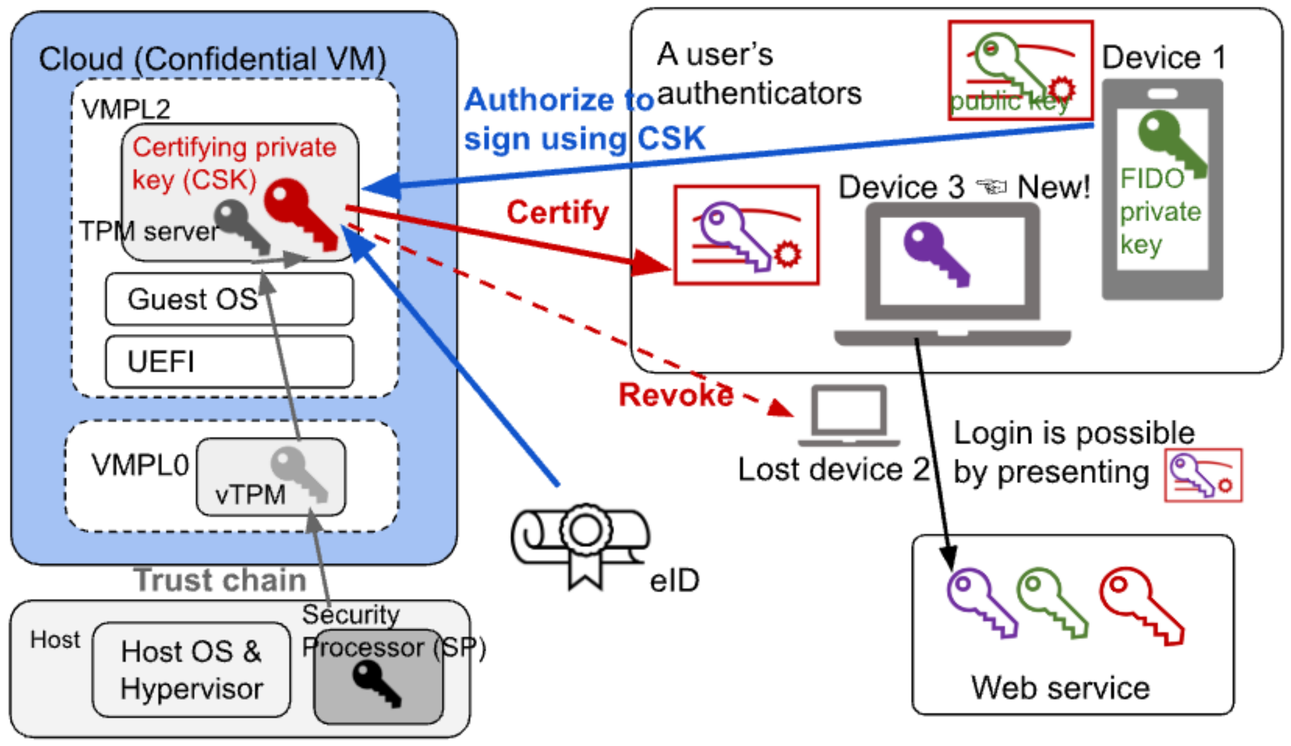
- A cloud-based FIDO authentication scheme
  - ***Certifying keys*** are maintained in a TEE in the cloud
    - Certifying that **a FIDO key** belongs to the legitimate user
  - **Certified FIDO keys** are used to login to web services
    - Even with a brand new authentication device
  - Old FIDO keys are revoked automatically
    - The cloud holds *Registered Keys & Services List*

✅ Credentials availability

- **Certifying keys** are always maintained in the cloud
- A new authentication device can be easily registered
  - Using existing authentication devices (if available)
  - Using the cloud with ID proofing methods
    - e.g., eID, ePassport, ...

✅ Credentials security

- **Certifying keys** are maintained in a TEE
  - Always encrypted in both memory and storage
    Even malicious cloud providers cannot access the keys
- **FIDO private keys** never leave the authentication devices
  - Kept in tamper-proof devices

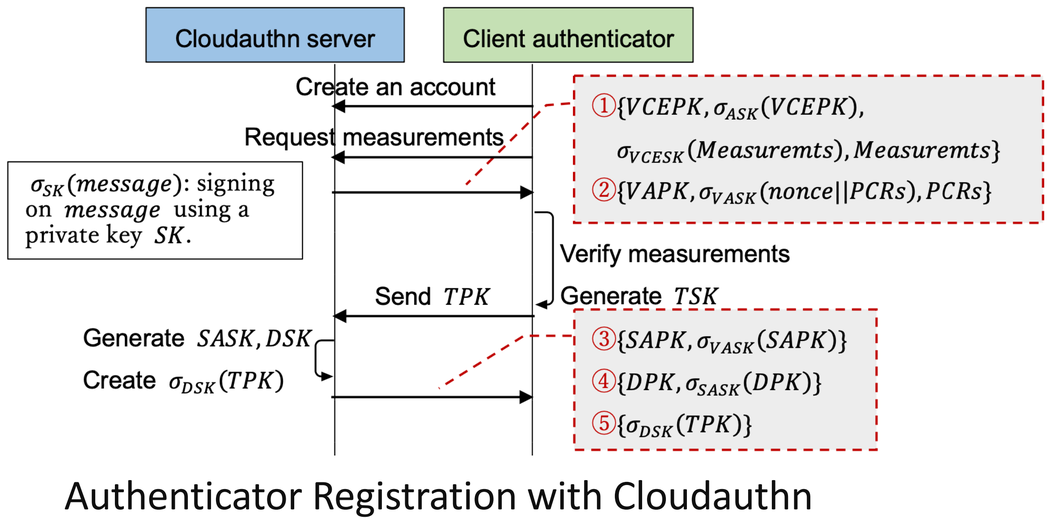


✅ Recovery scalability

- The cloud maintains Registered Keys & Services List
  - Certifying keys, registered FIDO key IDs, domains of websites
- Users notify the cloud of lost authentication devices
  - The cloud automatically revokes the old FIDO keys
- Users can immediately access the registered web services
  - Users register a new authentication device to the cloud
  - The cloud certifies **FIDO keys** of the authentication device
  - Web services accept **the keys** certified by the cloud

4 Implementation

- The cloud is **a confidential VM** (AMD SEV-SNP)
- **Certifying keys** are stored in **Non Volatile (NV) files of a TPM server**
- Each NV file is encrypted with **each authenticator's key**
- Users can verify the cloud's environment through **attestation**
- At registration with the cloud, users obtain
  - certificates on **FIDO keys** issued by the cloud
  - attestation proofs for the **certifying keys** based on **hardware trust**
- At registration with web services, users submit these proofs



Authenticator Registration with Cloudauthn

5 Future Works

- Detailed security & performance analysis
- Comparison with previous studies

References
[1] N. Frymann et al. Asynchronous Remote Key Generation: An Analysis of Yubico's Proposal for W3C WebAuthn. ACM CCS. (2020)
[2] Alex Takakuwa. Moving from Passwords to Authenticators. Ph.D. Dissertation. (2019)
[3] S. Arora et al. Avoiding lock outs: Proactive FIDO account recovery using managerless group signatures. Cryptology ePrint Archive. (2022)
[4] S. Lyastani et al. Is FIDO2 the kingslayer of user authentication? A comparative usability study of FIDO2 passwordless authentication. IEEE S&P. (2020)