MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

IN COLLABORATION WITH MIT MANAGEMENT SLOAN SCHOOL

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

MASTER MEIM 2022-2023

Security Issues in Cloud Computing

PART TWO – SELECTED TOPICS IN CLOUD SECURITY

Luigi CATUOGNO, PhD

Associate Professor in Computer Science at Università degli Studi di Napoli Parthenope (ITALY)

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Selected Topics in Cloud Security

User Authentication

Access Control and Security Policy Enforcemement (Authorization)

Secure Data Outsourcing

Multi-tenancy and Workload Isolation

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

User authentication

Mechanisms for user recognition through

- PIN/password
- Biometric measures
- Cryptographic tokens
- Multi-factor authentication schemes

3

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

User authentication

In the cloud, due to the potentially huge number of user and the high services interoperability, an authentication system plays a fundamental role.

In particular, it is required to be:

- Fast and scalable
- Able to handle the whole user account lifecycle automatically
- Able to identify and solve a wide range of possible faults or abuse without human intervention
- interoperable

4

MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

User authentication

SINGLE RESOURCE/SINGLE DOMAIN

In origin, the authentication system were designed to protect:

Single resources

- e.g. one computer/server, a DBMS system

Within a single domain

- i.e. the entity which groups together a pool of resources and the users that are allowed to use them.

5

MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

User authentication

SINGLE RESOURCE/SINGLE DOMAIN

For example, in a UNIX host, the domain includes the host computer and its users (that are listed in the password file)

- Only users included in such database: are allowed to log-in the computer
- Users listed in the password file are able to log-in only this computer

6

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

User authentication

MULTIPLE RESOURCES/SINGLE DOMAIN

Within distributed systems, domains encompass multiple resources, so that a centralized user authentication system is used by every resource in the domain

- (Kerberos, Raidus, Active Directory, LDAP...)

For example:

- In a corporate network, users are registered with the central authority
- user are able to sign-on every computer of the network

7

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

User authentication

MULTIPLE RESOURCES/MULTIPLE DOMAINS

What if users need to access to resources from multiple domains?

8

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

User authentication

MULTIPLE RESOURCES/MULTIPLE DOMAINS

Traditional (centralized) systems are not designed to *interoperate* so, either:

- *Users are asked to handle multiple credentials in order to access resources from different domains*

or:

- *Domain authorities agree tp disclose each others information about their users, and their internal resources*

9

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Federated Authentication *(single sign-on)*

MULTIPLE RESOURCES/MULTIPLE DOMAINS

Joining the *federation,* multiple domain tenants agree on a common set of policies and protocols in order to manage identification and trust among their respective users and resurces

- users transparently access services operating in any federated domain, authenticating themselves with their home domain authority
- only information related to users' privilege determination are transferred among domains

10

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Shibboleth

FEDERATED AUTHENTICATION SYSTEM

Developed by the Internet2 consortium since 2000

- Version 1.0 was released in 2003
- Version 2.0, released in 2008

Current version :2.4 is maintained by the Shibbolet Consortium

https://shibboleth.net

11

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Shibboleth

FEDERATED AUTHENTICATION SYSTEM

Components:

- Web browser
  - Is the agent through which the user starts the sign-on process
- Resource
  - The service the user wishes to access to
- Identity Provider
  - The component which authenticates the user
- Service Provider
  - Performs the sign-on process for the resource

12

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Shibboleth

FEDERATED AUTHENTICATION SYSTEM

- Access Control is performed by matching attributes provided by Identity Providers against rules stated by Service Providers
- Attributes and protocol messages (assertions) are described using the Secure Assertion Markup Language (SAML) standards

13

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Shibboleth

FEDERATED AUTHENTICATION SYSTEM

- Trust is established within a Public Key Infrastructure (usually by means of X509 certificates)
- Terms and conditions of use of information exchanged between peers are set out in the agreement
  - Confidentiality, retention…

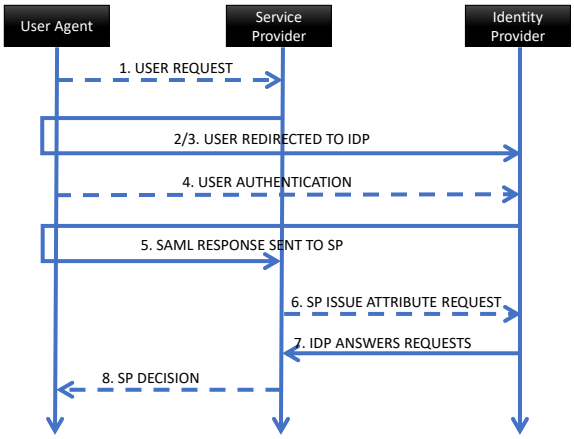
14

MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Shibboleth

FEDERATED AUTHENTICATION SYSTEM



15

MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

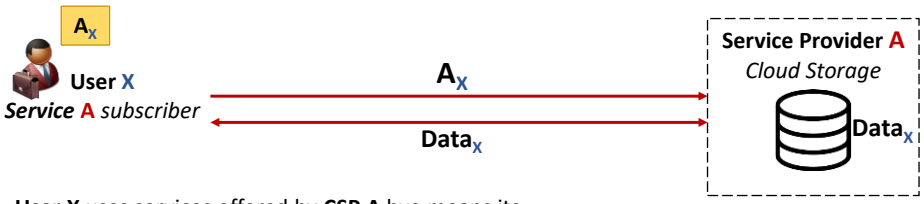
Delegated Authorization

16

MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Delegated Authorization



User X uses services offered by **CSP A** bye means its front-end application (or through its web interface)

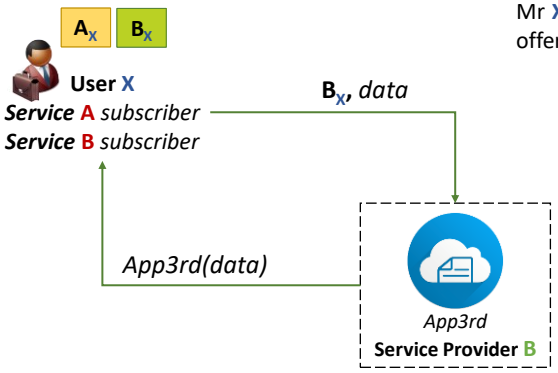
User X has previously subscribed with **CSP A** and has got his private access credentials A_x

17

MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Delegated Authorization



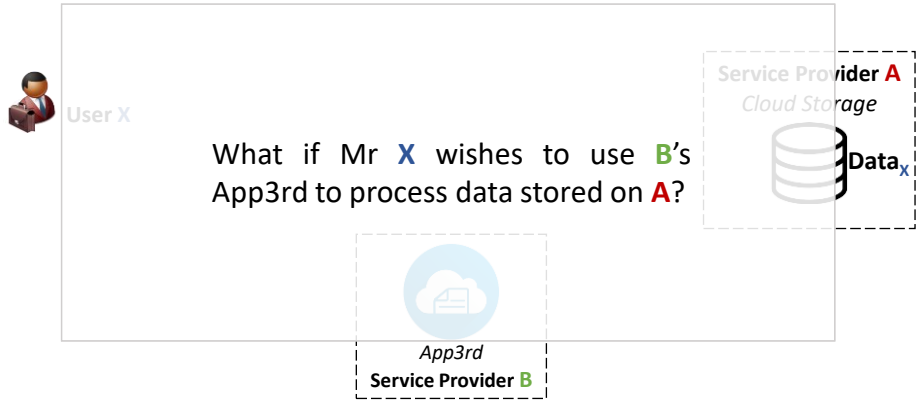
Mr X also subscribes the service by CSP B which offers an application for data processing…

18

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Delegated Authorization



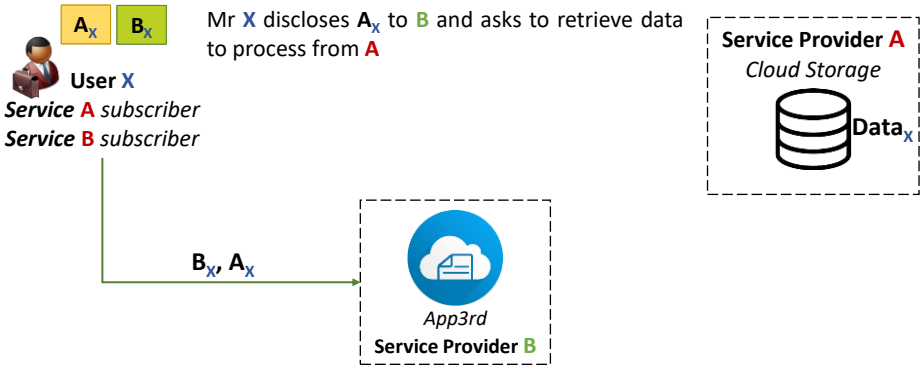
19

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Delegated Authorization

CREDENTIAL DISCLOSURE



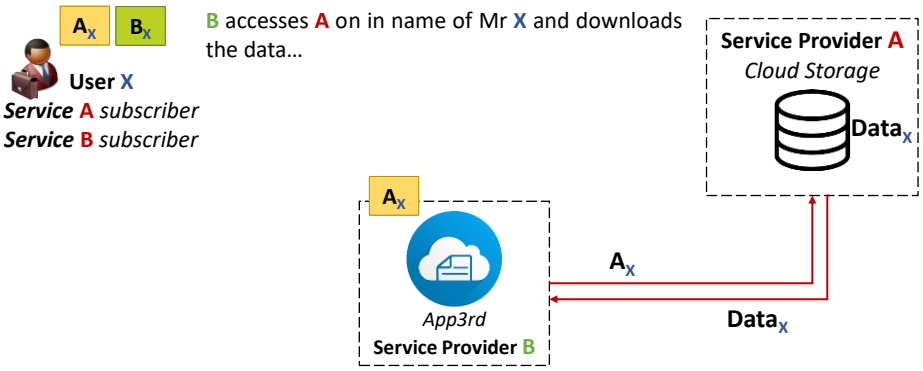
20

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Delegated Authorization

CREDENTIAL DISCLOSURE



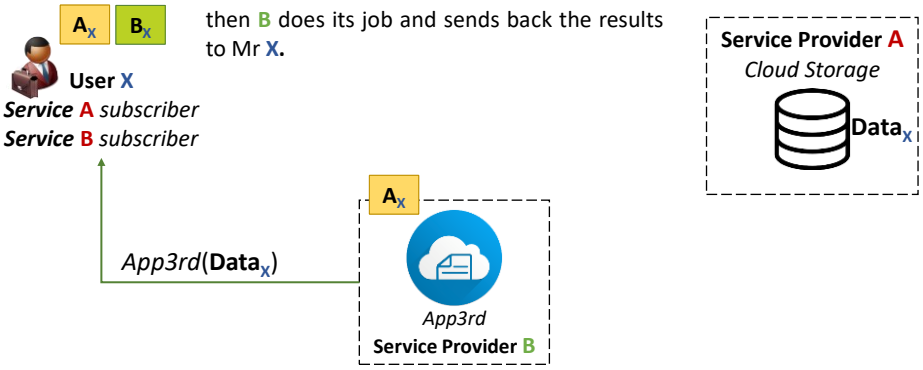
21

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Delegated Authorization

CREDENTIAL DISCLOSURE



22

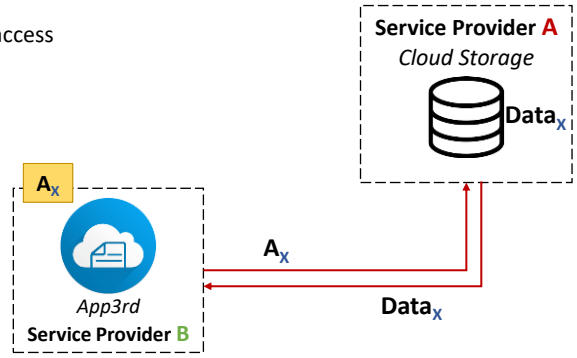
MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Delegated Authorization

CREDENTIAL DISCLOSURE

The point is that now CSP **B** has got free access to the data Mr **X** has stored on **A**...



23

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

OAuth (OpenAUTHorization)

DELEGATED AUTHORIZATION

Open standard protocol for delegated authentication. It enables *front-end applications* to use a remote resource (e.g. a cloud based service) on behalf of a subscriber, without releasing its credentials.

- Developed since 2006 by Blain Cook
- Version 1.0 was released in 2007 (RFC-5849)
- Version 2.0 (OAuth2) was released in 2012 (RFC-6750)

24

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

OAuth2

DELEGATED AUTHORIZATION

Resource Owner: *(Mr X, in our example)* is the owner of remote resources. She subscribed an agreement with the *Resource Server* to manage (e.g. store) her resources remotely.

Resource/API Server: *(CSP A)* is the Service Provider by whom the Resource Owner stored her data. The Resource Server allows to access to such data to whoever provides an *Access Token* on behalf of the Resource Owner.

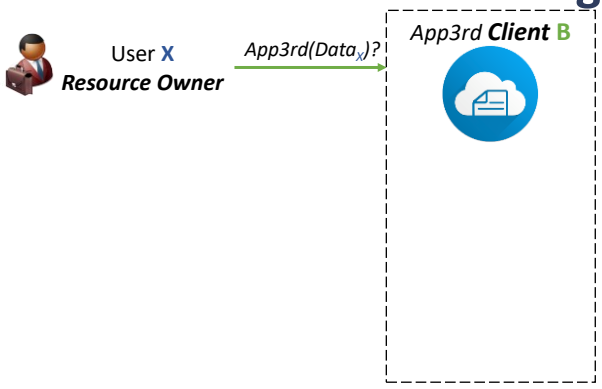
The Client *(CSP B)* is the application which requests the access to the data. It must previously request the proper Access Token.

25

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

OAuth2: authorization code grant



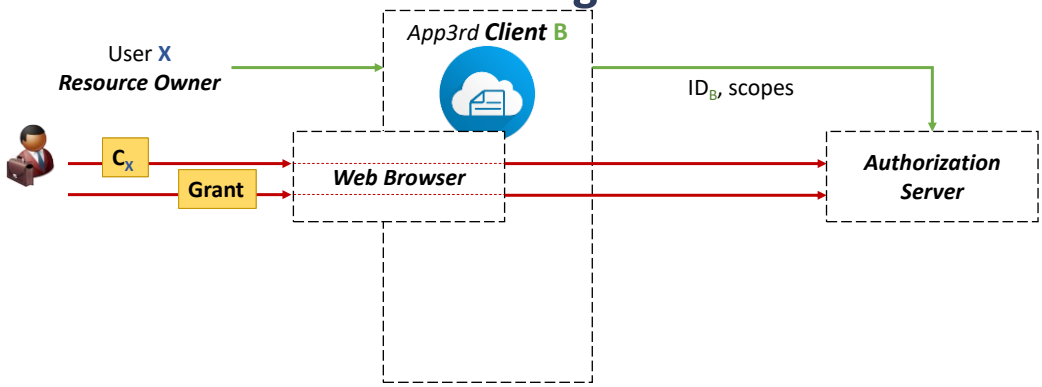
1 User **X** ask **B** to process $Data_X$ stored in **A**

26

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

OAuth2: authorization code grant



2 ***Client*** **B** contacts the Authorization Server, sends its ID and asks for the required privileges(scopes) to accomplish.

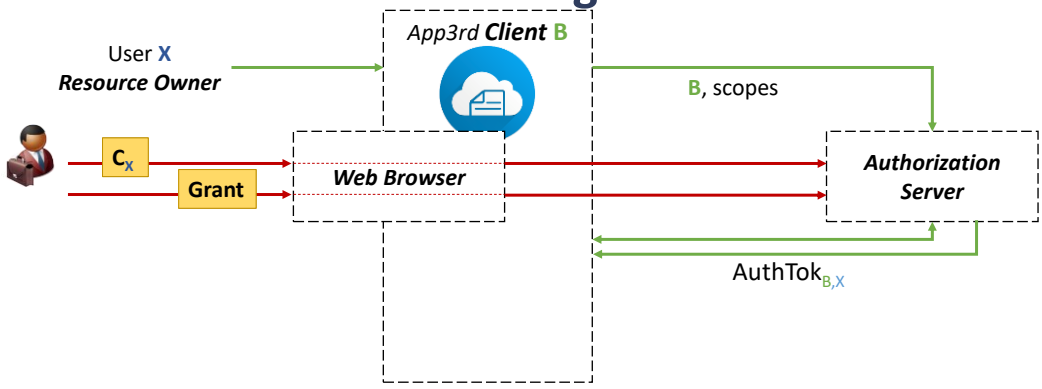
3 ***Client*** **B** redirects **X** to the authorization in order to grant such privileges

27

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

OAuth2: authorization code grant



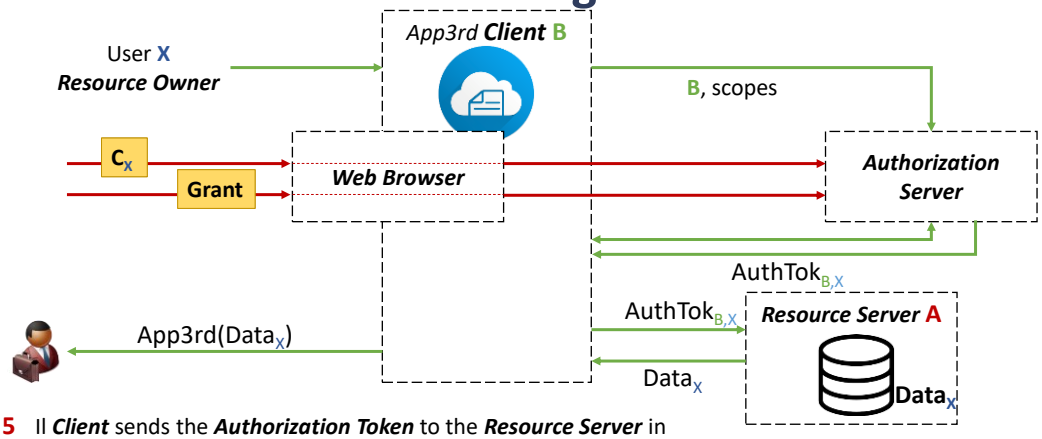
4 L'***Authorization Server*** first authenticates the ***Client*** then sends it an ***Authorization Token***

28

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

OAuth2: authorization code grant



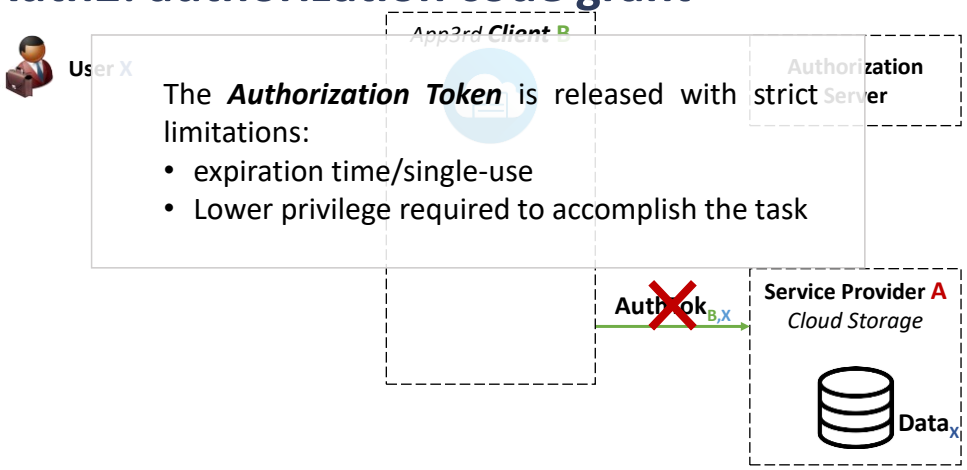
5 Il ***Client*** sends the ***Authorization Token*** to the ***Resource Server*** in order to download the data

29

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

OAuth2: authorization code grant



30

MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Secure Data Outsourcing

HOMOMORPHIC ENCRYPTION

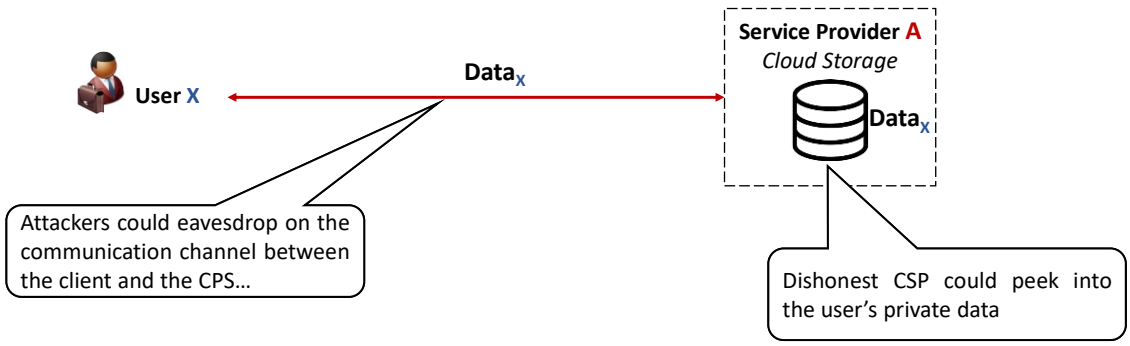
31

MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Secure data outsourcing

THREAT MODEL



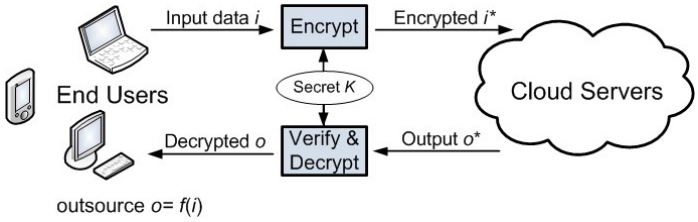
32

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Secure Data Outsourcing

NAIVE SOLUTION



1 The data owner locally encrypt the data with a simmetric key ***K*** before uploading it to the cloud storage

Whoever has the key ***K*** is *authorized* to read/modify such data

2 The data owner uploads encrupted data. Neither possible eavesdropers nor anybody at the CSP have access to data contents

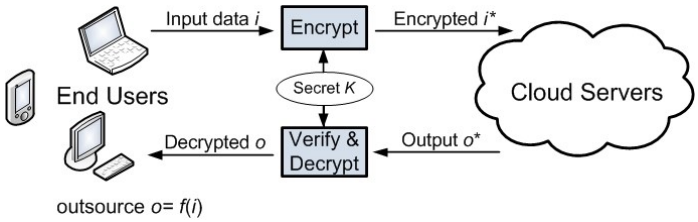
33

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Secure Data Outsourcing

NAIVE SOLUTION



3 to accesse the data, whoever is in charge can…

- first download and then decrypted it locally (using ***K***)
- Decrypting (and re-encrypting once the task is completed) directly on the cloud…

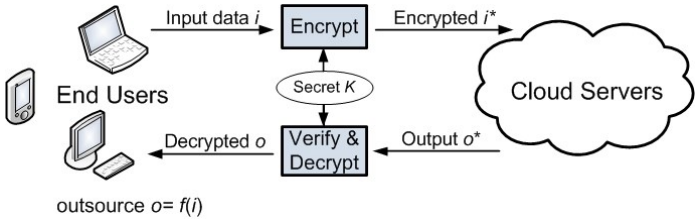
34

MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Secure Data Outsourcing

NAIVE SOLUTION



outsource $o = f(i)$

3 to accesse the data, whoever is in charge can…

- first download and then decrypted it locally (using ***K***) **NOT EFFICIENT**
- Decrypting (and re-encrypting once the task is completed) directly on the cloud… **INEFFICIENT**

MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Homomorphic encryption

Leads to the capability to perform certain computation on encryped date without decrypting it first

Entails *cryptographic primitives* in which (every) operation to do on a *plaintext* has a *peer* (possibly different) that can be done on the corresponding *cyphertext* to compute the same result.

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Homomorphic Encryption

Data: strings «Hello, » and «World!»
Operation: concatenation(s_1,s_2)→s_3

37

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Homomorphic Encryption

Data: strings «Hello, » and «World!»
Operation: concatenation(s_1,s_2)→s_3

Informally, an HE primitive H is such that: given an encryption key K, let:

- $X_1=H_{Enc}(K,s_1)$, $X_2=H_{Enc}(K,s_2)$ and foo() *is somehow* $H_{Enc}(K,$*concatenation()*$)$

Then:

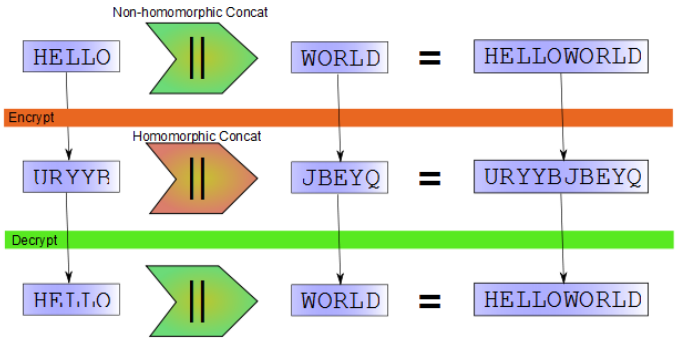
- $X_3=foo(X_1,X_2)$ and $H_{Dec}(X_3)=S_3$

38

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Homomorphic Encryption



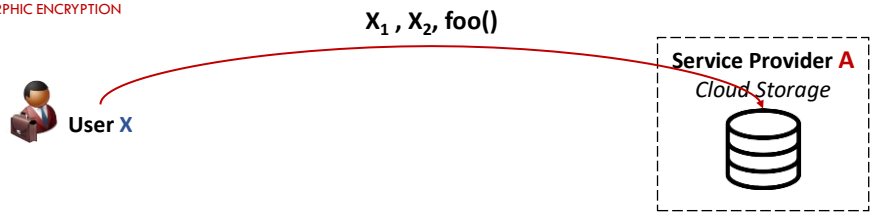
39

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Secure data outsourcing

HOMOMORPHIC ENCRYPTION



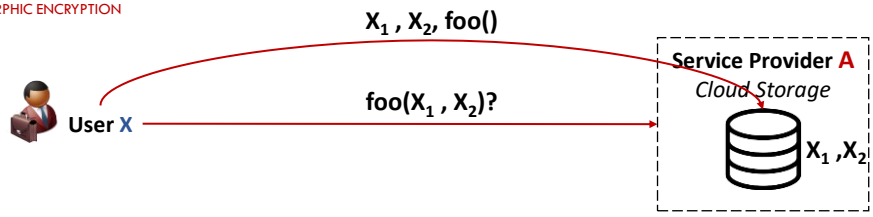
40

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Secure data outsourcing

HOMOMORPHIC ENCRYPTION



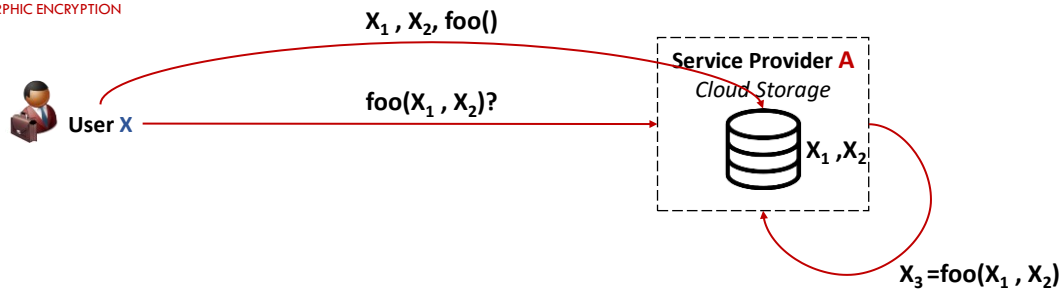
41

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Secure data outsourcing

HOMOMORPHIC ENCRYPTION



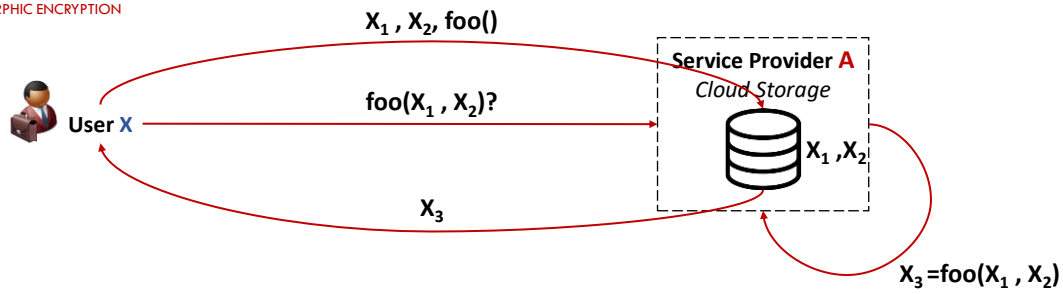
42

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Secure data outsourcing

HOMOMORPHIC ENCRYPTION



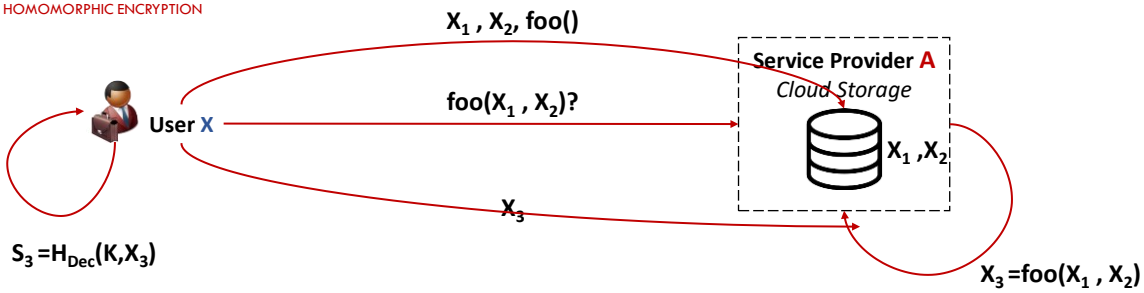
43

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Secure data outsourcing

HOMOMORPHIC ENCRYPTION



44

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Encrypted queries to Encrypted Databases

A CASE STUDY

45

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Actors…

ENCRYPTED QUERIES TO ENCRYPTED DATABASES

One *Data Owner* - **DO**

- Manages access rights to the data originating from *data sources*
  - Allows data sources to directly upload data to the storage server without any intervention
  - Has complete control on the type of queries each query source is allowed to issue

Several *Data Sources* – **DS**

- Store data to the *storage server* in encrypted form, on behalf of *data owner*

Several *Query Sources* – **QS**

- Issue `SELECT-FROM-WHERE` queries to the *query processor* under the control of the *data owner*

One *Query Processor* – **QP**

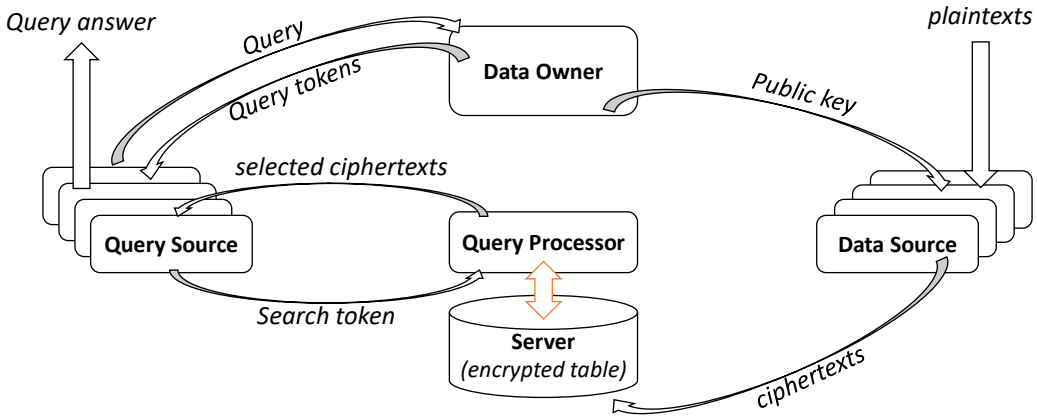
- Enjoys physical access to the encrypted data and performs the queries issued by the *query sources*

46

MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Encrypted Queries to Encrypted Databases



47

MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Multi-tenancy and Workload Separation

TRUSTED VIRTUAL DOMAINS (TVD)

48

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Trusted Virtual Domains (TVD)

Trusted Virtual Domains (TVDs) are a facility ensuring different workloads (belonging to different tenants) can share a common ITC infrastructure (data center, network) beeing kept strictly isolated each other.

Workload: Applications / Virtual Machines

ICT Infrastructure: Physical Machine + hypervisor + Trusted Computing + Network infrastructure

TVDs fit the *multi-tenant data center* scenario, in which a data-center provider offers its server farm to host and execute multiple (possibly) interconnected workloads. Every workload owner *has the impression* to be the only who uses the infrastructure.

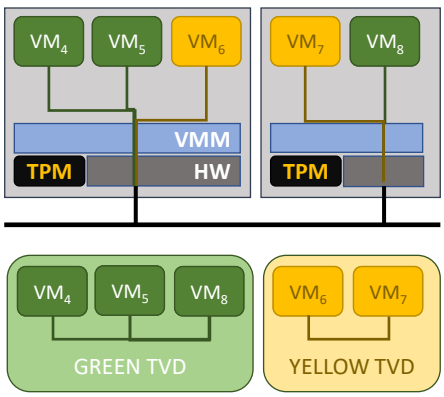
49

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Trusted Virtual Domains (TVD)

- Coalition of Virtual Machines (VM) that
  - Trust each other
  - Enforce a common security policy (TVD Policy)
  - Span over a physical infrastructure, shared with other TVDs
- The underlying virtualization layer
  - Isolates virtual machines of different TVDs in separated compartments
  - Connects virtual machines of the same TVD through a dedicated and isolated VLAN



50

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

TVD Policy

TRUSTED VIRTUAL DOMAINS

Enforcement of a twofold access control policy:

- Physical platform eligibility criteria to host any TVD workloads
- Virtual Machines eligibility to join any TVD

TVD Deploy protocol

- A «TVD Master» measures (attestation) the physical platform and check it fits the requirements to run VMs in its domain
- Eventually a «TVD Proxy» is instantiated on the platform

TVD Join protocol

- The TVD Proxy measures any VM running on the pysical platform that requests to access the TVD. Access is granted if VM integirty and requested properties are successfully verified

51

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Enterprise Rights Management

A CASE STUDY

52

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Application scenario: Remote Maintenance

A CASE STUDY

Complex equipment come with a technical on-site support facility

On-site operators are provided of mobile devices which let them…

- Searching and browsing any knowledge source provided by the manufacturer
- Interacting with a remote «expert room» through the network
- Performing in situ probing, measurement and diagnostic tasks

53

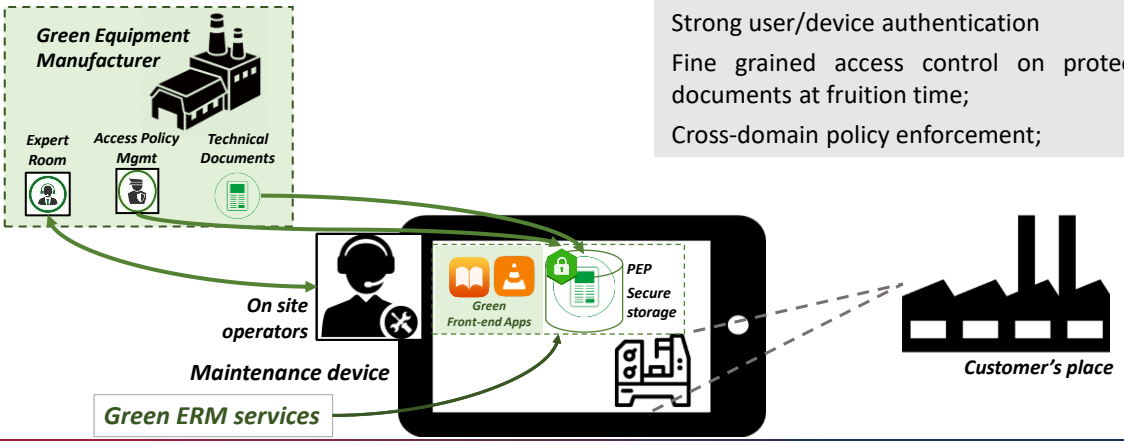
MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Enterprise Rights Management

A CASE STUDY: REMOTE MANAGEMENT

- Document encyption;
- Strong user/device authentication
- Fine grained access control on protected documents at fruition time;
- Cross-domain policy enforcement;



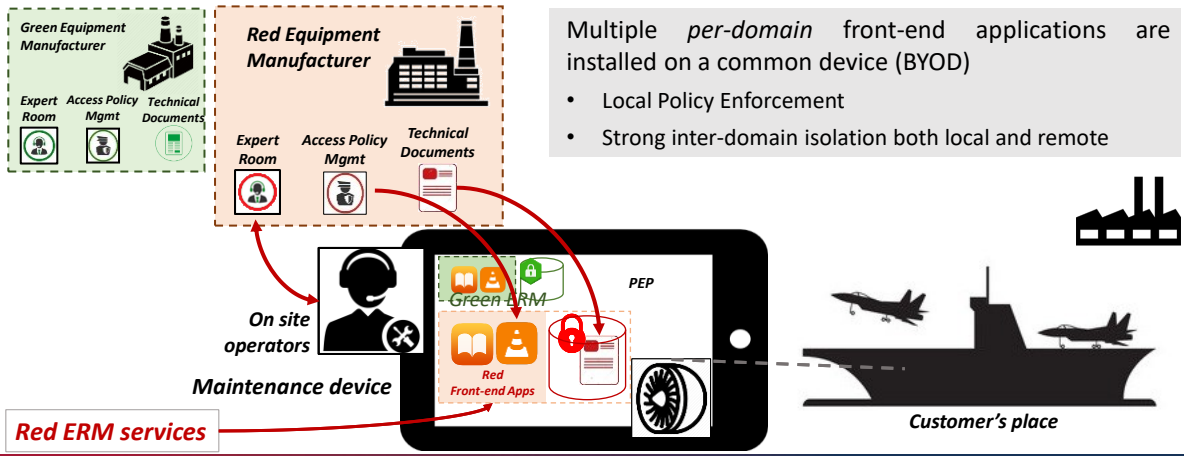
54

MEIM MASTER IN ENTREPRENEURSHIP INNOVATION MANAGEMENT IN COLLABORATION WITH MIT SLOAN

UNIVERSITÀ DEGLI STUDI DI NAPOLI PARTHENOPE

Enterprise Rights Management

A CASE STUDY: REMOTE MANAGEMENT



Multiple *per-domain* front-end applications are installed on a common device (BYOD)

- Local Policy Enforcement
- Strong inter-domain isolation both local and remote

55