SUPER CLOUD

User-centric management of security and dependability in clouds of clouds

MISSION OF SUPERCLOUD:

SUPERCLOUD aims to support user-centric deployments across multi-clouds, enabling the composition of innovative trustworthy services, to uplift Europe's innovation capacity and thus improve its competitiveness. **SUPERCLOUD** will thus build a security management architecture and infrastructure to fulfil the vision of user-centric secure and dependable cloud of clouds.

Motivation:

Despite many benefits in terms of business, distributed cloud computing raises many security and dependability concerns. At stake are an increase in complexity and a lack of interoperability between heterogeneous, often proprietary infrastructure technologies. The SUPERCLOUD project proposes new security and dependability infrastructure management paradigms that are:

- **user-centric,** for self-service clouds-of-clouds where customers define their own protection requirements and avoid provider lock-ins

and

- **self-managed,** for self-protecting clouds-of-clouds that reduce administration complexity through security automation.

Concept:

Our approach will be to define a new distributed architectural plane, the **SUPERCLOUD,** providing an end-to-end interface both between user-centric and provider-centric views of multiple clouds. Its role will be both to provide a distributed resource abstraction and flexible but unified control for management of security and resilience.

Objectives:

Self-Service Security: Implementation of a cloud architecture that gives users the flexibility to define their own protection requirements and instantiate policies accordingly.
Self-Managed Security: Development of an autonomic security management framework that operates seamlessly over compute, storage and network layers, and across provider domains to ensure compliance with security policies.
End-to-End Security: Proposition of trust models and security mechanisms that enable composition of services and trust statements across different administrative provider domains.
Resilience: Implementation of a resource management framework that composes provider-agnostic resources in a robust manner using primitives from diverse cloud providers.

Expected Results:

Design and implementation of a SUPERCLOUD security management infrastructure
This infrastructure features a 360° monitoring famework that captures both horizontal (multi-domain) and vertical (cross-layer) dimensions of multi-cloud systems. Such an autonomic security management infrastructure monitors resource security and guarantees secure computation, storage and communications, also enabling a continuum of security services.
**Design and implementation of a data management framework**
This framework will rely on cryptographic tools that address multiple aspects including key management for access control, data availability and resilience, secure data computation and verifiability. It will also include a resilience framework allowing the implementation of multi-cloud storage systems that can survive provider-scale failures.
Design and implementation of a multi-cloud network management infrastructure
This includes a virtual network abstraction platform that spans multiple heterogeneous clouds and provides resilient Network-as-a-Service to cloud users. It serves as foundation to an autonomic security management framework that provides fine-grained network monitoring and flexible threat management support.

SUPERCLOUD structure and work packages:
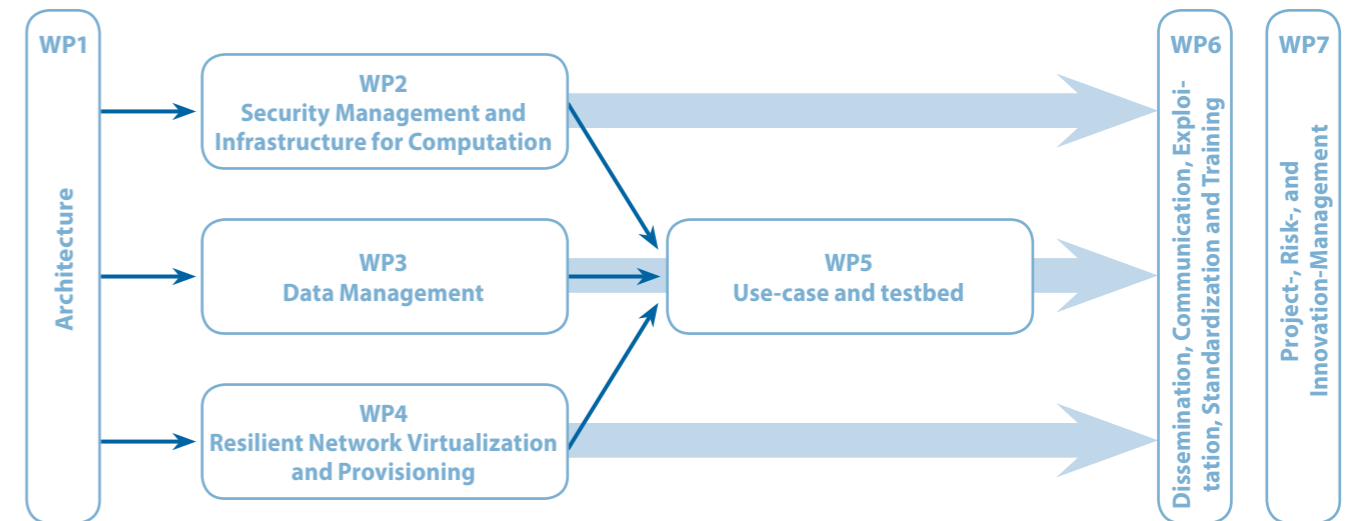
Technical Approach:

The SUPERCLOUD project is planned to run for 36 months. It is organized into seven work packages with significant dependencies and expected synergies between them which are described shortly in the following.

WP1   Architecture
WP1 is the technical backbone of the SUPERCLOUD project as it defines the architecture and framework for the remaining work packages. The focus is put on protocols and services that require interaction between the different building blocks.

WP2   Security Management and Infrastructure for Computation
WP2 specifies and implements the main components and protocols of the federated cloud infrastructure for computing and the design of the corresponding security self-management framework. The developed solutions will be used in WP5 for demonstrations and WP6 for dissemination and exploitation.

WP3   Data Management
WP3 designs and implements SUPERCLOUD protection of user assets in the distributed cloud, focusing on autonomic security provisioning and end-to-end security. This WP provides a common user experience of data protection across multiple underlying clouds through modular and on-demand data security services such as access control, blind computation, integrity and verifiability, and data availability.

WP4   Resilient Network Virtualization and Provisioning
WP4 enables to create virtual networks for multi-clouds with resilience and security guarantees both for the control plane and for the data plane, using the software-defined network-

ing (SDN) approach. SUPERCLOUD also provides 360° network monitoring and forensics to guarantee a sanitized and auditable network environment.

WP5   Use-case and testbed
WP5 enables to demonstrate and validate SUPERCLOUD core technology. A testbed that will enable the reproduction in realistic settings of the two use cases, using component configuration and virtualization, will be set up. The first use case deals with a medical imaging platform and will show the move of the platform towards a secure cloud tesbed platform. The second use case deals with a healthcare laboratory information system (LIS) and will show that the SUPERCLOUD infrastructure allows deploying a healthcare LIS on a self-service distributed cloud.

WP6   Dissemination, Communication, Exploitation, Standardization and Training
WP6 focuses on communication and dissemination of scientific research results achieved within the individual work packages to outside parties as well as to participating entities. Furthermore, this WP will support the partners to exploit the achieved results and impact the European as well as the international market. Moreover, WP6 results will lead to contributions in terms of trainings or standardization.

WP7   Project-, Risk-, and Innovation-Management
Finally, WP7 ensures a successful project lifetime with respect to risk and innovation management. There are dependencies to all other work packages as this work package coordinates the tasks so that they are in line with the project work plan in order to reach the objectives of SUPERCLOUD.
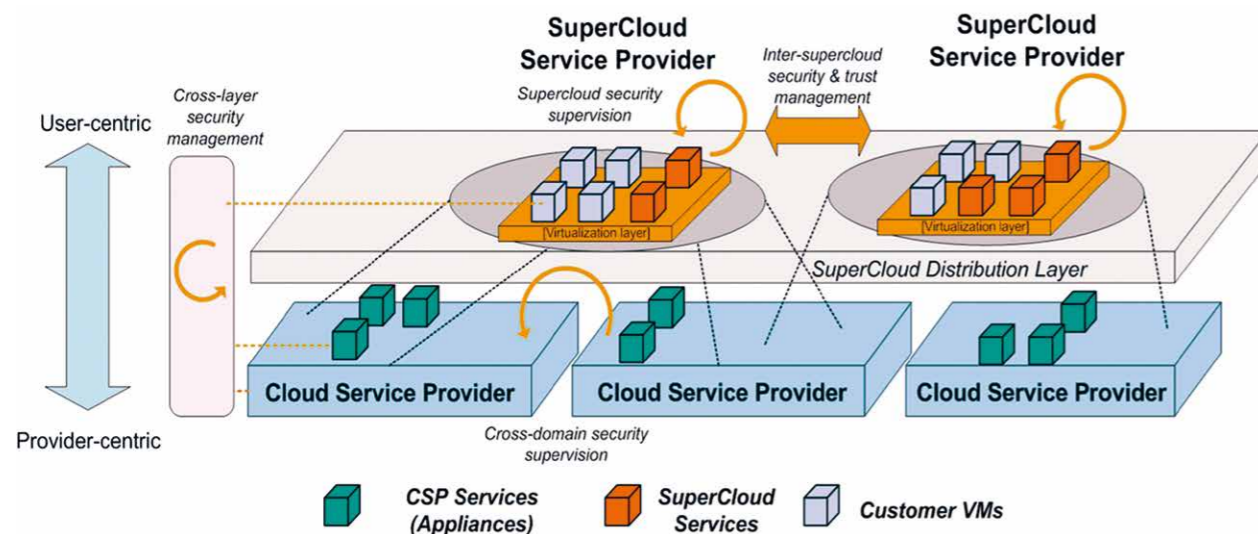
Contact:

Project Coordinator
Dr. Klaus-Michael Koch
Technikon Forschungs- und
Planungsgesellschaft mbH
Burgplatz 3a
9500 Villach
Austria
Tel.:   +43 4242 233 55 – 71
Fax: +43 4242 233 55 – 77
Email: coordination@supercloud-project.eu
Web: www.supercloud-project.eu

Technical Lead
Dr. Marc Lacoste
Orange Labs, Department of Security
38-40 rue du Général Leclerc
92794 Issy-Les-Moulineaux, France
Tel.:   +33 1 45 29 67 24
Email: marc.lacoste@orange.com

Consortium:

The consortium of the SUPERCLOUD project brings together a European team of recognized organizations and respected universities with scientific and technological backgrounds, making it well-positioned to achieve its objectives. All in all there are 9 partners from 6 different European countries including 2 SMEs, 4 industrial companies, 2 universities, and 1 research institution.
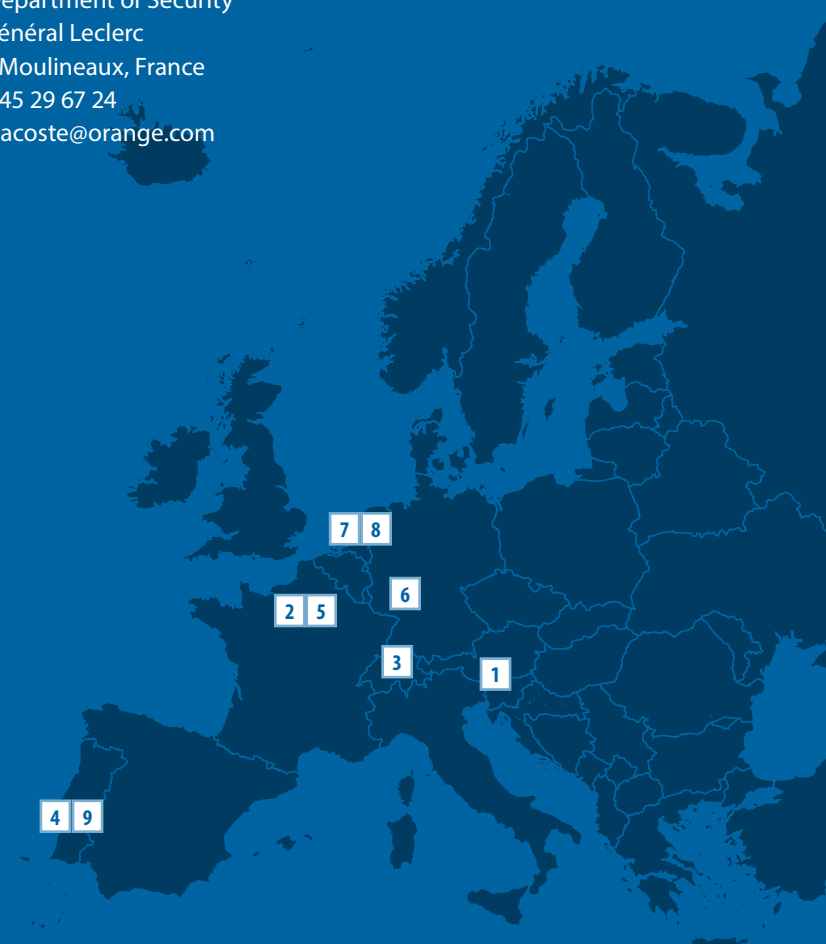
1 **Technikon Forschungs- und Planungsgesellschaft mbH (Austria)**

2 **ORANGE SA (France)**

3 **IBM Research GmbH (Switzerland)**

4 **Fundação da Faculdade de Ciências da Universidade de Lisboa (Portugal)**

5 **Institut Mines-Telecom (France)**

6 **Technische Universität Darmstadt (Germany)**

7 **Philips Medical Systems Nederland (Netherlands)**

8 **Philips Electronics Nederland B.V. (Netherlands)**

9 **MAXDATA Software SA (Portugal)**