

# N. 3 NEWSLETTER

November 2020



RESilience enhancement and risk control platform  
for communication infraSTructure Operators



## IN THIS ISSUE

- Insight from the RESISTO project Coordinator
- RESISTO project | Technical highlights
- KSI Blockchain timestamping in RESISTO

... and MORE



THE RESISTO PROJECT HAS RECEIVED FUNDING FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME UNDER GRANT AGREEMENT NO. 786409.

## SUMMARY

- pag. 3      **Insight from the RESISTO project Coordinator**  
*by Bruno Saccomanno, Leonardo S.p.A*
- pag. 4      **RESISTO project | Technical highlights**  
*by Valerio Di Claudio, Leonardo S.p.A.*
- pag. 5      **KSI Blockchain timestamping in RESISTO**  
*by Kristo Klesment, Guardtime*
- pag. 7      **Open Access Book: “Cyber-Physical Threat Intelligence for Critical Infrastructures Security**  
*by Federica Battisti and Federica Pascucci, Università degli Studi RomaTre*
- pag. 9      **RESISTO social media: “Follow us and stay tuned!”**  
*by Marco Ferraro and Arianna Magni, APRE - Agency of the Promotion of European Research*



RESISTO newsletter is the official, semi-annual newsletter from Horizon 2020 RESISTO project. Each RESISTO newsletter issue aims to disseminate project updates as well as news. It is developed and compiled with the contributions from the RESISTO Consortium Partners and relevant Stakeholders.

## INSIGHT FROM THE RESISTO PROJECT COORDINATOR



Dear RESISTO follower,

We are pleased to present you our **third RESISTO Newsletter!**

Unfortunately, the COVID-19 emergency has had and continues to have a much more marked impact than could have been imagined ... and also RESISTO, like many other projects, had inevitable delays: we're working to extend the duration of the project beyond its natural deadline (planned for April 2021).

Therefore, the validation phase, which we expected could start already during the summer, is not yet fully operational. Not being able to carry out activities in the field, we still used the time **to redesign and rationalize the validation process**, which consists of two runs:

- The **first run** aims at verifying how the RESISTO *Short Term Control Loop* reacts by applying the use cases foreseen for each scenario: Resilience Indicators (RIs) will be measured during the trials, the first run ends with a comparison between measured RIs and estimated RIs;
- The **second run** starts with a *Long Term Control Loop* cycle taking into account first run results. Long Term Control Loop could identify interventions in order to improve the Critical Infrastructure and the RESISTO platform, such as workflows and countermeasures refinements, detectors tuning etc. The identified interventions will be put in place. Then, the use cases will be executed again in order to evaluate RESISTO Short Term Control Loop improvement.

We're sure that the comparison among estimated and measured Resilience Indicators will trigger a continuous resilience improvement process!

As regards the **dissemination and communication activities**, we would like to point out that in recent months RESISTO has participated - naturally in a strictly virtual way - in the **first workshop organized by the European Cluster for Securing Critical Infrastructures (ECSCI)**, and has actively contributed to the **activities of the Community of Users for Security Research**. Finally, he took part in the **Kick-off Meeting on ICT Verticals and Horizontals for Blockchain Standardization**, and expressed his willingness to participate in some of the thematic Roundtables scheduled in the coming months.

*Stay tuned with the project progress by following our newsletters, social network accounts and web site ([www.resistoproject.eu](http://www.resistoproject.eu)), to be informed about future developments towards a faster and more efficient critical infrastructures protection.*



**Bruno Saccomanno,**  
Leonardo S.p.A,



# RESISTO PROJECT - TECHNICAL HIGHLIGHTS:

by Valerio Di Carlo, Leonardo S.p.A.

**RESISTO activities in this last months** were focused on the **validation phase of scenarios and use cases**, which was one of the main objective of the project.

The main challenge inherent **the validation task** is the capability of multiple actors to cooperate together, collecting alarms and events from several sources, frequently using different protocol and formats. So, detectors of physical or cyber-attacks, as well as meteorological or seismic sensors shall feed the **RESISTO platform in order to exploit its capability to correlate information and to propose countermeasures to mitigate effects of adverse events, to definitely improve Resilience Indicators of the whole system.**

But this challenge is standard for system needing integration of heterogeneous sources and technologies: the true challenge of the RESISTO project is to start this task during **Covid-19**, where all partners suffered travel restrictions, limiting the possibility to organize live meetings and integration sessions and, also, the wide adoption of smart working, often restraining access to physical assets also to people of the same organization.

Even if delays are the first logical consequence of this context, **the interesting aspect is the effort of partners to adapt the architecture of the test beds to these new constraints, for example substituting physical components with simulators and deciding to use the RESISTO platform virtualized in the cloud.**

Moreover, the interaction of short term and long-term approaches was refined to improve applicability and benefits to already defined use cases' scenarios.

**In conclusion**, we are testing now the secure communication infrastructure connecting all partners and all test beds, scattered in different countries, and, in parallel, adapting and testing common protocols and formats to complete the integration, to start soon the validation phase.



Read our public access **DELIVERABLES\*** from the project:

> [www.resistoproject.eu/resources/](http://www.resistoproject.eu/resources/)

\* These documents and its content are the property of the RESISTO Consortium. The content of all or parts of these documents can be used and distributed provided that the RESISTO project and the document are properly referenced.



# KSI BLOCKCHAIN TIMESTAMPING IN RESISTO

by Kristo Klesment, Guardtime

RESISTO project have implemented future-proof and scalable solution for cyber security, data protection and long-term archiving. KSI® Blockchain timestamping unlocks the digital trust needed for ambitious digitization RESISTO project, as going cloud-native, adopting AI, and moving to automated machine-to-machine processes.

KSI® Blockchain was first developed in 2008 for the [Government of Estonia](#) to secure its critical health, justice and business data. Since then, it has been deployed by the world's most demanding customers, including the numerous governments and leading companies in telecoms, aerospace, defense, energy, financial services and insurance.

Guardtime's KSI Blockchain Timestamping Service is compliant with the eIDAS regulation and is included in the [European Trusted List](#).

KSI® is the first blockchain-based technology to receive an eIDAS accreditation and marks an important step in the evolution of digital trust technologies. Accreditation was conducted by TÜV Nord, Germany.

## Unique benefits compared to existing timestamping solutions:

- **MASSIVE VOLUME**

KSI Blockchain timestamping scales to millions of events per second to support the volumes needed for the most ambitious data-driven solutions in the public and private sectors.

- **INDEPENDENT VERIFICATION**

KSI Blockchain timestamps can be verified independently of Guardtime or any third-party service provider by a widely witnessed blockchain-based trust anchor.

- **LONG-TERM**

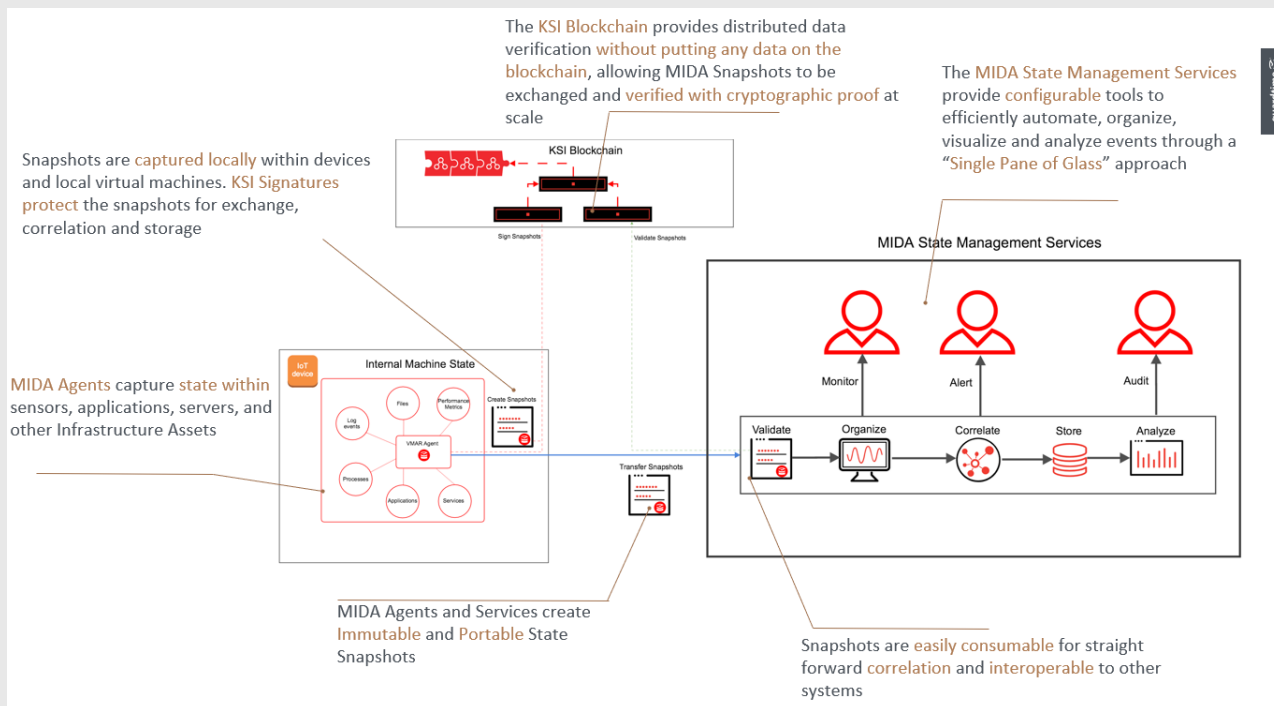
KSI timestamps can be stored and verified indefinitely, without the need for complex crypto-lifecycle management. KSI Timestamps are immune to quantum computing attacks, which makes them ideal for long term archiving and future-oriented projects.

- **RELIABLE**

KSI Blockchain has been in continuous operation for over a decade and is designed to exceed enterprise reliability requirements, backed by industry-leading SLAs.

## KSI Blockchain Timestamping in RESISTO

by Kristo Klesment, Guardtime



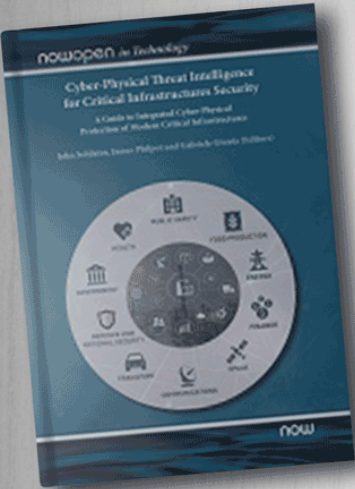
RESISTO has used KSI blockchain based monitoring tool (named MIDA) and developed its features and services.

Baseline configuration has been made RESISTO platform specific. It captures common intrusions and is ready for context specific extensions.

Output plug-in has been developed. It connects to RESISTO shared backend and uses shared KAFKA message streaming. IDEA language profile is used for semantical interoperability. Tool maturity have been improved as partners have taken part in development process.

# OPEN ACCESS BOOK: “CYBER-PHYSICAL THREAT INTELLIGENCE FOR CRITICAL INFRASTRUCTURES SECURITY”

by Federica Battisti e Federica Pascucci, Università degli Studi RomaTre



**RESIST**  
RESilience enhancement and risk control platform  
for communication infraSTRUCTure OPERATORS

## OPEN ACCESS BOOK

### Cyber-Physical Threat Intelligence for Critical Infrastructures Security

*A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures*

**Now available for download!**

According to Industry 4.0 paradigm, in the last few years, classical production engineering, automation, and intelligent computation systems met the Internet of Things (IoT). As a result, advanced Cyber-Physical Systems (CPS) are used in safety and security critical applications such as industrial control systems, autonomous vehicles, and critical infrastructures. Critical Infrastructures, that were not designed to be connected, are now open to Internet. Edge computing is largely adopted for monitoring and analyzing the production process; cloud-based services are used to optimize complex supply chains; machine learning algorithms are used to predict machine failure, hence reducing maintenance costs.

This trend is foreseen to continue and be further enhanced by the advent of 5G communication technology. Nonetheless, beside enabling a number of services, the introduction of interconnected devices presents several issues. CPS exchange a large amount of safety-critical data and represent appealing targets for different type of attacks. Moreover, some recent large-scale security incidents against critical infrastructures highlight that attacks to cyber systems could result in damages to physical assets. Therefore, critical infrastructures security must be implemented based on a holistic, integrated approach that protects cyber and physical assets at the same time.





## SECTION 04

### OPEN ACCESS BOOK: “Cyber-Physical Threat Intelligence for Critical Infrastructures Security”

by Federica Battisti e Federica Pascucci, Università degli Studi RomaTre

In this framework, the book “*Cyber-Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures*” edited by John Soldatos, James Philpot, and Gabriele Giunta, (freely available at this link <https://www.nowpublishers.com/article/BookDetails/9781680836868>) presents novel solutions for integrated security of critical infrastructures, with emphasis on solutions in four sectors, namely finance, healthcare, energy, and communications. The book presents various technologies and building blocks for integrated security, along with sector-specific solutions.

**The book is structured in five parts.** The first four parts are dedicated to presenting solutions for the sectors of finance, healthcare, energy, and communications, respectively. The fifth part comprises sector-agnostic solutions including technologies and best practices that are applicable to critical infrastructures. The fourth part has been developed by RESISTO consortium and proposes the achievements of the project.

Since September 2020, the book has gained large interest, obtaining **more than 8000 downloads**.

**MORE INFO HERE >** [https://bit.ly/OpenAccessBook\\_RESISTO](https://bit.ly/OpenAccessBook_RESISTO)



## RESISTO SOCIAL MEDIA: “FOLLOW US AND STAY TUNED!”

by Marco Ferraro and Arianna Magni, APRE - Agency of the Promotion of European Research

RESISTO posts every week interesting updates's project on its social media!

We regularly share most recent developments in the project and its project results and show our activities like event participation, invitation to project events, publications, articles etc.



... and more!

If you want to be updated, **FOLLOW RESISTO PROJECT** on:

**Twitter:** @RESISTO\_project

**Facebook:** @RESISTO.eu.project

**Linkedin:** RESISTO project





**RES**ilience enhancement and risk control platform  
for communication infra**ST**ructure **O**perators

## PROJECT COORDINATOR

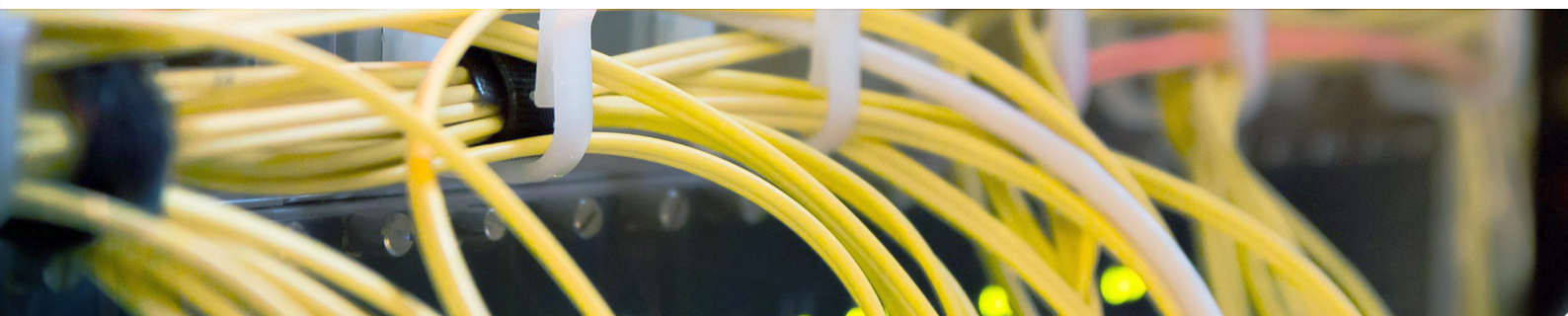


**Bruno Saccomanno**  
bruno.saccomanno@leonardocompany.com

## RESISTO PARTNERS



(RM3 third party) is responsible of Dissemination, Communication and awareness raising activities.



[www.resistoproject.eu](http://www.resistoproject.eu)

Follow us

