Custos
A Flexibly Secure Key-Value Storage Platform

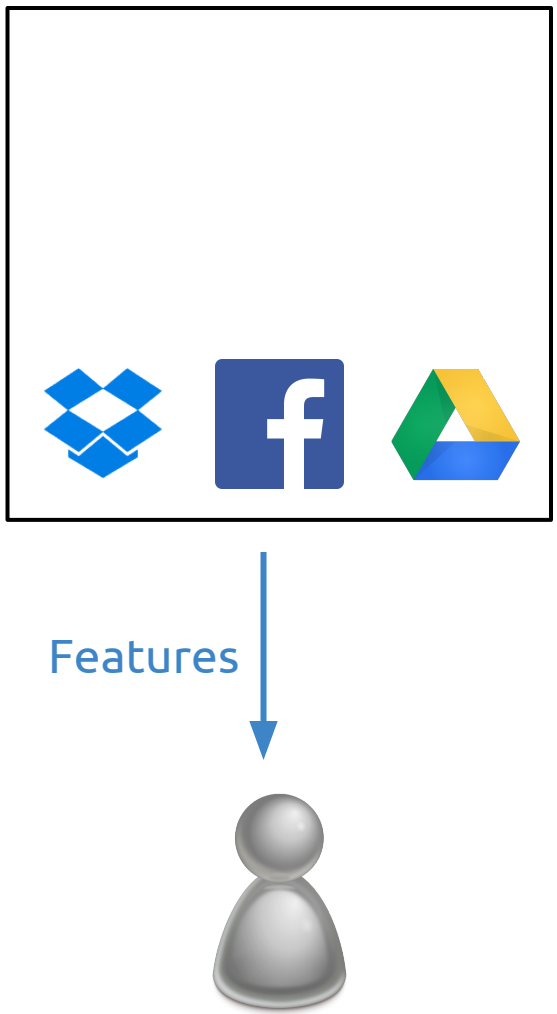
Andy Sayler
www.andysayler.com
University of Colorado, Boulder

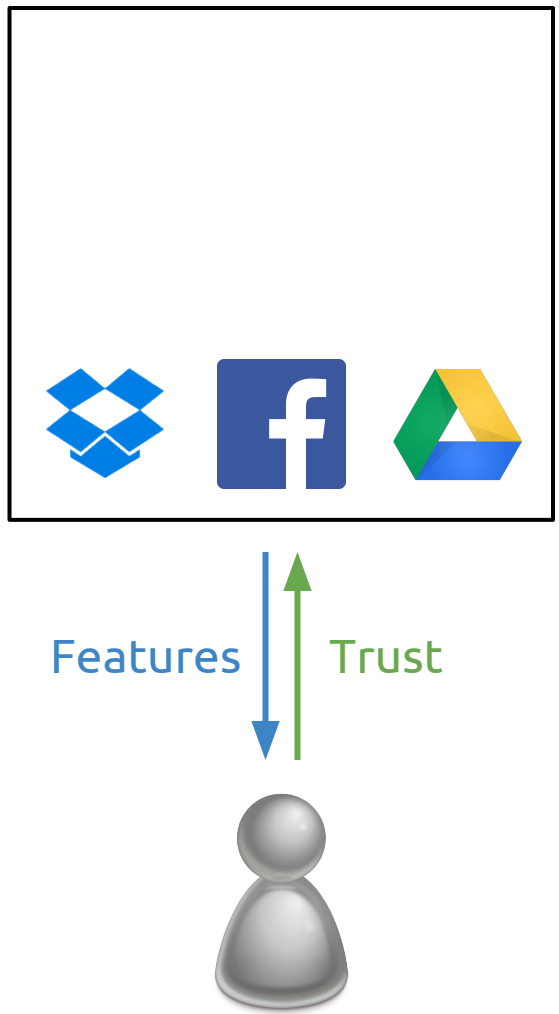
Masters of Science
Computer Science

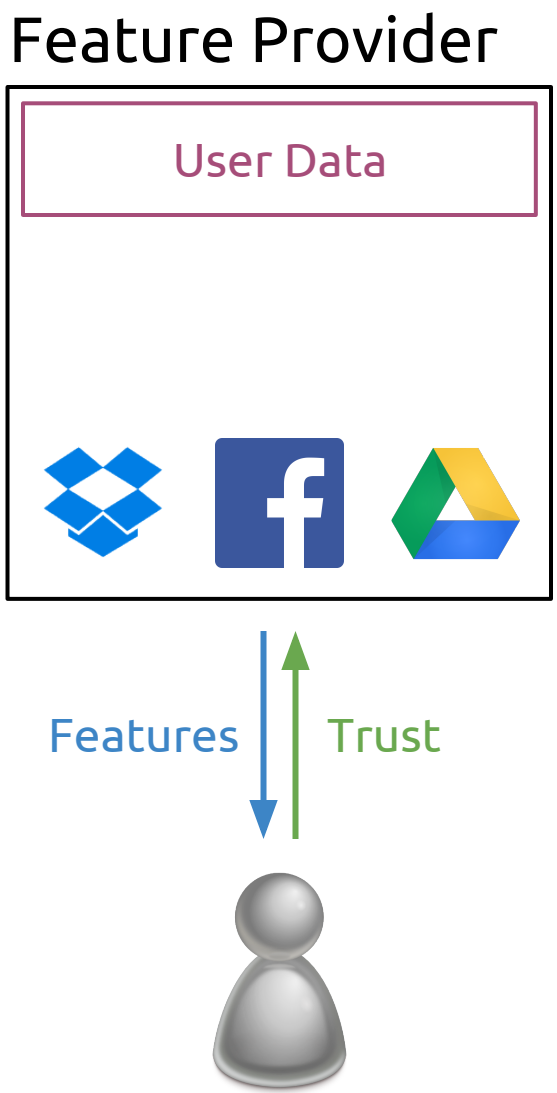
Trust

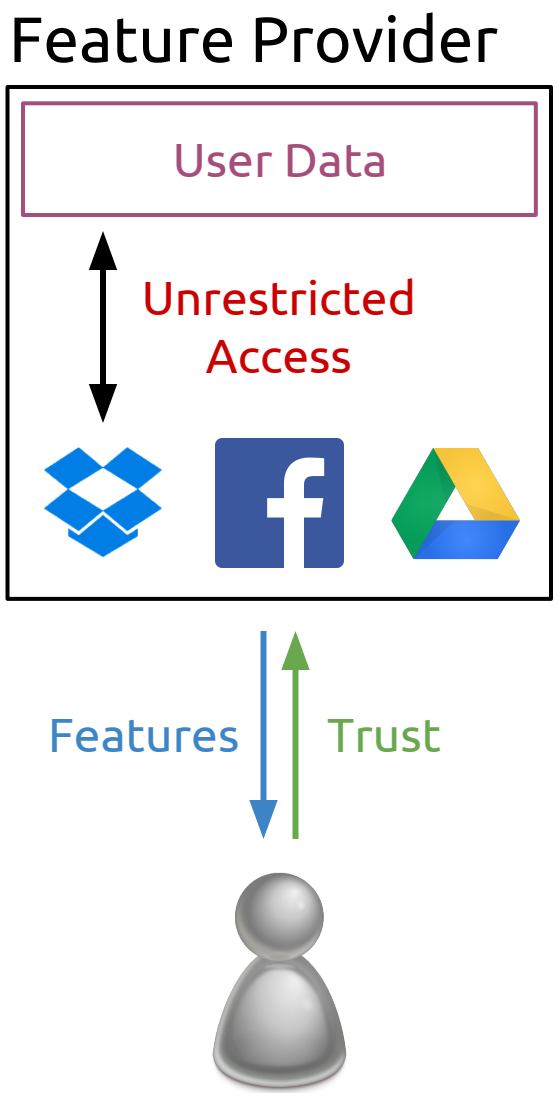
Who do we trust
with our data?

Today…


Feature Provider
Features


Feature Provider
Features
Trust


Feature Provider
User Data
Features
Trust


Feature Provider
User Data
Unrestricted Access
Features
Trust

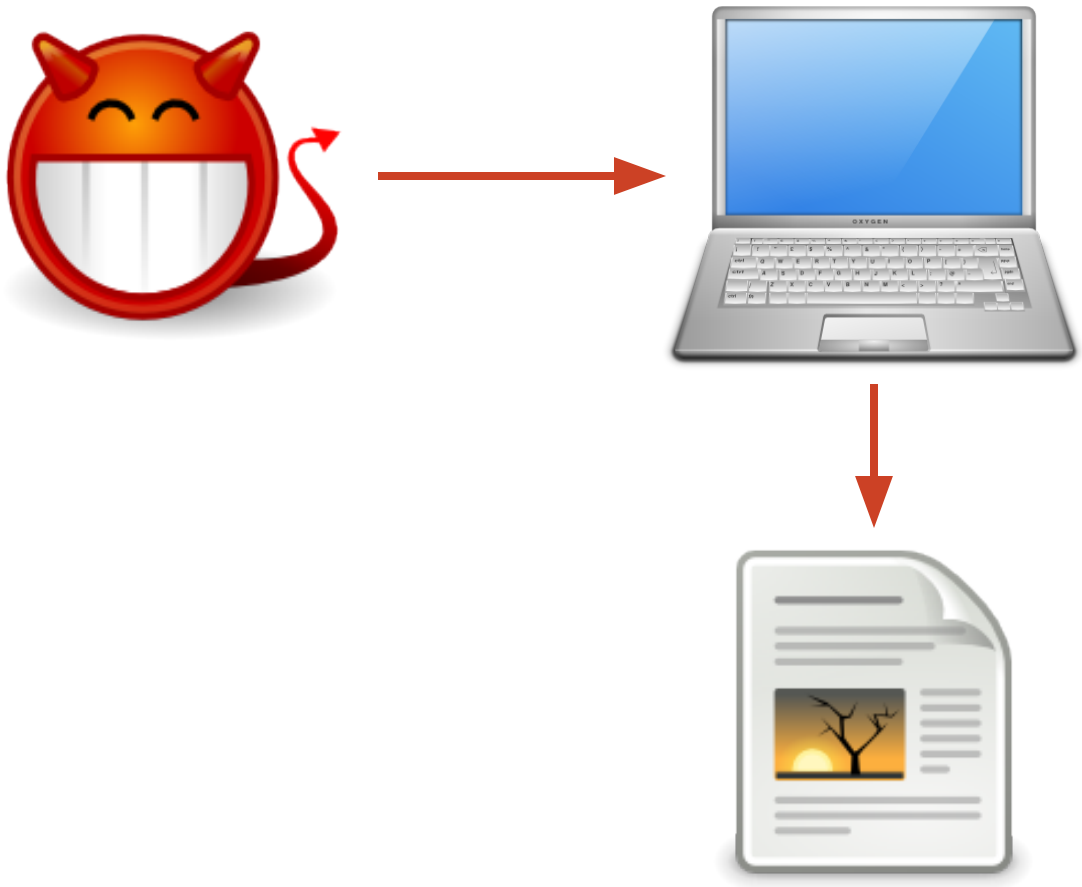
Conflicts of Interest

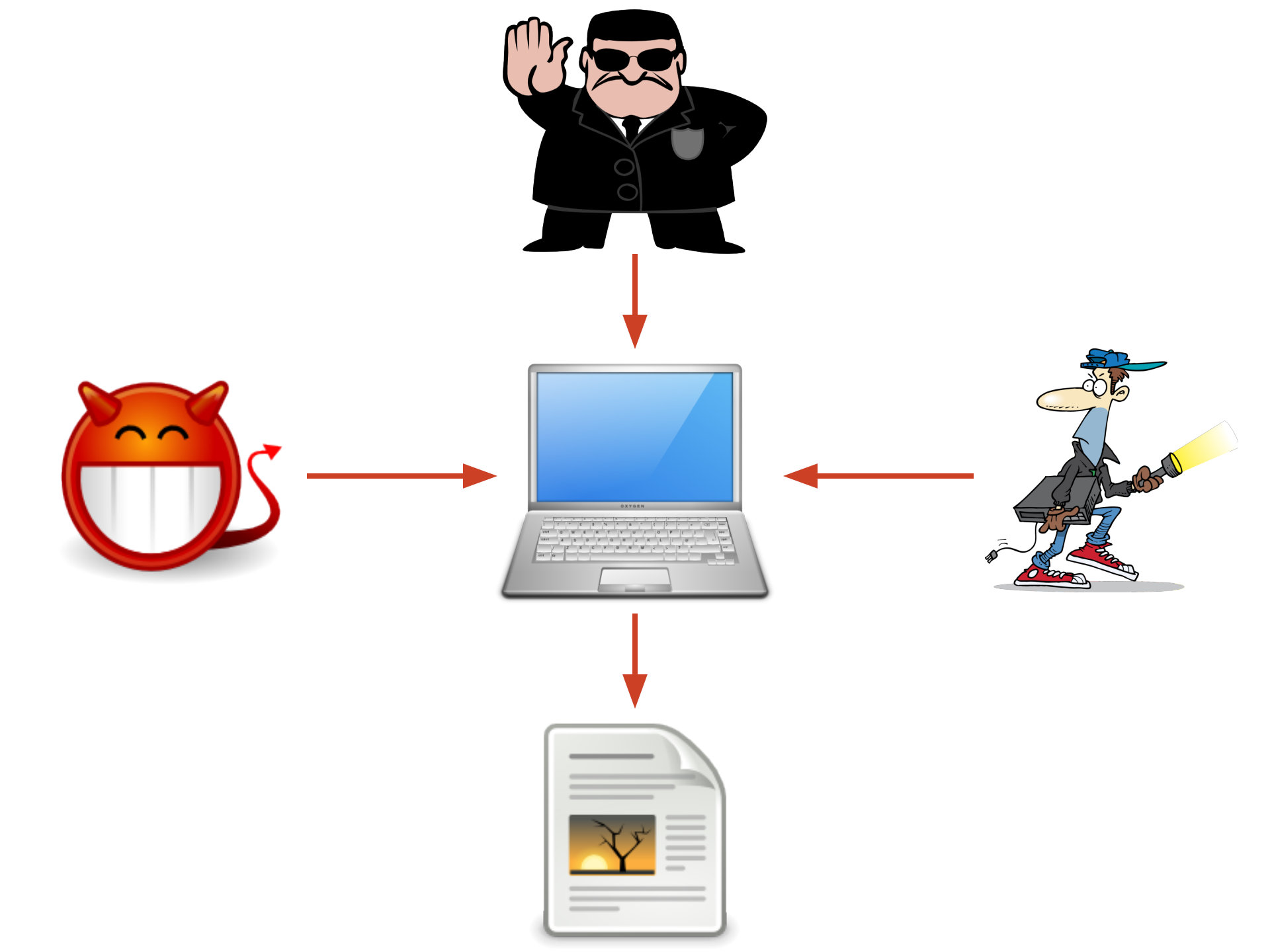
Lack of Control

Absence of Oversight

So you don’t
use cloud services...

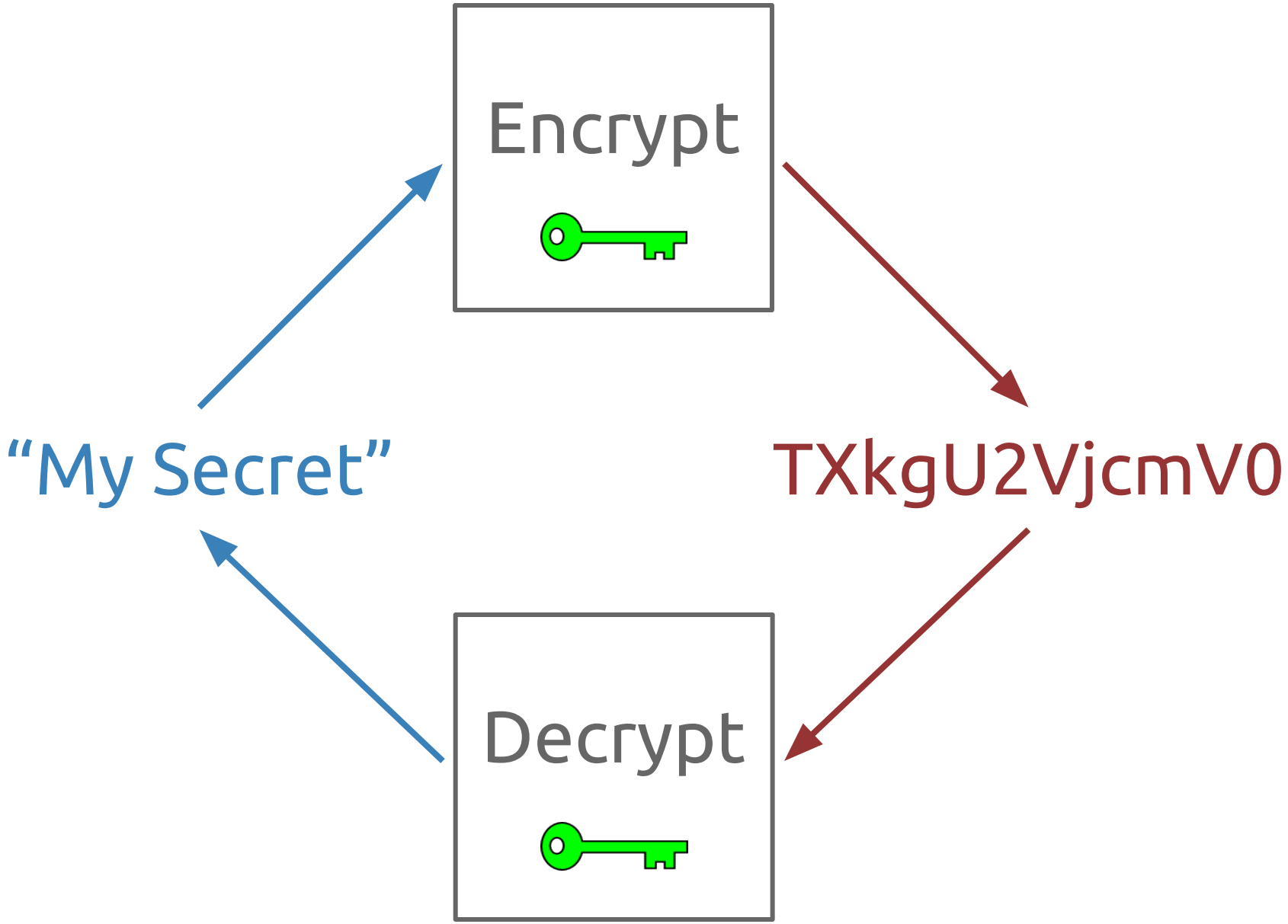

OXYGEN



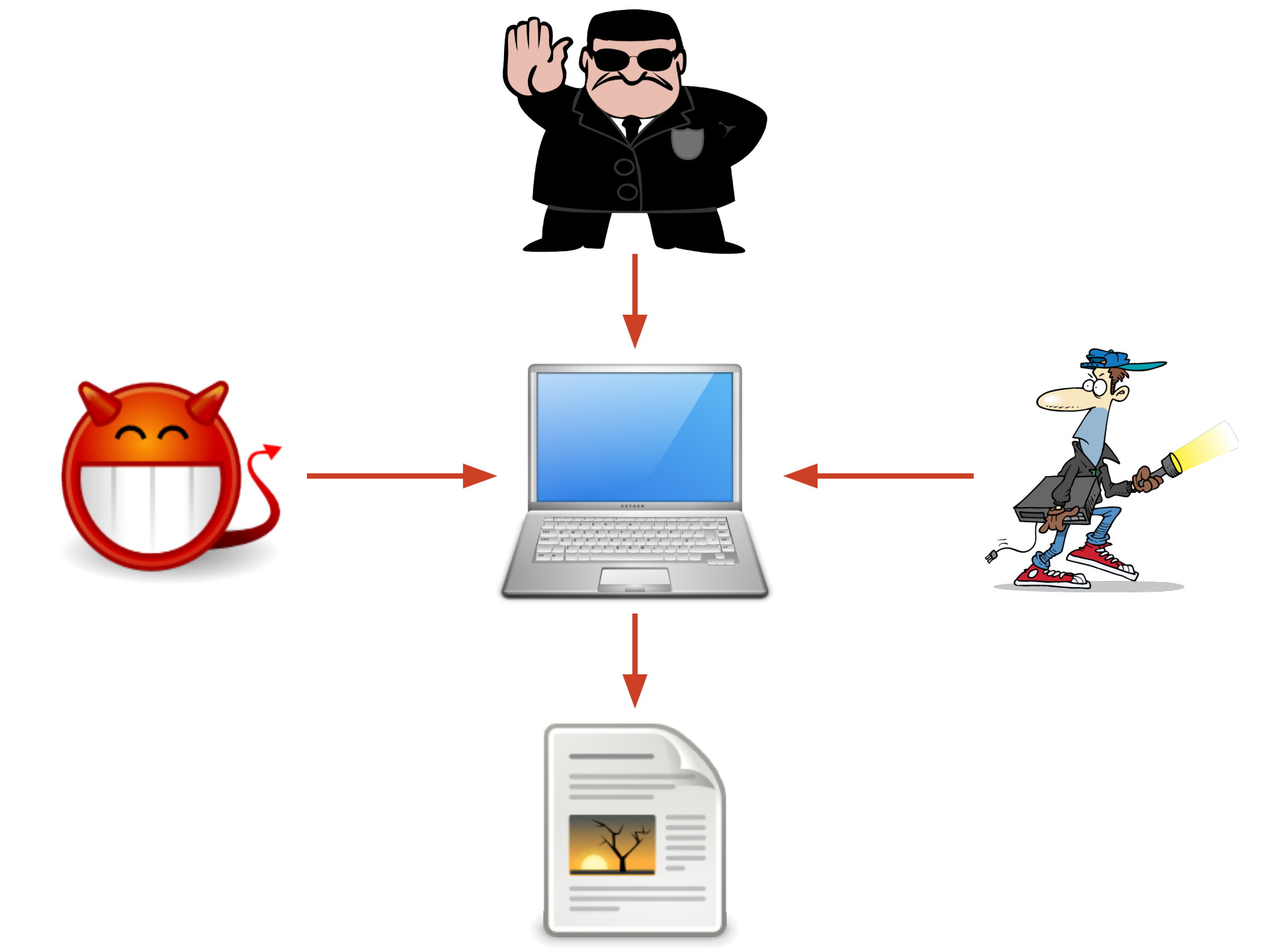


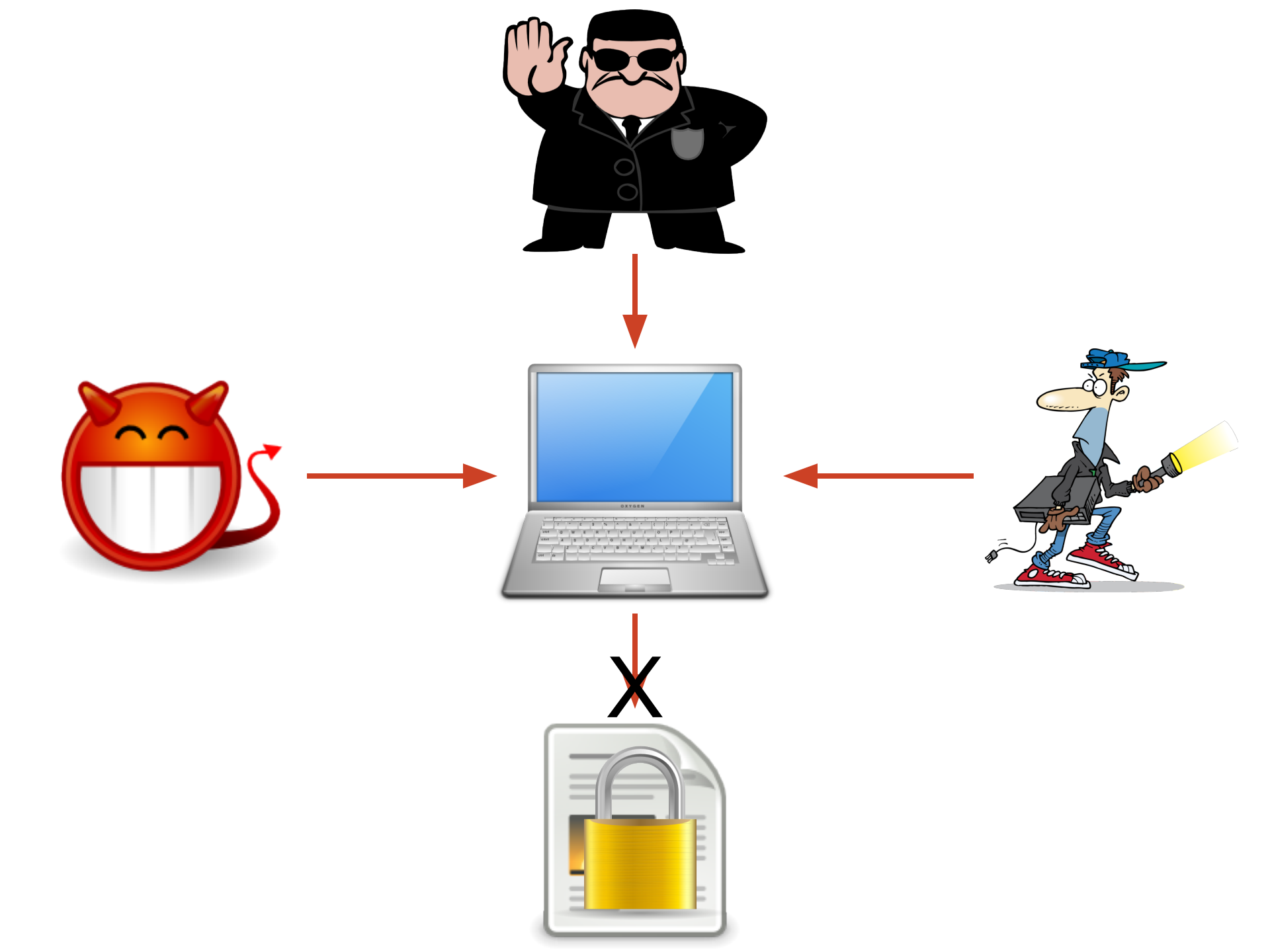
How can we control and protect our data?

Encryption

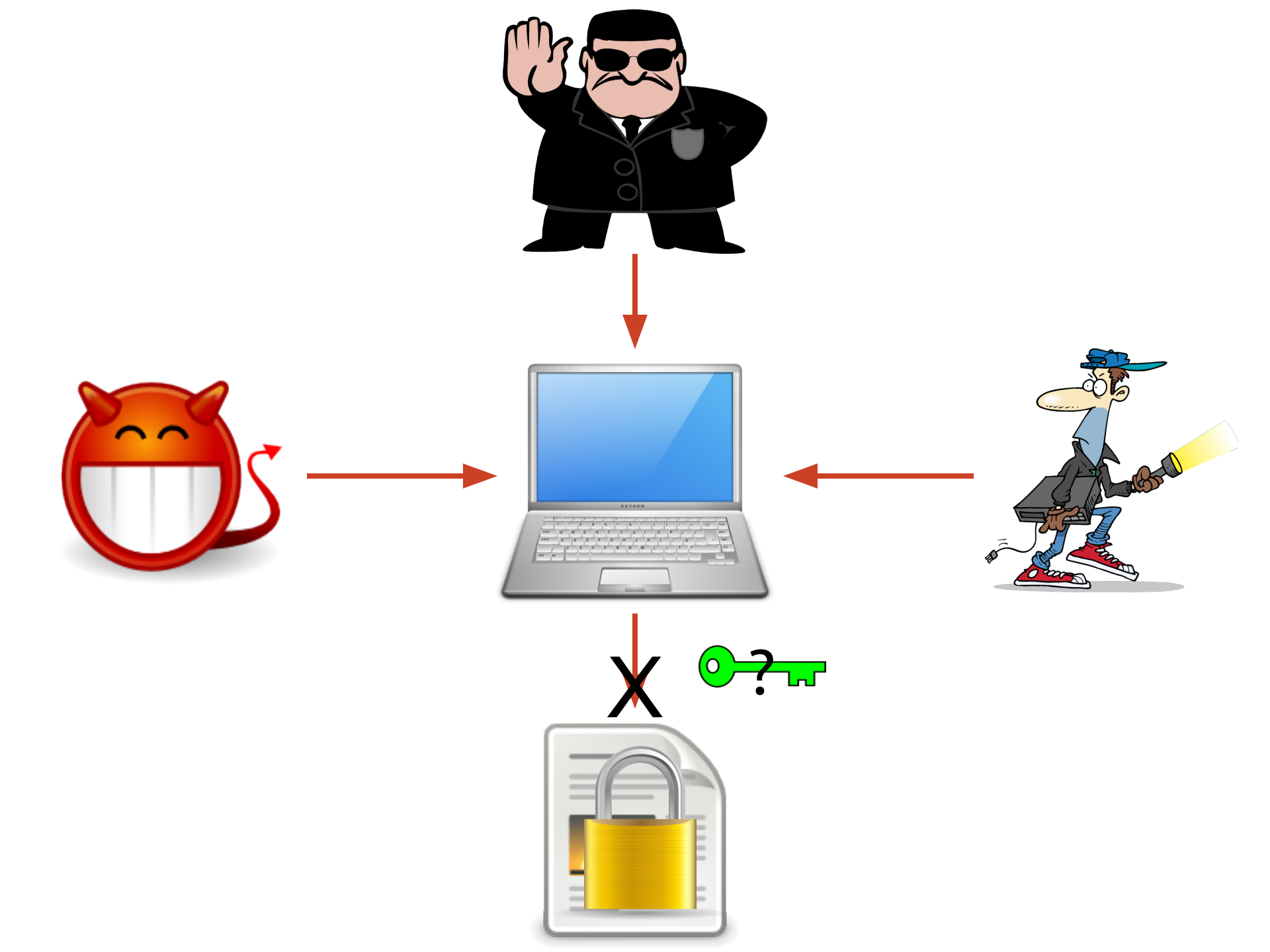

Encrypt
"My Secret"
TXkgU2VjcmV0
Decrypt

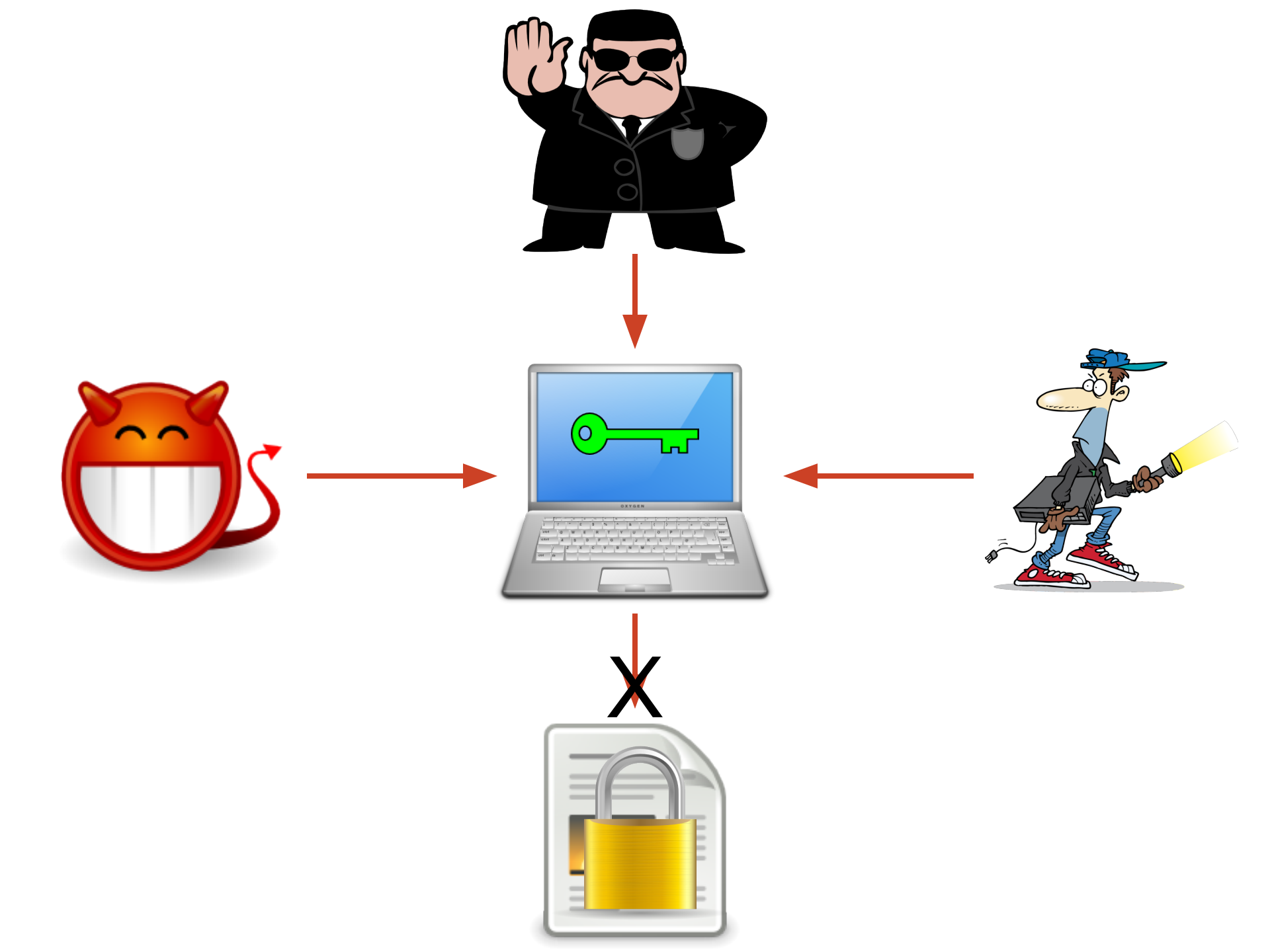
How does it help us?

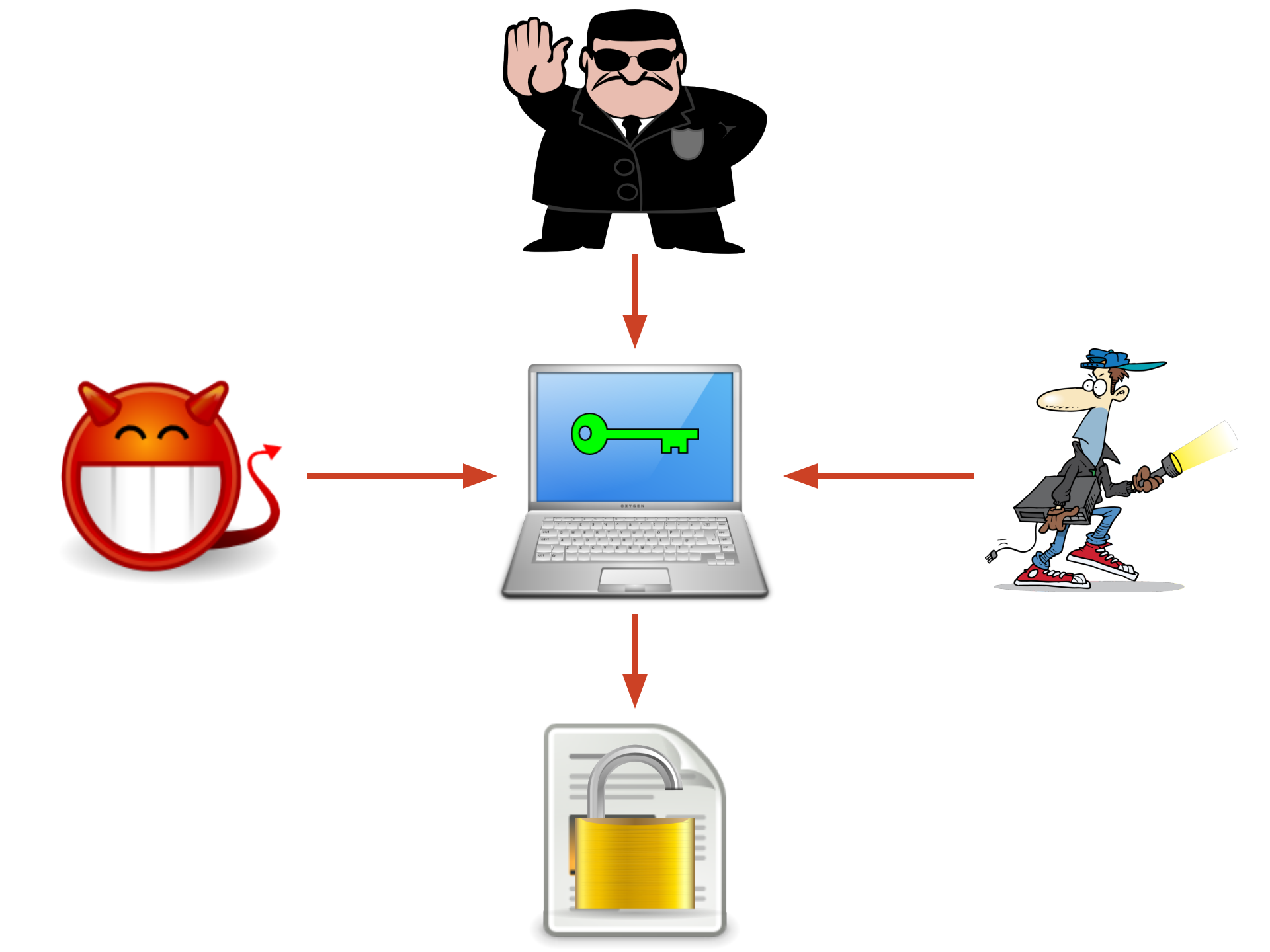




But what about the keys?

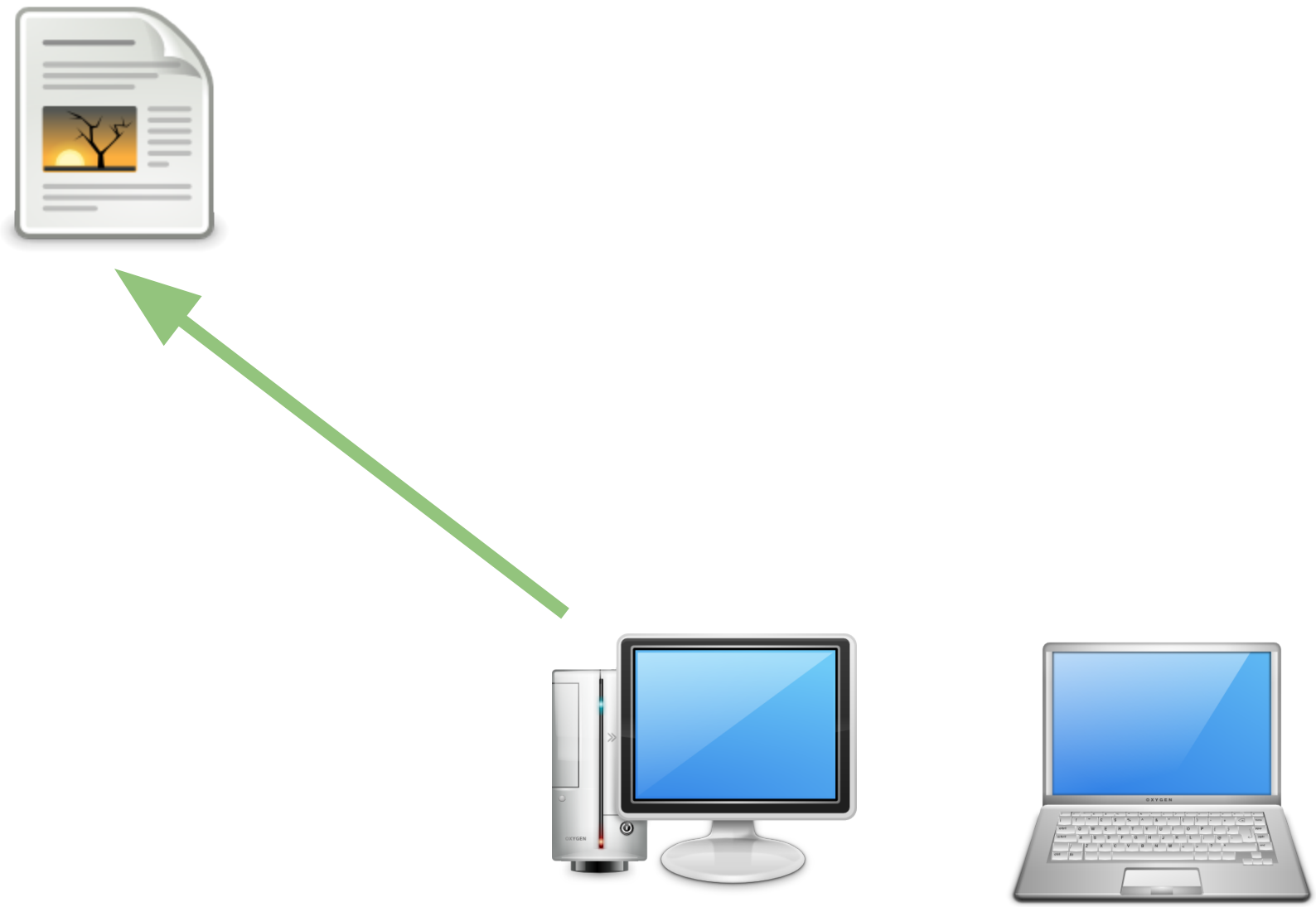


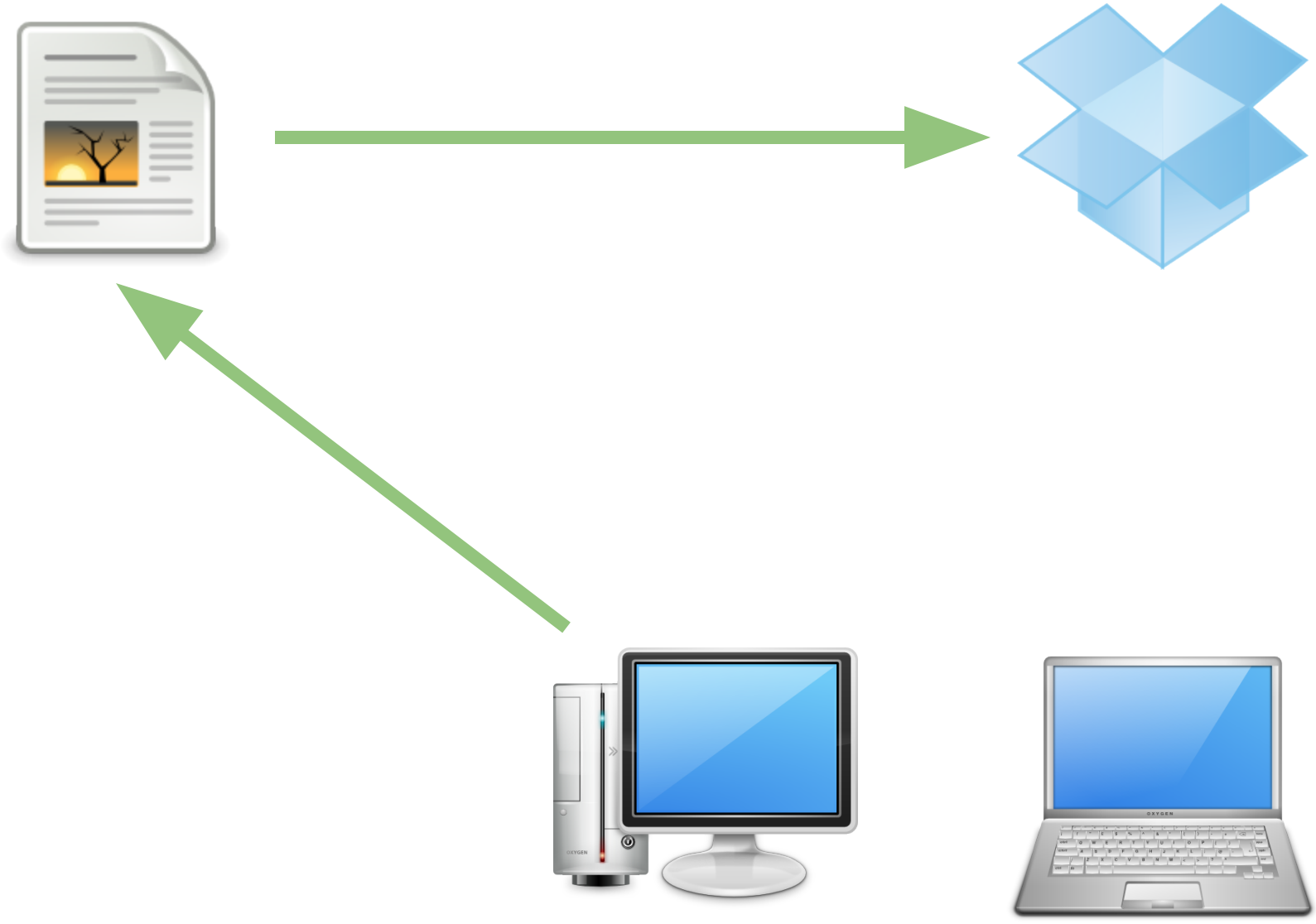


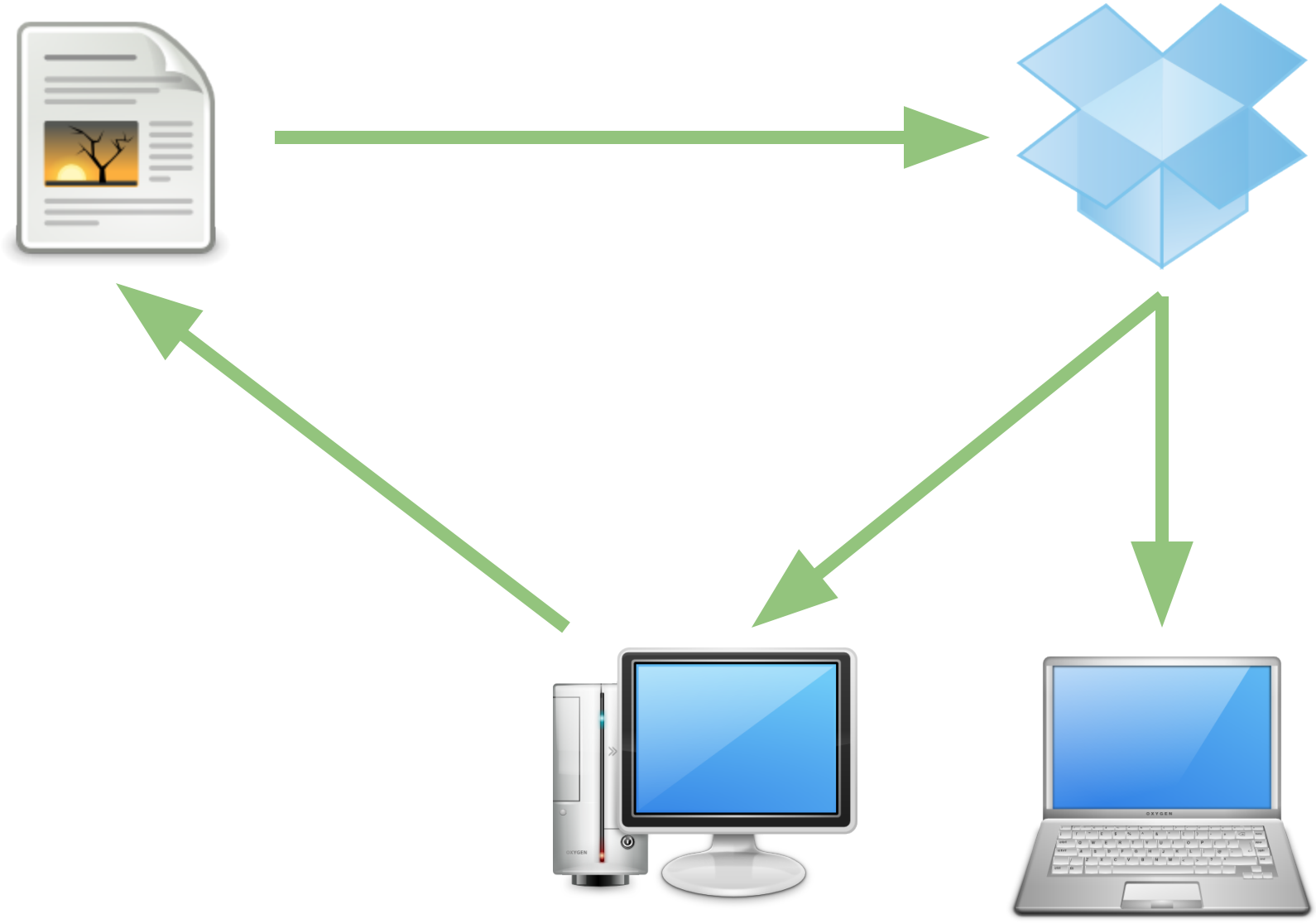


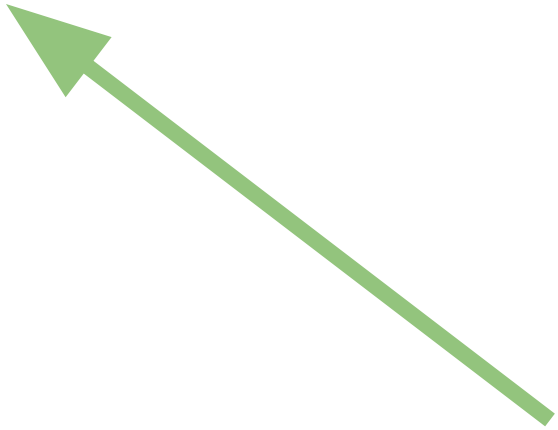
Key Management Challenges

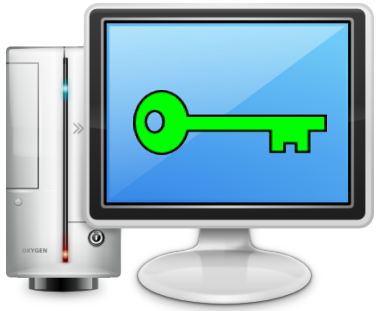
Multi-Device Sync

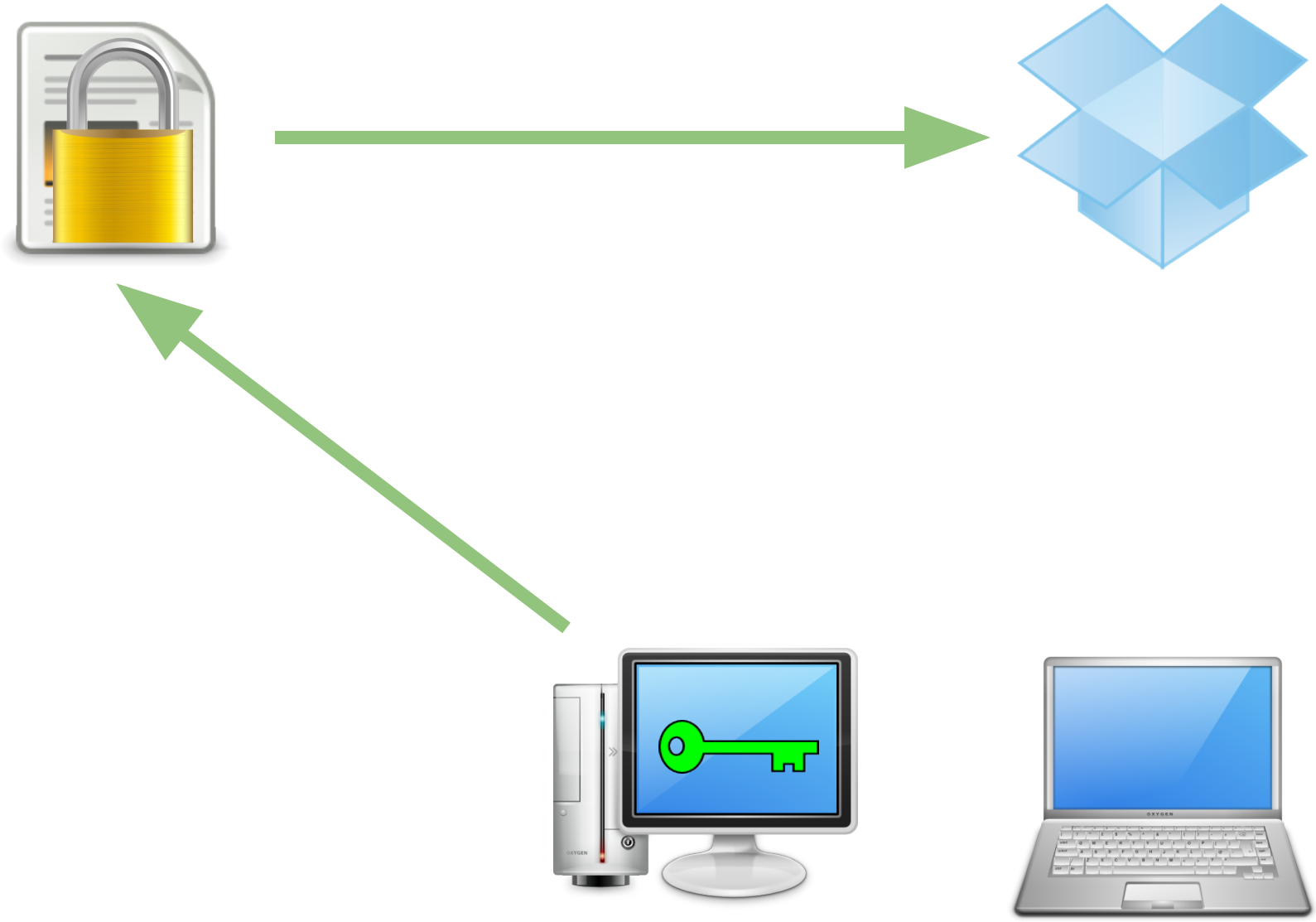


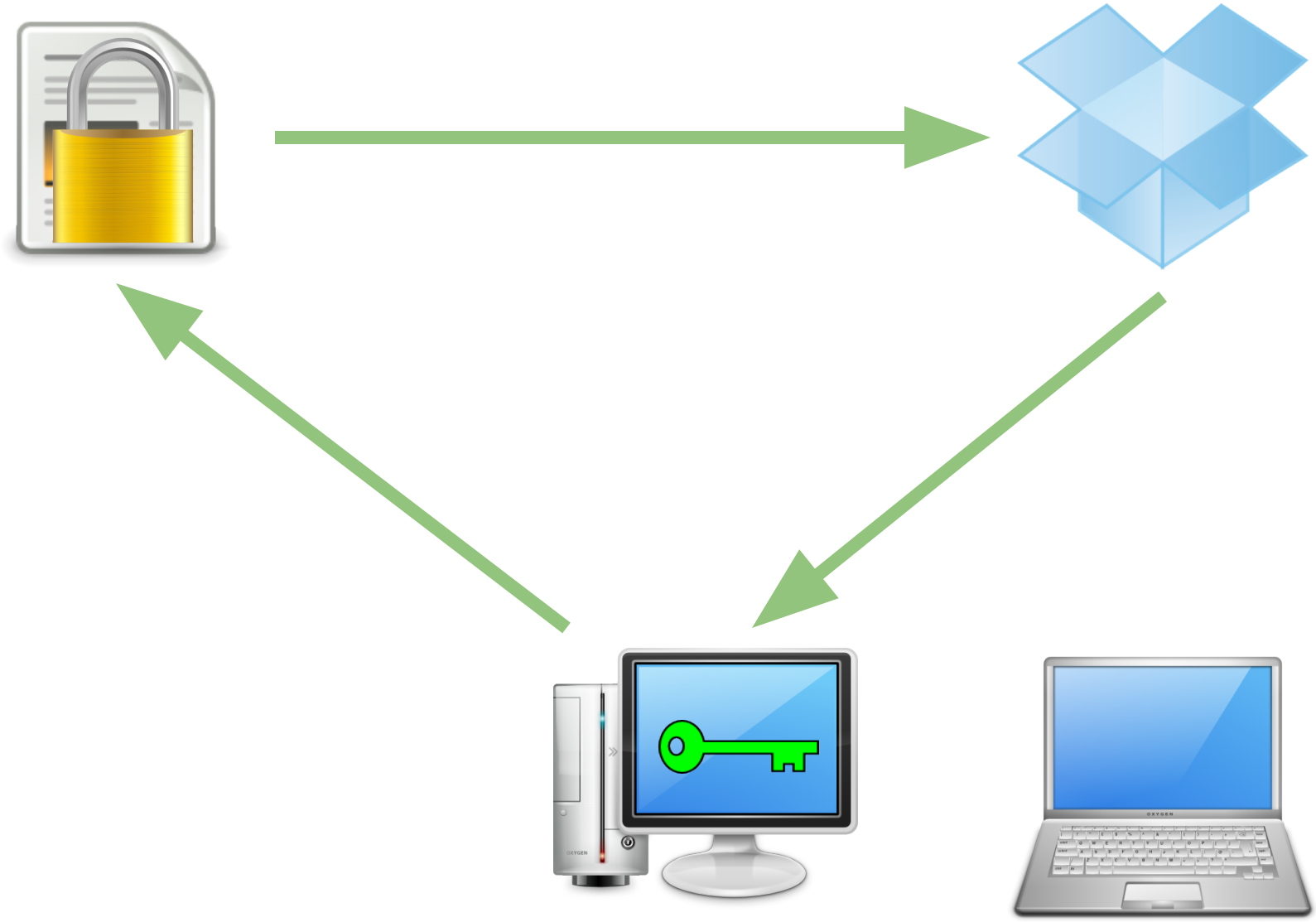


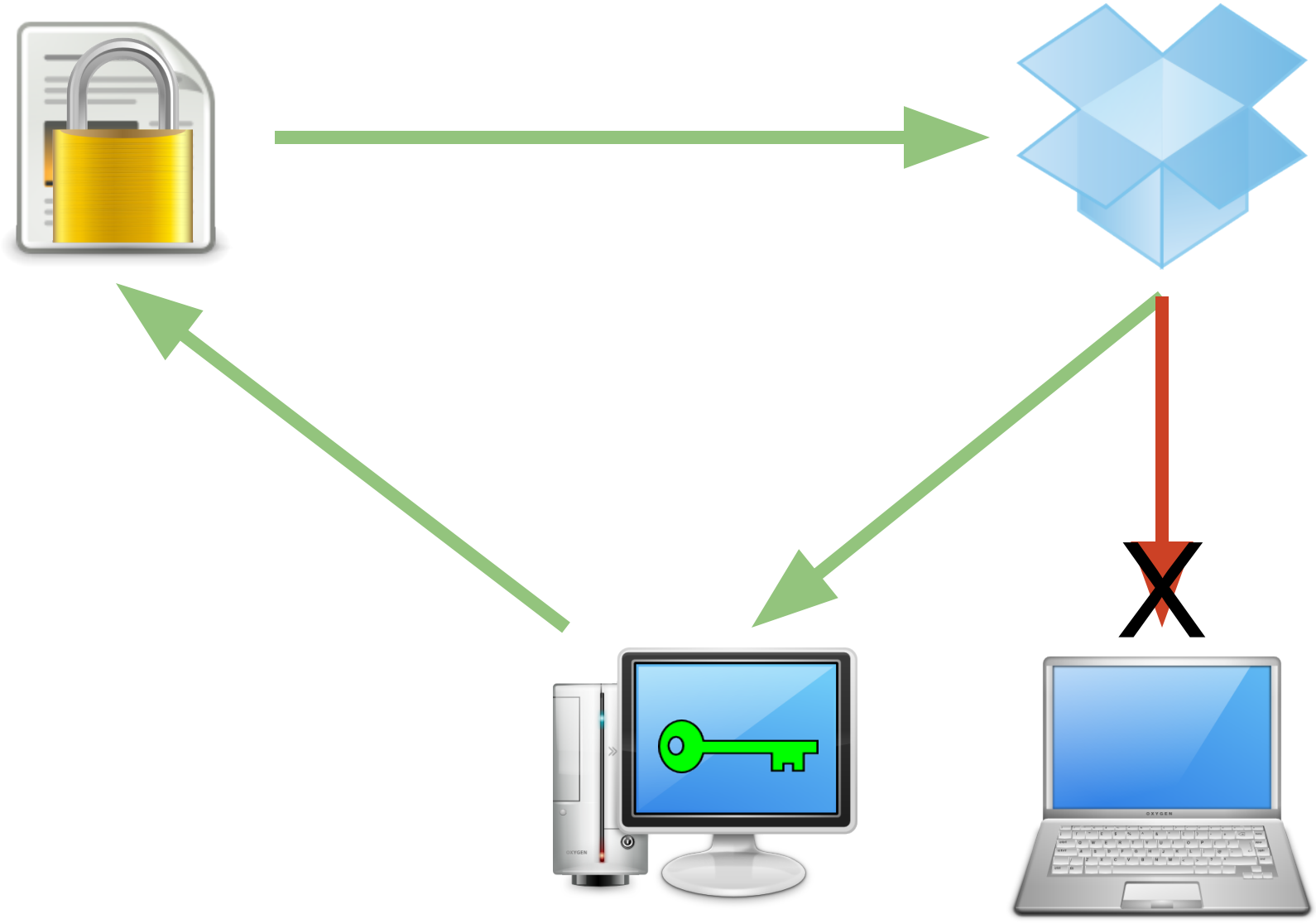




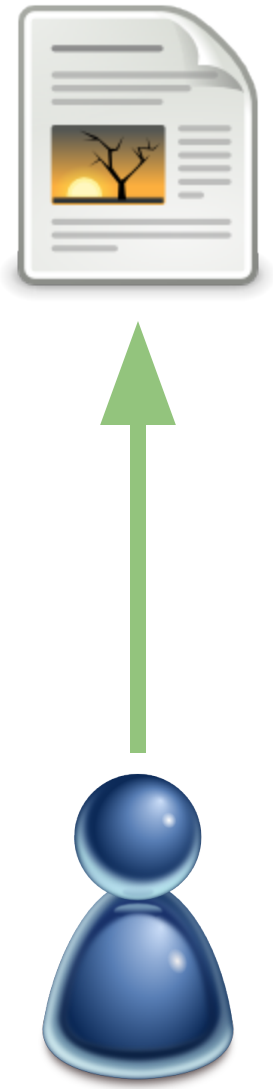


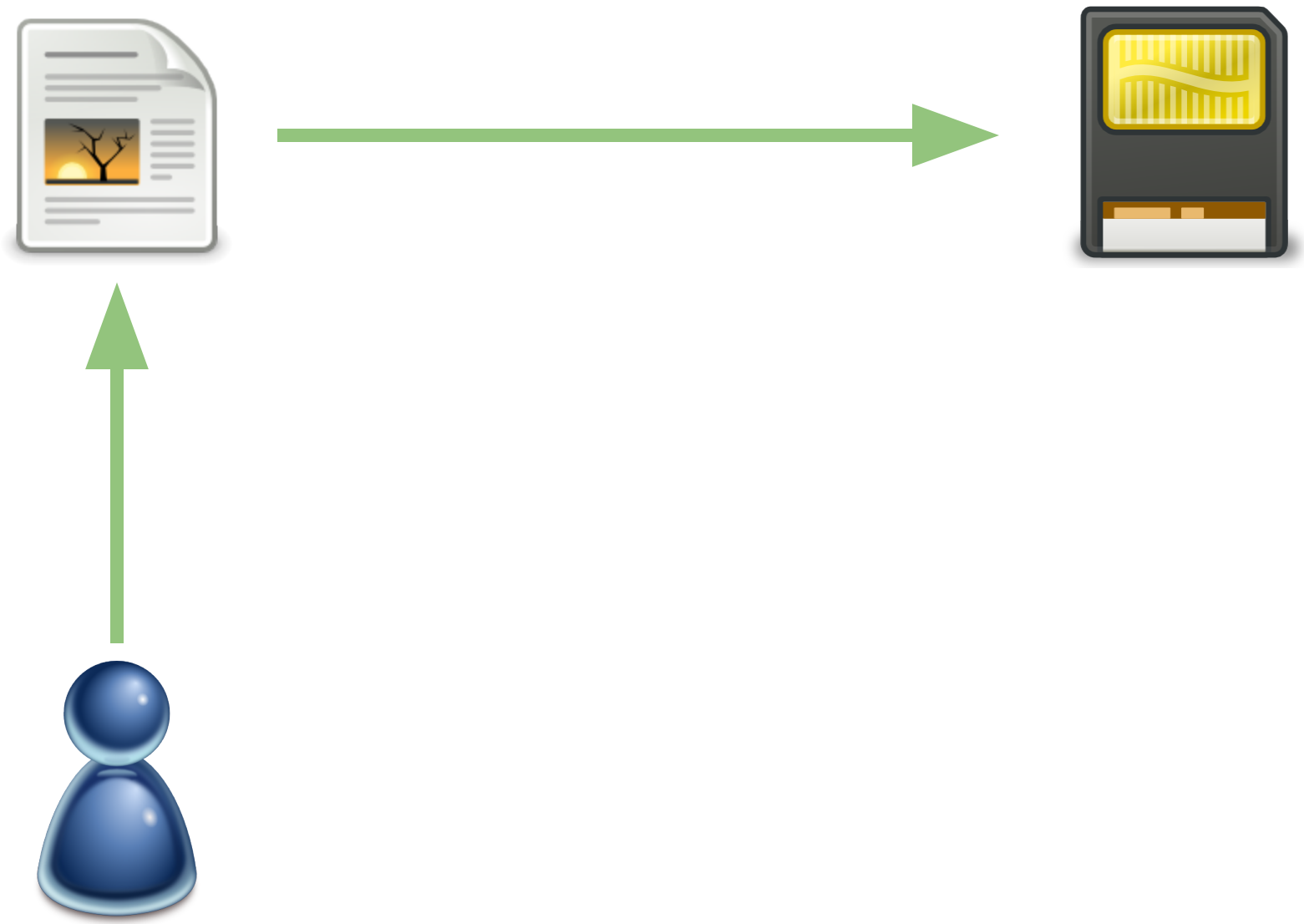


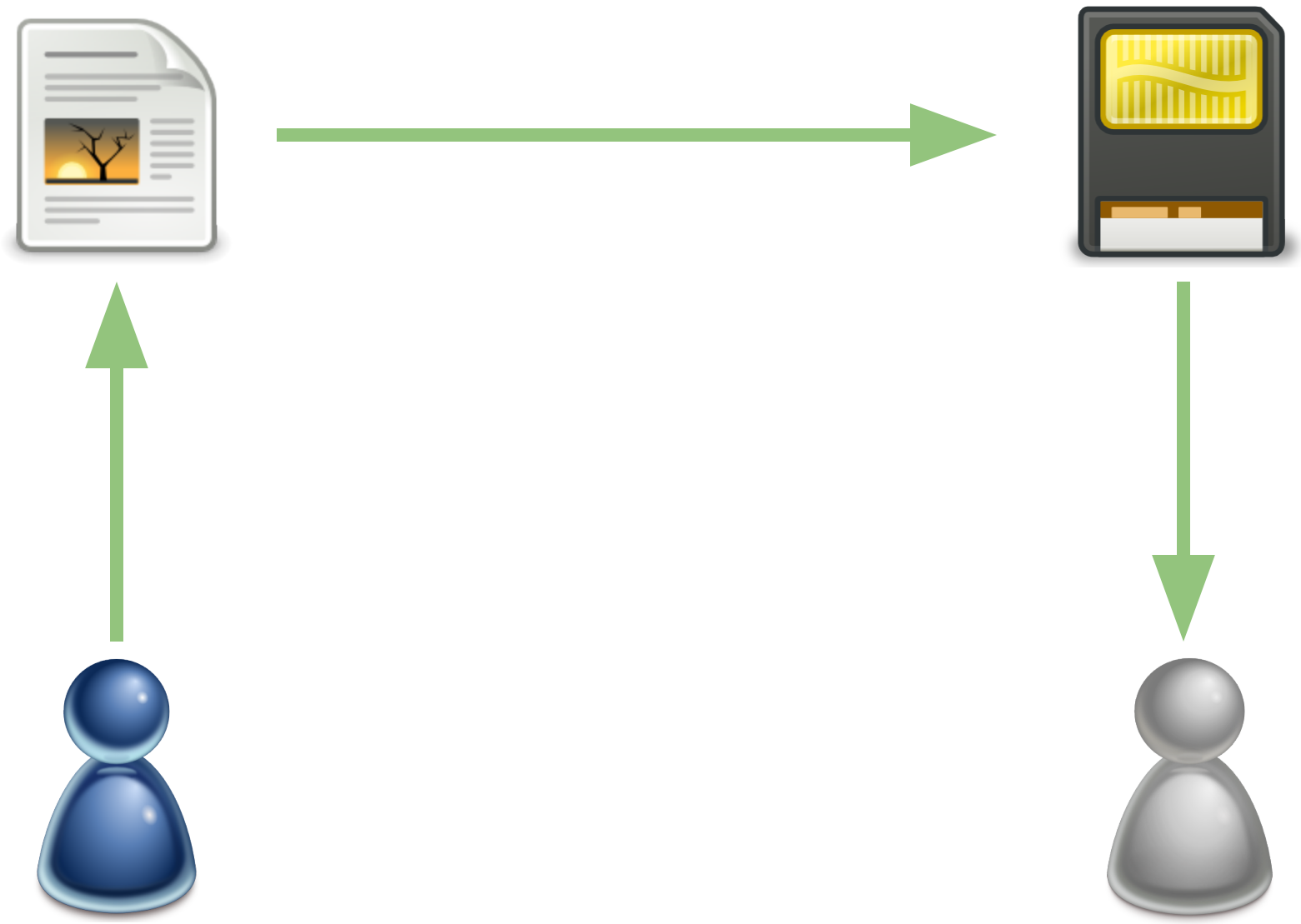


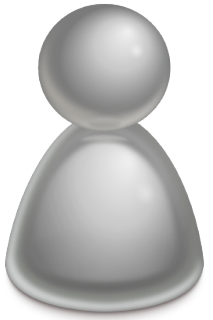


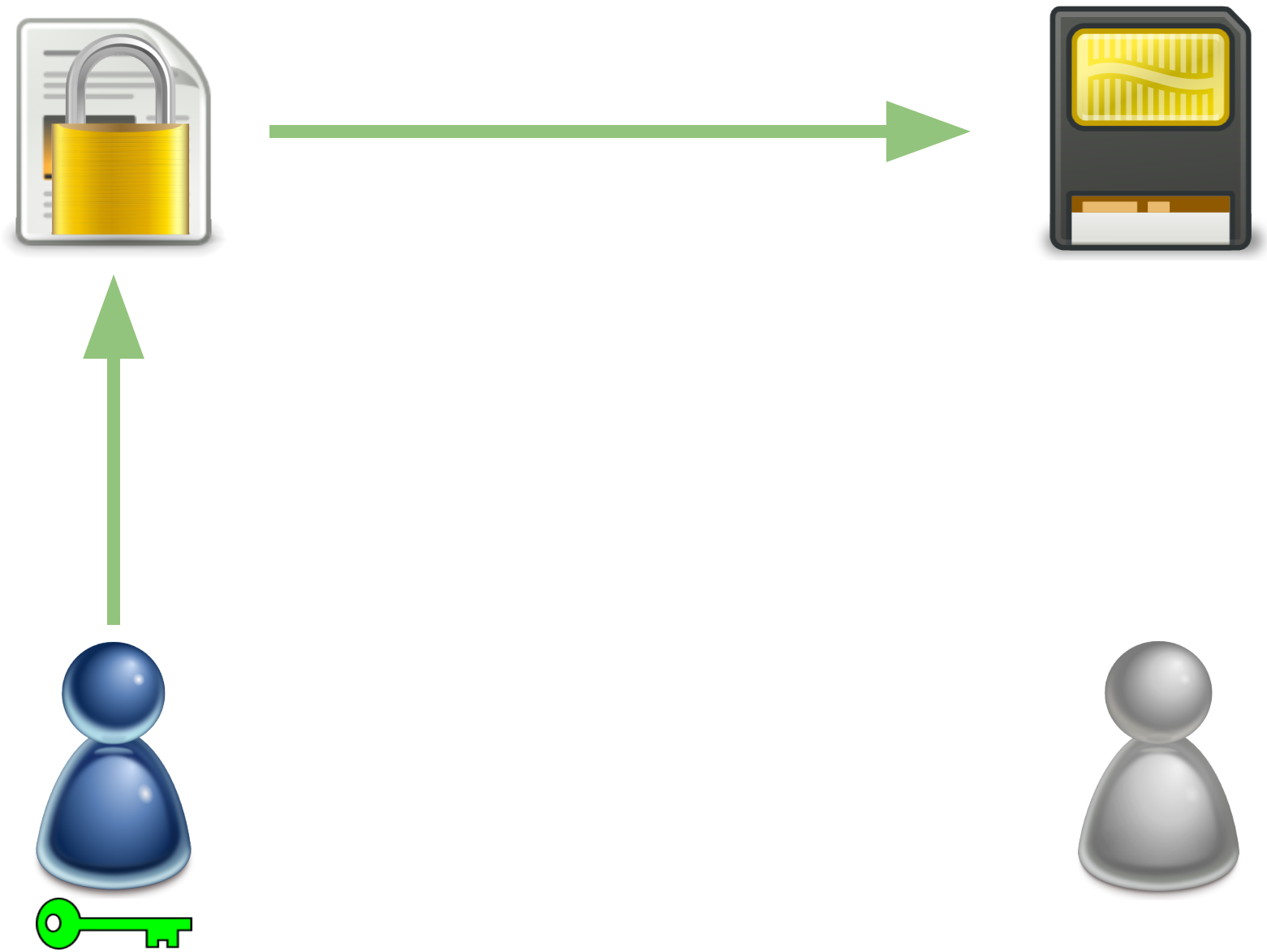
Out-of-Band Sharing

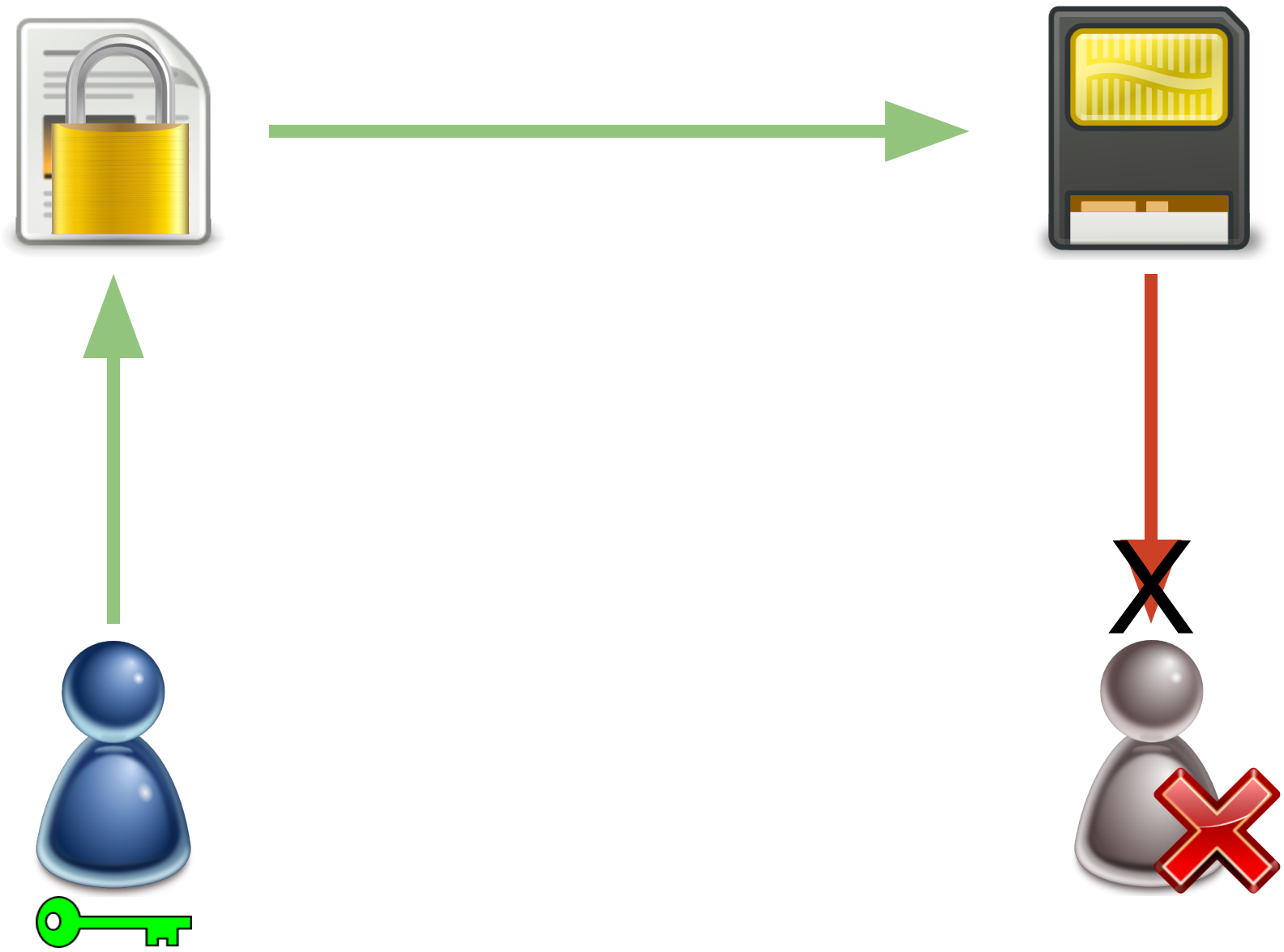




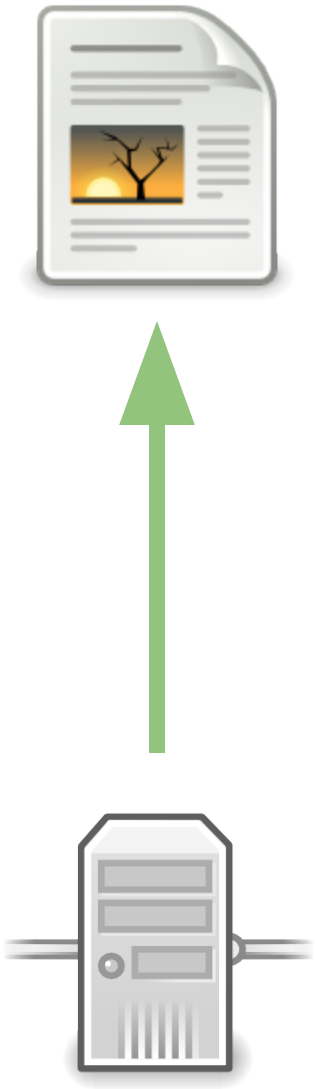


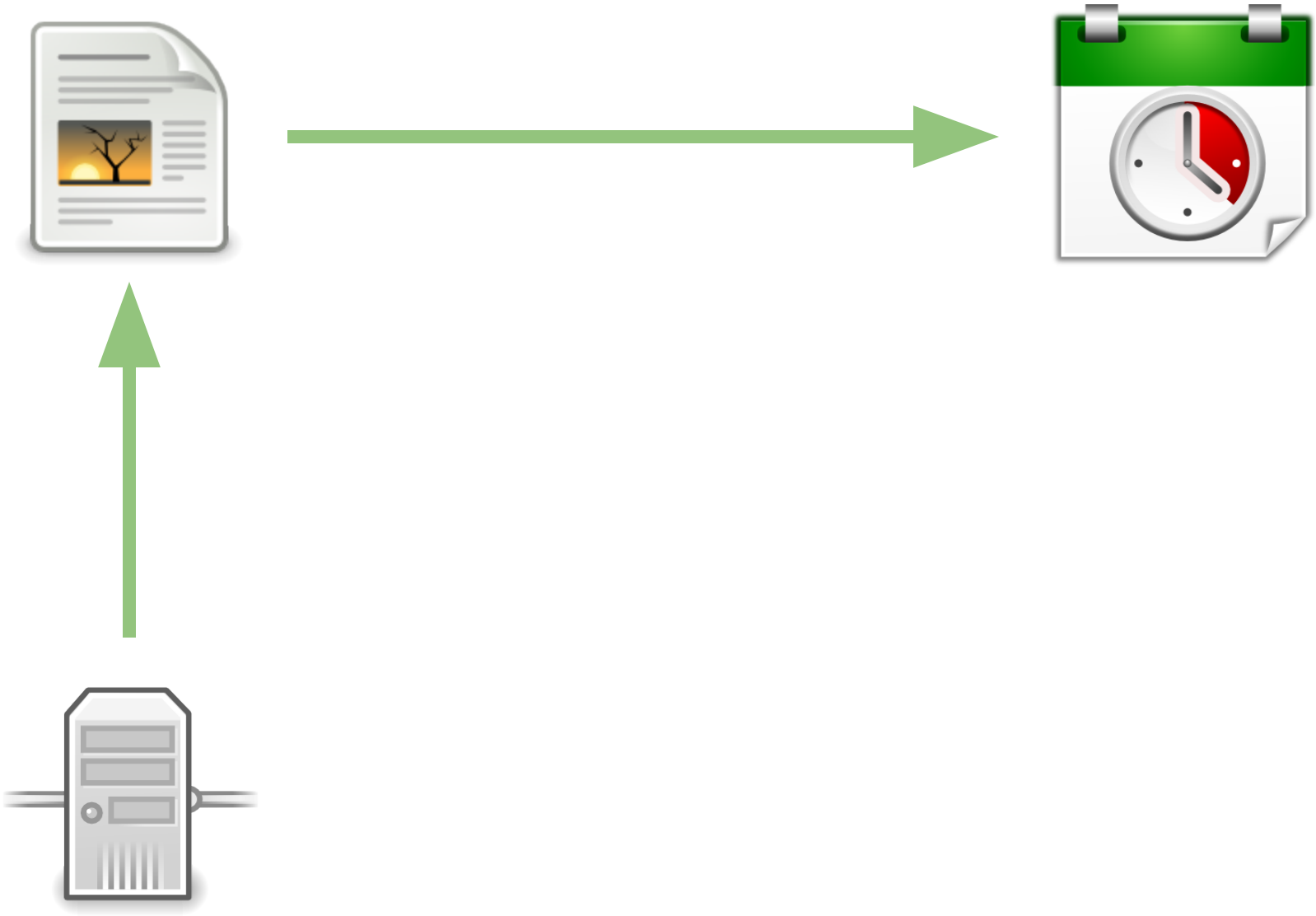


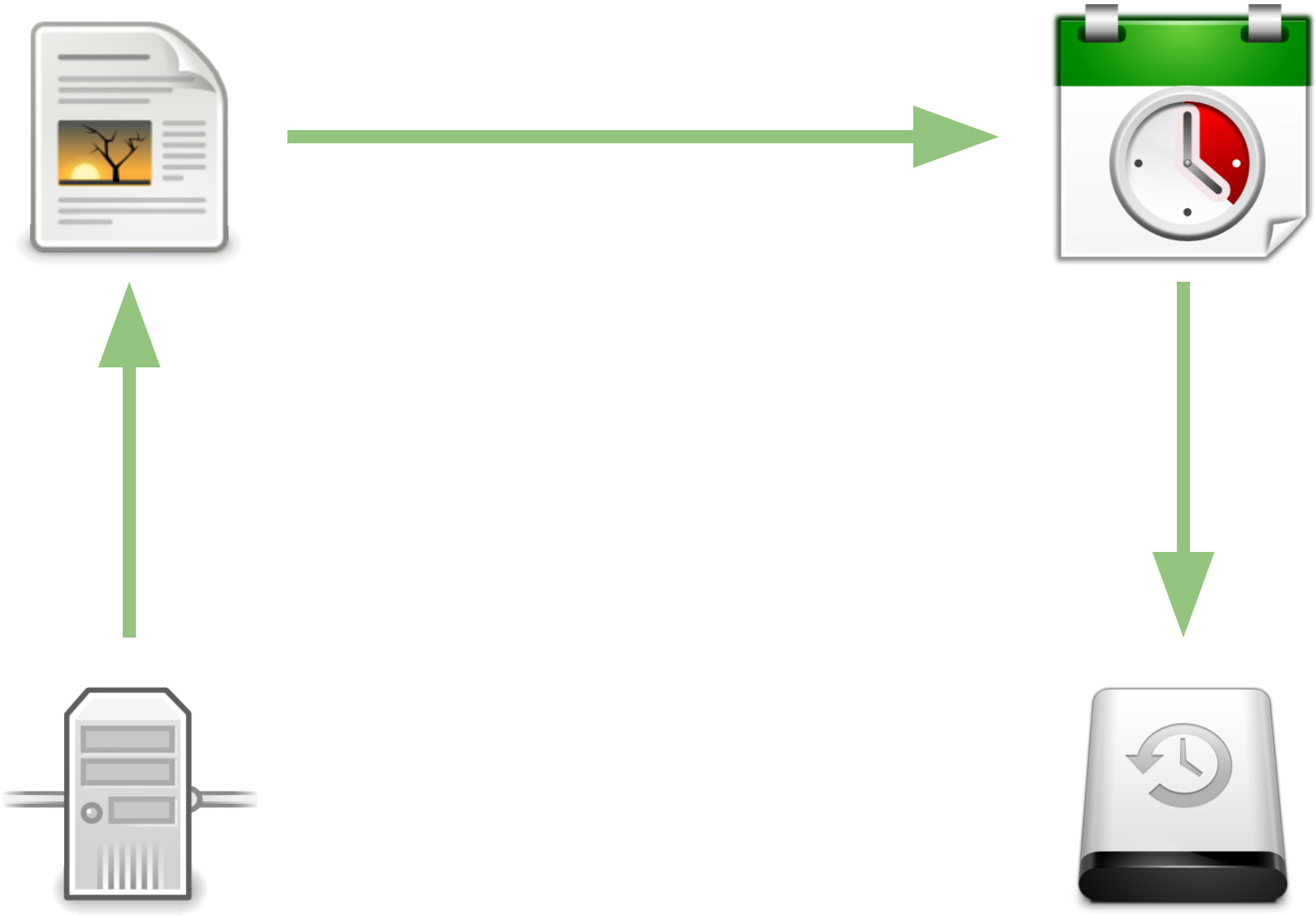


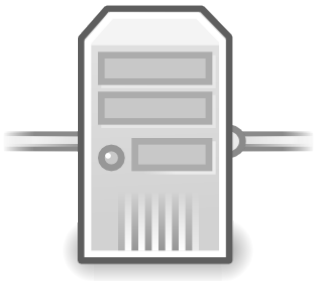


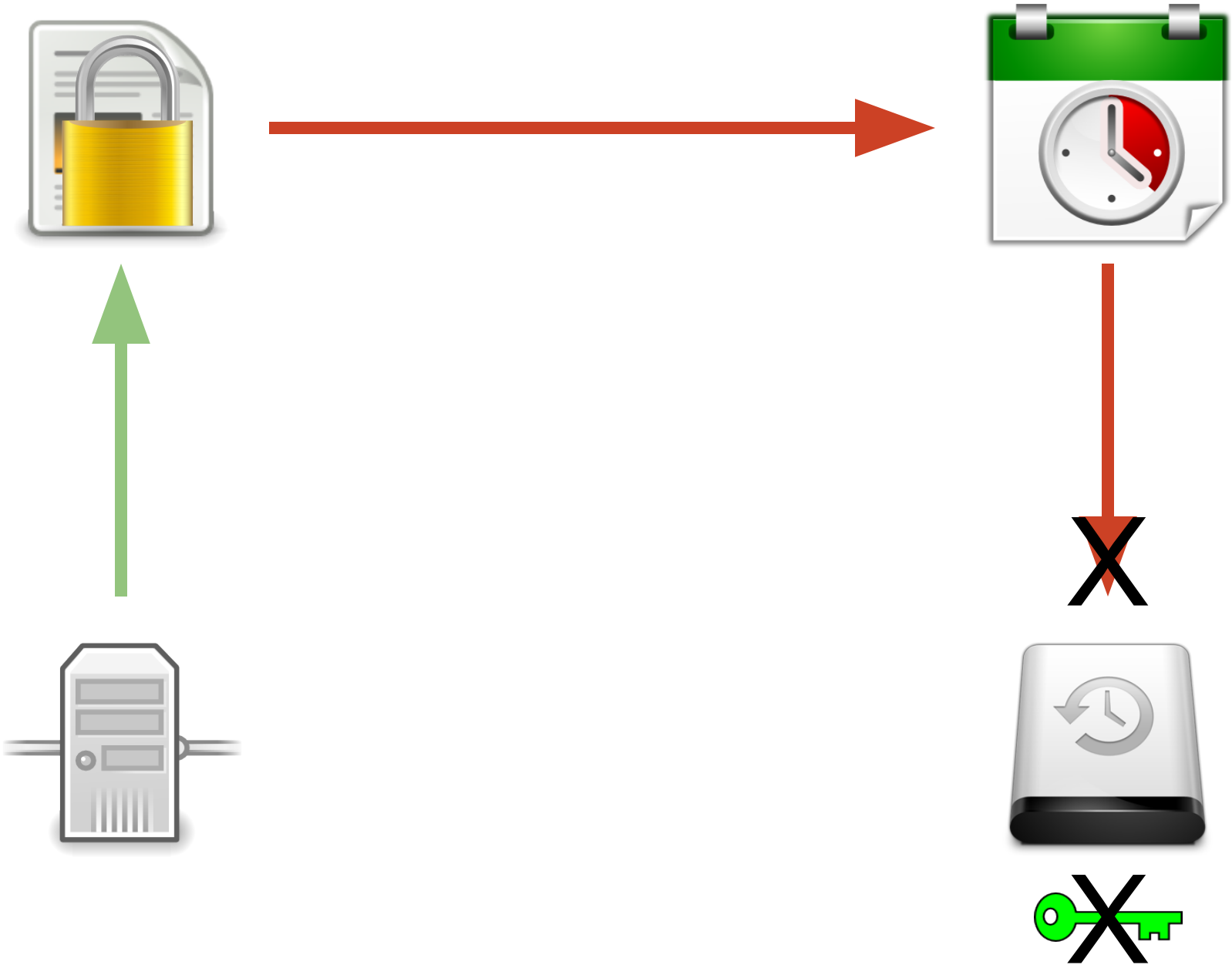
Autonomous Access



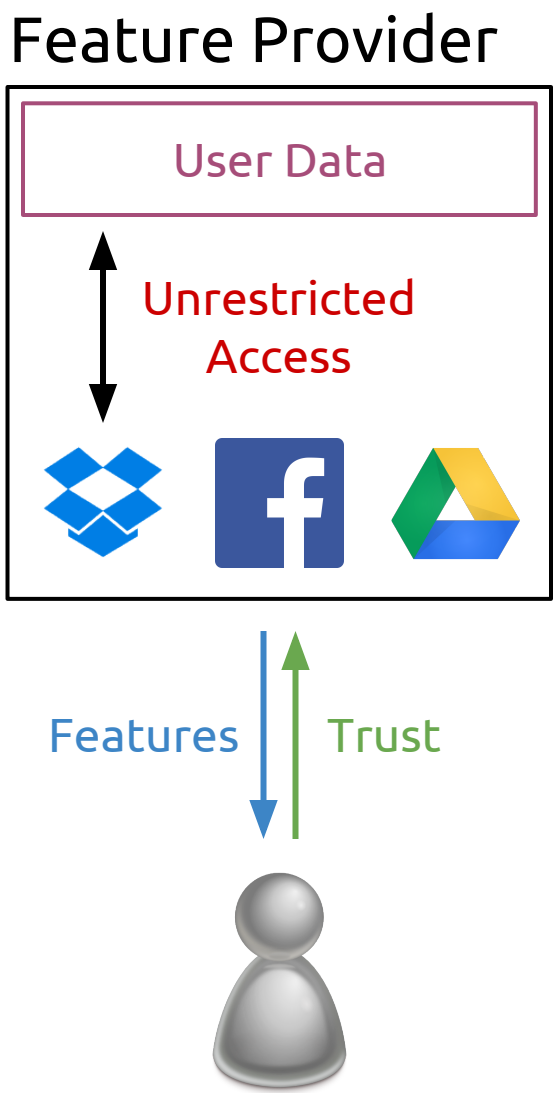


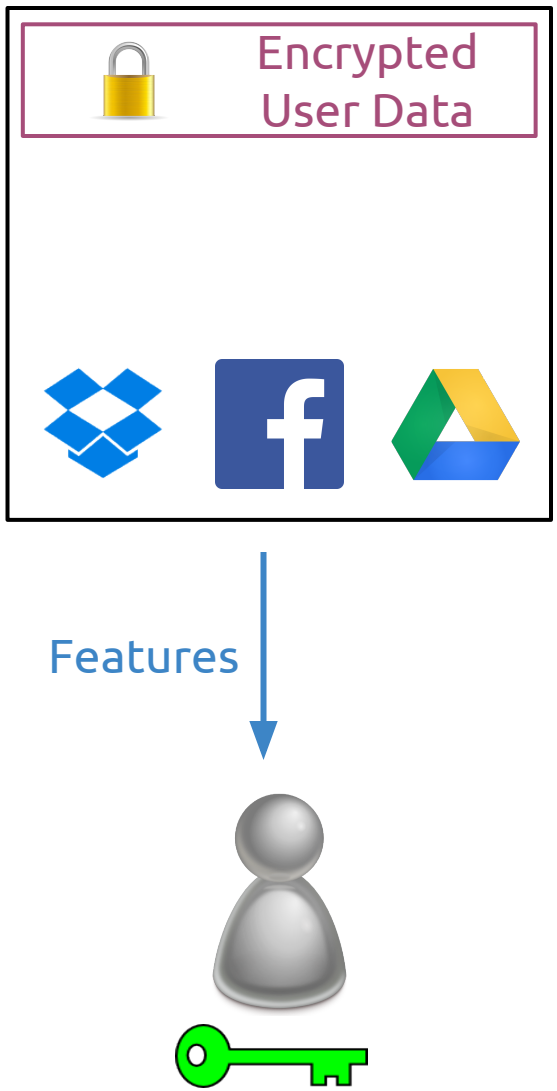


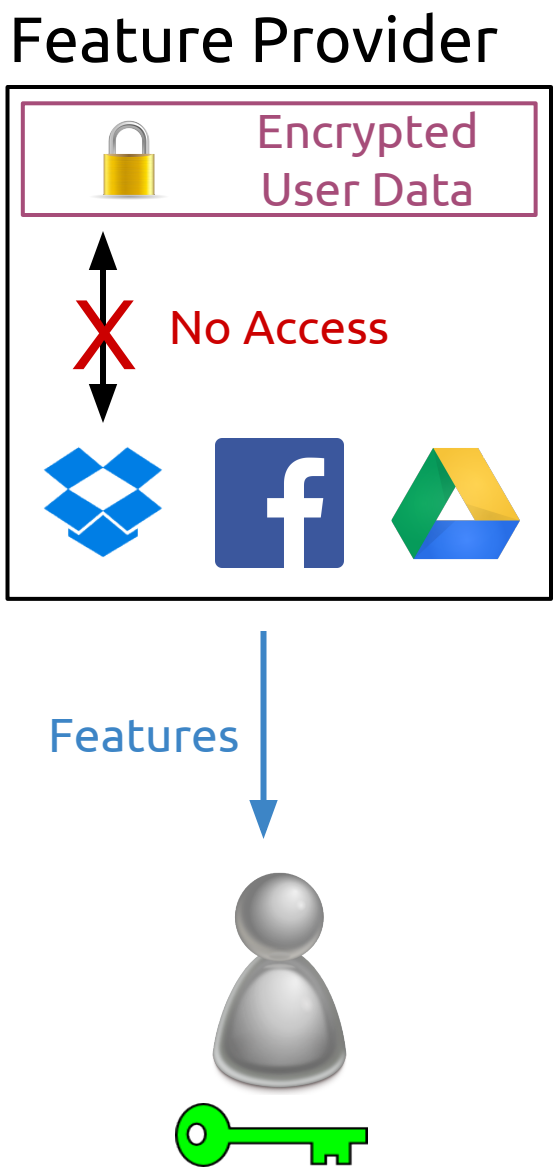




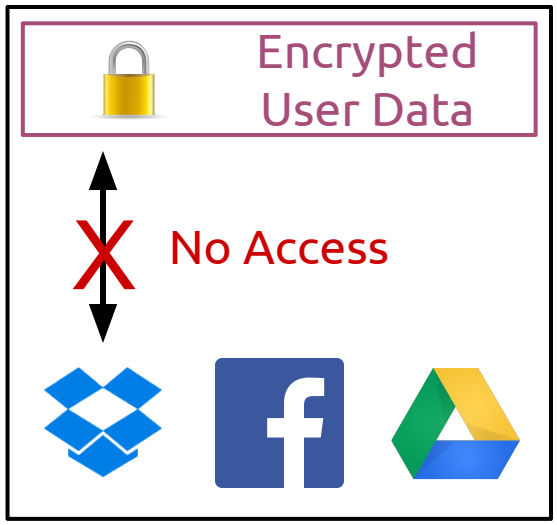
The Cloud

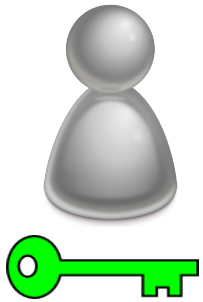

Feature Provider
User Data
Unrestricted Access
Features
Trust


Feature Provider
Encrypted
User Data
Features


Feature Provider
Encrypted
User Data
No Access
Features

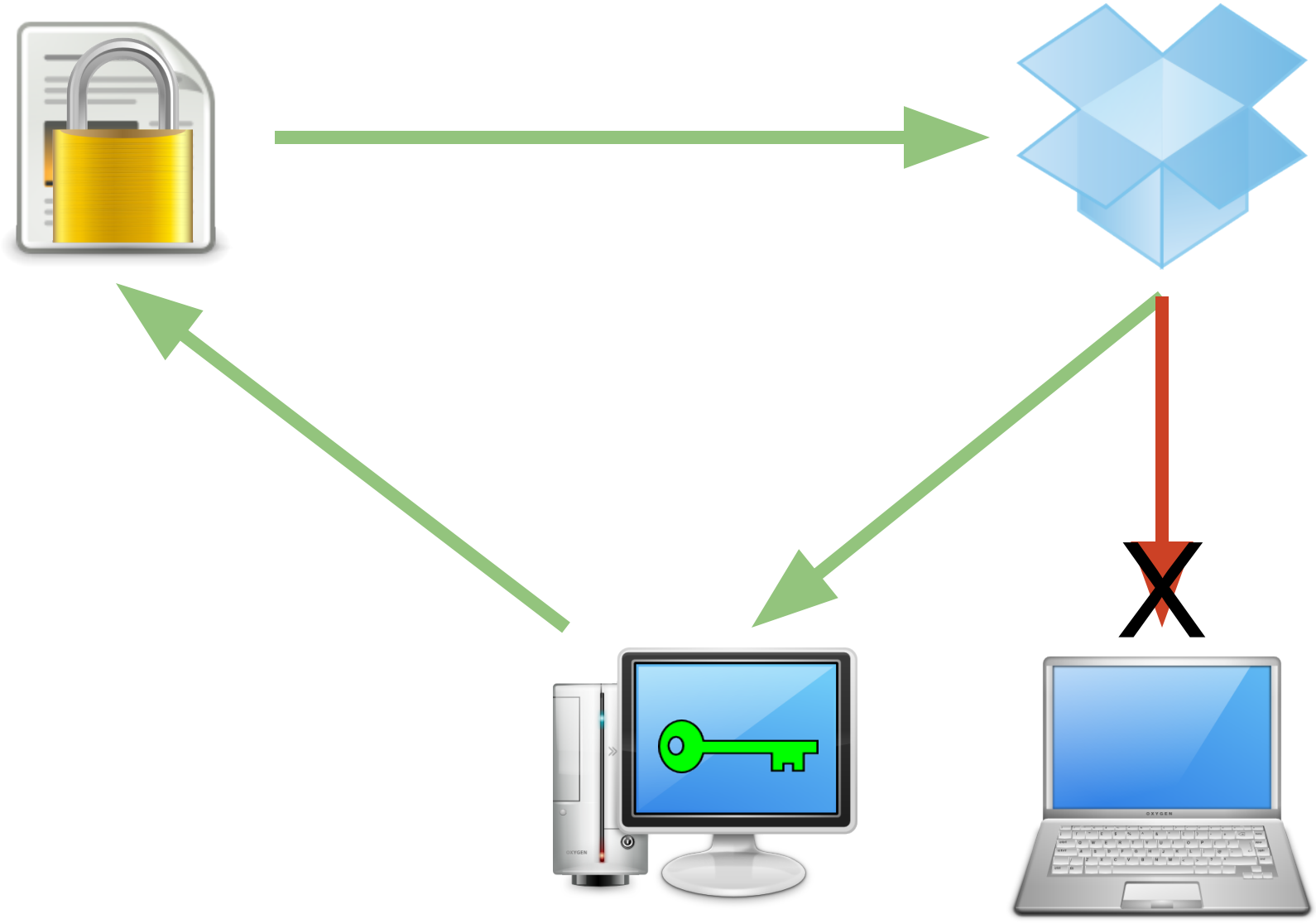
Feature Provider

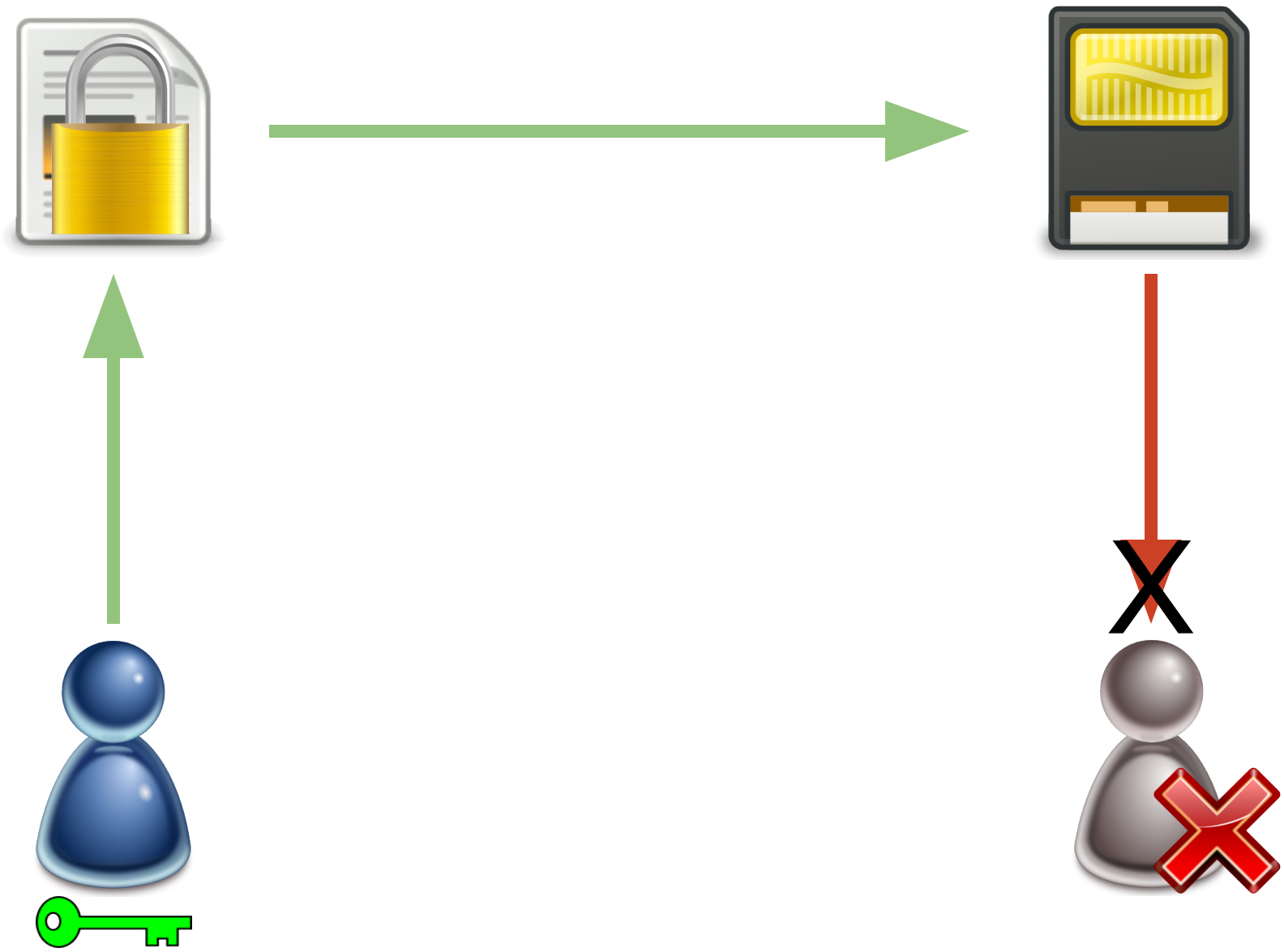


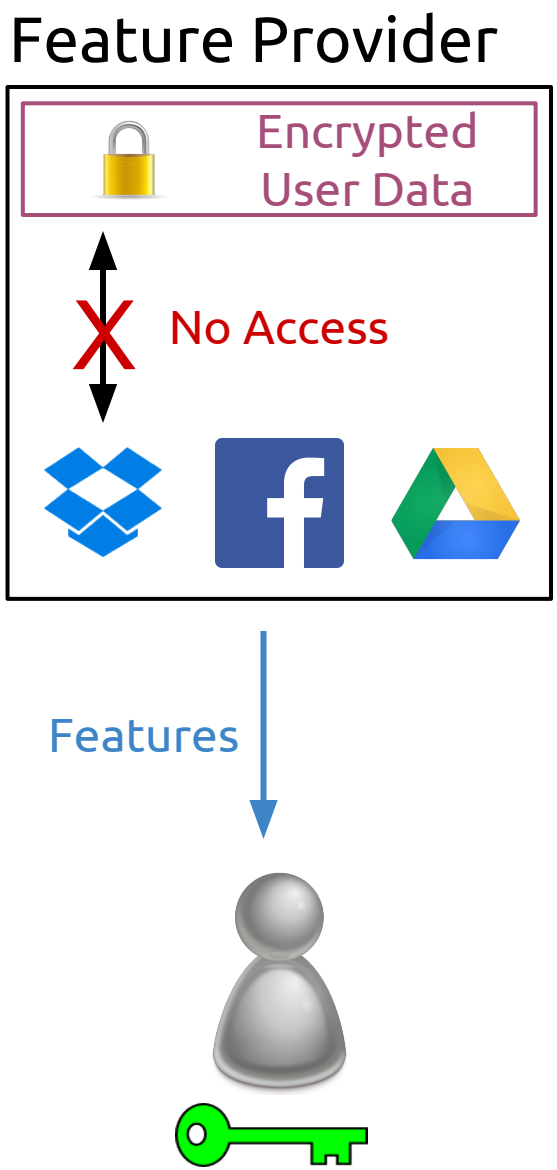


Encryption is broken

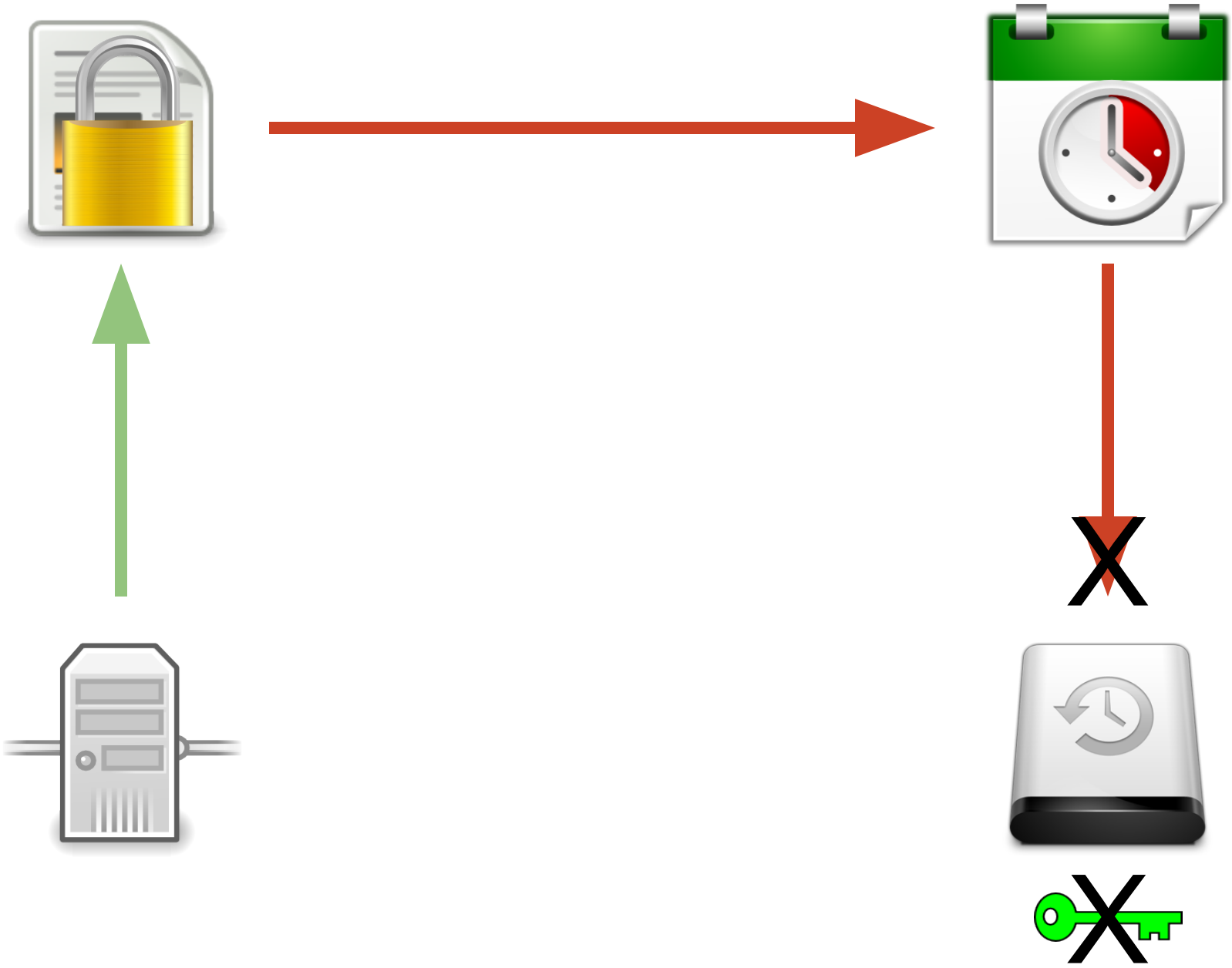
Lack of key access



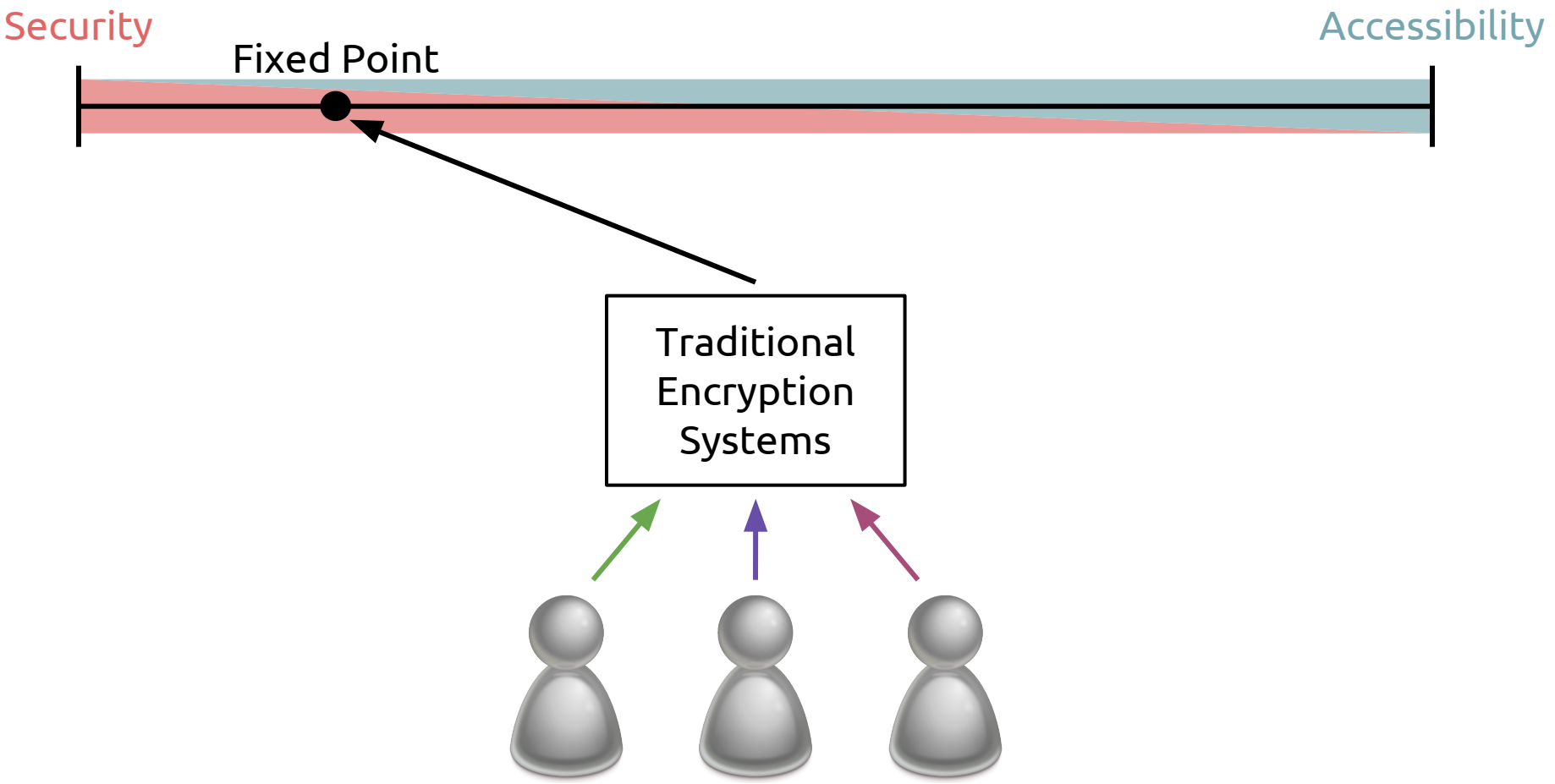



Feature Provider
Encrypted
User Data
No Access
Features

Lack of flexibility




Security
Accessibility


Security
Accessibility
Fixed Point
Traditional
Encryption
Systems

Ill-suited for
Modern Application

Difficult to Use

Doesn’t Solve
the Real Problem

Encryption is broken

Encryption is fine

Encryption
is fine

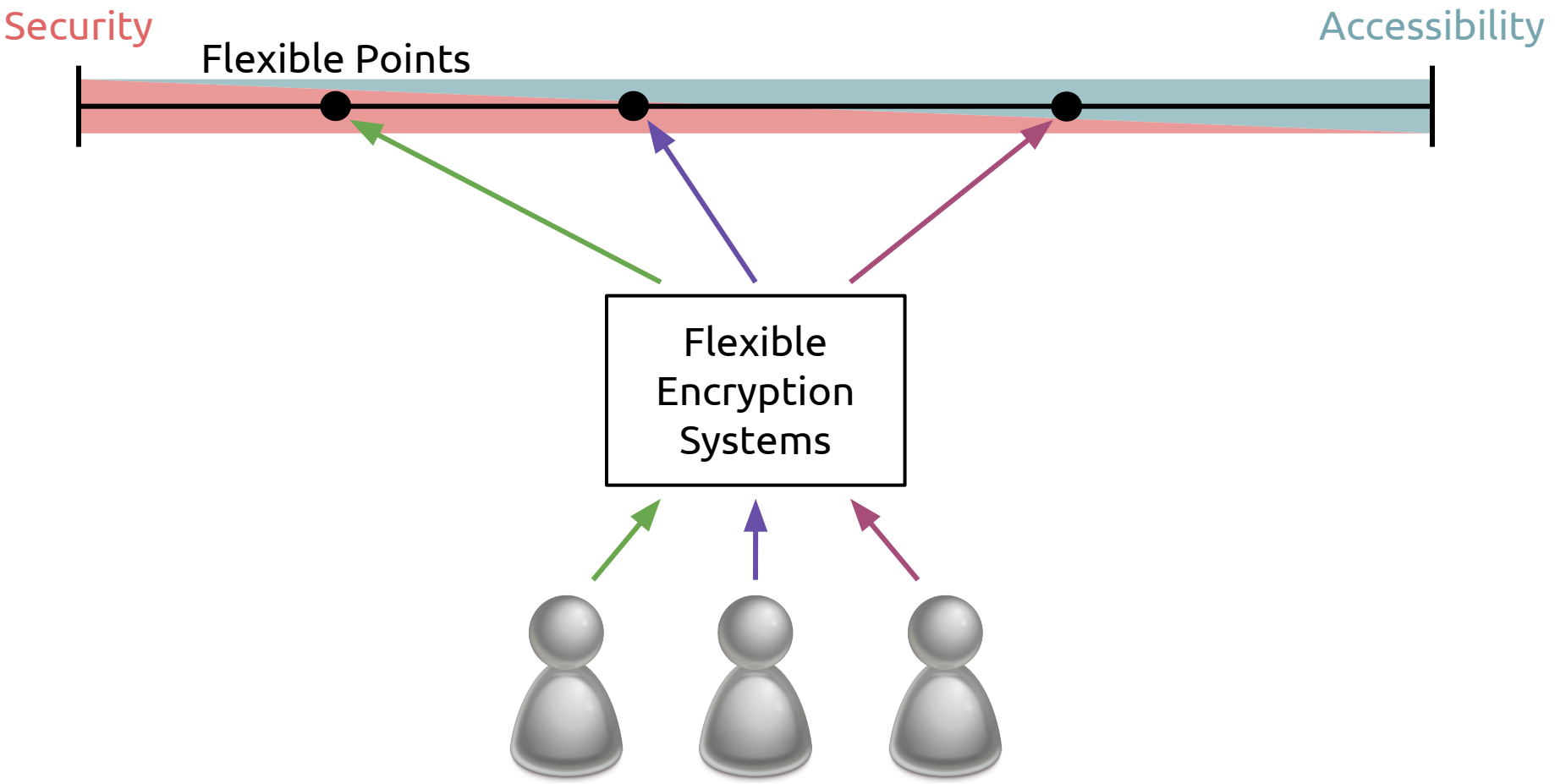
Key storage
is broken

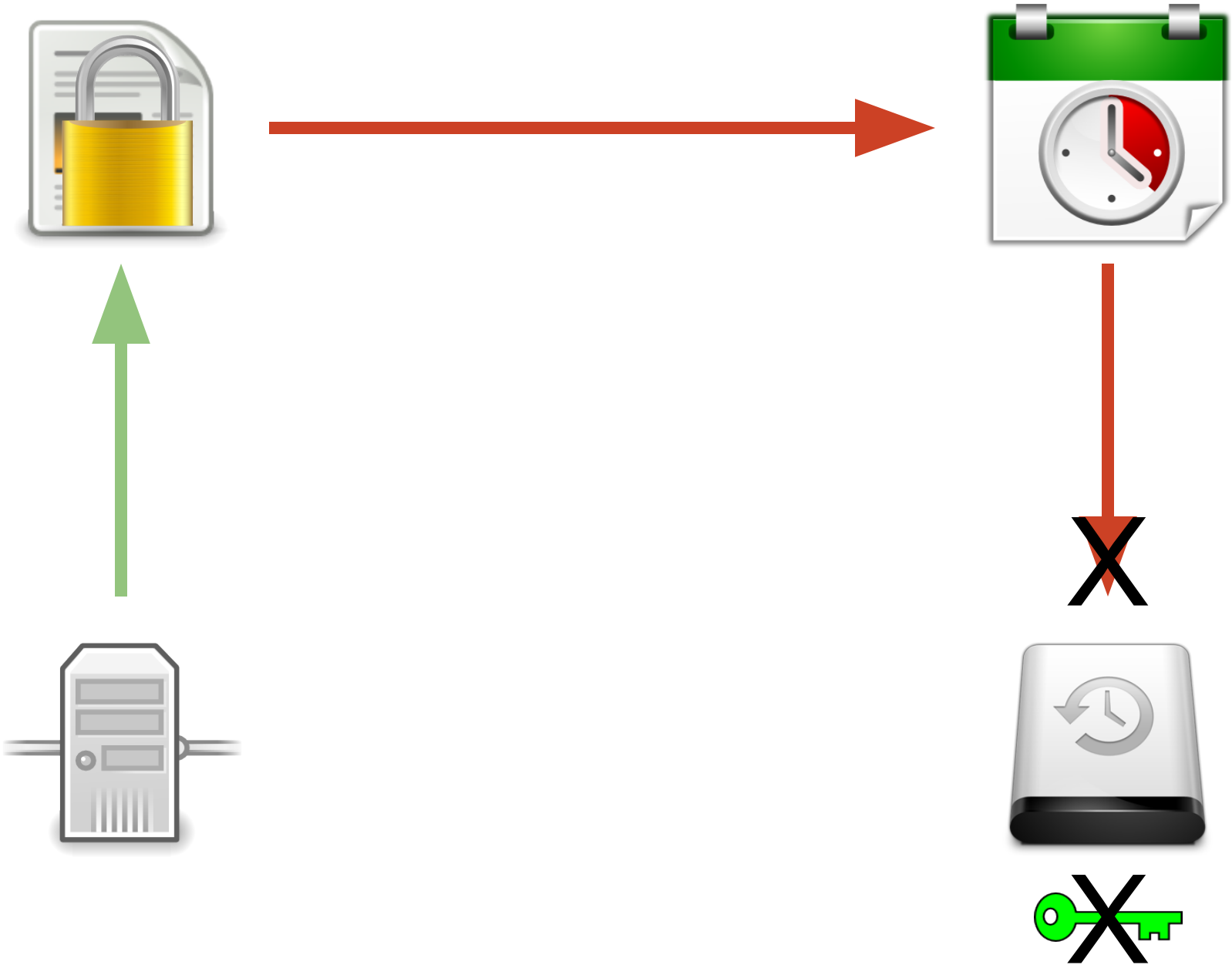
To fix key storage...

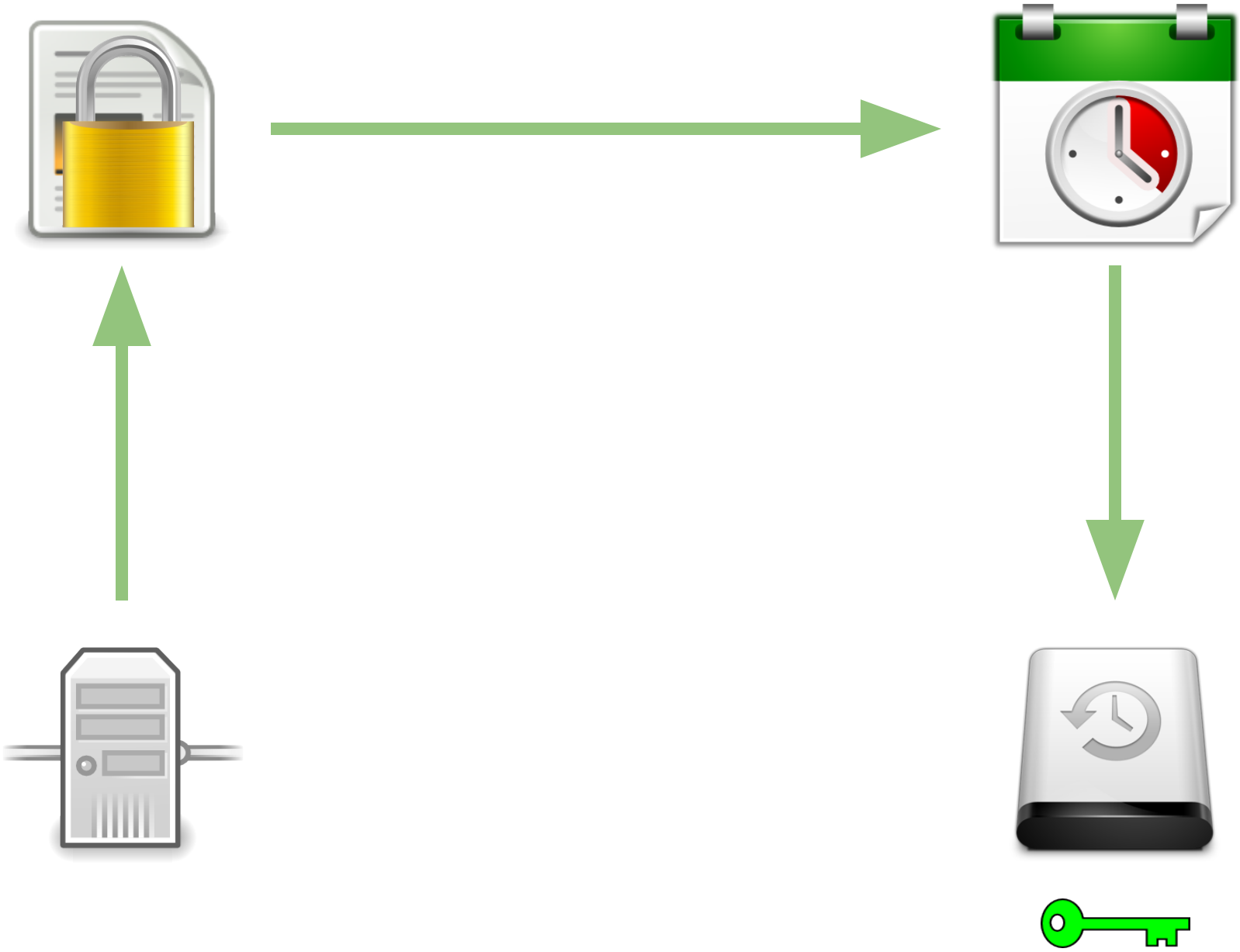
Flexibility

Centralization

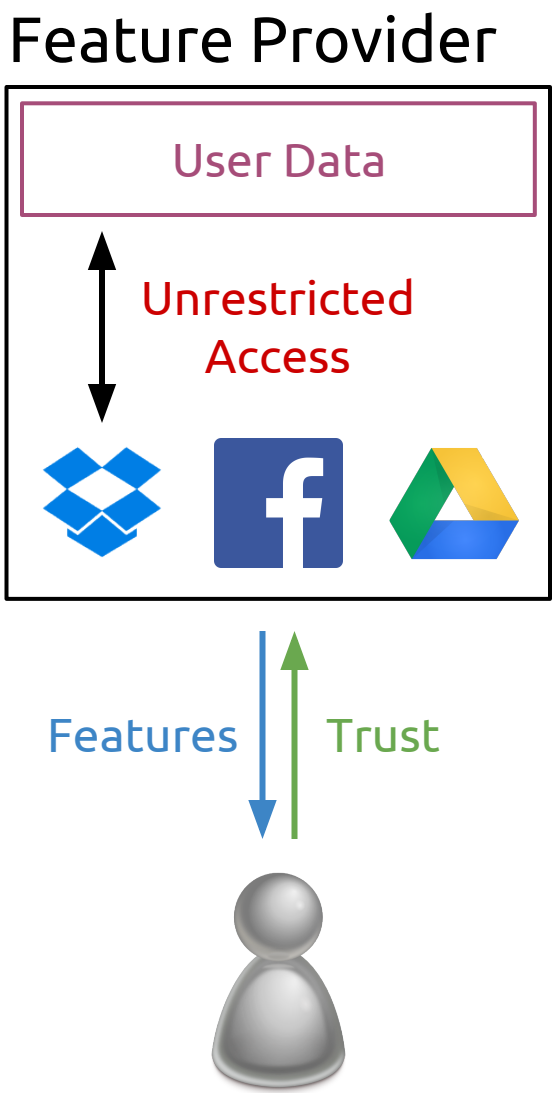
Flexibility

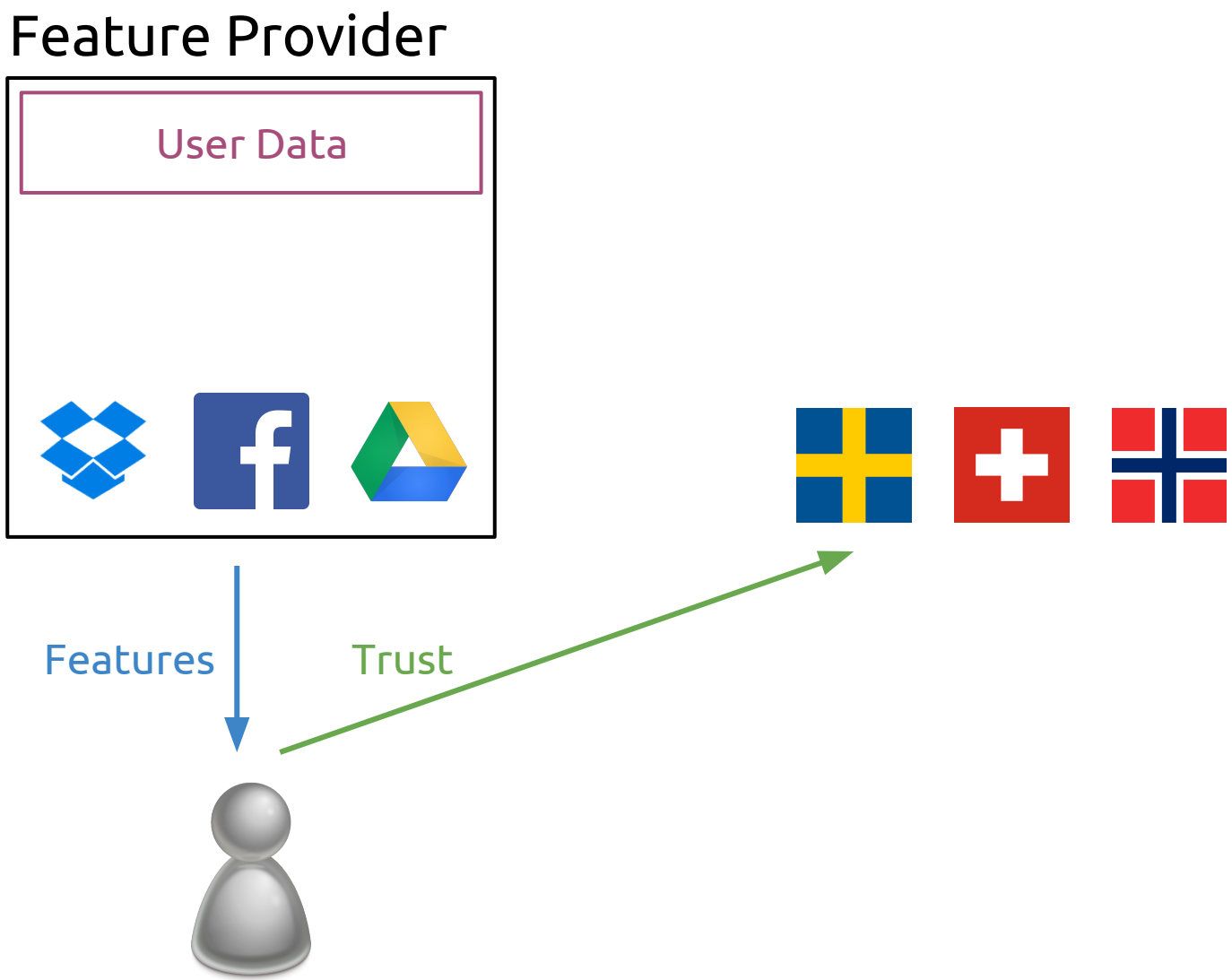

Security
Flexible Points
Accessibility
Flexible
Encryption
Systems

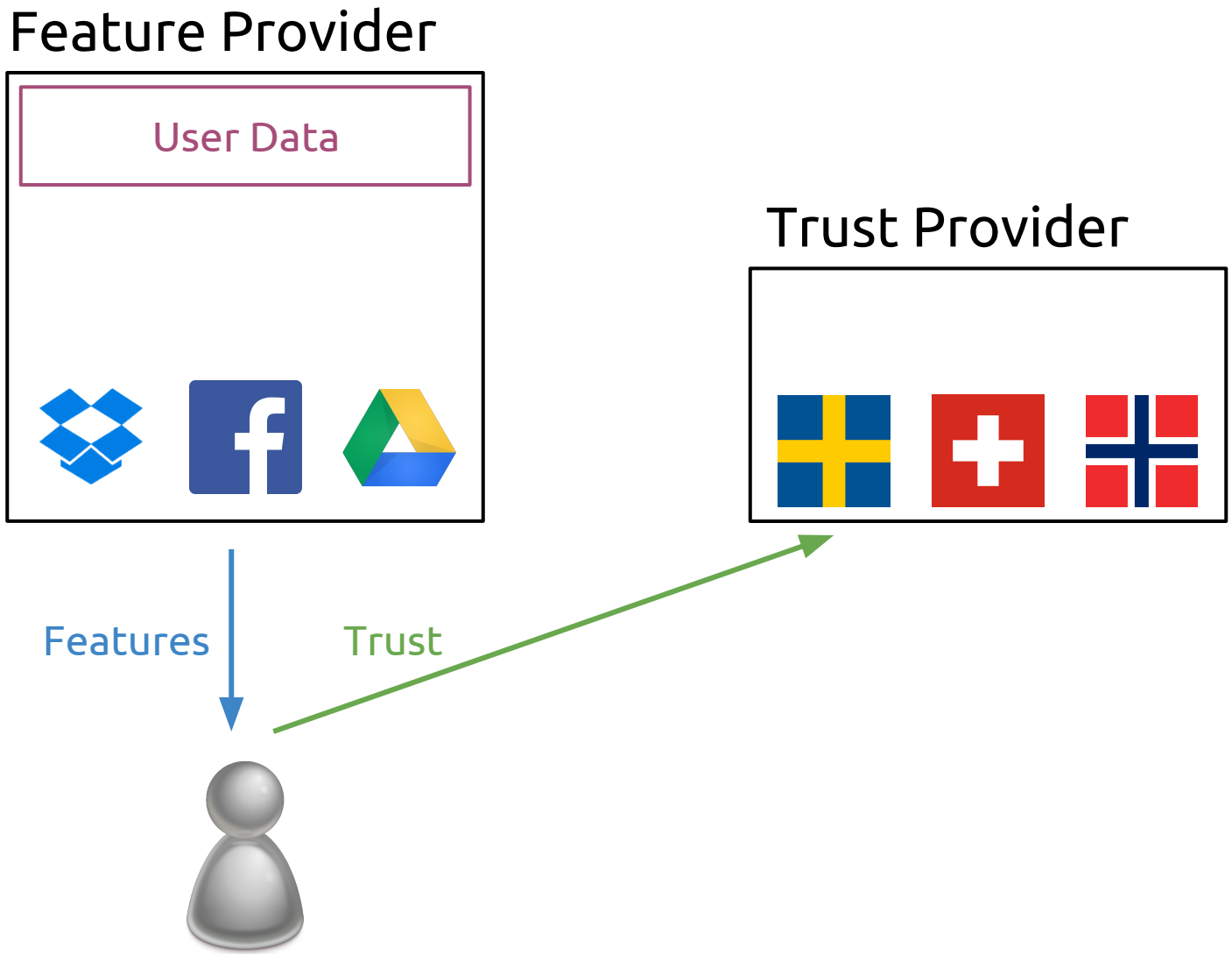


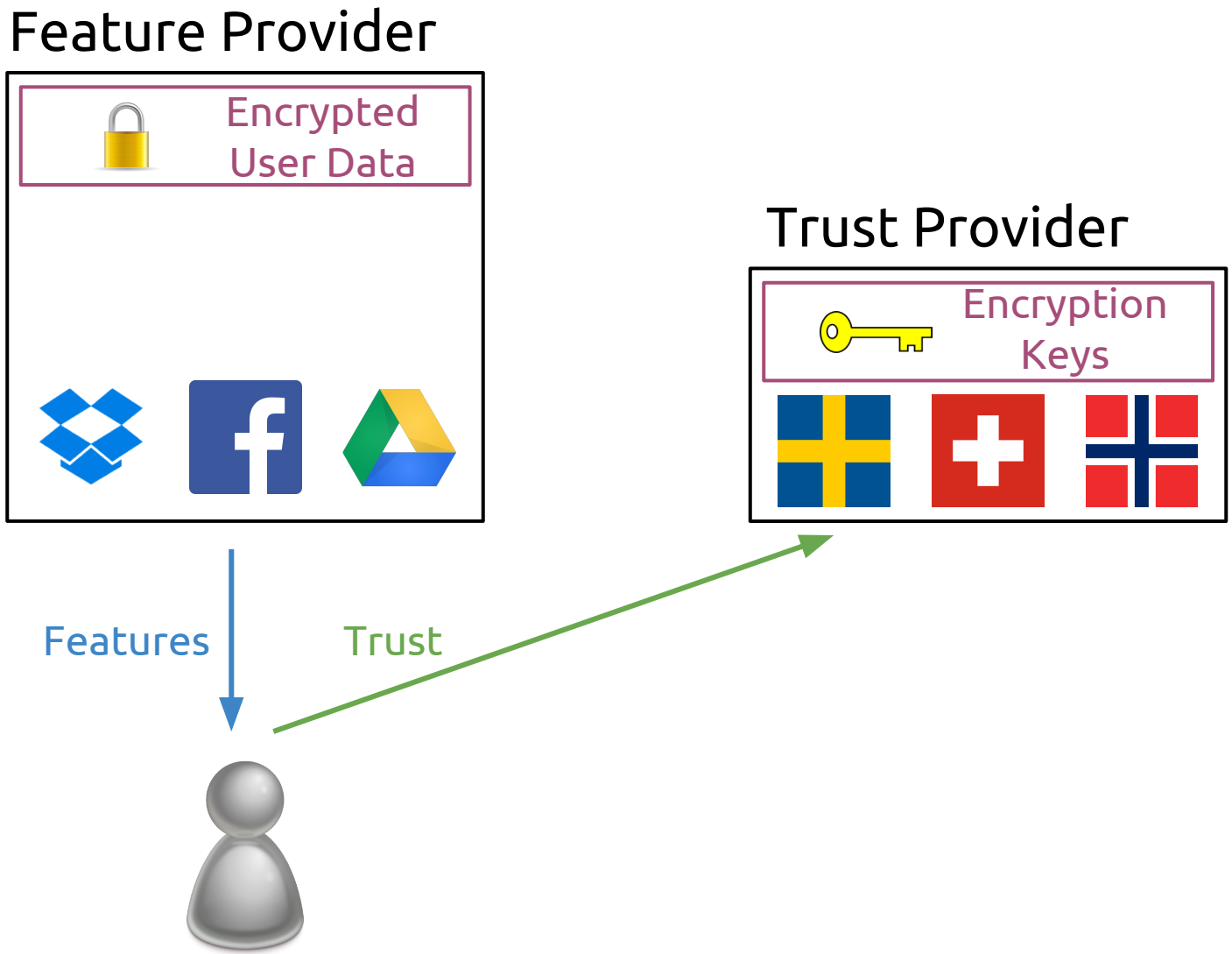


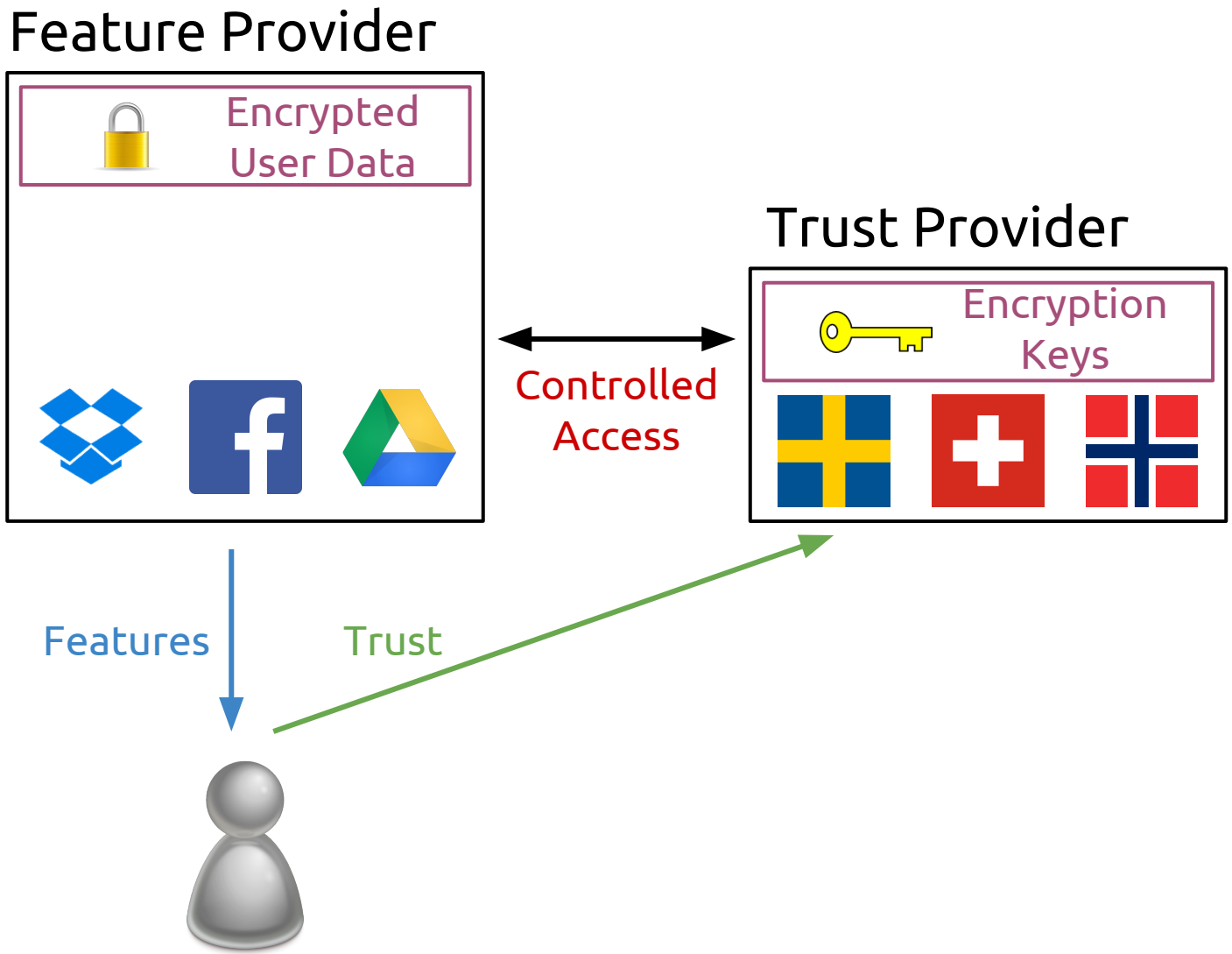
Centralization

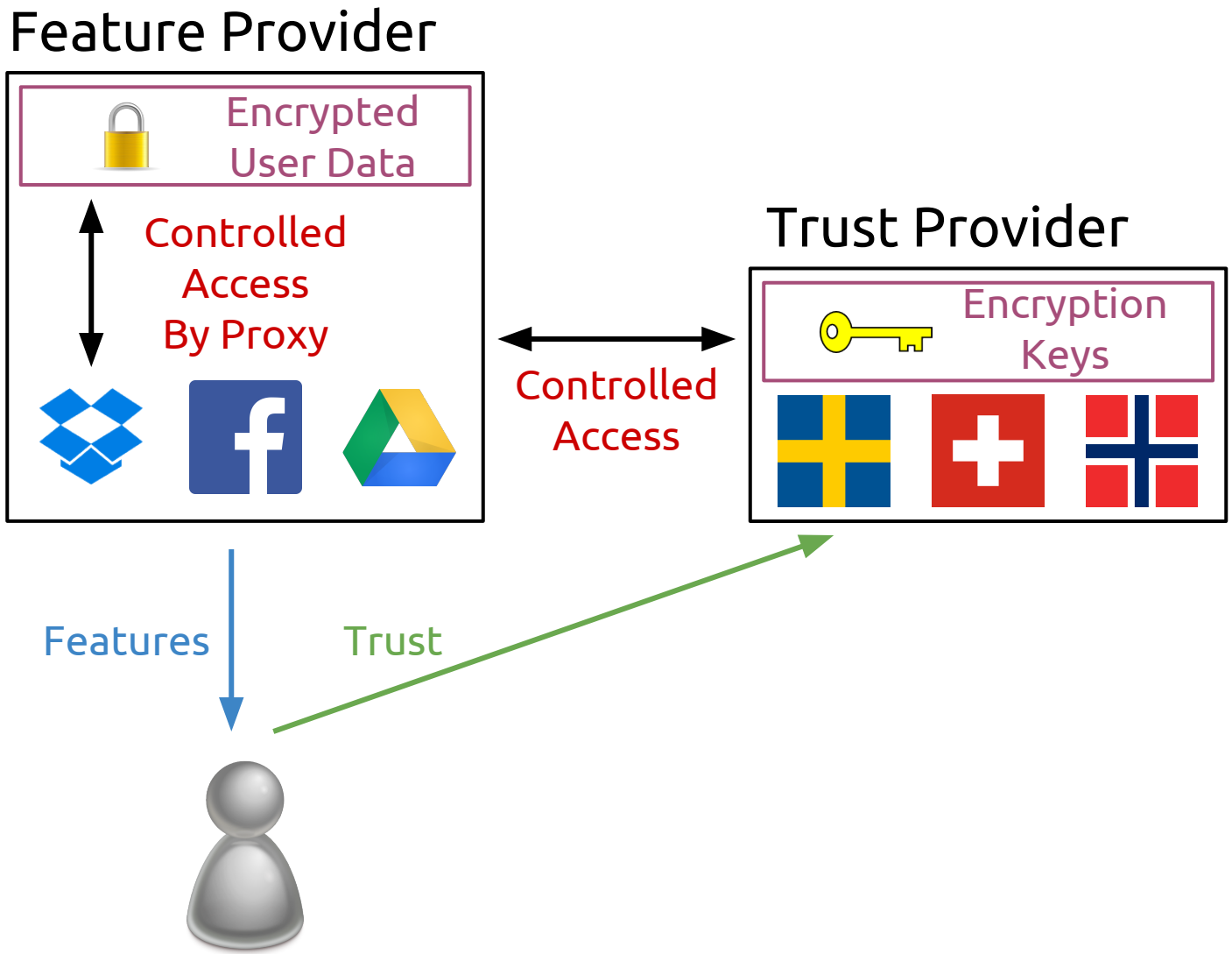

Feature Provider
User Data
Unrestricted Access
Features
Trust

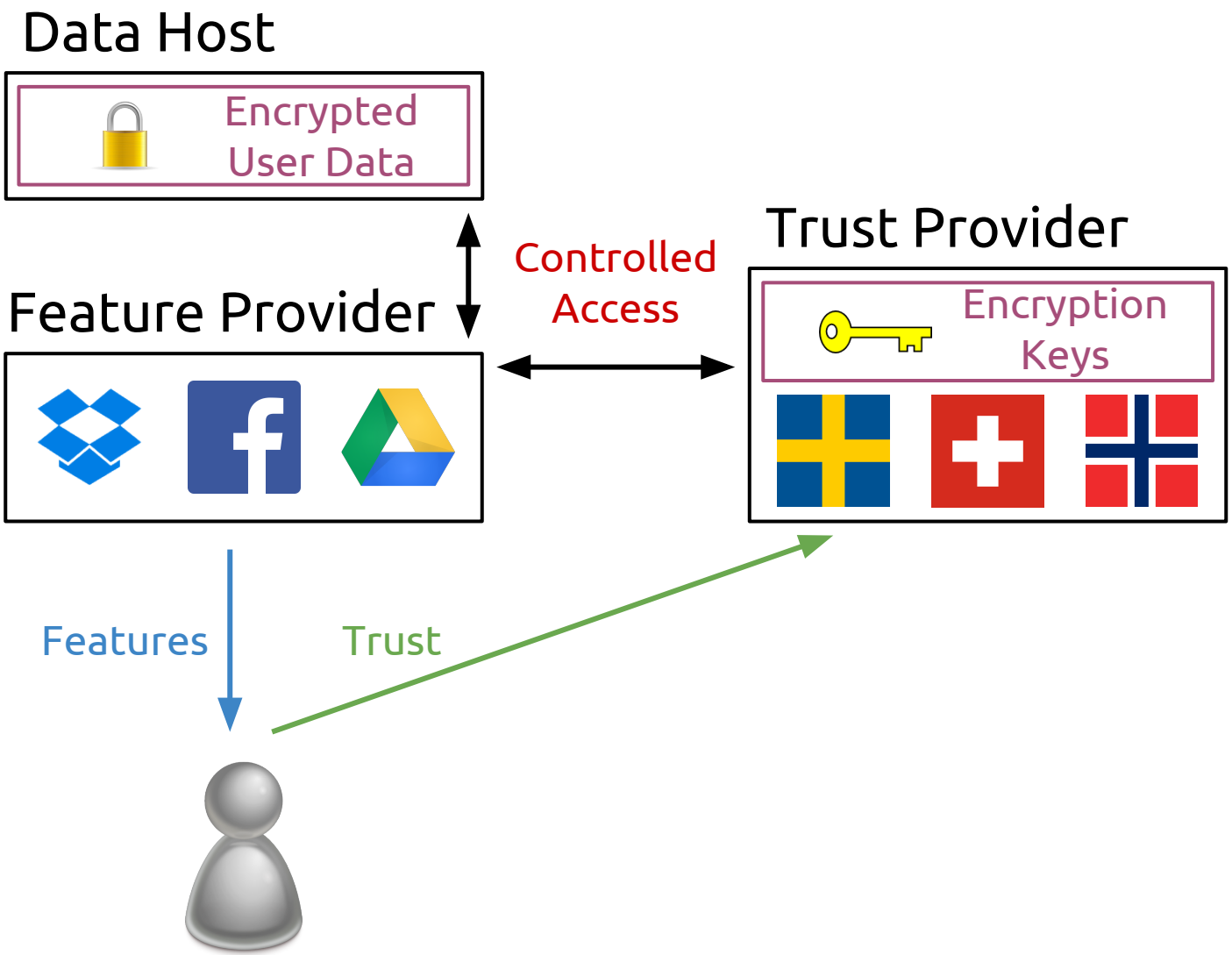

Feature Provider
User Data
Features
Trust


Feature Provider
User Data
Trust Provider
Features
Trust


Feature Provider
Encrypted
User Data
Trust Provider
Encryption
Keys
Features
Trust


Feature Provider
Encrypted
User Data
Trust Provider
Encryption
Keys
Controlled
Access
Features
Trust


Feature Provider
Encrypted
User Data
Controlled
Access
By Proxy
Controlled
Access
Trust Provider
Encryption
Keys
Features
Trust


Data Host
Encrypted
User Data
Feature Provider
Controlled
Access
Trust Provider
Encryption
Keys
Features
Trust

Custos

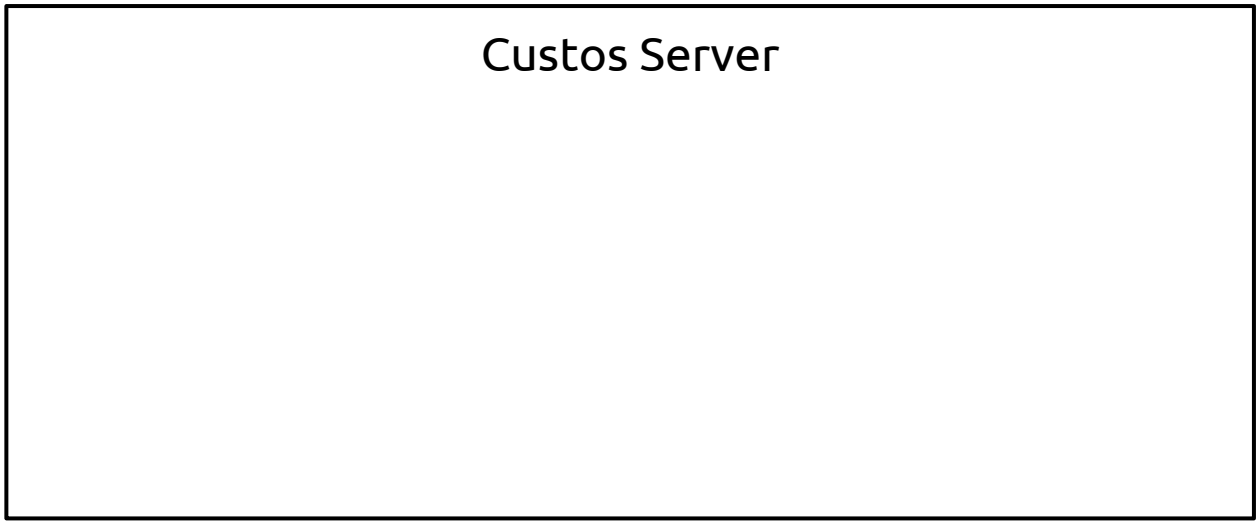
“Secret Storage as a Service”

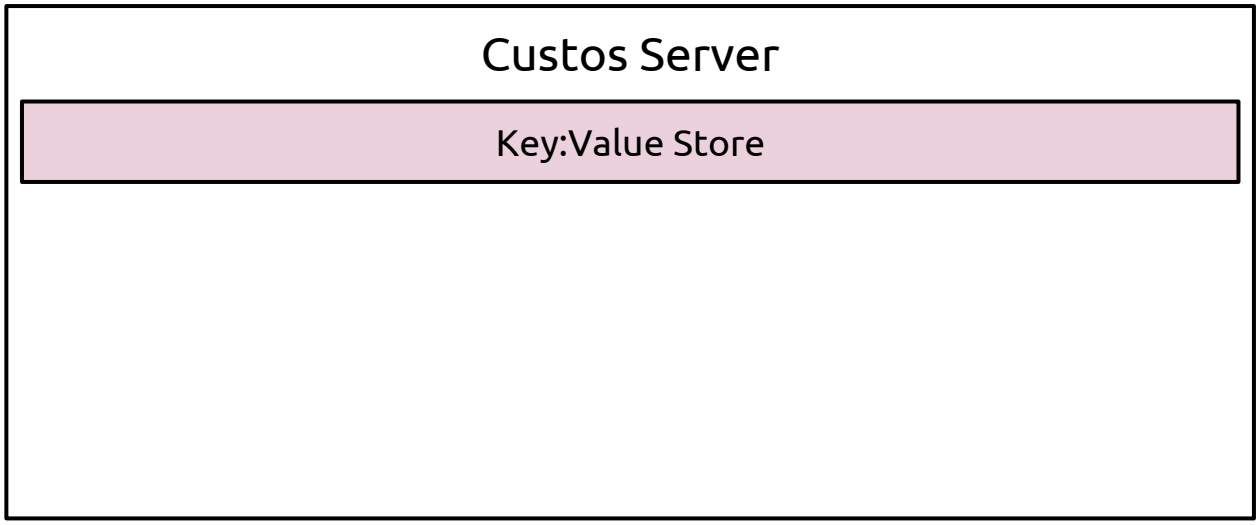
“Key Storage as a Service”

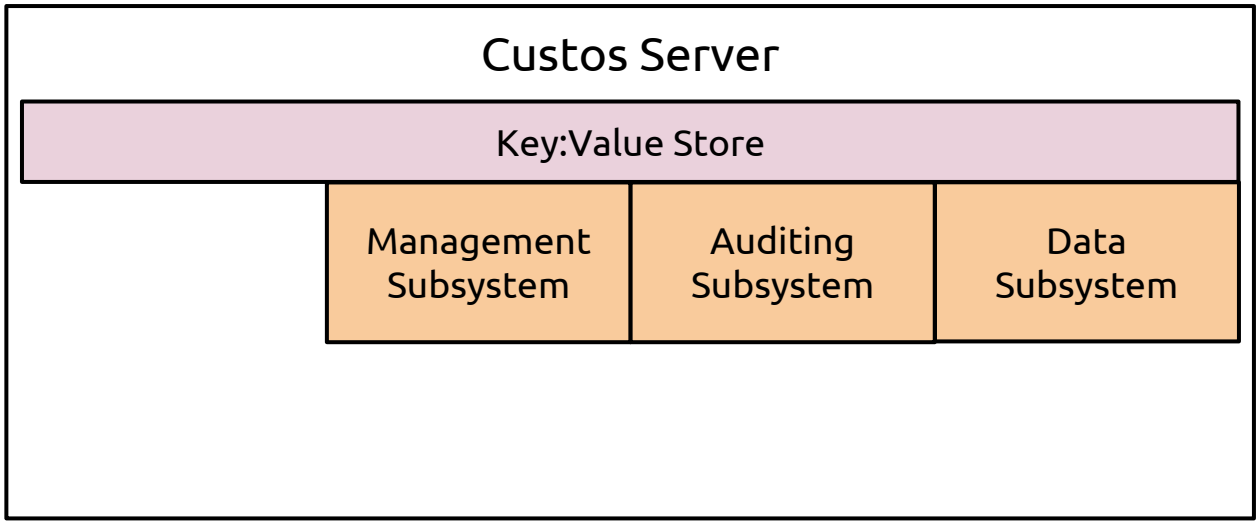
Central Key:Value Storage

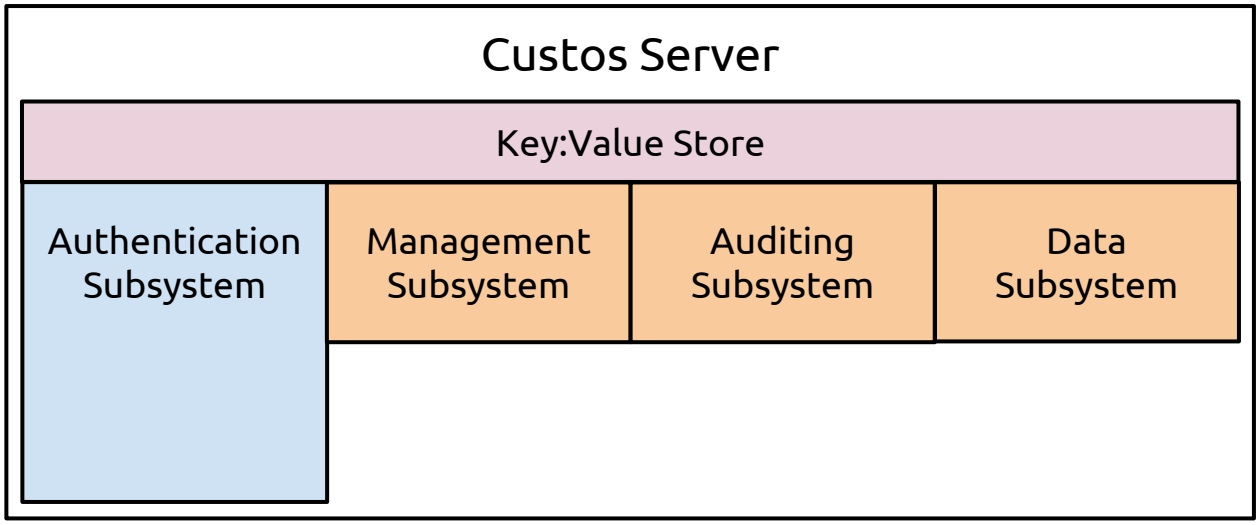
Flexible Access Control

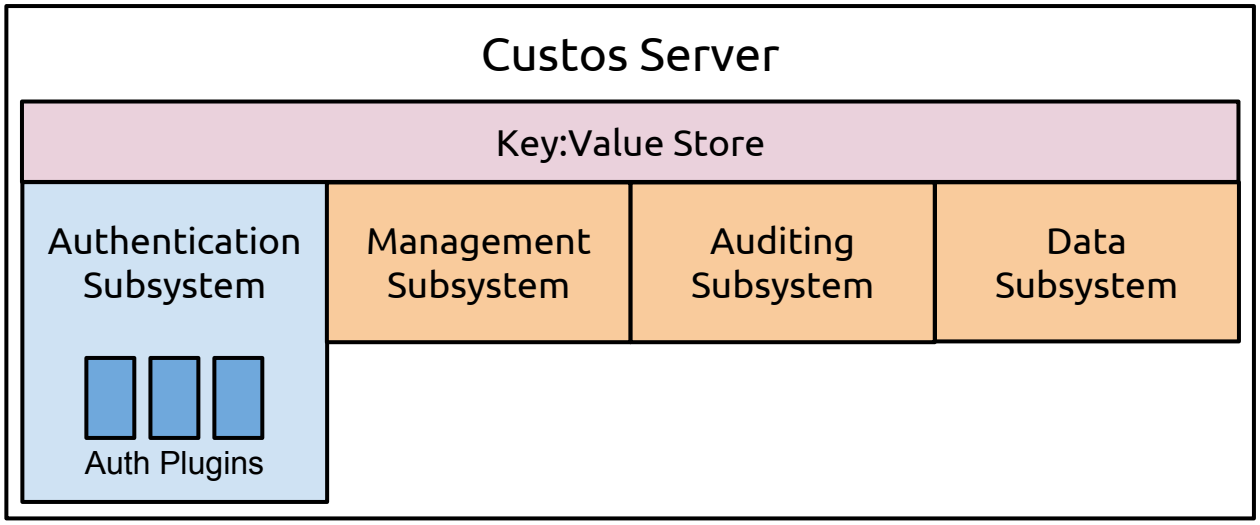
Access Auditing

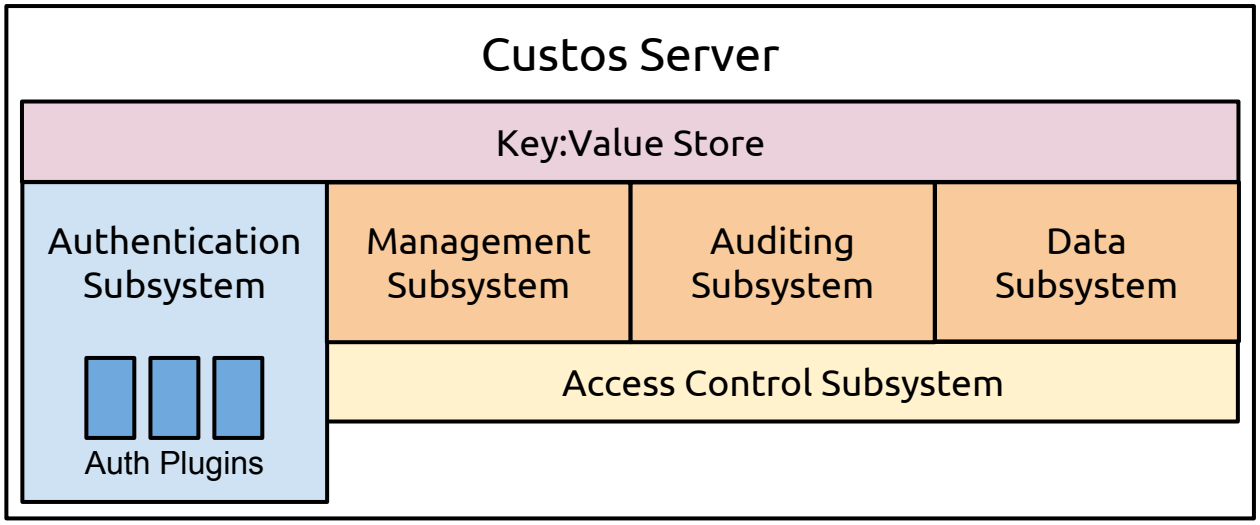

Custos Server

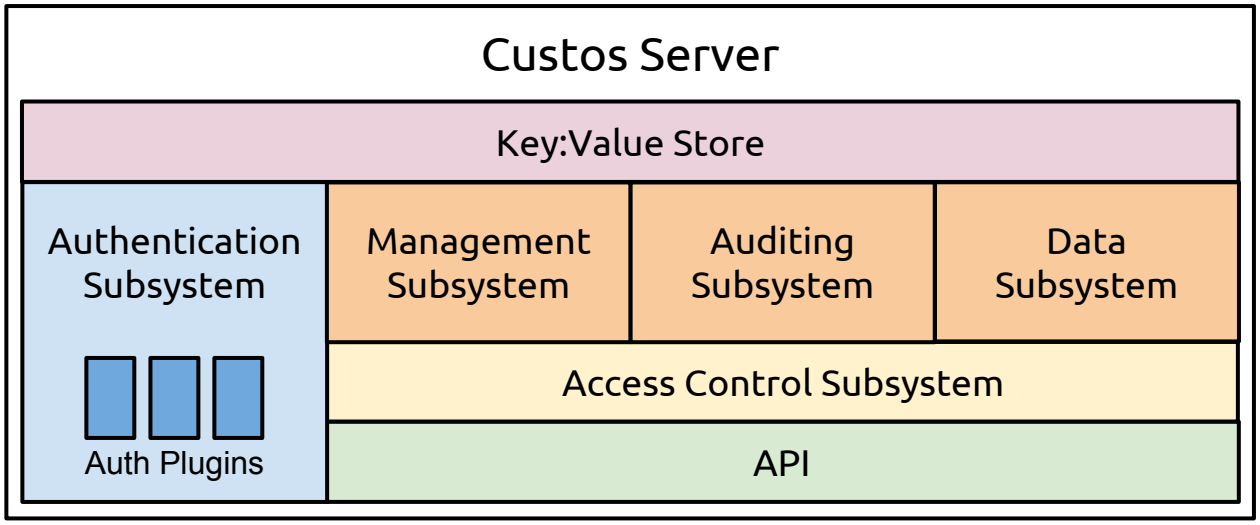

Custos Server
Key:Value Store

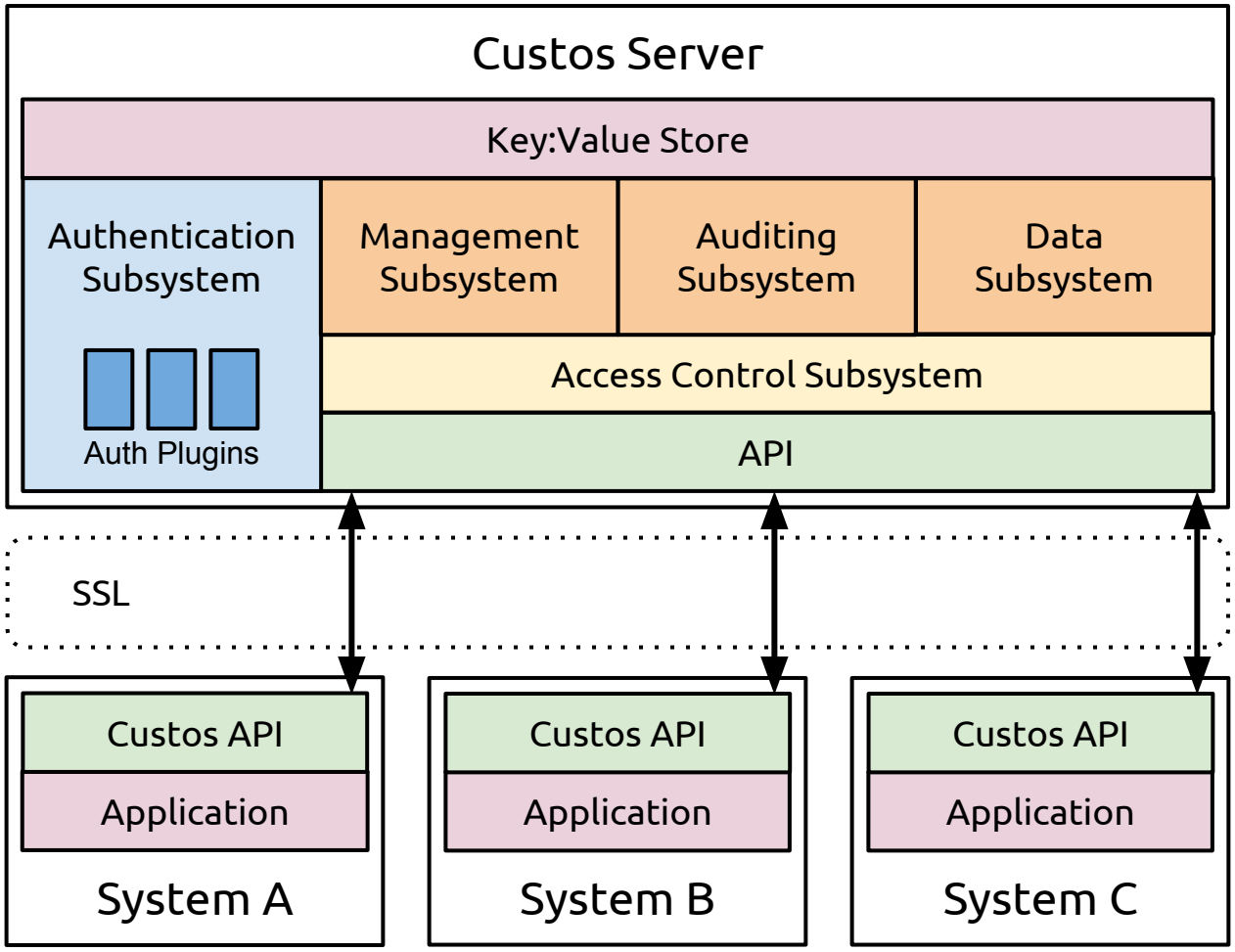

Custos Server
Key:Value Store
Management Subsystem
Auditing Subsystem
Data Subsystem


Custos Server
Key:Value Store
Authentication Subsystem
Management Subsystem
Auditing Subsystem
Data Subsystem


Custos Server
Key:Value Store
Authentication Subsystem
Auth Plugins
Management Subsystem
Auditing Subsystem
Data Subsystem

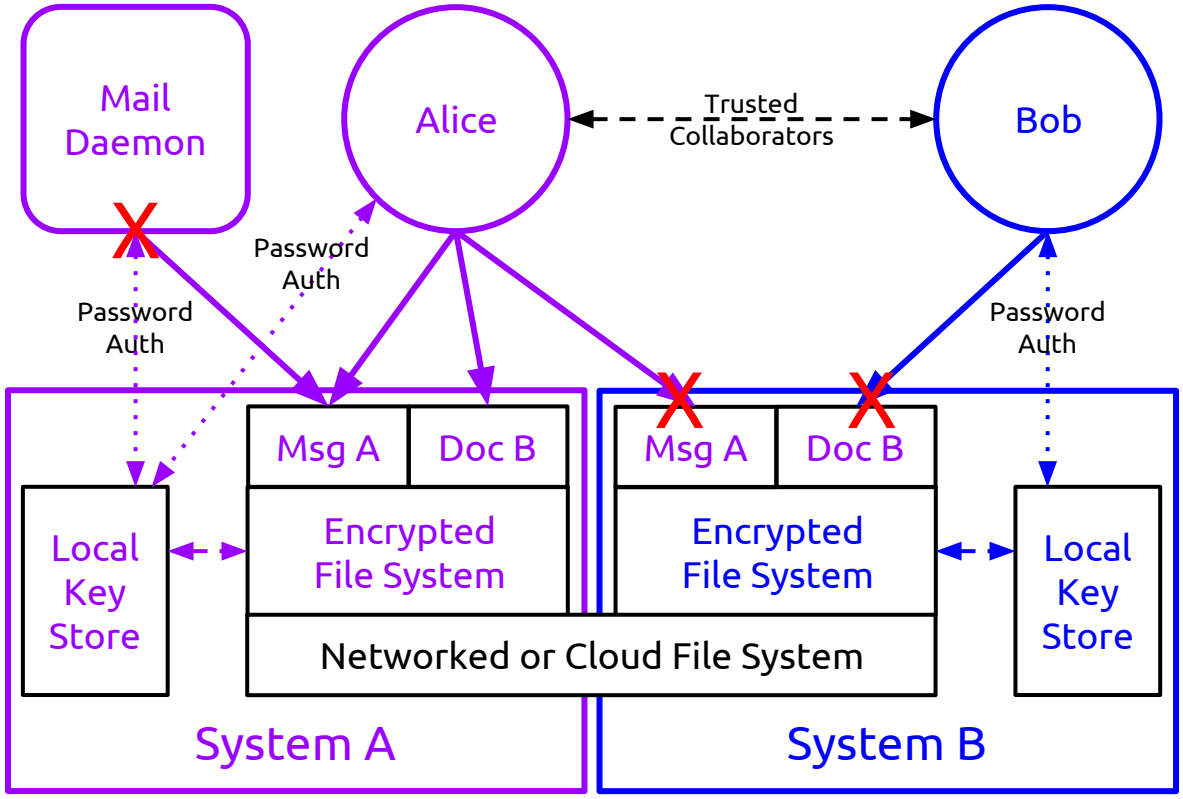

Custos Server
Key:Value Store
Authentication Subsystem
Auth Plugins
Management Subsystem
Auditing Subsystem
Data Subsystem
Access Control Subsystem

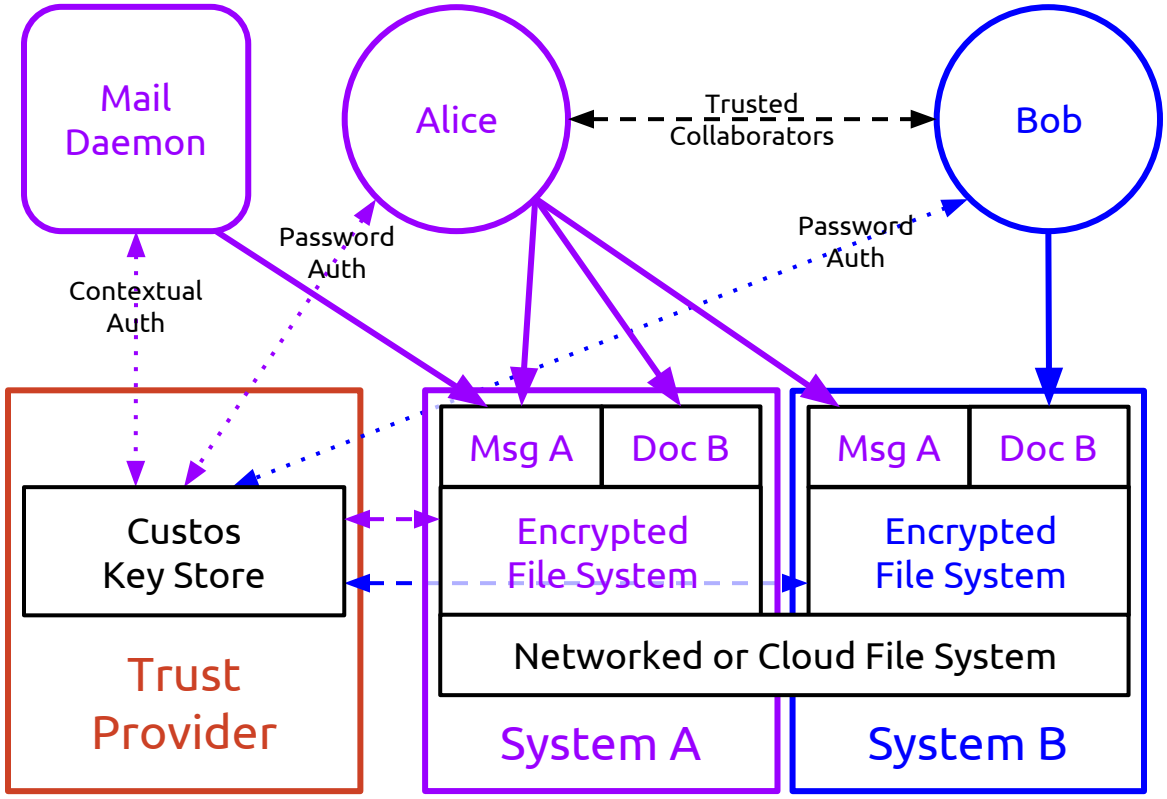

Custos Server
Key:Value Store
Authentication Subsystem
Auth Plugins
Management Subsystem
Auditing Subsystem
Data Subsystem
Access Control Subsystem
API


Custos Server
Key:Value Store
Authentication Subsystem
Auth Plugins
Management Subsystem
Auditing Subsystem
Data Subsystem
Access Control Subsystem
API
SSL
Custos API
Application
System A
Custos API
Application
System B
Custos API
Application
System C

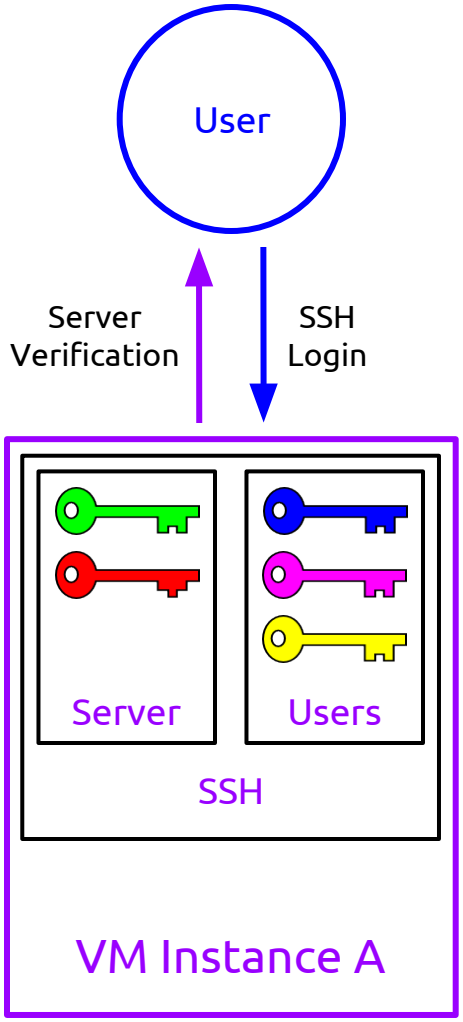
Application Domains

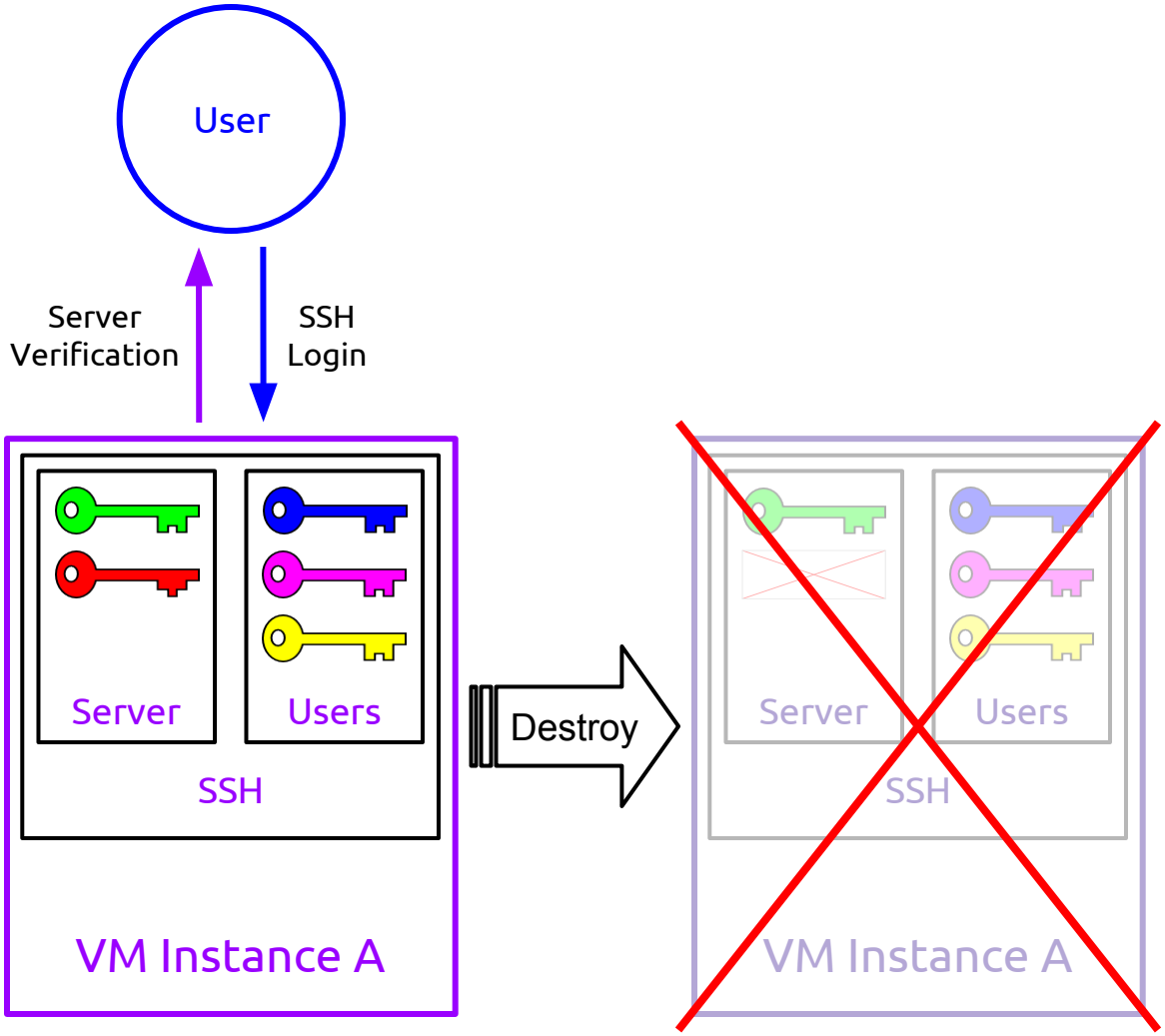
File Systems

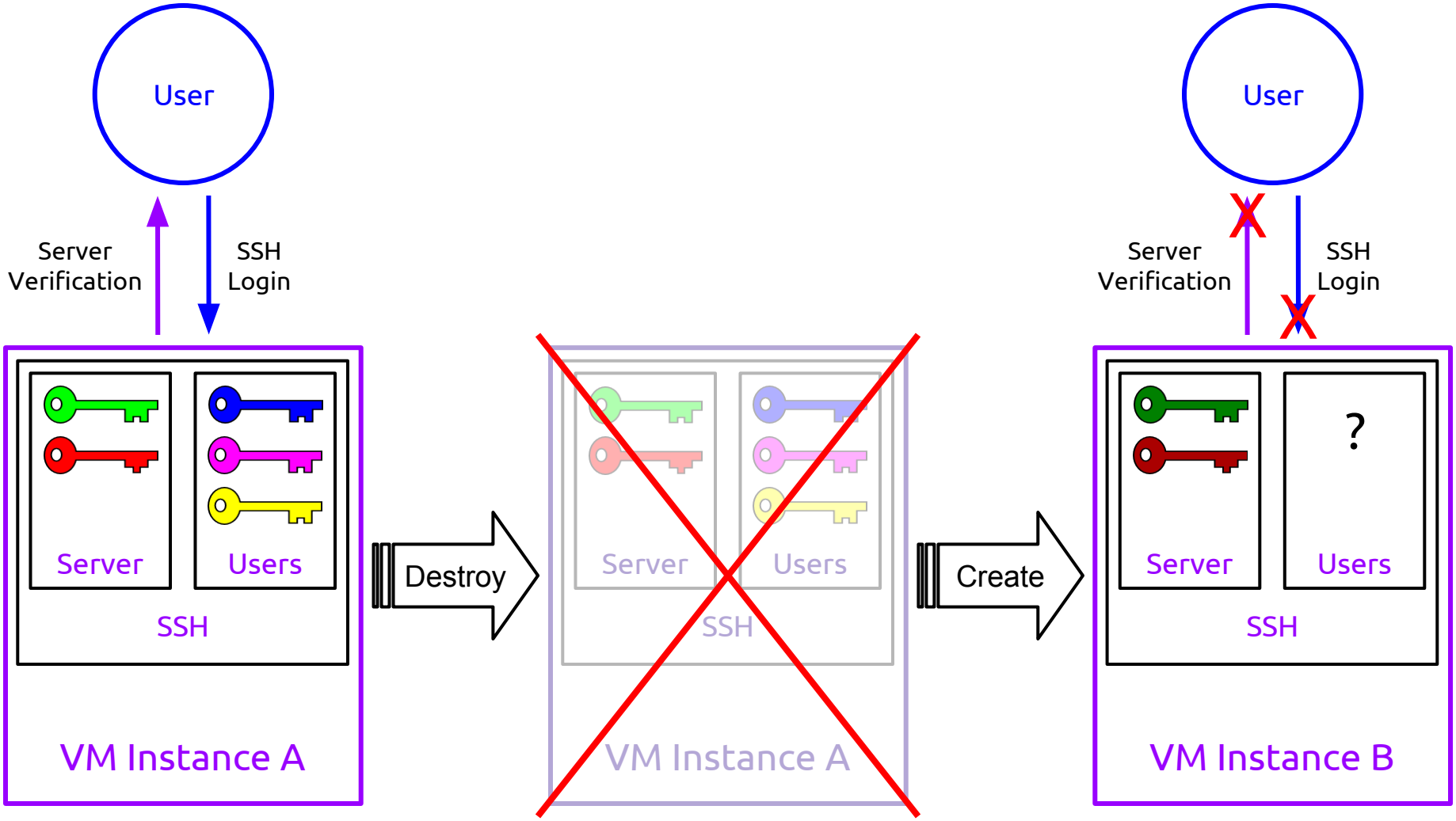

Mail Daemon
Alice
Trusted Collaborators
Bob
Password Auth
Password Auth
Password Auth
Msg A
Doc B
Msg A
Doc B
Local Key Store
Encrypted File System
Encrypted File System
Local Key Store
Networked or Cloud File System
System A
System B

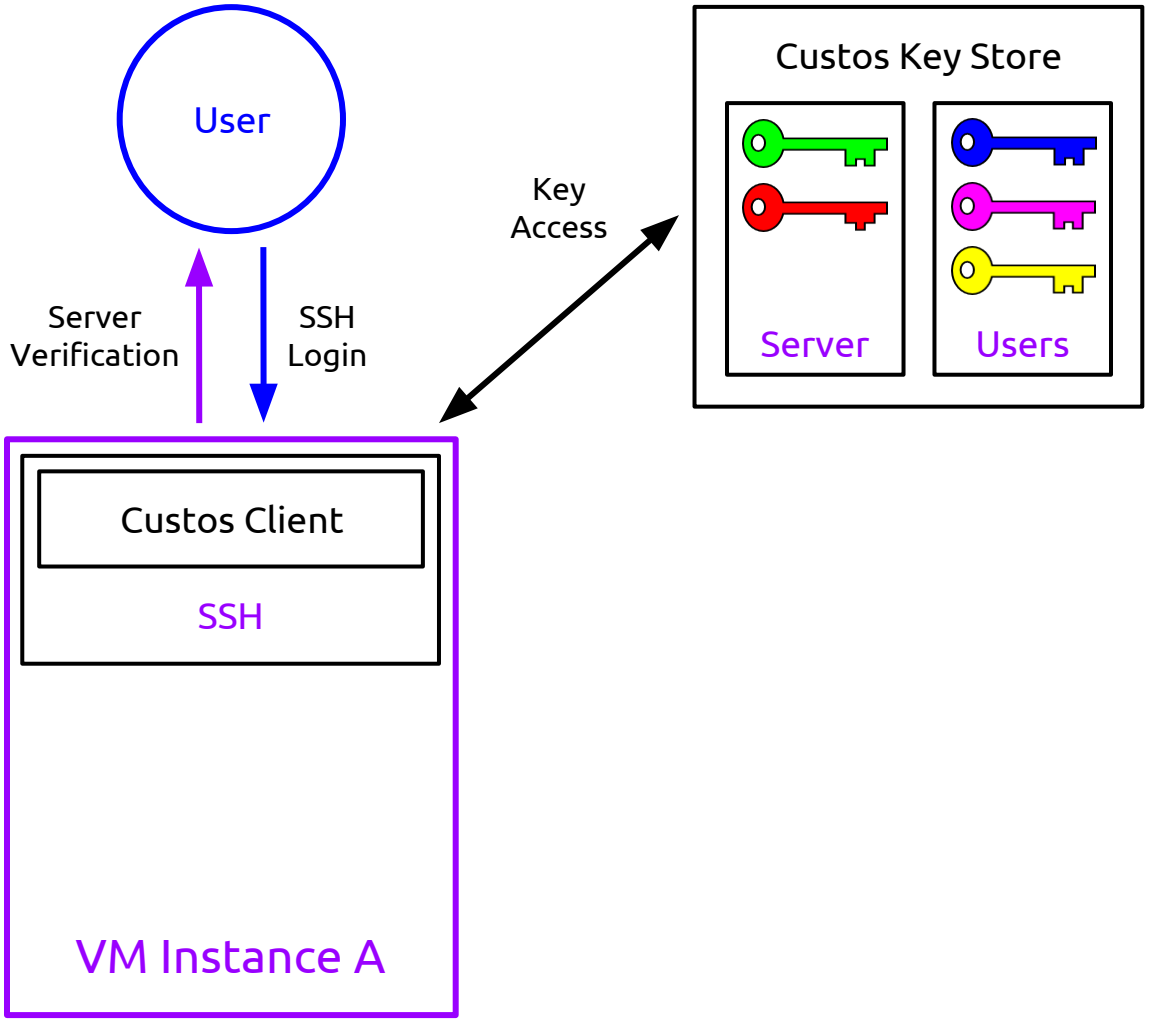

Mail Daemon
Alice
Trusted Collaborators
Bob
Password Auth
Password Auth
Contextual Auth
Msg A
Doc B
Msg A
Doc B
Custos Key Store
Encrypted File System
Encrypted File System
Networked or Cloud File System
Trust Provider
System A
System B

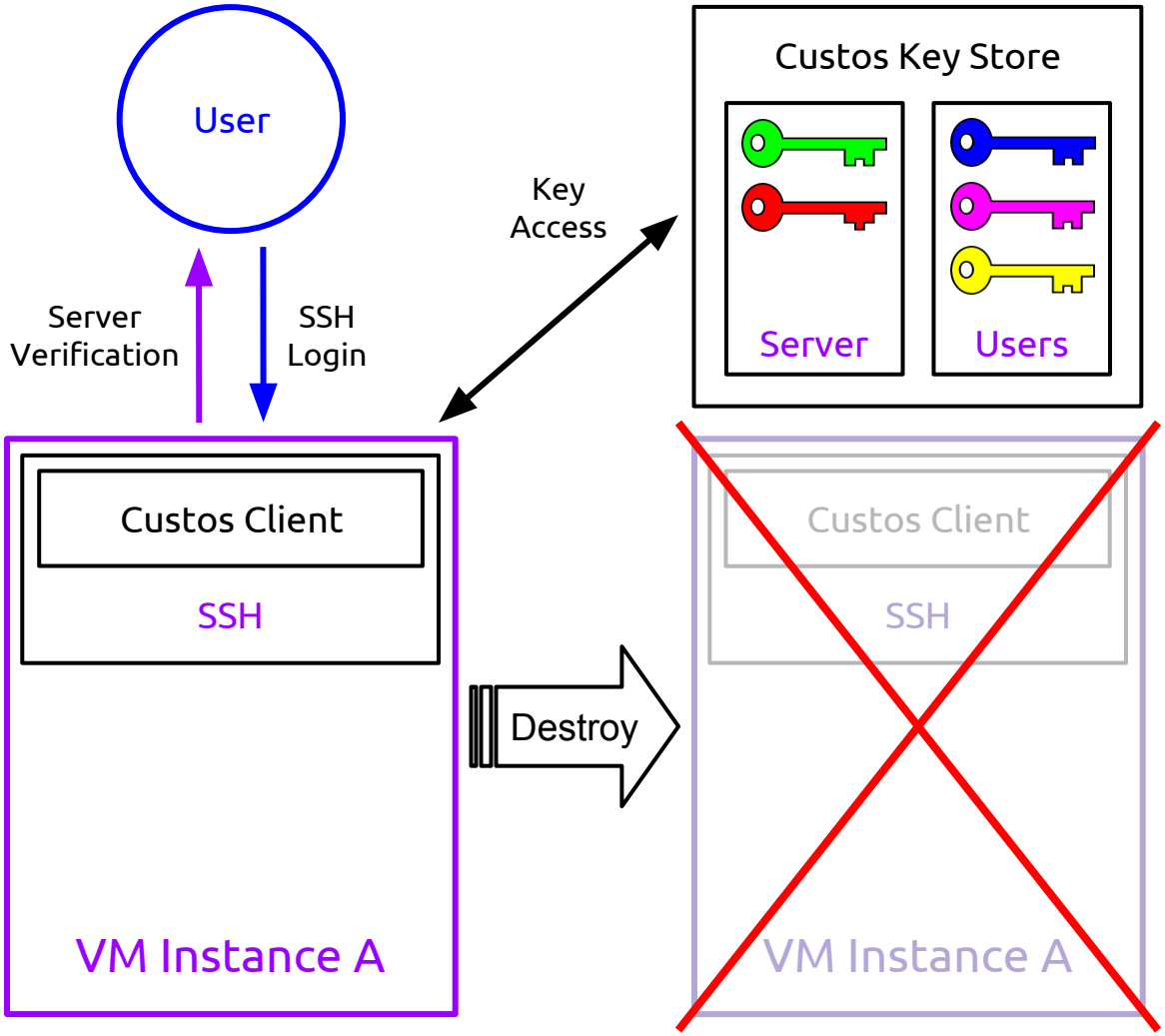
Data Centers

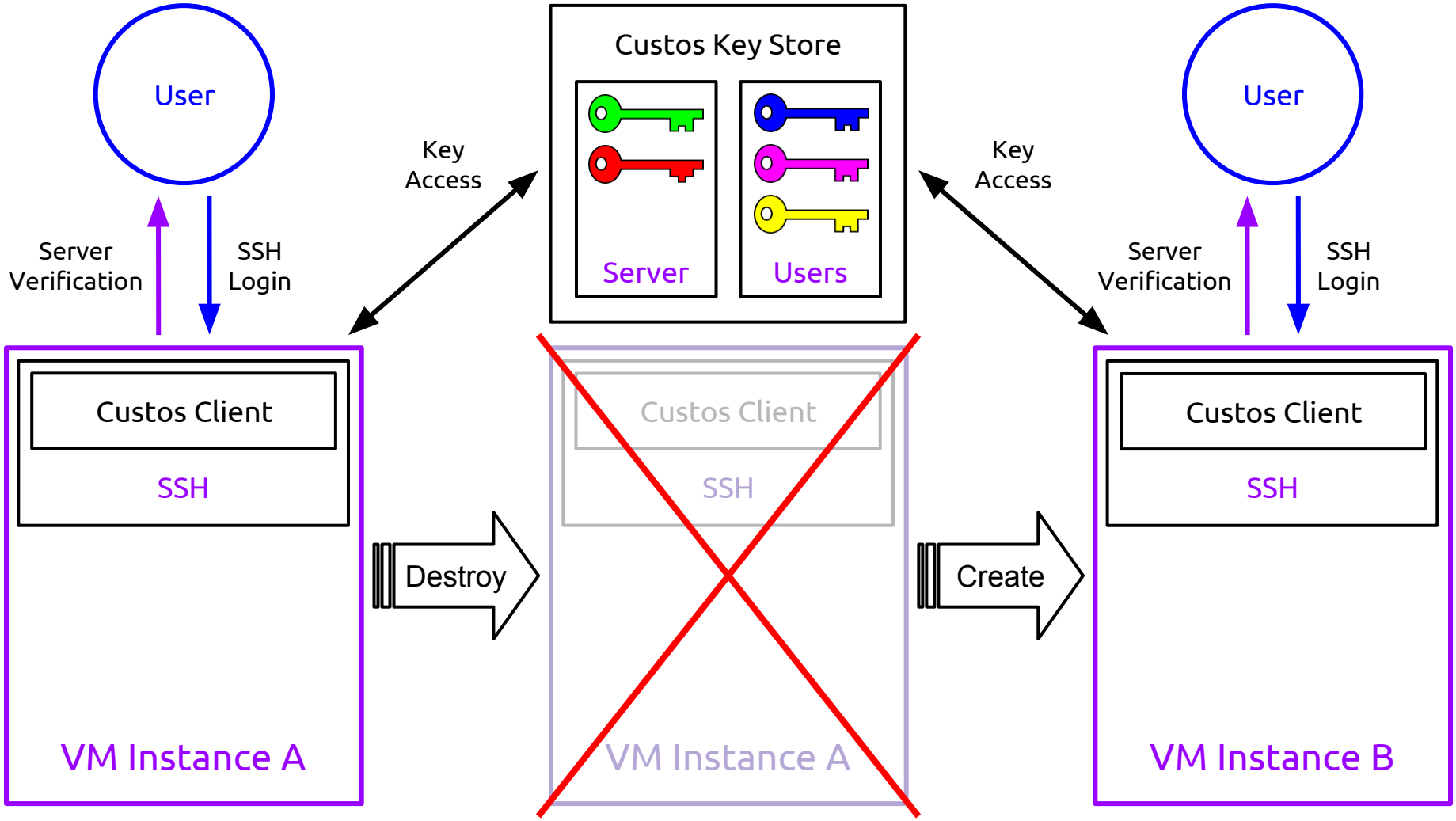

User
Server
Verification
SSH
Login
Server
Users
SSH
VM Instance A


User
Server Verification
SSH Login
Server
Users
SSH
VM Instance A
Destroy
Server
Users
SSH
VM Instance A


User
Server Verification
SSH Login
Server
Users
SSH
VM Instance A
Destroy
Server
Users
SSH
VM Instance A
Create
User
Server Verification
SSH Login
Server
?
Users
SSH
VM Instance B


User
Server
Verification
SSH
Login
Key
Access
Custos Key Store
Server
Users
Custos Client
SSH
VM Instance A


User
Server
Verification
SSH
Login
Key
Access
Custos Key Store
Server
Users
Custos Client
SSH
VM Instance A
Destroy
Custos Client
SSH
VM Instance A


User
Server Verification
SSH Login
Key Access
Custos Key Store
Server
Users
Key Access
User
Server Verification
SSH Login
Custos Client
SSH
VM Instance A
Destroy
Custos Client
SSH
VM Instance A
Create
Custos Client
SSH
VM Instance B

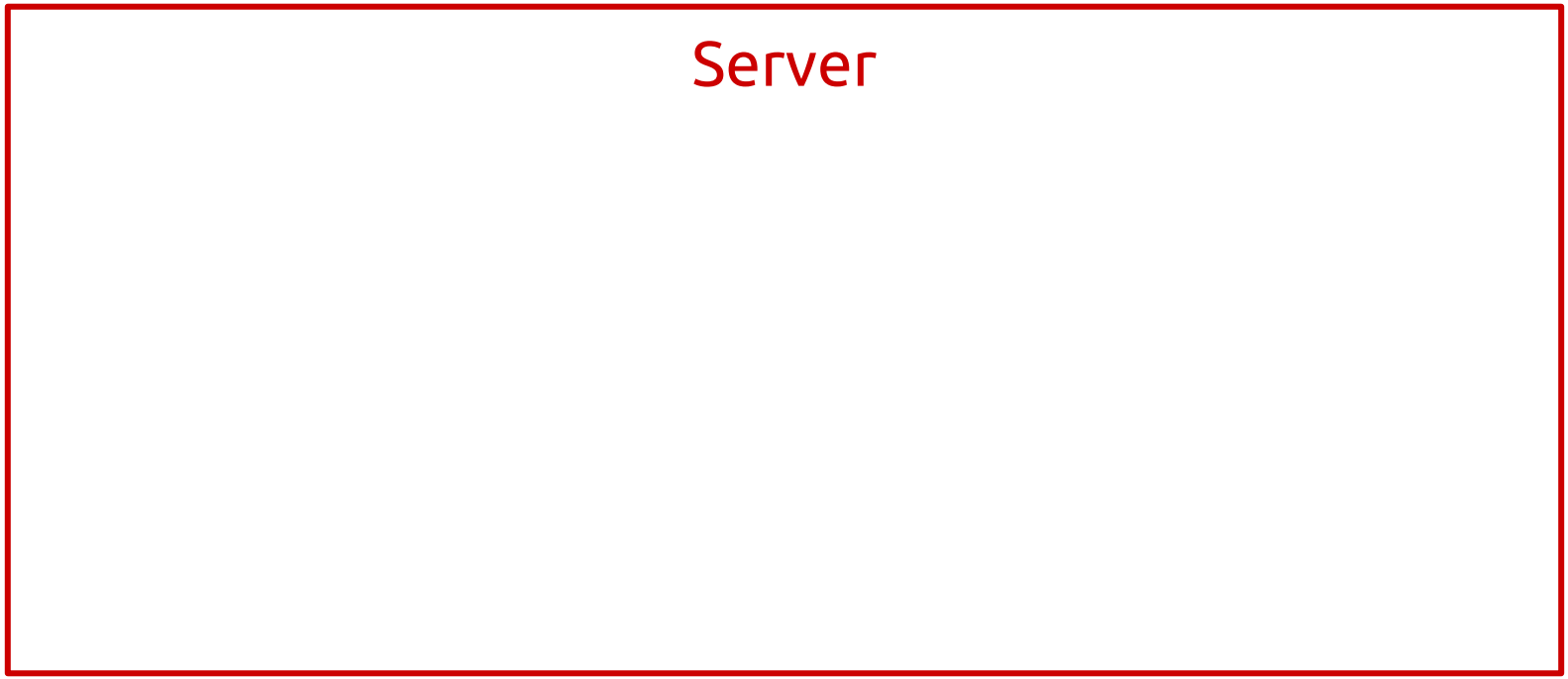
Password Management

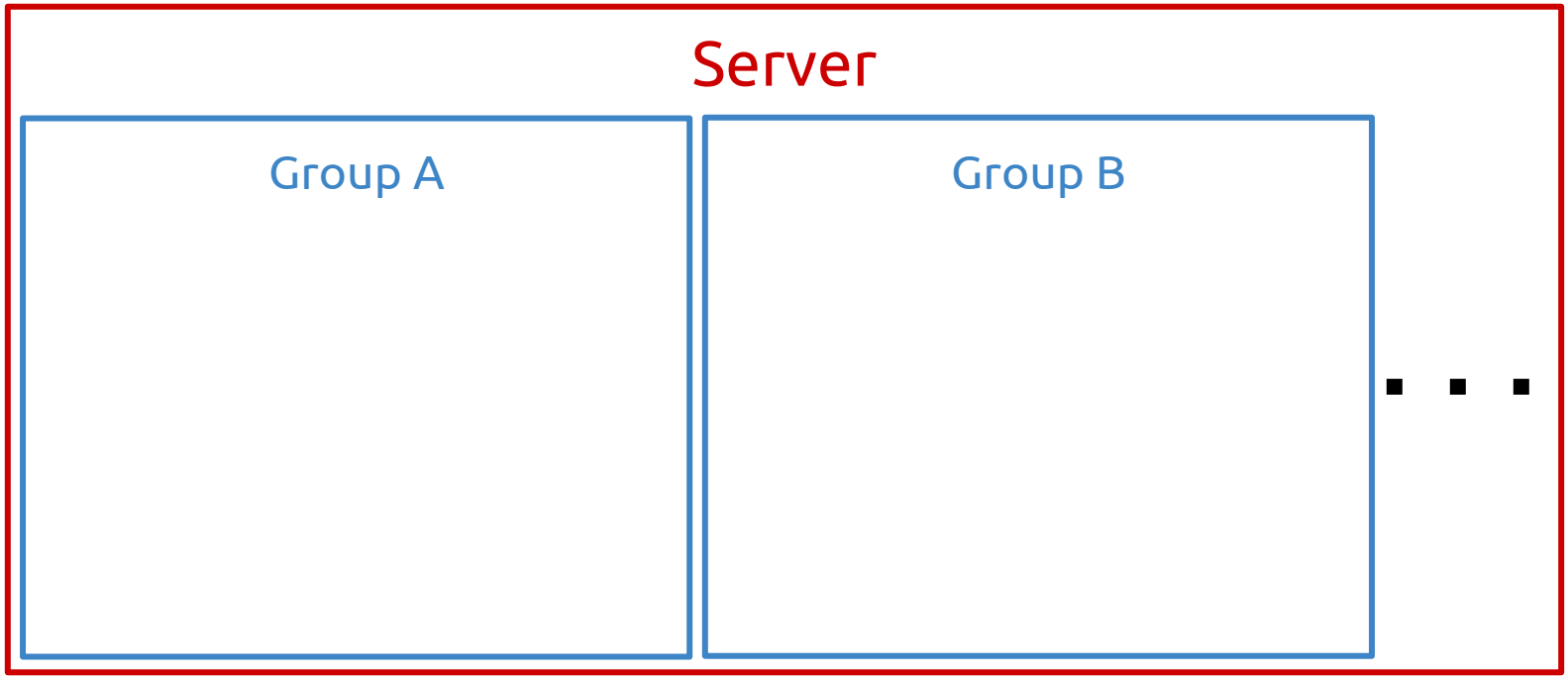
Personal Data Storage

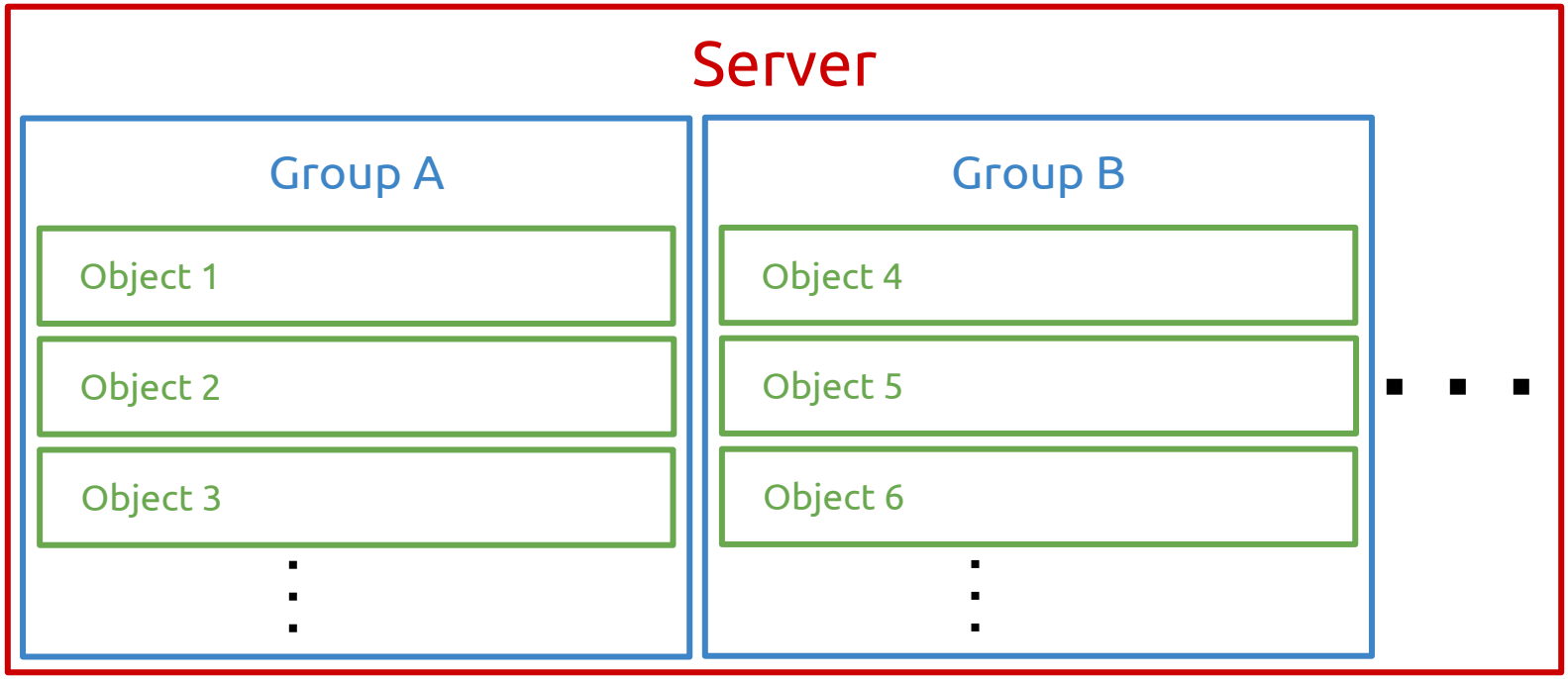
...

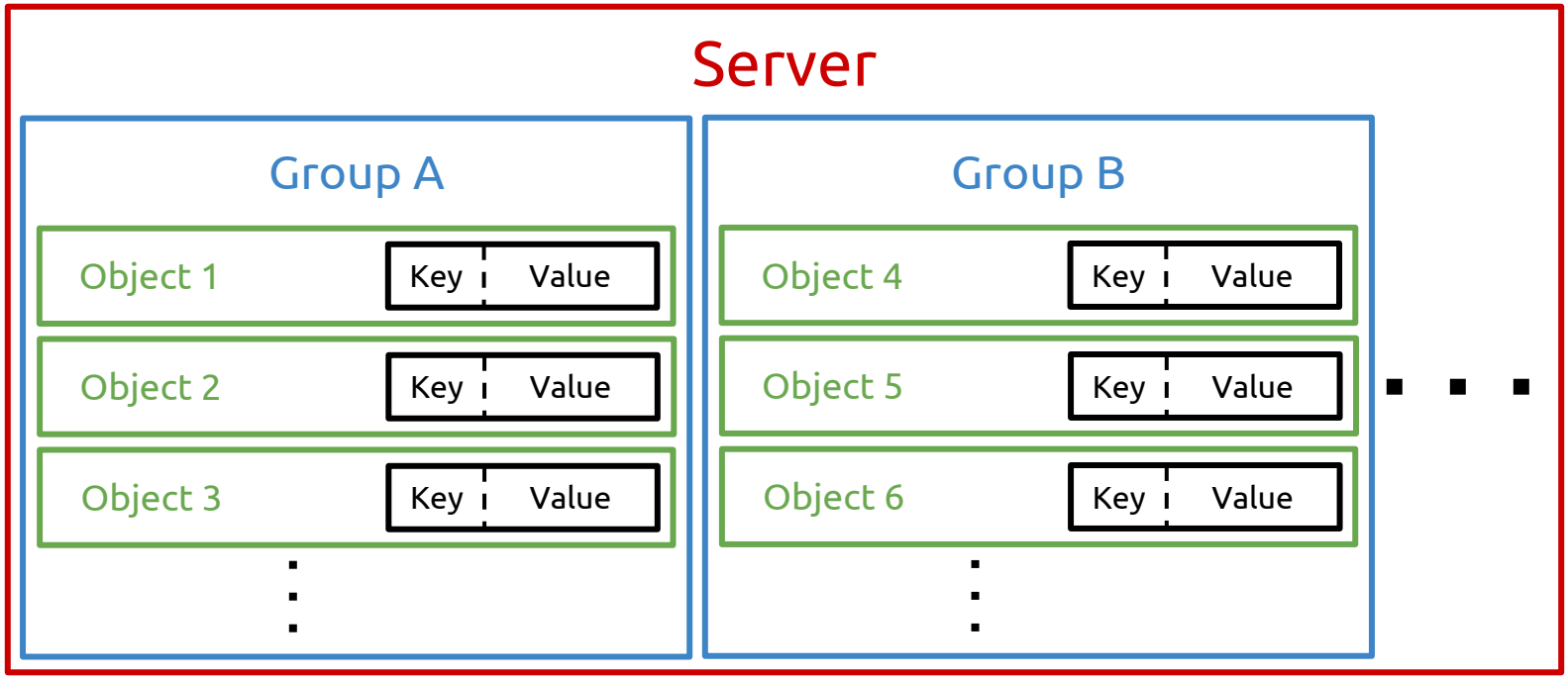
Custos Design

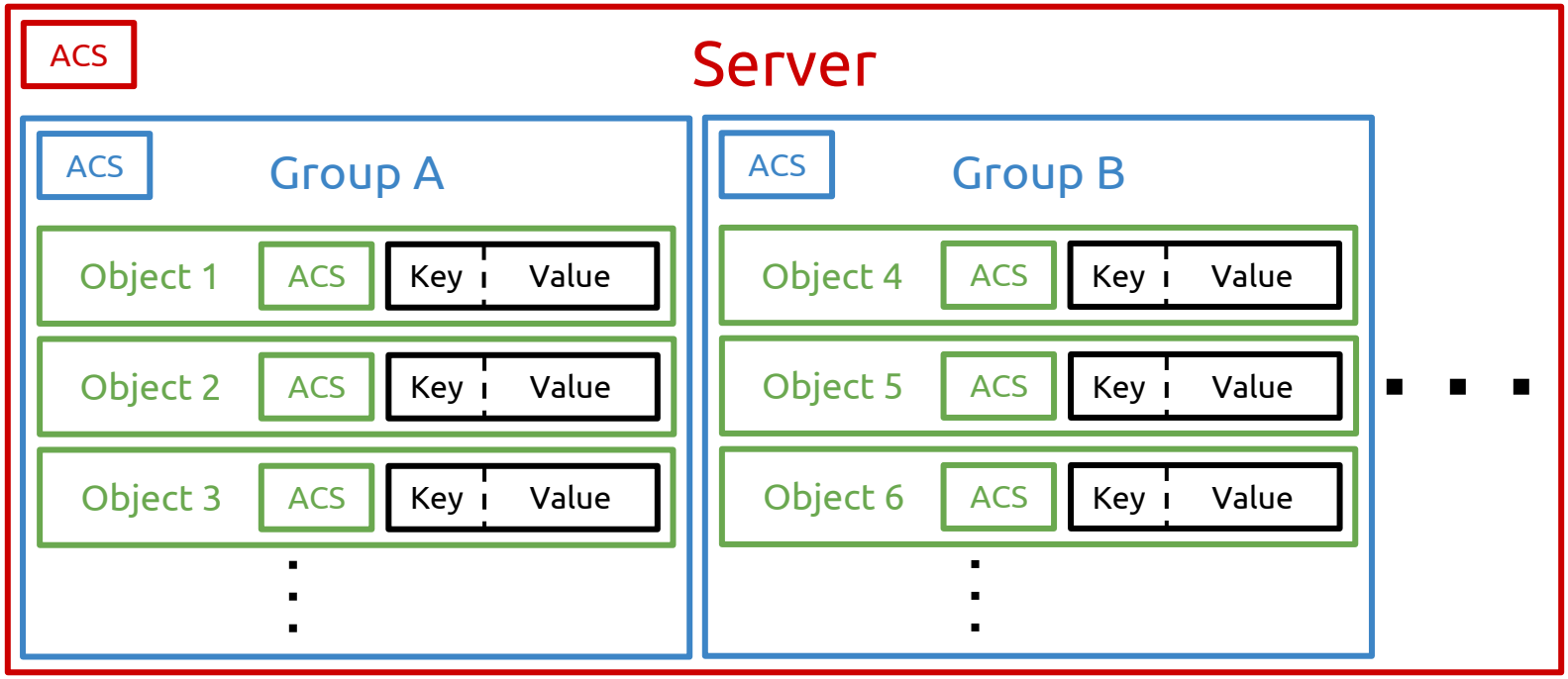
Organizational Units


Server

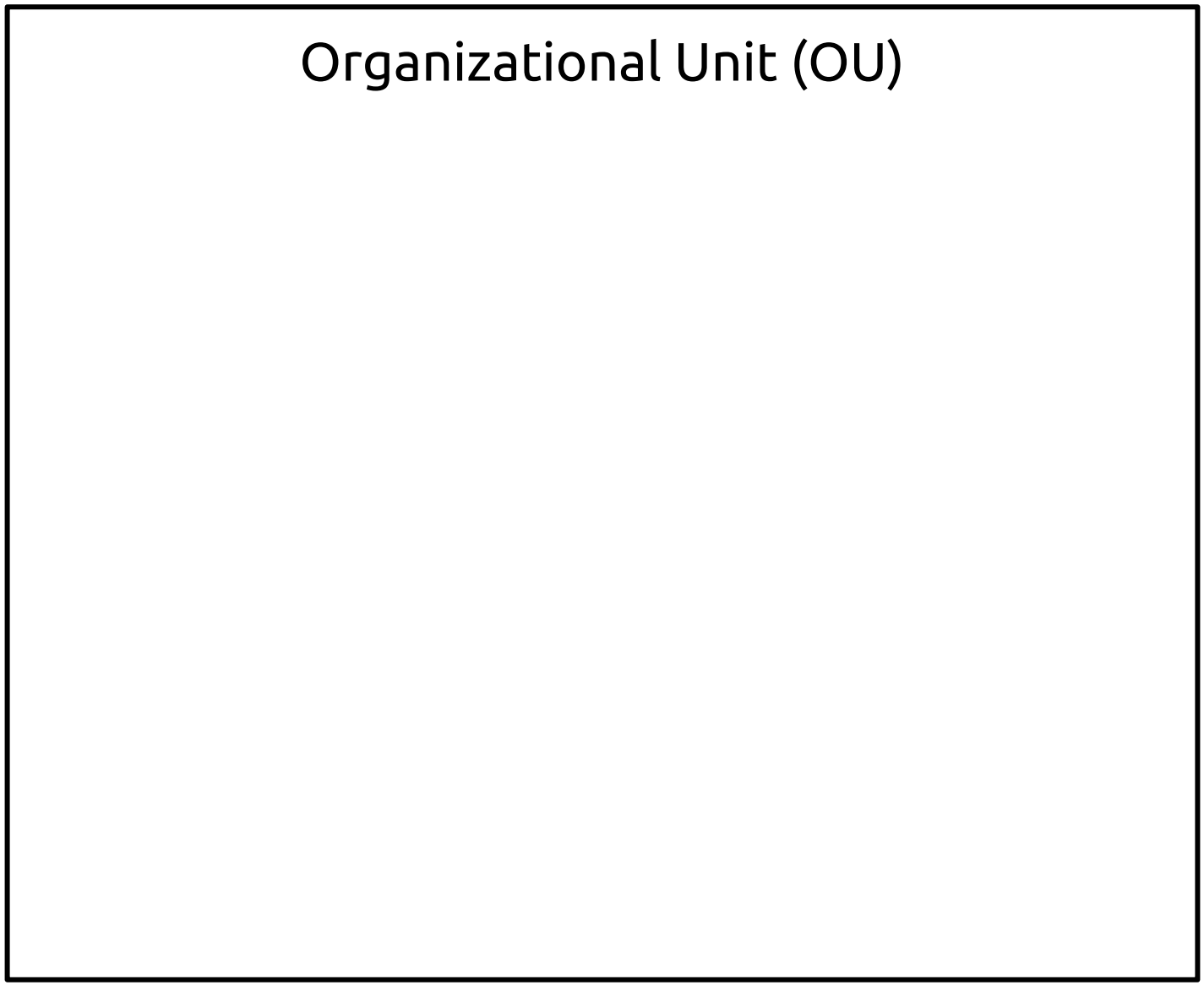

Server
Group A
Group B

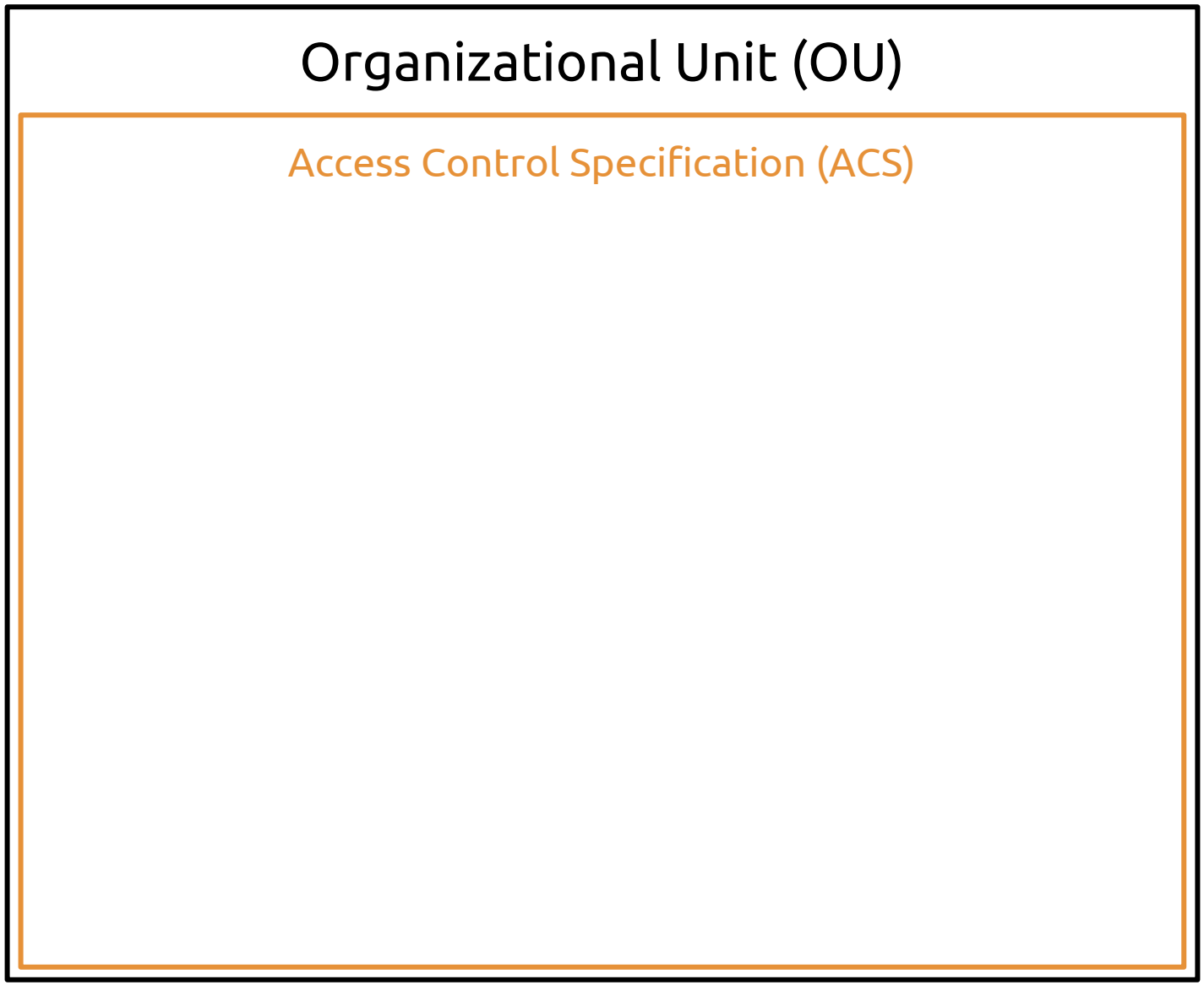

Server
Group A
Object 1
Object 2
Object 3
Group B
Object 4
Object 5
Object 6

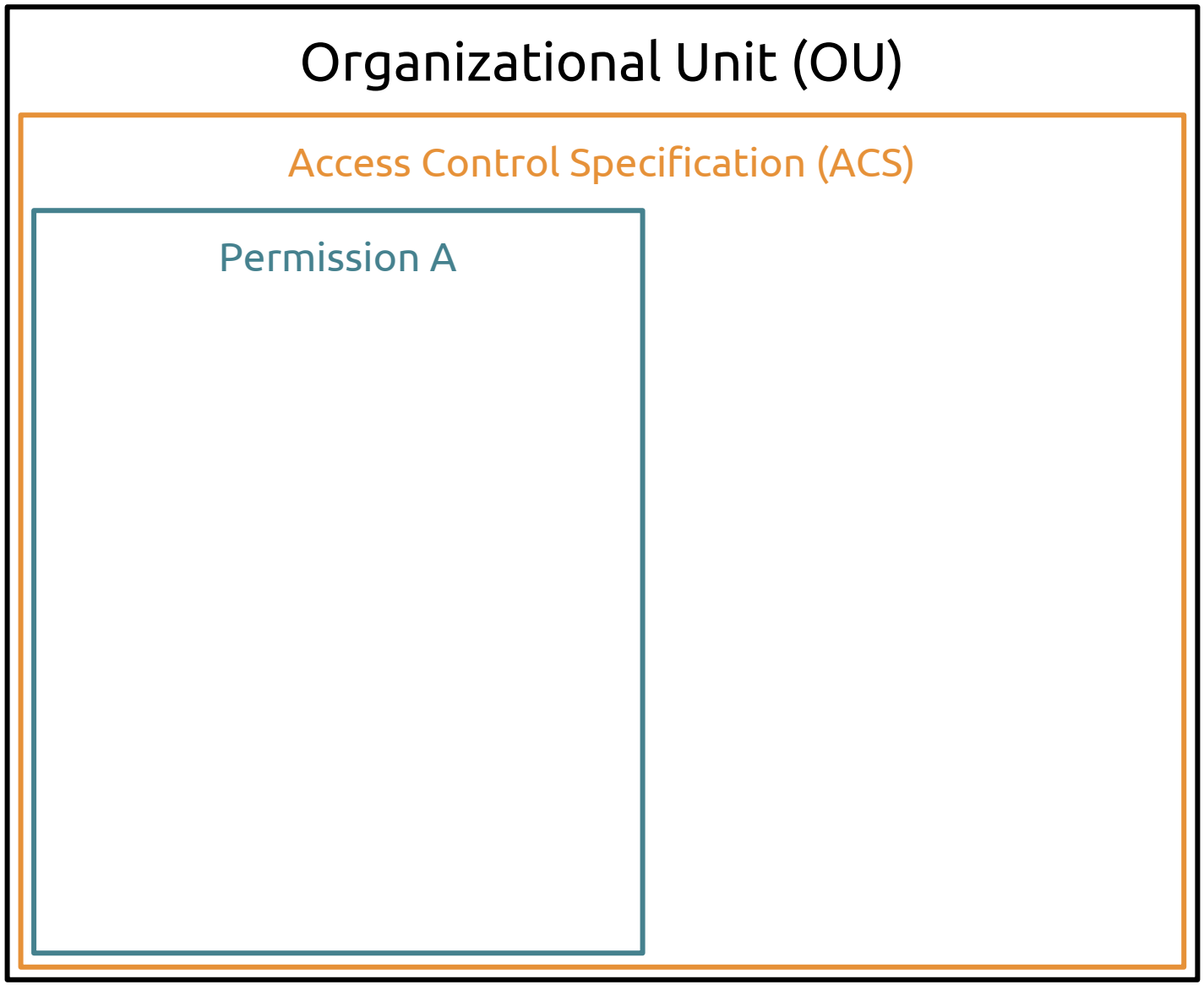

Server
Group A
Object 1
Key
Value
Object 2
Key
Value
Object 3
Key
Value
Group B
Object 4
Key
Value
Object 5
Key
Value
Object 6
Key
Value

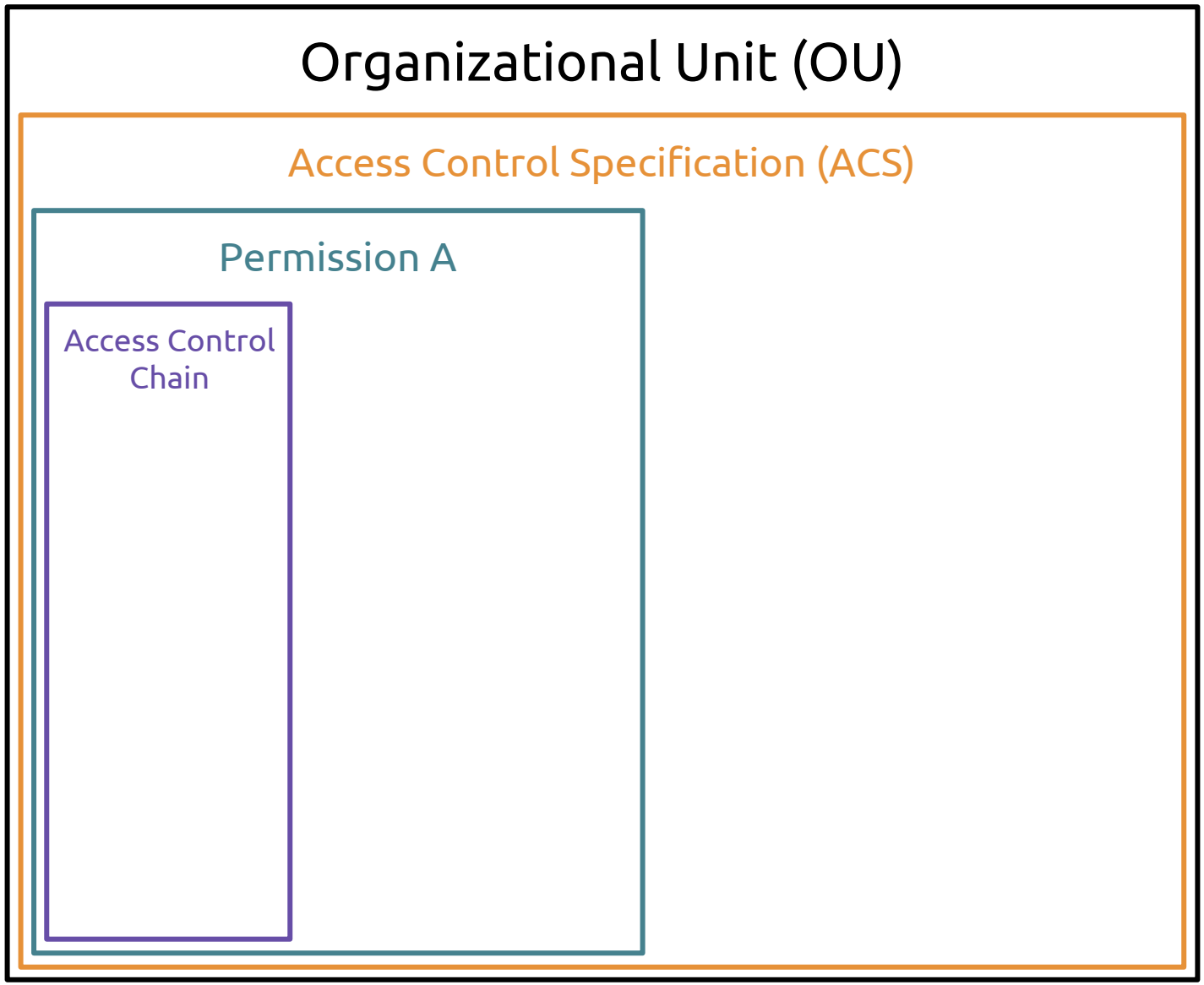

ACS
Server
ACS
Group A
Object 1
ACS
Key
Value
Object 2
ACS
Key
Value
Object 3
ACS
Key
Value
ACS
Group B
Object 4
ACS
Key
Value
Object 5
ACS
Key
Value
Object 6
ACS
Key
Value

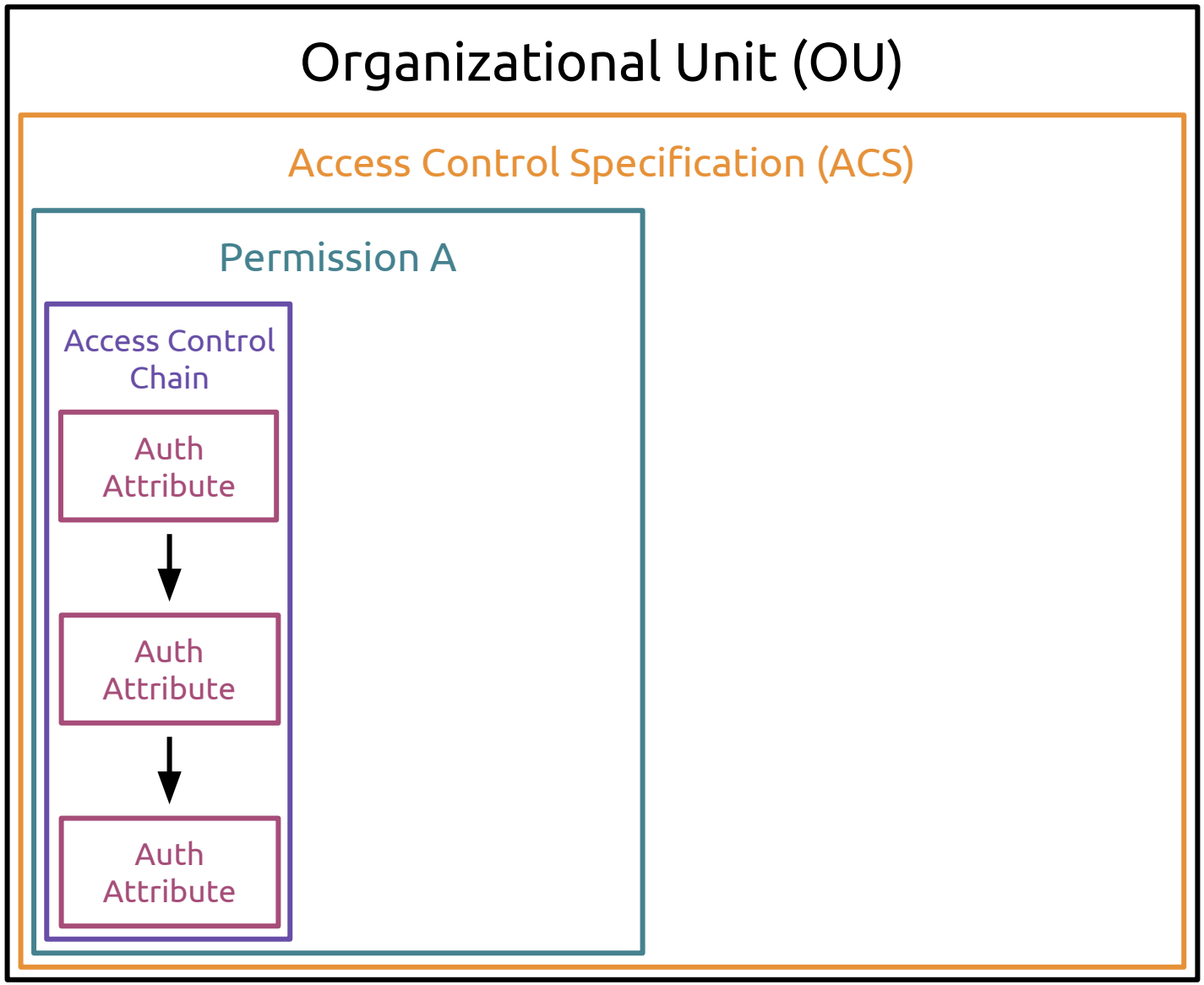
Access Control Specification (ACS)

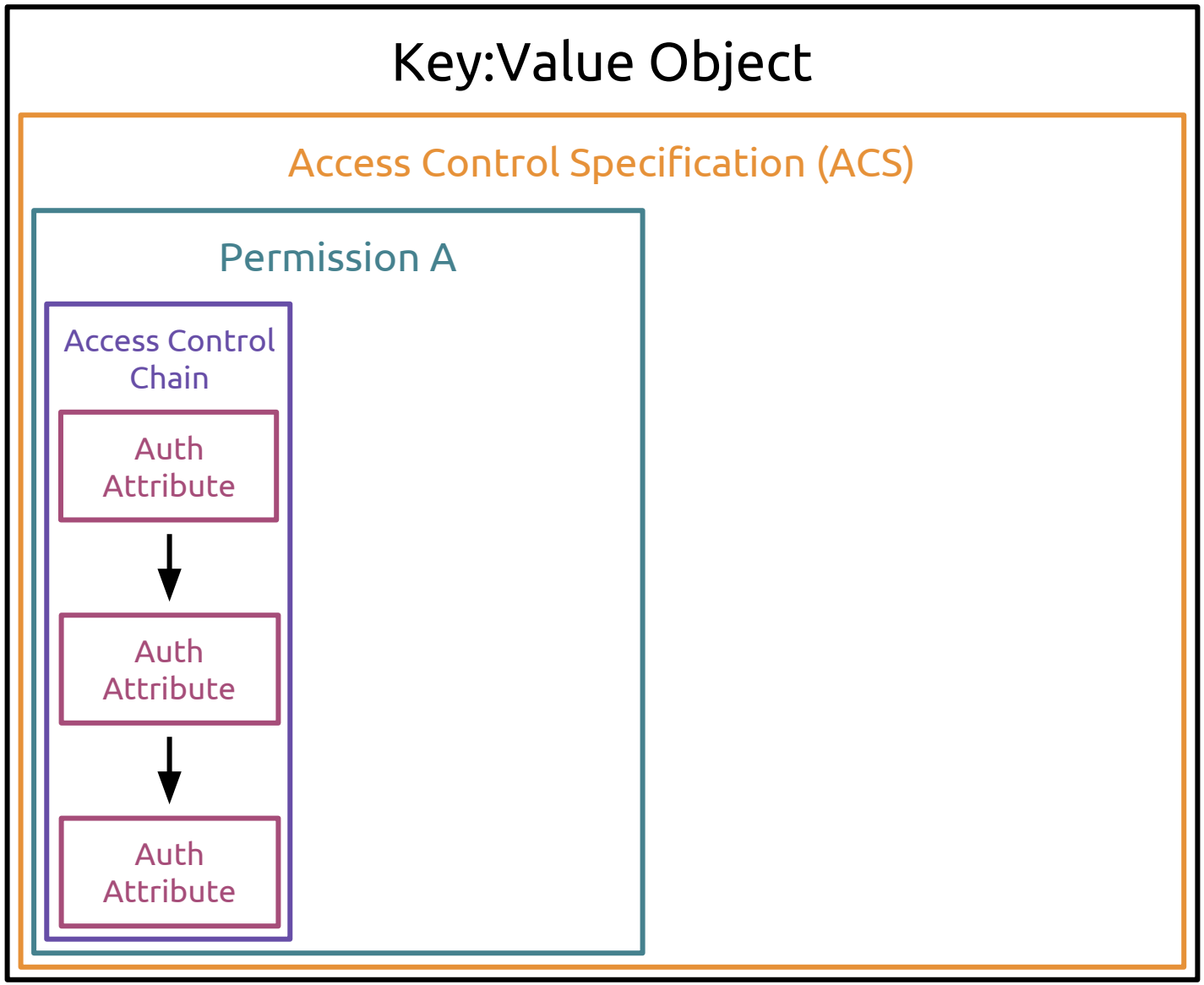

Organizational Unit (OU)

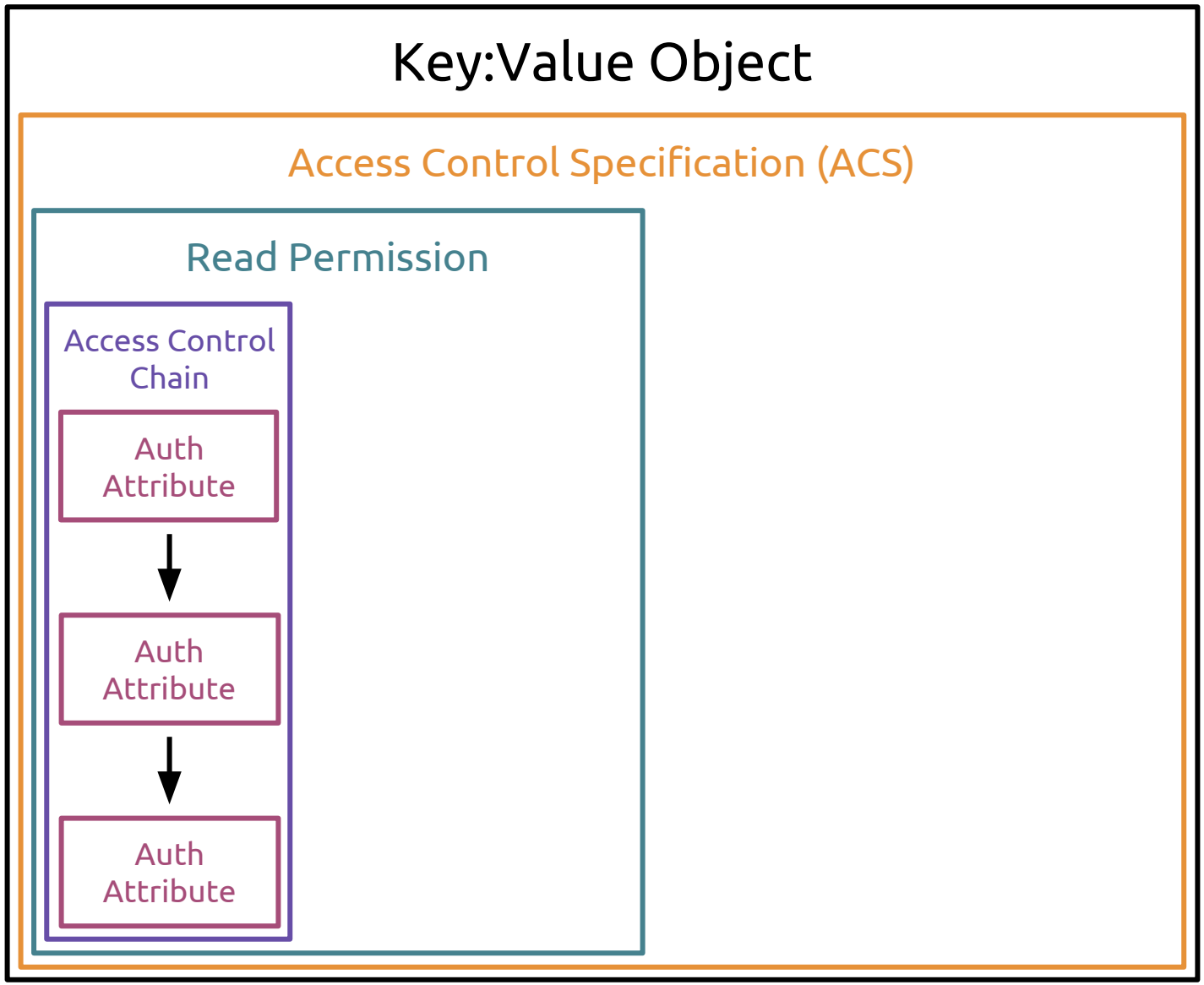

Organizational Unit (OU)
Access Control Specification (ACS)

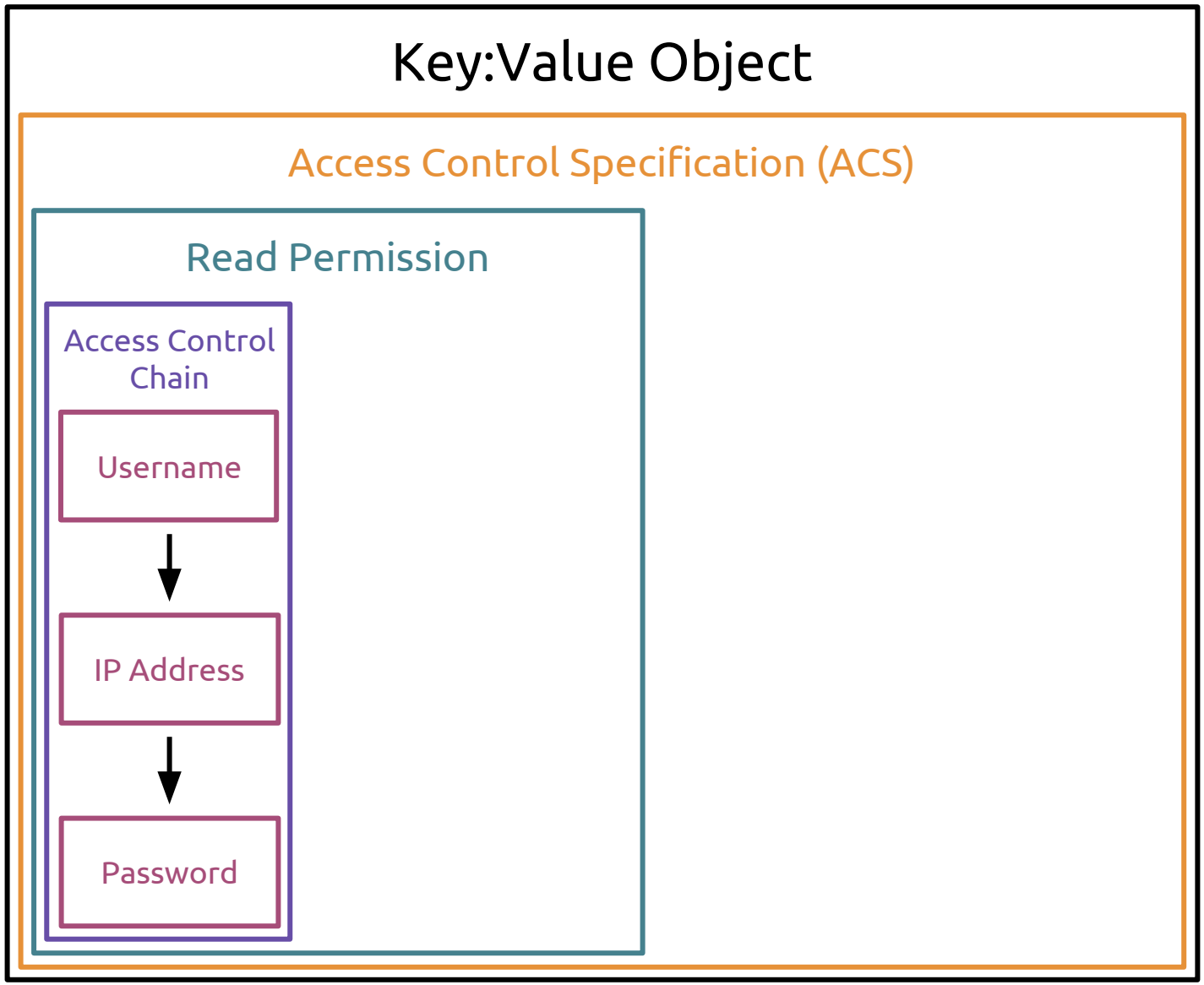

Organizational Unit (OU)
Access Control Specification (ACS)
Permission A

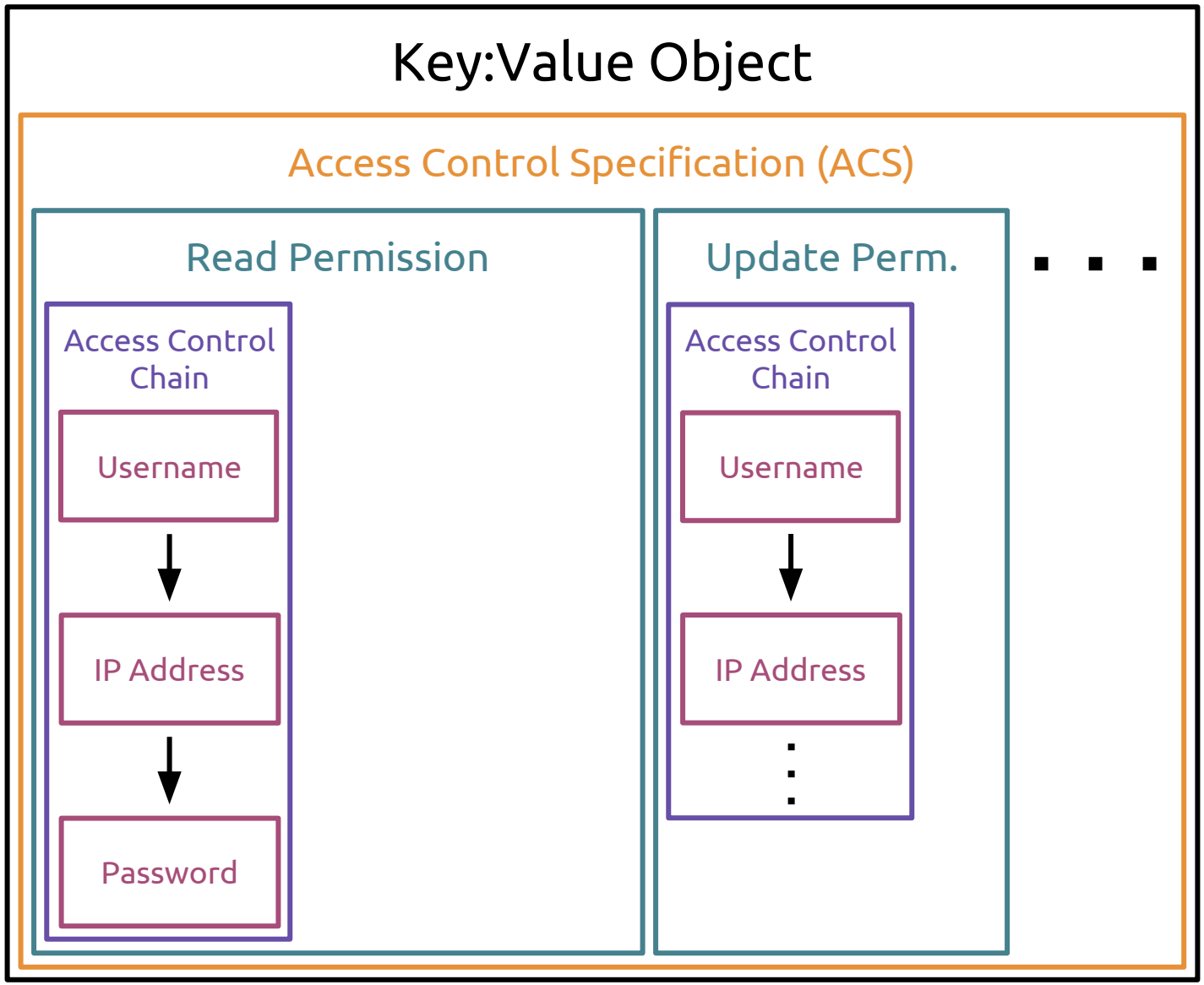

Organizational Unit (OU)
Access Control Specification (ACS)
Permission A
Access Control Chain

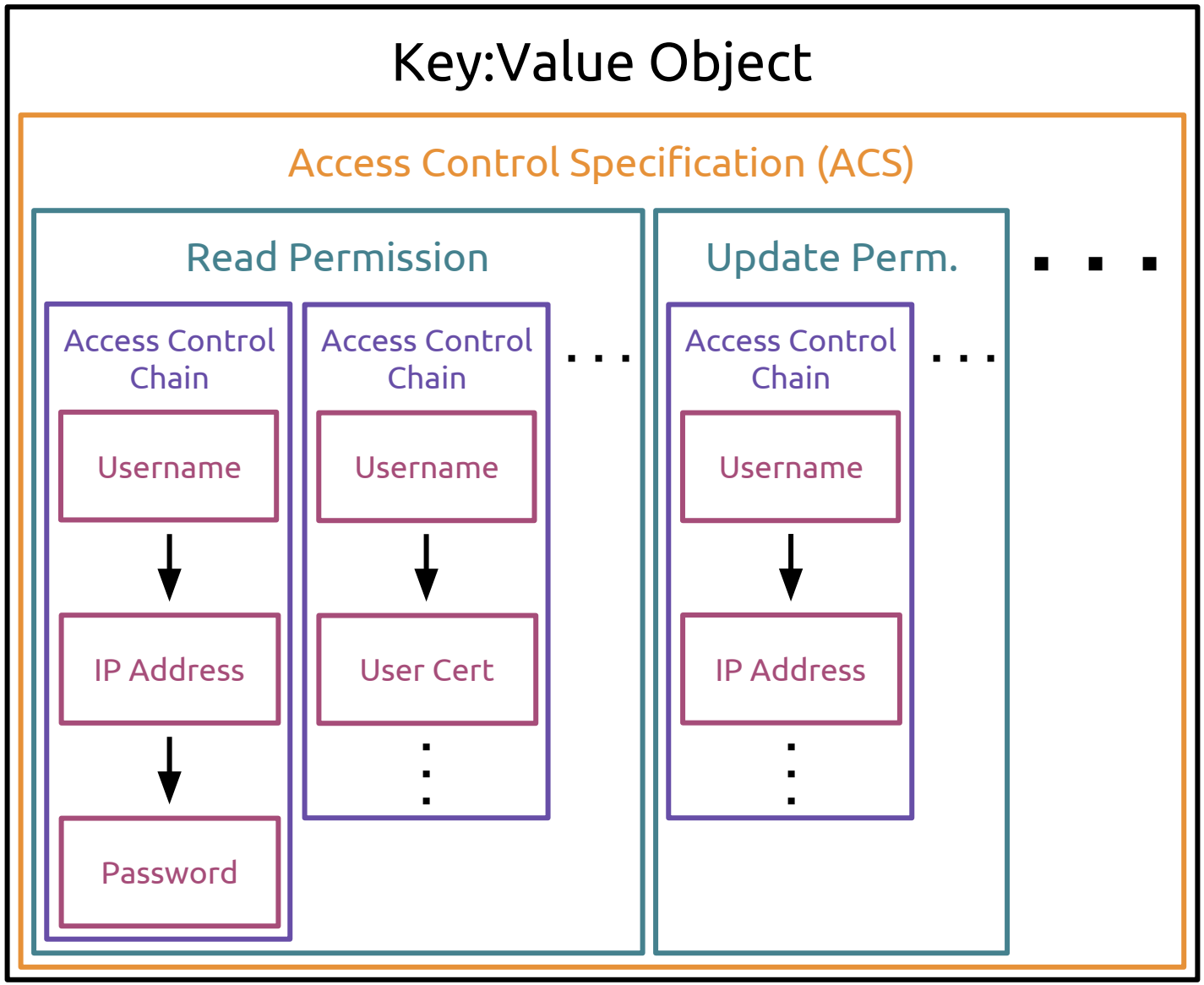

Organizational Unit (OU)
Access Control Specification (ACS)
Permission A
Access Control Chain
Auth Attribute
Auth Attribute
Auth Attribute


Key:Value Object
Access Control Specification (ACS)
Permission A
Access Control Chain
Auth Attribute
Auth Attribute
Auth Attribute


Key:Value Object
Access Control Specification (ACS)
Read Permission
Access Control Chain
Auth Attribute
Auth Attribute
Auth Attribute


Key:Value Object
Access Control Specification (ACS)
Read Permission
Access Control Chain
Username
IP Address
Password


Key:Value Object
Access Control Specification (ACS)
Read Permission
Access Control Chain
Username
IP Address
Password
Update Perm.
Access Control Chain
Username
IP Address


Key:Value Object
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

Permissions

Server

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

Group

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

Object

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

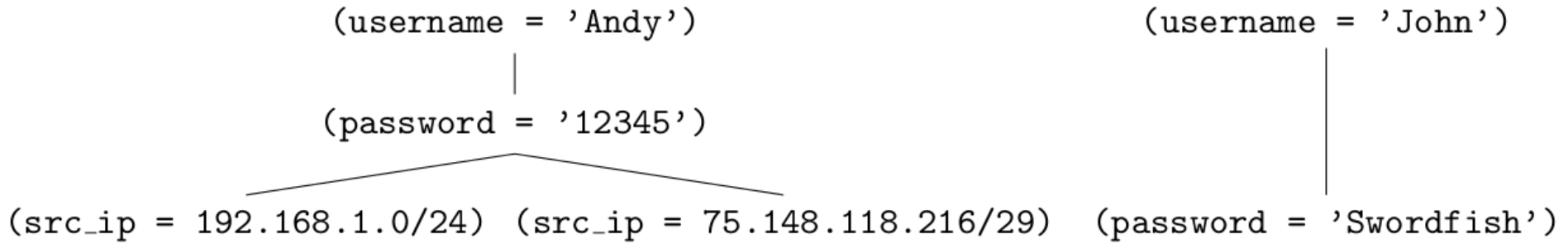
Access Control Chain

Ordered List of Authentication Attributes

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

Multiple Lists per Permission

```
[
  [ (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')

Authentication Attributes

Plugins

Explicit

- ip_src
- user_agent
- auth_type
- auth_value
- time_utc
- ...

Implicit

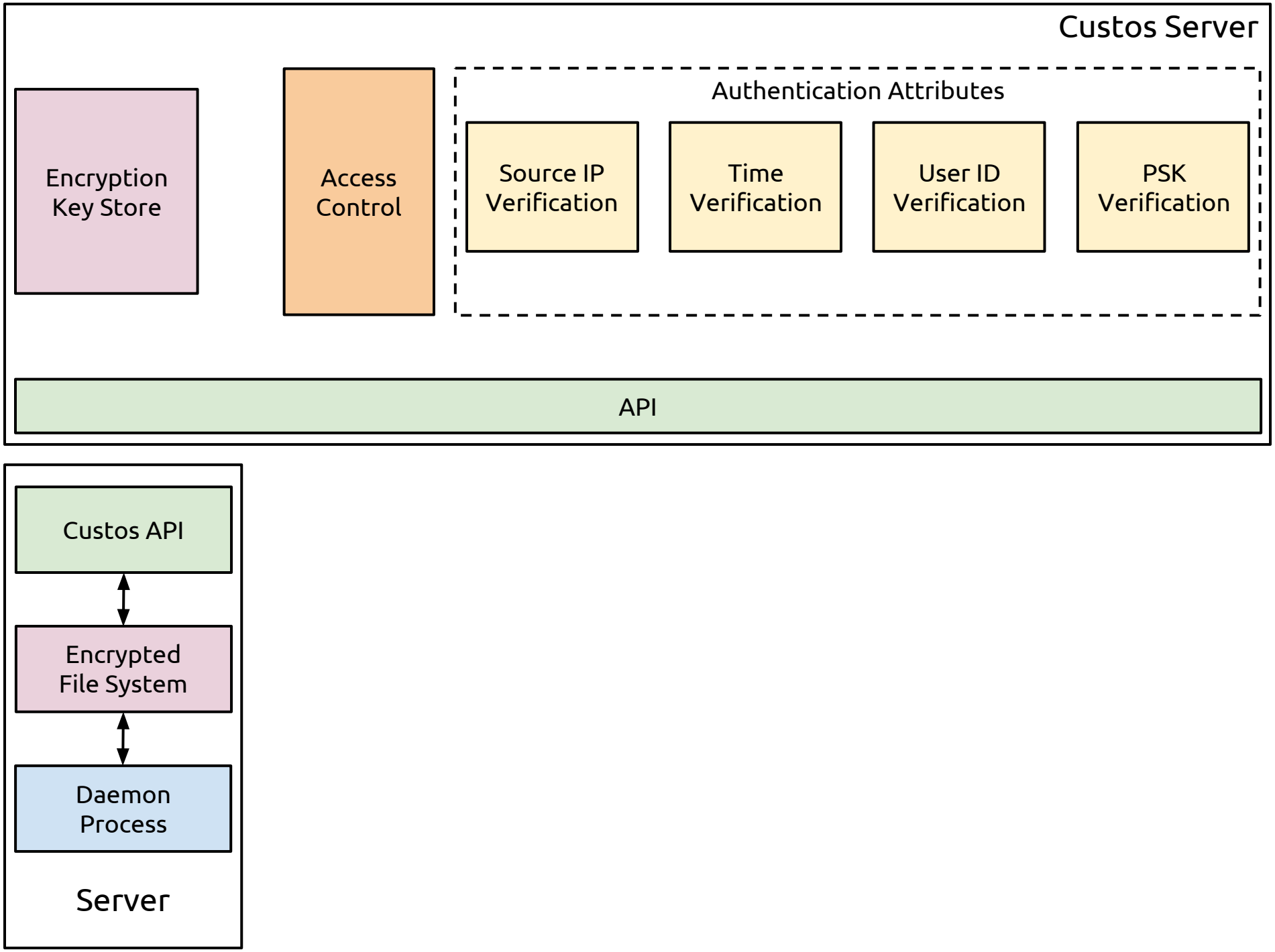
- user_id
- psk
- psk_sha256
- ...

Access Example

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

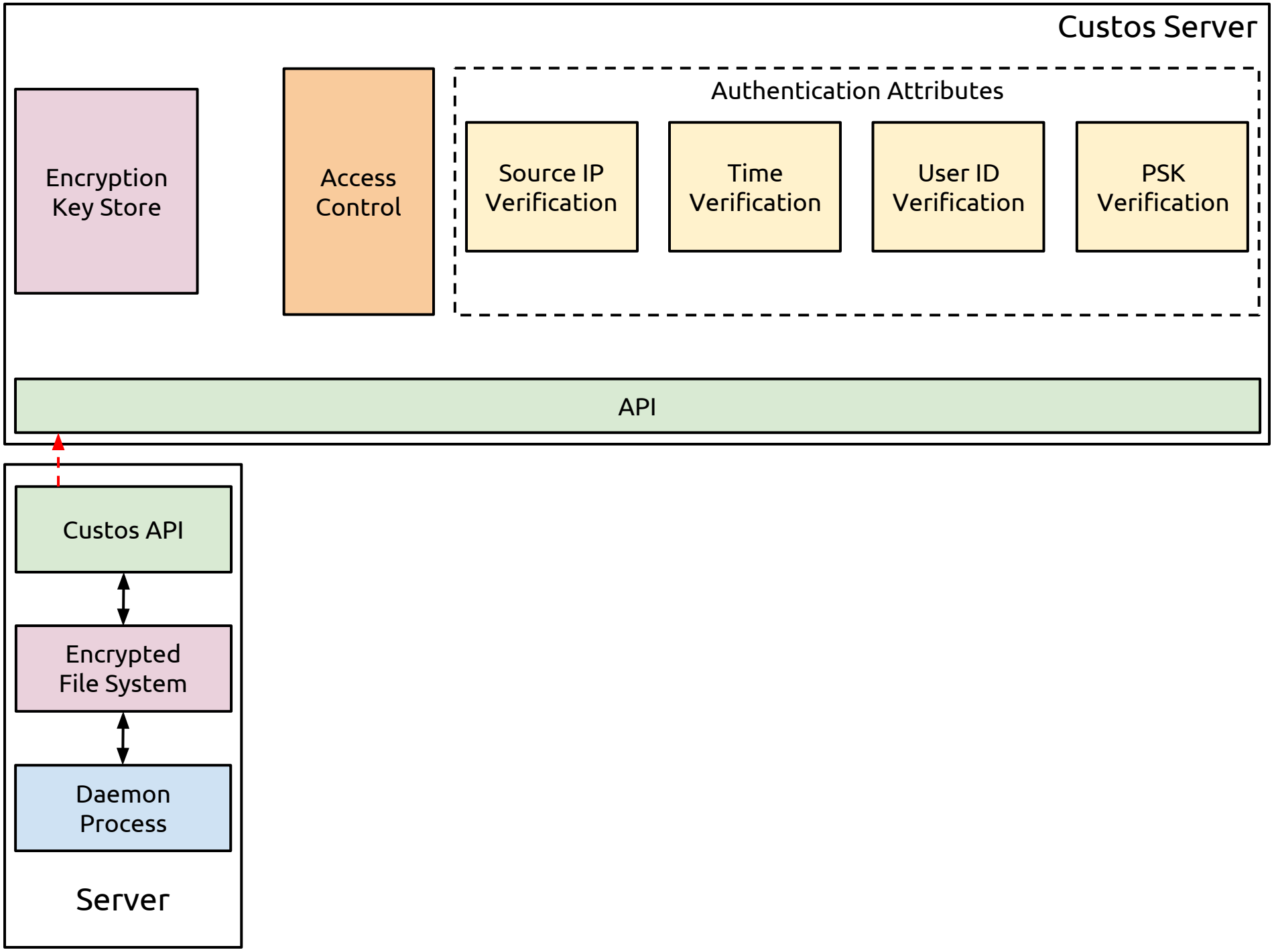
```
{
  obj_read:
    [
      [ (ip\_src = ’1.2.3.4’),
        (time\_utc = ’1300 +/- 5’) ],
      [ (user\_id = ’Dirk’),
        (psk = ’ImaHakzor’) ]
      ...
    ]
    ...
}
```

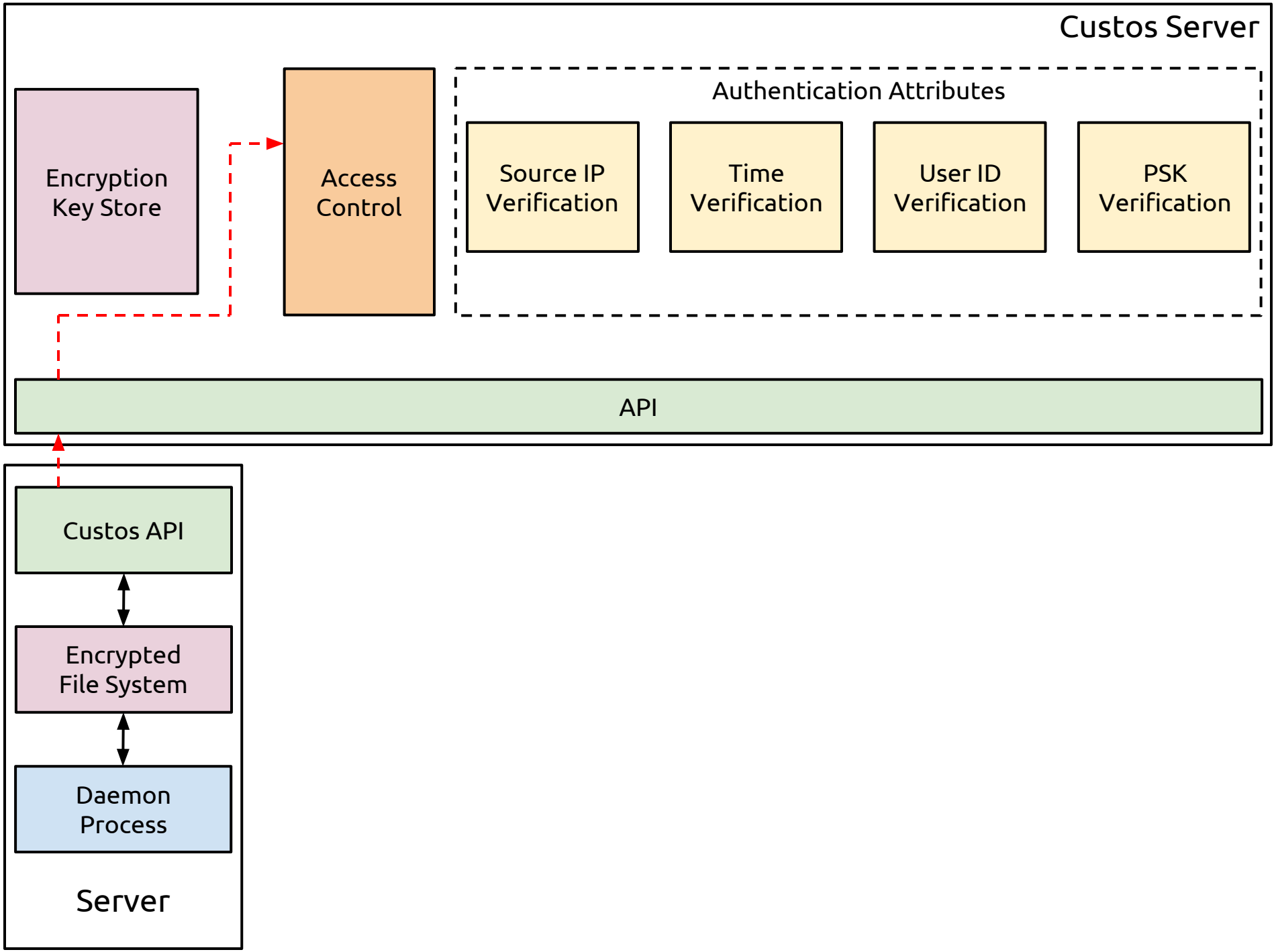
Daemon Access


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
Daemon Process
Server

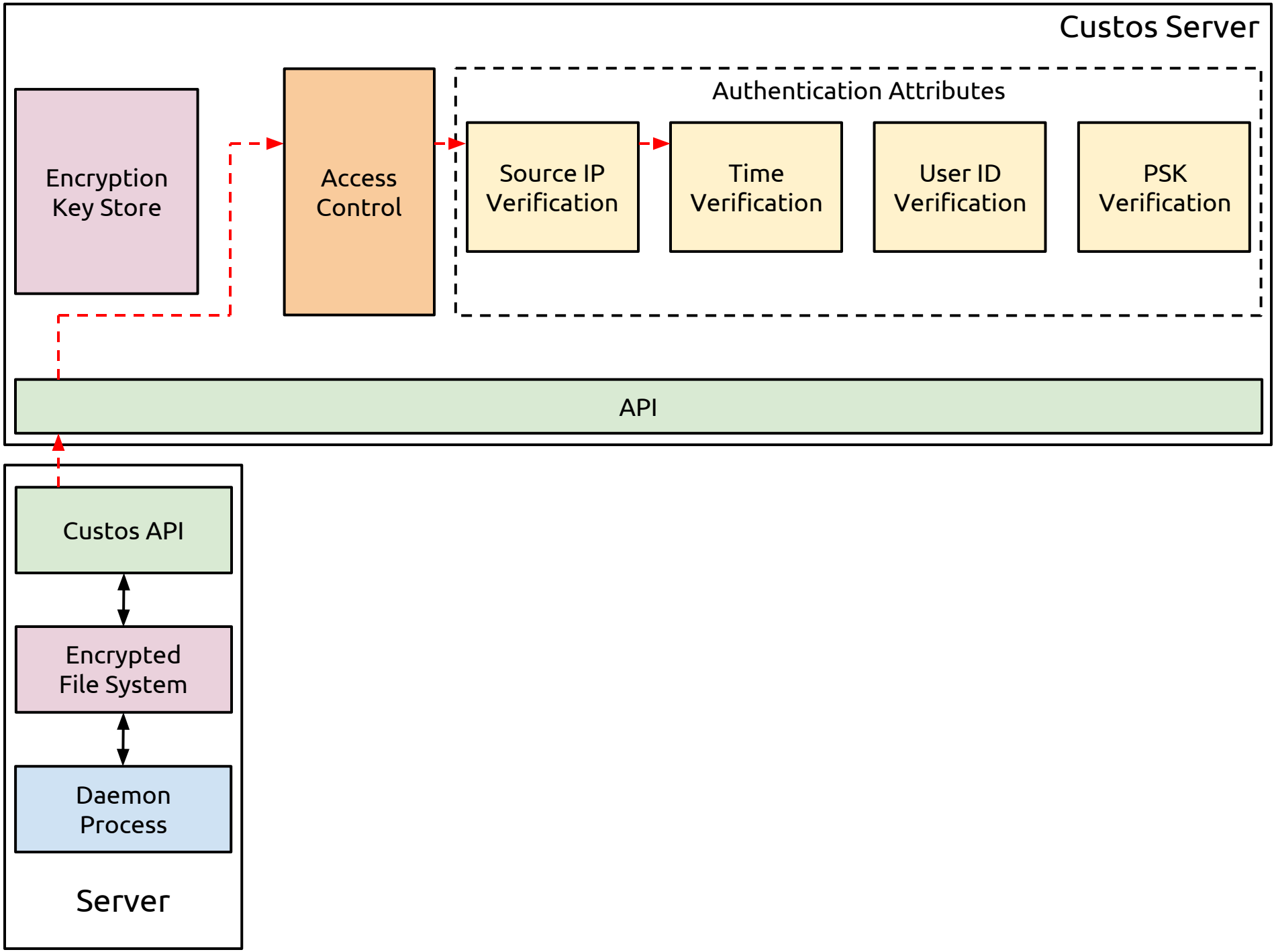
Request:
619a06f0-50af-11e3-8f96-0800200c9a66

Authentication Attributes:
(ip_src = ‘1.2.3.4’)
(time_utc = ‘1303’)


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
Daemon Process
Server


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
Daemon Process
Server

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

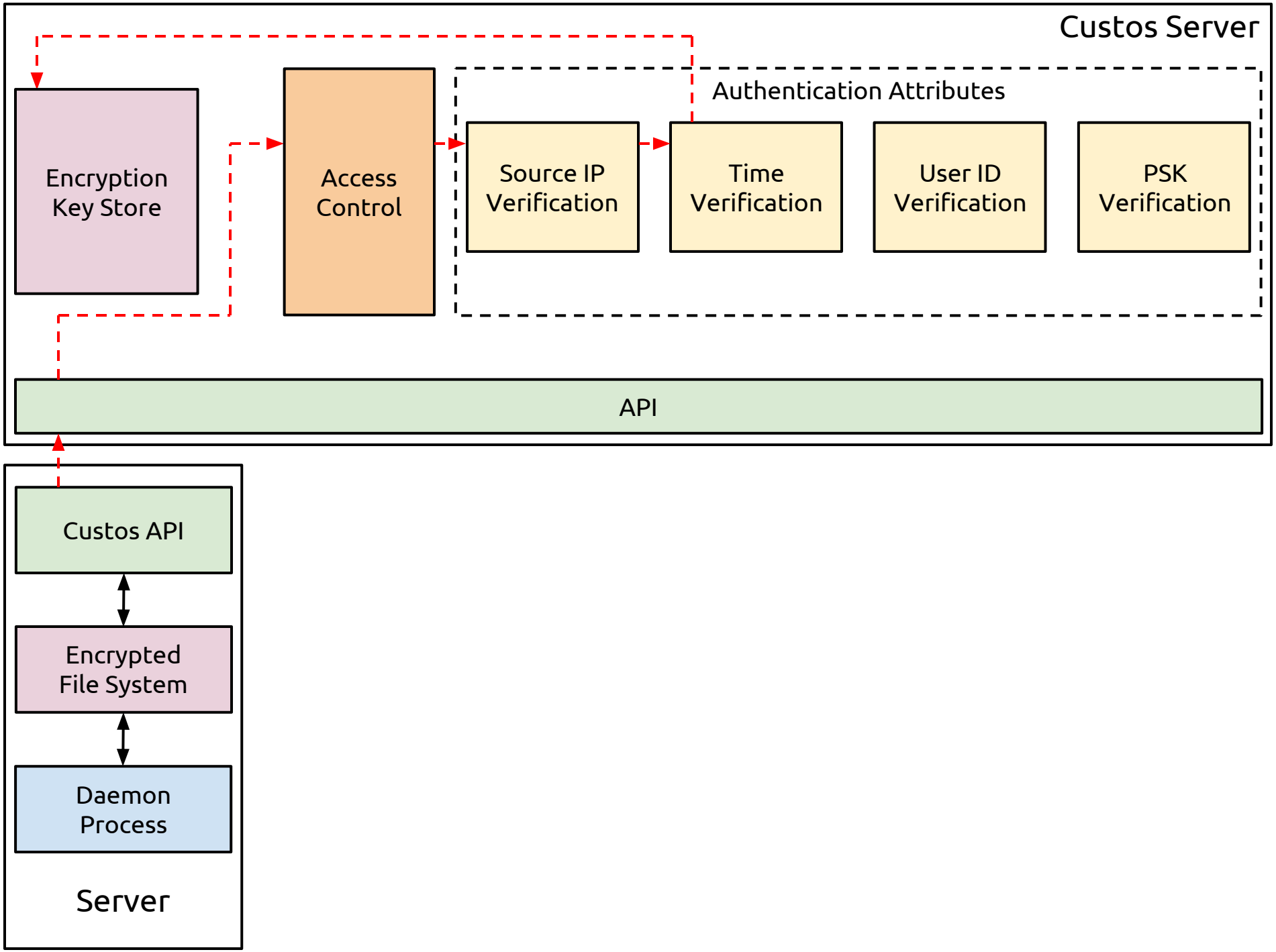

Custos Server
Encryption Key Store
Access Control
Authentication Attributes
Source IP Verification
Time Verification
User ID Verification
PSK Verification
API
Custos API
Encrypted File System
Daemon Process
Server

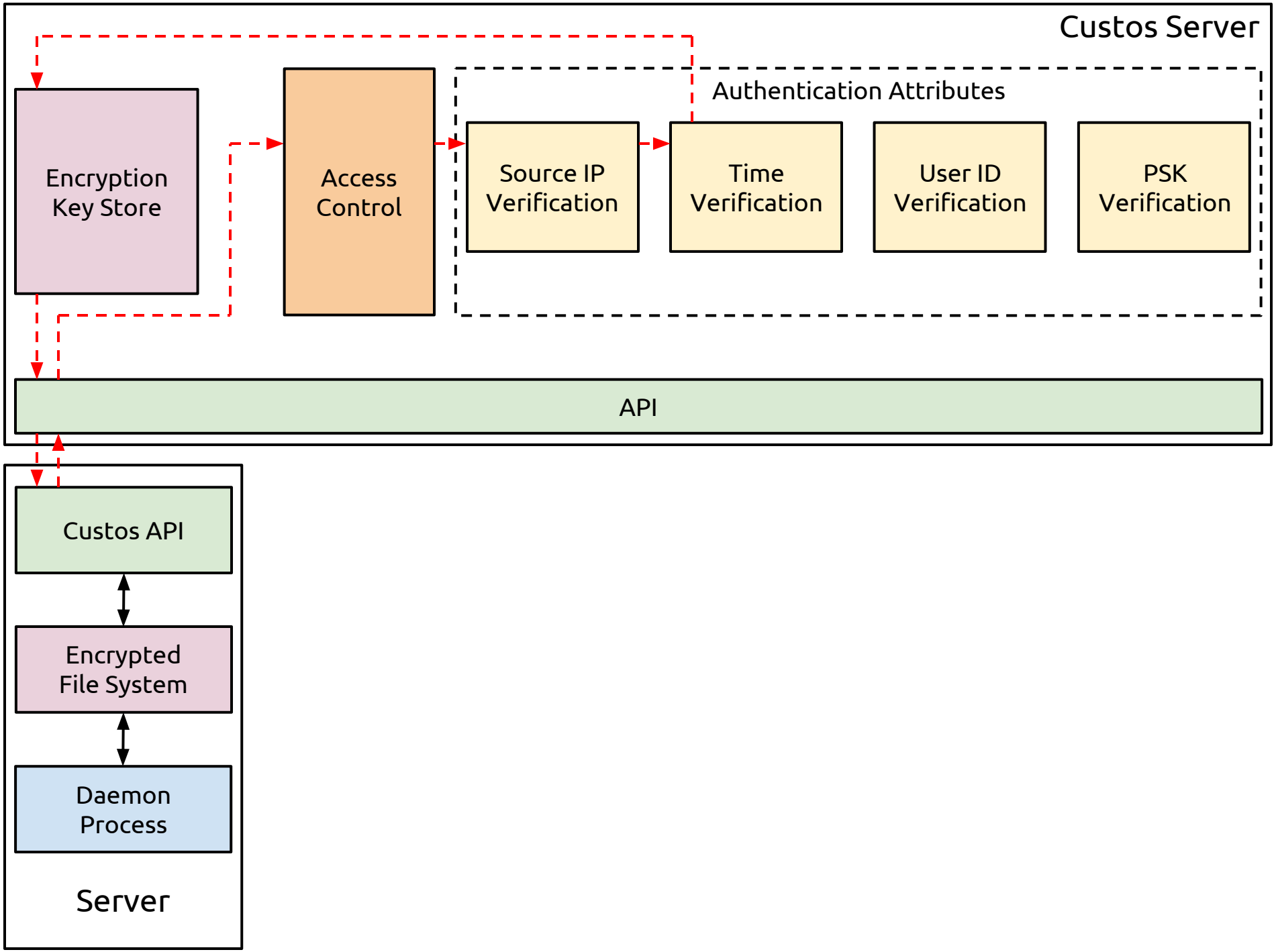
Request:
619a06f0-50af-11e3-8f96-0800200c9a66

Authentication Attributes:

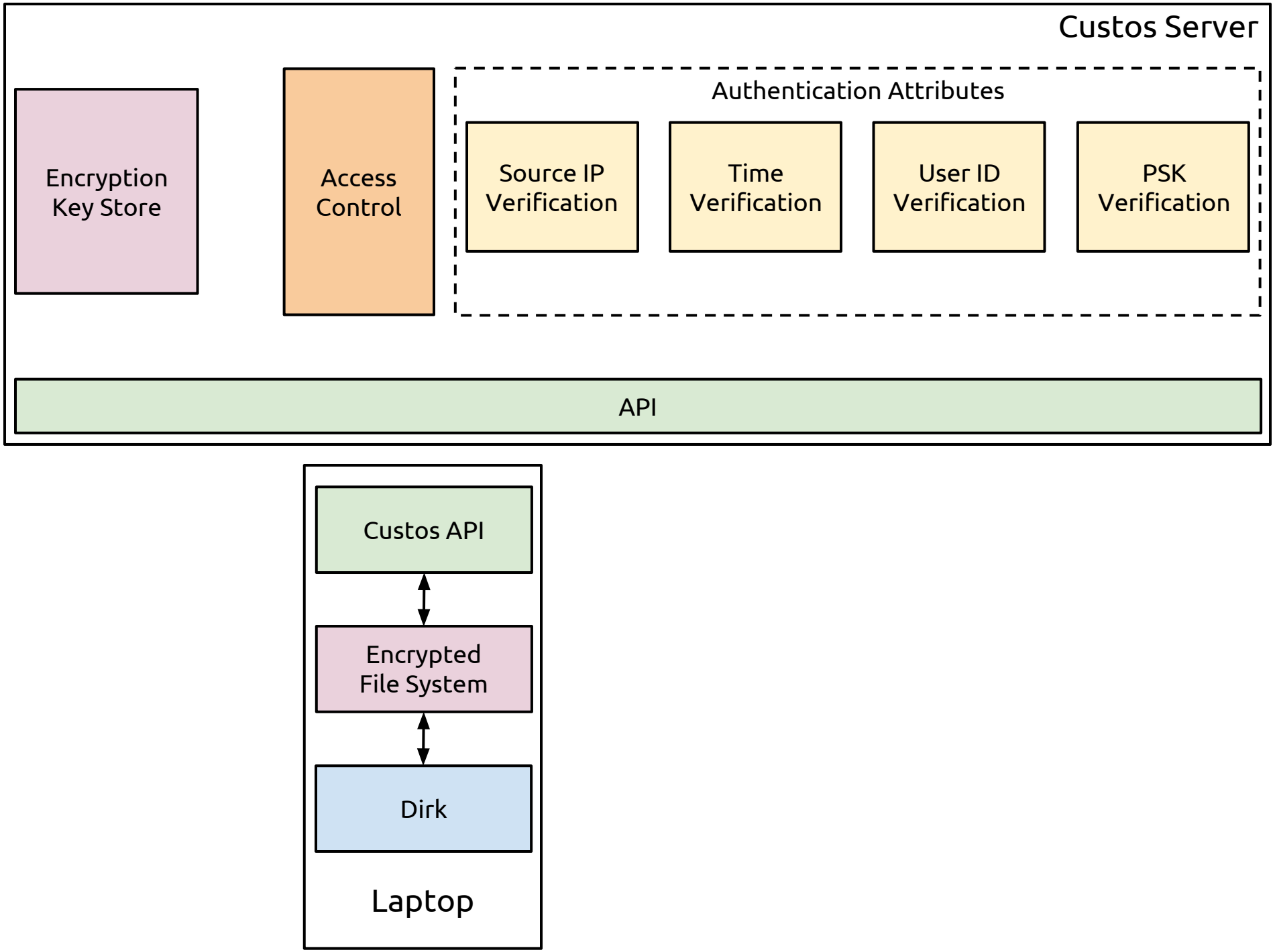
(ip_src = ‘1.2.3.4’)

(time_utc = ‘1303’)


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
Daemon Process
Server

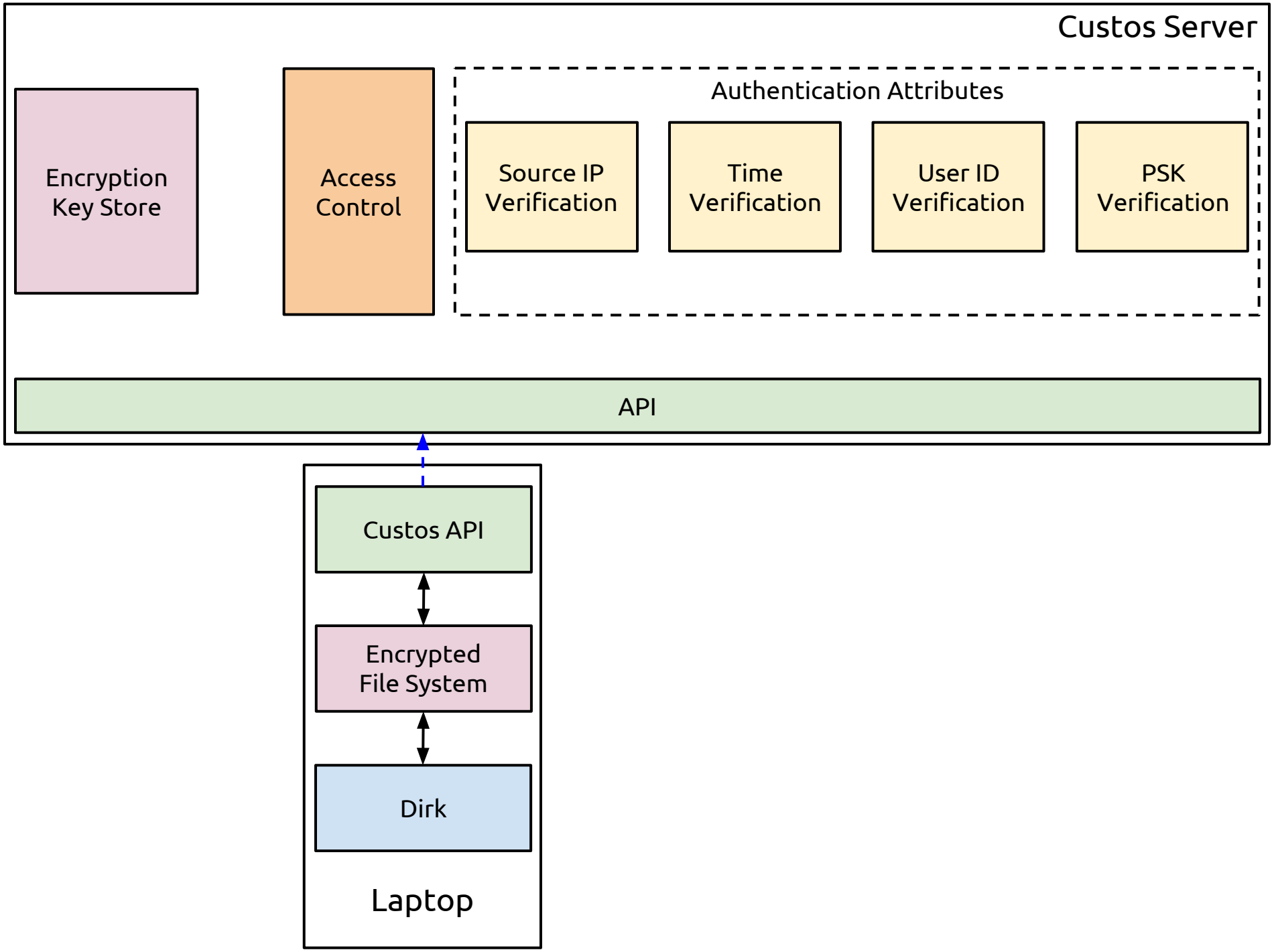

Custos Server
Encryption Key Store
Access Control
Authentication Attributes
Source IP Verification
Time Verification
User ID Verification
PSK Verification
API
Custos API
Encrypted File System
Daemon Process
Server

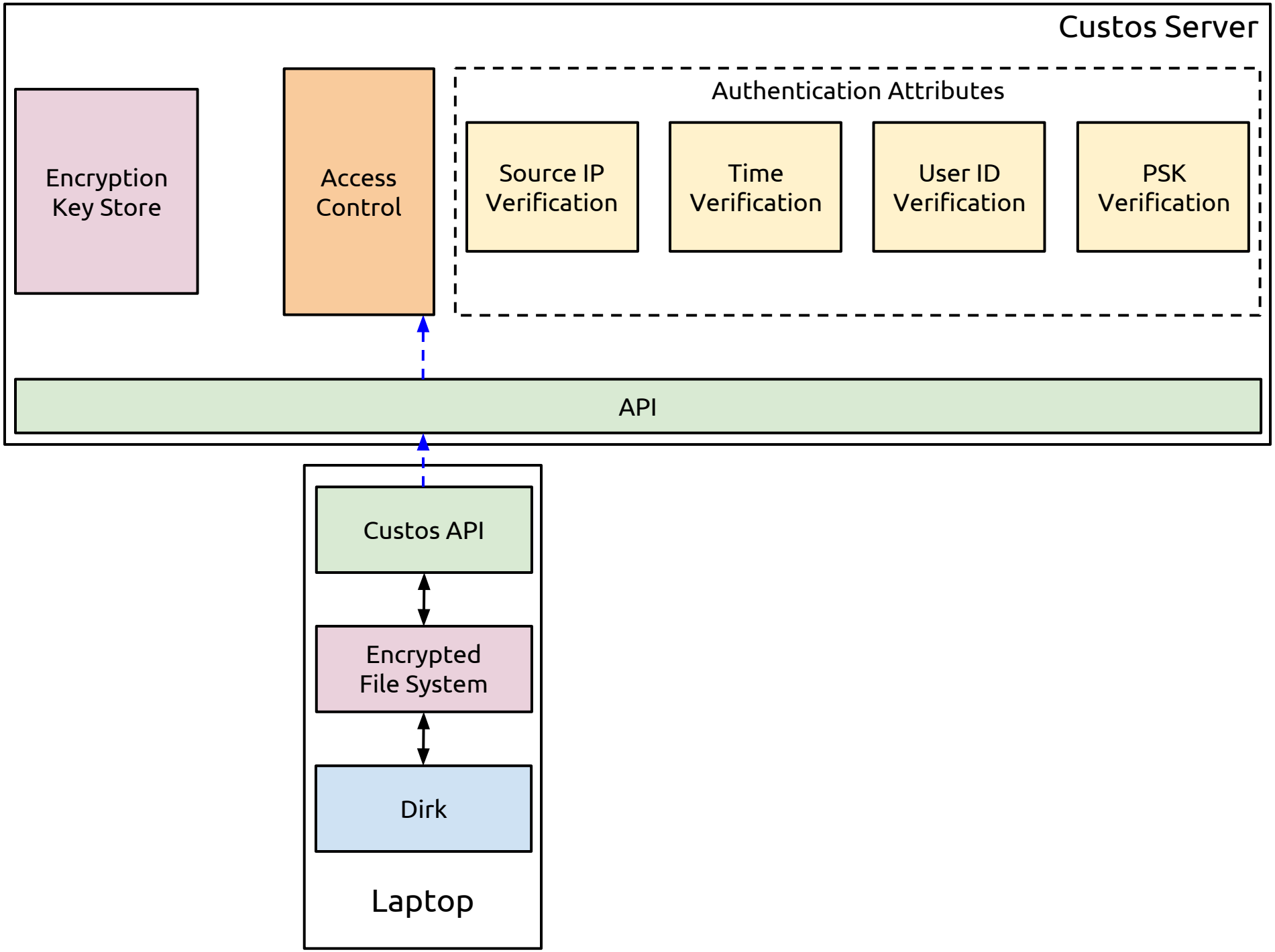
User Access


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

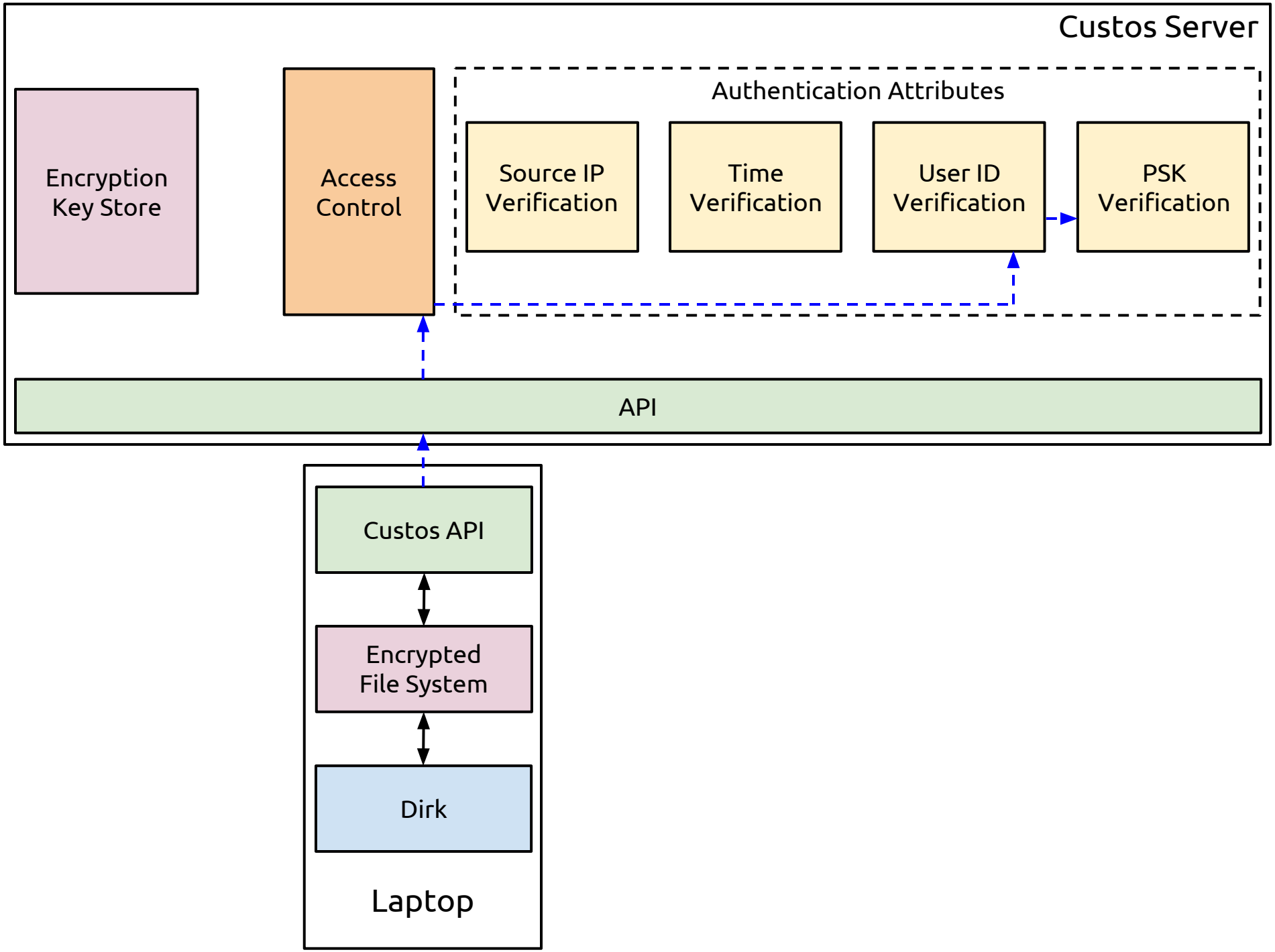
Request:
619a06f0-50af-11e3-8f96-0800200c9a66

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

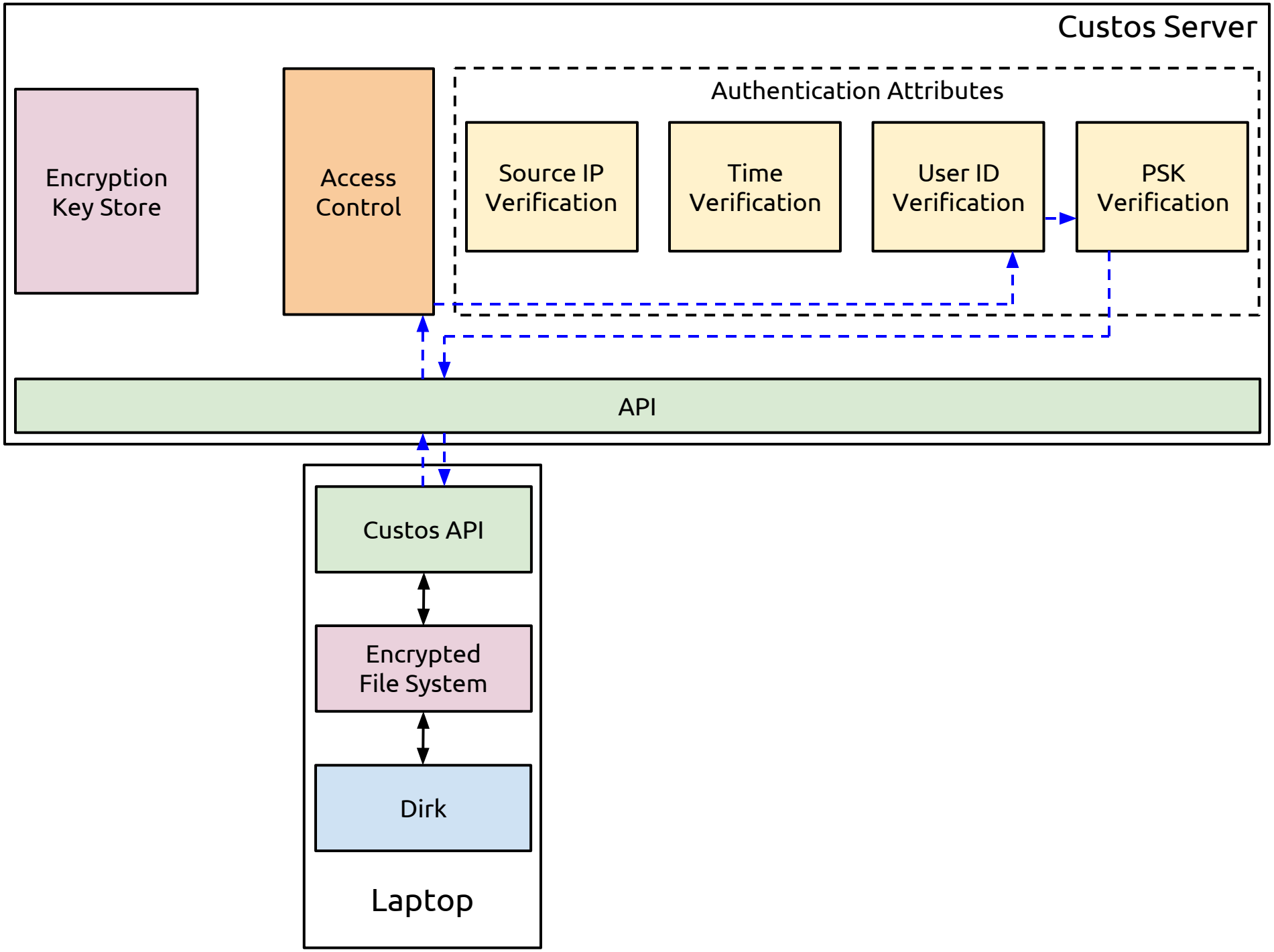

Custos Server
Encryption Key Store
Access Control
Authentication Attributes
Source IP Verification
Time Verification
User ID Verification
PSK Verification
API
Custos API
Encrypted File System
Dirk
Laptop

```
{
  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

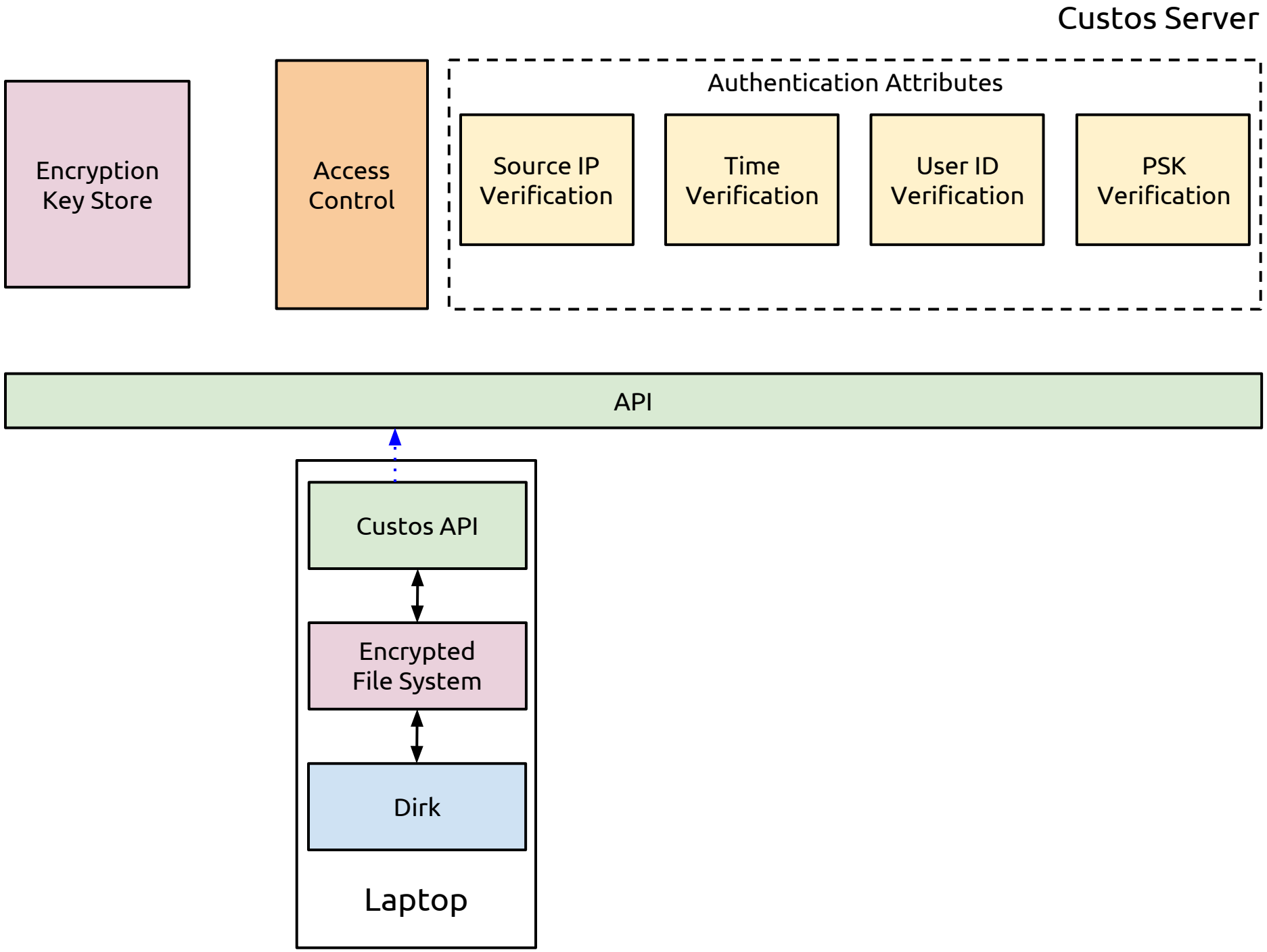
Authentication Attributes:
user_id = Dirk
(ip_src = ‘1.2.3.4’)
(time_utc = ‘1133’)

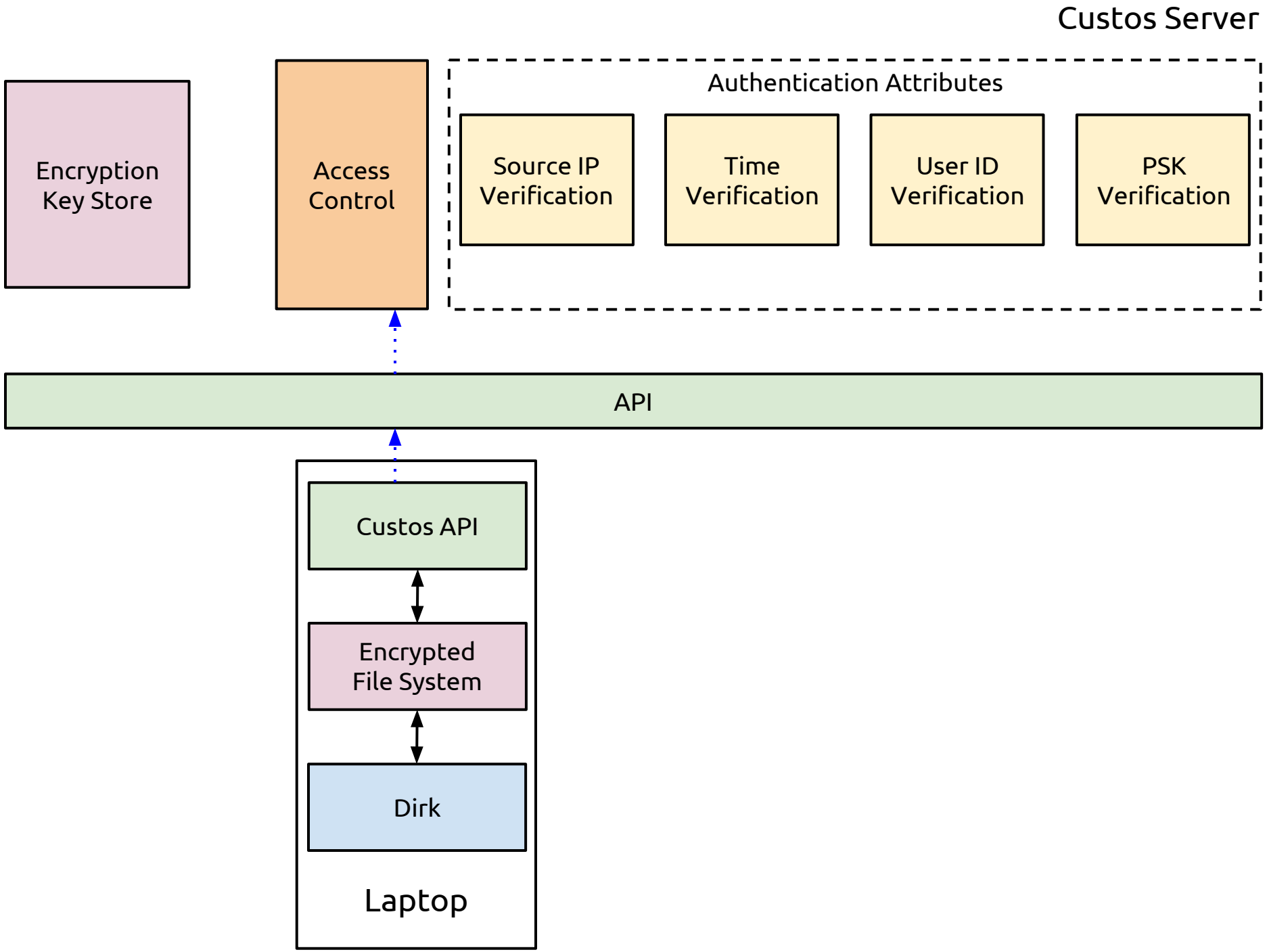

Custos Server
Encryption Key Store
Access Control
Authentication Attributes
Source IP Verification
Time Verification
User ID Verification
PSK Verification
API
Custos API
Encrypted File System
Dirk
Laptop

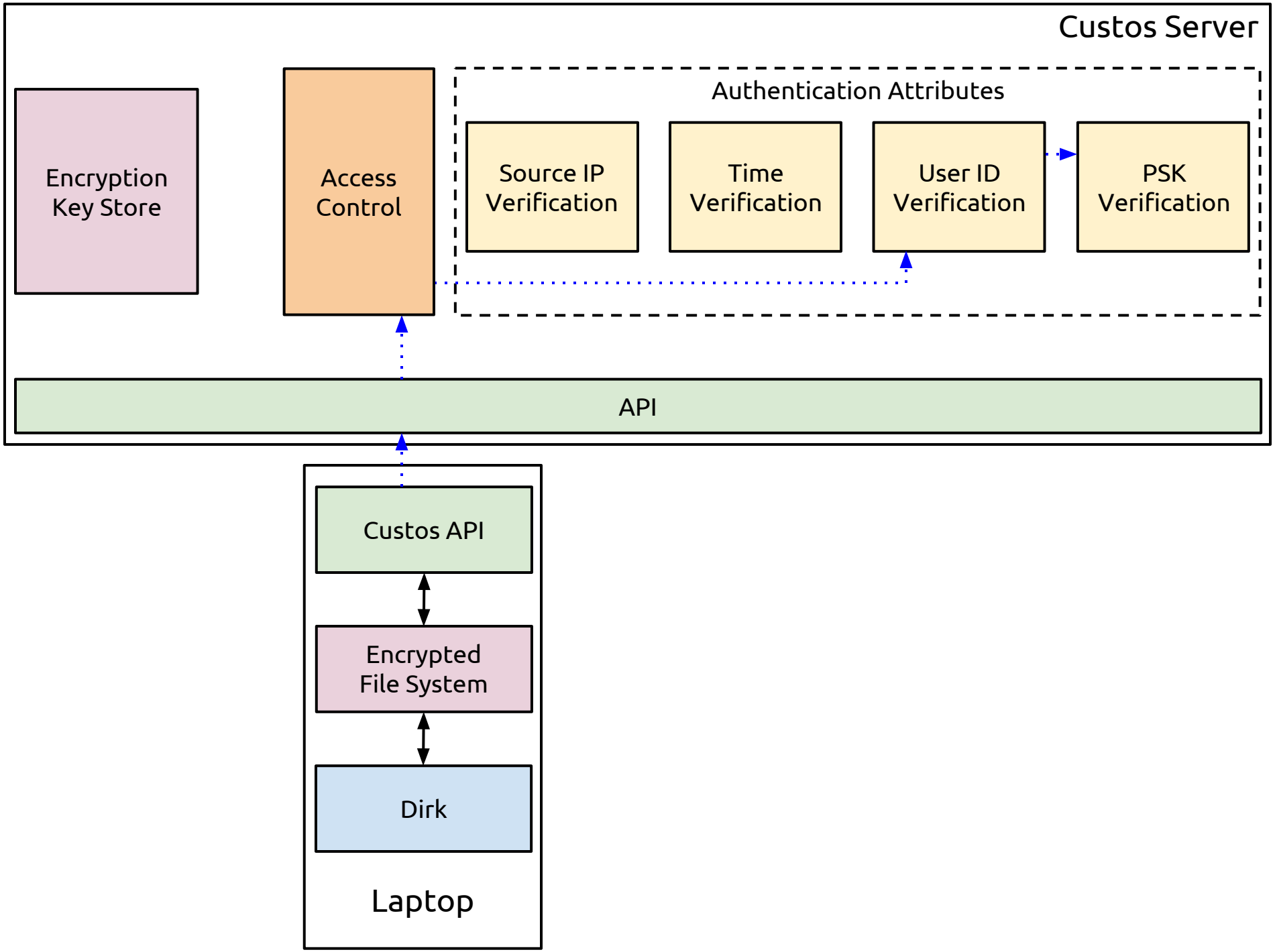
```
{
  obj_read:
    [
      [ (ip\_src = ’1.2.3.4’),
        (time\_utc = ’1300 +/- 5’) ],
      [ (user\_id = ’Dirk’),
        (psk = ’ImaHakzor’) ]
      ...
    ]
    ...
}
```

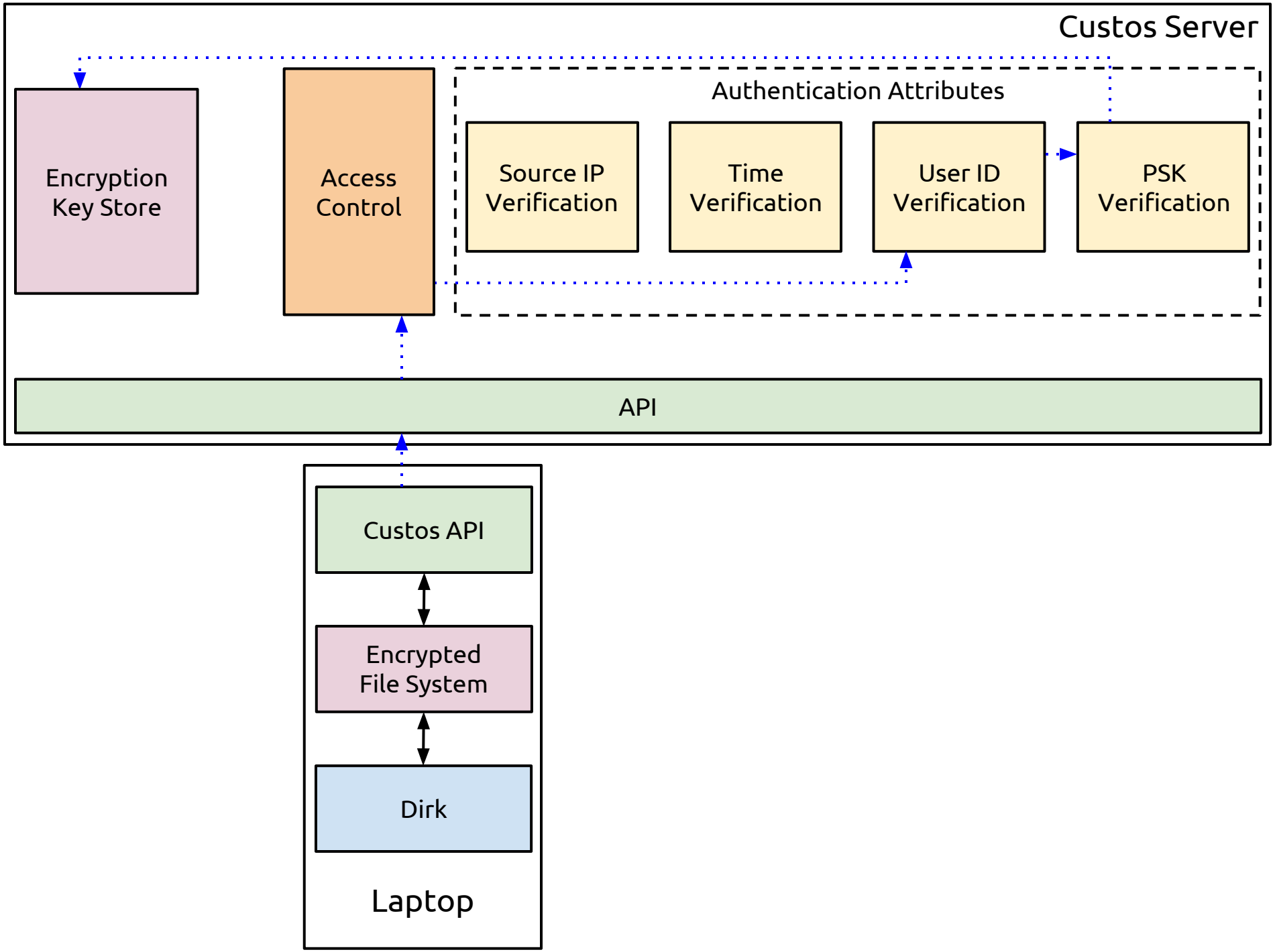
Request:
619a06f0-50af-11e3-8f96-0800200c9a66

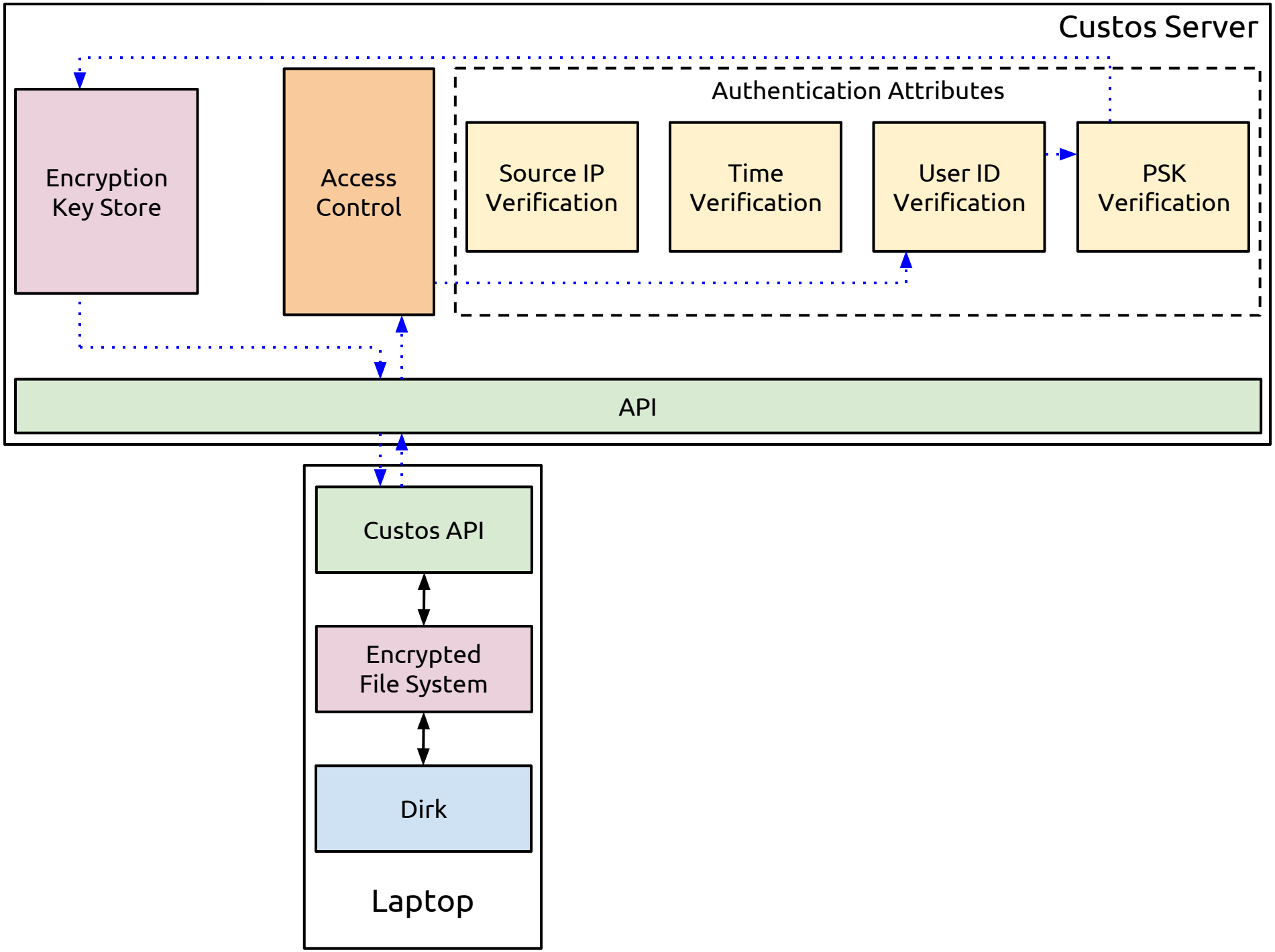
Authentication Attributes:
user_id = ‘Dirk’
psk = ‘ImaHackzor’
(ip_src = ‘1.2.3.4’)
(time_utc = ‘1133’)


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

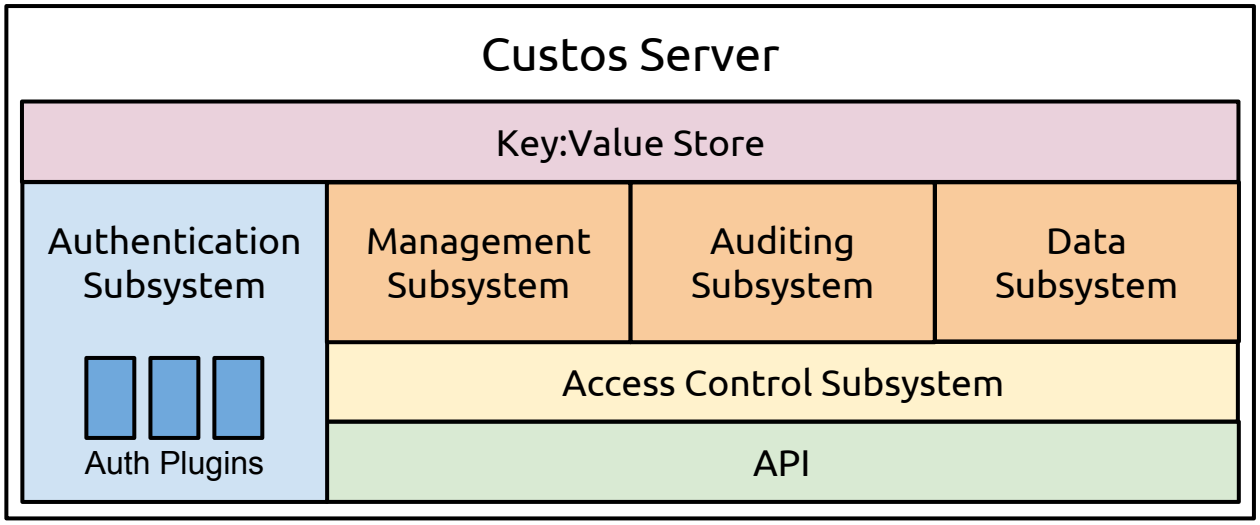

Custos Server
Encryption Key Store
Access Control
Authentication Attributes
Source IP Verification
Time Verification
User ID Verification
PSK Verification
API
Custos API
Encrypted File System
Dirk
Laptop

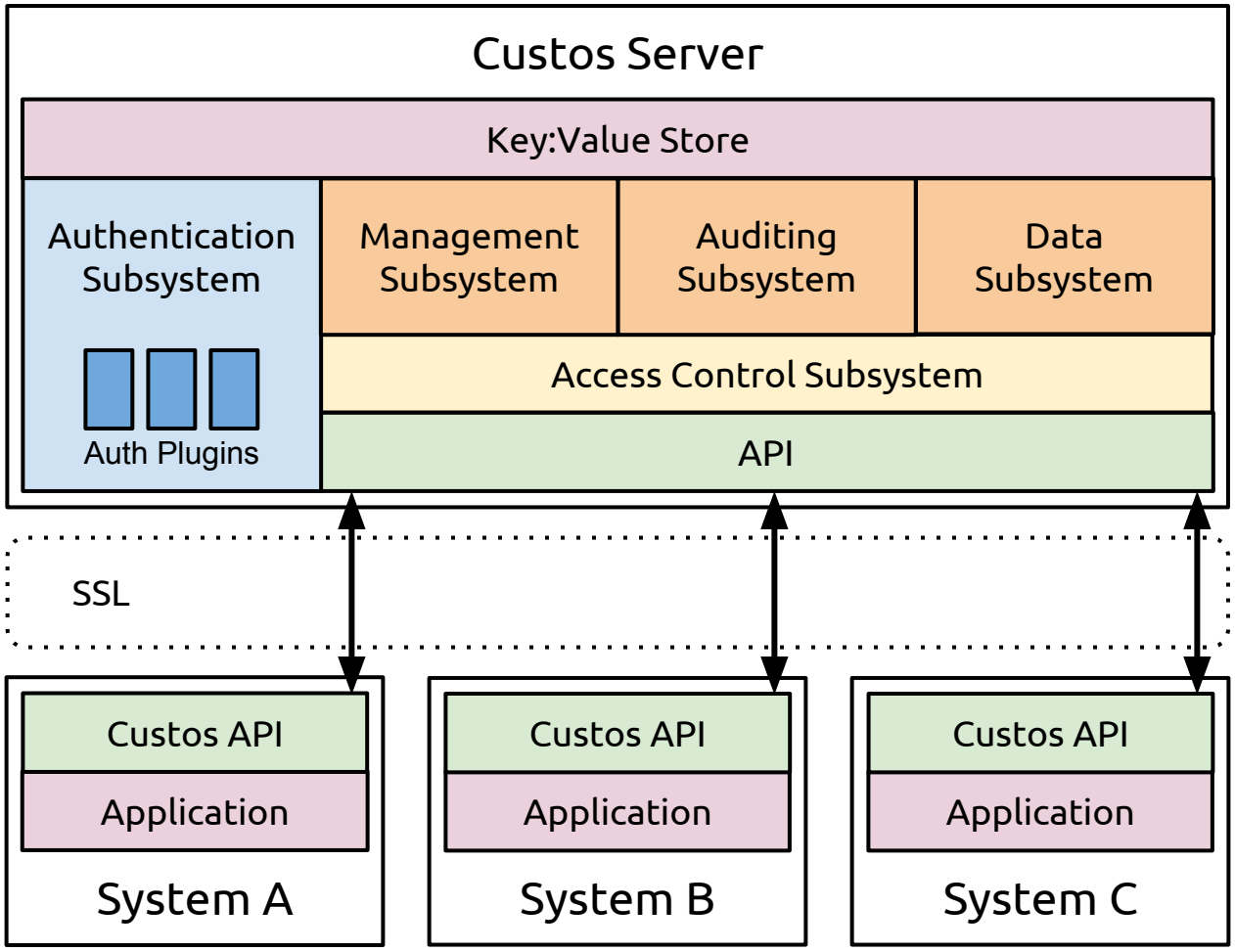
API

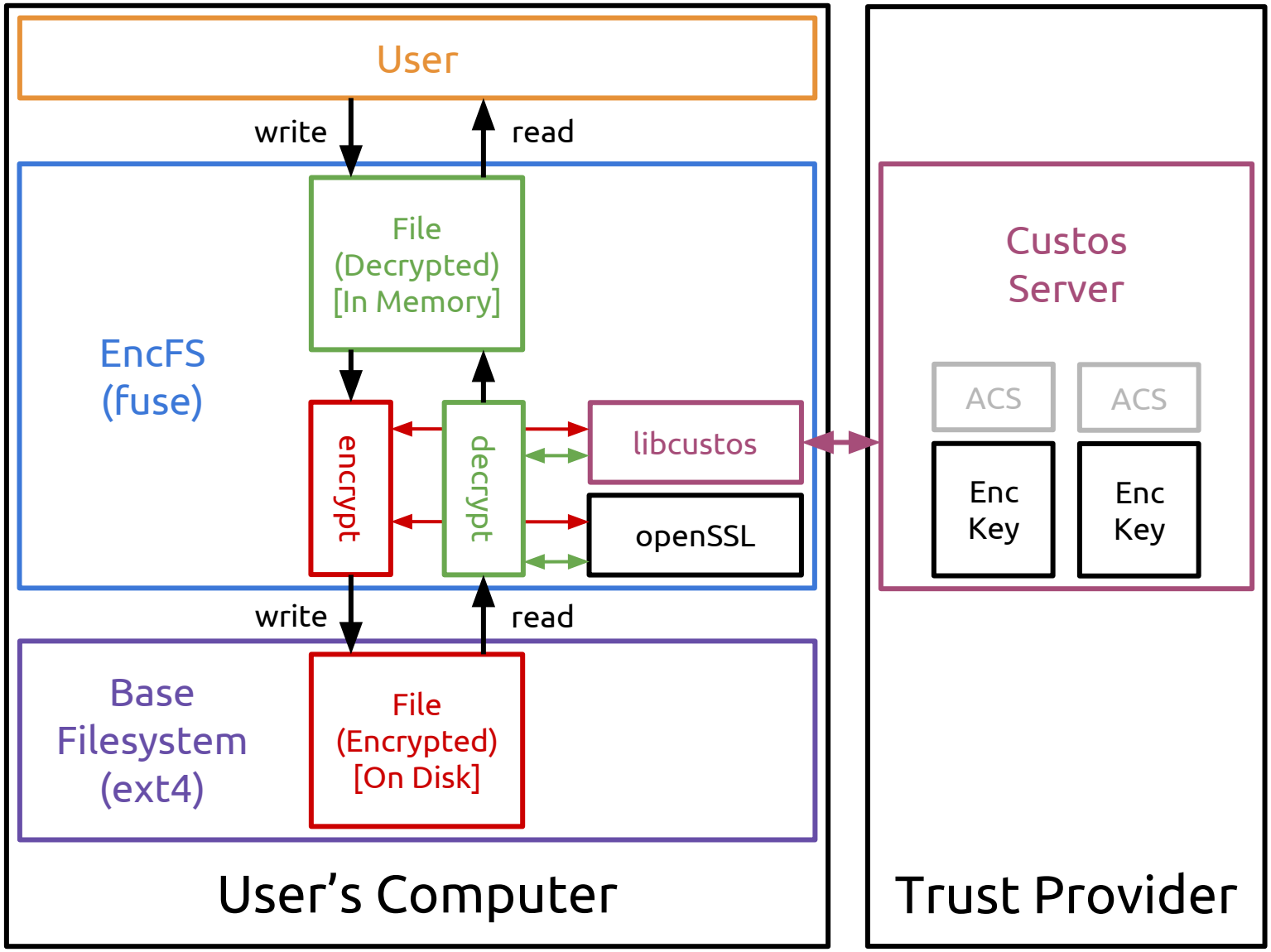
RESTful

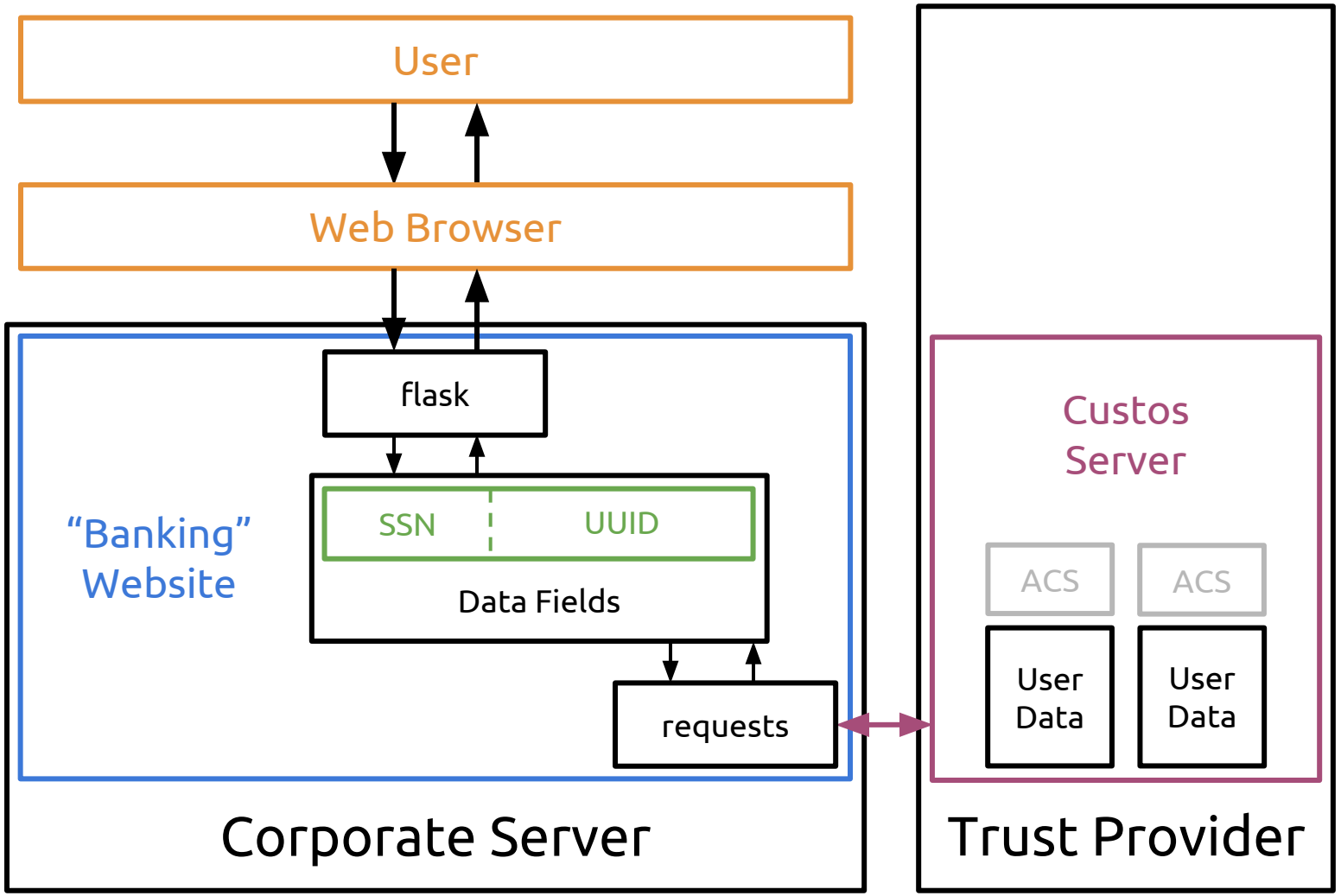
Endpoint	Verb	Required Permission	Purpose
/grp	POST	srv_grp_create	create a new group, returning the group's UUID
/grp	GET	srv_grp_list	return the list of all groups
/grp/⟨grp_uuid⟩	DELETE	grp_delete	remove a group
/grp/⟨grp_uuid⟩/obj	POST	grp_obj_create	create a new key:value object, returning the object's UUID
/grp/⟨grp_uuid⟩/obj	GET	grp_obj_list	return a list of all key:value objects
/grp/⟨grp_uuid⟩/obj/⟨obj_uuid⟩	PUT	obj_update	update an existing key:value object
/grp/⟨grp_uuid⟩/obj/⟨obj_uuid⟩	GET	obj_read	return a key:value object*
/grp/⟨grp_uuid⟩/obj/⟨obj_uuid⟩	DELETE	obj_delete	delete a key:value object

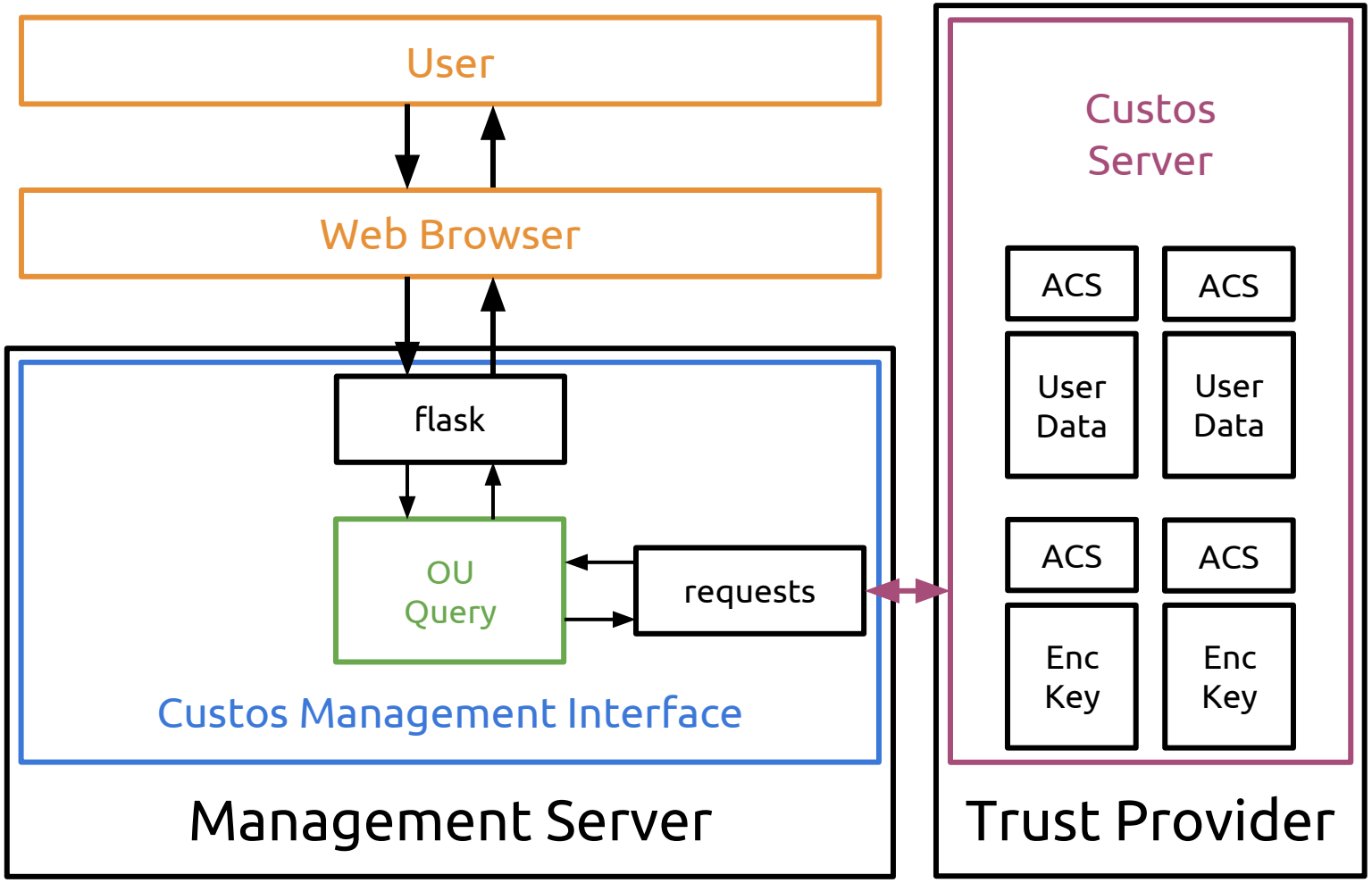
Prototype


Custos Server
Key:Value Store
Authentication Subsystem
Auth Plugins
Management Subsystem
Auditing Subsystem
Data Subsystem
Access Control Subsystem
API


Custos Server
Key:Value Store
Authentication Subsystem
Auth Plugins
Management Subsystem
Auditing Subsystem
Data Subsystem
Access Control Subsystem
API
SSL
Custos API
Application
System A
Custos API
Application
System B
Custos API
Application
System C


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


User
Web Browser
flask
"Banking"
Website
SSN
UUID
Data Fields
requests
Corporate Server
Custos
Server
ACS
ACS
User
Data
User
Data
Trust Provider


User
Web Browser
flask
OU
Query
requests
Custos Management Interface
Management Server
Custos
Server
ACS
ACS
User
Data
User
Data
ACS
ACS
Enc
Key
Enc
Key
Trust Provider

Future Work

Expand Prototypes

Usability Studies

Distributed Usage

...

Conclusion

Attempt to solve the

Key Storage Problem

Provides a

Secret Storage Service

With...

Flexible Authentication

Powerful Access Control

Standardized Interface

Making Encryption...

Tolerant of Modern Uses Cases

Easier to Use

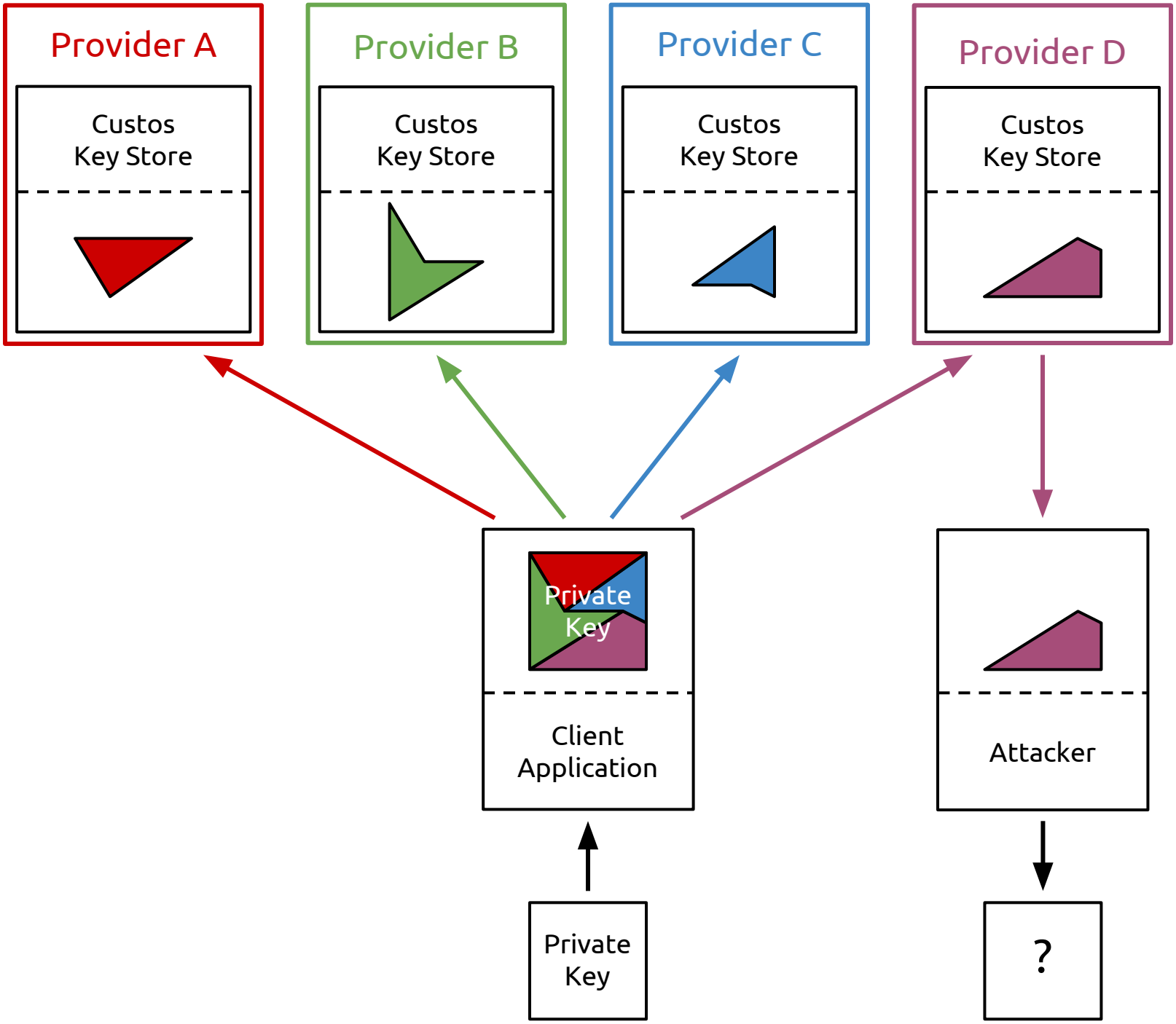
Better at Protecting Our Data

Questions

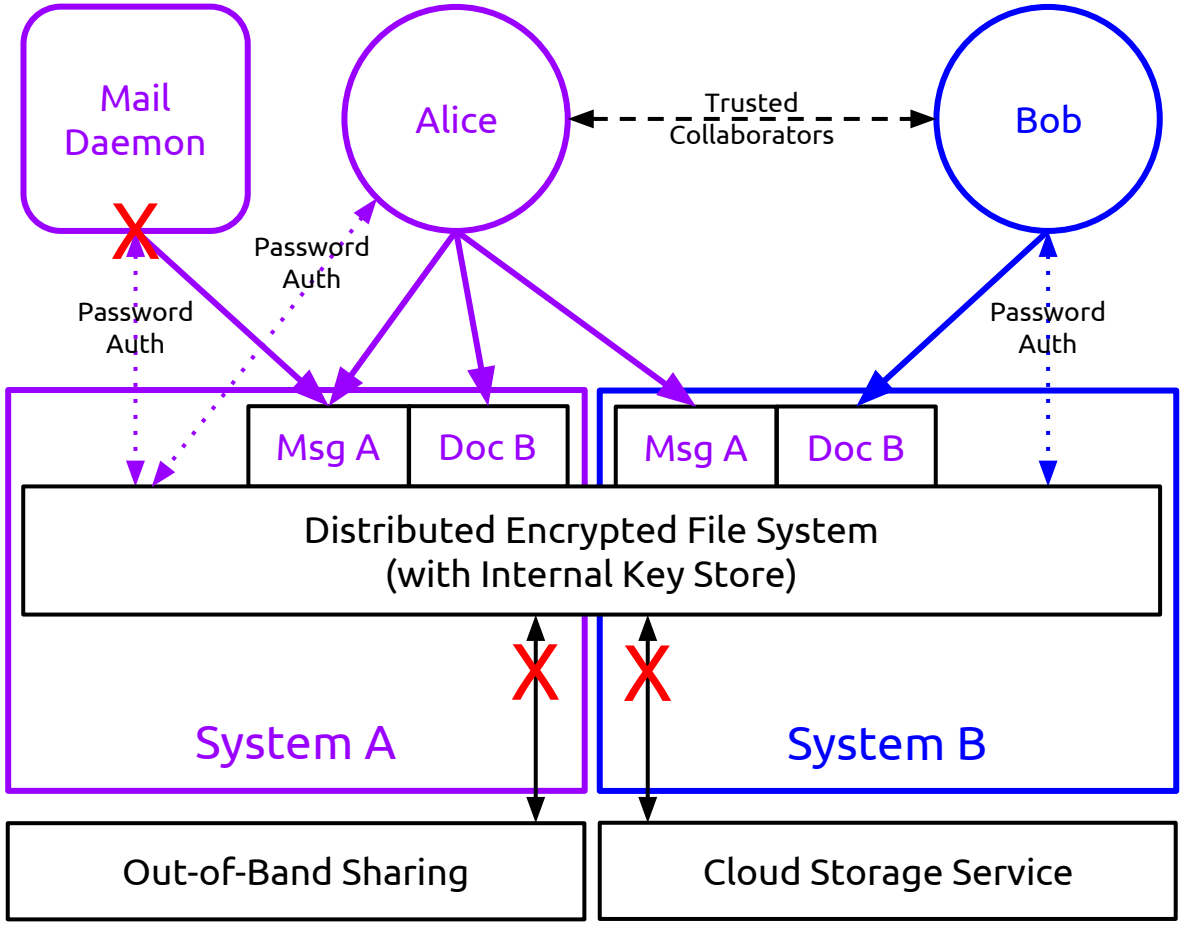
Extra Slides

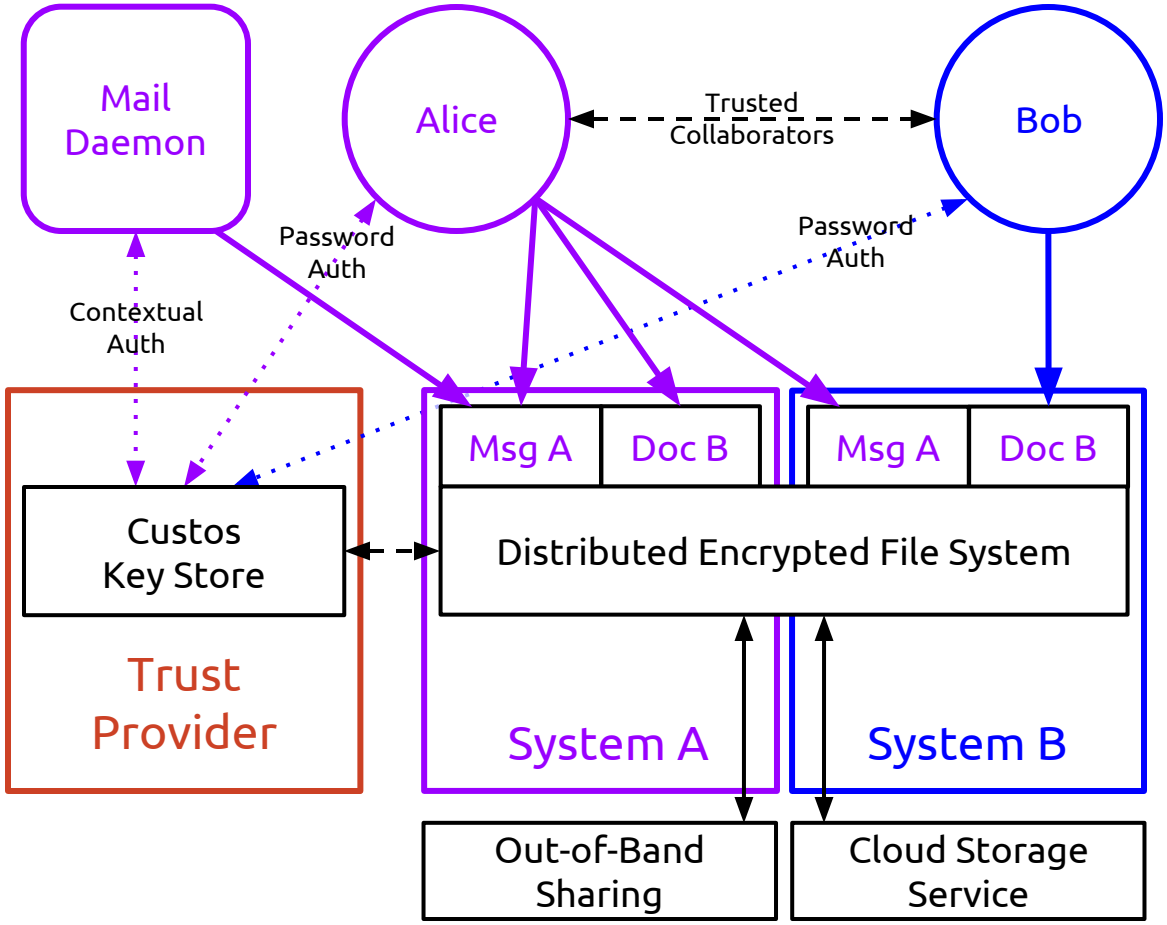
Avoiding a Trusted Third Party

Shamir’s Secret Sharing


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

Full Stack File Systems


Mail Daemon
Alice
Trusted Collaborators
Bob
Password Auth
Password Auth
Password Auth
Msg A
Doc B
Msg A
Doc B
Distributed Encrypted File System
(with Internal Key Store)
System A
System B
Out-of-Band Sharing
Cloud Storage Service


Mail Daemon
Alice
Trusted Collaborators
Bob
Password Auth
Password Auth
Contextual Auth
Msg A
Doc B
Msg A
Doc B
Custos Key Store
Distributed Encrypted File System
Trust Provider
System A
System B
Out-of-Band Sharing
Cloud Storage Service

Example “Create” API Call

Authentication Attributes (JSON)


```
[
    {
        "Class": "explicit",
        "Type": "user_id",
        "Value": "YXNheWxlcgA=",
        "Echo": true
    },
    {
        "Class": "explicit",
        "Type": "psk",
        "Value": "TXlPYmplY3RDcmVhdGlvblBhc3N3b3JkA
                  A==",
        "Echo": false
    }
]
```

Request URL

```
POST https://custos.net/grp/cc4273ae-4e1e-11e3-90d4-
10bf487b3e94/obj?aa=%5B%20%7B%20%22Class%22%3A%20%
22explicit%22%2C%20%22Type%22%3A%20%22user_id%22%2C%
20%22Value%22%3A%20%22YXNheWxlcgA%3D%22%2C%20%
22Echo%22%3A%20true%20%7D%2C%20%7B%20%22Class%22%3A%
20%22explicit%22%2C%20%22Type%22%3A%20%22psk%22%2C%
20%22Value%22%3A%20%
22TXlPYmplY3RDcmVhdGlvblBhc3N3b3JkAA%3D%3D%22%2C%20%
22Echo%22%3A%20false%20%7D%20%5D
```

Request Body (JSON)

```
{
    "Keys": [
        {
           "Value": "VHdhcyBicmlsbGlnLC
                     BhbmQgdGhlIHNsaXRo
                     eSB0b3ZlczsgRGlkIG
                     d5cmUgYW5kIGdpbWJs
                     ZSBpbiB0aGUgd2FiZQ
                     A=",
           "Echo": true
        }
    ],
    ...
```

Request Body (JSON) - Continued

```
...
    "ACSs": [
       {
           "Permissions":
           {
              "obj_delete": null,
              "obj_read": [
                  [
                     {
                         "Class": "explicit",
                         "Type": "user_id",
                         "Value": "YXNheWxlcgA=",
                         "Echo": true
                     }
                  ]
              ]
               ...
```

Response (JSON)


```
{
    "Status": "okay",
    "Keys": [
        {
            "Value":"VHdhcyBicmlsbGlnLC
                     BhbmQgdGhlIHNsaXRo
                     eSB0b3ZlczsgRGlkIG
                     d5cmUgYW5kIGdpbWJs
                     ZSBpbiB0aGUgd2FiZQ
                     A=",
            "Echo": true,
            "Revision": 0,
            "UUID": "7af8c95d-479a...",
            "Status": "accepted"
        }
    ],
...
```

Response (JSON) - Continued

```
...
    "ACSs": [
        {
            "Permissions":
            {
                "obj_delete": null,
                "obj_read": [
                    [
                        ...
                    ]
                ]
                ...
            },
            "Echo": true,
            "Status": "accepted"
        }
    ],
...
```

Response (JSON) - Continued

```
...
"Attrs": [
        {
            "Class": "explicit",
            "Type": "user_id",
            "Value": "YXNheWxlcgA=",
            "Echo": true,
            "Status": "accepted",
            "ResValue": null
        },
        ...
```

Filesystem References

Kubiatowicz, et. al. OceanStore. ASN 2000.

Kallahalla, et. al. Platus. FST 2003.

Wilcox-O'Hearn, et. al. Tahoe. SSS 2008.

Mahajan, et. al. Depot. TCS 2011.

Geambasu, et. al. Keypad. EuroSys 2011.

Usability References

Whitten & Tygar. Why Johnny Can't Encrypt. USENIX Security. 1999

Anderson. Why information security is hard. CSAC. 2001

Furnell. Usability versus Complexity. Network Security. 2010

Crypto References

Diffie & Hellman. New directions in cryptography. IEEE Trans. on IT. 1976

Shamir. How to share a secret. Comm ACM. 1979.

Schneider. Applied Cryptography. 1996

Denning & Branstad. A Taxonomy for Key Escrow Encryption Sys. Comm ACM. 1996