"Cloud computing offers a new frontier in computation and storage that can meet the needs of organisations. Despite this potential, trust is essential to wider uptake of cloud services but it can only come from solid mechanisms that ensure greater control over the security of this multi tenant infrastructure and the privacy and confidentiality of data."

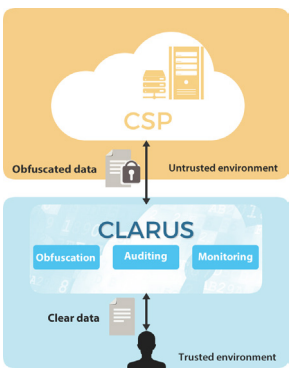
ENABLING PRIVACY AND SECURITY FOR DATA OUTSOURCED TO THE CLOUD

A holistic security-by-design approach that views security, privacy and confidentiality of data outsourced to the cloud, as system properties that must be continuously managed during the whole lifetime cycle.

Clarus

A framework for user centred privacy and security in the cloud

CLARUS pillars to pave the way towards more transparent, standardised, auditable and controllable cloud services are:



- A secure proxy based solution for the storage and processing of data outsourced to honest-but-curious cloud service providers (CSP).
- New technological privacy-preserving mechanisms to obfuscate data outsourced to the cloud.
- Monitoring and audit services to give users control over outsourced data.
- An interoperability-by-design approach.
- A comprehensive analysis of the EU legal framework for the protection of sensitive data.

INTEROPERABILITY-BY-DESIGN TO OVERCOME MISTRUST IN CLOUD COMPUTING BY IMPLEMENTING STANDARDISED CLOUD SERVICES

CLARUS case studies lead to a set of data storage/retrieval/management functions for data protected via data encryption, data splitting or data anonymisation, and will implement a set of standardised communication interfaces and protocols:

- Between the end user and the CLARUS proxy.
- Among different CLARUS instances running at different organisations.
- Between the CLARUS proxy and the cloud service providers.

www.clarussecure.eu | contact@clarussecure.eu | @CLARUSecure

A DISRUPTIVE TECHNOLOGY FOR THE MARKET

Clarus
A framework for user centred privacy and security in the cloud

Cloud Service Providers will gain the trust and confidence of customers by offering user and privacy-friendly services leveraging CLARUS.

Citizens will no longer need to be wary of their sensitive data being leaked when such data are stored and managed by CLARUS-enabled clouds.

The sensitive nature of health data makes cloud solutions problematic. With the CLARUS solution in place, the health sector will gain from more transparent standardised auditable and controllable cloud services. CLARUS will offer security and privacy-enabling mechanisms to ensure that patient records are properly protected before outsourcing to the cloud service provider. CLARUS will make the cloud a viable alternative for the healthcare sector.

Geo-reference data applications encompass mission-critical data for public safety and security (natural hazards prevention) and also environmental data and associated services can have a business value when very specific exploitation needs are fulfilled (for insurance companies, construction and public work sectors...). A CLARUS-enabled platform might mitigate security and privacy threats by strengthening the trust in the domain.

CLARUS innovative solutions will help to reinforce trust and security in digital services for handling personal data addressing action 12 of the Digital Single Market strategy of the European Commission.

"CLARUS will allow users to retain the best of the cloud (plenty of storage and computational power) while avoiding the worst (having to surrender their sensitive information to the cloud).... By agreeing to offer the CLARUS solution, cloud service providers will be able to enter a new important market, the one of customers (e.g. in healthcare, banking, etc.) wishing to store and process sensitive data on the cloud."

Prof. Dr. Josep Domingo-Ferrer
Distinguished Professor, IEEE Fellow, Academia Europaea
Coordinator of H2020 CLARUS project

CLARUS has received funding from the European Union's Horizon 2020 programme - DG CONNECT Software & Services, Cloud. Contract No. 644024