Welcome

- About this adventure:
  github.com/CuboCyberSecurity

- Consider all these modules as an introduction and as a way of sharing some key ideas (some *puzzle pieces*).

- It is a *free version* training:
  - Incomplete and imprecise information.
  - If you get confused, do not run away and make your own interpretations.

- Eventually, I’m going to share a much more complete and clear picture on the Wiki.

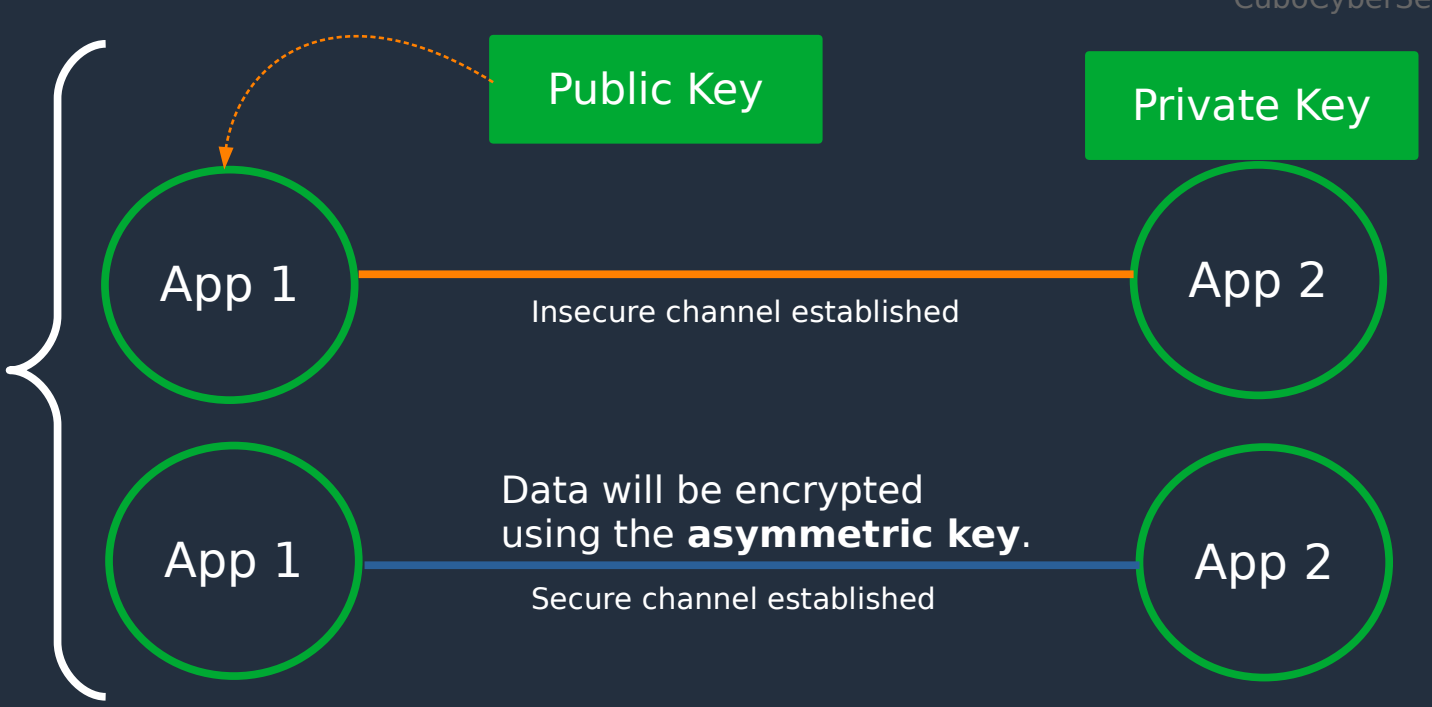
Module 4

- Cryptology
- Data Security
- Access Control
- Threat Modeling

Step 1

Asymmetric Cryptography

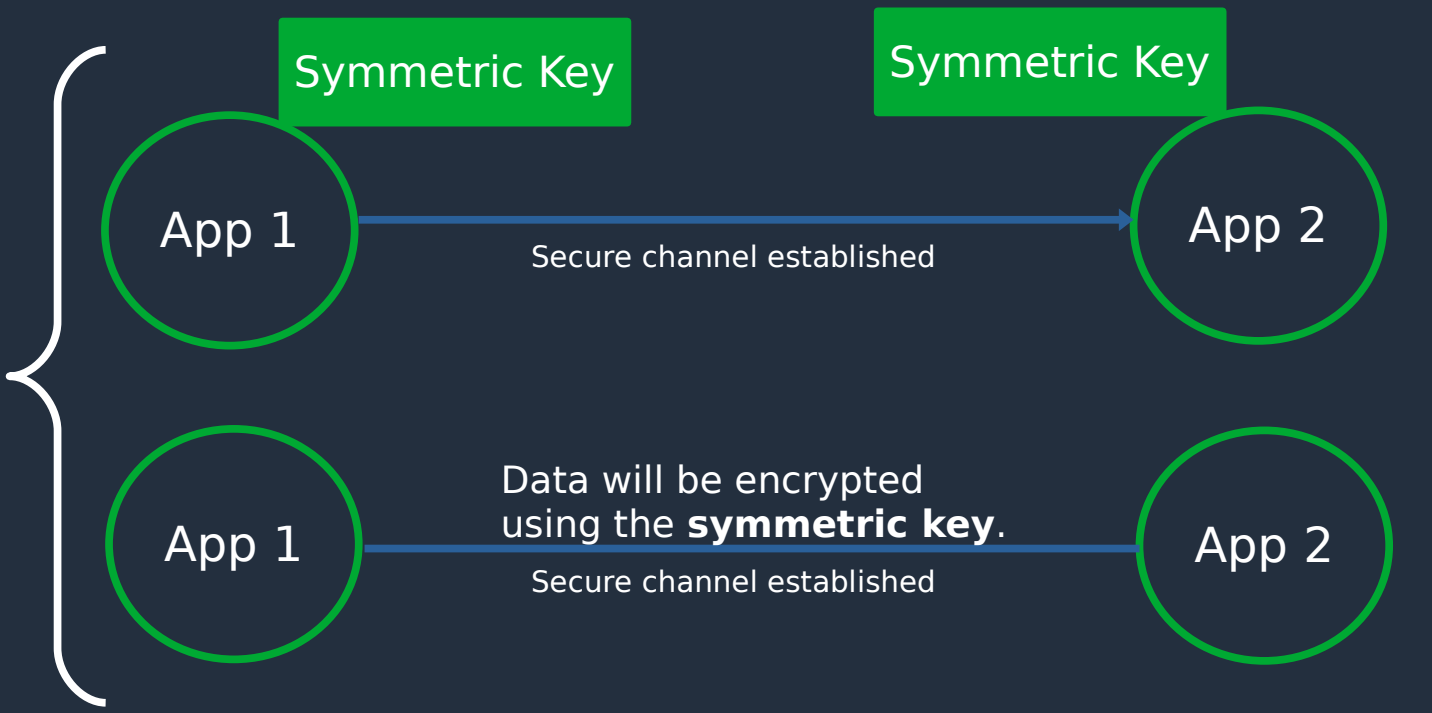
It's a "slower" process

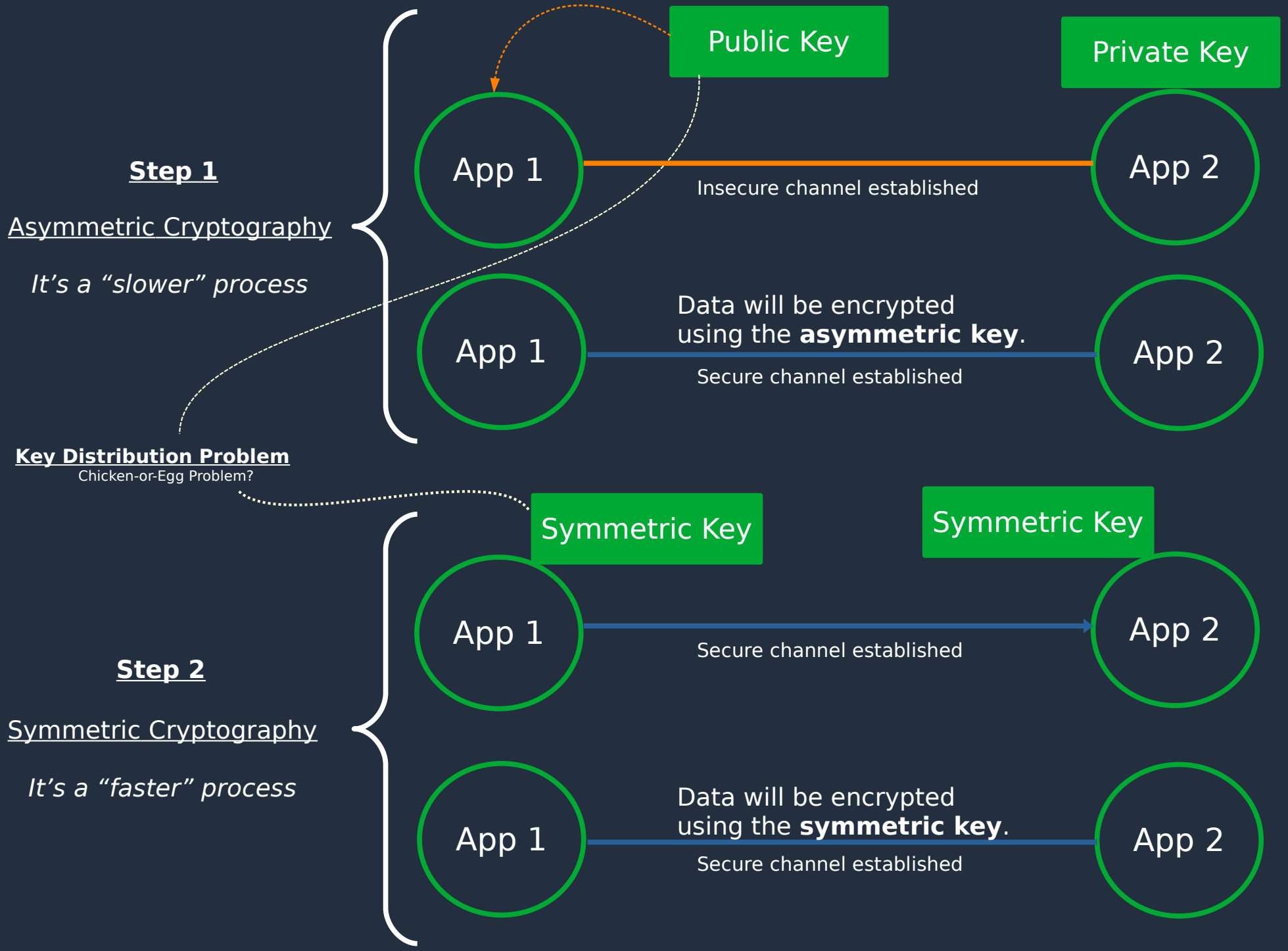


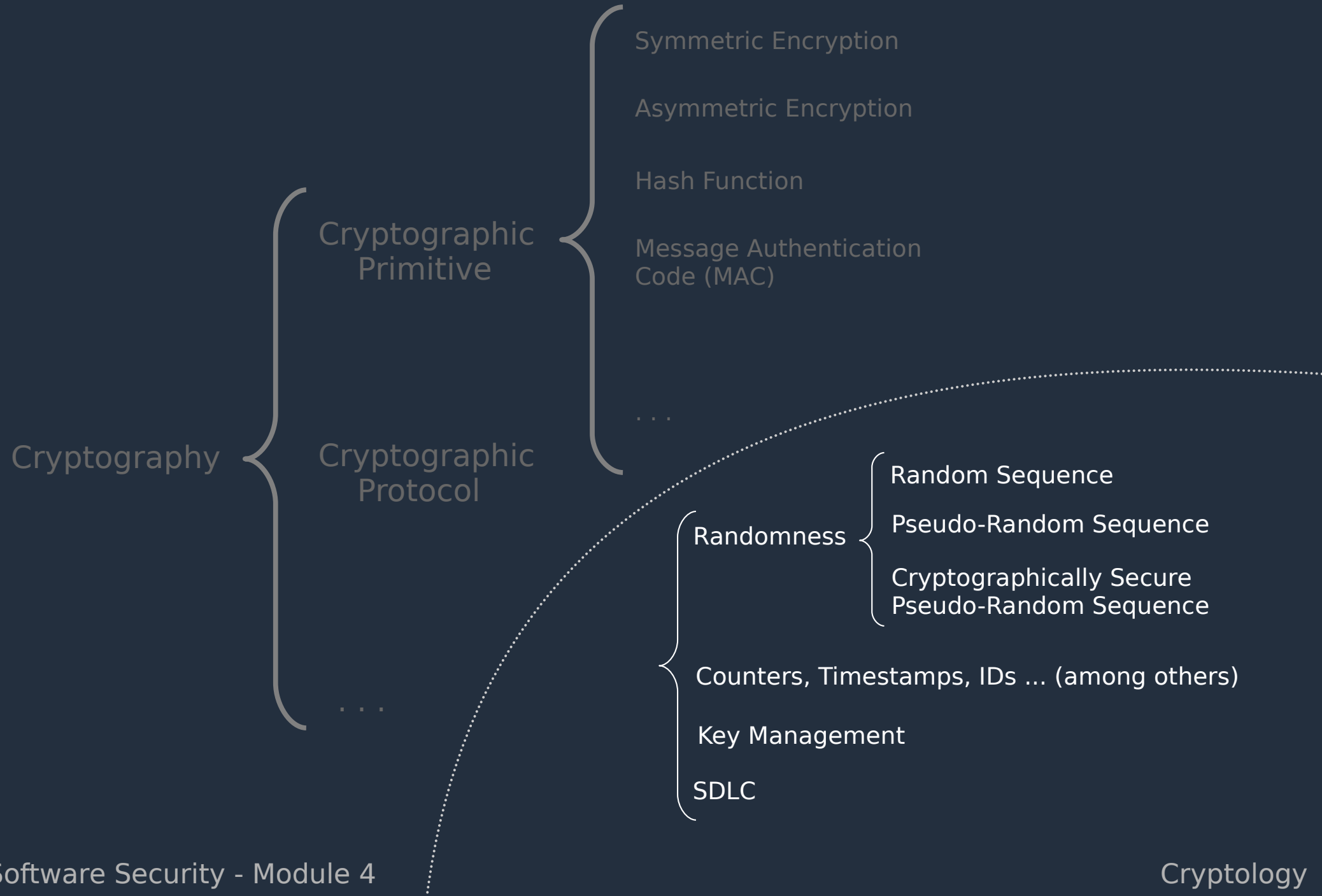
Step 2

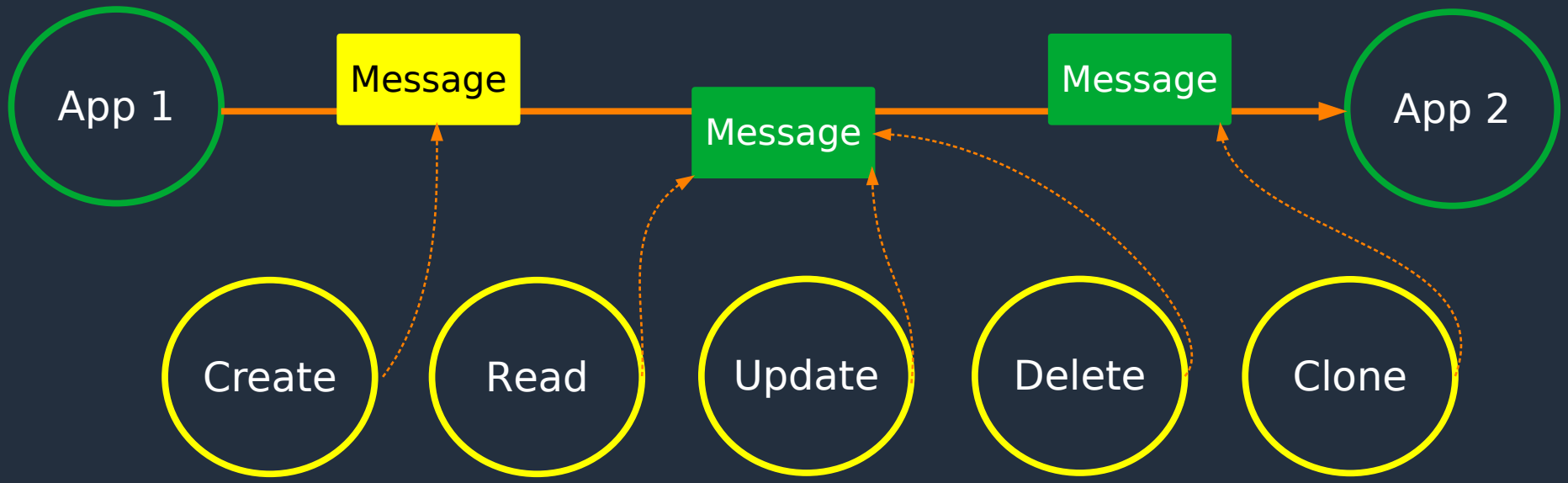
Symmetric Cryptography

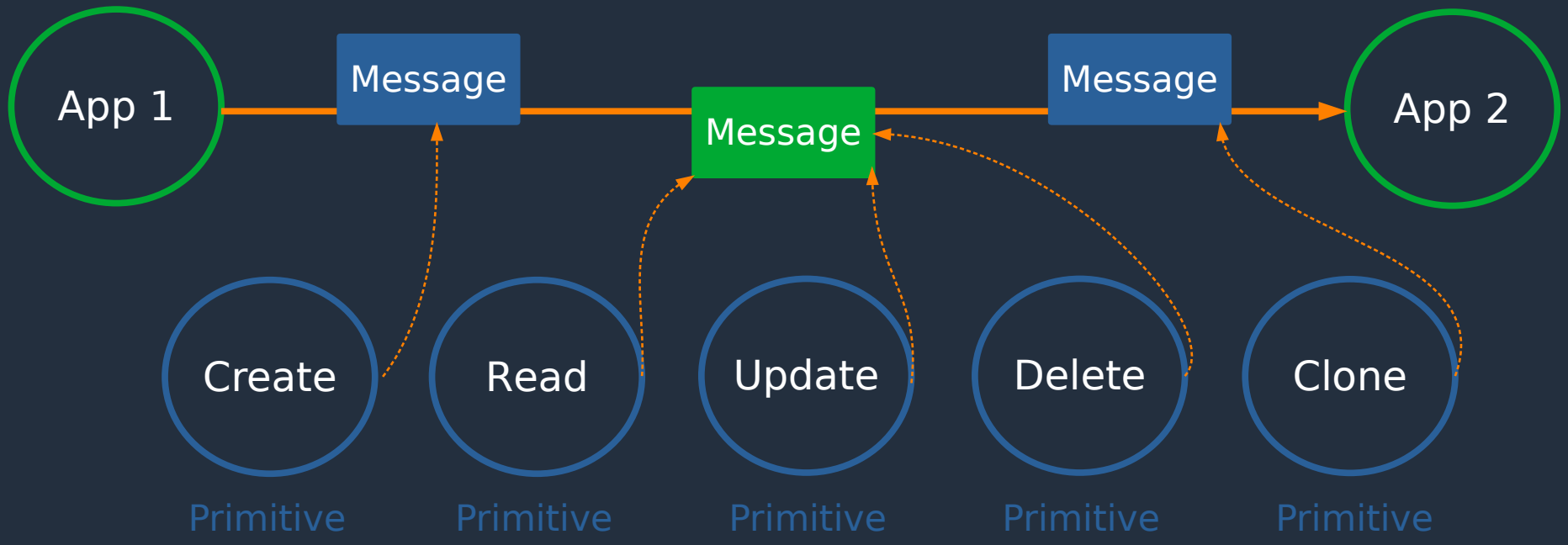
It's a "faster" process




Public Key
Private Key
Step 1
Asymmetric Cryptography
It's a "slower" process
App 1
App 2
Insecure channel established
App 1
Data will be encrypted
using the asymmetric key.
App 2
Secure channel established
Key Distribution Problem
Chicken-or-Egg Problem?
Symmetric Key
Symmetric Key
Step 2
Symmetric Cryptography
It's a "faster" process
App 1
App 2
Secure channel established
App 1
Data will be encrypted
using the symmetric key.
App 2
Secure channel established

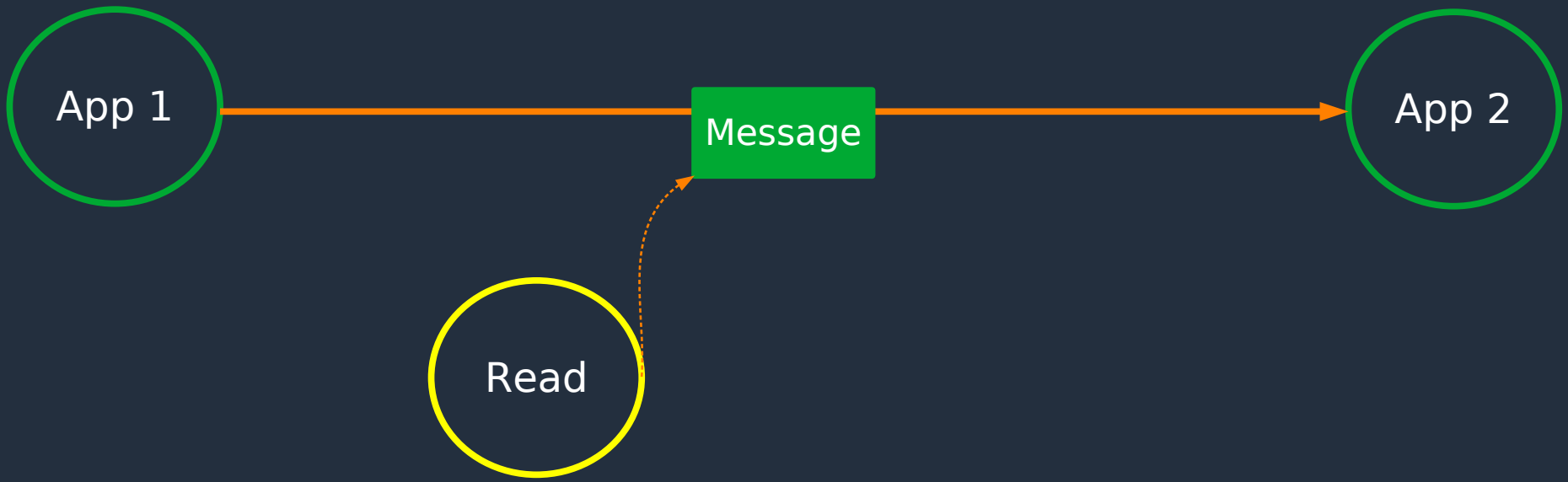

Cryptography
Cryptographic Primitive
Symmetric Encryption
Asymmetric Encryption
Hash Function
Message Authentication Code (MAC)
. . .
Cryptographic Protocol
Randomness
Random Sequence
Pseudo-Random Sequence
Cryptographically Secure Pseudo-Random Sequence
Counters, Timestamps, IDs ... (among others)
Key Management
SDLC
. . .


App 1
Message
Message
Message
App 2
Create
Read
Update
Delete
Clone



Task

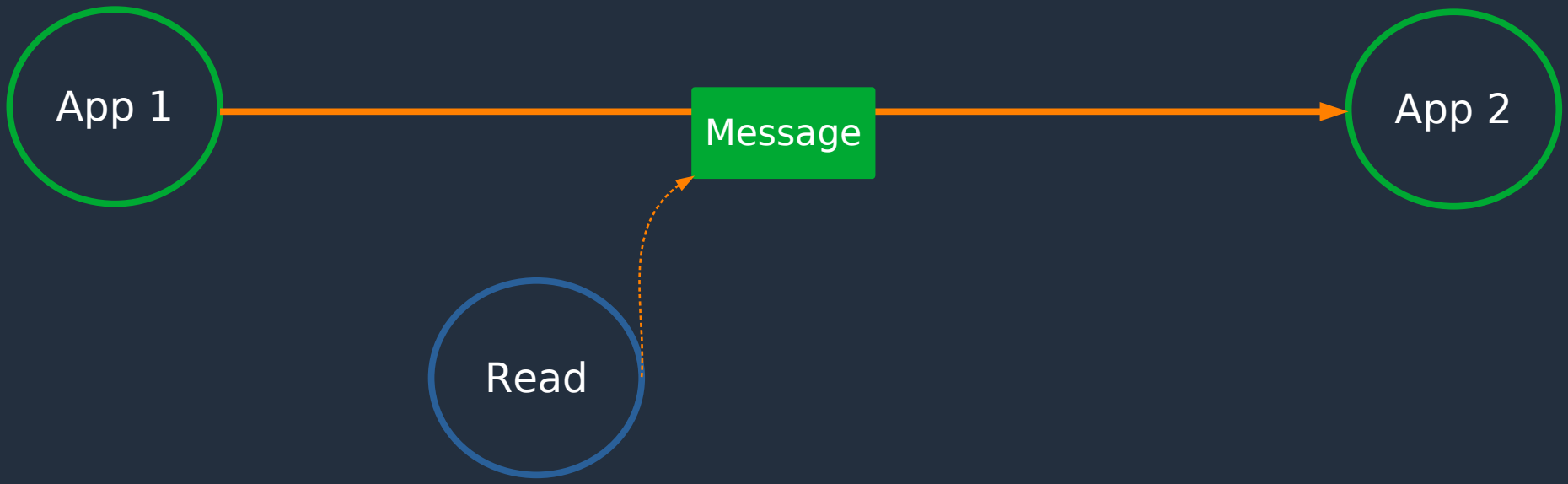
Use Cryptographic Primitives to mitigate these threats.

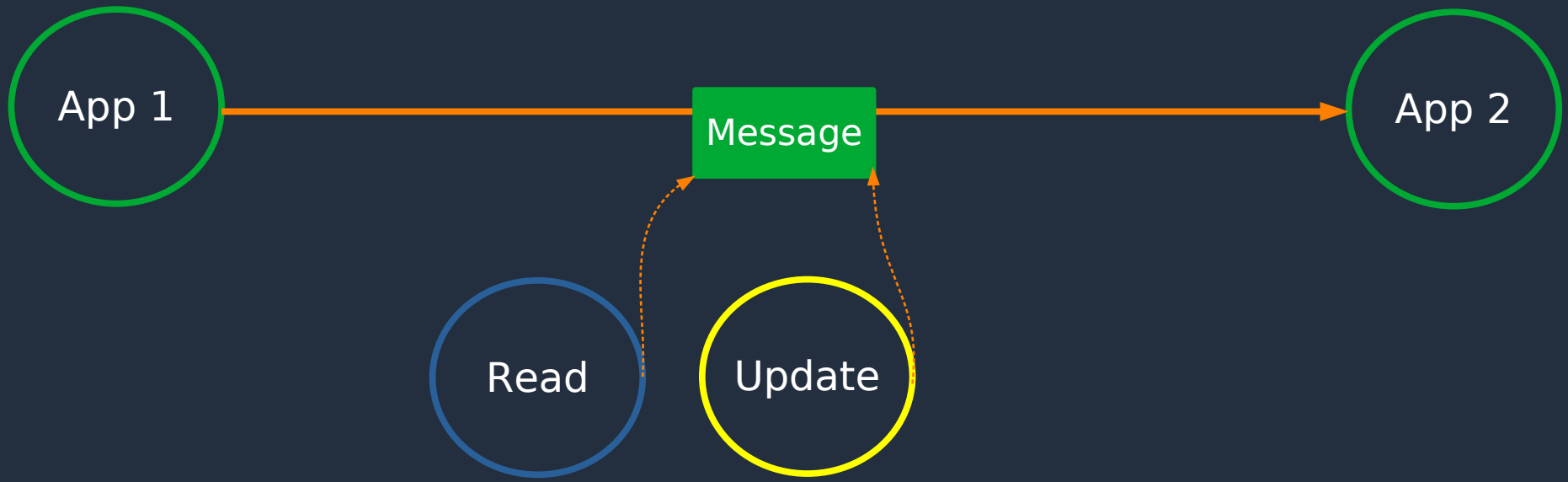


Threat
Read.

Reason
Confidentiality Violation.

Mitigation
Symmetric Encryption **?**

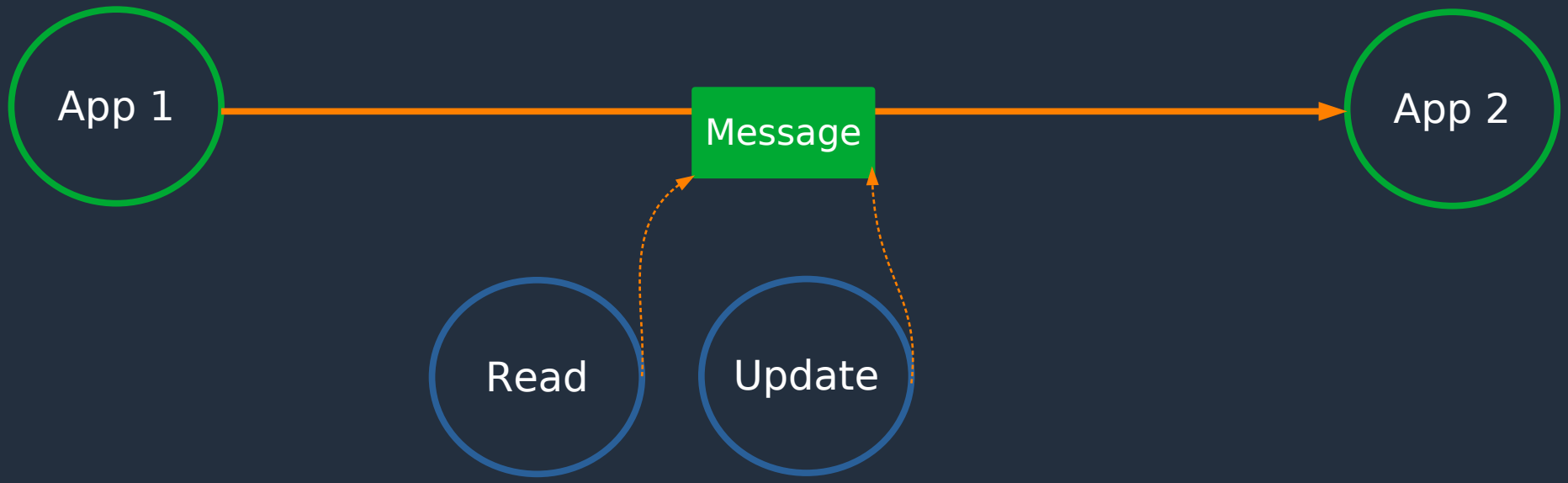

App 1
Message
App 2
Read

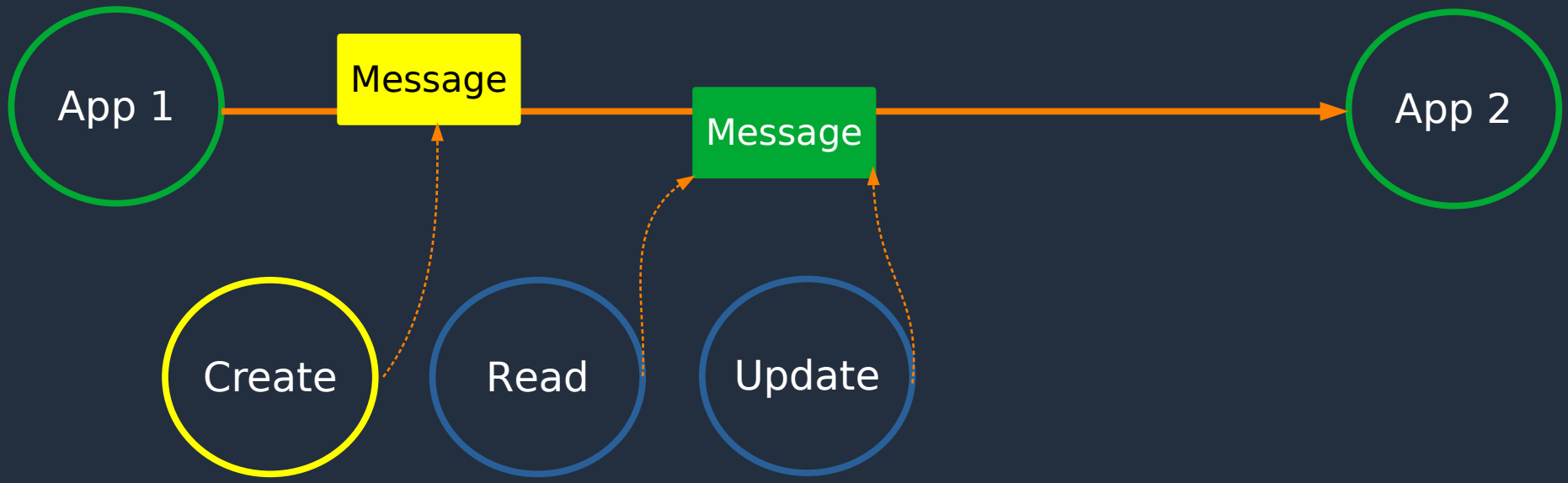


Threat
Update.

Reason
Integrity Violation.

Mitigation
Hash Function **?**
Message Authentication Code (MAC) **?**


App 1
Message
App 2
Read
Update



Threat

Create.

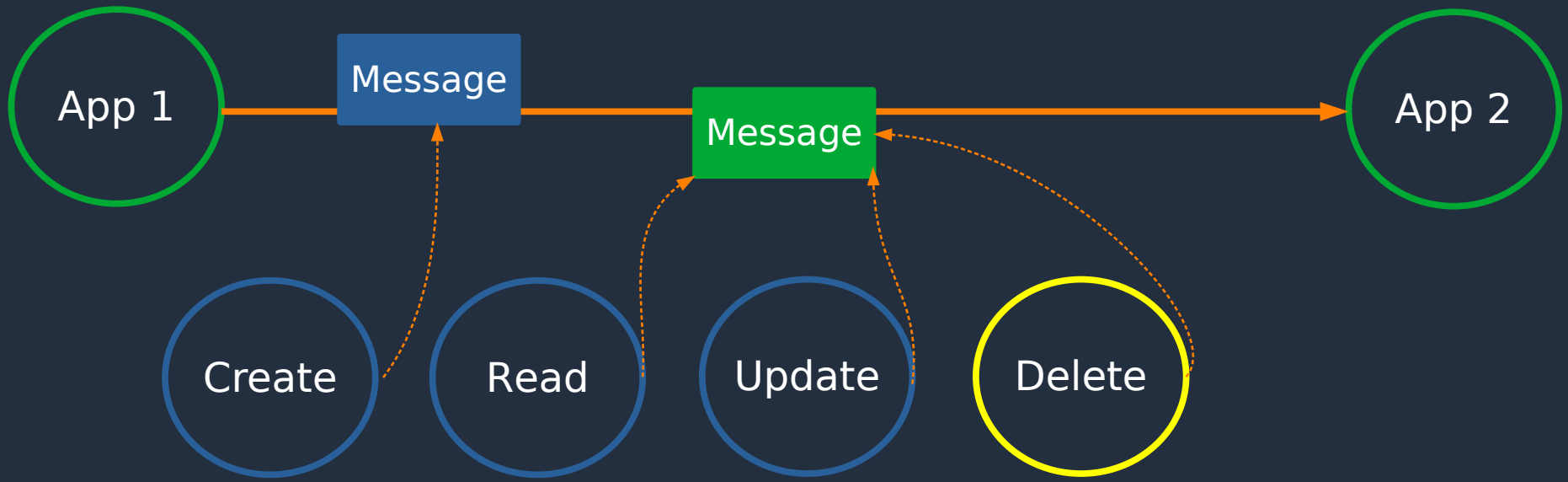
Reason

Authentication Violation.

Mitigation

MAC + counter **?**

Signature **?**



Threat

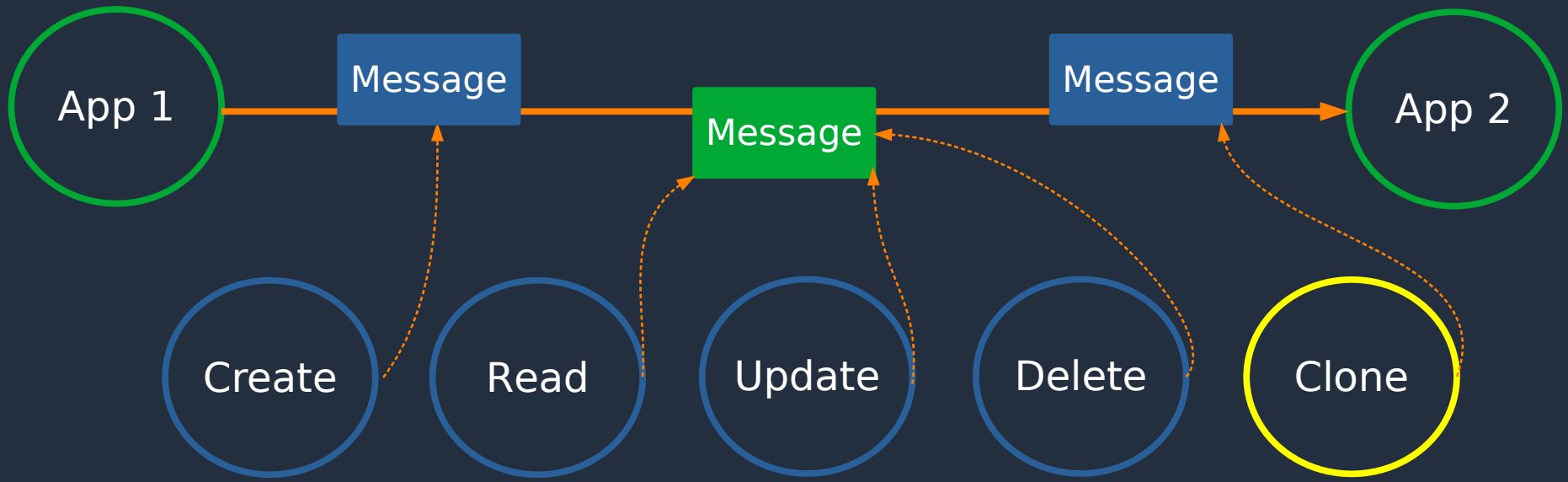
Delete.

Reason

Integrity Violation.
Availability Violation.

Mitigation

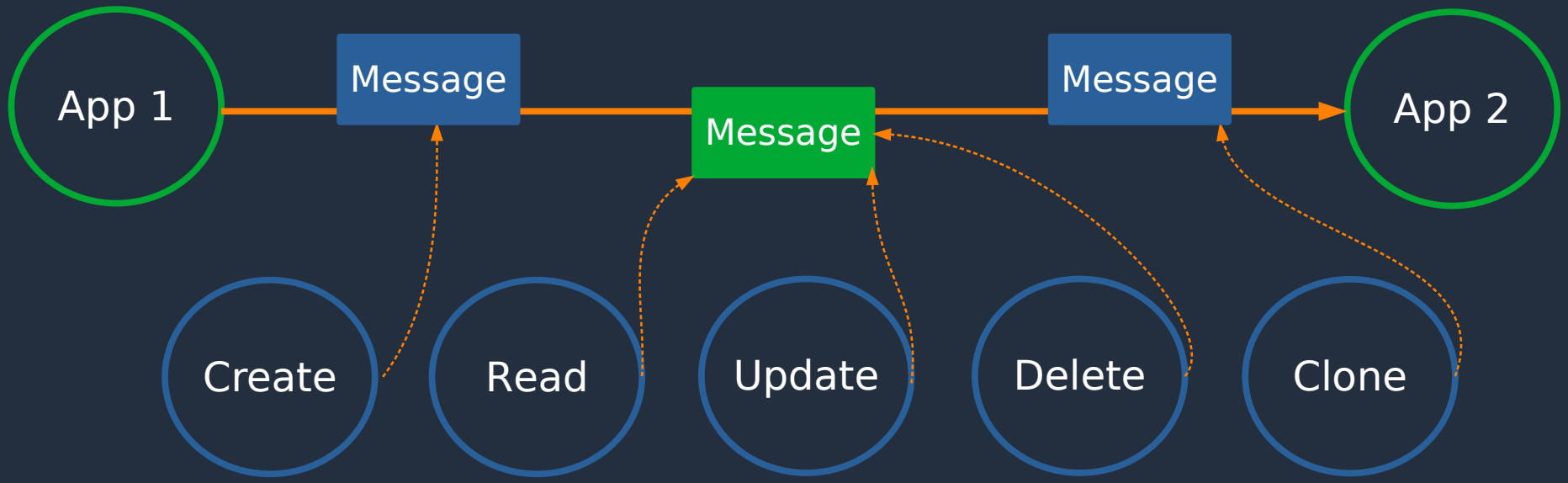
MAC + Counter + more **?**

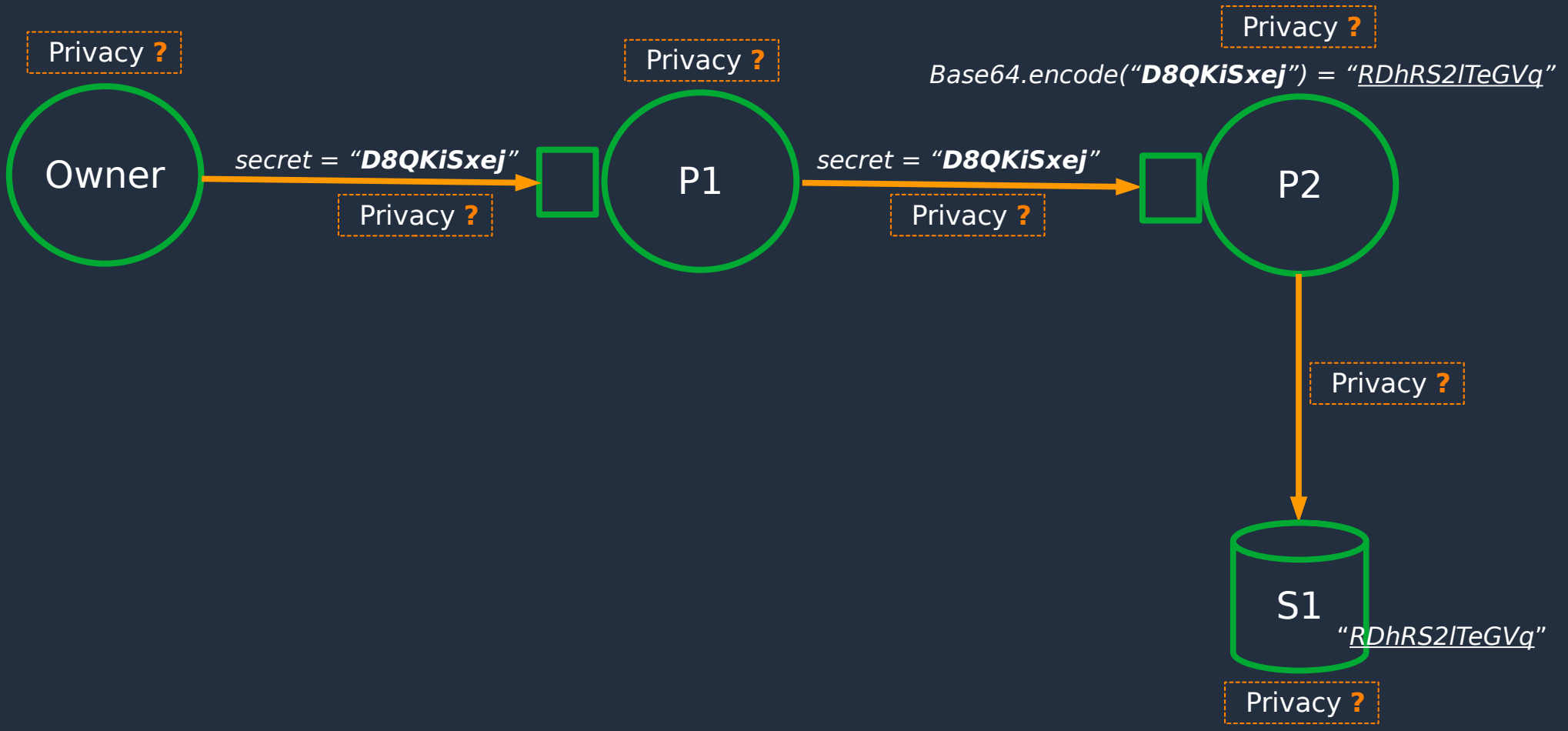


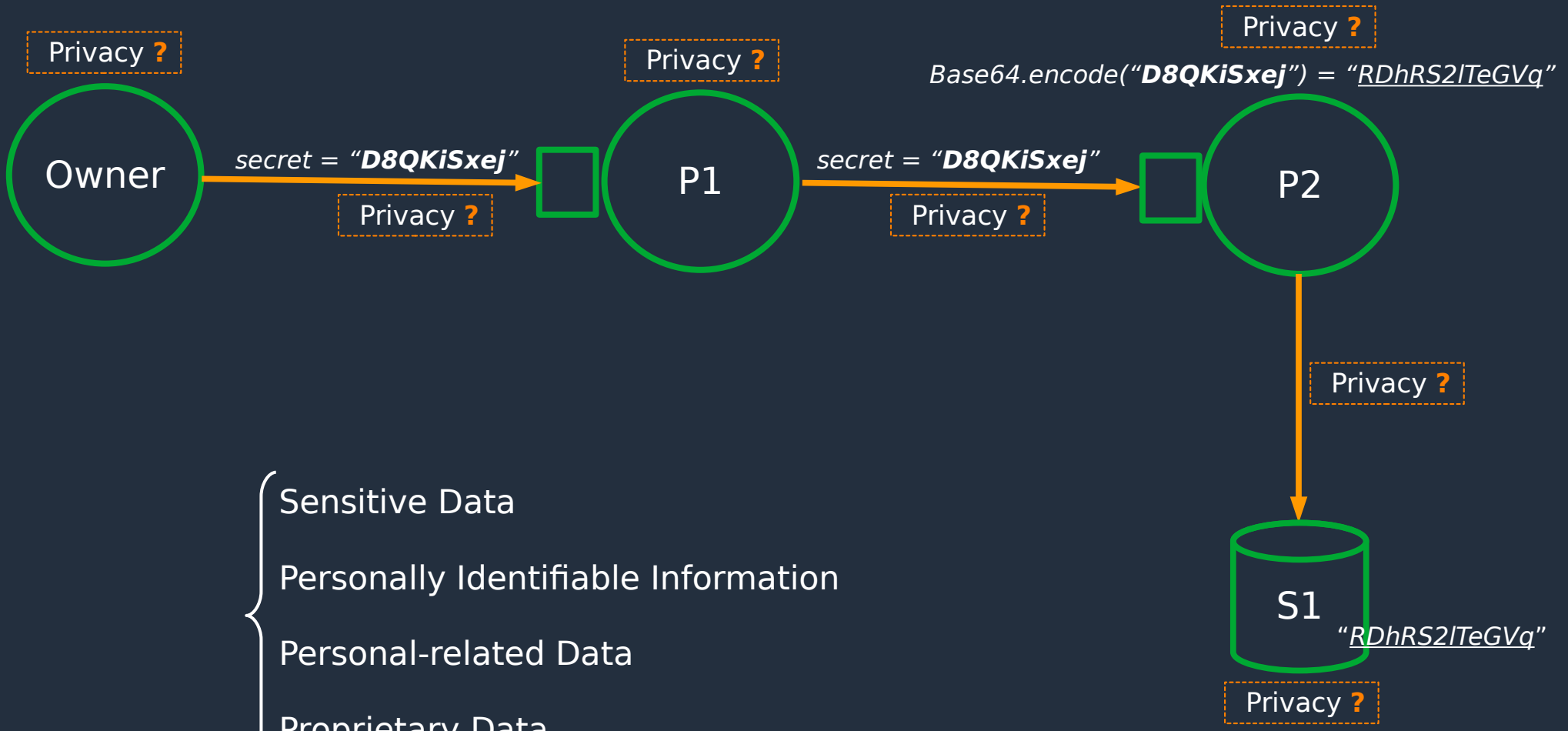
Threat
Clone.

Reason
Non-Repudiation Violation.

Mitigation
MAC + Counter **?**

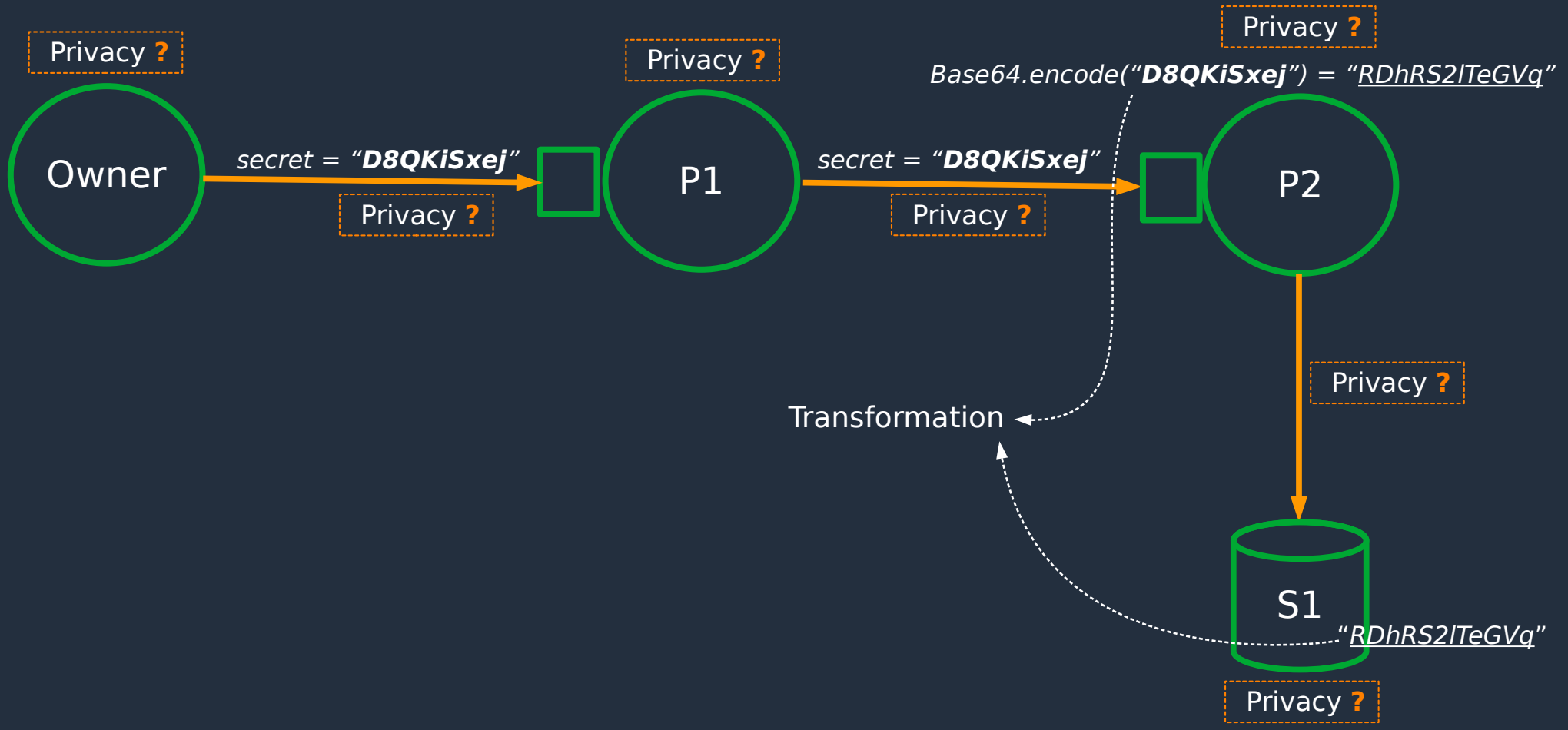

App 1
Message
Message
Message
App 2
Create
Read
Update
Delete
Clone

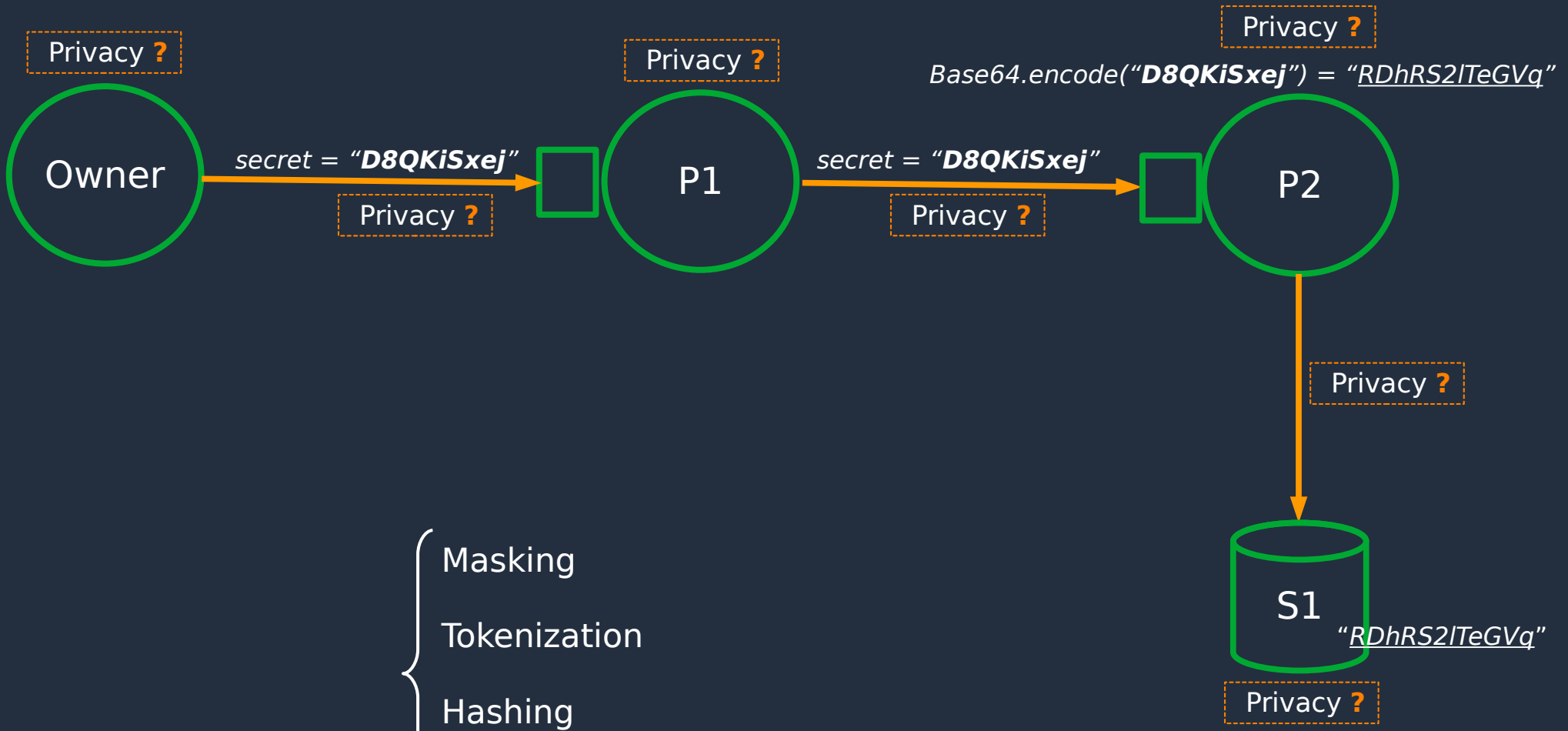

Privacy ?
Owner
secret = "D8QKiSxej"
Privacy ?
Privacy ?
P1
secret = "D8QKiSxej"
Privacy ?
Privacy ?
Base64.encode("D8QKiSxej") = "RDhRS2lTeGVq"
P2
Privacy ?
S1
"RDhRS2lTeGVq"
Privacy ?



- Sensitive Data
- Personally Identifiable Information
- Personal-related Data
- Proprietary Data

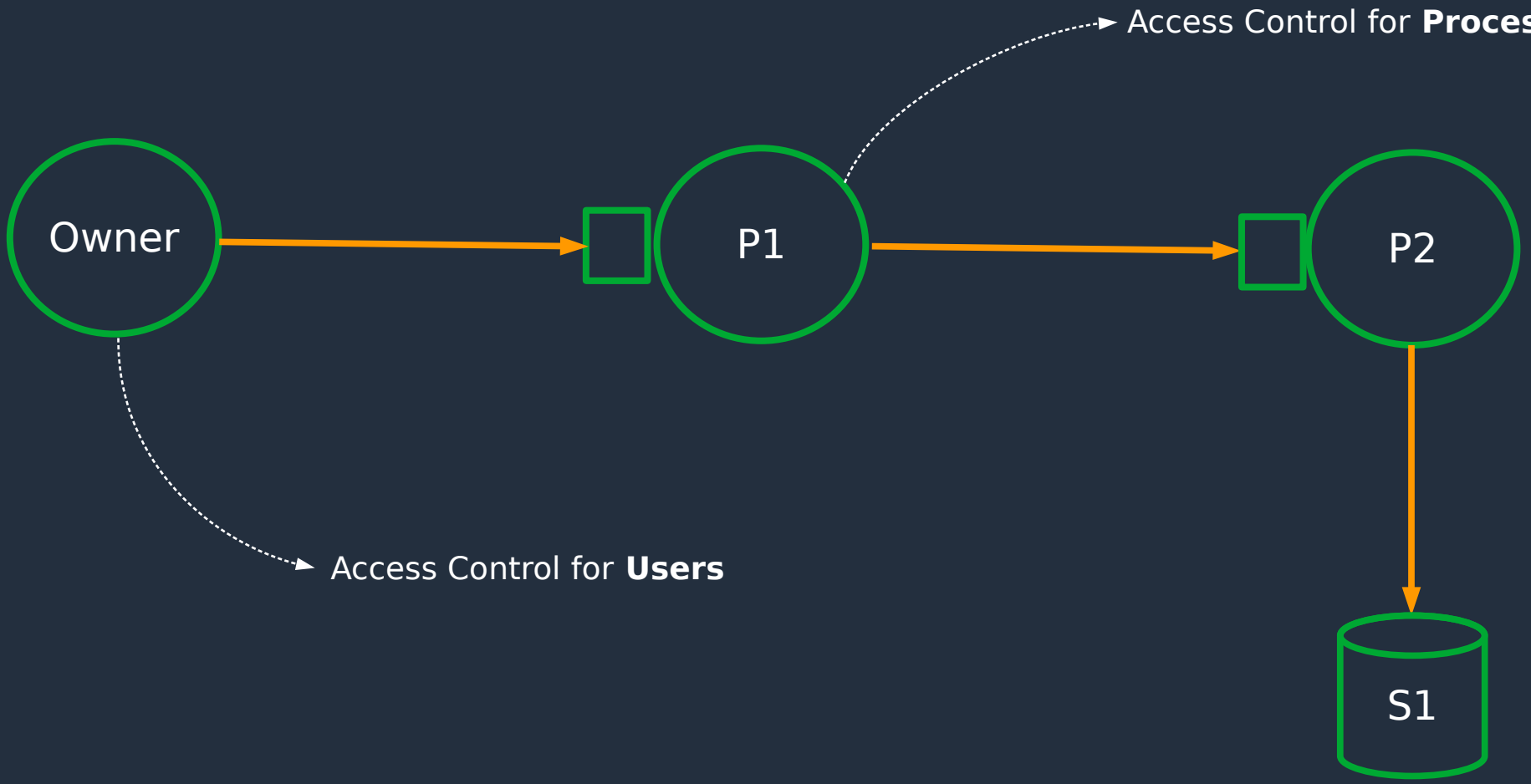
... "Mind Mapping Chaos" ...

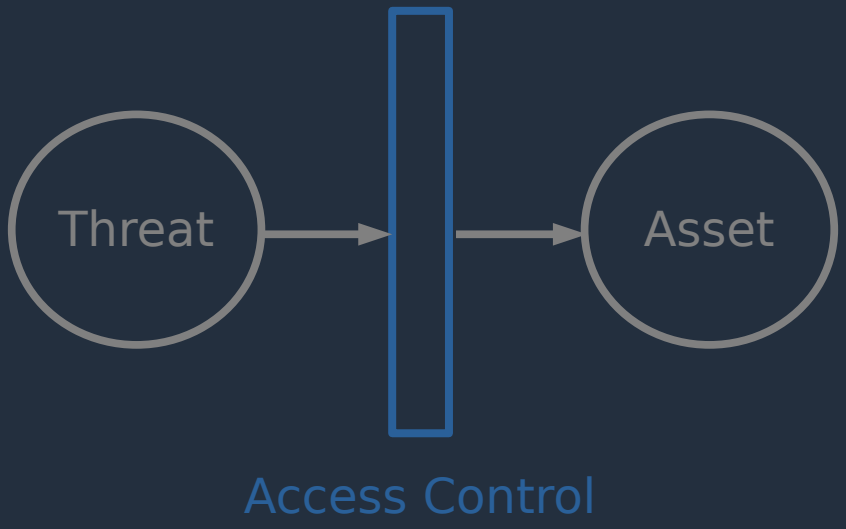

Privacy ?
Owner
secret = "D8QKiSxej"
Privacy ?
Privacy ?
P1
secret = "D8QKiSxej"
Privacy ?
Privacy ?
Base64.encode("D8QKiSxej") = "RDhRS2lTeGVq"
P2
Privacy ?
Transformation
S1
"RDhRS2lTeGVq"
Privacy ?

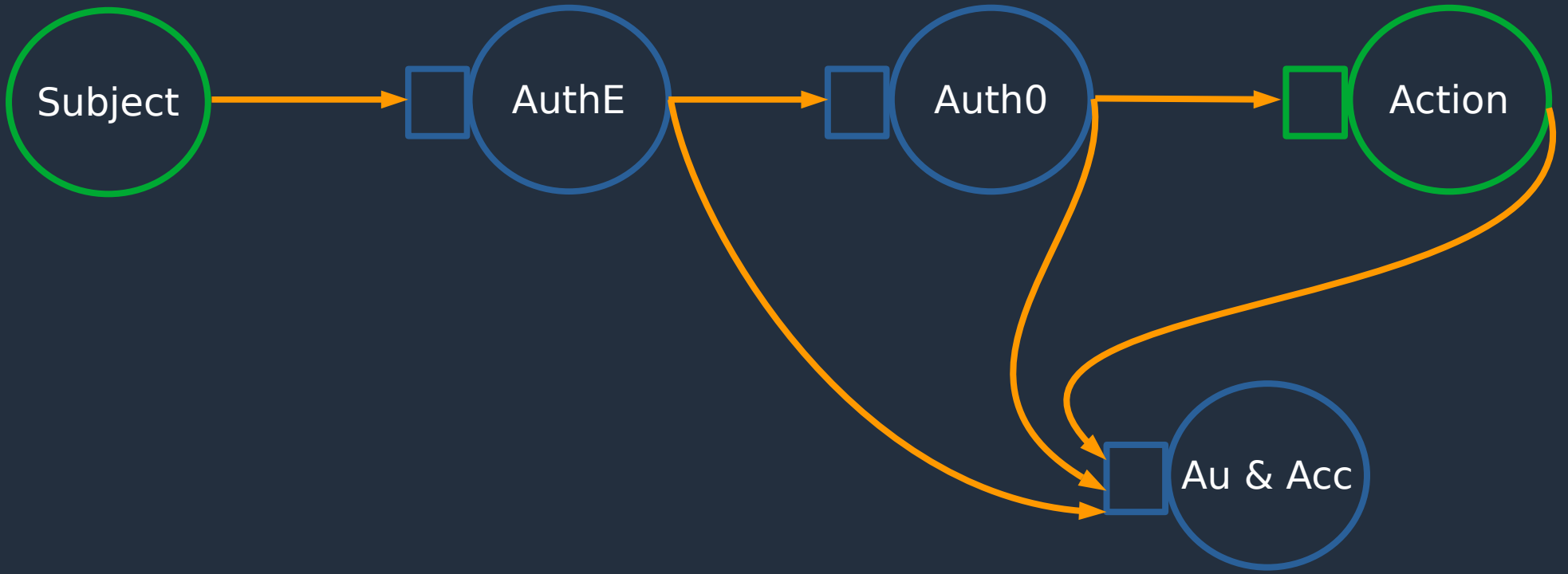


- Masking
- Tokenization
- Hashing
- Format-Preserving "Encryption"

... ? ...


Access Control for **Processes**
Owner
P1
P2
Access Control for **Users**
S1


Threat
Asset
Access Control


Subject
AuthE
Auth0
Action
Au & Acc

Security Framework – Access Control

1) **Identification**

… *“Creating Subject's Identity”* …

2) **Authentication**

… *“Verifying Identity”* …

3) **Authorization**

… *“Verifying Permissions”* …

4) **Auditing**

… *“Monitoring”* …

5) **Accountability**

… *“Saving evidence”* …

	NIST Framework				
Asset_Name	Identify	Protect	Detect	Respond	Recover
C ~~R U D~~					
~~C~~ ***R*** ~~U D~~					
~~C R~~ ***U*** ~~D~~					
~~C R U~~ ***D***					

Keep it simple.