DPSP CLUSTER

Data Protection, Security and Privacy in cloud.

Erkuden Rios, Tecnalia

Net Futures 2016, 21st April 2016

Strong community of experts

25 projects (€78M): 16 in H2020 (€56M), 6 in FP7 (€17M), 2 in CIP (€5M).

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

PaaSword

MUSA

SWITCH

witdom

SERECA

prisma cloud

tredisec

ESCUDO CLOUD

SUNFISH

O{P}ERANDO
online privacy enforcement, rights assurance & optimization

CREDENTIAL

SecureCloud

slalom

SLA - Ready
Making Cloud SLAs readily usable in the EU private sector

CloudWatchHUB

AppHub
The European Open Source Market Place

SecCord

coco cloud

SPECS

TRESCCA

CLOUD ACCOUNTABILITY PROJECT

CLIPS
Cloud Approach for Innovation in Public Services

strategiC

Results so far

- Whitepaper on Future Challenges towards DSM.
- Map of synergies of the projects.
- 1st joint Workshop in Feb 2016, Naples.
- Project fiches & presentations.
- Participation at CloudForward 2015, Net Futures 2016 (booth).
- Website, logo, collaborative area.

https://eucloudclusters.wordpress.com/data-protection-security-and-privacy-in-the-cloud/

Map of synergies

- Map of synergies between the clustered projects
- Released in Dec 2015.
- 11 projects participated.
- Catalogue of projects’ main challenges and approach.
- **R&I topics map**, including examples of contributions.
- **Innovation map**: main outcomes (products/prototypes), intended release dates, license, and links.
- **Map of technologies used** (cloud and security).
- **Map of standards used and contributed to** (cloud and security).

Innovation map

(example)

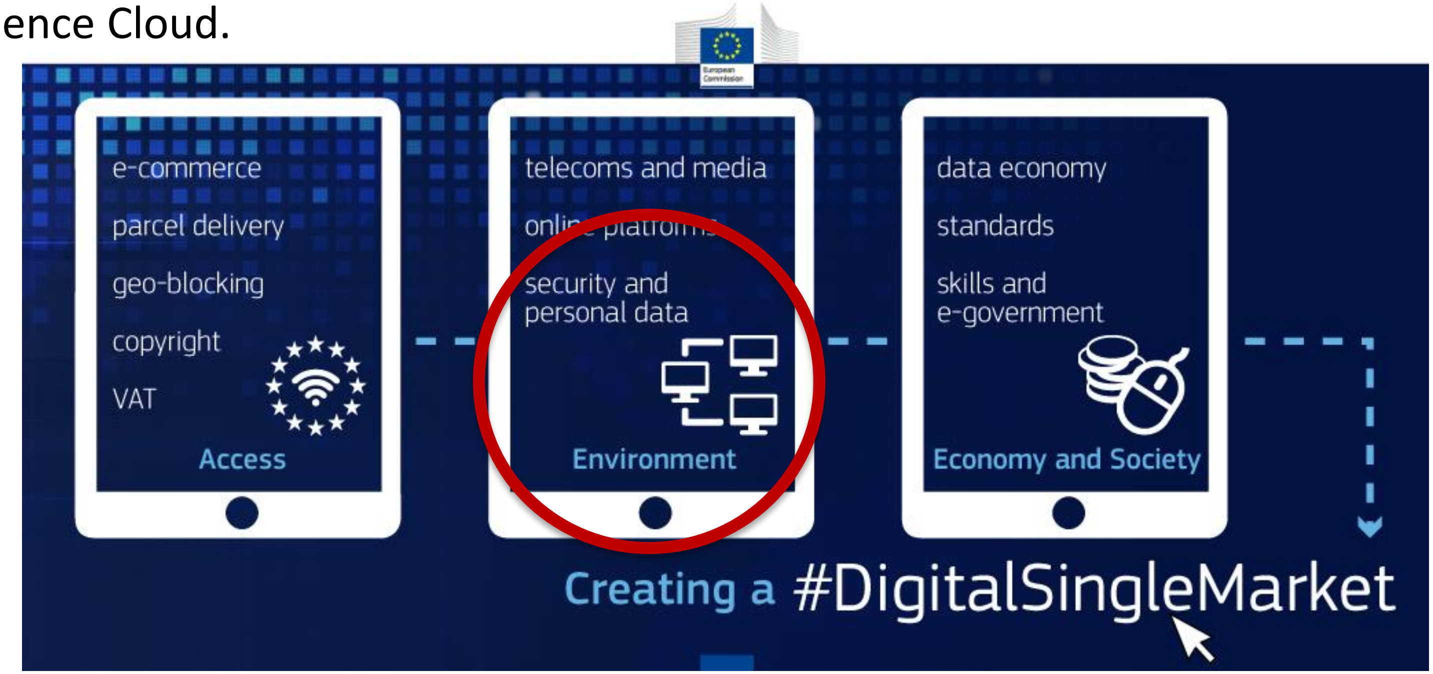
TOOL/SERVICE NAME	BRIEF INFO	OPEN SOURCE (Y/N)	SUPPPORTED LICENSES (if open source)	COMMUNITY	PATENT	INTENDED MARKET	DATE OF RELEASE	LINK (URL)
PROJECT: SPECS								
SPECS SLA Platform	The SPECS SLA Platform is composed of a set of web applications that, run on top of an existing Platform-as-a-Service, enable the management of cloud services according to Security SLA life cycle	Y	Apache			Cloud Service Providers, Cloud Service brokers	Available	bitbucket.org/specs-team
SPECS SLA Negotiation	The SPECS SLA negotiation module is composed of a set of web applications that, run on top of SPECS SLA Platform, enable the negotiation of Security SLA	Y	Apache			Cloud Service Providers, Cloud Service brokers	Available	bitbucket.org/specs-team

Whitepaper on Future Challenges

- Challenges for trustworthy (multi-)Cloud-based services in the Digital Single Market
- Released in Jan 2016.
- Challenges towards DSM initiative #14 Free Flow of Data.
- A total of 16 projects (21 authors) contributed.
- 47 challenges identified, 35 challenges for 2018-2020.

Future challenges for DSM #14

- Free movement of data
- Location of data
- Ownership
- Interoperability
- Usability
- Access to (Public) Data
- Certification
- Contracts
- Switch of CSPs
- Research Open Science Cloud.



Whitepaper on Future Challenges (cont.)

- Challenges description format:

Short name: Summary of challenge description.
Description: Challenge short description.
Timeframe: 2016-2017/2018-2020/beyond
Project works on it: Yes/No
Topics of the DSM Initiative #14: Free movement of data / Location of data/ Ownership/Interoperability/Usability/ Access to Data/Access to Public Data/Certification/Contracts/Switch of CSPs/Research Open Science Cloud.
Importance to DSM Initiative #14: high/medium/low.
Risk of not filling the gap: Short description of major risk(s) faced if the challenge is not addressed in the future.

Challenges 2018-2020 (1/3)

DATA PROTECTION & PRIVACY

- **Full control of data flow** including data in transit, data in use, but also data at rest, meaning controlled access and usage of data across country and cloud boundaries. Context based access control policies are part of this challenge.
- **Efficient searchable encryption** for enabling to efficiently search and edit the encrypted data stored and processed in the cloud.
- Privacy **preserving cloud-based (identity) services:** Improved and novel cryptographic methods to securely protect, store and share (private) data, including encrypted identity data.
- **Fully secure APIs** that enable to securely communicate the identity and user attributes (authentication and authorization) among cloud services.
- **Data Protection legal framework transparency.**

Challenges 2018-2020 (3/2)

SECURITY

- **Definition and enactment of fine-grained security policies:** integration and composition of security and privacy policies across different cloud services.
- **Security-aware SLA management support** for security and privacy terms formalisation, negotiation, composition, monitoring, continuous assurance and automation. All these applied to multi-cloud or federated cloud-based applications and cloud-services themselves.
- **Risk assessment frameworks for applications at scale:** innovative frameworks to assess risk in multi-technology and distributed applications mixing cloud, IoT, Big Data, Mobile,…
- **Secure dynamic composition of cloud services, including dynamic benchmarking and brokering** of Cloud services for multi-cloud scenarios as well as federation of clouds.
- **Cloud Security Certification:** cloud security standards and auditing.

Challenges 2018-2020 (3/3)

SECURITY & PRIVACY

- **Security- and privacy-by-design in cloud services.**
- **Continuous control of security and privacy conditions and obligations and adherence to them**, including continuous monitoring, assurance, enforcement, and automated reaction in inter-clouds, multi-cloud, federated clouds.
- **Efficient secure and privacy-preserving multi-tenancy** in Infrastructure, Platform and Software as a Service models.
- **Improve market readiness of security and privacy solutions from projects.**

First Workshop

23rd of Feb 2016

in Naples.

- 98 registered attendees: 60 companies , 11 RTOs, 27 Universities.
- 5 organising projects (SPECS, COCO-CLOUD, MUSA, SERECA and CLIPS), others participating (SLALOM, CLARUS, PRISMACLOUD, CREDENTIAL, CLOUDWATCH2,…).
- Project presentations & demos.
- Cluster members panel & Industrial panel discussions.

Technical groups (proposal 1)

- According to challenges identified towards **DSM Free flow of data**:

  WG1: Security and privacy-by-design
  - Security and privacy-by-design
  - Security and privacy Requirements modelling
  - Fine-grained policy definitions
  - Risk assessment frameworks (scalability, multi-technology)

  WG2: Trust & Interoperability
  - Data protection legal framework transparency
  - Security & privacy aware cloud SLA management.
  - Cloud security certification
  - Continuous control and assurance
  - Secure dynamic composition (brokering, CSP benchmarking)
  - Interoperability mechanisms

  WG3: Advanced data protection mechanisms
  - Full control of data flow (including cross-border).
  - Efficient (searchable) encryption and key management.
  - Secure and privacy-preserving multi-tenancy.
  - Fully secure APIs.

Planned results 2016

- Launch the technical Working Groups for focused discussions.
- Whitepaper on technological options for the future *European Commission Legislative Proposal on Free Flow of Data* (due in Nov 2016).

  Whitepaper ready for Mid July 2016.
- Organisation of the 2nd Joint Workshop:

  Currently evaluating the opportunity to be at Cloud Forward 2016 (11th-13th Oct 2016, Madrid).

Contact

Erkuden Rios tecnalia Inspiring Business

ICT – European Software Institute Division

erkuden.rios@tecnalia.com

Francisco Medeiros, DG-CNET

Key Research Areas & Challenges

DSM Initiative #14 topics	Challenges (as in Section 5)
Free movement of data	CLARUS Ch1, CLARUS Ch2, CLARUS Ch3, CLARUS Ch4, COCO CLOUD Ch1, COCO CLOUD Ch2, MUSA Ch1, MUSA Ch4, MUSA Ch5, PAASWORD Ch1, PAASWORD Ch3, PRISMACLOUD Ch2, SLA-READY Ch1, SLA-READY Ch2, SPECS Ch1, SPECS Ch2, SPECS Ch3, STRATEGIC Ch1, STRATEGIC Ch2, SUNFISH Ch1, SWITCH Ch1, SWITCH Ch2, TREDISEC Ch3.
Location of data	CLARUS Ch2, CLARUS Ch3, PAASWORD Ch3, SLA-READY Ch2, SUNFISH Ch2, SUNFISH Ch3.
Ownership	CLARUS Ch2, CLARUS Ch3, ESCUDO-CLOUD Ch1, PAASWORD Ch3, SLA-READY Ch2, SUNFISH Ch3, WITDOM Ch2.
Interoperability (security interoperability)	CLARUS Ch4, CREDENTIAL Ch2, CREDENTIAL Ch3, ESCUDO-CLOUD Ch3, MUSA Ch1, MUSA Ch4, MUSA Ch5, PAASWORD Ch1, PRISMACLOUD Ch3, PRISMACLOUD Ch4, PRISMACLOUD Ch5, STRATEGIC Ch1, STRATEGIC Ch2, SUNFISH Ch2, WITDOM Ch1.
Usability (usability of security)	AppHub Ch1, CLOUDWATCH2 Ch3, PRISMACLOUD Ch1, SLA-READY Ch1.
Access to data	CLARUS Ch1, CLARUS Ch6, CREDENTIAL Ch1, CREDENTIAL Ch2, CREDENTIAL Ch3, ESCUDO-CLOUD Ch3, PAASWORD Ch2, PRISMACLOUD Ch2, PRISMACLOUD Ch3, STRATEGIC Ch1, STRATEGIC Ch2, SUNFISH Ch1, SUNFISH Ch2, SUNFISH Ch3, TREDISEC Ch2, TREDISEC Ch3, WITDOM Ch1.
Access to public data	AppHub Ch1, STRATEGIC Ch1, STRATEGIC Ch2 SUNFISH Ch1.
Certification	CLOUDWATCH2 Ch2, MUSA Ch2, MUSA Ch3, PRISMACLOUD Ch5 (Standards).
Contracts	CLARUS Ch3, CLOUDWATCH2 Ch3, MUSA Ch5, SLA-READY Ch1, SPECS Ch1, SPECS Ch2, SPECS Ch3, SUNFISH Ch3, SWITCH Ch1, SWITCH Ch2.
Switch of CSPs	CLARUS Ch4, MUSA Ch2, MUSA Ch3, MUSA Ch4, MUSA Ch5, SWITCH Ch1, SWITCH Ch2, WITDOM Ch1.
Research open science cloud	AppHub Ch1, CLOUDWATCH2 Ch1.

Key Research Areas & Challenges

Other topics	Challenges (as in Section 5)
Improve market readiness of EU projects’ results	CloudWatch2 Ch1.
Respect of customer rights	SPECS Ch1, SPECS Ch3.
Leverage of efficiency vs. security	TREDISEC Ch1

Challenges w.r.t. Initiative #14 topics

Project	Challenge	DSM Initiative #14
APPHUB	Improve market readiness of security and privacy solutions	Usability (usability of security), Access to public data, Research open science cloud (first step to this).
CLARUS	Making the cloud ecosystem secure for outsourced data	Free movement of data, Access to data.
	Privacy-enabling mechanisms to protect sensitive data	Free movement of data, Ownership, Location of data.
	Data protection and legal jurisdiction	Free movement of data, Location of data, Ownership, Contracts.
	Interoperability-by-design to overcome mistrust in cloud computing by implementing standardized cloud services	Switch of CSPs, Free movement of data, Interoperability (security interoperability).
	Data anonymisation and access to data	Access to data.
CLOUD WATCH2	Cloud Security Certification & Definition of Risk profiles	Certification.
	Data Protection legal framework transparency	Usability (usability of security), Contracts.
COCO CLOUD	Data flow control	Free movement of data.
	Control of privacy conditions and obligations and adherence to them	Free movement of data.
CREDENTIAL	Design novel privacy preserving cloud-based (identity) services	Access to data.
	Adapt and improve cryptographic methods to securely store and share identity data	Access to data, Interoperability (security interoperability).
	Protect access to identity data with strong authentication mechanisms	Access to data, Interoperability (security interoperability).

Challenges w.r.t. Initiative #14 topics

Project	Challenge	DSM Initiative #14
ESCUDO-CLOUD	Secure and private information sharing in the cloud	Access to data.
MUSA	Risk assessment frameworks for applications at scale	Interoperability (security interoperability), Free movement of data.
	Continuous Assurance of CSP performance	Certification, Switch of CSPs.
	Standard certificates of CSP, including security features	Certification, Switch of CSPs.
	Dynamic benchmarking and brokering of Cloud offers	Switch of CSPs, Interoperability (security interoperability), Free movement of data.
	Composition of evolving security-aware SLAs	Contracts, Switch of CSPs, Interoperability (security interoperability), Free movement of data.
PAASWORD	Fully secure APIs	Free Movement of Data, Interoperability (security interoperability).
	Access Control Policies based on context attributes	Access to data.
	Searchable Encryption	Free movement of data, Ownership, Location of data.
PRISMACLOUD	Security and privacy by design in cloud services	Usability (usability of security).
	Authenticity and verifiability of data and infrastructure use	Free movement of data, Access to data.
	Development of a methodology for secure service composition	Interoperability (security interoperability).

Challenges w.r.t. Initiative #14 topics

Project	Challenge	DSM Initiative #14
SLA-READY	Simpler contractual terminology and commonly used taxonomy	Free movement of data, Usability (security usability), Contracts.
SPECS	Security SLA Automatic Implementation	Free movement of data, Contracts.
	Security SLA Monitoring	Free movement of data, Contracts, Respect of customer rights.
STRATEGIC	Secure interoperable authentication in cross-border scenarios	Free movement of data, Access to data (data federation), Access to public data, Interoperability (security interoperability).
	Definition and enactment of fine-grained security policies	Free movement of data, Access to data (data federation), Access to public data, Interoperability (security interoperability).
SUNFISH	Security policy management and enforcement in heterogeneous cloud federations	Access to data, Interoperability (security interoperability), Location of data.
	Continuous monitoring and security assurance of inter-cloud communication	Access to data, Contracts, Ownership, Location of data.
SWITCH	Security and privacy terms in SLA Negotiation	Free movement of data, Switch of CSPs, Contracts.
	SLA transmission security	Free movement of data, Switch of CSPs, Contracts.
TREDISEC	Deduplication on encrypted multi-tenant data	N/A.
	Mechanisms to check the integrity and availability of multi-tenant data in presence of storage efficiency	Access to data.
	Privacy-preserving analytics/processing over confidential and efficient outsourced databases.	Free movement of data, Access to data.