Department of Information Engineering and Computer Science

Master's degree in Computer Science - AY 2018-2019

FINAL DISSERTATION

A Pragmatic Approach to Handle "Honest but Curious" Cloud Service Providers: Cryptographic Enforcement of Dynamic Access Control Policies

Student
Stefano Berlato

Supervisor
Prof. Silvio Ranise

Co-supervisor
Dr. Roberto Carbone

Agenda

1. Introduction
2. Analysis of the Cryptographic AC Scheme
3. Architectures
4. Implementation with AWS
5. Conclusions and Future Work


amazon
web services


Google Cloud


IBM Cloud


Azure

amazon web services | Google Cloud | IBM Cloud | Azure

56%

EU Large Companies use Cloud

2º Service in Cloud

Store of Data

the statistical office of the European Union Eurostat. *Cloud computing services used by more than one out of four enterprises in the EU.*

56%

EU Large Companies use Cloud

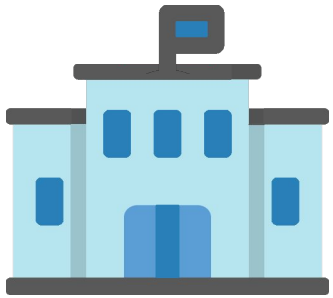
2° Service in Cloud

Store of Data

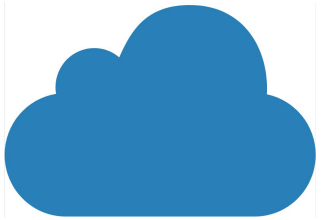
Also Italian PA is moving to the Cloud

"AGID - Il Cloud della Pubblica Amministrazione"

Agenzia per l'Italia Digitale AGID. *Il Cloud della Pubblica Amministrazione. L'adozione del modello cloud computing nelle amministrazioni italiane.*



Municipality



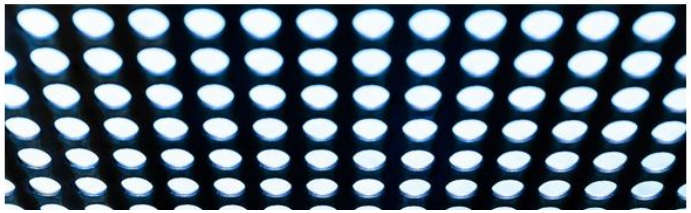
CSP

The Scarily Common Screw-Up That Exposed 198 Million Voter Records

GEAR IDEAS SCIENCE

LILY HAY NEWMAN SECURITY 06.19.17 07:37 PM

THE SCARILY COMMON SCREW-UP THAT EXPOSED 198 MILLION VOTER RECORDS



https://www.wired.com/story/voter-records-exposed-database/

The Scarily Common Screw-Up That Exposed 198 Million Voter Records

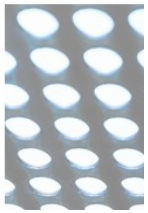
GEAR IDEAS SCIENCE

Here's What It's Like to Accidentally Expose the Data of 230M People

GEAR IDEAS SCIENCE

LILY HAY NEWMAN

THE SC
UP THA
VOTER



ANDY GREENBERG SECURITY 03.18.19 07:00 AM

HERE'S WHAT IT'S LIKE TO ACCIDENTALLY EXPOSE THE DATA OF 230M PEOPLE

https://www.wired.com/story/exactis-data-leak-fallout/

The Scarily Common Screw-Up That Exposed 198 Million Voter Records

GEAR IDEAS SCIENCE

Here's What It's Like to Accidentally Expose the Data of 230M People

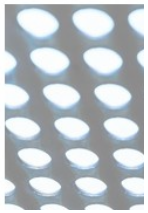
LILY HAY NEWMAN

GEAR IDEAS SCIENCE

THE SC
UP THA
VOTER

ANDY GREENBERG SECURITY 03

HERE'S WH
ACCIDENTA
DATA OF 23



Blame Human Error for WWE and Verizon's Massive Data Exposures

GEAR IDEAS SCIENCE

LILY HAY NEWMAN SECURITY 07.15.17 08:00 AM

BLAME HUMAN ERROR FOR WWE AND VERIZON'S MASSIVE DATA EXPOSURES

https://www.wired.com/story/amazon-s3-data-exposure/

The Scarily Common Screw-Up That Exposed 198 Million Voter Records

GEAR IDEAS SCIENCE

Here's What It's Like to Accidentally Expose the Data of 230M People

LILY HAY NEWMAN

GEAR IDEAS SCIENCE

THE SC
UP THA
VOTER

ANDY GREENBERG SECURITY 03

HERE'S WH
ACCIDENTA
DATA OF 23

Blame Human Error for WWE and Verizon's Massive Data Exposures

GEAR IDEAS SCIENCE

LILY HAY NEWMAN SECURITY

BLAME HU
WWE AND
DATA EXPO

Security News This Week: The Pentagon Left Data Exposed in the Cloud

GEAR IDEAS SCIENCE

BRIAN BARRETT SECURITY 11.18.17 09:00 AM

SECURITY NEWS THIS WEEK:
THE PENTAGON LEFT DATA
EXPOSED IN THE CLOUD

https://www.wired.com/story/security-news-this-week-the-pentagon-left-data-exposed-in-the-cloud/

Only 4% data involved in breaches was encrypted

Breach Level Index. *Data Breach Statistics. Data Records Lost or Stolen since 2013.*

→ Field Encryption

https://www.mongodb.com/blog/post/mongodb-42-previewed-at-mongodb-world

Field Encryption

Personal Vault

https://www.microsoft.com/en-us/microsoft-365/blog/2019/06/25/onedrive-personal-vault-added-security-onedrive-additional-storage/

→ Field Encryption

→ Personal Vault

→ Secure Google Cloud

https://atos.net/en/2019/press-release_2019_05_16/veolia-chooses-atos-to-develop-its-secure-collaborative-environment-with-g-suite-from-google-cloud-2

→ Field Encryption

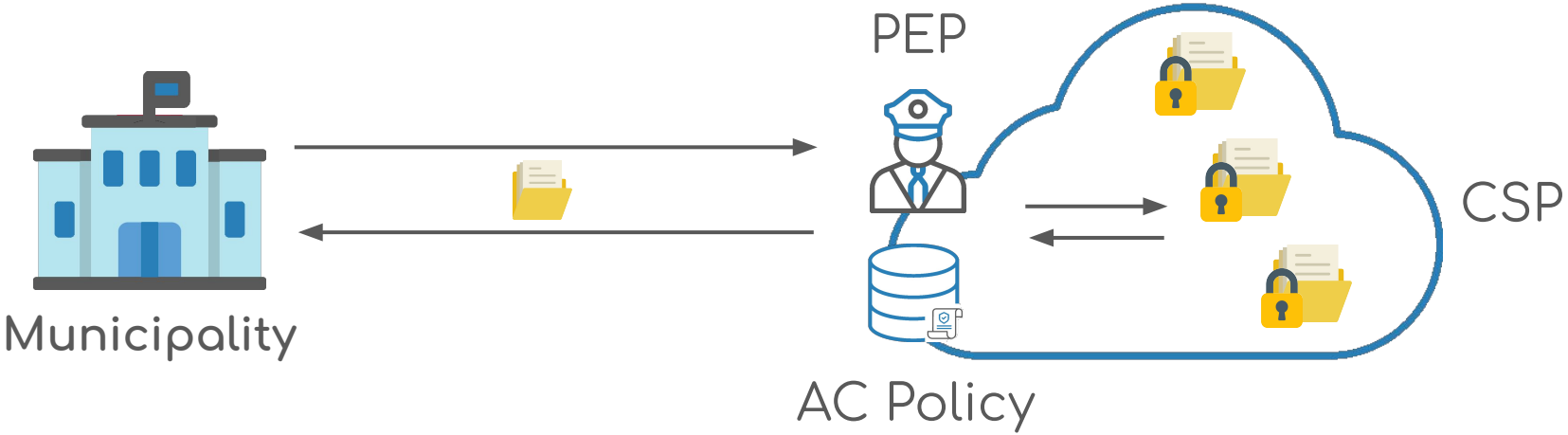
→ Personal Vault

→ Secure Google Cloud

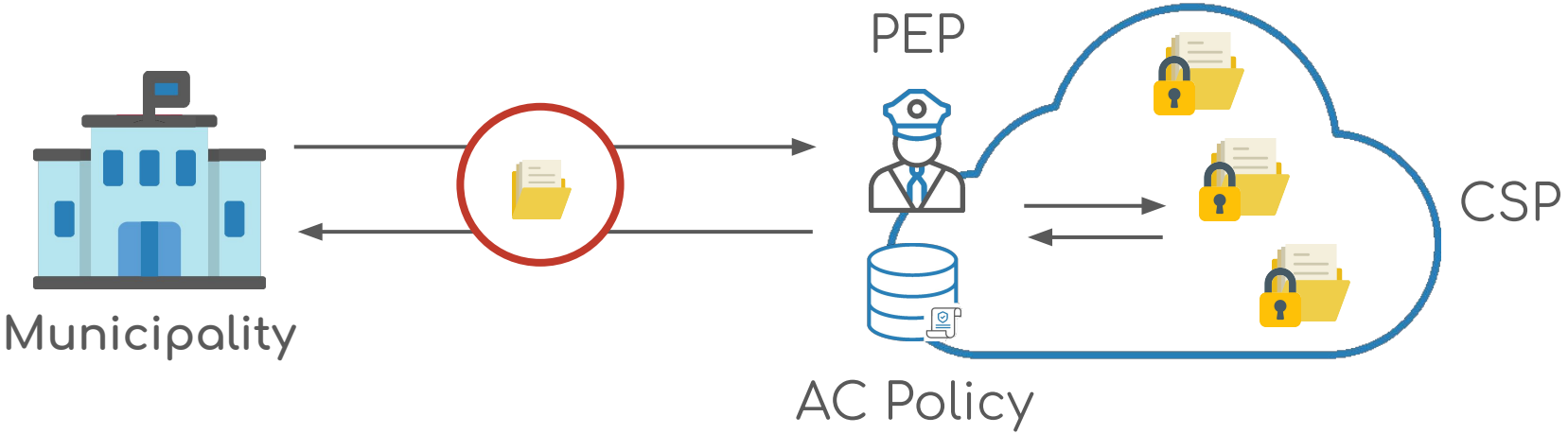
→ Cloud-side Encryption

https://docs.aws.amazon.com/en_us/AmazonS3/latest/dev/bucket-encryption.html

Cloud-side Encryption

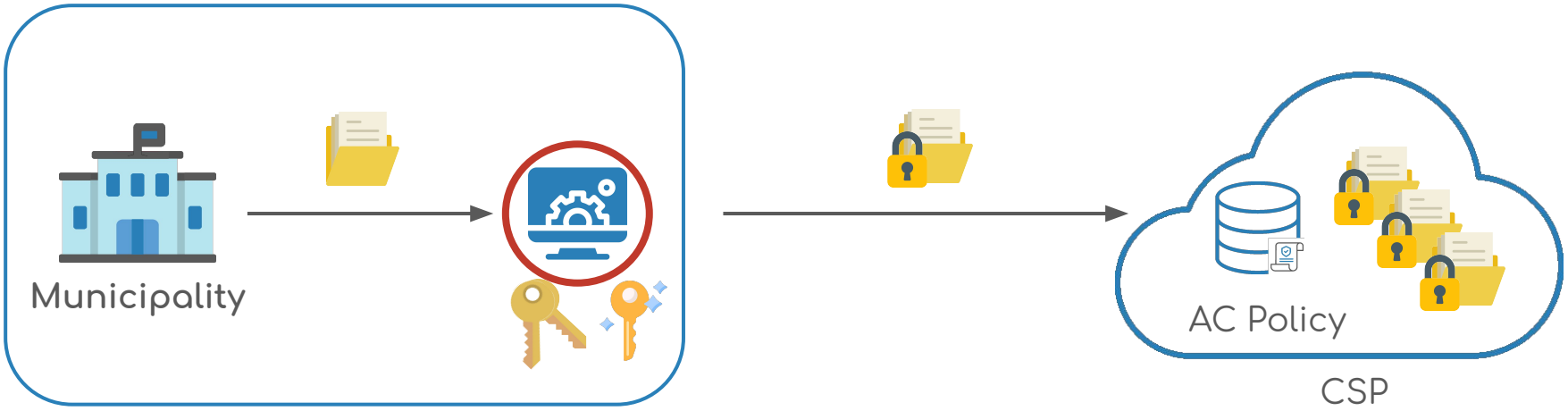


CSP is Honest but Curious



Cryptographic Access Control

Abstract Approaches



Abstract Approaches

No pragmatic issues (e.g. Keys Management) [1,2]

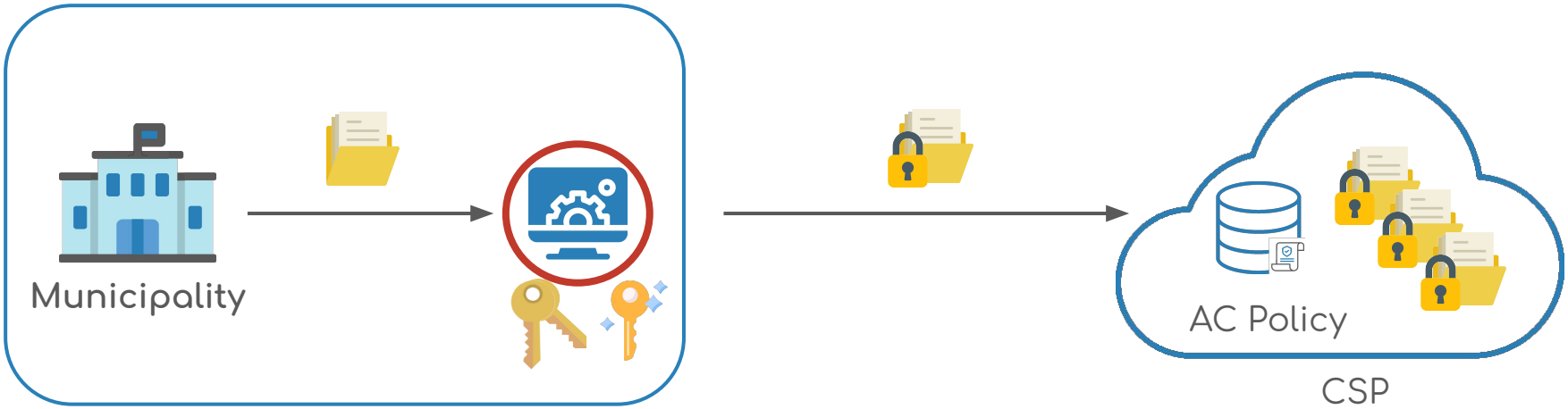
[1] Sascha Muller and Stefan Katzenbeisser. *Hiding the Policy in Cryptographic Access Control*. In: "Security and Trust Management". 2012, pp. 90–105. DOI: 10.1007/978-3-642-29963-6_8.
[2] Yang Tang, Patrick P. C. Lee, John C. S. Lui, and Radia Perlman. *FADE: Secure Overlay Cloud Storage with File Assured Deletion*. In: "Security and Privacy in Communication Networks". 2010, pp. 380–397.

Abstract Approaches

No architecture or fixed [3,4]

[3] Somchart Fugkeaw and Hiroyuk Sato. *Design and Implementation of Collaborative Ciphertext-Policy Attribute-Role based Encryption for Data Access Control in Cloud*. In: 2015.
[4] Saman Zarandioon, Danfeng (Daphne) Yao, and Vinod Ganapathy. *K2C: Cryptographic Cloud Storage With Lazy Revocation and Anonymous Access*. In: "International Conference on Security and Privacy in Communication Systems"

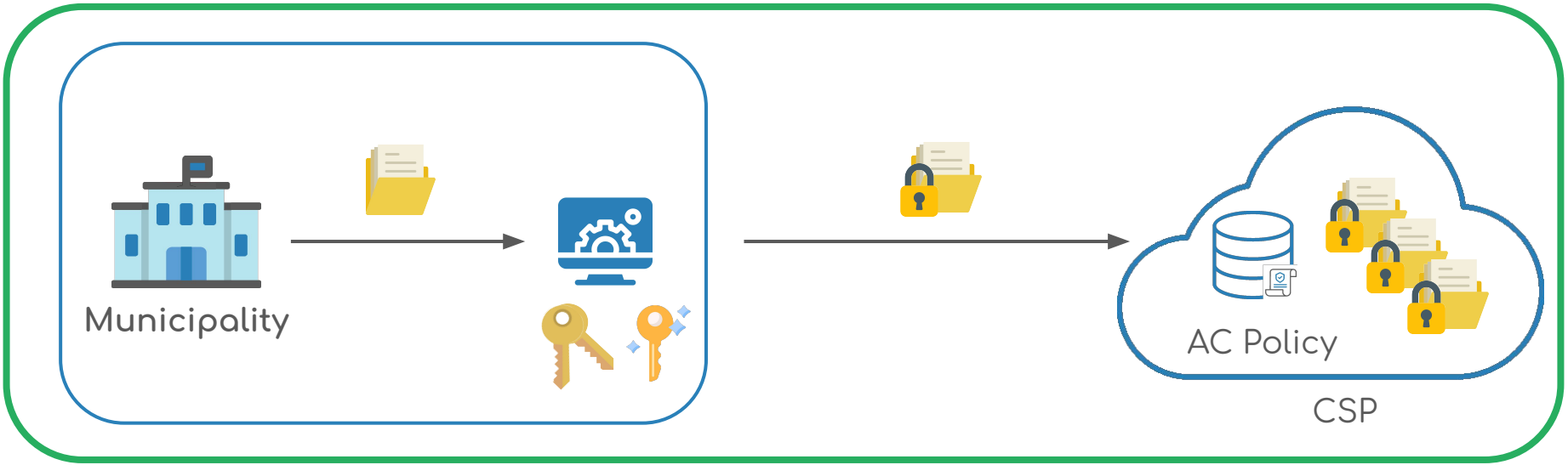
Abstract Approaches



Only prototypes for performance analysis [5,6]

[5] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. *Attribute-based encryption for fine-grained access control of encrypted data*. In: "Proceedings of the ACM Conference on Computer and Communications Security".
[6] Valentin Ghita, Sergiu Costea, and Nicolae Tapus. *Implementation of Cryptographically Enforced RBAC*. In: "The Scientific Bulletin - University Politehnica of Bucharest" 79.2 (2017), pp. 9-3–102.

Pragmatic Approach



Pragmatic approach to deploy a cryptographic AC scheme to handle Honest but Curious CSP

Pragmatic approach to deploy a cryptographic AC scheme to handle Honest but Curious CSP

1. **Analysis** of the cryptographic AC scheme

Pragmatic approach to deploy a cryptographic AC scheme to handle Honest but Curious CSP

1. **Analysis** of the cryptographic AC scheme
2. High-level properties, **requirements** and **assumptions***

*(not in this presentation)

Pragmatic approach to deploy a cryptographic AC scheme to handle Honest but Curious CSP

1. **Analysis** of the cryptographic AC scheme
2. High-level properties, **requirements** and **assumptions***
3. Design of alternative **architectures** and evaluation

*(not in this presentation)

Pragmatic approach to deploy a cryptographic AC scheme to handle Honest but Curious CSP

1. **Analysis** of the cryptographic AC scheme
2. High-level properties, **requirements** and **assumptions***
3. Design of alternative **architectures** and evaluation
4. **Implementation** of the chosen scheme with AWS

*(not in this presentation)

Pragmatic approach to deploy a cryptographic AC scheme to handle Honest but Curious CSP

1. **Analysis** of the cryptographic AC scheme
2. High-level properties, **requirements** and **assumptions***
3. Design of alternative **architectures** and evaluation
4. **Implementation** of the chosen scheme with AWS
5. **Requirements compliance** of the implementation*

*(not in this presentation)

1. Introduction
2. Analysis of the Cryptographic AC Scheme
3. Architectures
4. Implementation with AWS
5. Conclusions and Future Work

"On the Practicality of Cryptographically Enforcing Dynamic Access Control Policies in the Cloud" by Garrison et al.

Proceedings of 2016 IEEE Symposium on Security and Privacy (SP '16)

"On the Practicality of Cryptographically Enforcing Dynamic Access Control Policies in the Cloud" by Garrison et al.

Proceedings of 2016 IEEE Symposium on Security and Privacy (SP '16)

- **Dynamic** $RBAC_0$ policy
- Formulated **assumptions**
- Considered **efficiency**
- Presented **pseudocode**

Clients

Interact with files

CryptoAC

Cryptographic operations

Policy

AC Policy

CSP

Stores files

Clients

Interact with files

CryptoAC

Cryptographic operations

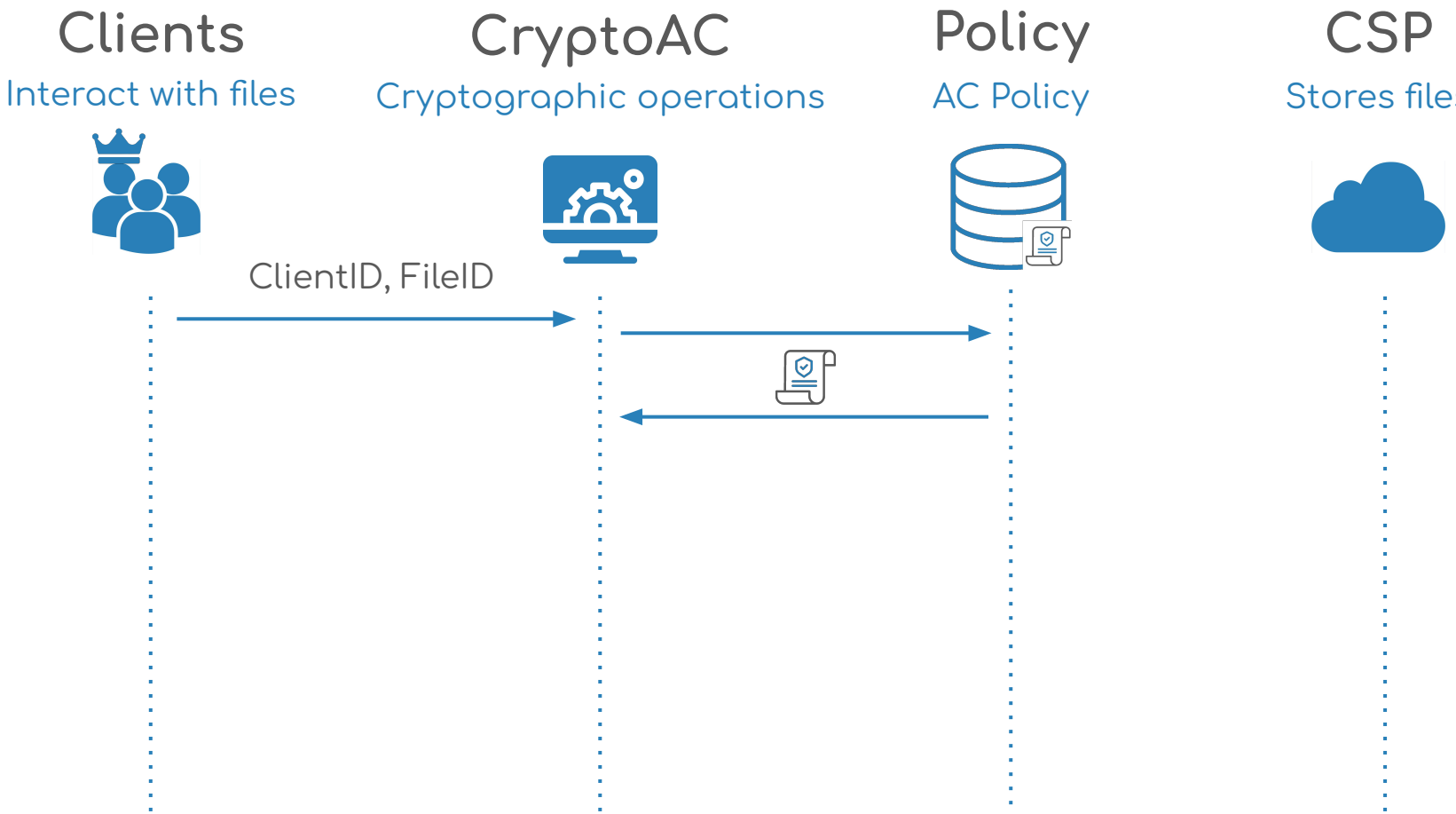
Policy

AC Policy

CSP

Stores files

ClientID, FileID


Clients
Interact with files
CryptoAC
Cryptographic operations
Policy
AC Policy
CSP
Stores files
ClientID, FileID

Clients

Interact with files

CryptoAC

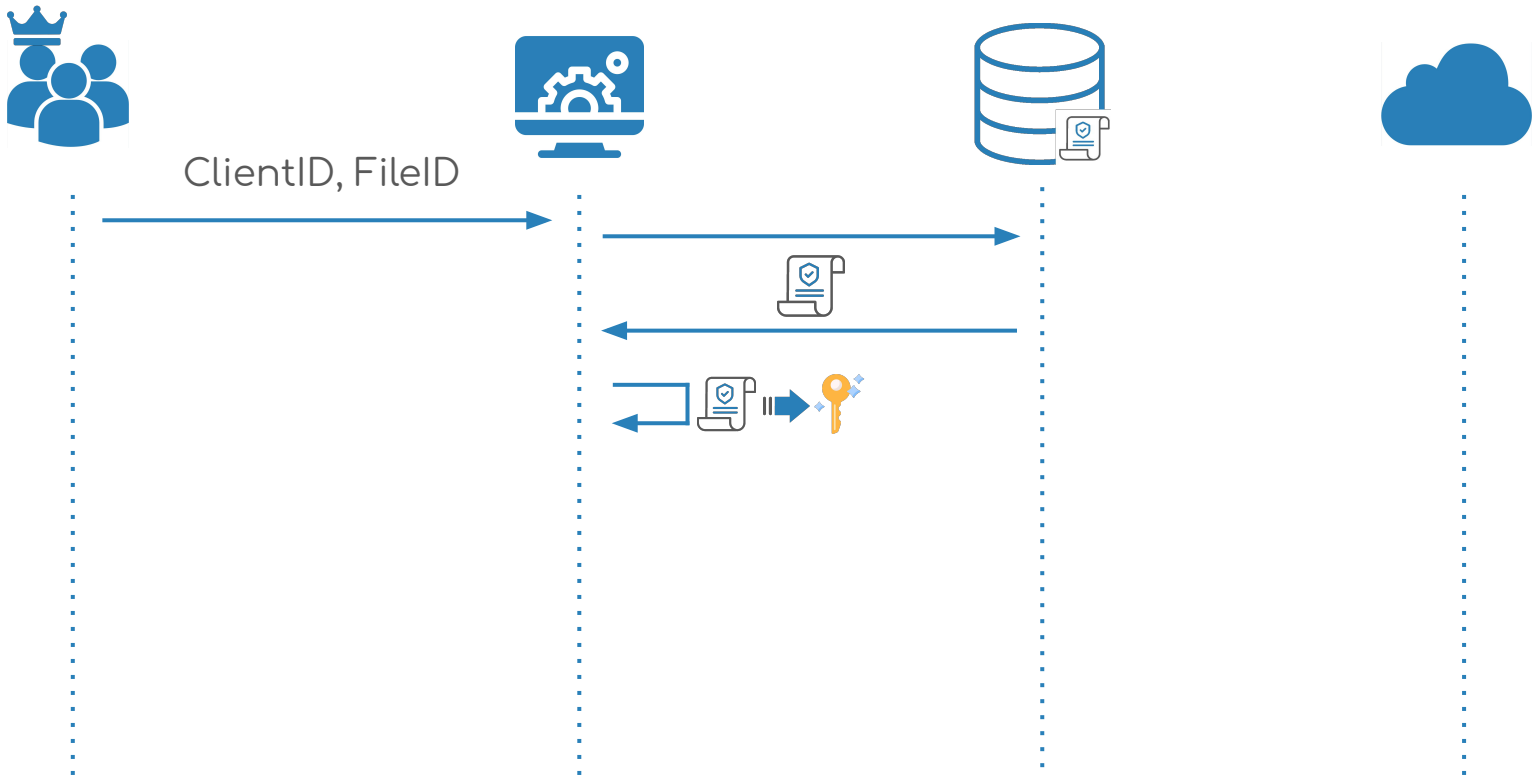
Cryptographic operations

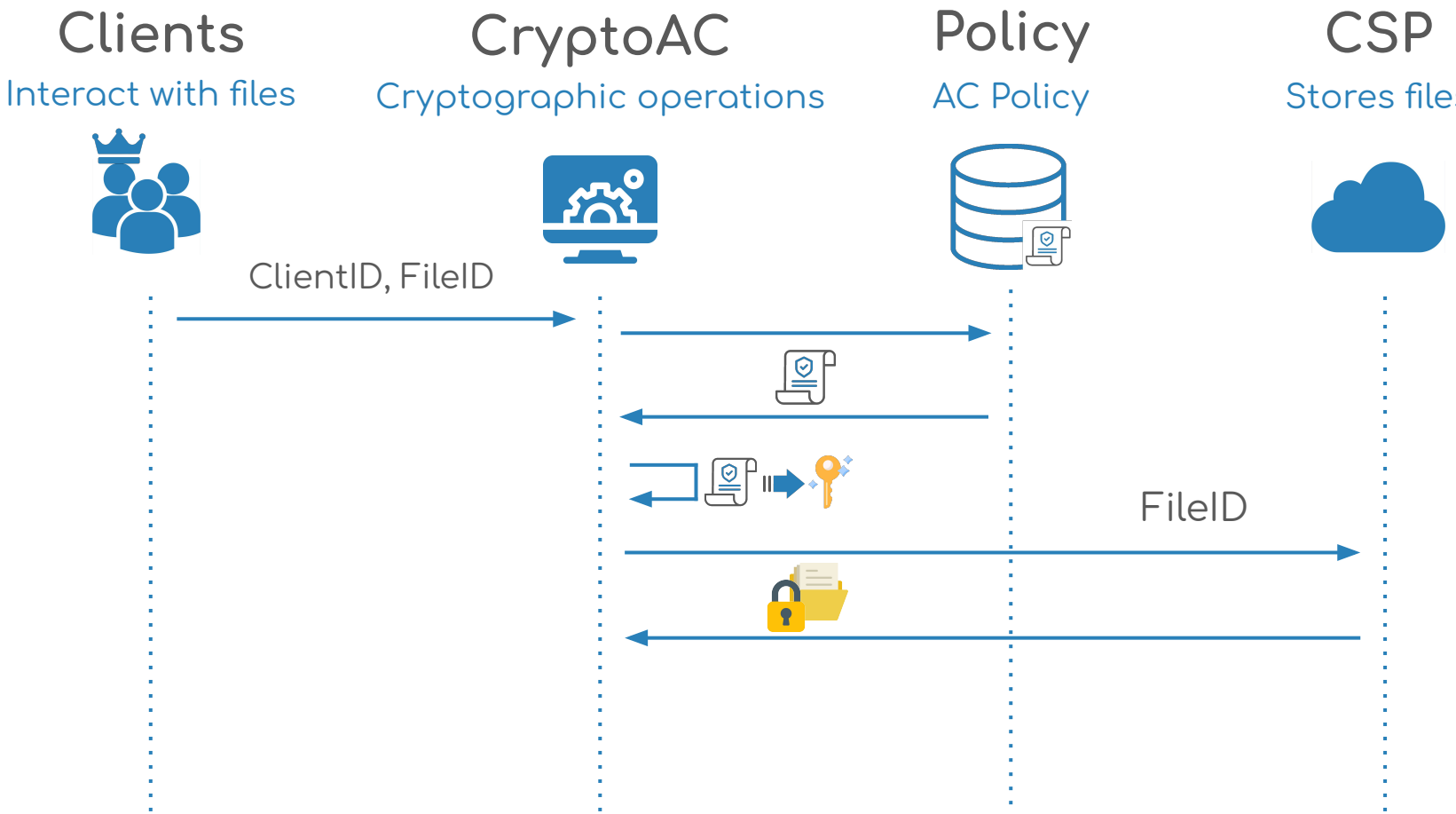
Policy

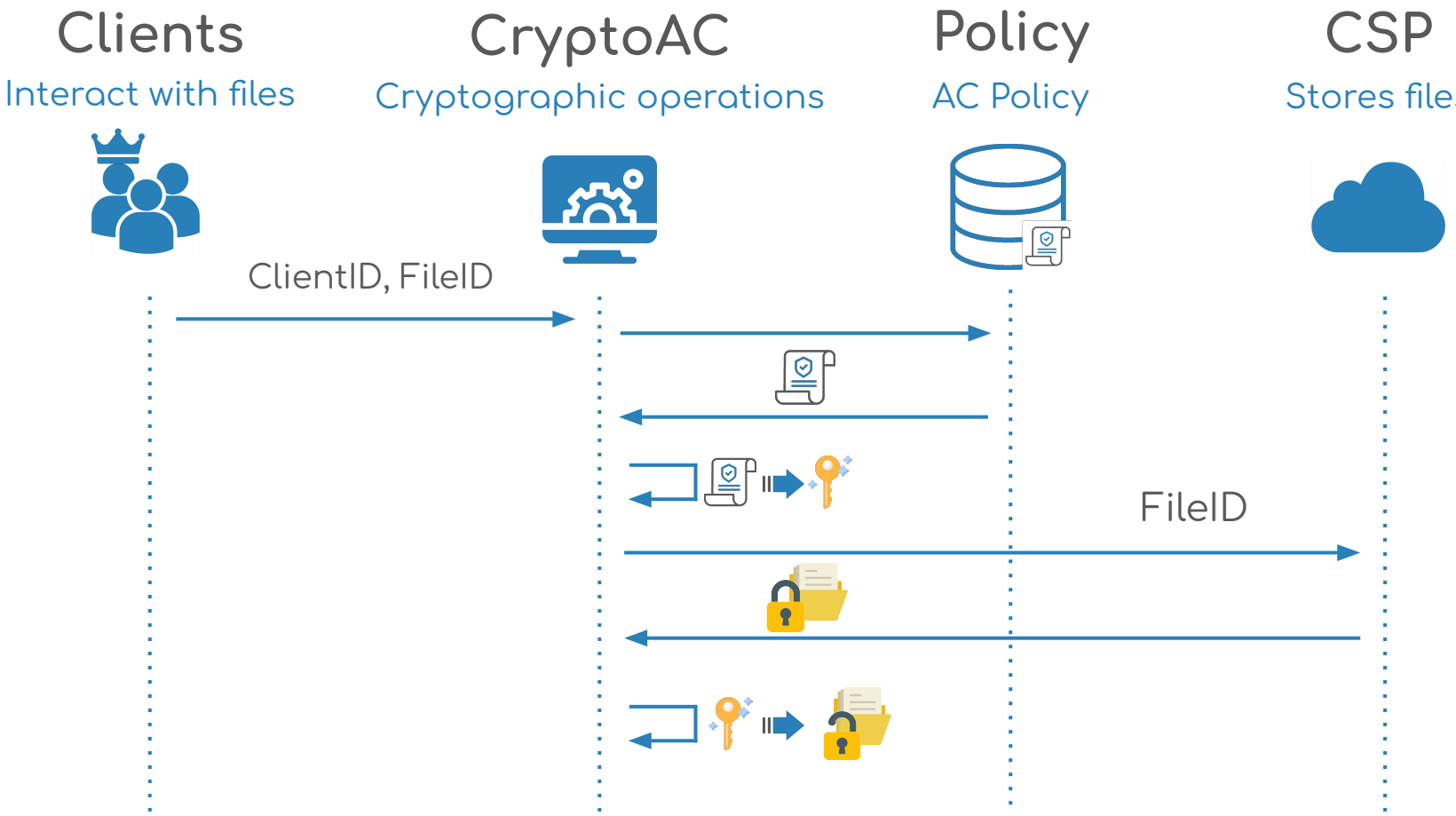
AC Policy

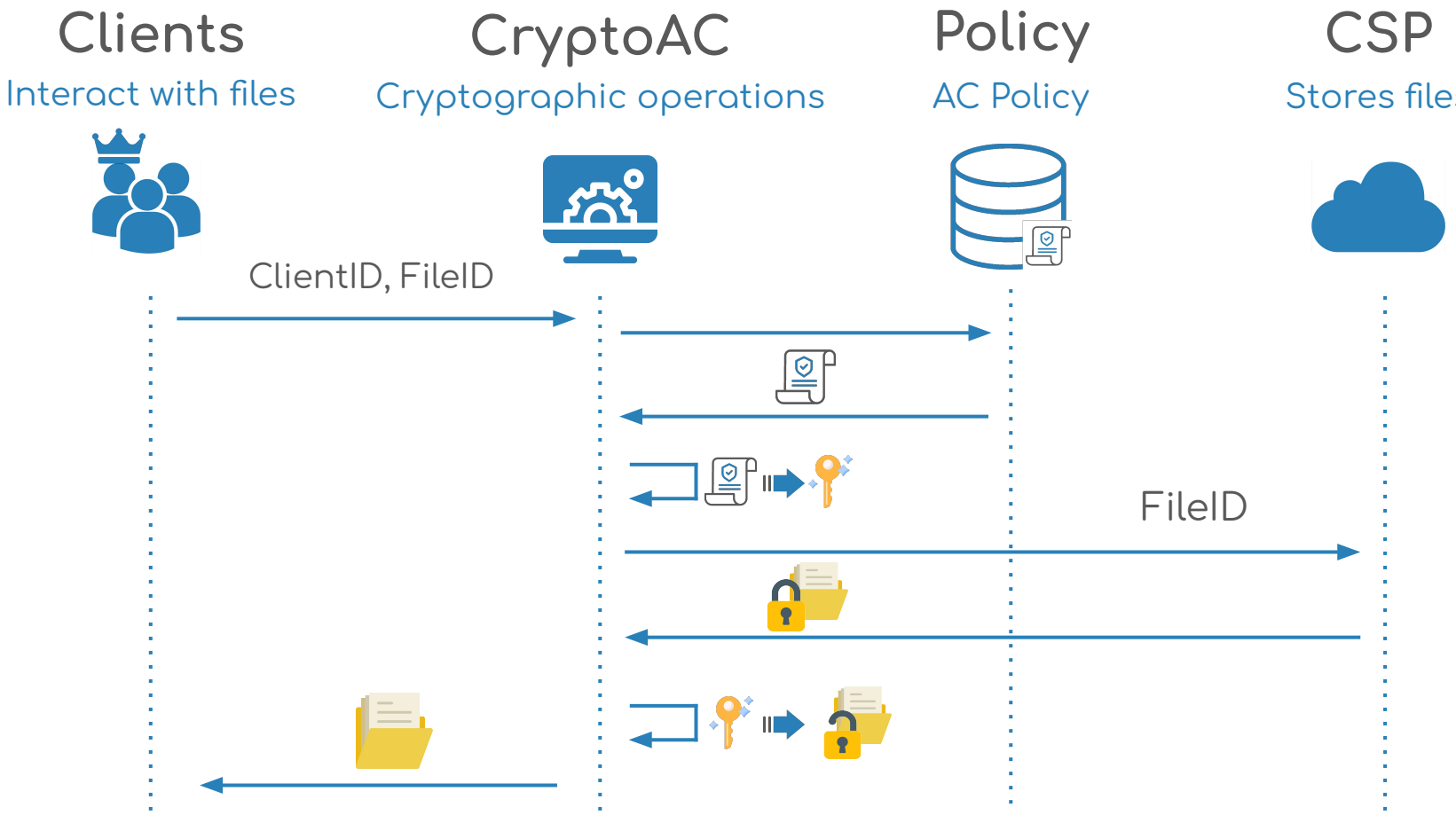
CSP

Stores files




Clients
Interact with files
CryptoAC
Cryptographic operations
Policy
AC Policy
CSP
Stores files
ClientID, FileID
FileID


Clients
Interact with files
CryptoAC
Cryptographic operations
Policy
AC Policy
CSP
Stores files
ClientID, FileID
FileID


Clients
Interact with files
CryptoAC
Cryptographic operations
Policy
AC Policy
CSP
Stores files
ClientID, FileID
FileID

Clients

Interact with files

CryptoAC

Cryptographic operations

Policy

AC Policy

RM

Checks clients' actions

CSP

Stores files

Clients

Interact with files

CryptoAC

Cryptographic operations

Policy

AC Policy

RM

Checks clients' actions

CSP

Stores files

ClientID,

Clients

Interact with files

CryptoAC

Cryptographic operations

Policy

AC Policy

RM

Checks clients' actions

CSP

Stores files

ClientID,

Clients

Interact with files

CryptoAC

Cryptographic operations

Policy

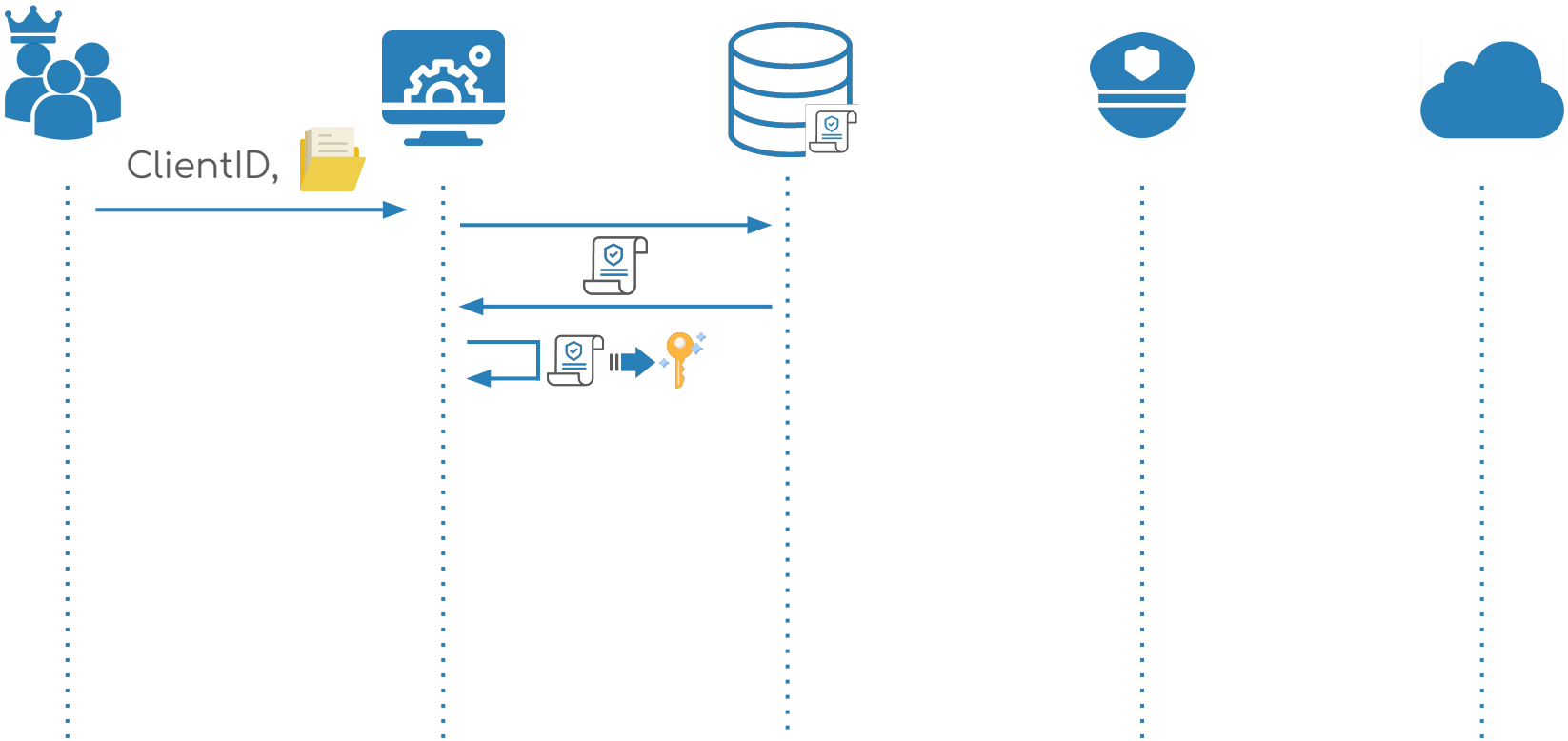
AC Policy

RM

Checks clients' actions

CSP

Stores files



Clients

Interact with files

CryptoAC

Cryptographic operations

Policy

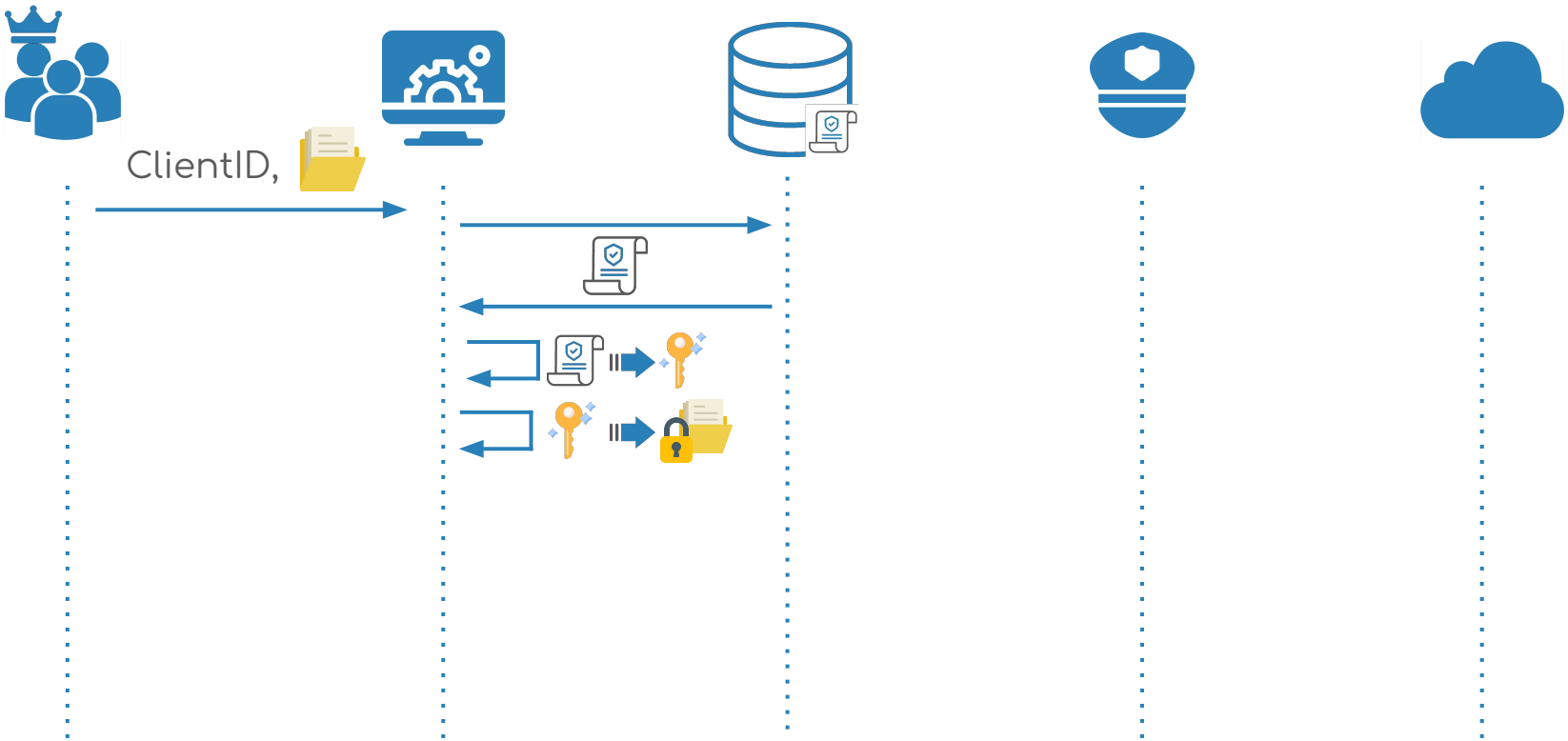
AC Policy

RM

Checks clients' actions

CSP

Stores files



Clients

Interact with files

CryptoAC

Cryptographic operations

Policy

AC Policy

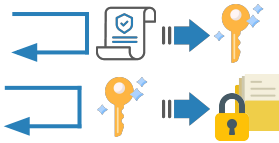
RM

Checks clients' actions

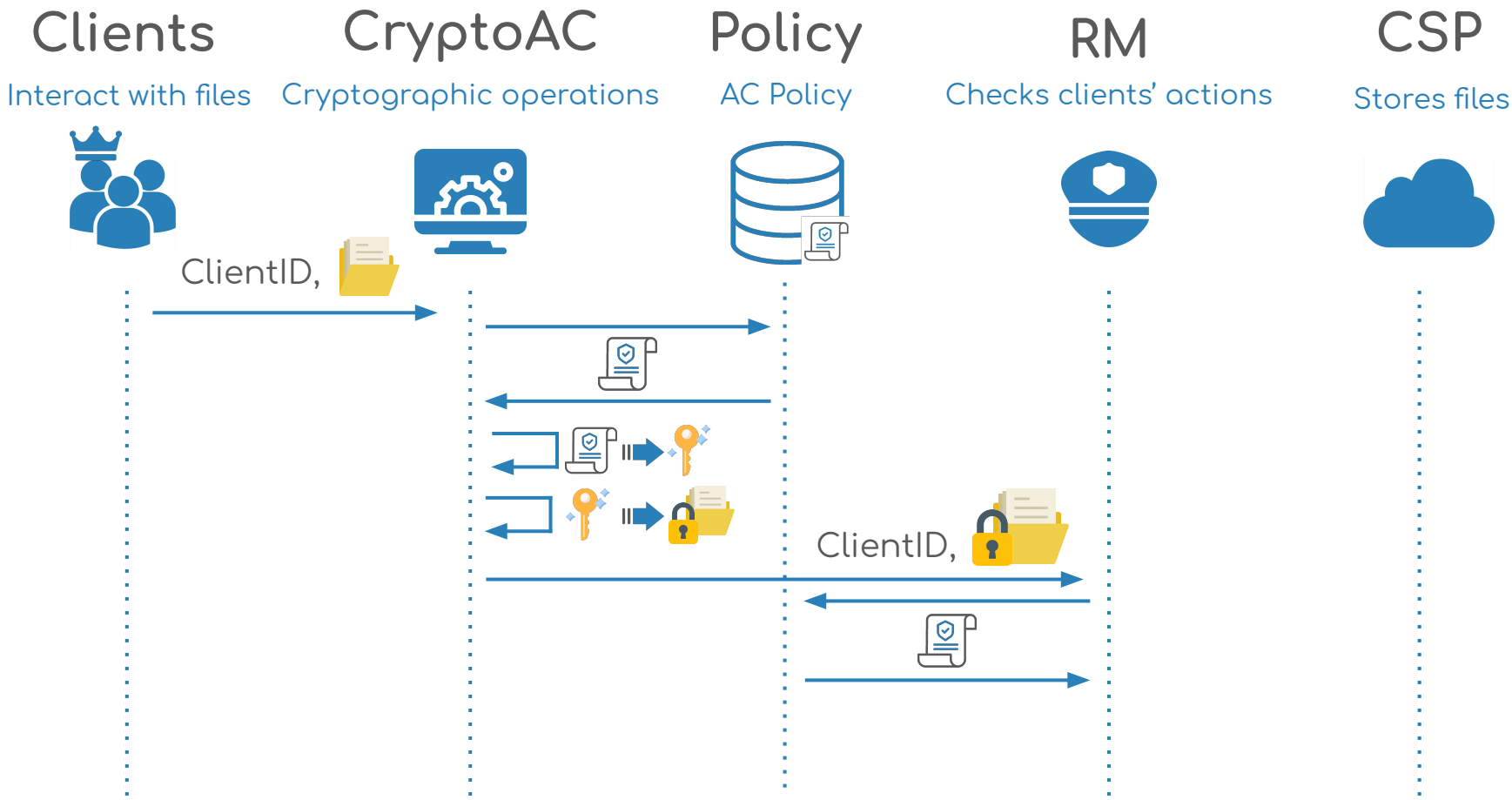
CSP

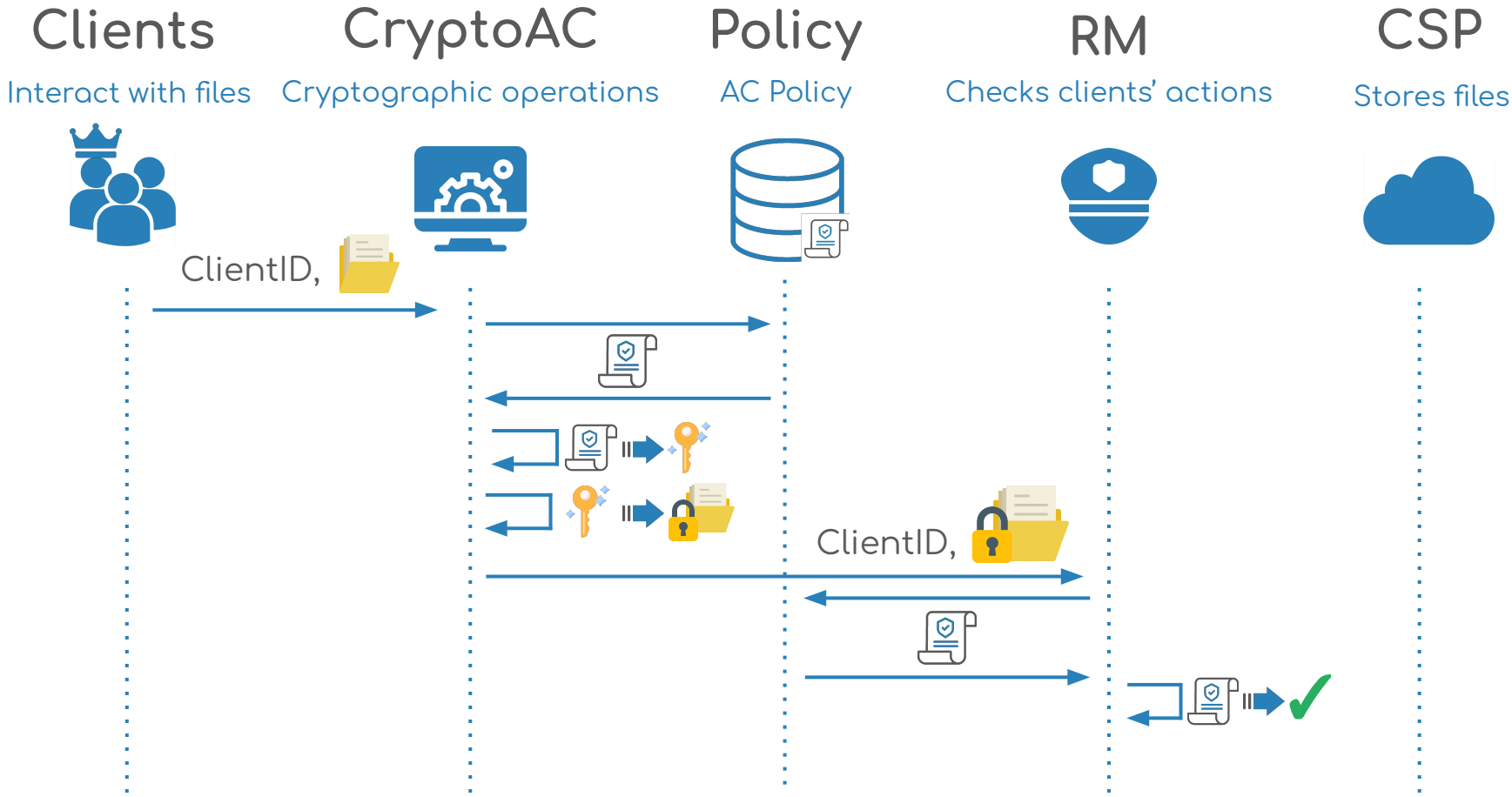
Stores files

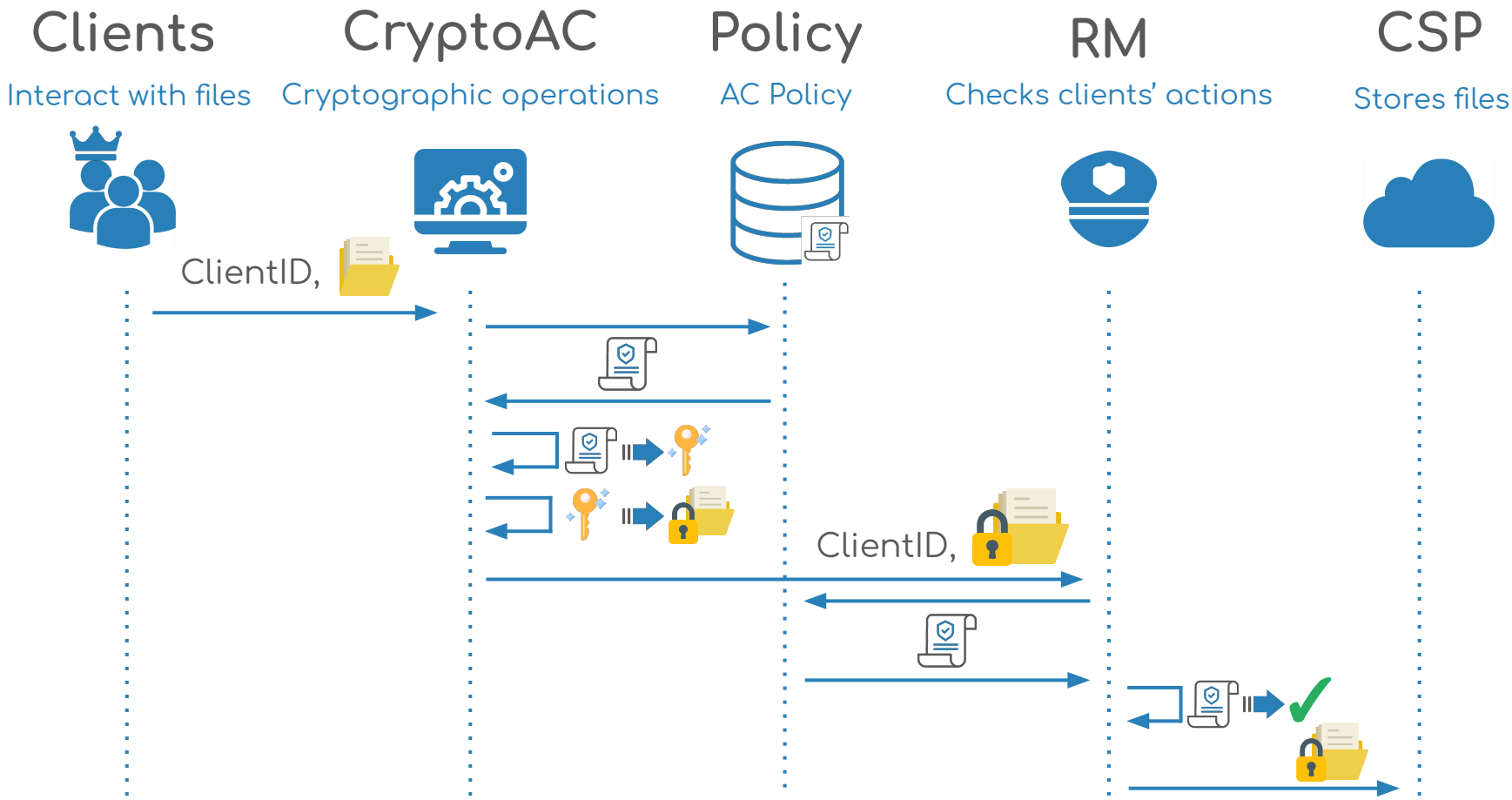
ClientID,



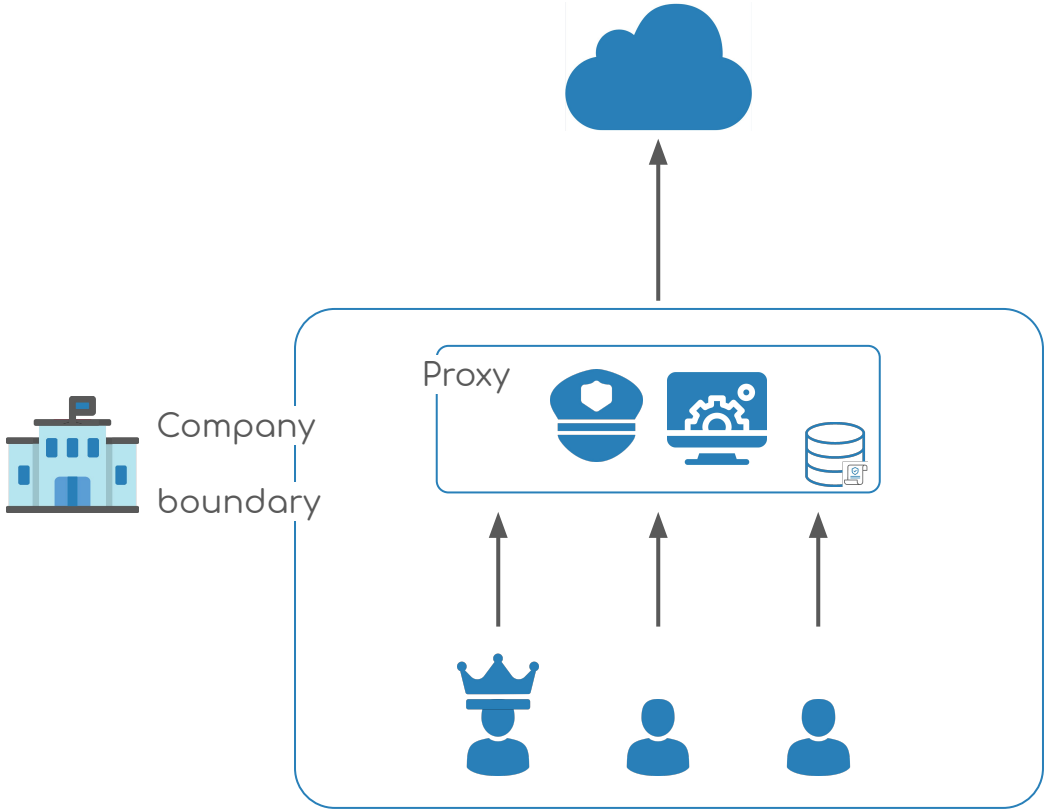
ClientID,

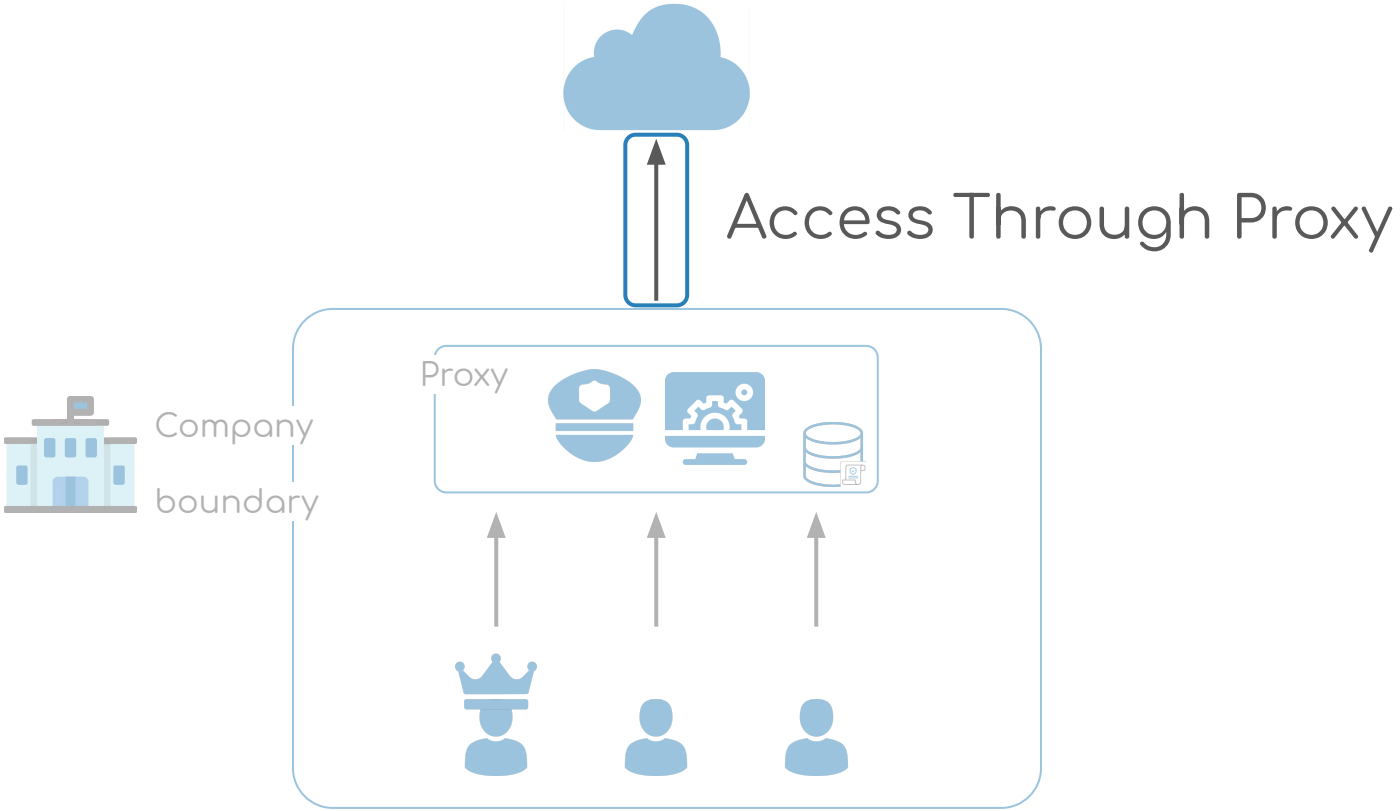

Clients
Interact with files
CryptoAC
Cryptographic operations
Policy
AC Policy
RM
Checks clients' actions
CSP
Stores files
ClientID,
ClientID,

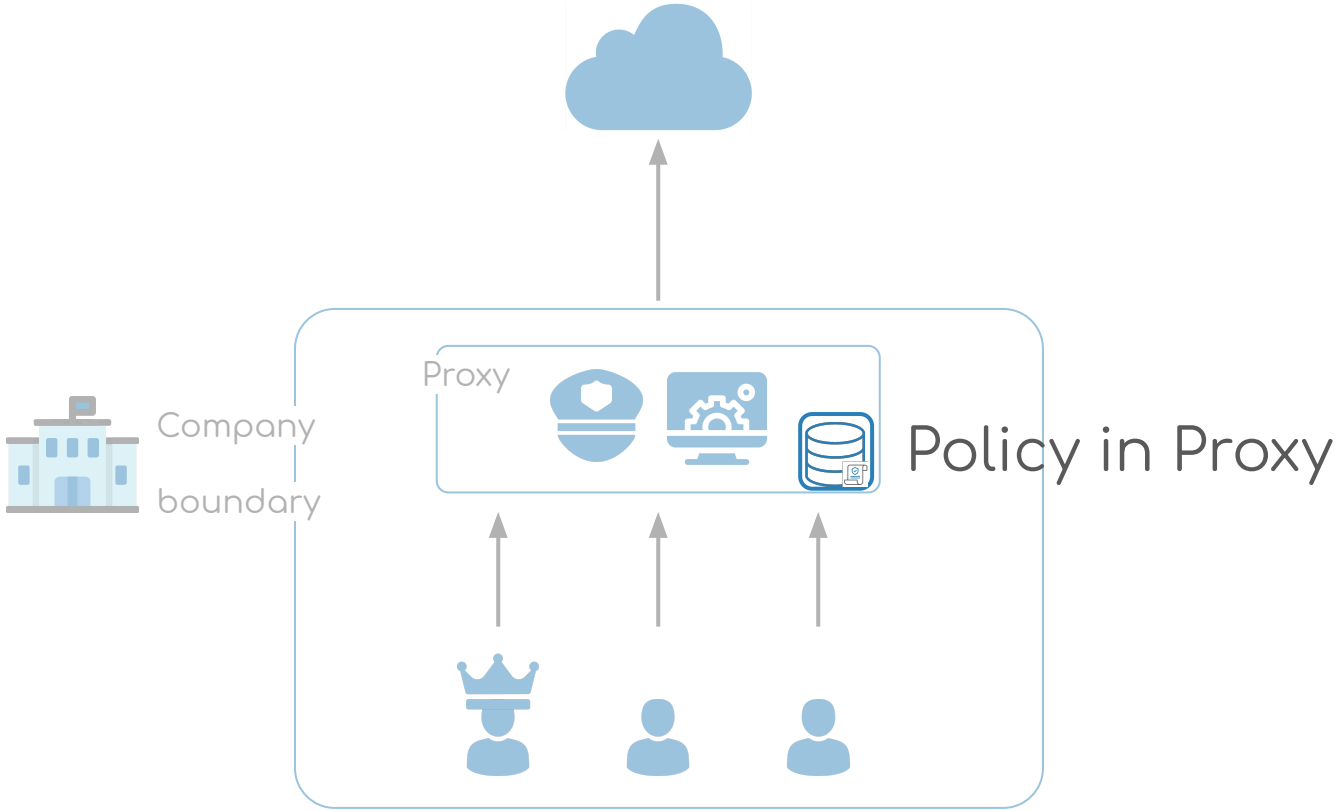

Clients
Interact with files
CryptoAC
Cryptographic operations
Policy
AC Policy
RM
Checks clients' actions
CSP
Stores files
ClientID,
ClientID,

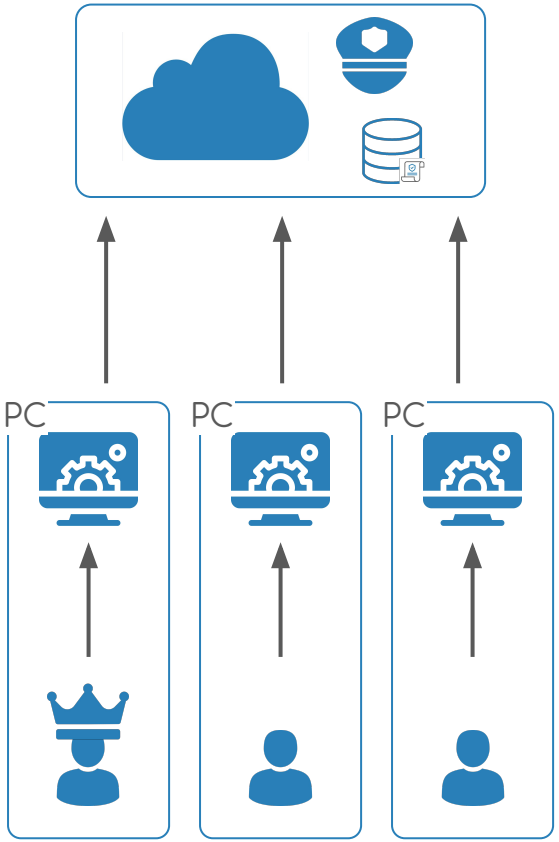

Clients
Interact with files
CryptoAC
Cryptographic operations
Policy
AC Policy
RM
Checks clients' actions
CSP
Stores files
ClientID,
ClientID,

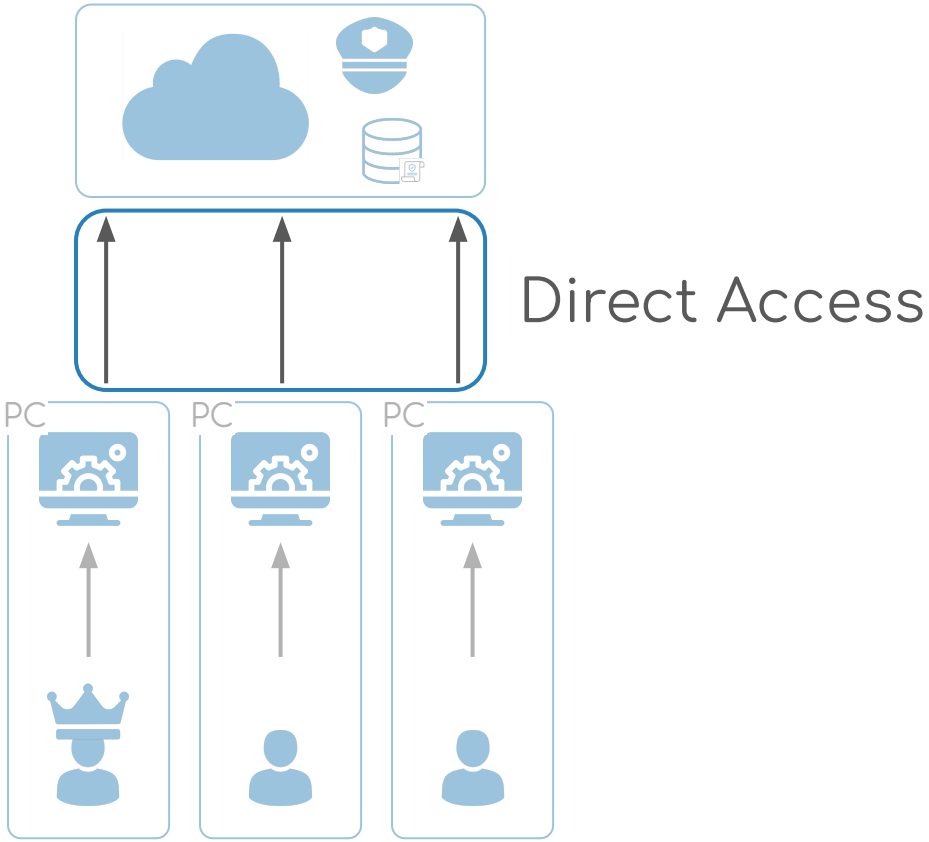
1. Introduction
2. Analysis of the Cryptographic AC Scheme
3. Architectures
4. Implementation with AWS
5. Conclusions and Future Work

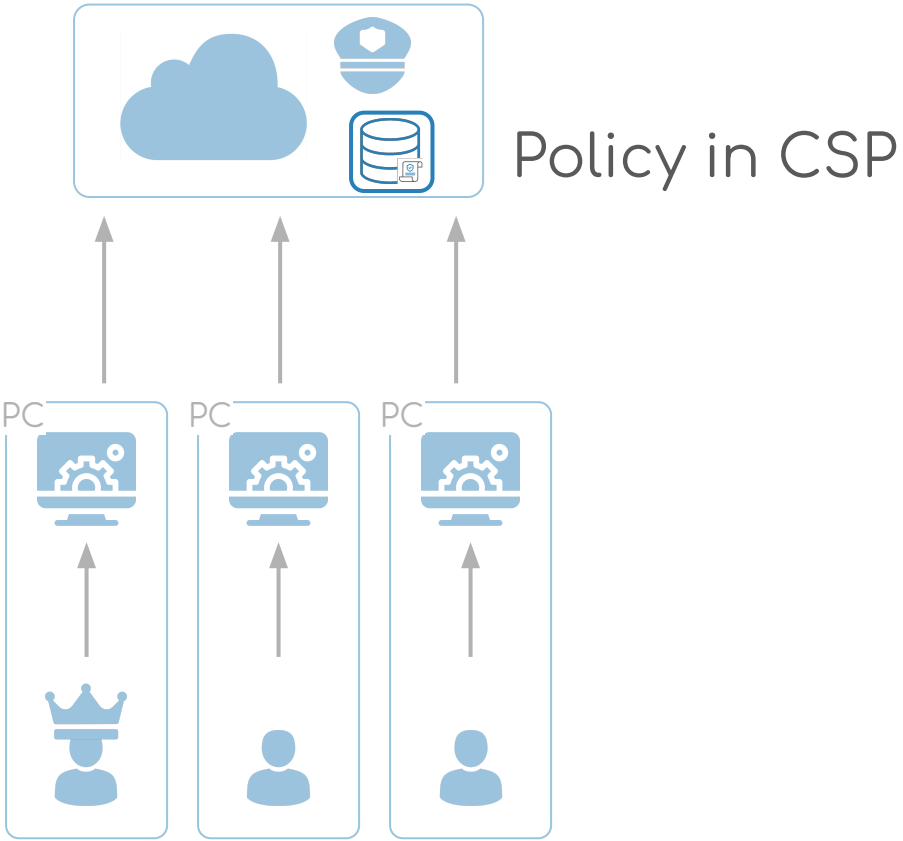

Proxy
Company
boundary


Access Through Proxy
Proxy
Company
boundary


Proxy
Company
boundary
Policy in Proxy


PC
PC
PC


Direct Access
PC
PC
PC


Policy in CSP
PC
PC
PC

Storage location of Policy

- Dedicated Server
- CSP
- Hybrid Solutions

Storage location of Policy

- Dedicated Server
- CSP
- Hybrid Solutions

Clients' access to CSP

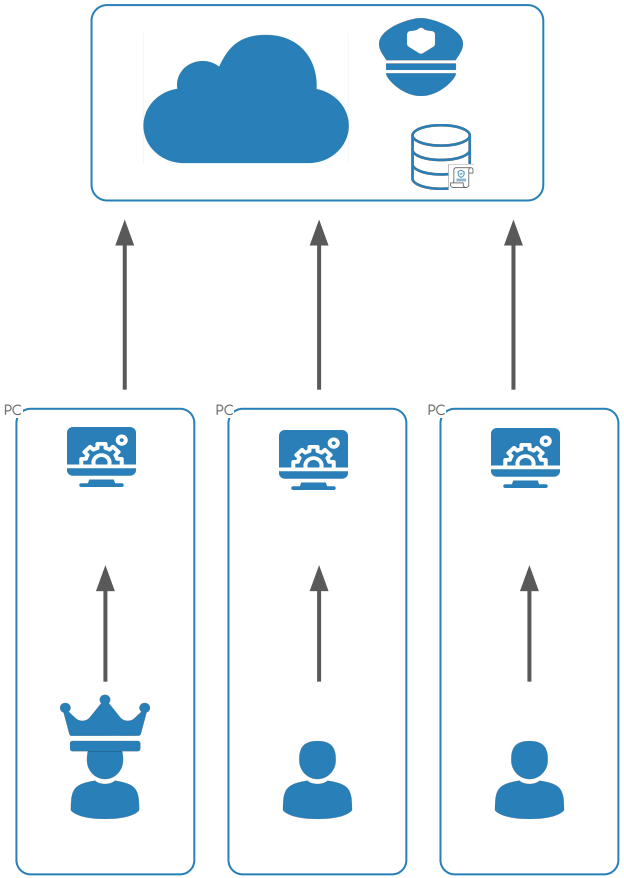
- Dedicated Proxy
- Direct Connection (personal credentials)
- Direct Connection (temporary credentials)

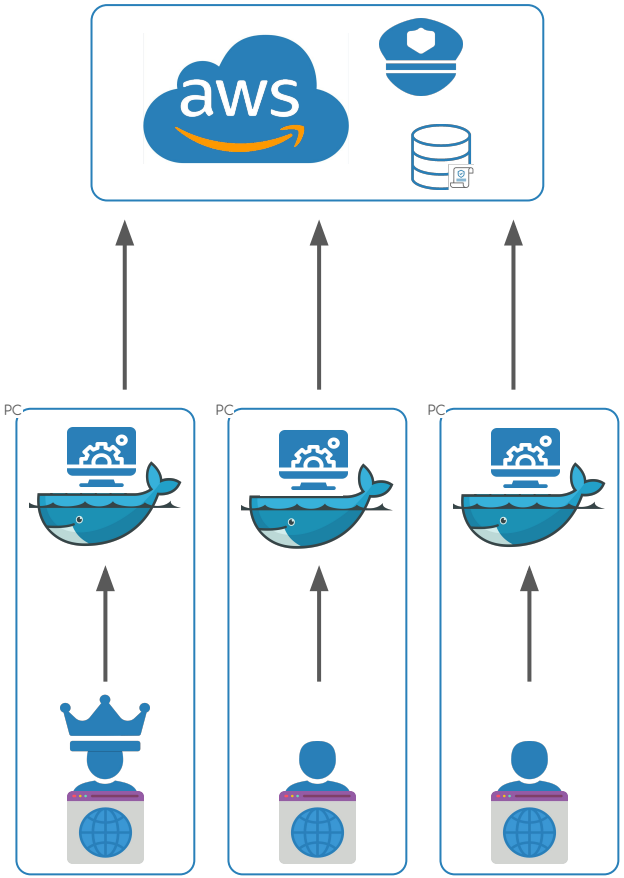
Feature	Proxy	Straight	...
Deployment Readiness	- -	+ +	
Keys Location	-	+	
Workload Management	- - - -	+ + + +	
Scalability	- - - -	+ + + +	
Robustness	- -	+ +	
Control on Policy Data	+ +	- -	
Policy Maintenance and Queries Speed	+ +	- -	
Monetary Savings (wrt CSP)	+ +	- -	
Multi-Device	+	-	
Control on Accesses	+ +	- -	

Feature	Proxy	Straight	...
Deployment Readiness	- -	+ +	
Keys Location	-	+	
Workload Management	- - - -	+ + + +	
Scalability	- - - -	+ + + +	
Robustness	- -	+ +	
Control on Policy Data	+ +	- -	
Policy Maintenance and Queries Speed	+ +	- -	
Monetary Savings (wrt CSP)	+ +	- -	
Multi-Device	+	-	
Control on Accesses	+ +	- -	

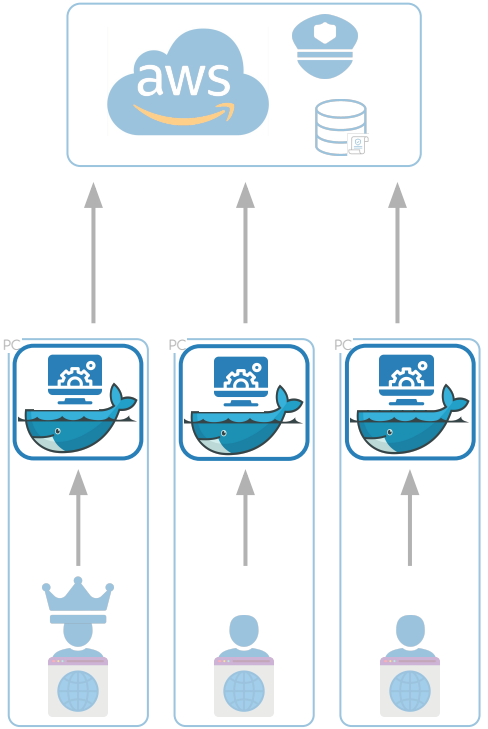
Feature	Proxy	Straight	...
Deployment Readiness	- -	+ +	
Keys Location	-	+	
Workload Management	- - - -	+ + + +	
Scalability	- - - -	+ + + +	
Robustness	- -	+ +	
Control on Policy Data	**+ +**	**- -**	
Policy Maintenance and Queries Speed	+ +	- -	
Monetary Savings (wrt CSP)	+ +	- -	
Multi-Device	+	-	
Control on Accesses	+ +	- -	

1. Introduction
2. Analysis of the Cryptographic AC Scheme
3. Architectures
4. Implementation with AWS
5. Conclusions and Future Work

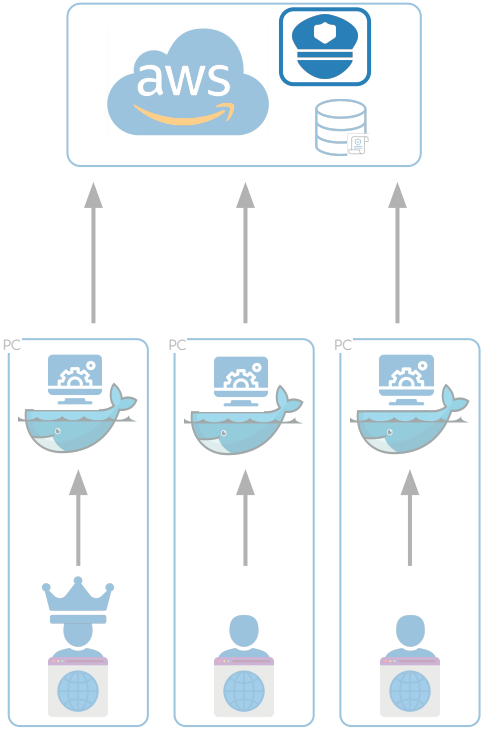

PC
PC
PC


aws
PC
PC
PC

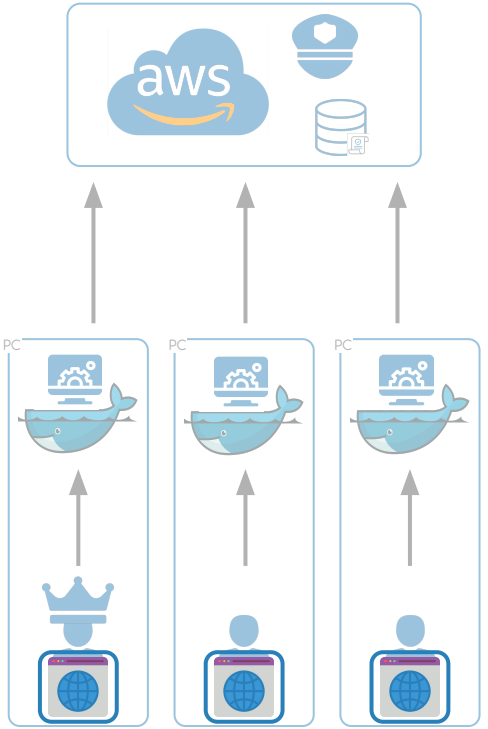
- CryptoAC - Java server in Docker
  - DAO Pattern for multi-CSP support
  - Multi-architecture



- CryptoAC - Java server in Docker
- RM - Java class
    - AWS Lambda function



- CryptoAC - Java server in Docker
- RM - Java class
- Interface - Web Technologies
  - Browser
  - RESTful APIs



1. Introduction
2. Analysis of the Cryptographic AC Scheme
3. Architectures
4. Implementation with AWS
5. Conclusions and Future Work

Conclusions

- Companies want to **securely** store data in the Cloud
- CSP is Honest but Curious
- **Pragmatic** approach to a cryptographic AC scheme
  - Uncovered **assumptions** and **requirements (20+)***
  - Designed and analyzed **different architectures (10+)**
  - Developed a multi-architecture tool with **AWS**
  - **Requirements Compliance** of implementation*

*(not in this presentation)

- Obvious **Improvements** (more CSPs, UI, ...)
- Enhance **Scheme Expressiveness**
- **Hybrid** Approach (SecurePG [4])
- **Paper** in Writing

[4] Umberto Morelli and Silvio Ranise. *Assisted Authoring, Analysis and Enforcement of Access Control Policies in the Cloud*. In: "IFIP SEC 2017 International Conference on ICT Systems Security and Privacy Protection".

Thanks

Assumptions

Abstract Assumptions	
A1.	CSP can Execute Code
A2.	CSP Trusted as Storage Solution
A3.	Consider only one CSP
A4.	No Spurious File Downloads
A5.	No Considering Concurrency
A6.	CSP Cannot Read Files
A7.	Digital Signatures on Tuples
A8.	Secure Communication Channels

From	Concrete Assumptions	
A1	CA1.	CSP can execute code
A2	CA2.	CSP Trusted as Storage Solution
A3	CA3.	Consider only one CSP
us	CA4.	Clients have personal credentials
us	CA5.	CSP can enforce AC policies

Requirements

From	Concrete Requirements
Flexibility 	CR1. Multi-CSP support
	CR2. Multi-Configuration
Portability 	CR3. Micro-Services
	CR4. Multi-Platform
Security 	CR5. Accountability
	CR6. Secure Keys Handling
Privacy 	CR7. Policy Hiding

From	Concrete Requirements
A4	CR11. No spurious file downloads
A5	CR12. Resolving Concurrency
A6	CR8. CSP Cannot Read Files
A7	CR9. Policy Integrity
A8	CR10. Secure Communication Channels

Hybrid Architecture