Universally Composable Auditable Surveillance

Valerie Fetzer Michael Klooß Jörn Müller-Quade

Markus Raiber Andy Rupp

Karlsruhe Institute of Technology

KASTEL

UNIVERSITÄT LUXEMBURG

Aalto University

Introduction

Ongoing debate

Law enforcement needs to be able to do constitutional searches

- Needs backdoors to anonymous systems

Introduction

Ongoing debate

Law enforcement needs to be able to do constitutional searches

- Needs backdoors to anonymous systems

Privacy activists argue that backdoors are vulnerable to abuse

- It should not be possible to abuse the existence of backdoors

Introduction

Ongoing debate

Law enforcement needs to be able to do constitutional searches

- Needs backdoors to anonymous systems

Privacy activists argue that backdoors are vulnerable to abuse

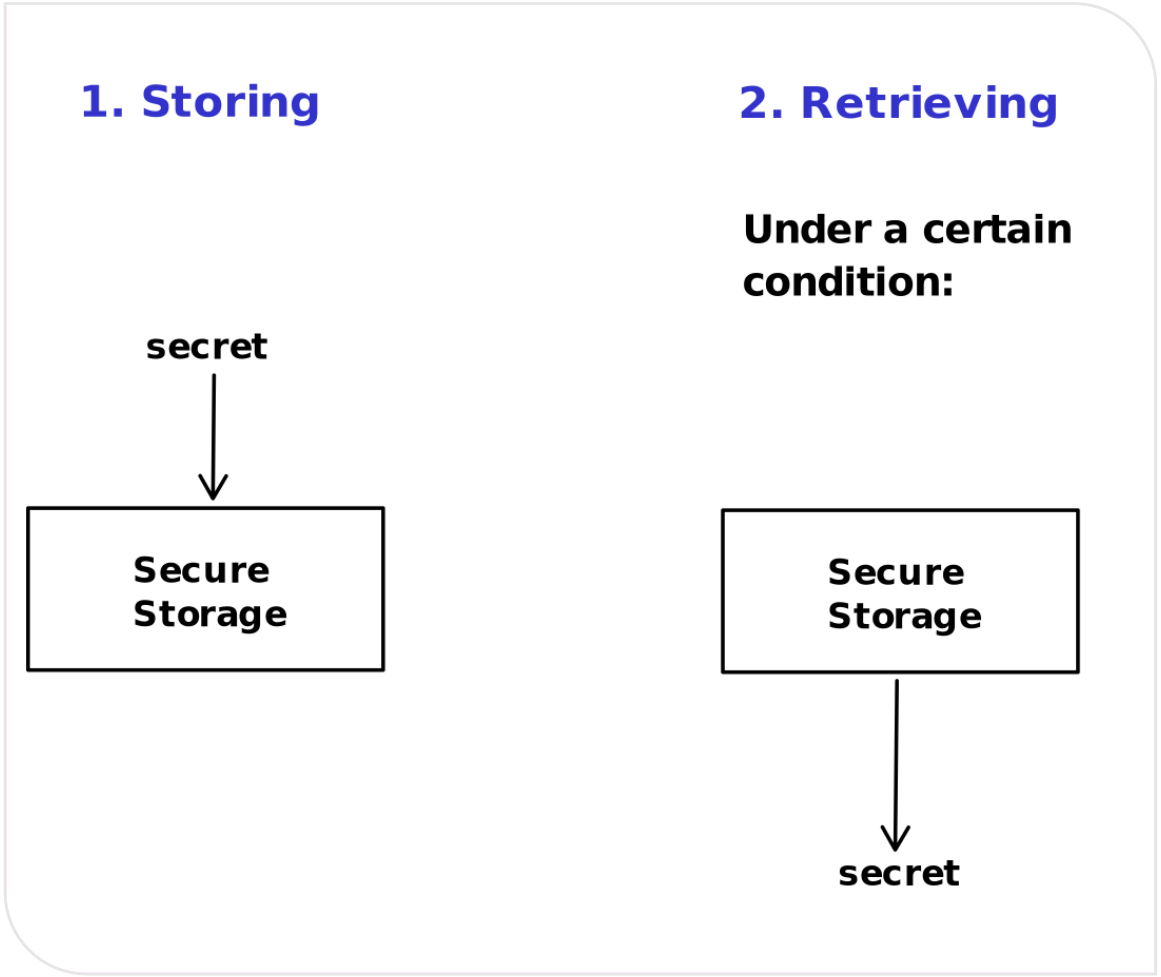
- It should not be possible to abuse the existence of backdoors

Our Research Question

How can we ensure in an auditable fashion that backdoors are only used for legitimate purposes?

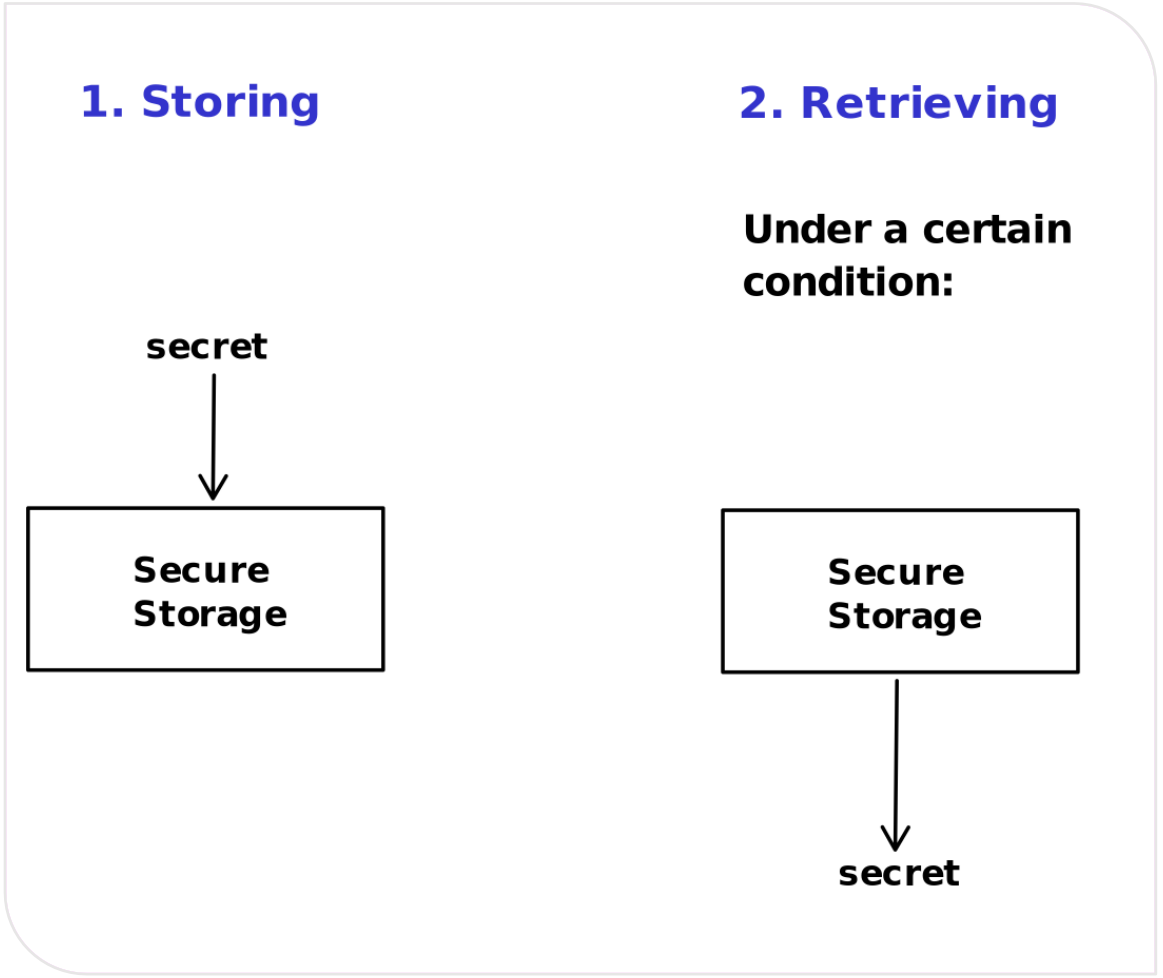
General Idea

- We have a secret (i.e., user-specific backdoor)
- We want to store it somewhere securely
- Only under a certain condition should the secret be released



Application Scenario: Anonymous Electronic Payments

1) Each user of the electronic payment scheme deposits a secret upon registration
2) User pays anonymously
3) If law enforcement suspects the user of money laundering, they can request the user‘s secret
4) Law enforcement can reconstruct all transactions of that user



Previous Methods and our Approach

- Key escrow mechanisms
  - Enable storage and retrieval of (user-specific) backdoors
  - But can be misused by the key escrow authorities (e.g., for silent mass surveillance)

Previous Methods and our Approach

- Key escrow mechanisms
  - Enable storage and retrieval of (user-specific) backdoors
  - But can be misused by the key escrow authorities (e.g., for silent mass surveillance)
- Usage of distributed ledger technology for accountability
  - Authorities publish information about surveillance measures on the ledger and can provide ZK proofs that they behave according to the laws
  - No measures to ensure that first evidence is published and *then* backdoor is used

Previous Methods and our Approach

- Key escrow mechanisms
  - Enable storage and retrieval of (user-specific) backdoors
  - But can be misused by the key escrow authorities (e.g., for silent mass surveillance)
- Usage of distributed ledger technology for accountability
  - Authorities publish information about surveillance measures on the ledger and can provide ZK proofs that they behave according to the laws
  - No measures to ensure that first evidence is published and *then* backdoor is used
- ▶ Our approach: Combine both methods
  - Secrets/Backdoors are user-specific and only valid for certain time periods
  - Store encrypted secret somewhere, e.g., at system operator
  - Use ledger and an anonymous evolving committee to manage the key to decrypt secrets
  - Authorities must *first* publish proof that they are eligible to get the secret on the ledger and *afterwards* get the decrypted secret

Contribution

- Building block that allows to enhance existing protocols with auditable surveillance
- Modeled as an ideal functionality in the Universal Composability (UC) framework
  - To ensure that the system's security and privacy guarantees still hold if the system is run in combination with many different other protocols
- Protocol that realizes the ideal functionality
  - Uses PKE, threshold PKE, commitments, signatures, NIZK proofs, abstract ledger model, …

Parties

User

- Uses the (payment) system

Parties

User

- Uses the (payment) system

System Operator

- Owns the (payment) system

Parties

User

- Uses the (payment) system

System Operator

- Owns the (payment) system

Law Enforcement

- Wants to deanonymize transactions of a user
- Needs a warrant to do so

Parties

User

- Uses the (payment) system

System Operator

- Owns the (payment) system

Law Enforcement

- Wants to deanonymize transactions of a user
- Needs a warrant to do so

Judge

- Grants or denies warrants

More Parties

The Public

- Can get some statistics about requested user secrets

More Parties

The Public

- Can get some statistics about requested user secrets

Auditor

- Can audit the secret request afterwards
- Can create more detailed statistics about requested secrets than the public

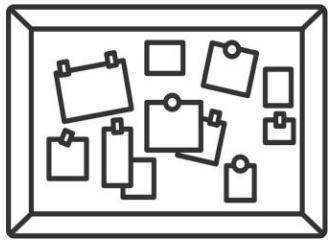
More Parties

The Public

- Can get some statistics about requested user secrets

Auditor

- Can audit the secret request afterwards
- Can create more detailed statistics about requested secrets than the public

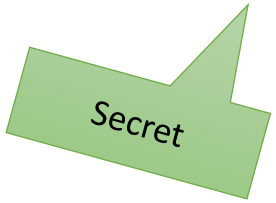


Committee Members

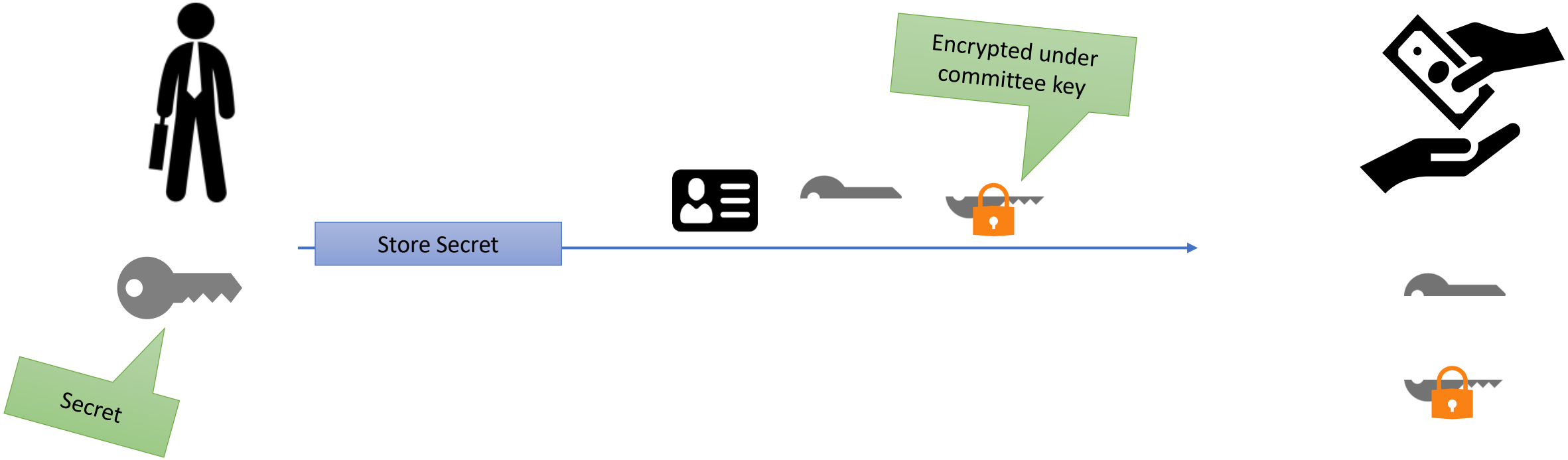
- Committee processes secret requests
- Communication with anonymous committee members through public bulletin board or append-only ledger

Store Secret & Payment Transaction

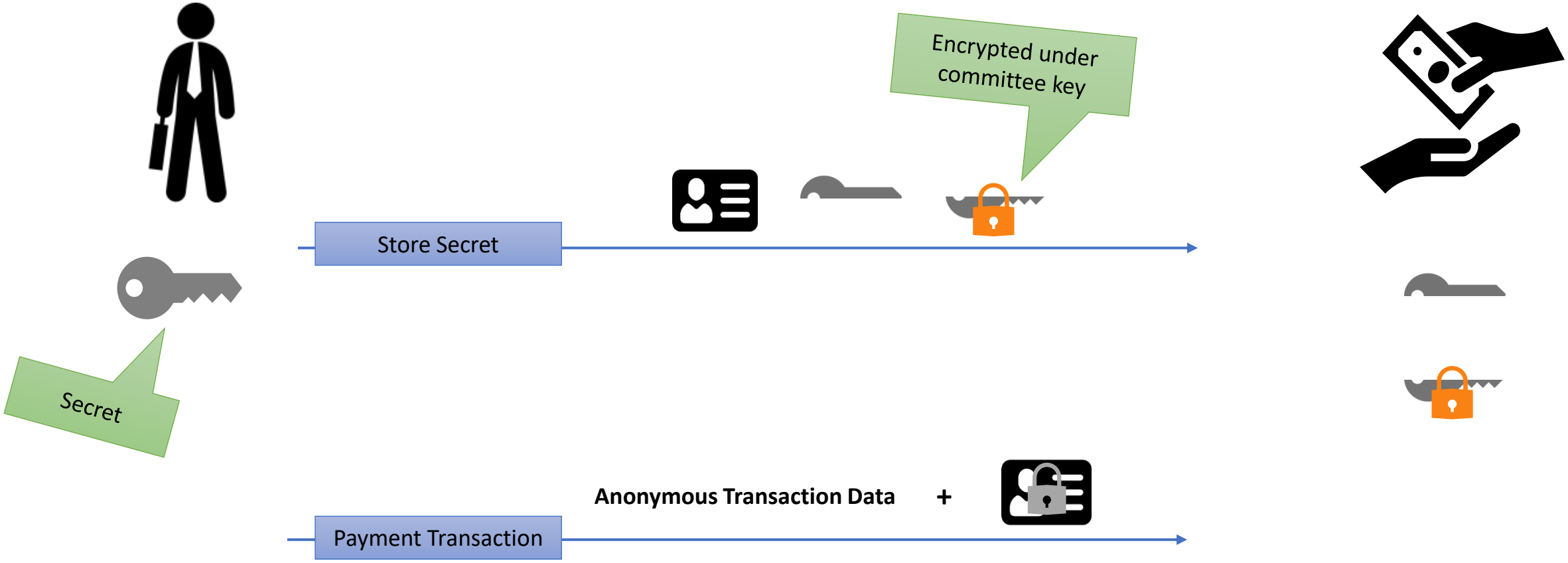
Store Secret & Payment Transaction



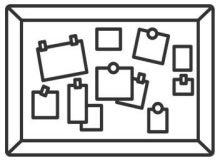
Store Secret & Payment Transaction



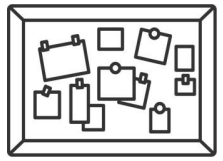
Store Secret & Payment Transaction

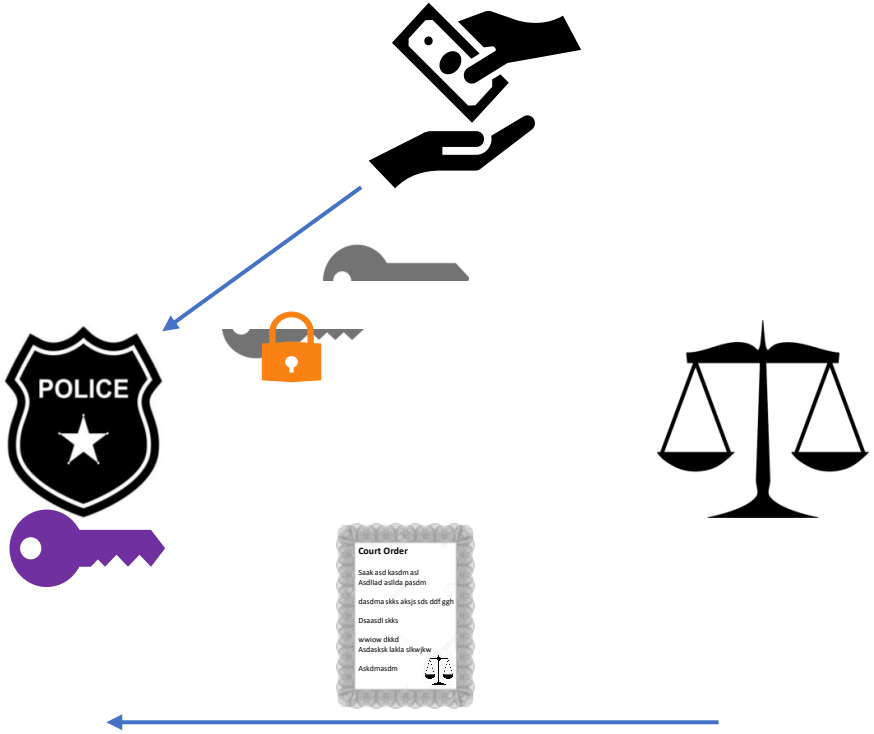


Requesting a Secret

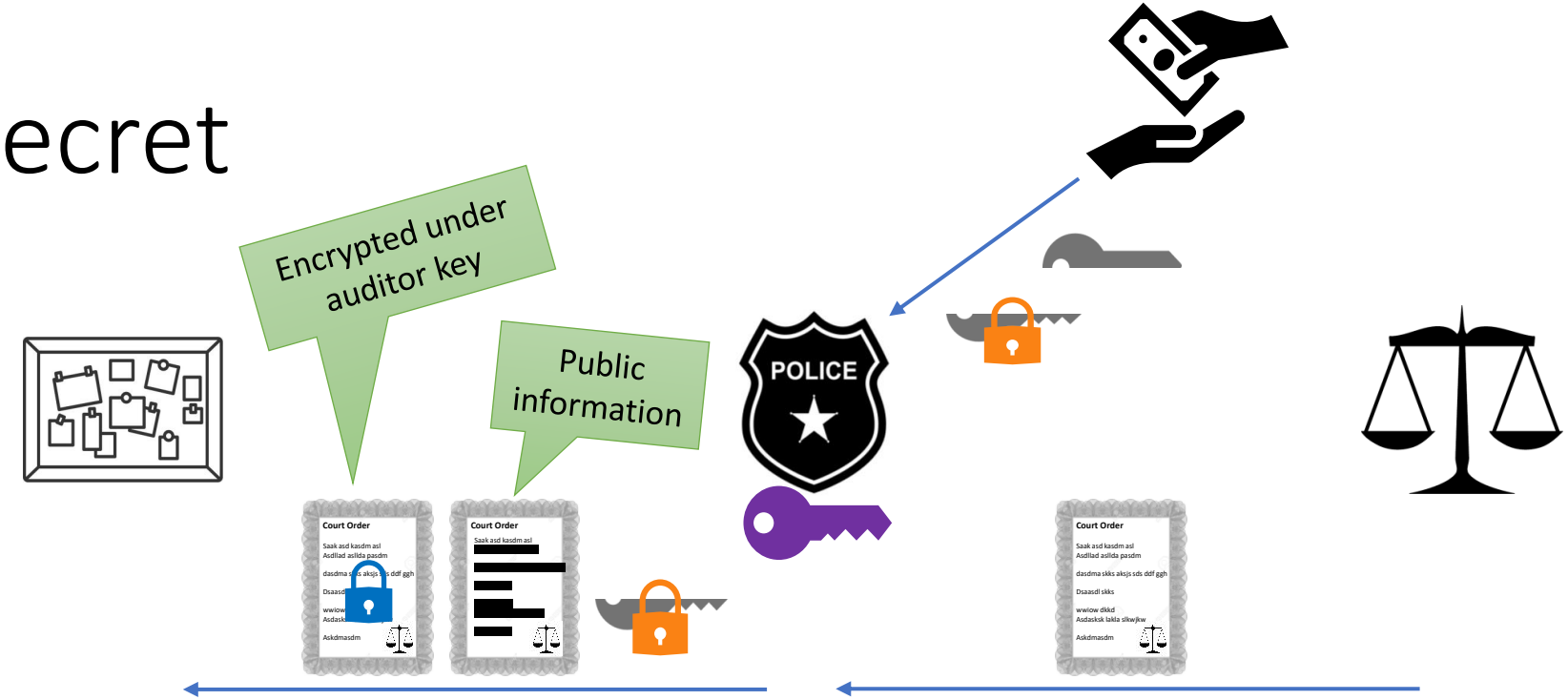


Requesting a Secret

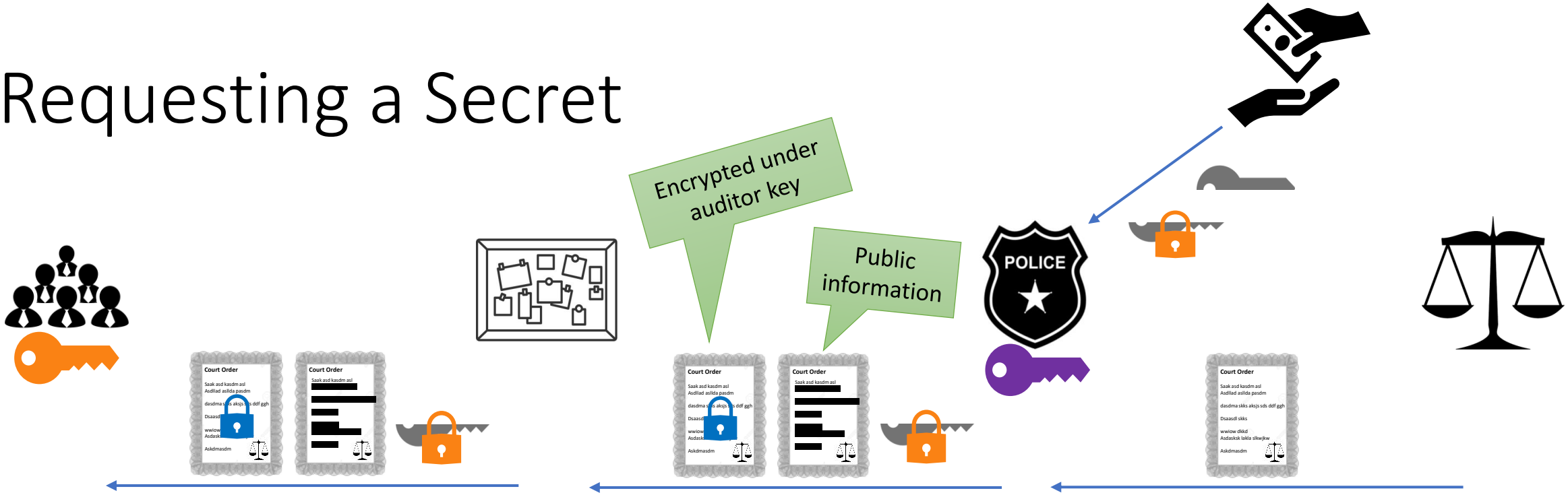




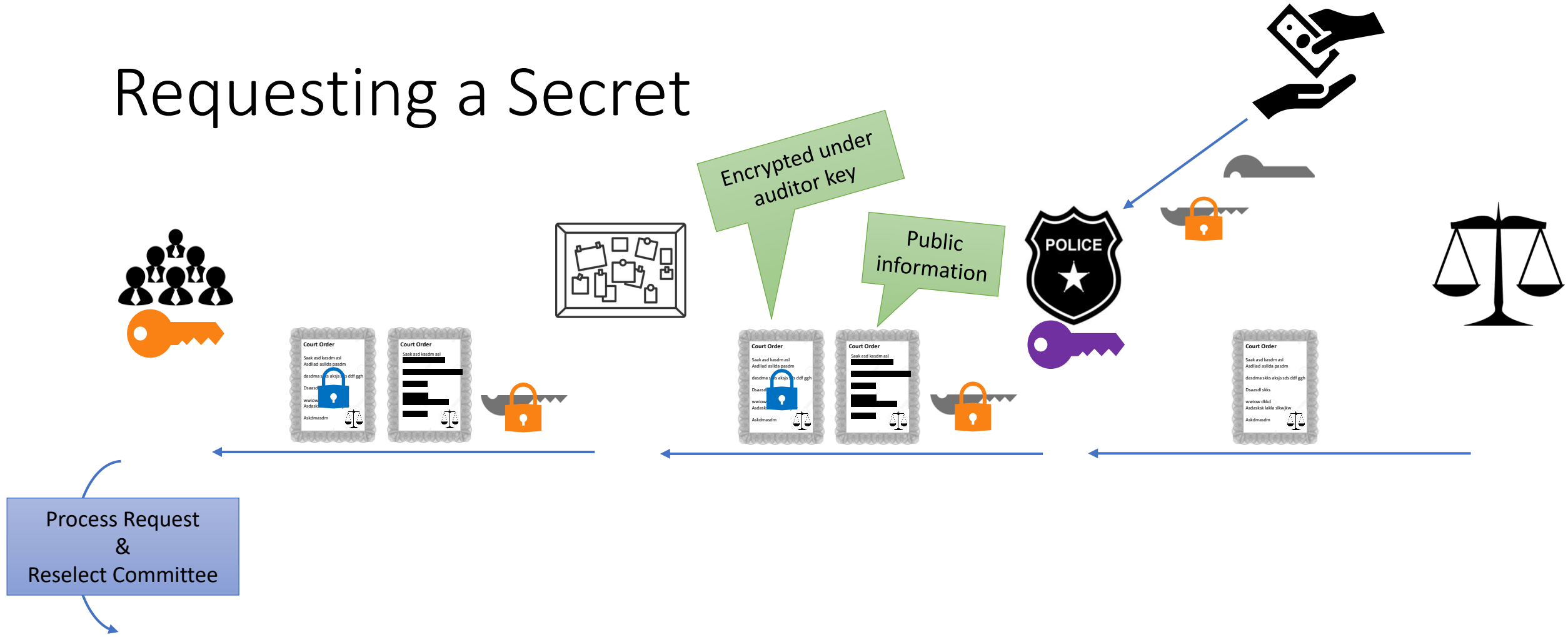
Requesting a Secret



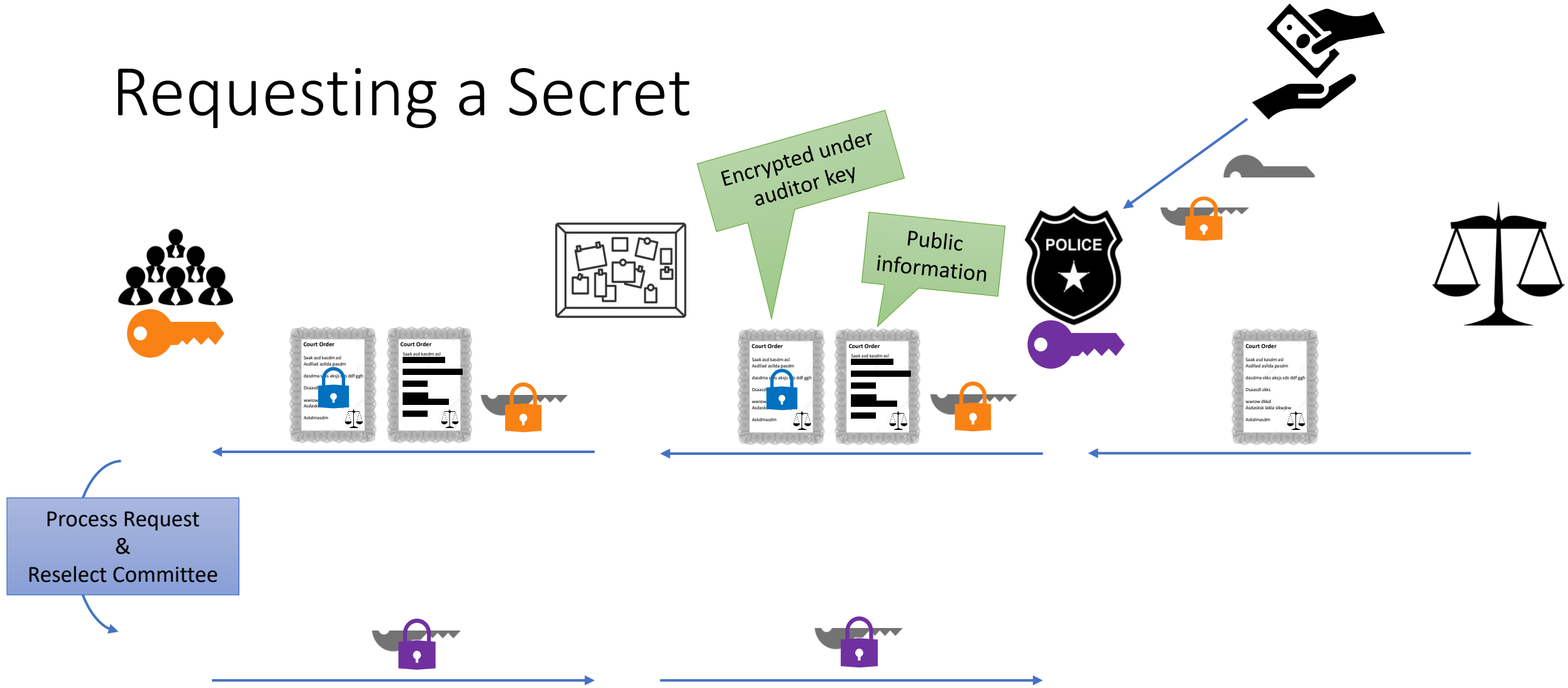
Requesting a Secret



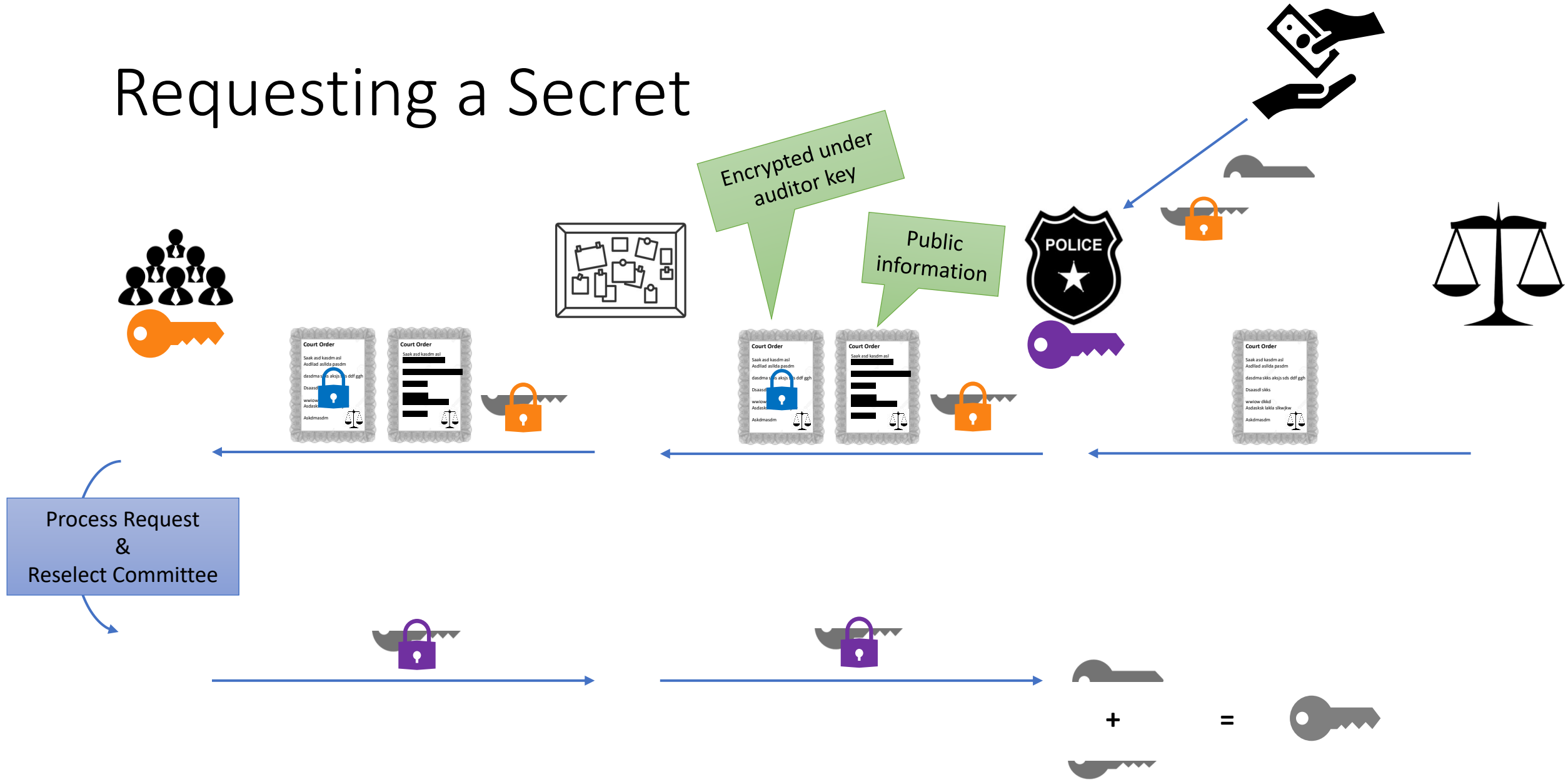
Requesting a Secret



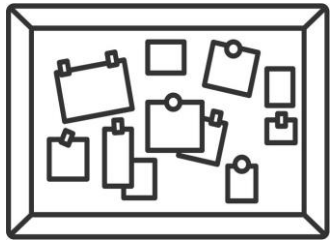
Requesting a Secret



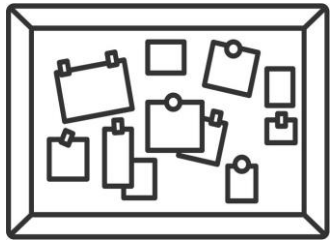
Requesting a Secret



Audit and Statistics

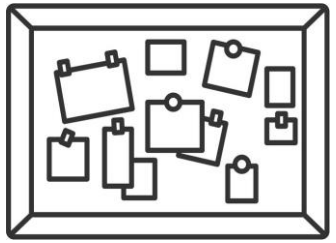


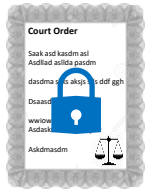
Audit and Statistics



Can create simple statistics, e.g., number of requested secrets

Audit and Statistics





Can create simple statistics, e.g., number of requested secrets

Can retrospectively examine surveillance decisions

Protection Mechanisms for Escrowed Secrets

- Secrets are short-term and user-specific
- Secrets are shared between trustworthy parties to avoid a single point of failure
- Escrow secret access is given conditionally (judge-signed warrant needed)
- There are audit trails and public statistics for every (granted) secret request
- Surveillance is silent, i.e., users do not know they are surveilled

Properties of the committee

- We use an anonymous evolving committee to manage the decryption key on the ledger

- Modeled in the YOSO (You-only-speak-once) model [Gen+21]
  - ▶ Committee members are anonymous until they finished their work
  - ▶ Prevents targeted corruption of committee members
  - ▶ Security against mobile adversaries

[Gen+21] Gentry et. al., “YOSO: You only speak once: secure MPC with stateless ephemeral roles”. CRYPTO 2021.

Conclusion

- Contributes to the current debate between law enforcement and privacy activists regarding the "need" for back doors
- Present a UC-secure building block to augment existing applications with auditable surveillance capabilities
- Backdoors are protected in mutliple ways

Thanks!

https://ia.cr/2023/1343