TREDISEC
Scientific & Technical Overview

6th International Conference on e-Democracy

10 – 11 December 2015, Athens, Greece

Co-funded by the Horizon 2020 Framework Programme of the European Union

TREDISEC Overall Objective

To develop a *unified* cloud security framework for data storage and processing based on modular *end-to-end security* primitives *compatible with functional requirements*

TREDISEC Partners

Atos

arsys

NEC

grnet
Networking Research and Education

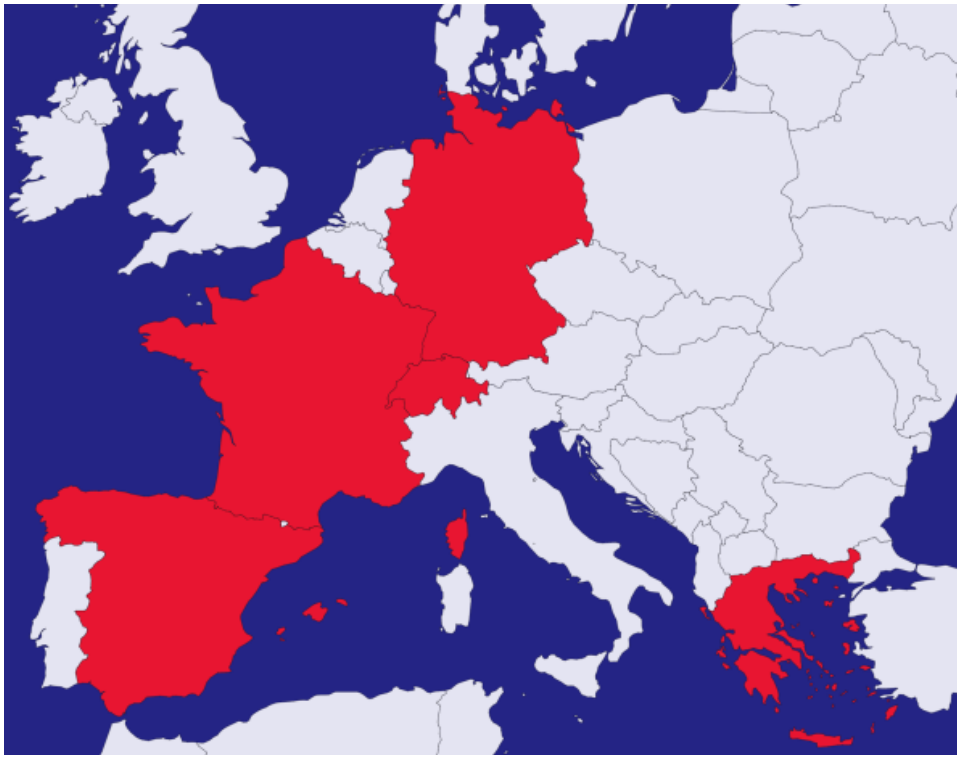
IBM

SAP

ETH zürich

SAFRAN
Morpho

EURECOM
Sophia Antipolis



tredisec

TREDISEC Time Plan

- Start: 1/4/2015
- Duration: 36 Months
- First year: Requirements and Use Cases
- Second year: Implementation
- Third year: Evaluation

Cloud Security Requirements

- Confidentiality
  - e2e data encryption:
    - encryption during transmission
    - encrypted data-at-rest
  - processing over encrypted data
- Integrity and availability
  - storage integrity and availability
  - computation verifiability
- Access control
  - policy enforcement
  - secure deletion

Cloud Functional Requirements

- Storage efficiency
  - data compression
  - data deduplication
- Multi-tenancy
  - hardware-level isolation
  - virtualization
  - application-level isolation

TREDISEC Challenges

- Data Confidentiality with Data Reduction
  - Cloud providers use deduplication to save space
  - Yet deduplication is at odds with encryption
- Current Solutions:
  - Convergent encryption seems promising
    - Data are first hashed to get key
    - Data are then encrypted with key
  - Existing solutions based on this technique either do not achieve desired security levels or rely on Trusted Third Party

TREDISEC Challenges

- Verifiability with Data Reduction and Multi-Tenancy
  - Users must have guarantee of storage in the presence of deduplication techniques
  - Users having uploaded data should be able to prove ownership even when deduplication is in use (Proof of Ownership, PoW)
- Current Solutions:
  - Existing storage integrity solutions rely on Proofs of Retrievability (PoR)
    - these solutions still induce high computational costs and cannot be combined with data reduction technique
  - Existing PoW solutions are not yet mature in terms of both performance and security

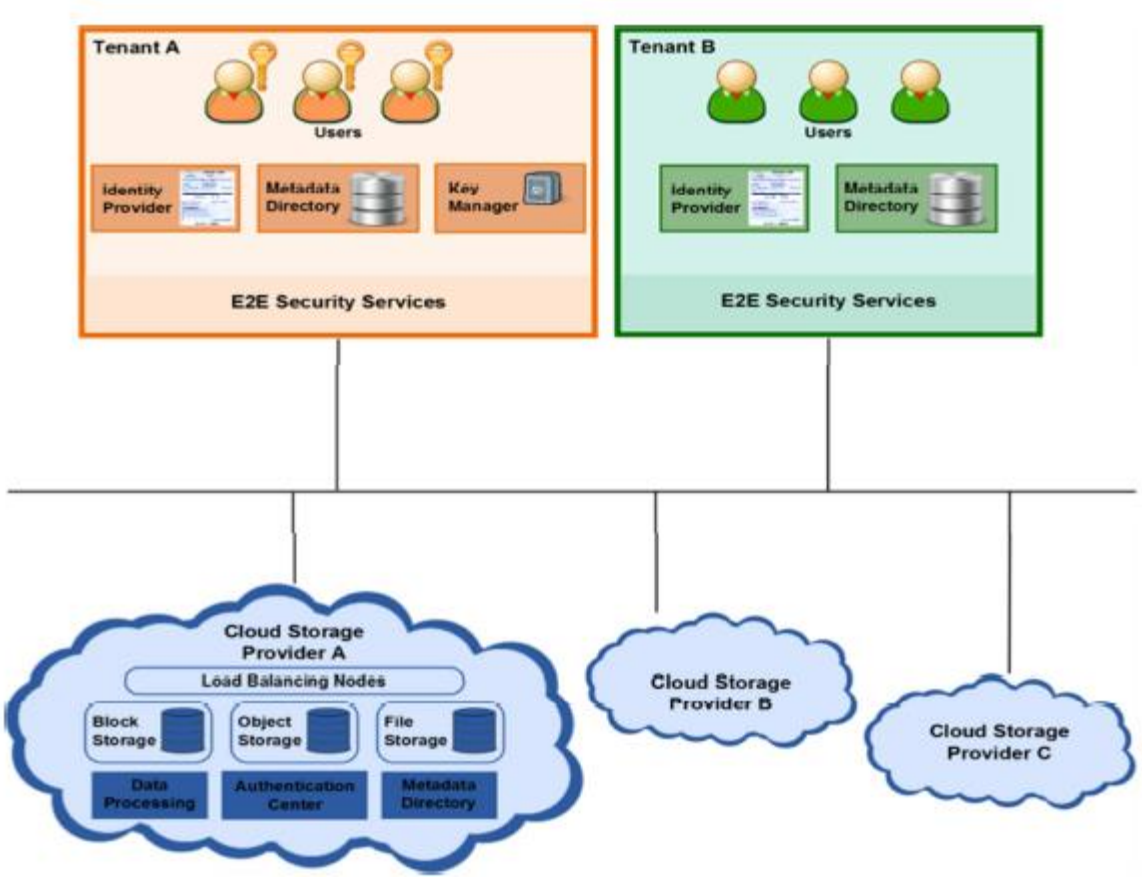
TREDISEC Challenges

- Secure Data Processing with Multi-Tenancy
  - There is a strong need for privacy preserving data processing solutions
  - In data processing, word search is the most common primitive
  - Classic encryption does not allow operations over encrypted data
- Current Solutions:
  - Recent privacy preserving word search solutions ensure privacy for both the data and the query
    - these solutions are not yet directly applicable to real industrial strength use cases
    - TREDISEC will either optimize or consider the delegation of search to trusted third parties

TREDISEC Challenges

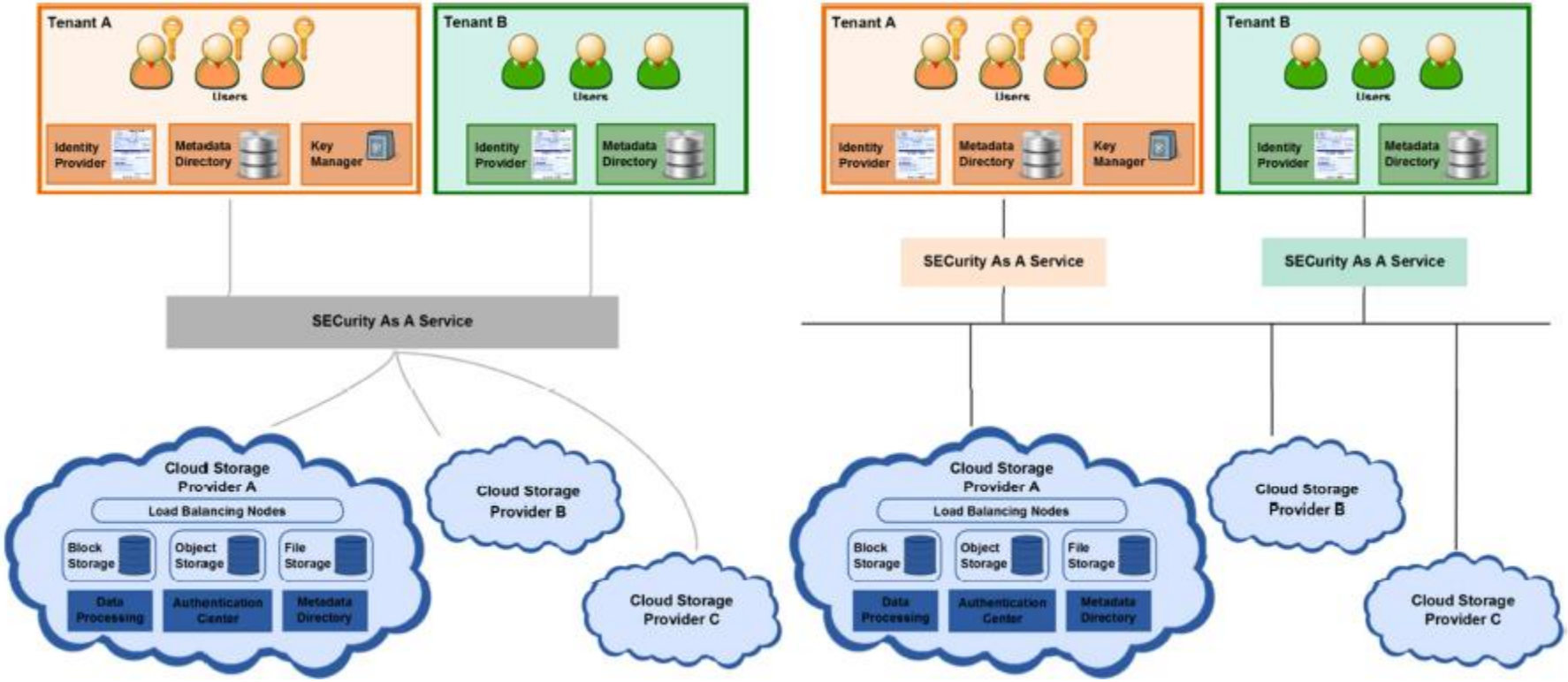
- Distributed Enforcement of Access Control Policies for Multi-Tenancy Settings
  - The security of a multi-tenant system require reliable access control polices, enforcement mechanisms, and the ability to safely delete data.
- Current Solutions:
  - Current Attribute Based Access Control (ABAC) models fall short in the multi-tenancy settings since users' attributes can be distributed across different trust domains.
    - TREDISEC will extend current ABAC models to govern access control in multi-tenant environments
  - Current cloud platforms cannot handle encryption and data sharing
    - TREDISEC will design new cryptographic primitives to enforce distributed usage of data while preventing malicious tenants from combining their credentials and escalating their access rights
  - Cloud providers do not handle secure data deletion
    - REDISEC will also investigate the problem of secure data deletion: end-users will have cryptographic guarantees on the timely deletion of their data and the back-up copies.

Architecture: E2E Security *(ideal case)*



tredisec

Architecture: Security as a Service



tredisec

Architecture: hybrid solution

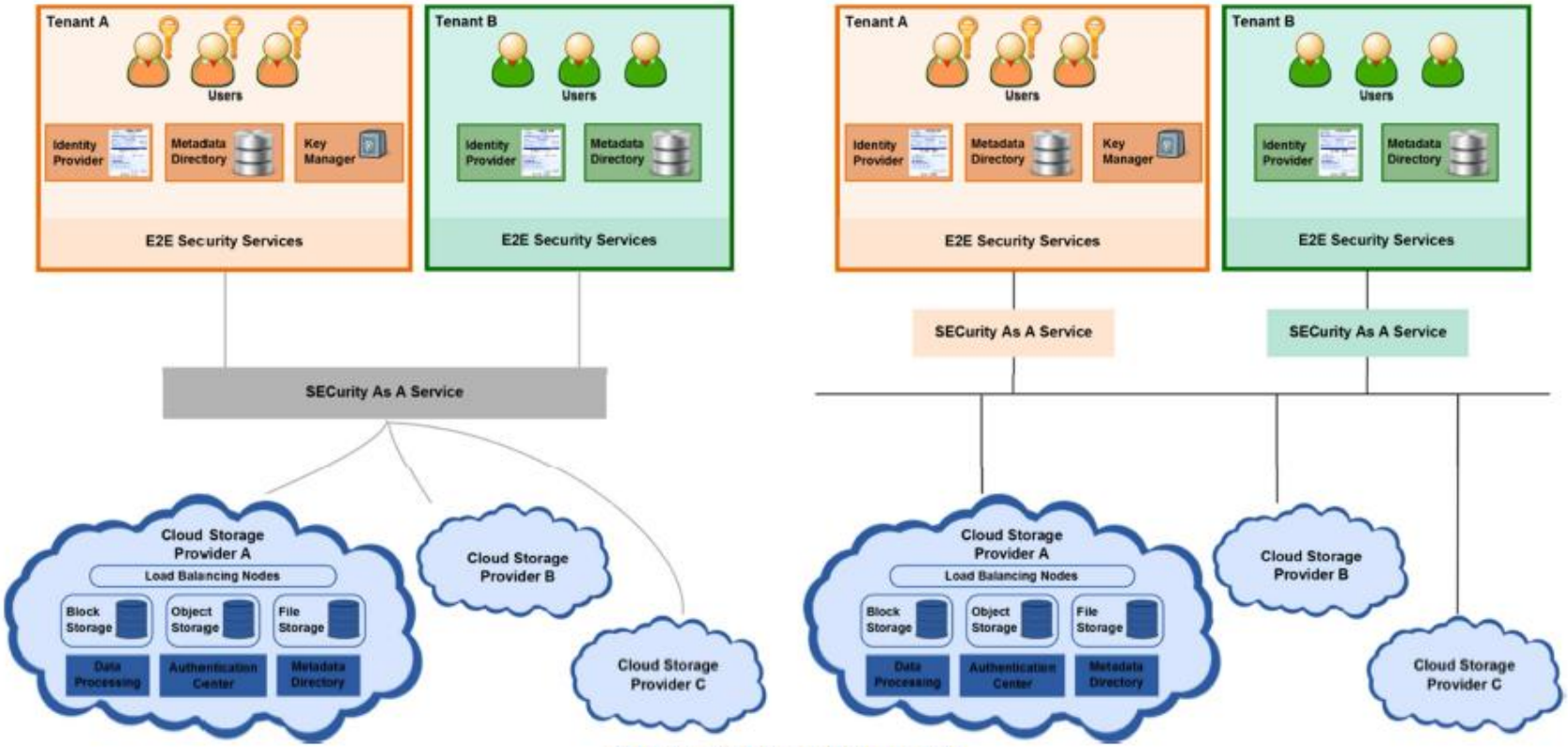


Figure 4 Hybrid Security

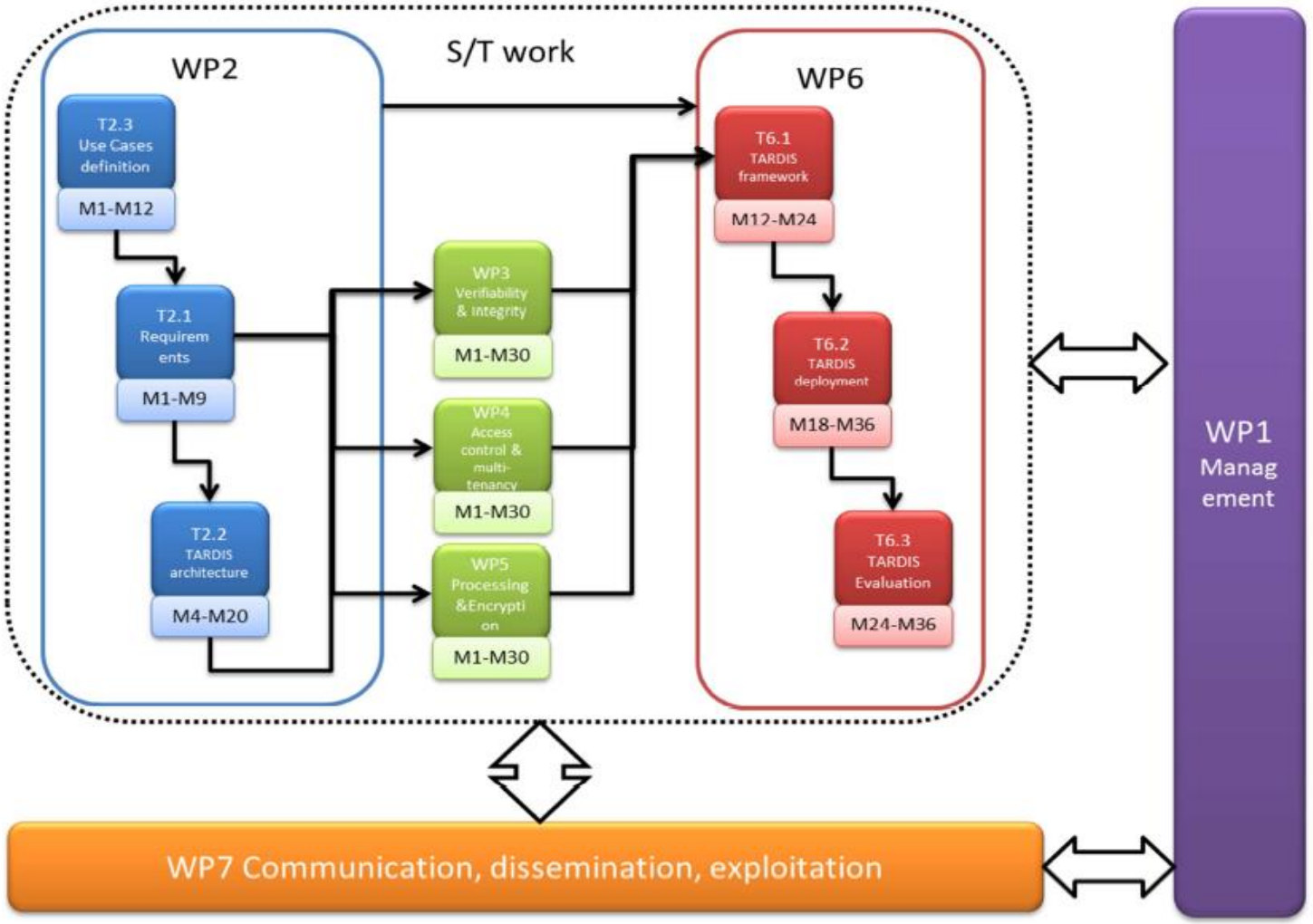
tredisec

TREDISEC Use cases

Partner	Cloud technology	Use Case	TREDISEC Challenge
GRNET	~Okeanos Pithos+	UC 1: Enhance Storage Efficiency Securely	Storage efficiency vs Confidentiality
		UC 2: Multi-Tenancy and Access Control	Multi-tenancy vs Access Control Multi-tenancy vs Data-at-rest Security Multi-tenancy vs Secure Deletion
ARSYS	CloudBuilder	UC 3: Secure WebDav service for Confidential Storage	Multi-tenancy vs Access Control Secure Cloud Storage Storage-Efficient Cloud
MORPHO	Outsourced cloud computations on Biometric data	UC 4: Enforcement of Biometric-based Access Control	Efficient and Strong authentication
		UC 5: Secure Upgrade of Biometric Systems	Processing Encrypted Data
SAP	HANA Enterprise Cloud (HEC)	UC 6: Database Migration into a Secure Cloud	Multi-tenancy vs Access Control

tredisec

Project Roadmap



tredisec