This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 312758

seccrit
SEcure Cloud computing for CRitical infrastructure IT

meta data & overall goal

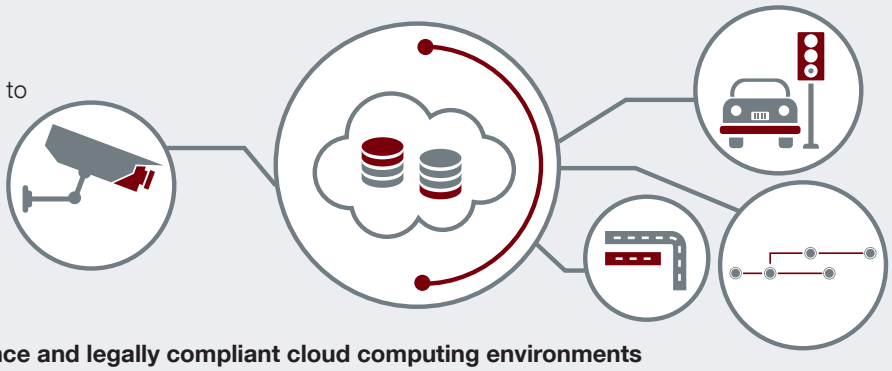
PROJECT META DATA

- 10 Partners from Austria, Finland, Germany, Greece, Spain and the UK.
- Project budget 4.8 Mio. EUR, partly funded by EC FP7 programme
- Project duration 1.1.2013 – 31.12.2015

OVERALL GOAL

- **analyse** and evaluate cloud computing with respect to security risks in critical infrastructures, e.g.:
  - Traffic Control
  - Public Safety (CCTV)
- **develop**
  - methodologies
  - technologies
  - best practices

  for secure & resilient, trustworthy, high assurance and legally compliant cloud computing environments
- **Involve** Stakeholders via a User and Advisory Board to ensure applicability of research outputs to real-world problems



objectives & anticipated output

KEY RESEARCH OBJECTIVES:

- **provide** legal guidance and evidence on data protection
- **understand** and manage risk associated with cloud environments
- **understand** cloud behavior in the face of security and resilience challenges
- **establish** best practices for secure cloud service implementations
- **demonstrate** project output in real-world application scenarios

ANTICIPATED RESEARCH APPLICATIONS:

- **Techno-legal Guidance:** In order to ensure that the technologies developed within the SECCRIT project are in line with fundamental legal requirements, constant techno-legal guidance is necessary. One stand-alone output of this activity is a document which explains how legal fundamentals map to technical problems.
- **Risk Assessment:** A cloud vulnerability catalogue and a novel approach to assess the risk when "cloudifying" CI IT services have been developed is available via seccrit.eu. In addition to this practical tool support has been created by developing a plugin for the risk assessment tool verinice.
- **Policy Specification, Decision and Enforcement:** These artefacts will be add-ons to existing cloud infrastructures based on cloud-specific extension of the generic policy decision and enforcement framework IND²UCE (Integrated Distributed Data Usage Control Enforcement). It will allow to introduce security policies beyond anything current infrastructures are capable of.
- **Resilience Framework including Anomaly Detection in the Cloud:** A resilience framework is being developed to be integrated in any cloud infrastructure. A fundamental part of this is the detection of anomalous network behaviour in the virtual environment (due to e.g. DDoS cyber-attacks). The framework offers dynamic reconfiguration of the network and cloud infrastructure as mitigation against such cyber-attacks.
- **Tools for Audit Trails and Root Cause Analysis:** These tools support forensic analysis of faults and include mechanisms for monitoring data being stored in a trusted third party storage system, supporting all or nothing encryption, this can be logged to provide evidence for later root cause analysis. Moreover, an independent Trust Enhancement Framework was developed that provides additional detailed information for tenants about the hosted virtual resources.
- **Cloud Assurance Profile:** An assurance approach and supporting tools are being developed to provide guarantees of specific security properties at various levels and layers aggregated for the high level virtual service. This approach allows to abstract over monitoring details and categorise virtual services in assurance levels.
- **Model Driven Security Guidelines:** A database will be developed to map best practice security guidelines focusing on SECCRIT outputs and established standards to identified risks. This will be supported by a modelling approach for mapping security issues in the given domain to solutions as proposed above.

www.seccrit.eu
info@seccrit.eu

AIT Austrian Institute of Technology · Ajuntament de Valencia · Amaris · etra I+D · Fraunhofer IESE · KIT Karlsruhe Institute of Technology · Lancaster University · Mirasys · NEC · OTE