Complete Dynamic Multi-cloud Application Management

Project no. 644925

Innovation Action

Co-funded by the Horizon 2020 Framework Programme of the European Union

Call identifier: H2020-ICT-2014-1

Topic: ICT-07-2014 – Advanced Cloud Infrastructures and Services

Start date of project: January 1st, 2015 (36 months duration)

Deliverable D3.4

Business Plans and Potential Market

Due date:	30/11/2017
Submission date:	29/12/2017
Deliverable leader:	IRT
Editors list:	Domenico Gallico (IRT), Matteo Biancani (IRT)

Dissemination Level

☒	PU:	Public
☐	PP:	Restricted to other programme participants (including the Commission Services)
☐	RE:	Restricted to a group specified by the consortium (including the Commission Services)
☐	CO:	Confidential, only for members of the consortium (including the Commission Services)

List of Contributors

Participant	Short Name	Contributor
Interoute S.P.A.	IRT	Domenico Gallico, Matteo Biancani
SixSq SARL	SIXSQ	Charles Loomis, Marc-Elian Bégin, Vincent Van Dongen
QSC AG	QSC	R. Fischer, A. Weinert, U. Hacker, D. Hacker, M. Kourkuli
Technische Universitaet Berlin	TUB	D. Thatmann
Fundacio Privada I2CAT, Internet I Innovacio Digital A Catalunya	I2CAT	Eduard Escalona
Universiteit Van Amsterdam	UVA	Y. Demchenko
Centre National De La Recherche Scientifique	CNRS	Christophe Blanchet, Victoria Dominguez del Angel

Change history

Version	Date	Partners	Description/Comments
0.1	02/10/2017	IRT	ToC definition
0.4	17/11/2017	IRT	Inputs and ToC refinement
0.4	20/11/2017	SIXSQ	Contribution
0.5	24/112017	IRT	ToC updated
0.6	27/11/2017	SIXSQ	Risks and Business Plan
1.0	01/12/2017	IRT	First consolidated version
1.1	05/12/2017	IRT	Second consolidated version
1.1	18/12/2017	I2CAT	Contribution
1.1	18/12/2017	QSC, CNRS	Contribution
1.2	18/12/2017	IRT	Third consolidated version
1.3	26/12/2017	CNRS	Internal review
FF	28/12/2017	IRT	Final Version

Table of Contents

Figures Summary

Tables Summary

1. Executive Summary

This document is “D3.4 - Business Plans and Potential Market” pertaining to WP3 which is devoted to the identification and implementation of the CYCLONE use-cases. In the framework of WP3, this deliverable constitutes the outcome of task 3.4 “Evaluation of Potential Market” and, as such, it deals with the analysis of the potential market placement of the CYCLONE solution. A preliminary market analysis mainly related with the Cloud market, has been reported in “D3.1 - Evaluation of Use Cases”. During this last Project’s period, exploitation activities have become a key activity, aiming at maximizing the Project impact. Project partners organized the work documented in this deliverable in three different steps each one covering one aspect of the consortium’s exploitation strategy. These steps are directly reflected in the document structure. The initial step deals with the identification of all the results or components that constitute the foreground of the Project. These components constitute the building blocks of the CYCLONE services which have been analysed in order to evaluate their potential market acceptance. The results of our analysis are reported in section 2. The succeeding step takes into account the risks related with the possible adoption of any result by the targeted market. These results are described in sec 3. The last step provides a business plan for the whole CYCLONE solution, reported in section 4, and for the use cases, in section 5, using a Lean canvas template.

2. Analysis of CYCLONE services

In order to outline the Project's exploitation strategy, it is important to identify and describe the assets that represent the outcome of the research and development activity carried out during the Project's life-cycle. The exploitable results have been identified by CYCLONE partners, and listed in Table 2-1.

CYCLONE Components/features	Owner
CNSMO (Cyclone Network Services Manager and Orchestrator)	i2CAT
Integration of a network application component in SlipStream and the security architecture	i2CAT
Lightweight Dockerized network services	i2CAT
Automation of network services deployment process	i2CAT
Deployment of network cloud services on any Cloud IaaS provider	i2CAT
Security Architecture for Federated Cloud Applications	TUB
Accelerated eduGAIN Cloud Application registration	TUB
Minimal Overhead Identity Management for FCA	TUB
Flexible, federated VM Login Reusing eduGAIN Identities	TUB
User Friendly Distributed Logging with Access Control	TUB
Aggregation of distributed applications of multi tenants over multi clouds	TUB
Service Catalog: Database of available cloud services and their properties	SIXSQ
Service-Based, Multi-Cloud Deployment Engine	SIXSQ
Authentication with External Identity Providers	SIXSQ
Multi-Cloud Resource Monitoring	SIXSQ

Table 2-1: List of CYCLONE components

All these components are grouped in order to build up the services provided by CYCLONE which constitute the main focus of this Document and are described in the following tables. In these tables, we have carried out a market-oriented analysis on the three services that compose the CYCLONE solution in order to evaluate the potential exploitability in the market. These services are briefly described below:

- CNSMO: A cloud overlay networking platform that allows organizations to design and configure network connectivity and services over a multi-cloud scenario with a high degree of flexibility and scalability. CNSMO's concept based on Software Defined Networking (SDN) and network virtualization enables the dynamic control and monitoring of all deployed network services and their status through a friendly and adaptive central dashboard.

- Security architecture: The security architecture for Federated Cloud Applications includes a flexible federated login service based on eduGAIN identities. This functionality is achieved with minimal management overhead and enables an aggregation of distributed applications of multiple tenants over multiple clouds. Furthermore, a distributed logging service allows a user-friendly assessment of all log files collected at a single point.
- SlipStream: A general cloud application management platform that allows organizations and users to create customized hybrid cloud infrastructures and manage applications on those infrastructures. High-level resource selection, management, and monitoring features make it a compelling choice for cloud brokerage scenarios. Its support of external authentication methods makes integration with an enterprise user management possible.

CNSMO	
Components involved	CNSMO uses software components to implement its network services. The basic components are the CNSMO server, the SDN controller and the OVS (virtual switch). Moreover, each deployed network service involves an additional component. The components implemented within the CYCLONE project are: CNSMO-VPN, CNSMO-LB, CNSMO-DNS, CNSMO-FW.
Innovativeness introduced compared to already existing Products/Services	The main innovation of CNSMO is that it offers a high degree of flexibility thanks to the usage of network virtualization, which makes it scalable, extensible and the most important, programmable.
Unique Selling Point (competitive advantages)	Unlike other multi-cloud networking solutions, CNSMO is open source and offers a purely overlay integrated platform based on SDN and network virtualization techniques. This implies that access to physical infrastructure is not required and users can build their own network services as they need compared to other solutions that are tied to the cloud or service provider.
Market Trends/ Public Acceptance	The market trends related to Cloud computing have been reported in D3.1 sec. 6.
Service Market Positioning	CNSMO offers an overlay service for seamless connecting multi-cloud applications and therefore can be used by application providers or enterprise customers in the cloud networking or SDWAN market.
Legal / normative / ethical requirements	There are no unusual legal, normative or ethical requirements for the usage of CNSMO.
Competitors	The cloud networking and SDWAN market has several players but most solutions require access to the infrastructure directly or indirectly through management systems and their services are limited. Examples are Midonet, K8s, Dragonflow, OVN, Console Connect or SDWAN solutions offered by telecom manufacturers.
Cost of Implementation (before Exploitation)	The implementation costs are essentially the personnel costs related to the WP5 development.
Time to market	CNSMO needs proper quality and assurance testing before commercialisation but could go to market in less than 6 months after the project ends.
Foreseen Product/Service Price	N/A
Adequateness of Consortium Staff	The service has been developed and it is maintained by i2CAT
External Experts/Partners to be	On the development side i2CAT has all the expertise needed. The

involved	involvement of an external partner would be needed to finalize the market placement.
Status of IPR: Background (type and partner owner)	All the background knowledge belongs to i2CAT but some external elements used by CNSMO are open source with Apache license.
Status of IPR: Foreground (type and partner owner)	The foreground knowledge is open-source and belongs to i2CAT
Which partner contributes to what (main contributions in terms of know-how, patents, etc.)	All CNSMO contributions for the implementation of CNSMO in CYCLONE come from i2CAT with requirements coming from all consortium partners.
Partner/s involved expectations	IRT is interested in the exploitation of the CNSMO service to enhance its product portfolio regarding the VDC platform and the SDN-WAN technologies.
Sources of financing foreseen after the end of the project (venture capital, loans, other grants, etc.)	For the time being, CNSMO will be further developed using internal resources and funding from i2CAT.

Table 2-2: CNSMO

Security architecture (Authorization and authentication)	
Components involved	The security architecture for Federated Cloud Applications includes a flexible federated login service based on eduGAIN identities. This functionality is achieved with minimal management overhead and enables an aggregation of distributed applications of multiple tenants over multiple clouds. Furthermore, a distributed logging service allows a user-friendly assessment of all log files collected at a single point.
Innovativeness introduced compared to already existing Products/Services	Innovative improvement of authentication and Single Sign-On (SSO): Providing SSO for web apps in general implies deciding whether to use SAML based Web browser SSO profile or OpenID connect that allows connecting web applications. The security architecture enables end-users possessing SAML tokens to: • login to SAML-ready web services and to OpenID connect enabled endpoints (compare e.g. the Cyclone Wordpress demo). • none-http services, such as SSH or XPra, a remote desktop service Innovative improvement od authorization: • Attribute based authorisation using XACML policies and attributes profile • Authorisation and general security management for authorisation session using SAML and proprietary tokens New trust bootstrapping protocol is implemented to allow trust bootstrapping (initial trusted key distribution) of the provisioned cloud based resources during deployment stage
Unique Selling Point (competitive advantages)	The security infrastructure implements federated access control model and uses both tokens based and Single Sign On for authentication and

	authorisation session management. It can use both SAML tokens (XML) and OpenID Connect tokens (JSON). Using eduGAIN allows for research infrastructure users to use their organisational accounts to login to their SlipStream/CYCLONE applications. Trust bootstrapping allows setup trusted key at application end points during deployment, and avoiding manual keys or certificates distribution.
Market Trends/ Public Acceptance	This is a common trend to use federated access control model for user or applications authentication. Using EduGAIN is a common approach among Research institutions, Open ID Connect allows connecting any other user and also federating with major public cloud provider. The developed access control infrastructure components can be integrated with and extend functionality of the Cloud Access Security Brokers (CASB) which are current trend in cloud security.
Service Market Positioning	Identity and Access Management, Cloud based applications using multiple cloud resources and multi-organisational users.
Legal / normative / ethical requirements	Comply with personal data protection and privacy requirements, when processing personal user data. But there are no unusual legal, normative or ethical requirements for operating or extending the components.
Competitors	For federated access control: Shibboleth, Gluu Server, OpenAM, Ping Identity, Connect2id, ForgeRock (analysed at the initial stage of the project, market situation has not changed). For trust bootstrapping: Keylime (that is still not a market product).
Cost of Implementation (before Exploitation)	Not available at this time. Provided code supported by SlipStream recipes are ready for use but production code will require general software engineering process.
Time to market	Estimated on year
Foreseen Product/Service Price	Market accepted pricing scheme can use software and update subscription scheme at price level 50-100 Euro per year
Adequateness of Consortium Staff	Finalising development will require professional software development staff not available in consortium. TUB and UvA can provide support.
External Experts/Partners to be involved	No external partners are required, just software development and production staff.
Status of IPR: Background (type and partner owner)	Open Source with different license models such as LGPL, MIT or Apache v2.
Status of IPR: Foreground (type and partner owner)	The xpra-eletron-client was released as Open Source under CC0 by TU Berlin which is GPL compliant. Newly developed components are published under Apache 2.0 license.
Which partner contributes to what (main contributions in terms of know-how, patents, etc.)	TU Berlin contributed to several software components and data flows, such as Keycloak-SimpleSAML PHP setup, the SAML-secured SSH login and XPA remote desktop login. UvA contributed to Attribute based access control service and trust bootstrapping component. All components are published as Open Source software. For further details see the GitHub project repository. [1]
Partner/s involved expectations	Both TU Berlin and UvA will continue to further develop their components, however this depends on future research and innovation

	projects and funding.
Sources of financing foreseen after the end of the project (venture capital, loans, other grants, etc.)	National and European funding, industry funding (in the process of search).

Table 2-3: Security architecture (Authorization and authentication)

SlipStream	
Components involved	SlipStream includes the Service Catalog, the advanced deployment engine, external authentication mechanisms, and multi-cloud resource monitoring in addition to the existing functionality for managing application definitions.
Innovativeness introduced compared to already existing Products/Services	Innovative improvements to SlipStream: • The ability to select resources based on high-level functional and non-functional application requirements. • Full support of multi-cloud applications with automated deployment and management, including scaling. • Ability to have a complete overview of resource utilization across all clouds. • Integration with an organization's identity management system via integration of CYCLONE Keycloak server and direct support for OIDC and GitHub authentication mechanisms.
Unique Selling Point (competitive advantages)	Nearly all cloud application management platforms are tied to a single cloud service provider. In contrast, SlipStream has been designed from the beginning to support multiple cloud service providers, including private cloud infrastructures. This allows the best offers from multiple providers to be used, simplifies data protection concerns via the possibility of using private clouds, and provides a global overview of all resource usage.
Market Trends/ Public Acceptance	At this point, cloud computing technologies are firmly entrenched in both academic and industrial IT strategies. Organizations are now encountering the technical complications related to heterogeneity of cloud services, making the market receptive to solutions such as SlipStream. Moreover, true brokering, where the SlipStream platform operator handles billing and account management with the underlying cloud service providers, also simplifies the administrative overheads involved in using multiple cloud providers, further increasing the appeal of the platform.
Service Market Positioning	Cloud brokerage service is the primary market for SlipStream. The hybrid cloud management features of the platform make the solution relevant for "edge computing" scenarios as well, including Smart City and Smart Grid deployment.
Legal / normative / ethical requirements	Operators of a SlipStream-based service must comply with data protection and privacy requirements, but there are no unusual legal, normative or ethical requirements for such a service.
Competitors	See D6.3, Section 6 for a complete comparative analysis for SlipStream. The market situation has not changed markedly since that deliverable was written.

Cost of Implementation (before Exploitation)	The implementation costs are essentially the personnel costs related to the WP6 development.
Time to market	SlipStream and Nuvla are already commercial products being sold by SixSq to customers and being used as a technological platform for other European and national projects.
Foreseen Product/Service Price	This information cannot be disclosed in this Document
Adequateness of Consortium Staff	SixSq has adequate staff to continue to market and to improve SlipStream as a commercial platform and Nuvla as a commercial service (based on SlipStream).
External Experts/Partners to be involved	SixSq continually takes feedback from customers and collaborators in order to improve the solution and to tailor it to particular market sectors. For example, improvements are being made that allow the Human Brain Project to use cloud computing through their training platform and to make SlipStream a better management platform for "edge computing" scenarios for Smart City deployments.
Status of IPR: Background (type and partner owner)	The background IPR consists of the copyrights in the SlipStream source code and various trademarks associated with the software, such as SixSq, SlipStream, Nuvla, and NuvlaBox. The background rights are completely owned by SixSq.
Status of IPR: Foreground (type and partner owner)	The foreground IPR consists of the improvements to the source code for SlipStream. These are completely owned by SixSq.
Which partner contributes to what (main contributions in terms of know-how, patents, etc.)	Based on feedback from project participants, both involved in the development work packages and well as those involved in the demonstration work packages, SixSq has identified and delivered the innovations listed above. The largest contribution from developers outside of SixSq has been from TUB via their Keycloak server; this enabled straightforward connections to eduGAIN and Elixir AAI, two identity federations in the European scientific community.
Partner/s involved expectations	SlipStream is the foundational product for all of SixSq's products and services. SixSq will continue to market and to improve SlipStream to meet our customers' needs.
Sources of financing foreseen after the end of the project (venture capital, loans, other grants, etc.)	The standard funding resources will be used to continue development of SlipStream and to continue to provide SlipStream as a commercial, market solution. Sources include internal financing from commercial activities, capital from SixSq partners, and continued participation in various national and European research projects. Capital from external investors may be solicited at some point in the future.

Table 2-4: SlipStream

3. Risk analysis

For each of the services, a risk analysis has been performed considering the factors reported in the following tables in order to evaluate the exploitability of each CYCLONE service. The risk factors taken into account have been grouped in 6 categories and for each risk factor we tried to quantify (where applicable) with a value between 1 and 10 the degree of importance of the risk, the probability of risk happening and the degree of success of the related mitigation action. This risk analysis is summarized in the three following tables.

CNSMO				
Risk factor	**Degree of importance of the risk related to the final achievement of this service. (1 low - 10 high)**	**Probability of risk happening (1 low - 10 high)**	**Mitigation Action (scope and type of potential intervention)**	**Feasibility/Success of Intervention (1 low - 10 high)**
Partnership Risk Factors				
Disagreement on further investments: some partners may leave.	1	2	The development of this service has been and will be led by i2CAT, so no other internal or external partners are needed. This risk is not applicable	9
Industrialization at risk: no developer for the exploitable result.	1	2	I2CAT is the only partner developing this service. This risk is not applicable	9
Industrialization at risk: an industrial partner leaves the market.	1	2	Even if i2CAT is a research institution a change in the focus of its research is not foreseen. This risk is not applicable	9
Industrialization at risk: a partner declares bankruptcy.	1	2	I2CAT is a consolidated Research Institution. This risk is not applicable	9
Disagreement on ownership rules	1	2	Not Applicable	9
Partners on the same market	1	1	Not Applicable	9
Technological Risk Factors				
Worthless result: ill-timed disclosure.	5	4	The CNSMO service brings different novel concepts that are relevant for the actual market.	7

			Due to the high configurability of the service, the addition of new features or the enhancement of the current ones would increase the acceptability of the service.	
Worthless result: earlier patent exists.	5	3	To the best of our knowledge no earlier patents exist.	8
Worthless result: equivalent technology/methodology exists.	5	5	The cloud networking and SDWAN market has a growing forecast and while we are not aware of solutions offering the same as CNSMO, new start-ups and solutions keep arising and we should keep a close eye on new tools in the market.	7
Significant dependency on other technologies.	6	5	The dependence on Slipstream could pose a limit, but the CNSMO service can be deployed also without it.	7
The life cycle of the new technology is too short.	4	1	CNSMO is based on SDN and NFV concepts and technologies, which will be the basis of future networking solutions. The programmability and flexibility offered by CNSMO makes it adaptable to technology changes.	9
Market Risk Factors				
Worthless result: performance lower than market needs.	6	6	Enhance the performance with further development	5
Nobody buys the product. Nobody needs it.	7	5	Detailed market analysis and a targeted communication strategy.	7
Nobody buys the product. Problems at the time of the first sales.	7	6	Improve the service and perform accurate performance tests before market placement	7
Nobody buys the product. Rejected by end-users.	7	6	Users acceptance tests would mitigate this risk	6
IPR Risk Factors				
No patents on background knowledge	4	4	I2CAT is the only owner of CNSMO copyright.	7
Foreground knowledge is not patentable	4	4	CNSMO will continue to be license under Apache open source.	7

Financial Risk Factors				Financial R
Multiple changes to original objectives.	2	2	CNSMO has been designed to be programmable and thus flexible to adapt to new technologies and services.	8
Weak exploitation. Inadequate business plan	8	6	A proper business plan should be elaborated to be able to exploit CNSMO prior to commercialization.	4
Environmental Risk Factors				
Nobody buys the product. Does not comply with the standards.	2	2	CNSMO can be used without any applicable standards but could be adapted to the SDN and NFV standard architectures.	9
Nobody buys the product. Standards to make it compulsory don't yet exist.	1	1	Standards to make use of the product are unlikely to be created.	10
Influence of laws and regulations.	4	3	Since CNSMO allows multi-cloud, regulation on network and cloud usage in different countries could have an influence. However, these regulations are to be complied by cloud and service providers.	8

Table 3-1: CNSMO – Risk analysis

Security Architecture				
Risk factor	**Degree of importance of the risk related to the final achievement of this service. (1 low - 10 high)**	**Probability of risk happening (1 low - 10 high)**	**Mitigation Action (scope and type of potential intervention)**	**Feasibility/Success of Intervention (1 low - 10 high)**
Partnership Risk Factors				
Disagreement on further investments: some partners may leave.	4	5	Code is available as Open Source on the project github [1] allows new team of partner to take over the further development.	8
Industrialization at risk: no developer for the exploitable result.	2	2	Access control in multi-cloud environment is in strong demand. Specific features in the proposed solution will guarantee the market support.	8
Industrialization at risk: an industrial	5	5	Open source license will allow other partner to take over but	7

partner leaves the market.			initial experience is required.	
Industrialization at risk: a partner declares bankruptcy.	n/a	n/a	n/a	n/a
Disagreement on ownership rules	2	2	N/a due to Open Source license	8
Partners on the same market	n/a	n/a	n/a	n/a
Technological Risk Factors				
Worthless result: ill-timed disclosure.	4	3	This is very active and competitive market, but majority of security applications will require tuning to applications. Proposed security solutions are already offered for project use cases what will guarantee their use.	7
Worthless result: earlier patent exists.	4	3	See above.	7
Worthless result: equivalent technology/methodology exists.	4	3	See above.	7
Significant dependency on other technologies.	6	6	All external technologies are Open Source. However modular design will allow replacing affected component.	7
The life cycle of the new technology is too short.	3	4	The security components are based on already established technology and standards. All existing solutions are maintaining compatibility with earlier versions.	7
Market Risk Factors				
Worthless result: performance lower than market needs.	4	4	In cloud environment performance issue can be addressed by selecting VM configuration	8
Nobody buys the product. Nobody needs it.	4	3	New integrated security solutions can be offered by cloud providers. Customers will prefer them even if limited functionality. But customers using multi-cloud applications may prefer CYCLONE solution.	7
Nobody buys the	4	4	Code should be prepared for	8

product. Problems at the time of the first sales.			production. Marketing campaign will be required.	
Nobody buys the product. Rejected by end-users.	3	3	There are already identified user groups among bioinformaticians and potentially energy sector.	7
IPR Risk Factors				
No patents on background knowledge	n/a	n/a	This is Open Source product	n/a
Foreground knowledge is not patentable	n/a	n/a	This is Open Source product	n/a
Financial Risk Factors				
Multiple changes to original objectives.	4	4	Additional exploitation planning is required when moving to market and sales.	7
Weak exploitation. Inadequate business plan	4	4	See above.	7
Environmental Risk Factors				
Nobody buys the product. Does not comply with the standards.	3	3	Product is standard based	8
Nobody buys the product. Standards to make it compulsory don't yet exist.	n/a	n/a	See above.	n/a
Influence of laws and regulations.	3	3	The compliance with the private data management should be addressed by organisational policies.	8

Table 3-2: Security architecture (Authorization and authentication) – Risk Analysis

SlipStream				
Risk factor	**Degree of importance of the risk related to the final achievement of this service. (1 low - 10 high)**	**Probability of risk happening (1 low - 10 high)**	**Mitigation Action (scope and type of potential intervention)**	**Feasibility/Success of Intervention (1 low - 10 high)**
Partnership Risk Factors				
Disagreement on further	3	3	The liberal licensing policies for the CYCLONE components	8

investments: some partners may leave.			ensures that the components can be exploited effectively even if the primary partner for a component withdraws, although this would increase the development and maintenance costs for the partners that continue with the exploitation.	
Industrialization at risk: no developer for the exploitable result.	2	2	If the market is sufficient to support continued development, then there is no associated risk. If the market is not sufficient, then others can exploit the result. The software is sufficiently general that alternate markets may be able to support continued development and exploitation.	8
Industrialization at risk: an industrial partner leaves the market.	5	5	If a consortium partner left, the license would allow continue exploitation of the result, although it would increase the costs for maintenance and support.	*5*
Industrialization at risk: a partner declares bankruptcy.	2	2	SixSq does not rely critically on other partners to deliver a solution around SlipStream. In addition, the licensing of other products allows SixSq to continue using and developing other partners' contributions.	*8*
Disagreement on ownership rules	2	2	SixSq is the sole owner of the IPR for SlipStream. Our contributor policies and explicit language within the consortium agreement ensure that this is the case. Given the preparation, a legal dispute is unlikely.	*8*
Partners on the same market	1	1	There are no other partners within the CYCLONE consortium that address the same markets as SixSq. The primary risk comes from other organizations within the market.	*10*
Technological Risk Factors				
Worthless result: ill-timed disclosure.	1	1	As part of its commitment to open source software, the core of SlipStream, including enhancements from CYCLONE, are publicly available throughout the development process.	*10*

Worthless result: earlier patent exists.	8	1	Generally, software patents within Europe are not possible and it is unlikely that a patent would be approved that covers the SlipStream software and methodologies. It is also unlikely that such a patent would hold up in other markets (e.g. the USA) because the brokerage services have existed in other domains and markets for some time.	*8*
Worthless result: equivalent technology/methodology exists.	5	5	Other cloud application management platforms exist and are becoming more viable competitors. However, the strong focus on multi-cloud support provides a unique selling point, even with competitions from the other solutions.	*5*
Significant dependency on other technologies.	6	2	Cloud technologies are embracing container-based solutions in addition to those based on hypervisors. SlipStream will incorporate those technologies to ensure that the product is as broadly applicable as possible.	*8*
The life cycle of the new technology is too short.	6	4	The SlipStream architecture and code base are designed to allow for rapid modification and incorporation of new features. By evolving, the product can remain relevant even if the underlying technologies shift.	*7*
Market Risk Factors				
Worthless result: performance lower than market needs.	7	5	The functionalities of the solution have been validated with both internal and external use cases, showing that the core functionality is sound. These validations have also identified areas that need improvement or expansion. Those areas have been added to the SlipStream roadmap.	*8*
Nobody buys the product. Nobody needs it.	8	6	Although there are already clients of SlipStream, we must determine that the market is large enough to support the product and its continued development.	*6*

Nobody buys the product. Problems at the time of the first sales.	8	4	The previous validations of the product along with existing sales, make this unlikely. Nonetheless, the roadmap is important to ensure that clients are highly satisfied with the product.	*6*
Nobody buys the product. Rejected by end-users.	8	4	See previous risk.	*6*
IPR Risk Factors				
No patents on background knowledge	4	4	The SlipStream code base is copyrighted with the copyright held solely by SixSq. In addition, the name "SlipStream" is a registered trademark in Switzerland and could be extended easily to Europe.	*8*
Foreground knowledge is not patentable	4	4	The consortium agreement explicitly defines that contributions to SlipStream from other partners become the IPR of SixSq. Moreover, all of the changes made over the course of the project are properly protected.	*8*
Financial Risk Factors				
Multiple changes to original objectives.	2	2	The platform is designed to be as flexible as possible to allow for broad market coverage. The ability to adapt to different scenarios and requirements is a benefit for users.	*8*
Weak exploitation. Inadequate business plan	8	5	As there are currently clients and sales of the platform, the core business plan is very likely to be adequate. Nonetheless, it must be refined so that SixSq and the other partners can maximize the exploitation.	*6*
Environmental Risk Factors				
Nobody buys the product. Does not comply with the standards.	1	1	No applicable standards.	*10*
Nobody buys the product. Standards to make it compulsory don't yet exist.	1	1	Standards to make use of the product are unlikely to be created.	*10*

Influence of laws and regulations.	1	1	Although operators of a platform based on SlipStream must conform to legal requirements concerning data protection and privacy, there is no legislation that particularly targets cloud computing. The update of the GDPR for Europe will however enhance interoperability and encourage use of a broader range of cloud services.	*10*

Table 3-3: SlipStream – Risk analysis

4. Business Plan

Over the last few years, the adoption of Cloud services by SMEs (Small Medium Enterprise) and LSEs (Large Scale Enterprise) is by now a well-established IT and business solution and its acceptance and deployment is continuously growing so that even mission-critical workloads are being moved to the cloud. Many IT and Data Center operators provides several services and products in order to target this increasing market demand. Year over year the business opportunities enabled by the cloud services demand are becoming more strengthened and thus profitable, generating conspicuous revenues that allows an always increasing effort and investments in IT facilities and infrastructures. Even if cloud computing is an evolving paradigm and its attributes and characteristics will evolve and change over time, the definition of Cloud computing provided by NIST has gained significant acceptance within the IT industry. According to this definition:

"*Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.*" [2]

The composition of the cloud service paradigm is outlined by the definition above. In particular we will provide a description of the different components of such paradigm, listing and detailing the "*five essential characteristics*", the "*three service models*" and the "*four deployment models*".

The five essential characteristics proposed in the NIST definition can be summarized as follow:

- On-Demand Self-Service: Customers must be able to obtain cloud services whenever they need them, in an automated and self-service way. For the cloud service provider standpoint, on-demand self-service requires that provisioning, account management, service instantiation, security control, service management, metering, billing and payment mechanisms are automatically established. These mechanisms will interface with operational systems so that services are created, started, run, and stopped according with the customer's needs.
- Broad Network Access: The broad network access for cloud computing will enable the usability of the whole platform, so that services can be successfully used by anyone, anywhere on the globe, using a variety of devices.
- Resource Pooling: The cloud provider's resources in terms of storage, computing, network, and virtual machines must be pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to customer demand.
- Rapid Elasticity: The ability to have a flexible computing service which can expand or contract in line with business demand, is one of the key benefits of cloud computing. This feature would be impossible for an in-house implementation without significant investment in resources. From a cloud service provider standpoint, this elasticity implies the challenge of forecasting the customer demand, in order to maximize profits.
- Measured Service: Cloud service providers must provide sufficient information about their charging procedures in order to allow customers to make informed choices. The provisioning of

cloud resources must cope with an accurate accounting system in order to support their bills, and give sufficient usage information to allow solutions to be managed operationally.

The three service models mentioned in the NIST definition of cloud service are described below:

- Infrastructure as a Service (IaaS): with this model, cloud service providers own, manage, and operate the computing hardware, making available and maintaining all the fundamental computing resources on top of which customers can deploy and run arbitrary software including operating systems.
- Platform as a Service (PaaS): in this case the cloud service providers in addition to the computing hardware, is also responsible of operating and maintaining the operating system and all the software that create the platform requested by the customer, including the related middlewares.
- Software as a Service (SaaS): this model provides the customer with a single application running on a cloud infrastructure, so that the customer is not aware of the underlying hardware and software configuration.

The deployment models define the way cloud services can be accessed by customer:

- Private Cloud: the cloud environment is operated for a single organization and can be managed on-premises or off-premises. On the one hand, this deployment implies a significant capital investment, but on the other hand it avoids any restriction related to security, network bandwidth and legal issues.
- Public Cloud: this is the most recognizable cloud deployment model, where the resources are made available to the general public. From the consumer point of view, the main benefit is the ease of access and fast self-service provisioning.
- Community Cloud: in this model, the cloud infrastructure is shared between different organizations. This model has similarities to both private and public cloud.
- Hybrid Cloud: using this model, customers can set up a cloud infrastructure by composing two or more cloud environments (e.g. public cloud and private cloud), that are bounded together and coordinated by a cloud broker that federates data, identity and security.

Beside the technical solutions enabled by cloud services' deployment, cloud computing has also, and maybe above all, created a new business model within the IT market. Many refer to cloud computing as a "disruptive innovation" in the IT market landscape, and indeed this is a true statement. A disruptive innovation, by definition, is the introduction of a better business model into an already existing market. The business model is focused on value creation and describes a company's core strategy to generate economic value, normally in the form of revenue. The model provides the basic template for a business to compete in the market place, it provides a template on how a company is going to generate profits, and how it will interact with regards to the internal resources and external players (stakeholders such as customers, suppliers, and investors). In summary, the business model deals with the methodology used to convert inputs (capital, raw materials and labour) into outputs (total value of services produced) and make a return that should be greater than the incurred cost of capital.

In the following sections, we have elaborated a Business model for each of the services delivered by CYCLONE using the Lean Canvas template since it outlines a more problem focused approach and it majorly targets entrepreneurs and start-up businesses.[3]

4.1. CNSMO Business Plan

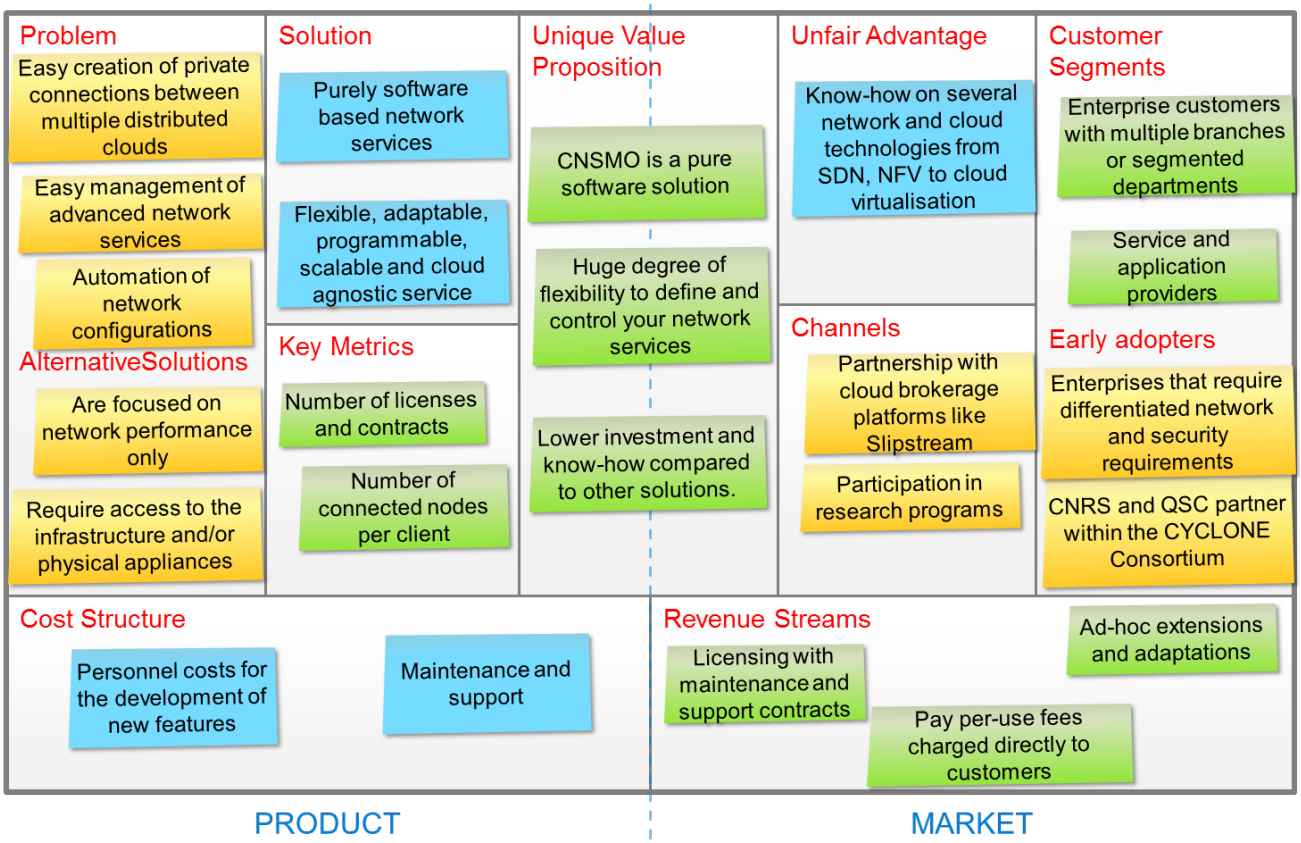

Figure 4-1: CNSMO Business plan

Below is reported a more detailed description of each field:

- **PROBLEM:**
  - Easy creation of private connections between multiple distributed clouds
  - Easy deployment and management of advanced network services
  - Automation of network configurations with support for dynamic scaling
- **CUSTOMER SEGMENT**
  Enterprise customers with multiple branches and/or segmented departments, service and application providers.

- **EARLY ADOPTERS:**
  Enterprises that require clear segmentation of their services with differentiated network and security requirements.

- **ALTERNATIVE SOLUTION:**
  Existing alternatives are focused on network performance rather than functionality, they require access to the infrastructure and/or physical appliances installed and many are dependent on the underlying technology.

- **UNIQUE VALUE PROPOSITION:**
  CNSMO is a pure software solution that requires no specific hardware to provide with a huge degree of flexibility to define and control your network services dynamically through a user friendly

simplified interface. Therefore, it requires lower investment and know-how compared to other solutions.

- **SOLUTION:**
  CNSMO is able to deploy and control network services that are purely software based, making it flexible, adaptable and scalable. It is also programmable so new network services can be added, modified and tuned thanks to the fact that is based on open source SDN and NFV components. Moreover, it is agnostic of any underlying cloud system or network technology as it is IP based.

- **UNFAIR ADVANTAGE:**
  Requires deep know-how on several network and cloud technologies from SDN, NFV to cloud virtualisation, which is nowadays difficult to find combined in an integrated and simplified platform.

- **CHANNELS**:
  Partnership with cloud brokerage platforms like Slipstream, industrial forums, technological exhibitions, participation in research programs.

- **REVENUE STREAMS**:
  Licensing with maintenance and support contracts, ad-hoc extensions and adaptations, pay per use.

- **KEY METRICS:**
  Number of licenses, number of contracts, number of connected nodes per client.

- **COST STRUCTURE:**
  Personnel costs for the development of new features, maintenance and support.

4.2. Security architecture Business Plan

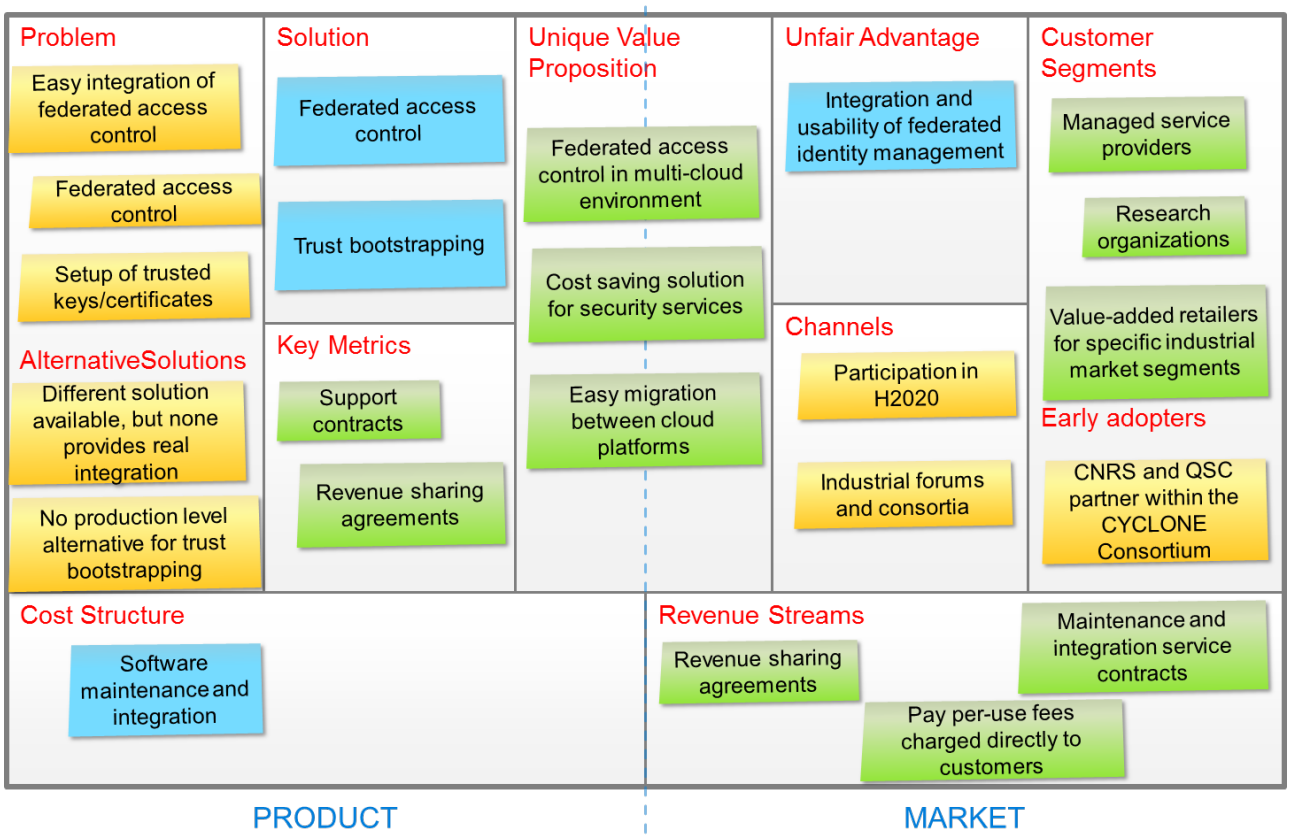

Figure 4-2: Security Architecture Business Plan

Below is reported a more detailed description of each field:

- **PROBLEM**:
  - Easy integration of the federated access control services with user applications.
  - Federated access control that allows using user home organisation credentials.
  - Initial distribution or setup of trusted keys/certificates for deployed cloud based applications.
- **SOLUTION**:
  - Federated access control using federated identity providers such as OpenID Connect, eduGAIN for authentication and security context management for authorisation service,
  - Trust bootstrapping for cloud resources deployment using TPM like functionality
- **ALTERNATIVE SOLUTION**:
  - Variety of alternative for federated identity providers but all can be integrated into the proposed solution
  - No production level alternative for trust bootstrapping and trust management in multi-cloud environment
- **KEY METRICS**: When sold as software supporting or integration service, number of organizational support contracts and number of revenue sharing agreements.
- **CUSTOMER SEGMENT**: Managed service providers and value-added retailers for specific industrial market segments. Research organizations (both industrial and academic).

- **EARLY ADOPTERS**: At the moment, the Security Architecture has been adopted by CNRS and QSC within the CYCLONE Consortium.
- **UNFAIR ADVANTAGE**: Integration and usability of federated identity management.
- **CHANNELS**: Through contacts arising from participation in H2020 and other research projects for research organizations. Through industrial forums and consortia around cloud computing for managed service providers and value-added retailers, and specifically managed security services providers and integrators.
- **UNIQUE VALUE PROPOSITION**: Federated access control in multi-cloud environment supported by SlipStream cloud applications platform and available deployment and integration recipes that can be re-used. This will allow to lower cost for adding security services and lower the technical barriers for migration between cloud platforms.
- **REVENUE STREAMS**: Software maintenance and integration service contracts. For a SlipStream-based service, either revenue sharing agreements with cloud service providers or per-use fees charged directly to customers.
- **COST STRUCTURE**: Primary costs for software maintenance and integration with the customer applications.

4.3. SlipStream Business Plan

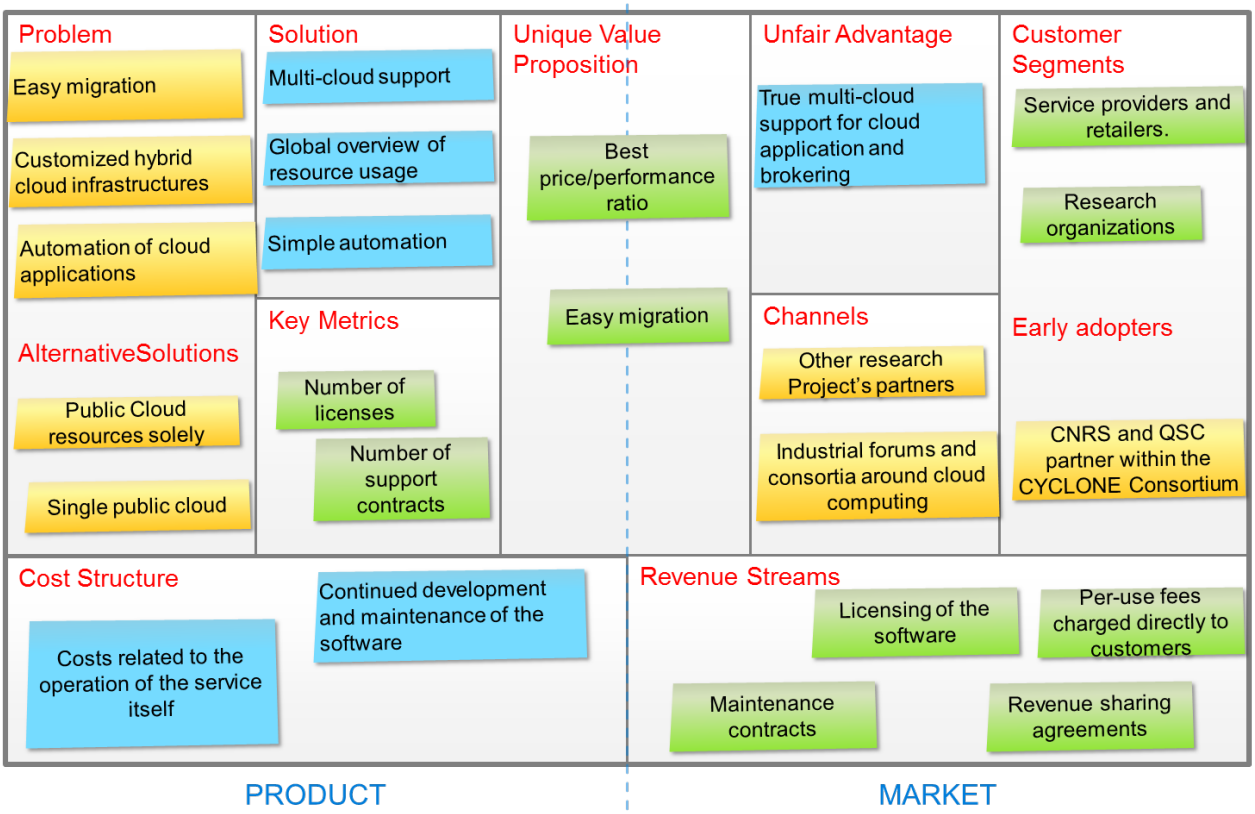

Figure 4-3: SlipStream Business Model

Below is reported a more detailed description of each field:

- **PROBLEM**:
  - Easy migration between cloud service providers by facilitating cloud application portability.
  - Creation of customized hybrid cloud infrastructures that allow customers' private clouds to be used and that minimize risks associated with data protection.
  - Automation of cloud applications with support for dynamic scaling and application optimization.
- **SOLUTION**: Provides true multi-cloud support allowing global overview of resource usage, comparison of offers to find the best price/performance ratio, simple automation across both public and private cloud resources.
- **ALTERNATIVE SOLUTION**: Potential customers are 1) using only public resources because of the data protection risks, 2) using only a single public cloud infrastructure to avoid complications from heterogeneous features/APIs, or 3) using only a single cloud to benefit from its proprietary cloud application management features. (See Deliverable D6.3 for full comparison of market alternatives).
- **KEY METRICS**: When sold as software, number of licenses. When sold as a service, number of organizational support contracts and number of revenue sharing agreements.
- **CUSTOMER SEGMENT**: Managed service providers and value-added retailers for specific industrial market segments. Research organizations (both industrial and academic).

- **EARLY ADOPTERS**: Research organizations needing to optimize their use of cloud resource and/or providing services to larger communities outside of the organization itself. CNRS and QSC within the CYCLONE consortium already adopted the Slipstream solution.
- **UNFAIR ADVANTAGE**: True multi-cloud support (both in terms of cloud application management and in terms of brokering). This is a strategic choice made possible because we are not a cloud service provider.
- **CHANNELS**: Through contacts arising from participation in H2020 and other research projects for research organizations. Through industrial forums and consortia around cloud computing for managed service providers and value-added retailers.
- **UNIQUE VALUE PROPOSITION**: Allows best price/performance ratio for different cloud providers to be easily found and lowers the administrative and technical barriers for migration between them to nearly zero.
- **REVENUE STREAMS**: Licensing of the software (with maintenance contracts) when sold for on premise use. For a SlipStream-based service, either revenue sharing agreements with cloud service providers or per-use fees charged directly to customers.
- **COST STRUCTURE**: Primary costs for both on premise and service-based offers are the continued development and maintenance of the software. For the service-based offers, there are additional costs related to the operation of the service itself.

5. Impact of the CYCLONE platform on the implemented Use Cases

In the previous sections, we have analysed the different services developed in the Project with an insight on the potential exploitability and the risks related to the market placement of such services. In this section, we try to capture the point of view of the different Use-Case owner, in order to understand how they can benefit from the use of the CYCLONE solution.

5.1. Energy Use case - Energy Management Platform in a Multi-Cloud Computing Infrastructure

5.1.1. Context

To fulfil the climate protection goals of the European Union and to ensure reliable energy supply in the future a new approach for energy management is required. The decarbonisation goals make the further development of renewable energy generation and its integration into the power distribution grid necessary. Renewable energy resources are both decentralized and volatile. To efficiently incorporate such resources the power grid must become smarter. The complexity of the future energy management requires the automation of the processes in the energy management and digitalization of the services.

The cloud-based Energy Management Platform is an advanced data processing platform which integrates modern data processing into the energy management infrastructure. The data are collected, stored, analysed and processed. Information is made available through different gateways for different services. Integrating sensor technology for measurement of energy generation and consumption data into an overall cloud solution is the focus in the Smart Utility use case. Ultimate goals are the improvement of the energy management infrastructure to enable the efficient usage of energy resources and the provision of a stable European power Grid. The latter is particularly within the task of TSOs (Transmission Service Operator operating Highest Voltage Power Grid) and DSOs (Distribution Service Operator operating medium Voltage Power Grid and local access power lines) within the different countries.

5.1.2. Impact of the CYCLONE Platform

The implementation of the Energy Management Platform has to consider the required security, resilience and reliability aspect for the energy system. It has to incorporate the multiple roles and requirements of the partners in this system. Furthermore, it has to take the decentralized and distributed energy resources into account. The deployment of the Energy Management Platform via the CYCLONE platform provides a reliable and time effective method to set up and manage the Smart Utility application in a multi-cloud environment. It benefits from the advanced deployment features and the added value provided by DACI for reliable authorization and CNSMO for flexible network management within the application. This enables the application provider to save the effort for development and maintenance of these services. The

CYCLONE platform enables the provider of the Smart Utility application to provide the services in a secure and reliable manner to the partners in the energy market.

5.1.3. Energy Management Platform business model canvas (Strategyzer AG)

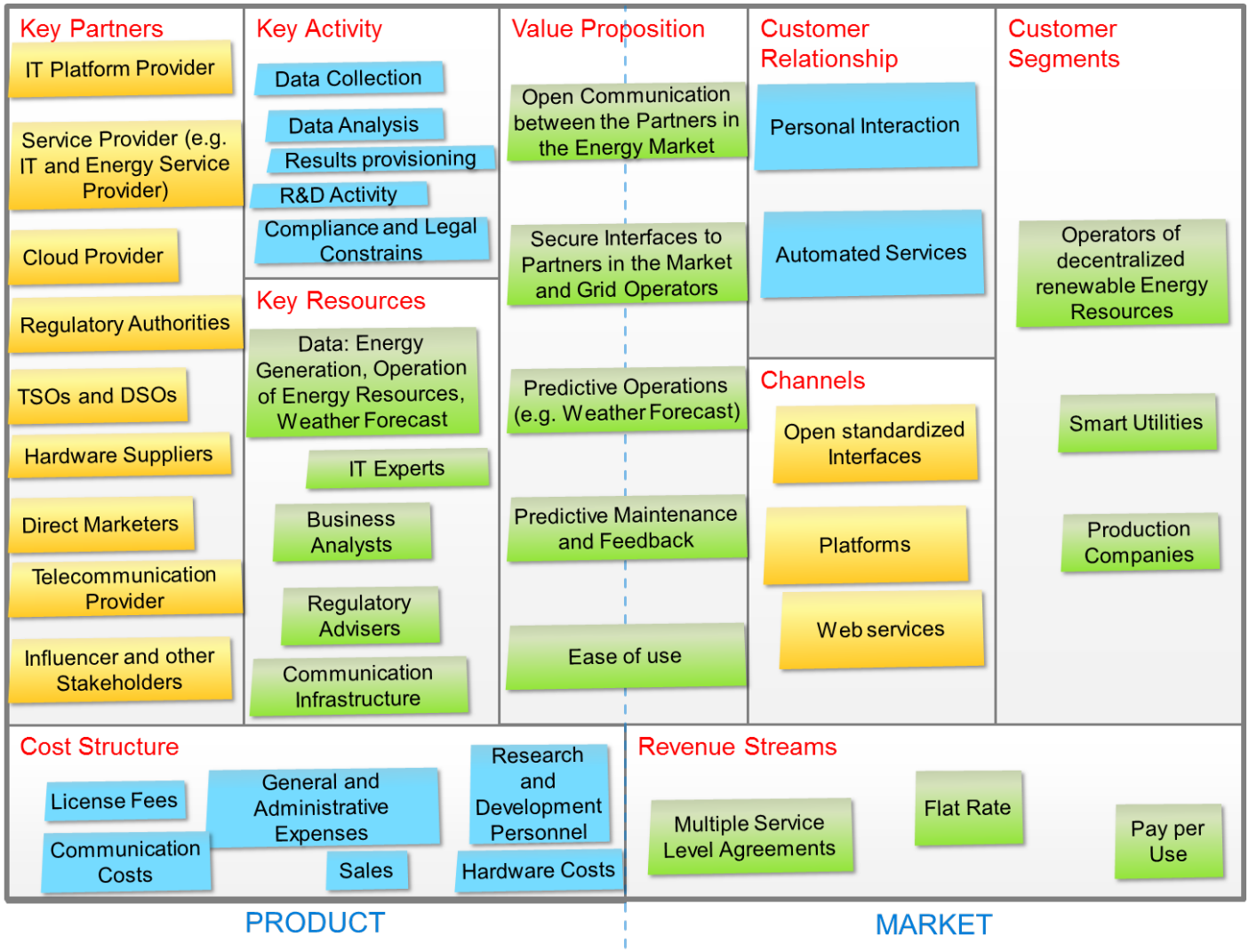

Figure 5-1: Energy Use-Case Business Model

5.2. Bioinformatic Use Case - Bioinformatic Services based on the Cloud Computing Infrastructure

5.2.1. Context

In the mid-2000s, massively parallel sequencing, also known as next-generation sequencing (NGS), has decreased the cost and increased the throughput of sequencing. The information explosion has been driven by these technical improvements. Today, large sequencing centers are able to produce genomic data at the rate of 10 terabytes of data in only one bioinformatic experiment. The databases such as the European Nucleotide Archive (ENA) or Sequence Read Archive (SRA) represent a challenge because they are too large for the classical sharing and because analyses are increasingly important.

In addition, the output data require complicated computing processing to transform raw data into biological and actionable value information. Problems such as reproducibility and repeatability have been reported as a major scientific issue when it comes to large scale data analysis.

Cloud computing is now a solid solution and also a commercial reality. This technology provides real advantages for the management of vast amounts of data generated by the omics technologies [4].

5.2.2. Impact of Cyclone Platform

The implementation of the bioinformatic use case in the CYCLONE platform brings immediate benefits to the research in bioinformatics, in terms of costs, scalability, repeatability and dissemination across a wide variety of environments.

Indeed, the advantages of this implementation are the following:

- An easy deployment of the applications in bioinformatics: with just a few clicks we can reproduce complete environments across multiple clouds.
- Overcoming problems regarding local IT resource limitations.
- A significant decrease in the calculation time thanks to horizontal scalability.
- A high data storage capacity and at the same time important reductions of data transfer requirements.
- The robustness in repeatability via an ongoing effort to standardise genome analysis tools with bioinformatic appliances into a marketplace.

5.2.3. Bioinformatics business model canvas (A. Osterwalder):

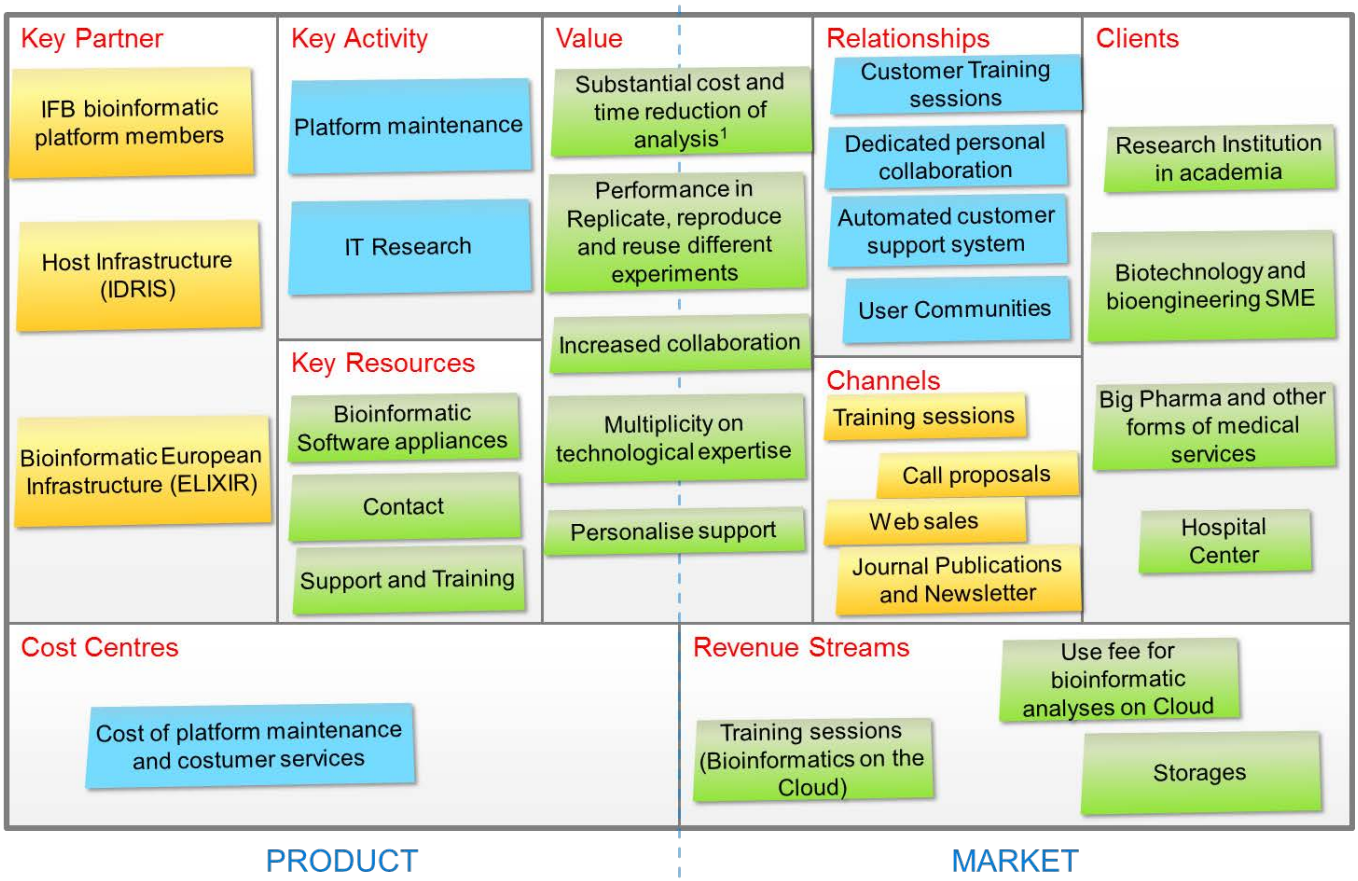

Figure 5-2: Bioinformatics Use-Case Business Model [5]

Conclusions

This Deliverable is the outcome of task 3.4 entitled “Evaluation of potential market”. We performed an analysis on the possible market acceptance and definition of a business plan for each CYCLONE service, aiming at establishing an initial step towards the market placement of such services. It is worth notice here that the services proposed by the CYCLONE project have different level of maturity both from a development and business point of view. The Slipstream service is a product already present on the market and has been enhanced and enriched with the CYCLONE features, while CNSMO and the Security Architecture services would need to undertake a product development phase in order to finalize the market placement with a more business and marketing related approach.

References

[1] https://github.com/cyclone-project

[2] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pd

[3] https://canvanizer.com/new/lean-canvas

[4] https://en.wikipedia.org/wiki/Omics

[5] http://www.nature.com/news/data-analysis-create-a-cloud-commons-1.17916

Abbreviations

B2B	Business to Business
DC	Data Center
E2E	End to End
IaaS	Infrastructure-as-a-Service
IPR	Intellectual Property Rights
IT	Information Technology
MaaS	Metal as a Service
NaaS	Network-as-a-Service
Net-HAL	Network Hardware Abstraction Layer
NFV	Network Function Virtualization
PaaS	Platform-as-a-Service
PC	Project Coordinator
PMB	Project Management Board
PoP	Point of Presence
SaaS	Software-as-a-Service
SCI	Smart Core Interworks
SDN	Software Defined Networks
SP	Service Provider
TC	Technical Coordinator
TCTP	Trusted Cloud Transfer Protocol
TMB	Technical Management Board
WP	Work Package
WPL	Work Package Leader

<END OF DOCUMENT>