REALIZATION OF A RESEARCH AND DEVELOPMENT PROJECT (PRE-COMMERCIAL PROCUREMENT) ON "CLOUD FOR EUROPE"

TECHNICAL SPECIFICATION: CHALLENGES AND GENERAL REQUIREMENTS

ANNEX IV (A)
TO THE CONTRACT NOTICE

TENDER NUMBER <5843932>
CUP <C58I13000210006>

CLOUD FOR EUROPE

FP7-610650

This project has received funding from the European Union's
Seventh Framework Programme for research, technological development
and demonstration under grant agreement no 610650.

EXECUTIVE SUMMARY

Note: This is an informative summary of the document. The actual specification relevant for the bids is in the remainder of the document.

Cloud for Europe is tendering research to assist take-up of cloud computing in the public sector. Such research is deemed necessary in order to bridge gaps and barriers existing with current technology. To describe these barriers addressed by Cloud for Europe we introduce "challenges" as:

> *A **challenge** is a high-level business requirement not yet fulfilled by available Cloud technology.*

This document discusses the challenges that economic operators shall address in their bids. Those challenges are assigned to a public authority's service provision lifecycle consisting of three consecutive phases: a procurement phase, a delivery phase, and an operations phase. Note that this are lifecycle phases which have no relation to the three PCP phases.

Cloud for Europe procures lots. Lots have been selected so that challenges identified are well covered.

> *A **lot** is comprised of at least one challenge.*

Three such lots have been defined. These lots are described in separate specification documents Annex IV(b), Annex IV(c) and Annex IV(d). The three lots are:

- Federated Certified Service Brokerage (FCSB)
- Secure, Legislation-Aware Storage (SLAS)
- Legislation Execution (LE)

Each lot is addressing a set of challenges which result in "lot-specific requirements" and "functional requirements" to be addressed by the bids. These requirements are described in the lot descriptions Annex IV(b) to Annex IV(d).

In addition, a set of common requirements to be addressed by each of the lots is given. These common requirements are described in this document as "General Requirements".

> *Each bid needs to address the common requirements that are defined in this document, as well as the lot-specific requirements and functional requirements.*

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 CHALLENGES AND USAGE SCENARIO

1.1 CHALLENGE COMPOSITION

The challenges Cloud for Europe addresses take a typical public sector service provisioning lifecycle into account. This consists of a service design phase that contains the service procurement. The transition phase delivers the services. Finally, the service is set into operation. This includes service administration, continuous security measures, and monitoring of the service. The operation may also contain a change of provider (e.g. re-procurement upon expiration of the service contract). This lifecycle is illustrated in figure 1 below. The lifecycle phases have no relation to the three PCP phases.

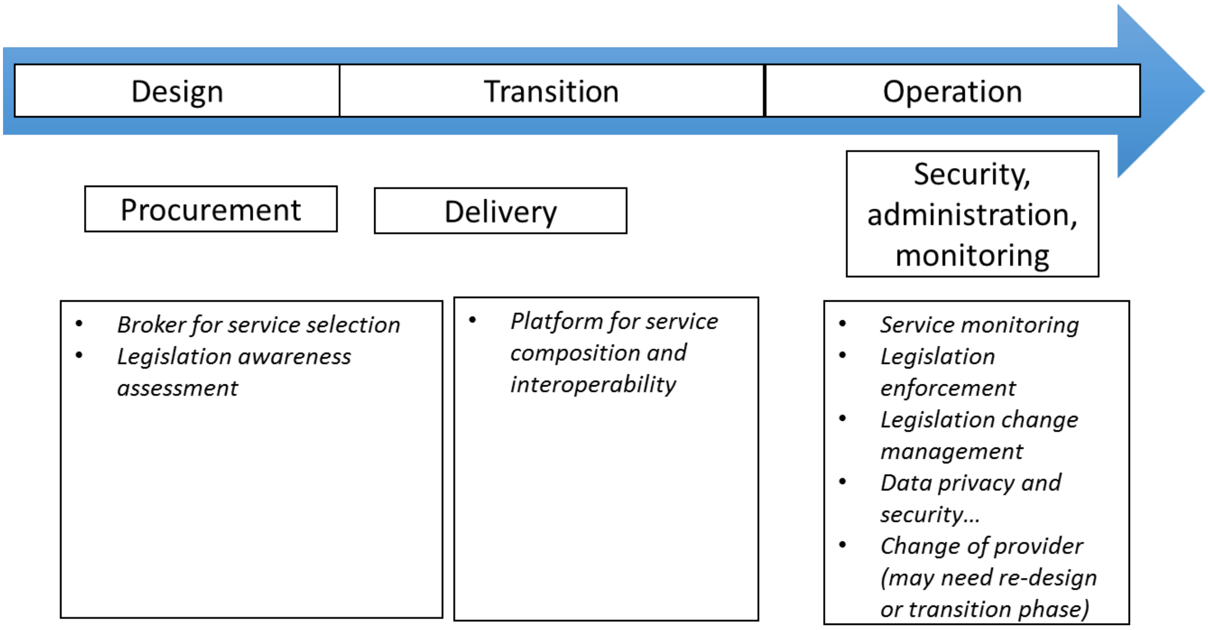
Design
Transition
Operation
Procurement
Delivery
Security, administration, monitoring
• Broker for service selection
• Legislation awareness assessment
• Platform for service composition and interoperability
• Service monitoring
• Legislation enforcement
• Legislation change management
• Data privacy and security…
• Change of provider (may need re-design or transition phase)

Figure 1 – Service provision lifecycle in a heterogeneous legislation environment

Apart from the three lifecycle phases, the figure also illustrates a few challenges that relate to them. The challenges that get addressed by the Cloud for Europe tender are discussed in the next sub-section.

1.2 CHALLENGES OVERVIEW

The challenges that Cloud for Europe feels that – by addressing these trough pre-commercial procurement – will support Cloud adoption by the public sector, are listed in the following Table 1. The table also links the challenges to the three lots Federated Certified Service Brokerage (FCSB, Annex IV(b)), Secure, Legislation-Aware Storage (SLAS, Annex IV(c)), and Legislation Execution (LE, Annex IV(d)), as well as to the applicable award criteria.

Bidders shall address these challenges by innovative technical solutions. The challenges are phrased as to define *"what"* the problem is, not as to *"how"* to actually address it. This allows bidders to be innovative in the research tasks and not to narrow the possible solutions.

Table 1 – Cloud for Europe Challenges and its relation to Lots

Phase	No.	Challenge Summary	Lot	Award Criteria
Design, Procurement	1	Interoperability for cross-border federated cloud service selection and competition	1: FCSB	Q1, I2, I3
	2	Matching customer requirements with cloud service specification	1: FCSB	I2, I3
	3	Assessing the legislation compliance of a cloud storage service to its contractual and functional description	2: SLAS	S1, S2
Transition, Delivery	4	Defining means of assuring service compliance with legislation of EU countries	1: FCSB	I2, I3
	5	Digital archiving and preservation of data	2: SLAS	S1, S2, S4
Operation, Security, Administration, Monitoring	6	Legislation-aware data provision and access	2: SLAS	I2, I3
	7	Overcome, or address legal barriers to cloud computing	3: LE	I2, C2, Q1, Q4, Q6, Q8
	8	Enable the cloud development community to create and maintain legislation execution	3: LE	Q1, Q4, Q6, Q8
	9	Legislation awareness, dynamic management, and propagation	1: FCSB	S1, S2

	10	Cloud service SLA assessment and monitoring	1: FCSB	S4
	11	Seamless change of service provider	1,2,3 (all)	Q1, I2, I3

1.3 CHALLENGE DESCRIPTIONS

Each of the challenges sketched in Table 1 above is described in the sub-sections below. The bidders are expected to explain how the challenges specific to the lot will be addressed.

1.3.1 *CROSS-BORDER INTEROPERABILITY*

Challenge Number:	1
Challenge Title:	Interoperability for cross-border federated cloud service selection and competition
Applies to Lot:	1 – Federated Certified Service Brokerage

The key aspect of this research challenge is the distributed manner of federated cloud service governance and smart allocation of responsibilities within such a federated ecosystem to balance the local authority preservation with the inter-connectivity and interoperability requirement which is essential for better cost-effectiveness, particularly:

- Design concepts and implement methods for service metadata registry governance in such a distributed ecosystem, supporting intelligent service discovery, context-aware service management and fluid service integration.
- Assure data portability, which significance gets emphasized in this federated ecosystem of services. The service and information co-location is not guaranteed and this needs to be addressed via development of a standardized information bus allowing secure and distributed information availability.
- Develop models and methods to guarantee proper identity propagation with service-specific granularity level of information (e.g.: identity metadata, authorization policies, etc.).

1.3.2 *MATCHING CUSTOMER REQUIREMENTS*

Challenge Number:	2
Challenge Title:	Matching customer requirements with cloud service specification
Applies to Lot:	1 – Federated Certified Service Brokerage

Public Administration (PA) customers in any EU country should be provided with a guarantee of security, legislation awareness and other non-functional requirements when using any cross-border service within heterogeneous environment of the Federated EU Public Administration Cloud. Therefore, matching customer functional and non-functional requirements in such heterogeneous federated ecosystem represents a research challenge (related to challenge 1 in section 1.3.1):

- Automated service discovery based on service metadata registry in all EU countries describing functional and non-functional attributes of all services certified for PA use.
- Automated assessment of possibility to meet customer requirements by services aggregation even if services are provided in different countries.
- Automated assessment of customer requirements matching level of pre-selected services in case none of them fully meets the requirements in order to provide data for human assisted decision/SLA negotiation.

1.3.3 *LEGISLATION COMPLIANCE OF A CLOUD STORAGE SERVICE*

Challenge Number:	3
Challenge Title:	Assessing the legislation compliance of a cloud storage service to its contractual and functional description
Applies to Lot:	2 – Secure Legislation-Aware Storage

A service is legislation-aware, if the processes forming the service are constrained by legal requirements. A legislation-aware cloud storage service would need all the processes to run in such legally constrained environment.

Processes like accessing (create, read, update, delete) or querying data objects, migrating, replicating, encrypting or backing-up should first check the legal requirements and adjust the behaviour to these constraints. The following key aspects need to be considered:

- Public administrations need to assess the compliance of cloud storage services to applicable laws and regulations, regarding, for example but not limited to, data privacy, data protection, data security, data location.
- Cloud Service Providers need to assess their storage services with respect to legislation frameworks of different countries and/or specific application domains (health records, justice …).
- Solution for easy and low-cost assessment of the adequacy and compliance of a given cloud storage service to a given target legislation framework

1.3.4 *DEFINING MEANS OF ASSURING SERVICE COMPLIANCE WITH LEGISLATION OF EU COUNTRIES*

Challenge Number:	4
Challenge Title:	Defining means of assuring service compliance with legislation of EU countries
Applies to Lot:	1 – Federated Certified Service Brokerage

The legislation and regulation is the main communication protocol for conveying the critical information through the hierarchy of organizational units within public administrations. The research theme overarching the challenges to bring this solely human to human communication to a computer understandable form.

1.3.5 *DIGITAL ARCHIVING AND PRESERVATION*

Challenge Number:	5
Challenge Title:	Digital archiving and preservation of data
Applies to Lot:	2 – Secure Legislation-Aware Storage

Digital archiving and preservation are both terms that refer to saving data for longer periods of time. Preservation in contrast to archiving also takes into account the fragility of digital media and the rate at which computer hardware and software become obsolete.

Public Administrations are required to archive and preserve their data for long periods of time and additionally comply with the corresponding data protection laws, regarding longterm encryption and strong authentication. Therefore, solutions have to tackle the problems of data archiving, data preservation, compatibility of the corresponding file formats and data protection.

1.3.6 *LEGISLATION-AWARE DATA PROVISION AND ACCESS*

Challenge Number:	6
Challenge Title:	Legislation-aware data provision and access
Applies to Lot:	2 – Secure Legislation-Aware Storage

Handling of data is subject to legal constraints. Public administrations need to manage the rights of the data subjects in a heterogeneous legal environment (European, national, local laws; sectoral or administrative rules). To give some examples, such legal constraints can be

- data access restrictions limiting access to the data controller, data subject and their representatives;
- data access permissions to government entities for special purposes (like access to health data for urgent first aid purposes)

The constraints can be dynamic, like parental or legal guardianship that expires when minors become adult or access restrictions may discontinue or change after a person is deceased.

The challenge is that the cloud environment automatically manages these complex relationships between the actors (data controller, data processor and data subject) in a legislation-aware manner, based on dynamic nature and heterogeneous legal environment.

1.3.7 *ADDRESS LEGAL BARRIERS TO CLOUD COMPUTING*

Challenge Number:	7
Challenge Title:	Overcome, or address legal barriers to cloud computing
Applies to Lot:	3 – Legislation Execution

The legislation brings certain barriers to cloud usage leading to no-go decisions for cloud adoption in the public sector. Eliminating the legal barriers may take considerable time. Another way of dealing with these constraints is to create innovative, technical cloud services that overcome, or address legal barriers by enforcing legislation in an operational cloud environment using technology.

1.3.8 *CREATE AND MAINTAIN LEGISLATION EXECUTION*

Challenge Number:	8
Challenge Title:	Enable the cloud development community to create and maintain legislation execution
Applies to Lot:	3 – Legislation Execution

The challenge is to address and overcome legal barriers to cloud computing in a better way by providing a framework. This framework enables and guides developers to create and maintain Legislation Execution functionality for cloud computing. The aim is to make the creation and maintenance easier, faster, and more professional.

1.3.9 *LEGISLATION-AWARENESS DYNAMIC MANAGEMENT*

Challenge Number:	9
Challenge Title:	Legislation awareness, dynamic management, and propagation
Applies to Lot:	1 – Federated Certified Service Brokerage

Based on the service legislation compliance governance defined in challenge 4 in Section 1.3.4 and because of the distributed nature of the *Federated Certified Service Brokerage*, the challenge is to develop the methods and interfaces for securing legislation compliance and easy legislation change propagation through the cross-bordered and composite services in legislation heterogeneous environment.

1.3.10 *CLOUD SERVICE SLA ASSESSMENT AND MONITORING*

Challenge Number:	10
Challenge Title:	Cloud service SLA assessment and monitoring
Applies to Lot:	1 – Federated Certified Service Brokerage

The core proposition of this challenge is the ability not only to oversee the manifold diverse properties of utilized services in real-time, but also to be able to provide all the critical information for the appropriate reaction when necessary, particularly:

- Define an architecture designed around a framework of components, one for each property to be assessed, that may be combined, extended and reused, all based on a core that generates and manages sets of requests, request streams, monitoring and timings.
- Develop methods for certification with assurance of consistency and elasticity properties in the presence of geo-distributed or geo-replicated cloud provider resources and instances.

1.3.11 *SEAMLESS CHANGE OF SERVICE PROVIDER*

Challenge Number:	11
Challenge Title:	Seamless change of service provider
Applies to Lot:	1, 2, 3 – ALL (FCSB, SLAS, and LE)

Public authorities need to be enabled to seamlessly change the service provider including all services, dependencies and associated data to avoid vendor lock-in and to be able to quickly react in situations like bankruptcy of the cloud provider or any other cases which causes outage of the service. This imposes to adhere to existing and established:

- Standards, standard interfaces, paradigms and
- Certification

1.4 USAGE SCENARIO

This section provides a high-level usage scenario to assist the bidders to get a better understanding of the Cloud for Europe aims.

The identified lots are independent from each other, however they are shaped in a way that they can be combined to bigger systems. Although this is not subject of the process or the project, it may help the bidders to get an overall picture of one of the possible scenarios.

Figure 2 shows one possible interaction of the aimed Cloud for Europe results:

- The public administration ***G$_A$*** wants to provide a personal digital data asset service to its citizens. Therefore the public administration requests from the *Federated Certified Service Brokerage* (FCSB) a storage solution that is compliant with the relevant legal framework. The FCSB returns a selection of storage solutions from across Europe that comply with the legal restrictions. All member states operating a FSCB (illustrated as **G**) can contribute and based on the requested requirements can get selected.

- The public administration selects – based on previously established criteria – a suitable solution and includes it, because it follows certain standards, into their local environment.
- The requesting public administration has the freedom to select different storage solutions for different types of data (e.g. personal data, confidential data…) which require different levels of data protection. Depending upon the level of protection offered, these solutions may differ in price.
- Once all the storage solutions are combined to a personal digital data asset service (PDA), the FCSB monitors, based on the contract, the mediated storage solution for legislative changes and informs the respective parties once changes are detected.
- The access to the personal digital data asset service is controlled by the implementation of the legislation-aware storage, which is aware of the legal provisions it is operated in and only allows access to authorized persons.
- If access is gained by an unauthorized individual, the legislation executing part detects the breach and informs, according to the corresponding legal requirements, individuals and the corresponding public administration.
- Because of the distributed nature of the storage and the complex relationships of many actors, an authorization matrix controls the access rights.

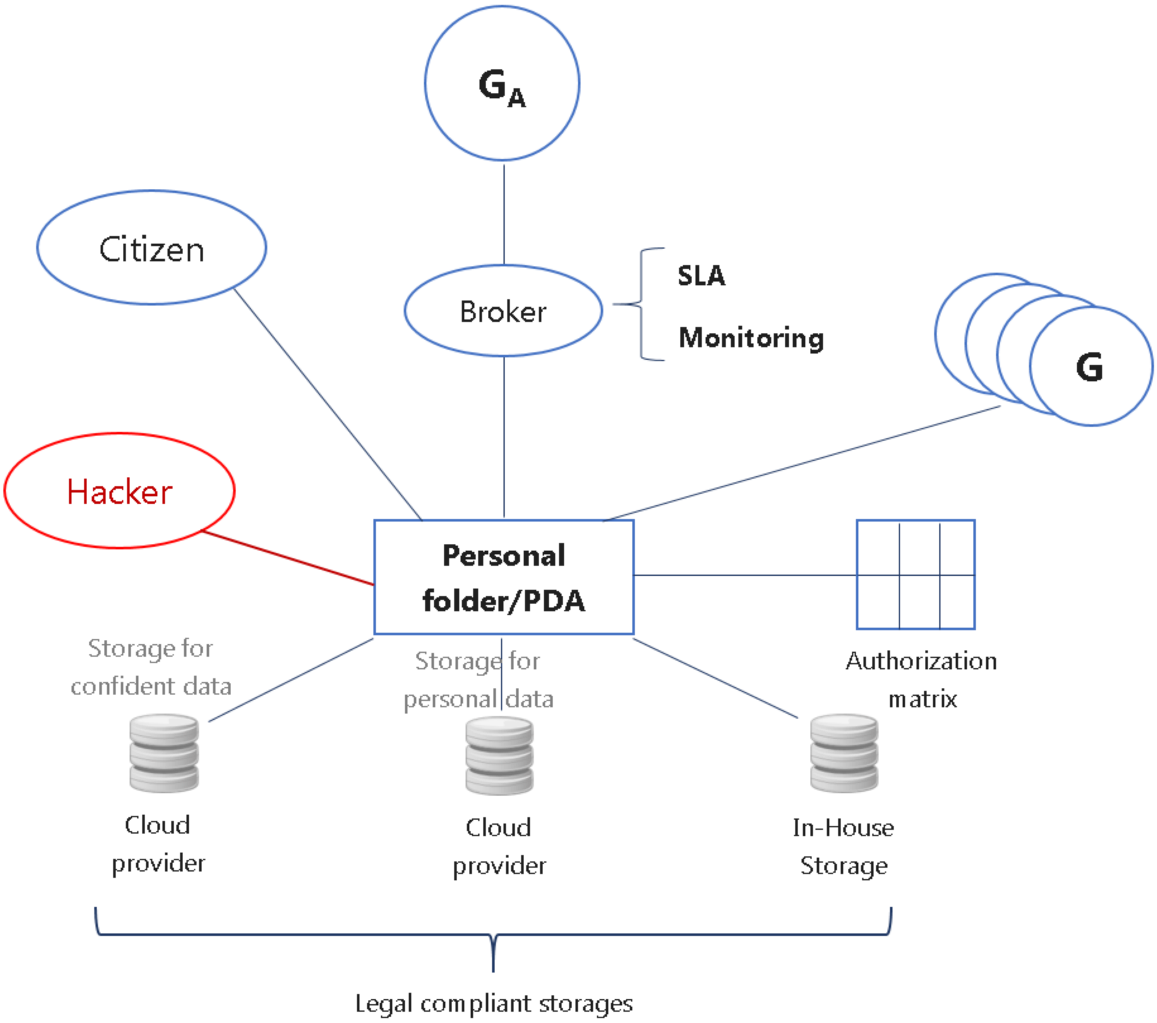

Figure 2 - Overall usage scenario

2 GENERAL REQUIREMENTS

Note: The following requirements apply to all three lots. Bidders are expected to respond to these requirements irrespective which lot they apply for (i.e. for each lot the bidder applies for, the response to lot-specific requirements and functional requirements need to be extended by these general requirements).

2.1.1 *SERVICE PORTABILITY AND DATA PORTABILITY*

Public authorities need to be enabled to easily change the service provider. This may e.g. be needed if a Cloud service contract expires and needs to be re-procured, a Cloud Service provider ceases operation, or a Cloud service disruption occurs. The bidders must demonstrate in each lot that the service including the data can be transferred at any time to an alternative provider.

ID	**SxGR1**
Actors	Cloud consumer, cloud provider
Description	There are many reasons a customer wants to change its cloud provider, e.g. the customer is not satisfied with the services offered, the current contract expires, the service provider can become bankrupt and consequently the public administration needs a way to (a) move its data to another provider and (b) transfer the service and all its dependencies. To avoid complete take-down of the service the migration should happen during operation.
Constraints	

Table 2 – Service Portability and Data Portability

Table 3 - Adhere to available standards and certifications

ID	**SxGR2**

Actors	Cloud consumer, cloud provider
Description	It is requested to adhere to available standards and certifications to avoid vendor lock-in. As a guidance, we refer to the ETSI standards map [1]. The bidder shall show which standards are most relevant for the solutions aimed at. According to the European Commission Cloud Communication [2]: *Standards in the cloud will also affect stakeholders beyond the ICT industry, in particular SMEs, public sector users and consumers. Such users are rarely able to evaluate suppliers' claims as to their implementation of standards, the interoperability of their clouds or the ease with which data can be moved from one provider to another. For this, independent, trusted certification is needed.*
Constraints	This requirements relates to Key Action 1 of the European Commission Cloud Communication [2], which forms an input to Cloud for Europe.

2.1.2 *SECURE INTEROPERABLE AUTHENTICATION*

All lots need some way of authentication. This can be by the public administration during service provision, or by the end user. Where authentication is involved, standard protocols need to be provided. In particular, the European cross-border interoperability framework provided by STORK and STORK 2.0 needs to be supported, the upcoming interoperability framework defined by the eIDAS Regulation, respectively.

ID	**SxGR3**
Actors	Cloud consumer, cloud provider, end user
Description	Where authentication is needed, standard protocols must be provided. The European eID interoperability framework provided by STORK and the eIDAS Regulation shall be supported. I.e., the provided service must allow holders of an European eID supported by STORK (a notified eID under the eIDAS Regulation, respectively) to use this eID to authenticate.
Constraints	The eIDAS Regulation (Regulation of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC) is to be considered. On the authentication process, the interoperability framework under article 12 of eIDAS is not yet defined. The bidders can take the STORK protocol (SAML 2.0, WebSSO) as working assumption.

Table 4 – Secure Interoperable Authentication

3 REFERENCES

[1] ETSI, Cloud Standards Coordination, Final Report Version 1.0, November 2013

[2] European Commission, Unleashing the Potential of Cloud Computing in Europe, COM(2012) 529 final