Call for projects for a participation in the Important Project of Common European Interest on Cloud Infrastructure and Services

The Luxembourg Ministry of the Economy plans to support projects that contribute to the emergence of the Distributed Multi Provider Cloud-Edge Continuum. The aim of this Call for projects is therefore to identify and select projects that will participate in this IPCEI on Cloud Infrastructure and Services (hereinafter "IPCEI-CIS").

Subject to the conditions set out in the IPCEI Communication[1] and to national legislation, the IPCEI framework allows for a funding of up to 100% of the eligible costs of a project, including a potential first industrial deploymentif this is justified by the funding gap analysis[2].

Projects selected to participate in the IPCEI-CIS according to the criteria outlined in Section 4 will have to participate in (i) "matchmaking" sessions, which will allow them to connect to projects selected in other participating Member States, as well as in (ii) the notification procedure before the European Commission. The indicative timeline of the IPCEI-CIS process is set out in Section 7 of this Call for projects.

The applicants should be aware that the notification process requires significant resources both on the part of the aid applicant and the national authorities and funding bodies.

Please note that it is not yet possible to indicate whether an IPCEI on Cloud Infrastructure and Services will actually be created as it will depend on the level and quality of participation of each Member State.

If the project does not fulfill the criteria of the IPCEI Communication, but still contributes to the emergence of the Distributed Multi Provider Cloud-Edge Continuum, it may be considered for funding under the RDI Law[3]. The latter allows for a funding of up to 80% of the eligible costs of an industrial research project and 60% of the eligible costs of an experimental development project. These projects identified for funding outside the IPCEI process will be invited to submit a formal application for State aid under the RDI Law at a later stage.

Please note that, in any case, an application under this Call for projects is non-binding and will not be considered as a formal application for State aid.

[1] Communication of the European Commission Criteria for the analysis of the compatibility with the internal market of State aid to promote the execution of important projects of common European interest (2014/C 188/02): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52014XC0620%2801%29

[2] Eligible costs are determined in accordance with the Annex of the IPCEI Communication and can include feasibility studies, costs of instruments and equipment, costs of acquisition (or construction) of buildings, infrastructure and land, personnel and administrative costs, other costs necessary for the project (including materials, supplies, components and similar products), costs associated with obtaining, validating and defending patents and other intangible assets. Operating costs (OPEX) can only be funded for projects within their first industrial application if this commercial use is the result of R&D&I activities and in itself includes an important R&D&I component.

[3] Loi modifiée du 17 mai 2017 ayant pour objet 1. le renouvellement des régimes d'aides à la recherche, au développement et à l'innovation; 2. les missions de l'Agence nationale pour la promotion de l'innovation et de la recherche; et modifiant la loi modifiée du 5 juin 2009 relative à la promotion de la recherche, du développement et de l'innovation: http://legilux.public.lu/eli/etat/leg/loi/2017/05/17/a544/jo

1. Background and objectives

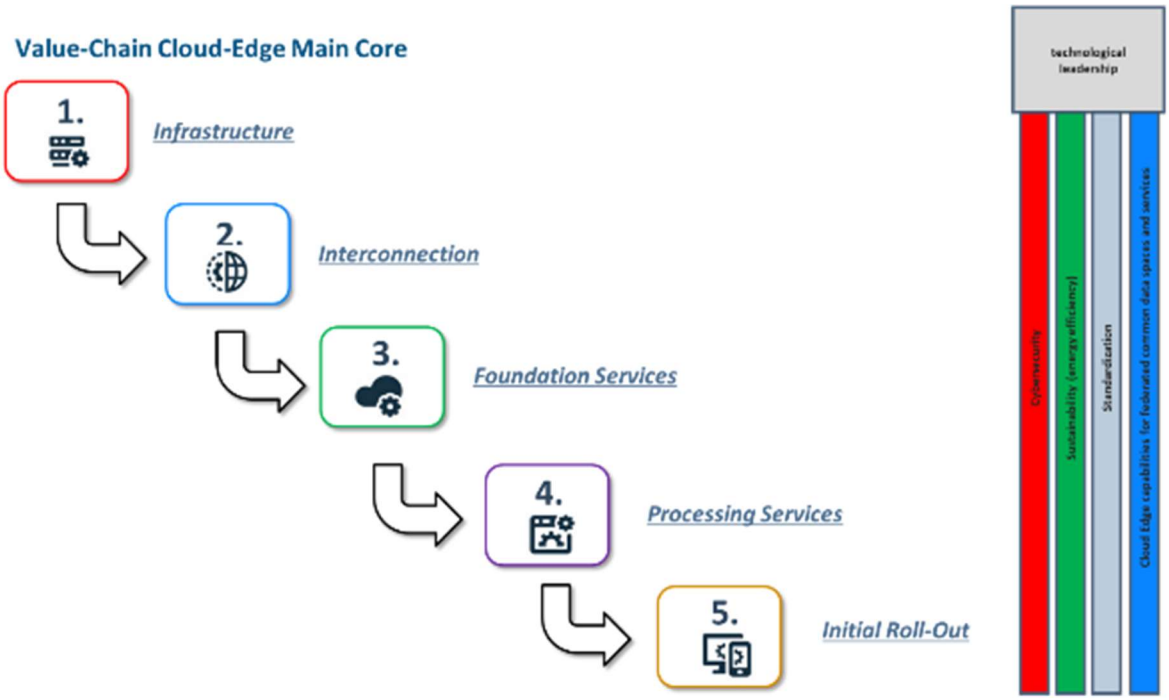
To seize the data opportunity and optimally respond to end-users' expectations in terms of computing capabilities, real-time, ultra-low latency, data security, interoperability and sustainability, the EU needs to become a global leader in data processing (cloud and edge) via investing into the development and first industrial deployment of a highly scalable next generation of cloud-edge infrastructure and services. **The core of the next generation infrastructure and services is the "Distributed Multi Provider Cloud-Edge Continuum"**, which is composed of a common centralized and decentralized data processing infrastructure, smart processing services and platform functionalities that aim at ultra-secure and low power storage, ultra-low latency data exchange and added value creation:

- Companies including SMEs, industrial sectors and public institutions get access to common, highly secure, interoperable and real-time data processing capacities with low power consumption.
- Citizens and businesses are getting better-off with better service delivery.
- New innovative, green business solutions and process efficiencies will be enabled by data processing technologies across the EU and beyond.
- Users can shift between service providers based on data portability while avoiding vendor lock-in.

Such a cloud-edge continuum will be based upon a common Multi-Provider data processing infrastructure, enabling value creation via the use of platform and application services as well as services provided across the EU territory, fulfilling key requirements of latency and bandwidth guarantee, assured data integrity, access security, resilience and sustainability. Boundaries will also disappear between cloud and edge computing in establishing the cloud edge continuum as technological basis for the first industrial deployment of cutting-edge data processing capabilities for key economic sectors such as automotive, manufacturing, energy, logistics as well as for service sectors such as tourism, education or public services (smart cities, health and more). The multi provider cloud-edge continuum will be a pillar for enabling the first industrial deployment of key digital technologies and applications like smart networks and services (e.g. AI), data driven robotics, data spaces applications and cloud-edge federation services.

The goal of the IPCEI on Cloud Infrastructure and Services ("IPCEI-CIS") is thus to develop and first industrially deploy the key interdependent building blocks and the associated transverse requirements (sustainability, cybersecurity) along the strategic value chain of the Distributed Multi Provider Cloud-Edge Continuum.

The value chain logically combines technological features and R&D&I aspects under each of its key building blocks to structure a common integrated project based on multiple projects. In each building block of the value chain and along the entire technology stack (infrastructure, platform, and services) interoperable, reliable and measurable framework conditions in relation to cybersecurity, sustainability, sovereignty, standardization and capabilities as horizontal requirements for a trusted cloud-edge continuum need to be guaranteed. The identified key building blocks and horizontal requirements along the value chain are detailed below:



Step 1: Infrastructure

Data processing in edge and cloud systems need suitable and highly scalable software and compatible hardware packages, this implies far edge data centres, fast energy-efficient next generation processors for data processing and communication, and dedicated components for real-time and security-critical data transfer operations. This IPCEI-CIS also focus on the evaluation of compatible soft- and hardware components. The deployment of advanced services requires significant increases in performance in terms of transmission rates, bandwidth, energy consumption, reliability and real-time capability.

Step 2: Interconnections

Next generation smart processing infrastructures will progressively rely on cloud and edge servers, edge devices and Internet-enabled mobile devices. Their combination will allow low power virtual interconnections among cloud and edge capabilities and their integration into future smart networks. This will enable the management of customer-oriented interconnectivity, interoperability and data or service portability, specific requirements with regard to end-to-end security, low power and ultra-low latency in data transfer and storage, real-time processing, bandwidth availability and load balancing for complex processes. Software Defined Networking (SDN) technologies will improve network transparency and interoperability. The next generation cloud-edge interconnection, including the telco edge computing infrastructure, will bring data processing capacities closer to where end users are physically located, making the multi provider cloud-edge continuum accessible across the EU.

Step 3: Foundation Services

An increasing number of real-world applications, including industrial processes, require the execution of highly specialized functions quickly and without errors. These applications require a high automation degree, ultra-low latency in data processing, reliability, access control, energy-saving options, and need to fulfil strict latency and resilience requirements. The establishment of a common highly automated Operation System, for orchestration e.g. load balancing, latency and resource optimization needs to be

developed. End-to-End Security is necessary while sharing resources and co-locating network functions. By using compute resources outside of the well-established data centre security controls, security challenges emerge both at the level of digital and physical security.

Step 4: Processing Services

Platform Services are cloud-based services where the provider offers to a customer an environment and tools for developing, deploying and managing applications across the multi provider edge-cloud continuum. To set up tailored services and new computing options in an interoperable and portable manner, the meshing of cloud providers, edge operators and infrastructure facilities is required. This is the basis to support the development and first industrial deployment of smart processing services designed to address multiple use-cases, on top of the platform services. These smart processing services will create further value by implementing AI-based technologies (e.g. federated learning), big data services, digital twin approaches, simulation and modelling data services.

Step 5: Initial Roll-out

The progress made in terms of connectivity, latency, data exchange, data processing and computing capabilities through the multi-provider edge cloud continuum enable the deployment of innovative use cases at first industrial deployment stage, showcasing a high scalability and interoperability of services and data in different domains, like manufacturing, energy, mobility, health, and public services. A wide variety of sectors can benefit from digital twins, virtual factories, remote operation and assistance, autonomous robots and other innovative services. The digitalisation of those sectors and industries will generate enormous amounts of data that can be used to maximize economic value. The sharing of data and its combined exploitation through advanced techniques of data analytics and AI, will allow companies and public administrations to build tailored products and services for customers and citizens.

2. Funding principles

Funding must be in line with article 107 (3) b) of the Treaty of the functioning of the European Union and the IPCEI Communication[4]. In this context, the content of the latter therefore forms the basis for this Call for projects and any subsequent project funding. Funding outside the IPCEI framework has to be in line with national legislation, notably the RDI Law[5].

Funding is approved in accordance with (i) the relevant provisions of national legislation, including any administrative regulations or decrees issued for the purpose, and (ii) the IPCEI Communication in the case of an IPCEI project.

Funding is subject to the availability of budgetary resources and approval of the project by the European commission following its notification in the context of an IPCEI project.

No entitlement to funding can be asserted by means of a legal claim.

[4] Communication of the European Commission Criteria for the analysis of the compatibility with the internal market of State aid to promote the execution of important projects of common European interest (2014/C 188/02): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52014XC0620%2801%29

[5] Loi modifiée du 17 mai 2017 ayant pour objet 1. le renouvellement des régimes d'aides à la recherche, au développement et à l'innovation; 2. les missions de l'Agence nationale pour la promotion de l'innovation et de la recherche; et modifiant la loi modifiée du 5 juin 2009 relative à la promotion de la recherche, du développement et de l'innovation: http://legilux.public.lu/eli/etat/leg/loi/2017/05/17/a544/jo

3. Funding object

The funding process aims to significantly contribute to the implementation of the Luxembourg Data Driven Innovation Strategy[6], the Luxembourg Cyber Security Strategy[7], the European Data Strategy[8] and the European Digital Strategy[9]. Accordingly, the following projects are included in the scope of this Call for projects:

1. Projects suiting the general value chain of the IPCEI-CIS, as described in **Section 1** of this Call for projects;
2. Projects suiting a specific part of the value chain as described in **Annex I**.;

These projects must entail:

- **Research, development and innovation** (R&D&I). In the context of the IPCEI- CIS, please note that the R&D&I activities to be funded must clearly go beyond the state-of-the-art in the sector;

  and/or

- **First Industrial Deployment (FID)** of highly innovative technology. Please note that projects comprising a first industrial deployment :
  - can only be funded in the context of a participation in the IPCEI-CIS;
  - must encompass the development of a new product or service with high research and innovation. Regular upgrades without an innovative dimension or the development of newer versions of existing products do not qualify as IPCEI.

Please note that costs incurred prior to the approval of the aid are not eligible for funding and may jeopardize the incentive effect of any aid.

4. Eligibility criteria

The entity requesting funding from the Grand Duchy of Luxembourg must:

- have a permanent establishment in the Grand Duchy of Luxembourg and incur the costs of the project, thereby bearing the risk of the project;
- be able to co-finance the project (*cf. infra*);
- at the time of the grant, not qualify as an undertaking in difficulty, as defined by the rescue and restructuring guidelines[10], or be subject to an outstanding recovery order following a previous Commission decision declaring an aid illegal and incompatible with the internal market;
- during the whole lifecycle of its contribution, comply with the European legislation;

[6] https://gouvernement.lu/de/publications/rapport-etude-analyse/minist-economie/intelligence-artificielle/data-driven-innovation.html
[7] https://cybersecurite.public.lu/fr/securite-information/strategie-nationale.html
[8] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en
[9] https://ec.europa.eu/digital-single-market/en/content/european-digital-strategy

- not be subject to EU extra-territorial legislation affecting the rights granted by the Human Rights Charter, the General Data Protection Regulation, the European legislation on intellectual property rights and the protection of undisclosed know-how and business information

Please note that consortia can apply to the Call for projects. In such a case, all undertakings participating in the consortium requesting funding from Luxembourg must comply with the above criteria and will have to go through the matchmaking and notification process before the European Commission and submit a separate application for State Aid if their project is selected.

The projects to be funded must meet the following requirements:

- The project must fit into the scope of this Call for projects outlined in Section 3;
- The project must fulfil the eligibility criteria outlined in Section 3 of IPCEI Communication, including one or more of the "*Specific criteria*" outlined in points 21 to 22 of the same document (i.e. be a major innovative R&D&I project, or a first industrial deployment with high research and innovation content). Please note in particular that:
    - The project must be co-financed by the entity requesting funding (point 18 of the IPCEI Communication)[11];
    - The project "*must be important quantitatively or qualitatively*", meaning that "*it should either be particularly large in size or scope and/or imply a very considerable level of technological or financial risk*" (point 24 of the IPCEI Communication);
- Without the aid, the project cannot be realised or can only be realized in a smaller size or scope or in a different manner that would significantly restrict its expected benefits;
- The majority of the costs of the project must incur on the territory of the Grand Duchy of Luxembourg;
- The project should not create infrastructures or services that could threaten security or public order of the Union.

In addition, the following criteria are used to select the projects to be funded:

- General funding criteria, in particular:
    - Consistency of the project outline;
    - Cost and funding efficiency and leverage effect;
    - Degree of innovation;
- Timely feasibility of the project;
- Positive outlook regarding the fulfilment of the requirements of the IPCEI Communication, in particular:
    - Contribution to and impact on the competitiveness of the EU, its sustainable growth, social challenges or the added value realised in the EU;

[11] In the future notification process before the Commission, projects that include a significant own contribution will be considered more favorably. Contribution of tangible and intangible assets, as well as land, shall be accounted at market price (Point 38 of the IPCEI Communication).

- Potential cooperation with at least one other entity from one or more Member State(s) participating in the IPCEI (this collaboration might be the outcome of the pan-European matchmaking taking place end of July and September);
- High degree of cooperation in terms of number and diversity of partners;
- High relevance and broad use of the project in the EU economy and society due to positive spill-over effects;
- Great importance in qualitative and quantitative terms and high technological and financial risk.

- Potential capacity to compete on the market in the medium to long-term;
- Contribution to future export opportunities of the technology;
- Participation of innovative small and medium enterprises (SME) or start-ups;
- Integrated approach of the IPCEI-CIS value chain, especially with respect to the potential inclusion of additional project partners.

Projects focusing on basic research as well as public actors that do not individually correspond to the funding object are not eligible for participating in the IPCEI-CIS.

5. Requirements for the project outline

The project outline should be submitted in PDF format and not exceed 20 DIN A4 pages including the cover sheet, excluding potential annexes. The concept description must contain: 1) details that allow the assessment of the project's content and its technical feasibility and 2) a financial plan, which allows to assess profitability and funding gaps related to the project proposal both with and without a State aid.

More specifically, it should provide information on the objectives, the organizational structure, the work programme, the time schedule, the cost / expenditure plan and the funding needs of the project in the light of the current state of research, technology, market, infrastructure and regulatory framework, as well as signal compatibility with the relevant funding criteria and, if applicable, provide indication on the cooperation with other participating companies.

<u>The project outline should follow the following structure:</u>

1. Cover sheet with project title, basic information of the applying company and details of the main contact person and one proxy (names, telephones, email addresses);
2. Summary of the project: title, keywords, applicant, project location, objectives with quantifiable key figures, brief description, overall timeline (start and end date), costs and funding amount. Detailed technical descriptions are not necessary in this section;
3. Presentation of the project:
   a) Detailed time and work schedule, milestones and interim goals of the project;
   b) Investment and financing plan, including rough cost estimation classification and budgeting in the form of a tabular financial overview (with specification of types of costs, own vs. third-party funds, person-months and, if applicable, additional costs / expenses, including operating costs). Where relevant, a clear breakdown between costs for (each of) the R&D&I activities and costs for (each of) the FID activities should be provided in a disaggregated manner. For costs arising from FID activities, the potential costs of R&D&I

carried out should be mentioned specifically in order to provide an indication of the overall importance of the R&D&I;

c) Presentation of the funding requirement and funding gap. (In case additional frameworks are necessary in addition to the IPCEI funding for the implementation of the project, these should also be explicitly stated);

d) Comments on the existing or potential connection of the project to (European) value chains as well as to up- or downstream activities or sectors (if applicable, participating partners as well as structure and status of the cooperation, strategic starting position of the partners involved, coverage of the value chain, supply and demand structure, etc.);

4. Justification of the necessity and adequacy of state funding (incentive effect of the aid), with regard to the technical and economic risk. This should include a clear description of the counterfactual scenario in the absence of the aid. The counterfactual scenario may correspond to a situation where there is no alternative project or a project that would be realised in a smaller size or scope, or in a different manner;
5. Estimation of the competitiveness of the project in the medium- to long-term on the regular market (specifying the expected boundary conditions);
6. Where relevant, remarks on the sustainability and environmental friendliness of production, transport and reutilisation measures foreseen in the project (if available, description of the greenhouse gas mitigation potential and comparison to alternative processes);
7. Intended spill-over effects (national and European) in terms of scientific-technical, economic and social contribution(s), support in strengthening Europe as a centre of commerce and industry (indication of activities with target location, target audience, content). Ideally a plan regarding knowledge dissemination should be provided, indicating in what form and to what extent (e.g. IP protected results, non-protected results, etc.) information about the project's results will be made available;
8. Assessment of the effects on the internal market (positive and negative effects), remarks on possible market distortion;
9. Other relevant information regarding the eligibility criteria mentioned in Section 4 of this document;
10. Disclosure of previous requests or approvals for state aid at national or EU level;
11. Self-declaration that the applicant(s) is(are) not subject to extra-territorial legislation affecting the rights granted by the Human Rights charter, the General Data Protection Regulation, the European legislation on intellectual property rights and the protection of undisclosed know-how and business information.

All information submitted will be treated confidentially. Projects that are invited to participate in the matchmaking process will however need to share sufficient information to make it possible to link the different projects and initiatives at EU level. The parties concerned will have the opportunity to approve the information that can be shared.

Application as a consortium:

Undertakings can also submit their documents as part of a consortium, possibly as an integrated proposal. In this case, the separate presentations of the projects from the participating companies should be

preceded by a general part, which contains in particular the joint programme, roadmap, project phases and timeline, as well as the information that applies equally to all individual projects.

Financial information should also be presented separately for the individual projects, in particular the indications listed in this section under items 3., letters b) and c) and 4., as well as the information directly related to the IPCEI notification, in particular items 7. and 8., and the self-declaration according to item 11. The decision about the agreement of an aid and its amount will be made separately for each applicant.

For the scope of a joint application, the maximum number pages stated above applies to each participating entity, not to the total length of the joint application.

6. Deadline for participating in the Call for projects

Applicants can submit their short project outlines expressing interest for funding by email to the following address, which also serves as a point of contact: IPCEI-CIS@eco.etat.lu.

Complete applications are to be sent until the **15th of July 2021** at the latest.

Late submission of a project can only be accepted in exceptional cases, provided that the project is of particular importance for achieving the goals above and that it does not cause a delay to the process agreed between the Member States and the Commission. Successful applicants will receive detailed information on how to proceed at a second stage of the process. Project executing organisations can be appointed to support during the operational implementation phase of the forecasted funded project.

7. Preliminary schedule for the IPCEI process

Subject to change, the preliminary schedule for the IPCEI process is as follows:

- **Deadline for submitting projects at national level: 15th of July 2021**

  As the matchmaking event might change some aspects of the project, its description may be subject to subsequent modifications. Any application to this call for projects should however contain the information specified in article 14 (2) of the RDI law[12].

- Companies **are not allowed to start the project** before being officially notified by the ministry of the Economy.
- Companies intending to participate should inform the Ministry via IPCEI-CIS@eco.etat.lu in order receive further information about matchmaking and organisational matters
- During June, information meetings will be organised.
- Matchmaking at national and especially at EU level between July and September 2021 (a joint “Fact Sheet” template will be provided at EU level to shortly describe the projects)
- Start of pre-notification: November 2021. At this point, all the necessary national and European forms must be finalised.
- Notification to the European Commission: Q1 2022
- **Earliest date for project acceptance: Q2/2022**

[12] http://legilux.public.lu/eli/etat/leg/loi/2017/05/17/a544/jo

Annexes:

1. **Cyber security projects**

Annex I - Cyber security projects

Introduction

Cyber security services and solutions are fuelled by high quality data about threats, their modus operandi, vulnerabilities and their way of exploitation.

Problem 1 – technical security

Technical security is about identifying and mitigating threats without disrupting legitimate business processes and without disturbing users. The common approach is to create tools that scan for known threats. However, since threats are constantly changing their appearance or the way they work (sequential attacks versus phased attacks, main target attacks versus supplier attacks) it is exceedingly difficult to integrate malware signatures or indicators of compromise into the tools in good time. If these description patterns are not available, attacks will not be recognized[13].

The cybersecurity skills shortage[14] greatly aggravates the challenge entities face to secure their systems. Due to the lack of available profiles, or lack of budgets, companies are unable to recruit experts and tend to externalise cybersecurity services to Security Operations Centre (SOC) providers that implement and monitor technical cybersecurity solutions of their customers.

Monitoring of the network and systems is necessary, because technical security solutions only automatically block known malicious activities in order to not disrupt business processes. For this reason, skilled cyber criminals try to obfuscate[15] their attacks and adopt evasive measures to prevent their attacks from being detected and mitigated automatically.

This adaptive behaviour of cyber criminals forces SOC operators to collect, store and analyse the logs (network, end-point, firewall, Intrusion Detection Systems, ...) of their customers and investigate low level security alerts to re-classify them if necessary and start an investigation to gather Indicators of Compromise (IOC) and implement curative measures accordingly (threat hunting). This process is complex and ties up a lot of resources and is, as a service very expensive[16]

[13] Please refer to the ENISA countermeasures handbook for detailled explanation: https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/developing-countermeasures-handbook/view

[14] https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union

[15] https://www.enisa.europa.eu/publications/etl2015

[16] https://www.enisa.europa.eu/publications/proactive-detection-good-practices-gap-analysis-recommendations - chapter 2.3. gap analysis - page 12

A skilled SOC team, with access to accurate and timely threat information, operating a modern technical cybersecurity infrastructure can achieve a high level of security.

This quality of service is however unaffordable for the vast majority of companies, especially SME. Even medium quality SOC, with less skilled or fewer experts, come with a high entry price[17] as the customer has to acquire the necessary hardware like network tabs, switches, servers and the necessary software licenses SOC operators need to collect and analyse network traffic and device log data.

Problem 2 – organisational security

Organizational security, especially risk management, depends on high-quality cyber weather data. Based on incorrect or incomplete information, incorrect governance decisions are made regarding the implementation and configuration of preventive, protective and reactive measures.

Problem 3 – territoriality of CSIRTs

Incident response management aiming at analysing, containing and eliminating cybersecurity threats from a compromised entity is mostly organized in a territorial way (country or sector of activities).

Most countries have various incident response teams, often the legal status, the missions and the responsibilities are very diverse[18] These teams are today not well equipped to manage incidents in the cloud. They face the following major challenges[19]:

- Legal issues including multiple ownership, multiple jurisdictions, and multiple tenancies;
- Limited access to remote and distributed physical infrastructure and storage;
- Lack of physical control and physical location of data;
- Lack of collaboration from the cloud provider(s);
- Segregation of duties among cloud actors;
- Difficulties in accessing and analysing the log data / lack of transparency of log data to the consumer;
- Proliferation of mobile devices and endpoints.

Most CSIRT teams for sure lack the capabilities for handling cross-border and cross-constituency incidents.

“In today's more and more interconnected world, cyber-attacks that involve several victims in more than one country (aka cross-border cases) become increasingly common - and so does cooperative international incident handling. Although this kind of joint effort constitutes a very helpful means for handling severe cases, it is also very complex and challenging.

These challenges originate not only from the particularities of the victims' organizations in the different countries, but are also caused by the characteristics of the helpers in their respective environments. Correspondingly, current cases show that there is still room for improvement regarding the collaboration of all involved parties in these kinds of incidents and that the implementation of agreed international incident handling operating procedures (I2HOP) has the great potential to considerably improve this process. That there is, in fact, a need for standardized procedures when it comes to coordinated incident

[17] https://www.enisa.europa.eu/publications/proactive-detection-good-practices-gap-analysis-recommendations - page 12

[18] https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map

[19] Exploring Cloud Incidents https://www.enisa.europa.eu/publications/exploring-cloud-incidents

management (nationally and internationally) is also reflected by the current efforts of the International Organization for Standardization (ISO) to implement a respective part for the ISO/IEC 27035 standard."[20]

Since the introduction of GDPR, it is still difficult for a CSIRT to query contact data for a given domain name or IP address[21]. These queries are however very important in order to contact potential victims of data breaches or cyber security incidents.

Problem 4 – High costs for cybersecurity

Especially SMEs suffer from an inadequate degree of awareness of the high level of threats and a lack of understanding and use of cybersecurity tools.[22] Furthermore, the lack of a dedicated budget also makes it difficult for SME to acquire the most advanced cybersecurity tools and in the case of acquisition of cybersecurity tools, the lack of specific skills for their implementation or management often makes the investment futile.[23]

SME are forced to use unattended automatic technical cybersecurity solutions that only provide a limited degree of security. They cannot afford SOC services, because firstly they can't pay for the preliminary investments needed for the acquisition of the necessary hardware and software licenses and secondly because of high price of SOC services, which is due to the the low level of automation within the SOC.

SME could save the costs of hardware for SOC services by on-boarding cloud services. However, their low awareness of the cyber secuirty challenges and the detriments[24] they face in cloud contracts prevent this.

SME are rarely covered by sectoral CSIRT teams (banking, energy, ...), they can't afford private contracts, they start having difficulties subscribing to cyber insurance contracts as they can't match the increasingly strict conditions. SME might get help from governmental financed CSIRT teams, but they are very hard to contact (vulnerability management, breach notification).

SME have no access at all to risk management. They do not have either the methodological knowledge nor do they have the necessary information to manage their risks. Their decisions in cybersecurity are fully based on assumptions and they are at the mercy of their cybersecurity provider.

Vision

Security breaches increase in numbers and severity every year, which indicates that companies either increase their digital footprint, that they buy the wrong services or products, that the products do not provide decent protection, or that the latter are misconfigured**. Intense collaboration in threat and vulnerability sharing could free scarce resources in cyber security and make them available to better design, implement and configure cyber security solutions and services**. **Cyber security services must stay affordable if the data driven economy is to become a success.**

To enhance collaboration, the call for projects seeks in specific parts for the creation of innovative open source solutions to enhance collaboration while enforcing a high level of security assurance.

---

[20] International Incident Handling Operating Procedures - BSI - https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/CERT-Bund/Links/links_node.html

[21] https://www.circleid.com/posts/20210119-whois-record-redaction-and-gdpr-whats-the-evolution-post-2018/

[22] PWC - Study on the Scale and Impact of Industrial Espionage and Theft of Trade Secrets through Cyber - page 20

[23] PWC - Study on the Scale and Impact of Industrial Espionage and Theft of Trade Secrets through Cyber - page 20

[24] https://ec.europa.eu/info/publications/study-economic-detriment-small-and-medium-sized-enterprises-arising-unfair-and-unbalanced-cloud-computing-contracts_en

Description of potential projects that enhance collaboration

"Open source" means: created and published under a copy left license like

EUPL or GPL.

1. Resource ledger, authorisations and mandates

Currently there is no normalized way of contacting cloud providers or even classic hosting providers, which is a pain point for legal inquiries such as take down notices, evidence acquisition, etc. Often legal bodies or CSIRT must go through unstructured email, phone calls or fax to send these queries, and only receive late replies, if any. In a highly distributed cloud environment spanning over multiple infrastructure providers and borders, these issues will become an even bigger bottleneck due to the high volatility of the targeted resources, which can freely move through the cloud-edge continuum.

New standardised ledger technologies, based on eIDAS trusted services, need to be developed to manage contracts and mandates of customers, cloud providers, SOC service providers and CSIRTs. This service will document where the services of cloud customers are instantiated within the European cloud continuum and allow SOC service providers to adapt their protective services accordingly, CSIRTs can find the instantiated services of their constituency.

Cloud customers can take full advantage of the elasticity of the European Cloud Continuum as SOC service providers and CSIRTs will be easily capable of following the movements of their customers.

To achieve this goal, a normalized and API-based way of sending such requests should be developed. Authentication and signatures should be based on eIDAS trusted services[25] and eIDs[26] [27] for the assurance level "high".

The authorizations would be granted based on criteria such as:

- country of operation of the legal body and targeted resource
- specific agreement between the resource holder and the legal body (e.g. in case of a private entity asking for a CSIRT investigation)
- agreement with CSIRT responsible for the headquarter of the entity or any other territorial CSIRT willing to share or cooperate with another legal body of any other member country
- agreement between a resource holder and a private entity such as SOC or cybersecurity professional
- ...

Based on such a resource ledger and associated authorization list, cloud providers could readily assess if an inquiry is valid, and would have at hand the base requirements to programmatically expose services or evidences or data acquisition would it be network capture, disk or memory dumps or any other technical items of interest.

2-1 Project proposal: Distributed resource allocation, authorisations and smart contract ledger

Design and implement an **open source ledger** (not necessarily on blockchain) and related **APIs** to document in real time at least the following information:

[25] https://webgate.ec.europa.eu/tl-browser/#/
[26] https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS
[27] https://digital-strategy.ec.europa.eu/en/policies/trust-services-and-eid

- Cloud-edge continuum resources used by a customer
- Cloud-edge continuum access rights (granted to SOCs, CSIRTs or other entities)
- Smart contracts for managing the above as well as territorial hand-overs or collaborations

The cloud customers can grant their respective cyber security providers access to their data, enabling them to secure the possibly very dynamic perimeter (e.g., cross-cloud or cross-country) and to perform a mandated intrusion test, for example. In the same spirit, the cloud customers can grant acces to CSIRTs in the case of incidents.

This authorisation system should take advantage of "smart contracts technology" and offer the possibility of contract hand-over if a CSIRT or SOC does not operate in a country where the customer movers his cloud services to. At least two assurance levels of the existing three (basic, substantial, high) should be foreseen. The assurance level "high" will require eIDAS trusted services and eIDAS eID for authentication and contract signature.

2. Security Operations Centre

The evolution of cyber threats since the 1988 Morris worm[28] is breath taking[29]. Cybercrime has professionalised[30] and is offered today "as a service"[31]. Its fast evolution is due to the abundance of badly protected IT systems, the broad usage of single factor authentication mechanisms and the avenue of foolproof criminal business models based upon ransom-ware[32] and crypto-currencies[33] since 2013.

The number of cyber-attacks is rising[34] at a huge pace and SMEs are particularly but of course not the sole victims of those attacks as they are "generally more vulnerable to cyber threats"[35].

The cybersecurity skills shortage[36] greatly aggravates this situation. Due to the lack of available profiles or lack of budgets, companies are unable to recruit experts and **tend to externalise cyber security services**.

2-01 Sensors and Log Collection API

There is no standardised way of accessing customer or infrastructure log data from cloud providers to feed customer-side Security Information and Event Manager (SIEM) to implement high security standards. The European Cloud Certification Scheme (ECCS) is not solving this issue, as it only requires the existence of logs and log interfaces, depending on the certified assurance level. The ECCS neither harmonizes nor does it define minimum criteria for log quality[37].

[28] https://en.wikipedia.org/wiki/Morris_worm
[29] https://cybersecurityventures.com/the-history-of-cybercrime-and-cybersecurity-1940-2020/
[30] Europol: INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2020
[31] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2019.pdf
[32] https://en.wikipedia.org/wiki/Ransomware
[33] Europol: INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2020
[34] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2020/cyber-security-breaches-survey-2020
[35] PWC - Study on the Scale and Impact of Industrial Espionage and Theft of Trade Secrets through Cybe - page 12
[36] https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union
[37] https://www.enisa.europa.eu/news/enisa-news/cloud-certification-scheme - OPS 13

2-01-1 Sensors - SOC blind spots

Develop open source sensors and look for synergies with the projects D4[38] and AIL[39] [40].

In computer networks, computers and other network appliances usually act as sensors by providing logs. These logs only participate to the awareness of the device's services status: a device will only report about the status of the services and protocols it provides and uses. Relying on these logs only means there are blinds spots in organization's situational awareness. Even worse, sometimes devices use services that administrators do not actively monitor because of their novelty. Some very well known examples of such issues is the unnoticed exploitation of ipv6 services on ipv4 networks, (see https://blog.fox-it.com/2018/01/11/mitm6-compromising-ipv4-networks-via-ipv6/) and the use of forbidden radio channels (see the additional Japanese wifi channel for instance).

There is therefore some value in monitoring the use of services, protocols and signals that are not actively 'in use' within an organization, and between organizations.

There is no open source mean today that provides the capability to build sensors to monitor these blind spots: removing the unknown unknowns in our organizations' SOC operations.

In order to fill this gap, an open source software stack should be developed to enable low-cost devices (single boards computers in the price range of latest raspberry pis, given the proper peripheral) **to monitor several aspects of our environment.** The goal is to understand if given services, bands, and protocols are provided, requested, or denied in the vicinity of the sensor. **In particular the sensors should be able to discriminate services, bands or protocols and give a measure of the amount of traffic, and when applicable, power**:

- all network protocols carried on Ethernet based network,
- all IP and TCP protocols used on management backplane especially cloud-based infrastructure or SDN,
- all Wifi bands, access points, and clients,
- all cellular networks generations, cells and clients,
- all Bluetooth bands, server and clients,
- most protocols carried on 315MHz, 433MHz, and 868MHz (ISM bands).

These devices should report their live measurements to a central node by using API-LC and/or support open protocols such as the [EU-funded D4 Project](https://github.com/D4-project/architecture/tree/master/format) protocol.

2-01-2 Log collection

Develop an open source standard API-LC for log collection. This API should be able to interface with current proprietary cloud provider API, with the developed sensors, as well as with end-point event and/or security logs. An end-point agent interfacing with the API-LC for at least one OS can be developed as well.

This API-LC will be adapted to the needs of the cloud-edge continuum as soon as the technical specifications will be available.

[38] https://d4-project.org/
[39] https://github.com/ail-project/ail-framework
[40] https://www.circl.lu/projects/

2-02 Log Storage and log manager

Develop an open source, cloud-based, platform independent, multi-tenant log storage and log manager. This can be extended with the appropriate research to the [3-01 CSIRT evidence manager]

Logs as well as sensor data (2-01-1) acquired via API-LC must be stored through an open source cloud based and platform-independent API (API-LS) into a platform-independent log storage and management system (**LSM**). The latter must properly separate logs obtained from different sources (e.g., with containers). This manager should help entities to comply with GDPR and manage collaboration with customers, other SOCs (national or cross-border initiatives), and CERTs (national and cross-border). Access to the logs will be subject to the existence of a valid authorisation. Check of authorisations is done via the **[1. Distributed resource allocation, authorisations and smart contract ledger]**.

The log manager should also be able to calculate costs that will be charged to each entity that is using the service. The LSM should be run by the cloud provider.

In edge cloud environments, due to the reduced storage capacities, specific reflections should be led.

2-03 SOC Tools

Develop open source SOC tools. With the creation of these SOC tools, Luxembourg intends to achieve several goals:

- Reduction of the price of services for SME due to absence of license fees.
- Foster intense collaboration between SOC teams in terms of threat information sharing via MISP[41] and the [**cyber security data space]**.
- Facilitate load balancing between teams in times of heavy workloads (such as in crises).
- Facilitate training.

The developed tools must support the achievement of these goals.

2-03-1 SIEM

Creation of a platform independent **open source SIEM** that runs a separated (containerized) instance for each customer. The SIEM processes logs stored in the **LSM** (the log storage and management system). Access control is based on authorisations granted by **[1. Distributed resource allocation, authorisations and smart contract ledger]** providing intra-SOC and cross-SOC collaborative possibilities and assuring live links to MISP as well to the Cybersecurity Data Space [**5. Cyber Security Data Space**]. The collaboration is encouraged through sharing of information (e.g., indicators of compromise) with either a regional, sectorial, national or European Data Space, or with other SOCs on a contractual level (depending on the decisions made by the data controllers with respect to the allowed spreading of the information). The sharing is made possible via APIs.

- Creation of a new taxonomy galaxy in MISP that can be interfaced via API by a machine.
- The SIEM should be able to interface with MISP (and other SIEMs run by other SOCs) in order to export events to enhance sharing and fostering the possibility to generate threat intel.
- The SIEM should be able to automatically update sighting of specific events in MISP (specific events, critical vulnerabilities, malicious campaigns, crisis statistics, …).
-

[41] https://www.misp-project.org/

2-03-2 from SOC to Intel

Development of next generation of digital services, to define and implement an interoperable framework that assists in the detection, modeling, sharing and remediation of cyber security incidents (including sharing of indicators of compromise (IoC), signatures, rules, remediation advices …).

Creation of intel should be based on MITRE ATT&CK matrix to foster interoperability. Do the necessary R&D&I to develop and implement algorithms to 1) extract risk scenarios from incident data and 2) estimate threat probabilities from data available in the cyber security data space.

2-03-3 from SOC to Action (not open source)

Develop classic or AI enhanced systems, based upon the **2-03-1 SOC tools,** to detect and recognize the cyber threats, to propose or trigger appropriate response, and pro-actively help to adjust security parameters to avoid breaches within the cloud. Create the necessary links to MISP and the **[5. Cyber Security Data Space].**

3. Computer Security Incident Response Team

3-01 Evidence Storage and evidence Manager

Integrate in [2.02] standards how logs are being dealt with to be able to be used as evidence in court.

Based on 2.02 [LSM], define a candidate standard on how logs (API-LC) as well as all other potential evidence must be handled to make it admissible in court.

Develop, based on 2.02 [LSM] an open source, platform independent, multi-tenant evidence storage, evidence manager and evidence collaboration platform. This platform should foster collaboration between CSIRTs within a cloud-edge continuum. Multiple platforms should be able to coexist and exchange information amongst themselves. Create the necessary links to MISP and the **[5. Cyber Security Data Space].**

Evidence acquired via API-LC must be stored through an open source API (API-EV) to a platform independent evidence storage and management system (**ESM**). The latter must properly separate evidence coming from different sources (e.g. through containerization). This manager should help entities to comply with GDPR and allow collaboration with customers, other CERTs (national or cross-border initiatives) or SOCs (national and cross-border). Access to the evidence will be subject to the existence of a valid authorisation. Check of authorisations will be done via the **[1. Distributed resource allocation, authorisations and smart contract ledger]**.

The evidence manager should also be able to calculate costs that will be charged to each entity that is using the service. The LSM should be run by the cloud provider.

In edge cloud environments, due to the reduced storage capacities, specific reflections should be led.

3-02 Open Source CERT tools

3-02-1 forensic tool sets

Creation of an **open source**, platform independent and containerised (for proper customer separation) **Forensic toolset** that is connected to both the **ESM**, the evidence storage and evidence management platform, **and LSM**[42], the log storage and log manager. Access control will be based on granted

[42] Access to operational security data can be of utmost importance for the management of an incident.

authorisations according to **[1. Distributed resource allocation, authorisations and smart contract ledger]**, providing intra-CERT and cross-CERT collaborative possibilities and assuring live links to MISP:

- Creation of a new taxonomy galaxy in MISP, that can be interfaced by a machine via API.
- The Forensic Tools should be able to interface with MISP. They should be able to export events and thus foster sharing and generating threat intel.
- The SIEM should be able to automatically update sightings of specific events in MISP, such as critical vulnerabilities, malicious campaigns, crisis statistics …).

3-03 Open source CERT collaboration platform

Develop a cloud-platform that fosters the collaboration of multiple CERTs on one event. This independent and containerised **collaboration platform must be** connected to the Forensic toolset, the **ESM** (evidence storage and evidence management platform) **and LSM** (log storage and log manager). Access control will be based on authorisations granted according to **[1. Distributed resource allocation, authorisations and smart contract ledger]**, providing intra-CERT and cross-CERT collaborative possibilities and assuring live links to MISP. The platform should enable massive cross-CERT collaboration and coordination.

4. Automatic end-point protection

Cloud-delivered endpoint security solution should include risk-based vulnerability management and assessment, attack surface reduction, behavioural-based and cloud-powered next generation protection, endpoint detection and response (EDR), automatic investigation and remediation, and managed hunting services. These solutions should be easily deployed, configured, and managed with a unified security management experience.

4-01 Non-Cloud end-point protection

Develop a system to provide these kind of services from a cloud based SOC and/or CERT to a non-cloud endpoint, also suitable for SME. A link to API-LC must exist. Create the necessary links to MISP and **[5. Cyber Security Data Space]**.

4-02 Edge protection

Develop a system to provide these kind of services from a cloud based SOC and/or CERT to a cloud-edge. A link to API-LC must exist. Create the necessary links to MISP and **[5. Cyber Security Data Space]**.

5. Cyber Security Data Space

5.01 Cyber Security Data Space governance

A Cybersecurity dataspace would allow to develop new security services. It would also enable more research on possible innovative technologies that require real life data to be designed. That's in particular the case for advanced statistical modelling of threats and risks related behaviours.

To allow such activities to take place, several generic services have to be implemented. As they don't exist yet, it's difficult to rely only on market mechanisms to fund them. They have to be bootstrapped through public-private cooperation.

The following governance requirements have been identified and are to be developed in a project and implemented in a First Industrial Deployment upon two redundant physical nodes:

- **Security framework** : there will be a need to develop a framework for designing and implementing a "DS-ISMS". It may have two levels : requirements for the Dataspace "coordinator", and requirements for the Dataspace participants.
- **Contractual framework** : There has to be generic obligations, and possibly contract templates, that will allow participants to easily build a layer of "legal safety" while interacting as providers and customers.
- **Conflict resolution framework** : the dataspace would increase its usage value for participants if it were able to provide a mechanism facilitating conflicts resolution. That would increase the overall efficiency of the interactions between participants as they would not need to systematically involve the more formal judicial institutions. It's particularly sensitive in the security realm as it's not well covered by the assurance industry and this increases the likelihood of damage coverage through civil law procedures.
- **Services catalog** : a dynamic discovery and broadcast of offered services. This is particularly important to ensure that the providers quickly find customers, and customers easily know if there is any provider able to fulfill their needs.
- Quality assurance mechanisms : these would be testing services that allow to ensure the reality and quality of the services proposed by participants. It can be related to the contractual framework and the conflict resolution framework.
- **Privacy enforcement framework** : this is required at two levels. The first is the datasets processing by third parties, and the second is the protection of the dataspace users' privacy. This will require anonymisation mechanisms to be put in place.
- **Intellectual property protection framework** : this should ensure that only what can be shared is shared, and that there is no risk of having intellectual property infringed through the exposure of data or information when services are being rendered.

Several use cases can be defined, which would allow to highlight how useful would be such a security dataspace.

- **National SOC data** to enhance collaboration and strengthen effectiveness of detective and protective services (see 5.1).
- **Smart regulation** : a NIS related regulator could access aggregated data in real time, in order to spot any emerging incident of national importance. The mechanism would have to be designed in a way that doesn't permit the regulation authority to pinpoint any of the contributing (and regulated) entity.
- **Security innovation** through access to real-life data : in constrained domains (example : health, finances...) researchers need to access real-life data in order to develop advanced statistical models, in particular for incident or fraud detection purposes. But this is not possible in the present context as it requires them to establish bilateral agreements and specific protection mechanisms for each possible partners providing the data. With a properly designed dataspace this could happen in a more automated and standardized way. Researchers would then focus their resources on experimenting with the data rather than to search for them. »

5.2. SOC data in the cybersecurity Data Space – national SOC

Luxembourg SOC dataset will be referenced within the cybersecurity Data Space. This dataset contains information about events flagged as being suspicious respectively malicious by a Luxembourg SOC operators. The client-side anonymization of this data will allow a broad sharing of the data.

- Define an open data structure to store SOC data within the SOC data lake (all IP rights let).

- Define API and functionalities to feed the data structure with customer-side anonymized data from a SIEM (2-03-1).
- Define a MITRE Att&ck mapper to describe the kill-chain of the event documented.
- Develop an **open source** API to query the data set for either specific Indicators of Compromise.
- Develop an **open source** API to extract all IOC matching specific kill chain situations.

6. Open source security assurance

Individuals and Organizations are getting hacked every day because of the lack of trust in code ownership, the centralized source of software providers, their dependencies, and its delivery. This leads to millions of computers compromised and millions of euro loss.

The fast pace of Technology innovation (Cloud, IOT, Fog Network, Serverless …) of software development and continuous delivery isn't suited anymore with the traditional Security model, that is not secured by design.

Design and develop an **open source** system necessary to build a community that provides guidelines and maintains a suite of Open Source tools to build trust and secure ecosystems where building, delivering and using software will be done with the confidence of not being compromised or altered by an unknown source.

These Tools, principles and practices will be integrated into any Software Development Life Cycle (SDLC) including GitLab-CI, etc ... on-premise or in the Cloud and will use the state of the art in cryptography, peer to peer networking, and blockchain technology to ensure the best practices of the software supply chain for big and small players.