Grant Agreement No.: 952697
Call: H2020-SU-ICT-2018-2020
Topic: SU-ICT-02-2020
Type of action: RIA

D7.7 PROJECT IMPACT ASSESSMENT (FINAL VERSION)

Work package	WP 7
Task	Task 7.5
Due Date	31/08/2023
Deliverable lead	DAEM
Version	1.0
Editors	Dimitra Tsakanika (DAEM), Ilia Christantoni (DAEM)
Reviewers	Stelios Basagiannis (UTRCI), Stefanos Venios (S5)
Abstract	Deliverable D7.7 provides the final report of the ASSURED consortium towards a concrete evaluation of the ASSURED framework and its building blocks. We first present the core technologies developed as part of ASSURED, as well as **the core innovations and value propositions** provided by these technologies. Next, we provide a detailed analysis on the **impact assessment of ASSURED in the context of the application domains defined by the four envisioned use cases**, namely *Smart Manufacturing, Smart Cities, Smart Aerospace, and Smart Satellites*. Specifically, we highlight the security, privacy, and trustworthiness challenges affecting these domains, and we provide details on how these challenges can be addressed and mitigated by ASSURED. We also provide an initial analysis for the potential adoption of ASSURED in other application domains, beyond the aforementioned ones showcasing and evaluating the benefits brought forth by ASSURED towards EU's vision of secure, interconnected societies. In this context, we evaluate further the strategic impacts of ASSURED, focusing on the core vision of the EU for enabling trust assessment of modern supply chain ecosystems, as well as improving the security posture (and autonomy) of the EU in the domain of cybersecurity.
Keywords	Validation Results, Adoptions Guidelines, Takeaway Messages, Project Impact Assessment

Funded by the Horizon 2020 Framework Programme of the European Union

Document Revision History

Version	Date	Description of change	List of contributors
v0.1	08.06.2023	Table of Contents	Dimitra Tsakanika (DAEM), Ilia Christantoni (DAEM)
v0.2	15.06.2023	Value propositions of ASSURED, description of highlights and core achievements (Chapter 2)	Edlira Dushku, Nicola Dragoni (DTU) Richard Mitev, Phillip Rieger, Marco Chilese (TUDA) Liqun Chen, Nada El Kassem (SURREY) Kaitai Liang (TUDE) Thanassis Giannetsos, Dimitris Karras (UBITECH) Sotiris Koussouris, Stefanos Venios (SUITE5) Ilias Aliferis, George Bekos, Thanassis Fameliaris (UNIS) Ioannis Avramidis, Andreas Zalonis (INTRA) Reyan Korel Erben (BIBA) Meni Orenbach, Ahmad Atamli (NVIDIA) Stelios Basagiannis, Riccardo Orizio (Collins Aerospace-UTRCI)
v0.3	27.06.2023	First draft of strategic impacts of ASSURED (Chapter 4)	Richard Mitev, Phillip Rieger, Marco Chilese (TUDA) Liqun Chen, Nada El Kassem (SURREY) Thanassis Giannetsos, Dimitris Karras (UBITECH) Reyan Korel Erben (BIBA) Meni Orenbach, Ahmad Atamli (NVIDIA) Stelios Basagiannis, Riccardo Orizio (Collins Aerospace-UTRCI)
v0.4	03.07.2023	Challenges, results, and impact assessment for Smart Aerospace application domain (Chapter 3)	Stelios Basagiannis, Riccardo Orizio (Collins Aerospace-UTRCI)
v0.5	07.07.2023	Challenges, results, and impact assessment for Smart Manufacturing application domain (Chapter 3)	Reyan Korel Erben (BIBA)
v0.6	17.07.2023	Challenges, results, and impact assessment for Smart Satellites application domain (Chapter 3)	Nikos Drosos, Emmanouil Bakiris (SPH)
v0.7	25.07.2023	Challenges, results, and impact assessment for Smart Cities application domain (Chapter 3)	Ilia Christantoni, Dimitra Tsakanika (DAEM)
v0.8	01.08.2023	Description of other application domains (Chapter 3)	Thanassis Giannetsos, Dimitris Karras (UBITECH)
v0.9	10.08.2023	Finalization of Strategic Impacts of ASSURED (Chapter 4)	Richard Mitev, Phillip Rieger, Marco Chilese (TUDA) Liqun Chen, Nada El Kassem (SURREY) Thanassis Giannetsos, Dimitris Karras (UBITECH) Reyan Korel Erben (BIBA) Meni Orenbach, Ahmad Atamli (NVIDIA) Stelios Basagiannis, Riccardo Orizio (Collins Aerospace-UTRCI)
v0.95	16.08.2023	Finalization of the Introduction and Conclusions sections (Chapters 1 and 5)	Thanassis Giannetsos, Dimitris Karras (UBITECH)
v0.96	22.08.2023	Review of the entire deliverable	Stelios Basagiannis (UTRCI), Stefanos Venios (S5)
v1.0	29.08.2023	Polishing of the language of the deliverable, updates based on review comments, finalization of the deliverable, and submission	Thanassis Giannetsos, Dimitris Karras (UBITECH)

Editors

Ilia Christantoni (DAEM), Dimitra Tsakanika (DAEM)

Contributors (ordered according to beneficiary numbers)

Edlira Dushku, Nicola Dragoni (DTU)
Richard Mitev, Phillip Rieger, Marco Chilese (TUDA)
Liqun Chen, Nada El Kassem (SURREY)
Kaitai Liang (TUDE)
Thanassis Giannetsos, Dimitris Papamartzivanos, Dimitris Karras (UBITECH)
Sotiris Koussouris, Stefanos Venios (SUITE5)
Ilias Aliferis, George Bekos, Thanassis Fameliaris (UNIS)
Ioannis Avramidis, Andreas Zalonis (INTRA)
Reyan Korel Erben (BIBA)
Nikos Drosos, Emmanouil Bakiris (SPH)
Meni Orenbach, Ahmad Atamli (NVIDIA)
Ilia Christantoni, Dimitra Tsakanika (DAEM)
Stelios Basagiannis, Riccardo Orizio (Collins Aerospace-UTRCI)

DISCLAIMER

COPYRIGHT NOTICE

Project co-funded by the European Commission in the H2020 Programme		
Nature of the deliverable:	**R**	
Dissemination Level		
PU	Public, fully open, e.g. web	✔
CL	Classified, information as referred to in Commission Decision 2001/844/EC	
CO	Confidential to ASSURED project and Commission Services	

* R: Document, report (excluding the periodic and final reports)

EXECUTIVE SUMMARY

Towards **enhancing the security landscape and operational assurance of Next-Generation Systems-of-Systems (SoS)**, ASSURED has provided a holistic solution that aims to address both **security and privacy concerns**, while taking into consideration the requirements of the heterogeneous devices running **mixed-criticality services** comprising such types of ecosystems. The endmost goal is to provide certifiable and auditable assurance of a supply chain ecosystem in real-time, throughout its operational lifecycle.

This deliverable, as part of the WP7 activities of Dissemination and Communication, builds upon the results provided in D7.6 [1] (and D6.4 [6] where a detailed evaluation and assessment of the core investigated technologies has been documented) and provides the **final version of the Impact Assessment of ASSURED in the context of safety-critical domains** that necessitate the secure integration of IoT in trusted environment, for a service graph chain, covering communication, data collection, data transport, and data processing. More specifically, the objective is to provide an assessment of the project's impact focusing on the various application domains that were tackled throughout the lifecycle of the project implementation, focusing on the core issues and challenges identified by the EU in the context of the considered types of supply chain ecosystems. In this regard, as it is further elaborated in Chapter 2, one core consideration which is at the forefront of the design philosophy of ASSURED is the notion of **zero trust** (*"never trust, always verify"*), meaning that no user or device can be considered trusted by default, even if they have been previously securely enrolled to the network. **The adoption of a zero-trust approach is increasingly important in modern supply chain ecosystems, as the handling of sensitive data is subject to strict privacy requirements**.

In order to evaluate the design and implementation of ASSURED in the context of all phases of supply chain management, capturing the entire operational lifecycle of a device and the system as a whole, the framework has been integrated into four envisioned use cases (*Smart Manufacturing, Smart Cities, Smart Aerospace,* and *Smart Satellites*), which have been selected in order to address the types of security and privacy requirements typically encountered in the type of supply chain ecosystems targeted by ASSURED. However, the ASSURED artefacts and strategic assets go beyond these use cases, and can be adopted by **a wide variety of organizations, regardless of the specific implementation of their infrastructure and belonging to a wide range of application domains**. Analysis of the challenges associated with the four aforementioned use cases, as well as the tools provided by ASSURED to address these challenges, are provided in Chapter 3.

As aforementioned, one core target of ASSURED is the enhancement of security and privacy in various operational stacks of all applications, towards **cementing the vision of the EU and leadership position in ICT trustworthiness**. In this direction, ASSURED offers a wide variety of technologies and components developed as part of the framework, including the **Risk Assessment and Policy Recommendation Engine**, the **Attestation Toolkit**, the **Blockchain Infrastructure**, and the **lightweight crypto and data management schemes**. It also supports core tenets of the vision of the EU, such as an **identity management** system for enabling users to provide evidence on their properties without breaching their privacy profile, as well as improving trust in the **Digital Single Market (DSM).** In this regard, the strategic impacts of ASSURED are outlined in detail in Chapter 4.

Overall, ASSURED has offered a wide array of value propositions, which present a high degree of applicability by a wide array of industrial domains, and provide significant advancement in the state-of-the-art of cybersecurity solutions, while working towards the core vision of the EU and improving the security posture of the EU as a whole.

TABLE OF CONTENTS

LIST OF TABLES

1 INTRODUCTION

Europe is in the midst of a digital transformation. Digital technologies are profoundly changing our daily life, our way of working and doing business, and the way people travel, communicate, and relate with each other. Digital communication, social media interaction, artificial intelligence, e-government, e-commerce, and digital enterprises are steadily transforming our world. They are generating an ever-increasing amount of data, which, if pooled and used, can lead to completely new means and levels of value creation. The more interconnected we are, however, the more we are vulnerable to cyber threats.

Digital disruption, notably caused by malicious cyber activities, not only threatens our economies but also our way of life, our freedoms, and values, and even tries to undermine the cohesion and functioning of our democracy in Europe.

Regardless of the economic, political, or personal motivations behind the cyber threats, securing our future wellbeing, freedoms, democratic governance, and prosperity depend on improving our capacity to shield the EU from malicious attacks and to address digital security weaknesses in general. The digital transformation requires improving cybersecurity substantially, so as to ensure the protection of the increasing number of connected devices and the safe operation of network and information systems, including the ones used in power grids, drinking water supply and distribution services, vehicles and transport systems, hospitals and the overall health system, finances, public institutions, factories, and homes. Europe must build resilience to cyber-attacks and create effective cyber deterrence, while making sure that data protection and freedom of citizens are strengthened. These efforts should include considerations for particularly vulnerable organizations and citizens.

The technological tools of cybersecurity are strategic assets, as well as being key growth technologies for the future. It is in the EU's strategic interest to ensure that the EU retains and develops the essential capacities to secure its digital economy, society, and democracy, to protect critical hardware and software and to provide key cybersecurity services.

Considering all the above, the cybersecurity research and innovation activities carried out as part of ASSURED will support a Europe fit for the digital age, enabling, and supporting digital innovation while simultaneously preserving privacy, security, safety, and ethical standards. They will contribute to the implementation of the digital and privacy policy of the Union, in particular the NIS Directive [2], the EU Cybersecurity Act [3], the EU Cybersecurity Strategy [4], the GDPR [5], and the future e-Privacy Regulation. The goal of this deliverable is to perform an assessment of how ASSURED has provided such cybersecurity and assurance controls as strategic assets. In this regard, we first demonstrate the **key growth that ASSURED can enable in the envisioned application domains**, and we expand on how these outcomes can extend to the entire vision of the EU through a series of **strategic impacts**.

1.1 SCOPE AND PURPOSE

The main goal of ASSURED is to provide operational assurance to large-scale, complex **Systems-of-Systems (SoS)** comprising multiple **heterogeneous devices with different security and privacy requirements**, running several **mixed-criticality services**. To this end, we have designed **novel security and assurance controls that can underpin the entire lifecycle of cyber-physical systems** and integrated them into the ASSURED framework, which consists of several components working in tandem in order to fulfill all security, privacy, and trustworthiness requirements of any organization that aims to benefit from the novel security methodologies and technologies developed and implemented as part of the framework. The technologies developed as part of ASSURED push the state-of-the-art in various multidisciplinary domains (e.g., attestation and runtime verification, trust assessment,

risk assessment and secure and privacy-preserving data sharing through the use of Blockchain for enhanced auditability and certification capabilities), **unveiling a realistic and practical approach to deliver strong assurance to multi-domain environments**.

Towards evaluating the outcomes of the ASSURED project, in D6.4 [6], we performed an analysis on the ASSURED framework from a **technological perspective**, focusing on each of its components separately and outlining the capabilities offered by each. We also provided a detailed impact assessment and key takeaway messages for all the components and technologies developed as part of ASSURED, highlighting the motivating factors behind the design of these technologies, and their innovations compared to state-of-the-art solutions. In D7.5 [7], we provided **exploitation strategies** for all the core offerings of ASSURED, highlighting their value propositions and their positioning in the market for modern cybersecurity solutions, highlighting the value they may offer to modern supply chain ecosystems. We also presented business strategies for the market deployment of various ASSURED Components. In this deliverable we approach the evaluation of ASSURED from an **application perspective,** by performing an assessment of the impact of ASSURED on various application domains, through the lens of the four envisioned use cases, namely *Smart Manufacturing, Smart Cities, Smart Aerospace,* and *Smart Satellites*.

One important consideration that is at the forefront of the design philosophy of ASSURED is the notion of **zero trust**. The main concept behind this security model is the motto *"never trust, always verify"*, which essentially means that no user or device can be considered trusted by default, even if they have been previously securely enrolled to the network. The notion of zero trust is increasingly important in modern supply chain ecosystems, as the handling of sensitive and personally identifiable data creates a wide variety of security and privacy requirements. For example, consider the *Smart Cities* use case envisioned in ASSURED. In this case, devices such as IP cameras and smoke sensors collect operational data in the context of public safety. It follows that we need to be able to provide strong **security and trustworthiness guarantees** with regard to the handling of such data, as well as guarantees on the **user and identity privacy** for the users participating in such systems. This extends to the notion of **granularity of data access**, since we should be able to ensure that only users with the required attributes (e.g., police officers or firefighters) are able to access a set of stored operational or attestation data.

Building upon the notion of zero-trust, which is the main model ASSURED depends on, we have developed all the aforementioned core enablers and technologies. These are coupled with **open-source implementations**, not only to avoid fragmented adoption from the framework, but also to **provide a pragmatic framework** that escapes pitfalls commonly present in similar large endeavors, that either create new technologies with limited applicability, or provide limited improvements to existing solutions. In this deliverable, we build upon the analysis provided in D7.4 [8] in order to evaluate how ASSURED achieves the fulfilment of the extended set of **requirements and business needs** of various application domains, not only for the ones defined by the aforementioned use cases, but also domains that go beyond these. The aforementioned business needs are related to **operational assurance requirements** of the devices, but also **security and privacy requirements** of the devices to capture various data sharing profiles.

1.2 RELATION TO OTHER DELIVERABLES

This deliverable is horizontally related to all ASSURED WPs, covering WP1 and WP6 as it pertains to the requirements of the ASSURED framework in the context of the envisioned use cases, but also to all the technical WPs (WPs 2, 3, 4, and 5) pertaining to the critical appraisal of the core technologies developed as part of ASSURED, including remote attestation, trusted computing, Blockchain technologies, runtime tracing, and lightweight crypto primitives.

This deliverable directly gets input from D6.4 [6] which provides the adoption guidelines for all the technologies developed as part of ASSURED, as well as D7.6 [1], where we provided an initial version of the impact assessment for all the core artefacts of ASSURED, key takeaways for each of the developed components, and strategic impacts of the ASSURED framework as a whole. In this deliverable, we build on these outcomes, and we expand on them, considering the implementation of the final version of the framework and the integration of all newly developed and updated components. Specifically, during the second reporting period, the integration of the TPM-based Wallet has been performed, which has enabled the interaction of the devices with the Blockchain Infrastructure, as well as the usage of the lightweight crypto schemes.

Towards the goal of ASSURED of achieving “security- and privacy-by-design” solutions, we have provided and critically appraised the research activities carried out as part of ASSURED, and incorporated in a novel architecture for the secure configuration, deployment, operation, and verifiable computing of safety-critical devices. All these trust extensions will be evaluated in the context of WP6, and specifically deliverable D6.3, where focus will be experimentation of all the ASSURED artefacts in the context of all the envisioned use cases, and their evaluation and performance analysis on top of the innovation analysis and impact assessment put forth in this deliverable.

D7.7 and D6.4 are essentially the two final deliverables of the ASSURED framework, where we evaluate and assess all features of ASSURED from a technical standpoint, but also from an integration standpoint. Specifically, we expand on the actions taken towards extending the state-of-the-art providing value propositions to fulfil the needs of the envisioned use cases. These deliverables take input from all previous deliverables of ASSURED, both the various technical deliverables, and the one related to the evaluation of the ASSURED framework in the context of the use cases (namely D6.2 and D6.3) in order to perform the final assessment of the project outcomes.

1.3 STRUCTURE OF THE DELIVERABLE

This deliverable is structured as follows: In **Chapter 2**, we provide a description of the strategic assets and core technical artifacts developed as part of the ASSURED framework, and we summarize the core achievements per component, focusing on the core value propositions pertaining to the vision and objectives of ASSURED. In **Chapter 3**, we analyze the impact and benefits of ASSURED in the context of the application domains represented by the four envisioned use cases (*Smart Manufacturing, Smart Aerospace, Smart Cities,* and *Smart Satellites*), by highlighting the key challenges for each domain, and the functionalities of ASSURED that are able to address these challenges. We also provide a summary of the initial analysis on how ASSURED can benefit other application domains beyond the four use case domains. In **Chapter 4**, we provide an analysis of the Strategic Impacts of ASSURED, focusing on the core vision of the EU for enabling trust assessment of modern supply chain ecosystems, as well as improving the security posture of the EU in the domain of cybersecurity. Finally, **Chapter 5** concludes the deliverable.

2 HARDENING THE SUPPLY CHAIN STACK: INTERTRUSTABILITY OF "SYSTEMS-OF-SYSTEMS"

As aforementioned, the purpose of this deliverable is to assess the various building blocks and technologies of ASSURED in the context of the envisioned use cases. Therefore, this Chapter is dedicated to the **core technologies** developed as part of ASSURED, as well as the **innovations and value propositions** set forth by these technologies. Note that these were extensively documented in D7.5 [7] and D6.4 [6], but here we provide, for the sake of completeness, a brief summary of the core dimensions where ASSURED has provided value propositions. Recall that the core target of ASSURED is to provide **operational assurance** to complex supply chain ecosystems comprising heterogeneous devices with various security and privacy requirements, running mixed-criticality services, throughout their operational lifecycle. To this end, ASSURED aims to fulfill the **requirements of the users and stakeholders** with regard to the **security and privacy** of the users and the handled data. Here, we outline how the ASSURED components work towards achieving the fulfillment of those requirements.

In order to achieve runtime operational assurance of the devices belonging to the service graph chain, we have implemented the **ASSURED Attestation Toolkit**, containing a variety of attestation schemes. These are essentially the core mitigation measures provided by the ASSURED framework in order to address any threats and vulnerabilities identified for the assets and devices belonging to a target system, and are supported by the TPM-based Wallet of each device. For example, the **Configuration Integrity Verification (CIV)** scheme can be used to attest to the correctness of the configuration state of a device, the **Control Flow Attestation (CFA)** scheme can attest to the correctness of the execution of a software process, and **Swarm Attestation (SA)** can attest multiple devices simultaneously in an efficient manner. The enhanced **Direct Anonymous Attestation (DAA)** designed as part of ASSURED provides privacy-preserving properties to these attestation schemes, as well as linkability and revocation capabilities. Finally, **Jury-Based Attestation** can resolve conflicts between devices in case of a contested attestation result, through a voting process among a jury of devices. These attestation schemes have been designed so that several different scenarios can be addressed in the context of the target use case application. For example, consider the *Smart Aerospace* use case, where the Ground Server Station (GSS) aims to securely deploy an update package to the Secure Service Router (SSR) of an aircraft. In this case, a CIV attestation is performed before the update in order to check that the aircraft is in a trustworthy state, and after the update in order to verify its correct installation. In addition, CFA is used in order to verify the correctness of the installation process itself.

The enforcement of the attestation schemes is managed through the **ASSURED Blockchain Infrastructure**, which is responsible for the **management, deployment, and enforcement of security policies** in an **efficient, auditable, and certifiable manner** through the use of **smart contracts**. This enables the monitoring and recording of the **correct execution of policies**, and enables the assessment of trust in the devices at any point in time. The outcomes of all attestation processes are recorded on the ledger, thus ensuring the **certifiability and auditability** of the entire process and providing **trust evidence collection and knowledge sharing capabilities**, while maintaining the security and privacy of the devices and the confidential data. Such evidence will be valuable and highly usable to current or future cyber-security certification authorities that seek up-to-date verifiable operational assurances for security-critical devices that remain intact from unauthorized accesses. This essentially creates a **hygiene data space**, which enables monitoring the state of the devices by keeping threat intelligence data in a secure and auditable manner, while providing system entities with the capability to check and verify the status of the devices, while also making this verification accessible to third party auditors.

For the creation of the optimal set of security policies to be deployed to the devices, we have developed the **Risk Assessment and Policy Recommendation Engines**. The Risk Assessment Engine is able to evaluate the risk level affecting the devices and the system as a whole, considering the **threats and vulnerabilities** affecting such devices, the **interdependencies** between the assets, as well as the **types of evidence that must be collected and monitored in a verifiable manner** in order to assess specific device properties, such as security, privacy, integrity, and correctness. The output of the Risk Assessment is forwarded to the Policy Recommendation Engine, which is responsible for calculating the optimal set of policies to be deployed to the devices, considering the available computational resources at the devices, any time constraints imposed by the specific use case, as well as the available mitigation enablers for the identified threats and vulnerabilities (e.g., attestation schemes).

All the aforementioned schemes are supported by the implementation of an **SSI-enabled Wallet** at the devices, leveraging the HW-based Trusted Component of the device, which aims to provide devices with control over their own identity through the **Self Sovereign Identities (SSI)** concept. The Wallet achieves the hardware binding of the device to the cryptographic keys, enables secure storage and management of the required cryptographic material, and enables each device to provide **verifiable evidence on its identity and configuration state**. This enables the issuance of a set of **Verifiable Credentials (VCs)** of the device containing the total set of device attributes. Afterwards, the device is able to create a **Verifiable Presentation (VP)** containing a subset of these attributes in order to access a service or set of data stored on the Blockchain.

Towards the conversion of the device into a **secure edge accelerator**, ASSURED has developed a set of lightweight crypto schemes that utilize the aforementioned cryptographic material. Specifically, **Attribute based Encryption (ABE)** serves to protect sensitive information (attestation evidence, such as control-flow and configuration traces) in order to make it available only to stakeholders that possess the necessary attributes (granularity of data access), while **Dynamic Symmetric Searchable Encryption (DSSE)** is used for performing queries on encrypted information, without revealing the information itself. Authentication and access to the information will be initiated firstly through the Secure Device Enrollment, and then through **Attribute Based Access Control (ABAC)** and ABE. Note that the **Secure Device Enrollment and Zero-touch Onboarding** scheme is required for the operation of all aforementioned schemes, since it connects to the need to correctly create and manage various types of keys to be used throughout the entire lifecycle of the device.

In the following, we expand on these topics, by providing details on the core value propositions set forth by ASSURED in the context of the aforementioned key aspects and components.

2.1 VALUE PROPOSITIONS OF ASSURED AND SUMMARY OF RESEARCH ACTIVITIES

We previously provided a brief summary of the core value propositions of ASSURED through the various components and technologies developed throughout the project. Here we expand on these, by providing further information on the innovations performed as part of these components, as well as their capability to fulfil the security, privacy, and trustworthiness requirements of the types of supply chain ecosystems considered in ASSURED.

2.1.1 Highlights and Core Achievements

The outcomes of ASSURED pertain to the completion of the design and implementation of all envisioned components, as well as their integration into the final version of the overall framework. Table 1, we provide a brief overview of each of the building blocks of ASSURED,

as well as the **core achievements** associated with each of the completed and integrated components, and how they operate towards achieving the **core objectives and vision** of ASSURED. Note that a more detailed analysis of these achievements is also provided in D6.4 [6] and D7.5 [7].

TABLE 1: ASSURED HIGHLIGHTS & STRATEGIC ASSETS

Risk Assessment Engine
In ASSURED, we have developed a Risk Assessment engine, which is able to identify the risks affecting the assets of a target system (and calculate the respective risk score), as well as the system as a whole, based on the identified threats and vulnerabilities of the assets. The Risk Assessment engine is also able to consider the interdependencies between the assets in the calculation of risk. To this end, we have designed and implemented a methodology to calculate an exhaustive list of attack paths containing the set of moves that an adversary may make in order to compromise a target asset. Note that different types of properties are impacted by different types of threats and attack vectors to differing degrees, and there are several properties that can be assessed based on evidence collected using the available evidence collection mechanisms. These may include security, privacy, integrity, consistency, verifiability, and accuracy. The Risk Assessment scheme also considers the type of evidence needed to assess each of these properties. To assess the risk level affecting the assets and the system as a whole, while we adopt CVSS v3.1 as the scoring system, the Risk Assessment scheme achieves a high level of modularity, since it enables the adoption of additional scoring systems and methodologies, that may be more appropriate for a specific application domain (such as TARA for automotive systems). Thus, we are able to merge and consolidate the outputs from potentially different methodologies into a singular Risk Assessment outcome, by integrating and leveraging these different types of methodologies. Note that the outcomes are provided in a universal specification language that we created, so that the output of the Risk Assessment engine can be universally interpretable by various types of systems and components. Notably, one of those is the Policy Recommendation Engine, which receives the output of the Risk Assessment and uses this information in order to calculate the optimal set of security policies.
Policy Recommendation Engine (PRE)
The Policy Recommendation Engine is able to calculate the optimal set of security policies to be deployed in the assets of the system, considering the time and resource constraints of the system, the available mitigation measures (considering sets of tasks to be considered depending on the level of security required), as well as the interdependencies in the assets in the context of the attack paths defined by the Risk Assessment engine. The optimization process considers also the priorities on the factors to be considered in the optimization process, such as security, time of execution, or a combination of the two. The solving of the optimization problem for optimal attestation policy calculation is quite efficient, since it was implemented based on **multi-objective optimization considering additional security and trust aspects**. This approach does not depend on an external solver and exhibits polynomial complexity relative to the number of assets (as opposed to the exponential complexity of existing solutions). In addition, in order to achieve the required level of granularity in the developed policies so that we are able to accurately capture all the security and privacy requirements of the target system, we use an XML-based and JSON-based expressive language, which is a human-readable format that can be used for the depiction of all information about the problem and its related optimal policy.
Attestation Toolkit
We have designed a fully-fledged attestation toolkit that is able to assess the correctness of a device, not only during bootup, but also during runtime. It provides mechanisms that attest to the correctness of the configuration state of the device, but also the correctness of the execution of a software process and the behavior of a device. Specifically, the **Configuration Integrity Verification (CIV)** scheme enables a device to attest to the correctness of its configuration state in a privacy-preserving manner through a local attestation mechanism based on the use of key restriction usage policies. These only allow the usage of the attestation key if the device is in a correct state, thus ensuring that the signature itself is proof of the correctness of the device, and no further information is needed from the Prover device (i.e., the Prover does not need to share a device state quote with the Verifier). The **Control Flow Attestation (CFA)** scheme is able to attest to the correctness of the execution of a software process, through the classification of control flow traces into benign and malicious. Note that ASSURED is the

first project of its kind to demonstrate AI-assisted CFA, which can significantly increase the accuracy of classification, not only against ROP attacks, but also against DOP attacks (which are typically very hard to detect, since they do not entail alterations in the control flow graph). In addition, it can operate with less semantically rich information, thus reducing the volume of data that needs to be traced and increasing the efficiency of the scheme, without reducing the accuracy of the classification. The **Swarm Attestation** scheme attests to the correctness of multiple devices simultaneously, leveraging the CFA or CIV schemes, depending on the type of attestation needed. It is able to support different sizes of swarms with varying numbers of devices, also considering devices that need to execute the same attestation task, or different attestation tasks. It is able to perform attestation in a privacy-preserving manner, while also enabling linkability and revocation features in case a device is deemed untrustworthy. It is also able to consider dynamic swarm topologies, where a mobility factor for the devices is considered. The attestation schemes are supported by an enhanced **Direct Anonymous Attestation (DAA)** scheme, which provides privacy-preserving features to the devices, with additional linkability and revocation features, and also enables devices to create privacy-preserving attribute-based signatures. Finally, **Jury-based Attestation** is able to solve conflicts between devices in case of a failed attestation, by formulating a jury of devices that provide their opinion on the correctness of the outcome of an attestation, and provide a second line of defense in addition to the primary attestations performed.

Runtime Tracer

The runtime tracing capabilities of ASSURED are able to collect configuration information about the device, or control flow information from the execution of a software process, so that they can be used as evidence in the aforementioned attestation schemes. ASSURED offers both SW-based and HW-assisted tracing capabilities, thus providing greater flexibility in the deployment of such mechanisms. These schemes are both able to achieve a high level of granularity and accuracy in the collected data, and can be used in tandem, depending on the computational capabilities of the device. Specifically, HW-assisted tracing is performed through the use of the ARM CoreSight architecture, which is supported by a wide range of modern commodity embedded systems, thus showcasing its feasibility and applicability in practical supply chain ecosystems. One core achievement of the Tracer is its execution in a secure environment, such as a Trusted Execution Environment (TEE), thus providing assurances on the correctness of its own traces, through the use of a Tracer Key used to sign the generated traces. This is a significant milestone in the establishment of tracing capabilities in a secure and authenticated manner, as part of the overall Trusted Computing Base (TCB) of the device. Finally, increased performance of the SW-based Tracer is achieved through the use of non-intrusive memory introspection over software instrumentation.

Use of Blockchain for certifiability and auditability

The ASSURED policy-compliant Blockchain Infrastructure has been designed for enabling enhanced auditability and certification of all data-sharing transactions throughout the operational lifecycle of a system, capturing relevant security and privacy requirements. Specifically, it offers the secure and auditable deployment and enforcement of security policies through the use of smart contracts, which can be downloaded by the devices responsible for their execution in a manner that enables the auditability of the performed actions. In addition, the outcomes of the attestation processes are stored in the form of an attestation report. These are accompanied by encrypted raw data used as attestation evidence, which is stored in an off-chain storage facility and associated with the corresponding attestation report. For querying over encrypted on-chain and/or off-chain data, ASSURED has developed a Dynamic Symmetric Searchable Encryption (DSSE) scheme, which enables efficient querying for a set of data based on a set of keywords, which is available on a public ledger and accessible to all external third parties. Identity management mechanisms for controlling access to on-chain data are also provided, leveraging the notion of Self-Sovereign Identities (SSI), through the management of Verifiable Credentials (VCs) and Verifiable Presentations (VPs) for only disclosing the attributes needed for accessing a resource on the ledger. For scalability purposes, ASSURED employs Blockchain Peers that manage interactions between devices and the Blockchain, and enables the addition of further Peers to increase the number of transactions and devices supported. The integration of Roots-of-Trust (RoTs) with the Blockchain Peer enables its conversion into a secure anchor which enables checking the veracity of the performed transactions. To support all the aforementioned interactions, appropriate interfaces and commands have been developed in order to enable the support of secure and verifiable data transactions through HW-based RoTs.

Identity Management with SSI Wallet

ASSURED offers an SSI-aligned Wallet which is based on the use of a HW-based RoT in order to enable devices to provide verifiable claims over their own identity, and is the cornerstone of the identity management schemes of ASSURED. Specifically, the Wallet enables the use of HW-based keys for achieving HW binding of the Wallet and the Host device, thus meeting all necessary trust requirements of a Holder as part of SSI ecosystems. The ASSURED Wallet is the first of its kind to support device binding, anonymity, unforgeability, and selective disclosure as part of Verifiable Credential (VP) and Verifiable Presentation (VP) management. Specifically, through the use of VCs and VP, ASSURED offers a two-step approach to access control with identity management: (i) At the first step, we use certificates that authenticate the validity of a device, ensuring that it is correctly enrolled and possesses a Wallet with a valid secure element. (ii) At the second level, we provide an Attribute-Based Access Control (ABAC) scheme, which enables a device to demonstrate that is possesses the attributes needed in order to access a specific resource, by leveraging its Wallet to create and provide a VP containing only the required attributes. Note that this action is performed through a smart contract, in order to ensure auditability and certifiability.

Lightweight Crypto

ASSURED provides a set of lightweight crypto and key management schemes which capture the traditional notions of confidentiality, integrity, and availability, but are also lightweight enough to run on the edge devices. These crypto schemes leverage the RoT embedded in the devices, and offer a wide array of benefits, such as (i) the ability to operate in **real-time** without much induced latency, (ii) capturing different types of **security, privacy, and trust requirements** belonging to various application domains, (iii) impose **minimal additional computational overhead**, and (iv) can be used in **highly distributed and/or remote applications** with significant resource and power constraints. Specifically, the **Attribute-Based Encryption (ABE)** scheme enables different levels of granularity, by enabling devices that have been securely enrolled into the ASSURED framework to encrypt their attestation raw data in a manner that enables them to control who can access and decrypt this data based on their attributes and privileges. In addition, ABE enables the Encryptor device to encrypt data in a manner that ensures that no entity can infer any information about which attributes correspond to which sets of data, thus providing the required security and privacy guarantees to the devices. We have also implemented a **Direct Anonymous Attestation (DAA)** scheme, which enables devices to create signatures as a zero-knowledge proof to convince the Verifier that the signer possesses a valid membership credential, but without the Verifier learning anything else about the signer's identity. The enhanced **Attribute-based DAA protocol (DAA-A)** scheme enables devices to leverage their Wallets with HW-based keys to demonstrate the possession of a set of attributes, without revealing the attributes themselves. Note that a core consideration in the design of the crypto schemes was **crypto agility,** meaning the ability to support various types of crypto schemes and signatures so as to capture different types of security and privacy requirements, but also to manage the specific resource constraints of edge devices.

Overall, the ASSURED project has drawn considerable attention from both the **Trusted Computing community, and the Decentralized Identity Foundation (DIF)**, whose purpose is to support and advance the research and development efforts towards establishing a set of interoperable global standards. More information on all the standardization activities performed by ASSURED in an attempt to shape the security and trust requirements as we are witnessing the evolution of interconnected societies is documented in D7.3 [19]. From all the above, it follows that significant advancements in the state-of-the-art have been performed by the ASSURED consortium, which not only advance the state of cryptographic research in the European Union, but also facilitate the transition from outdated traditional notions of security to holistic, continuous, runtime operational assurance of complex large-scale Systems-of-Systems.

3 ASSURED IMPACT ASSESSMENT IN TARGET APPLICATION DOMAINS

As aforementioned, four different use case demonstrators have been envisioned in the design and implementation of the ASSURED framework, namely *Smart Manufacturing, Smart Cities, Smart Aerospace*, and *Smart Satellites*. These have been chosen as safety-critical application domains with varying security, privacy, and trustworthiness requirements, and varying time- and safety-critical functions running in the infrastructures of each use case. The motivation behind the selection of these verticals was to capture a wide range of application domains, in order to provide a versatile way to assess how ASSURED can capture requirements of complex service graph chains as part of modern supply chain ecosystems. These use cases gave ASSURED the capability to evaluate the designed and implemented components and technologies in **all phases of supply chain management**, starting from device manufacturing and enrollment, including runtime operational assurance of the devices, and capturing the entire operational lifecycle of a device and the system as a whole.

It is important to note that the ASSURED artefacts have been designed in a generic manner, that **enables their adoption by a wide variety of organizations, regardless of the specific implementation of their infrastructure** and belonging to a wide range of application domains, even going beyond these defined by the four aforementioned use cases (thus, achieving high degrees of interoperability). They have been designed in a manner that is able to address security and privacy requirements that typically characterize the types of supply chain ecosystems targeted by ASSURED, regardless of their scope, scale, and purpose. This highlights the high adaptability and applicability of ASSURED, which took practical concerns into account in its design and implementation.

This chapter aims to analyze the impact and the benefits that the ASSURED framework brings forth to the application domains envisioned by the project's internal demonstrators. More specifically, in what follows we elaborate on how the ASSURED developments have contributed to form a new standpoint for each one of the demonstrators in the application domains of **Smart Manufacturing, Smart Aerospace, Smart Cities for Public Safety, and Smart Satellites**. In Table 2, we briefly present the key aspects of ASSURED that we focus on in each domain, which represents the impact that we should evaluate in the context of this deliverable.

TABLE 2: KEY ASPECTS OF ASSURED PER APPLICATION DOMAIN

Use Case	Discussion
Safe Human Robot Interaction in Automated Assembly Lines (Smart Manufacturing)	A safety-critical application where human workers and robotic arms work in tandem within a manufacturing floor, and aims to ensure the safety of the workers by using reliable indoor positioning systems and activity recognition systems. The purpose is to avoid collisions and accidents between these entities. It follows that it is imperative to ensure the correctness of the accident prevention system, in order to reliably prevent physical harm to human workers.
Secure Collaboration of Platforms-of-Platforms for Enhanced Public Safety (Smart Cities)	This use case involves the development of the smart cities concept, and aims to ensure the secure operation of critical infrastructure and systems, as well as the physical safety of citizens. Since this use case involves the use of sensors (e.g., smoke and gas sensors) and IP cameras in the context of public safety, ASSURED aims to ensure the privacy of users and citizens participating in such environments, as well as the protection of sensitive information handled by the aforementioned devices.
Secure and Safe Aircraft Upgradability and	This use case involves the operation and maintenance of safety-critical aircraft services that entail the execution of secure software processes

Maintenance (Smart Aerospace)	and component upgrades. In this context, ASSURED aims to ensure the correctness of the deployment of software packages from the Ground Station Server (GSS) to the Secure Service Router (SSR) of the aircraft, while also ensuring the correctness of the update process, as well as the state of the aircraft before and after the update.
Digital Security of Smart Satellites (Smart Satellites)	This use case entails the collaborative execution of safety-critical processes between low-earth orbit satellites, referred to as CubeSats. In this context, ASSURED aims to attest to the correctness of the operational state of the CubeSats, as well as the safety-critical mission applications executed on them. In addition, the integrity and confidentiality of the data exchanged is of paramount importance, as there are very strong requirements regarding the integrity and the confidentiality of the communication between the Ground Station and the CubeSats.

3.1 DEMONSTRATOR #1 – SMART MANUFACTURING

In the context of applications belonging to the *Smart Manufacturing* application domain, one of the core operations pertains to the execution of real-time indoor localization services that monitor the movement of machinery (e.g., robotic arms) operating within a manufacturing floor, and detect the positions of machinery in relation to human workers, in order to prevent collisions and accidents. These services are particularly needed for manufacturing processes that require the involvement of humans and robots to assemble heavy and complex units such as car engines or power supplies, with robots assisting in carrying these heavy products for assembly. Therefore, it follows that such organizations are subject to **strong trustworthiness requirements**, and **timely and efficient mitigation** of any threats or vulnerabilities (such as malfunctioning devices or location sensors) is imperative.

Typical cyber-physical components in a Smart Manufacturing environment include **robots**, **Programmable Logic Controllers (PLCs)**, safe **microcontrollers**, **wearables** (e.g., human motion capture suit), **positioning systems**, and **wired and wireless communication technologies**. In addition, there may be a central **gateway** responsible for the aggregation of information originating from these devices. Ensuring the safe operation of these systems, as well as the establishment of secure communication channels between the devices and the gateway, presents security challenges that require assurance of the correct behavior of these systems at all times. Potential breaches of the integrity and trustworthiness of the devices and the data generated by these systems by malicious actors can lead to fatal incidents. However, even relatively simpler attacks that result in unwanted halting of the system may lead to significant monetary damage for the manufacturing organization.

The integration of the ASSURED framework into such manufacturing environments is able to provide the security and trustworthiness guarantees required for the smooth and uninterrupted operation of the entire system. By integrating ASSURED, the system is protected at all stages of the manufacturing process, including the secure enrolment of devices, the verification of the correctness of the system's hardware and software, the continuous monitoring of the system during runtime, and the establishment secure communication channels. It can also ensure that only authenticated personnel or trusted devices can access the system. Therefore, **the focus of the Smart Manufacturing case is the security and safety in the establishment of trust relationships between users and devices.**

3.1.1 Challenges in Future Proofing the IIoT Domain

The industrial Internet of Things has revolutionized the smart manufacturing landscape, offering unprecedented efficiency and productivity gains. However, this transformation also brings along a myriad of safety challenges. One of the primary concerns is the **vulnerability of interconnected devices and systems** to cyber threats. As IIoT devices are often

interconnected through networks, they become potential entry points for malicious attackers to infiltrate the manufacturing infrastructure, leading to data breaches, system disruptions, and intellectual property theft. Moreover, the sheer number of connected devices makes it challenging to monitor and secure each one effectively. **Ensuring data privacy and integrity while transmitting sensitive information is another pressing issue. Additionally, the integration of autonomous robots and collaborative robots introduces new safety risks, such as human-machine interactions, which require careful planning and risk assessment**. Addressing these safety challenges is essential for the successful and sustainable growth of the smart manufacturing sector.

Therefore, in the Smart Manufacturing domain, since there are many devices communicating between them as previously outlined, we must ensure the integrity of the location sensors providing localization data for workers and devices in order to ensure the **trustworthiness of the exchanged data**. In this regard, the two dimensions that need to be addressed for future proofing this domain are (i) the **integrity of the devices**, which entails the real-time and timely monitoring of all device states, and (ii) the **communication integrity** in communications between devices and between a device and the gateway by ensuring that all data is encrypted and correctly signed, towards creating a community of trust between all the sensors operating within a manufacturing floor. In addition, we need to provide mechanisms for **a trust domain to securely exchange information with another trust domain**. A trust domain may be a manufacturing floor, that needs to securely exchange device state information with a different manufacturing floor.

Considering all the above, Table 3 outlines the key security challenges, their potential impact, and the functionalities of the ASSURED framework that address them.

TABLE 3: KEY CHALLENGES IN SMART MANUFACTURING DOMAIN

Security Challenge	Impact	ASSURED Functionality
Unauthorized Access	Access to the connected devices of the smart manufacturing infrastructure by a malicious actor can compromise safety critical processes of the manufacturing floor which can result in harm to infrastructure and more importantly the workers. Unauthorized access can appear in different dimensions, such as (i) introduction of a malicious device in the framework, and (ii) unauthorized access to device state information.	ASSURED offers security services in order to address the various dimensions of unauthorized access. (i) In order to prevent the introduction of malicious devices, the **secure enrollment** process is able to authenticate the device before it becomes part of the network, and verify that it possesses an authentic Wallet. It can also verify that the device is in a correct and expected state, based on the Manufacturer Usage Definition (MUD), which is downloaded for each device from a MUD server. If these checks are successful, the device can create the required cryptographic material and keys in order to utilize the security services of ASSURED. (ii) In order to prevent unauthorized reading or querying for device state information, ASSURED provides the policy-compliant **Blockchain Infrastructure** that enables secure and privacy-preserving data sharing, with mechanisms such as ABAC and ABE. In the case of device-to-device communications, the **key migration** scheme is able to establish secure and authenticated communication channels between devices.
Malicious Hardware and Software Updates	A malicious device, software or an update to existing software can be introduced to gain access, extract information, or hinder the	In order to prevent malicious software and hardware updates, the ASSURED attestation toolkit provides the mechanisms needed to ensure the trustworthiness of the update process. For example, the CIV scheme can ensure the

	underlying manufacturing process. Therefore, we need to provide methods that ensure both the correctness of the configuration state of the device, and the correctness of the execution of a software process.	correctness of the configuration state of the device both before and after the update, while CFA can ensure the correctness of the update process itself. In addition, Jury-based Attestation can be used in case where the correctness of the device state is contested, so that the devices belonging to the network can decide on the result of the attestation process.
Software Vulnerabilities	Software vulnerabilities may be introduced for various reasons. In addition to tampering by a malicious party, they may be caused by outdated software, incorrect configuration, or compatibility issues. Such vulnerabilities can be exploited during the runtime of the manufacturing process, resulting in malicious behavior explained above.	In order to prevent compromises caused by software vulnerabilities, the CFA scheme is able to perform continuous monitoring of such safety-critical software processes. Specifically, after the Runtime Tracer collects control flow information from the execution of such a process, the ML-based CFA scheme leverages AI-assisted techniques in order to distinguish between benign and malicious traces (and detect potential malicious activity, such as ROP and DOP attacks). Afterwards, in case the CFA identifies such a deviation, the Attack Validation component can be used in order to pinpoint the exact point in time in the execution flow of the process where this deviation was detected, so that the security officer or administrator of the system can use it in order to perform further analysis.
Secure Communication	An intrusion of the communication of the interconnected devices can result in extraction of secret or safety critical information. Furthermore, the communication can be poisoned to attack the manufacturing process and compromise the integrity of safety-critical information, such as localization data.	In ASSURED, we have provided the mechanisms required in order to establish secure and authenticated channels and to ensure the integrity of the transmitted data. In this regard, we identify two key aspects: (i) In order to establish secure device-to-device communication, ASSURED provides the aforementioned **key migration** scheme. This is supported by the attestation agents responsible for handling communication between the devices, and the Wallet which is the overarching component responsible for managing credentials and cryptographic keys. (ii) In order to securely disseminate attestation evidence and sensitive information (such as localization data), ASSURED provides the ABE scheme, which enables the secure storage of such data.
Secure Storage	Safety critical information or secrets about the processes are needed to be stored securely in order to prevent leaking of information and potential attack vectors to the system, while only allowing authenticated parties to access the information.	ASSURED provides an Off-chain Storage Facility, which is able to store ABE-encrypted operational data (such as localization information), or raw traces used as attestation evidence. These are associated with the corresponding attestation report stored on the ledger through a location pointer to the off-chain data. Both the attestation reports and the attestation- and operational-related data can only be accessed by devices that can verifiably demonstrate the required attributes through the creation of a VP.
Zero Trust	Incorporating zero trust principle allows minimizing the risk of unauthorized access, data breaches, and cyber-attacks, safeguarding	In ASSURED, pertaining to the adoption of the zero-trust principle, we assume that no device is considered trustworthy by default, and that the deployed devices do not have an inherent level of trust. In this regard, the **secure enrolment** scheme

	sensitive production information, intellectual property, and operational processes within a smart manufacturing ecosystem.	provides mechanisms that check and verify the correctness of devices before they are onboarded to the framework and are able to create the required cryptographic material. In addition, we provide the **runtime tracing mechanisms** that operate within the Trusted Computing Base (TCB) of the device, thus enabling the collection of evidence that can be used to assess the level of trust in a device in a verifiable manner through the various attestation enablers.
Interoperability of Different Trust Domains	A smart manufacturing system requires diverse systems and devices from various manufacturers and industries working together. Lack of interoperability of these systems results in operational inefficiencies which limits the systems potential to maximize productivity.	In the context of Smart Manufacturing, we consider that each manufacturing floor with the devices and machinery within the floor can be considered as its own trust domain. Recall that, through the SSI-enabled Wallet, ASSURED enables each device to make verifiable statements on its identity and operational/configuration state. ASSURED is able to consider the hierarchical composition of these devices, for example in the consideration of device interoperability in **Risk Assessment**, as well as to aggregate these statements with the **Swarm Attestation** of devices. These can be used to make statements to be disseminated to different trust domains, i.e., manufacturing floors.
Ease of Deployment	A successful smart manufacturing system must be able to integrate new technologies into its existing infrastructure quickly in order to reduce downtime and operational disruptions. In addition, simplified deployment enables scalability, leading to increased productivity and flexibility in adapting to changing industry demands.	All security controls of ASSURED can be placed in the context of converting a device into a **secure edge accelerator**. This has been designed in a manner that enables the easy deployment of the security mechanisms through libraries, as well as provide crypto agility regarding the employed cryptographic primitives in a transparent manner.

3.1.1 Results and Impact Assessment

In the previous Section, we discussed the challenges posed by highly interconnected systems used to create smart manufacturing infrastructures. Especially with the emergence of Industry 5.0, which aims for more human-centric solutions where humans and machines work together, mitigating these security challenges and creating a safe environment for workers is paramount. In the context of ASSURED, we have performed experimental evaluations on the implemented security enablers in order to assess its ability to create a trusted and secure infrastructure. In our results, detailed in D6.3 [9], we were able to secure all aspects of our demonstrator, from enrolling all our devices securely, ensuring correct behavior of the systems during runtime, creation of secure communication channels and providing authenticated access. With these results, ASSURED provides a strong value proposition, especially as an open source out-of-the-box security solution that can compete with closed source proprietary systems.

In Table 4, we summarize our key results on how ASSURED played the role of the much-needed security solution. In D6.4 [6], we presented an extensive set of security challenges of the ASSURED framework. Here, we detail how ASSURED assists in capturing the business needs and challenges in the Smart Manufacturing use case.

TABLE 4: KEY RESULTS OF INTEREST FOR ASSURED TESTING IN SMART MANUFACTURING

Smart Manufacturing: Deployed sensors and data must be protected with appropriate controls to ensure their integrity, confidentiality, and availability throughout their entire life cycle
Key Results of Interest for ASSURED Testing
Only the devices and software that are trusted and secured are allowed to function in the smart manufacturing infrastructure. In this regard, only **certified software** can be deployed, booted up, and updated in the uploaded devices. The devices are continuously monitored in order to ensure the correctness of the executed process or the configuration state of the devices, as defined by the manufacturer through MUD profiles.
All devices in the infrastructure with different trust domains have successfully established trust relationships and can now operate together. ASSURED is able to establish different trust relationships inside a complex ecosystem, both regarding the exchanged data, but also the devices which operate as nodes of the service graph chain. These nodes may be deployed to different trust domains (i.e., manufacturing floors), which may adhere to different security requirements. ASSURED gives the capability for devices to provide verifiable statements on their identity, needed in order to establish trust relationships. Even if the communicating parties reside in different trust domains, they can exchange these attributes towards the establishment of the required level of trust. This gives us the capability to enable and capture different types of trust relationships, through the hierarchical composition of systems-of-systems.
All the devices are continuously monitored against malicious behavior, based on optimally calculated security policies, which can also be updated during runtime. For example, in the case of a failed attestation, it is possible to identify new threats and zero-day vulnerabilities. Using the Attack Validation component, it is possible to pinpoint the specific point of intrusion and identify the type of attack, thus enabling the creation of appropriate policies with the mitigation actions needed to address the newly identified threat.
The communication channels between all devices are secured on multiple levels through cryptographic agility provided by ASSURED and adhere to strict confidentiality requirements. This is achieved not only through the aforementioned key migration scheme used to establish secure communication channels, but also through the lightweight crypto schemes of ASSURED, which are able to capture the different types of security, privacy, and trust requirements that might imposed by the varying actors and stakeholders of a smart manufacturing system.
Manipulation of the devices and software by malicious third parties are prevented through robust authentication and secure update procedures that enable one update to many devices and many updates to many devices. Through the attestation enablers, particularly CIV and CFA, it is possible to ensure the correctness of the update process, as well as the device state before and after the update.
Flexibility and scalability of the supply chain without compromising security is achieved through easy deployment of ASSURED. This is achieved through the provision of libraries and APIs, as well as the open-source deployment of most ASSURED components, including readme files with instructions on building, compiling, and deploying these components.
Ability to integrate new and legacy systems using ASSURED APIs and libraries. Note that it is very easy to integrate the ASSURED components into legacy systems. In contrast to closed-source security solutions that cannot be introduced to other systems or communicate with other security mechanisms, ASSURED is modular, open-source, and can overcome the challenges of closed-source or protected solutions which hinder applicability of the security solution.
In ASSURED, we have followed a novel software-hardware co-design approach in remote attestation, which has demonstrated significant promise in the domain of Device Manufacturing. This approach has been shown through experiments to be very efficient, while also providing strong security guarantees, thus providing a promising approach for the types of low-end embedded devices typically available in such systems, that unlocks the security capabilities of these devices in safety-critical domains.

The IIoT market can greatly benefit from such advanced security enablers, first and foremost to significantly reduce the number of accidents that can result from an attack on a vulnerable system. In addition, the trust and operational assurance provided by these enablers would ensure the uptime of the underlying system, preventing monetary losses from a system failure

resulting from an attack on a system vulnerability. Furthermore, offloading the security aspects of the system to these enablers would significantly reduce the development time of the underlying industrial system and the certification process, allowing earlier market entry.

It is important to note that the results of this section also apply to application domains with similar requirements, that entail the use of multiple devices operating in tandem, which are subject to strict security and privacy requirements. For example, this may refer to the use of medical equipment in hospitals, which consist of multiple departments with different requirements characterizing each department.

3.2 DEMONSTRATOR #2 – SMART AEROSPACE

The Smart Aerospace domain entails securing business processes and information flows in the communication between the components of the aircraft. Typically, there is a central component, referred to as the **Secure Server Router (SSR)**, which is responsible for interfacing between all other components (e.g., sensors and avionics computers). In addition, a **Ground Station Server (GSS)** is responsible for communication between the aircraft and the ground station (e.g., in order to deploy secure updates or to receive health information from the aircraft. All these components formulate the service graph chain in a typical Smart Aerospace system.

One example of a SSR device of an aircraft is the SSR7000. The SSR7000 (known also as Aircraft Identification Device – AID) is the primary communication facilitator between the aircraft's cockpit and the components of the aircraft. It allows for a data exchange between the avionics computer to the electronic flight bag devices at the cockpit where the pilots are using to inspect and react to certain events. At the same time, SSR7000 is enabled with a series of communication modules interfacing with dual ethernet-based ARINC protocols, LTE/4G and Wi-Fi, as well as radio communications. An additional usage is in the infotainment services for the passengers, as these services route Wi-Fi and other requests through established external links (through SATCOM or Mobile sessions). It follows that, in order to ensure the correct operation of all components in the aircraft during a flight and ensure that there are no accidents that may be caused by communication errors or malfunctioning components, there are strong security requirements that need to be fulfilled. In addition, in the deployment of secure updates from the GSS to the SSR during flight, it must be ensured that the aircraft is in a correct operational state before, during, and after the deployment of the update.

Therefore, in the context of the Smart Aerospace domain, we need to provide security services that are able to fulfil all the aforementioned requirements. In the context of the remote update services, a secure remote attestation service is required in order to securely update the firmware of the SSR (such as the SSR7000) in order to validate and verify its data integrity from an operation (installation and execution) point of view. Compatibility checks may also be part of a distributed attestation case where the aircraft as whole is being validated for its integrity and service correct functionality after the system's upgrade. One of the main challenges though that have to be faced is the certification evidence that ASSURED mechanisms need to yield in order to verify that its execution will not – at any point - harm the safety critical and security critical services of the system. In this regard, ASSURED is able to provide the security enablers so that a smart aerospace service provider can be used in order to provide operational assurance to the entire service graph chain. In addition, the automation capabilities of the ASSURED framework enable flawless integration on the end user side with respect to the attestation mechanism and the policy recommendation and enforcement engine.

3.2.1 Challenges in Security and Certifiability of Aerospace Systems

As it was previously outlined, Smart Aerospace applications are subject to strict security requirements pertaining to the correct operation of all the components running on an aircraft,

in order to ensure that device malfunctions or malicious activity do not impede the normal operation of the aircraft, or cause accidents or other incidents. In addition, it is imperative to ensure the integrity of the communications between the components, in order to ensure the integrity of the data transmitted between components, whether this refers to the deployment of a software update package, exchange of operational data between aircraft components, or transmission of health information from the SSR to the GSS. In this regard, in Table X we outline the security challenges that may affect a Secure Aerospace system, as well as the functionalities of ASSURED that can assist in addressing those challenges.

TABLE 5: KEY CHALLENGES IN SMART AEROSPACE DOMAIN

Security Challenge	Impact	ASSURED Functionality
Device secure remote firmware update using existing networks	Compromising the update process, either by malfunction or by the intervention of a malicious party, may cause the installation of incorrect or compromised firmware on the SSR, which may cause adverse effects on the operation of the aircraft. Enabling secure remote attestation through SATCOM or LTE/5G networks in order to enable over-the-air firmware updates of aircraft devices can drastically accelerate SSR device maintenance, reducing costs by a factor of 80% while monitoring its operation.	In order to enable secure updates on the SSR of an aircraft, ASSURED offers a set of attestation enablers that can provide trustworthiness guarantees to the update process. Specifically, we have implemented a scheme which consists of a CIV process both before and after the update has been deployed by the GSS in order to verify the correctness of the device state, as well as a CFA attestation to ensure the correctness of the update process itself. In addition, the **key migration** scheme enables the establishment of a secure communication channel between the GSS and the SSR, in order to ensure the integrity of the deployed software update package. This process enables the remote deployment of updates, which would typically need to be performed on a grounded aircraft.
Security Policy recommendation and enforcement not existing in current aircraft ecosystem	Enabling security policy enforcement in the computing infrastructure of an aircraft may be pivotal to the future air-mobility, maintenance, and safe and secure operations. Its impact will open further technology opportunities and air-services as the acceleration of new product and service deployment will not only impact current technology transition cycles (5-10 years) but also create a more regulated air-transport domain for safety and security regulations.	Typically, in the Smart Aerospace domain, the deployment of security policies is performed in an “all-or-nothing” manner, considering the aircraft as a black box, and without considering the inner workings of the aircraft. For example, the aircraft may consist of heterogeneous devices originating from different vendors or OEMs, which are subject to varying security and privacy requirements and may be more vulnerable to different types of threats. The ASSURED Risk Assessment and Policy Recommendation engine is able to provide security policies with the required level of granularity, to achieve the requirements of each asset (e.g., the sensors corresponding to the engine may need different security policies than the motors controlling the wheels of the aircraft).
Need for verification in the integration of new vendor products and system level solutions	The unverified integration of new components and devices can cause serious security concerns. New vendor products and system level solutions for the aircraft should be seamlessly authenticated as part of	In order to ensure that no untrustworthy components are integrated into the aircraft, the **secure enrollment and zero-touch onboarding** scheme is used in order to ensure that only trustworthy devices, which can demonstrate the possession of a valid device Wallet, can be onboarded into the system. In addition, the secure enrollment process is responsible for the required

	existing supply chain, in order to verify their integrity and ensure they do not represent a malicious party that may aim to harm the Smart Aerospace application.	cryptographic material that can be used by the device, organized in a secure key hierarchy with the DAA Key as a root. In addition, it is possible to download the Manufacturer Usage Description (MUD) from the MUD server, in order to register the correct state of the device, in order to enable integrity checks throughout the lifecycle of the device.
Need to perform integrity and conformance on aircraft during flight	Currently, no viable, certified solution exists in the aerospace domain that is trusted by airframers to enforce new system maintenance processes and actions into their systems by remote-enabled operations. Therefore, there is a need to remotely perform conformance and integrity checks, while the aircraft is in the air.	The remote attestation enablers of ASSURED provide the capability to the GSS, acting as a Verifier, to verify the integrity of the components of the aircraft. Specifically, by using the **CIV** scheme, the GSS can verify that the components of the aircraft are in a correct configuration state, specified by the Manufacturer Usage Description (MUD) provided by the device manufacturer, which was integrated in the secure enrollment process. In addition, the **CFA** scheme can verify the correctness of a software process running on the device. Finally, the **Swarm Attestation** scheme enables the GSS to verify the integrity of multiple components simultaneously and efficient in a single attestation operation, which are organized in a tree-based structure with the SSR of the aircraft as the root of the tree.
Deployment of security policies in a certifiable and auditable manner	Smart Aerospace applications are typically subject to various regulations and standards, so there need to be methods that ensure conformance to these standards. In this regard, the execution of the aforementioned security policy and attestation actions should be recorded in a certifiable and auditable manner, and their outcomes should become available to certification bodies and auditors.	The deployment and execution of security policies is performed through the use of **smart contracts**, which leverage the Blockchain Infrastructure in order to ensure the certifiability and auditability of the performed actions. In addition, the outcomes of the attestation actions are stored in the ledger in the form of an attestation report, while the corresponding attestation data (raw traces collected by the Runtime Tracer and used as attestation evidence) is **ABE-encrypted**, stored off-chain, and associated with the attestation report through a location pointer. These operations contribute to the creation of a **hygiene data space**, which contains threat intelligence information and aircraft health information that should become accessible to any concerned parties.
Access control on threat intelligence and aircraft health data	The aforementioned hygiene data space containing threat intelligence data contains information regarding identified threats and vulnerabilities for various components of the aircraft. However, since these components may be subject to different privacy requirements, it should be ensured that only parties with the appropriate permissions should be able to access the data.	ASSURED offers a two-layer access control scheme: (i) at the first layer, it is verified whether a device has the appropriate certificates and credentials required in order to access a particular ledger, and (ii) at the second layer, the level of granularity of data access is determined, so that only devices that can verifiably demonstrate the required set of device attributes through a Verifiable Presentation by leveraging their Wallet can access a particular set of threat intelligence or aircraft hygiene data. Thus, it is possible to control which user profiles are able to access which types of data with a high level of granularity, even within the same data chunk.

Integrity of sensitive data	The integrity of the threat intelligence and aircraft health data to be stored on-chain or off-chain needs to be ensured, so that no unauthorized party is able to access the data.	The ASSURED **ABE** scheme enables a device to encrypt their operational- or attestation-related data before it is stored, so that its integrity is ensured both during its transmission, and when it is stored. In this regard, ASSURED offers not only the mechanisms required for the protection of the data, but also the management of the keys required for their encryption and decryption. In addition, the ABE scheme offers privacy-preserving capabilities, so that it is not possible to associate specific attributes with an encrypted data set. Finally, a core consideration in ASSURED is **crypto agility**, in the sense that the provided methods are able to support different types of crypto primitives, depending on the needs of the application.

3.2.2 Results and Impact Assessment

A fundamental aspect of the ASSURED framework is the provision of the seamless deployment of all ASSURED components for any potential end-user. This aspect as part of the Smart Aerospace demonstration for the final evaluation, through an extensive set of experimental activities, which have been outlined in detail in D6.3 [9].

From the user-end standpoint, the status of the attestation solution at M36 has enabled the instrumentation, exhaustively validation, and effective assessment of the security analysis of ASSURED in the context of the Smart Aerospace domain. Although a certain level of expertise is required to use the ASSURED tooling – some guidance is advisable from security and embedded systems experts – a very small level of human intervention is required to have the tools in place for a successful firmware update. In terms of development and testing, the developed attestation solution has provided a qualitative improvement compared to the typical “bare-metal” setup bringing a clear enhancement from previous state-of-the-art. The Policy Recommendation engine had a clear effect on reducing the effort required to create the optimal mapping in complex embedded architectures, instrument the regions of interest, deploy, and enforce the synthesized rules, collect and analyze the traces to generate necessary evidence, and finally effectively export the most sounding results to be used on in the future by certification authorities.

These security analysis activities tend to be very tedious and error-prone to perform manually due to their repetitiveness. In quantitative terms and from the user perspective, ASSURED technology has enabled the user-friendliness of a series of security operations (attestation, Blockchain, wallets, policy rules) in a semi-automated manner. Results obtained throughout the lifecycle of the project the project have been promising, and will allow a faster adoption of ASSURED technology modules by the Smart Aerospace community.

The security services of ASSURED have also led to the acceleration of the adoption of firmware updates on the aircraft improving drastically the maintenance time, both reducing the involved actors (airliner, service provider, airframer engineer, Collins engineer), therefore positioning Collins Aerospace in an advantageous position compared to its competitors. ASSURED enables Smart Aerospace organizations to adopt certifiable security operations, reduce the development lifecycle, and deliver products in a faster and secure way. Finally, creating new internal capabilities such as the generation of optimized secure policies for the given hardware and software architecture against security requirements is considered a valuable asset for the next-generation secure air-trustworthiness domain.

Considering all the above, in Table 6 we outline the key results of interest from the testing of ASSURED in the Smart Aerospace domain.

TABLE 6: KEY RESULTS OF INTEREST FOR ASSURED TESTING IN SMART AEROSPACE

Smart Aerospace Use Case: Deployed sensors and data must be protected with appropriate controls to ensure their integrity, confidentiality, and availability throughout their entire life cycle
Key Results of Interest for ASSURED Testing
The security of aircraft components (devices, networks) will be strengthened through the use of the ASSURED attestation enablers; primarily CIV for the configuration integrity of all electronic units comprising an aircraft, and CFA to verify the execution flow of safety-critical processes running on the aforementioned units. Certification results of the attestation solution will be produced to be showcased to the certification authorities.
All the aircraft devices will be monitored against unauthorized software upgrades. This is achieved through the integration of the key migration scheme for the establishment of secure communication channels, the CIV scheme to ensure the integrity of the device before and after the update, and the CFA scheme to ensure the correctness of the update process itself.
In the creation of security policies, we need to consider the specific requirements of heterogeneous components originating from different manufacturers or OEMs. Therefore, the Policy Recommendation engine should generate specific rules per device, in order to create policies with the required level of granularity, considering the specific needs of each device.
Optimal and secure policy enforcement for aircraft systems, sub-systems, and devices, which is achieved as the Policy Recommendation Engine determines the best set of attestation policies by solving an optimization problem. These policies are afterwards deployed in a secure manner in the form of Smart Contracts.
Ease of deployment for new trusted devices in existing aircraft networks is achieved by employing the TPM-based Wallets and the Blockchain infrastructure in order to perform the ASSURED secure enrollment mechanism. This also ensures that the appropriate configuration state of the device is registered based on the MUD profile of the device.
Recording the attestation results in a secure, certifiable, and auditable manner on the Blockchain, so that any concerned stakeholder can have access to the stored results. The solution can also help for gathering and validating all data generated from the attestation results as verified evidence presented to the certification authorities.
In order to achieve secure and privacy-preserving data sharing for different data, not only for the aircraft, but also for all actors in the supply chain, we can use the Blockchain Infrastructure to perform secure and privacy-preserving data sharing for different types of data with the required level of granularity. Therefore, data may be accessed not only by the Smart Aerospace service provider itself, but also by other authorized and authenticated actors. Therefore, we provide secure, traceable, and flexible management of the entire supply chain through the sharing of different types of data in a certifiable and auditable manner through the Blockchain Infrastructure.
Secure and safe compatibility version checking and validation for each aircraft, which is achieved by employing the ASSURED Configuration Integrity Verification scheme to verify the correctness of the software versions installed on the aircraft electronics.
The software-hardware co-design approach, which has already been outlined in Section 3.1.1, unlocks the security capabilities of low-end embedded devices belonging to the safety-critical Smart Aerospace domain.

3.3 DEMONSTRATOR #3 – SMART CITIES

Typically, applications belonging to the Smart Cities domain consist of a set of interconnected devices, such as **sensors**, **gas detectors**, and **surveillance cameras**, which collaborate in order to provide services in the context of public safety to citizens residing within an urban area. In this regard, the Smart Cities infrastructure needs to communicate and collaborate with various **protection agencies** in case of emergencies, such as police departments and fire services.

One core consideration in such use cases is the **privacy of citizens and users** since the aforementioned components may collect sensitive information or potentially personally identifiable information. Therefore, it is imperative to follow a **privacy-by-design** approach, in

which the transmission and storage of sensitive operational data is performed in a privacy-preserving manner, while also ensuring the integrity of the communications between components. In addition, it is necessary to ensure the **integrity of the data sources**, such as sensors and security cameras, in order to verify the integrity of the information originating from such sources. In this regard, the application of security enablers and attestation schemes that require the collection of trace data (such as configuration or control flow data), it needs to be ensured that the privacy of the devices is not compromised, and that the verifying entities cannot infer any information on the identity or implementation details of the devices.

In addition, different **data sharing profiles** may need to be implemented, in order to access operational or attestation-related data. Recall that various parties may need to interact with the Smart Cities ecosystem, such as police officers or firefighters. In this regard, it needs to be ensured that only users and stakeholders with the appropriate permissions can access a set of data. Therefore, such applications require data access controls that provide the **required level of granularity** (even within the same data chunk), so that a set of data can only be accessed by parties that can verifiably demonstrate the appropriate set of attributes. Another core consideration with regard to data access is **controlled linkability**, meaning that it must be possible to control whether it is possible to link a set of data with the device it originated from, or the location of the device. Therefore, security controls are needed, that enable users to provide linkability to their data only if it is required.

In this regard, ASSURED is able to offer the security controls required in order to provide operational assurance to all aforementioned types of devices, which are able to provide **timely responses in case of security events**, while achieving the strict privacy requirements set forth by such use cases. In addition, it is able to provide the data access controls that achieve the requirements related to data access, as well as the linkability features. All these services can be offered in a **scalable manner**, in order to address any size of urban environment, as well as intercommunication between different municipalities (which define a trust domain).

3.3.1 Challenges in Security, Privacy, Trust of Public Safety Systems

As outlined in the previous section, applications belonging to the Smart Cities domain introduce various challenges, pertaining not only to the privacy of users and devices, but also to the integrity of the data in order to be able to provide public safety services to citizens with a high level of trustworthiness. In this regard, ASSURED provides a wide range of functionalities and security enablers that are able to address those challenges. In Table 7, we outline the key security challenges related to the Smart Cities domain, their potential impact on the correct operation of the system, and the functionalities of ASSURED which are able to address these challenges and mitigate any related threats and vulnerabilities.

TABLE 7: KEY CHALLENGES IN SMART CITIES DOMAIN

Security Challenge	Impact	ASSURED Functionality
Secure access to public data, validation of data flows, user privacy.	An unauthorized access to city systems hosting sensitive citizen data can cause data breaches and compromise the privacy requirements of the system, both regarding identity privacy (identity of the devices and users), and data privacy (such as attestation evidence privacy).	All ASSURED components have been designed with the consideration of strong privacy requirements. For instance, the attestation enablers of ASSURED have been designed to be able to attest to the correctness of devices in a privacy-preserving manner, since we cannot make assumptions on the trustworthiness of the Verifier. The **CIV** scheme, through the use of local attestation with key restriction usage policies, enables a device to attest to the correctness of its configuration state without divulging any implementation or system information. In the

		context of the **CFA** scheme, we employ a trusted intermediate Worker employing zkSNARK proofs who performs the attestation logic, so that only the result of the attestation is forwarded to the Verifier.
Secure and Privacy-preserving Dissemination of data	When sharing operational data that originates from the sensors or IP cameras, but also raw trace data used as attestation evidence, it must be ensured that an adversary is not able to infer any information on the identity of the device or the location of the user, in order to avoid any breaches of the privacy requirements of a public safety system.	while it should be verified that the data originates from a valid device that has been securely enrolled into the framework, it should not be possible to link the data back to the device itself or its location unless deemed necessary due to a possible misbehavior (or device malfunction) been detected based on plausibility checks performed on this data. In this regard, the **DAA** scheme offers the capability to authenticate operational data in terms of their origin, without revealing the identity of the device, while also offering capabilities for **user-controlled linkability and accountability**. The DAA scheme can be used not only for signing operational data, but also attestation data. However, in this regard, the DAA scheme offers **revocation** capabilities in order to revoke the credentials of a potentially compromised device in a privacy-preserving manner.
Secure and privacy-preserving data access management	A data access management approach is needed, which ensures that only the parties with the appropriate attributes can access a particular set of data, based on their permissions and data access profile (e.g., police and firefighters). In addition, data sharing services should preserve the privacy of both the devices the data originates from, and the devices that aim to access a set of data.	A device aiming to access a set of data while leveraging its attributes must be able to do so in a privacy-preserving manner, without disclosing information it does not need to share. In this regard, the ASSURED **ABAC** scheme enables devices and users to access a set of data, while only disclosing the attributes needed in order to do so (selective disclosure) in a verifiable manner through the creation of a VP. Besides privacy when sharing attributes, ASSURED goes one step beyond, with the adoption of the zero-knowledge principle, by enabling a device to prove that it possesses an attribute without revealing the value of an attribute itself. Similarly, the **ABE** scheme enables a device to encrypt data in a manner that ensures that no entity can infer any information about which attributes correspond to which sets of data.
Trustworthiness of onboarded devices	In case an unauthorized or malicious device becomes part of the network, it may be able to access sensitive data originating from legitimate devices, or may compromise the correct operation of the system as a whole by obtaining illicit access to an authorized device.	The **secure enrollment and zero-touch onboarding** scheme is used in order to ensure that only trustworthy devices, which can demonstrate the possession of a valid device Wallet, can be onboarded into the system. This process securely creates all the required cryptographic material that may be used by the device throughout its operational lifecycle, including the DAA key, as part of a **secure key hierarchy**. Note that the DAA Key is set as the root key of the key hierarchy, in order to enable anonymizing the signature and blinding the DAA credential in order to achieve further extended privacy.
Identification and mitigation of risks	Various threats and vulnerabilities affect the types of devices participating in a Smart Cities environment,	The ASSURED **Risk Assessment** scheme is able to take into consideration the types of assets, the threats and vulnerabilities typically affecting these assets, and the interconnectivity between assets,

	which may compromise their ability to provide trustworthy sensor or operational data, or ones that compromise the privacy of the users. It is also possible that further risks and vulnerabilities arise during the operation of the system.	in order to produce a holistic evaluation of the risk that may affect those assets, as well as the system as a whole. Particular focus is given on the assessment of **privacy risk**, by consideration of not only hardware assets, but also **data assets**. This enables ASSURED to quantify the impact of attacks on data sharing, through the use of the CVSS scoring method, as well as the Automated Privacy and Security Impact Assessment (APSIA) methodology, in order to assess the assets and the system as a whole with regard to privacy. In addition, the **modularity** of the Risk Assessment scheme enables the consideration of additional risk scoring systems that may be applicable to smart cities applications. In addition, the **Policy Recommendation Engine** is able to calculate the optimal set of security policies specifying the mitigation measures in order to address the identified vulnerabilities.
Complexity of large-scale urban environments	When aiming to provide operational assurance to large-scale Smart Cities environments, there is a need to attest to the correctness of multiple devices with limited computational abilities. In addition, there is a need to handle the volume of data originating from these devices simultaneously, in an efficient manner that does not induce overhead to the operation of the system.	ASSURED has been designed considering the scalability of the provided services. Specifically, **Swarm Attestation** is able to attest to the correctness of the configuration state of a swarm of devices simultaneously, in a manner that is more computationally efficient than attesting each device individually. In addition, the Swarm Attestation scheme leverages the aforementioned DAA scheme, in order to provide privacy-preserving features, while also enabling the anonymous revocation of a device that caused a failed attestation has deemed to be untrustworthy. In addition, scalability features have been provided to the ASSURED Blockchain Infrastructure through the addition of **Blockchain Peers**, which act as the mediators between devices and the ledger. It is possible to include multiple Blockchain Peers in the system in order to enable the support of large numbers of concurrent Blockchain interactions (such as reading, recording, or querying for data stored on the ledger), as well as to alleviate the computational load from the devices.
Trustworthiness of data flows	Data flows originating from devices such as sensors or surveillance cameras should be protected, so that they cannot be accessed by untrusted sources. If the communication channels are compromised, this would pose a serious risk to the trustworthiness and confidentiality requirements of the transmitted data.	The **key migration** scheme of ASSURED can be used in order to establish secure communication channels between devices, in order to establish the trustworthiness and integrity of the transmitted data. This scheme utilizes the HW-based RoT of the devices, thus providing strong HW-based guarantees that go beyond what can be offered by classic Diffie-Hellman secure channel establishment. In addition, the aforementioned **ABE** scheme can provide trustworthiness guarantees to encrypted attestation-related or operational data that is stored either on-chain or off-chain.

Decentralized Identity Management	In a Smart Cities ecosystem, it is possible that a malicious party may aim to impersonate a legitimate device, manipulate the use of credentials, or even steal the credentials for illicit use. This may lead not only to compromises in the correct operation of the device, but may also endanger confidential and sensitive information, making it accessible by malicious parties.	The ASSURED Wallet leverages a HW-based Trusted Component as a Root-of-Trust. This enables the creation of HW-based keys that enhance the security of the Wallets, and achieve properties such as device binding, Holder binding, selective disclosure, and unforgeability, while maintaining a high level of assurance in the interaction of the Wallet with external entities. In addition, it enables the secure management of cryptographic material, including the VCs and VPs. This approach provides strong guarantees to devices that wish to provide proof of their identity for accessing a particular set of data or service, which may also refer to data stored on the ledger.

3.3.2 Results and Impact Assessment

In order to evaluate the effectiveness of the security services provided by ASSURED towards addressing the security challenged outlined in the previous section, extensive experimental activities have been conducted in an experimental testbed corresponding to an actual Smart Cities ecosystem. The results of these experiments have been outlined in D6.3 [9], and demonstrate their ability to provide operational assurance in a timely and efficient manner, while also retaining the strict privacy-preserving capabilities required in order to address the needs of Smart Cities applications. Therefore, it was concluded that ASSURED provides a strong value proposition with an out-of-the-box solution that can compete with already available commercial solutions, and provides high capabilities for adoption in existing Smart Cities applications.

In D6.4 [6], we presented a detailed impact assessment and key takeaways for the various technologies and components provided by ASSURED. In Table 8, we provide some core insights from the application of the security services provided by ASSURED, in order to detail how ASSURED assists in capturing the business needs and challenges in the Smart Cities use case.

TABLE 8: KEY RESULTS OF INTEREST FOR ASSURED TESTING IN SMART CITIES

Smart Cities Use Case: Deployed sensors and data must be protected with appropriate controls to ensure their integrity, confidentiality, and availability throughout their entire life cycle
Key Results of Interest for ASSURED Testing
Smart Cities applications are subject to strict privacy requirements, both regarding the identity of the users, and the confidentiality of the transmitted data. In this regard, the ASSURED attestation enablers (CFA, CIV, Swarm Attestation) have been designed in order to enable device attestations, without requiring them to divulge sensitive information about their identity or their configuration state.
The ABE and ABAC schemes ensure that only parties and stakeholders that can verifiably demonstrate the required attributes can decrypt a set of data, or access a set of data stored on the Blockchain, respectively. This ensures that the data originating from devices such as sensors and IP cameras, which is subject to strict privacy and confidentiality requirements, can be accessed only by the parties who are authorized to do so, with the required level of granularity. This enables the creation of data access profiles based on the roles of each party and stakeholder (e.g., police or firefighters) who should only need to access specific types of data.
The authentication of different types of roles and devices is supported by the provision of features such as the secure enrolment and zero-touch onboarding scheme, and the use of an SSI-enabled device Wallet. Therefore, new users and devices are securely authorized before granting access to the system, only if they possess a trustworthy Wallet. The secure enrolment process validates the

correct operational state and properties of the device and proceeds to registration. This also enables the continuous verification of devices that have already been enrolled into the ASSURED framework.
The AI-assisted, ML-based CFA scheme is able to attest to the correctness of the control flow of a software process, and is able to detect deviations from the correct execution of SW processes, which may indicate malicious activity (such as ROP and DOP attacks). The ML-based CFA scheme is supported by the deployment of the Runtime Tracer, that operates in a trustworthy manner within the Trusted Computing Base of the device, and is tailored to provide the required granularity of control flow traces to ensure the efficient operation of the CFA scheme.
Secure handling of credentials of city authorities is enabled through the use of Wallets, supported by HW-based Trusted Components. These provide the required HW-based guarantees for identity management, through the use of HW-based keys and device binding. The Wallet also supports the issuance of Verifiable Credentials during device registration, and the creation and management of Verifiable Presentations based on the issued credentials.
Smart Cities environments require the transmission of notifications and alerts in case of attacks in an accepted time-window, in near real-time. The ASSURED attestation enablers have been designed so that they can operate in a timely and efficient manner in the resource-constrained devices typically belonging to Smart Cities applications. In addition, following a failed attestation, the Attack Validation component is able to identify the point of intrusion, which may lead to the identification of new types of threats or vulnerabilities. The Runtime Risk Assessment Engine enables their integration into the risk graph and the updating of the attestation policies accordingly through the Policy Recommendation Engine. This feature is critical in an urban environment for the enforcement of cyber-security policies, strategic planning on reliable city systems, and structuring of a roadmap for countermeasures in case of cyber-attacks.
Smart Cities environments consist of a large number of interconnected devices, such as sensors and security cameras. In this regard, the specific threats and vulnerabilities targeting each asset are considered by the Risk Assessment tool, as well as the interdependencies between the assets, in order to perform a holistic risk assessment for the entire system. This also includes privacy risk considerations (i.e., security relationships between data assets in the context of transmitting sensitive information), as well as the consideration of potential attack paths involving several assets.
Reports containing information of potential cyber-security attacks can be used for effective city strategic planning, following a failed attestation scheme. These reports are stored securely in the Blockchain infrastructure in a certifiable and auditable manner, and made accessible to any concerned users and stakeholders who have the appropriate credentials to access them, through the ABE and ABAC schemes. In addition, the related attestation- or operational-related data is stored off-chain and made accessible to parties and stakeholders with the appropriate level of access.
The software-hardware co-design approach, which has already been outlined in Section 3.1.1, unlocks the security capabilities of low-end embedded devices belonging to the Smart Cities domain.

3.4 DEMONSTRATOR #4 – SMART SATELLITES

Applications belonging to the Smart Satellites domain are subject to strict security requirements, in order to ensure the correct operation of satellites, which may operate collaboratively for the execution of safety-critical operations. In case one or more of these satellites is compromised, this may impede the correct execution of these operations, or even compromise the integrity of the satellites themselves. The service graph chain supporting the execution of such safety-critical applications includes a **mission center** and a **ground station**, which are able to communicate with the **satellites** in order to deploy secure updates or receive health information on the satellites. It is also possible for the satellites to communicate between them for the aforementioned collaborative execution of various functions and operations. Therefore, there is a need to provide guarantees on the integrity of the devices themselves, the integrity of the data originating from these devices, and the communication channels between these devices.

The increasing prominence of Smart Satellite systems has led to an increased need for the provision of security services to provide operational assurance to the entire service graph chain. Specifically, in recent years, the rise in prominence of business applications such as

Satellites-as-a-Service has been observed. These involve the use of a satellite grid by academic, research, or industrial organizations in order to deploy and perform computationally intensive operations (such as large-scale experiments). Therefore, Smart Satellite systems are a lucrative target for attackers and malicious parties who aim to compromise the integrity of the system and potentially obtain illicit access to such data. Therefore, there is an increasing need to address the ever-evolving set of security challenges affecting such environments. For example, since data is exchanged and transmitted in the open, it may be exposed to attacks such as Man-in-the Middle (MITM) and replay attacks. In addition, the satellites may be targeted by other software-related attacks, such as the **deployment of malicious updates** (leading to possible **backdoor invocation**), or control-flow attacks such as **Return-Oriented Programming (ROP)** and **Data-Oriented Programming (DOP)**.

In this regard, ASSURED can contribute through security enablers that are able to provide the required security and trustworthiness guarantees to the operation of a Smart Satellite ecosystem. In addition, ASSURED can contribute towards implementing protocols and guidelines, like the CCSDS communication protocol, and enable low budget missions to provide satellite systems that can implement more efficient security mechanisms, ensuring the confidentiality, integrity, and availability of data transmitted between satellites and ground stations. At the same time, ASSURED provides a holistic security platform that enables the secure and unimpeded execution of mission applications as collaborative functions on the satellites.

The security measures provided by ASSURED can protect the satellites against threats such as unauthorized access, data tampering, and interception, thereby enhancing the overall security posture of satellite communications. ASSURED mechanisms for key management of multiple CubeSats can fill the need for them to communicate with the Ground Station in different locations, while enriching availability, and ensuring the confidentiality and integrity of the data transmitted in the open air. At the same time, the ability to apply security policies in a dynamic manner can unlock further vital features for mission operations. For example, **energy efficiency** needs can be considered, which are closely related to the **efficient utilization of the computational resources** of the satellites. In addition, a security extension for the CCSDS protocol itself could be considered to be added.

3.4.1 Challenges in Secure Communication Capabilities of Smart Satellites

The Smart Satellite sector faces a number of significant security challenges that have profound implications for its growth and stability. As satellites become increasingly advanced and interconnected, they also become more vulnerable to various threats. This necessitates a security platform that can adequately address these issues and address the security challenges that may be present in such systems. Satellites, like all interconnected systems, are susceptible to cyber threats that can disrupt their operation and compromise their data. Attacks can take numerous forms, ranging from sophisticated hacking attempts to simpler, yet no less destructive, attacks like jamming signals. A robust security platform must be able to verify the secure operation and detect these threats in real-time.

Another crucial challenge involves device integrity and authentication. Satellites must be able to verify their own authenticity, as well as that of the signals they receive. This is essential to preventing unauthorized access or false data injection. A security platform must provide authentication mechanisms that can validate the integrity of both hardware and software components, while also ensuring their ease of integration into practical satellite communication systems.

The establishment of secure communication channels between mission center, ground station and CubeSats is also a significant concern. Communication over vast distances, often in

challenging environments, introduces the risk of interception or disruption. A secure channel must ensure the confidentiality, integrity, and availability of communications at all times. At the same time, providing secure mechanisms to handle vast amounts of sensitive data, including scientific research, intelligence, and private communications and been able to share them with external stakeholders. Therefore, there is a need for mechanisms to enable the protection and secure sharing of this data, providing adjustable encryption mechanisms and preventing unauthorized access.

Also, addressing the threats posed by malicious software and attacking activities is crucial. Critical operations (like SW updates) should be executed in a secure and verifiable manner. The provision of information about the state of CubeSats to external members and the capability to check the health state of an entire chain of communicative satellites is another complex task that needs to be addressed as part of the security solution to be applied.

In Table 9, we summarize the challenges faced by the smart satellite sector, along with the potential impact of these challenges and the related ASSURED functionalities that can be used to address these challenges.

TABLE 9: KEY CHALLENGES IN SMART SATELLITES DOMAIN

Security Challenge	Impact	ASSURED Functionality
Device Integrity and Authentication	An unauthorized malicious device that aims to participate in the satellite network may cause issues, such as compromising the integrity of the mission app, obtaining unauthorized access to information about the satellites or the software running on them, or cause harm to the satellites.	The **secure enrollment** process offered by ASSURED ensures that only satellites that possess a valid Wallet are able to become part of the satellite network. This process is also able to create the required cryptographic material in order to utilize the security services of ASSURED, as it was previously outlined in Section 3.3.1. Recall that the DAA Key is the root key of the secure key hierarchy, containing all the keys that can be used by the security services of ASSURED, such as the key migration scheme and the lightweight crypto schemes. In addition, it provides the basis for the creation of key restriction usage policies, that bind the usage of the key to a correct configuration state, so that it can only be used if the integrity of the Wallet has not been altered in an unauthenticated manner.
Establish Secure Communication channel between Ground Station and CubeSats	Since communication between satellites, as well as between a satellite and the ground station, is performed over open air, a malicious party may intercept communications between two or more parties. If this is performed over an insecure (or improperly secured) channel, this may lead to a compromise of the integrity of the information.	In order to ensure the integrity of communications, ASSURED offers a **key migration** scheme which is able to leverage the HW-based Trusted Components (TCs) of the devices in order to create secure communication channels. Note that the introduction of the aforementioned TCs provides hardware-based guarantees that are not provided by a typical Diffie-Hellman key exchange. This can be used, for example, in order to ensure the integrity of an update package deployed from the Ground Station to the satellites. In addition, it can ensure the correct collaborative execution of a safety-critical process by a group of satellites.
Deployment of secure updates	When the ground station deploys a secure software update package, it should be ensured both that the integrity of the update itself is not	As aforementioned, in order to ensure the secure deployment of a secure update package from the ground station to the satellite, the **key migration** scheme is able to provide guarantees on the integrity of the data through the establishment of a

	compromised, and that the satellite is in an appropriate condition to receive the update (i.e., fulfils all prerequisites to accept the update, and is in a correct and uncompromised operational state). Otherwise, this may lead to vulnerabilities that may be exploited by malicious parties.	secure communication channel. However, in addition to this, the ASSURED framework provides a method to ensure the correctness of the update based on the attestation enablers: (i) Before the update is deployed, a **CIV** attestation is executed on the satellite, to ensure that it has not been compromised and it is in a correct and expected state. (ii) A **CFA** process is executed to ensure the correctness of the update process itself. (iii) A **CIV** is executed after the update is complete, based on the new updated state of the device, to ensure that it was performed correctly.
Correct execution of mission applications and software	When executing a mission application, such as orienting an imaging device to a set of requested coordinates and taking a picture, the integrity of the execution process needs to be protected, in order to ensure that the correct execution of the mission app is not compromised (either by a malicious party or a software vulnerability). Such a compromise may even affect the correct operation of hardware components.	In order to ensure the correct execution of a mission app (or any software process running on the satellite), ASURED provides the **ML-based CFA** scheme. First, control flow traces from the executed software are collected via the **Runtime Tracer**, and the ML-based CFA classifies the traces as benign or malicious. If any deviation from the correct execution is detected, the traces are forwarded to the **Attack Validation** component in order to pinpoint the exact point of intrusion, so that a security officer or system administrator can extract further information on the type of threat detected. In addition, the threat intelligence information is stored on the ledger as an attestation report, and the corresponding traces are stored on the off-chain storage facility.
Provide information about the state of CubeSats to External Members	Control flow traces extracted from the execution of critical mission applications should be stored in an efficient manner, ensuring the confidentiality, integrity, and availability of the data. In addition, External Members should be able to retrieve information about the devices and attestation reports, in a secure and efficient way, in order to check the health state of the Overall System.	With the use of the **Blockchain Infrastructure**, ASSURED demonstrated the creation of a **hygiene data space**, which enables monitoring of the state of all devices, where all threat intelligence data and device audits can be kept in a certifiable and auditable manner, and enables the assessment of trust of the devices at any point in time. By leveraging the notion of SSI with **Decentralized Identifiers (DIDs)**, devices are able to leverage their Wallets to selectively disclose only the attributes needed in order to access a set of data. In addition, through the **Dynamic Symmetric Searchable Encryption (DSSE)** scheme, it is possible to perform queries on encrypted on-chain or off-chain threat intelligence data based on a set of publicly available keywords, which are stored on the public ledger, without needing to decrypt the data itself.
Verification of correctness of a swarm of satellites	As aforementioned, the collaborative execution of safety-critical applications involves using the computational capabilities of multiple satellites simultaneously. In this regard, a method is needed to ensure the integrity of the entire swarm of satellites in a timely and efficient manner.	The ASSURED **Swarm Attestation** scheme is able to efficiently attest to the correctness of the configuration state of an entire swarm of satellites, or attest to the correctness of the execution of a software process on multiple satellites simultaneously, in a manner that is more efficient than attesting each satellite individually. In addition, the Swarm Attestation provides privacy-preserving properties, but with **linkability and revocation** capabilities in case of a failed attestation.

3.4.2 Results and Impact Assessment

The ASSURED platform was successfully integrated and tested in an experimental Smart Satellite lab-based testbed, as it has been documented in D6.3 [9]. Based on initial results, ASSURED provides an innovative set of security mechanisms for space technologies, and it can have significant impact towards further enhancing the secure operations of space missions.

More specifically, the ability of ASSURED ability to provide advanced attestation and verification mechanisms contributes to effectively enabling secure operations of smart satellites. It can establish a robust and secure infrastructure for data exchange and collaboration between the mission center, ground stations, and satellites. Furthermore, ASSURED's key capability to provide verifiable evidence can contribute to ensure that only certified devices can perform specific operations and be able to interact with the satellites. Considering specific critical operations performed in Smart Satellites ecosystem, such as software updates, it can offer a much-needed guarantee that these operations are executed securely, whether they occur on the ground station or directly on the satellites. In that way ASSURED can provide a significant enhancement towards space operations security and certification.

Another key feature of ASSURED is its dynamic policy enforcement, which is achieved by defining and implementing security policies and sub-policies. This gives the opportunity for appropriate and adaptable security mechanisms to be applied and, therefore, ensures the security of all operations according to the policies and the protocols of the mission operator.

In addition, ASSURED authentication mechanisms and procedures enable the secure and easy onboarding of new devices. In addition, also with its modular design could facilitate several relevant future expansions. For example, the capacity to adapt security policies on the runtime can be further developed, considering the overall mission context and objectives. Thus, it can further contribute to achieving higher levels of security for the overall space mission operations, while at the same time enabling the operator to fine tune other mission parameters like energy consumption.

In Table 10 we summarize the benefits ASSURED brings in satellite security, unlocking new ways to provide mission operations (like mission as a service) in the Smart Satellites application domain.

TABLE 10: KEY RESULTS OF INTEREST FOR ASSURED TESTING IN SMART SATELLITES

Smart Satellites Use Case: Deployed sensors and data must be protected with appropriate controls to ensure their integrity, confidentiality, and availability throughout their entire life cycle.
Key Results of Interest for ASSURED Testing
The security of the execution of safety-critical mission applications can be achieved in an effective and efficient manner. Specifically, the ML-based Control Flow Attestation scheme collects the appropriate control flow trace information with the assistance of the HW-based and SW-based tracing capabilities of ASSURED, and categorizes the traces as benign or malicious. The ML-based CFA scheme has been demonstrated to achieve a high level of efficiency, as well as high accuracy in the detection of threats and vulnerabilities.
Optimal and secure policy enforcement for CubeSats is achieved through the Risk Assessment and Policy Recommendation Engine, based on the interconnectivity between the satellites, and the threats and vulnerabilities typically affecting satellite systems. The optimal set of security policies is determined after solving an optimization problem by the Policy Recommendation Engine, taking into consideration the security needs of the satellites, as well as the available resources at the target devices.
In the case of mission applications with particular confidentiality requirements, ASSURED provides the Direct Anonymous Attestation (DAA) scheme, that enables devices to provide anonymized

signatures that do not reveal information about their identity. Thus, the attestation enablers of ASSURED can be performed in a privacy-preserving manner.
The whole space mission supply chain (including mission center, ground station and satellites) can be secured, and the correctness of the devices can be verified before executing critical operations. Monitoring of all components involved and confirming their integrity before enabling the execution of critical mission functions can be performed with the CIV scheme. The integrity of not only individual CubeSats but also the whole chain (e.g., constellation of CubeSats and Ground Station) can be validated with the use of the Swarm Attestation mechanism in a secure and efficient manner.
The deployment and installation of secure updates is achieved through the key migration scheme to establish a secure communication channel between the ground station and the satellite (for the transmission of a software package), the CIV scheme to ensure the integrity of the satellite before and after the update, and the CFA scheme to ensure the integrity of the software update itself.
External stakeholders consuming or providing services with the use of smart satellites can receive data collected with higher levels of granularity, by leveraging the Blockchain infrastructure, where data is recorded in a certifiable and auditable manner. This is achieved via the ABAC scheme with the assistance of the device Wallets, that enable devices to create Verifiable Presentations containing only the set of attributes required to access a set of data.
The use of lightweight cryptographic schemes supports the integrity of attestation- or operational-related data, by providing hardware-based guarantees to the encryption of the data. The ABE scheme also collaborates with the device Wallet, which is able to create and manage the cryptographic material required to perform encryption and decryption operations.
Efficient security monitoring with the Runtime Tracer, which operates within the Trusted Computing Base (TCB) of the satellite, in order to ensure the integrity of the extracted traces.
Low budget organizations (e.g., SMEs) can deploy complex software processes, such as experimental activities, to a swarm of satellites to perform collaborative execution of the process, while also achieving a high level of guarantees with regard to the trustworthiness of the execution process and the integrity of the data.
The software-hardware co-design approach, which has already been outlined in Section 3.1.1, unlocks the security capabilities of low-end embedded devices belonging to the safety-critical Smart Satellites domain.

3.5 OTHER APPLICATION DOMAINS AND SUPPLY CHAIN SECURITY

In the context of the business portfolio and services offered by the ASSURED partners beyond the envisioned use cases, we have also conducted an initial analysis of how ASSURED could provide significant benefits to other application domains beyond the one defined by the use cases. This essentially provides further evidence of the feasibility and pragmatic nature of the ASSURED framework.

Here, we provide some examples of application domains where the security services provided by ASSURED can provide significant added value to supply chain ecosystems operating within these domains.

3.5.1 Activity and Health Data Tracking

As technology continues to play an integral role in the healthcare industry, applications in the health domain face a range of cybersecurity challenges. Safeguarding patient data, securing medical devices, and protecting sensitive information from unauthorized access are critical priorities. This section refers to the most prominent cybersecurity challenges faced by applications in the health domain and discusses how ASSURED could have an impact on the health domain by attempting to address those.

TABLE 11: KEY CHALLENGES IN ACTIVITY AND HEALTH TRACKING DOMAIN

Security Challenge	Impact	ASSURED Functionality

Data Breaches and Privacy Concerns	Data breaches pose a significant challenge to the security of applications in the health domain. The theft or unauthorized access to sensitive patient information can lead to serious consequences, including identity theft, financial fraud, or even manipulation of medical records. The Ponemon Institute's **Cost of a Data Breach Report 2022** [10] found that breaches related to healthcare increased by nearly USD 1 million to reach USD 10.10 million. Healthcare breach costs have been the most expensive industry for 12 years running, increasing by 41.6% compared to the Ponemon Institute's 2020 report.	With ASSURED, all the devices in a given infrastructure are continuously monitored against malicious behavior. They are trusted and secured throughout the entire lifecycle, starting from the trusted boot (through the ASSURED CIV scheme) to the runtime configuration, to the correct executional behavior (through the ASSURED CFA scheme). Each new user or device is securely authorized before being granted access to the system, by employing the secure enrolment process to ensure the registration of the device in the system, only if it is in a correct operational state and is characterized by the correct properties. ASSURED optimally calculates security policies. Notifications are delivered in case of attacks, in near real-time, by observing the outputs of the attestation enablers, and using the Runtime Risk Assessment Engine in order to update the attestation policies during runtime, i.e., always including the latest threat detection knowledge available.
Vulnerabilities in Medical Devices	Vulnerabilities in medical devices represent a significant cybersecurity challenge for applications in the health domain. These devices, ranging from pacemakers to infusion pumps, are increasingly interconnected and rely on software systems to deliver critical healthcare services. However, the rapid integration of medical devices with networked environments often overlooks adequate security measures, making them attractive targets for cyber attackers. The European Union Agency for Cybersecurity (ENISA) publishes a comprehensive report titled **ENISA Threat Landscape**; in its 2021 [11] release, it reported state-backed cyber espionage operations related to COVID-19 as well as using COVID-19 related lures for social engineering, resulting in healthcare, pharmaceutical, and medical research sectors being heavily targeted. Furthermore, in those yearly ENISA reports the vulnerabilities and risks associated with medical devices in the European continent are highlighted, emphasizing that the increasing complexity and connectivity of medical devices enlarge the attack surface for malicious actors to exploit.	Continuous monitoring of a given SoS through ASSURED Control Flow Attestation secures the system against introduced or already existing vulnerabilities which can be exploited during the runtime of a given system process, resulting in malicious behavior. Assets are continuously monitored through the security assessment feature, by employing the Runtime Tracer in order to collect software flow evidence that is required for the application of the CFA scheme.

Ransomware Attacks	Ransomware attacks pose a severe threat to applications in the health domain, targeting sensitive patient data and disrupting critical healthcare services. The European law enforcement agency, Europol, published in 2021 the **Internet Organized Crime Threat Assessment** [12] (IOCTA) which provides valuable insights into the current landscape of cyber threats, including ransomware attacks, in the European continent. The IOCTA report highlights the increasing prevalence and impact of ransomware attacks on various sectors, with a specific focus on healthcare. Some of these crimes make use of COVID-19-related lures, such as phishing or the sale of counterfeit medical products, especially in countries in which medical services are linked to mobile bank IDs. Healthcare organizations have become prime targets for ransomware attacks due to the critical nature of their operations and the high value of the data they possess.	With ASSURED, the communication channels between all devices in the infrastructure are secured through the inclusion of TPM-based wallets that can support the establishment and protection of the appropriate cryptographic primitives. This prevents intrusions in the communication of the interconnected devices, or communications poisoning, both of which may result in extraction of secret or safety critical information. Furthermore, ASSURED monitors all components involved and confirms their integrity before enabling the execution of critical mission functions by using the CIV scheme.
Insider Threats	Insider threats, either intentional or accidental, are a significant challenge in healthcare applications. Employees with access to sensitive data may inadvertently expose it to unauthorized individuals or intentionally misuse it for personal gain. Robust employee training programs and implementing stringent access controls are crucial to mitigating this risk. The Ponemon Institute's **Cost of a Data Breach Report 2022** found that 47% of healthcare organizations reported insider incidents caused by negligence or malicious intent.	ASSURED, by design, assigns access control rights to specified accounts based on the properties of the devices that are allowed to have access to certain data and/or services, controlled through the ABE and ABAC schemes. Furthermore, in order to share collected data with external stakeholders with high level of integrity and confidentiality, ASSURED leverages the Blockchain infrastructure, where data is recorded in a certifiable and auditable manner. With those functionalities in place, ASSURED can minimize the possibilities of the exploitation of available data from an insider to the extent possible.
Third-Party Security Risks	Third-party security risks present a significant challenge for applications in the health domain, as healthcare organizations often rely on external vendors and services for various functionalities. The European Data Protection Board (EDPB) published guidelines on the concepts of controller and processor in the General Data Protection Regulation (GDPR), shedding light on the complexities and risks associated with third-party data processing in the European continent. The EDPB's guidelines provide detailed	The ASSURED framework is rather easily integrated with a legacy system. The expression of the policies using the MSPL language guarantees a high degree of abstraction that is able to express the security and privacy requirements of legacy devices. Together with the update of the attestation policies during runtime by the Runtime Risk Assessment Engine, ASSURED offers a great line of defense against common third-party security risks.

	explanations of the roles and responsibilities of controllers and processors under the GDPR, with a specific focus on data protection in the context of third-party relationships. Thorough vetting and ongoing monitoring of third-party vendors' security practices are essential to mitigate these risks.	

In conclusion, it is evident that applications in the health domain face several critical cybersecurity challenges, including data breaches, vulnerabilities in medical devices, ransomware attacks, insider threats, and third-party security risks. Safeguarding patient data and ensuring the integrity of healthcare systems require constant vigilance, robust security measures, and adherence to industry best practices. The ASSURED Framework has been demonstrated to successfully reply to challenges in those areas across the four demonstrators in the project; ASSURED virtues could be applied to systems of healthcare organizations in order to better protect sensitive information and maintain trust in the digital healthcare landscape.

3.5.1 Connected Cars and Autonomous Driving

Connected vehicles, as part of the emerging types of Cooperative Intelligent Transportation Systems (C-ITS), are positioned to transform the nature of the mobility, enabled by the capability of vehicles to communicate with other entities formulating the V2X landscape. Specifically, vehicles and infrastructure are able to transmit and exchange status information, as well as information pertaining to unexpected events. Exchanging this type of information enables the realization of warning applications, such as collision avoidance warning. The communication services adopted for the generation and management of this information are based on the exchange of Cooperative Awareness Messages (CAMs), and Decentralized Environmental Notification Messages (DENMs).

With regard to the development of the connected cars ecosystem, the CAR 2 CAR consortium has developed a comprehensive deployment roadmap [13] consisting of three distinct phases:

- **Day 1**: Refers to awareness driving applications, pertaining to collision avoidance, collection of infrastructure information, status and dynamic signage, status dynamics, and notifications.
- **Day 2**: Refers to sensing driving applications, such as advanced warnings, pedestrian protection, semi-automated driving, collaboration with traffic light controllers, etc. These services are supported by misbehavior detection and improved positioning support systems.
- **Day 3**: Refers to cooperative automated driving services, which include cooperation with the infrastructure for automated driving, and is based on advanced services, such as automated coordination.

The development of this roadmap is based on empirical observations of automation trends in the commercial vehicle industry and the growing prevalence of V2X-equipped systems. Through these phases, the evolution of V2X technology is depicted, starting with its initial function of exchanging status information, and gradually progressing towards the development of cooperative automated driving capabilities. The aforementioned vision not only presents a trajectory for the seamless development of intelligent mobility, but also emphasizes the pivotal significance of V2X technologies in shaping the safety and interaction of vehicles.

However, this highlights a core issue in the connected cars ecosystem: *Even though establishing trust in the V2X communication part of C-ITS systems is somehow addressed, the*

problem of assessing trust on the exchanged information in such a highly dynamic, distributed, and ubiquitous environment, remains open. That is because we lack tools to reason about trust relationships between data sources that were previously unknown to each other. In CCAM emerging scenarios, it might be the case that the sources of evidence offered by others are untrusted, or the evidence is indirect and obtained through a referral chain.

However, the shift towards higher levels of automation (particularly Day 2 and Day 3+ services) poses a significant challenge, i.e., the need for external data to facilitate partially automated or fully automated driving functions. In this context, there is a need for the provision of strong integrity and trustworthiness guarantees of external data sources, such as external sensor information, maps, and positioning data, because entities need to rely on this information to make safety-critical decisions. If the integrity of this data is compromised or not provided with the expected quality, the building blocks of the automated operation functions will use incorrect data to control the vehicle. Therefore, tools that enable the measurement and management of trust levels, based on incomplete and/or subjective information provided by potentially untrustworthy sources, are needed. In addition, these tools should accommodate dynamically changing trust relationships due to the high level of mobility exhibited by cars and other vehicles. This is one of the core challenges to be resolved for unlocking the full potential of CCAM ecosystems.

In this regard, ASSURED provides the security tools and mechanisms that are able to address the trustworthiness requirements of connected cars services, towards the establishment of trust relationships between cars and other actors. Specifically, the **attestation enablers of ASSURED** offer the capability to perform dynamic trust assessment, in order to verify the integrity of the modules pertaining to the collection of sensor information, as well as information required for the operation of the aforementioned services. In addition, the **runtime Tracing** capabilities of ASSURED offer the capability to collect verifiable evidence based on which trust assessment is performed. The **lightweight crypto** schemes of ASSURED offer capabilities for the secure and trustworthy exchange of information, in order to protect its integrity and ensure their correct usage in the context of the various connected cars services.

It follows that the tools and methodologies of ASSURED provide a strong basis towards the achievement of trust establishment between components and vehicles in the context of connected cars ecosystems, and can provide significant value propositions to organizations operating within this application domain.

4 STRATEGIC IMPACT

As it has been outlined throughout several deliverables, one of the core targets of ASSURED is the *creation of a holistic security framework, which enables the adoption of the zero-trust principle, provides operational assurance of large-scale Systems-of-Systems (SoS) comprising multiple heterogeneous devices running mixed-criticality services, and is aligned with the vision of the EU of building trust and resilience in such SoS*. The final version of the ASSURED framework has been constructed keeping this goal in mind, while also aiming to fulfill the security, privacy, and trustworthiness requirements of vertical domains and services envisioned as part of the next generation-smart connectivity SoS. As evidence towards the achievement of this goal, ASSURED has been applied and evaluated in the context of four envisioned use cases, namely *Smart Manufacturing, Smart Cities, Smart Aerospace*, and *Smart Satellites*.

In D7.6 [1], we had provided a detailed analysis on the **pathway of the project towards achieving a core set of strategic impacts** through the core value propositions and envisioned contributions. In the following, we expand on this analysis considering the completion of the final version of the ASSURED framework. Recall that the strategic impact can be summarized as *the enhancement of the **security, safety, resilience, and data trustworthiness** of the aforementioned type of SoS through a harmonized approach that integrates tools for **runtime trust establishment and reasoning**, through which the devices belonging to a service graph chain can **establish trust for cooperatively executing safety-critical functions**, while also **building and expanding on the zero-trust concept***.

While several independent mechanisms and tools exist in the literature, ASSURED is **the first project of its kind to provide a holistic and harmonized toolchain for the efficient and continuous security and privacy assessment and management throughout the entire lifecycle of a supply chain**, that can provide strong and verifiable artifacts in a **certifiable and auditable manner**, while also enabling devices to provide verifiable claims on their identity and state in a **zero-knowledge manner**. *In this regard, ASSURED provides the tools that enable enhancing and cementing the vision of the EU and leadership position in ICT trustworthiness.* ASSURED also aims to enhance security and privacy in various operational stacks of all applications. This is achieved through a wide variety of technologies and components which have been developed as part of the ASSURED framework, including the **Risk Assessment and Policy Recommendation Engine**, the **Attestation Toolkit**, the **Blockchain Infrastructure**, and the **lightweight crypto and data management schemes**. These are supported by the use of **HW-based trust anchors** and have been instantiated with the use of TPMs.

In the context of future research, ASSURED technologies could also provide the baseline for interdependable safety-security analysis, especially motivated by our safety critical use-cases' results. Since safety and security engineer artefacts (requirements, models) are often decoupled during products design cycle, ASSURED features could be utilized to ensure that heterogeneous – yet dependable – requirements could be realized and enforce at system level, protected by a series of security mechanisms. In the future, through ASSURED (e.g., the Policy Recommendation Engine), we could specify policies in the micro and macro security world: overarching (macro) requirements to be enforced at system level, as well as micro-architecture requirements (micro) for RISC-V based accelerators.

In the following tables, we provide the core **strategic impacts** of ASSURED, fully aligned with the vision of the EU, in order to cement the position of ASSURED in the enhancement of supply chain ecosystems operating within the EU. We also outline how these strategic impacts are achieved through all the components of the ASSURED framework, as they have been implemented and integrated into the final version of the framework.

TABLE 12: STRATEGIC IMPACT #1

Strategic Impact #1: Increased trust by all stakeholders in the supply chain including developers using/integrating the ICT components and the end-users of IT systems and services.
One of the core visions of the EU is to enable the trust assessment of systems comprising multiple heterogeneous assets, based on the multitude of trust relationships between them. As it has been outlined throughout multiple deliverables, and has been elaborated in D6.4 [6] and D7.5 [7], the enhancement of **trust and trustworthiness of a device**, as well as all the comprising devices of a **supply chain ecosystem**, is at the heart of ASSURED. Specifically, we aim to provide the **means that enable dynamic trust assessment**, while also capturing complex trust relationships between stakeholders, and operating within the **zero-trust** concept. However, this type of convergence between security and trust is not the only core dimension targeted by ASSURED. Specifically, **privacy** has been identified as an additional core consideration of users of such ecosystems, as it affects how users and stakeholders perceive the notion of trust. In this regard, in ASSURED we have provided features, innovations, and capabilities that enable the enhancement of perceived **trust level of all stakeholders and actors involved in the supply chain**, thus leading to increased user acceptance, thus unlocking existing **service silos** and unveiling new capabilities of next generation SoS, which will be consumed by the users. To this end, ASSURED provides a set of remote attestation mechanisms as part of the **attestation toolkit**, that are able to operate in different kinds of assets and to capture all aforementioned types of requirements, thus providing evidence towards the establishment of trust. For example, the **Configuration Integrity Verification (CIV)** scheme is able to ensure the correctness of the configuration state of a device in a **zero-knowledge** manner, by not requiring the device to divulge any personally identifiable configuration information, through **key restriction usage policies** that allow devices to locally attest to the correctness of their configuration state. The **Control Flow Attestation (CFA)** scheme is able to attest to the correctness of the execution of a software process, by utilizing control flow information extracted through the Runtime Tracer. In case there are strict privacy requirements and in cases where the Verifier device is not considered trustworthy, the **zero-knowledge CFA** scheme is able to delegate the processing of the traces to a trusted **Worker** node, so that the result of the attestation is forwarded to the Verifier without divulging any sensitive information about the Prover device. However, while the aforementioned schemes consider the attestation of single devices, ASSURED also provides mechanisms for assessing trust domains. Specifically, while these single-Prover, single-Verifier attestation schemes aim to achieve the core EU dimension of **trust establishment in the edge**, the **Swarm Attestation (SA)** scheme of ASSURED is a crucial steppingstone towards **establishing trust in the network**, where devices are not considered as standalone components, but as part of a service graph chain. In this regard, SA is able to attest to the correctness of the entire path in a composable manner, without breaching the privacy profiles of the devices. In addition, the SA scheme is enhanced with revocation capabilities, which enable the anonymous removal of a compromised device from the network. The core artefact of all the aforementioned attestation schemes is the **increase of the user and stakeholder confidence level in the devices comprising the service graph chain**, as well as the services offered by the target organization. This leads to an increase in the confidence level of users in the outcomes of the system, thus widening the customer segment consuming such segments, and leading to an increase in the financial prosperity and stability of the EU. The core impact of ASSURED is the ability to provide these guarantees in a wide variety of applications and industrial domains. In order to guarantee the **verifiability of the evidence** used towards the establishment of trust, ASSURED offers a set of **lightweight crypto mechanisms** that are provided to Edge devices. In the types of systems considered in ASSURED, there has been an effort to **shift away from centralized architectures** where trusted third parties are needed to securely manage operations such as the issuance of credentials and the management of keys, and **shifting the notion of trust from the cloud to the edge**. This is in line with the zero-trust paradigm, where no implicit trust is granted to users and devices, thus creating the need for the definition of crypto schemes and key management systems that capture the traditional notions of confidentiality, integrity, and availability, but are

lightweight enough to run on the edge, while also leveraging the Root-of-Trust capabilities integrated in the edge devices. In this regard, the crypto schemes offered by ASSURED are able to **operate in real-time** without significant added latency with minimal additional computational burden, while also capturing the **different types of security, privacy, and trust requirements** imposed by various actors and stakeholders across a complex supply chain ecosystem. Note that, up until now, this type of crypto has remained largely at a concept level rather than put in practice, because of feasibility concerns. However, ASSURED demonstrated the practical applicability of such crypto schemes in the types of devices comprising modern supply chain ecosystems.

For organizations aiming to benefit from the capabilities of ASSURED to increase the trustworthiness level of their assets, we also provide tools with a high level of **interoperability**, thus facilitating their integration process into any system, including legacy systems. Specifically, the security services of ASSURED are provided in a **highly modular manner** through a set of **universal harmonized APIs and on-device libraries of reusable functions** that can assist developers in the integration of the provided ASSURED services into the service graph chain. In addition, note that all the security services provided by ASSURED (except the Runtime Tracer) are provided as **open source**, in order to minimize the barrier of entry for new parties and stakeholders in the supply chain.

TABLE 13: STRATEGIC IMPACT #2

Strategic Impact #2: Protect the privacy of citizens and trustworthiness of ICT.
In the previous strategic impact, we outlined the consideration of privacy as a crucial factor in how the notion of trust is perceived by the users. As an extension of this, an additional core feature envisioned by the EU towards the enhancement of citizen privacy is the achievement of **digital and data sovereignty**. In this regard, there has been a concentrated effort by the EU towards the adoption of **Self-Sovereign Identities** and the use of **Decentralized Identifiers (DIDs)**, so that a decentralized identity management system can be implemented. This is of paramount importance, as we are moving forward towards the creation of a universal identity management system encompassing the entire EU. This approach aims to empower the users by **enabling them to control their own identities and verifiable attributes**, but also the **data originating from the devices or services they are controlling**. This includes both **operational data** (i.e., data related to the execution of software processes and services on the device), but also **threat intelligence data** (i.e., data collected by the tracing capabilities of the device as attestation evidence). ASSURED also provides a set of novel **crypto capabilities** for enhancement of security in data sovereignty. With regard to digital and data sovereignty, ASSURED not only adopted the SSI concept, but also provided core milestones to enhance not only the security of all core building blocks of the SSI even further, but also the trust level of the users in the Wallets representing their identities. ASSURED is the first project of its kind to leverage **HW-based keys** with the highest level of assurance with regard to the trust of the users in their Wallets, thus providing strong assurance capabilities to users when managing their own identities, as well as the policies based on which they will share their data. This is a significant steppingstone in how to put citizens at the forefront of identity management, in order to provide them with the capability to manage their own identities, as well as the policies based on which they can share their own data. The use of HW-based keys in the Wallets enables the achievement of properties required by the EU, such as *device binding, Holder binding, selective disclosure, unforgeability*, and *privacy,* while maintaining a high level of assurance in the management of credentials and cryptographic keys. The ASSURED Wallet supports identity management through the issuance of **Verifiable Credentials (VCs)** containing the total set of verifiable attributes of the device, as well as the creation and management of **Verifiable Presentations (VPs)** containing a subset of these attributes, that can be used in order to access a particular service of set of data. This is in line with the notion of **selective disclosure**, that enables devices to only provide the set of attributes they wish to disclose. The approach followed by ASSURED with regard to the identity management system has been designed to achieve the **minimum level of intrusion in the architecture specified by the current SSI standards** (which has defined entities such as the VC Issuer, the Verifier, the Holder, and the Wallet) by focusing only on the Holder and the leveraged Wallet in order to enhance the security of the Wallet

through the use of hardware-based keys to enhance the operational assurance of a device. This provides a **fast path to the adoption of the Wallet by the industry**, but also its **wide applicability**.

The aforementioned approach enables ASSURED to offer a wide variety of benefits in applications aligned with the core vision of the EU. Specifically, significant focus and resources have been put forth by the EU towards providing citizens with an efficient and secure manner to selectively disclose their attributes, without breaching their privacy profile. In this regard, we highlight two applications where ASSURED is able to provide significant value: (i) **Sustainable EU Mobility**, which entails the integration of the ID card and passport of the citizen into their Wallet, thus providing a more seamless manner for people to travel abroad, while disclosing their properties in a more secure manner. (ii) **Widening Access to Talents** [14], which provides users with a *Digital Certificate for Learning*, in order to enable them to selectively disclose their professional skills in a verifiable manner. This approach could lead to the creation of an international data space with a pool of users, thus enabling employers to better predict the suitability of existing candidates for their job openings. In order to support such applications, ASSURED demonstrates the ability to provide core features, such as **HW-based key binding** and **selective disclosure**, which can assist the EU to move these initiatives closer to fruition.

TABLE 14: STRATEGIC IMPACT #3

Strategic Impact #3: Acceleration of the development and implementation of certification processes.
With regard to any process performed as part of the supply chain, starting from the **onboarding of the device to the network** and including the **deployment and execution of security policies**, as well as the **monitoring of the state of the devices**, a core dimension envisioned by the EU pertains to the **certifiability and auditability** of all performed actions. Therefore, all stakeholders and entities of the supply chain should be certain about the correctness of the entire lifecycle of supply chain management, as analyzed in detail in D7.5 [7]. In recent years, there is a consensus that **Blockchain architectures** provide the required mechanisms in order to achieve this certifiability. In this regard, ASSURED extends beyond the state-of-the-art towards providing enhanced certification processes for all stages of the security lifecycle of a device. This is achieved through the deployment of security policies as **smart contracts**, as well as the recording of all outcomes of attestation actions on the ledger in the form of **attestation reports**. By providing these means, ASSURED can ensure the auditability of supply chain logistics, enhance the safety of transport flows, and contribute to increasing the levels of *safety*, *security*, *reliability*, and *comfort* in supply chains, thereby maintaining the EU's leadership in such certification and conformity assessment for providing even more trustworthy systems. As an extension of this core feature, another core need envisioned by various types of stakeholders pertains to the **remote management of assets** and the **deployment of secure updates**. In this regard, ASSURED demonstrates that it is possible to combine the use of **attestation enablers** with **monitoring capabilities**, in order to enable an efficient and certifiable software update process, thus making **Over-the-Air (OTA)** updates a reality. This approach has the potential to save manufacturers money, enable critical bugs to be patched immediately, and allow compelling new features to be added to the system at any time during its lifecycle. This culminates in the achievement of **enhanced automation**, even in safety-critical application domains where it has not yet been considered, such as the *Smart Aerospace* domain. In this case, ASSURED provides an efficient update process, which expands upon already existing, third-party enabled and error-prone state-of-the-art approaches. ASSURED has demonstrated the high level of automation achieved in all phases of the remote management process, including the collection of trustworthy evidence, the execution of the attestation enablers, and the recording of the related outcomes.

TABLE 15: STRATEGIC IMPACT #4

Strategic Impact #4: Advanced cybersecurity products and services are developed for improving trust in the Digital Single Market.
The **Digital Single Market (DSM)** is an initiative by the European Commission to remove virtual borders, boost digital connectivity, and make it easier for consumers to access cross-border online

content. There are several advanced cybersecurity products and services being developed to improve trust in the DSM. Specifically, these include designing algorithms, software, and hardware systems with security, privacy, data protection, fault tolerance, and accountability in mind from their design phase in a measurable and attestable manner.

To be able to provide the aforementioned products and develop the mechanisms that measure the performance of ICT systems, **tracing mechanisms** are required, which are able to monitor the security and privacy measures performed as part of the DSM. In this regard, ASSURED has provided novel SW-based and HW-based tracing capabilities, that enable efficient real-time tracing, with a high level of trustworthiness on the extracted trace data. In addition, a vast amount of open-source security and assurance controls have been provided by ASSURED, which can enhance the security profile of the devices, while simultaneously ensuring the accountability of the security and privacy services, and increasing the level of trust of the consumer of digital products and services.

Therefore, ASSURED not only demonstrated the feasibility of complex tracing mechanisms in resource-constrained embedded systems, but also provided all the necessary mechanisms and interfaces for HW-based solutions (implemented by MLNX/NVIDIA), thus accelerating possible **exploitation and commercialization capabilities from the EU**. These mechanisms are also characterized by a high degree of **interoperability**, thus enabling their adoption in a wide variety of systems. Specifically, the SW-based capabilities of ASSURED can be integrated into any type of embedded system, while the provided HW-tracing capabilities can be integrated into any system that supports the ARM Coresight architecture.

TABLE 16: STRATEGIC IMPACT #5

Strategic Impact #5: Validation platforms will provide assessments with less effort compared with nowadays and assure a better compliance with relevant regulations and standards, while being applicable to modern application scenarios.
There has been a great deal of discussion and analysis within the EU regarding the available state-of-the-art validation platforms, which aim to assess the entire software stack of the device, from its Firmware and OS to its application stack. We have observed that, regardless of the validation platforms and methodologies used, the assessment of the correctness and level of trust in the entire software stack induces a **significant computational overhead**. In this regard, ASSURED has provided significant impact through the development of a validation platform that offers very fast validation and verification of the correctness of **safety-critical properties** of various devices and services, and has demonstrated that there is a need within the community to converge on the types of properties that need to be attested regarding property-based attestation. Therefore, ASSURED provides a method to perform **dynamic system analysis** by extending static code analysis mechanisms, while being aligned with such validation techniques from ISO. Note that ASSURED has been presented as a use case of conceptual trustworthiness, as it has been detailed in D2.4 [15]. In this regard, in ASSURED we provide tools and procedures for **runtime, dynamic,** and **continuous assessment** of the trust and security of a system, which can unlock the capability for the **automated re-certification** of ICT products, services, and processes. Therefore, the provision of such automated tools leads to a reduction of time and effort by service providers, by enabling the efficient reuse of information and evidence relevant to certification, as well as the support of multi-scheme reuse. Specifically, the **runtime Tracing** and **remote attestation** capabilities of ASSURED provide the means for collecting, using, and reusing information relevant to the state of a device, thus enabling a much more **efficient certification of the system as a whole**. To this end, the ASSURED **Blockchain Infrastructure** enables all concerned stakeholders to perform certification of the system by checking the required information.

TABLE 17: STRATEGIC IMPACTS #6 AND #7

Strategic Impact #6: Increase the trustworthiness of European ICT services and products and the competitiveness of the European cryptography industry. **Strategic Impact #7: Data security "by design", e.g., via secure crypto building blocks**
In modern supply chains and next-generation smart connectivity systems, there are increased needs for data exchanges, which unlock new types of services. For example, in the case of Cooperative,

Connected and Automated Mobility (CCAM), the increased capability of vehicles to exchange information and intentions on their behavior on the road has enabled the deployment of Day 1, Day 2, and Day 3 applications (as previously analyzed in Section 3.5.1), thus leading to cooperative driving services. One of the core targets of ASSURED in this regard is to increase the trustworthiness of not only physical assets, but also **data assets**. Therefore, ASSURED aims to safeguard the data flows and data sharing operations between devices belonging to a supply chain ecosystem and is an advocate of the **"security-by-design"** approach, which works towards this target through the design and implementation of secure **lightweight crypto** algorithms. These aim to achieve the security, privacy, and trustworthiness requirements pertaining to the management of both operational and threat-intelligence (attestation) data.

Specifically, in continuation of Strategic Impact #1 on how ASSURED has increased the trustworthiness of the devices comprising a supply chain, as well as the perceived trust level of all stakeholders and actors in the supply chain as a whole, a core building block which has been identified by the community is the need to establish **dynamic trust relationships within all entities in a complex supply chain ecosystem**. In this regard, the designed lightweight crypto schemes of ASSURED can facilitate the conversion of edge devices into **security hardened tokens**. Thus, ASSURED has the potential to increase the **competitiveness of the European cryptography industry** by providing a new breed of lightweight crypto schemes for enabling functionalities that up until now remained largely a concept rather than being put into use, since there were feasibility concerns on integrating them into resource-constrained devices. ASSURED, by providing (open-source) primitives including Attribute-based Encryption (ABE), Attribute-based Access Control (ABAC), Attribute-based Direct Anonymous Attestation (DAA), and all other security (attestation) capabilities, not only **unlocks new research avenues,** but also **eliminates the barrier for entry in new SMEs that wish to become part of the supply chain ecosystem**; *ASSURED ensures increased trustworthiness of all ICT infrastructures, thereby maintaining the EU's leadership in the development of cyber-security products and services*.

For all the lightweight crypto schemes designed as part of ASSURED, we have also provided **security proofs and formal verifications**, which provide strong mathematical guarantees on the trustworthiness of the cryptographic processes. Specifically, we utilized the **Universal Composability (UC)** framework, which is able to guarantee the security of a protocol, even in the presence of an unbounded number of attackers, and independent of the capabilities of the attacker. By providing these formal verifications, ASSURED has provided a set of mathematically sound crypto schemes that push forward the state-of-the-art, provide the basis for the expansion of the research domain, and enable research and academic organizations within the EU and beyond to work on security enhancements. It should also be noted that several talks, master theses, and PhDs have been carried out as part of ASSURED. This has greatly assisted in the enhancement of the competitiveness of the EU crypto industry, by strengthening the expertise of researchers working in the field of cryptography within the EU.

TABLE 18: STRATEGIC IMPACT #8

Strategic Impact #8: Protecting the European Fundamental Rights of Privacy and Data Protection.
ASSURED aims to enhance and protect the Single Cybersecurity Market in Europe, which is considered a top priority. The project focuses on promoting the growth of this market by following the principles of **"duty of care"** and a **"security- and privacy-by-design"** approach. The objective is to benefit citizens, service providers, and businesses by improving products, services, and processes in terms of security and privacy, to ensure that they don't breach or compromise personally identifiable information on the users. In the context of ASSURED, "security- and privacy-by-design" refers to the utilization of various methods, techniques, and tools that aim to enforce security and privacy measures at both the network and software levels starting from the initial design phase. Specifically, as it has also been outlined in previous strategic impacts, a core vision of ASSURED has always been the convergence of security with other core properties, such as **safety**, **privacy**, and **trust**. Thus, ASSURED has considered all types of data that may be exchanged in the context of the considered systems, starting from

personally identifiable information, and moving towards **threat intelligence data**. For the former, the main challenge is how to achieve the management of such information with a high level of assurance, without breaching the privacy of the user. For the latter, ASSURED is one of the first projects of its kind to consider how assurance controls can be used in a zero-knowledge manner, thus avoiding implementation disclosure attacks.

In this regard, all schemes and operations designed as part of ASSURED aim to enhance the security profile of devices in a privacy-preserving manner. For instance, the **zero-knowledge attestation** schemes of ASSURED enable devices to attest to the correctness of their configuration state or a software process without divulging sensitive information to the Verifier, and **privacy-preserving attribute-based identity management** to access a service or a set of data. In this direction, ASSURED, in alignment with the European Fundamental Rights of Privacy and Data Protection, such as the GDPR, aims to protect personally identifiable information by **placing the user in the forefront** of identity management, towards empowering the users to have control over their own identity, and achieving user privacy when disclosing data as part of a service. This requires the Wallet to use a signature algorithm that enables the construction of Verifiable Presentations (VPs) with **selective disclosure**, while also being able to create attribute attestations that provide proof-of-possession about the unique Holder identifier ("credential blinding" capabilities). To the best of our knowledge, there has not been a technical solution for this, blocking decentralized user-centric identity management frameworks from becoming both privacy-preserving, legal and regulatory compliant (e.g., GDPR) and in alignment with emerging regulations and standards that require higher level of assurances for services (e.g., eIDAS). At the same time, enhanced privacy does not come at the expense of **accountability,** as ASSURED has provided novel and efficient **privacy-preserving revocation mechanisms** for devices that are deemed untrustworthy.

Consequently, ASSURED aligns with the cybersecurity principles outlined in the Joint Communication to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions regarding the Cybersecurity Strategy of the European Union, with particular emphasis on the article regarding the shared responsibility for ensuring security. ASSURED also supports an **automated privacy-preserving, legal and regulatory compliant infrastructure** (i.e., GDPR) in alignment with emerging **European regulations and standards (eIDAS)**. This comes in time with the ongoing process of reforming eIDAS Regulation so that it can further empower user control. There exists a strong interplay between the proposed eIDAS Regulation and the GDPR. In principle, eIDAS will be *lex specialis* to the GDPR, as its provisions will deal with specific personal data processing operations concerning electronic identification and trust services. For example, the eIDAS rules will allow EU citizens to prove their identity via mobile app, access public and private services online, pay online and facilitate everyday situations. However, such electronic signatures will still have to be implemented in accordance with the GDPR principles. Currently, the proposal is under trilogue negotiations, so the text has not been finalized and adopted. Privacy activists and Members of the EU Parliament, such as MEP Patrick Breyer, have highlighted that while the revised eIDAS text can be an important tool for the modernization and digitization of services within the EU, the initial proposal was problematic and could pose risks for the protection of personal data and privacy online. Moreover, the **EU Digital Rights (EDRi)** network has underlined that a thorough assessment of the privacy risks that arise from the eIDAS text. ASSURED has the ambition to have an impact on this ongoing discussion through the new specifications that it has provided.

TABLE 19: STRATEGIC IMPACT #9

Strategic Impact #9: Assurance/risk management, advanced assurance, and security/privacy-by-design.
Currently available state-of-the-art methodologies typically consider risk assessment and management in a fragmented manner, by either performing assessment based on **one specific property**, or by performing assessments on individual assets **without considering the interdependencies between them**. In ASSURED, we go beyond the state-of-the-art by highlighting the need for a holistic risk assessment methodology, that considers all properties required for the establishment of trust (such as security, safety, and privacy, as have been defined in the international standards ISO/IEC 22624:2020 [16], Y.3057 [17], and ISO/IEC TS 5723:2022 [18]), as well as the security relationships between the assets. The approach followed in ASSURED is able to **consolidate**

all these dimensions towards performing a better classification of the most impactful attacks targeting the types of systems considered in ASSURED, and enhancing the security posture of supply chain ecosystems operating within the EU. This culminates in supporting end-to-end ICT-based system certification processes, which are accelerated through the ASSURED services that handle security threats and vulnerabilities and evaluate the security and resilience of supply chain ecosystems. The risk assessment process starts from a security- and privacy-by-design approach, but is executed **dynamically during runtime**, thus providing updated policies for advanced operational assurance throughout the operational lifecycle of the target system. This dynamic nature supports different types of security and privacy conformity assessment through novel dynamic evidence-based processes, considering that the runtime execution of Risk Assessment can update the conformity assessment of the target system.

In addition, risk quantification methodologies are typically **targeted and tailored to specific application domains**, and selecting the most suitable risk assessment methodology is of paramount importance for the better assessment of risk for a topology, depending on the domain where it is applied. This modularity is needed in order to support **cybersecurity autonomy** in EU services and the creation of **hygiene marketplaces**, which require the development of approaches concerning dynamic, real time, collaborative risk assessment and information sharing. In this regard, ASSURED provides a **highly modular design and implementation**, capable of integrating several methodologies, based on which the set of quantified risks can be fused for better assessing the impact of any identified threats and risks. Therefore, the ASSURED Risk Assessment scheme is easily extendable, and facilitates the inclusion of appropriate scoring systems for the targeted application domain (i.e., TARA for automotive systems) into a holistic Risk Assessment process. This enhances the applicability of ASSURED in a wide variety of domains, thus extending its adoption capabilities by any type of supply chain ecosystem operating within the EU and beyond.

TABLE 20: STRATEGIC IMPACT #10

Strategic Impact #10: Protecting the ICT infrastructures (including Cyber Threats Management, System Security, Trusted Hardware/Edge Devices Security/IoT Security).
Up until now, the protection of ICT infrastructures has been based on **centralized security solutions**, with the Public Key Infrastructure (PKI) being at the forefront of these designs. However, regardless of the benefits offered by PKI pertaining to the security and privacy of ICT infrastructures, there is still a number of challenges to be addressed, such as the **scalability** of the provided security solutions, as well as the achievement of a **secure continuum between the Cloud and the Edge**. Specifically, the evolution of our interconnected society brings multiple layers of cloud, edge computing, and IoT platforms that continuously interact with each other. Yet this always-connected ecosystem populated with potentially vulnerable entities requires advanced, smart, and agile protection mechanisms to manage the security and privacy of individual components throughout their lifecycle, and of the overall systems. The complexity of such interconnected environments underlines the need for the proactive and automated detection, analysis, and mitigation of cybersecurity attacks in cloud, at the edge, for OT, IoT deployments, and in application domains, such as *Smart Cities*. Integrating end-to-end security and user-centric privacy in complex distributed platforms requires work to address security threats and vulnerabilities over the entire platform ecosystem. In this regard, as part of the efforts taken in the context of supply chain ecosystems operating within the EU in recent years, ASSURED aims to facilitate the transition towards **decentralized architectures**, thus enabling secure infrastructures, secure identities, and usability for a security chain, covering communication, data collection, data transport, and data processing. These aim to shift not only the notion of trust closer to the edge, but also the resources required for trust achievement, materializing the vision of the EU towards a secure computing continuum. A core prerequisite for the design and realization of such an approach is the **secure integration of untrusted IoT devices in trusted environments** which, in turn, requires the conversion of edge device into security hardened conversion of the edge devices into **security hardened tokens**. In this regard, ASSURED pioneered by offering all the necessary tools that enable secure edge acceleration, and demonstrated the use of **HW- or SW-based Roots-of-Trust (RoTs)** to enable the move towards distributed and decentralized solutions. Note that such commodity RoTs are becoming increasingly affordable, thus enabling this chip-to-cloud assurance provided as part of ASSURED, considering

also the innovations brought forth by the MEC. This approach is able to provide a high level of scalability in the protection of ICT infrastructures, while also minimizing the dependencies with the backend, weakening the trust assumptions for devices and verifying entities, and moving closer to achieving an edge-to-cloud continuum. Thus, ASSURED enacts upon the expected core driving force in the following years, i.e., the adoption of the **zero-trust paradigm**. Based on this, no device is considered trusted by default, and should be able to provide verifiable claims regarding its identity and state.

In addition, the side research performed as part of ASSURED has provided some initial insights on how existing crypto schemes (such as DAA) can be converted into **quantum-secure** schemes. In this regard, ASSURED has provided the foundation for the EU to be able to protect ICT infrastructures in the long term, even when quantum computing has reached a high level of maturity and applicability.

TABLE 21: STRATEGIC IMPACT #11 AND #12

Strategic Impact #11: Effective Access Control to System Components and Management of Trustworthy Updates **Strategic Impact #12: Tools for providing assurance that third-party and open-source components are free from vulnerabilities, weaknesses and/or malware**
In next-generation supply chain ecosystems comprising multiple heterogeneous devices and services with varying security and privacy requirements, there is a need for **methodologies for assessing the level of trust** for systems that may consist of various heterogeneous and insecure components. This calls for new best practices on cyber-security that enable devices to make assurance statements on their correctness as part of a hierarchical SoS. The firmware of devices, implementations of communication protocols and stacks, Operating Systems (OSs), Application Programming Interfaces (APIs) supporting interoperability and connectivity of different services, device drivers, backend cloud and virtualization software, as well as software implementing different service functionalities, are some examples of how software provides the essence of systems and smart (networked) objects. In addition, supply chain issues, including integration of software and hardware, should be considered appropriately. Therefore, a holistic methodology is needed, integrating **runtime methods for monitoring and enforcement,** methods for **detecting security flaws and vulnerabilities**, and **access control methods for accessing the outcomes** of these assessments. As an extension of Strategic Impact #1 related to the increase of the level of trust in the considered type of systems, ASSURED provides a wide array of methods for the creation of such a holistic methodology. In general, for the **detection of security flaws and vulnerabilities**, there are two types of analysis frameworks of software applications: **dynamic analysis** and **static analysis**. Up until now, the core focus of such frameworks was **static analysis**, where several techniques have been proposed. However, such techniques are typically inefficient for large-scale supply chain ecosystems and suffer from the **path explosion problem** (i.e., the exponentially increasing requirement for computing power to verify more complex software). Therefore, we conclude that **dynamic analysis** is required in order to be able to monitor a system efficiently in real-time. While there have been several attempts to design such a versatile method for capturing and identifying vulnerabilities, a core challenge in this regard is the **tradeoff between performance and accuracy**. In other words, to achieve high accuracy, a high overhead on the system performance would be required. In this regard, ASSURED demonstrated the how a high level of performance and accuracy can be achieved in the context of dynamic analysis through the **Control-Flow Attestation (CFA)** enabler, which is a type of attestation that can provide diagnoses regarding control flow hijacking at the Prover device. The design of CFA provides a significant step forward in the state-of-the-art in this regard, since it uses **AI-assisted** methods in order to achieve a high level of accuracy not only in the detection of **Return-Oriented Programming (ROP)** attacks, but also in **Data-Oriented Programming (DOP)** attacks, compared to available solutions in the literature. Note that these are notoriously difficult to detect, since they do not involve the attacker making any changes in the control flow graph, thus highlighting a core contribution of ASSURED in securing software processes against highly advanced attacks. In addition, ASSURED has pioneered by designing and implementing **HW- and SW-based tracing variants** that demonstrated both a **high level of accuracy**, and are **efficient enough to operate in resource-constrained edge systems**. These operate in tandem with the aforementioned AI-enhanced CFA scheme in order to require less rich tracing information in order to achieve a high level of accuracy,

thus significantly increasing the efficiency of the tracing process. In addition, the HW-based tracing variant is based on **commodity microcontrollers typically encountered in edge devices**. In this regard, ASSURED has provided designs and interfaces which significantly enhance the industry of open-source components for the detection of vulnerabilities, and opens the path for the commercialization of such solutions to facilitate their adoption by a wide range of industries operating within the EU.

In the context of the aforementioned types of systems running heterogeneous devices and multiple types of services, as aforementioned, one core need towards providing trust assessment methodologies is the implementation of an **access control mechanism with a high level of granularity that can be supported by such devices**. Up until now, while there have been several advanced cryptographic schemes proposed in the literature towards achieving this goal, the majority of the proposed schemes are not able to run efficiently in resource-constrained edge devices typically present in this type of systems. In this regard, ASSURED has provided novel mechanisms that provide the management of data with a much higher level of granularity, in a manner that can be supported by the aforementioned types of devices. Specifically, the **Attribute-Based Encryption (ABE)** scheme is able to protect the confidentiality of data based on access control policies, and **Attribute-Based Access Control (ABAC)** is able to support access control mechanisms that provide the capability to manage data access with a much higher level of granularity, even within the same data chunk. This is particularly important in modern service graph chains where different types of roles and authorities need to access different types of data. Consider, for instance, the *Smart Cities* application domain, where different types of entities (e.g., police officers and firefighters) need to access different types of data, depending on the protection services that need to be provided.

In order to achieve the necessary level of vigor to achieve the target level of trustworthiness for the types of aforementioned systems, ASSURED has unveiled new capabilities that can include cyber-security and resilience as an integral part into the development process of **Over-the-Air (OTA)** mechanisms by OEMs. To this end, the protection of IT components and devices against a series of new attacks, or the mitigation of existing ones, can be performed with a **trustworthy update** mechanism. In this context, ASSURED aims to make secure remote updates a reality (even in the case of OTA updates in the context of the *Smart Aerospace* domain, where such mechanisms have not yet seen widespread adoption) through the use of attestation enablers that ensure the correctness of the device before and after the update, as well as the update process itself. Such a secure update solution can be also utilized at the device level by existing RTOS solutions.

TABLE 22: STRATEGIC IMPACTS #13 AND #14

Strategic Impact #13: Instrumentation and secured communication with system components for dynamic tracing and testing **Strategic Impact #14: Methods and environment for secure coding by-design and by-default and secure hardware and software construction**
Instrumentation refers to the process of adding instructions to a program. In this regard, one useful instrumentation tool pertains to gathering information about the program's behavior during runtime, which is also referred to as **runtime tracing**. **Dynamic instrumentation** in particular is a technique that allows the insertion of instructions at runtime for current off-the-shelf (COTS) binaries, without the need to stop or restart the program or maintain multiple instrumented versions of their dependent libraries. This is especially useful for tracing and testing, as it allows developers to gather information about the behavior of a program in real-time, without interrupting its execution. Dynamic instrumentation can also be used for tracing and collecting runtime information from the execution of software processes in embedded devices. However, such existing approaches are rather immature in the scientific community. In this regard, ASSURED demonstrated how dynamic instrumentation and dynamic binary rewriting can be used in order to not only achieve runtime tracing and aggregate the collected traces, but also **validate the correctness of the traces**, i.e., verify that they originate from a correct and trustworthy tracer. Thus, ASSURED overcomes a core challenge regarding the authentication of the Tracer. Specifically, the ASSURED Tracer provides assurances on its own security through its execution in secure environments. This is a milestone in the current

efforts of the (standardization) community on how to establish such tracing capabilities in a secure and authenticated manner, as part of the device's overall **Trusted Computing Base (TCB)**.

TABLE 23: STRATEGIC IMPACT #15

Strategic Impact #15 – Formally verified methods to make supply chains secure
In order to enable and accelerate the certification of the security and assurance controls used in the context of a supply chain, the implemented cryptographic schemes need to be **formally verified**, with **sound mathematical proofs** of their security and correctness. In this regard, in ASSURED, we employed the **Universal Composability (UC)** model, which provides the capability to model various attacker capabilities, while allowing the construction of proofs that are applicable in the context of any application domain. This is a core innovation of ASSURED towards providing cryptographic enablers that can enhance the security posture of any supply chain ecosystem operating within the EU and beyond, capturing a wide array of industries and domains. Specifically, the UC framework guarantees that the security of a protocol is preserved under an internal composition operator, but also provides stronger guarantees for maintaining the security of the scheme in any context, **even in the presence of an unbounded number of attackers and independent of the capabilities of the attacker**. The UC framework achieves the formal verification of the security proofs under these strong assumptions, thus serving towards the scalability, certifiability, and universal applicability of the lightweight crypto protocols. Specifically, the UC framework allows specifying the security requirements of practically any cryptographic task in a systematic way by identifying the ideal functionality model. A core challenge that has been identified by the EU at the beginning of 2023 is **trusted path routing**, i.e., the establishment of trusted topologies which only include trust-verified network devices, towards ensuring that all devices in a path have an acceptable level of trust and enhancing the security of the supply chains. This challenge can be alleviated by the mathematically proven and formally verified methods provided by ASSURED.

TABLE 24: STRATEGIC IMPACT #16

Strategic Impact #16 – Secured disruptive technologies
Due to the complexity of modern supply chain ecosystems and next generation Systems-of-Systems (SoS), there is a consensus that the adoption of a singular security control is not enough for providing operational assurance to the entire service graph chain. There is also the need for an approach with the required level of agility, to enable the addition of several different security controls depending on the **security and privacy requirements**, as well as the **available resources** at the considered system, in order to protect all phases of the operational lifecycle of the system. This consideration motivated the **multidisciplinary approach** of ASSURED, pertaining to the development and analysis of novel security and assurance controls that can underpin the entire lifecycle of cyber-physical systems, as part of modern supply chain ecosystems. In this regard, the ASSURED consortium has pushed forward the state-of-the-art in various multidisciplinary domains, such as attestation, runtime verification, trust assessment, risk assessment, as well as secure and privacy-preserving data sharing through the use of Blockchain for enhanced certification and auditability capabilities. All these innovations have been coupled with **open-source implementations**, in order to avoid a fragmented adoption from the industry, thus leading to a **pragmatic framework** that escapes the pitfalls of similar large endeavors, that either create new technologies with limited applicability and user acceptance, or provide limited improvements to existing solutions. In contrast to such approaches, ASSURED has provided **disruptive new technologies**, as part of a framework with a pragmatic view towards operational assurance in modern supply chain ecosystems with a high level of complexity and heterogeneity. These technologies have been demonstrated to offer a high level of applicability and adoption potential by organizations belonging to a wide variety

of application domains, and pave the path for the development of a concrete exploitation plan, as well as a business and commercialization roadmap, as outlined in D7.5 [7].

5 CONCLUSIONS

In this deliverable, we performed an assessment of the impact of the ASSURED on various application domains, in order to evaluate the achievement of the core vision of ASSURED, to provide operational assurance to large-scale complex Systems-of-Systems comprising heterogeneous devices with various security and privacy requirements and running mixed-criticality services. Specifically, we presented the **value propositions** of ASSURED and the various technical and **research activities** performed by the ASSURED consortium in order to achieve the aforementioned vision. In the previous version of the deliverable (D7.6 [1]), we provided the impact assessment of ASSURED based on the components that were implemented during the first reporting period. Here, we provide an updated version of this assessment, also considering the newly updated and implemented components which were integrated into the final version of the ASSURED framework.

Next, we provided a summary of the value propositions and research activities carried out throughout the second reporting period of ASSURED. These include the updated version of the **zero-knowledge CIV scheme** which employs **key restriction usage policies** in order to enable devices to attest to the correctness of their configuration state without revealing any information on the device itself. The updated **ML-based CFA** scheme employs a Graph Neural Network (GNN)-based approach in order to enable classification between benign and malicious traces, and the **zero-knowledge CFA** scheme employs zkSNARK proofs in order to delegate the attestation tasks to an intermediate worker. These attestations are supported by the updated **SW-based** and **HW-based Tracer**, that have been updated in order to be tailored to the type of attestation evidence required. In addition, the **TPM-based Wallet** has been fully integrated into the ASSURED framework, thus enabling interactions of the device with the Blockchain Infrastructure, as well as the execution of the data management schemes of ASSURED, namely **Attribute-Based Encryption (ABE)**, **Attribute-Based Access Control (ABAC)** and **Dynamic Symmetric Searchable Encryption (DSSE)**.

The impact of these technologies was investigated in the context of the four envisioned use cases. Specifically, in the *BIBA Smart Manufacturing* demonstrator, ASSURED ensures that all devices participating in a manufacturing floor successfully establish trust relationships and prevents manipulation of devices and software by malicious third parties, in order to reliably provide accident prevention between human workers and robotic arms. In this context, the ASSURED framework is characterized by a high degree of scalability, in order to be easily deployed to industrial environments of various sizes without compromising security. In the *UTRC Smart Aerospace* use case, ASSURED provides security protection to the aircraft components (devices and networks) through the use of attestation enablers, particularly CIV for the configuration integrity of the electronic units belonging to the architecture of the aircraft, and CFA for the verification of the execution flow of safety-critical processes, through the optimal, secure, and certifiable policy deployment through the Blockchain Infrastructure. In the *DAEM Smart Cities* use case, ASSURED fulfills the strict privacy requirements characterizing the data collected by devices such as smoke sensors and IP cameras, while also providing the appropriate level of granularity in data access pertaining to operational- or attestation-related data so that only the parties with the required attributes (e.g., police officers or firefighters) can access a specific set of data. Finally, in the *SPH Smart Satellites* use case, ASSURED aims to achieve the protection of the hardware of the CubeSats against malicious activity that can exploit vulnerabilities that can affect the operation of hardware components.

The results presented throughout this deliverable culminate into the presentation of the **strategic impacts** of the ASSURED framework, considering the purpose of ASSURED to enhance the **security**, **safety**, **resilience**, and **data trustworthiness** of the aforementioned types of supply chain ecosystems. Specifically, these strategic impacts include protection of the ICT infrastructures and the achievement of increased trust of all stakeholders in the

operations performed in the supply chain, while also protecting the privacy of all participating users. This is achieved through the provision of advanced **risk management**, **assurance**, and **security/privacy-by-design**. In addition, ASSURED focuses on the acceleration of the development and implementation of certification processes, by ensuring all operations and attestation or operational data are auditable and certifiable, and that the framework is compliant with the relevant regulations and standards. ASSURED is also focused on contributing to the competitiveness of the European cryptography industry through a series of advancements in the state-of-the-art, the development of services for the **Digital Single Market (DSM)** founded by the European Commission, and the protection of **European Fundamental Rights of Privacy and Data Protection**. Finally, it is important to note that the ASSURED artefacts (except the runtime Tracer) are provided as open-source, towards contributing in the research efforts in various academic and industrial domains.

Overall, a large number of technological advancements and research innovations has been carried out throughout the lifecycle of the ASSURED project, thus not only pushing forward the state-of-the-art in various research domains, but also providing significant value to supply chain ecosystems and organizations aiming to benefit from the security services offered by ASSURED.

ABBREVIATIONS

Abbreviation	Description
ABAC	Attribute-based Access Control
ABE	Attribute Based Encryption
AK	Attestation Key
API	Application Programming Interface
BFT	Byzantine Fault Tolerance
BGP	Byzantine Generals Problem
CA	Certification Authority
CFA	Control-Flow Attestation
CFI	Control-Flow Integrity
CIV	Configuration Integrity Verification
CPS	Cyber Physical System
CP-ABE	Ciphertext Policy Attribute Based Encryption
CRED	AK Credential
DAA	Direct Anonymous Attestation
DApps	Distributed Applications
DLT	Distributed Ledger Technology
DoA	Description of Action
DOP	Data Oriented Programming
DPos	Delegated Proof of Stake
Dx.x	Deliverable x.x
ECDSA	Elliptic Curve Digital Signature Algorithm
EK	Endorsement Key
HLF	Hyperledger Fabric
IoT	Internet of Things
KDF	Key Derivation Function
KP-ABE	Key Policy Attribute Based Encryption
MSP	Membership Service Provider
PBFT	Practical Byzantine Fault Tolerance
PCR	Platform Configuration Register
PK	Public Key
PLC	Programme Logic Controller
PoA	Proof of Authority
PoB	Proof of Burn
PoC	Proof of Capacity
PoET	Proof of Elapsed Time
PoS	Proof of Stake
PoW	Proof or Work
PPoS	Protection Profiles
RA	Revocation Authority

ROP	Return Oriented Programming
SA	Swarm Attestation
SCB	Security Context Broker
SE	Searchable Encryption
SGX	Software Guard Extensions
SK	Secret Key
SoS	Systems-of-Systems
TC	Trusted Component
TCB	Trusted Computing Base
TEE	Trusted Execution Environment
TPM	Trusted Platform Module
WPx	Work Package X

REFERENCES

[1] "D7.6 Project Impact Assessment," *The ASSURED Consortium,* 30 June 2022.

[2] "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union," *Official Journal of the European Union,* 19 July 2016.

[3] "Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)," *Official Journal of the European Union,* 7 June 2019.

[4] "JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL The EU's Cybersecurity Strategy for the Digital Decade," *European Commission, Directorate-General for Communications Networks, Content and Technology,* 16 December 2020.

[5] "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC," *Official Journal of the European Union,* 4 May 2016.

[6] "D6.4 Performance Evaluation and Adoption Guidelines," *The ASSURED Consortium,* August 2023.

[7] "D7.5 Market Analysis, Business and Sustainability Plan," *The ASSURED Consortium,* August 2023.

[8] "D7.4 Market Analysis, Business and Sustainability Plan," *The ASSURED Consortium,* October 2022.

[9] "D6.3 Final Demonstrators Implementation Report," *The ASSURED Consortium,* August 2023.

[10] "Cost of a Data Breach Report 2022," IBM Security, 2022. [Online]. Available: https://www.ibm.com/downloads/cas/3R8N1DZJ. [Accessed 29 August 2023].

[11] "ENISA Threat Landscape 2021," European Union Agency for Cybersecurity, 27 October 2021. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021. [Accessed 29 August 2023].

[12] "Internet Organised Crime Threat Assessment 2021," European Union Agency for Law Enforcement Cooperation, 2021. [Online]. Available: https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf. [Accessed 29 August 2023].

[13] "Guidance for Day 2 and Beyond Roadmap," *CAR 2 CAR Communication Consortium,* 25 September 2019.

[14] "Credentials to Employment: The Last Mile," *Digital Credentials Consortium Report,* 30 September 2022.

[15] "D2.4 ASSURED Runtime Risk Assessment Framework - version 2," *The ASSURED Consortium,* February 2023.

[16] "ISO/IEC 22624:2020 Information technology — Cloud computing — Taxonomy based data handling for cloud services," *ISO/IEC JTC 1/SC 38 Cloud computing and distributed platforms,* February 2020.

[17] "Y.3057 : A trust index model for information and communication technology infrastructures and services," *International Telecommunication Union (ITU),* 10 December 2021.

[18] "ISO/IEC TS 5723:2022 Trustworthiness — Vocabulary," *ISO/IEC JTC 1 Information technology,* July 2022.

[19] "D7.3 – Dissemination, Exploitation and Standardization (Final Version)," *The ASSURED Consortium,* August 2023.