

Custos

Increasing Security with Secret Storage as a Service

Andy Sayler
Dirk Grunwald

TRIOS14
10/05/14

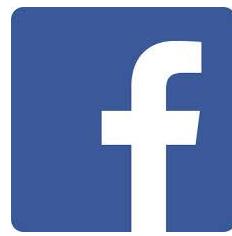


University of Colorado **Boulder**

Where do we store data today?









Trust?



Secure?

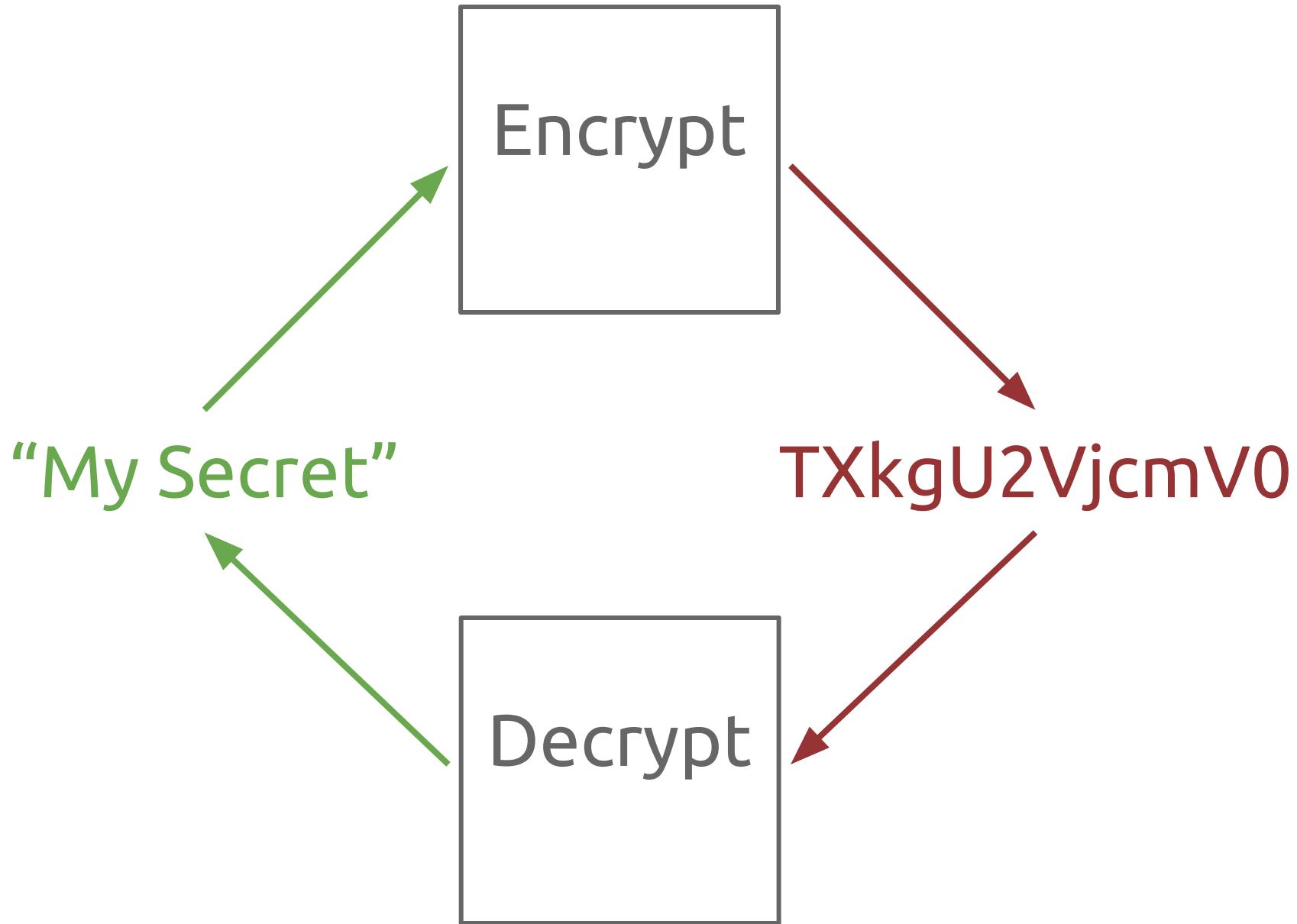


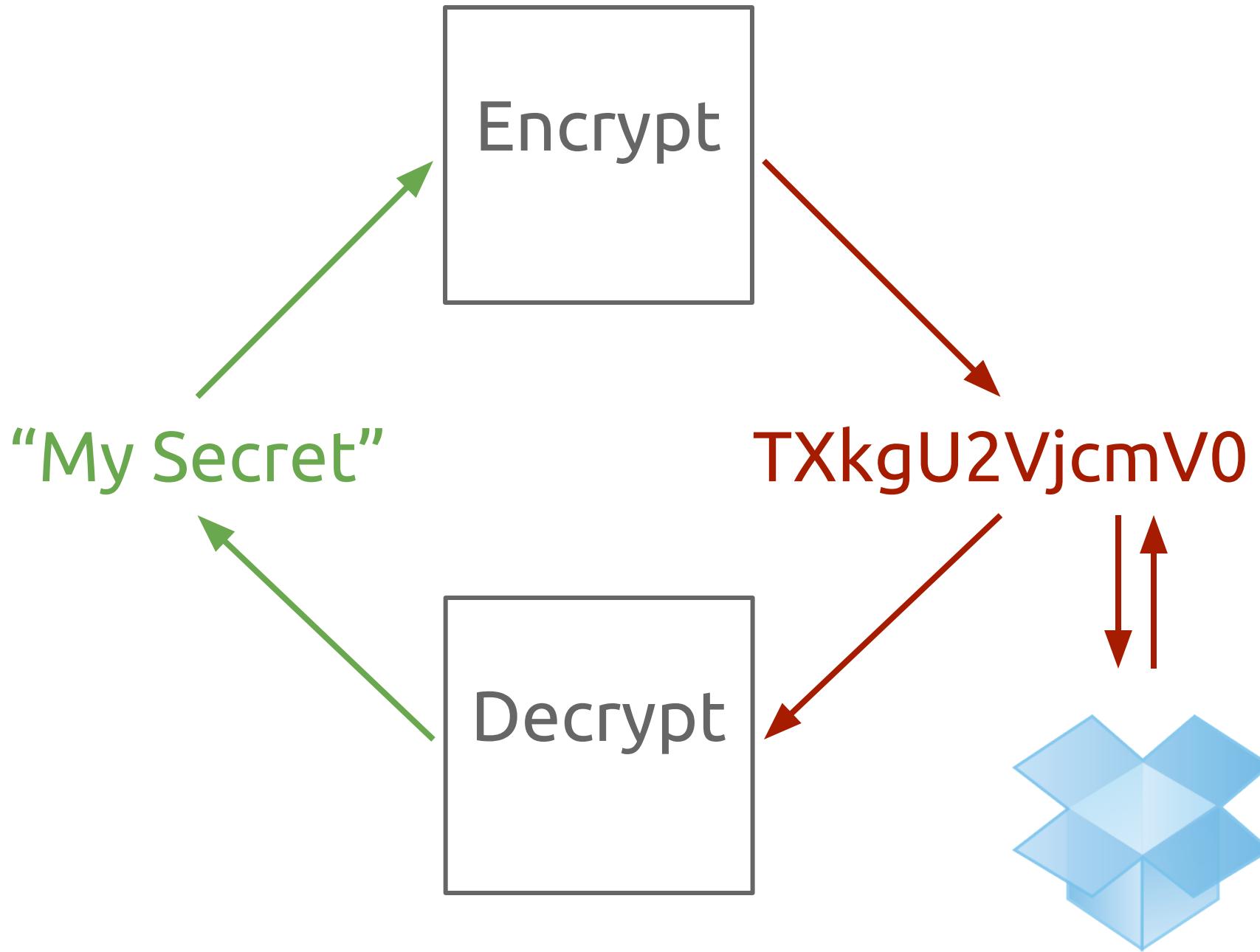
How can we control
and protect our data?

How can we control and protect our data?

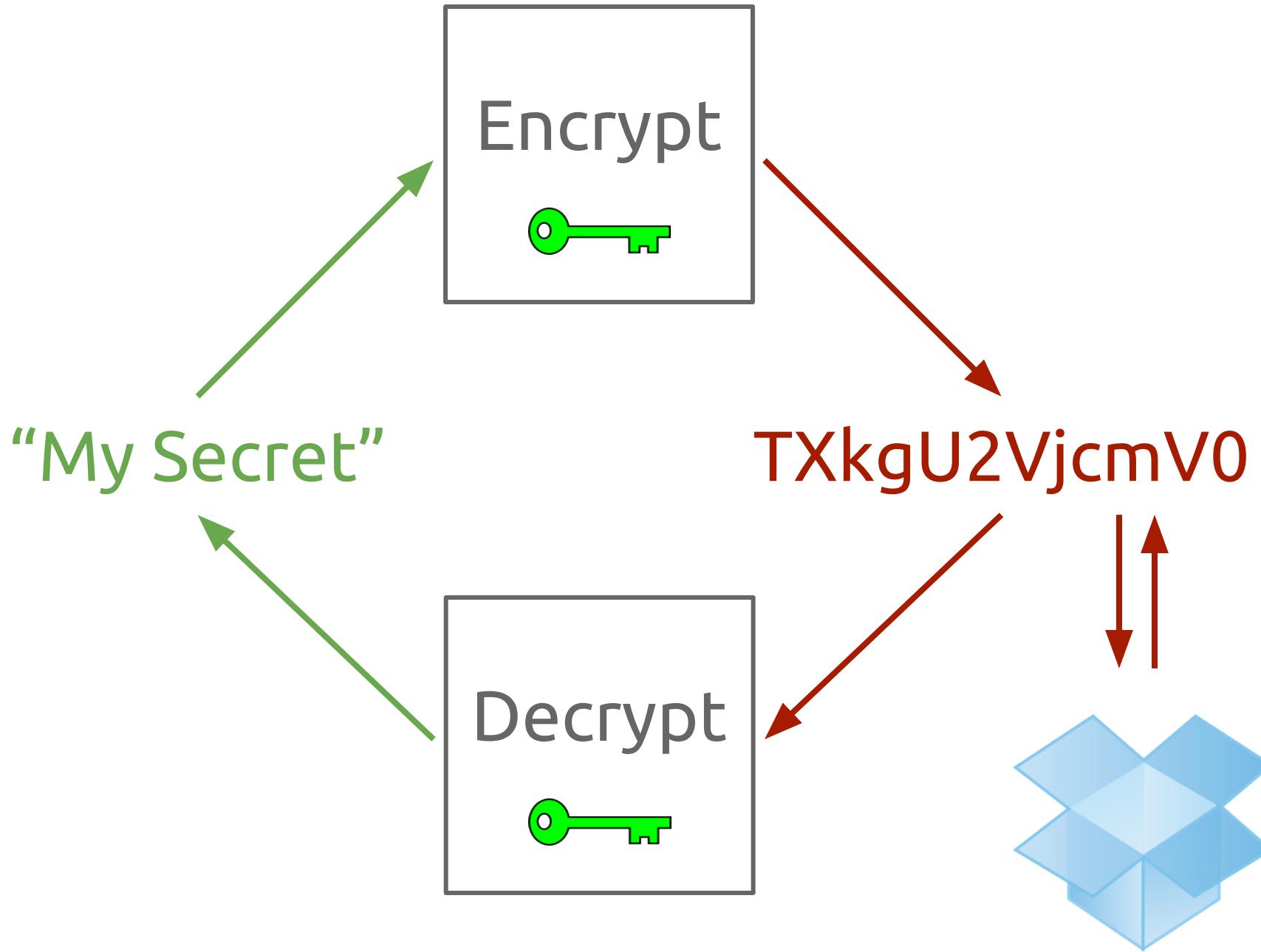
(even when storing it with third parties)

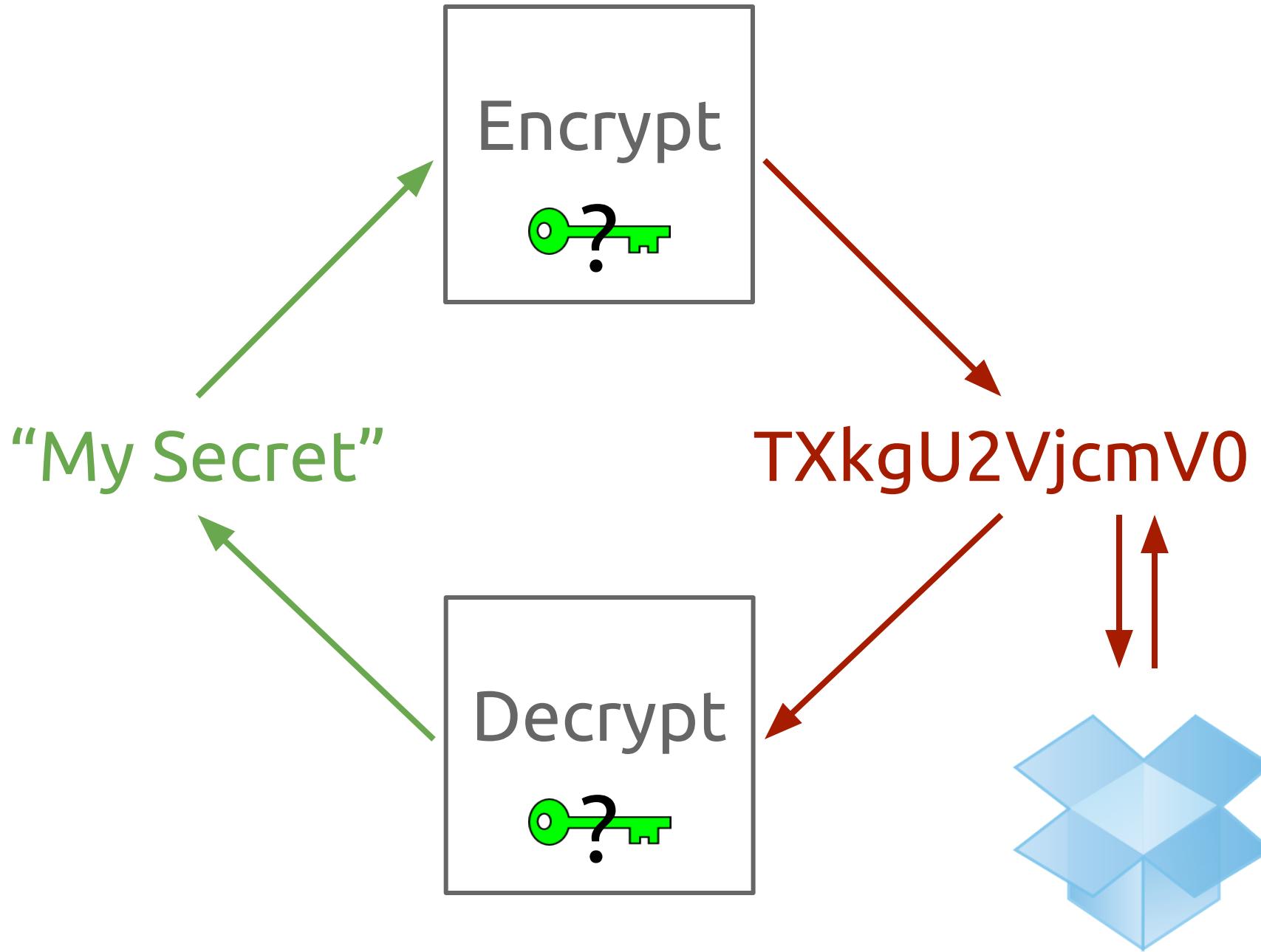
Client-Side Encryption?





But What About the Keys?





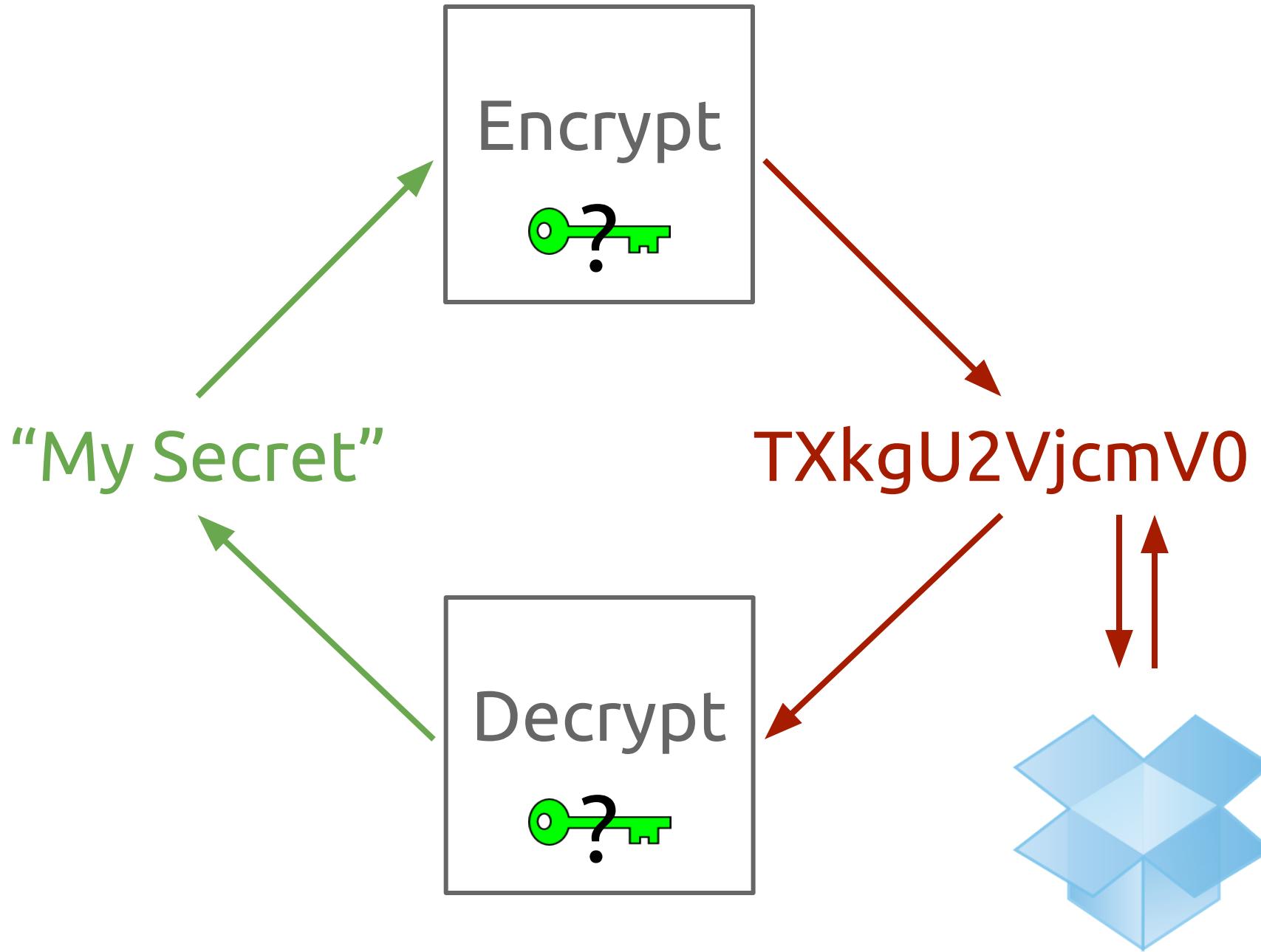
Custos

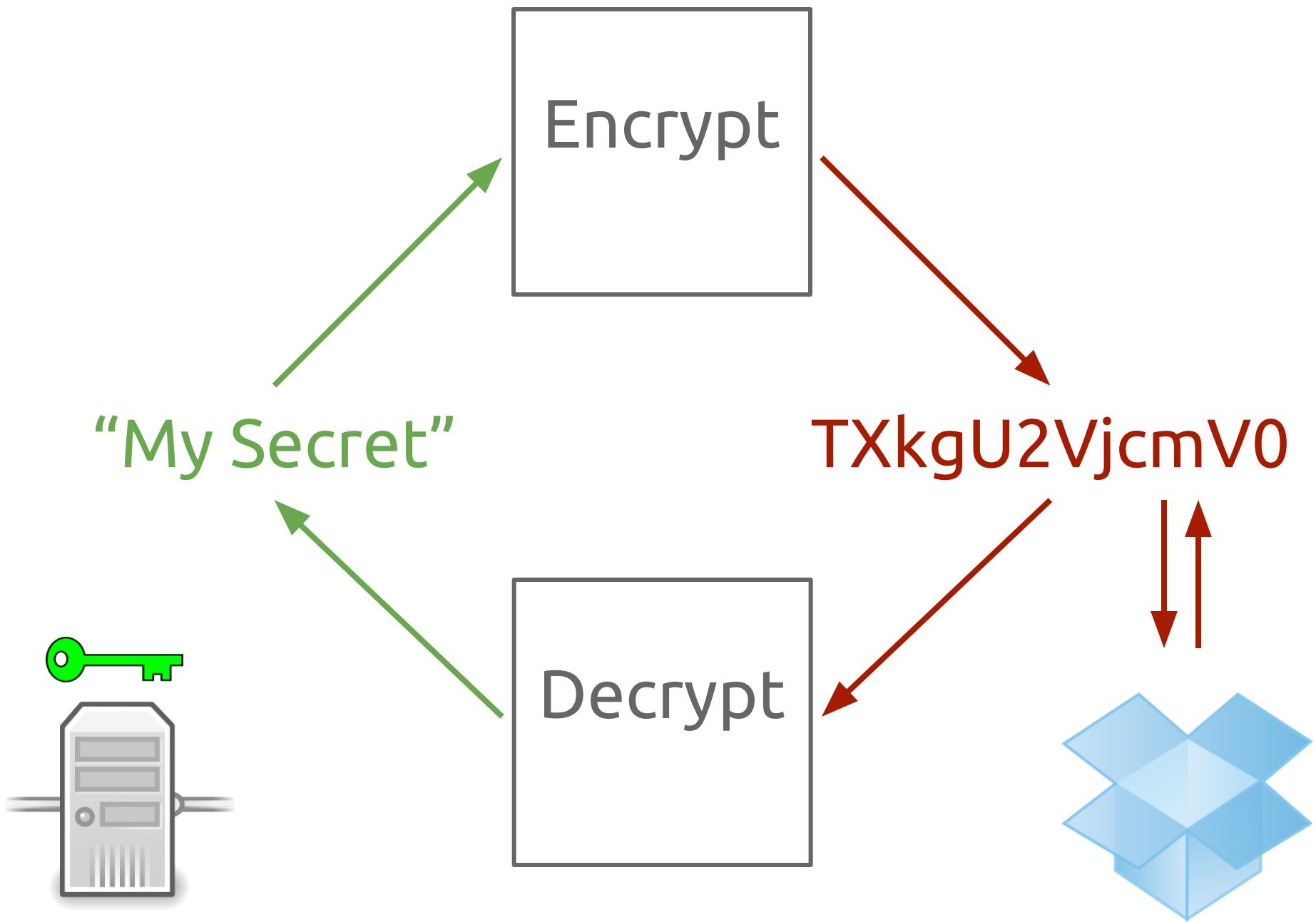
Custos

Latin for “Guard”

“Key Storage as a Service”

“Secret Storage as a Service”





Core Features

Centralized Secret Storage

Centralized Secret Storage

Flexible Access Control

Centralized Secret Storage

Flexible Access Control

Auditing and Revocation

Centralized Secret Storage

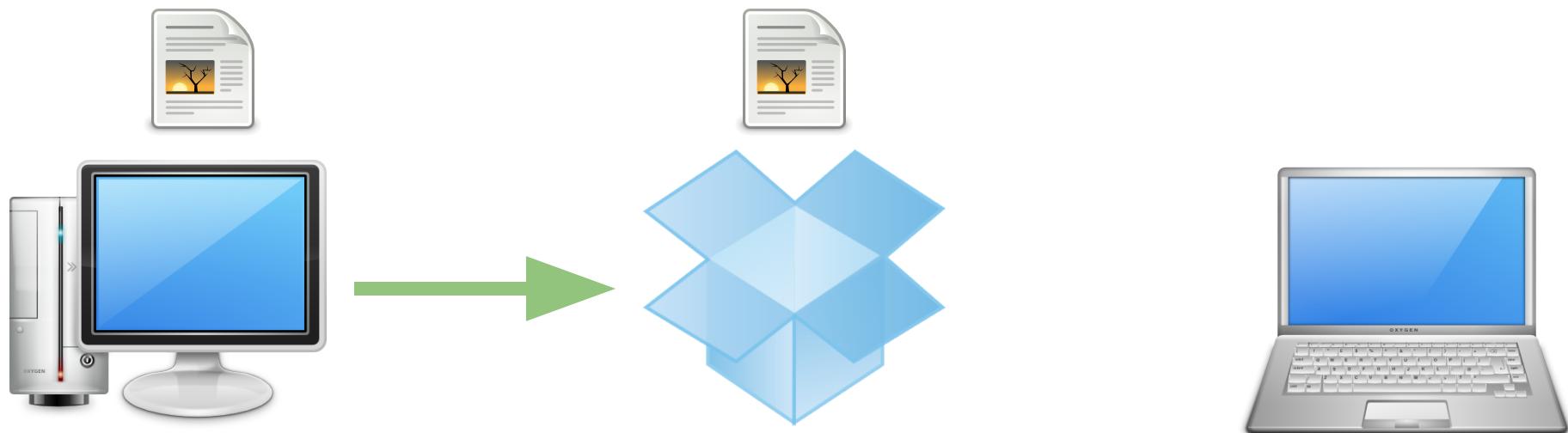
Example: Multi-Device File Sync



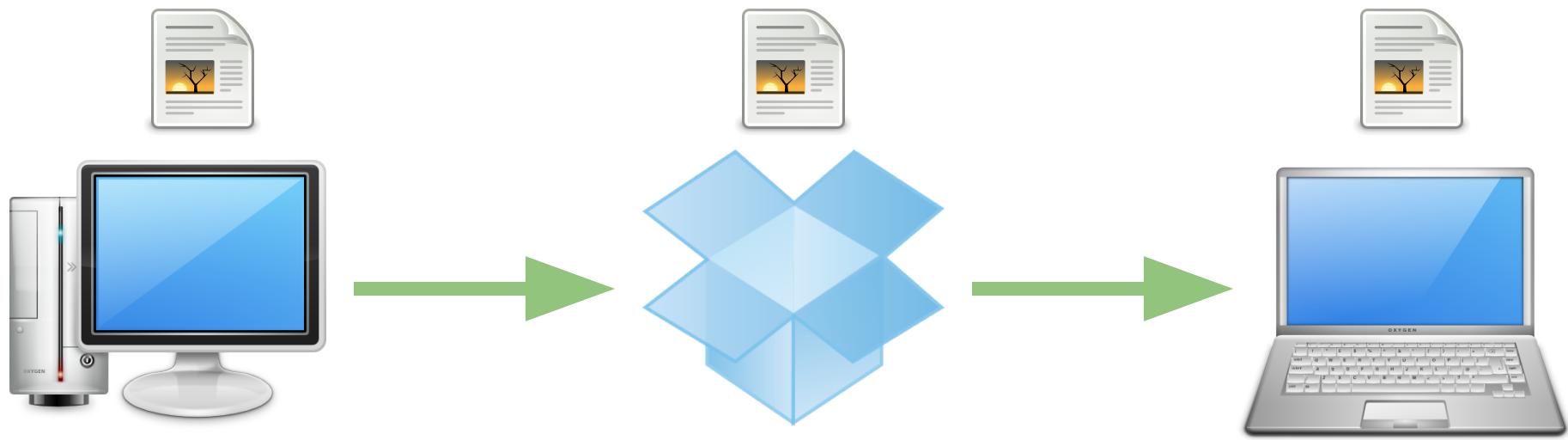
Example: Multi-Device File Sync



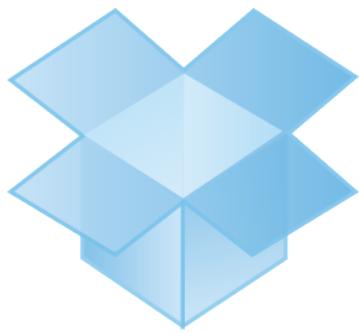
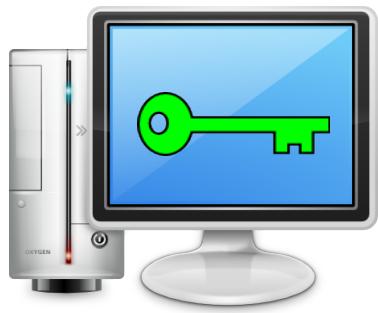
Example: Multi-Device File Sync



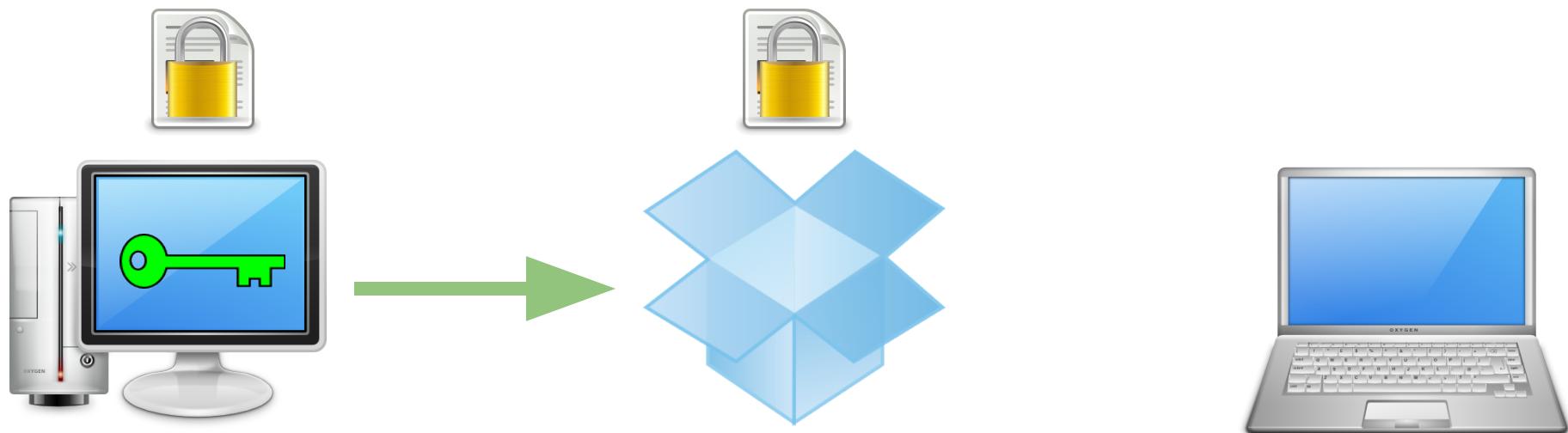
Example: Multi-Device File Sync



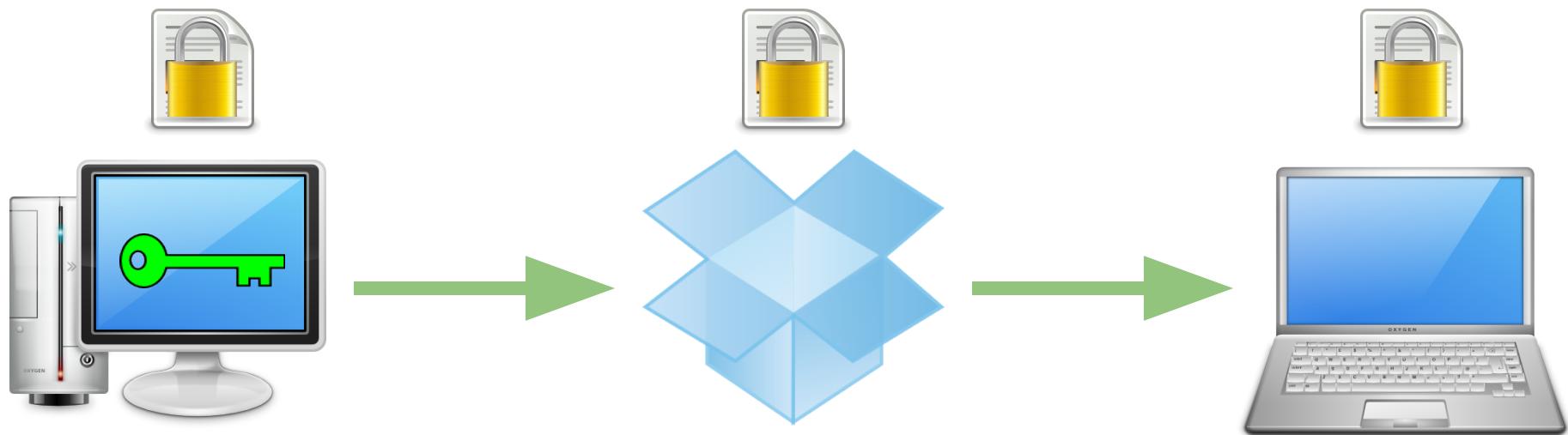
Example: Multi-Device File Sync



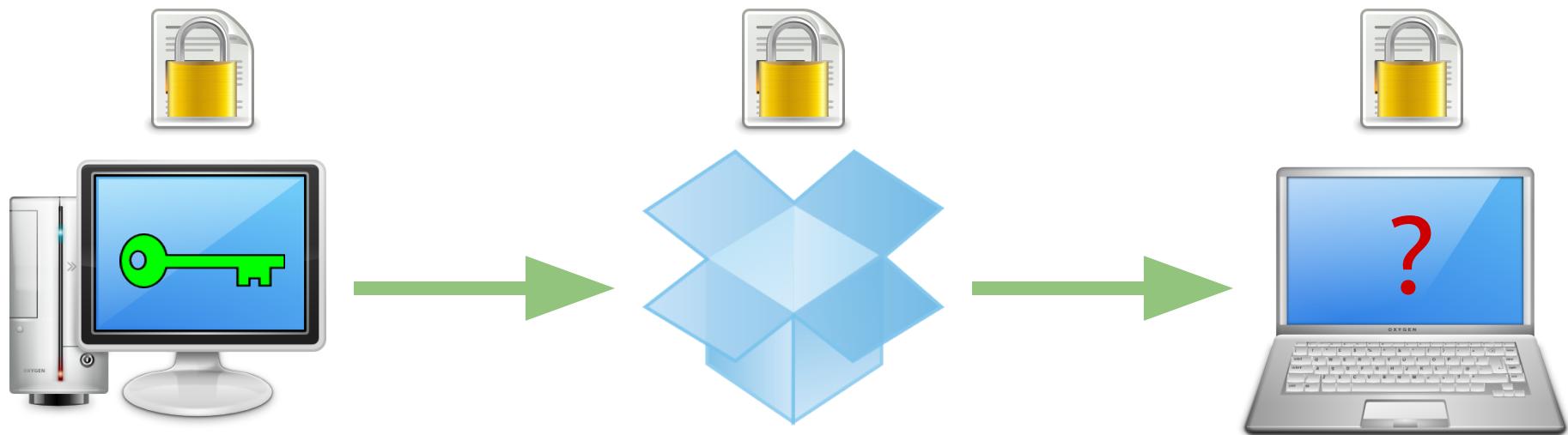
Example: Multi-Device File Sync



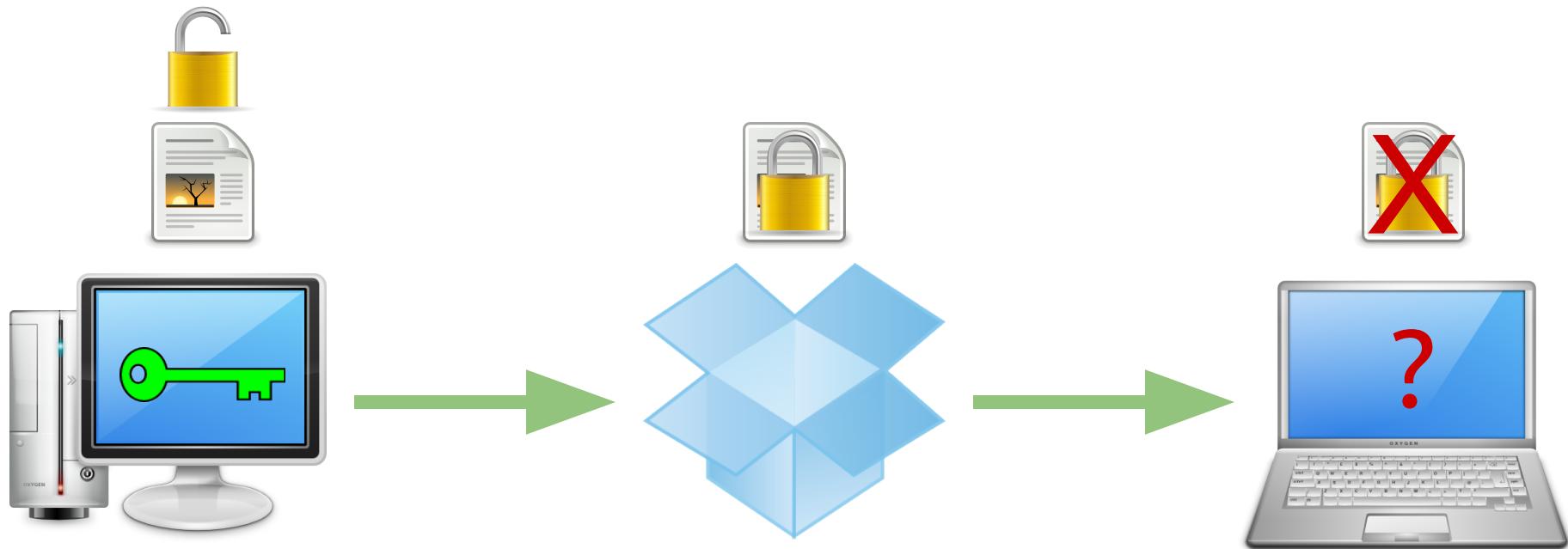
Example: Multi-Device File Sync



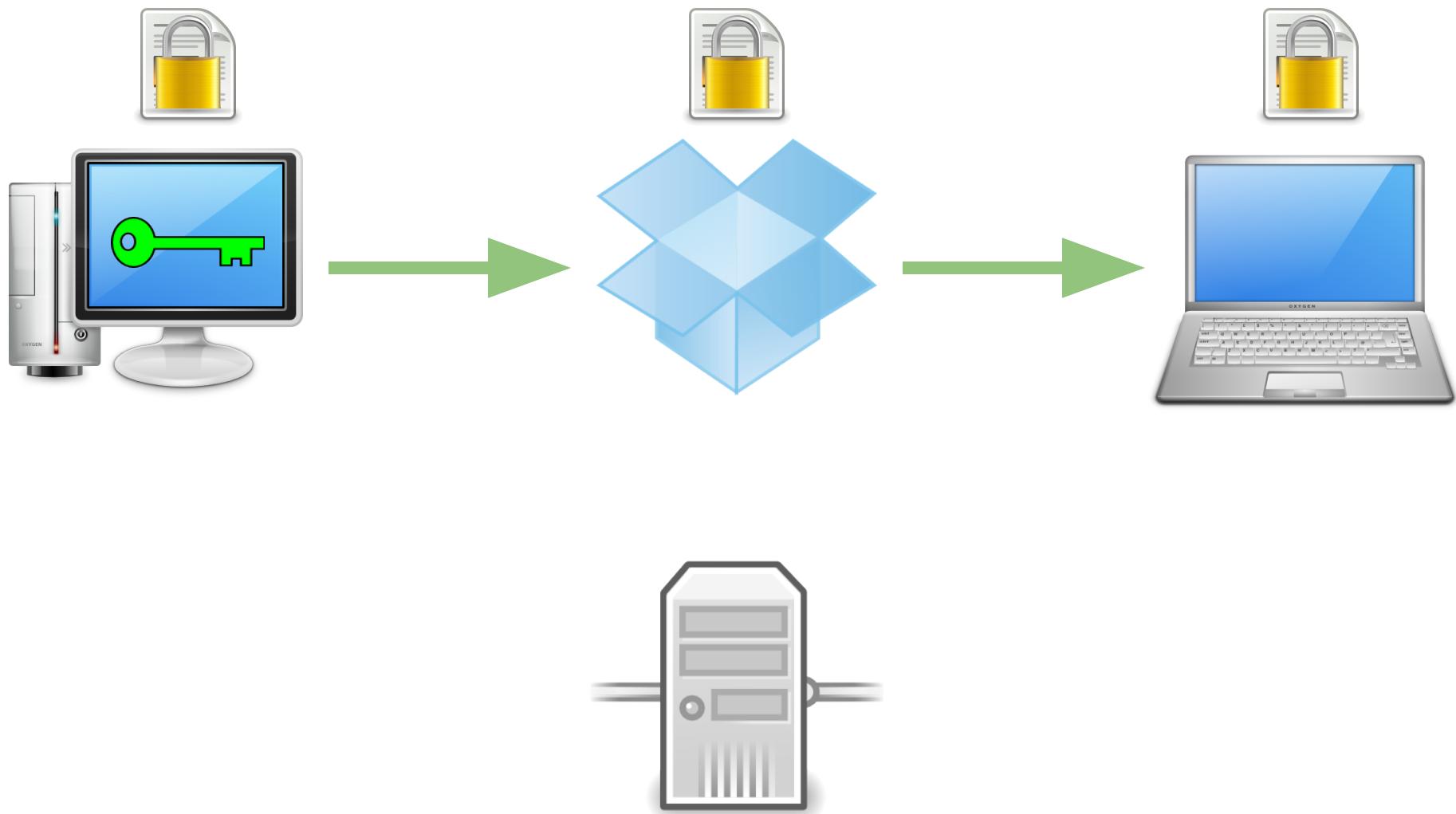
Example: Multi-Device File Sync



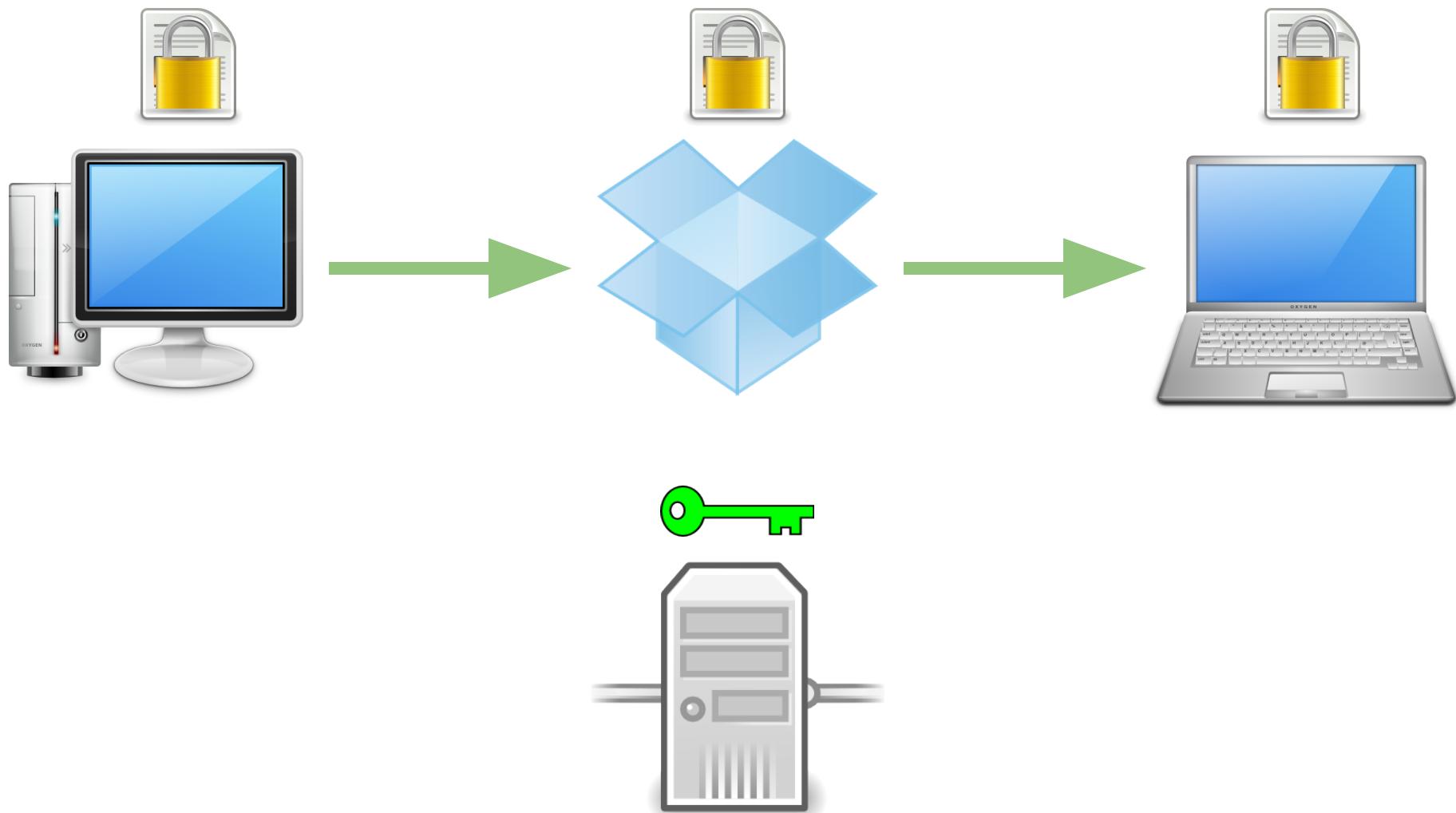
Example: Multi-Device File Sync



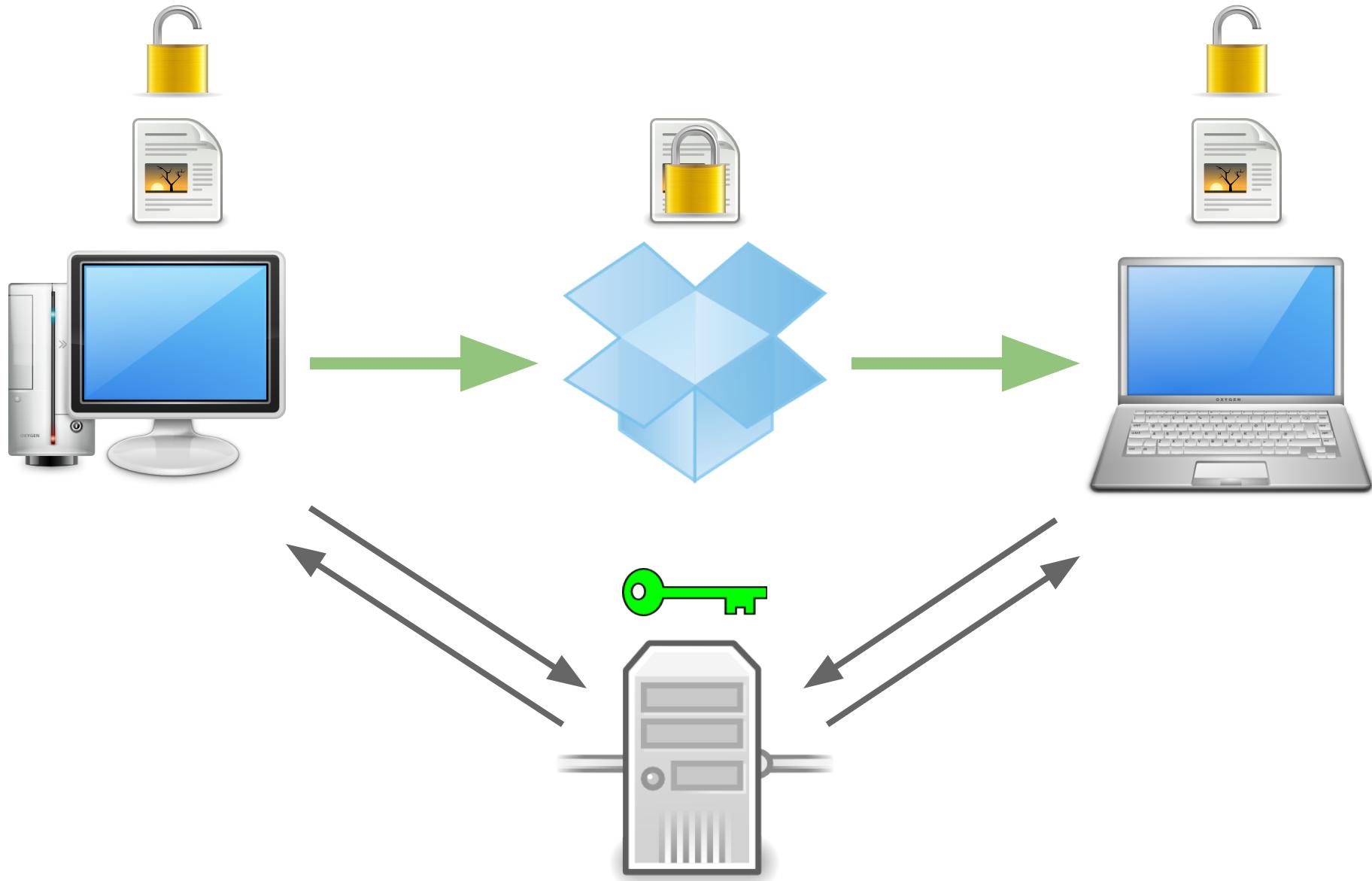
Example: Multi-Device File Sync



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

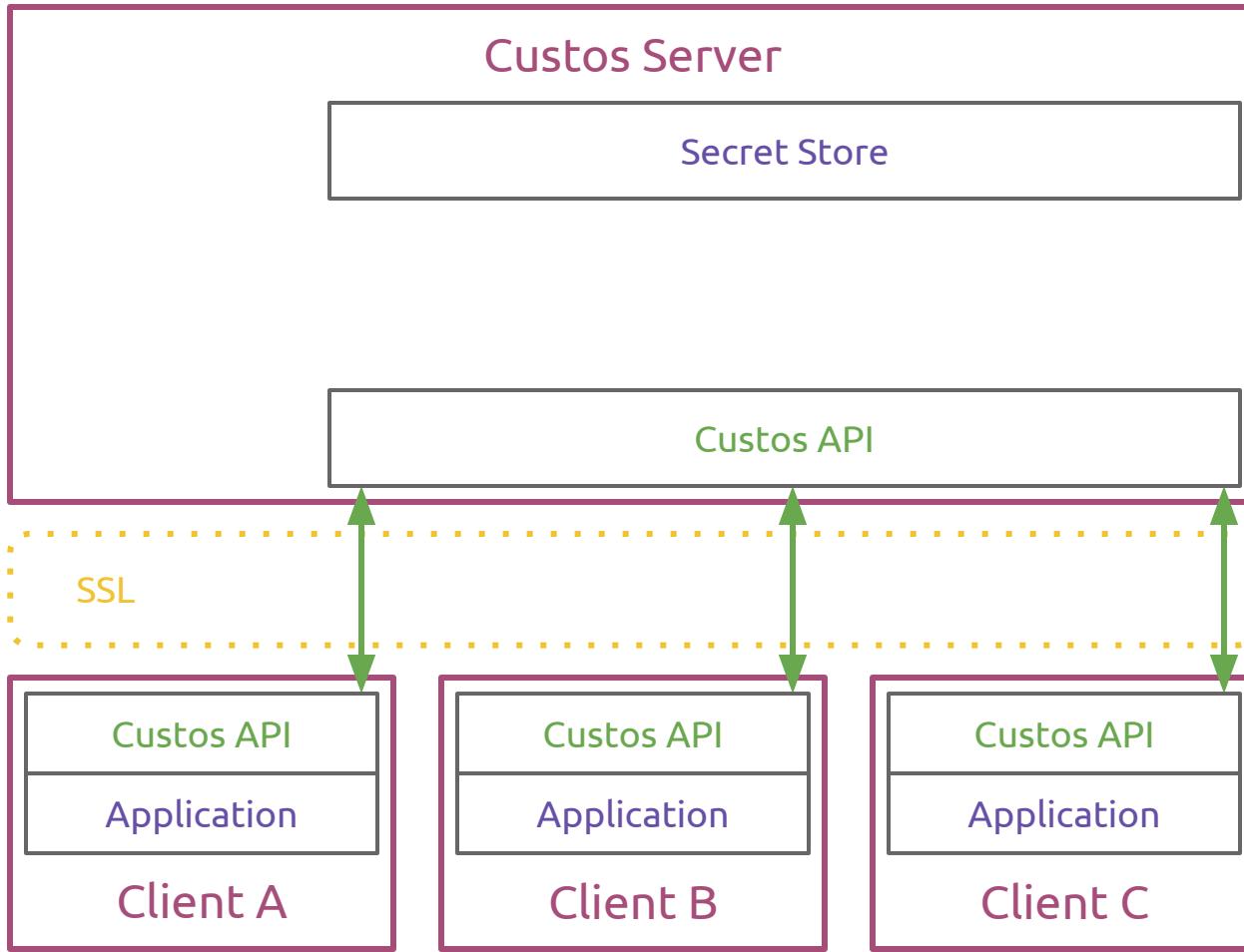
Client A

Application

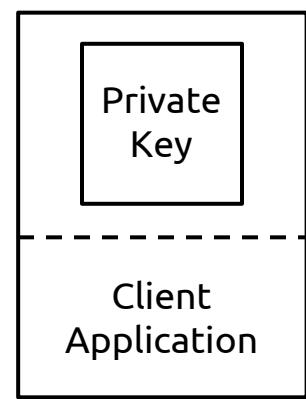
Client B

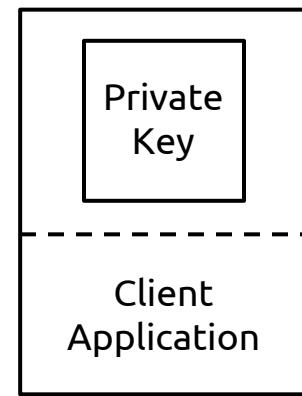
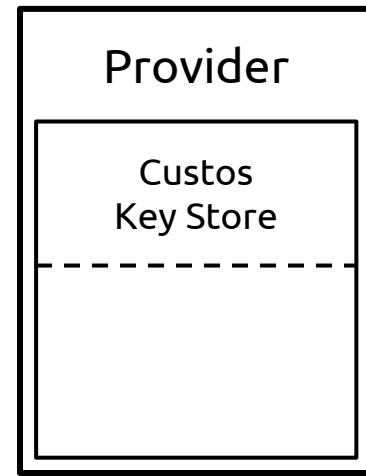
Application

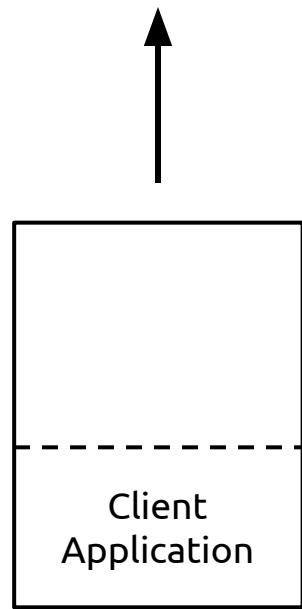
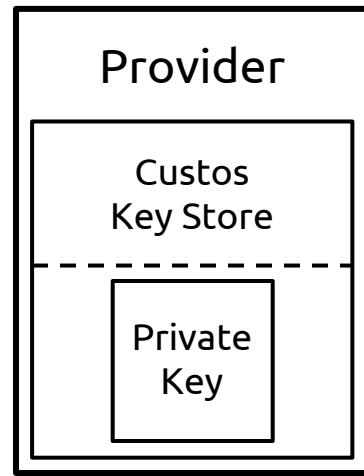
Client C



Trust?





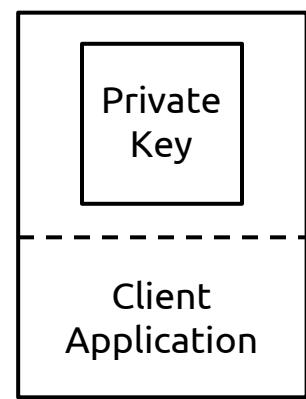


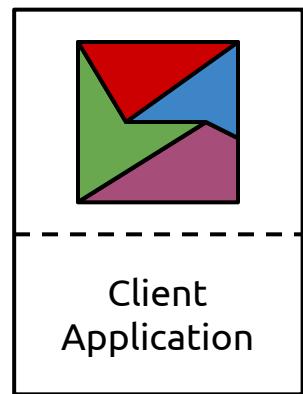
Do you have to trust
a single provider?

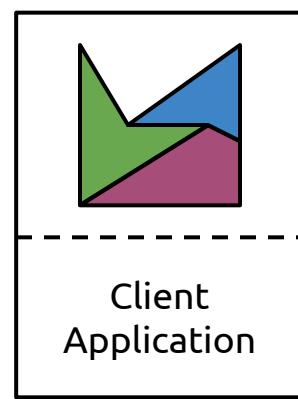
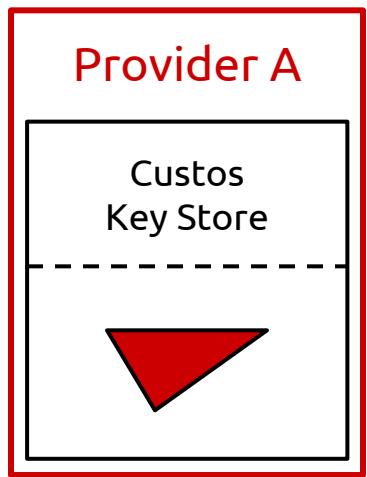
Multi-Provider Sharding

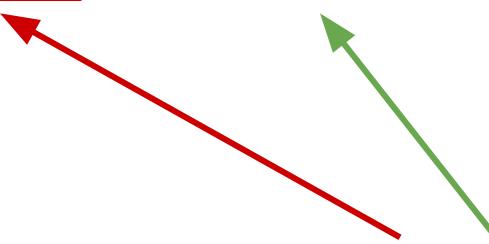
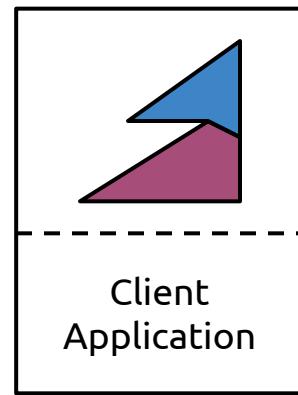
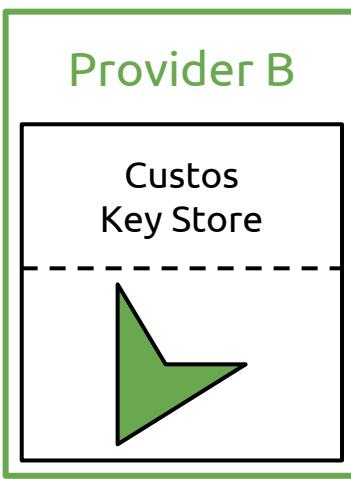
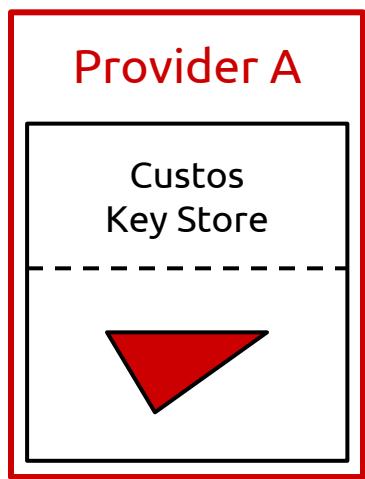
Multi-Provider Sharding

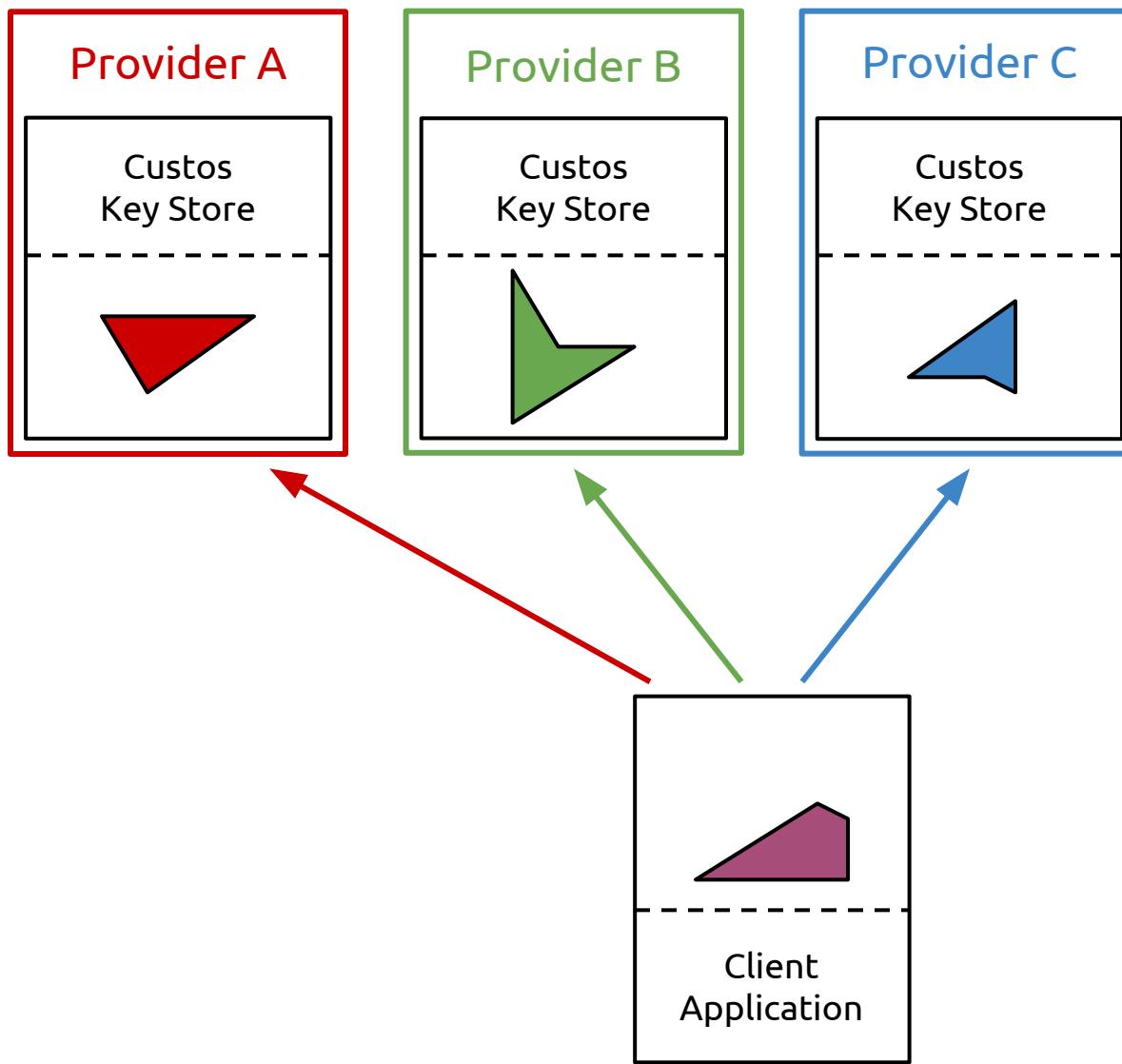
Shamir Secret Sharing

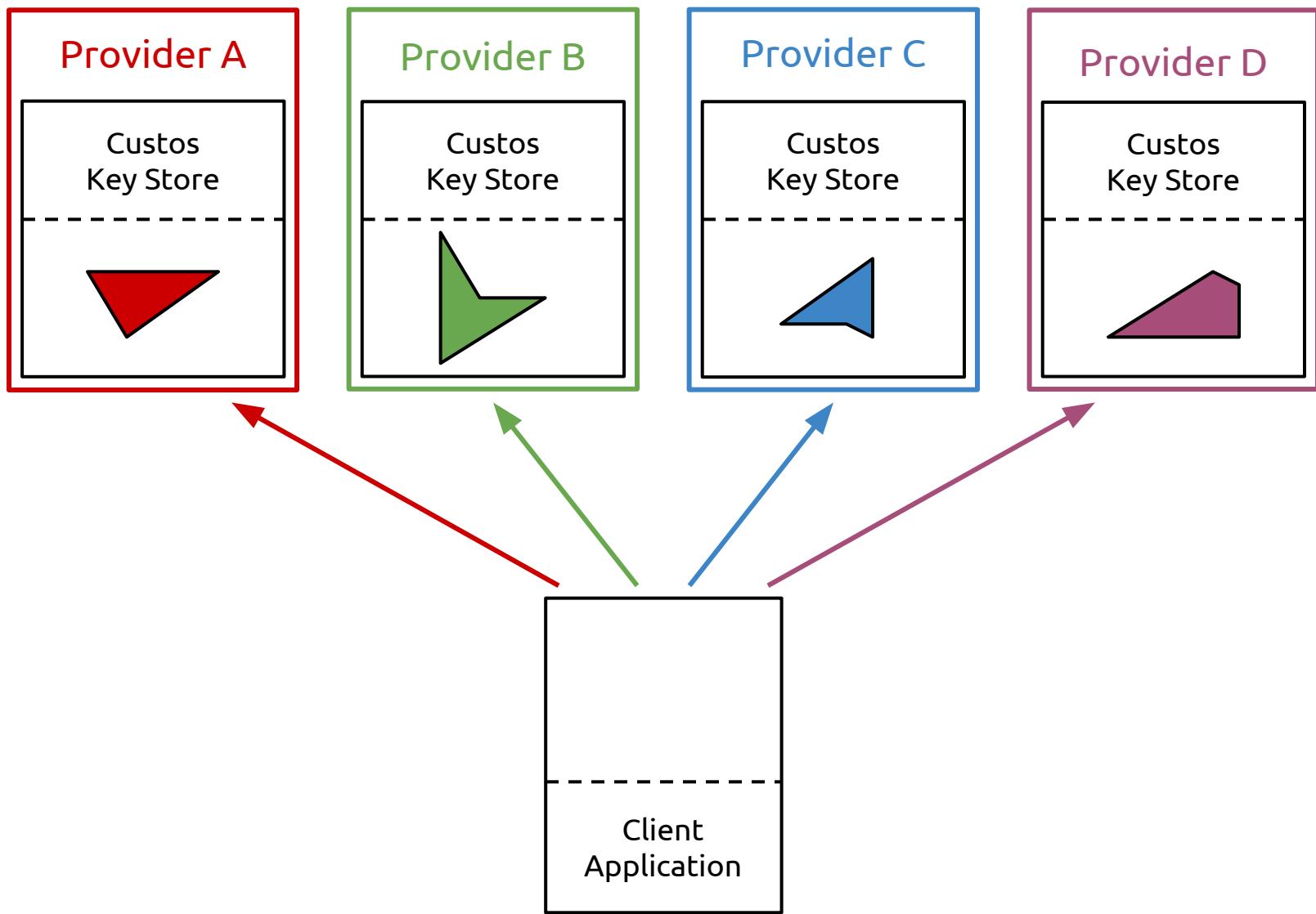


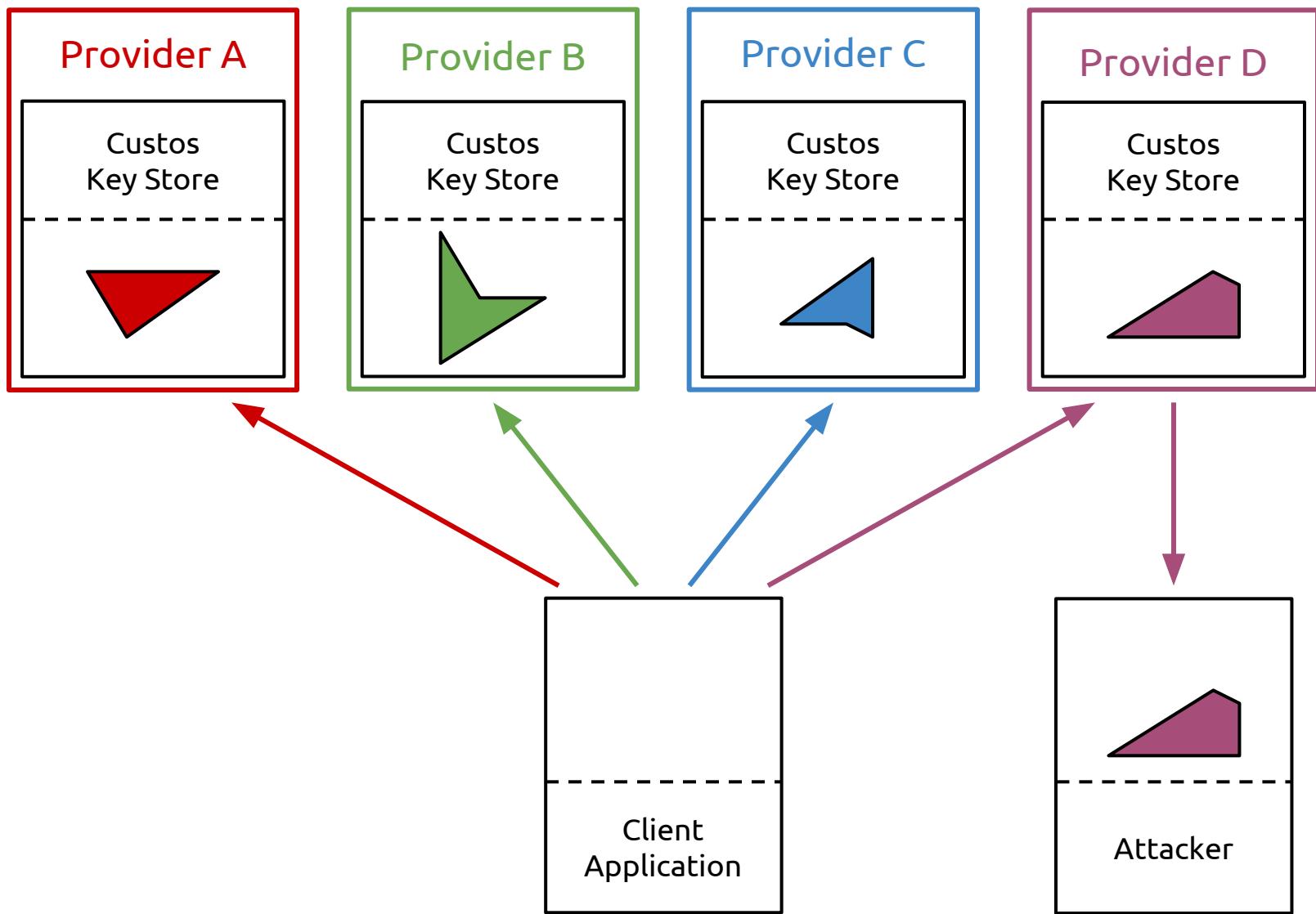


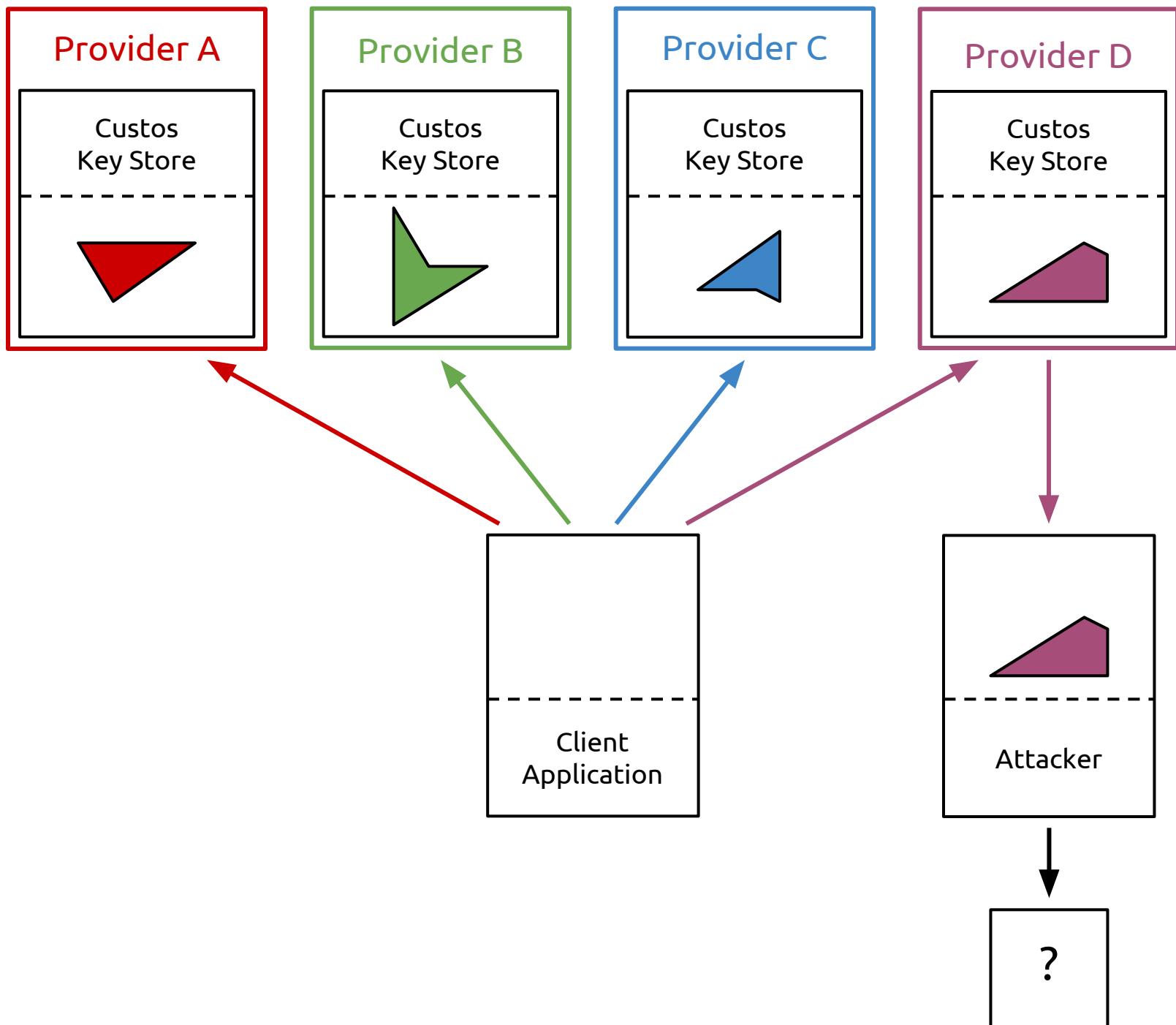












Availability

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



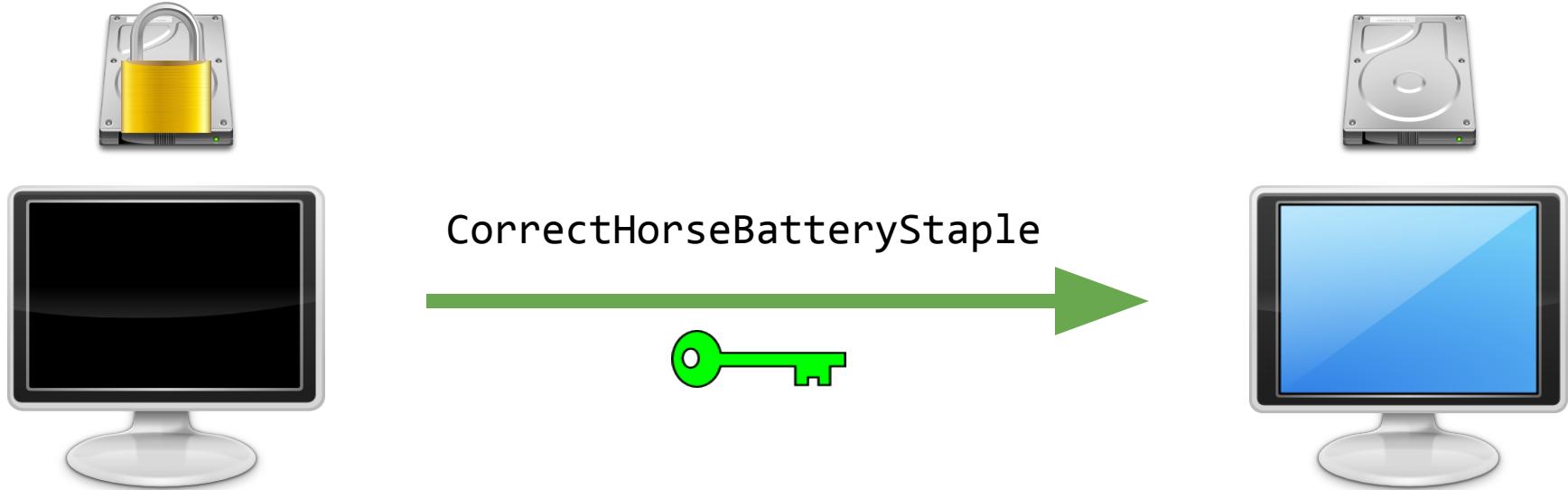
Example: Autonomous Server Bootup



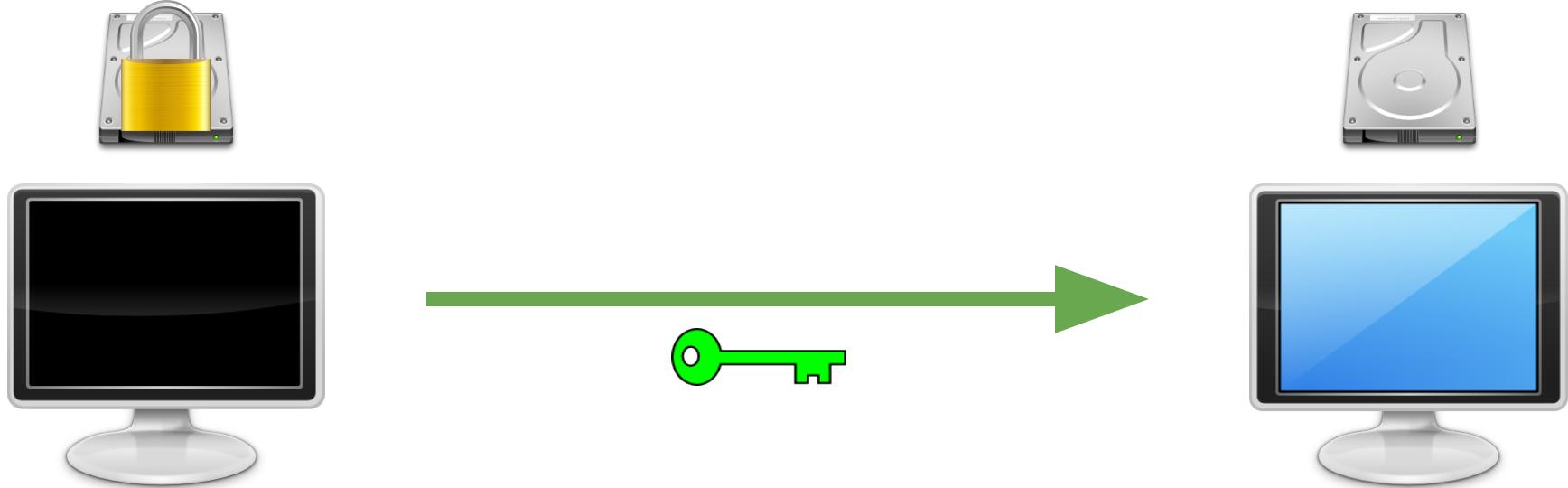
CorrectHorseBatteryStaple



Example: Autonomous Server Bootup



Example: Autonomous Server Bootup



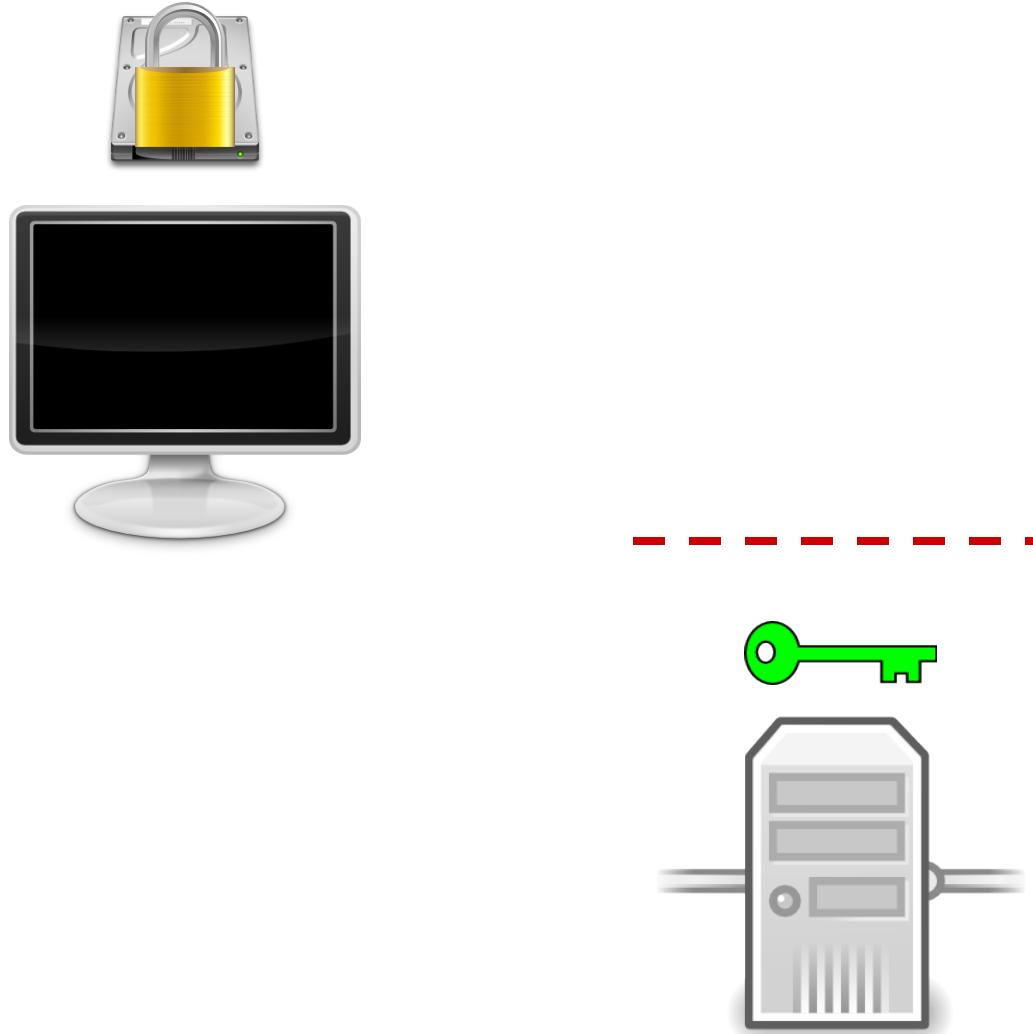
Example: Autonomous Server Bootup



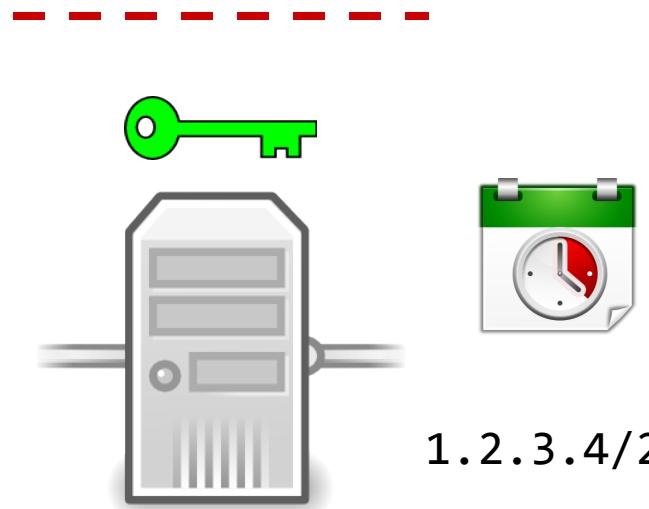
Example: Autonomous Server Bootup



Example: Autonomous Server Bootup

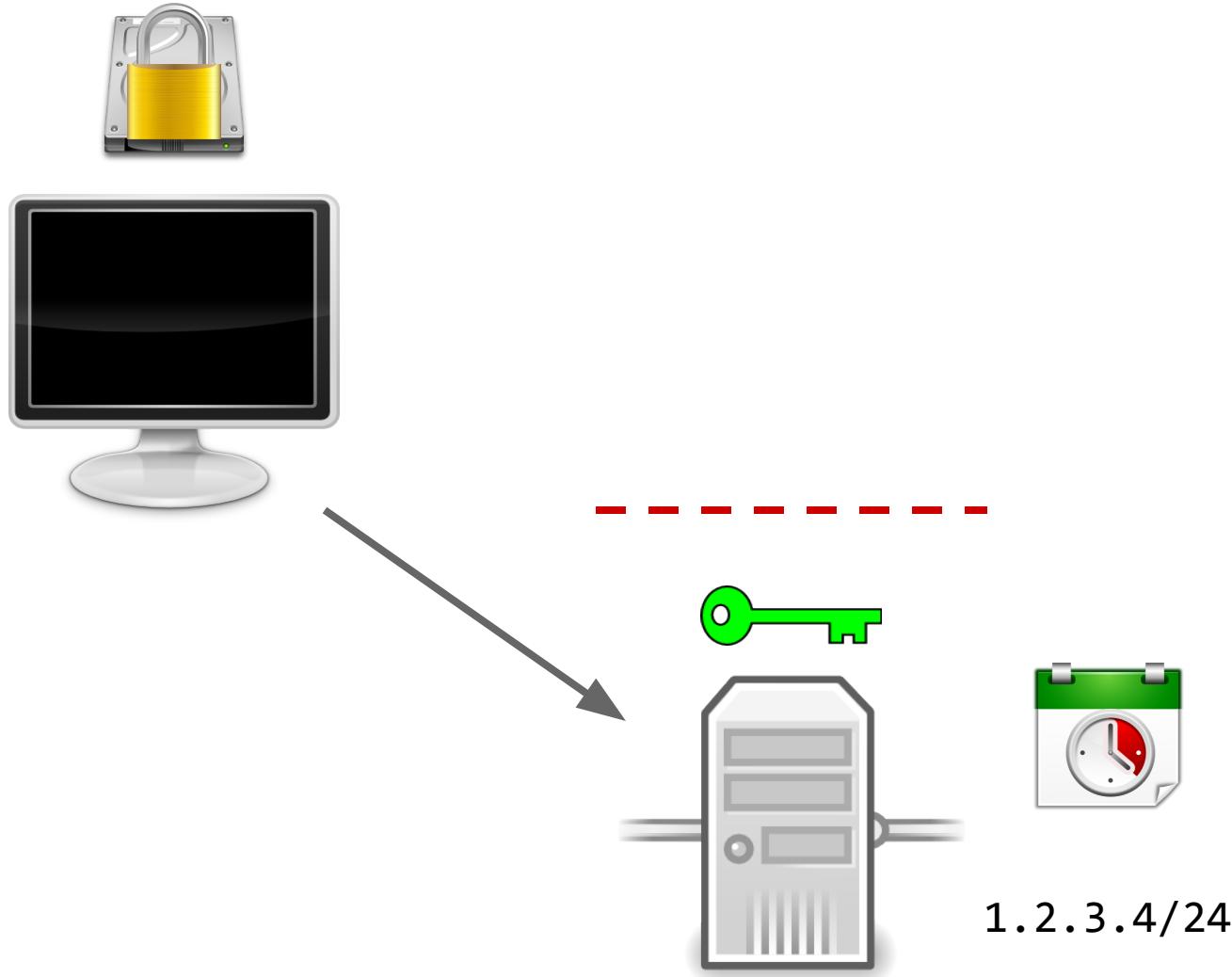


Example: Autonomous Server Bootup

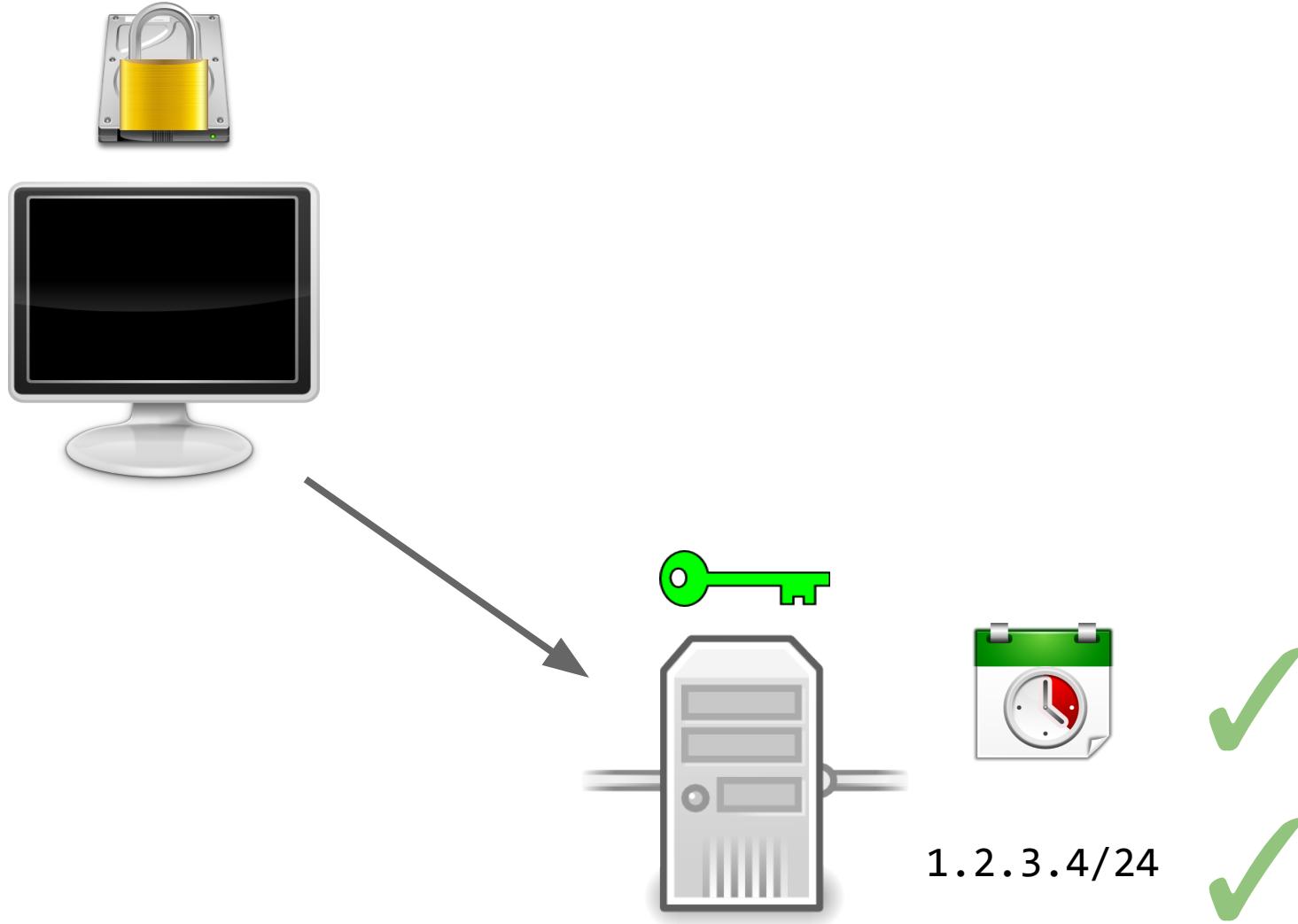


1.2.3.4/24

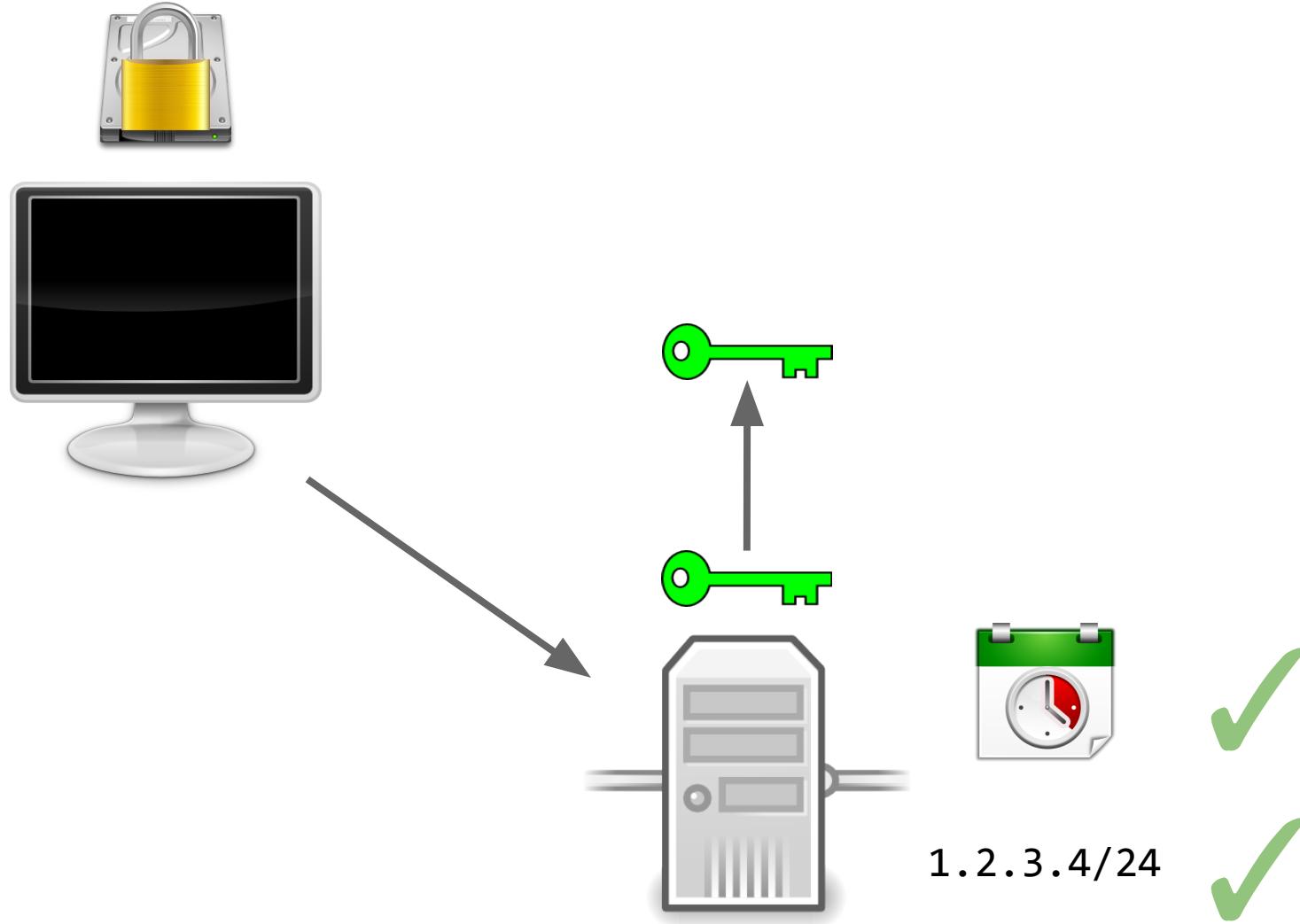
Example: Autonomous Server Bootup



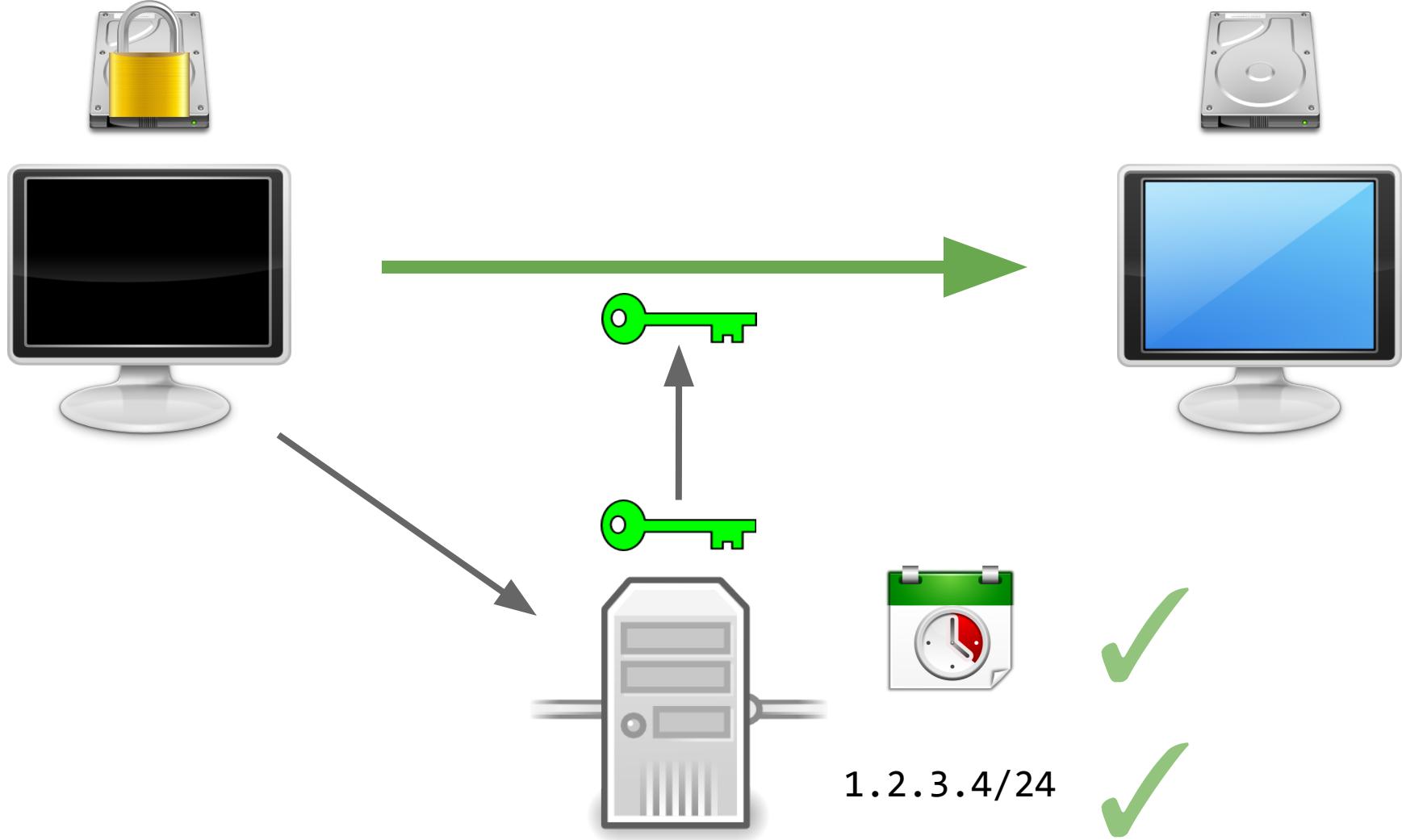
Example: Autonomous Server Bootup



Example: Autonomous Server Bootup



Example: Autonomous Server Bootup

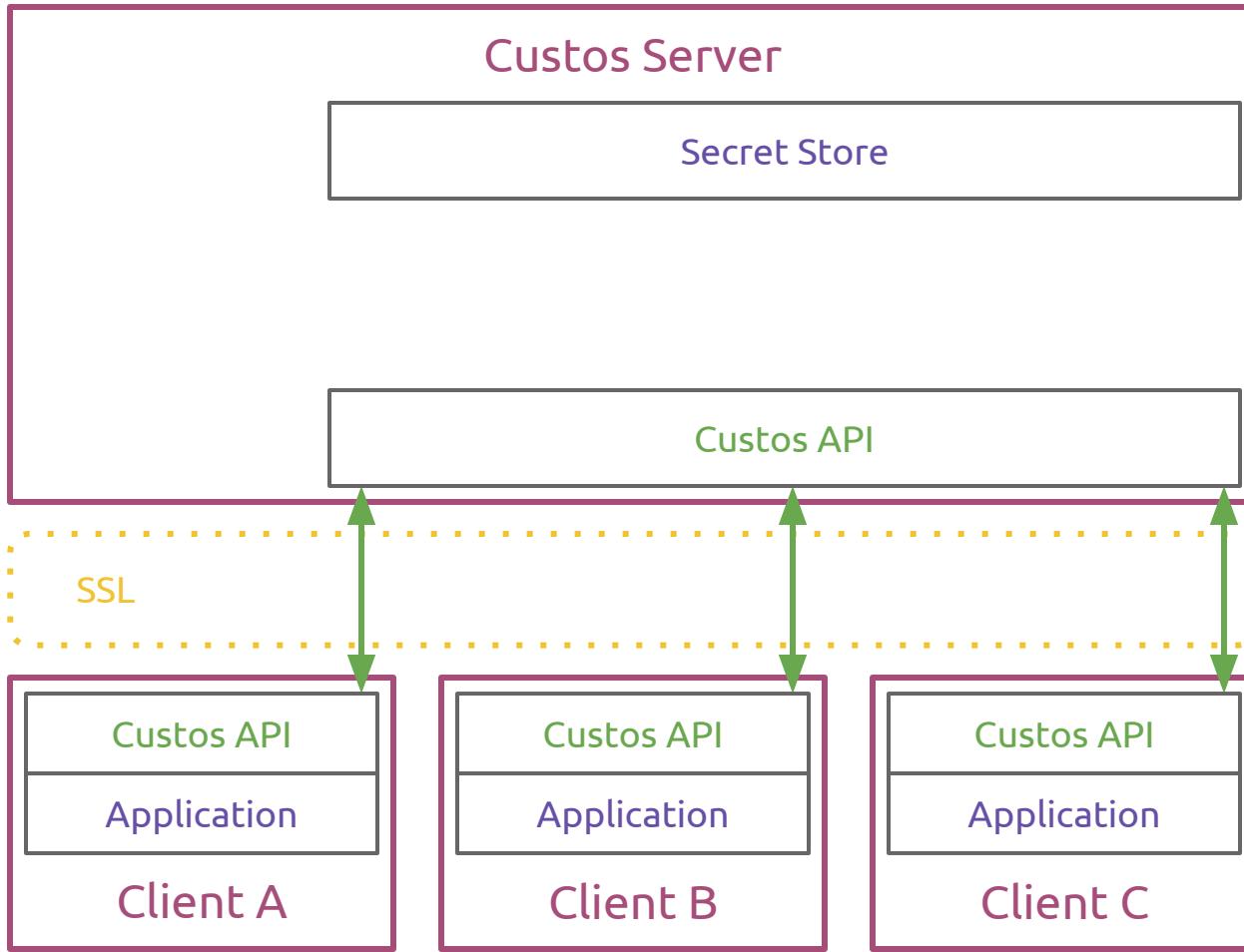


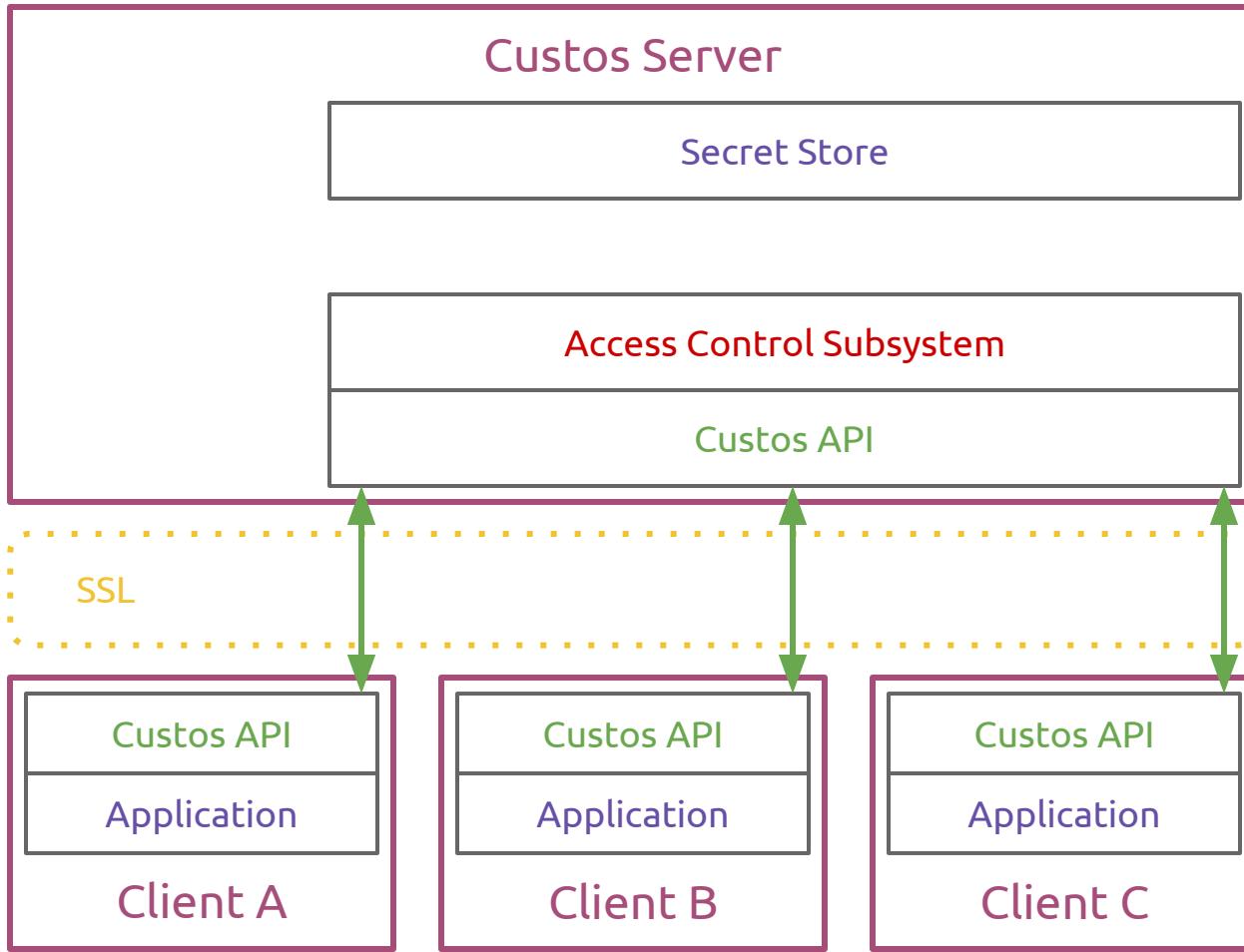
Backup Systems

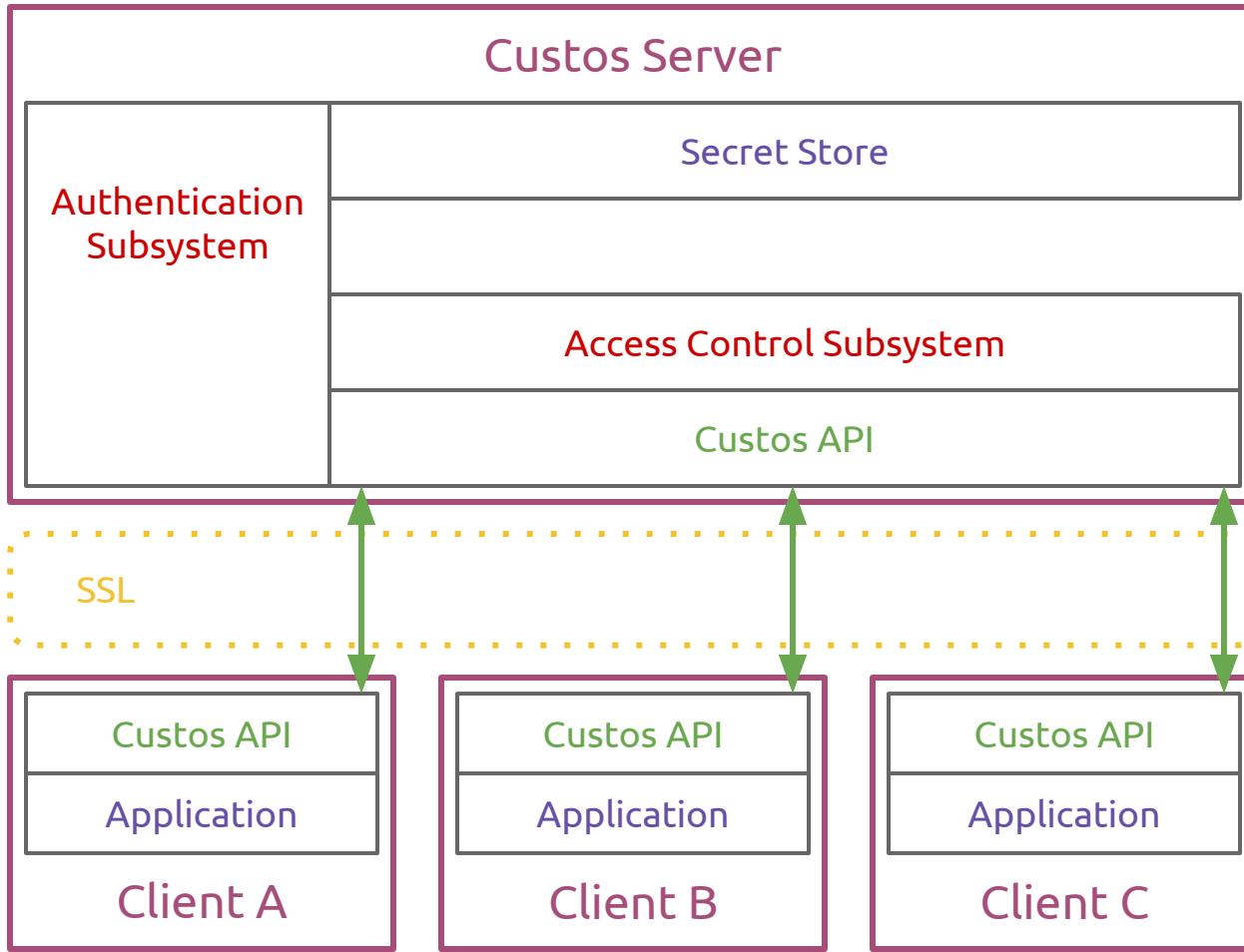
Backup Systems Time-Limited Access

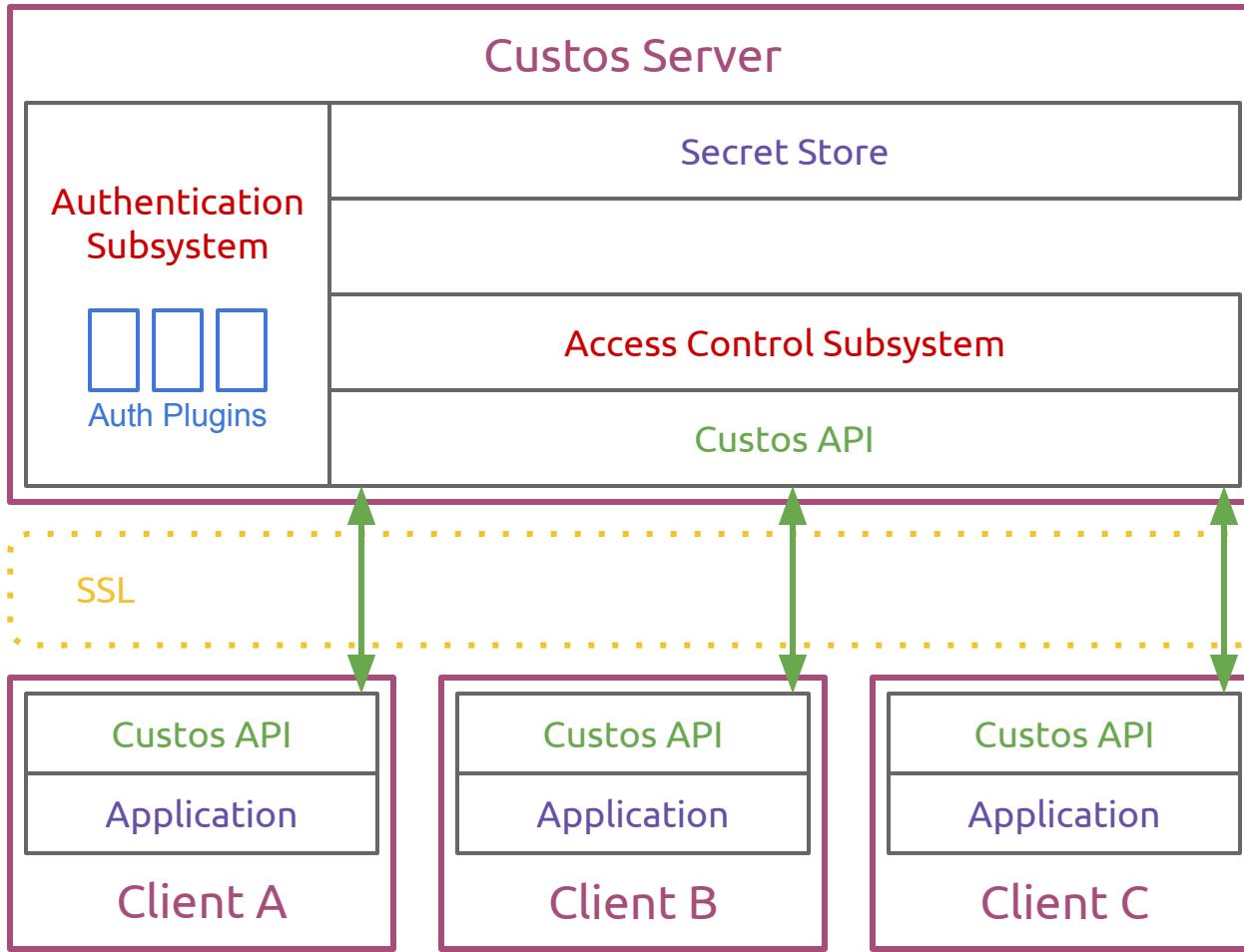
Backup Systems
Time-Limited Access
Etc...

Flexible Access Control in Custos









“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



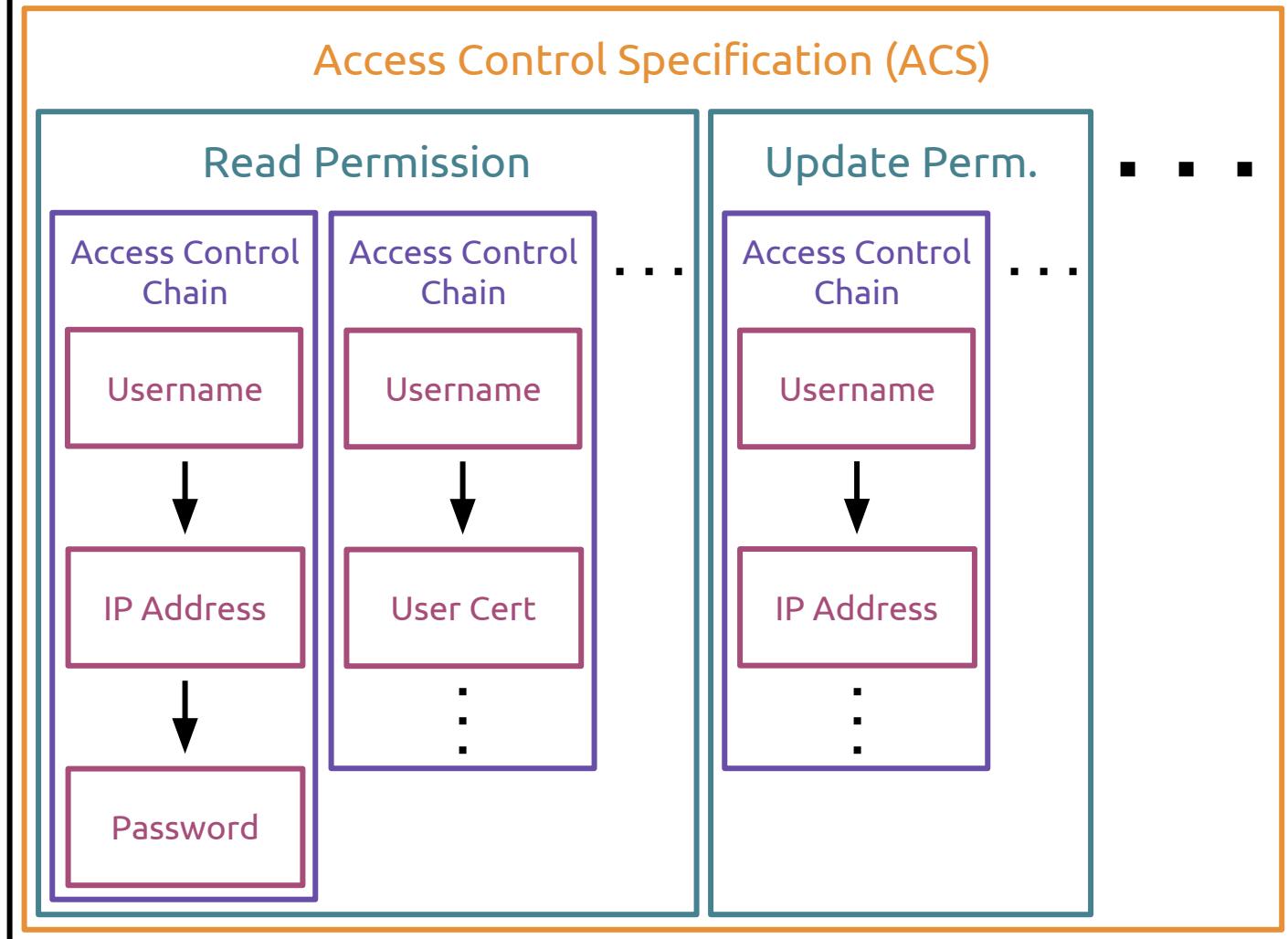
IP Address



:

■ ■ ■

“Secret”



Authentication Attributes

Authentication Attributes

Plugin-Based

Explicit

ip_src

user_agent

time_utc

...

Implicit

user_id

psk

psk_sha256

...

Centralized Secret Storage

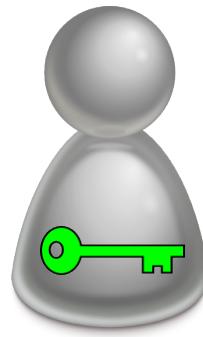
Flexible Access Control

Centralized Secret Storage

Flexible Access Control

Auditing and Revocation

Example: Revoke Shared Access



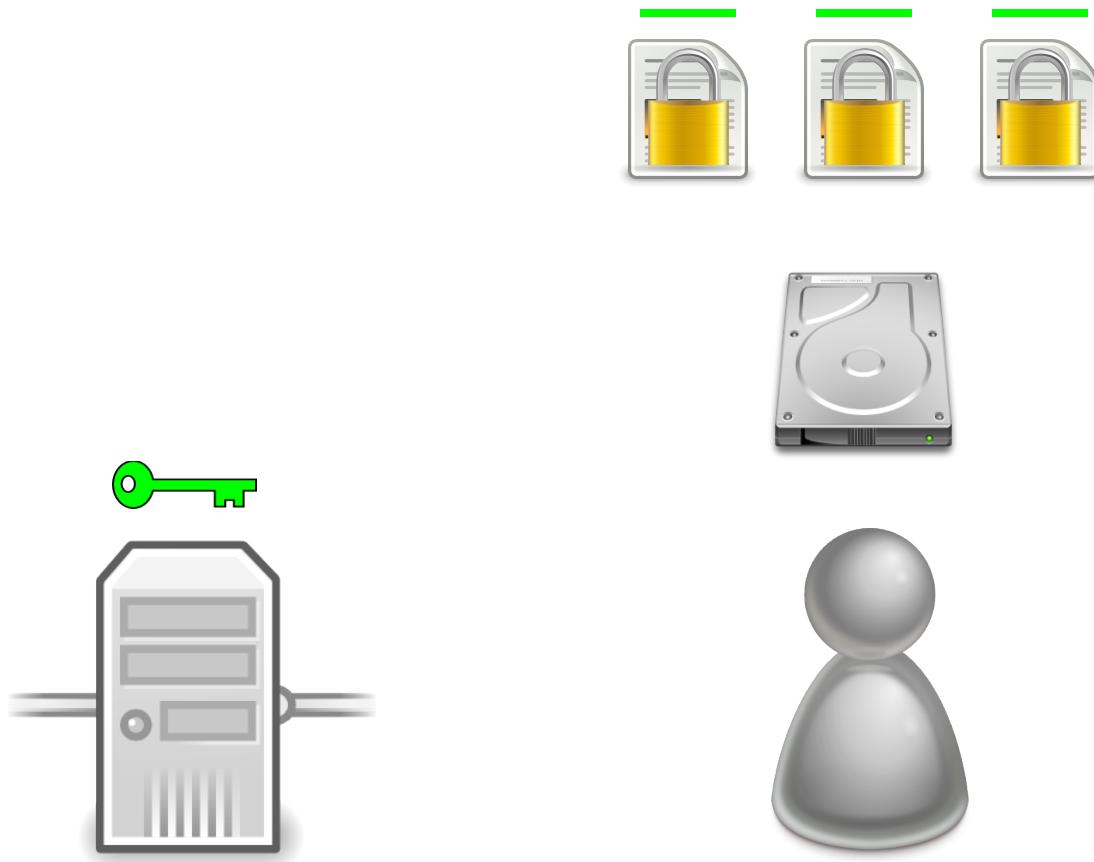
Example: Revoke Shared Access



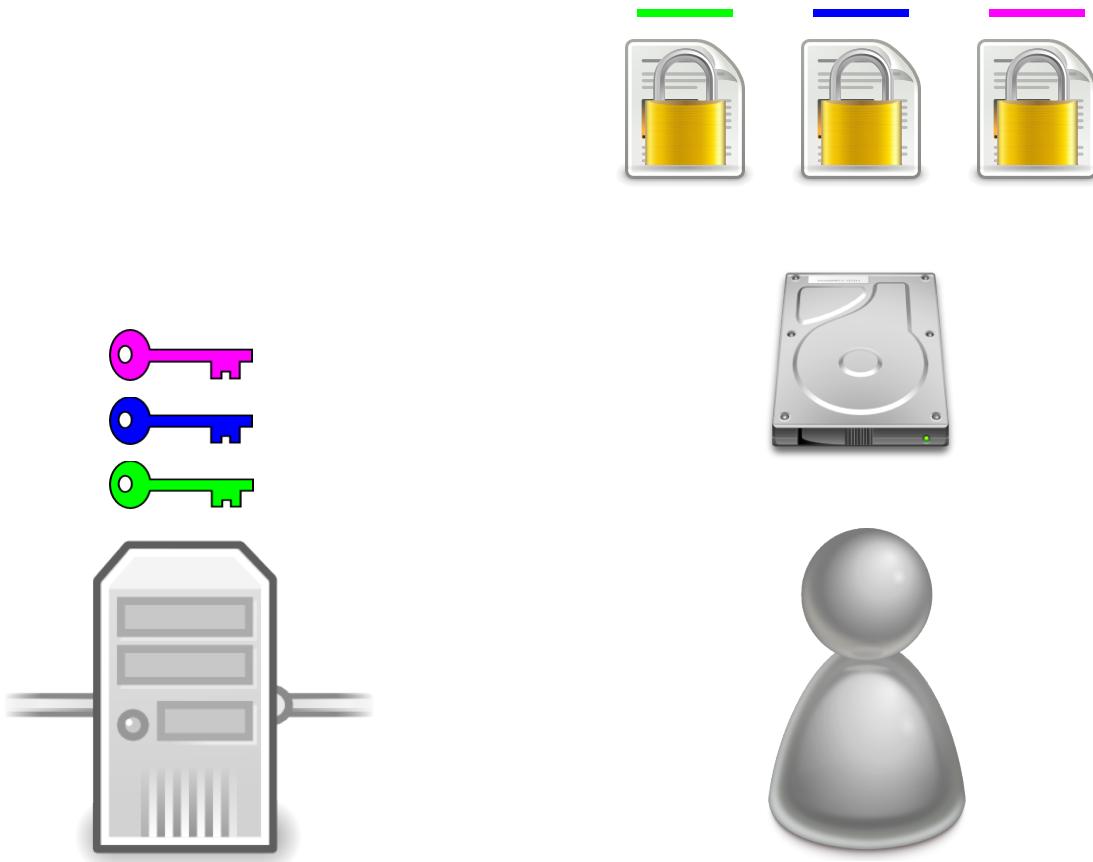
Example: Revoke Shared Access



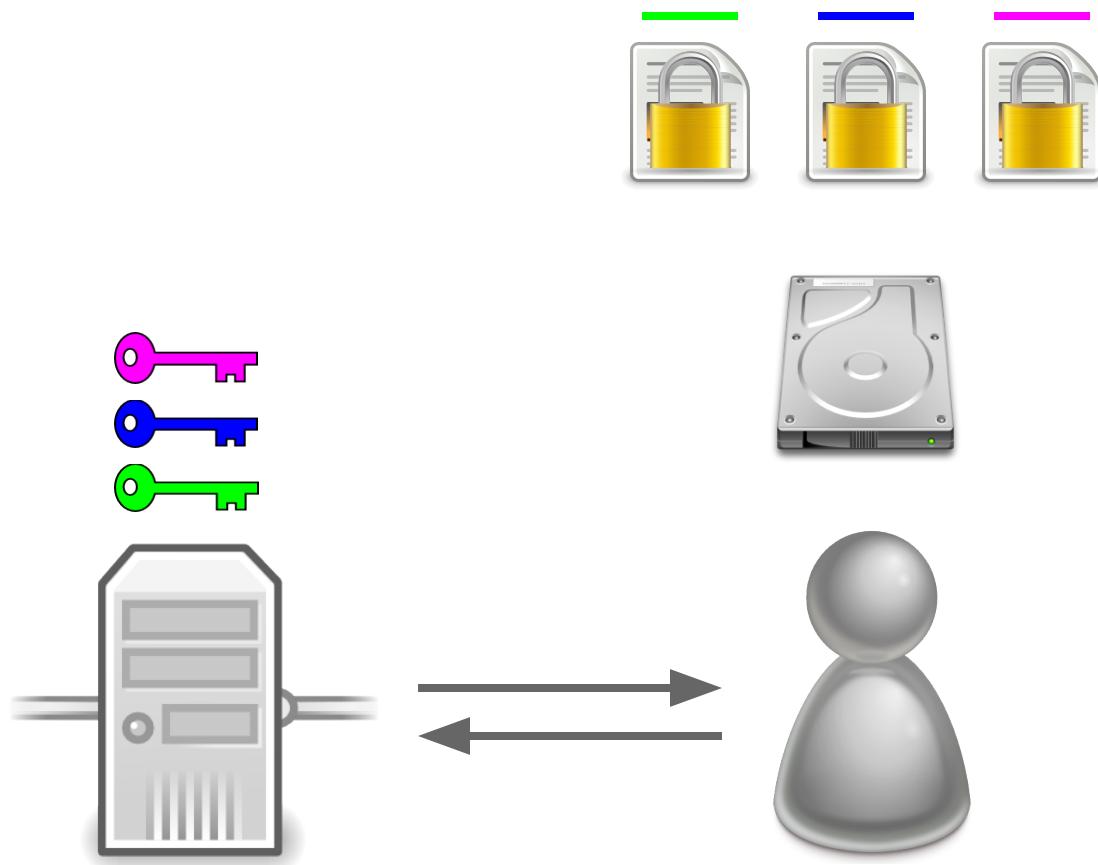
Example: Revoke Shared Access



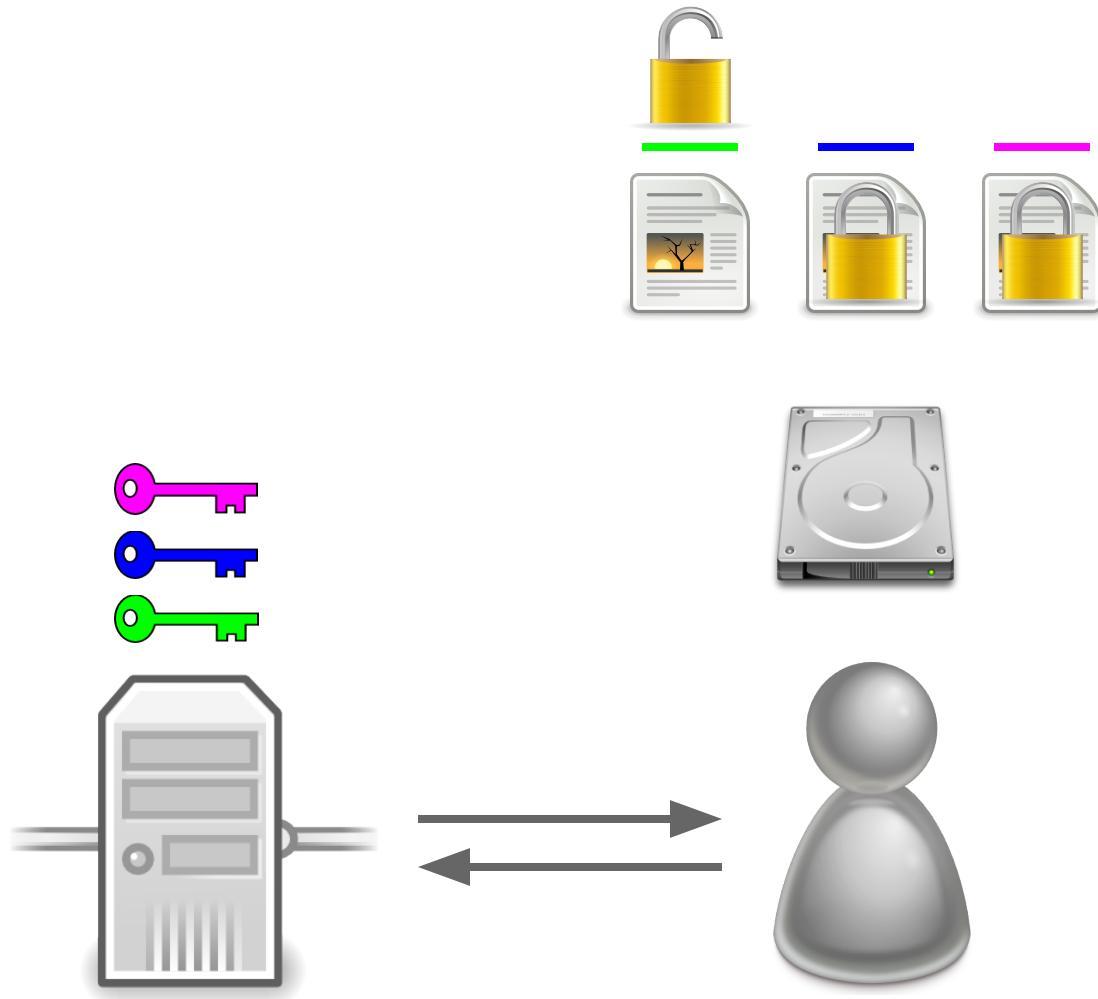
Example: Revoke Shared Access



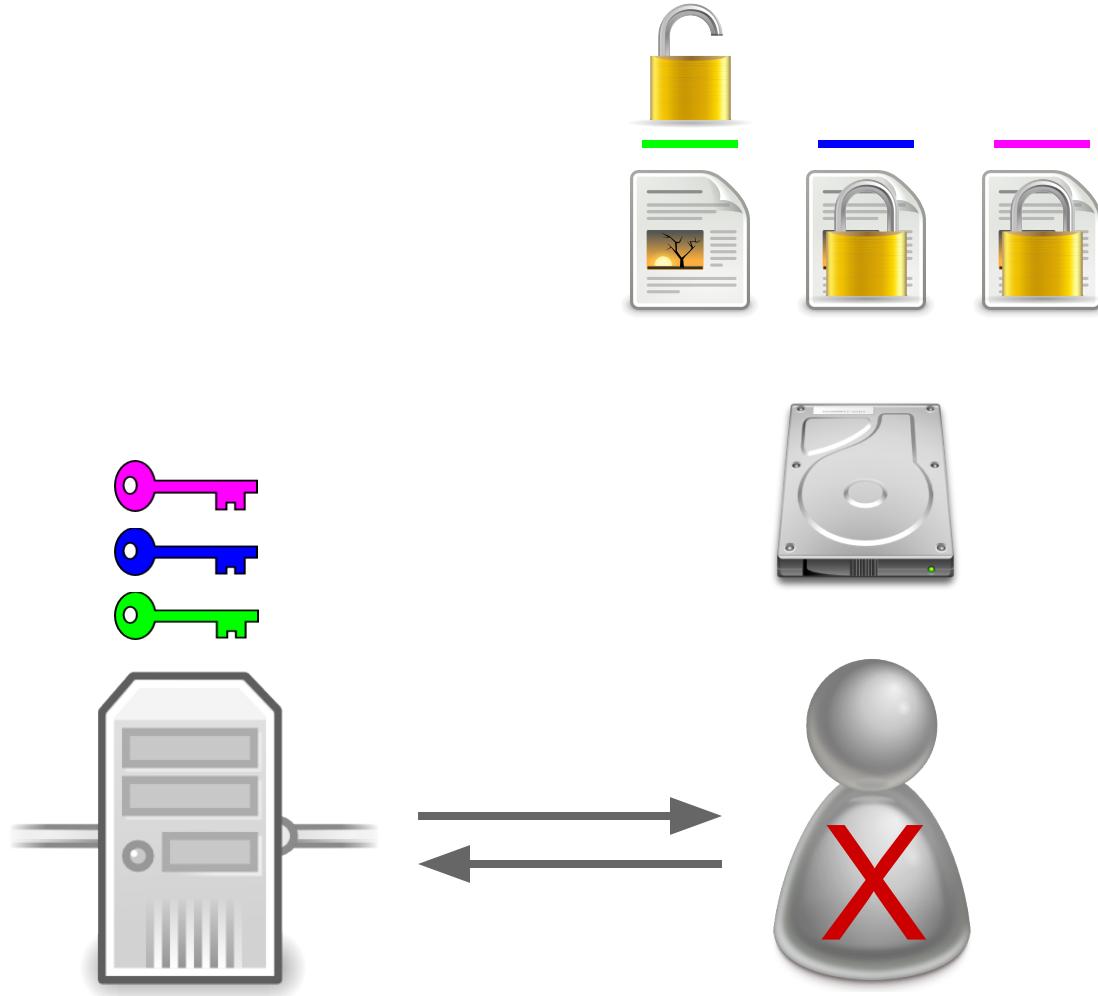
Example: Revoke Shared Access



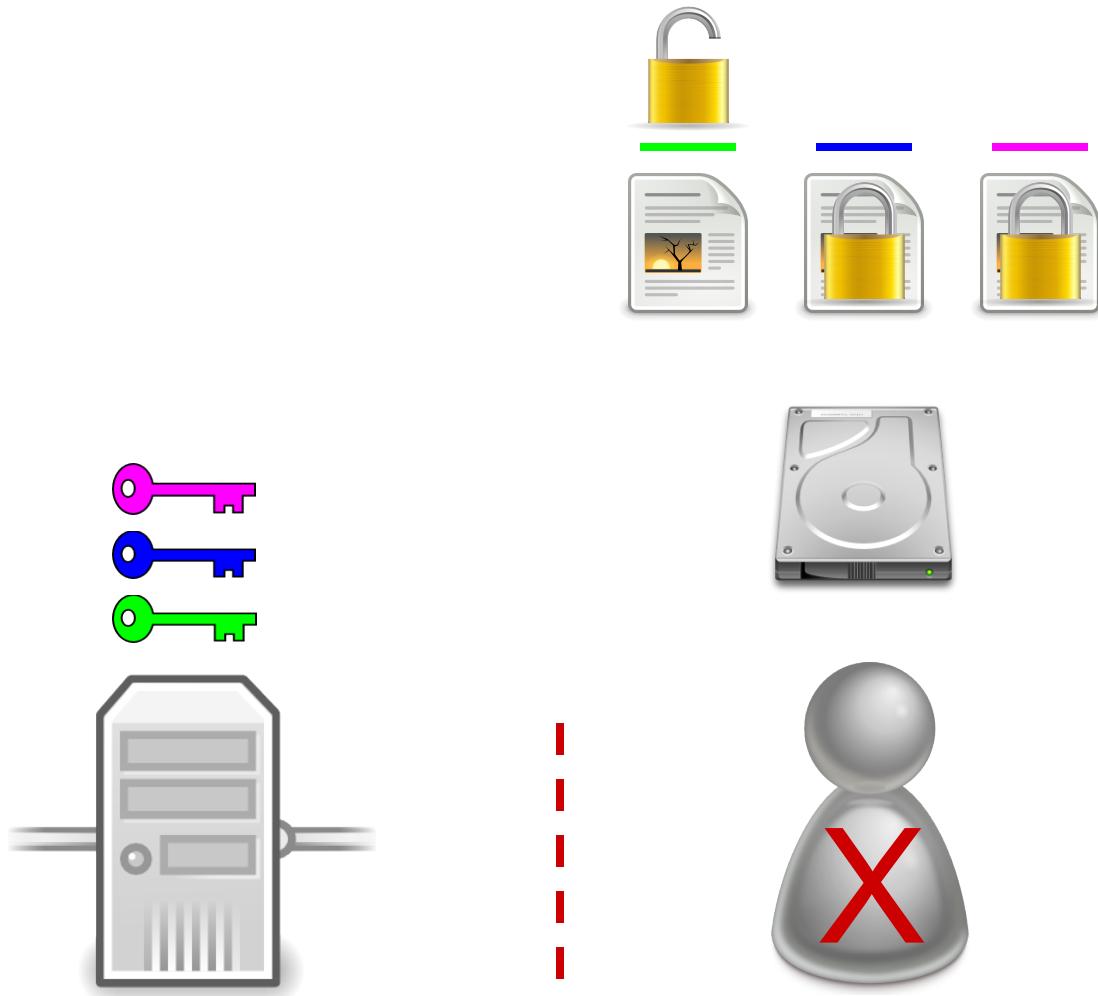
Example: Revoke Shared Access



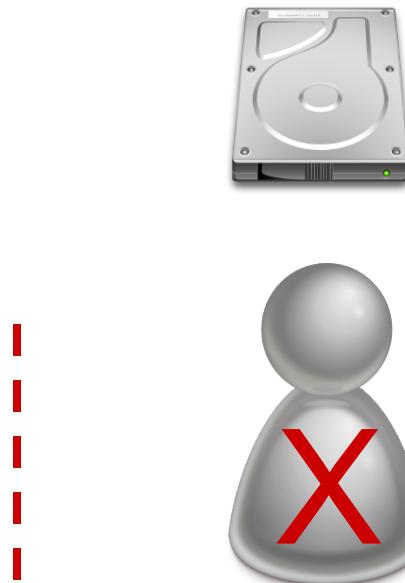
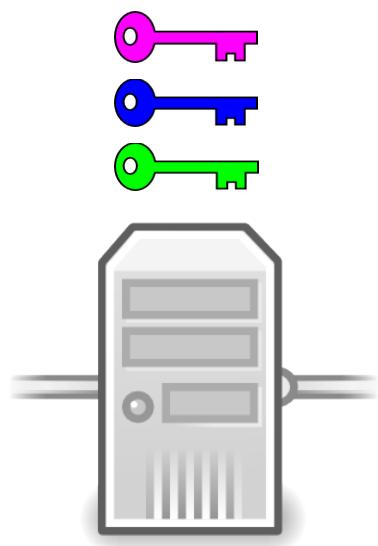
Example: Revoke Shared Access



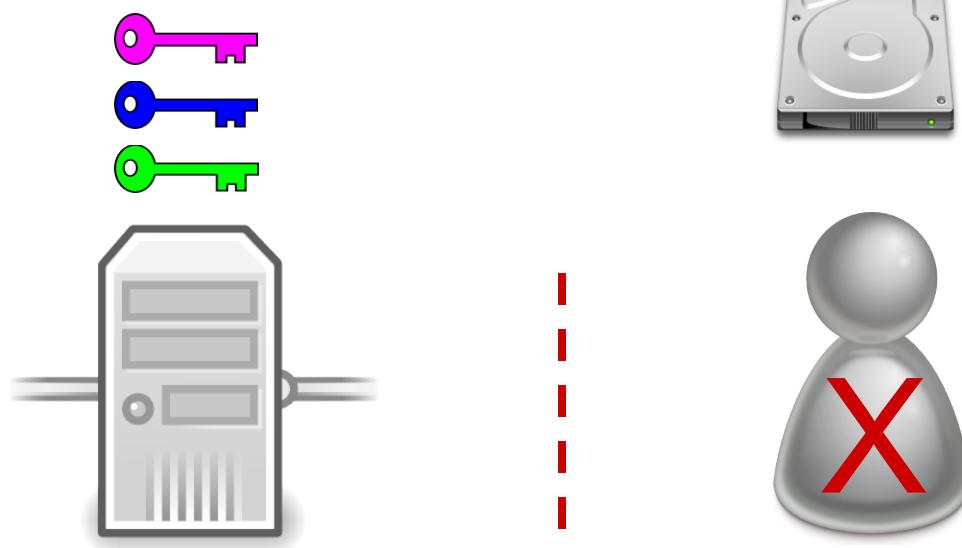
Example: Revoke Shared Access



Example: Revoke Shared Access



Example: Revoke Shared Access



140813: Bob Accessed



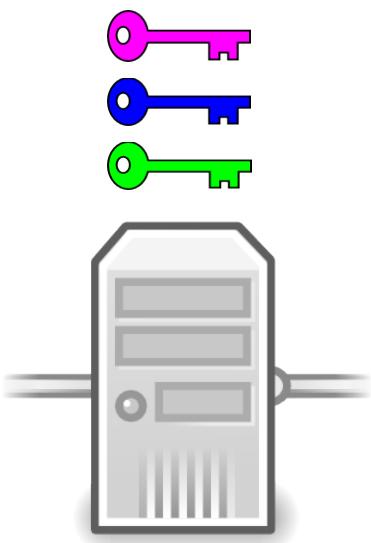
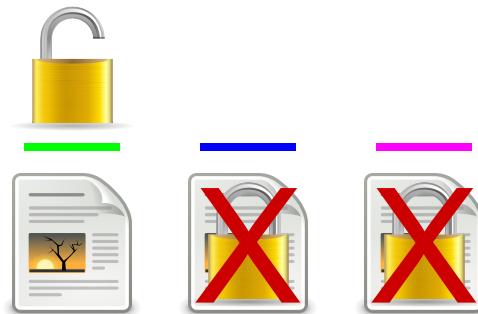
140906: Bob Accessed



141003: Bob Accessed



Example: Revoke Shared Access



140813: Bob Accessed



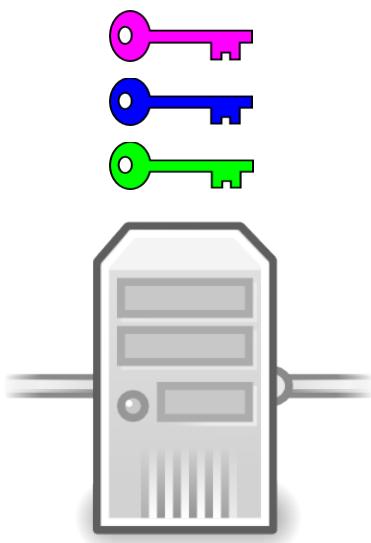
140906: Bob Accessed



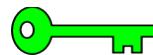
141003: Bob Accessed



Example: Revoke Shared Access



140813: Bob Accessed



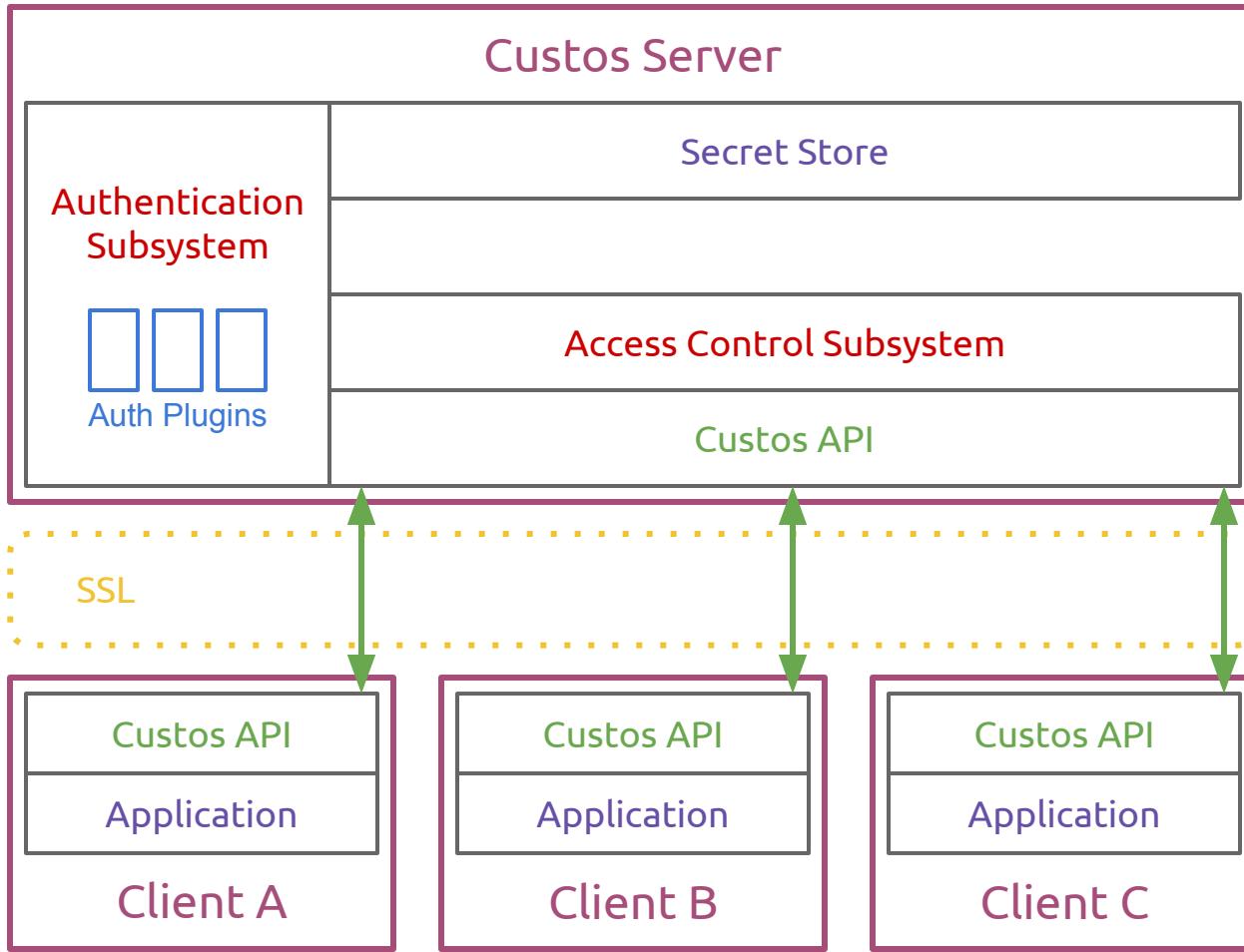
140906: Bob Accessed

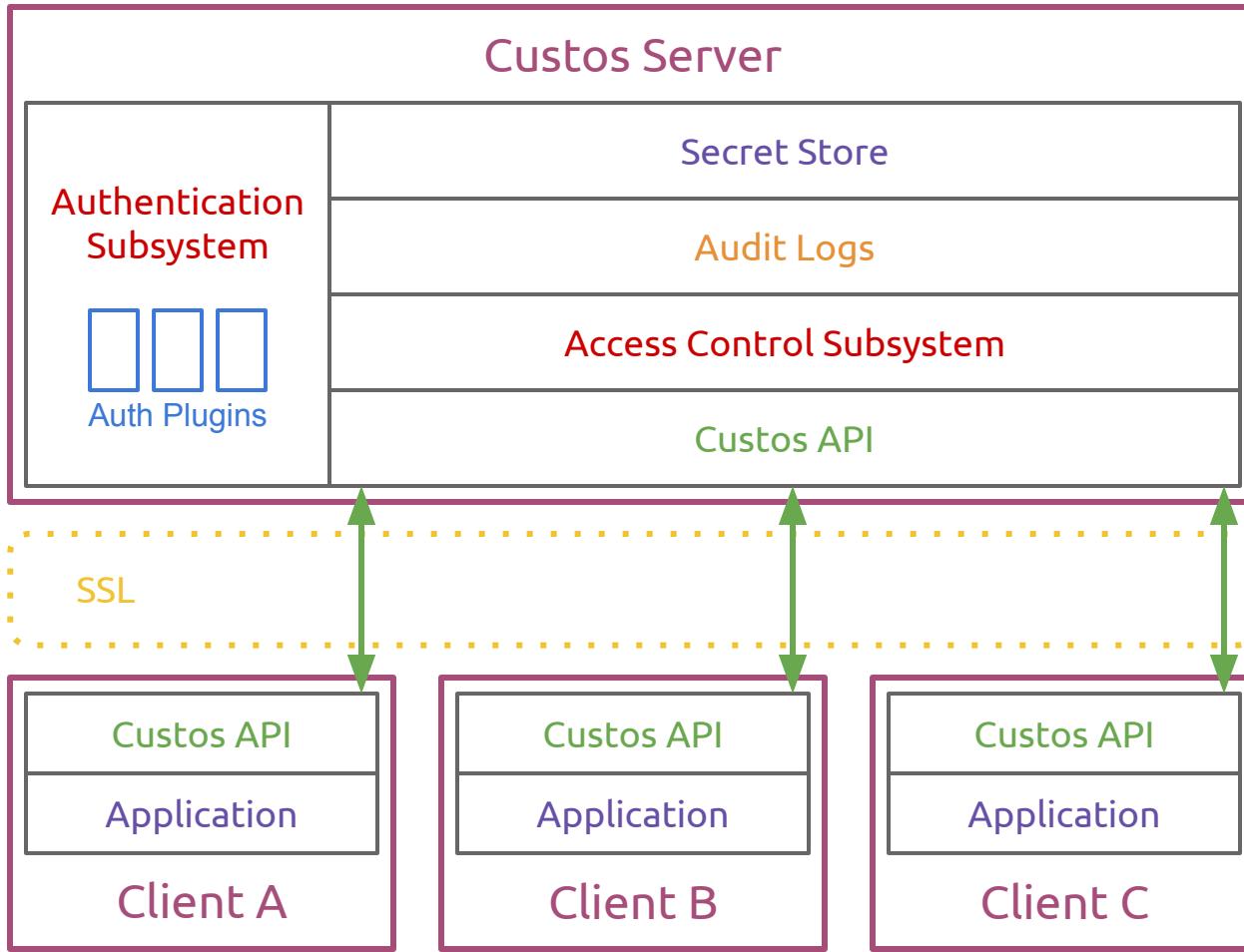


141003: Bob Accessed



Auditing and Revocation in Custos





140813: Bob Accessed Key A

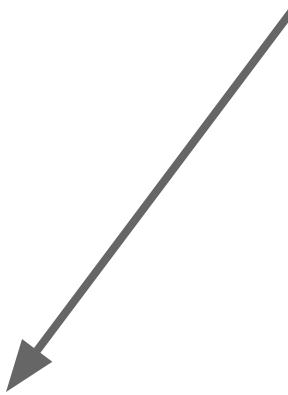
140906: Bob Accessed Key B

141003: Bob Accessed Key A

140813: Bob Accessed Key A

140906: Bob Accessed Key B

141003: Bob Accessed Key A

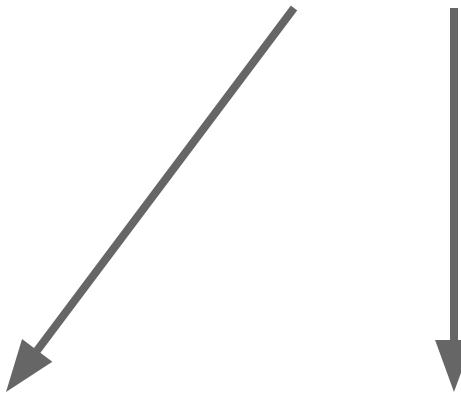


Revocation
Semantics

140813: Bob Accessed Key A

140906: Bob Accessed Key B

141003: Bob Accessed Key A



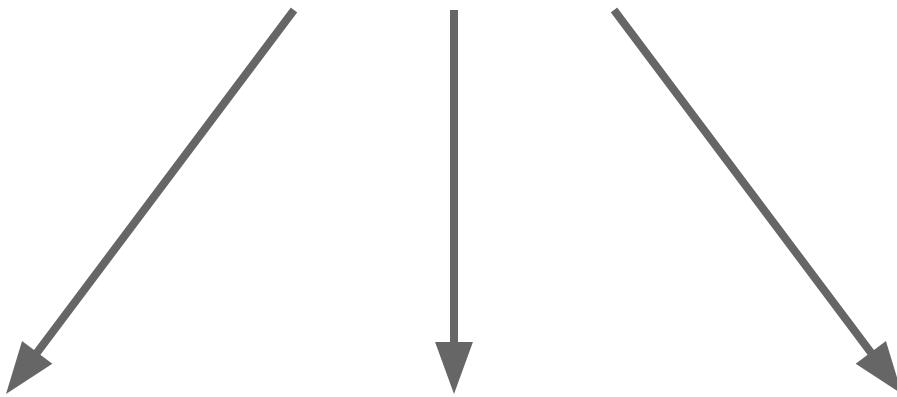
Revocation
Semantics

Intrusion
Detection

140813: Bob Accessed Key A

140906: Bob Accessed Key B

141003: Bob Accessed Key A



Revocation
Semantics

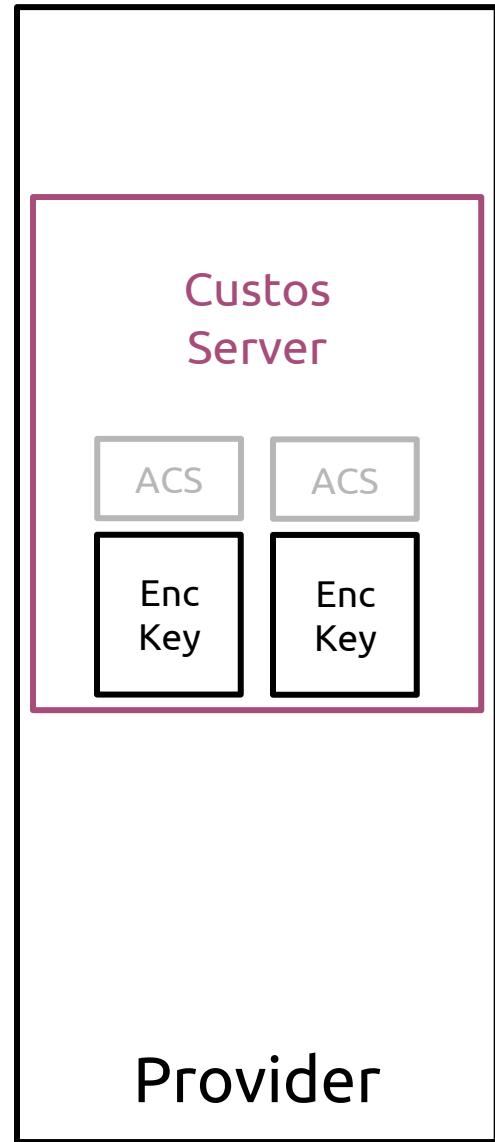
Intrusion
Detection

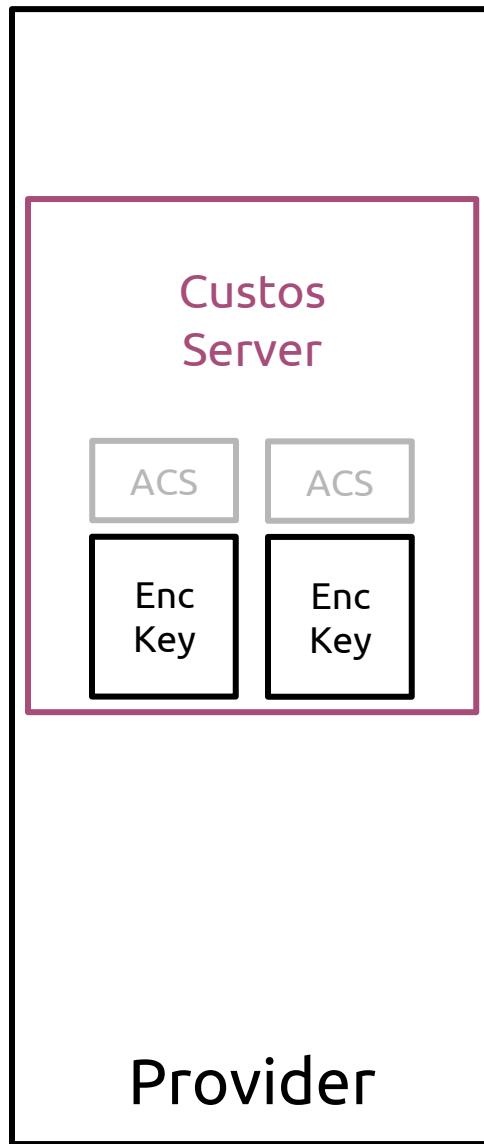
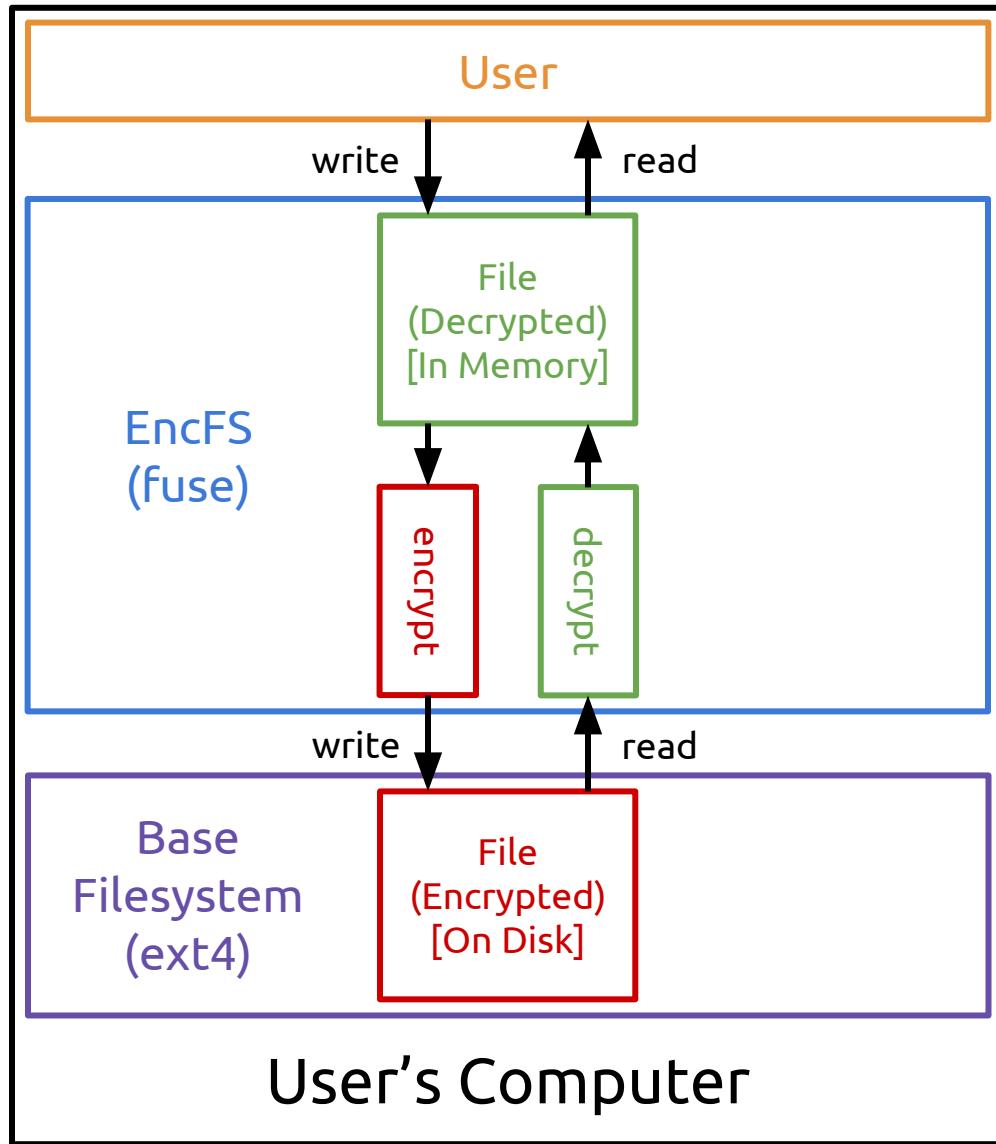
Compliance
Verification

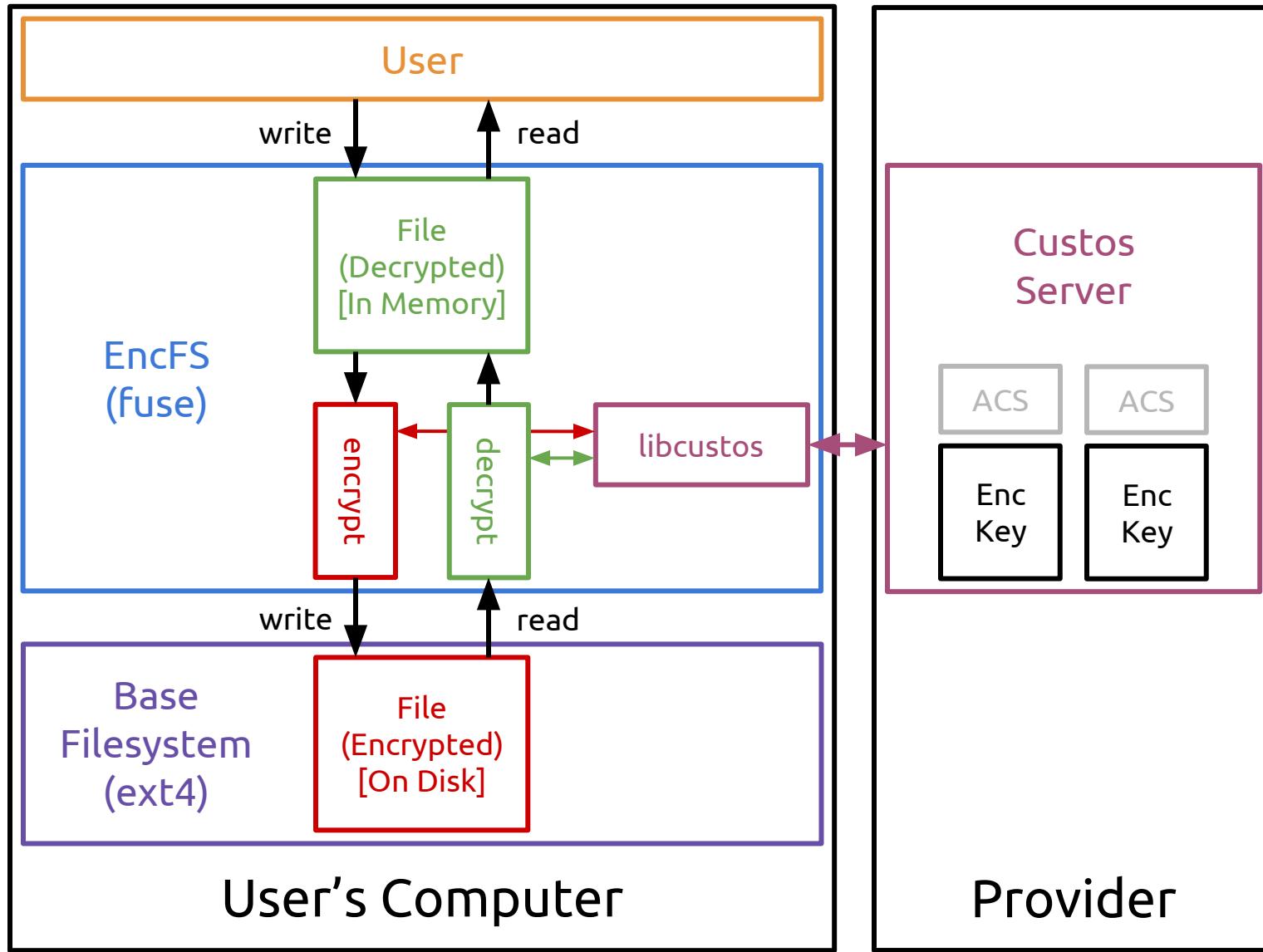
Custos Prototype

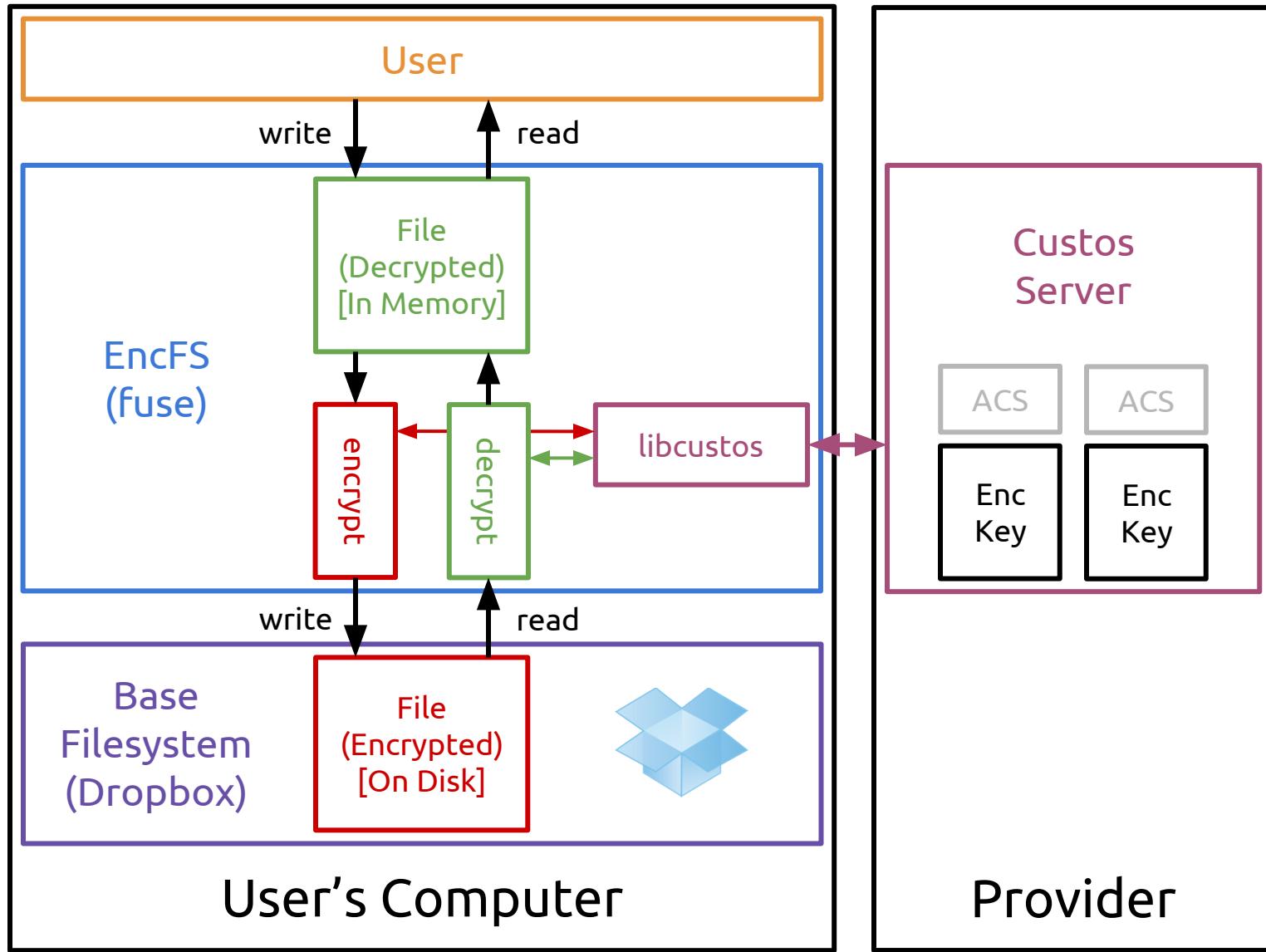
Custos Prototype

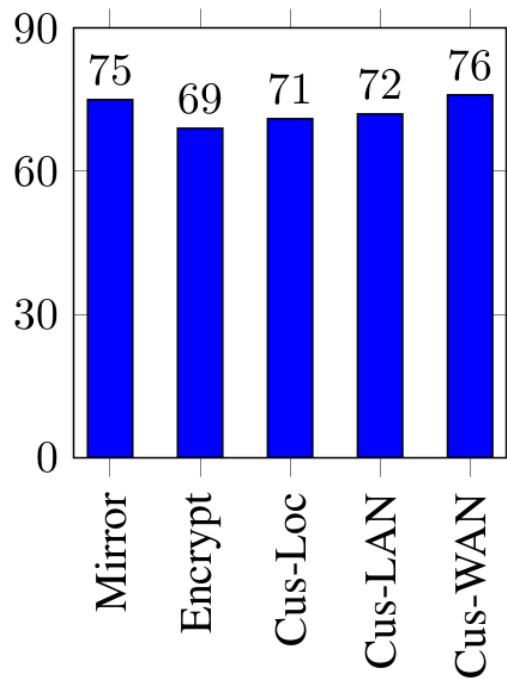
EncFS: Custos-Backed Encrypted File System



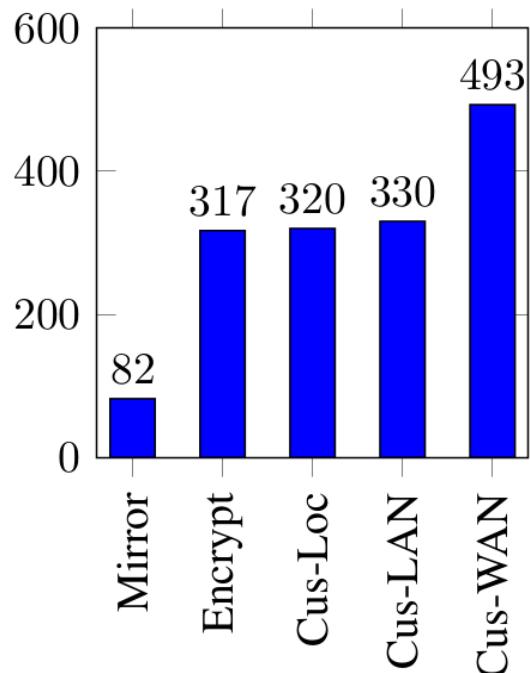




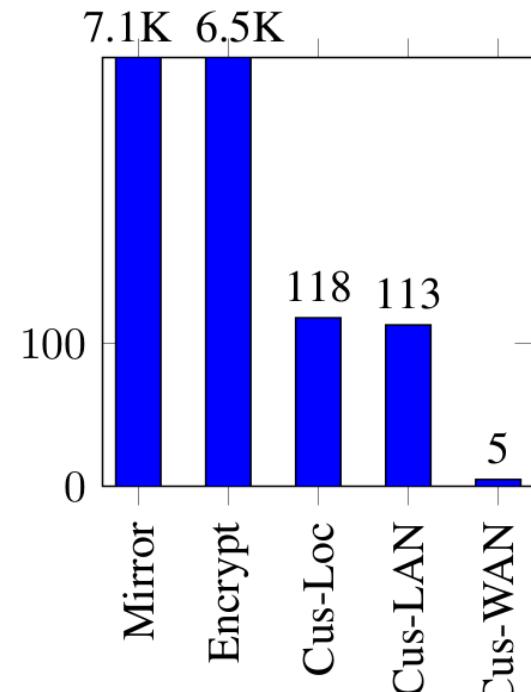




(a) `dd` Copy Throughput (MB/s)



(b) `ioping` Write Latency (ms)



(c) `bonnie++` Create IOPS

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

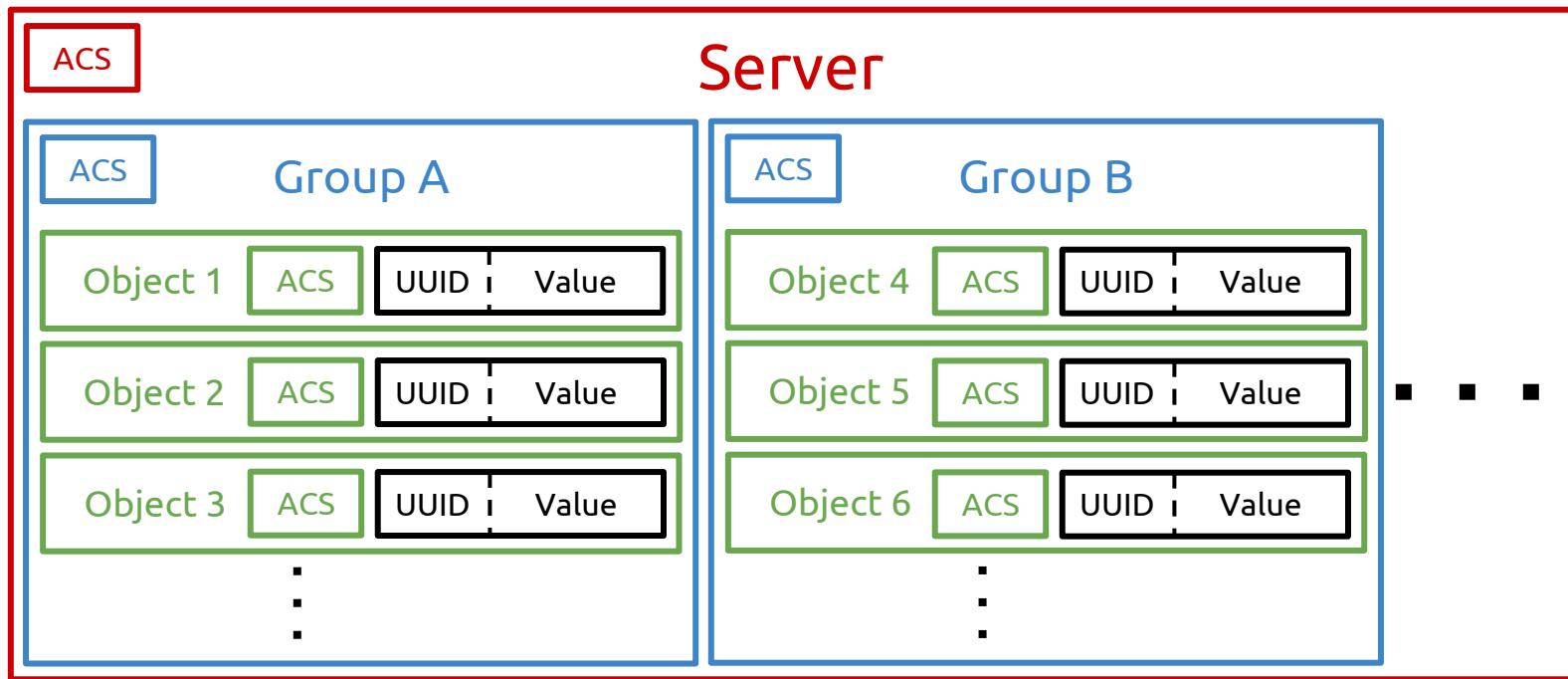
Ecosystem

Thank You

Questions?

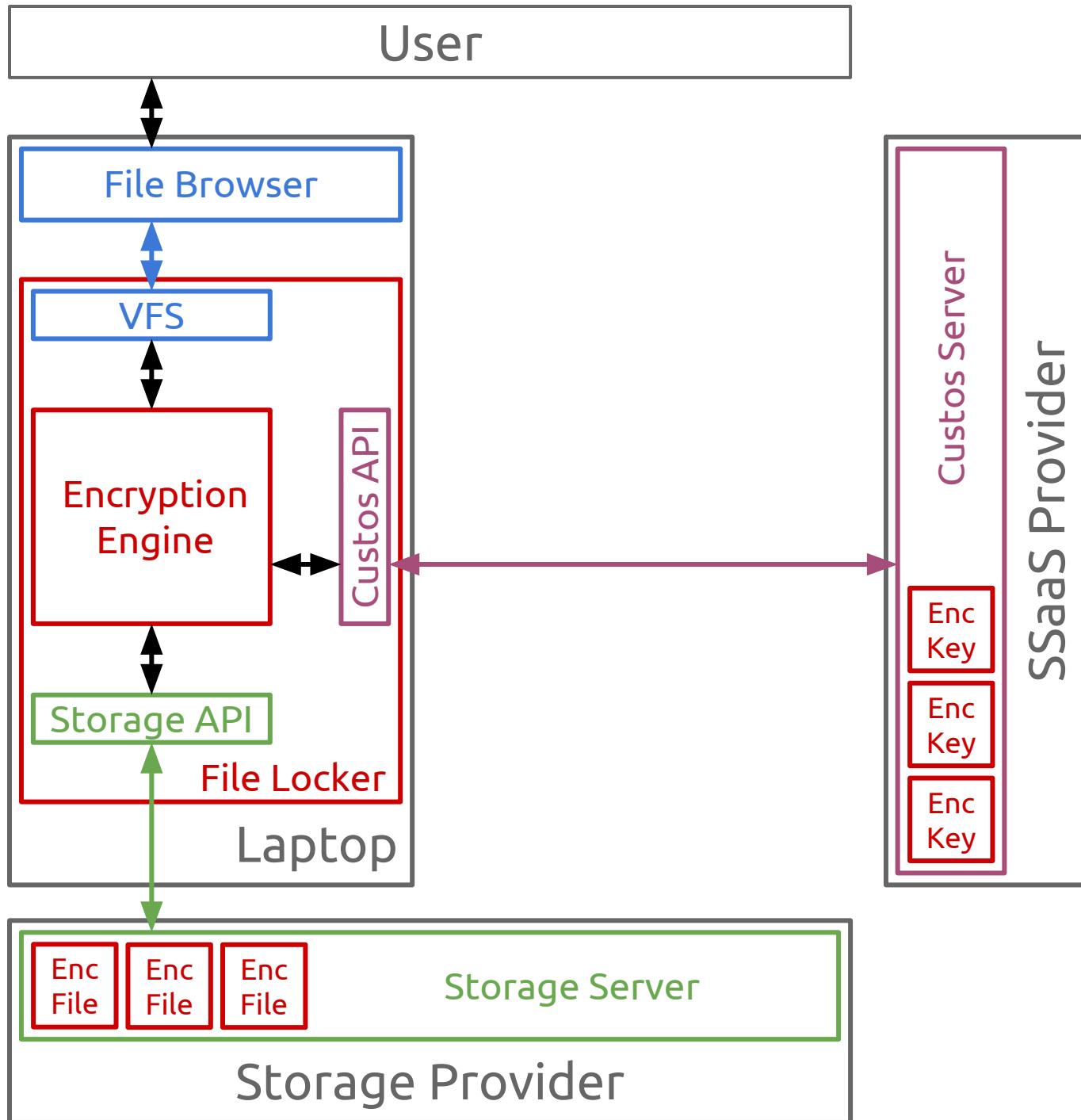
Extra Slides

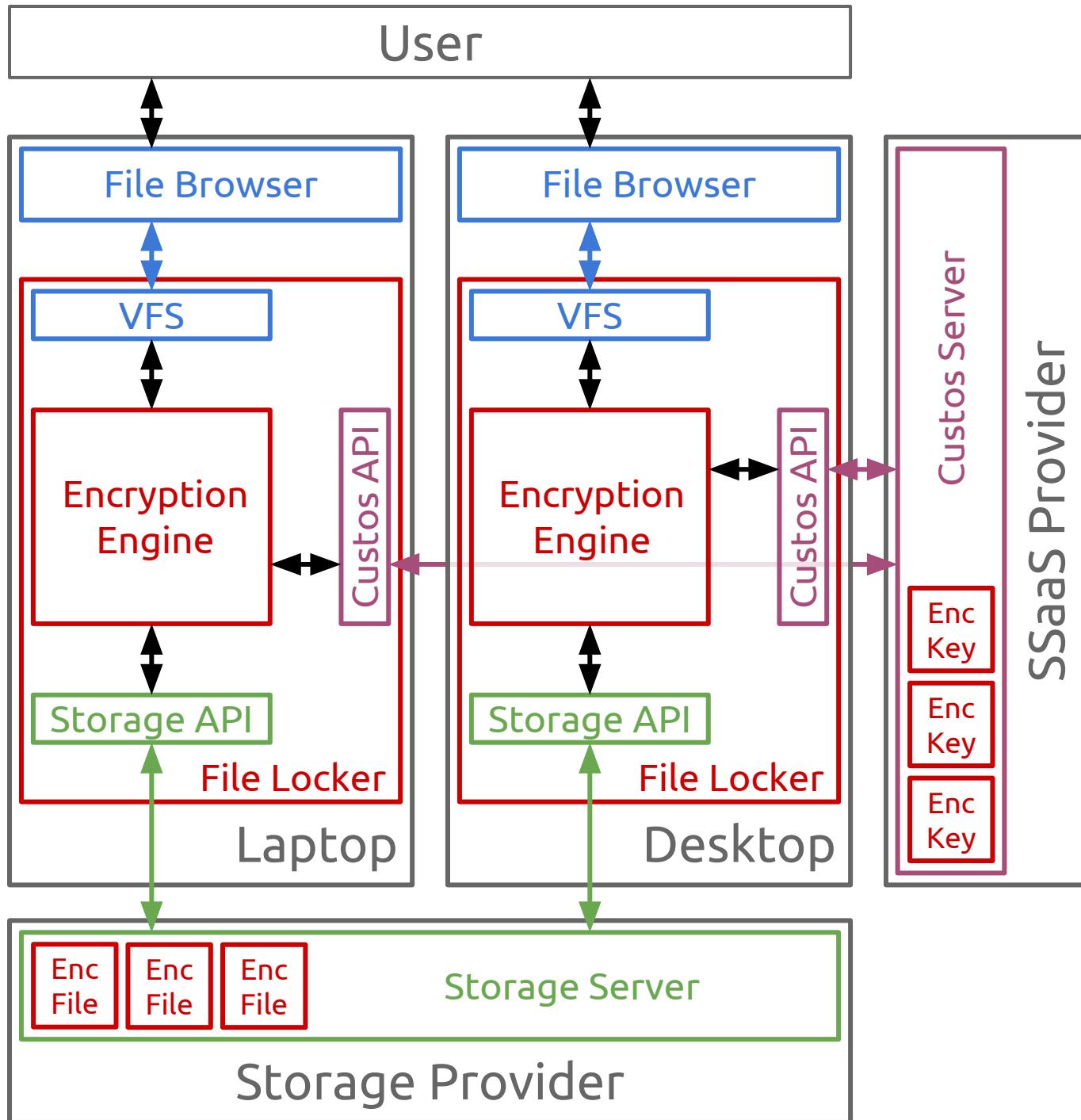
Custos Organizational Units



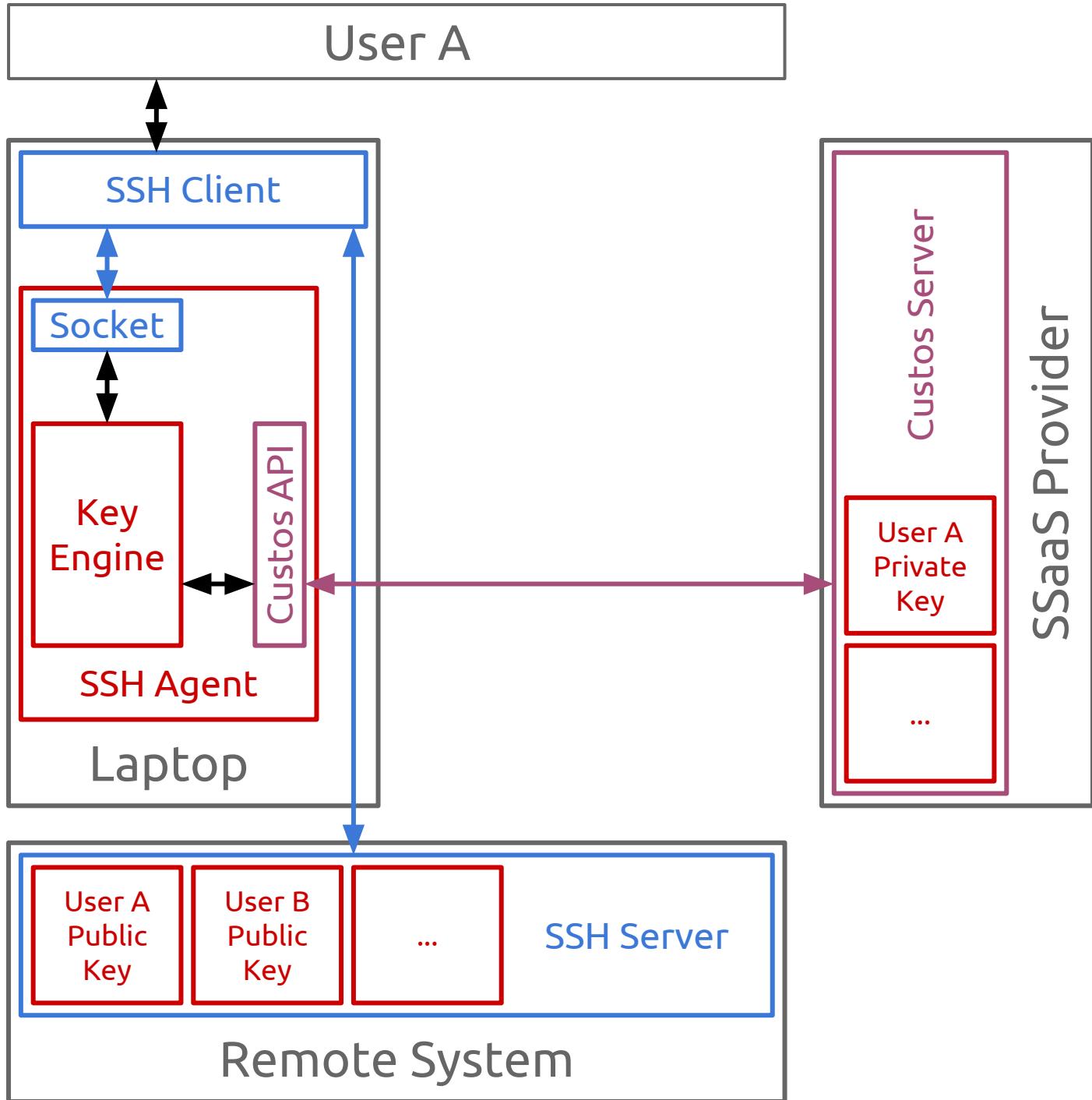
Example Applications

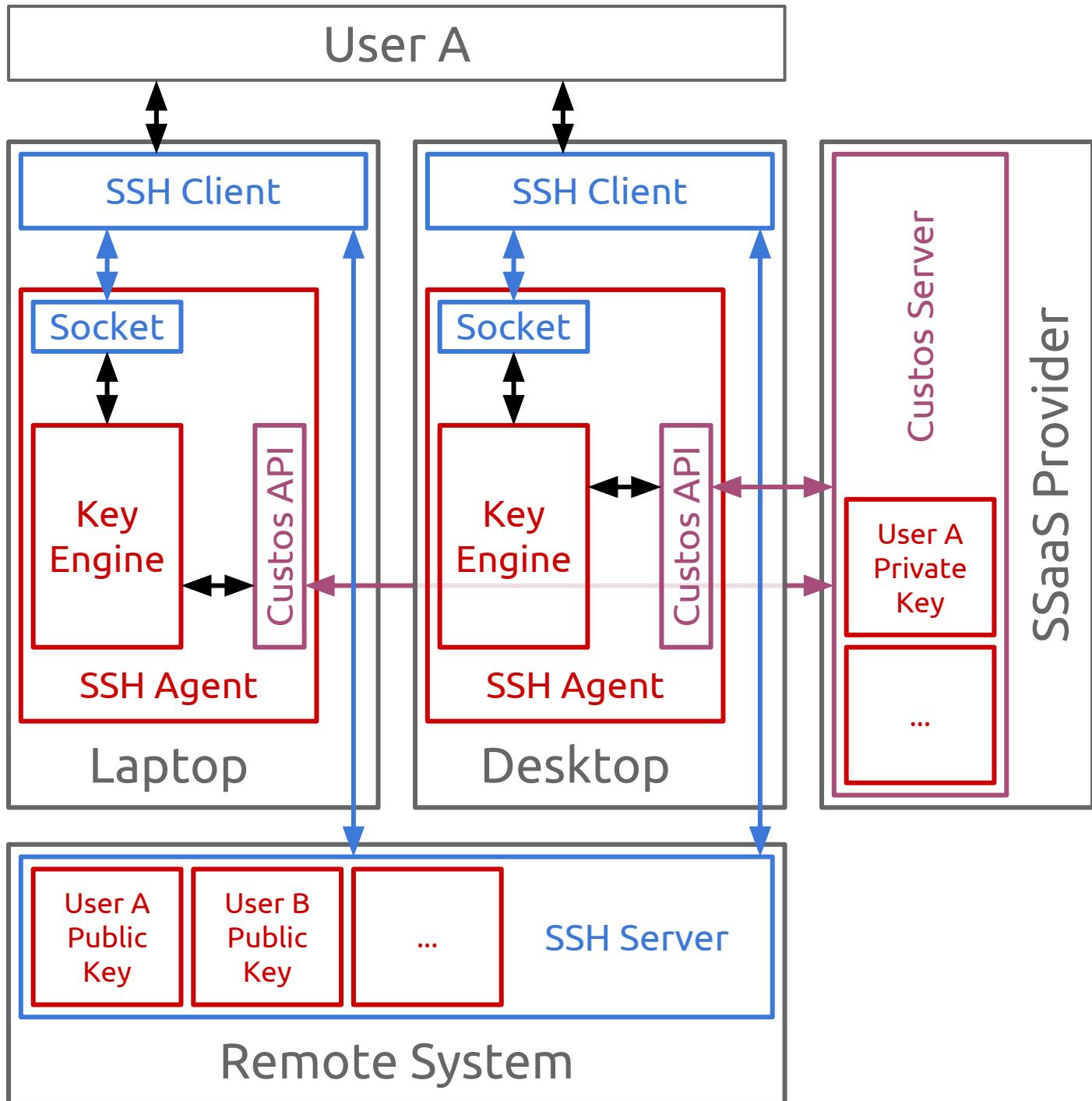
Client-Encrypted File Locker



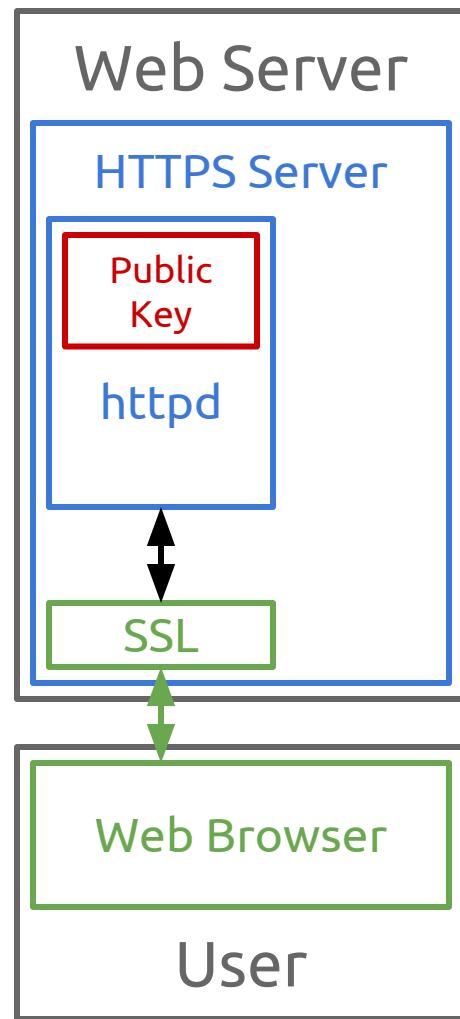


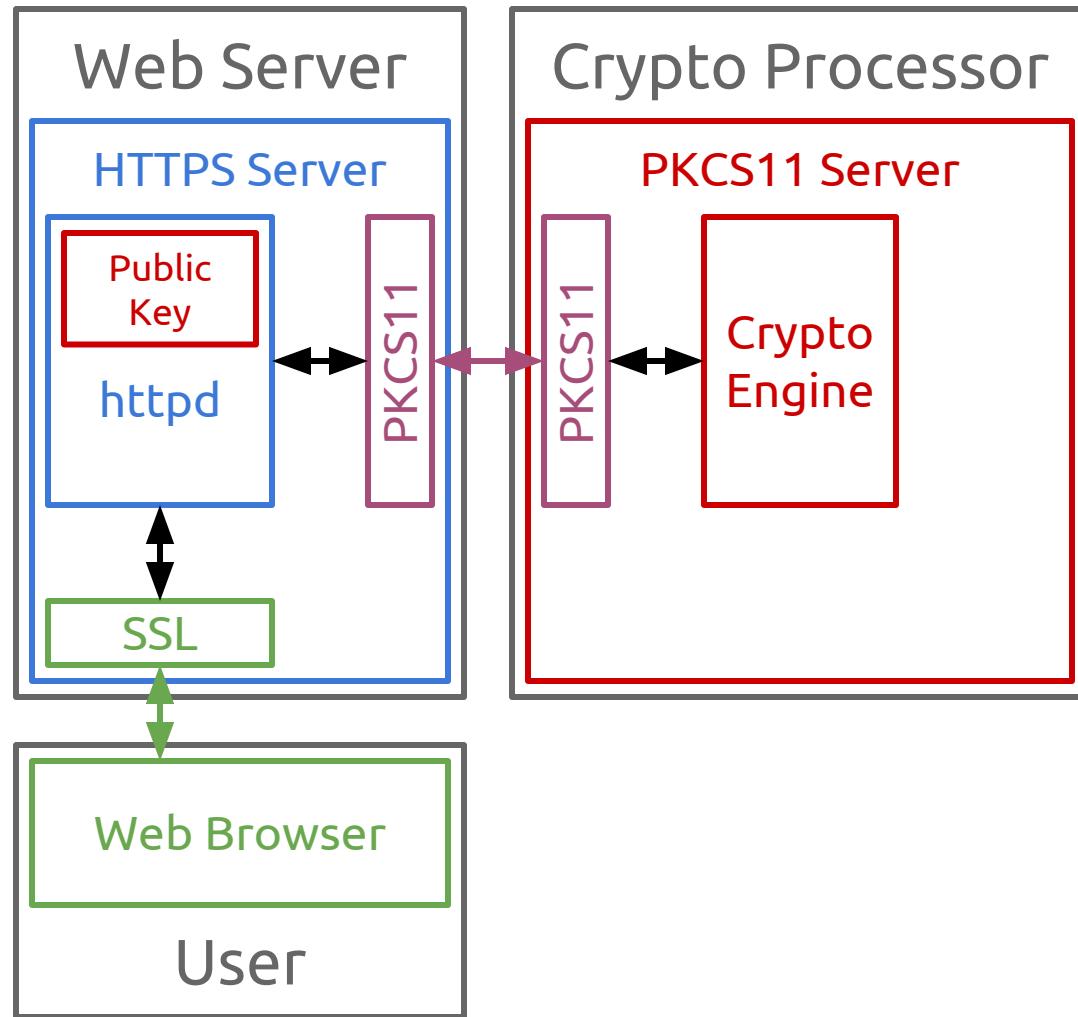
Multi-Device & Managed SSH Agent

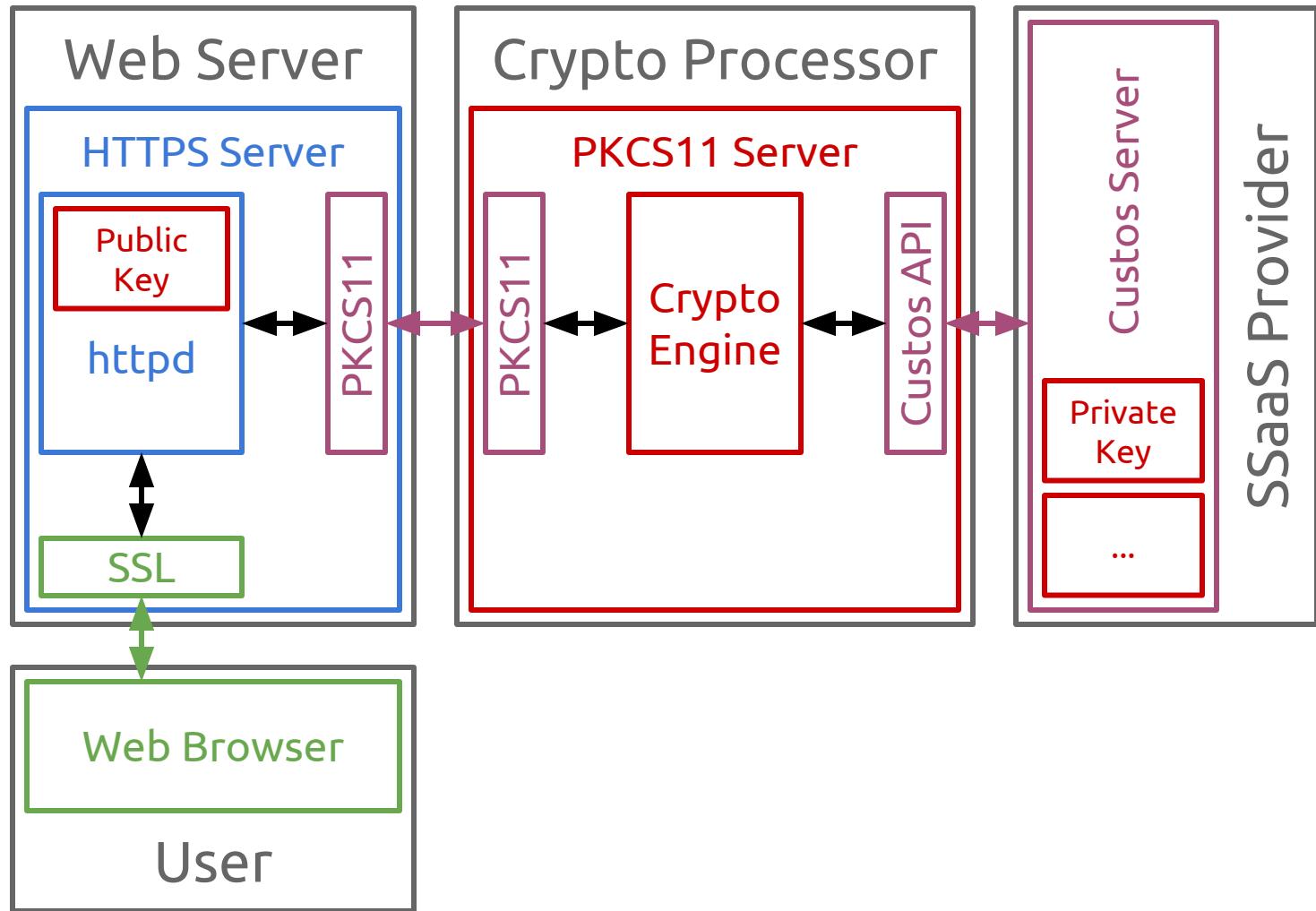




Dedicated Crypto Processor







Permissions

Permission	Rights
<code>srv_grp_create</code>	create groups on a Custos server
<code>srv_grp_list</code>	list groups on a Custos server
<code>srv_grp_override</code>	escalate to any group-level permission, overriding the per-group ACS
<code>srv_audit</code>	read all server-level audit information (i.e. group creation logging, group override logging, etc)
<code>srv_clean</code>	delete all server-level audit information (i.e. group creation logging, group override logging, etc)
<code>srv_acs_get</code>	view the server-level ACS controlling the permissions in this list
<code>srv_acs_set</code>	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
srv- grp	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
<code>srv_grp_create</code>	create groups on a Custos server
<code>srv_grp_list</code>	list groups on a Custos server
<code>srv- grp- obj- audit- clean- acs-</code>	Permission
<code>srv- grp- obj- audit- clean- acs-</code>	Rights
<code>grp_obj_create</code>	create a key:value objects within the given group
<code>grp_obj_list</code>	list key:value objects within the given group
<code>srv- grp- obj- audit- clean- acs-</code>	Permission
<code>srv- grp- obj- audit- clean- acs-</code>	Rights
<code>obj_delete</code>	delete the given key:value object within the given group
<code>obj_read</code>	read the given key:value object within the given group
<code>obj_update</code>	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)
<code>obj_audit</code>	read all object-level audit information (i.e. object read logging, object update logging, etc)
<code>obj_clean</code>	delete all object-level audit information (i.e. object read logging, object update logging, etc)
<code>obj_acs_get</code>	view the object-level ACS controlling the permissions in this list
<code>obj_acs_set</code>	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)
```

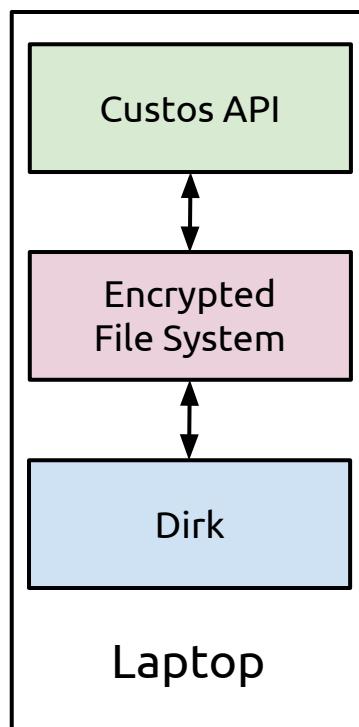
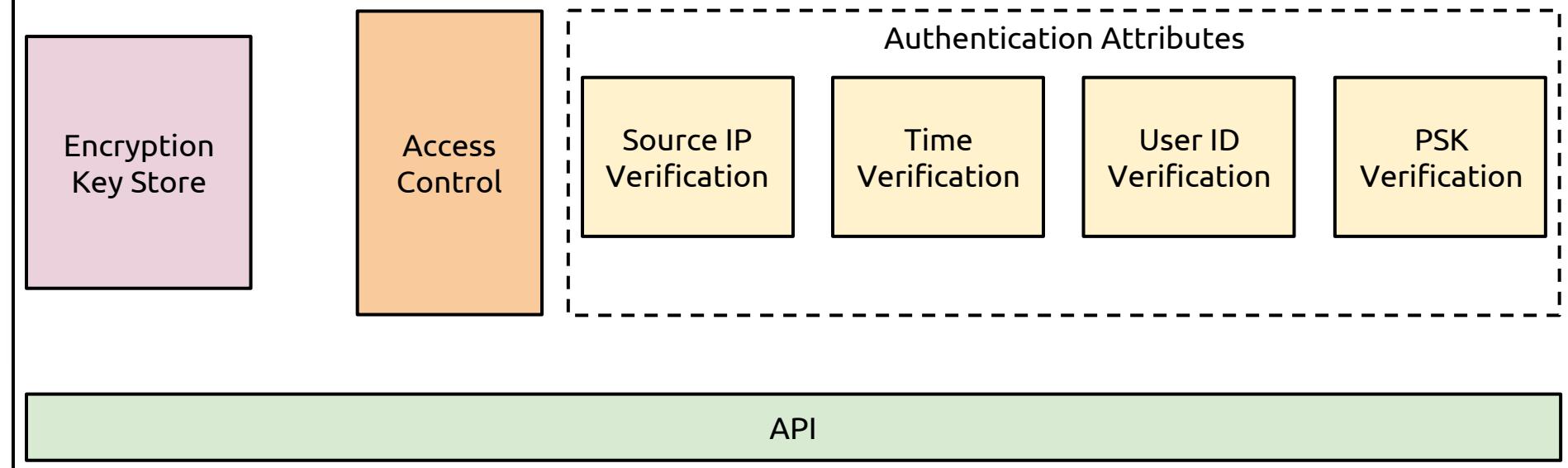
```
(username = 'John')
|
(password = 'Swordfish')
```

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



Request:

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

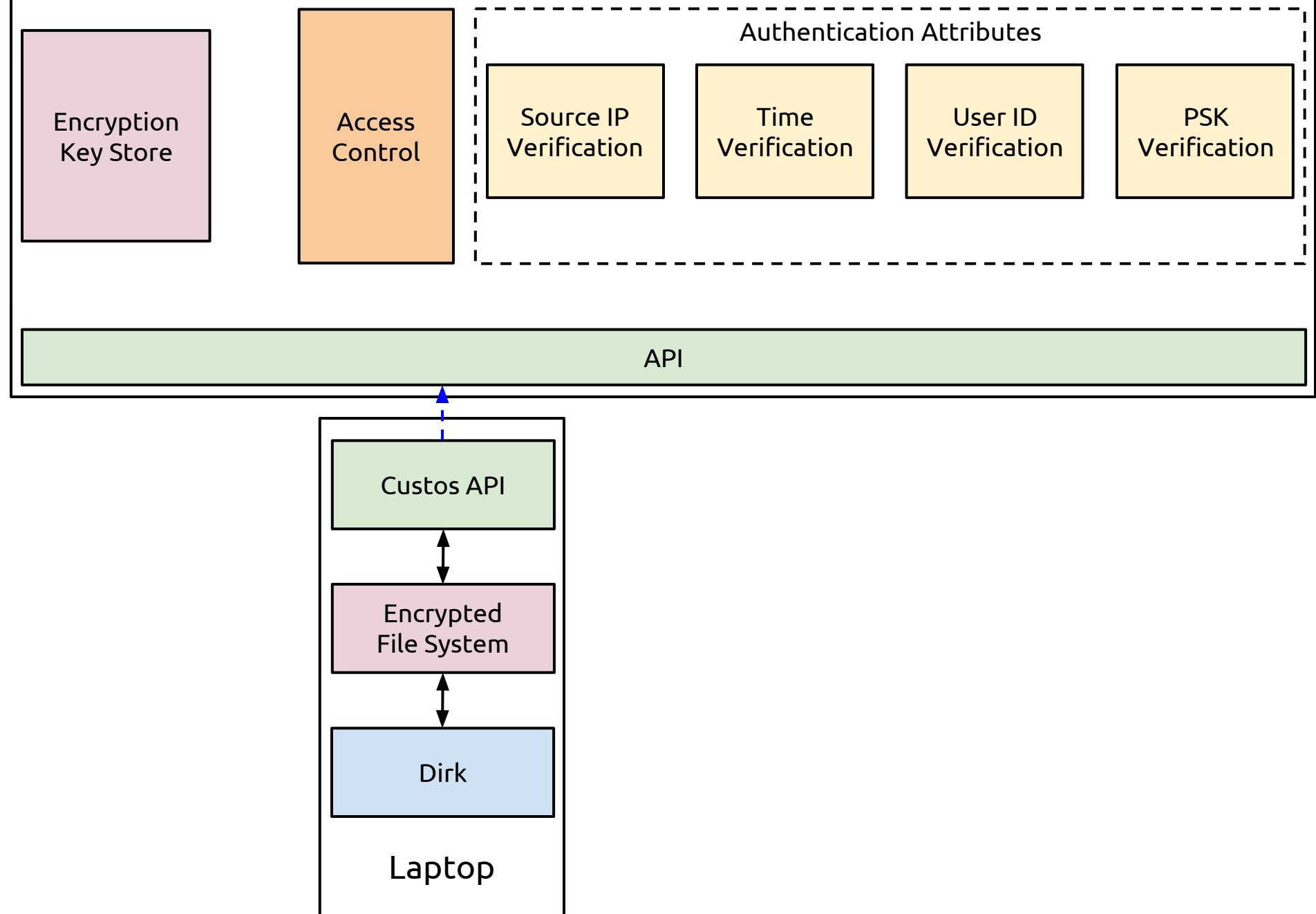
Authentication Attributes:

user_id = Dirk

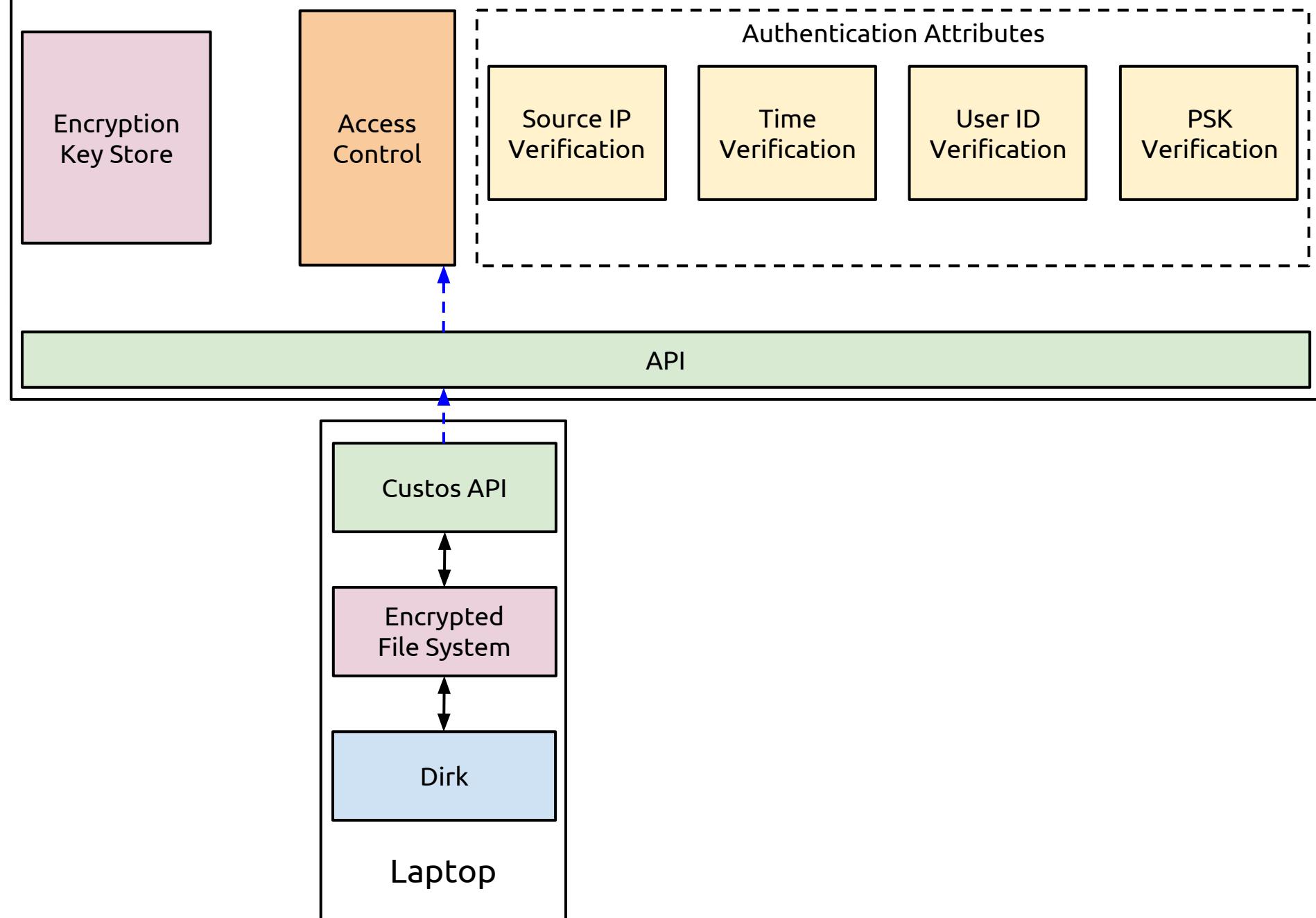
(ip_src = '1.2.3.4')

(time_utc = '1133')

Custos Server

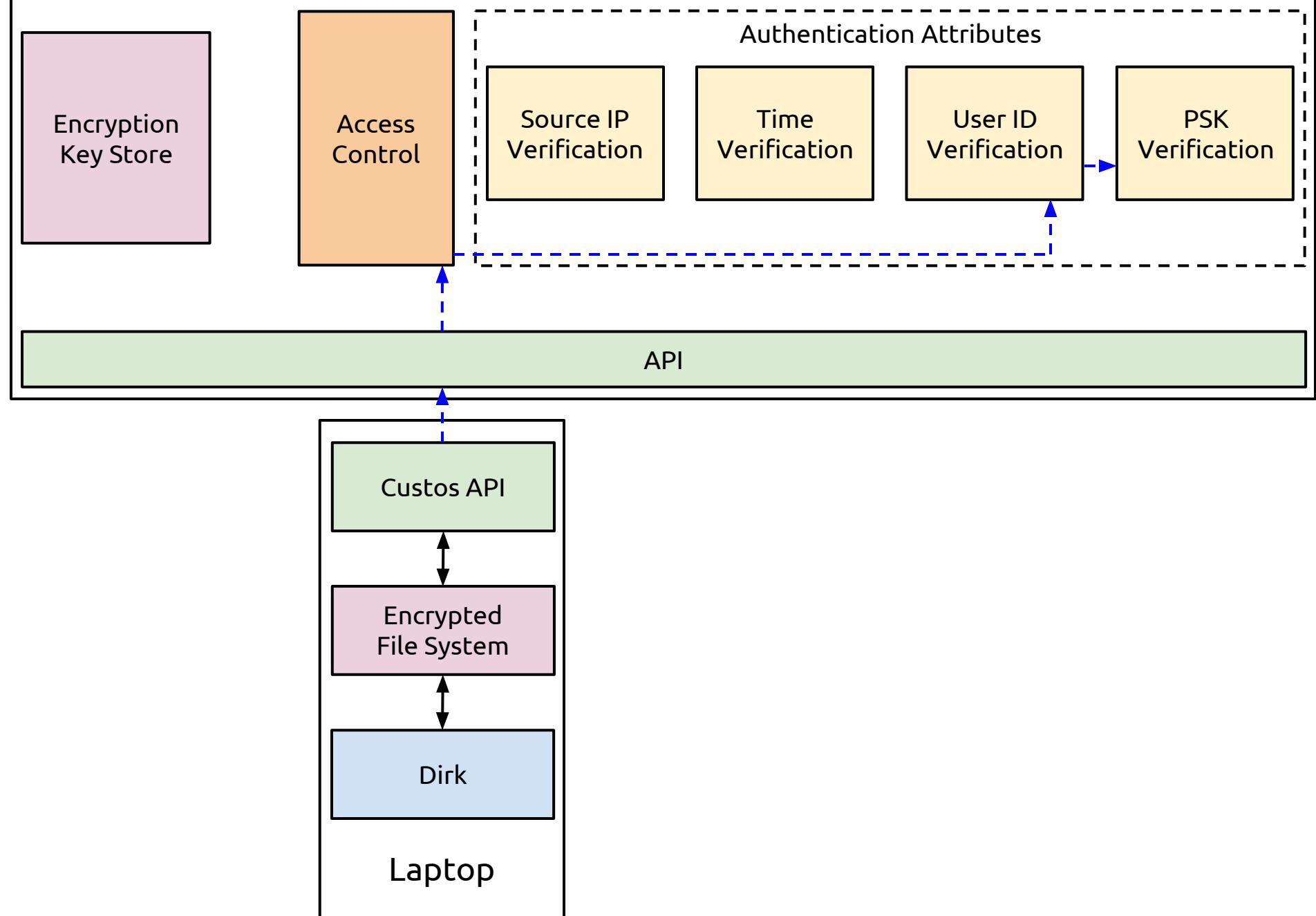


Custos Server



```
{  
    obj_read:  
        [  
            [ (ip\src = '1.2.3.4'),  
              (time\utc = '1300 +/- 5') ],  
            [ (user\id = 'Dirk'),  
              (psk = 'ImaHakzor') ]  
            ...  
        ]  
        ...  
}
```

Custos Server



Request:

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

Authentication Attributes:

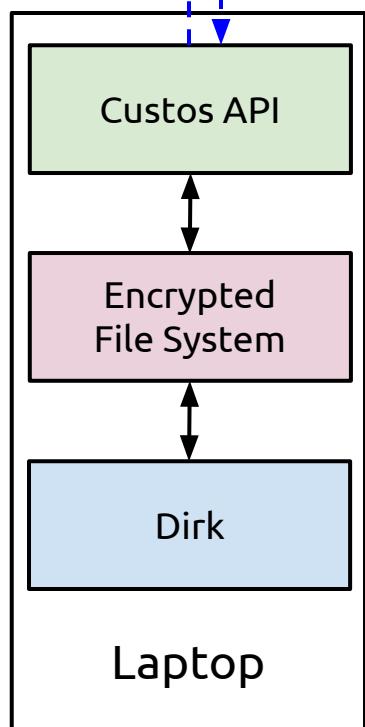
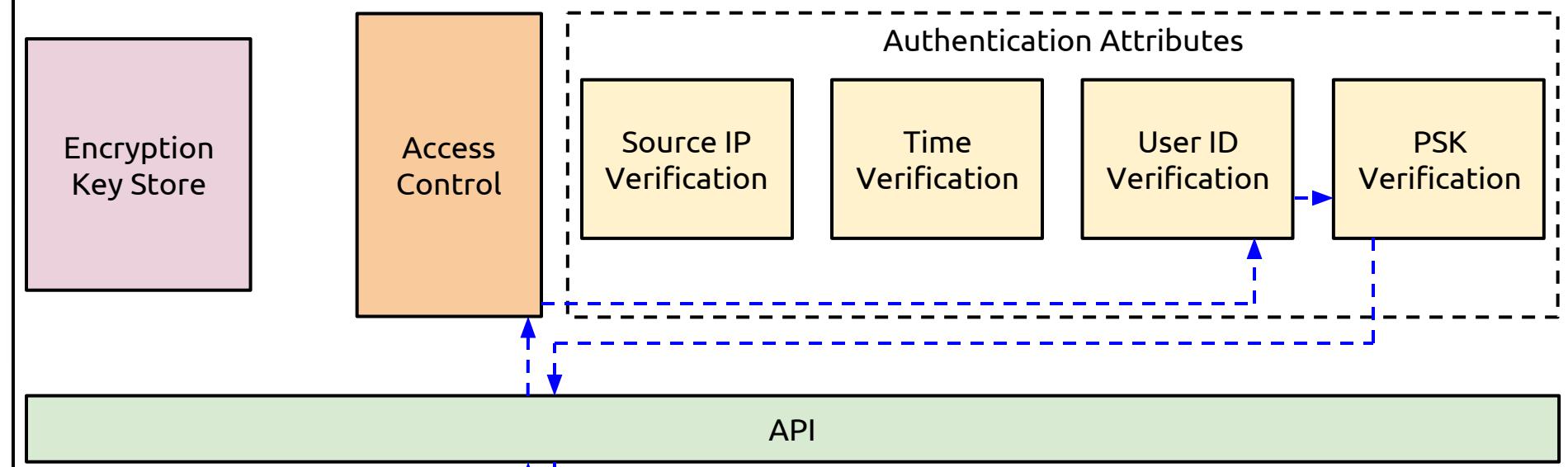
user_id = Dirk

(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



Request:

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

Authentication Attributes:

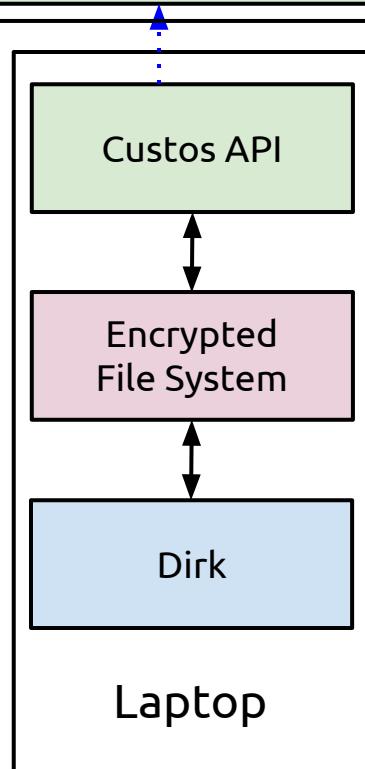
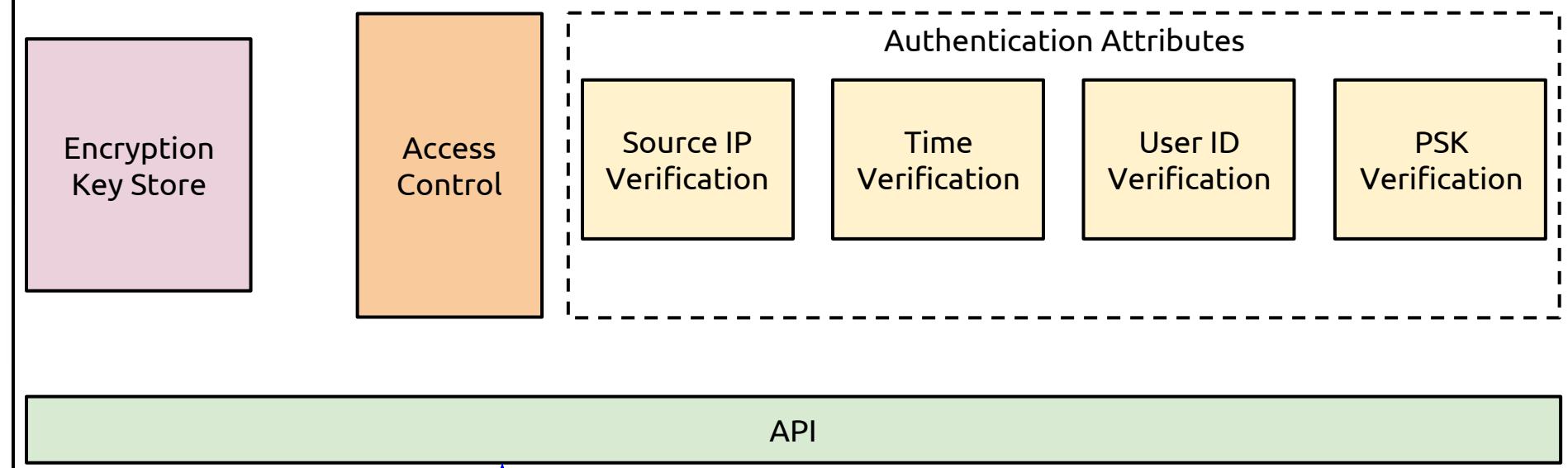
user_id = ‘Dirk’

psk = ‘ImaHackzor’

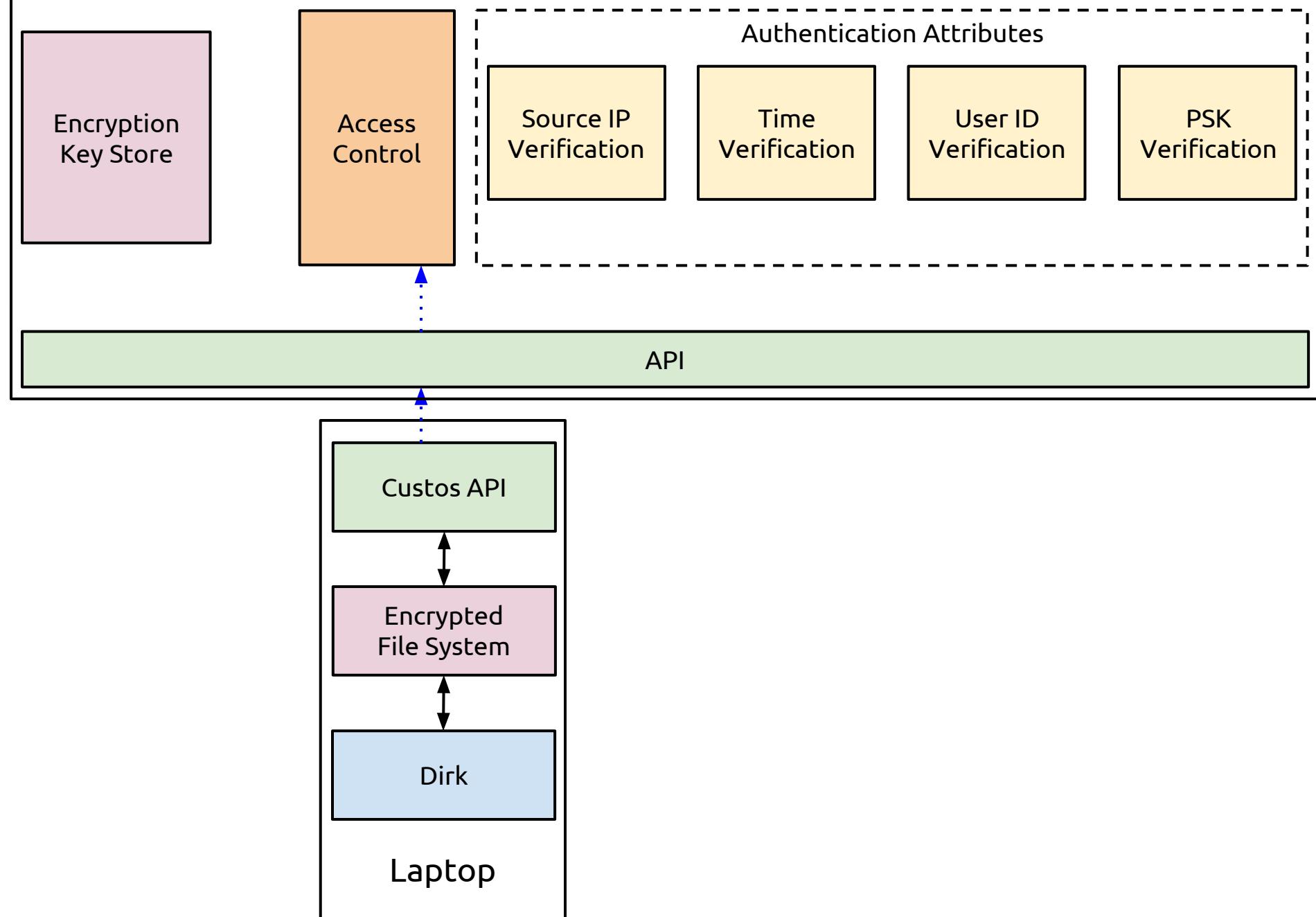
(ip_src = ‘1.2.3.4’)

(time_utc = ‘1133’)

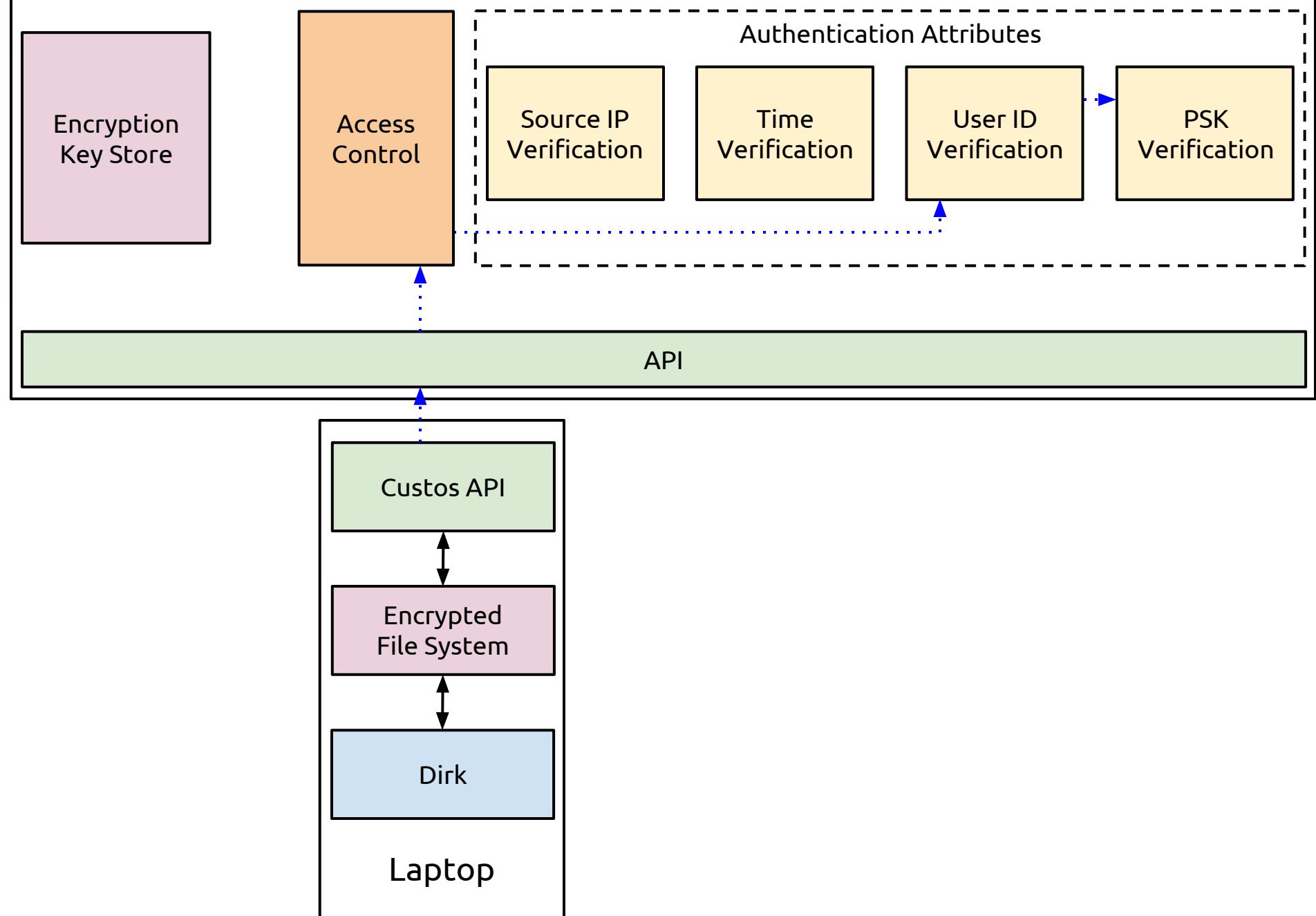
Custos Server



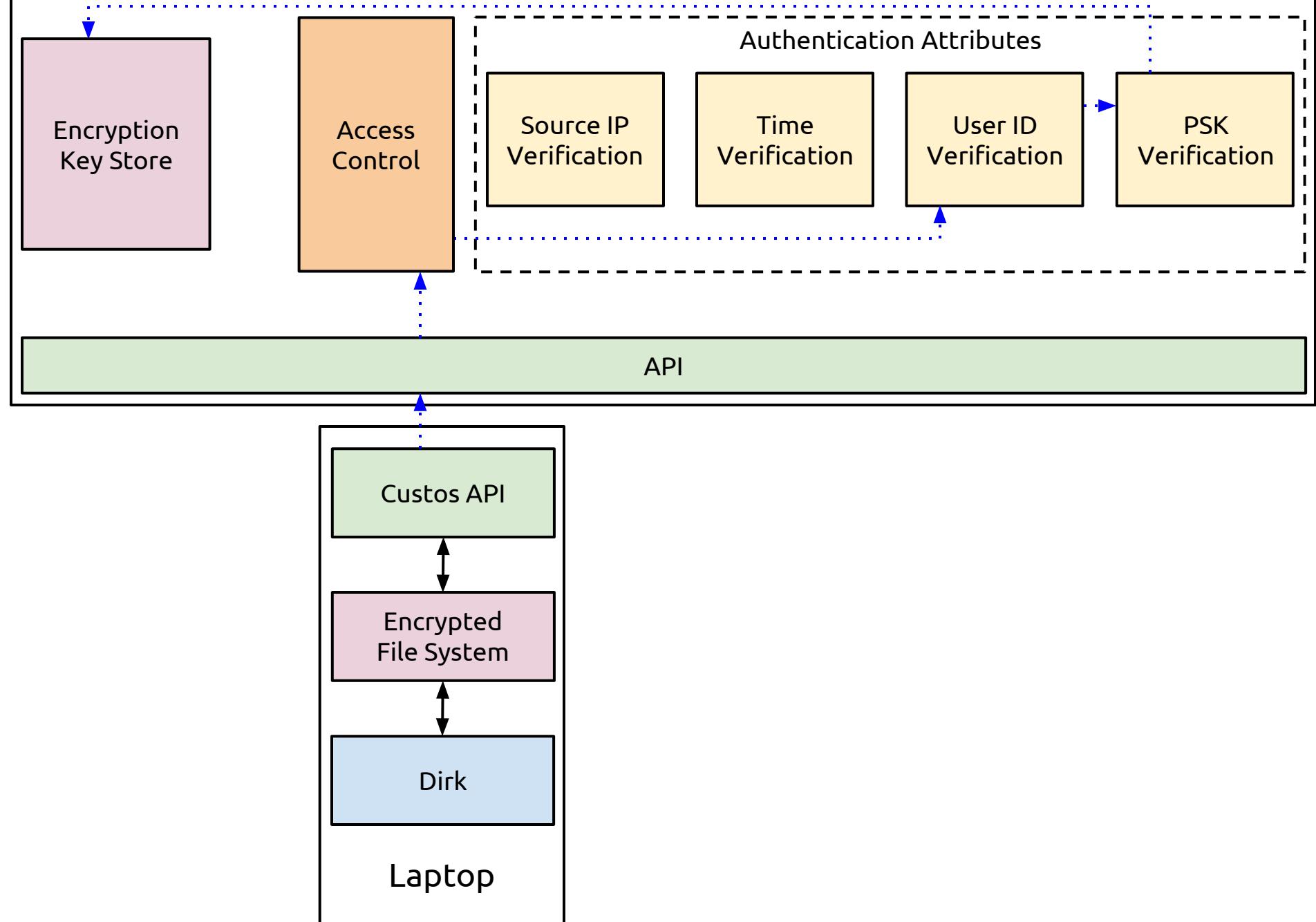
Custos Server



Custos Server



Custos Server



Custos Server

