Custos

Increasing Security with Secret Storage as a Service

Andy Sayler
Dirk Grunwald

TRIOS14
10/05/14

University of Colorado **Boulder**

Where do we store data today?






Trust?


PRISM

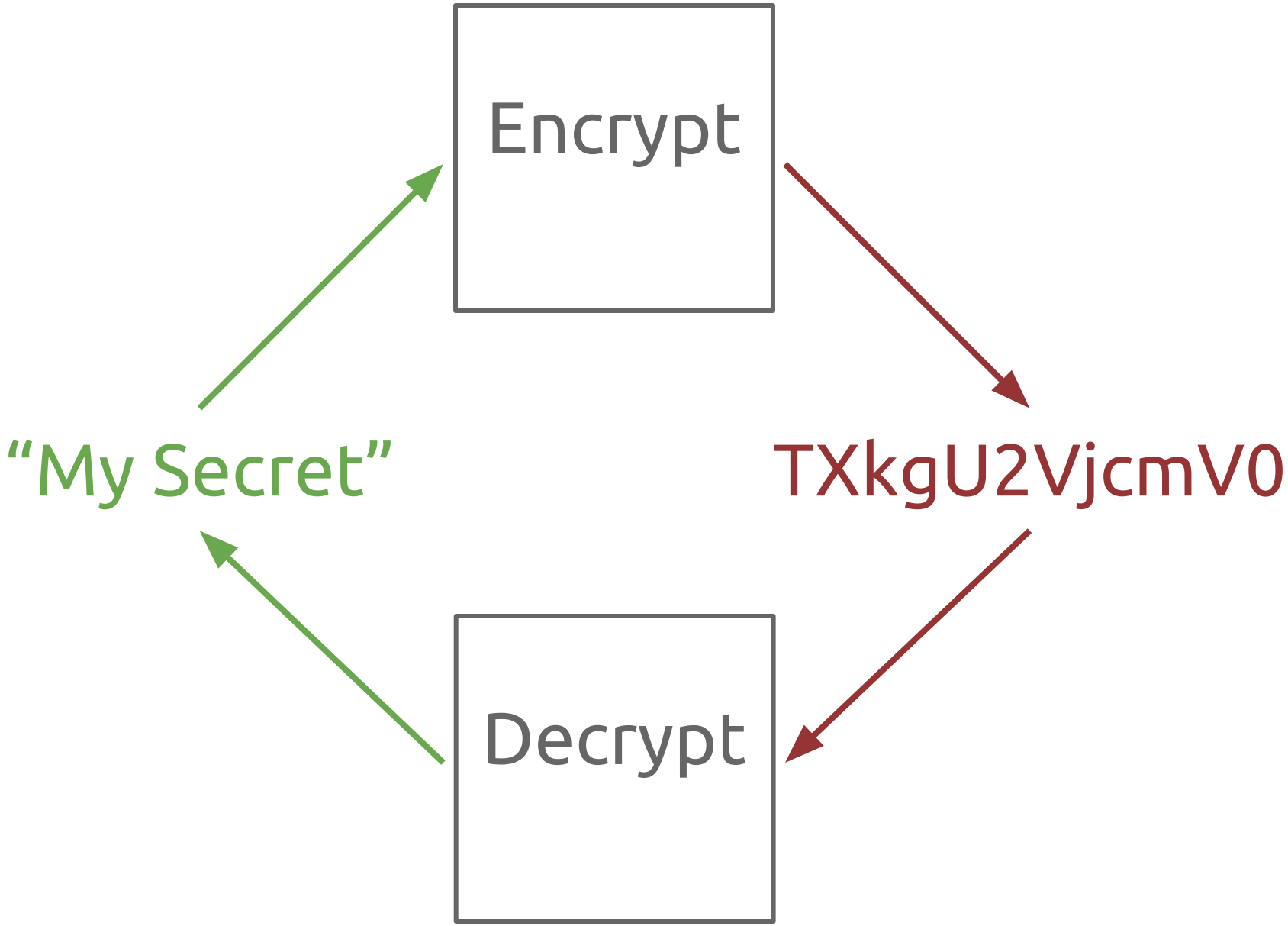
Secure?

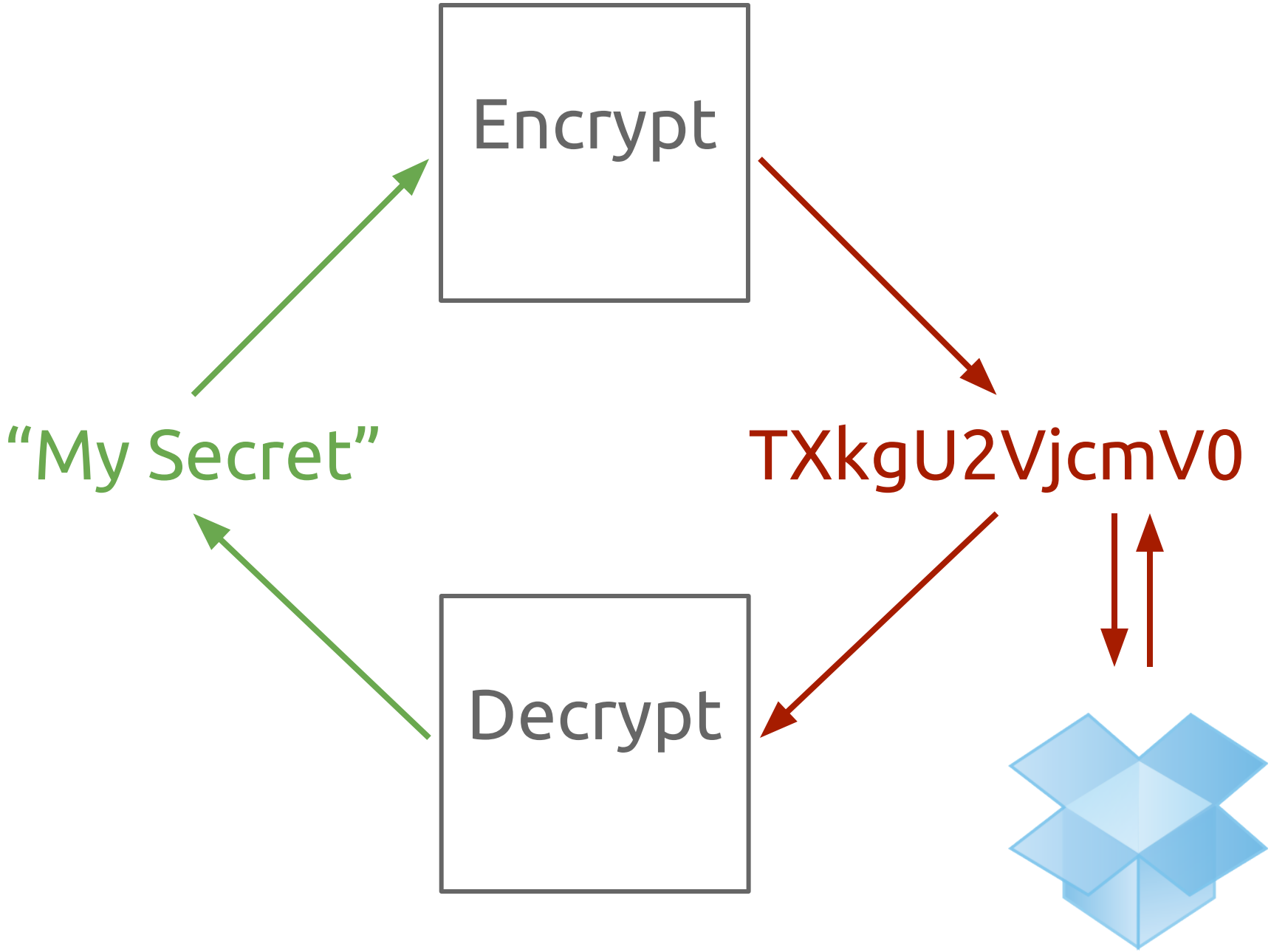
How can we control and protect our data?

How can we control and protect our data?

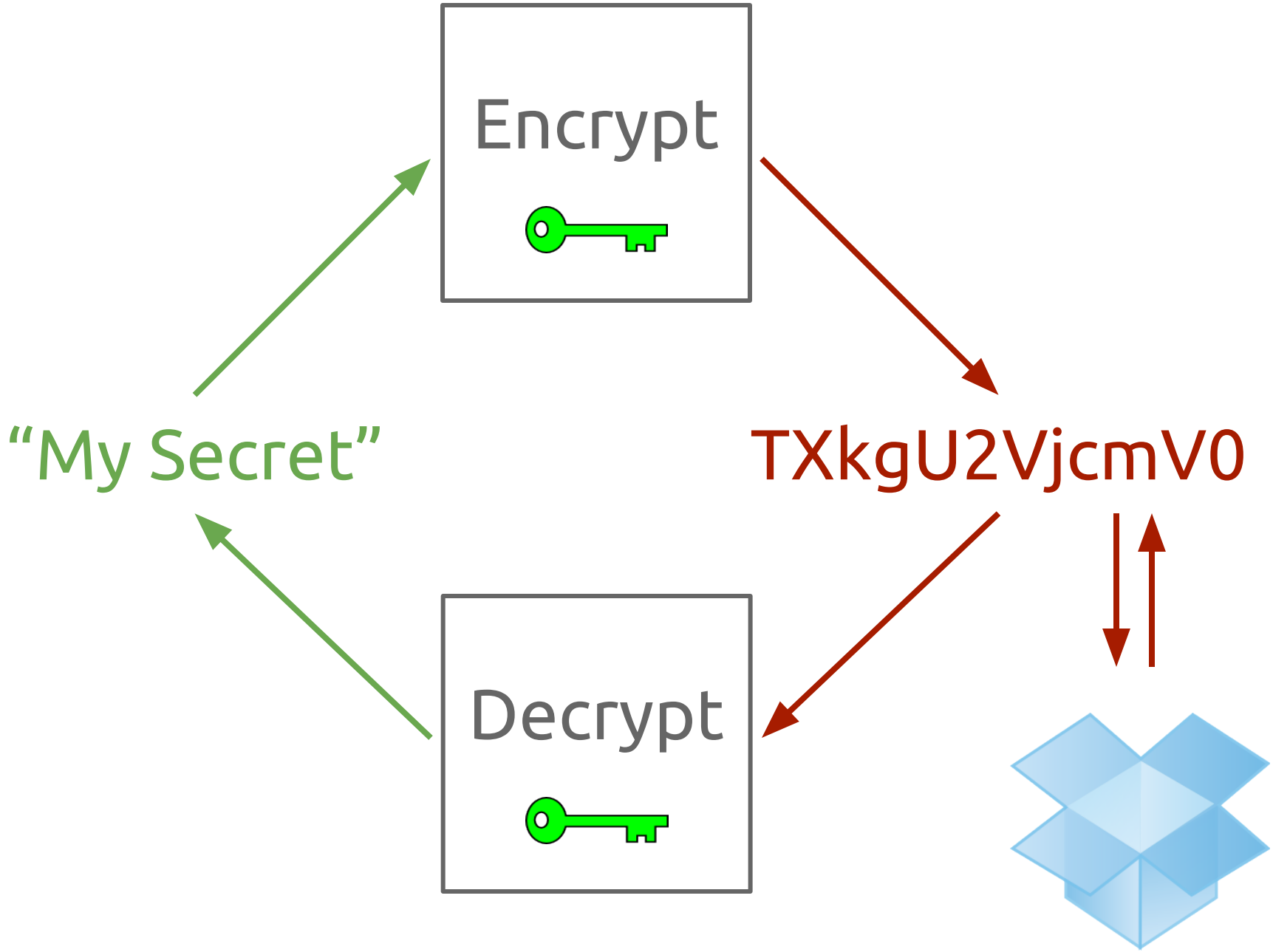
(even when storing it with third parties)

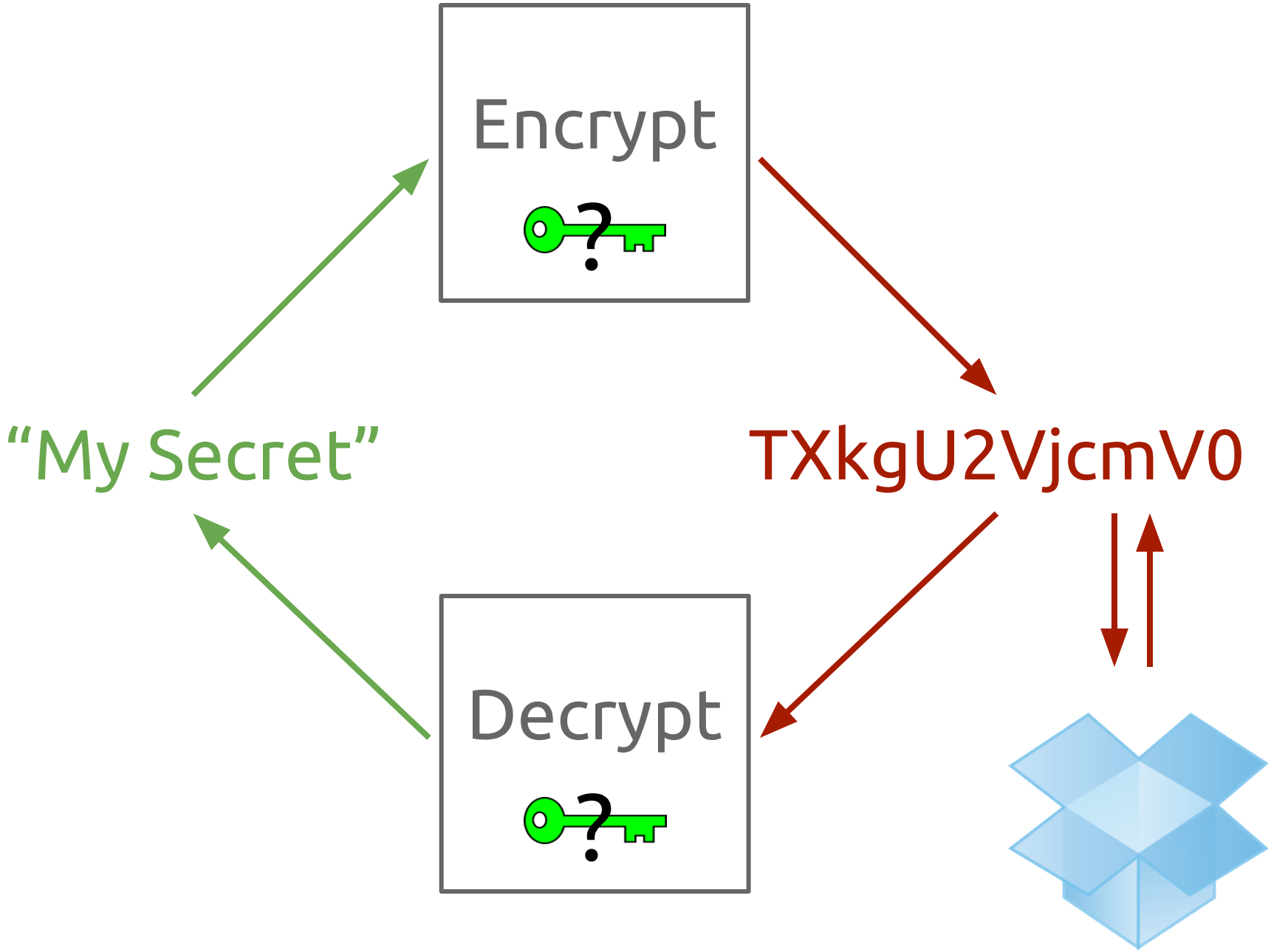
Client-Side Encryption?


Encrypt
“My Secret”
TXkgU2VjcmV0
Decrypt


Encrypt
“My Secret”
TXkgU2VjcmV0
Decrypt

But What About the Keys?


Encrypt
"My Secret"
TXkgU2VjcmV0
Decrypt


Encrypt
“My Secret”
TXkgU2VjcmV0
Decrypt

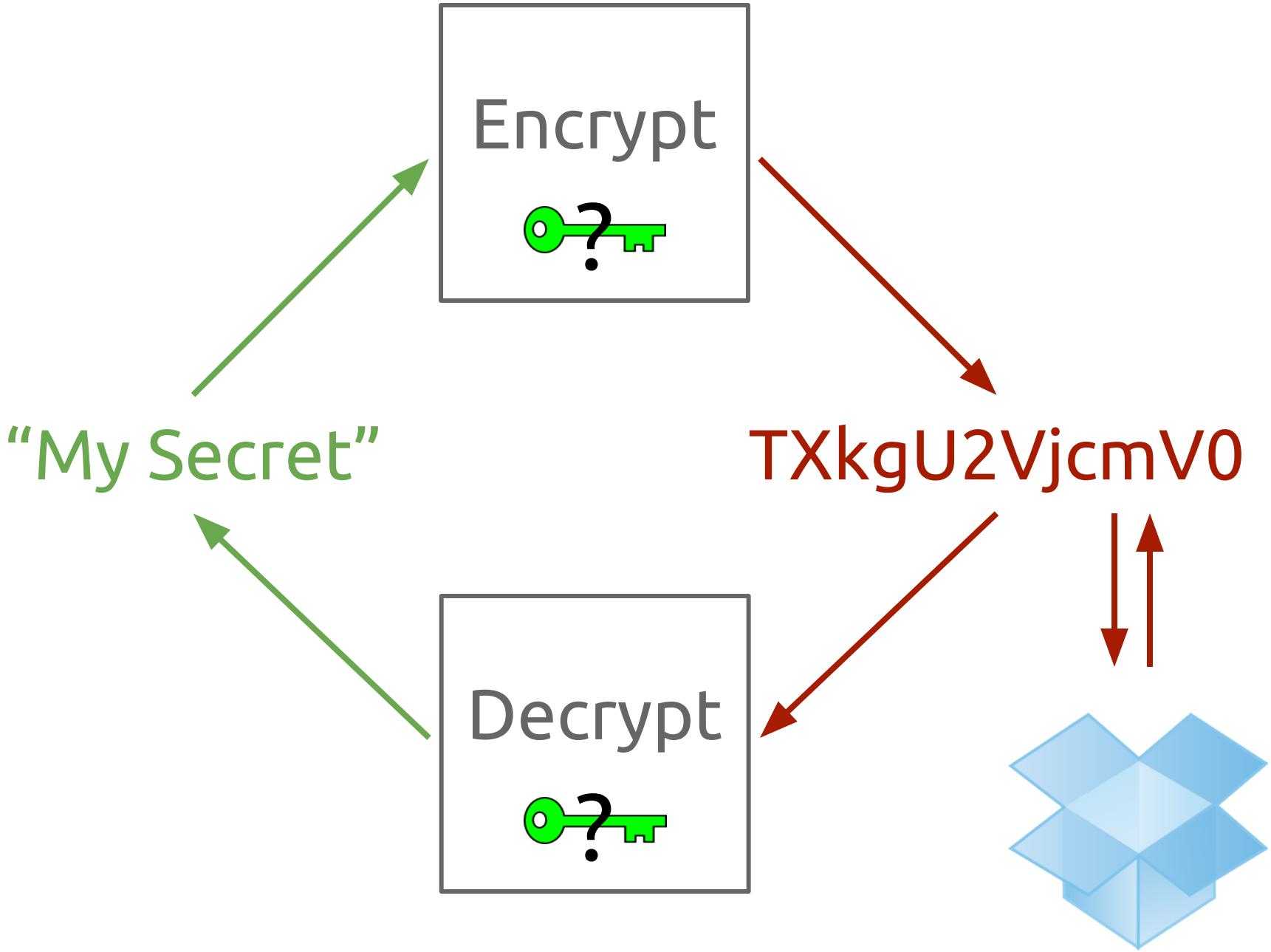
Custos

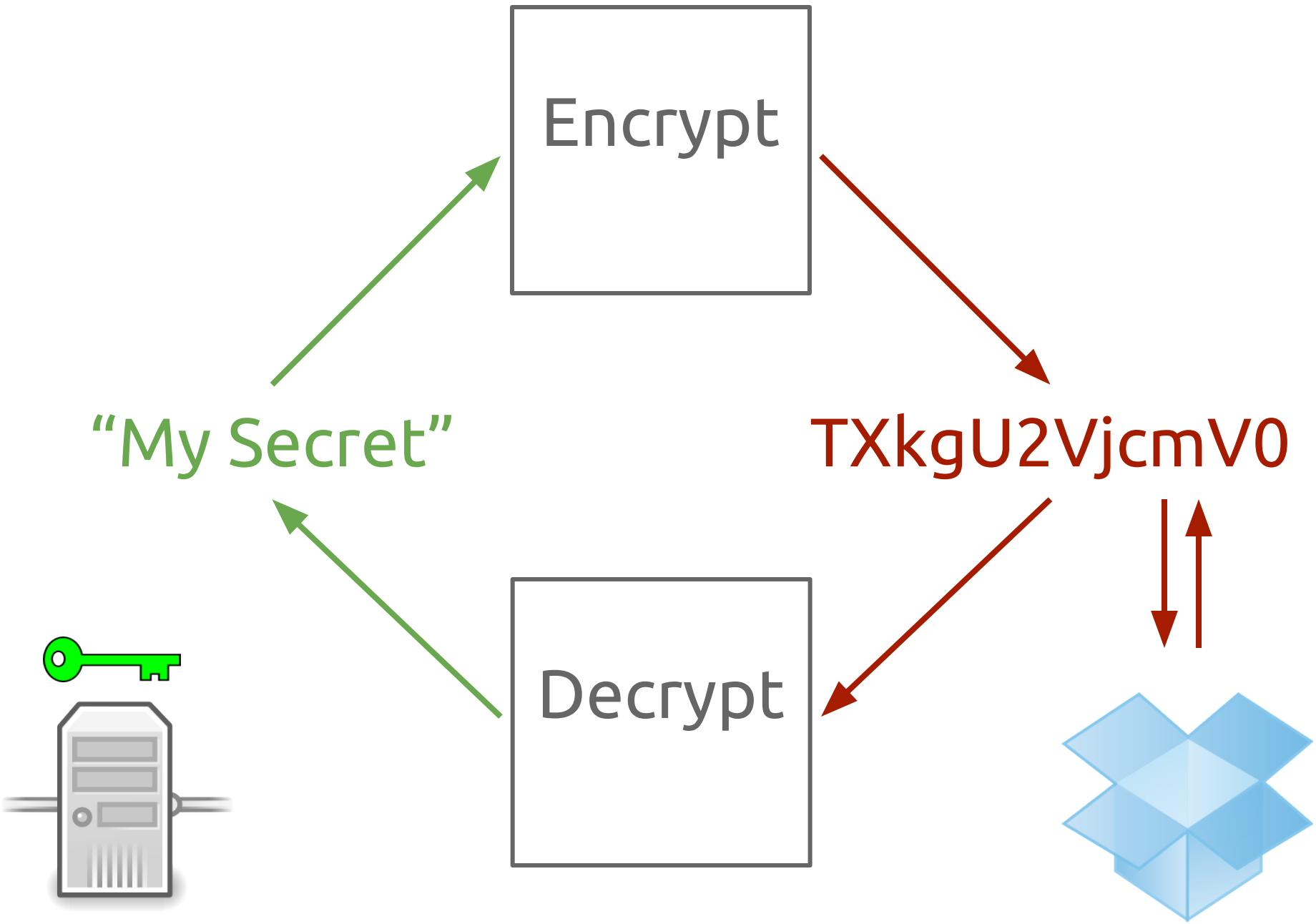
Custos

Latin for “Guard”

“Key Storage as a Service”

“Secret Storage as a Service”


Encrypt
“My Secret”
TXkgU2VjcmV0
Decrypt


Encrypt
“My Secret”
TXkgU2VjcmV0
Decrypt

Core Features

Centralized Secret Storage

Centralized Secret Storage

Flexible Access Control

Centralized Secret Storage

Flexible Access Control

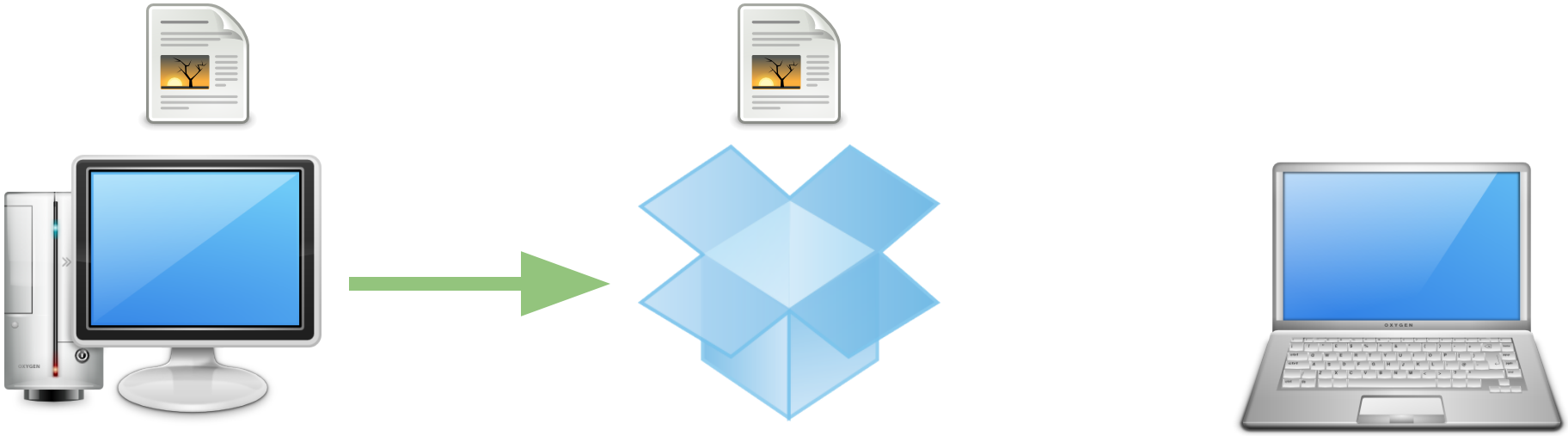
Auditing and Revocation

Centralized Secret Storage

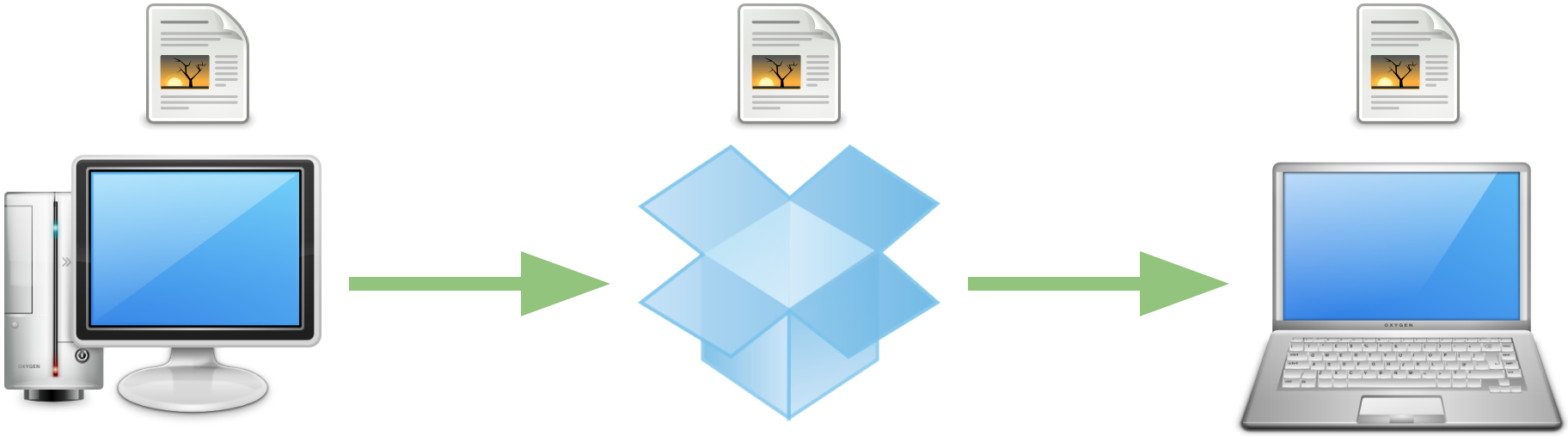
Example: Multi-Device File Sync

Example: Multi-Device File Sync

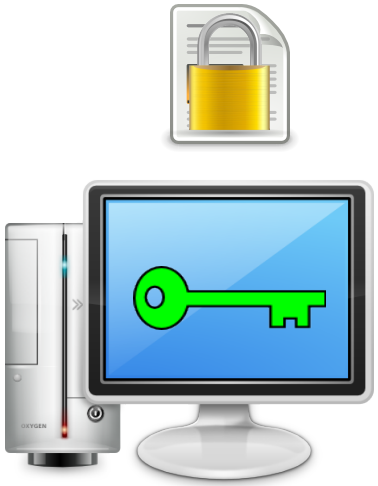
Example: Multi-Device File Sync



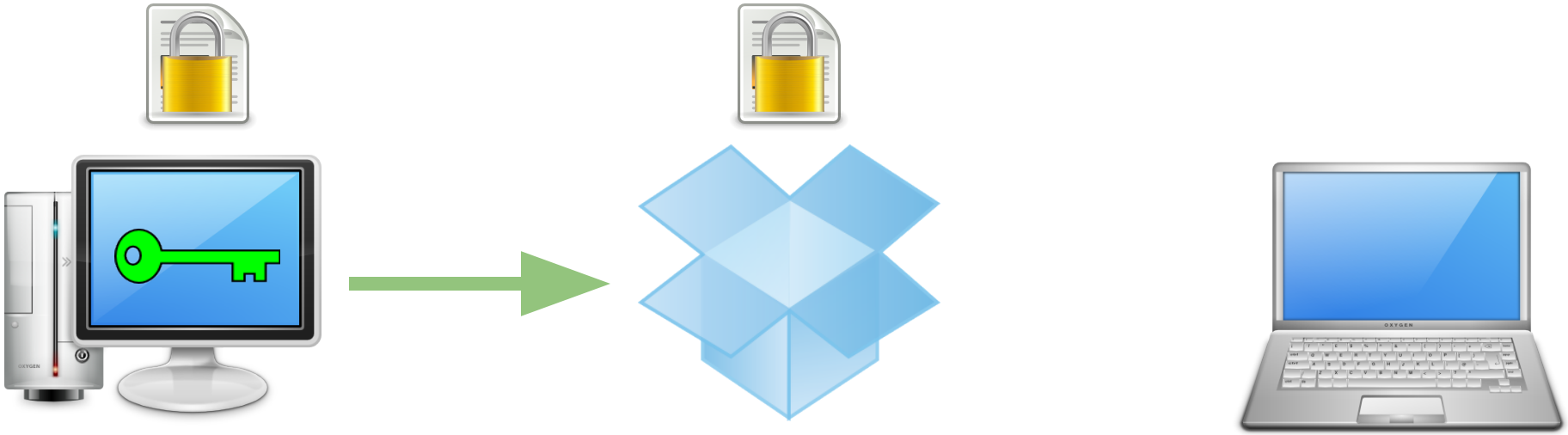
Example: Multi-Device File Sync



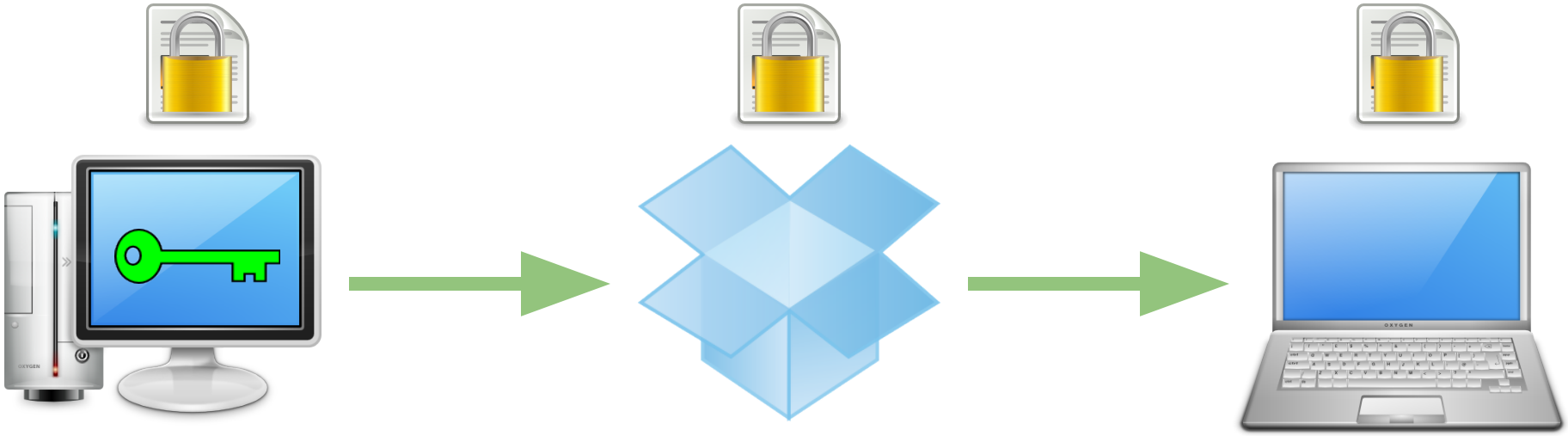
Example: Multi-Device File Sync



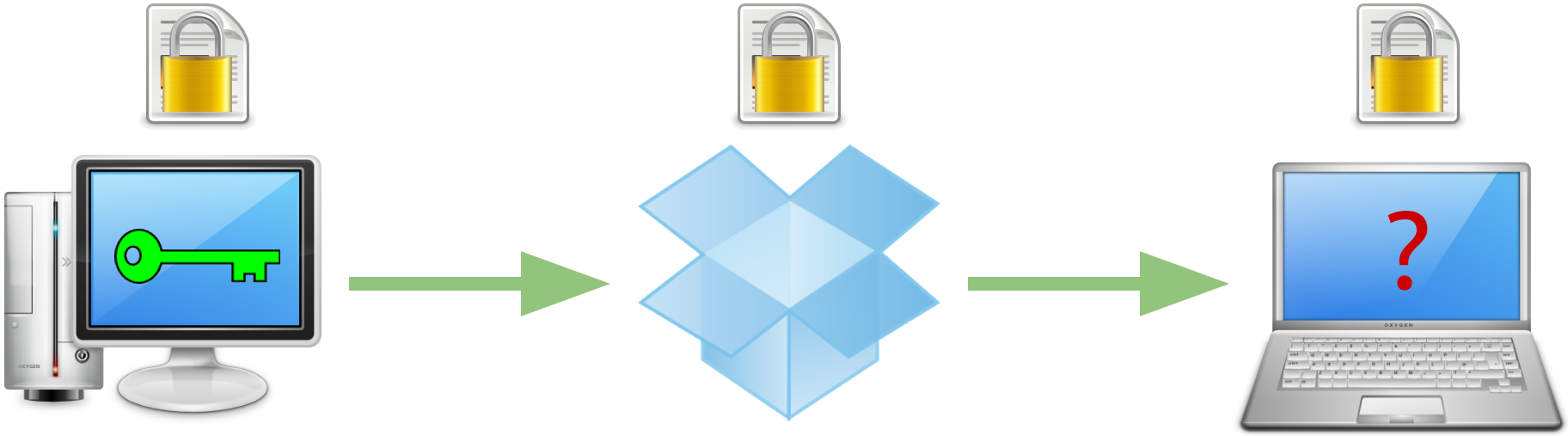
Example: Multi-Device File Sync



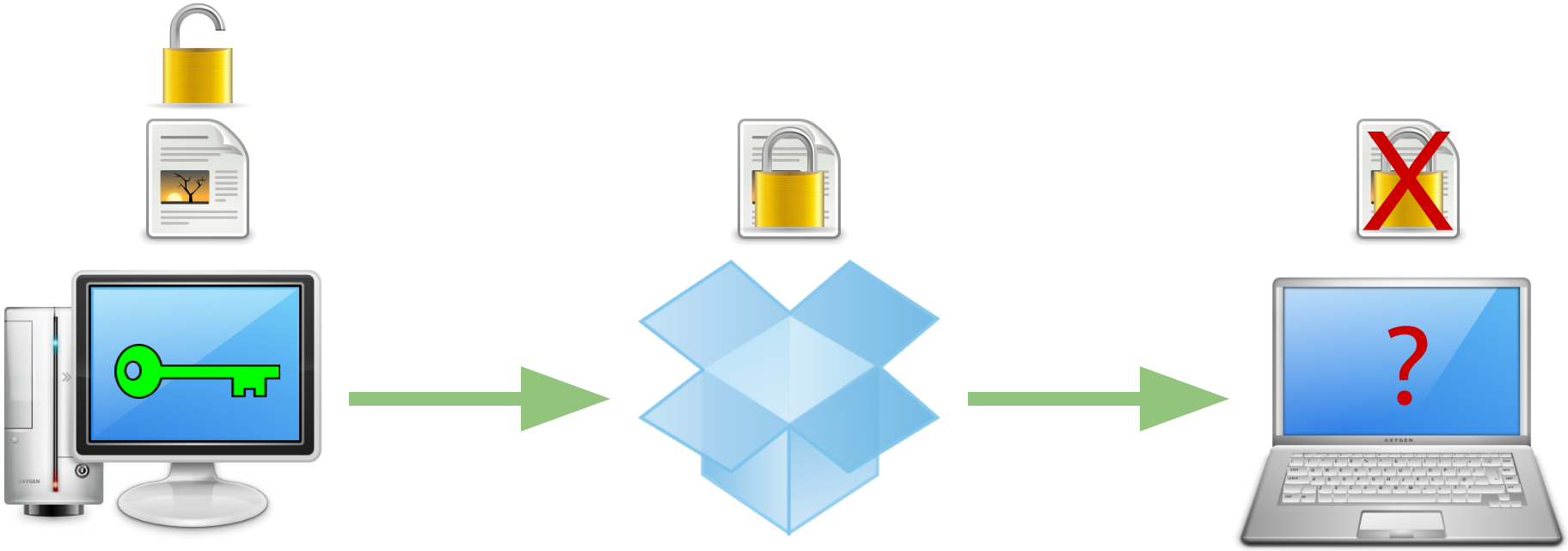
Example: Multi-Device File Sync



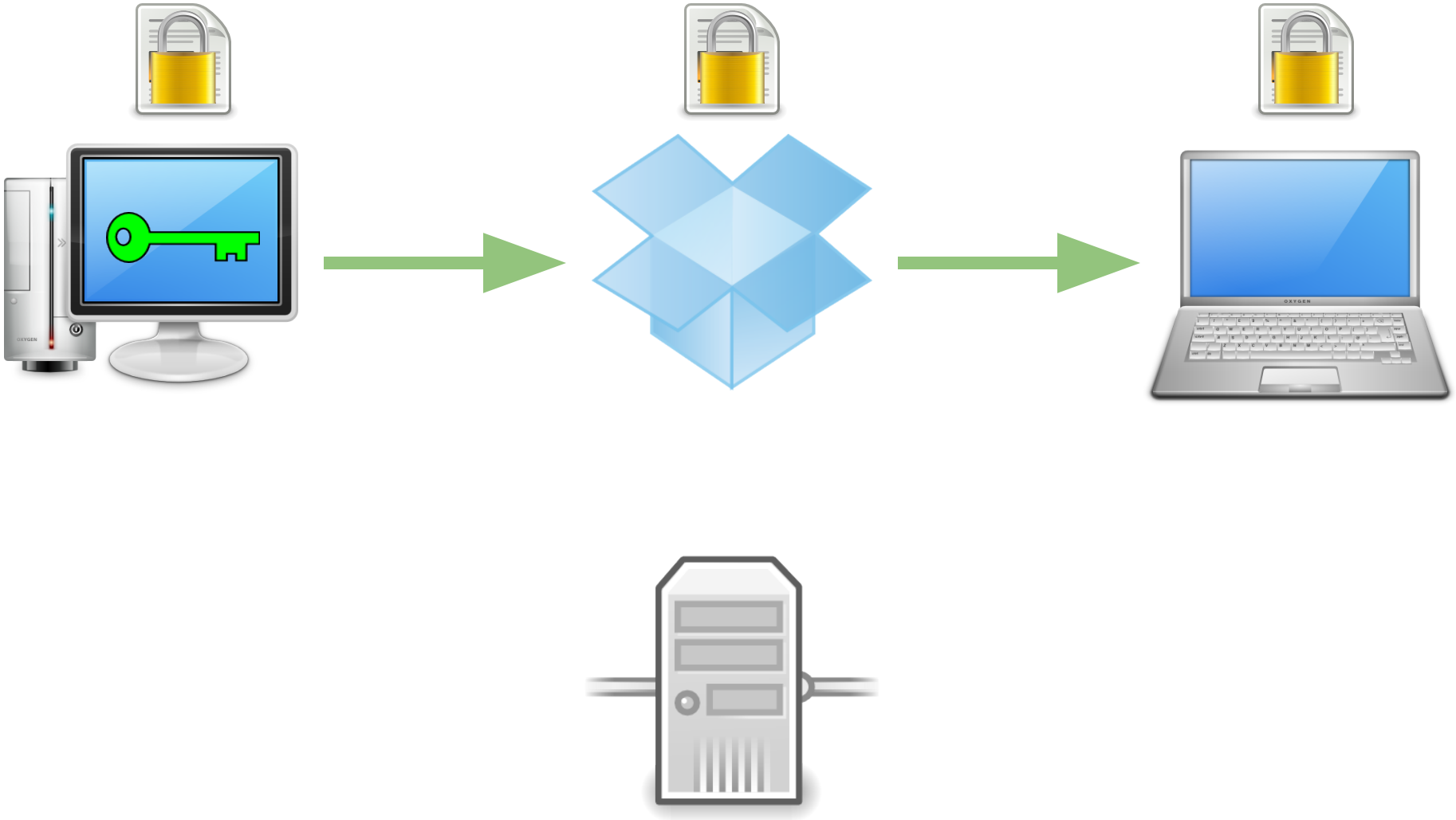
Example: Multi-Device File Sync



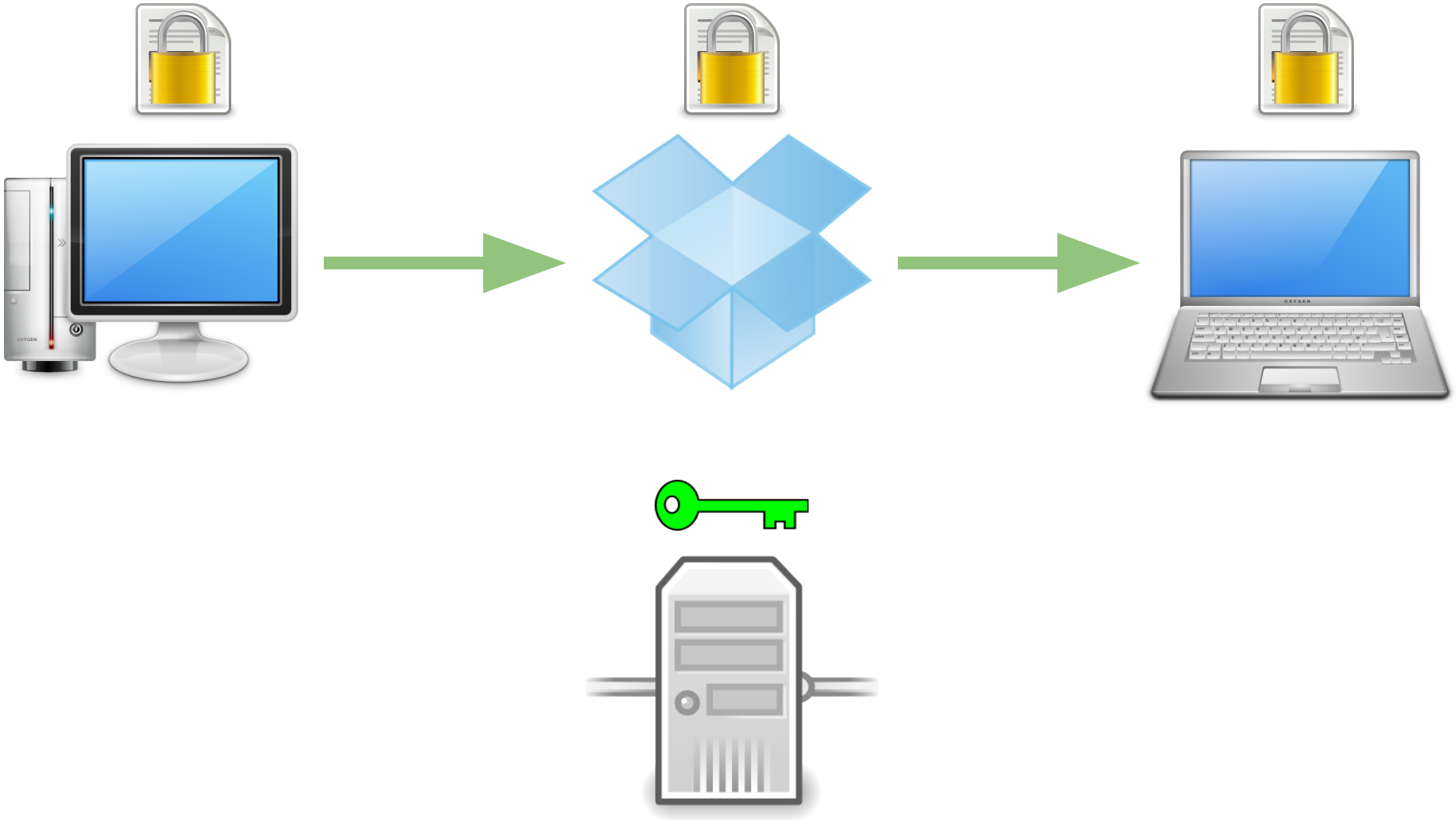
Example: Multi-Device File Sync



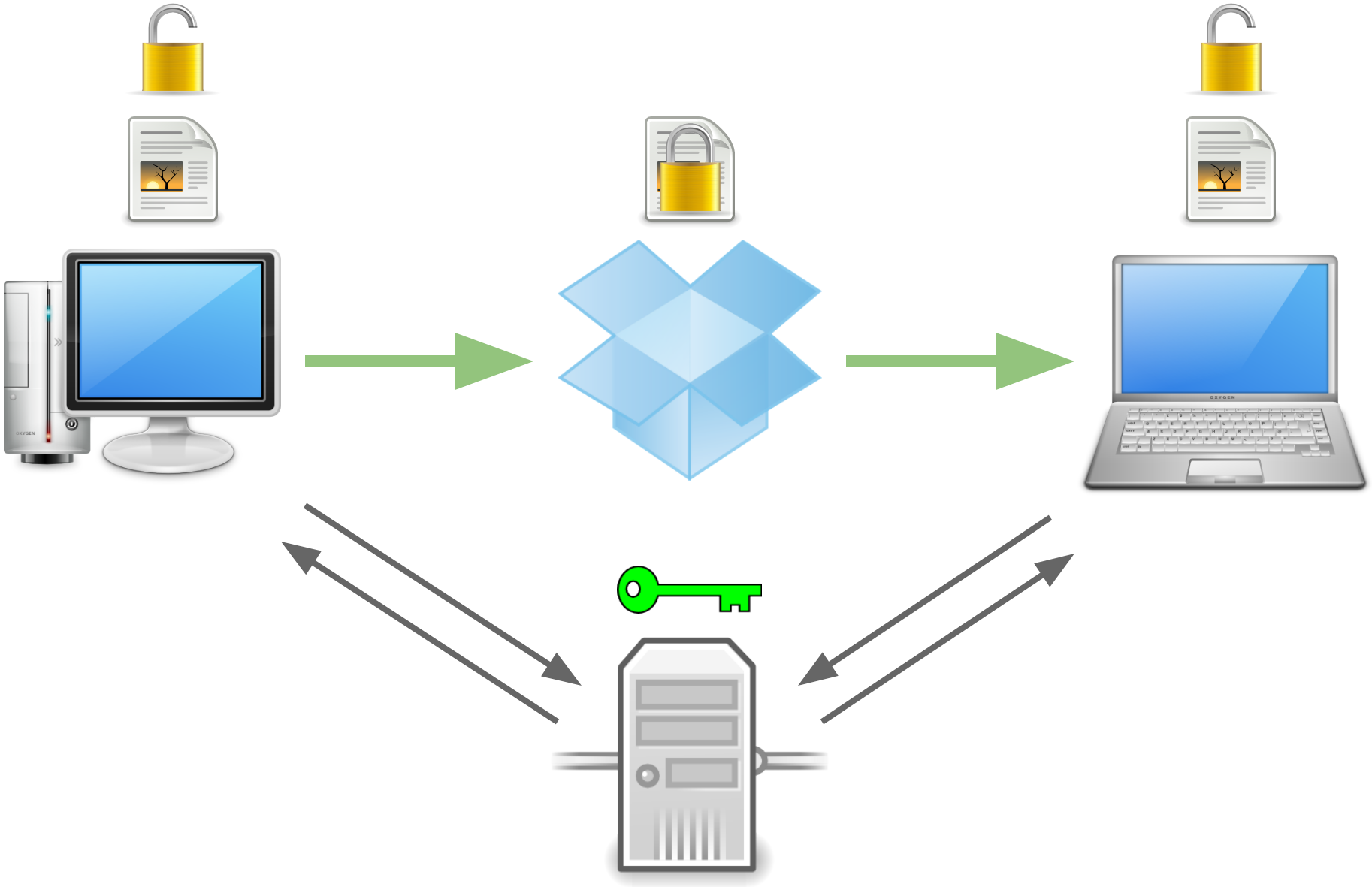
Example: Multi-Device File Sync



Example: Multi-Device File Sync



Example: Multi-Device File Sync



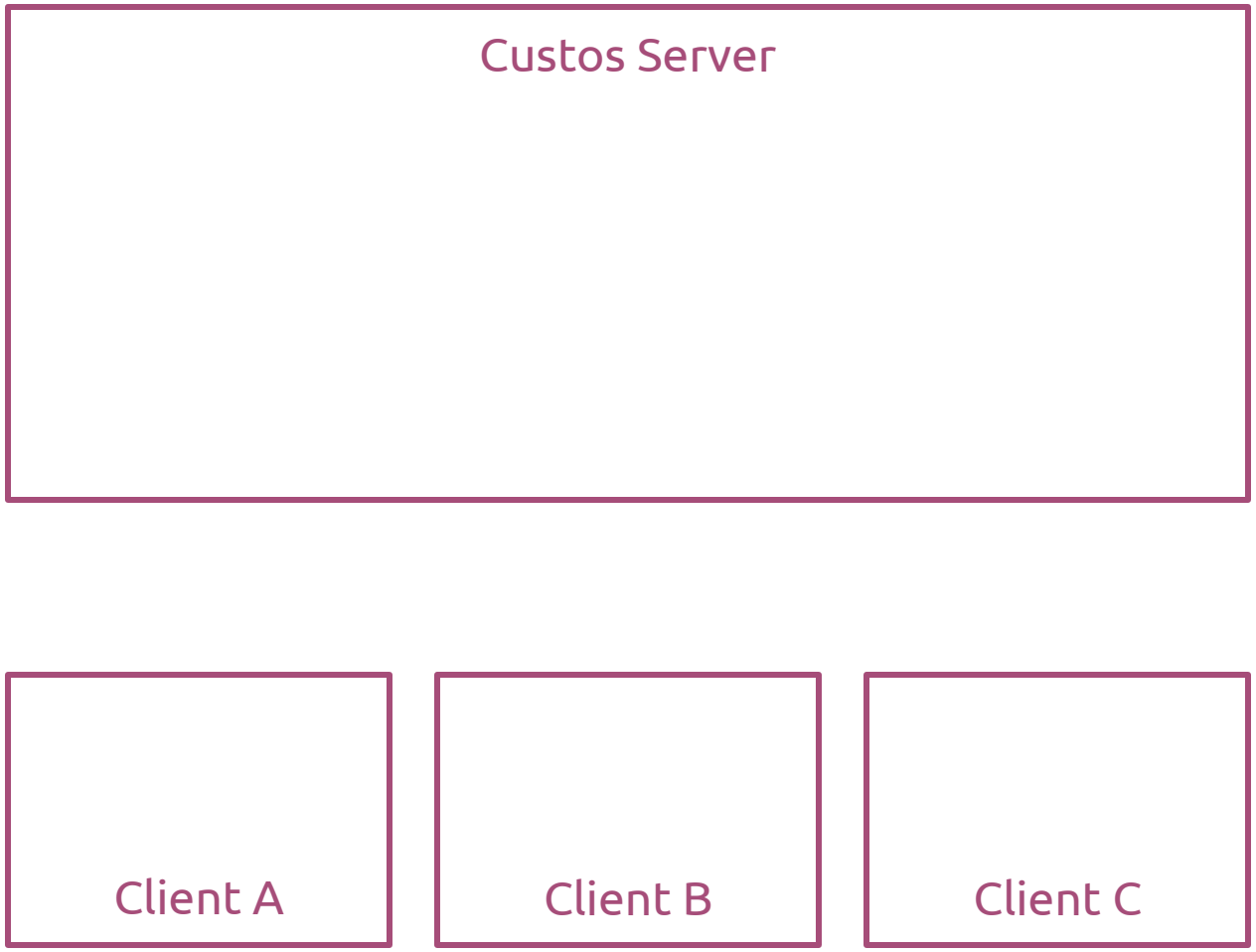
Managed SSH Agent

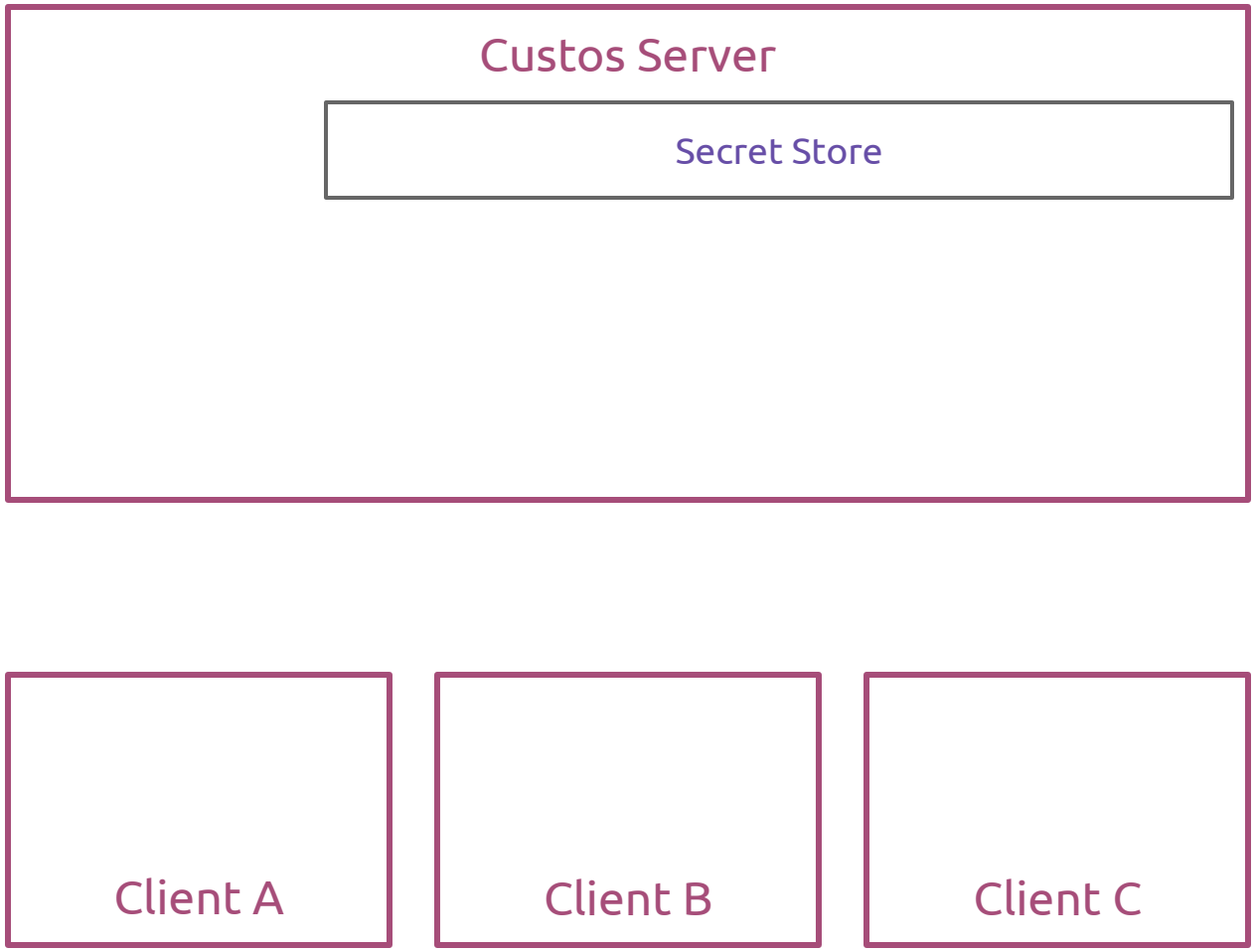
Managed SSH Agent
Scalable SSL Processor

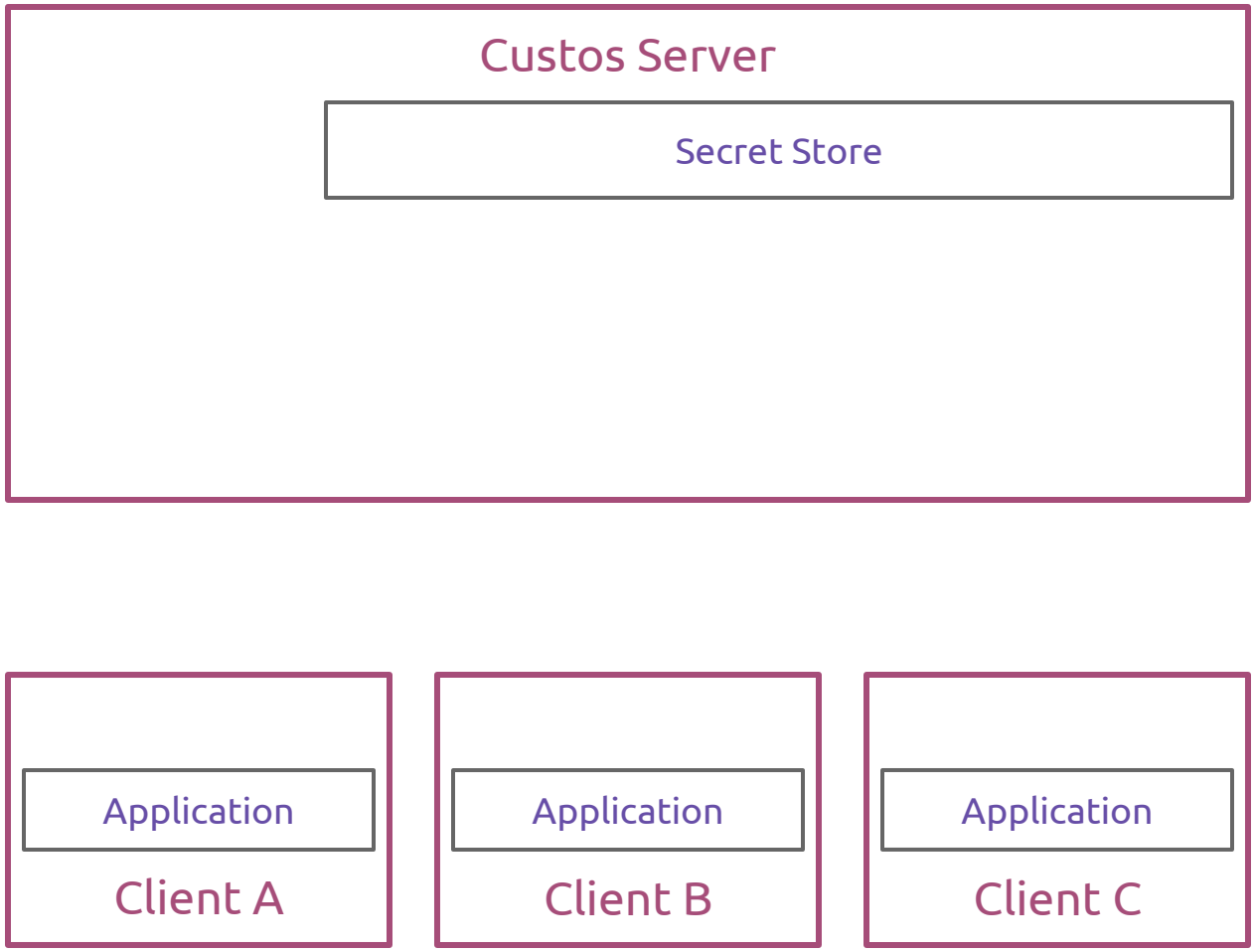
Managed SSH Agent
Scalable SSL Processor
Etc...

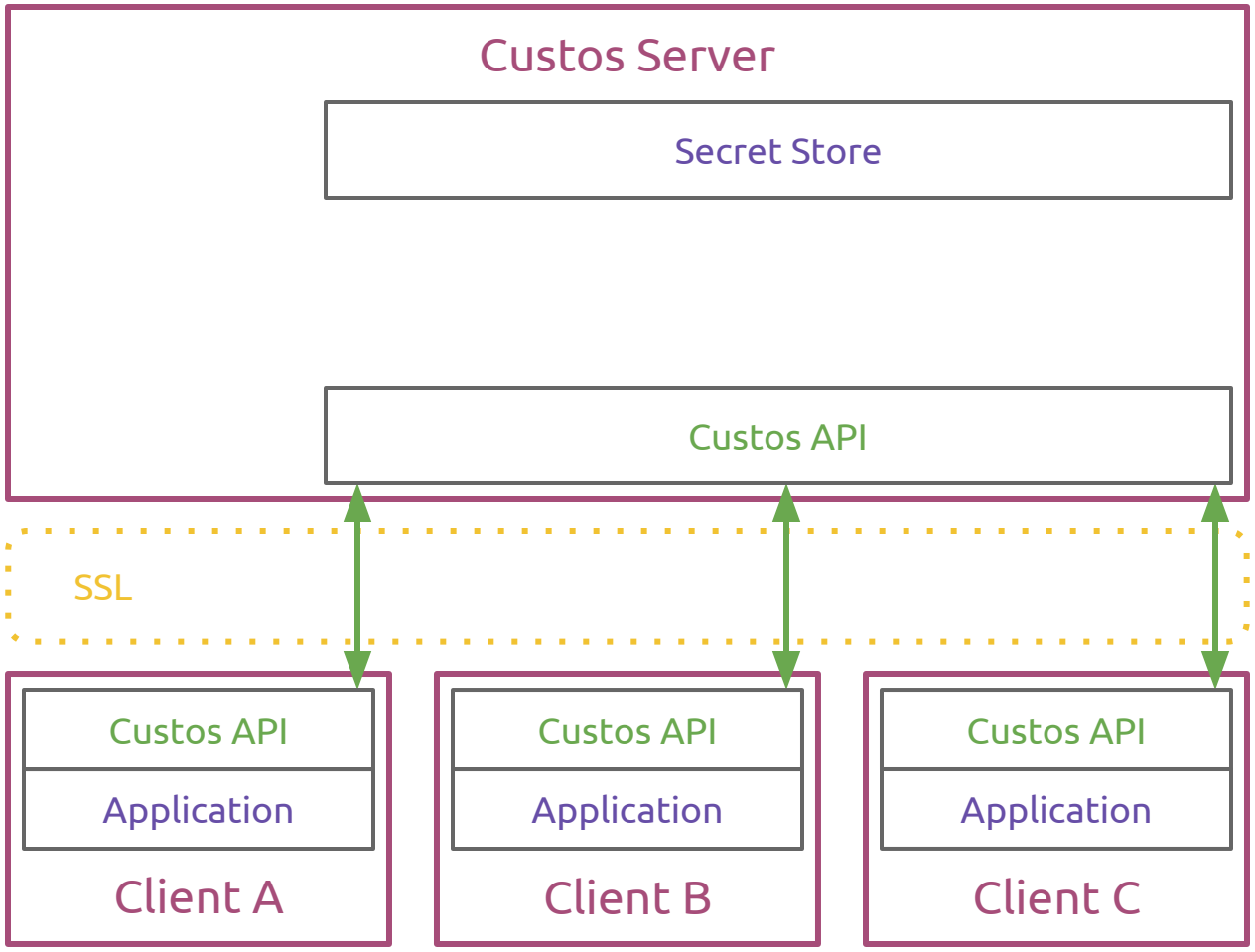
Centralized Secret Storage in Custos


Custos Server

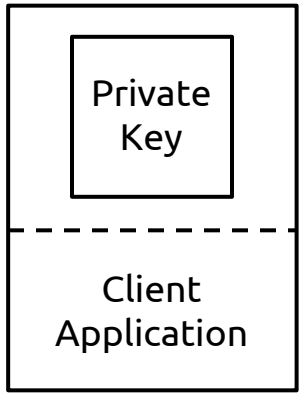

Custos Server
Client A
Client B
Client C

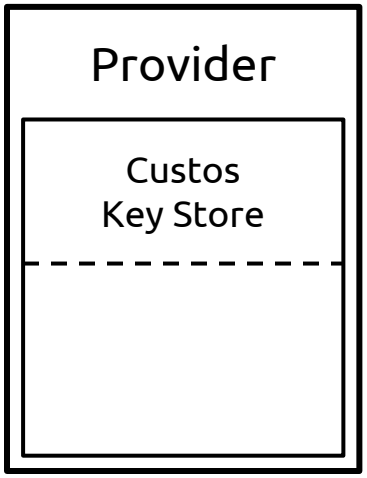

Custos Server
Secret Store
Client A
Client B
Client C

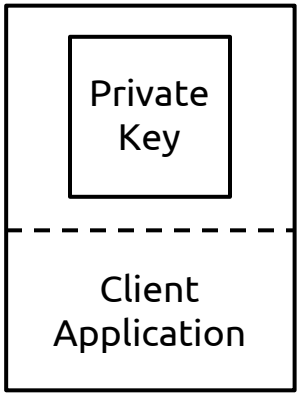

Custos Server
Secret Store
Application
Client A
Application
Client B
Application
Client C

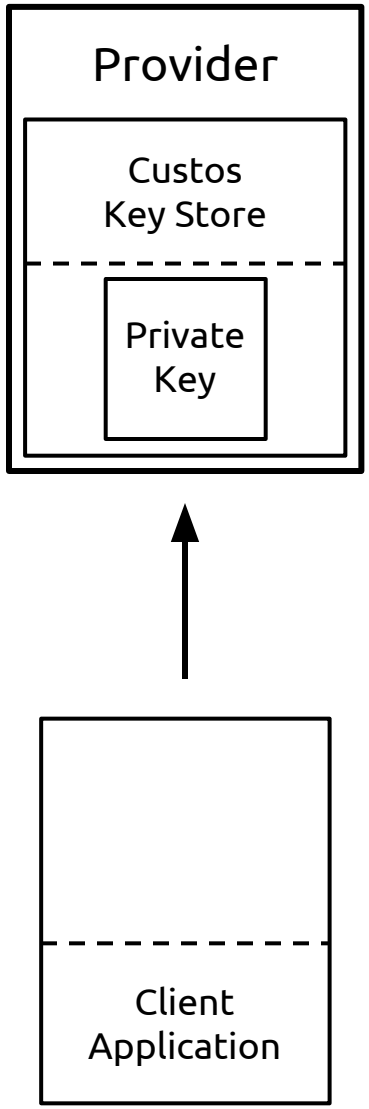

Custos Server
Secret Store
Custos API
SSL
Custos API
Application
Client A
Custos API
Application
Client B
Custos API
Application
Client C

Trust?


Private
Key
Client
Application


Provider
Custos
Key Store


Private
Key
Client
Application


Provider
Custos
Key Store
Private
Key
Client
Application

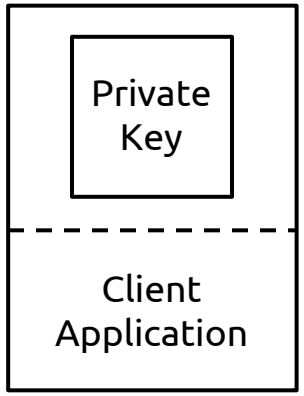
Do you have to trust

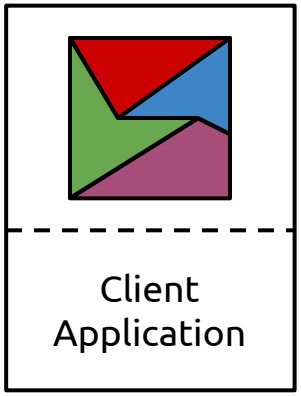
a single provider?

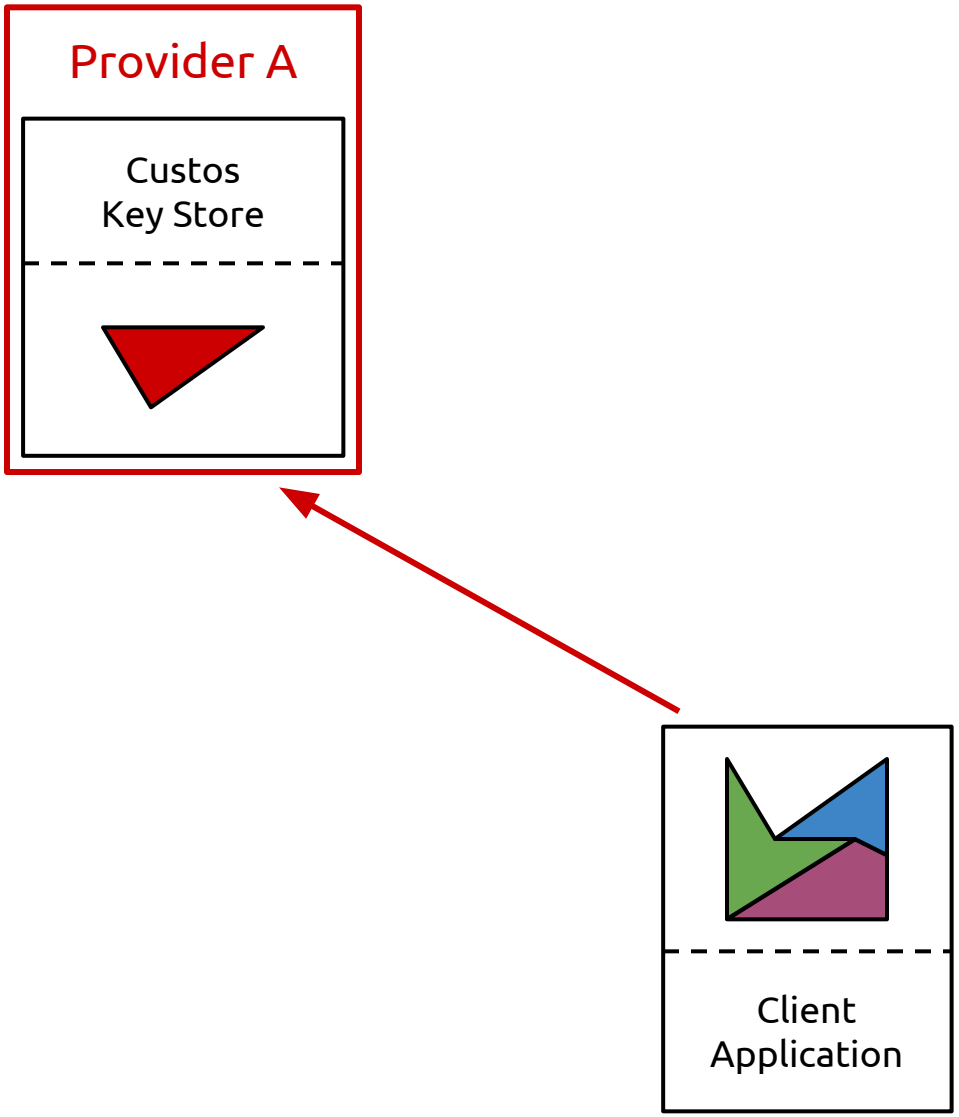
Multi-Provider Sharding

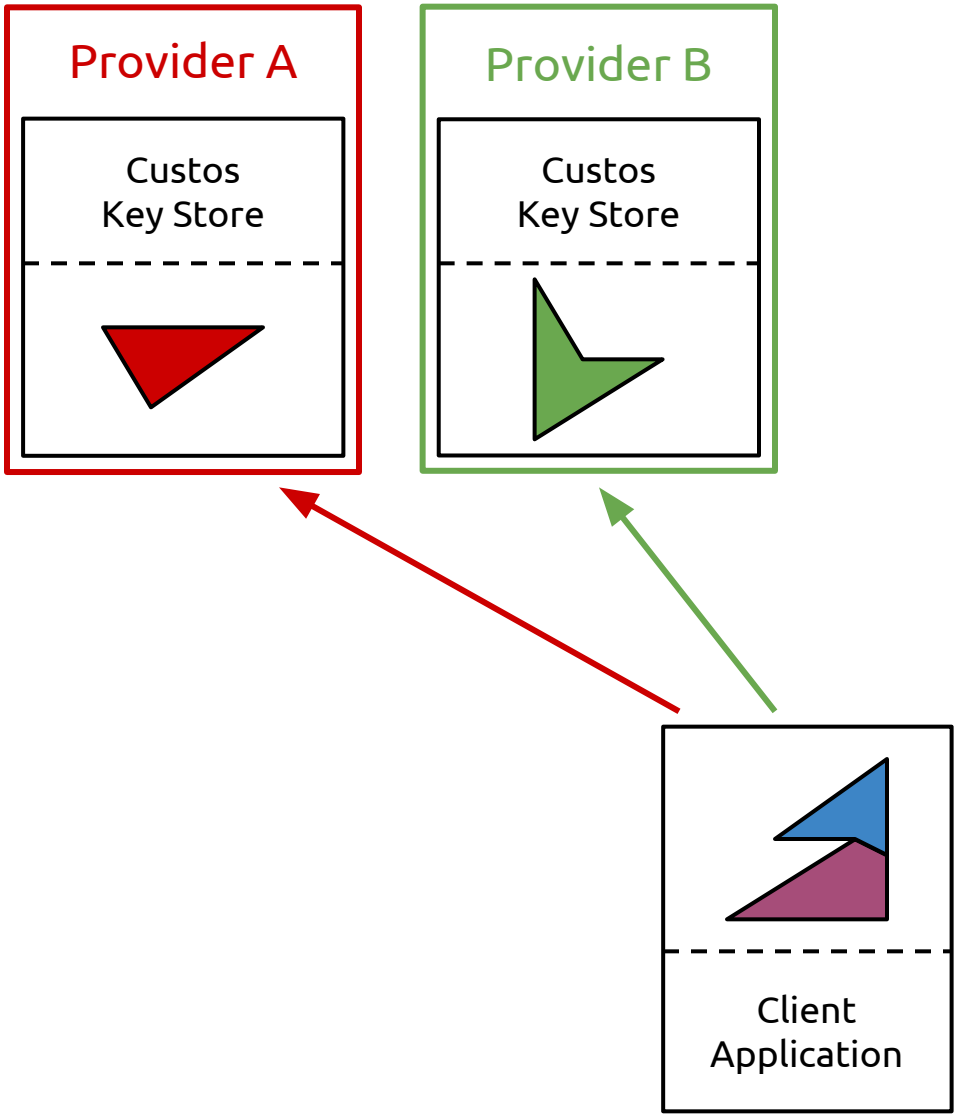
Multi-Provider Sharding

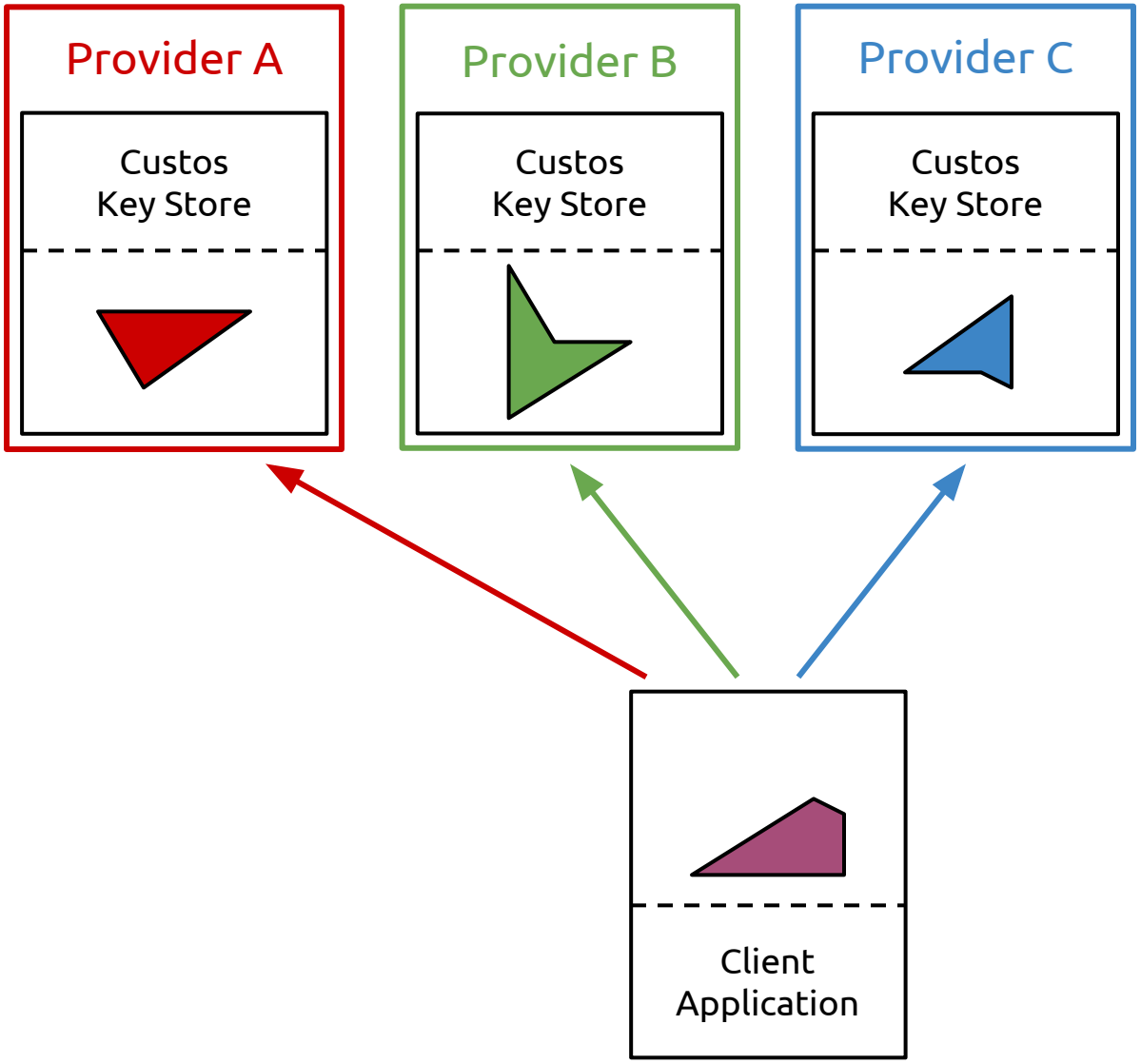
Shamir Secret Sharing

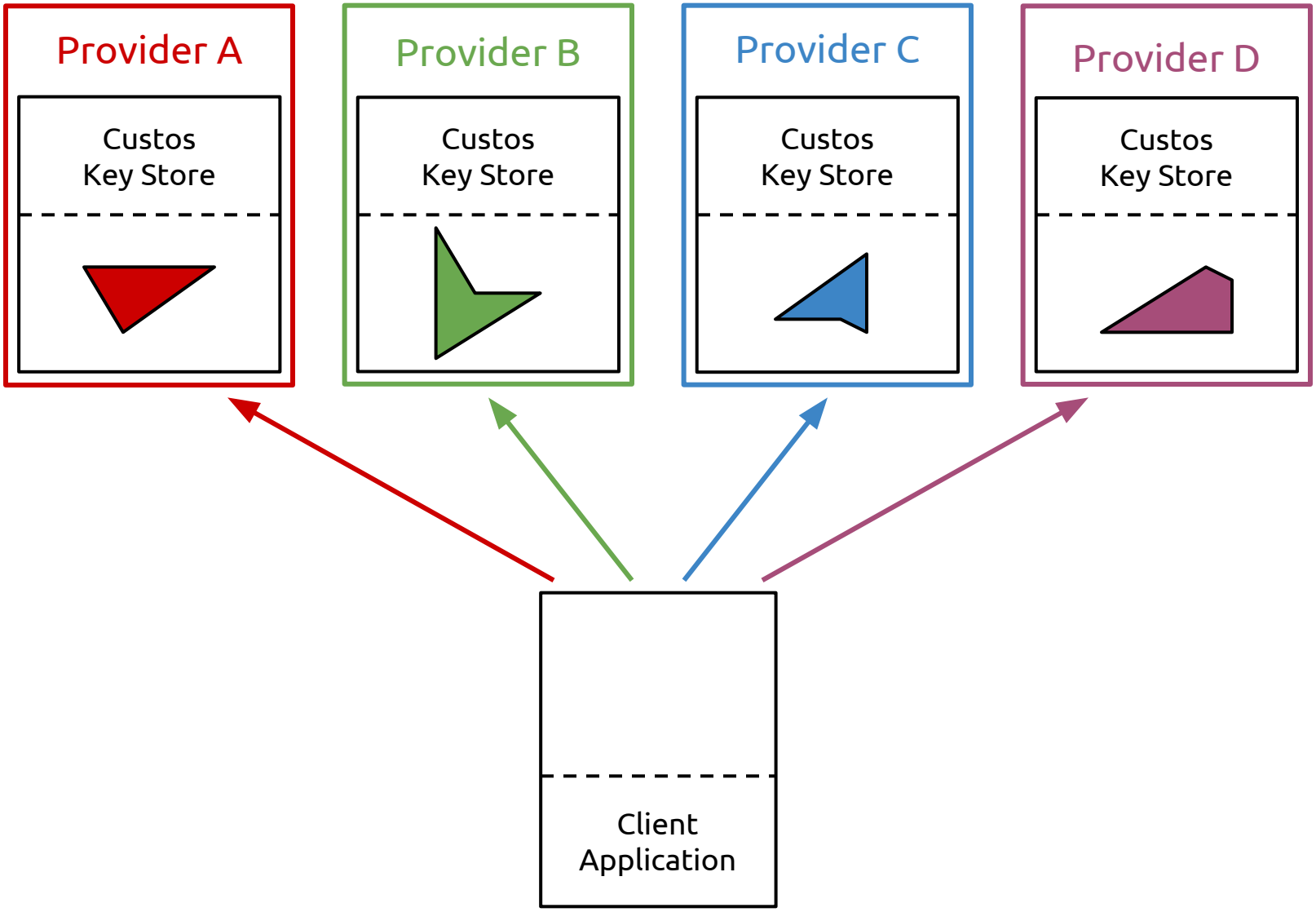

Private
Key
Client
Application

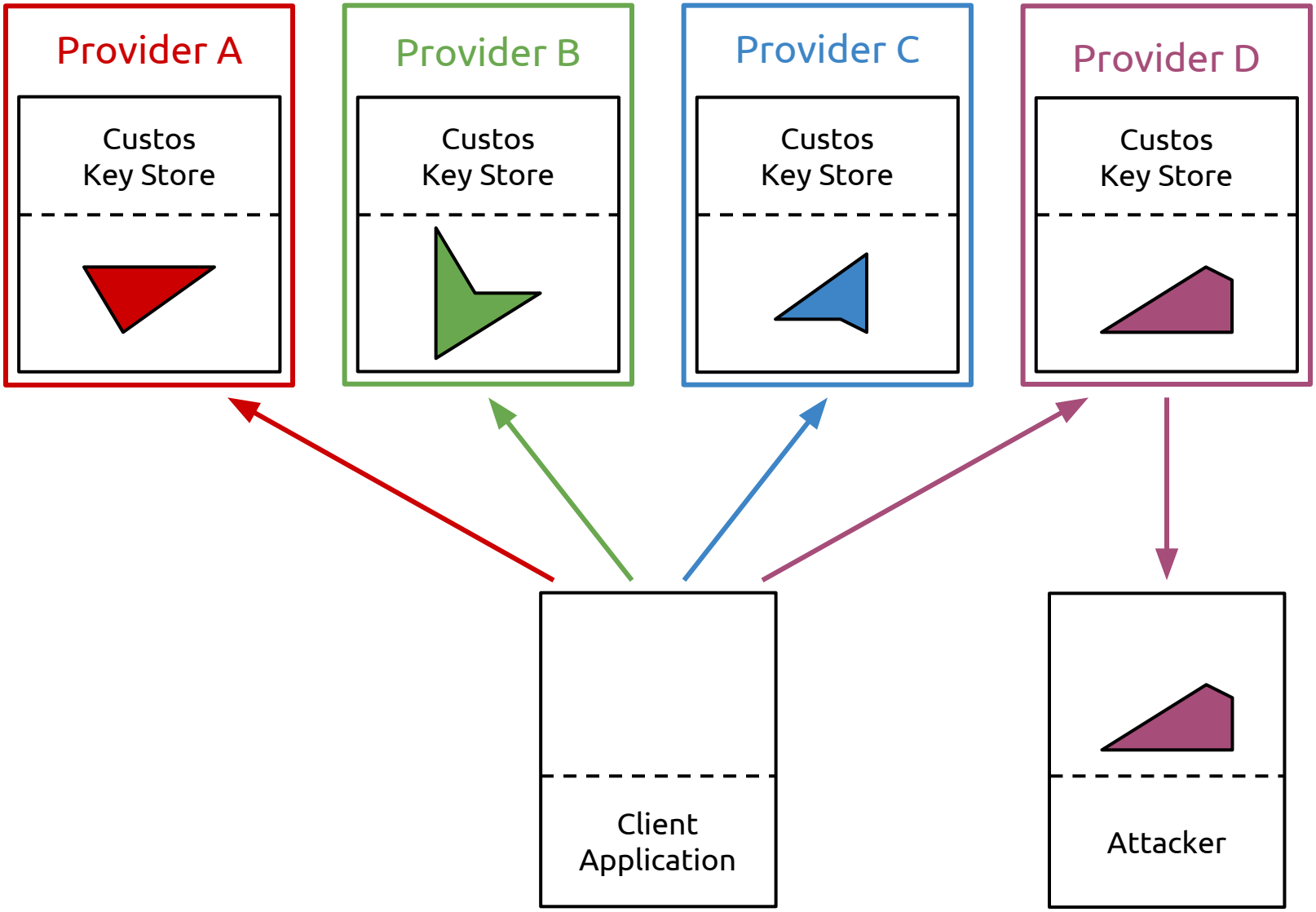

Client
Application

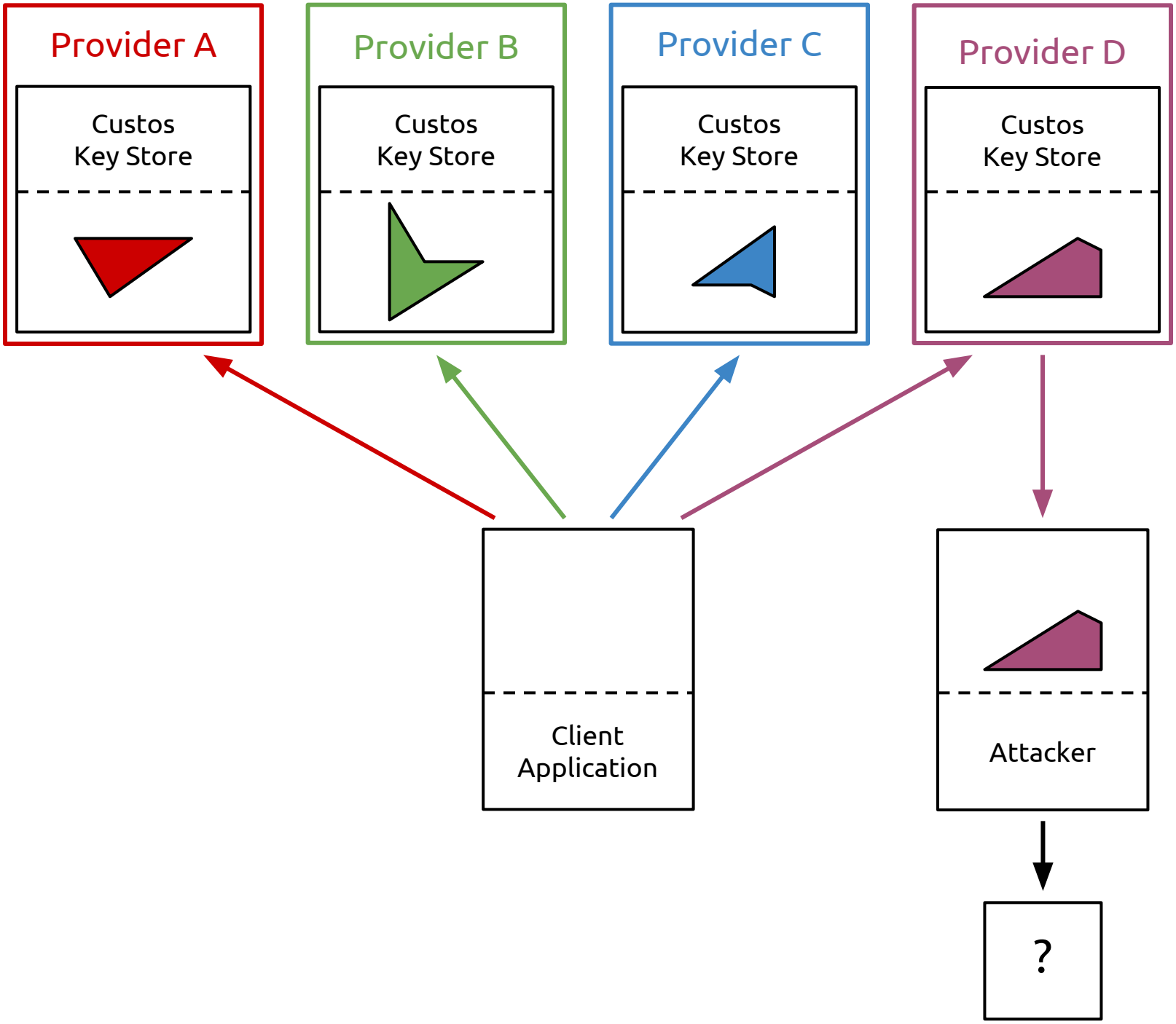

Provider A
Custos
Key Store
Client
Application


Provider A
Custos
Key Store
Provider B
Custos
Key Store
Client
Application


Provider A
Custos
Key Store
Provider B
Custos
Key Store
Provider C
Custos
Key Store
Client
Application


Provider A
Custos
Key Store
Provider B
Custos
Key Store
Provider C
Custos
Key Store
Provider D
Custos
Key Store
Client
Application


Provider A
Custos
Key Store
Provider B
Custos
Key Store
Provider C
Custos
Key Store
Provider D
Custos
Key Store
Client
Application
Attacker


Provider A
Custos
Key Store
Provider B
Custos
Key Store
Provider C
Custos
Key Store
Provider D
Custos
Key Store
Client
Application
Attacker
?

Availability

Availability

Sharding with (k, n) Threshold Scheme

Centralized Secret Storage

Centralized Secret Storage

Flexible Access Control

Example: Autonomous Server Bootup

Example: Autonomous Server Bootup

Example: Autonomous Server Bootup

Example: Autonomous Server Bootup

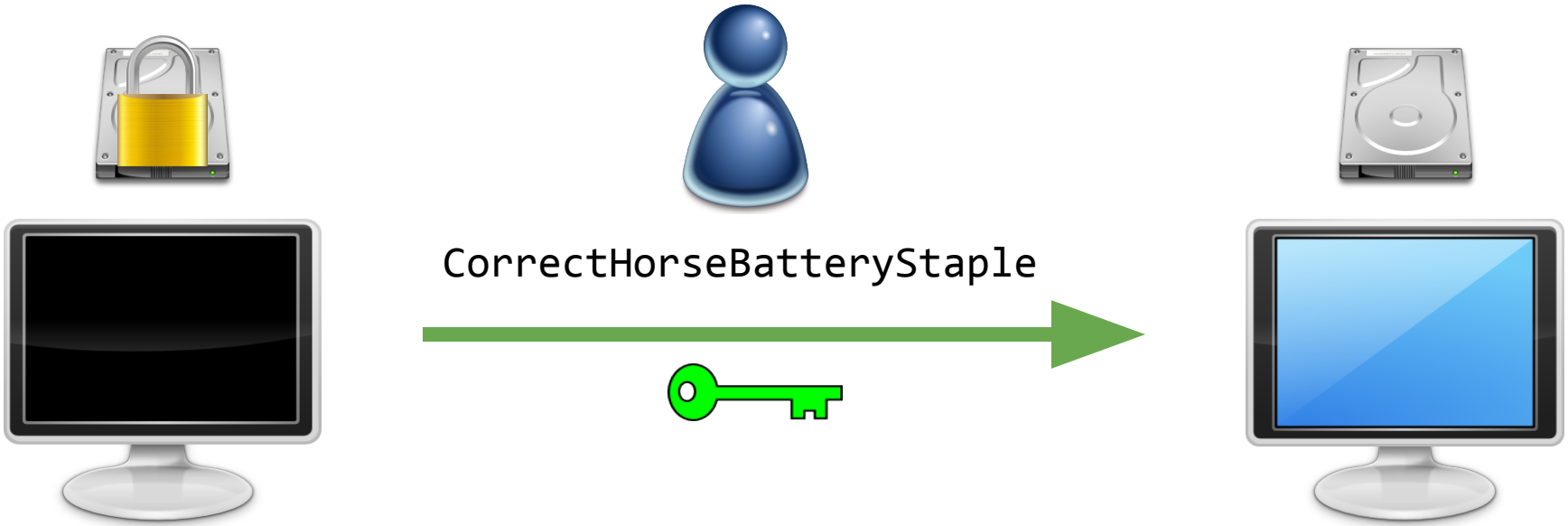
Example: Autonomous Server Bootup

```
CorrectHorseBatteryStaple
```

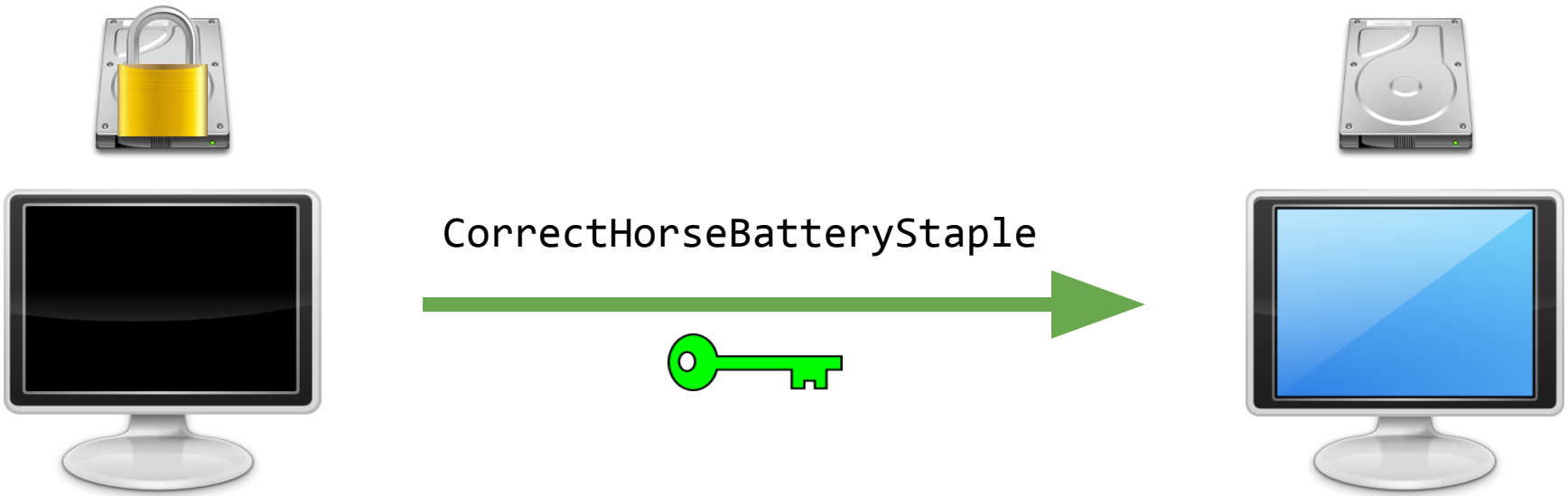
Example: Autonomous Server Bootup

`CorrectHorseBatteryStaple`

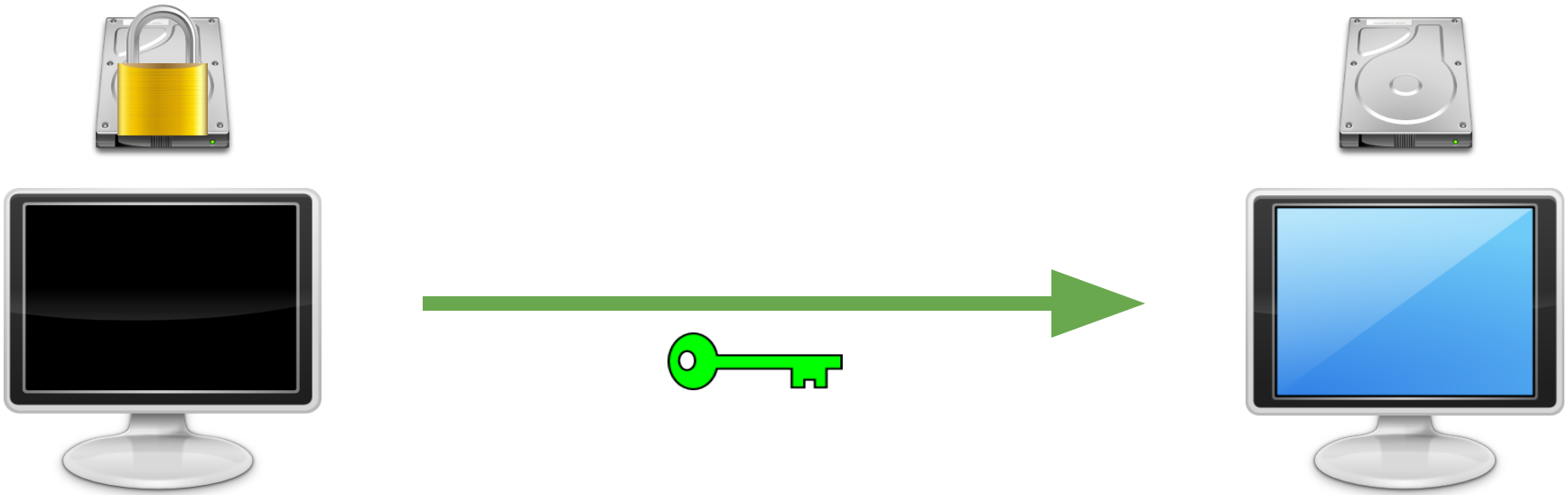
Example: Autonomous Server Bootup



Example: Autonomous Server Bootup



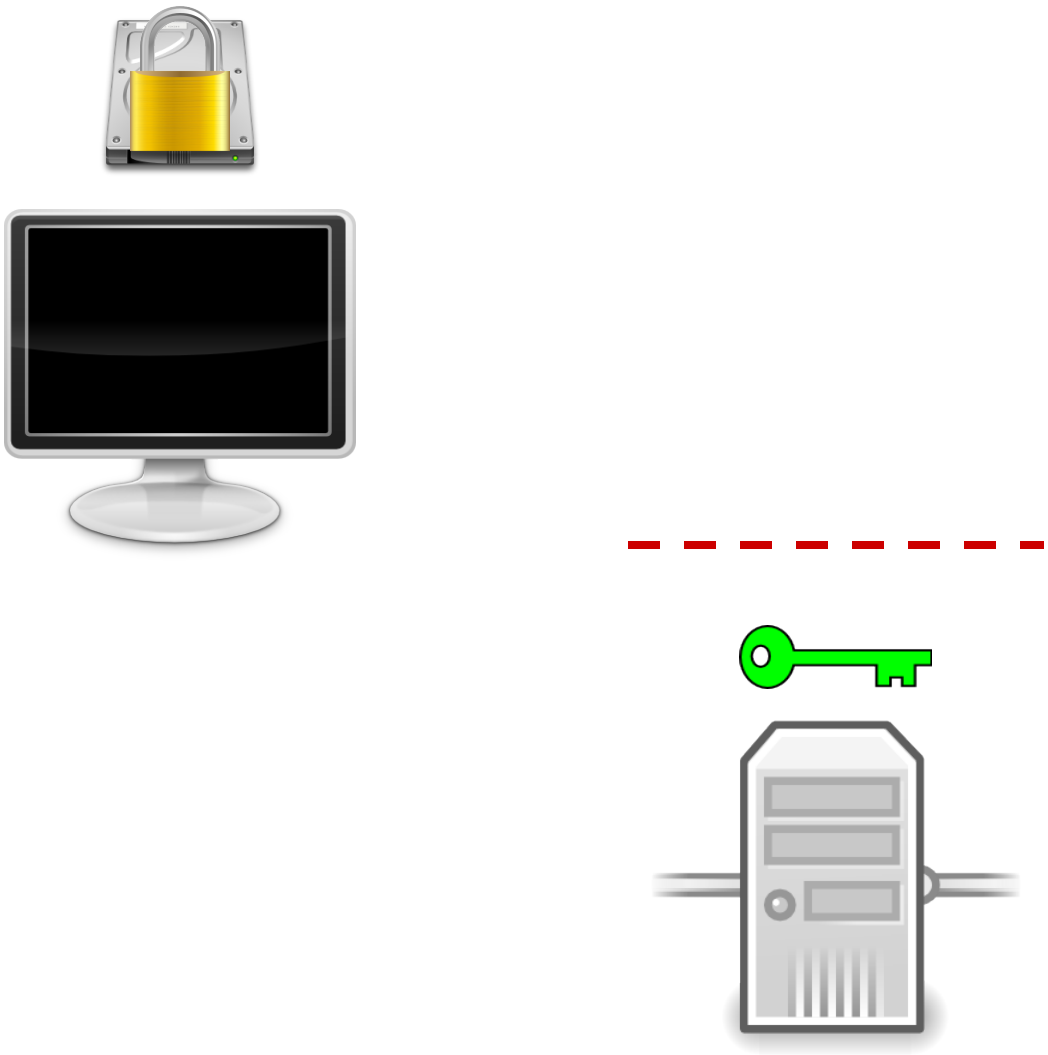
Example: Autonomous Server Bootup



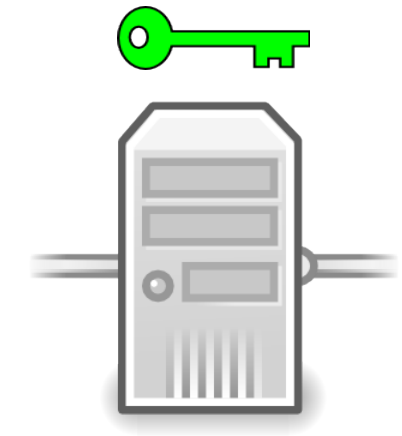
Example: Autonomous Server Bootup

Example: Autonomous Server Bootup

Example: Autonomous Server Bootup

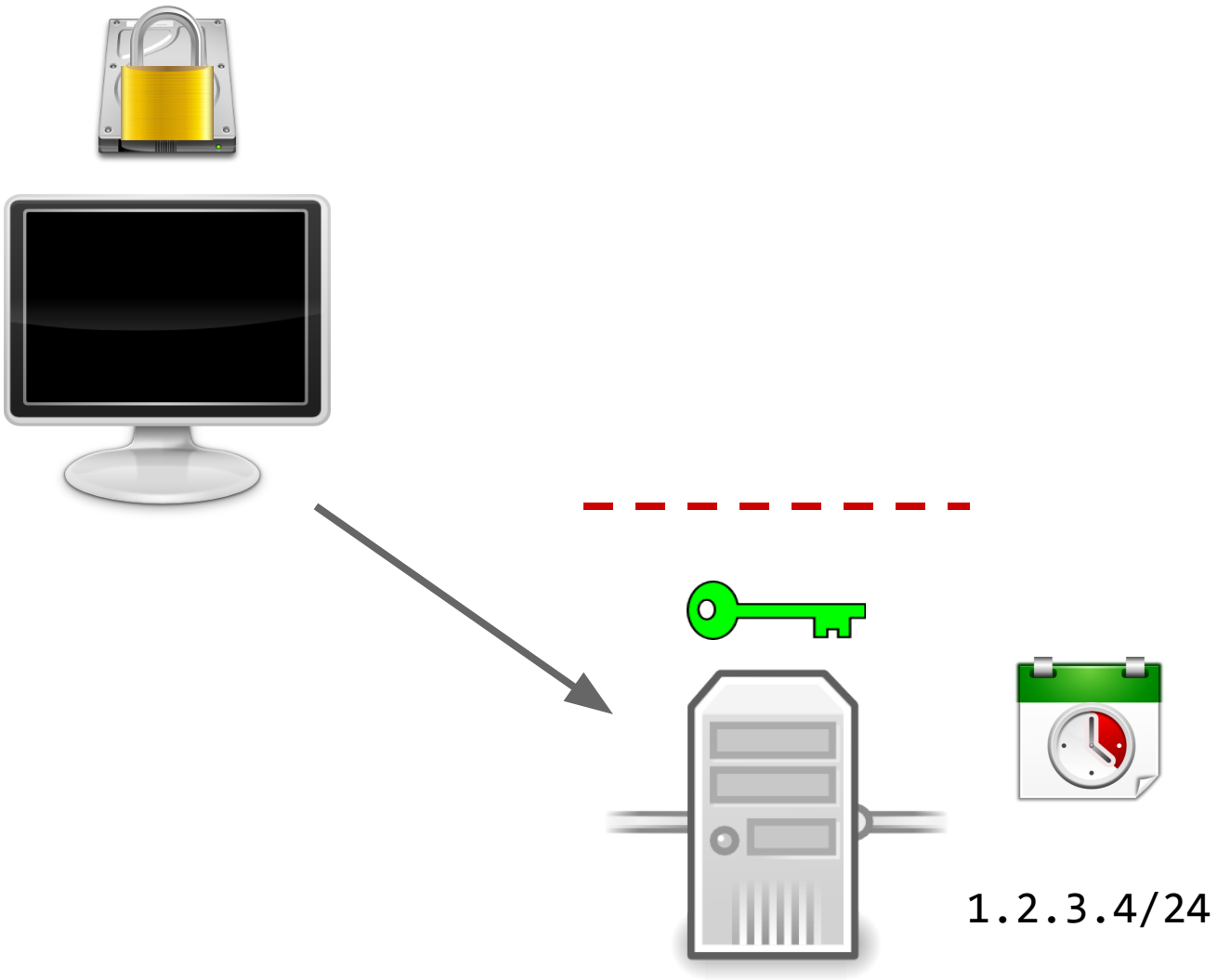


Example: Autonomous Server Bootup

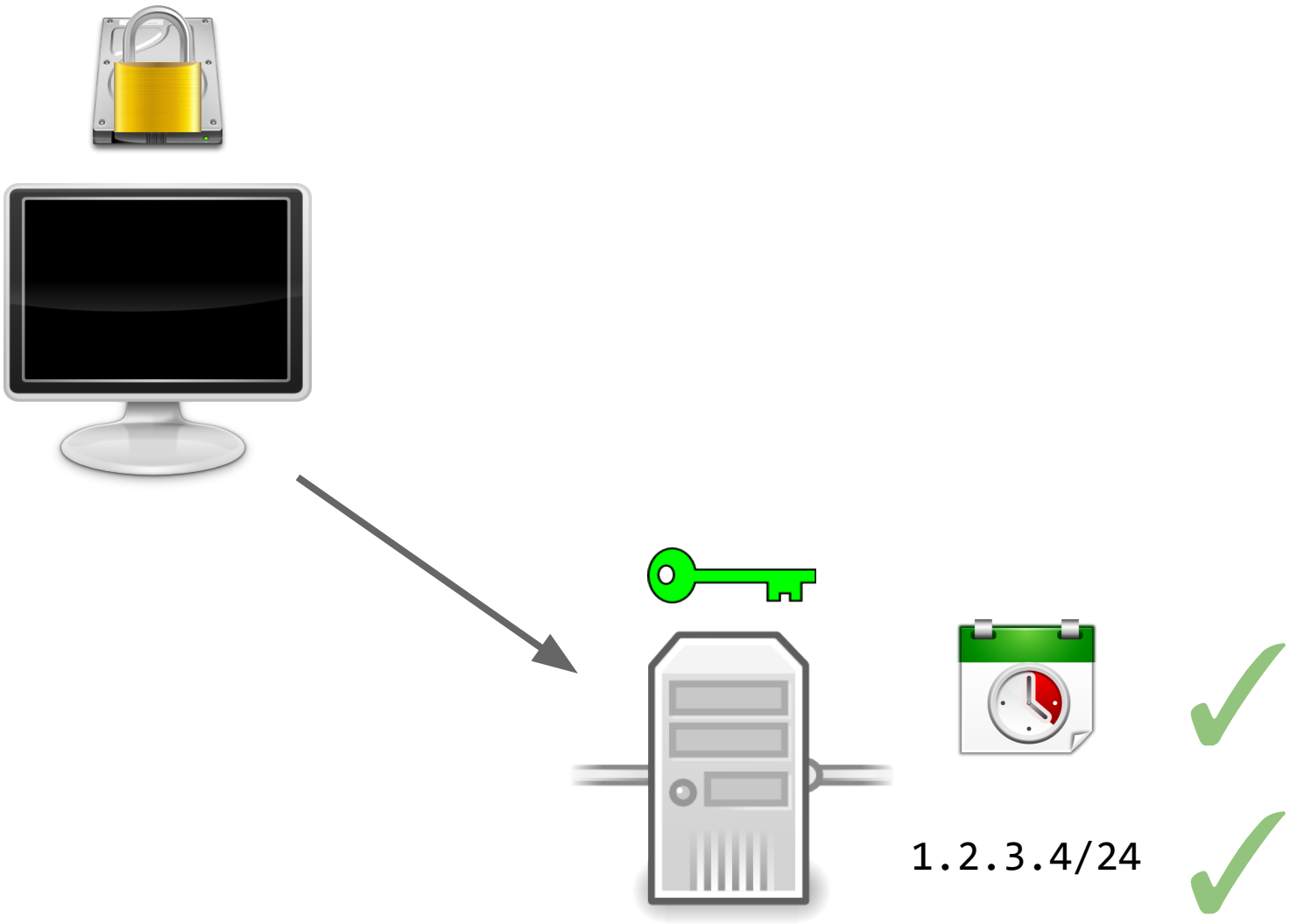


1.2.3.4/24

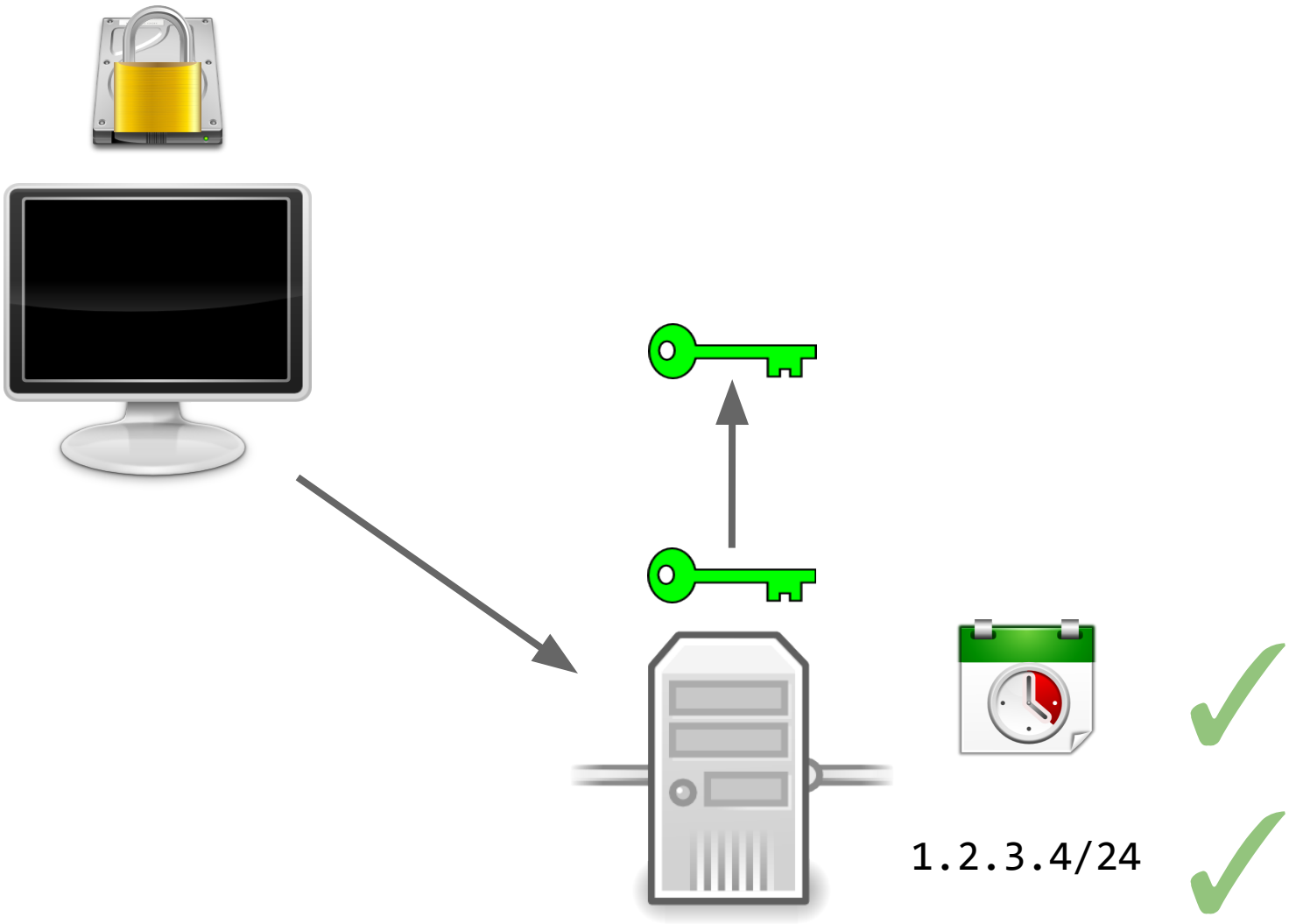
Example: Autonomous Server Bootup



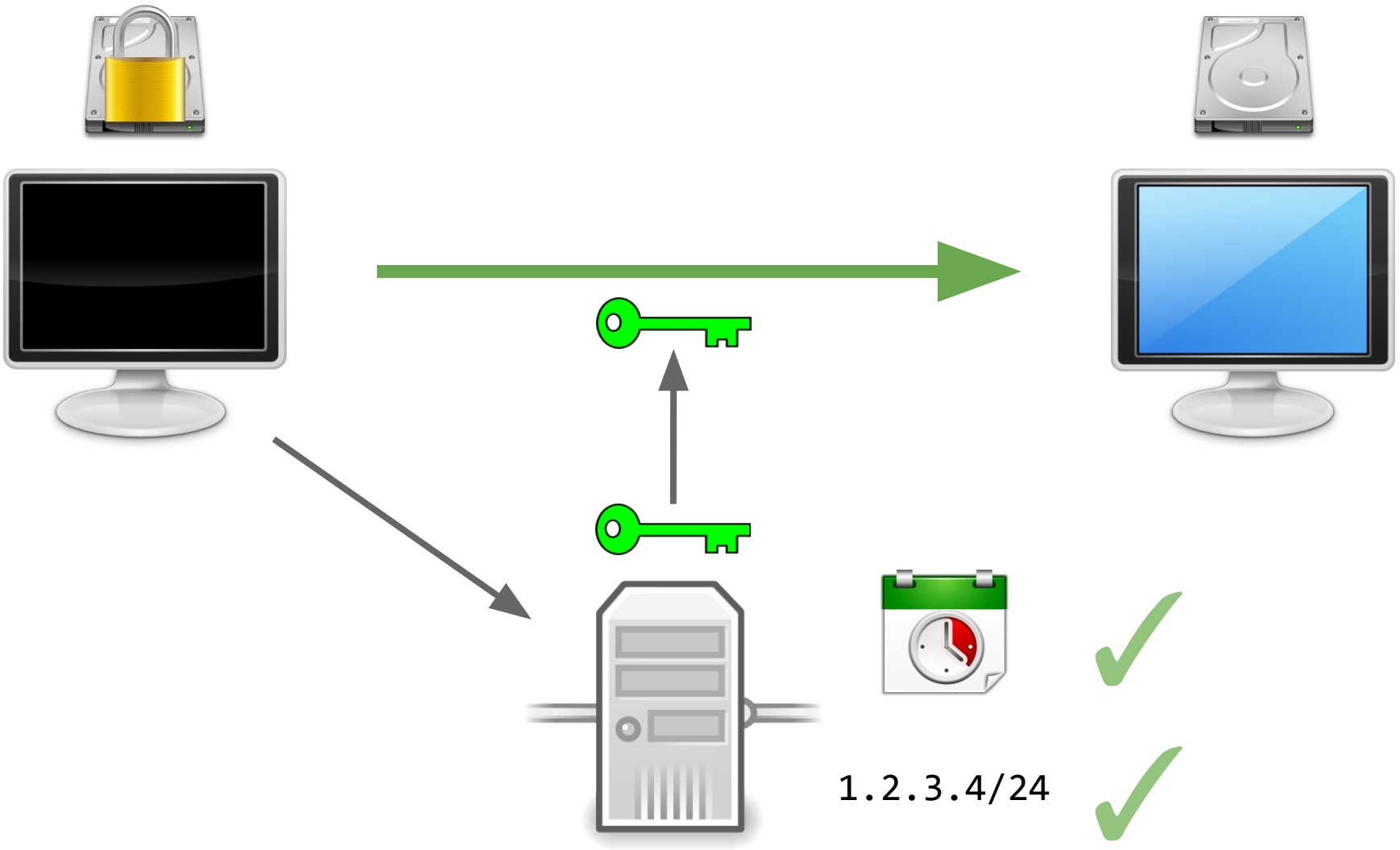
Example: Autonomous Server Bootup



Example: Autonomous Server Bootup



Example: Autonomous Server Bootup

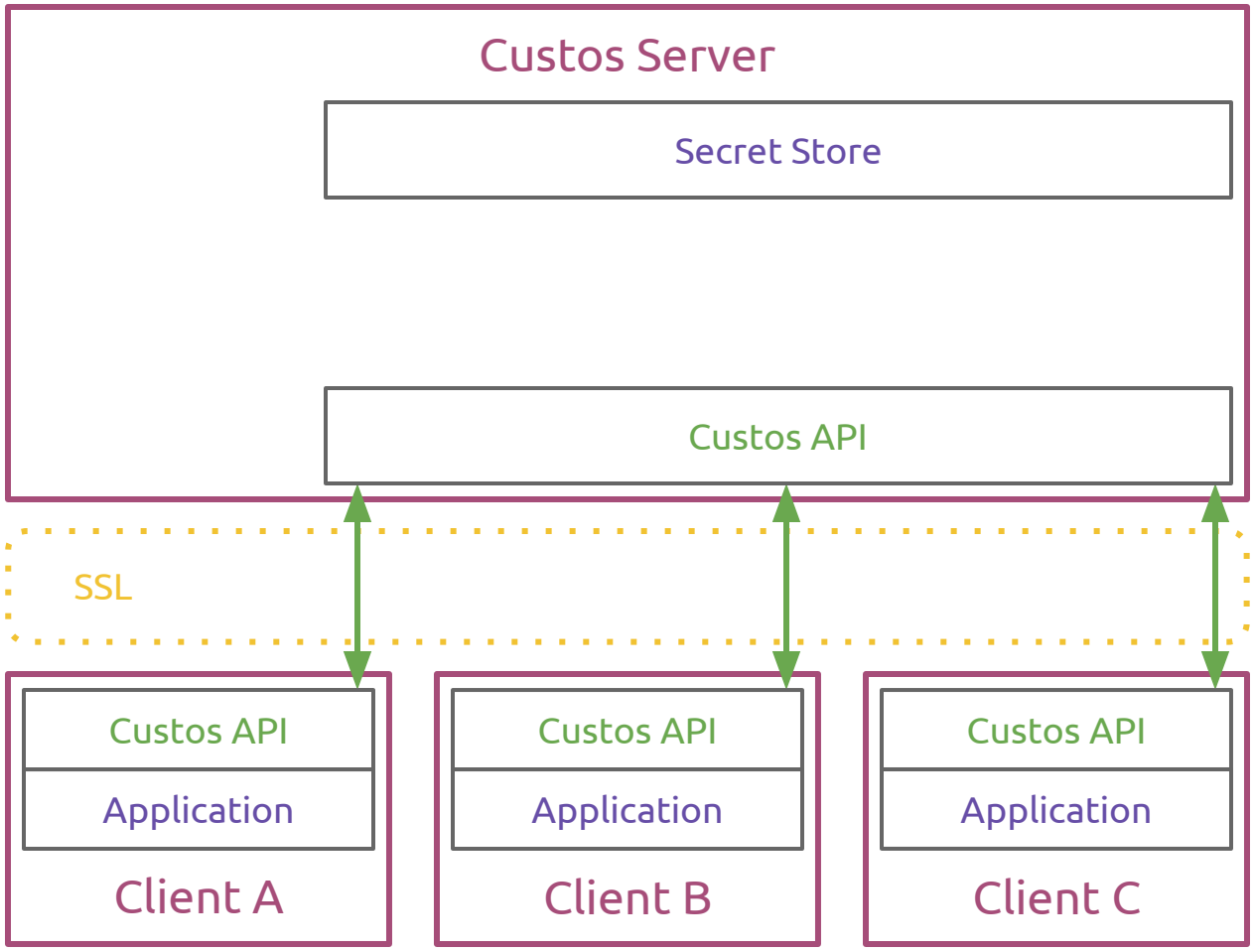


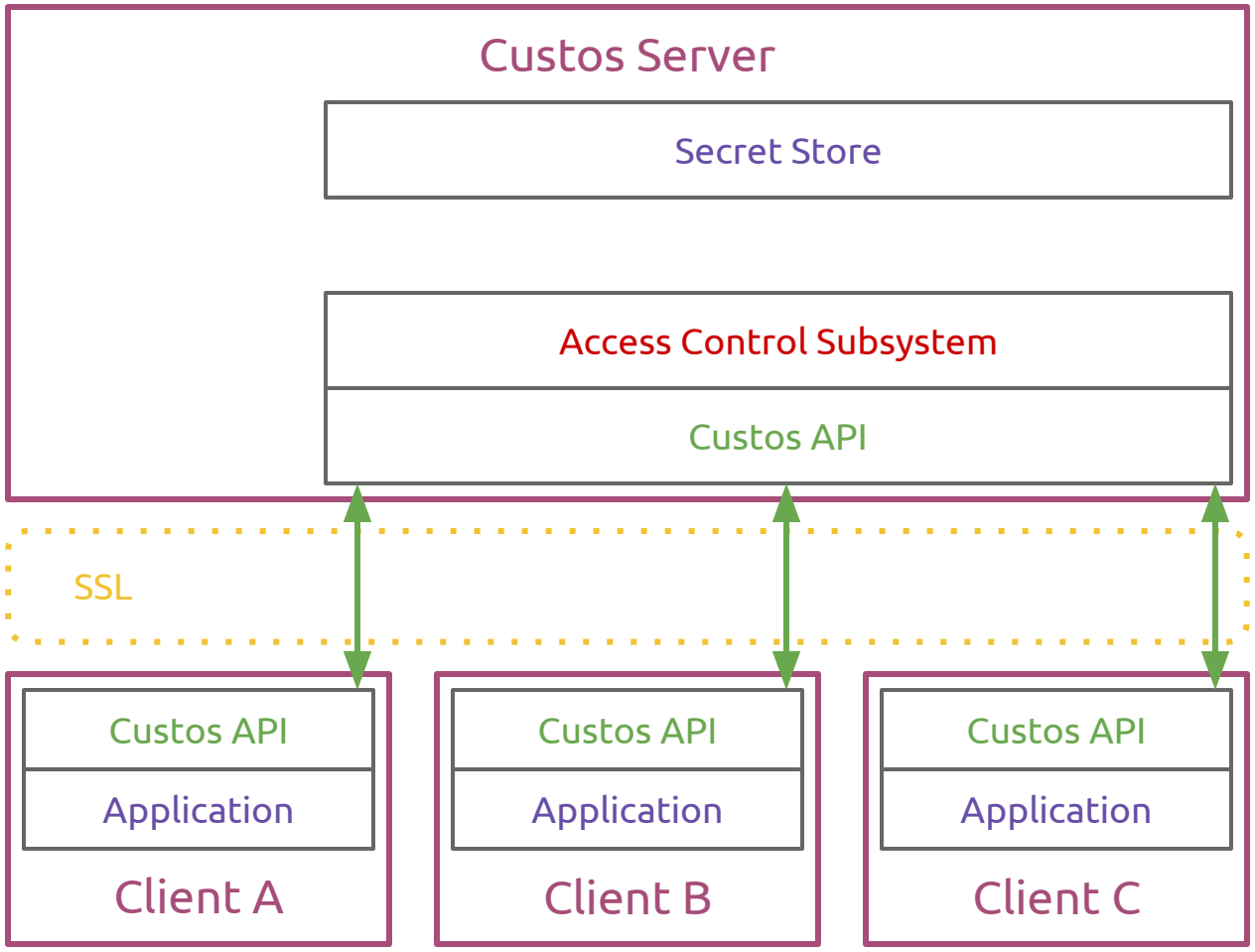
Backup Systems

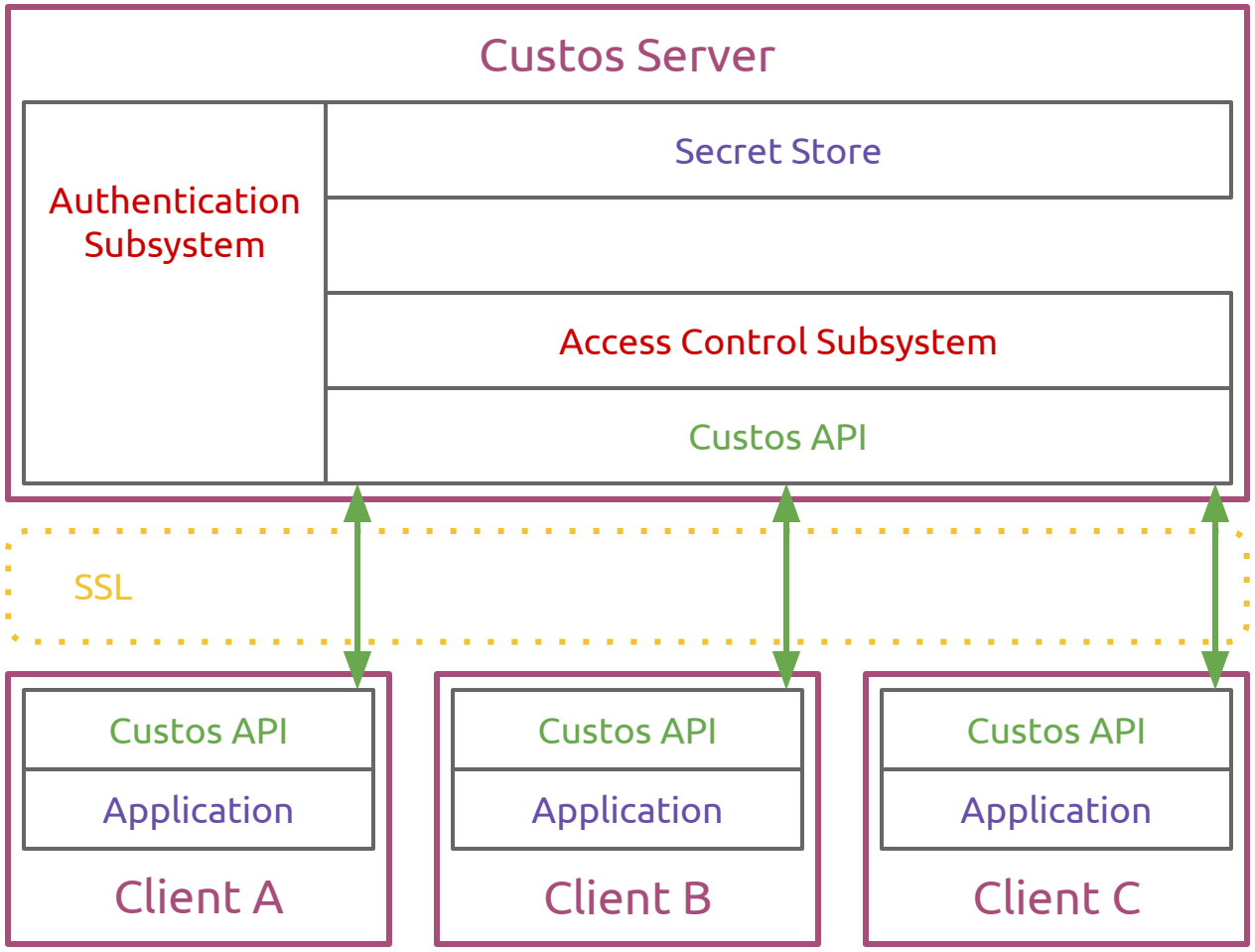
Backup Systems
Time-Limited Access

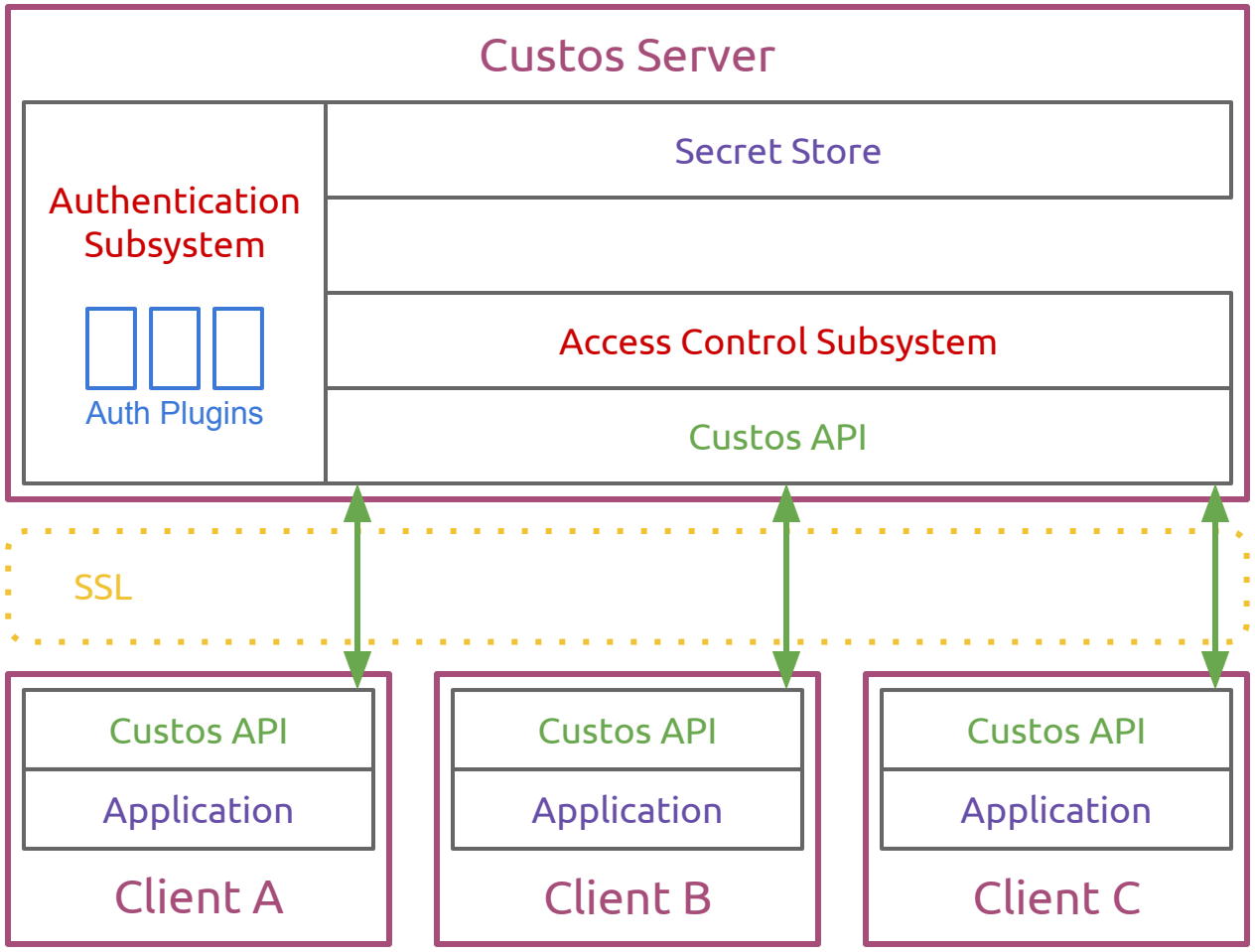
Backup Systems
Time-Limited Access
Etc...

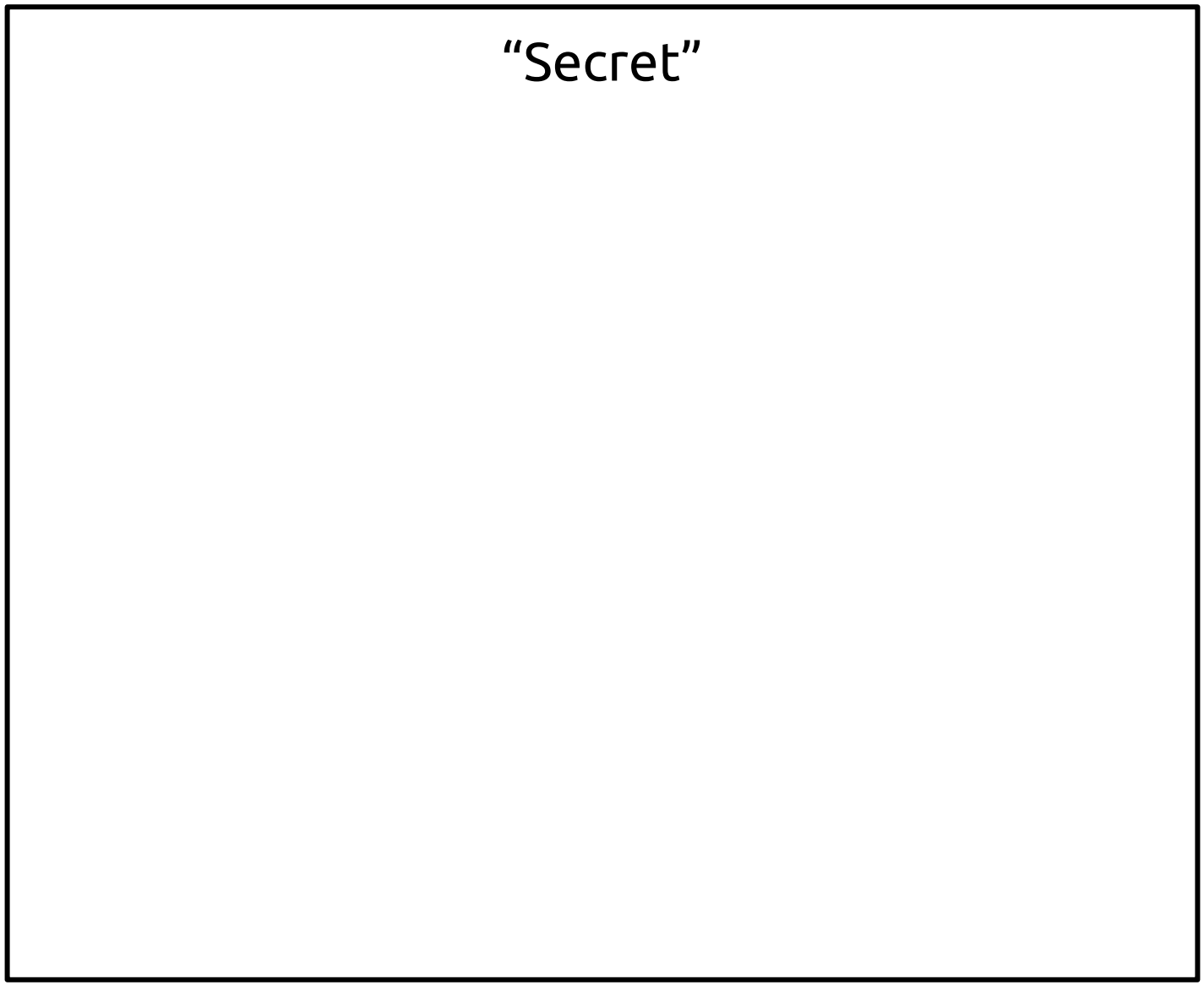
Flexible Access Control in Custos

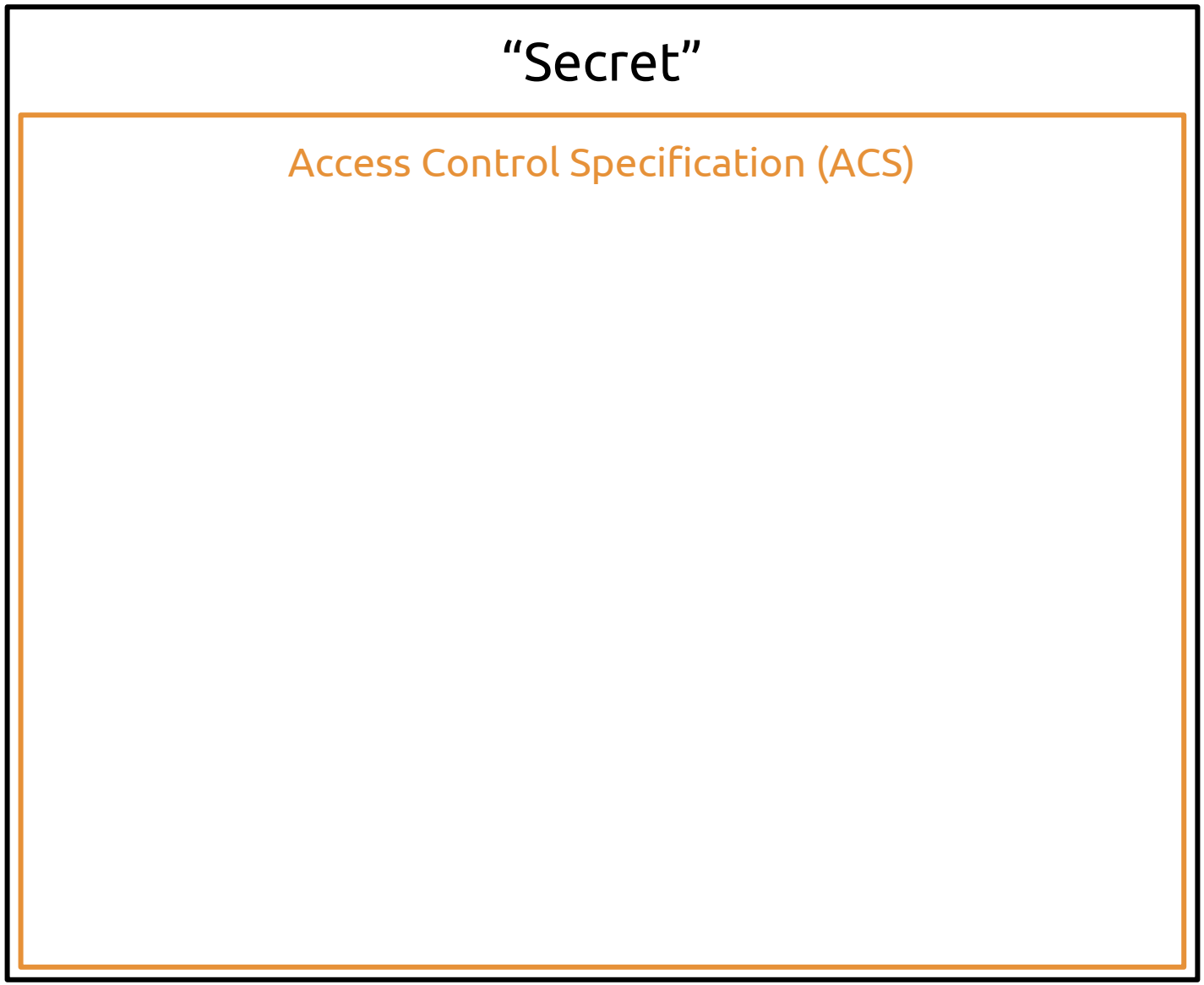

Custos Server
Secret Store
Custos API
SSL
Custos API
Application
Client A
Custos API
Application
Client B
Custos API
Application
Client C

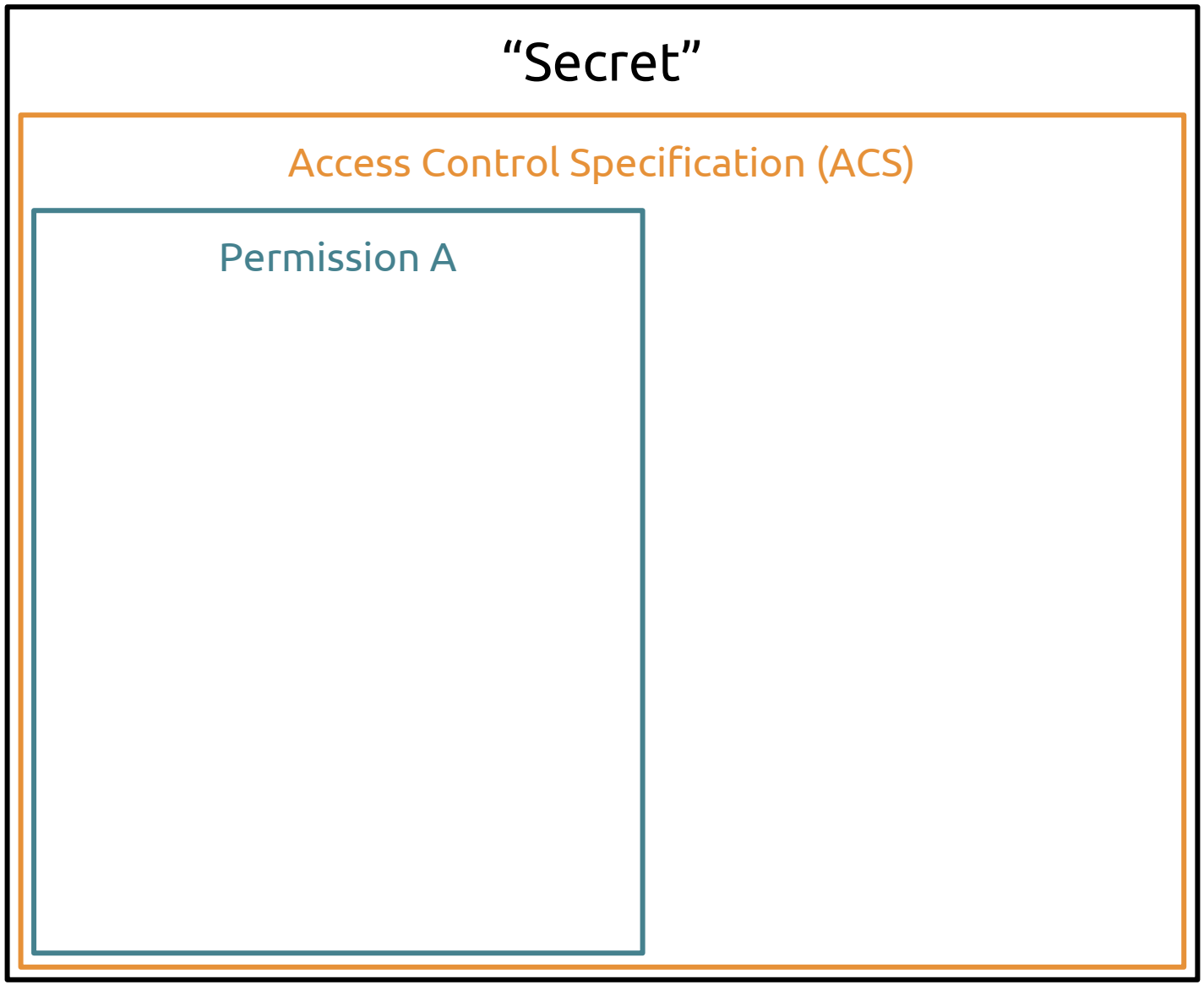

Custos Server
Secret Store
Access Control Subsystem
Custos API
SSL
Custos API
Application
Client A
Custos API
Application
Client B
Custos API
Application
Client C

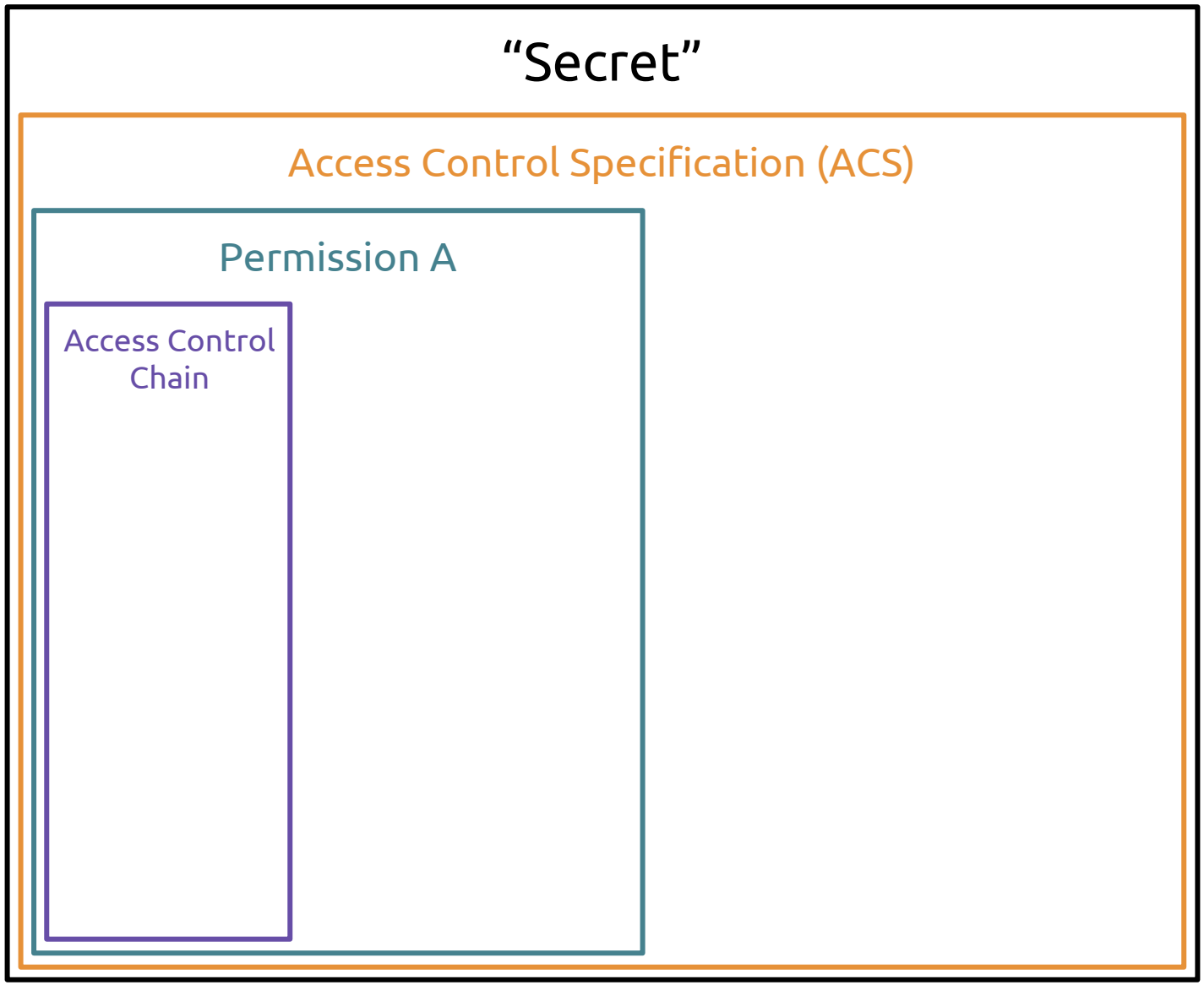

Custos Server
Authentication Subsystem
Secret Store
Access Control Subsystem
Custos API
SSL
Custos API
Application
Client A
Custos API
Application
Client B
Custos API
Application
Client C

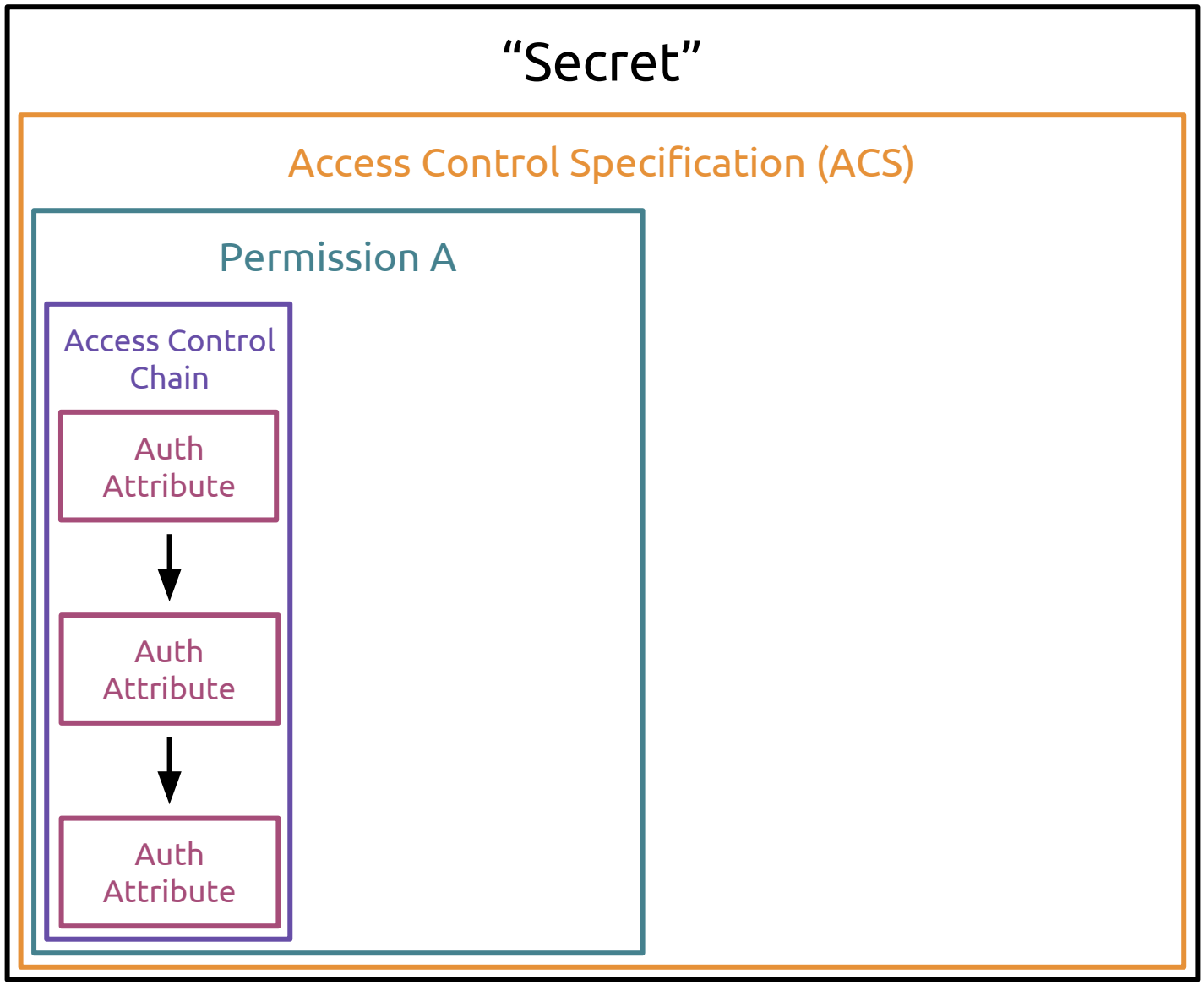

Custos Server
Authentication Subsystem
Auth Plugins
Secret Store
Access Control Subsystem
Custos API
SSL
Custos API
Application
Client A
Custos API
Application
Client B
Custos API
Application
Client C

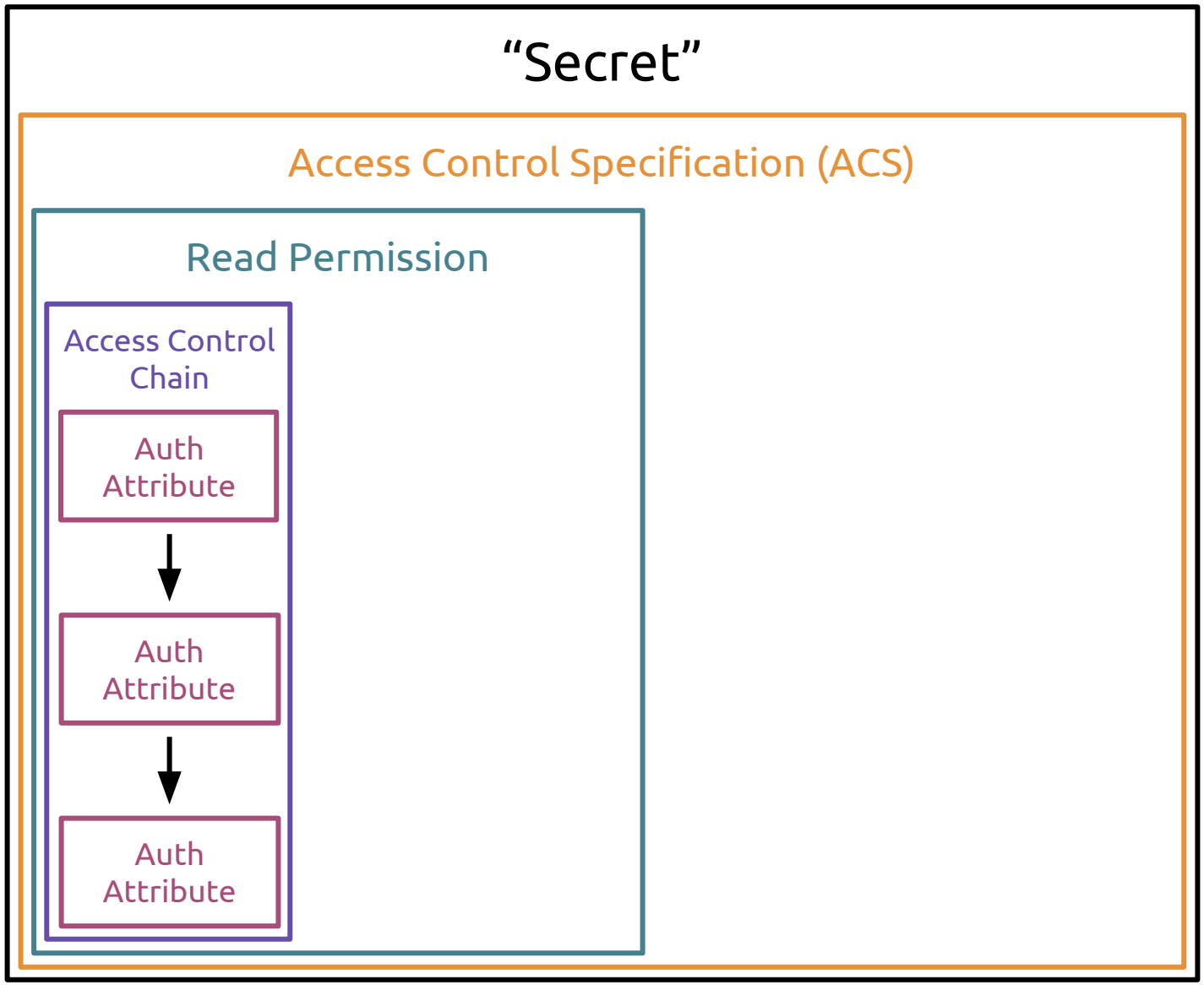

“Secret”

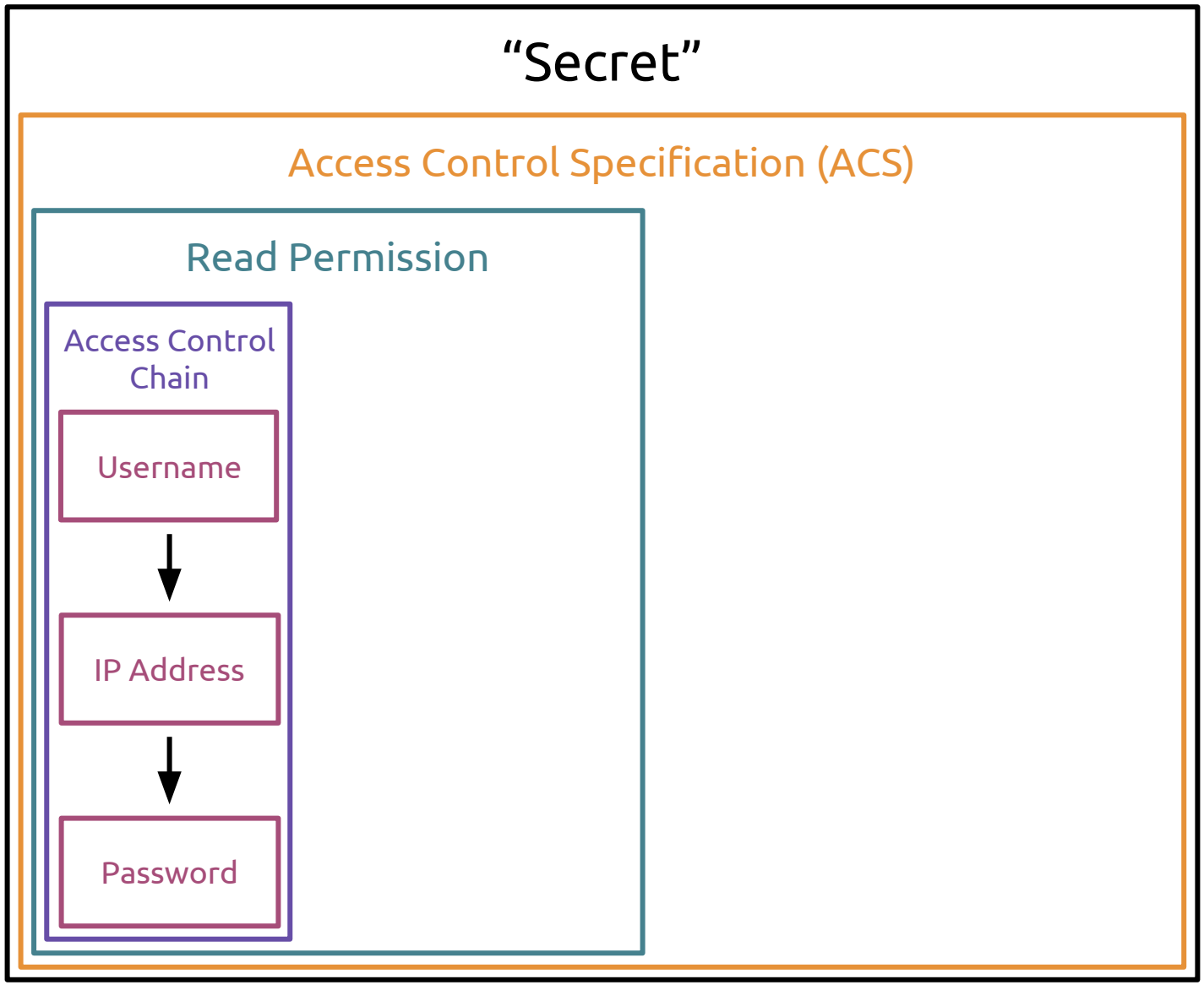

“Secret”
Access Control Specification (ACS)

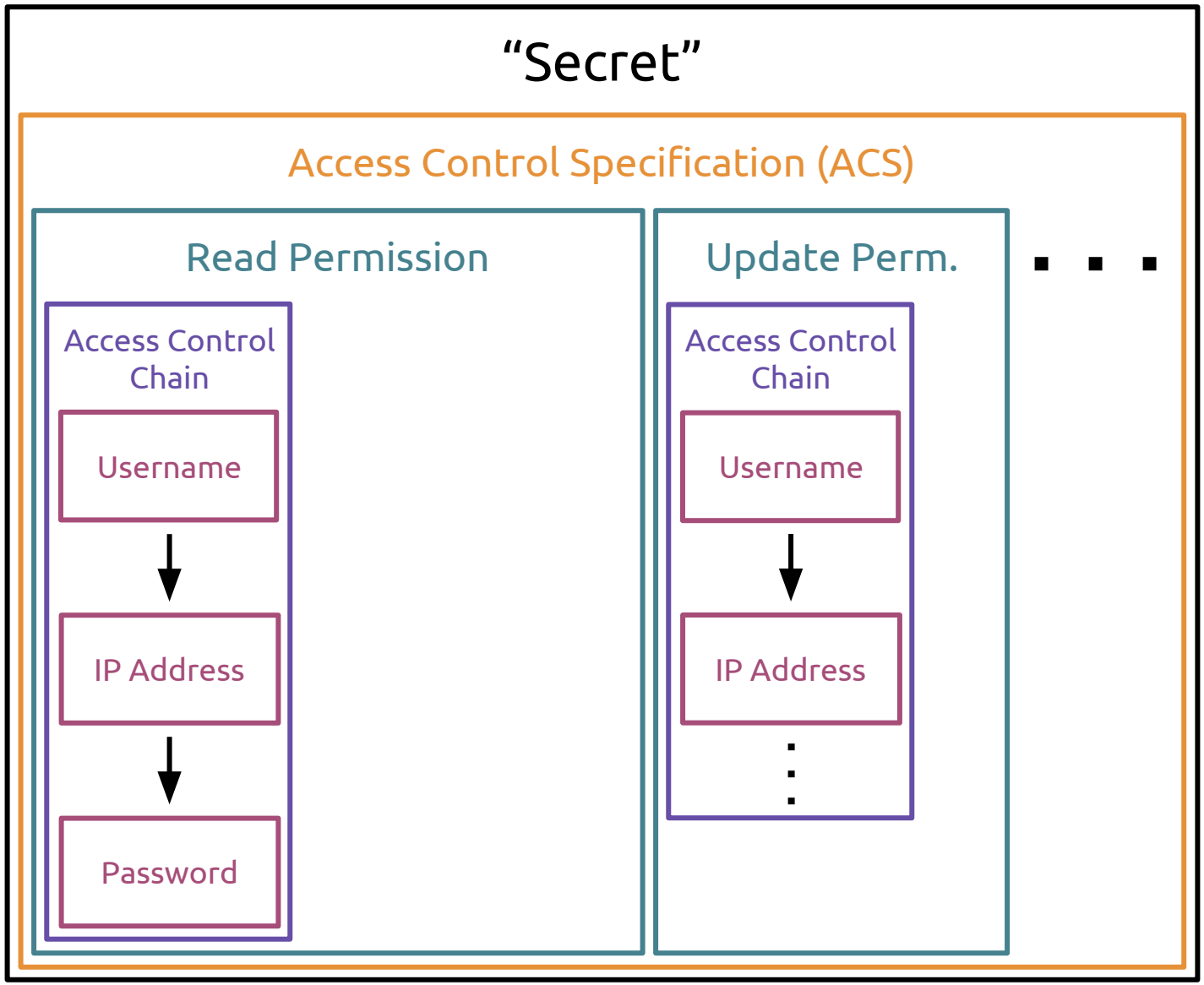

“Secret”
Access Control Specification (ACS)
Permission A

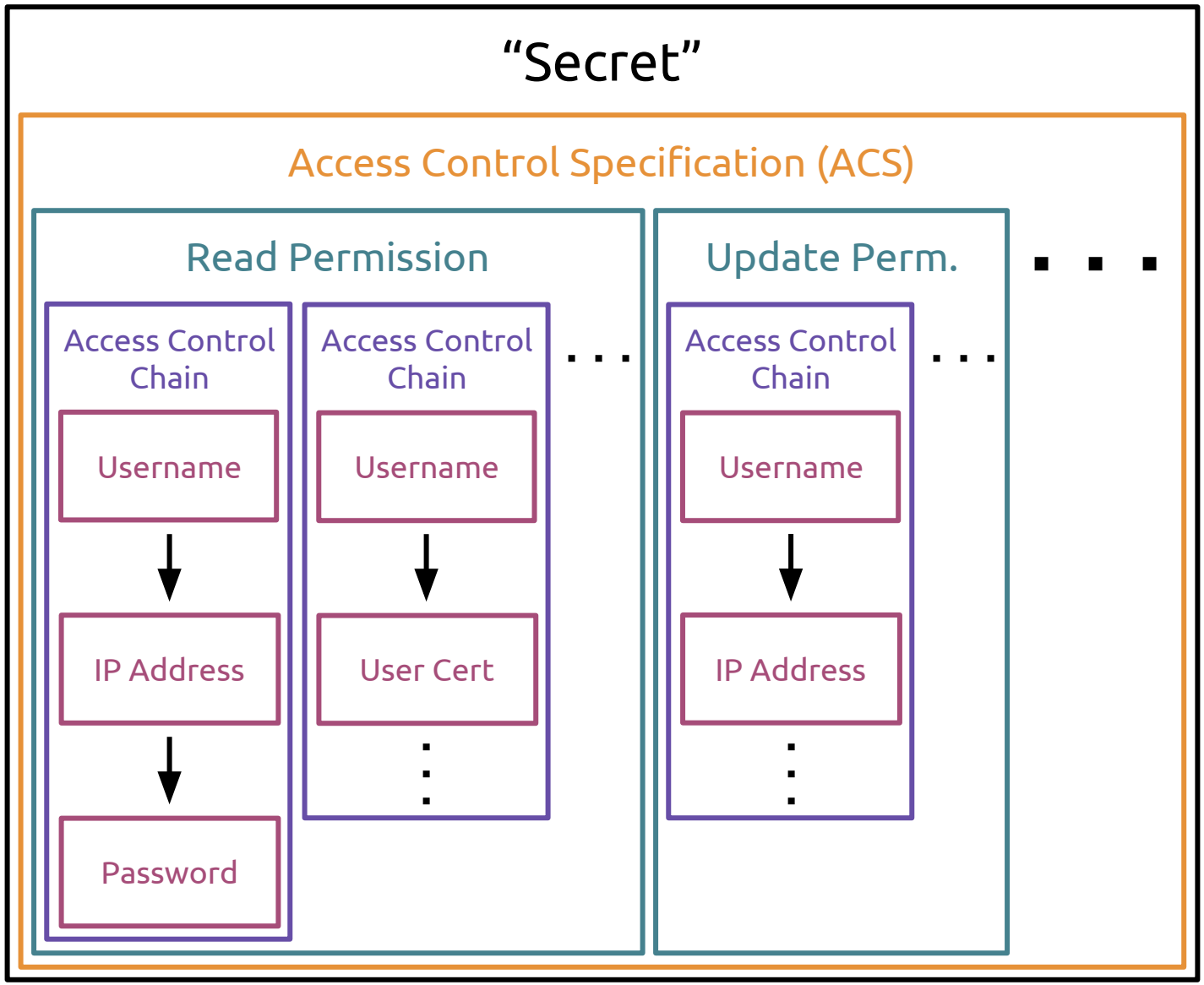

“Secret”
Access Control Specification (ACS)
Permission A
Access Control Chain


"Secret"
Access Control Specification (ACS)
Permission A
Access Control Chain
Auth Attribute
Auth Attribute
Auth Attribute


"Secret"
Access Control Specification (ACS)
Read Permission
Access Control Chain
Auth Attribute
Auth Attribute
Auth Attribute


"Secret"
Access Control Specification (ACS)
Read Permission
Access Control Chain
Username
IP Address
Password


"Secret"
Access Control Specification (ACS)
Read Permission
Access Control Chain
Username
IP Address
Password
Update Perm.
Access Control Chain
Username
IP Address


"Secret"
Access Control Specification (ACS)
Read Permission
Update Perm.
Access Control Chain
Username
IP Address
Password
Access Control Chain
Username
User Cert
Access Control Chain
Username
IP Address

Authentication Attributes

Authentication Attributes

Plugin-Based

Explicit

- ip_src
- user_agent
- time_utc
- ...

Implicit

- user_id
- psk
- psk_sha256
- ...

Centralized Secret Storage

Flexible Access Control

Centralized Secret Storage

Flexible Access Control

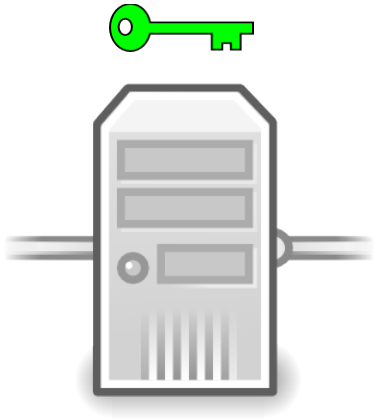
Auditing and Revocation

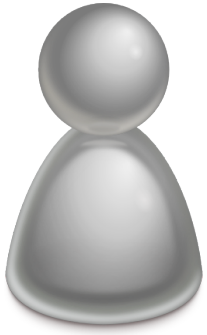
Example: Revoke Shared Access

Example: Revoke Shared Access

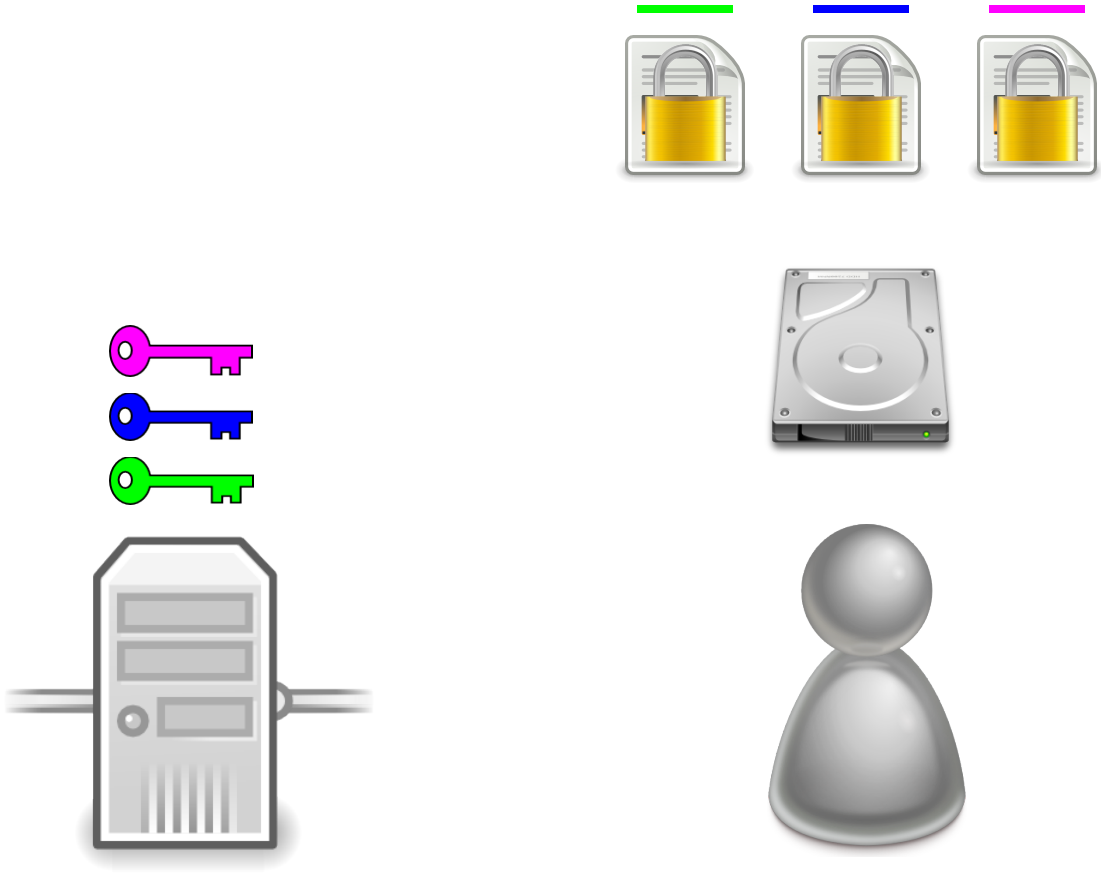
Example: Revoke Shared Access

Example: Revoke Shared Access

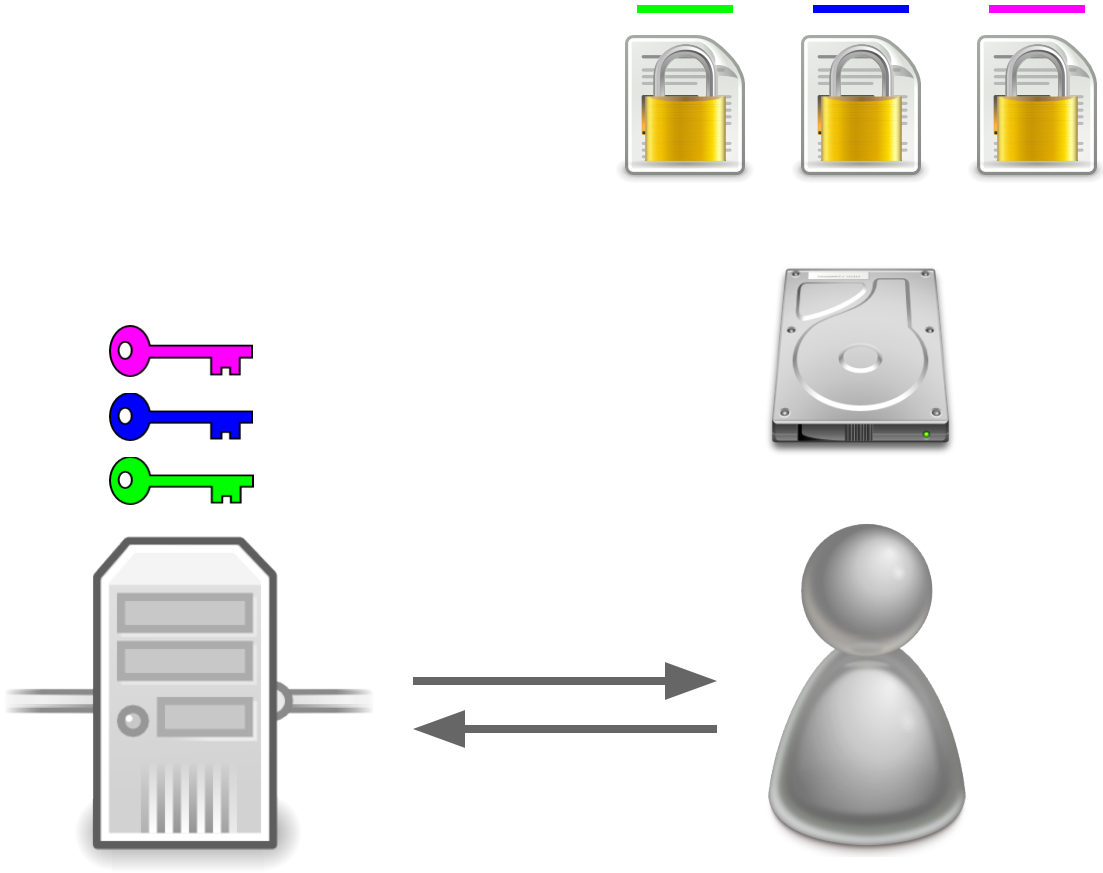




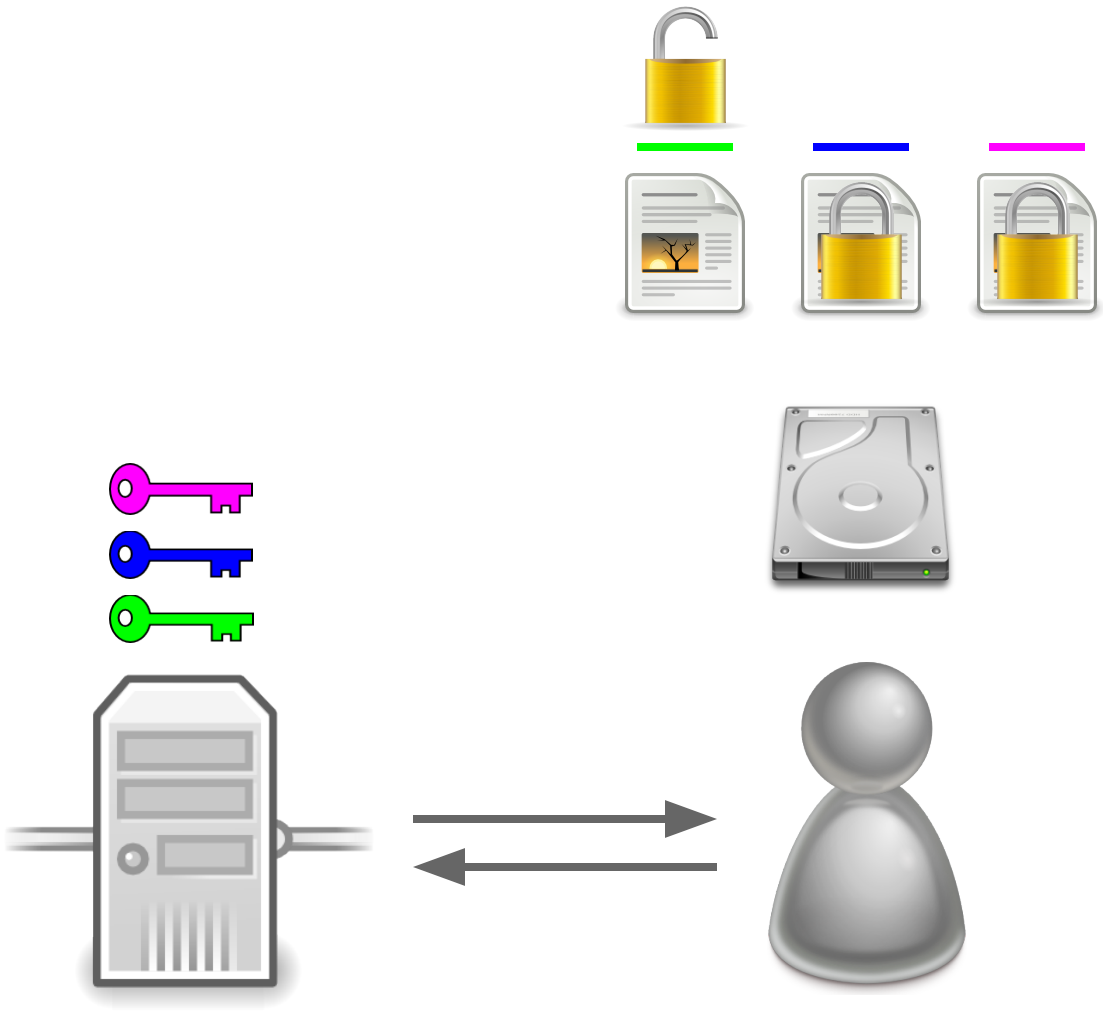
Example: Revoke Shared Access



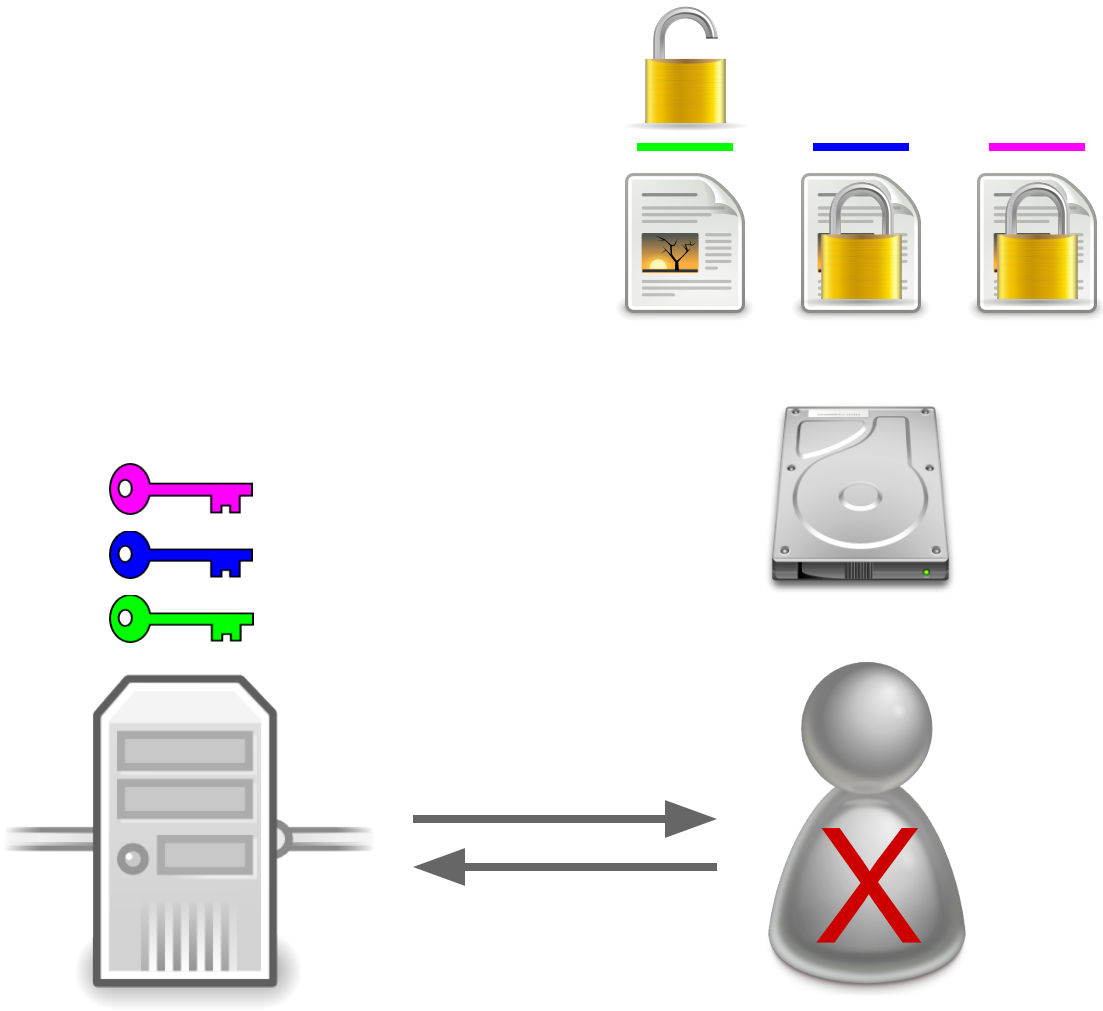
Example: Revoke Shared Access



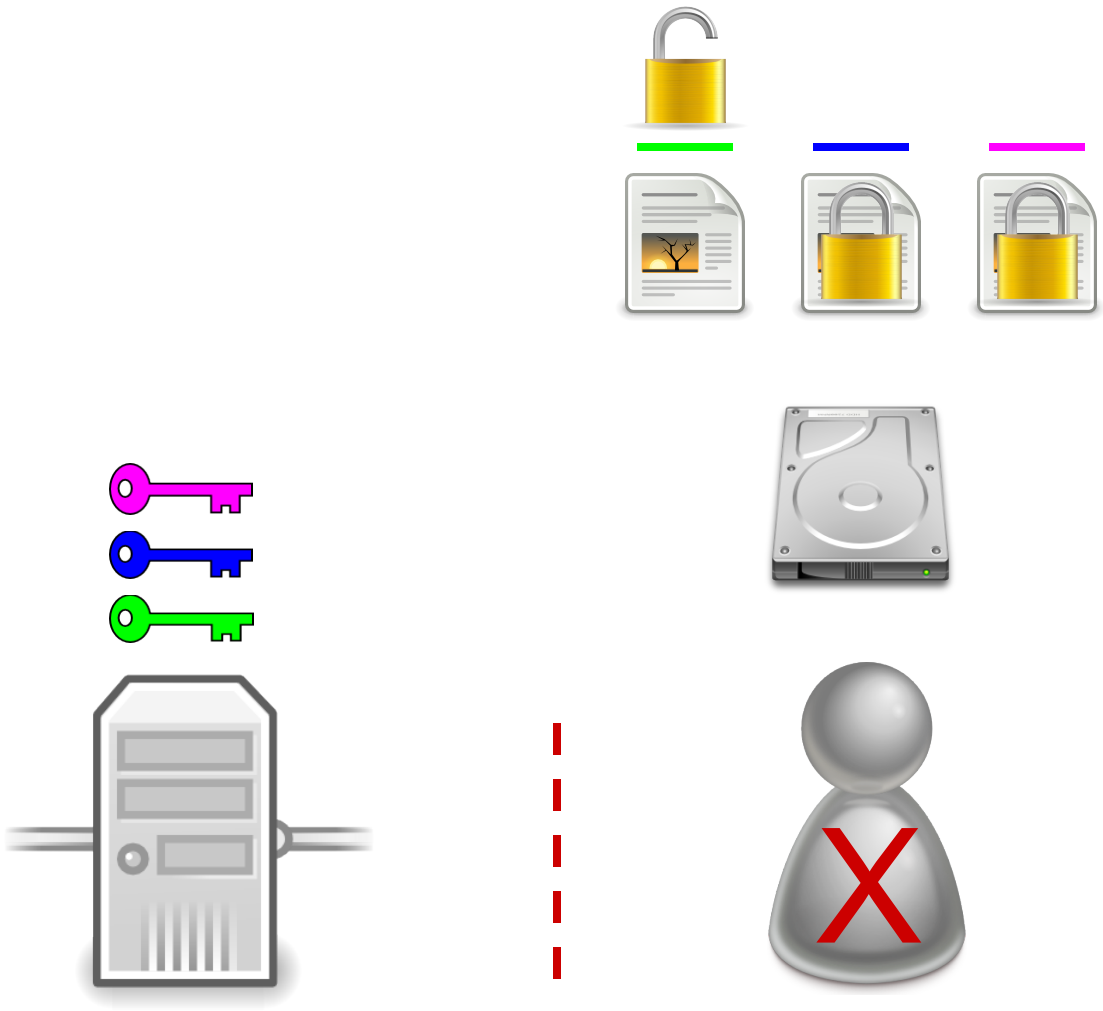
Example: Revoke Shared Access



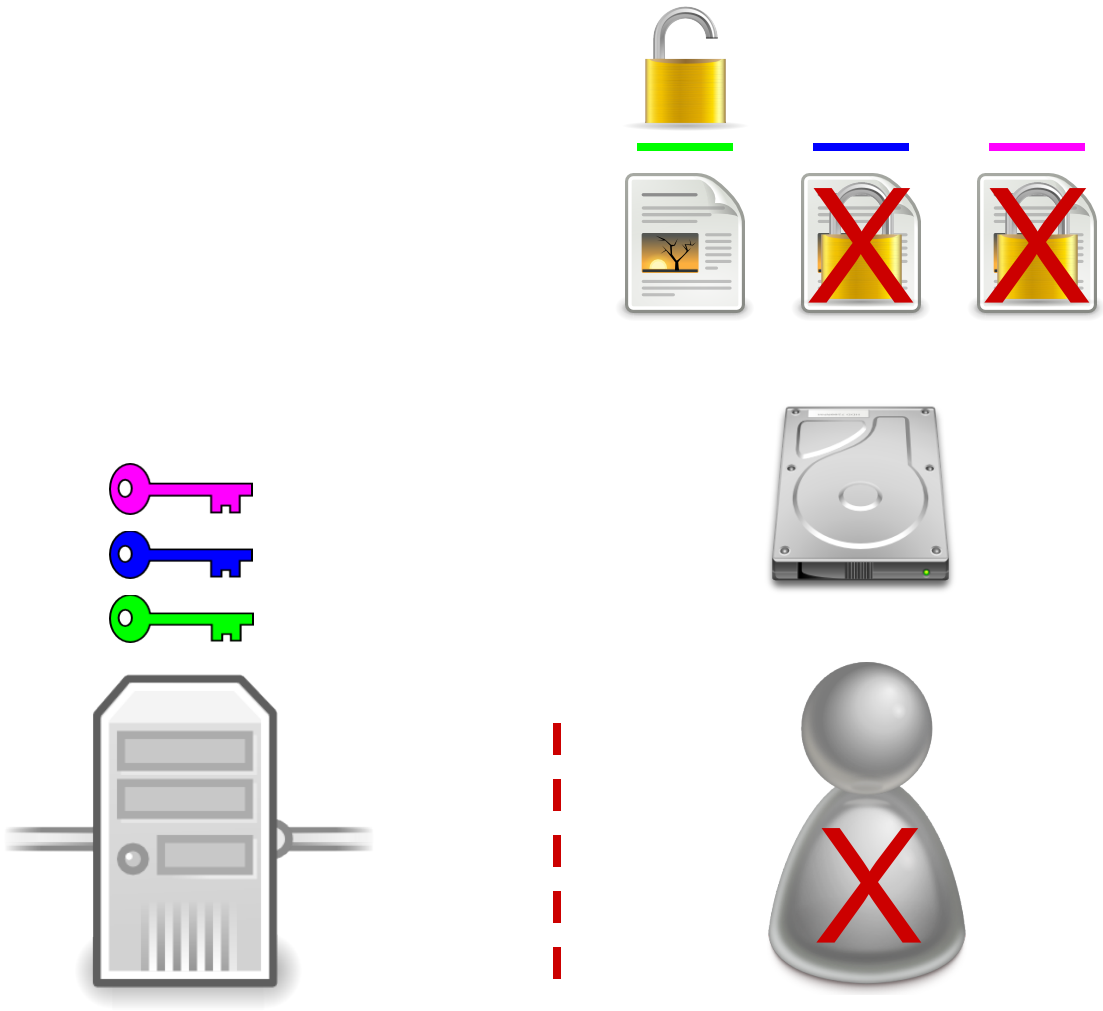
Example: Revoke Shared Access



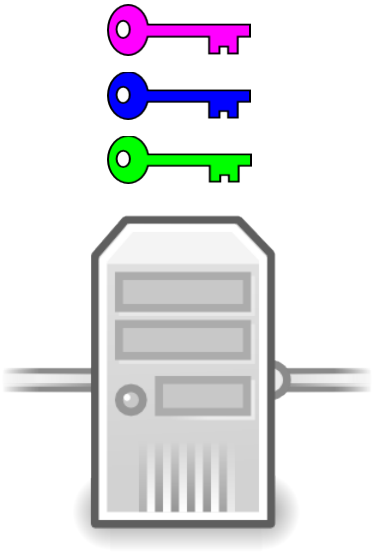
Example: Revoke Shared Access



Example: Revoke Shared Access

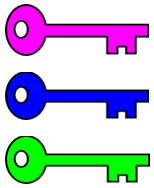


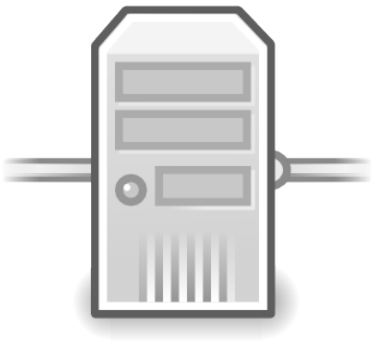
Example: Revoke Shared Access



140813: Bob Accessed 
140906: Bob Accessed 
141003: Bob Accessed 

Example: Revoke Shared Access



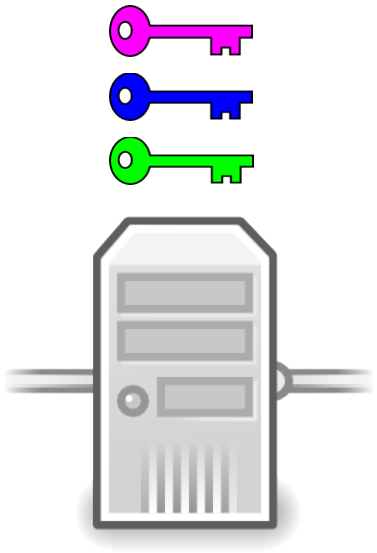


140813: Bob Accessed 

140906: Bob Accessed 

141003: Bob Accessed 

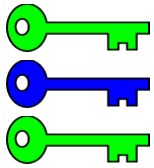
Example: Revoke Shared Access



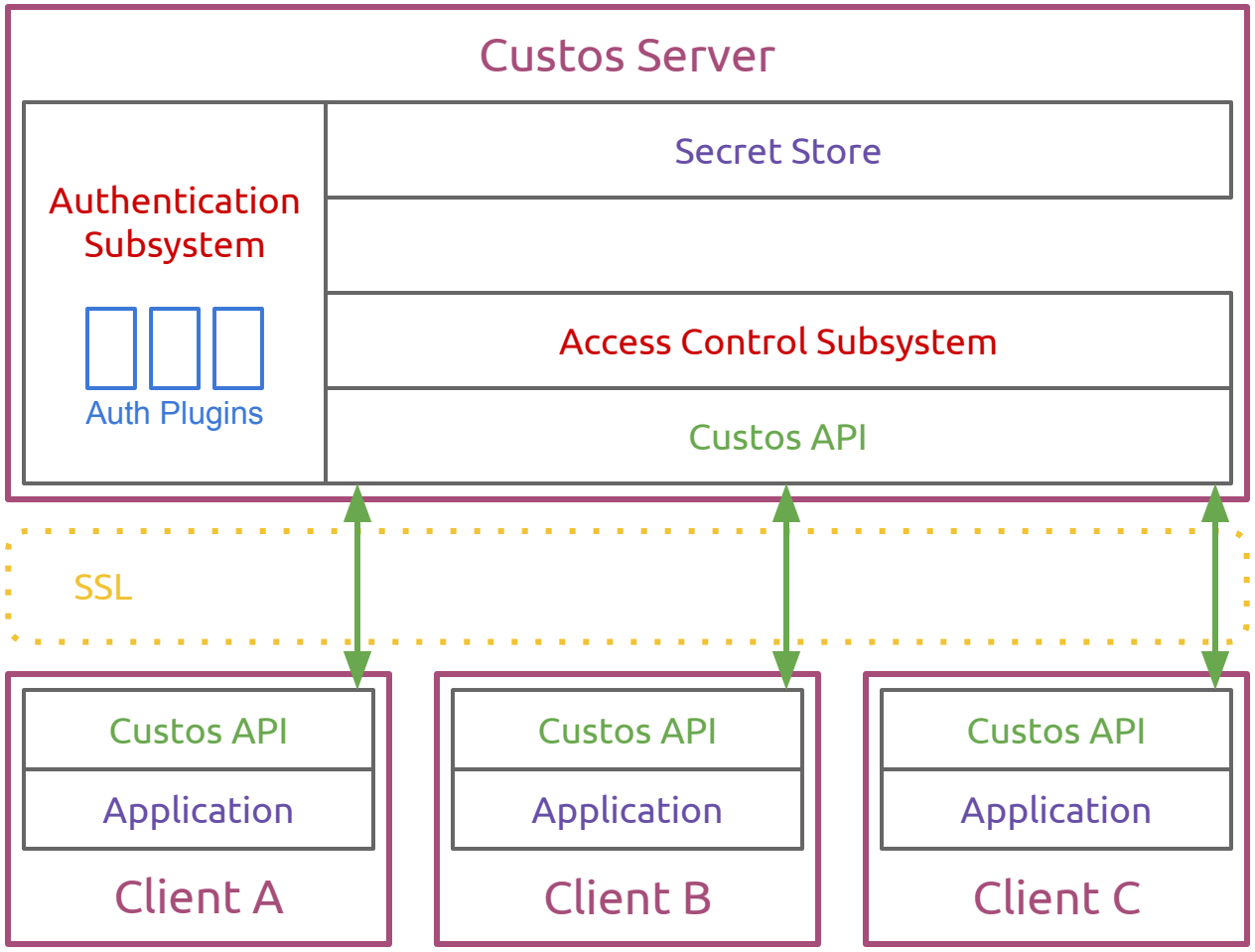
140813: Bob Accessed

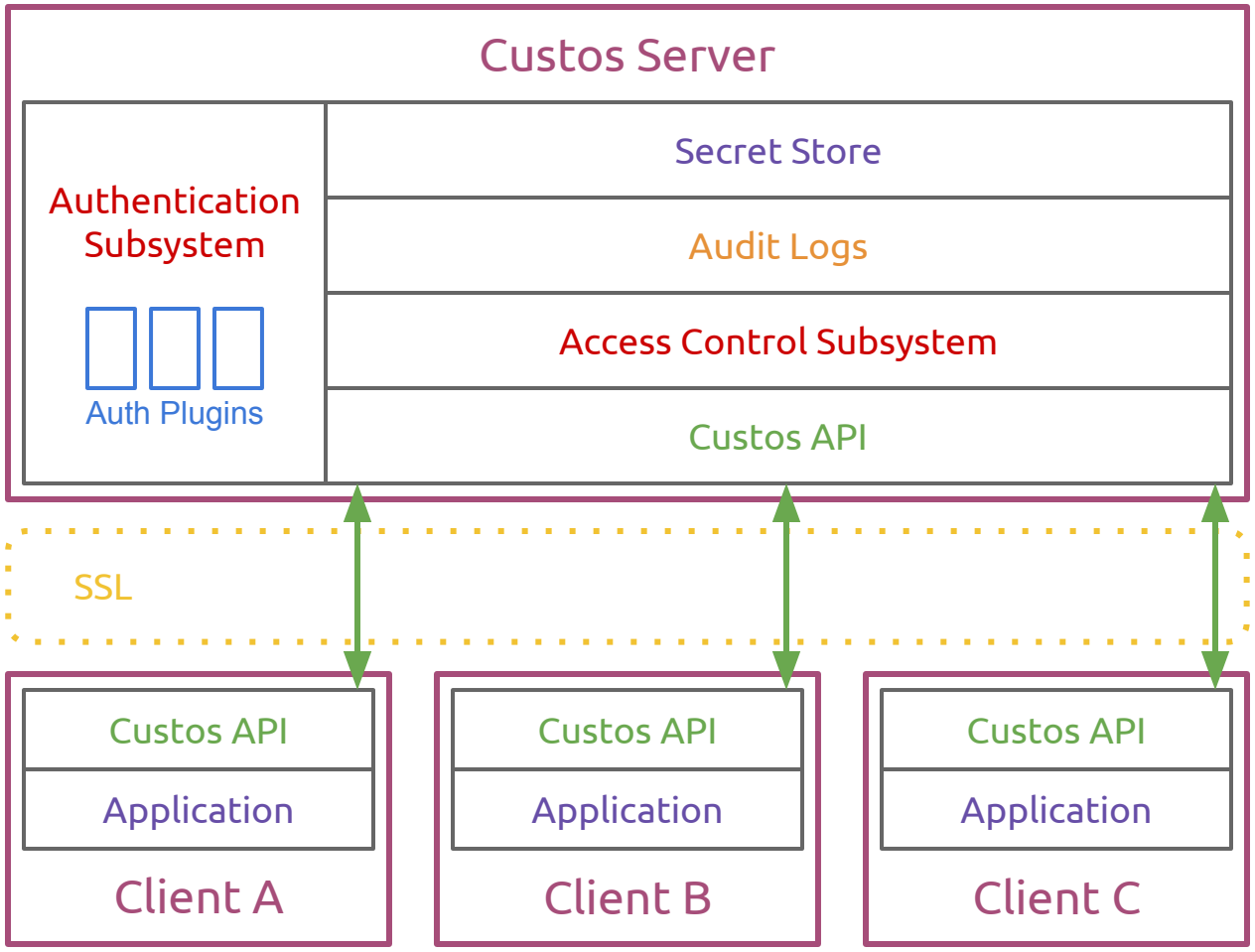
140906: Bob Accessed

141003: Bob Accessed



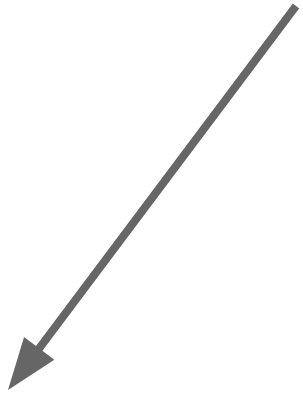
Auditing and Revocation in Custos


Custos Server
Authentication Subsystem
Auth Plugins
Secret Store
Access Control Subsystem
Custos API
SSL
Custos API
Application
Client A
Custos API
Application
Client B
Custos API
Application
Client C


Custos Server
Authentication Subsystem
Auth Plugins
Secret Store
Audit Logs
Access Control Subsystem
Custos API
SSL
Custos API
Application
Client A
Custos API
Application
Client B
Custos API
Application
Client C

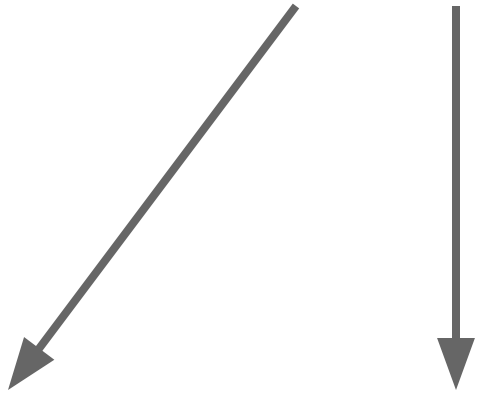
140813: Bob Accessed Key A
140906: Bob Accessed Key B
141003: Bob Accessed Key A

```
140813: Bob Accessed Key A
140906: Bob Accessed Key B
141003: Bob Accessed Key A
```



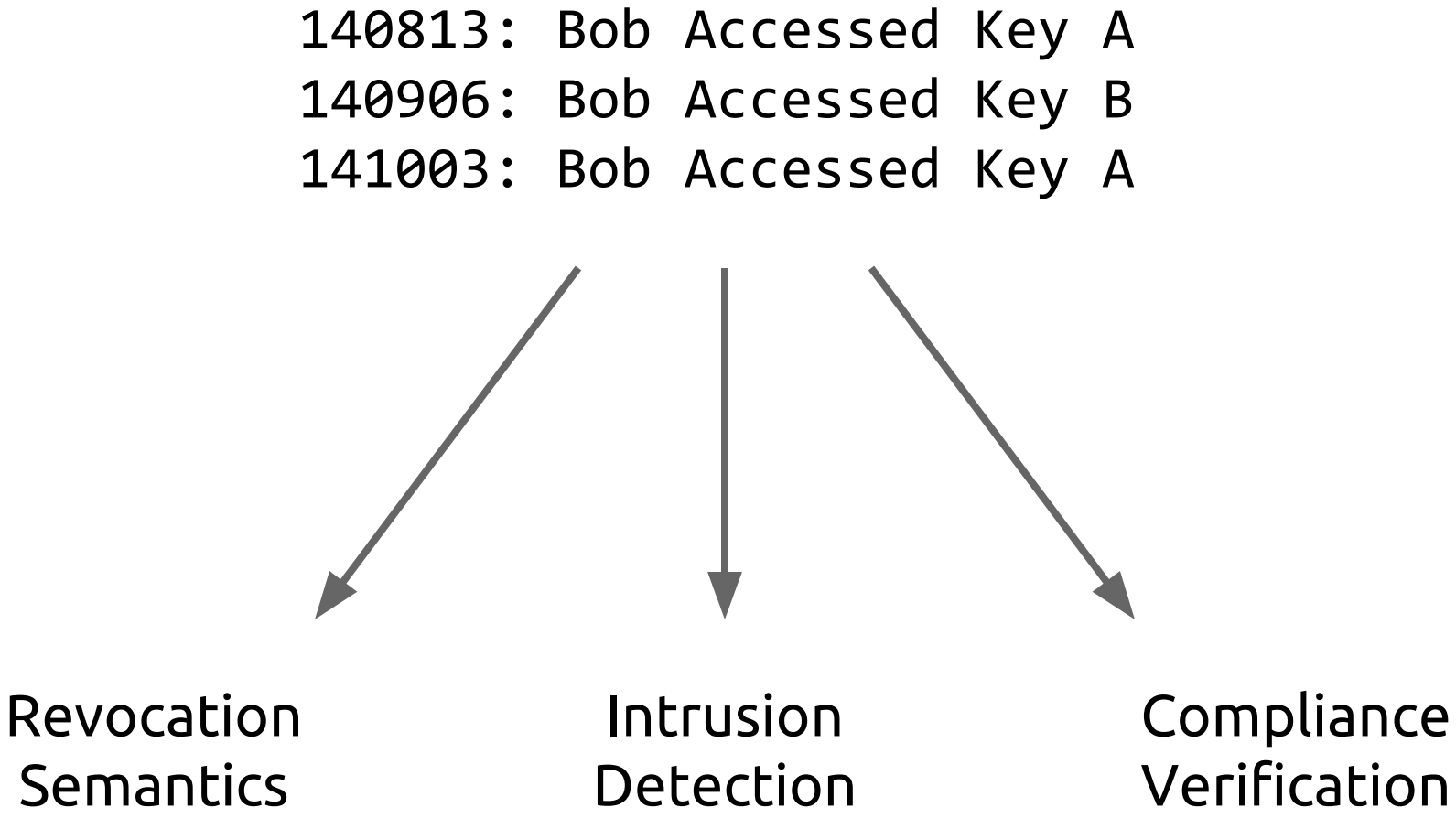
Revocation
Semantics

```
140813: Bob Accessed Key A
140906: Bob Accessed Key B
141003: Bob Accessed Key A
```



Revocation Semantics

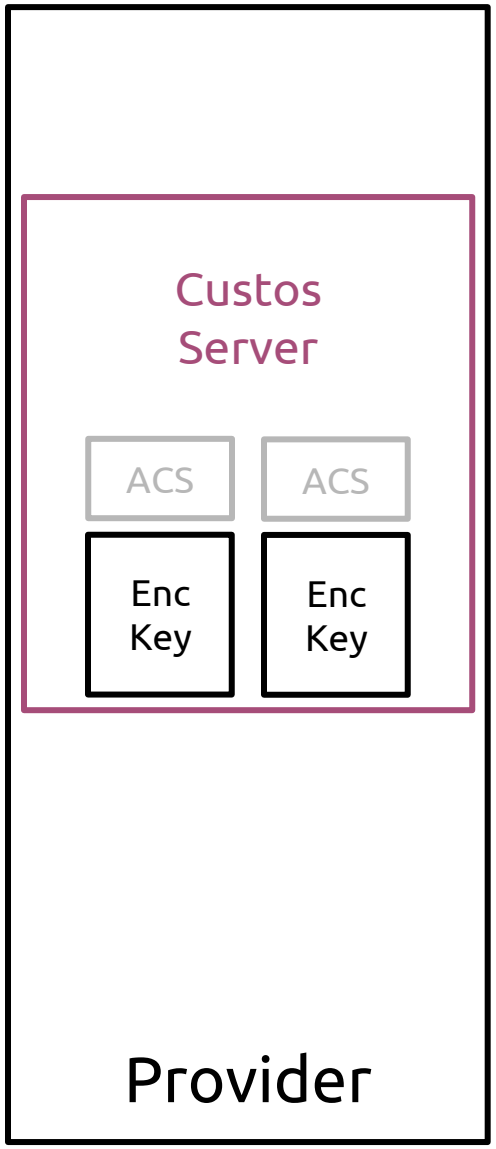
Intrusion Detection

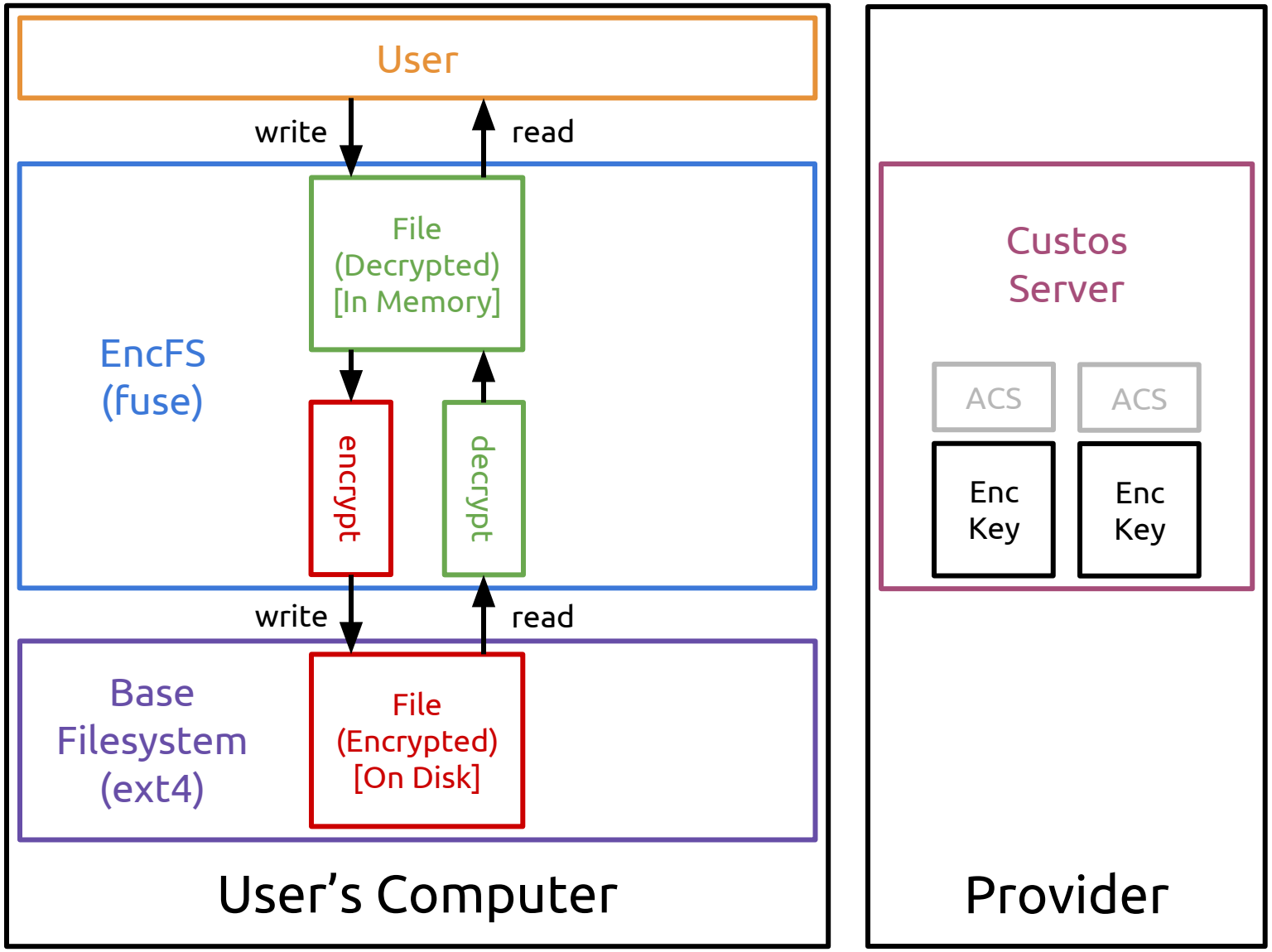

140813: Bob Accessed Key A
140906: Bob Accessed Key B
141003: Bob Accessed Key A
Revocation Semantics
Intrusion Detection
Compliance Verification

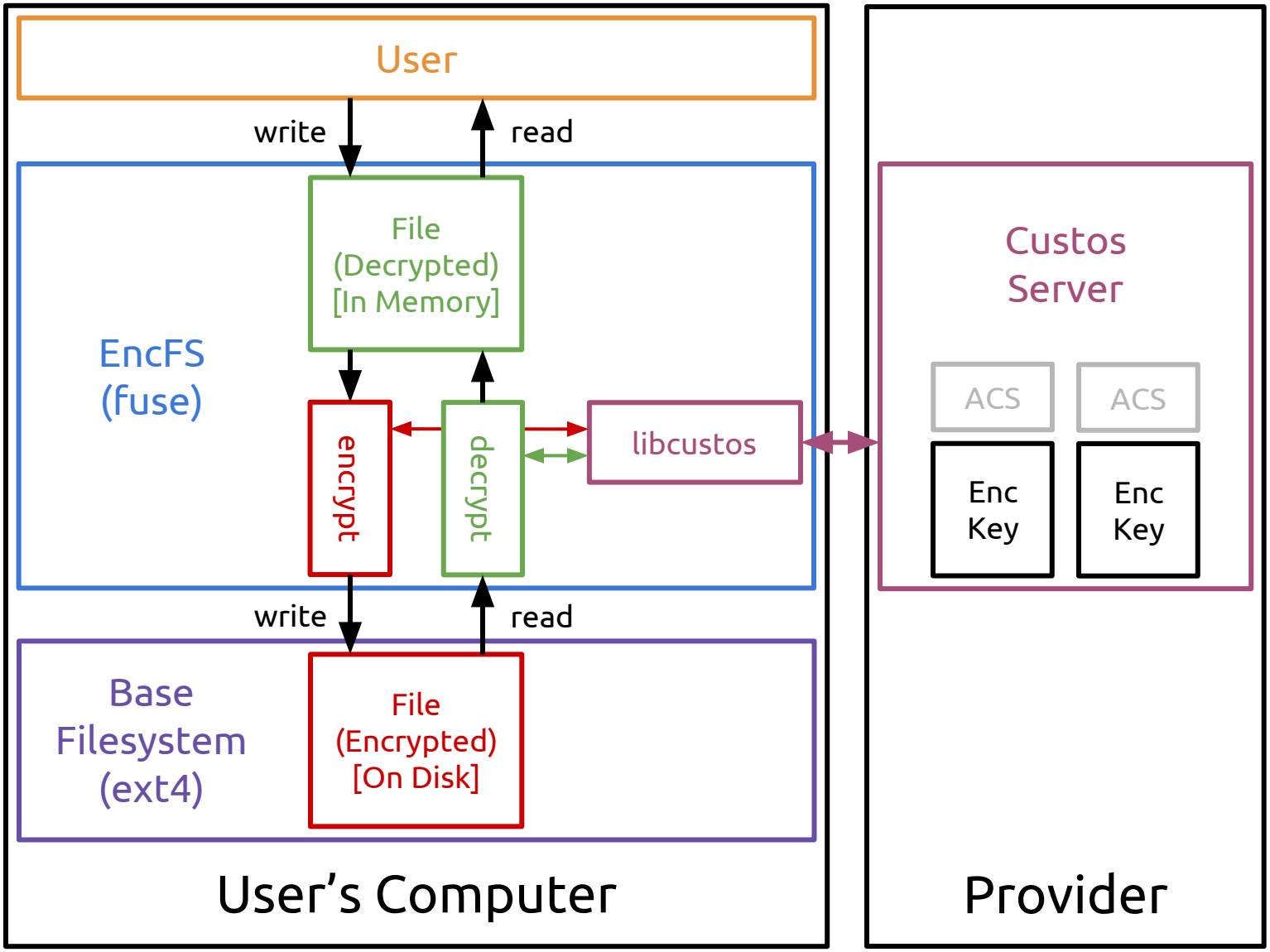
Custos Prototype

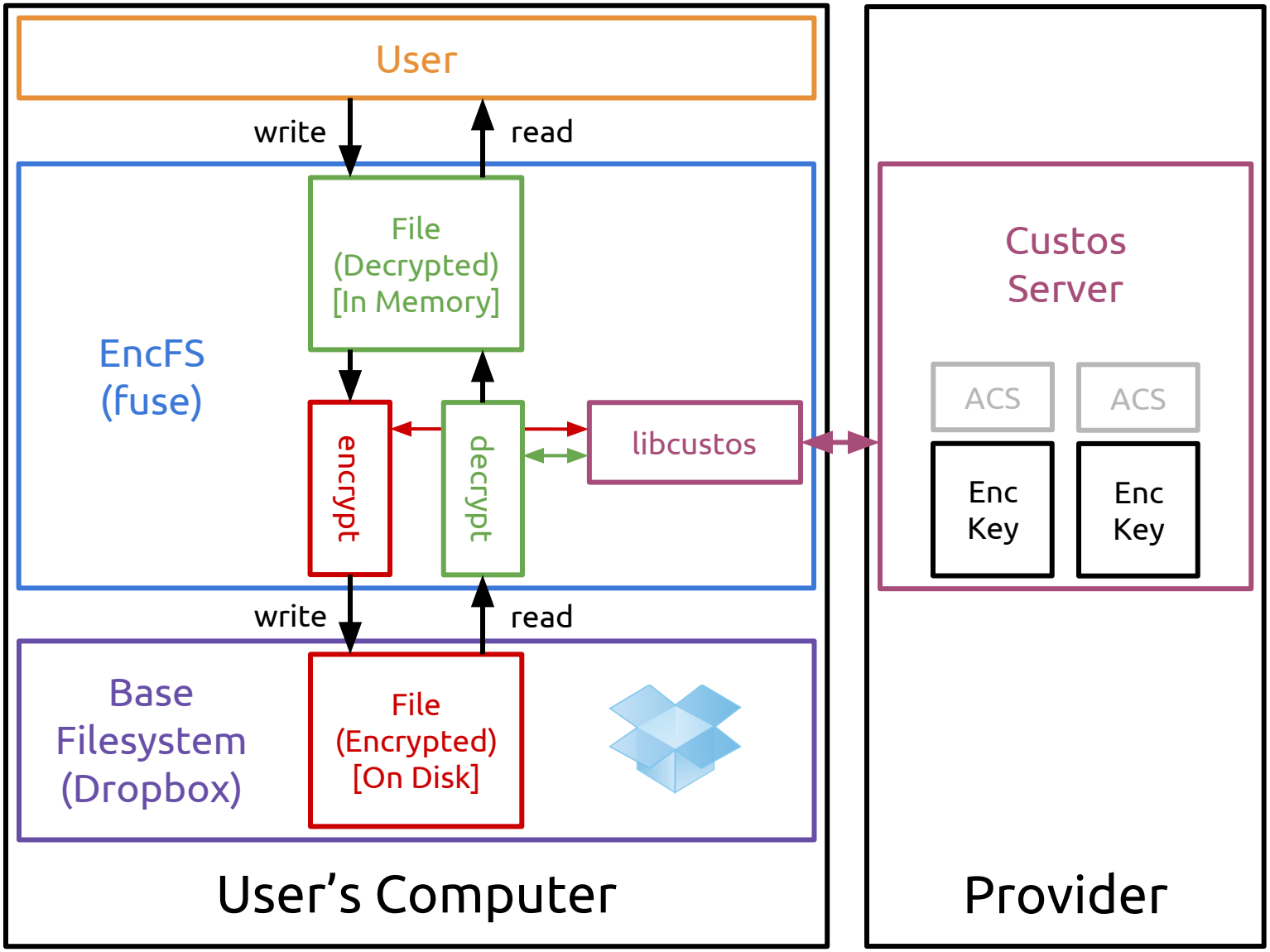
Custos Prototype

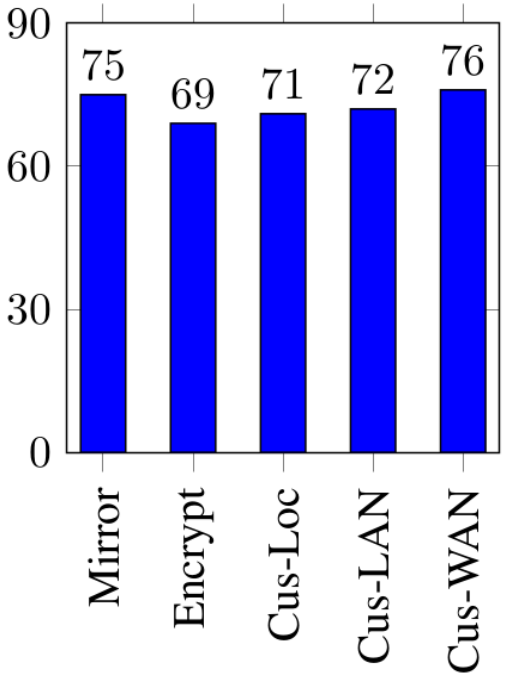
EncFS: Custos-Backed Encrypted File System


Custos
Server
ACS
ACS
Enc
Key
Enc
Key
Provider

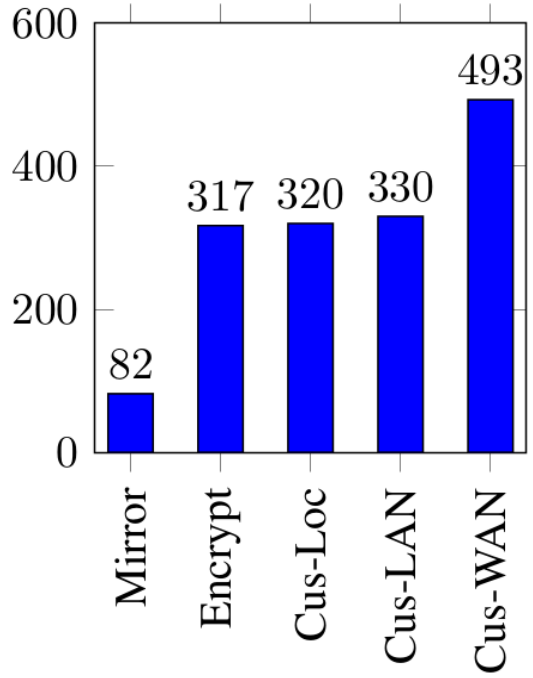

User
write
read
File
(Decrypted)
[In Memory]
EncFS
(fuse)
encrypt
decrypt
write
read
Base
Filesystem
(ext4)
File
(Encrypted)
[On Disk]
User's Computer
Custos
Server
ACS
ACS
Enc
Key
Enc
Key
Provider


User
write
read
File
(Decrypted)
[In Memory]
EncFS
(fuse)
encrypt
decrypt
libcustos
write
read
Base
Filesystem
(ext4)
File
(Encrypted)
[On Disk]
User's Computer
Custos
Server
ACS
ACS
Enc
Key
Enc
Key
Provider

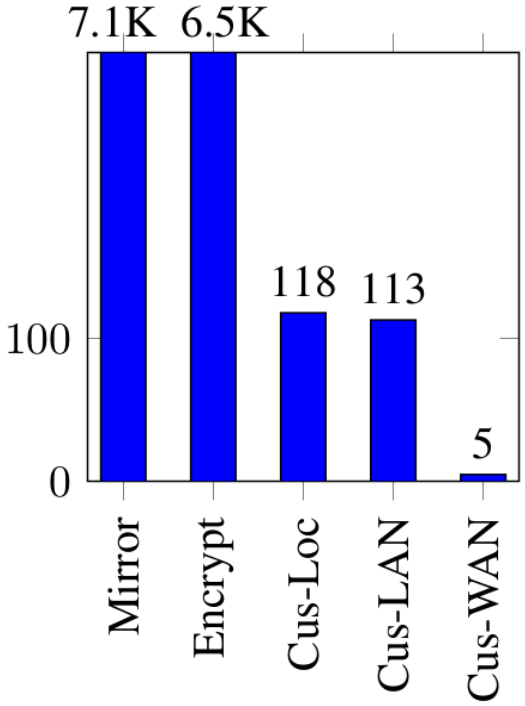

User
write
read
File
(Decrypted)
[In Memory]
EncFS
(fuse)
encrypt
decrypt
libcustos
write
read
Base
Filesystem
(Dropbox)
File
(Encrypted)
[On Disk]
User's Computer
Custos
Server
ACS
ACS
Enc
Key
Enc
Key
Provider



(a) `dd` Copy Throughput (MB/s)



(b) `ioping` Write Latency (ms)



(c) `bonnie++` Create IOPS

Current and Future Work

Additional Client Applications
(SSH Key Manager, PKCS11 SSL Processor, Etc)

Additional Client Applications
(SSH Key Manager, PKCS11 SSL Processor, Etc)

Better Management of Secret Sharing

Additional Client Applications
(SSH Key Manager, PKCS11 SSL Processor, Etc)

Better Management of Secret Sharing

Audit Log Heuristics and Analysis

Custos

Key Storage as a Service

Centralized Secret Storage

Centralized Secret Storage

Flexible Access Control

Centralized Secret Storage

Flexible Access Control

Auditing and Revocation

Making Encryption More

Usable | Flexible | Applicable

Key Storage as a Service

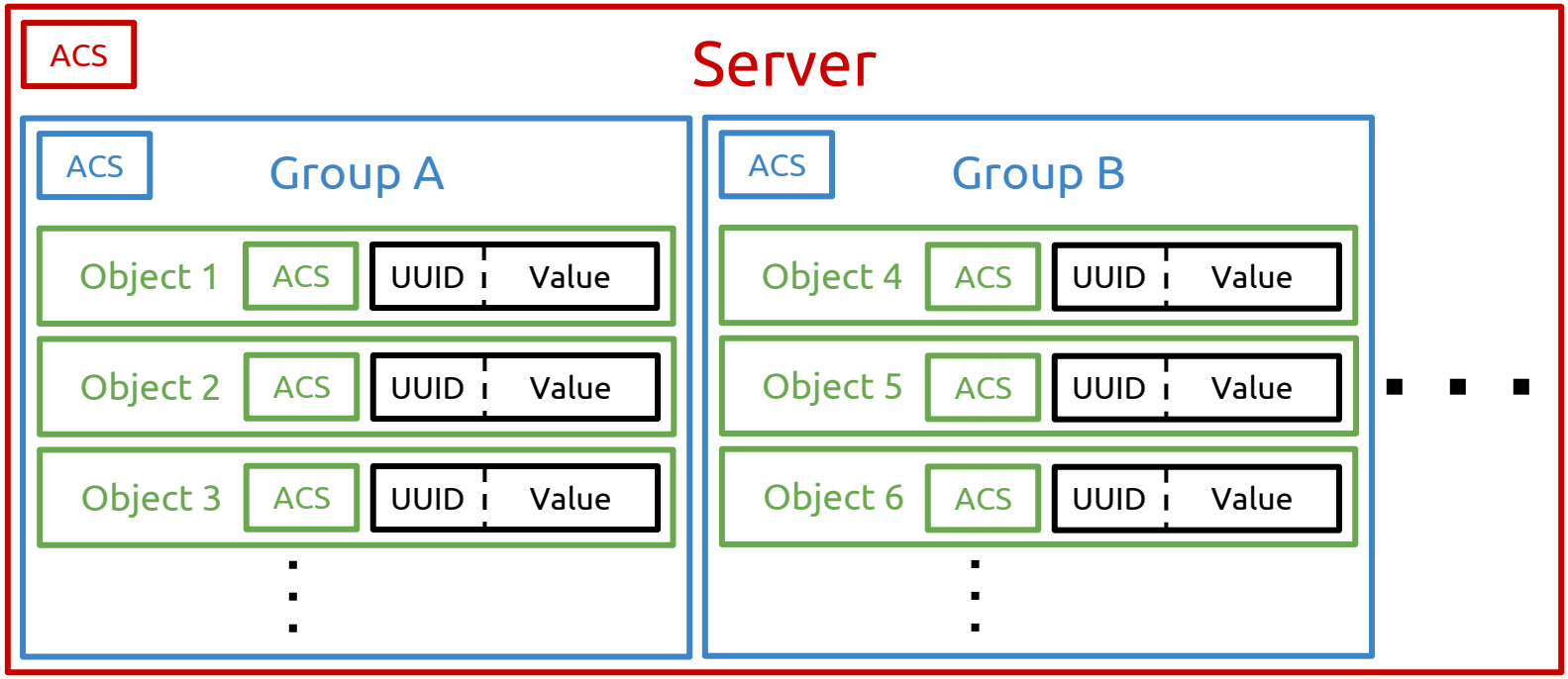
Ecosystem

Thank You

Questions?

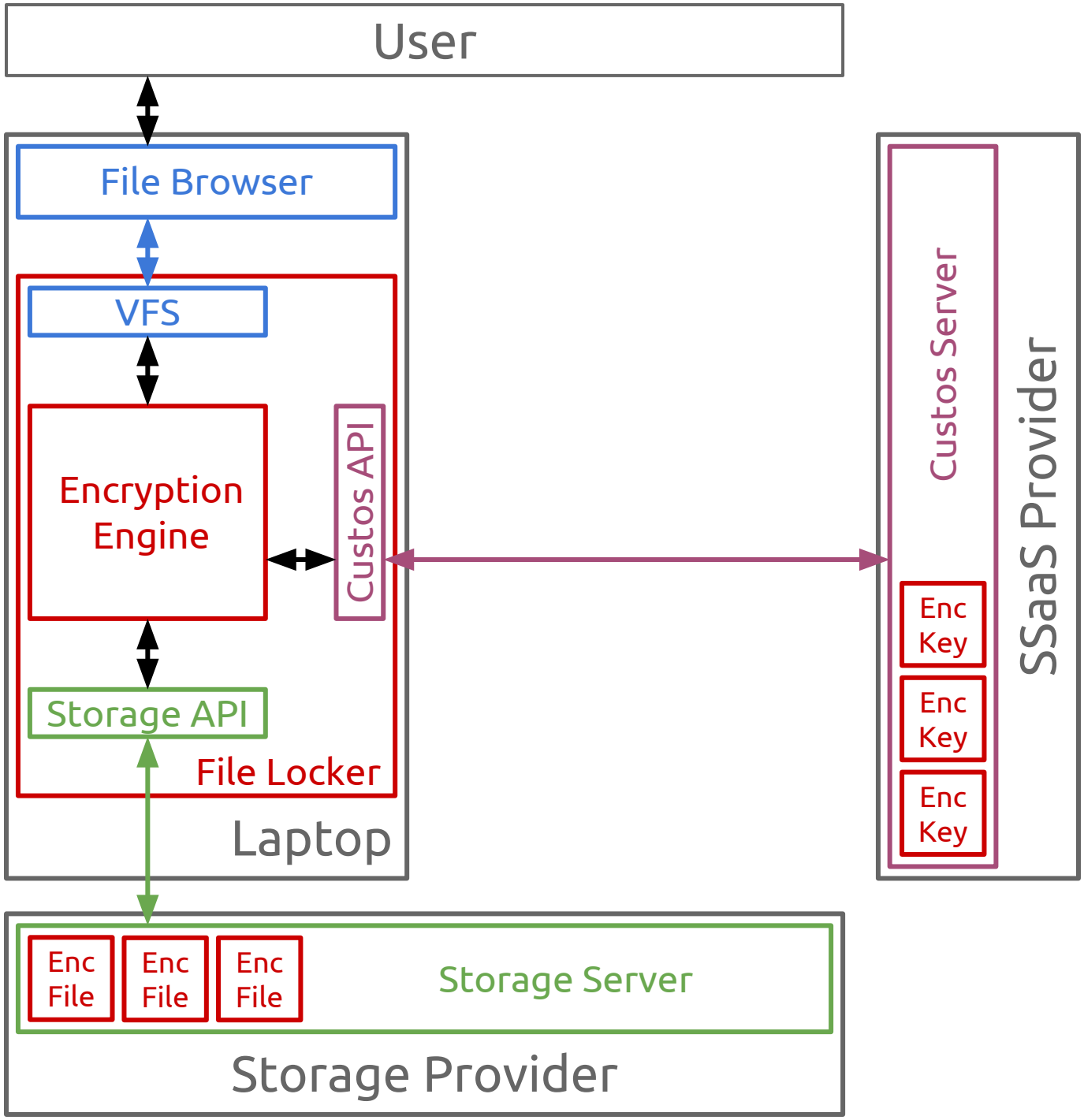
Extra Slides

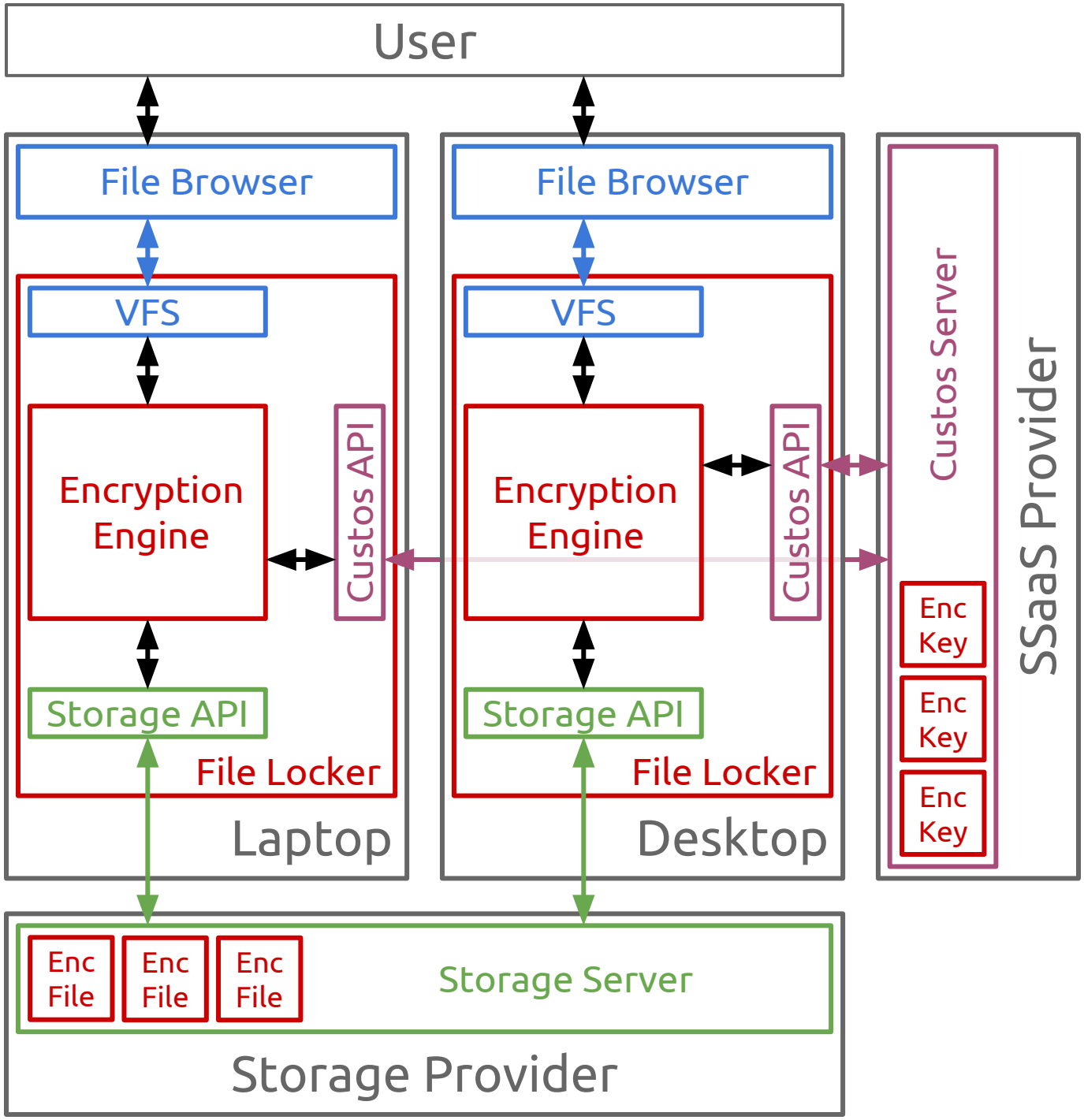
Custos Organizational Units


ACS
Server
ACS
Group A
Object 1
ACS
UUID
Value
Object 2
ACS
UUID
Value
Object 3
ACS
UUID
Value
ACS
Group B
Object 4
ACS
UUID
Value
Object 5
ACS
UUID
Value
Object 6
ACS
UUID
Value

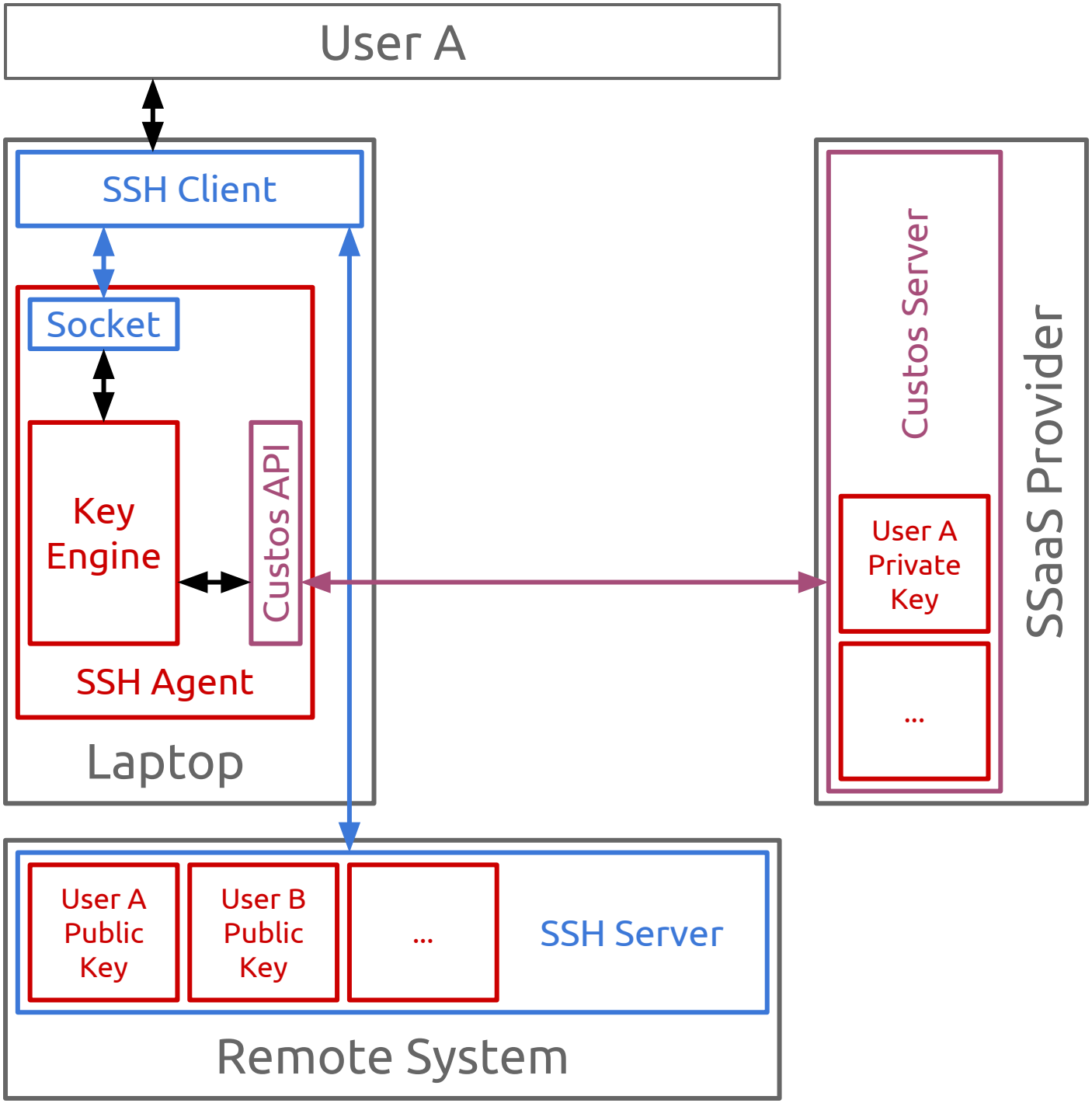
Example Applications

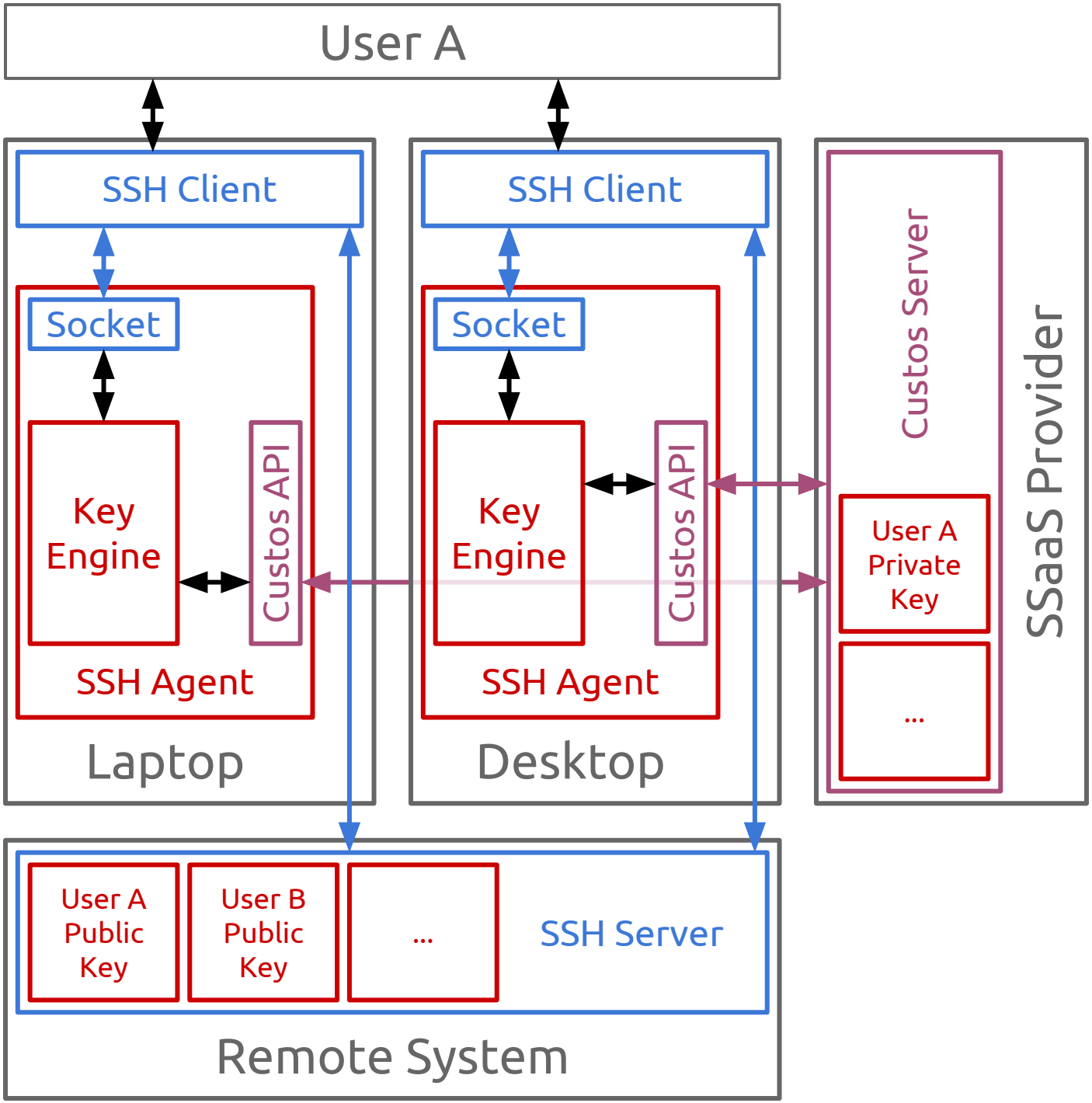
Client-Encrypted File Locker


User
File Browser
VFS
Encryption Engine
Custos API
Storage API
File Locker
Laptop
Custos Server
Enc Key
Enc Key
Enc Key
SSaaS Provider
Enc File
Enc File
Enc File
Storage Server
Storage Provider

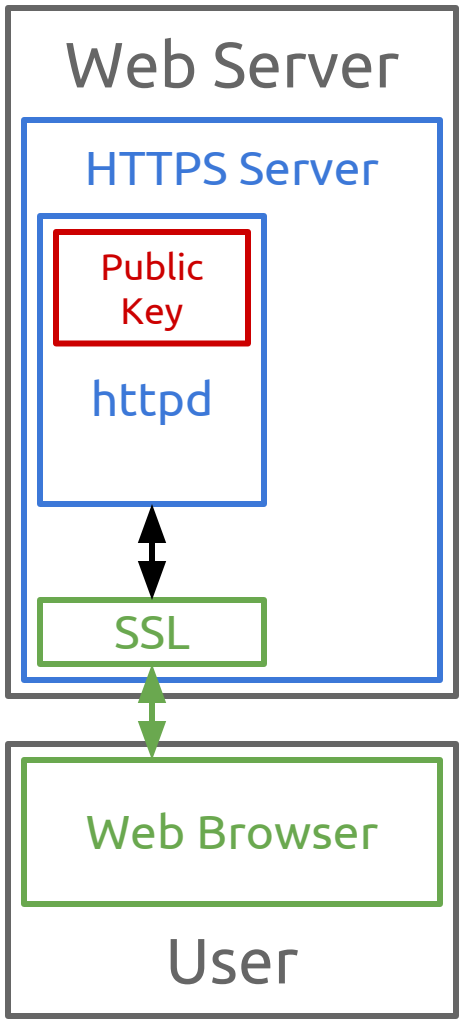

User
File Browser
VFS
Encryption Engine
Custos API
Storage API
File Locker
Laptop
File Browser
VFS
Encryption Engine
Custos API
Storage API
File Locker
Desktop
Custos Server
Enc Key
Enc Key
Enc Key
SSaaS Provider
Enc File
Enc File
Enc File
Storage Server
Storage Provider

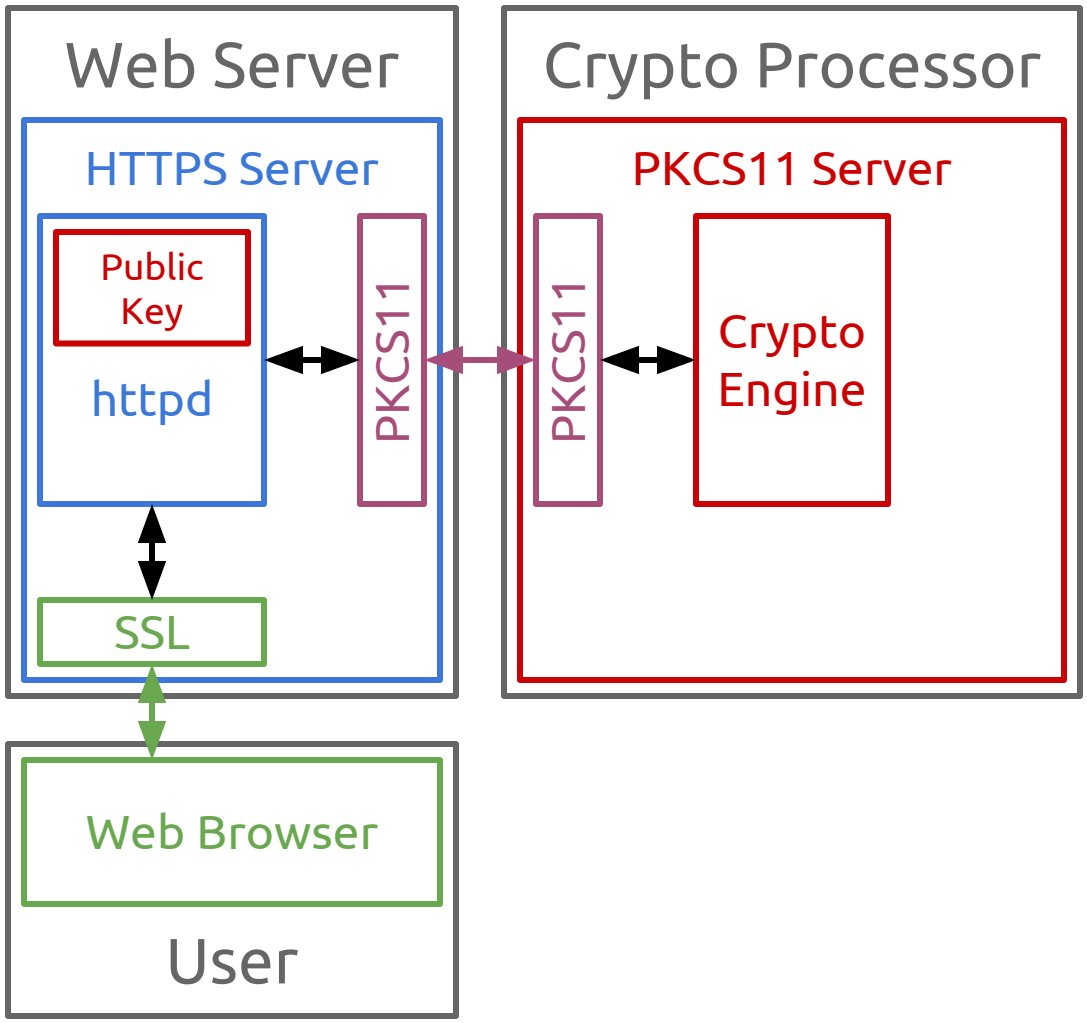
Multi-Device & Managed SSH Agent

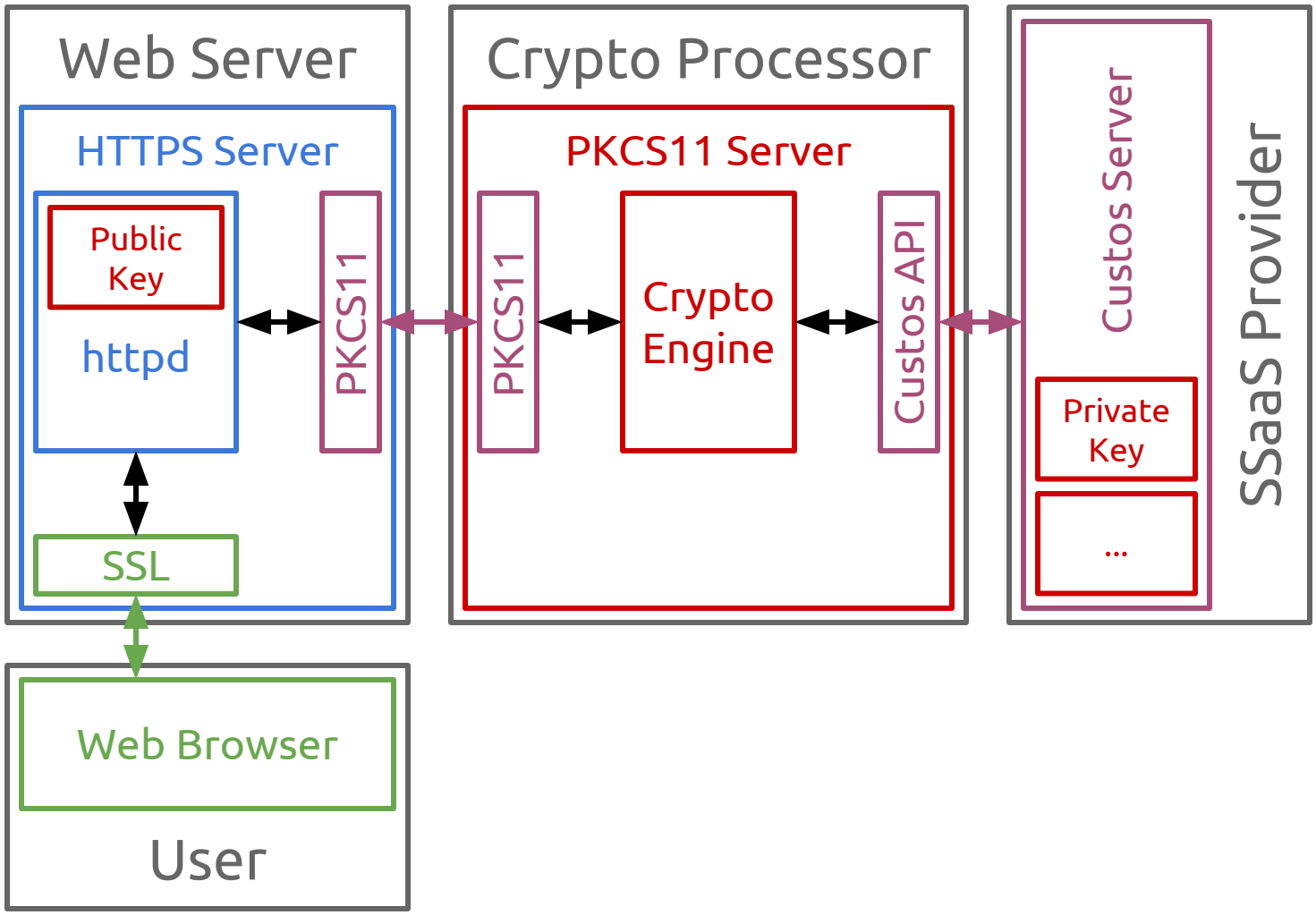

User A
SSH Client
Socket
Key Engine
Custos API
SSH Agent
Laptop
Custos Server
User A Private Key
...
SSaaS Provider
User A Public Key
User B Public Key
...
SSH Server
Remote System


User A
SSH Client
SSH Client
Socket
Socket
Key Engine
Custos API
Key Engine
Custos API
SSH Agent
SSH Agent
Laptop
Desktop
Custos Server
User A Private Key
...
SSaaS Provider
User A Public Key
User B Public Key
...
SSH Server
Remote System

Dedicated Crypto Processor


Web Server
HTTPS Server
Public Key
httpd
SSL
Web Browser
User


Web Server
HTTPS Server
Public Key
httpd
PKCS11
SSL
Crypto Processor
PKCS11 Server
PKCS11
Crypto Engine
Web Browser
User


Web Server
HTTPS Server
Public Key
httpd
SSL
PKCS11
Web Browser
User
Crypto Processor
PKCS11 Server
PKCS11
Crypto Engine
Custos API
SSaaS Provider
Custos Server
Private Key
...

Permissions

Permission	Rights
`srv_grp_create`	create groups on a Custos server
`srv_grp_list`	list groups on a Custos server
`srv_grp_override`	escalate to any group-level permission, overriding the per-group ACS
`srv_audit`	read all server-level audit information (i.e. group creation logging, group override logging, etc)
`srv_clean`	delete all server-level audit information (i.e. group creation logging, group override logging, etc)
`srv_acs_get`	view the server-level ACS controlling the permissions in this list
`srv_acs_set`	update the server-level ACS controlling the permissions in this list

Permission	Rights
srv_grp_create	create groups on a Custos server
srv_grp_list	list groups on a Custos server

Permission	Rights
grp_obj_create	create a key:value objects within the given group
grp_obj_list	list key:value objects within the given group
grp_obj_override	escalate to any object-level permission, overriding the per-object ACS
grp_delete	delete the given group on a Custos server
grp_audit	read all group-level audit information (i.e. object creation logging, object override logging, etc)
grp_clean	delete all group-level audit information (i.e. object creation logging, object override logging, etc)
grp_acs_get	view the group-level ACS controlling the permissions in this list
grp_acs_set	update the group-level ACS controlling the permissions in this list

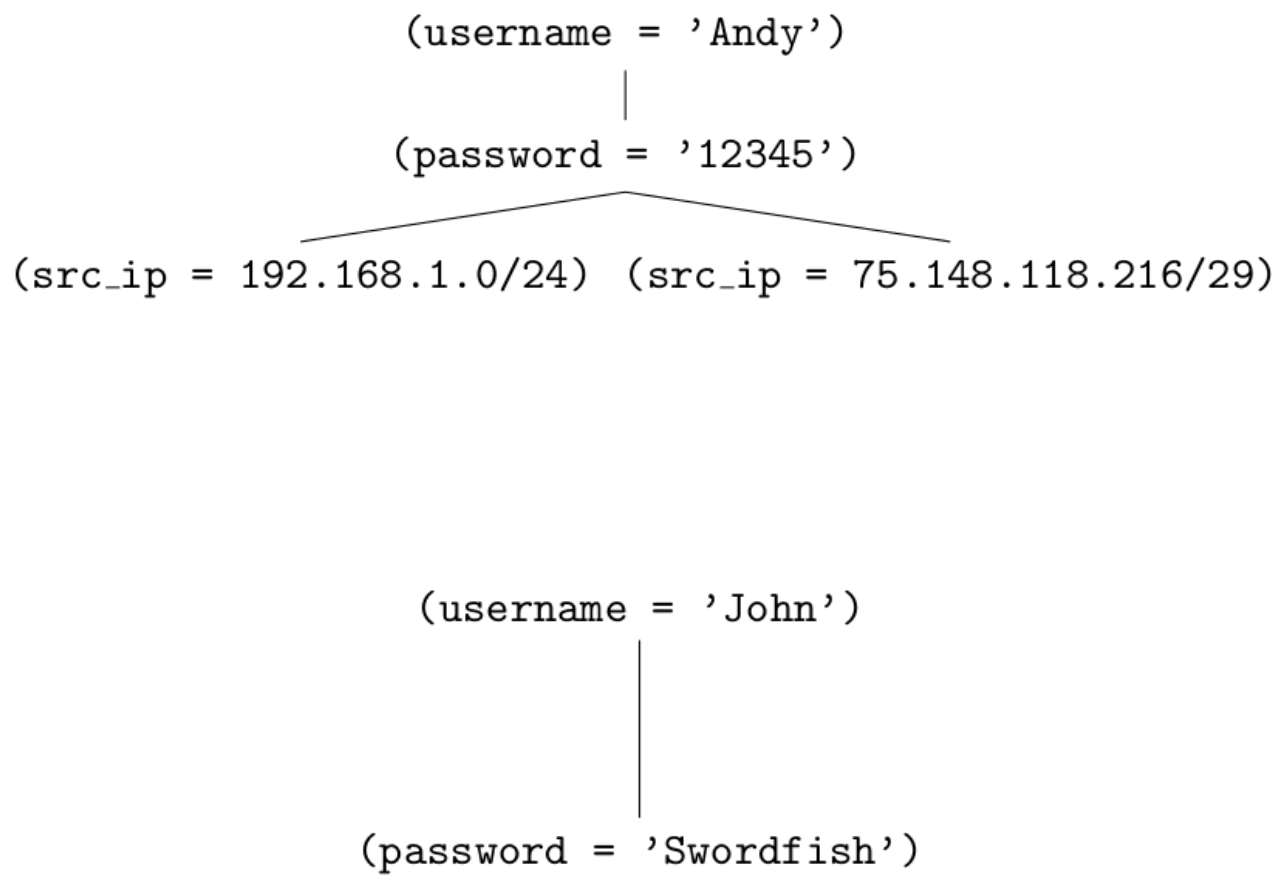
Permission	Rights
srv_grp_create	create groups on a Custos server
srv_grp_list	list groups on a Custos server

Permission	Rights
grp_obj_create	create a key:value objects within the given group
grp_obj_list	list key:value objects within the given group

Permission	Rights
obj_delete	delete the given key:value object within the given group
obj_read	read the given key:value object within the given group
obj_update	create a new version of the given key:value object within the given group (the equivalent of a "write" permission for the Custos write-once system)
obj_audit	read all object-level audit information (i.e. object read logging, object update logging, etc)
obj_clean	delete all object-level audit information (i.e. object read logging, object update logging, etc)
obj_acs_get	view the object-level ACS controlling the permissions in this list
obj_acs_set	update the object-level ACS controlling the permissions in this list

Access Control Chain

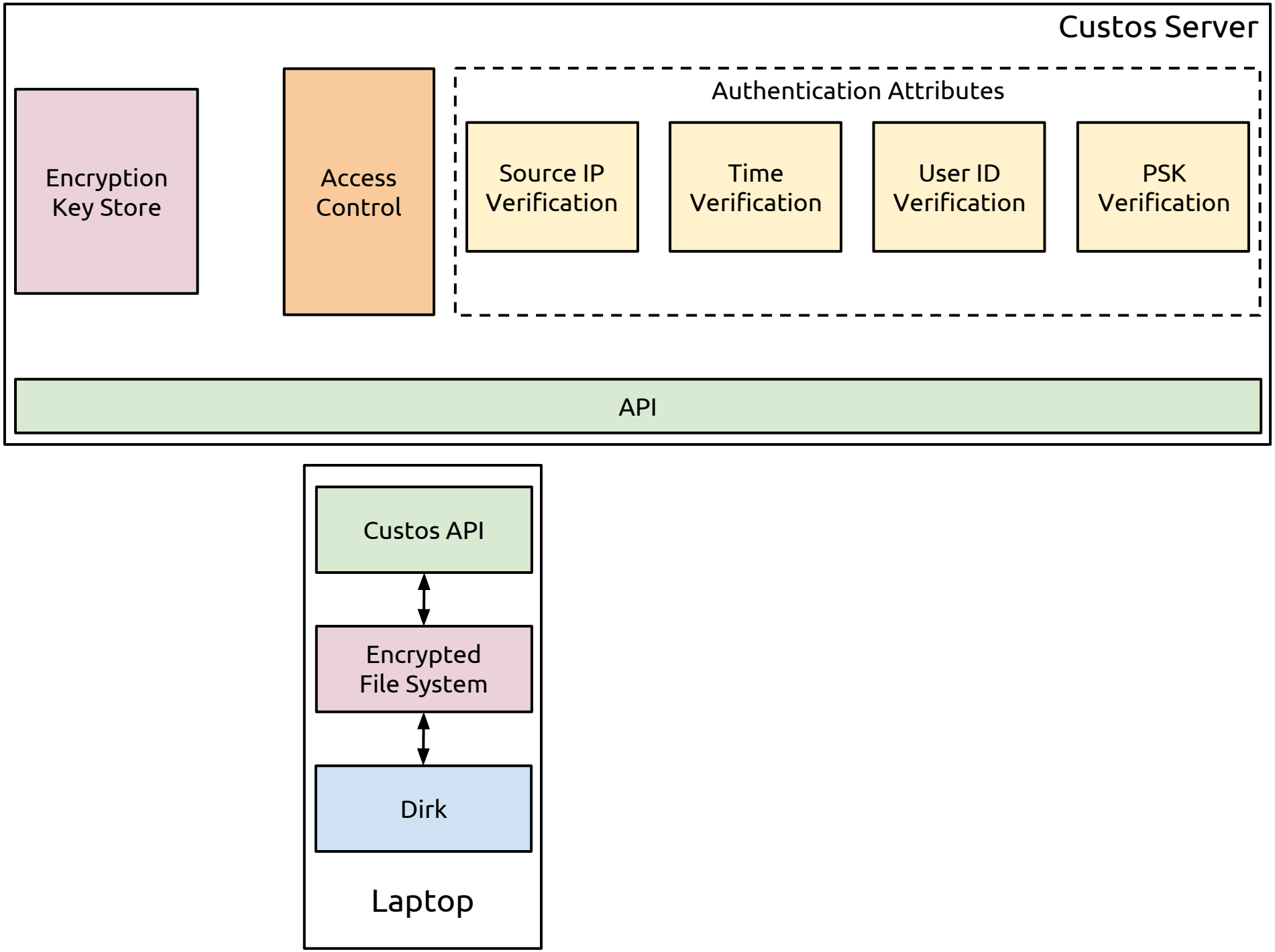
```
[
  [ (username = ’Andy’),
    (password = ’12345’),
    (src_ip = 192.168.1.0/24) ],
  [ (username = ’Andy’),
    (password = ’12345’),
    (src_ip = 75.148.118.216/29) ],
  [ (username = ’John’),
    (password = ’Swordfish’) ]
]
```


(username = 'Andy')
(password = '12345')
(src_ip = 192.168.1.0/24)
(src_ip = 75.148.118.216/29)
(username = 'John')
(password = 'Swordfish')

Access Example

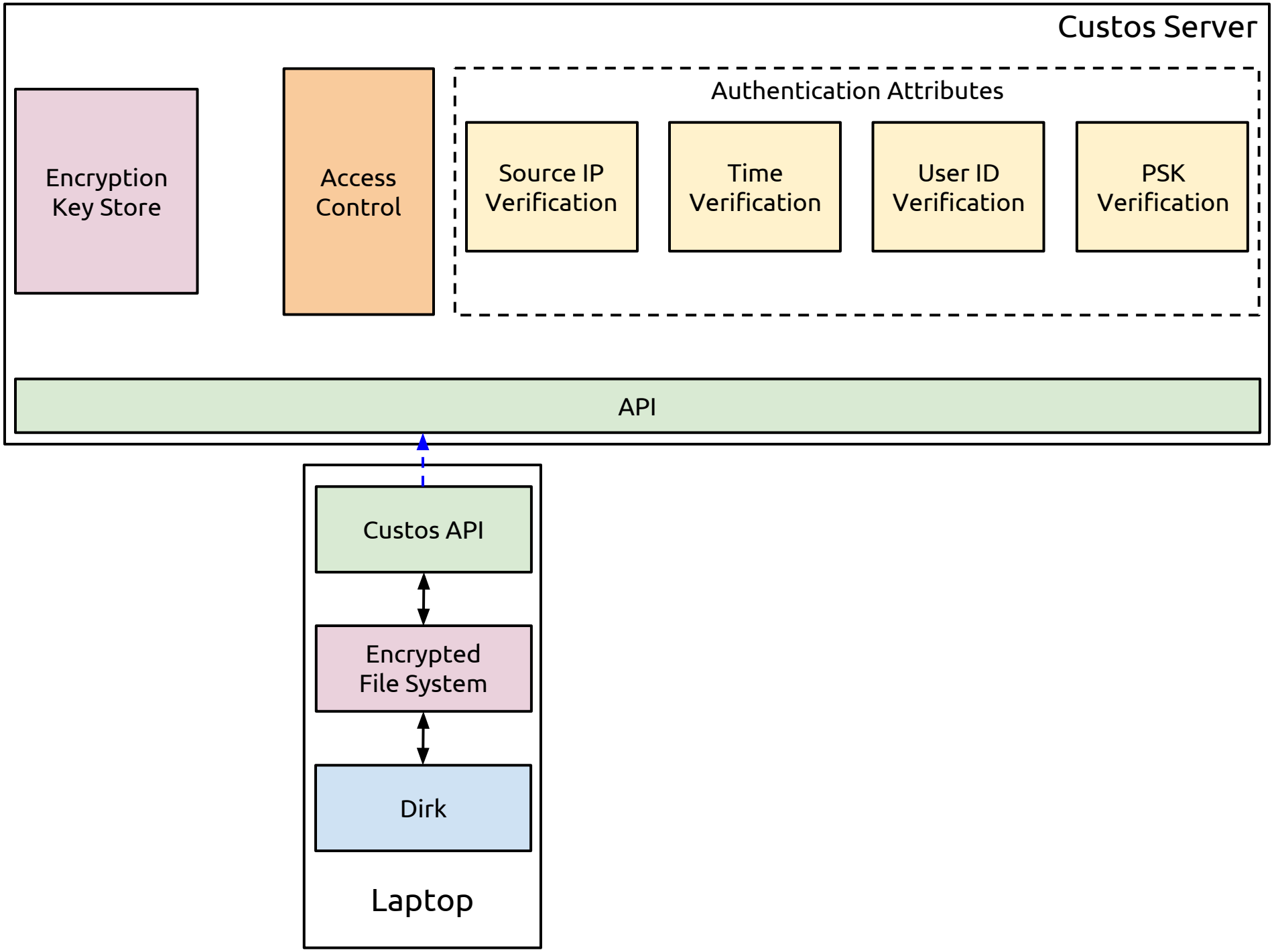
619a06f0-50af-11e3-8f96-0800200c9a66 ACS

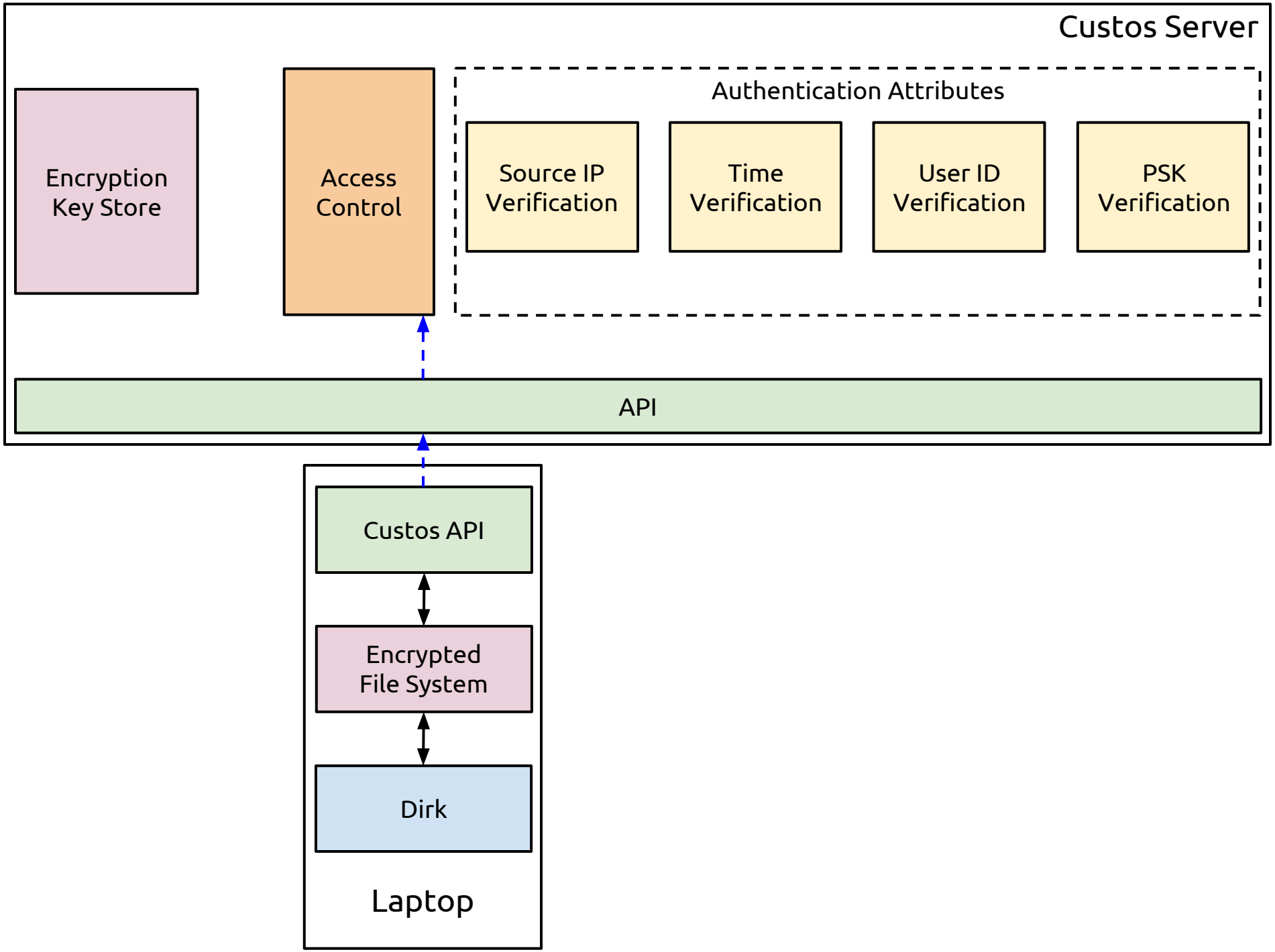
```
{
  obj_read:
    [
      [ (ip\_src = ’1.2.3.4’),
        (time\_utc = ’1300 +/- 5’) ],
      [ (user\_id = ’Dirk’),
        (psk = ’ImaHakzor’) ]
      ...
    ]
    ...
}
```


Custos Server
Encryption Key Store
Access Control
Authentication Attributes
Source IP Verification
Time Verification
User ID Verification
PSK Verification
API
Custos API
Encrypted File System
Dirk
Laptop

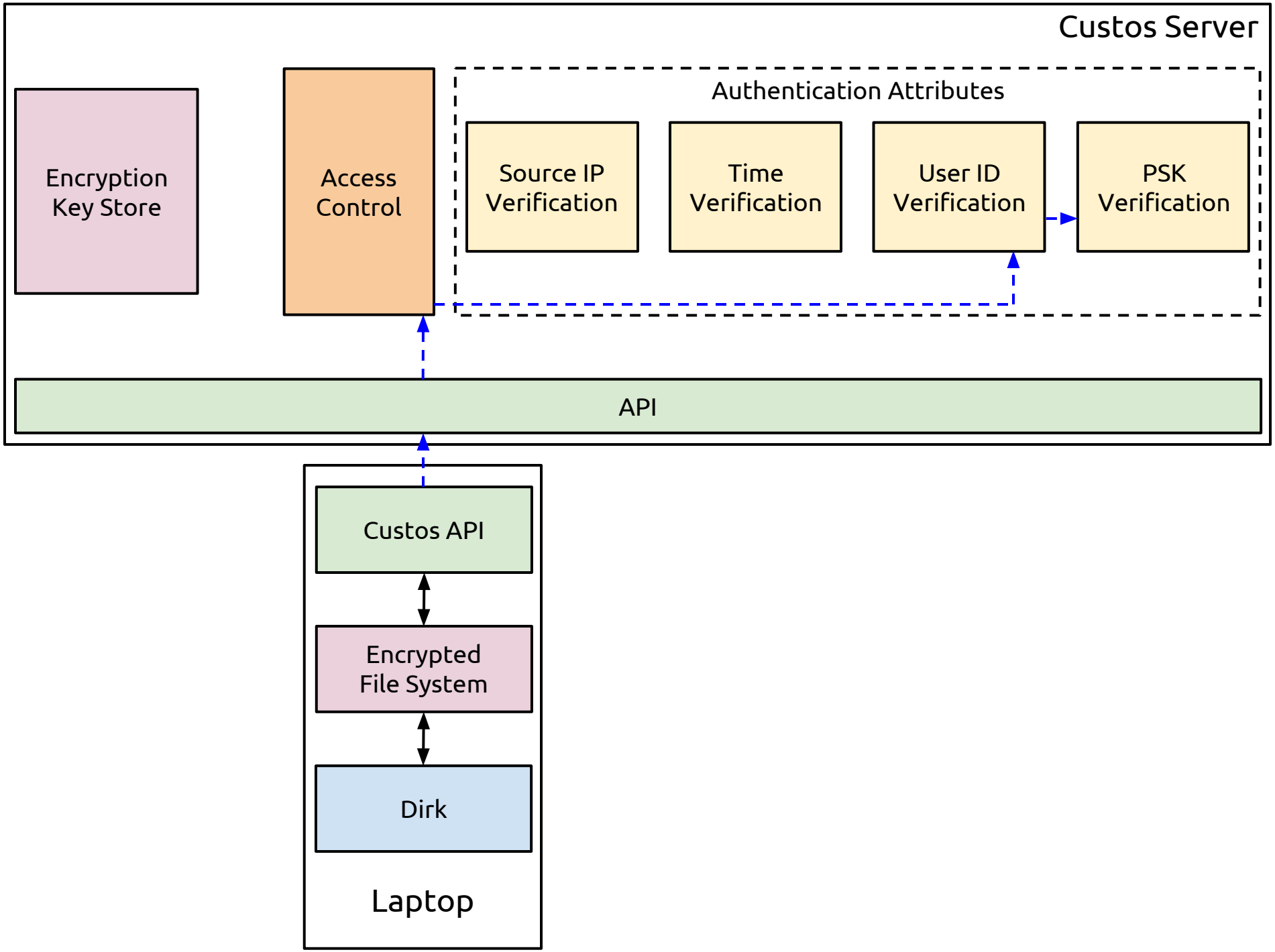
Request:
619a06f0-50af-11e3-8f96-0800200c9a66

Authentication Attributes:
user_id = Dirk
(ip_src = ‘1.2.3.4’)
(time_utc = ‘1133’)


Custos Server
Encryption Key Store
Access Control
Authentication Attributes
Source IP Verification
Time Verification
User ID Verification
PSK Verification
API
Custos API
Encrypted File System
Dirk
Laptop


Custos Server
Encryption Key Store
Access Control
Authentication Attributes
Source IP Verification
Time Verification
User ID Verification
PSK Verification
API
Custos API
Encrypted File System
Dirk
Laptop

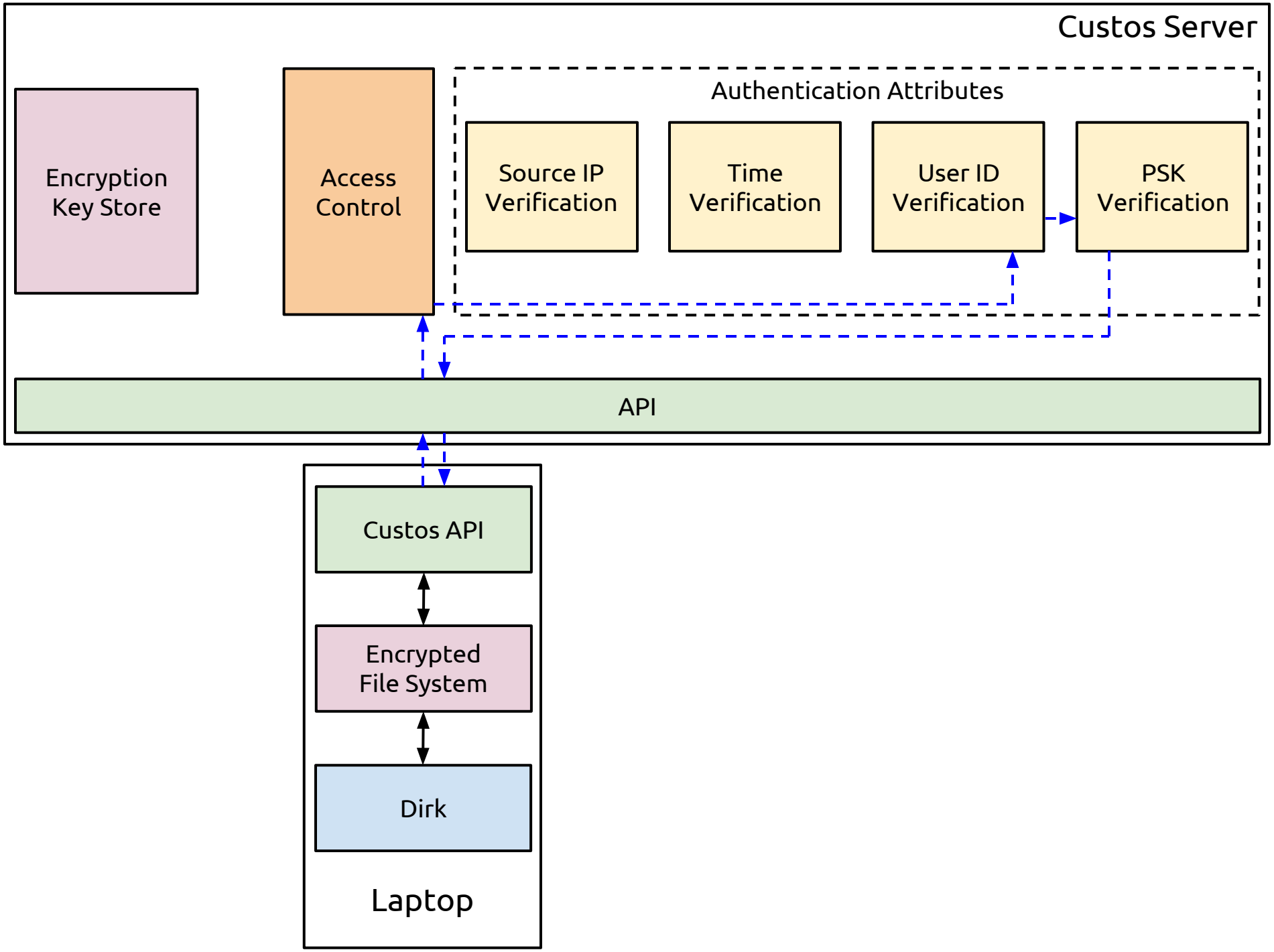
```
{
  obj_read:
    [
      [ (ip\_src = ’1.2.3.4’),
        (time\_utc = ’1300 +/- 5’) ],
      [ (user\_id = ’Dirk’),
        (psk = ’ImaHakzor’) ]
      ...
    ]
    ...
}
```


Custos Server
Encryption Key Store
Access Control
Authentication Attributes
Source IP Verification
Time Verification
User ID Verification
PSK Verification
API
Custos API
Encrypted File System
Dirk
Laptop

Request:
619a06f0-50af-11e3-8f96-0800200c9a66

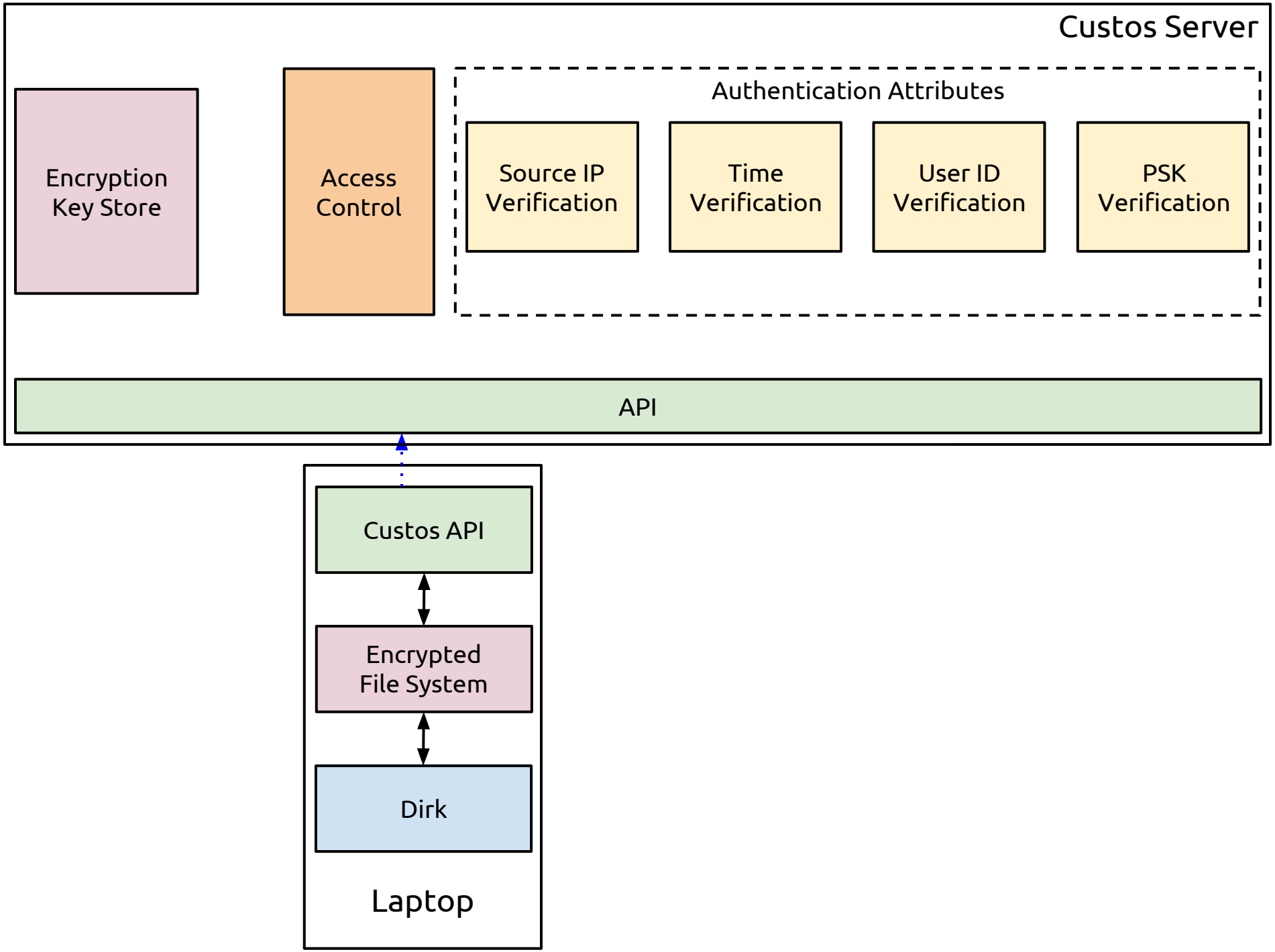
Authentication Attributes:
user_id = Dirk
(ip_src = ‘1.2.3.4’)
(time_utc = ‘1133’)

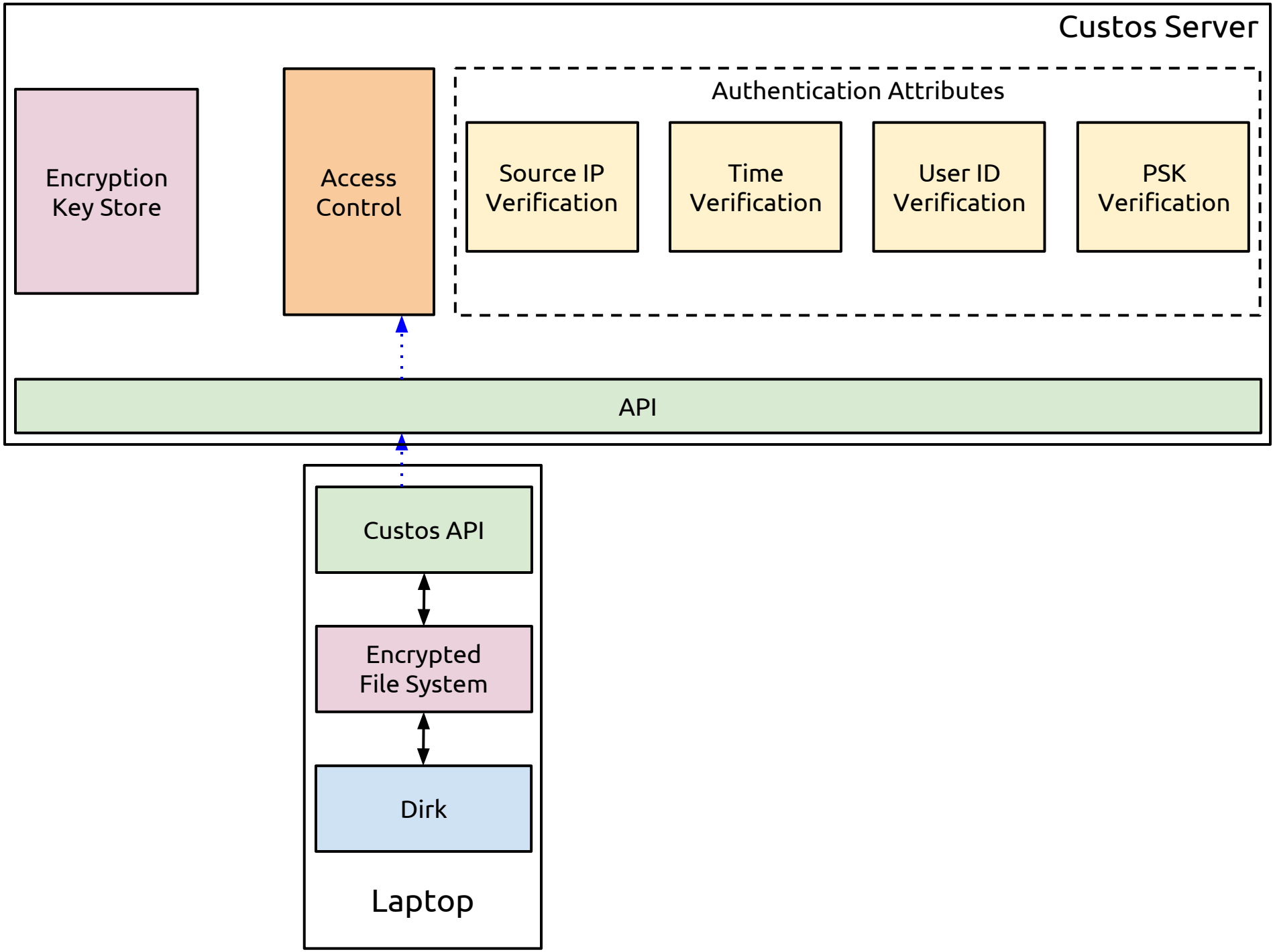
```
{
  obj_read:
    [
      [ (ip\_src = ’1.2.3.4’),
        (time\_utc = ’1300 +/- 5’) ],
      [ (user\_id = ’Dirk’),
        (psk = ’ImaHakzor’) ]
      ...
    ]
    ...
}
```

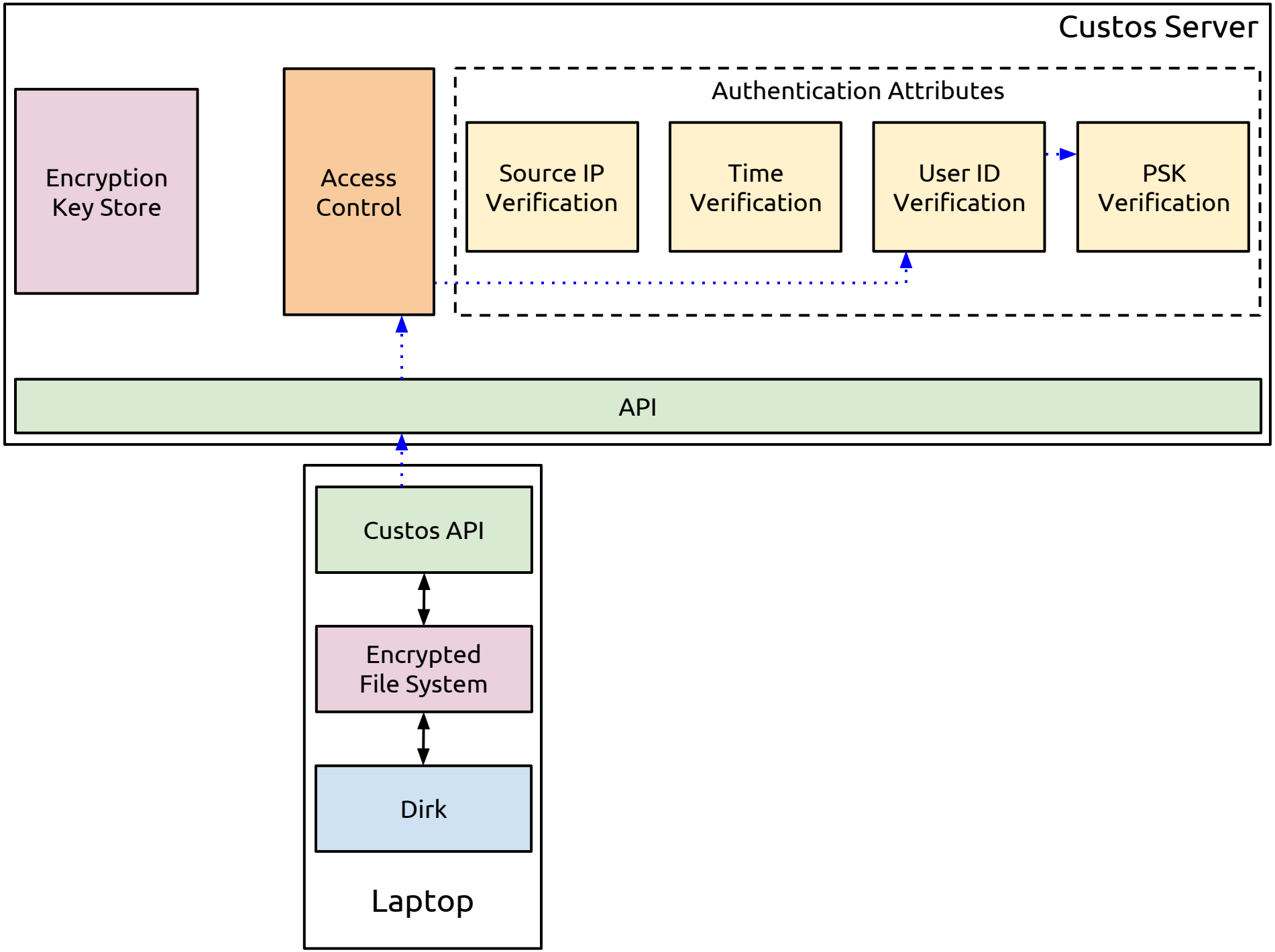

Custos Server
Encryption Key Store
Access Control
Authentication Attributes
Source IP Verification
Time Verification
User ID Verification
PSK Verification
API
Custos API
Encrypted File System
Dirk
Laptop

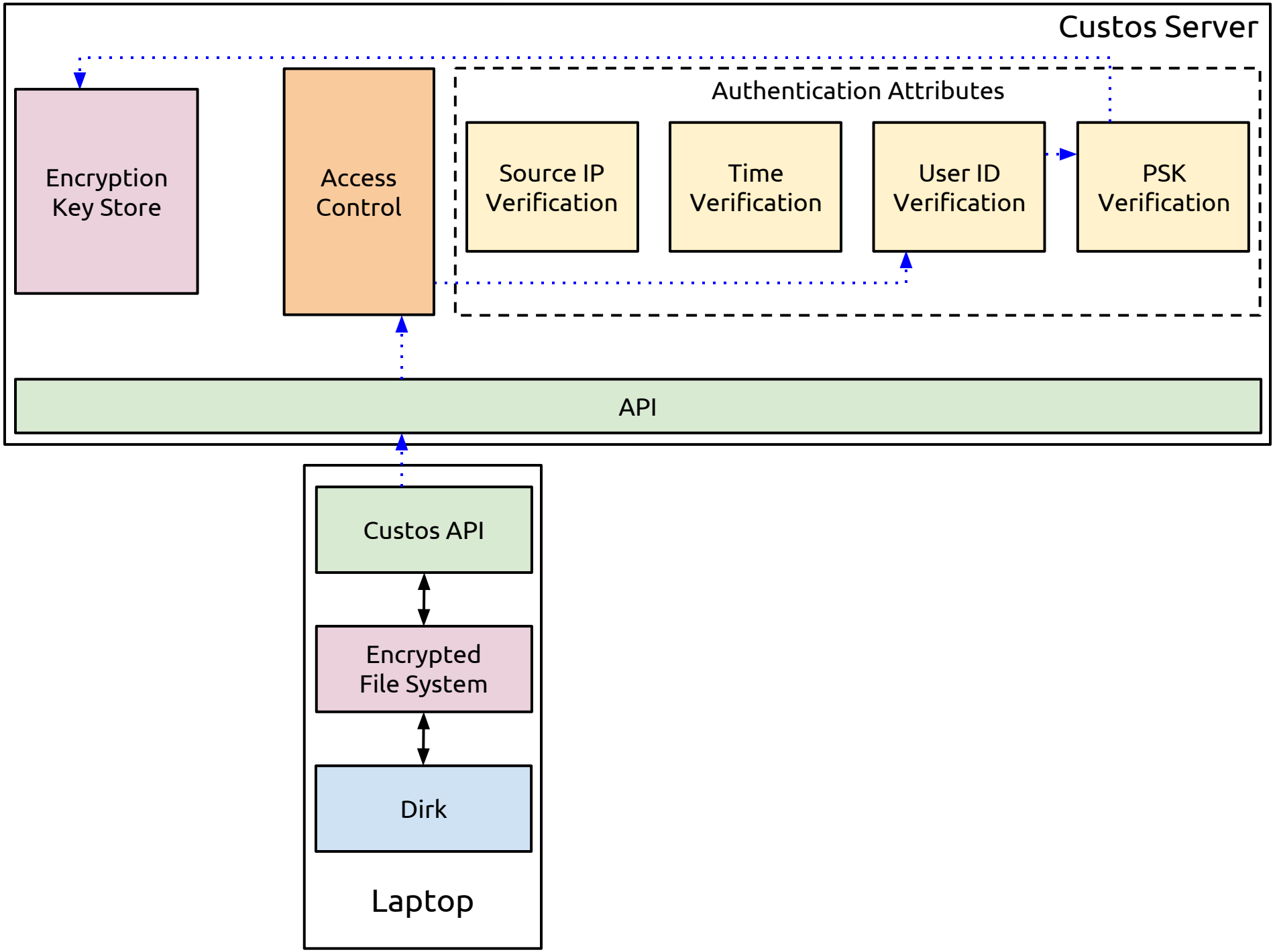
Request:
619a06f0-50af-11e3-8f96-0800200c9a66

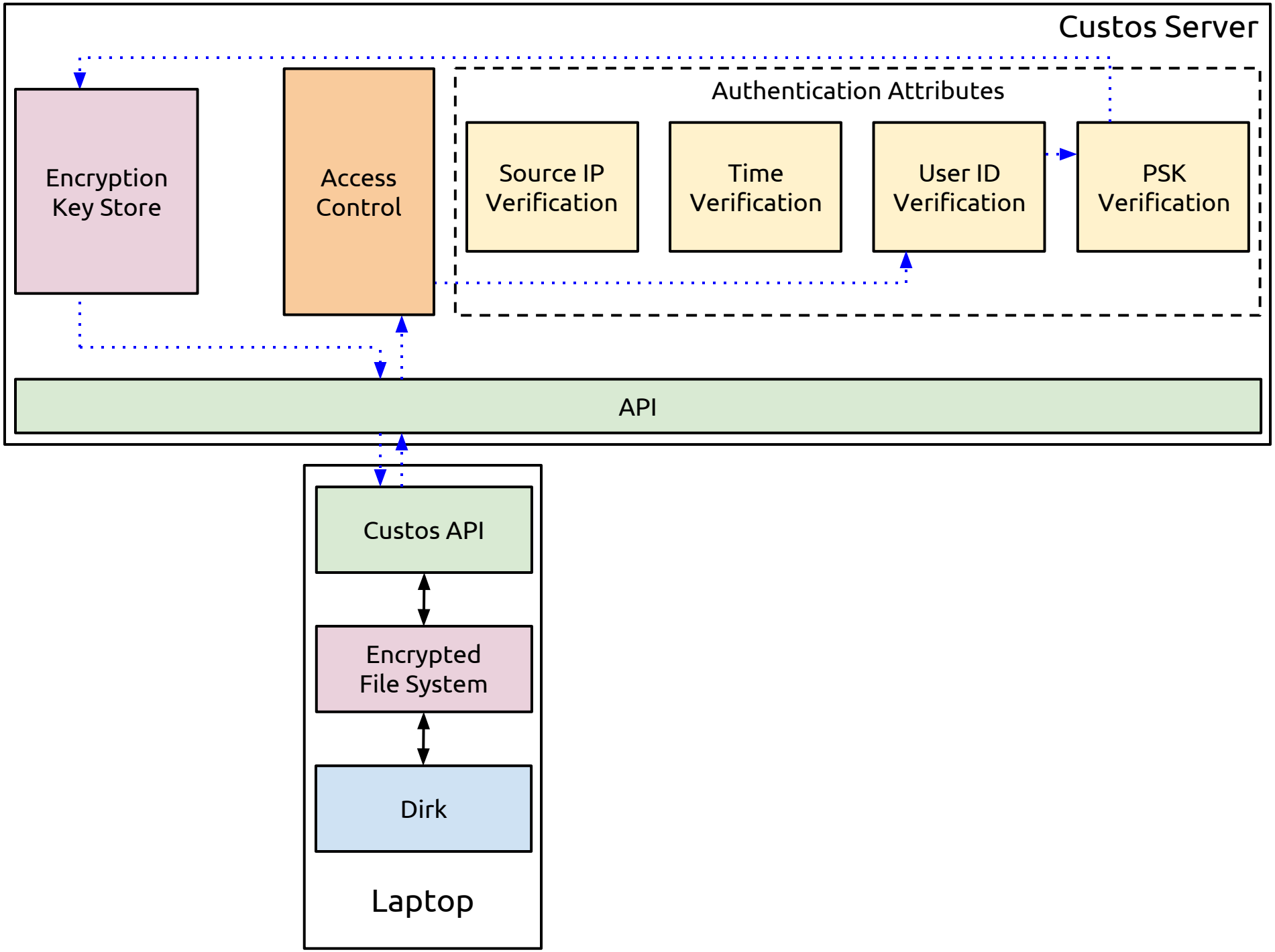
Authentication Attributes:
user_id = ‘Dirk’
psk = ‘ImaHackzor’
(ip_src = ‘1.2.3.4’)
(time_utc = ‘1133’)


Custos Server
Encryption Key Store
Access Control
Authentication Attributes
Source IP Verification
Time Verification
User ID Verification
PSK Verification
API
Custos API
Encrypted File System
Dirk
Laptop


Custos Server
Encryption Key Store
Access Control
Authentication Attributes
Source IP Verification
Time Verification
User ID Verification
PSK Verification
API
Custos API
Encrypted File System
Dirk
Laptop


Custos Server
Encryption Key Store
Access Control
Authentication Attributes
Source IP Verification
Time Verification
User ID Verification
PSK Verification
API
Custos API
Encrypted File System
Dirk
Laptop


Custos Server
Encryption Key Store
Access Control
Authentication Attributes
Source IP Verification
Time Verification
User ID Verification
PSK Verification
API
Custos API
Encrypted File System
Dirk
Laptop


Custos Server
Encryption Key Store
Access Control
Authentication Attributes
Source IP Verification
Time Verification
User ID Verification
PSK Verification
API
Custos API
Encrypted File System
Dirk
Laptop