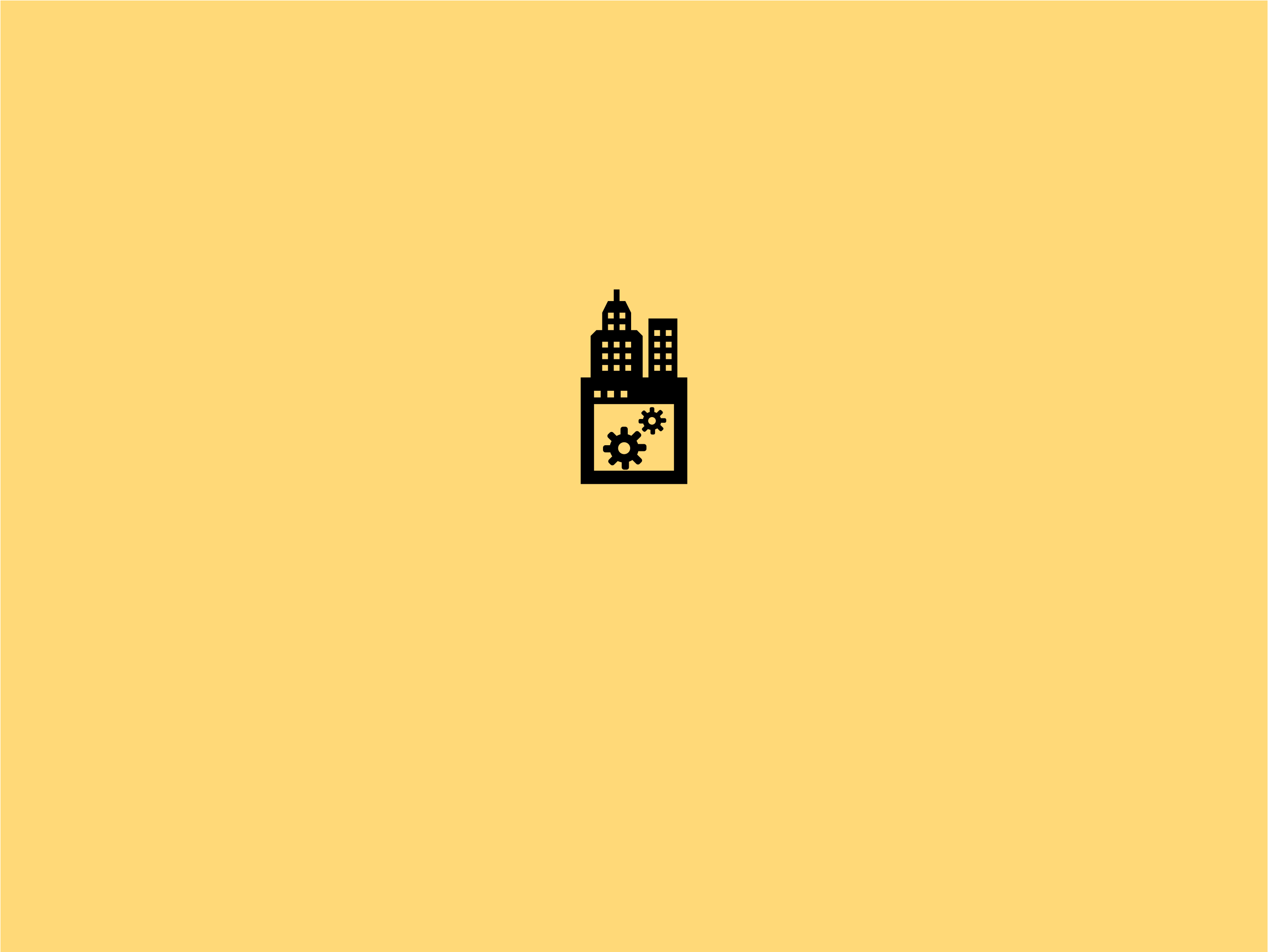
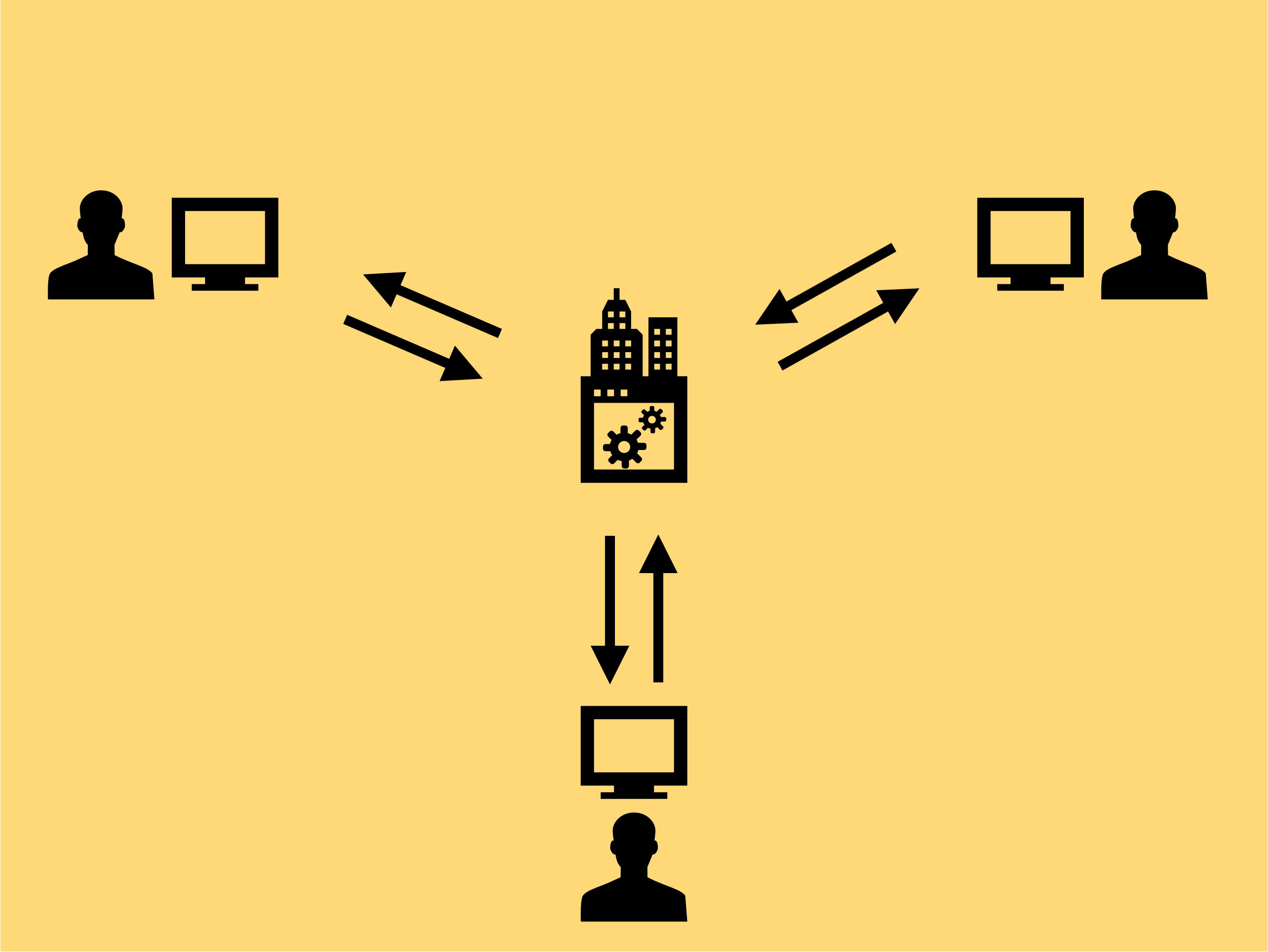
SECURELY STORING AND EXECUTING BUSINESS PROCESSES IN THE CLOUD

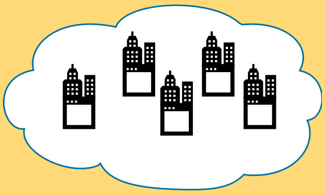
David Martinho

#SBP'12

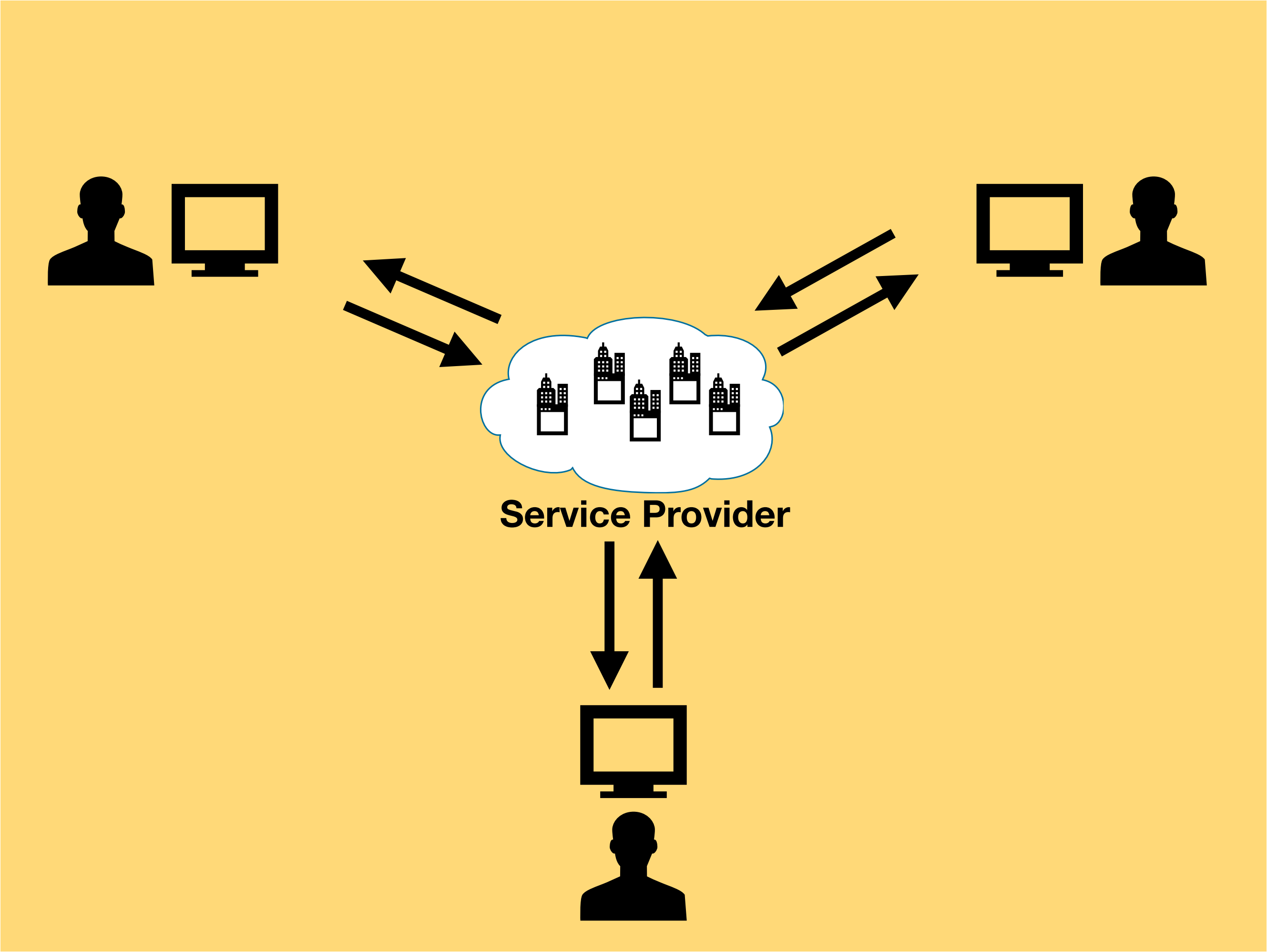
Diogo R. Ferreira

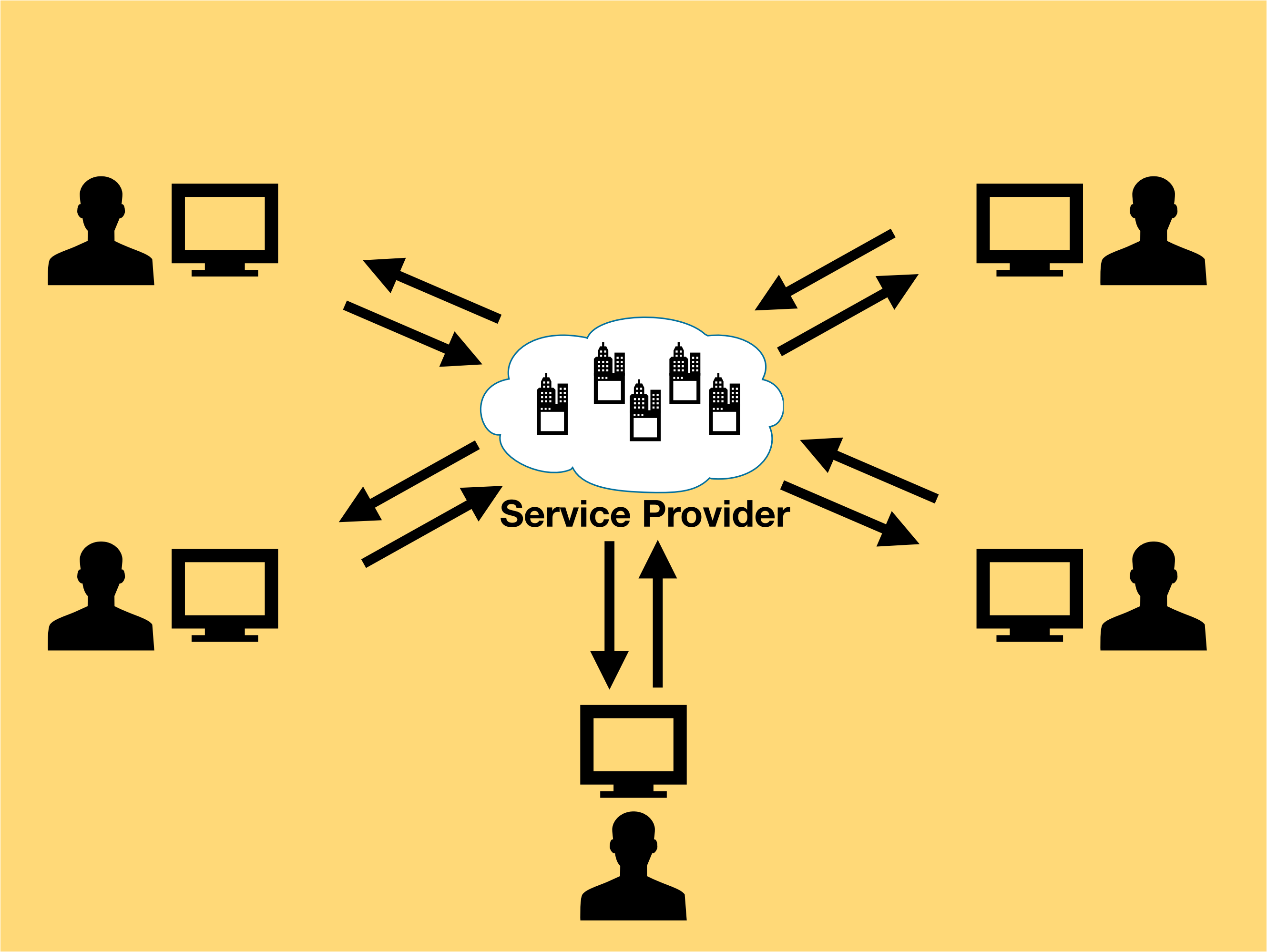


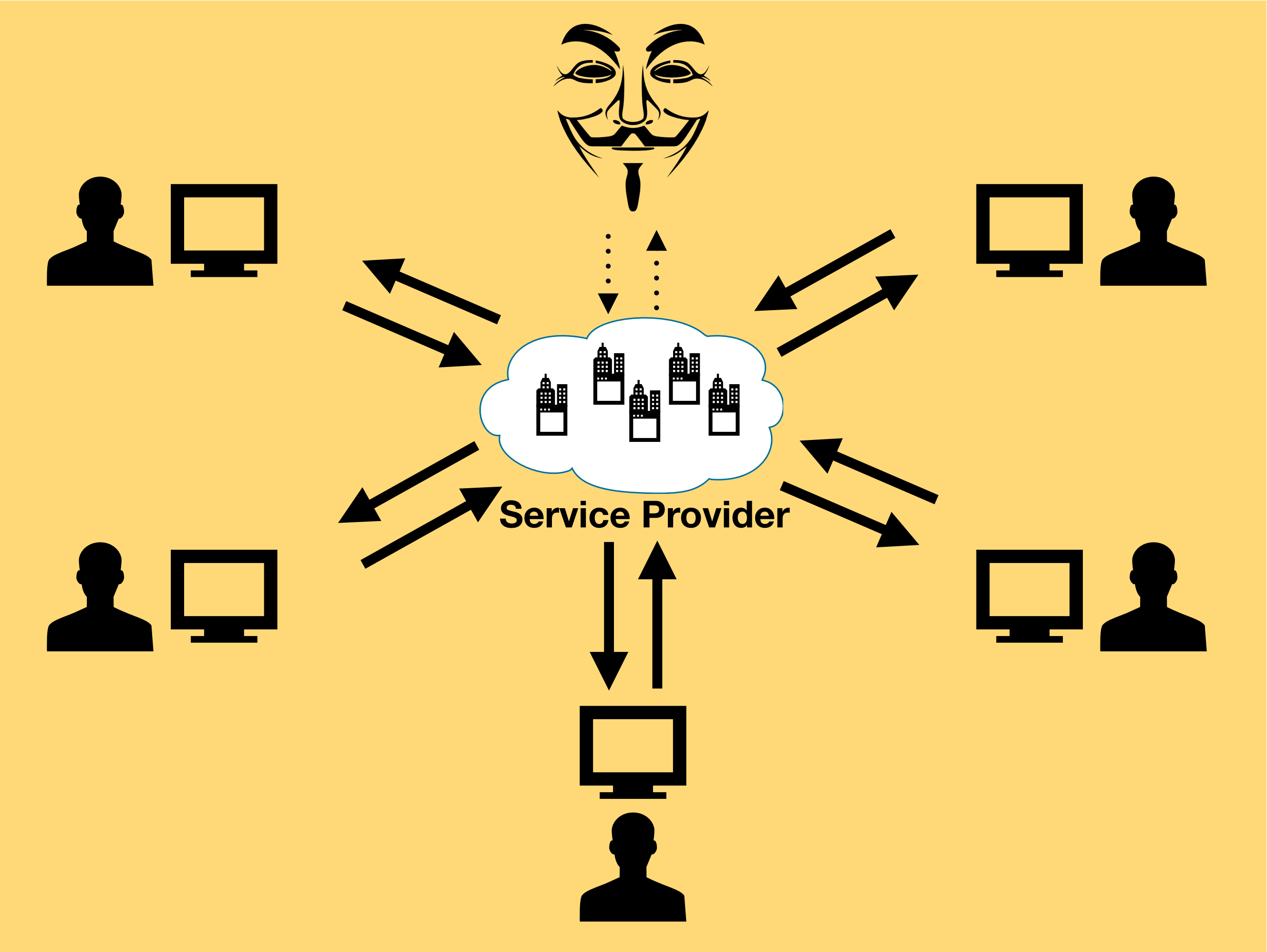




Service Provider


Service Provider


Service Provider

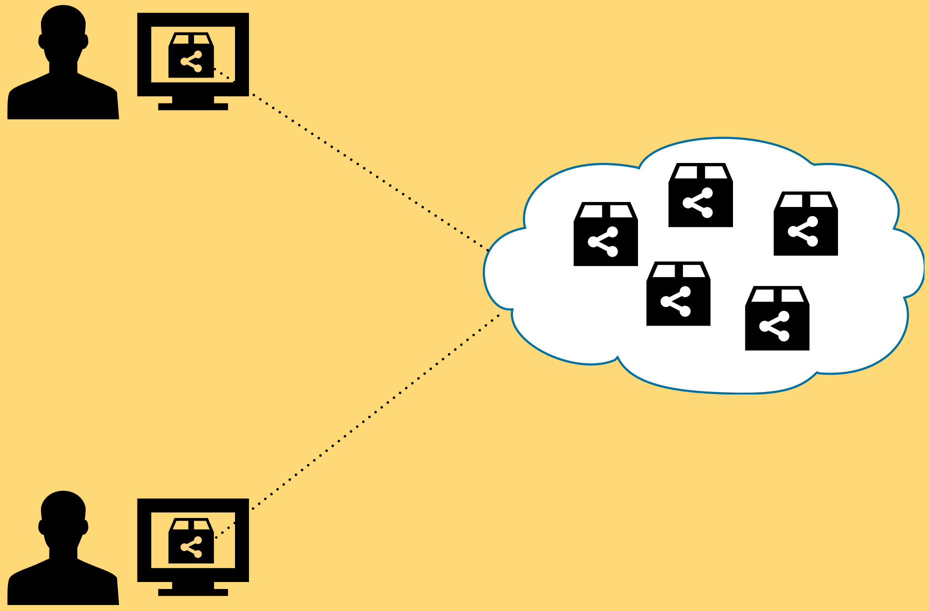

Service Provider

WE MUST SECURE OUR BUSINESS PROCESSES

WHAT DOES THAT INVOLVE?

REQUIREMENT #1

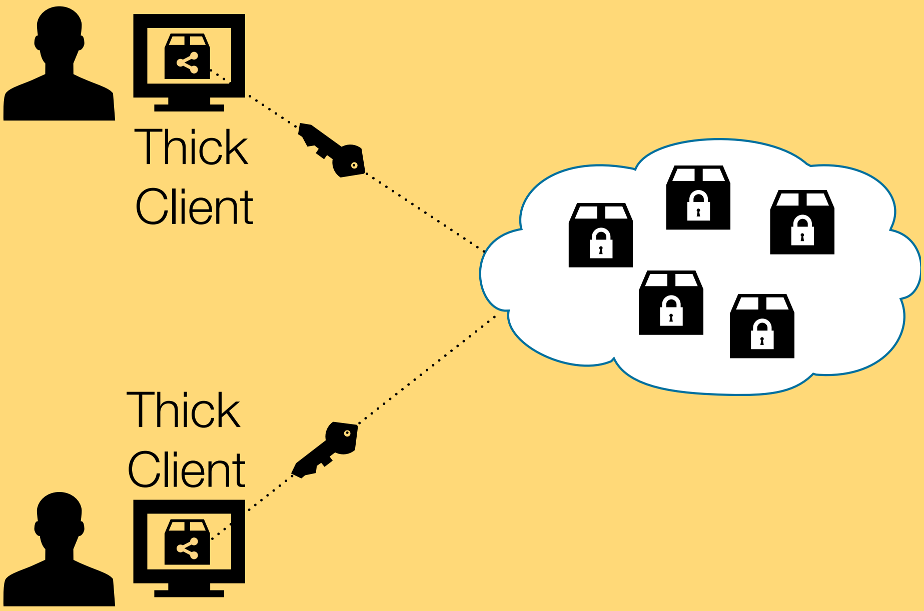
Process instance must be shared among its participants



The "Cloud" is already supported by a client-server architectural pattern

REQUIREMENT #2

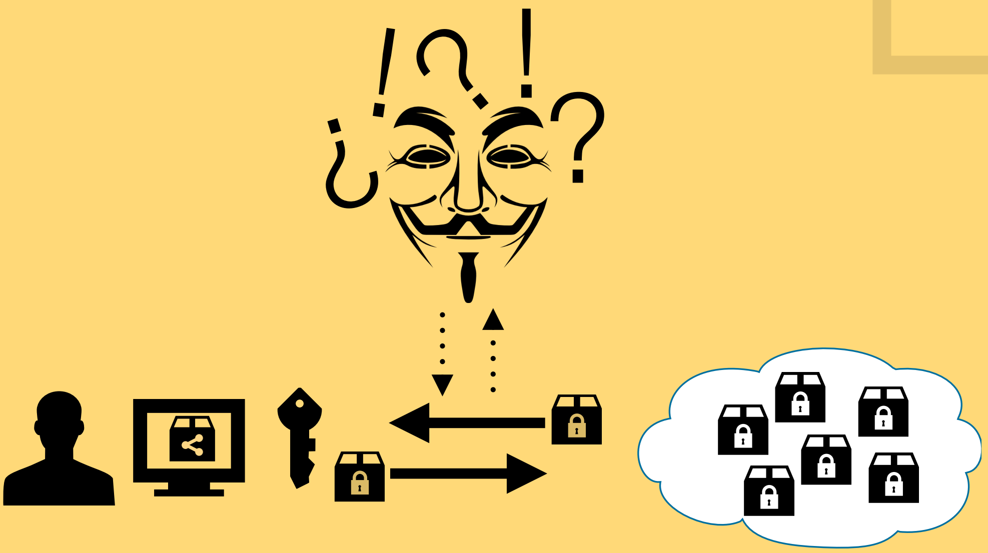
Service Provider (SP) must never have access to processes



Encrypt the process instance before sending it to the service provider

REQUIREMENT #3

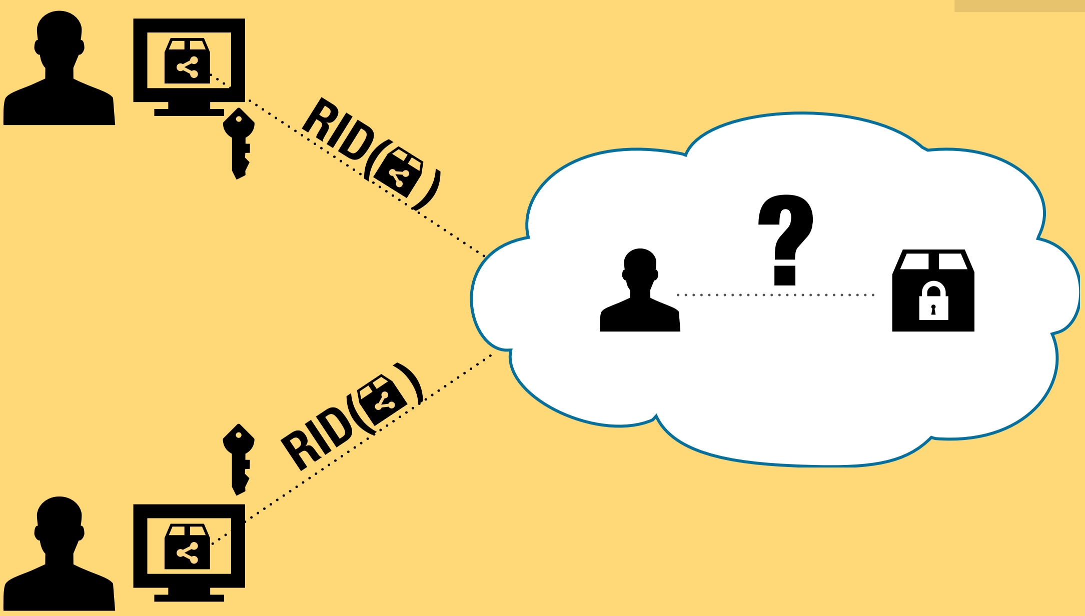
Never compromise communication via eavesdropping



Since the process is already encrypted, no eavesdropping is possible

REQUIREMENT #4

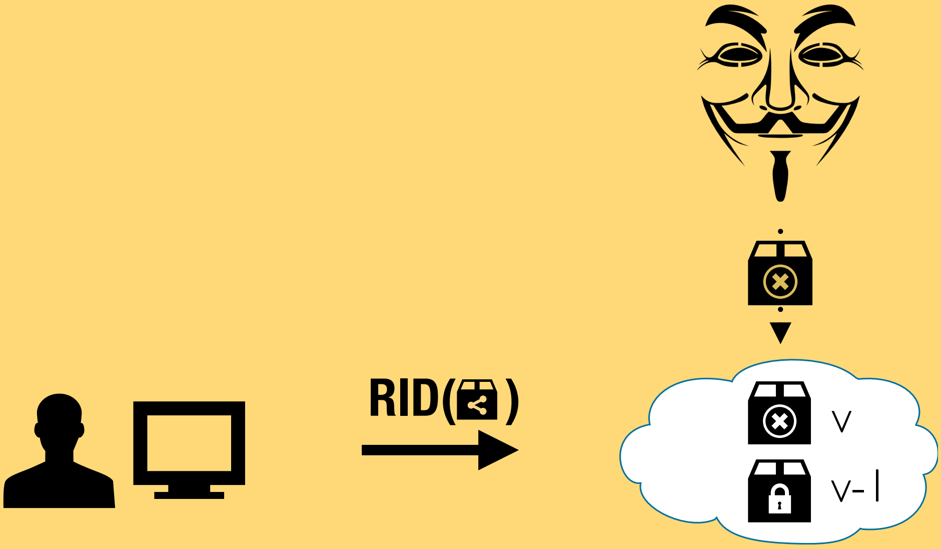
SP should not be able to link participants to processes



Unauthenticated fetch and store of encrypted business processes

REQUIREMENT #5

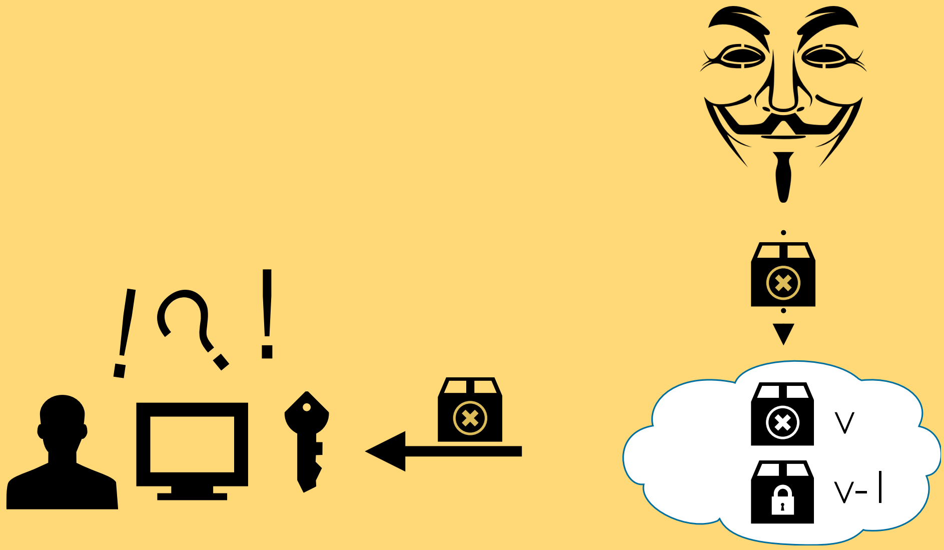
Always ensure access to authorized participants



SP should version process instances on each storage operation

REQUIREMENT #5

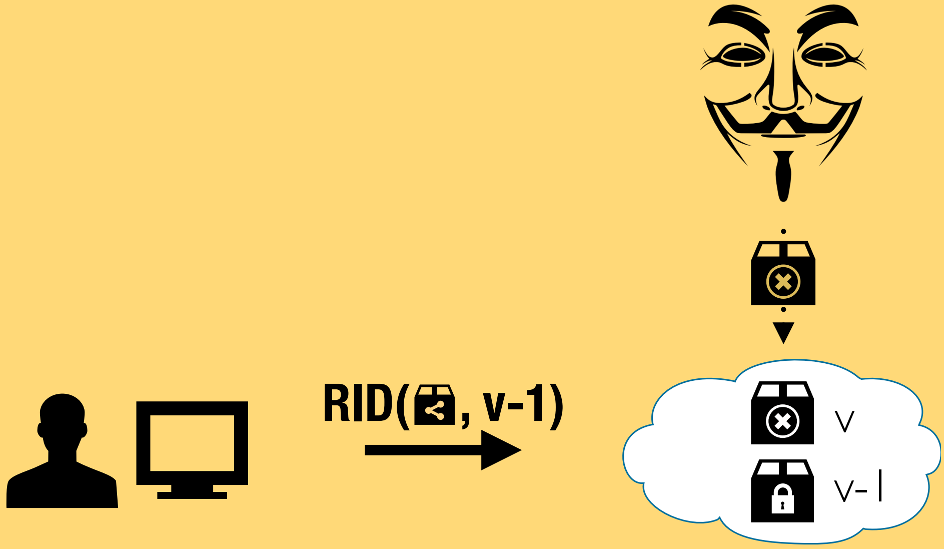
Always ensure access to authorized participants



SP should version process instances on each storage operation

REQUIREMENT #5

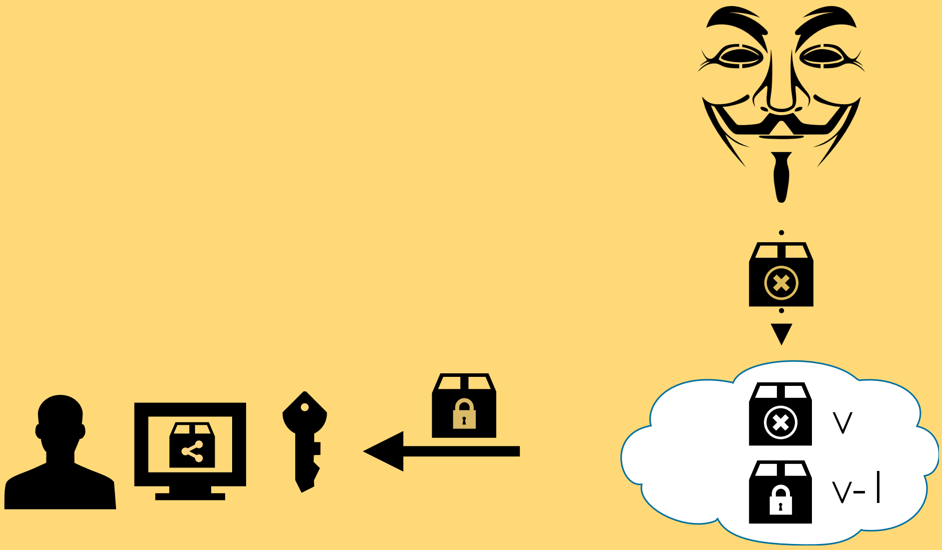
Always ensure access to authorized participants



SP should version process instances on each storage operation

REQUIREMENT #5

Always ensure access to authorized participants



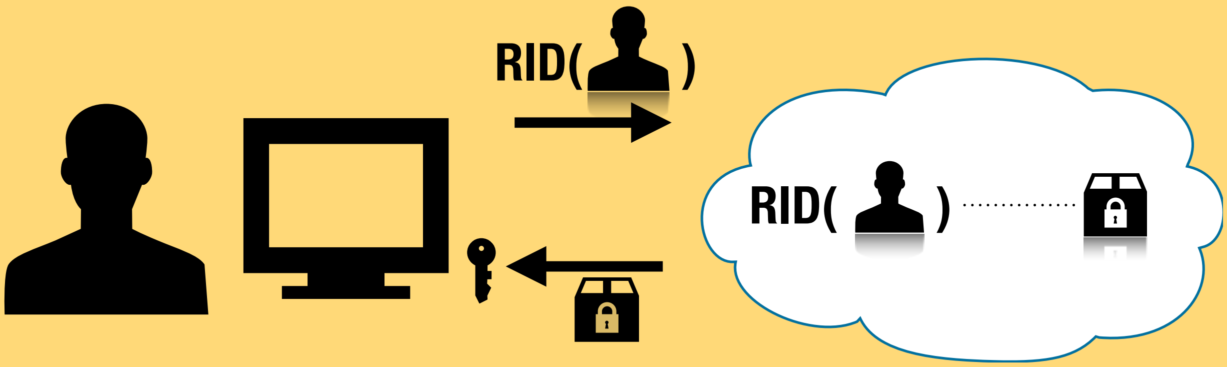
SP should version process instances on each storage operation

SO HOW DO THESE SOLUTIONS COMBINE?

PASSPORT

The end-user secrets

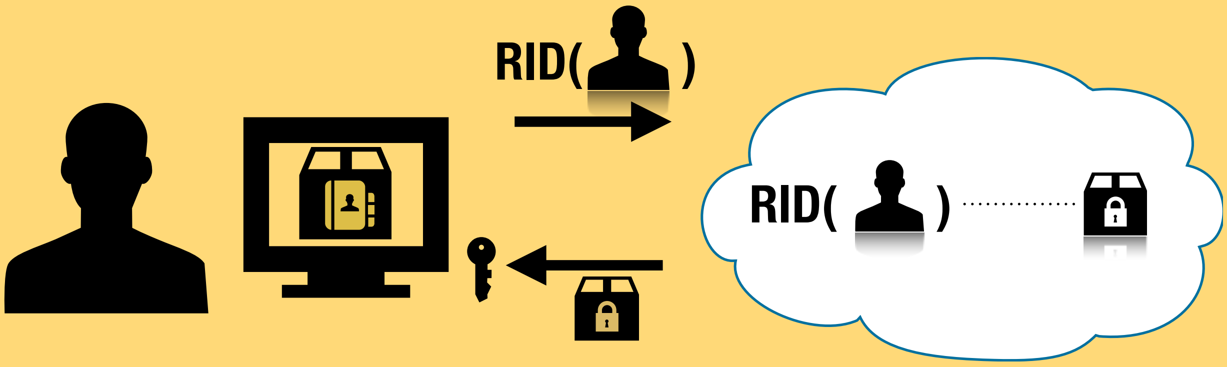
- Hosted in the server
- Encrypted with the user’s symmetric key
  (generated from his password)



PASSPORT

The end-user secrets

- Hosted in the server
- Encrypted with the user’s symmetric key
  (generated from his password)



PASSPORT

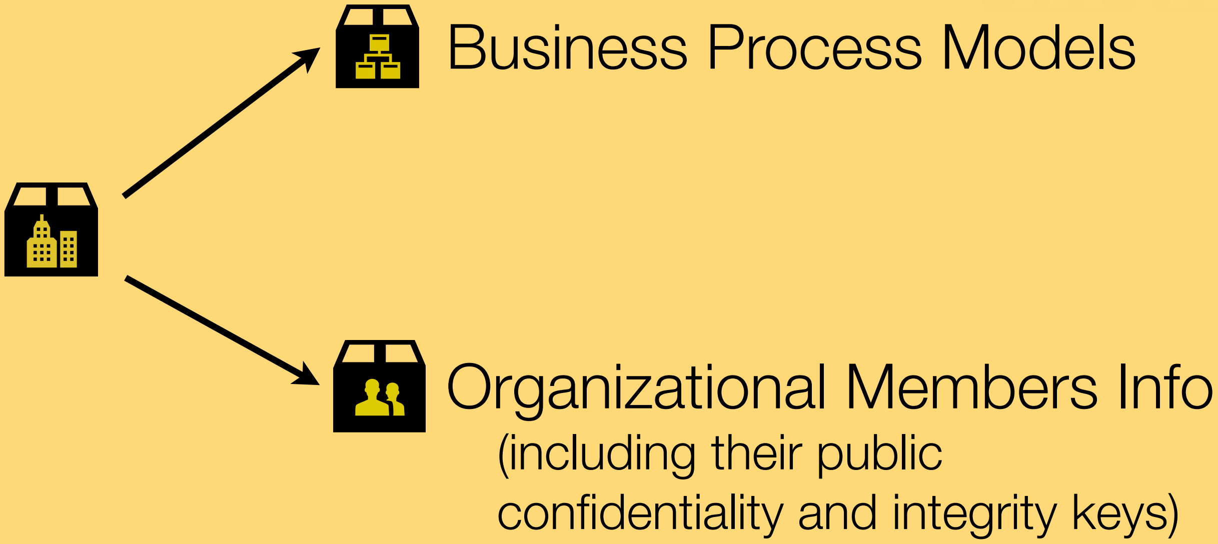
The end-user secrets

A passport is a 5-tuple

- Organization Identity
- Organization Shared Symmetric Key
- Process List
- User Decryption Key (Confidentiality)
- User Encryption Key (Integrity)

ORGANIZATION IDENTITY

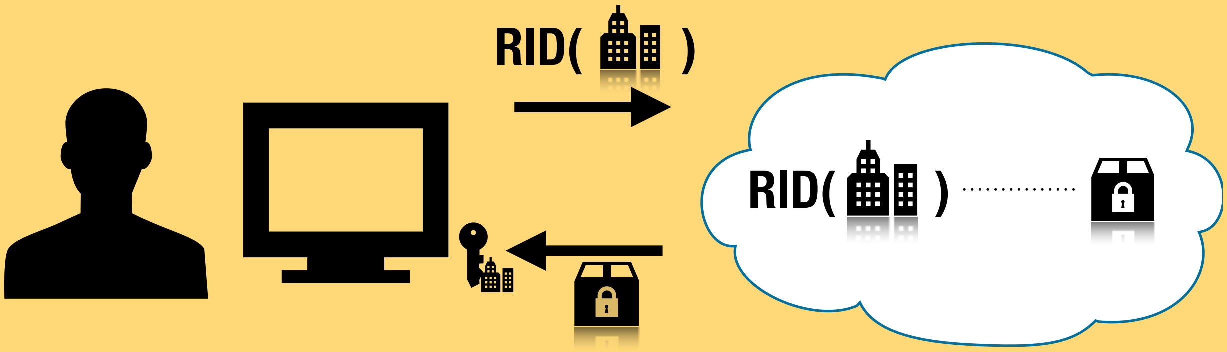
The organization’s information



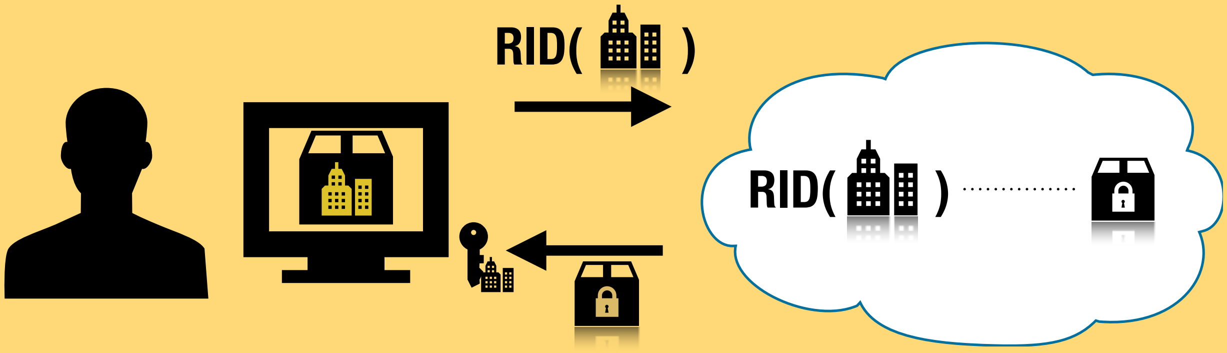
Business Process Models

Organizational Members Info
(including their public
confidentiality and integrity keys)

ORGANIZATION SHARED SYMMETRIC KEY

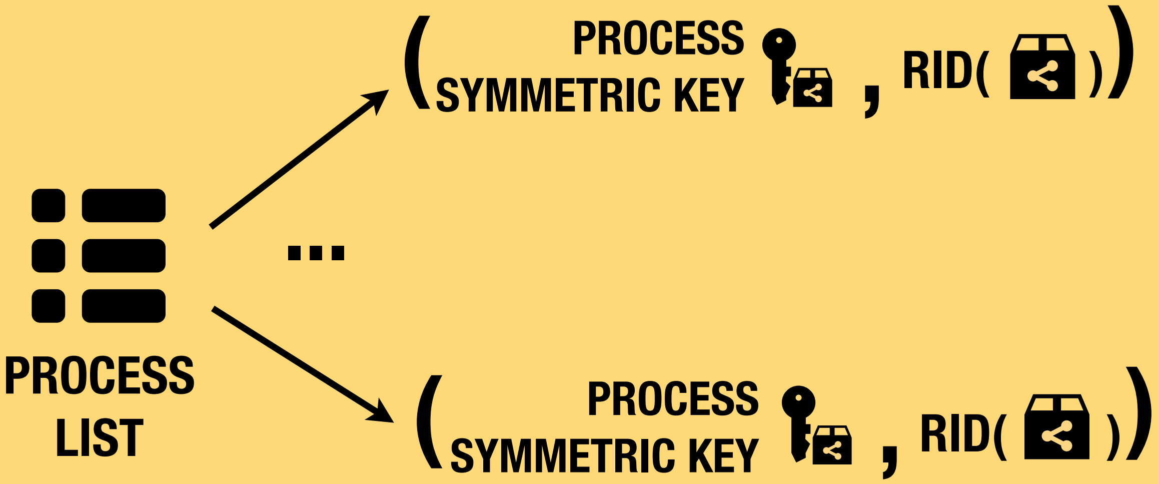


ORGANIZATION SHARED SYMMETRIC KEY



PROCESS LIST

User's ACL to process instances

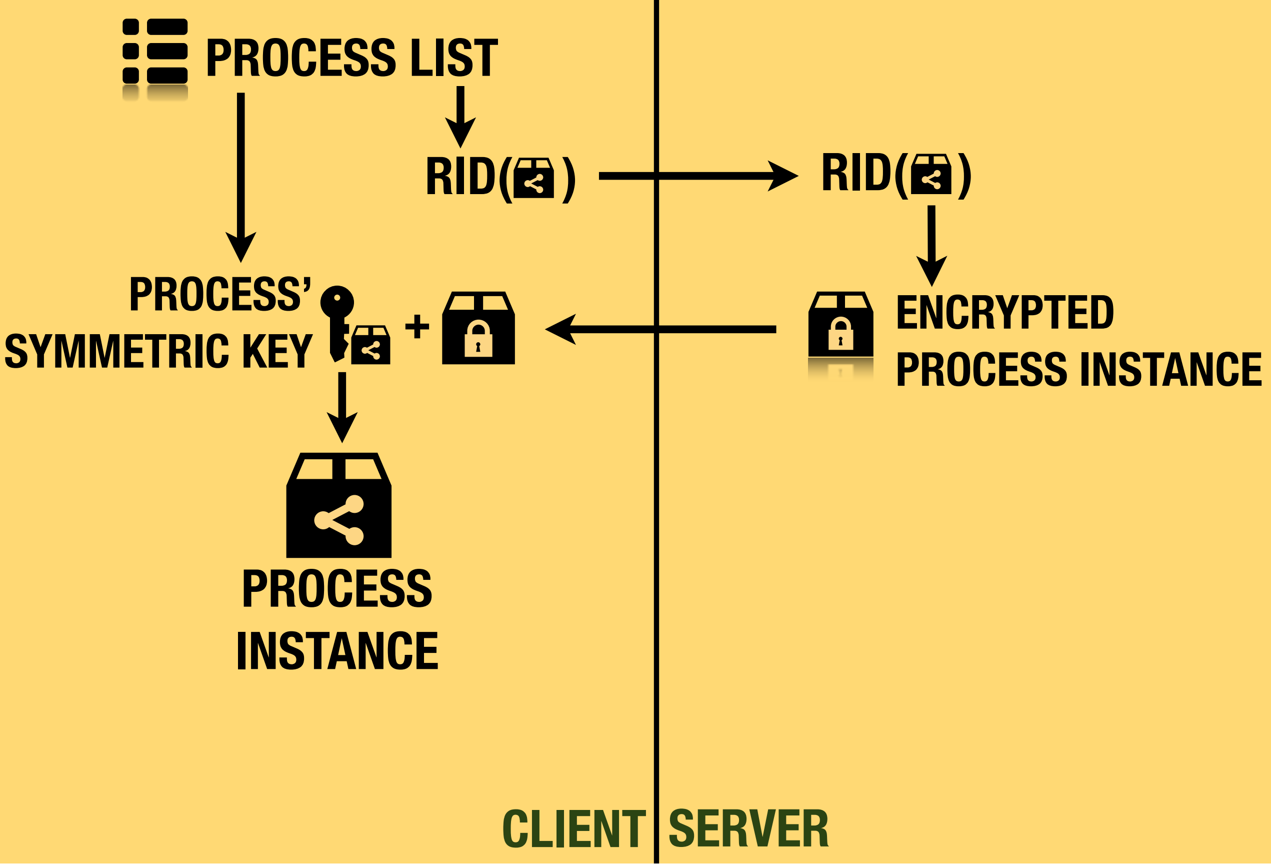


PROCESS LIST

(PROCESS SYMMETRIC KEY , RID( ))

...

(PROCESS SYMMETRIC KEY , RID( ))



PROCESS LIST

RID( )

RID( )

PROCESS' SYMMETRIC KEY +

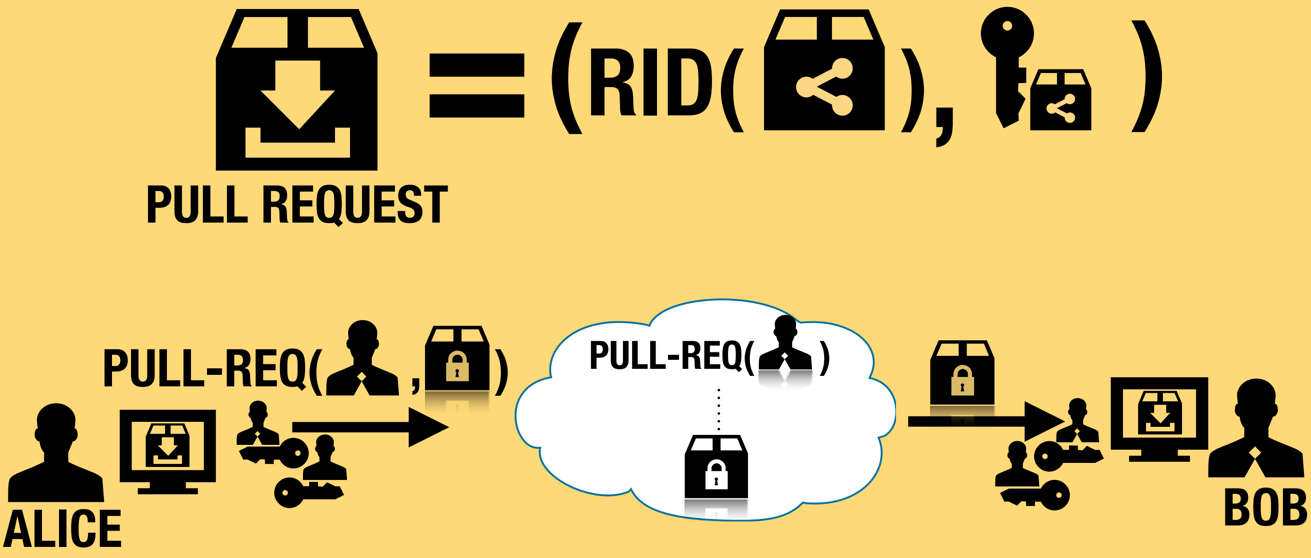
ENCRYPTED PROCESS INSTANCE

PROCESS INSTANCE

CLIENT | SERVER

USER ENC/DEC KEY

Send Signed Pull Requests to new participants



CONCLUSIONS

We can store and “execute” business processes in the “cloud”

☑ We must ensure the architectural solution proposed

☑ Service Provider is completely unaware of the organization’s business processes

The solution proposed can be extended to support choreographies among organizations, requiring them to:

- ☑ Have compatible business process models
- ☑ Use the same architectural solution proposed

THANK YOU

Questions?

davidmartinho@ist.utl.pt

diogo.ferreira@ist.utl.pt