[4. Members of the consortium 1](#_Toc464754480)

[4.1 Participants (applicants) 1](#_Toc464754481)

[4.1.1 SIListra Systems GmbH (TUD) 1](#_Toc464754482)

[4.1.2 Sync Lab S.r.l. (SYNC) 5](#_Toc464754483)

[4.1.3 EXUS Ltd (Exus) 7](#_Toc464754484)

[4.2 Third parties involved in the project (third party resources) 8](#_Toc464754485)

[4.2.1 SIListra Systems GmbH (SIL) 8](#_Toc464754486)

[4.2.2 Sync Lab S.r.l. (SYNC) 8](#_Toc464754487)

[4.2.3 Exus (Exus) 8](#_Toc464754488)

[5. Ethics and Security 9](#_Toc464754489)

[5.1 Ethics 9](#_Toc464754490)

[5.2 Security 9](#_Toc464754491)

[Annex 1: Drafted Coordination Agreement 10](#_Toc464754492)

[References 16](#_Toc464754493)

# Members of the consortium

## Participants (applicants)

### SIListra Systems GmbH (TUD)

| SIListra Systems GmbH | | | |  | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| http://silistra-systems.com/ | | | |
| **Short name** | SIL | **Type** | SME | **Country** | D | **Partner no.** | 1 |
| **General description of the organisation** | | | | | | | |
| **SIListra Systems GmbH (SIL)** is an IT company (SME) focusing on functional safety and security. Its core competence is the simulation and detection of hardware execution errors which could harm both safety and security of a given (embedded) system. Across several industry sectors, SIListra Systems is well-known for being experts in Software-based Failure Injection and, especially, Software Coded Processing – a software technique allowing to fulfill highest requirements of industry standards for functional safety and requirements for security. SIListra Systems was founded in 2012 as a spin-off from the Technical University of Dresden. | | | | | | | |
| **Name and Description of the Department(s) contributing to the execution of the Project** | | | | | | | |
| **Research and Development** | | | | | | | |
| **Main attributed tasks and role in the project** | | | | | | | |
| SIL will coordinate and build the secure container infrastructure and ... | | | | | | | |
| **Relevant skills and previous experiences** | | | | | | | |
| ... | | | | | | | |
| **Profile description of key personnel carrying out the work** | | | | | | | |
| **Dr. Martin Süßkraut** (m)is co-founder and Head of Research and Development of the SIListra Systems GmbH. Before that he worked as project manager and researcher at Technische Universität Dresden. He received his degree as Dr.-Ing. in 2010 from the same university. His research interests focus on software implemented fault tolerance and source code quality. He also worked as software developer for IBM and Siemens**.**  **Prof. Dr. Christof Fetzer** (m) (consultant) has received his diploma in Computer Science from the University of Kaiserlautern, Germany (Dec. 1992) and his Ph.D. from UC San Diego (March 1997). He then joined AT&T Labs-Research in August 1999 and had been a principal member of technical staff until March 2004. Since April 2004 he heads the endowed chair (Heinz-Nixdorf endowment) in Systems Engineering in the Computer Science Department at TU Dresden. He is the chair of the Distributed Systems Engineering International Masters Program at the Computer Science Department. Prof. Dr. Fetzer has published over 150 research papers in the field of dependable distributed systems, has won five best paper / best student paper awards (DEBS2013, LISA2013, CLOUD2014, SRDS2014, DSN2015) in recent years.  **Dr. André Martin (M)** (consultant)graduated with a Diploma (2008) and a PhD in Computer Science (2015). In his doctoral thesis, he explored novel mechanisms for low overhead fault tolerance in data streaming systems. He has been selected twice as a DEBS challenge finalist in 2014 and 2015 and won the UCC Cloud Challenge award in 2014. His expertise includes in cloud computing, distributed systems, elasticity and fault tolerance in large scale data processing systems.  **Dr.-Ing. Irina Karadschow** (F) (consultant)is a project coordinator/ manager. Dr. Karadschow has extensive experiences in managing and coordinating EU, BMBF, DFG, AiF and BMWi- funded research projects. She has received her Magister degree (2002- Industrial Management) at the Technical University Sofia, her Diploma degree (2005- Business Administration and Management) and her Doctor title (2015 Mechanical Engineering) at the Technical University Dresden. | | | | | | | |
| **Publications, other research or innovation products, or patents related to the project** | | | | | | | |
| |  |  |  | | --- | --- | --- | | **No.** | **Title of Publication or Name and Short Description of the Product/Service** | **Relevance for the Project** | | 1 | Sergei Arnautov, Bohdan Trach, Franz Gregor, Thomas Knauth, André Martin, Christian Priebe, Joshua Lind, Divya Muthukumaran, Daniel O'Keeffe, Mark L Stillwell, David Goltzsche, Dave Eyers, Rüdiger Kapitza, Peter Pietzuch, Christof Fetzer, „SCONE: Secure Linux Containers with Intel SGX”, Usenix OSDI, 2016. | Describes the secure container approach. | | 2 | Dmitrii Kuvaiskii, Oleksii , Sergei , Bohdan Trach, Pramod , Pascal Felber, Christof Fetzer, “SGXBounds: Memory Safety for Shielded Execution”, submitted | Describes how to ensure memory safety to protect programs against attacks. | | 3 | Stefan Brenner (TU Braunschweig), Colin Wulf (TU Braunschweig), Matthias Lorenz (TU Braunschweig), Nico Weichbrodt (TU Braunschweig), David Goltzsche (TU Braunschweig), Christof Fetzer (TU Dresden), Peter Pietzuch (Imperial College London), Rüdiger Kapitza (TU Braunschweig), „SecureKeeper: Confidential ZooKeeper using Intel SGX“, Middleware 2016 | Describes our experience with SGX. | | 4 | Rafael Pires (University of Neuchatel), Marcelo Pasin (University of Neuchatel), Pascal Felber (University of Neuchatel), Christof Fetzer (TU Dresden), “Secure Content-Based Routing Using Intel Software Guard Extensions”, Middleware 2016. | Describes our experience with SGX. | | | | | | | | |
| **Relevant previous projects/activities** | | | | | | | |
| SIListra Systems is a project partner of the BMFT FAST project (<http://de.fast-zwanzig20.de/)>. It participates in the sub-project FastCloud (<http://de.fast-zwanzig20.de/konnektivitaet/fast-cloud/)>. Within FastCloud, SIListra focuses on secure and resilient cloud computing. The approach investigated within FastCloud is complementary to the approach investigated in SCP. | | | | | | | |
| **Relevant available infrastructure / equipment description** | | | | | | | |
| The development will be performed using cloud resources. | | | | | | | |

### 

### Sync Lab S.r.l. (SYNC)

| **SYNC LAB SRL** | | | | http://www.synclab.it/wp-content/themes/synclab/_include/images/logo_synclab.png | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| http://www.synclab.it/ | | | |
| **Short name** | SYNC | **Type** | SME | **Country** | IT | **Partner no.** | 2 |
| **General description of the organisation** | | | | | | | |
| **Sync Lab** (http://www.synclab.it/) is an Italian SME active in the ICT field with focus on software and service development and integration. It was established in Naples in 2006, South of Italy, and has currently four branches in four of the major Italian cities, namely: Naples, Rome, Milan, and Padua.  Since its inception, Sync Lab has made massive investments in R&D activities. Sync Lab R&D division has been involved in major research projects, funded by the European Commission or by national Ministries and/or local governments. Sync Lab has consolidated partnerships—both at the business and at the research level—with leading companies in technology fields that are central to the project, and in particular: security monitoring, Business Activity Monitoring (BAM), cloud computing, Complex Event Processing, IP video surveillance, Geographic Information Systems (GIS), and banking. | | | | | | | |
| **Main attributed tasks and role in the project** | | | | | | | |
| Sync Lab will redesign and reimplement one its key products, namely Streamlog ([www.synclab.it/prodotti/streamlog/](http://www.synclab.it/prodotti/streamlog/)), to enable the security critical parts of the application to benefit from the superior security guarantees that will be provided by the secure container technology developed by the project. Streamlog is an activity monitor, based on log analysis, specifically designed for logging and tracing the activities of system administrators. The system was designed as a solution to comply with the November 2008 Italian regulation on Data Protection, which mandates that abuses by System Administrators be detected, notified to the data owners, and prosecuted in court. Streamlog has challenging security requirements, which can only be satisfied to a limited extent using currently available technologies. The new version of Streamlog that will be developed in the project will resist to attacks by powerful users, including the system administrator. In order to achieve this goal, SYNC will: 1) redesign and partition the application in such a way that security critical parts be encapsulated in a secure container; 2) extende and enhance the data collection support; 3) improve event storage support. | | | | | | | |
| **Relevant skills and previous experiences** | | | | | | | |
| Sync Lab has a long time experience in the development and deployment of integrated security solutions, especially in the field of log analysis, data correlation for anomaly detection, and big data analytics for banking. Sync Lab has made significant investments to improve their skills in the field of cloud computing and big data. It has recently become Silver Partner of Citrix, a major player in the field of virtualization and cloud computing.  Sync Lab has been participating to several EU and national research projects. In particular, it is one of the partners of the LEANBIGDATA project (leanbigdata.eu), funded by the EC within the context of FP7, which aims at building an ultra-scalable and ultra-efficient integrated big data platform addressing important open issues in big data analytics. Also importantly, it was one of the partners of the NAVRURAL project that was approved within the context of the EC Eurostars-Eureka funding program with the objective of developing a GPS navigator for cyclists. | | | | | | | |
| **Profile description of key personnel carrying out the work** | | | | | | | |
| **Salvatore Belfiore** (M) Sync Lab CEO, founded the company in 2002. Under his guidance Sync Lab has grown to its current four branches structure and has acquired customers of primary importance in the Italian and international scene.  **Ferdinando Campanile** (M) is the general manager of Sync Lab and the leader of its R&D department. He has lead Sync Lab in European as well as national research project, funded by the EC or Italian Ministries. He holds a Master degree in Electronic Engineering and has co-authored several scientific papers on topics that are closely related to activity monitoring in IT systems.  **Luca Lo Presti** (M) is the technical leader of Sync Lab “Applications” division. He also leads the development and commercialization of Streamlog product line.  The company has strong relationships with Italian universities and research centres, particularly with the University of Naples “Parthenope”, with which it has a continued fruitful cooperation. **Prof. Luigi Romano** (M), **Luigi Coppolino** (M), and **Salvatore D’Antonio** (M) from the University of Naples “Parthenope”, who have a valuable experience in FP7 and H2020 EC funded projects on topics that are key to the SCP project, will support Sync Lab as consultants. | | | | | | | |
| **Publications, other research or innovation products, or patents related to the project** | | | | | | | |
| **StreamCrusher** is a solution able to collect, index, and interpret the large amounts of data that an organization data centre generates daily: custom application logs, system logs, alerts, clickstream data, data feeds, configuration data, changes to the file system, message queues, and many others. From these heterogeneous data, StreamCrusher extrapolates information that the IT management can use to discover new business opportunities ([www.synclab.it/prodotti/streamcrusher/)](http://www.synclab.it/prodotti/streamcrusher/)).  **WAVE** (wide area videosurveillance environment) is based on the milestone video surveillance suite (DVMS). Its main innovative aspect is the strict integration with GIS (geographical information system) that enables management of video surveillance systems for very large areas ([www.synclab.it/prodotti/wave/](http://www.synclab.it/prodotti/wave/)). | | | | | | | |
| **Relevant previous projects/activities** | | | | | | | |
| Sync Lab has a long time experience in the development and deployment of integrated security solutions, especially in the field of log analysis, data correlation for anomaly detection, and big data analytics for banking. Sync Lab has made significant investments to improve their skills in the field of cloud computing and big data. It has recently become Silver Partner of Citrix, a major player in the field of virtualization and cloud computing.  Sync Lab has been participating to several EU and national research projects. In particular, it is one of the partners of the SecureCloud project (https://www.securecloudproject.eu/) and of the LeanBigData project ([leanbigdata.eu](http://leanbigdata.eu/)), funded by the EC within the context of H2020 and FP7, respectively. Also importantly, it was one of the partners of the NavRural project that was approved within the context of the EC Eurostars-Eureka funding program. | | | | | | | |
| **Relevant available infrastructure / equipment description** | | | | | | | |
| The lab facilities of the four sites will be made available to project partners for development, demonstration, and validation activities. | | | | | | | |

### EXUS Ltd (Exus)

## Third parties involved in the project (third party resources)

### SIListra Systems GmbH (SIL)

|  |  |
| --- | --- |
| Does the participant plan to subcontract certain tasks? | NO |
| Does the participant envisage that part of its work is performed by linked 3rd parties? | NO |
| Does the participant envisage the use of contributions in kind provided by 3rd parties? | NO |

### Sync Lab S.r.l. (SYNC)

|  |  |
| --- | --- |
| Does the participant plan to subcontract certain tasks? | NO |
| Does the participant envisage that part of its work is performed by linked 3rd parties? | NO |
| Does the participant envisage the use of contributions in kind provided by 3rd parties? | NO |

### Exus (Exus)

|  |  |
| --- | --- |
| Does the participant plan to subcontract certain tasks? | NO |
| Does the participant envisage that part of its work is performed by linked 3rd parties? | NO |
| Does the participant envisage the use of contributions in kind provided by 3rd parties? | NO |

# 

# Ethics and Security

## Ethics

*Questions we answered with YES in the Ethics issues table (Part A)*

2. Humans

Does your research involve human participants? No

Are they volunteers for social or human sciences research? No

4. Personal Data

Does your research involve personal data collection and/or processing? No

Does your research involve further processing of previously No  
collected personal data (secondary use)?

## Security

This project will **not** involve activities or results raising security issues and will **not** involve 'EU-classified information' as background or results.

# Annex 1: Drafted Coordination Agreement

Coordination Agreement

Concerning the Coordinated EU Project on

SCP

Contract No xxxx

between

Partners:

SIListra Systems GmbH, Dr. Martin Süßkraut

Sync Lab SRL, Italy, Ferdinando Campanile

EXUS

The institutions parties to this Coordination Agreement agree to carry out the coordinated EU Brazil project called “SecureCloud”.

These institutions, detailed in Annex I[[1]](#footnote-1), are hereinafter collectively referred “Brazilian partners” or respectively as “EU partners”; the Coordination Agreement as the “Agreement”; and the research on secure and dependable big-data cloud computing as the “research activity”.

In order to support scientific collaboration and research cooperation, the European Union and the Federative Republic of Brazil entered into an international agreement entitled “Agreement for Scientific and Technological Cooperation between the European Community and the Federative Republic of Brazil” dated November 11, 2005 (hereinafter referred to as the EC-Brazil Agreement).

This agreement specifies the research to be conducted; the process through which the partners will assure effective oversight and management of the research; and the arrangements through which the partners will report to their respective funding agencies.

**Article 1: Scope**

The partners shall jointly carry out the research activity as set out in the Description of Action (Annex II[[2]](#footnote-2)), which forms an integral part of this agreement.

The partners shall use reasonable endeavors to achieve the results intended for the research activity and fulfill the mutual obligations arising from this agreement, subject to force majeure and their obligations towards their respective funding agencies.

A partner shall not be liable to take action beyond its reasonable control. The partners shall agree on measures to be taken in the case of force majeure.

**Article 2: Duration**

This agreement shall cover a period of 36 months. The starting date is the same as the starting date of the joint EU-BRA proposal SecureCloud.

A partner may withdraw from this agreement without any liability towards the other parties following consultation with its funding agency, by giving two months notice to the other partners.

For the avoidance of doubt the validity of this agreement is dependent on a positive funding decision.

The partners, acting jointly and unanimously and subject to the prior approval of their funding agencies, may terminate this agreement or the participation of any individual partner for major technical or economic reasons substantially affecting the research activity, by giving two months written notice to such individual partner.

**Article 3: Financial provisions**

* 1. Each party shall bear its own costs incurred in connection with the performance of the Contract with its grant agency and this Coordination Agreement, carrying out and implementation of this research activity.The financial contribution of the European Commission will be distributed according to the projects Grant Agreement.
  2. Each party shall be solely liable for its own financial data. No other Party, including the Coordinator or their representatives acting within the scope of this Coordination Agreement may change these data without expressly given prior written permission of the party concerned.

**Article 4: Management of the Coordination**

4.1 Overall Management

The partners will assure effective overall management of the research activity through:

1. communication among themselves and with their respective funding agencies;
2. timely production of deliverables as set out in Annex II; and
3. integration of their work.

The partners will meet at least once every 12 months and will interact on a day-to-day basis between meetings via electronic means.

Each consortium undertakes to follow the schedule in the technical provisions of project. In view of the evolving character of the project, these production timetables are generally subject to change. To limit the risk, it is desirable to provide for a strict and effective supervision system managed by the coordination structure including:

* frequent progress meetings (ranging from once a month to once per quarter), preferably via electronic means;
* frequent technical and financial progress reports (actions completed and results obtained);
* optional extraordinary meetings as soon as agreed estimated deadlines have been overrun, including the right for the parties to review their position within the co-operative venture based on clearly stated reasons

Scientific workshops will be used with flexibility during the research activity to plan, implement and summarize specific tasks.

**Article 5: Publications**

Joint publications generated from the research activity are encouraged. They must include references to funding sources, including relevant award or contract numbers.

Each partner shall, subject to the confidentiality provisions of Article 6, have the right to make public the knowledge and information it generates under this agreement, consistent with good scientific practices, within the laws and regulations of the country within which the partner resides.

**Article 6: Confidentiality**

In general, the exchange of information between the partners shall be of a non-confidential nature. However, in the event that one partner desires to impose a restriction of confidentiality on any proprietary information or materials it provides to another partner under this agreement, the partner must clearly label such information or materials “confidential” (hereinafter known as “confidential information”). If disclosed verbally, confidential information must be reduced to writing within thirty (30) days.

A partner that receives Confidential Information under this Agreement shall use reasonable efforts to prevent its disclosure to third parties, and shall have imposed through appropriate arrangements an obligation on all partners receiving such information to keep it confidential. The obligation to keep information confidential shall continue in effect for the time period agreed by the relevant partners.

A partner that receives Confidential Information under this Agreement shall not be required to maintain confidentiality if the information or materials: (1) are, or subsequently become, public information through no breach of this Agreement; (2) are rightfully in the receiving partner’s possession prior to disclosure, as demonstrated by written records; (3) are rightfully disclosed to the receiving partner by a third party; (4) are independently developed by the receiving partner, without reliance upon Confidential Information received under this Agreement; or, (5) are required to be disclosed under local or national laws or regulations to which the receiving partner is subject or court order.

If a partner that receives Confidential Information becomes aware that, under its laws or regulations, it will be, or may reasonably be expected to become, unable to meet the non-disclosure provisions, it shall immediately inform the disclosing partner. The affected partners shall thereafter consult to define an appropriate course of action.

The provisions of this Article shall survive the expiration or termination of this Agreement for one year.

**Article 7: Intellectual Property**

Intellectual property first developed in the performance of the research activity shall be governed by Annex I of the EC-Brazil Agreement, with the following clarification: all rights to intellectual property made solely by employees of one partner will belong solely to that partner and shall be disposed of in accordance with that partner’s policies and Annex I of the EC-Brazil Agreement. Rights to intellectual property developed by staff of two or more partners shall be held jointly by such partners.

In case of joint ownership, the joint owners will establish an agreement regarding the allocation and terms of exercise of that joint ownership. Such an agreement may involve issues such as how to govern the difficulties in continuing with joint ownership depending on the circumstances. If joint ownership is maintained, it could be agreed:

* to have some form of territorial division, by virtue of which one party to the invention owns the invention only in some countries and the other parties are free to register it in other specified countries;
* to have some form of division of application markets, by virtue of which one party to the invention owns the discovery only in business sectors in which it is already active;
* to set up a regime for the protection (e.g. when and how to protect and who bears the costs for protection and possible enforcement);
* to set up a regime for use (including licensing) by the joint owners, within for example specified limits and possible profit sharing.

Joint ownership issues will be regulated in separate joint ownership agreements developed for each joint ownership situation (as a one-size-fits-all approach may not be appropriate in this project).

This agreement will also provide rules on access rights between the participants of the EC project and the participants of Brazilian project if this is needed for implementation purposes or for using the results generated in the project.

**Article 8: Handling and Use of Data**

Scientists participating in the research activity are encouraged to disseminate their data widely to other interested scientists. The scientists participating in the research activity will retain control of their individual data for 6 months to allow the partners’ participants to finish compiling their data for generation of joint databases and publication of scientific results.

The development of joint databases is encouraged. If distributed databases are established, they should be carefully linked to facilitate easy access.

**Article 9: No Legal Formation**

No provision of this Agreement, whether express or implied, shall be construed as establishing, constituting, giving effect to or otherwise recognizing any partnership, joint venture, pooling arrangement, or formal business organization of any kind, even if the term “Partner” is used. No party to this Agreement shall have the right to bind any other party.

**Article 10: Dispute Resolution**

10.1. Disputes between Brazilian and EU partners

In case of a dispute arising out of or in connection with this agreement between one or more Brazilian partners on the one hand, and one or more EU partners on the other, the partners shall use their best endeavors to settle the dispute amicably.

Any such dispute, which cannot be solved through such endeavors, should be brought to the attention of the funding agencies, which will be invited to take action as necessary to resolve the dispute. Such action should be based on hearing all parties and applying the rules of the individual grants/contracts, the Brazil-EU Agreement, and this Coordination Agreement. Upon mutual agreement of the funding agencies, the partners may agree to submit the dispute to an arbitral tribunal for binding arbitration. Unless the partners agree otherwise in writing, the arbitration rules of United Nations Commission on International Trade Law (UNCITRAL) would govern.

10.2. Other disputes

In case of a dispute between partners other than those referred to in Article 10.1 arising out of or in connection with this agreement, the partners shall use their best endeavors to settle the dispute amicably.

Any such dispute, which cannot be solved through such endeavors, should be brought to the attention of the competent funding agency, which will be invited to take action as appropriate to resolve the dispute. The partners shall assure that the funding agency is provided with all information necessary to resolve the dispute.

**Article 11: Liability Limitations**

Each partner shall be liable towards the other partners in respect of negligent acts or omissions of itself and of its employees, agents officers and directors and shall secure indemnification for the benefit of the other partners from its subcontractors provided always that such liability shall not extend to claims for indirect or consequential loss or damages such as, but not limited to, loss of profit, revenue, contract or the like and provided that the total, aggregate limit of liability of that partner and any subcontractor of a partner towards all of the other partners collectively in respect of any and all such claims shall not exceed the amount of funding received by the liable partner from the funding agency for the performance of this agreement as specified in the individual grant for that partner.

To the extent permitted by law and subject always to such other undertakings and warranties as are expressly provided for in this agreement, each partner shall be solely liable for any loss, damage or injury to third parties resulting from the execution of its assigned tasks under this agreement and/or from its use of the project results and/or any material provided for the performance of this agreement by the other partners hereunder.

**Article 12: Amendment**

This Agreement may only be amended in writing and signed by authorized representatives of each of the partners. This may cover situations when changes to the initial specifications get necessary, and could go as far as including the termination of certain tasks, the withdrawal of certain parties, the inclusion of new partners etc.

**Article 13: Miscellaneous**

13.1. The parties acknowledge that if any information and data generated as a result of this coordination is subject to any Export Control Laws or Regulations, the parties agree to comply with the applicable Export Control Laws or Regulations.

13.2. Nothing in this Coordination Agreement shall preclude any party from offering or performing any activities or services that it may regularly offer even though such activities or services may be included in the scope of services covered by this Coordination Agreement.

13.3. No party will be responsible for any failure to perform due to unforeseen circumstances or to causes beyond the party’s reasonable control, including but not limited to acts of God, war, riot, embargoes, acts of civil or military authorities, fire, floods, accidents, strikes, shortages of transportation, facilities, fuel, energy, labor or materials, or changes in applicable laws or regulations affecting this Agreement.

**Article 14: Number of copies, languages and signature process**

The Parties have caused this Coordination Agreement to be duly signed by the undersigned authorised representatives in separate signature pages the day and year first above written.

**Article 15: Applicable law & Settlement of disputes**

This Consortium Agreement shall be construed in accordance with and governed by the laws of Belgium.

Authorized to sign on behalf of:

……………………………………………………………………………………………………………………….

Name: ………………………………… Signature ………………………………………

Title ………………………………… Date ………………………………………

Name: ………………………………… Signature ………………………………………

Title ………………………………… Date ………………………………………

# References

1. Trusted Computing Base. http://www.trustedcomputinggroup.org/.
2. Craig Gentry. “Computing Arbitrary Functions of Encrypted Data”. In: Commun. ACM 53.3 (2010), pp. 97–105. DOI: 10.1145/1666420.1666444.
3. Seny Kamara and Mariana Raykova. “Parallel Homomorphic Encryption”. In: Workshop on Applied Homomorphic Encryption (WAHC ’13). 2013.
4. M. Tebaa, S. El Hajji, and A. El Ghazi. “Homomorphic encryption method applied to Cloud Computing”. In: Network Security and Systems (JNS2). 2012, pp. 86–89.
5. Arvind Arasu et al. “A secure coprocessor for database applications”. In: Field Programmable Logic and Applications (FPL), 2013 23rd International Conference on. IEEE. 2013, pp. 1–8.
6. J.G. Dyer et al. “The IBM Secure Coprocessor: Overview and Retrospective”. In: IEEE Computer (2001), pp. 57–66.
7. PRACTICE. http://www.practice-project.eu/.
8. C.P. Ram and G. Sreenivaasan. “Security as a Service (SasS): Securing user data by coprocessor and distributing the data”. In Trendz in Information Science and Computing, 2010.
9. Anati, Ittai, et al. "Innovative technology for CPU based attestation and sealing." Proceedings of the 2nd International Workshop on Hardware and Architectural Support for Security and Privacy. 2013.
10. Burrows, Mike. "The Chubby lock service for loosely-coupled distributed systems." *Proceedings of the 7th symposium on Operating systems design and implementation*. USENIX Association, 2006.
11. Hunt, Patrick, et al. "ZooKeeper: Wait-free Coordination for Internet-scale Systems." *USENIX Annual Technical Conference*. Vol. 8. 2010.
12. Jonathan M. McCune et al. “How low can you go?: recommendations for hardware-supported minimal TCB code execution”. In: ASPLOS. 2008, pp. 14–25.
13. Ahmad-Reza Sadeghi et al. “TCG inside?: a note on TPM specification compliance”. In: STC. 2006, pp. 47–56.
14. Marten Van Dijk et al. “Fully homomorphic encryption over the integers”. In: Advances in Cryptology– EUROCRYPT 2010. 2010, pp. 24–43
15. Zhenfei Zhang, Thomas Plantard, and Willy Susilo. “Reaction Attack on Outsourced Computing with Fully Homomorphic Encryption Schemes”. In: ICISC. 2011, pp. 419–436.
16. G. Edward Suh et al. “AEGIS: Architecture for Tamper-evident and Tamper-resistant Processing”. In: Proceedings of the 17th Annual International Conference on Supercomputing. 2003, pp. 160–171. DOI: 10.1145/782814.782838.
17. David Lie Chandramohan Thekkath et al. “Architectural Support for Copy and Tamper Resistant Software”. In: Proceedings of the Ninth International Conference on Architectural Support for Programming Languages and Operating Systems. 2000, pp. 168–177. DOI: 10.1145/378993.379237
18. Baumann, Andrew, Marcus Peinado, and Galen Hunt. "Shielding applications from an untrusted cloud with haven." *USENIX Symposium on Operating Systems Design and Implementation (OSDI)*. 2014.
19. Candea, George, James Cutler, and Armando Fox. "Improving availability with recursive microreboots: a soft-state system case study." *Performance Evaluation* 56.1 (2004): 213-248.
20. Madhavapeddy, A., Mortier, R., Rotsos, C., Scott, D., Singh, B., Gazagnaire, T., Crowcroft, J. (2013). Unikernels: Library Operating Systems for the Cloud. In *Proceedings of the 18th International Conference on Architectural Support for Programming Languages and Operating Systems* (pp. 461–472).
21. M. Sipos, F. H. P. Fitzek, D. E. Lucani, and M. V. Pedersen, “Distributed cloud storage using network coding,” in IEEE Consumer Communications and Networking Conference, Jan. 2014.
22. A. Dimakis, V. Prabhakaran, and K. Ramchandran, “Ubiquitous access to distributed data in large-scale sensor networks through decentralized erasure codes,” in Information Processing in Sensor Networks, 2005. IPSN 2005. Fourth International Symposium on, 2005, pp. 111–117.
23. A. G. Dimakis, P. B. Godfrey, M. J. Wainwright, and K. Ramchandran, “Network coding for distributed storage systems,” in IEEE International Conference on Computer Communications (INFOCOM), 2007.
24. M. Sathiamoorthy, M. Asteris, D. S. Papailiopoulos, A. G. Dimakis, R. Vadali, S. Chen, and D. Borthakur, “Xoring elephants: Novel erasure codes for big data,” CoRR, vol. abs/1301.3791, 2013.
25. C. Huang, H. Simitci, Y. Xu, A. Ogus, B. Calder, P. Gopalan, J. Li, and S. Yekhanin, “Erasure coding in Windows Azure Storage,” in Proceedings of the 2012 USENIX Conference on Annual Technical Conference, Berkeley, CA, USA, 2012.
26. Dean, Jeffrey, and Sanjay Ghemawat. "MapReduce: simplified data processing on large clusters." *Communications of the ACM* 51.1 (2008): 107-113.
27. White, Tom. *Hadoop: the definitive guide: the definitive guide*. " O'Reilly Media, Inc.", 2009.
28. Neumeyer, Leonardo, et al. "S4: Distributed stream computing platform." *Data Mining Workshops (ICDMW), 2010 IEEE International Conference on*. IEEE, 2010.
29. Jain, S., Kumar, A., Mandal, S., Ong, J., Poutievski, L., Singh, A., Zhu, M. (2013). B4: Experience with a Globally-Deployed Software Defined WAN. In *Proceedings of the ACM SIGCOMM 2013 Conference* (pp. 3–14).
30. Kelly, J., and Knottenbelt, W. *Disaggregating Smart Meter Readings using Device Signatures*. Imperial Computing, Science MSc Individual Project, (Sep. 2011).
31. Boccuzzi, C. *Smart grid and the energetic big brother*. Metering International América Latina, 3, (2010), 82-83.
32. Ulrich Greveler, Benjamin Justus and Dennis Löhr: *Multimedia Content Identification Through Smart Meter Power Usage Profiles* Proceedings of the International Conference on Information and Knowledge Engineering IKE'12, Las Vegas, 2012.
33. Cuijpers, Colette and Koops, Bert-Jaap: *Smart Metering and Privacy in Europe: Lessons from the Dutch Case* . In: S. Gutwirth et al. (eds), European Data Protection: Coming of Age, Dordrecht: Springer, pp. 269-293 (2012).

1. This annex to the coordination agreement will be skipped in this proposal as the content of the annex could be directly derived from the partner lists presented at the cover page. [↑](#footnote-ref-1)
2. This annex to the coordination agreement is skipped as well because it would be in essence a copy of the relevant sections of this proposal. [↑](#footnote-ref-2)