MANAGING ACCESS CONTROL SYSTEMS IN DISTRIBUTED ENVIRONMENTS WITH DYNAMIC ASSET PROTECTION

PHD THESIS

University of Murcia

Author

D. Daniel Orlando Díaz López

Advisors

Dr. Félix Gómez Mármol

NEC Laboratories Europe

Prof. Dr. Gregorio Martínez Pérez

University of Murcia

November 30th, 2015

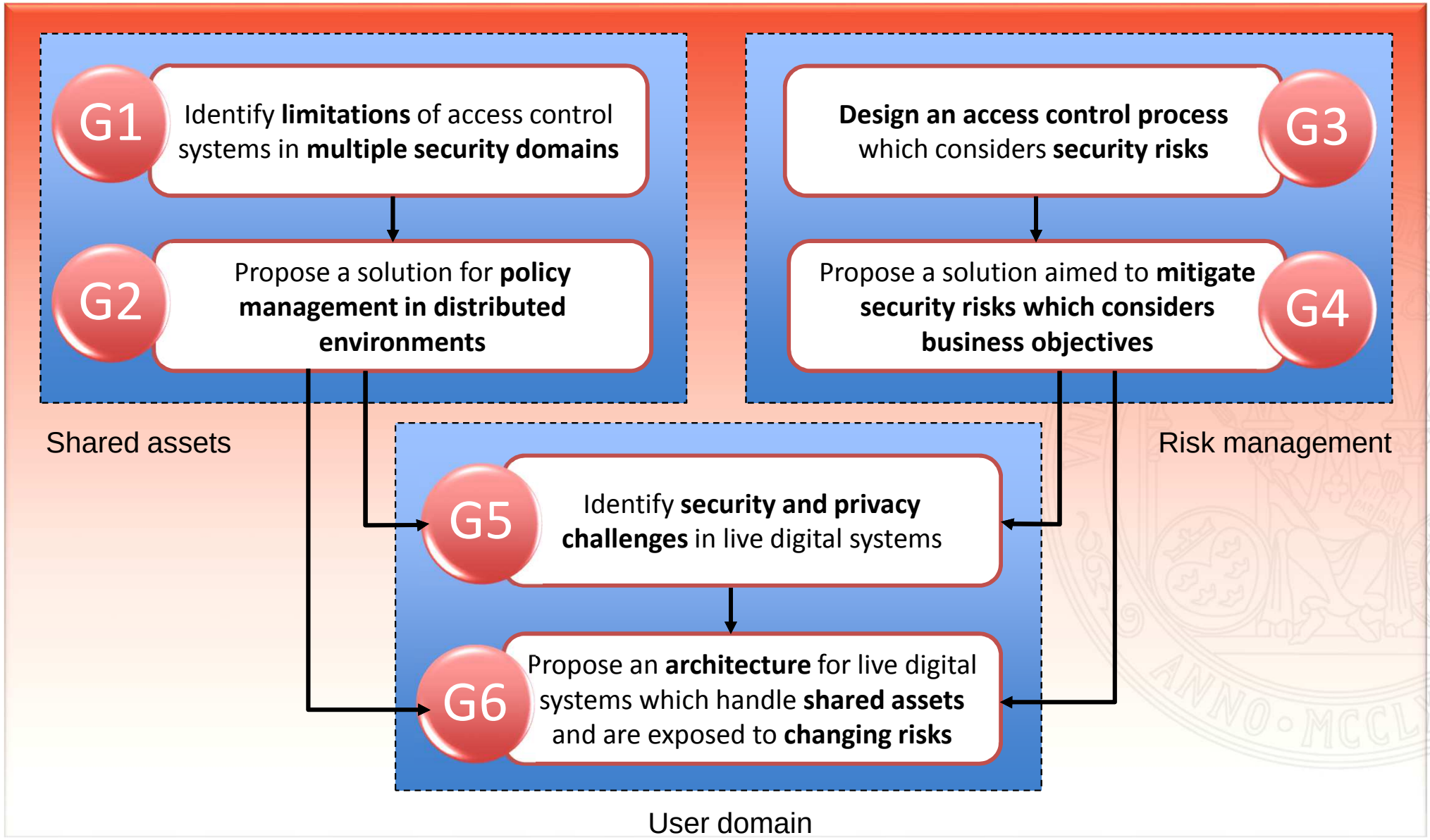
I. MOTIVATION

- **Access control** is a key element to guarantee protection of **assets**
- Information security risks are **changing** all the time, so safeguards to protect **assets** should adapt accordingly
- There are new business models based on **shared assets** in distributed environments
- Almost each one of us has a **digital life (asset)** exposed to privacy risks in a hostile environment

I. MOTIVATION

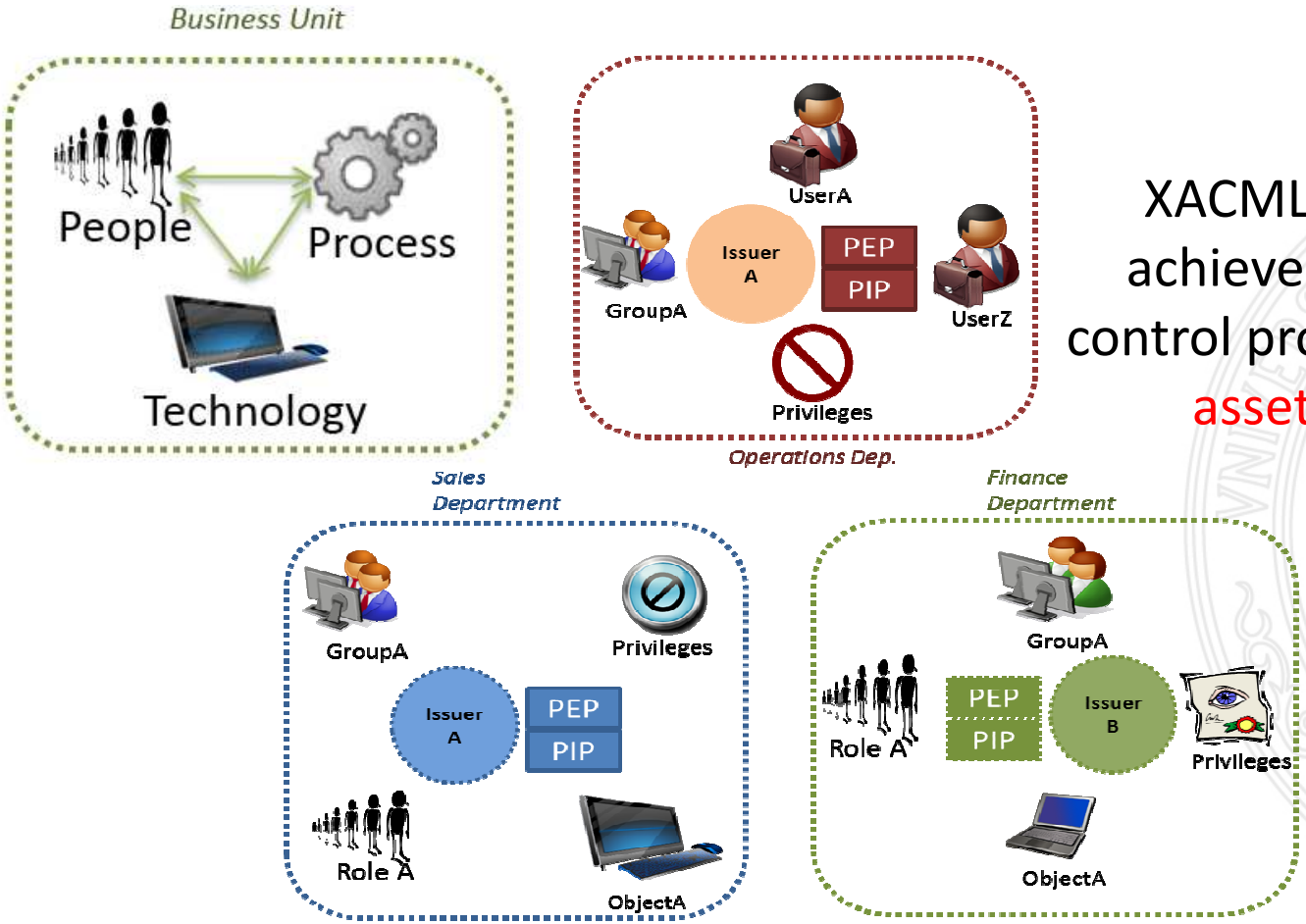
OUR MAIN GOAL IS TO ACHIEVE AN EFFECTIVE **MANAGEMENT OF ACCESS CONTROL SYSTEMS** IN DISTRIBUTED SCENARIOS WHICH PROTECTS **INFORMATION ASSETS**

II. ROADMAP


G1
Identify **limitations** of access control systems in **multiple security domains**
G2
Propose a solution for **policy management in distributed environments**
Shared assets
G3
Design an access control process which considers **security risks**
G4
Propose a solution aimed to **mitigate security risks which considers business objectives**
Risk management
G5
Identify **security and privacy challenges** in live digital systems
G6
Propose an **architecture** for live digital systems which handle **shared assets** and are exposed to **changing risks**
User domain

III. MANAGING XACML INFRASTRUCTURE
Isolated access control processes

We know that the **authorization aspect** (privileges) over corporative **assets** is a must in security of information



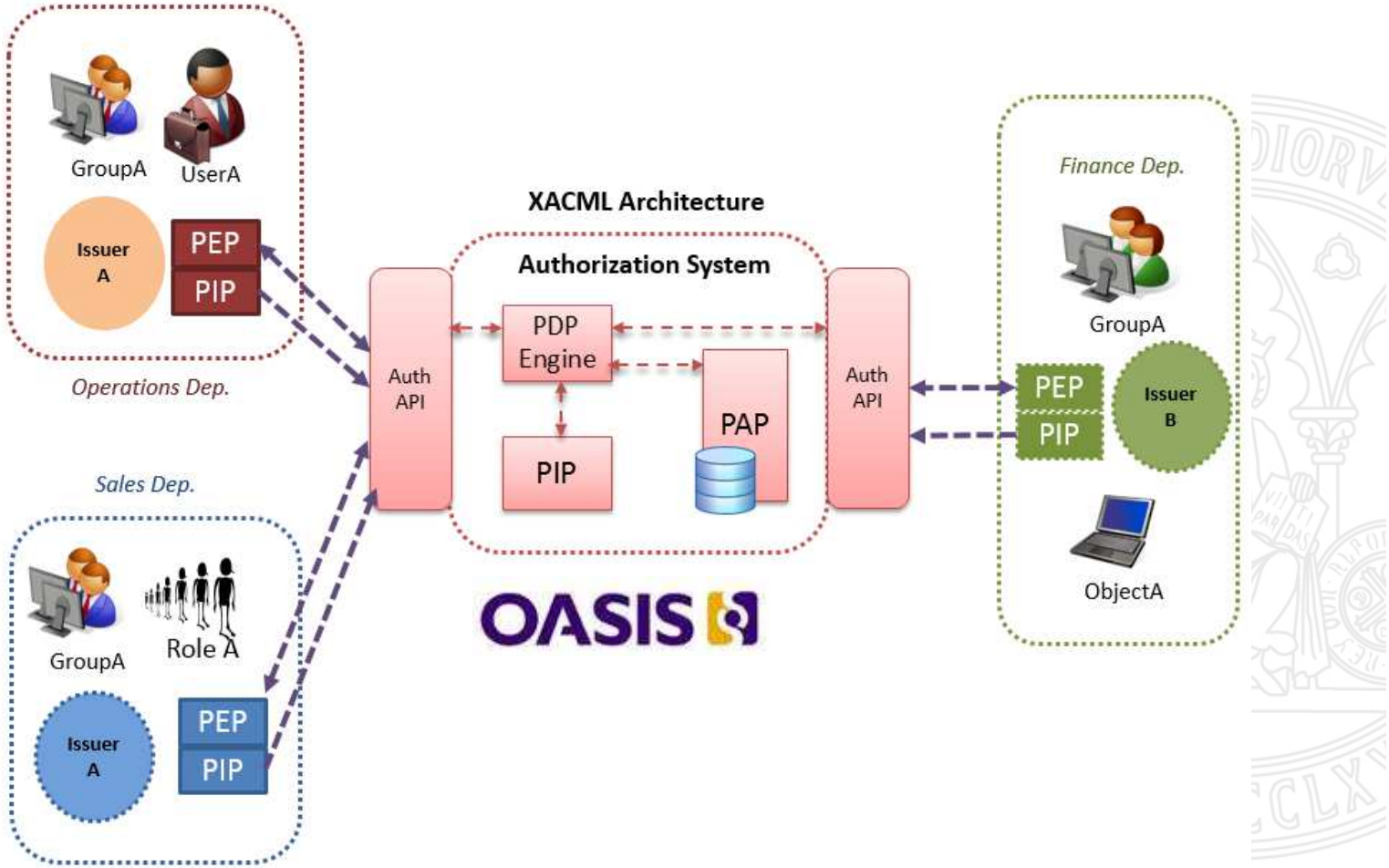
XACML offers a way to achieve a central access control process and supports asset governance!

However in real world **each corporate area** initially implements its **own access rules** to control access to **corporative assets** in their business unit

III. MANAGING XACML INFRASTRUCTURE
XACML definitions

XACML defines **XML schemas** for access policies, access request, response; and an **architecture** composed of PAP, PDP, PEP and PIP.

This architecture works for **one security domain**, but...



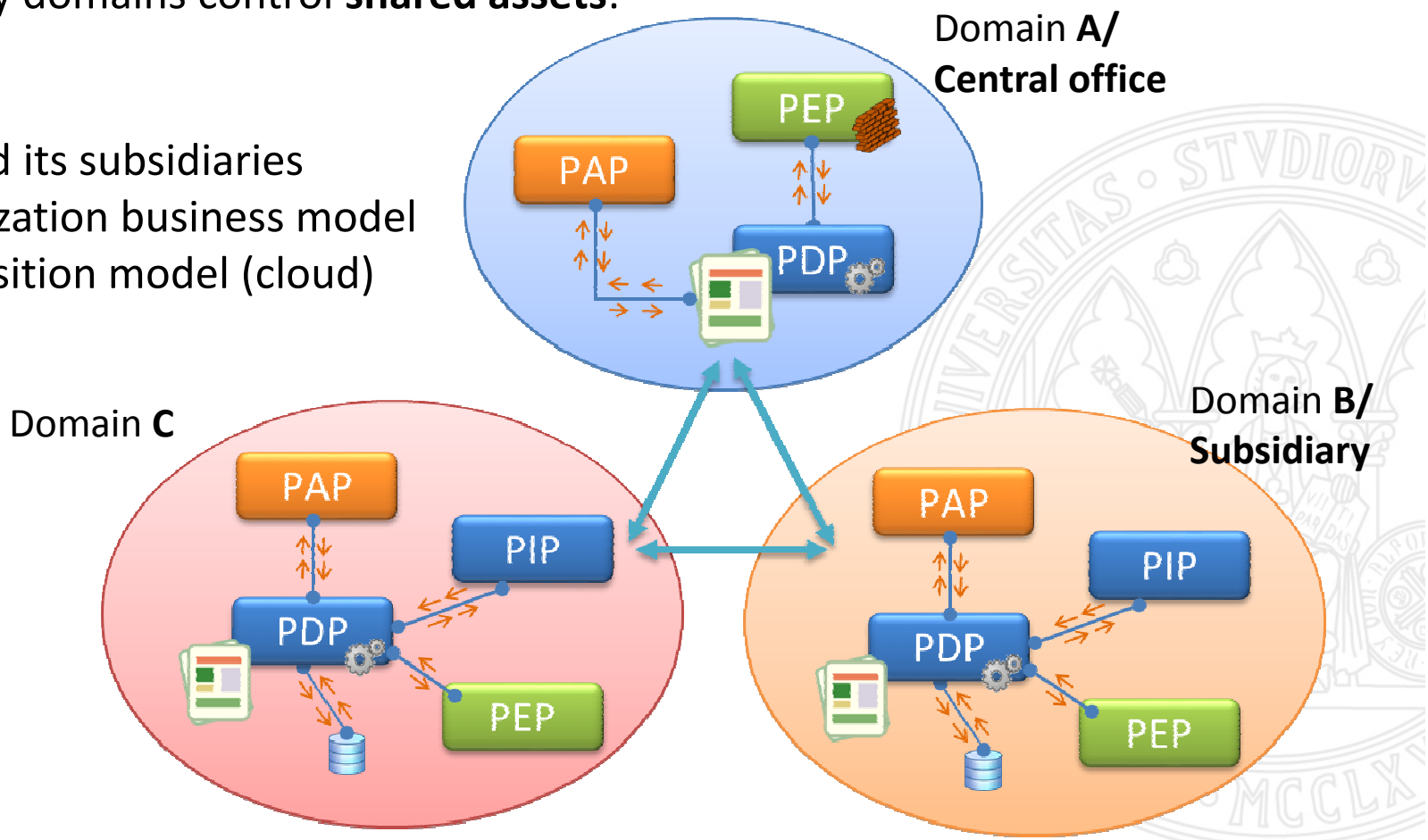
1) Is this suitable for larger environments where there are multiple **"owners" of an asset**?

2) Is this suitable for supporting **distributed access control architectures**?

III. MANAGING XACML INFRASTRUCTURE
XACML limitations

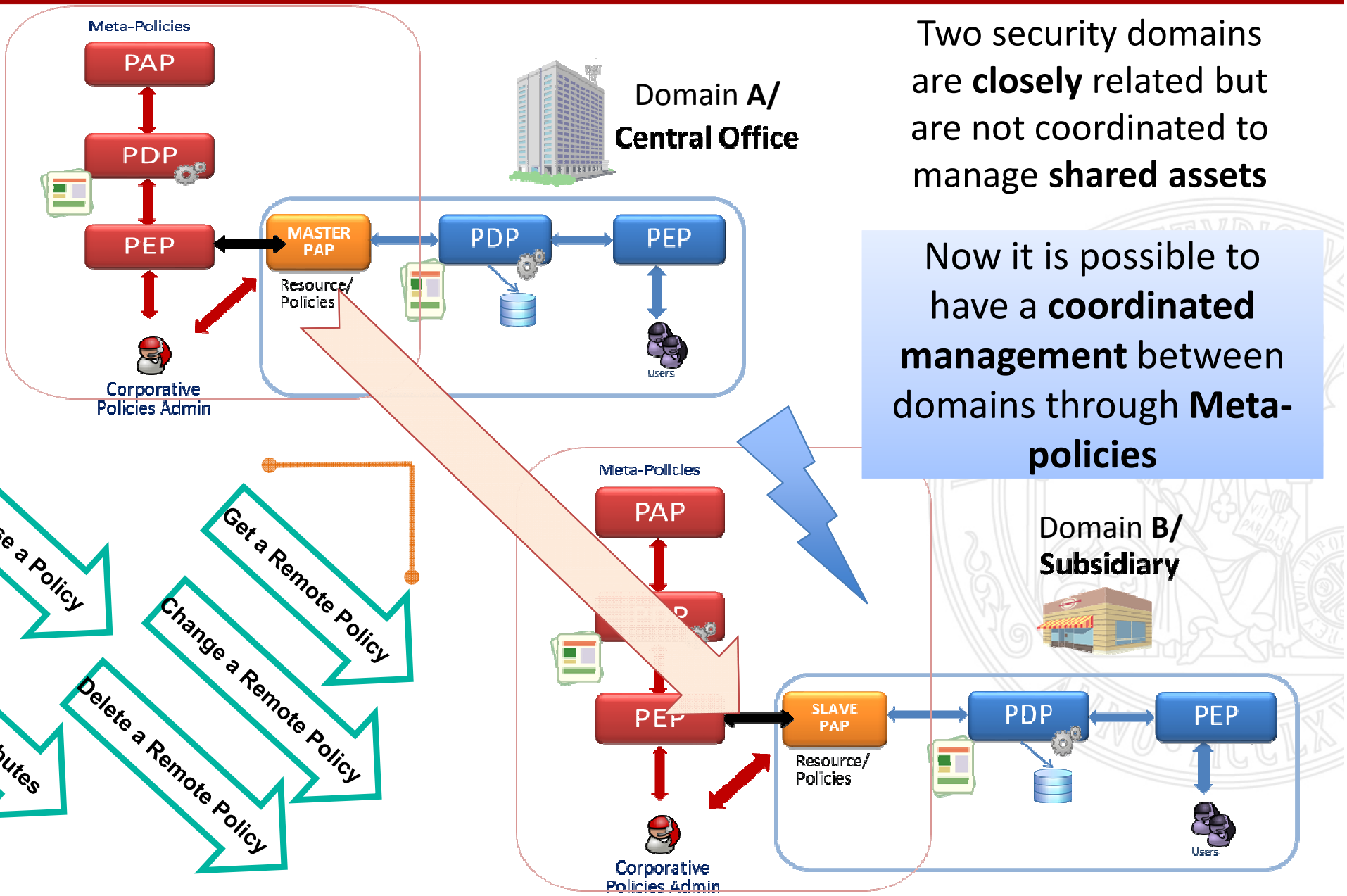
We are talking about extension of XACML to **distributed/collaborative environments** where many security domains control **shared assets**:

- A main office and its subsidiaries
- A service virtualization business model
- A service composition model (cloud)



If each security domain deploys an independent XACML architecture with its own access policies how would it be possible to get a coordinated management?

III. MANAGING XACML INFRASTRUCTURE
Distributed XACML access policies management architecture



Two security domains are **closely** related but are not coordinated to manage **shared assets**

Now it is possible to have a **coordinated management** between domains through **Meta-policies**

III. MANAGING XACML INFRASTRUCTURE
Distributed XACML access policies management architecture

How do we manage Access control policies in **another** domain?

XACML Policy

$$Policy = \langle Target \parallel (\varnothing \mid Rule_1, \ldots, Rule_n) \parallel RuleCombiningAlgorithm \parallel (\varnothing \mid Obligation_1, \ldots, Obligation_n)\rangle$$

$$Rule = \langle Target \parallel (\varnothing \mid Condition_1, \ldots, Condition_n) \parallel Effect\rangle$$

$$Target = \langle (\varnothing \mid Subject_1, \ldots, Subject_n) \parallel (\varnothing \mid Resource_1, \ldots, Resource_n) \parallel (\varnothing \mid Action_1, \ldots, Action_n) \parallel (\varnothing \mid Environment_1, \ldots, Environment_n)\rangle$$

XACML MetaPolicy

$$MetaPolicy = \langle Target \parallel (\varnothing \mid Rule_1, \ldots, Rule_n) \parallel RuleCombiningAlgorithm \parallel (\varnothing \mid Obligation_1, \ldots, Obligation_n)\rangle$$

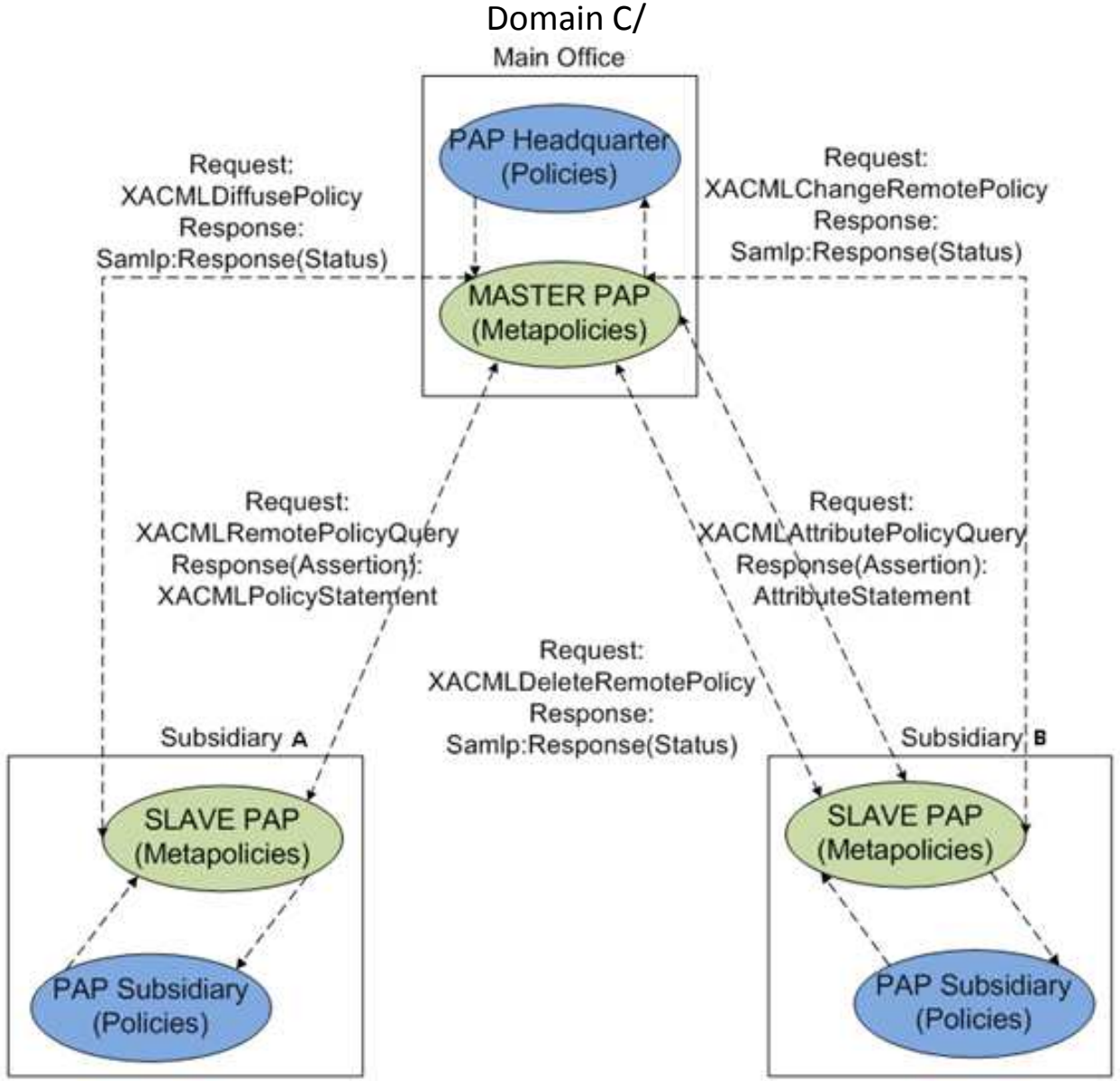
$$Rule = \langle Target \parallel (\varnothing \mid Condition_1, \ldots, Condition_n) \parallel Effect\rangle$$

$$Target = \langle (\varnothing \mid Subject_1, \ldots, Subject_n) \parallel ((\varnothing \mid Policy_1, \ldots, Policy_n) \mid (\varnothing \mid PolicySet_1, \ldots, PolicySet_n)) \parallel (\varnothing \mid Action_1, \ldots, Action_n) \parallel (\varnothing \mid Environment_1, \ldots, Environment_n)\rangle$$

XACML architecture is **reused and its fine-grained access control capacity** is applied to policy management

III. MANAGING XACML INFRASTRUCTURE
Security extensions for distributed access control policies management

XACML does not define protocols or transport mechanisms, but it can be secured by SAML



We propose a new group of **5 queries and 5 responses** to support the new policy management operations

Risks against **confidentiality** and **integrity** on policies are reduced

III. MANAGING XACML INFRASTRUCTURE
Security threat analysis

There at least two possible attacks:

i. Attempt to **tamper messages (integrity)** involved in a policy management operation during the communication processes

ii. Attempt to execute any ill-intentioned action to get access to **information assets** (i.e. policies and attributes) in one domain (**confidentiality**)

These attacks can be executed through some of the following **threats**:

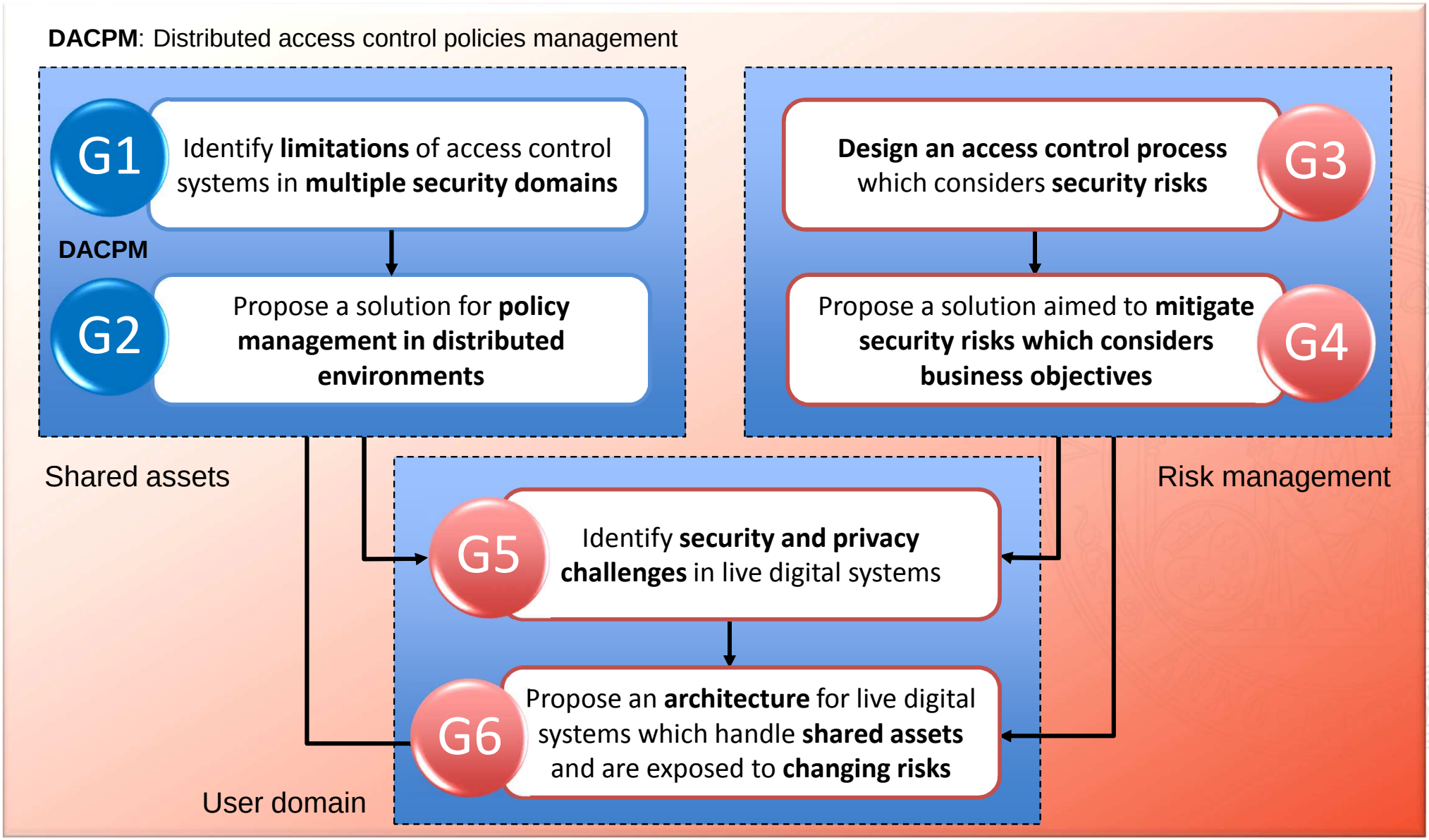
And these threats can be faced with the following **three valid security controls:**

		Technologies		
		XML encryption over SAML	XML signature over SAML	SSL/TLS
Threats	Data modification		X	X
	Eavesdropping	Partially		X
	Identity spoofing		X	X
	Man-in-the-Middle	Partially		X
	Denial-of-Service		Partially	Partially
	Forged Claims		X	X
	Replay of Message parts		X	X

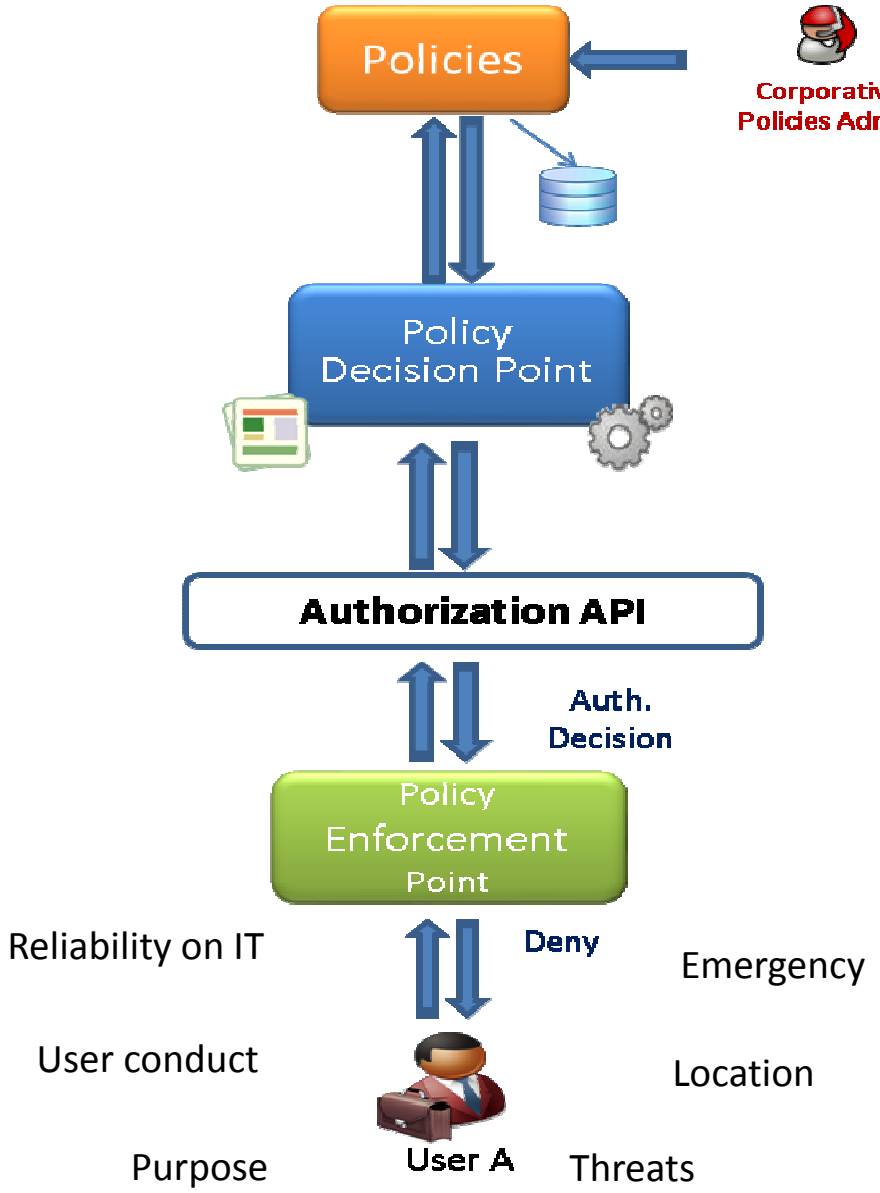
CENTUM
CIEN AÑOS DE LA UNIVERSIDAD DE MURCIA
1915 | 2015

ROADMAP

UNIVERSIDAD DE MURCIA



IV. RISK-BASED ACCESS CONTROL SYSTEMS
Regular operation of access control systems



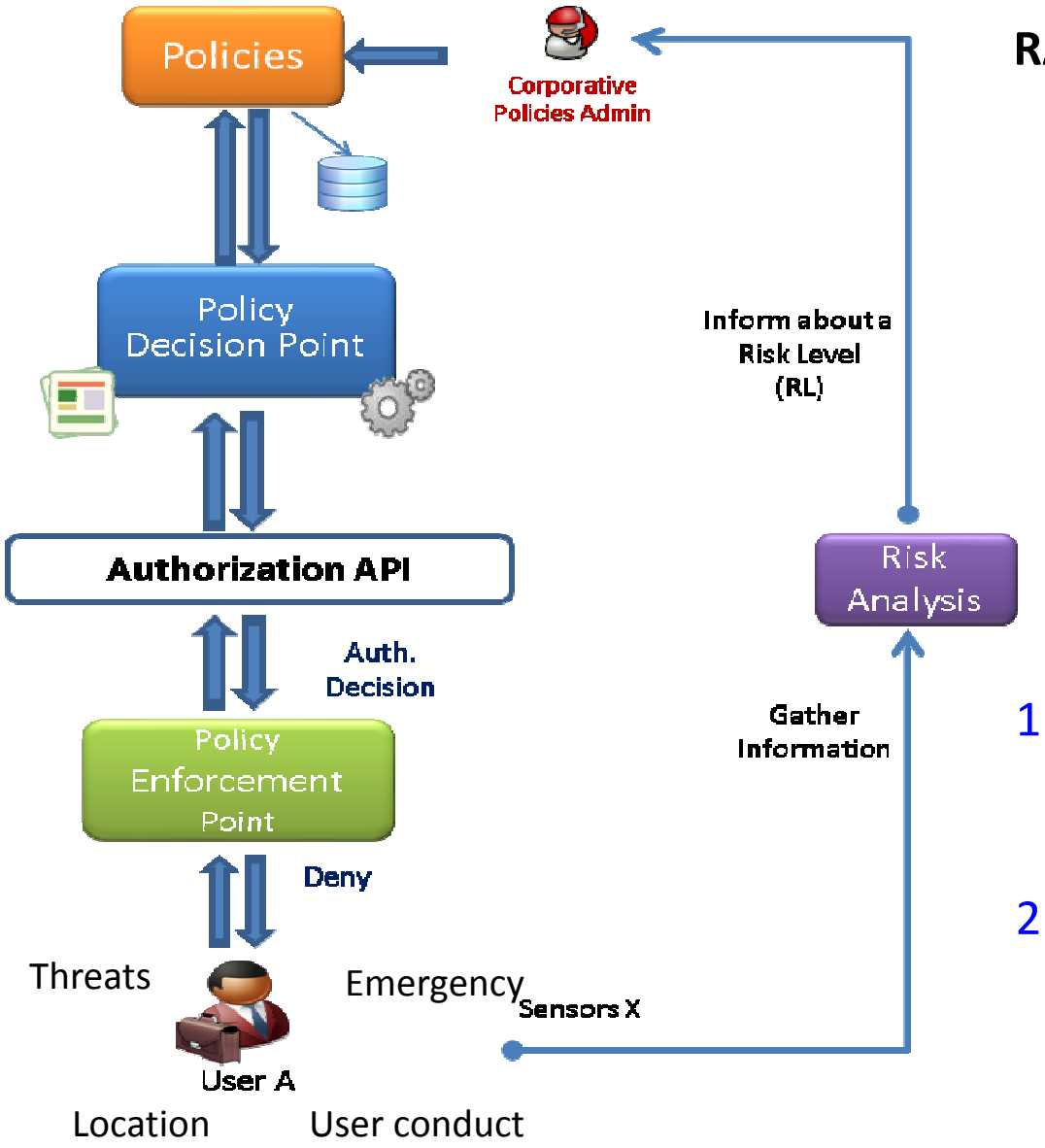
There is a general assumption in access control systems: **homogeneity** (requesters, endpoints, context, etc.)

But in fact access conditions are constantly changing: user, environment, assets, vulnerabilities, threats, etc.

Thus, there are two limitations of a regular XACML architecture:

- **Lack of dynamism.** Access control policies need to be adapted to cover each case.
- **Lack of efficiency.** Hard to manage manually in medium/large organizations

IV. RISK-BASED ACCESS CONTROL SYSTEMS
Considering risk to compute authorization



RADAC SYSTEMS (opposite to regular systems), incorporates a **Risk Analysis** as a key input for the authorization decision process

$$RL = \frac{P * I}{E}$$

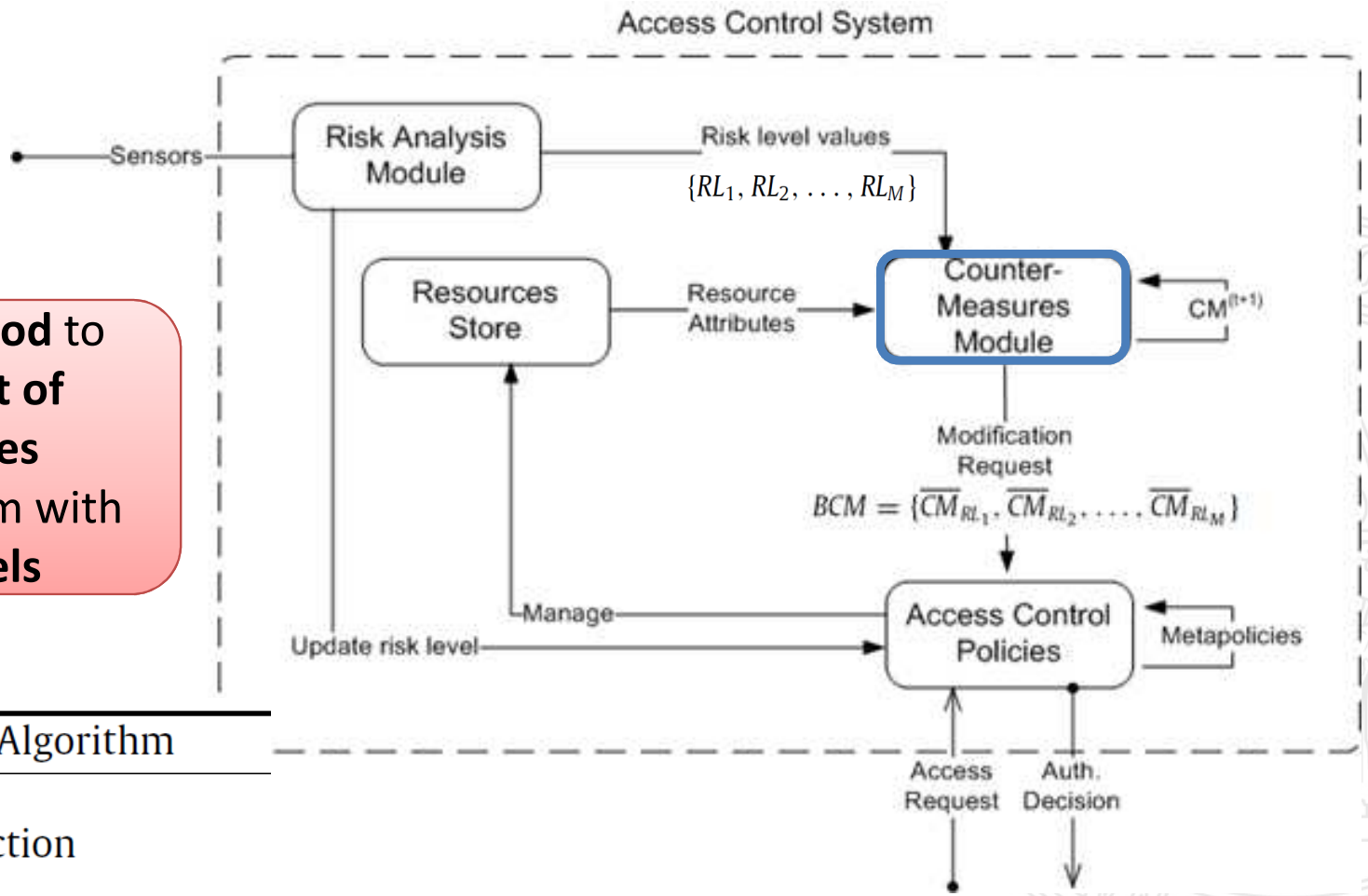
But, next facts can occur:

1. If P, I or E do not change, decision will not change: **The access to the asset is denied**
2. When ***RL*** is intolerable, the system admin must trigger counter-measures to protect the asset properly: **Not the most effective option**

IV. RISK-BASED ACCESS CONTROL SYSTEMS
Architecture and proposed modules

Threat detected

We propose a **method** to chose the **best set of counter-measures** applicable in a system with **variable risk levels**



Algorithm Optimization Algorithm

repeat
- i. Best individuals selection
- ii. Crossover
- iii. Mutation
- iv. New generation

until *StopCondition*

Counter-measures applied **Dynamic policies**

Asset protected

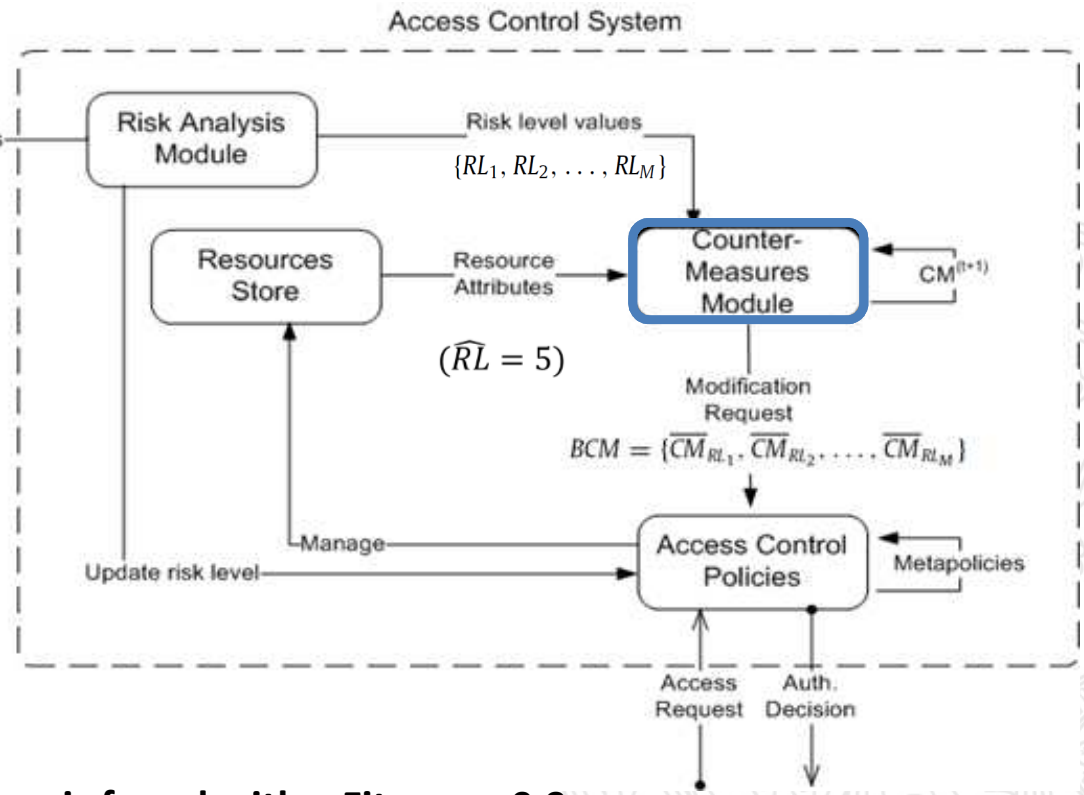
IV. RISK-BASED ACCESS CONTROL SYSTEMS
Best solutions found varying measured risk levels and aceptable risk levels

Conditions detected:

1. Failed connection from two different locations
2. Dictionary attacks have been registered
3. One new encryption vulnerability discovered
4. The file server contains confidential information

Non-negligible **"Unauthorized Access threat"** with RL = 10

Now, RL <= $\widehat{RL}$



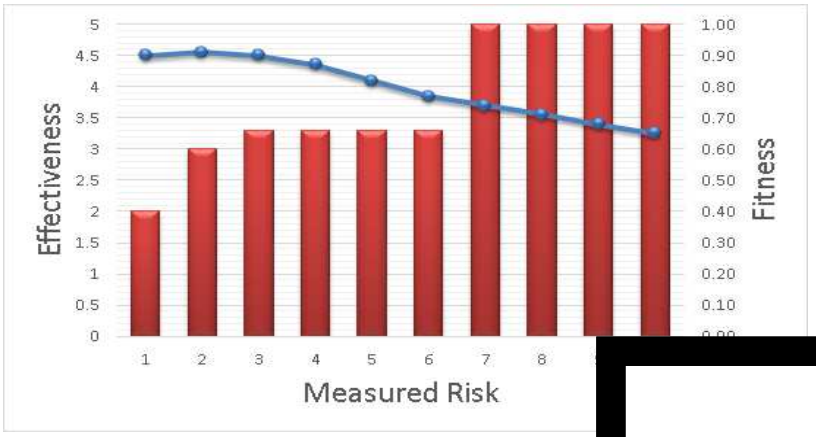
After 69 generations, a Best set of counter-measures is found with a Fitness = 0,9:

i. Authentication mechanism (E = Low)
ii. Encryption techniques (E = Low)
iii. Attestation techniques (E = **Medium**)
iv. Isolation means (E = Medium)
v. Input validation strategies (E = Low)
vi. Change management strategies (E = **Medium**)
vii. Monitoring Strategy (E = Low)
viii. Software execution schema (E = **Medium**)
ix. Session Time Assignment (E = **Medium**)
x. Resource Exposure (E = **High**)
xi. Alert Mechanism (E = **Medium**)
xii. User Advertising Strategy (E = Low)

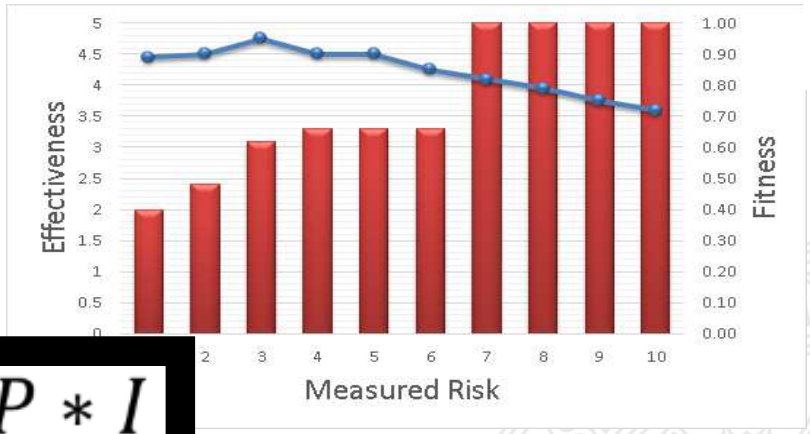
IV. RISK-BASED ACCESS CONTROL SYSTEMS

Best solutions found varying measured risk levels and aceptable risk levels

$\widehat{RL} = 1$

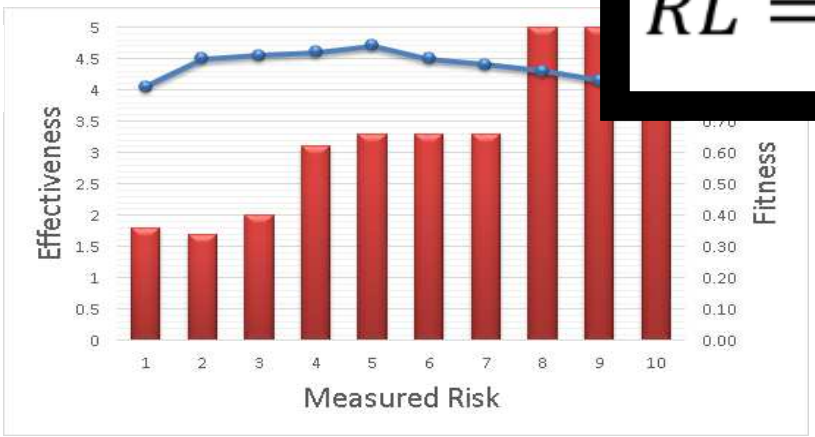


$\widehat{RL} = 2$

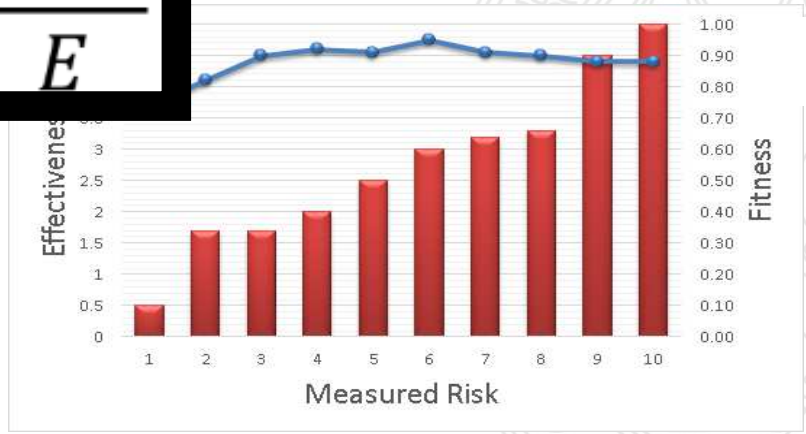


$$RL = \frac{P * I}{E}$$

$\widehat{RL} = 3$



$\widehat{RL} = 4$



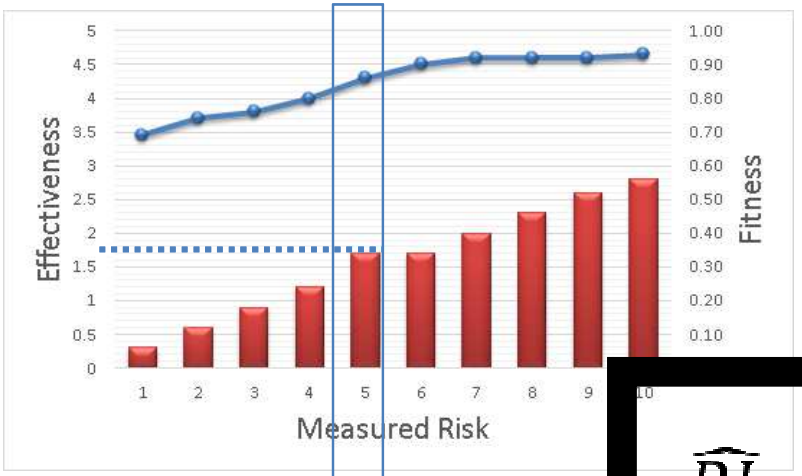
Effectiveness Fitness $\widehat{RL}$= Acceptable risk

As the **MEASURED** risk level **increases,** having a **CONSTANT** acceptable risk , the counter-measures must be **more effective**

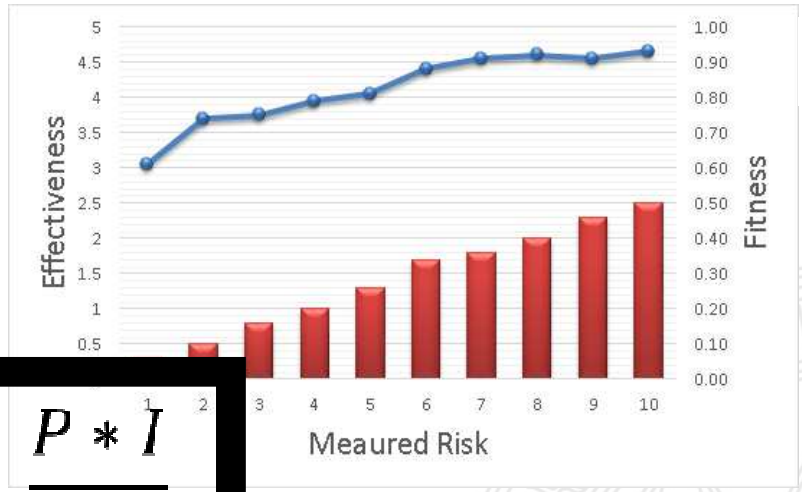
IV. RISK-BASED ACCESS CONTROL SYSTEMS

Best solutions found varying measured risk levels and aceptable risk levels

$\widehat{RL} = 7$

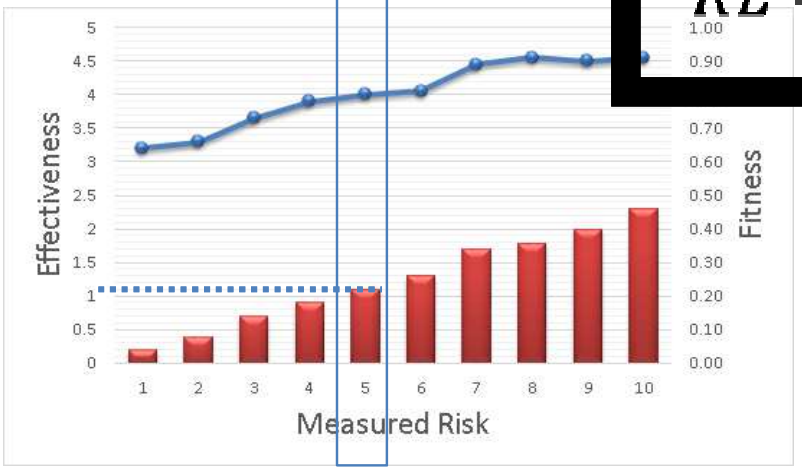


$\widehat{RL} = 8$

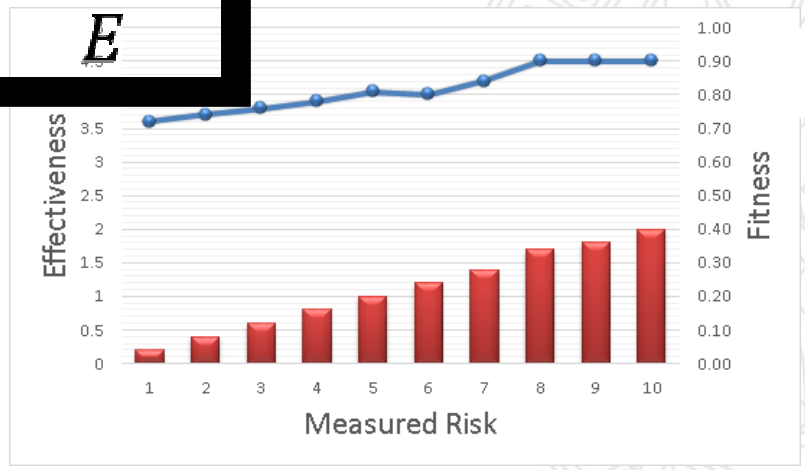


$$\widehat{RL} = \frac{P * I}{E}$$

$\widehat{RL} = 9$



$\widehat{RL} = 10$



Effectiveness Fitness

$\widehat{RL}$= Acceptable risk

As the **ACCEPTABLE** risk level **increases**, **,** having a **CONSTANT** measured risk, the counter-measures effectiveness **decrease**

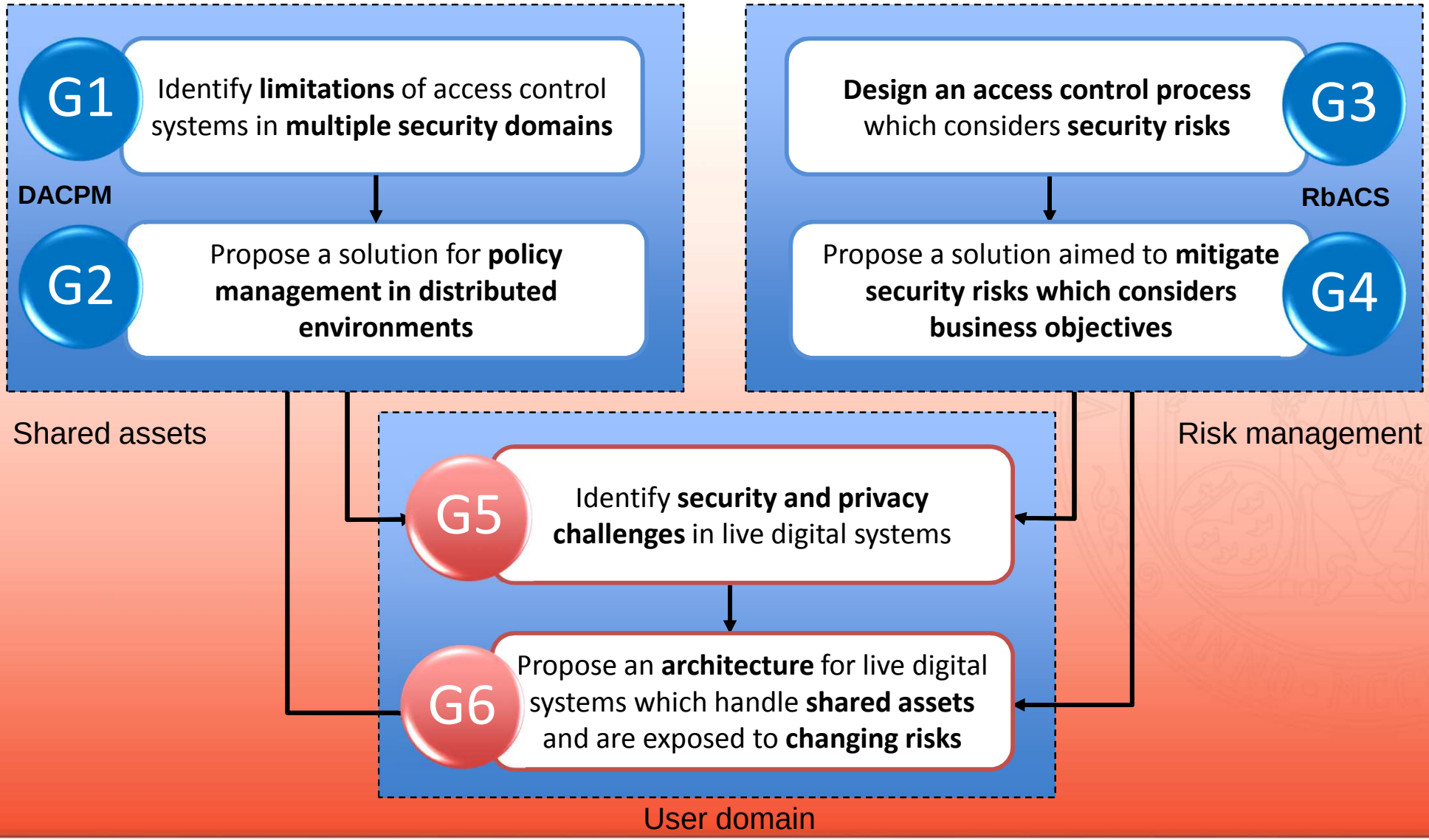
CENTUM
CIEN AÑOS DE LA UNIVERSIDAD DE MURCIA
1915 | 2015

ROADMAP

UNIVERSIDAD DE MURCIA

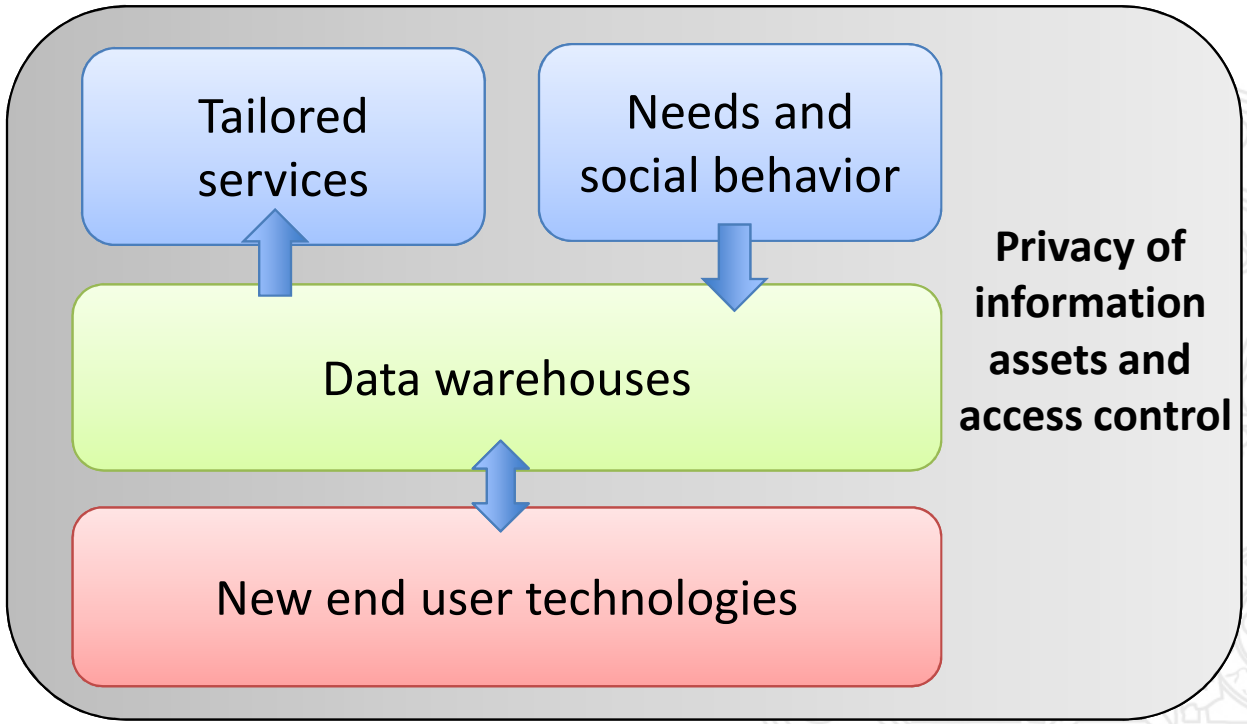
DACPM: Distributed access control policies management

RbACS : Risk-based access control system



V. LIVE DIGITAL REMEMBER DIGITAL
A regular digital life

"Your online life, permanent as a tattoo"
Juan Enriquez, TED Talks speaker



The **greater** our digital experience, the **greater** the amount of information we generate is distributed and stored along different computer systems

V. LIVE DIGITAL REMEMBER DIGITAL
Related solutions

	Desktop Search Tools				MyLifeBits Project	E-Model
	Copernic	Locate32	Google	Yahoo		
Search within files	Yes	No	Yes	Yes	Yes	Yes
Work across network shares	Until Copernic 3.0	Yes	Yes	No	No	No
Sources of personal information						
Processes over information and storage						
Processes over results						
Running	Continuously	Manual starting	Continuously	Continuously	Continuously	Manual starting
Scope						
Project Status	Up. Version 3.5	Up. Version 3.1	Discontinued (sep 2011)	Discontinued. New commercial version is X1	Current	Current

Extend toward new sources of information: IoT devices

Process and store information preserving privacy

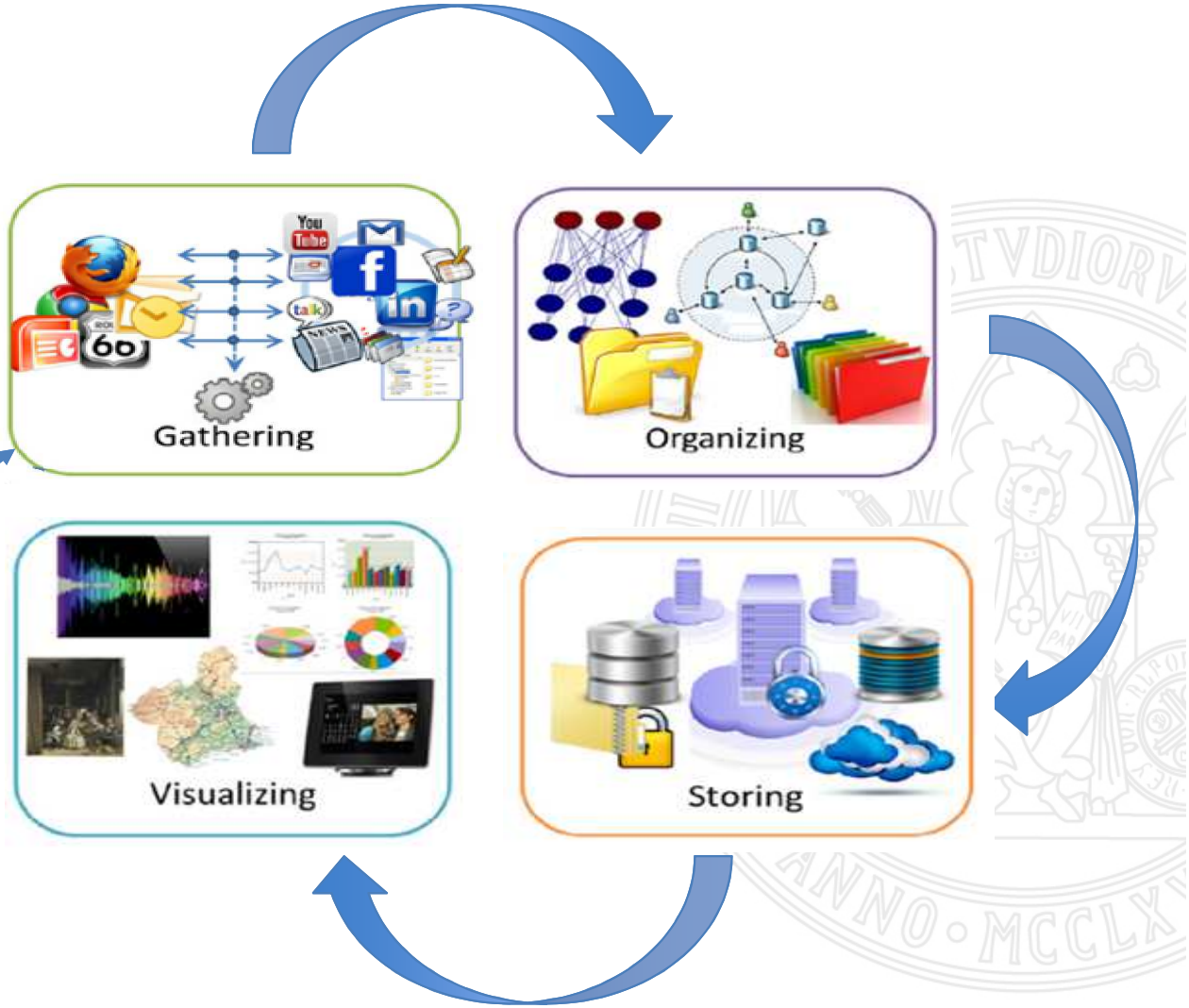
Include multiple service providers as part of the result

Develop new operations: sharing, auditing, etc.

V. LIVE DIGITAL REMEMBER DIGITAL
Main steps in live digital solutions

Raw data

- ✓ Visited websites
- ✓ Accessed documents
- ✓ Used applications
- ✓ Outgoing information
- ✓ Received e-mails
- ✓ Phone calls



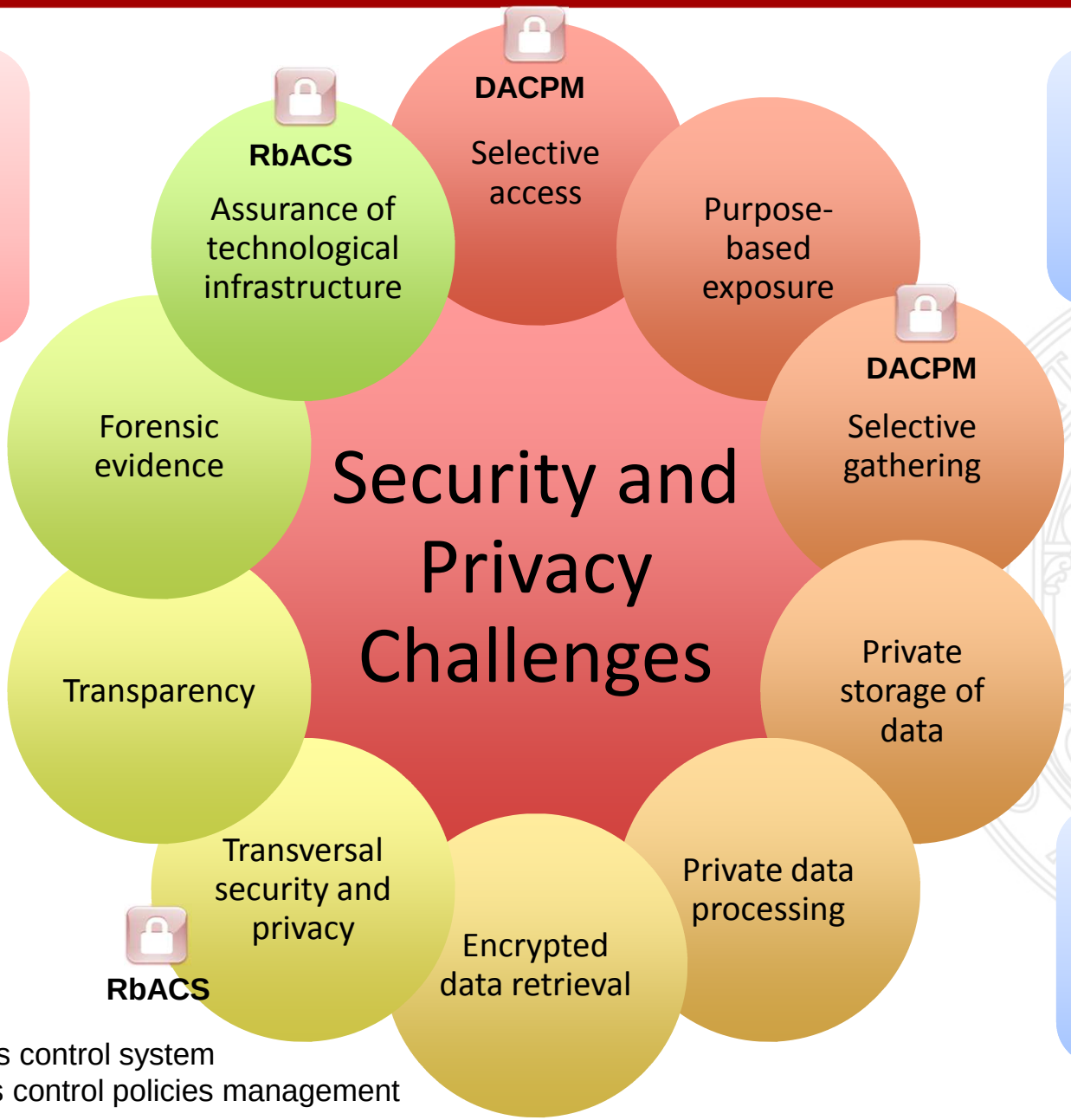
Benefits

- ✓ Efficient Search
- ✓ Information Sharing
- ✓ Audit (Protect yourself)
- ✓ Ubiquitous Recall
- ✓ Navigation through info
- ✓ Organize (by Time, Events)

We have now defined the different involved steps, but these bring many challenges …

V. LIVE DIGITAL REMEMBER DIGITAL
Live digital challenges

It is in different ways a context with **shared assets** and **variable risks**

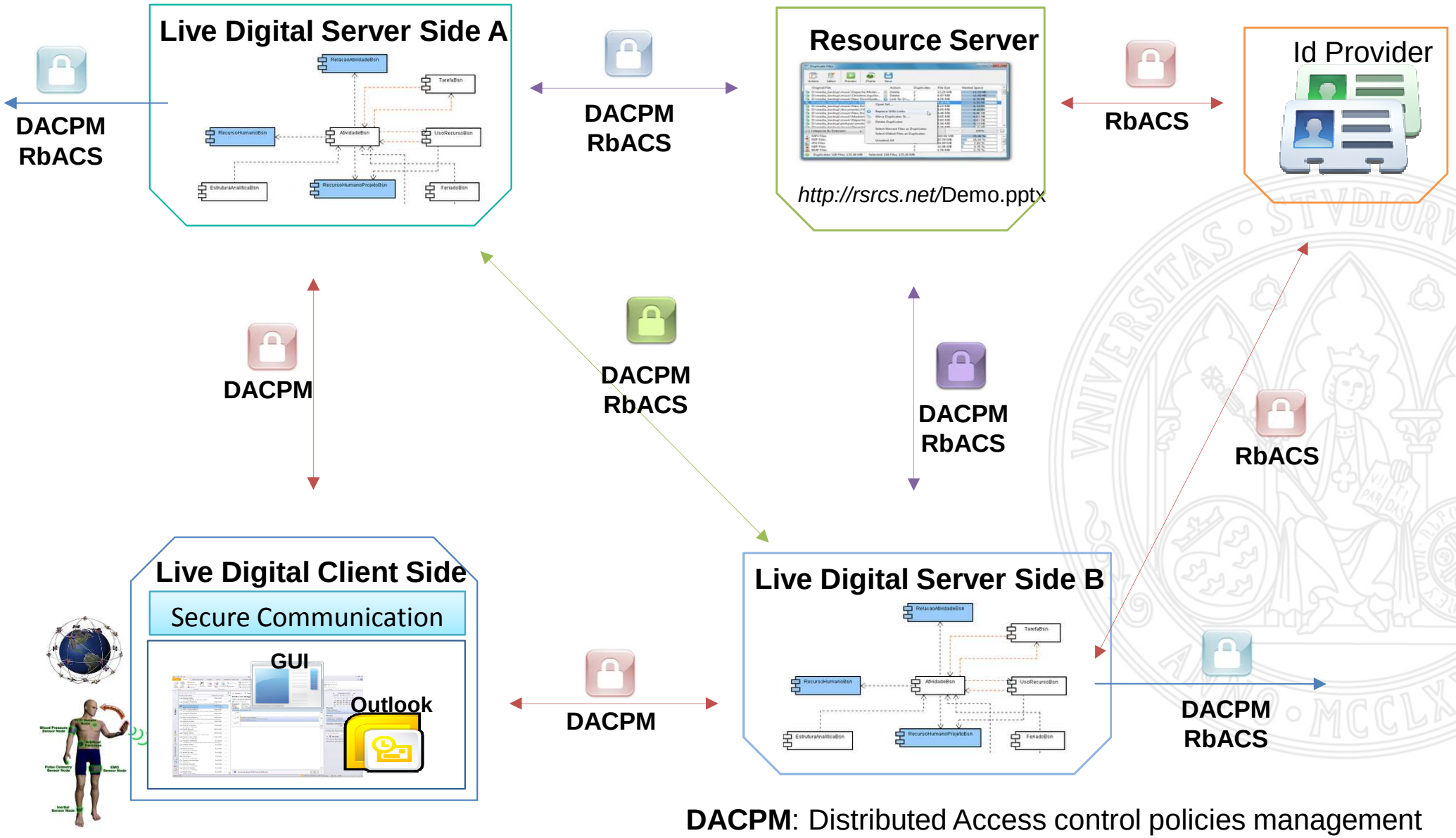


Where would it be possible to apply **access control policies management?**

Where would it be possible to apply **variable risk mitigation?**

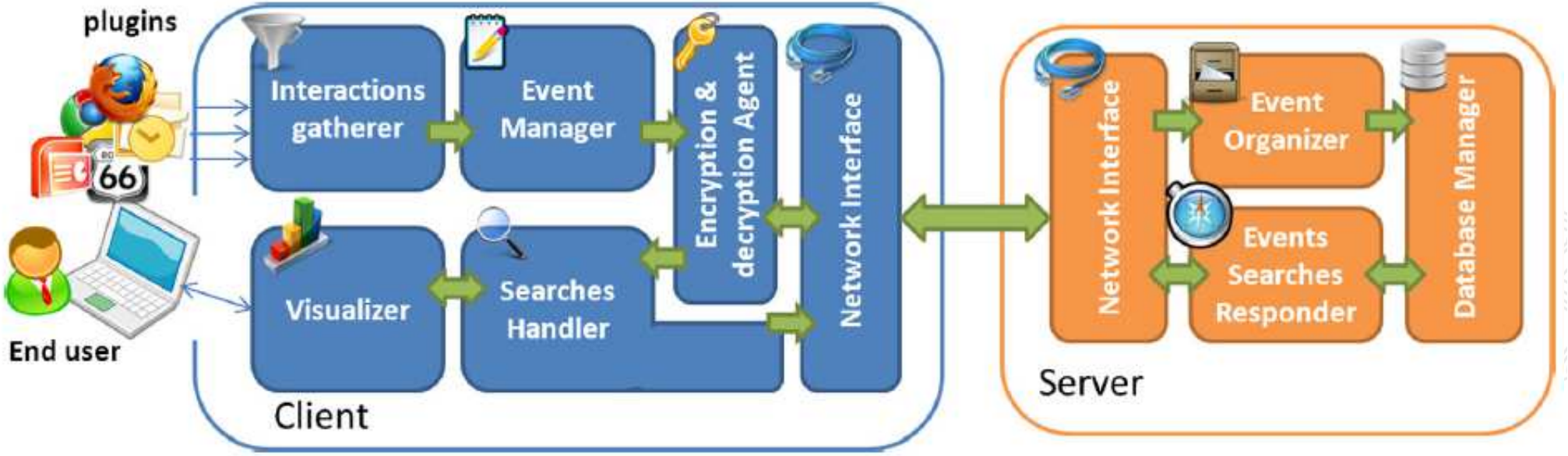
RbACS : Risk-based access control system
DACPM: Distributed Access control policies management

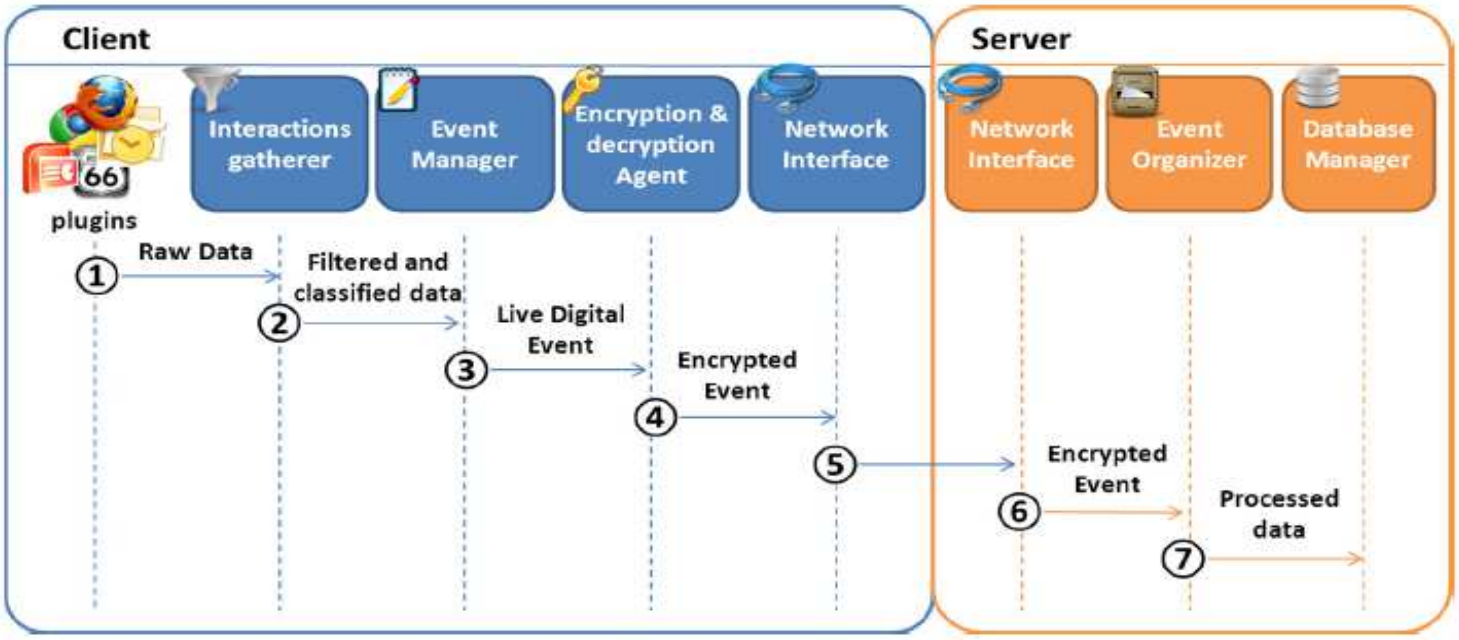
V. LIVE DIGITAL REMEMBER DIGITAL
Privacy and security challenges



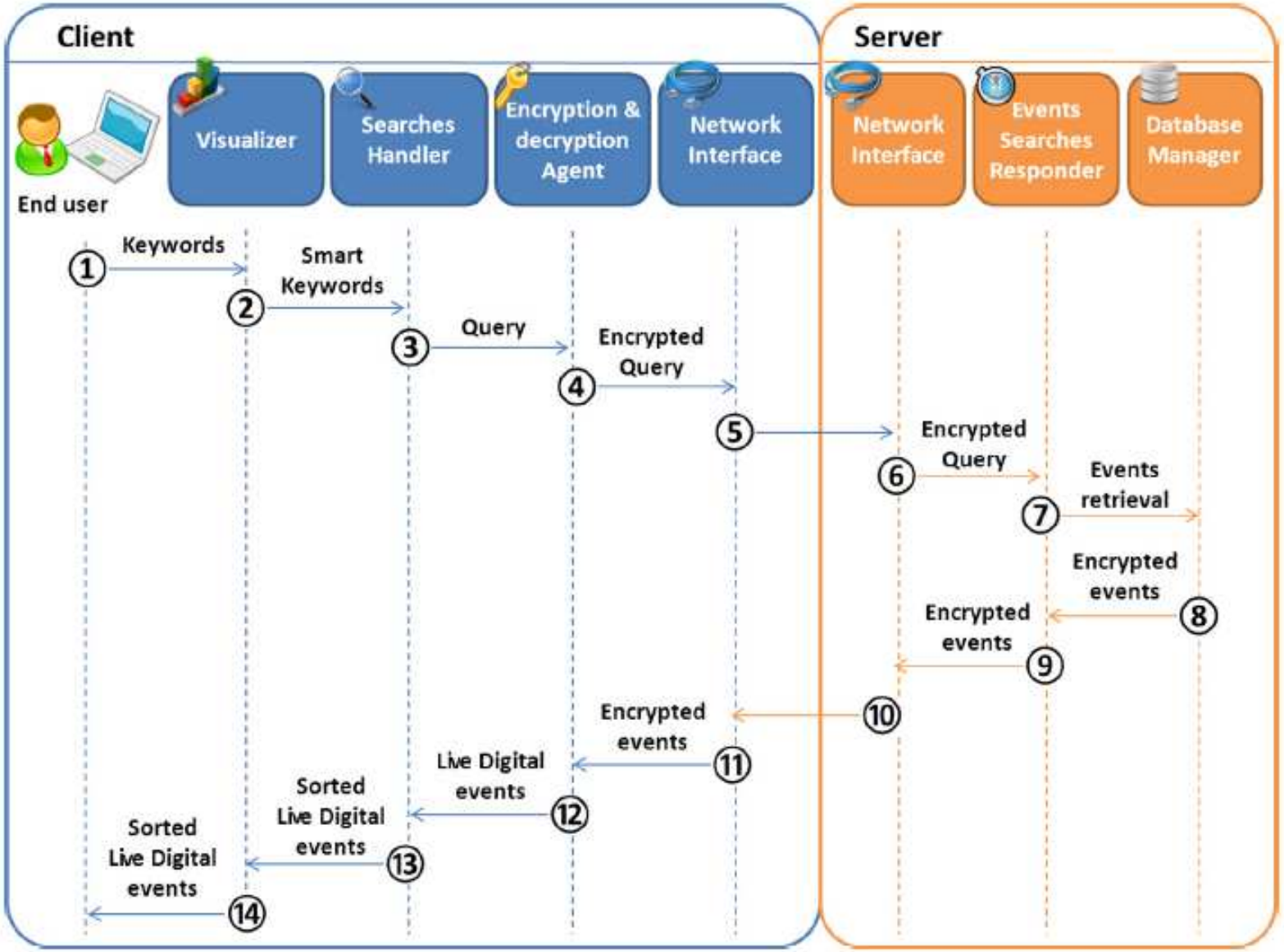
DACPM: Distributed Access control policies management
RbACS : Risk-based access control system

V. LIVE DIGITAL REMEMBER DIGITAL
High-level architectural components and data capturing process





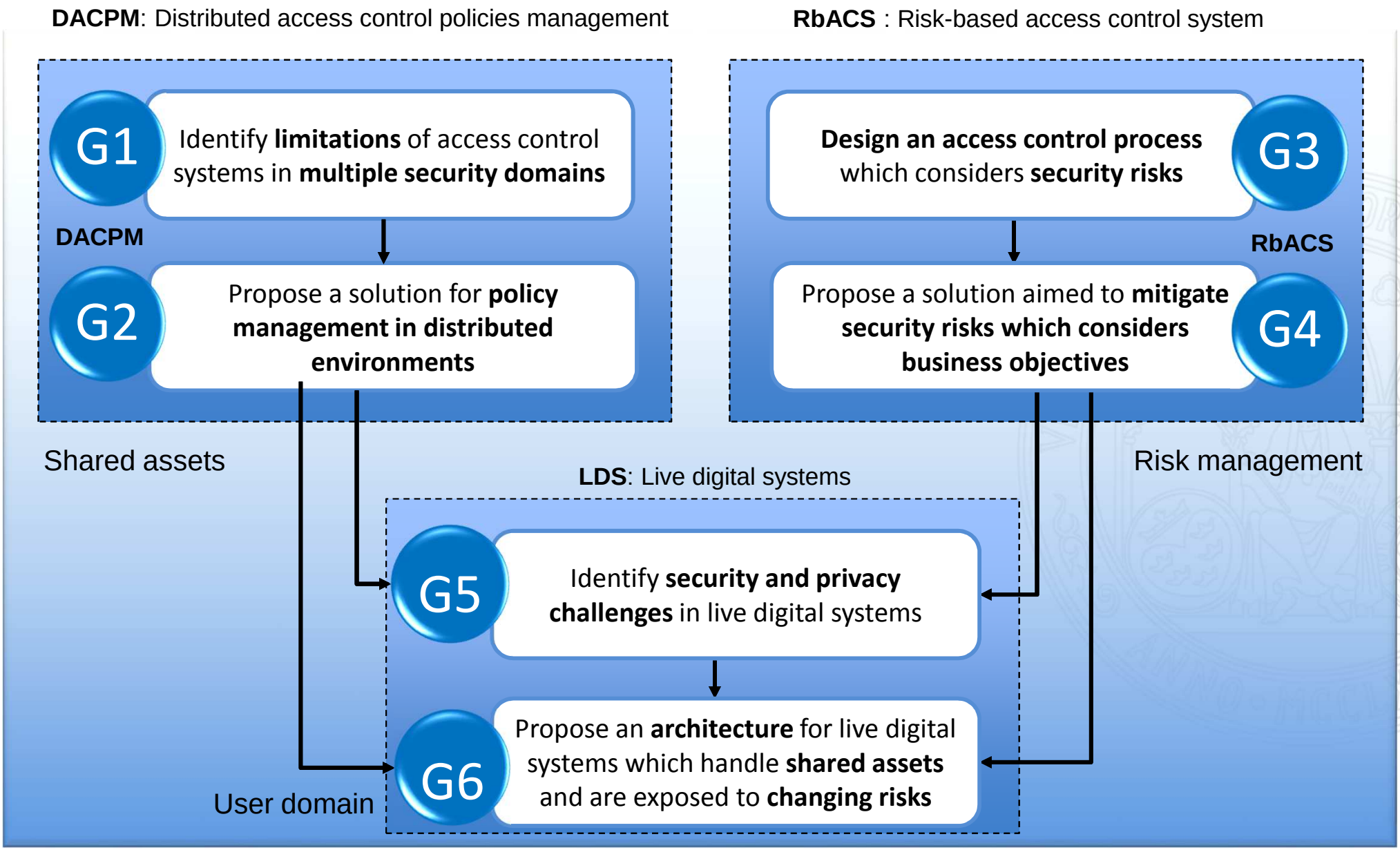
V. LIVE DIGITAL REMEMBER DIGITAL
Data recovery process



CENTUM
CIEN AÑOS DE LA UNIVERSIDAD DE MURCIA
1915 | 2015

GOALS

UNIVERSIDAD DE MURCIA



MAIN GOAL

OUR MAIN GOAL IS TO ACHIEVE AN EFFECTIVE **MANAGEMENT OF ACCESS CONTROL SYSTEMS** IN DISTRIBUTED SCENARIOS WHICH PROTECTS **INFORMATION ASSETS**

VI. CONCLUSIONS

- A well thought-out **access control process** contributes significantly to the success of an **information society**.
- Our proposal for managing XACML systems in **distributed environments** through Meta-Policies allows to manage **shared assets** in a secure way.
- Considering the **security risk** in an authorization context helps to perform operations based on business objetives and to get a practical application.
- The **dynamic** countermeasures integrated in risk-adaptable access control systems provide a way to protect assets without denying access.
- The **live digital systems** bring different **challenges** in the field of security and privacy in order to make these services effectively usable.
- The **architecture** proposed for live digital systems, plus the results obtained previously in this PhD Thesis set the first step in the road to a nearby implementation.

VII. FUTURE WORKS

- *Management of XACML systems in distributed environments:*
  - New operations, kind of policies, others resources
  - New services around shared assets
  - Legal compliance, cyber defense, etc.
- *Risk-adaptable Access control systems:*
  - New risk methodologies, threats, assets and counter-measures
  - Integration with a cyber defense decision process (OODA, CAESARS)
  - Extension to offensive purposes (Ethical hacking)
- *Live digital systems:*
  - Purpose-based exposure, storage and processing of private data, encrypted data retrieval, forensic evidence, selective access, etc.
- *Integration of the live digital architecture with shared asset and risk-adaptable access proposals*

VIII. CONTRIBUTIONS
Journals with Impact Factor (JCR)

Publications Compilation Thesis

Daniel Díaz - López, Ginés Dólera - Tormo, Félix Gómez - Mármol, Gregorio Martínez - Pérez, **"Managing XACML systems in distributed environments through Meta-Policies"**, Computers & Security, Volume 48, February 2015, Pages 92-115, ISSN 0167-4048, Impact Factor (2014) = 1.031

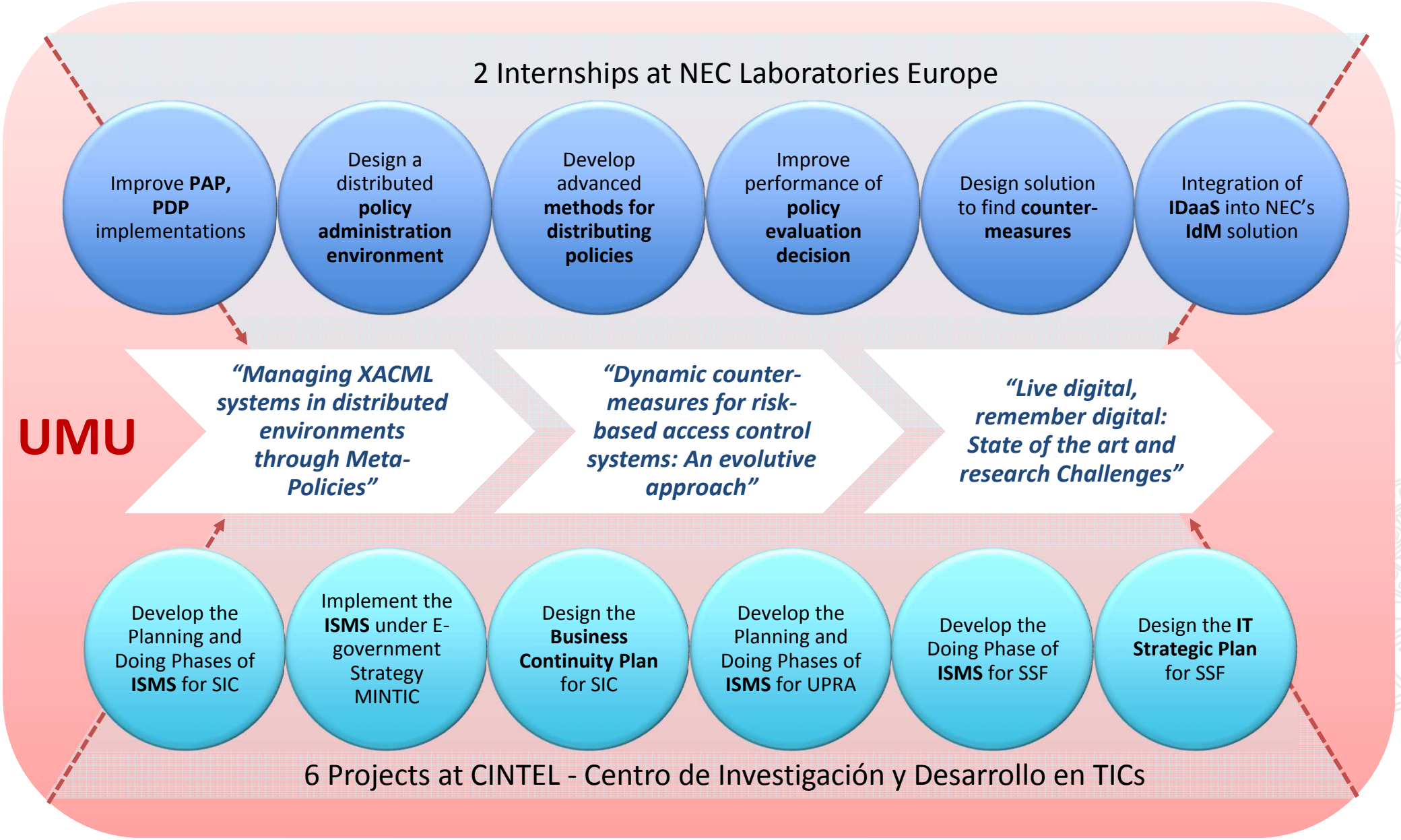
http://dx.doi.org/10.1016/j.cose.2014.10.004

Daniel Díaz - López, Ginés Dólera - Tormo, Félix Gómez - Mármol, Gregorio Martínez - Pérez, **"Dynamic counter-measures for risk-based access control systems: An evolutive approach"**, Future Generation Computer Systems, Available online 12 November 2014, ISSN 0167 - 739X, Impact Factor (2014) = 2.786

http://dx.doi.org/10.1016/j.future.2014.10.012

Daniel Díaz - López, Ginés Dólera - Tormo, Félix Gómez - Mármol, Jose M. Alcaraz-Calero, Gregorio Martínez-Pérez, **"Live digital, remember digital: State of the art and research challenges"**, Computers & Electrical Engineering, Volume 40, Issue 1, January 2014, Pages 109-120, ISSN 0045-7906, Impact Factor (2014) = 0.817
http://dx.doi.org/10.1016/j.compeleceng.2013.11.008

VIII. CONTRIBUTIONS
Internships and projects



CENTUM

CIEN AÑOS DE LA UNIVERSIDAD DE MURCIA
1915 | 2015

UNIVERSIDAD DE
MURCIA