PRIVACY-PRESERVING ALIBI SYSTEMS

Benjamin Davis, Hao Chen, Matthew Franklin

University of California, Davis

ASIACCS 2012

Motivation

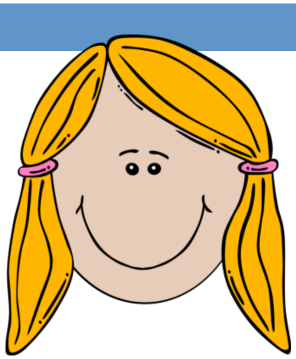
- “Murder Case Dropped After MetroCard Verifies Alibi” – New York Times, January 2009
- Limitations of traditional alibis
  - Not ubiquitous
  - Can’t provide privacy

Motivation

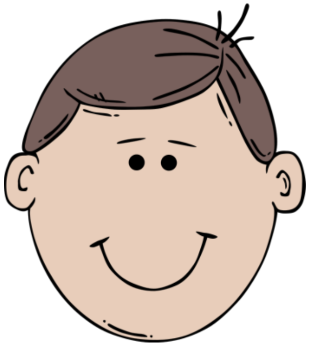
- Can we use our mobile devices to create alibis for us… without giving up our privacy?
  - *We can create alibis without revealing our identity*
  - Facilitate opportunistic alibi creation

Participants in an Alibi Scheme

- Alibi Owner: "Olivia"
  - Privacy always protected



- Alibi Corroborator: "Charlie"
  - Identity may be public or private



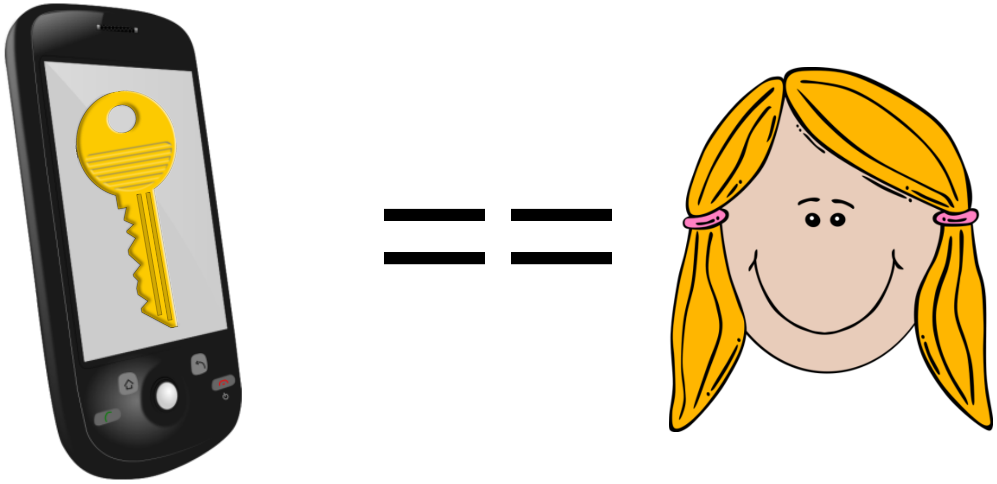
- Judge:

Requirements for our Schemes

- Privacy: owner identity hidden unless claimed
- No centralized or trusted third-party
- No storage burden on corroborators

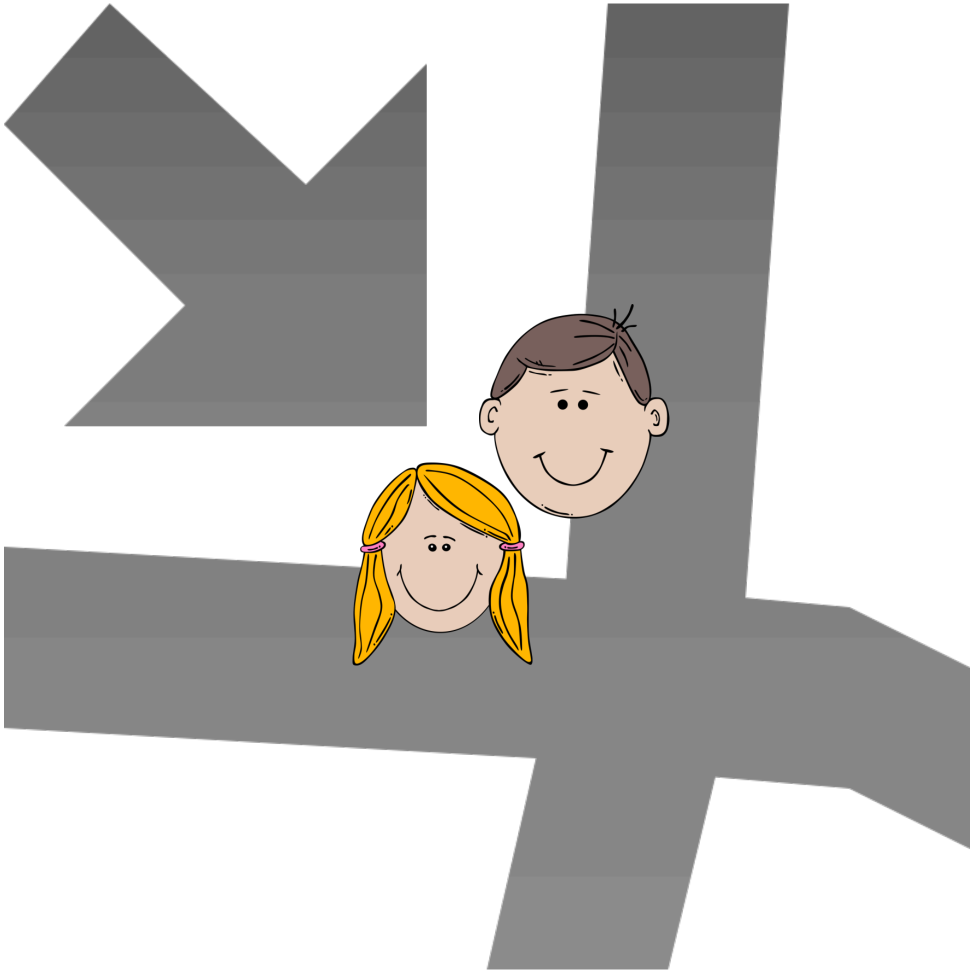
Assumptions

- Public Key Infrastructure
  - Public/private keys for all owners, corroborators
- Devices with private keys are not shared
  - ID of private key user == ID of private key owner



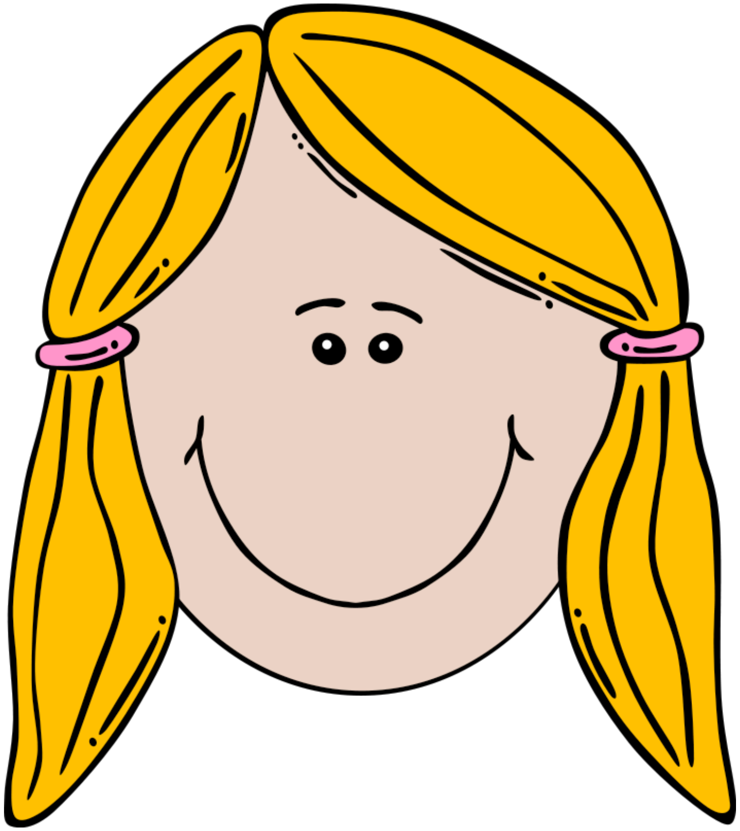
Alibi Creation

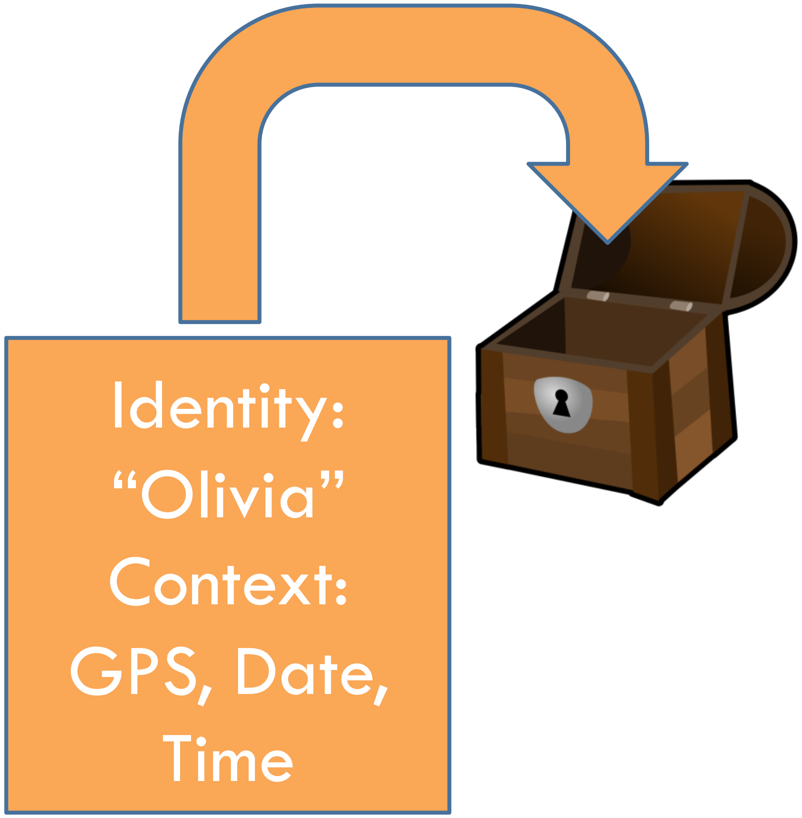
- □ Two participants are in the same place



Alibi Creation

- □ Owner records her identity and context

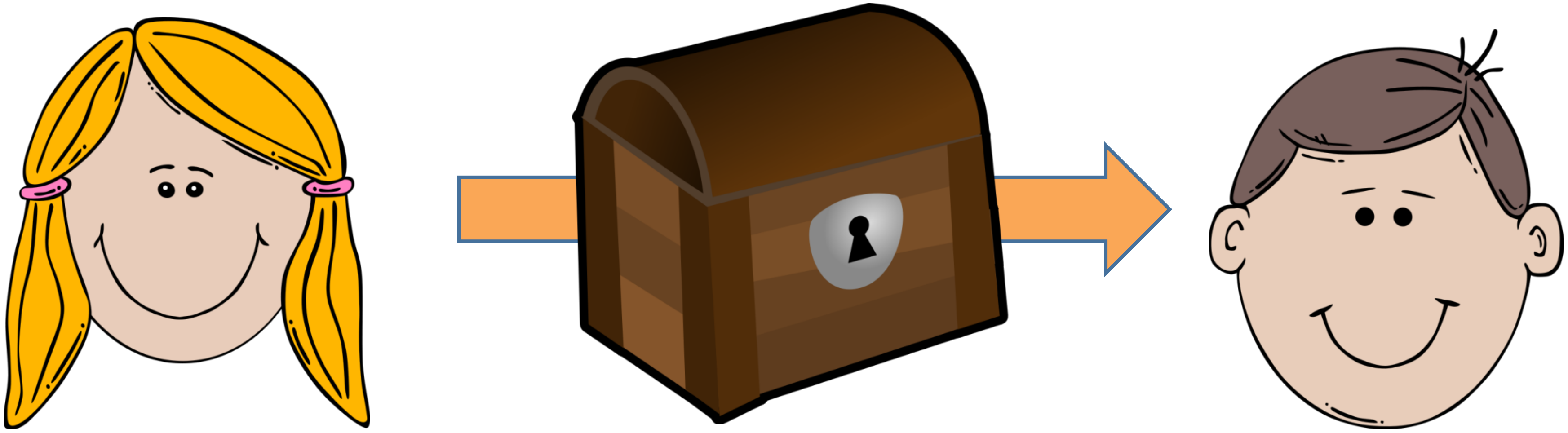




Identity: “Olivia”
Context: GPS, Date, Time

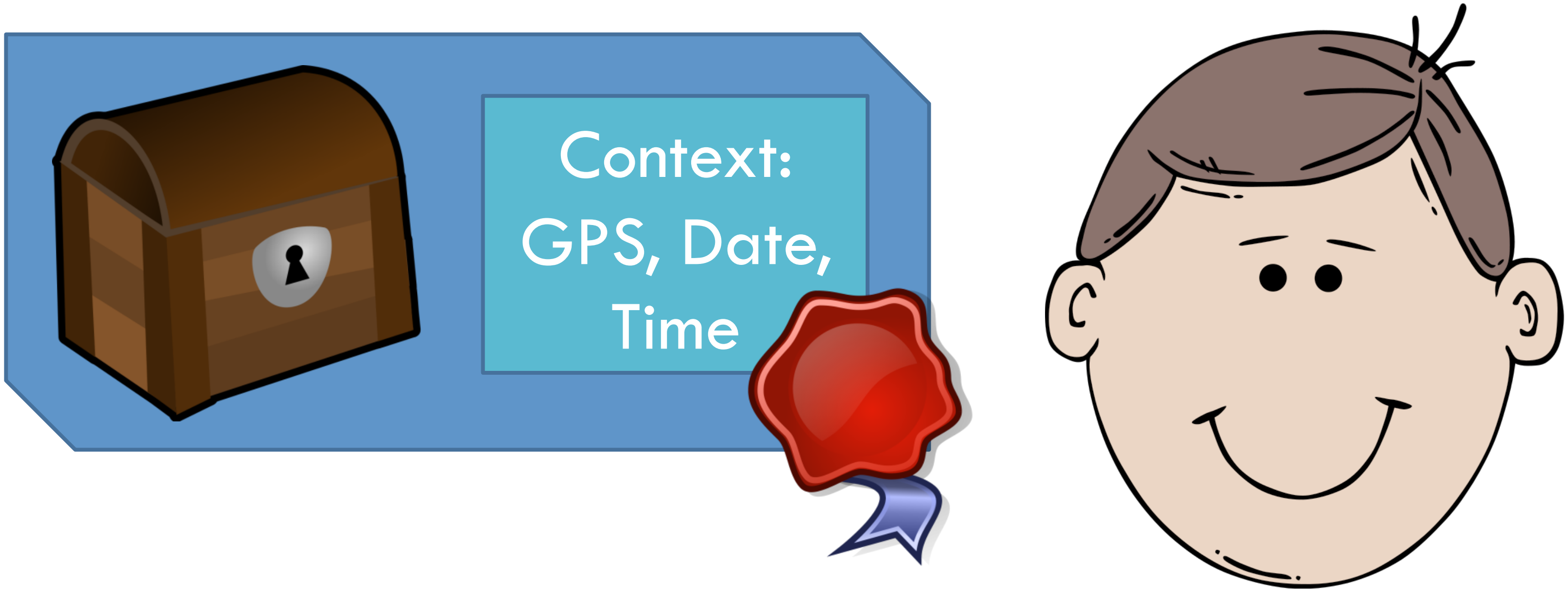
Alibi Creation

- □ Owner sends sealed record to Corroborator



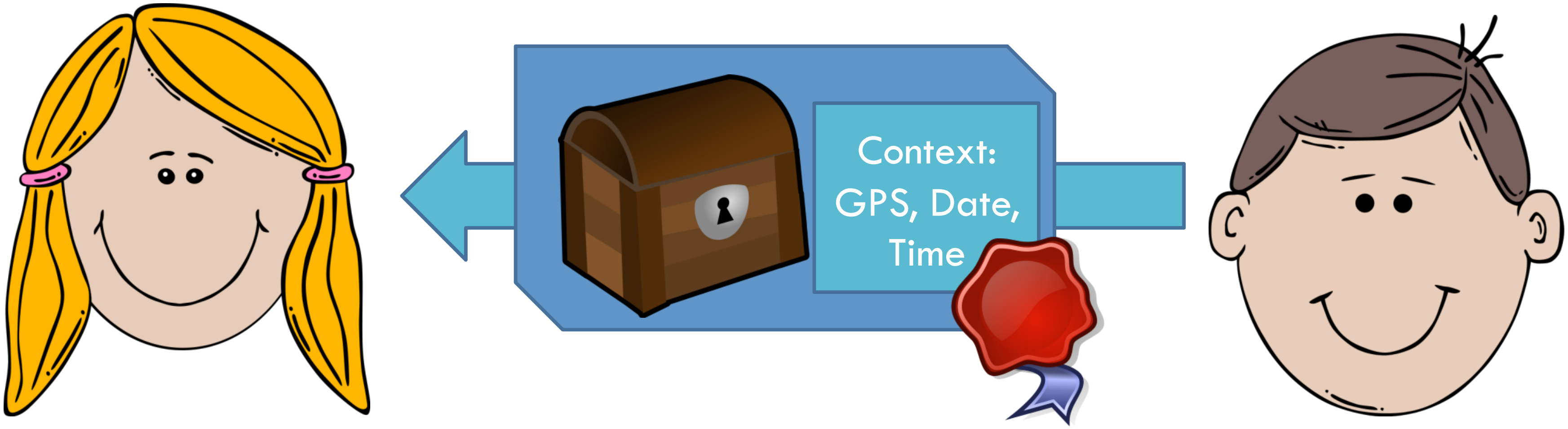
Alibi Creation

- Corroborator certifies observation of record and context



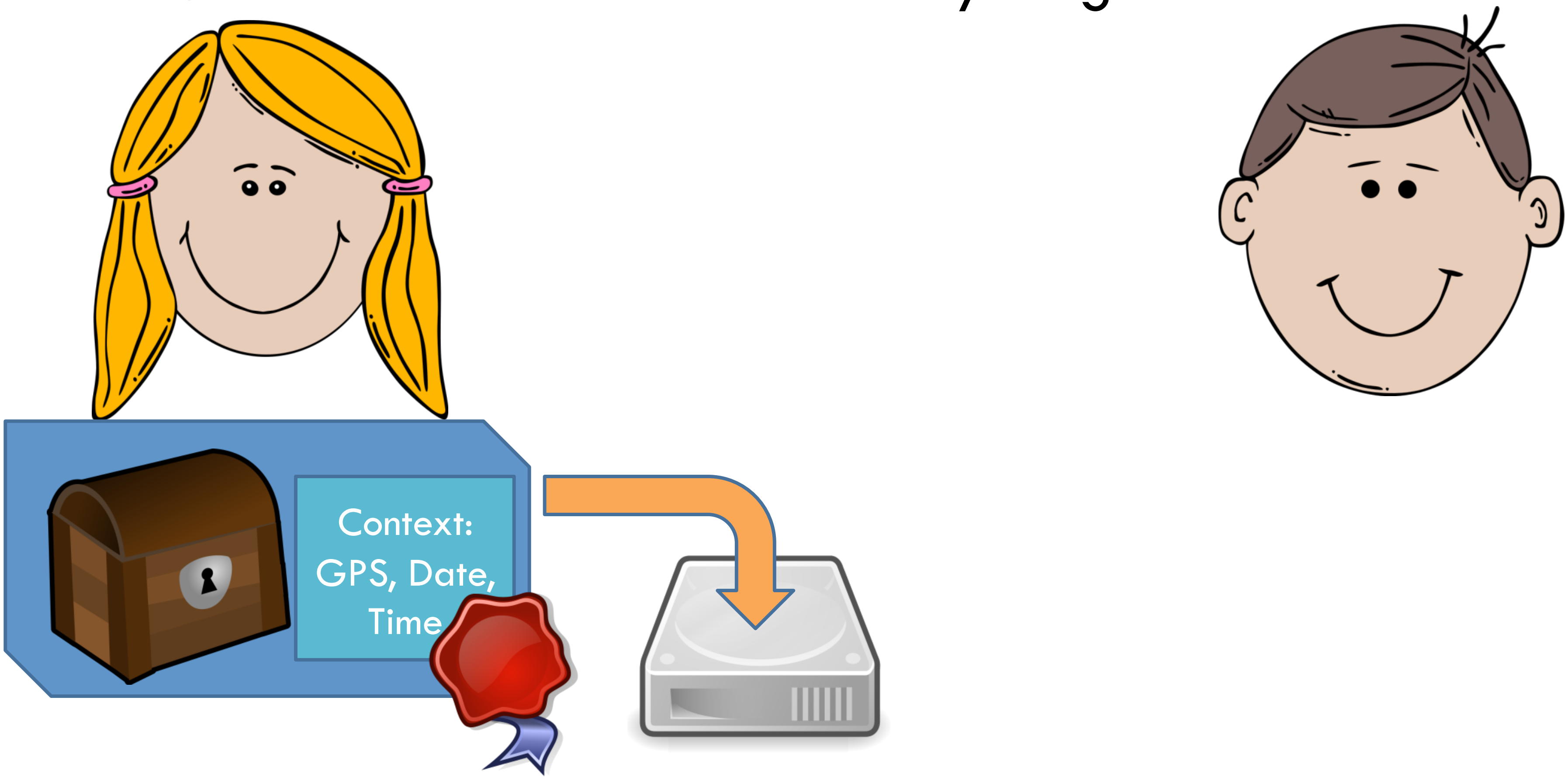
Alibi Creation

- □ Corroborator sends certification back to Owner



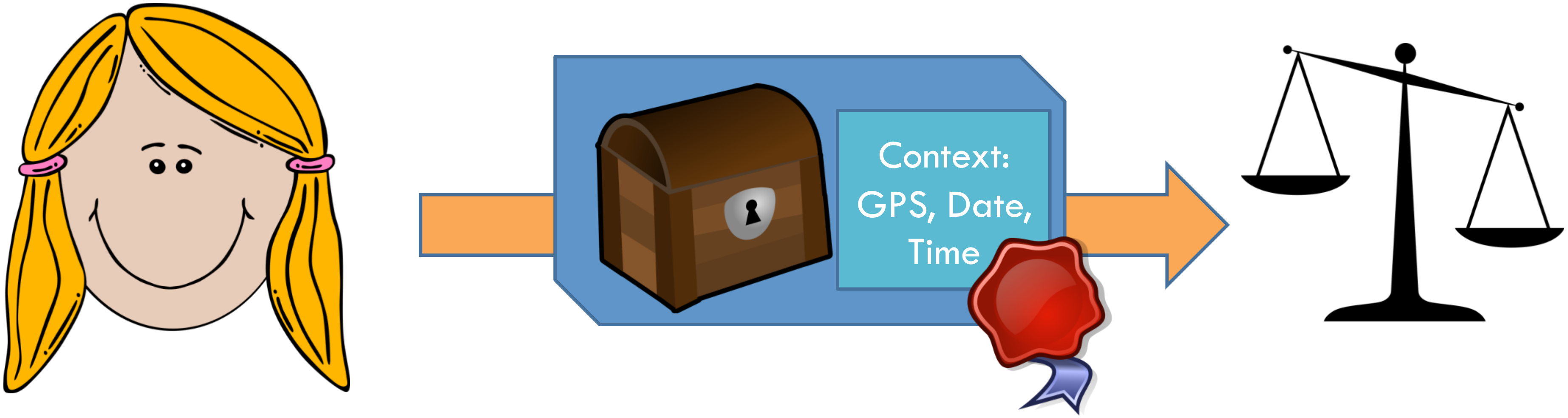
Alibi Storage

- □ Owner stores “testimony” from corroborator
- □ Corroborator doesn’t store anything



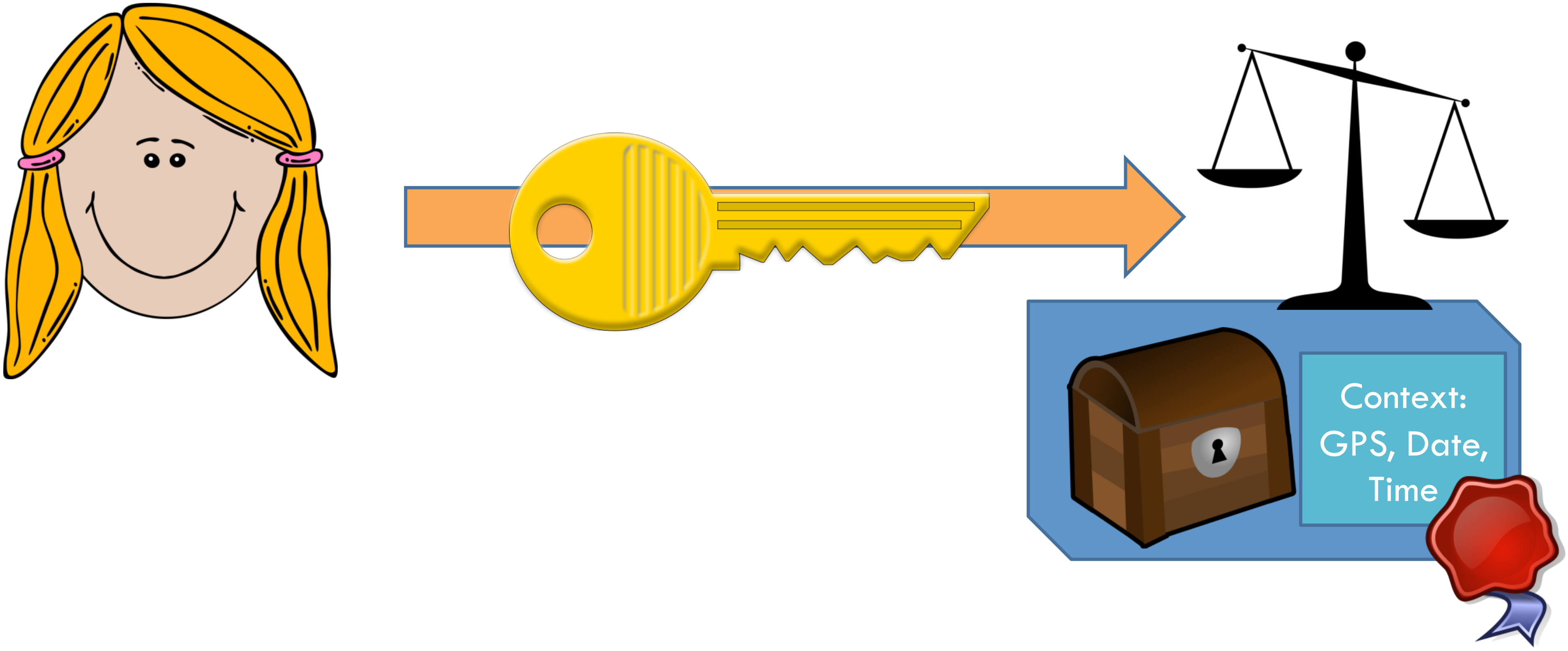
Claiming an Alibi

- Alibi owner sends testimony to Judge



Claiming an Alibi

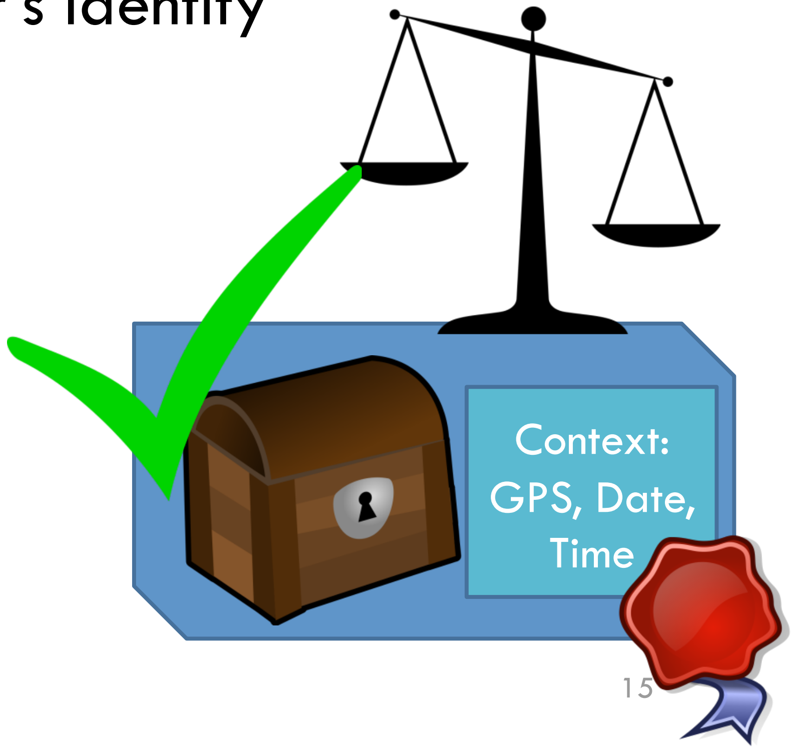
- Alibi owner links identity to record



Alibi Verification

- Judge confirms
  - Corroborator’s testimony matches owner’s claim and can be attributed to the corroborator
  - Link between record and owner’s identity

Identity:
“Olivia”
Context: GPS,
Date, Time



Background: String Commitment Schemes

- Cryptographic commitment schemes provide:
  - **Commit**: commit to a value without revealing the value
  - **Decommit**: reveal the committed value
- Our implementation uses [Halevi & Micali '96]
  - Noninteractive
  - Efficient computation and storage

Alibi Creation (public corroborator)

- □ **Owner Statement**

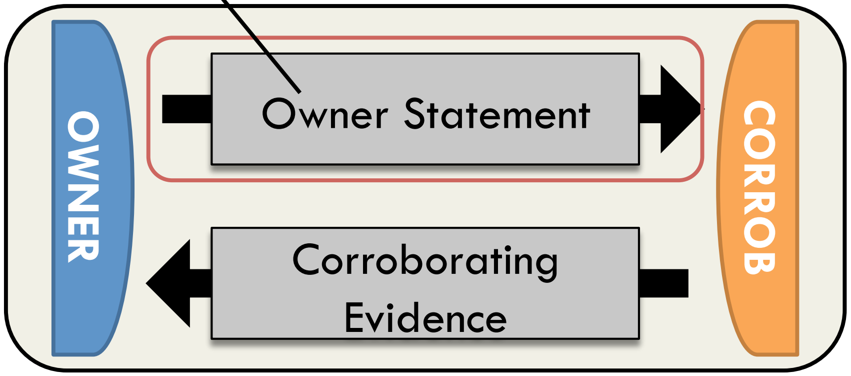
COMMITMENT TO {

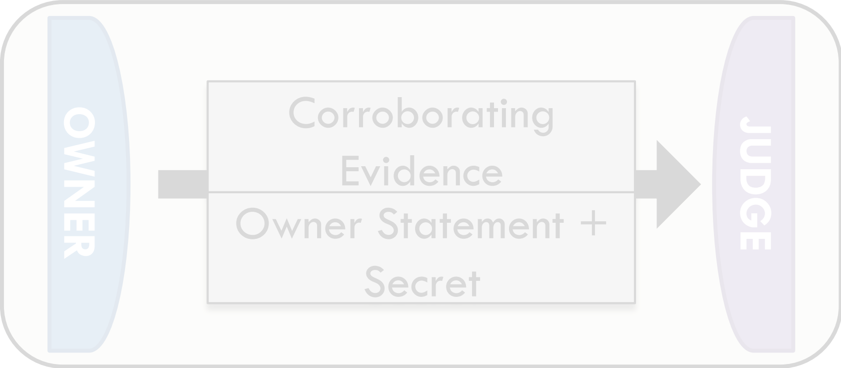
Owner identity,

Owner's view of Context

Owner's signature

}





Alibi Creation (public corroborator)

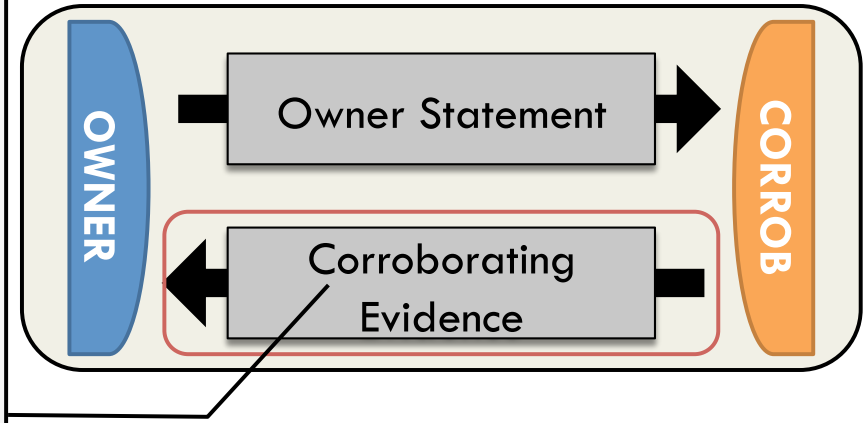
- **<u>Corroborating Evidence</u>**

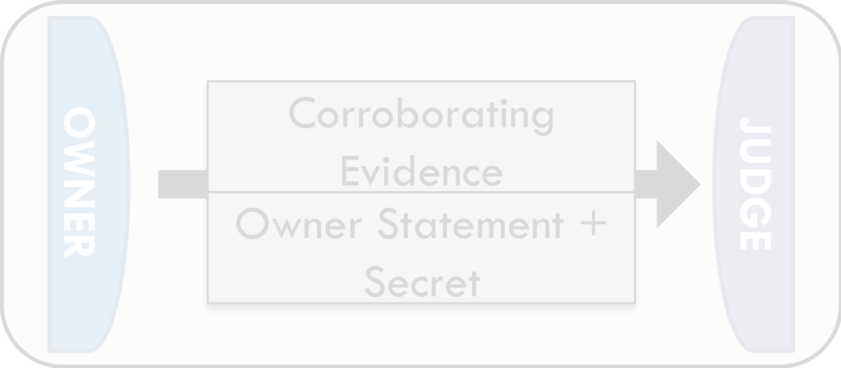
{

Corroborator’s view of the Context,

Corroborator’s signature over (OwnerStatement || Corroborator’s Context)

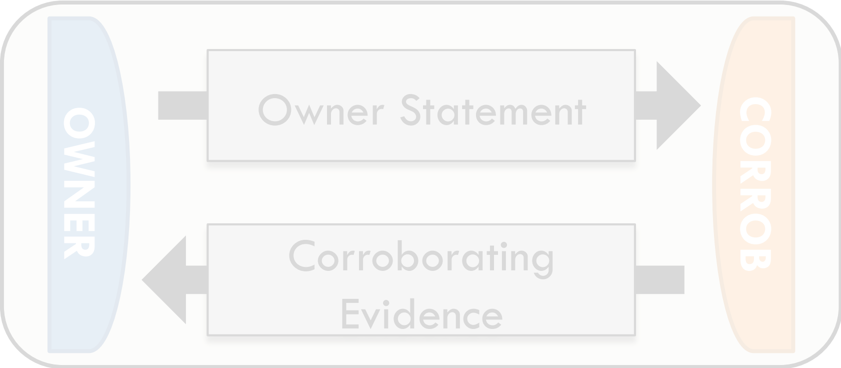
}

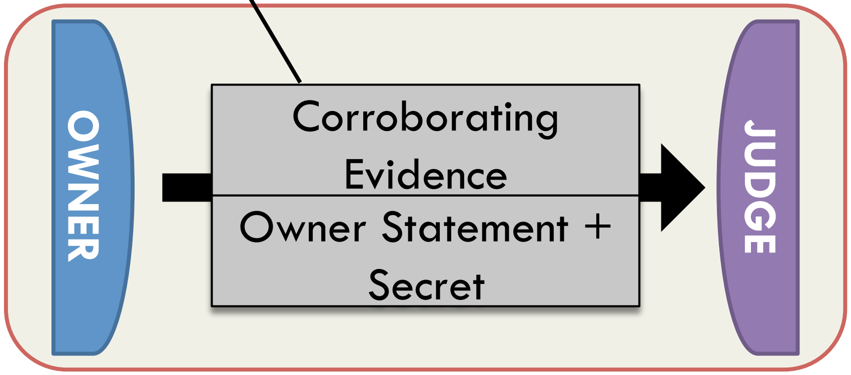




Alibi Verification (public corroborator)

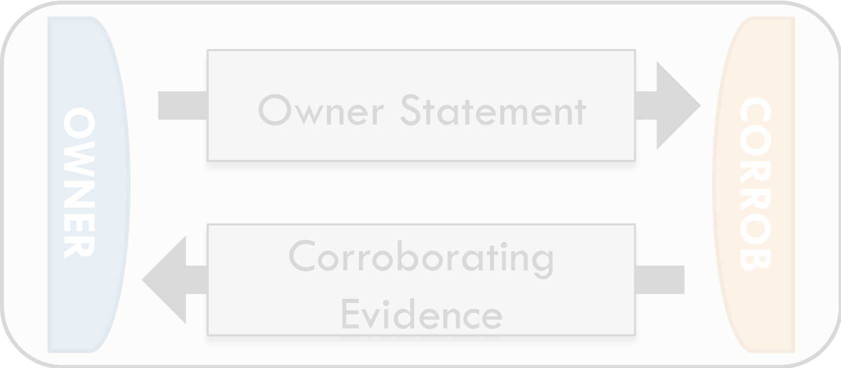
- Owner presents:
  - Corroborating Evidence
  - Owner Statement
  - Decommitment for Owner Statement

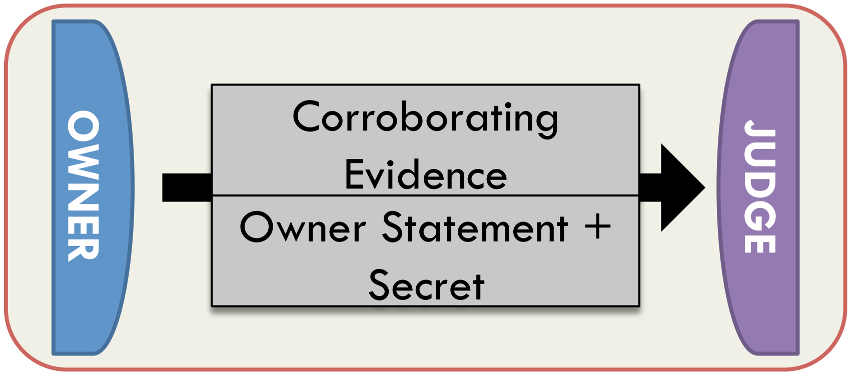




Alibi Verification (public corroborator)

- Judge checks:
  - Corroborator's signature
  - Decommit Owner Statement
    - Owner's signature
    - Owner's context matches Corroborator's context





Security Against Malicious Alibi Owners

- Alibi owner can’t modify context
- Alibi owner can’t transfer alibi
- Can’t reuse Corroborating Evidence

Security Against Malicious Alibi Corroborators

- Identity of alibi owner is hidden until alibi is claimed
- Corroborator can’t reuse or fabricate Owner Statement

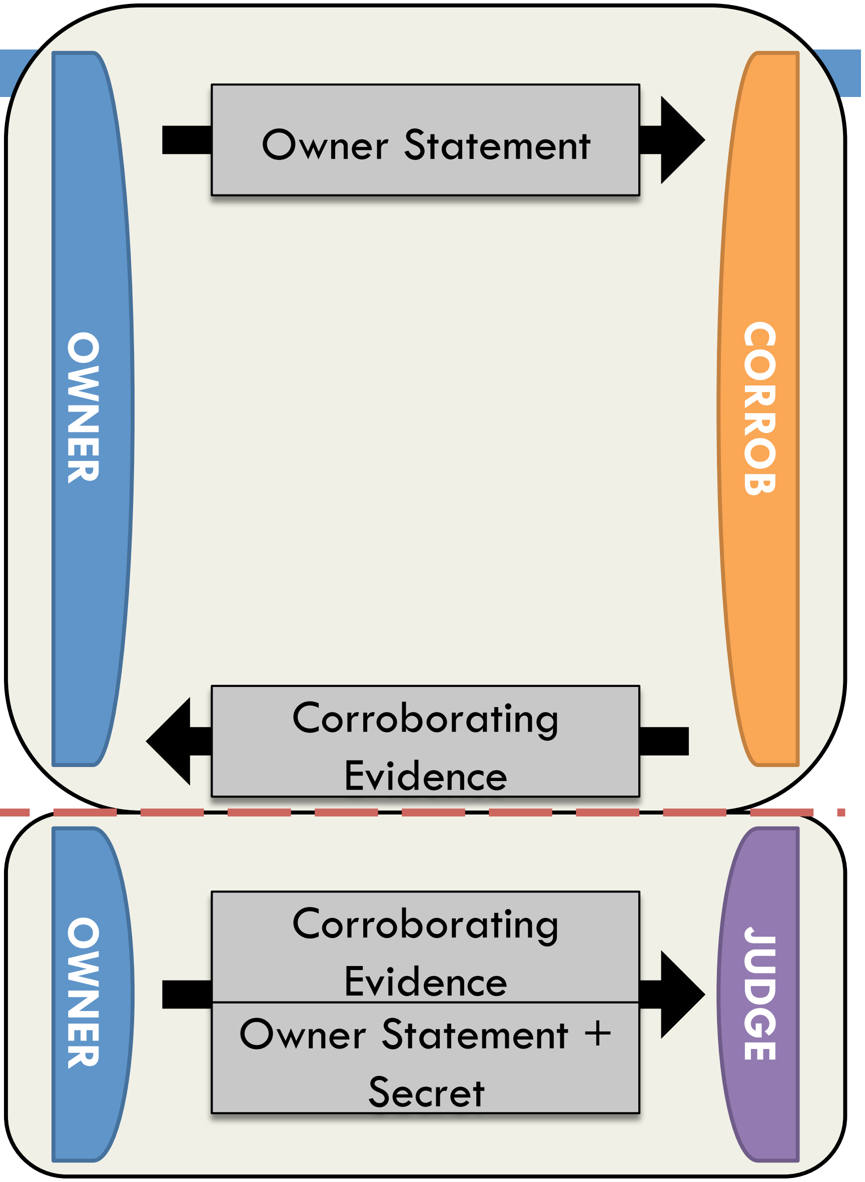
Private Corroborator Scheme

- Limitations of Public Corroborator Scheme
  - Corroborator must reveal identity during creation
- Naïve solutions to this problem
  - Corroborator decides at creation time?
    - usability nightmare
  - Corroborator maintains state until owner claims alibi?
    - misaligned incentives

Review: Public Corroborator Scheme

1) Alibi Creation

Owner learns corroborator's identity



2) Alibi Verification

Private Corroborator Scheme

1) Alibi Creation

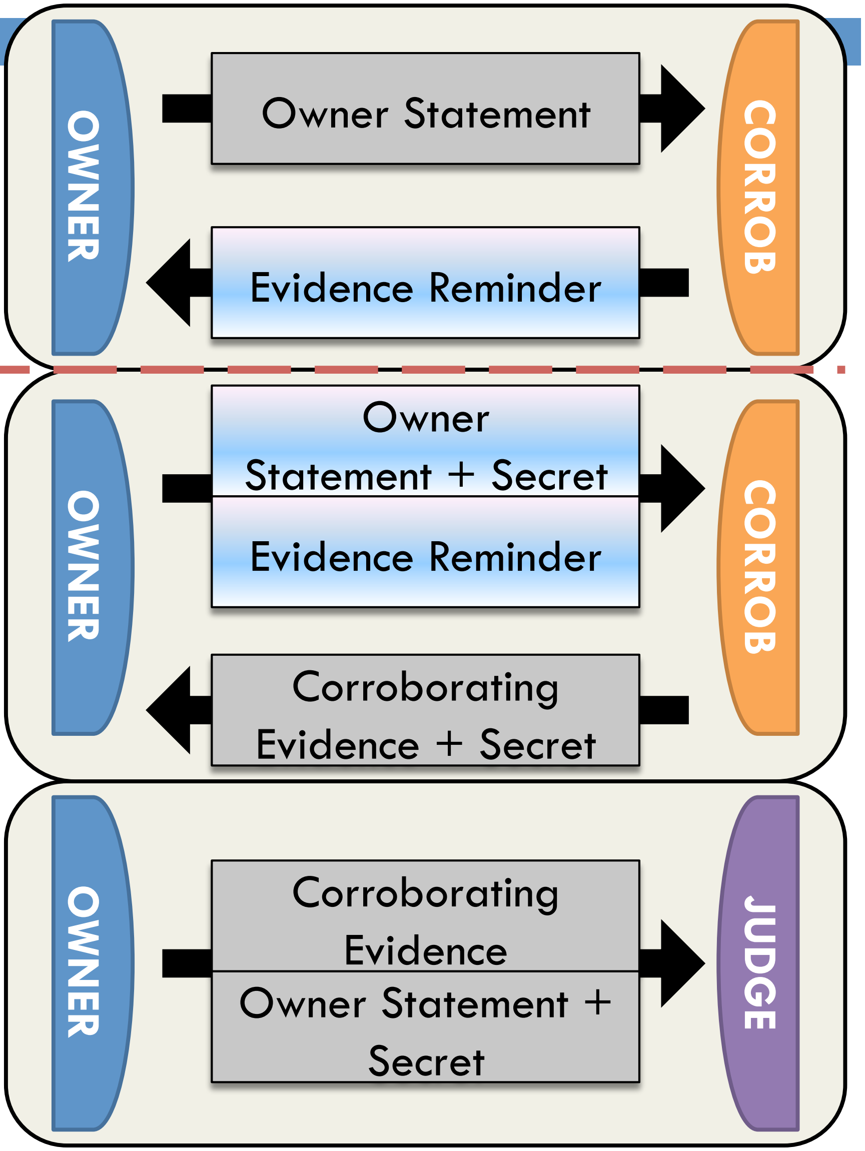
- Neither identity revealed

2) Alibi Corroboration

- Both must choose to participate

3) Alibi Verification

- Same as public scheme



Private Corroborator Scheme

- New requirement: anonymous messaging system*
  - Only for message delivery, not our security/privacy properties
- Owner contacts corroborator to obtain corroboration before claiming an alibi

* E.g. SMILE [Manweiler, Scudellari, Cox. CCS 2009]

Advantages over Traditional Alibis

- Alibi owner's consent required to
  - Create alibi
  - Reveal identity
- Alibis are unambiguous, nontransferrable
- Owner can't fabricate corroboration without the corroborator's participation
- Corroborator can't fabricate an alibi without the owner's participation

Limitations Shared with Traditional Alibis

- Some forms of perjury
  - Alibi owner and alibi corroborator collude
  - Someone makes alibi on owner's behalf (sharing of private key/device)

Conclusion

- Privacy-preserving alibi systems
  - Privacy not compromised when creating alibis
- Efficient design and implementation for mobile devices
  - Fast, small for alibi owners
  - Stateless for alibi corroborators