PRIVATEER

Privacy-first Security Enablers for 6G Networks

WHITE PAPER

Security- and Privacy-related KPIs/KVIs for 6G

v.1.0, May 2024

Co-funded by the European Union

6G SNS

PRIVATEER has received funding from the Smart Networks and Services Joint Undertaking (SNS JU) under the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101096110

Space Hellas SA, NCSR "Demokritos, Telefónica I&D, RHEA System SA, INESC TEC, Infili Technologies PC, Ubitech Ltd, Universidad Complutense de Madrid, Institute of Communication and Computer Systems, Forsvarets Forksninginstitutt, Iquadrat Informatica SL, Instituto Politecnico do Porto, ERTICO ITS Europe

Contributors

Name	Organization
Maria Christopoulou, Dimitris Santorinaios, Ioannis Koufos, George Xilouris	NCSR "Demokritos"
Georgios Gardikis, Victoria Katsarou	Space Hellas S.A.
Lampros Argyriou, Antonia Karamatskou, Antonis Litke, Nikolaos Papadakis	Infili Technologies S.A.
Fábio Silva, Ricardo Santos	Instituto Politécnico do Porto
Antonio Pastor, Mattin Elorza	Telefonica Innovacion Digital S.L.

License and Disclaimer

1 Related work

A critical area of 6G-oriented research involves the development of Key Performance Indicators (KPIs) and Key Value Indicators (KVIs) for several operational aspects of 6G networks, including security and privacy. This section presents an overview of relevant studies that contribute to the definition of 6G KPIs and KVIs, explicitly focusing on security and privacy aspects:

Hexa-X [1][2]: As a flagship initiative for 6G technology, the Hexa-X project has proposed a comprehensive set of KPIs and KVIs related to 6G networks. The project has been instrumental in advancing the understanding and establishment of relevant KPIs and KVIs for the future 6G networks, addressing various aspects of 6G, such as network performance, security, and privacy. The KPIs and KVIs produced by Hexa-X serve as essential guides for evaluating the progress and effectiveness of 6G solutions in various domains, including network capacity, latency, and the critical areas of security and privacy.

White Paper "Beyond 5G/6G KPIs and Target Values", 5G-PPP [3]: In this white paper, the 5G Public Private Partnership (5G-PPP) presents the available Beyond 5G (B5G) and 6G Key Performance Indicators (KPIs) as of 2022, obtained from 5G PPP Phase III Projects. While the majority of these KPIs primarily focus on network-related aspects (e.g., area traffic capacity, bandwidth, latency), the paper also identifies three KPIs specifically addressing security and privacy concerns:

- *Anomaly detection precision*: This KPI measures the Precision-recall Area Under Curve (AUC) with at least minimum scoring in precision and recall. The project that provided this KPI set a target value of >0.85 with at least 85% scoring in both precision and recall.
- *Security conformance*: Conformance to security constraints includes, among others, Network slice controller authentication and Data integrity of a network slice. No target value is provided, because the use of security mechanisms or the security violation is not directly observable by the network slice consumer and cannot be measured as a quantifiable metric.
- *Tenant data privacy*: This relates to confidential information shared between the tenants and the infrastructure owner, which is needed to optimize the whole system's performance. The target value is not provided.

White Paper "Beyond 5G, Message to the 2030s", Beyond 5G Promotion Consortium [4]: Japan's Beyond 5G Promotion Consortium (B5GPC) actively supports Beyond 5G (B5G) advancement by conducting relevant studies and identifying trends based on societal needs toward its commercialization in the 2030s. This White Paper delves into B5G concepts, requirements, and architectures, considering key technologies and

anticipated use case scenarios. Additionally, the Consortium proposes several KPIs, including target indicators for "Trustworthiness, Security, and Robustness":

- Cryptographic processing speeds exceeding the peak data rate (100Gbps and more)
- Support for 256-bit key length for post-quantum cryptography
- Instantaneous recovery from disasters and failures

Strategic Research and Innovation Agenda, Networld Europe [5]: Networld Europe is a European initiative that brings together researchers, industry professionals, and policymakers to coordinate research efforts in advanced communication networks and services, such as 5G and beyond. Networld Europe published the Strategic Research and Innovation Agenda (SRIA) 2022, addressing various aspects of next-generation communication technologies in Europe, including system services, network and service security, radio access innovations, and future emerging technologies. The document also proposes representative KPIs in the field of Security, such as the "*Response time of protection and restoration mechanisms*," with a target value of below 1 sec by 2025.

The roadmap to 6G Security and Privacy, Porambage et al. [6]: This paper discusses the potential security and privacy challenges and solutions in 6G wireless networks. The authors present the possible 6G threat landscape based on the anticipated 6G network architecture and examine security considerations associated with 6G enabling technologies, such as distributed ledger technology (DLT), physical layer security, and AI/ML (Artificial Intelligence/Machine Learning), among others. They also share their vision on 6G security and privacy KPIs, including a guaranteed *Protection level* against threats and attacks, *Time to respond* against malicious activity, the *Coverage* of security functions over the 6G service elements and functions, *AI robustness*, *i.e.*, AI algorithms hardened for security, *Security AI-model convergence time* (training time), *Security Function Chain round-trip-time*, referring to the time it takes for chained security functions to process, analyse, decide and act, and *Cost to deploy security functions*, measuring the cost of deploying security functions.

2 Security and Privacy KPIs/KVIs for 6G

PRIVATEER proposes representative KPIs and KVIs for 6G networks as a contribution to the SNS Programme, emphasizing Security and Privacy, aligned to the project's scope, objectives and technical approach. As 6G is expected to incorporate various advanced technologies, augmenting these KPIs with technology-specific indicators is essential. This will ensure that these emerging technologies are adequately assessed and integrated into the envisioned 6G architecture, providing robust performance, security and privacy guarantees.

2.1 Incident-detection KPIs

Incident detection is commonly driven by a combination of (federated) AI and rule-based techniques. In order to quantify how well intrusion-detection mechanisms work, a number of KPIs are typically defined. Firstly, the accuracy of threat classification models is measured, and a reasonable reference value is greater than 80%. Moreover, *the number of false positives* and *false negatives* should be reduced to less than 10% in a federated scheme. Another aspect that is insightful regarding the security aspects of intrusion-detection and prevention systems is the mean time of detection. Two numbers can be measured: the *mean time to detect a threat* and the *mean time to classify* it. Both should be smaller than 10 seconds, which can be compared to the KPIs envisaged previously. Finally, for federated-learning schemes, the *accuracy loss* can be defined by comparing the centralized with the federated models. This loss is given by *(1 – accuracy of federated model/accuracy of centralized model)*. Such a loss should be less than 10%.

2.2 Differential-privacy KPIs

Differential Privacy (DP) is a probabilistic privacy mechanism that provides an information-theoretic security guarantee. Given two neighboring data sets, D and D' differing by one record, differential privacy defines privacy loss of a randomized algorithm as its sensitivity on the datasets. Differential privacy and its variants guarantee the upper bounds on privacy loss of an ML model. Those bounds are affected by the DP mechanism applied to the algorithm, the iterations and complexity of the algorithm as well as the communication of the participants in the case of a federated-learning framework.

DP may be accurately parametrised using two numbers (ε, δ), where ε describes the maximum distance between two data sources, and δ describing the probability of data being leaked accidentally.

Privacy guarantees come with utility trade-offs. Since more noise is needed to provide higher privacy guarantees, usually the performance of the models tends to deteriorate. A metric that has the capacity of tracking that trade-off is *Accuracy loss [7]* which is calculated as follows:

```
Accuracy Loss = 1 - (Accuracy of Private Model/Accuracy of Non-
                    Private Model)
```

Another way to evaluate the privacy perseverance of an ML model is to evaluate *the success of adversarial privacy attacks*.

Such attacks are the following:

- *Inference of Membership:* Privacy attack that attempts to determine whether a specific individual's data was included in a dataset that was used to train a machine learning model. In this case, we could use the reverse of the Adversarial Accuracy during Inference [8].
- *Inferring properties of private training data (model inversion):* The basic idea behind an inference of private training data attack is to use the trained model to infer properties of the training data, such as the distribution of the data. This can be done by analysing the output of the model and using it to construct a proxy for the training data. Most of the time this proxy is used to train meta-classifiers, so one way that we could measure the adversarial success is by the Precision and Recall of meta-classifiers [9].
- *Inferring Training Input & labels (reconstruction attack):* These attacks aim to reconstruct the original training data samples and the corresponding labels. In this case, we could measure the *MSE (Mean-Squared Error) between a target and its reconstruction [10]*.

Finally, for measuring the quality/utility of data after anonymization, usually, a quality loss metric is employed, which measures how much quality is lost by reporting anonymized data instead of real data. It is the difference/distance between the anonymized data and the original data, and, therefore, data-type dependent (for example, for location data, it could be the Euclidean distance between original data and anonymized data). The *accuracy loss* metric proposed above is equivalent to measuring the accuracy loss of applying a private vs non-private model. It can be applied at the exit of the AI/ML mechanism, or at the exit of the anonymization mechanism (e.g., before data being fed to the AI/ML mechanism). Therefore, the *accuracy loss* serves as a general-purpose quality metric that can be used for both ML models as well as anonymization models.

2.3 Adversarial protection KPIs

As mentioned above, for privacy, adversarial protection comes with utility trade-offs. One possible KPI relates to the fact that adversarial protection mechanisms introduce *performance reduction* with respect to common incident detection metrics, such as accuracy, precision, recall and F1. When training a detection engine using secure multiparty computation (MPC), a run-time performance overhead (from introducing adversarial protection mechanisms) of no more than 10x seems reasonable. For differential privacy, *sensitivity* [11] could be used as a measure, and it should be less than a given value with negligible performance reductions with respect to common incident-detection metrics (e.g., with epsilon at 1 and delta around 10^{-6}). For model poisoning attacks, one potential KPI is the *amount of adversarial workers/agents that can be tolerated (with negligible performance loss)*. For example, the system should handle 10% adversarial workers.

2.4 Orchestration (Intrusion Response) KPIs

In an envisioned 6G network environment, the rapid response to security incidents becomes crucial due to the increased network complexity and the massive number of interconnected devices. The *Mean Time to Respond* (MTTR) is a KPI that measures the average time it takes for security functions or network management systems to detect, analyze, and counteract malicious activities or security incidents.

A shorter MTTR indicates that the 6G network can quickly identify and respond to security threats, thereby minimizing the impact of attacks on network performance, user experience, and data integrity. The MTTR is essential to streamline and accelerate the response process and monitor the effectiveness of automated incident response solutions, such as security Orchestration, Automation, and Response (SOAR) systems.

The *Decision Time* is a KPI used to evaluate the efficiency of a trained ML model in making predictions or decisions about network resource orchestration. In the context of 6G, where an ML model is orchestrating resources, the decision time becomes critical to the overall performance and responsiveness of the network. When an ML model orchestrates resources in a 6G network, it must make real-time or near real-time decisions to allocate resources effectively, manage network traffic, and adapt to changing conditions, e.g., induced by malicious activity. The Decision Time KPI indicates how fast the ML model can process input data, analyze the current network state, and make informed decisions to protect the network. Representative values from the literature include 220ms for a deep reinforcement learning model trained on a simulated 5G environment [12]. Several design considerations affect this KPI, including the ML-model optimization techniques, whether hardware acceleration is used, and whether edge computing is employed to reduce the latency associated with data transfer.

We further elaborate with more ad-hoc Key Performance Indicators (KPIs) exclusively specialized on the slicing & orchestration of 6G networks infrastructure, specifically *after* a malicious cybersecurity incident is detected and a response must be enforced.

Time to resource preparation end-to-end: from the moment an order is expressed as intent until all multi-party resources that comply with corresponding privacy service requirements have been discovered and provisioned. *KPI target:* discover and provision multi-party resources in *less than 1 minute*.

Time to repair: from the moment a security anomaly breach is detected (or predicted) until relevant intra- or inter-domain adaptation primitives have been triggered and completed, bringing the system back to a stable and privacy-by-default SLA-compliant state. *KPI target:* complete intra-domain adaptation actions in *less than 1 minute* and inter-domain in *less than 5.*

Time to compose: from the moment a slice that includes PaaS services (from Cloud to Edge) as well as IoT devices (Far Edge), is requested until the time that it is successfully deployed over the compute continuum infrastructure with full Privacy SLAs guaranteed; *< 5 min.*

Time to migrate: from the moment that it is decided that a PaaS service should migrate, until the time that migration is completed, bringing the PaaS to a fully operational state (in terms of PaaS fulfillment of agreed condition); *< 1 min* in case of intra-domain migration, and *< 3 min* in case of inter-domain migration.

2.5 Distributed Ledger KPIs

Blockchain and distributed ledger solutions have been around for some years. Nevertheless, their integration with 6G services is a field currently under research. Thus, specific KPIs have not been established yet. Consequently, the proposed KPIs for the Blockchain technology are based on values from existing implementations that are not dedicated to 6G.

In general, the blockchain has two basic metrics those are i) the *latency* and ii) the *throughput*. The latency refers to the time between the receipt of the request and the commitment of the transaction (i.e., the operation), while the throughput refers to the total number of transactions supported. Quantifiable metrics, based on scalability and unit testing regarding the number of transactions and the trust anchors that can be supported by a blockchain peer, can be acquired from [14][15]. Based on this, regarding the KPIs for the latency, they is further broken down into the writing and reading transaction phases, while for the throughput, a single blockchain peer should be able to perform > 1000 transactions concurrently and engage with 3 sources.

According to [13] there are several factors that may influence the two metrics, depending on the use case scenario. One of these metrics is the number of nodes that constitute the network. An increased number of nodes signifies that more time is

needed for the execution of the transaction. For this indicator, 1 peer is considered per 200 devices as per [15]. [13] further defines other factors that may influence the latency and throughput such as the consensus protocol used and the geographical distribution of the nodes, nevertheless, these metrics are highly dependent on the chosen Hyperledger technology and the use case.

Apart from the traditional metrics, though, an important KPI for blockchain in 6G may be network security. The 6G networks have adopted the concept of security by design, to deploy virtual elements with adequate trust anchors. Nevertheless, this is far from reaching maturity, while the complexity and the growing size of such an infrastructure introduces new challenges through new threat vectors. Towards this direction, PRIVATEER has defined some metrics that can be utilised to evaluate the network's security. These are the following:

- Auditability of data on the blockchain: Auditability is a key feature for the transparency of blockchain networks in general, providing the ability to trace and verify records, thus transactions, within the decentralised ledger. The key metric here is to audit the *correctness of the transaction* and its effects on the latency. The correctness of the transaction is achieved by employing crypto primitives (i.e., signatures). These crypto mechanisms though should not affect the latency >10%.
- Representation of chain of trust: Similarly to the auditability, the representation of the *chain of trust* is a basic characteristic of distributed ledgers, to maintain transparency, by providing tamper-proof record of the history of transactions. In blockchain each transaction is cryptographically linked to the previous one (i.e., using hashes or signatures), creating a chain of blocks. This chain of blocks ensures the integrity of the transactions, while it represents the history for each actor/device/ virtual element, based on history of trust indicators on the blockchain. This metric again is considered in terms of its effects on the latency, when queuing the data. Note that this data is linked with each other due to the chain format. Consequently, the transaction representing a reading query for on-chain data should be efficient in time (in the order of ms) and should not consume more than 5% of the peer resources
- Certifiability: Processes and functionalities shall be updated in a certifiable manner. This aspect is translated to the assurance provided to the stakeholders that the blockchain follows certain standards (i.e., ISO 27001). Similarly to the auditability, the certifiability, which is achieved by employing crypto primitives, shall not introduce overhead (in the order of ms) to the network. In a quantifiable definition, they should not consume more than 5% of the peer resources.
- Secure and Privacy-preserving data sharing: Offering support to different data sharing profiles with different levels of granularity while differentiating parts of these data in terms of access (i.e., attribute-based). The ability to share data

securely, leveraging a distributed architecture is pivotal. Towards this direction, tamper-proof, verifiable records of transactions are available, while advanced encryption techniques are also employed to ensure access to data and to the blockchain for only authorised entities. In terms of quantifiable metrics, >3 *crypto primitives*, supporting the selected data sharing profiles, should be available.

- Decentralised Identity Management and Service Requirements: Provide service discovery based on the concept DIDs. The identity management is an important feature for the security of the distributed network, to ensure access to authorised entities only both to the network and to the actual data exchanged. DIDs can be employed in this direction of managing identities in distributed environments. Additionally, DIDs, combined with the notion of Verifiable Credentials (VCs) can further provide privacy protection, by employing advanced encryption techniques.
- Data portability: Each provider may support different blockchain and distributed ledger solutions. Data portability is a critical feature in the forecasted 6G environment, where multiple service or infrastructure providers may support their own distributed ledger solution. It provides the option to individuals to transfer securely their data from one solution to the other, without losing the sovereignty of their data. Therefore, this metric should ensure that the state of the data is not different from one solution to another thus double spending cannot be achieved.

2.6 Key Value Indicators (KVIs)

Trustworthiness is one of the crucial KVIs for 6G networks. Trustworthiness encompasses multiple facets, such as “security, privacy, availability, resilience, compliance with ethical frameworks” [1]. Other sources use similar descriptions, which have in common that security and privacy are considered crucial properties of trustworthy systems. A relevant aspect is how to translate and assess the trustworthiness properties of 6G systems. A potential solution is to combine several of the above-mentioned metrics into the concept of a Level of Trust (LoT) and consider it part of SLA demanded to 6G system. The LoT can be calculated as a combination of several metrics that can be monitored on different domains, through a Trust management Service [16], or the combination of them into services and offer the user assurance of the trustworthiness of the given service. The metrics can include the following: Attestation level (SW, HW), Traffic path attestation (confirmed Proof-of-Transit), Traceability (e.g., via Smart Contracts: allows conducting verifiable accounting & SLAs), Security issues related to the SDN Controller, NFVO & Slice Manager (e.g., compromised slices), AI-related and Privacy KPIs.

It should be noted that as it pertains to the trustworthiness metric, any system should be able to support the appropriate indicators of trust. One example is the case of NFV,

which enables the classification of at least 5 levels of assurance, as defined by ETSI [17]. These levels of assurance capture the required level of trust compared to the actual one of elements and actors comprising a 6G infrastructure, stemming from the infrastructure to the virtual elements and the exchanged data.

There are six distinct levels of assurance (LoA) defined by ETSI, using a number from 0-5 to represent a scale of relative trust, where a greater number denotes a higher level of trust. These are the following:

- LoA 0: denoting the complete absence of any form of integrity verification.
- LoA 1: covering the local integrity verification of the hardware and virtualization platform's (hypervisor) during boot and application loading. No proof of integrity is offered.
- LoA 2: Adding to LoA 1 the remote attestation of the hardware and virtualization platform integrity. Measurements of boot time and application load time are considered.
- LoA 3: Adding to LoA 2, LoA 3 incudes the local verification of VNF software packages as they are loaded on VNF startup.
- LoA 4: Adding to LoA 3 the remote attestation of VNF software packages.
- LoA 5: Adding to LoA 4 the remote verification of the infrastructure network set up to enable the VNF as well as the remote verification of the virtualization layer and VNF software.

Extended classification methods for LoT will be needed to cover 6G systems trustworthiness in the future to cover additional technologies depicted here.

3 Summary

The table below summarizes the KPIs proposed by the PRIVATEER consortium, related to privacy and security technologies for 6G.

Category	KPI	Description
Intrusion Detection	**Number of False Positives/Negatives**	The percentage of incorrect threat identifications by the (AI) intrusion-detection system.
	Mean Time to Detect/Classify a Threat	The average time taken by the system to detect/classify a security threat.
	Accuracy Loss (Federated Model)	The decrease in accuracy of the federated model compared to a centralized model.
Privacy Preservation of ML models & Adversarial Protection	**Success of Adversarial Privacy Attacks: Inference of Membership / Model inversion / Reconstruction**	The accuracy of inferred ML-model information (depending on the attack type)
	Accuracy Loss (Private Model)	The decrease in accuracy of the private model compared to a non-private model due to privacy mechanisms.
	Performance Loss/Overhead	The performance impact of introducing adversarial protection mechanisms, measured against metrics such as accuracy, precision, recall, and F1.

	Model Poisoning	The percentage of adversarial workers or agents that can be tolerated without significant performance degradation.
Data Anonymization & Differential Privacy	**Quality Loss**	The difference/distance between the anonymized/DP data and the original data/how much quality is lost by reporting anonymized data instead of real data
Security Orchestration	**Time to repair**	From the moment a security anomaly breach is detected (or predicted) until relevant intra- or inter-domain adaptation primitives have been triggered and completed, bringing the system back to a stable and privacy-by-default SLA-compliant state
	Time to resource preparation end-to-end	From the moment an order is expressed as intent, until all multi-party resources that comply with corresponding privacy service requirements have been discovered and provisioned
	Decision time	How fast the ML model can process input data, analyze the current network state, and make informed decisions to protect the network
Distributed Ledger	**Latency**	The time between the receipt of a request and the commitment of the transaction.
	Throughput	The total number of transactions supported by a single blockchain peer.

	Auditability of Data	The ability to trace and verify records within the decentralized ledger.
Trustworthiness	**Level of Trust (LoT)**	A composite metric calculated from several indicators (e.g., attestation levels, traffic attestation, traceability, security issues) to assess the trustworthiness of 6G services.
	Levels of Assurance (LoA)	Defined by ETSI, these levels range from 0 to 5, representing the scale of relative trust, with higher numbers denoting greater levels of trust.

References

[1] Hexa-X Consortium, “D1.2 Expanded 6G vision, use cases and societal values – including aspects of sustainability, security and spectrum,” April 2021. [Online]. Available: https://hexa-x.eu/wp-content/uploads/2022/04/Hexa-X_D1.2_Edited.pdf

[2] Hexa-X Consortium, “D1.3 Targets and requirements for 6G – initial E2E architecture,” February 2022. [Online]. Available: https://hexa-x.eu/wp-content/uploads/2022/03/Hexa-X_D1.3.pdf

[3] 5G Public Private Partnership, Test, Measurement and KPIs Validation Working Group, “White Paper: Beyond 5G/6G KPIs and Target Values,” 2022. [Online]. Available at: https://5g-ppp.eu/wp-content/uploads/2022/06/white_paper_b5g-6g-kpis-camera-ready.pdf

[4] Beyond 5G Promotion Consortium, White Paper Subcommittee, “Beyond 5G White Paper ~Message to the 2030s~,” March 2022. [Online]. Available: https://b5g.jp/w/wp-content/uploads/pdf/whitepaper_en_1-0.pdf

[5] Networld Europe, “Strategic Research and Innovation Agenda 2022, Technical Annex,” 2022. [Online]. Available at: https://bscw.5g-ppp.eu/pub/bscw.cgi/d516614/SRIA%202022%20Technical%20Annex%20Published.pdf

[6] P. Porambage, G. Gür, D. P. M. Osorio, M. Liyanage, A. Gurtov and M. Ylianttila, "The Roadmap to 6G Security and Privacy," in IEEE Open Journal of the Communications Society, vol. 2, pp. 1094-1122, 2021, doi: 10.1109/OJCOMS.2021.3078081.

[7] Jayaraman, Bargav, and David Evans. "Evaluating differentially private machine learning in practice." USENIX Security Symposium. 2019.

[8] Nasr, Milad, Reza Shokri, and Amir Houmansadr. "Comprehensive privacy analysis of deep learning: Passive and active white-box inference attacks against centralized and federated learning." 2019 IEEE symposium on security and privacy (SP). IEEE, 2019.

[9] Ateniese, Giuseppe, et al. "Hacking smart machines with smarter ones: How to extract meaningful data from machine learning classifiers." International Journal of Security and Networks 10.3 (2015): 137-150.

[10] Balle, Borja, Giovanni Cherubin, and Jamie Hayes. "Reconstructing training data with informed adversaries." 2022 IEEE Symposium on Security and Privacy (SP). IEEE, 2022.

[11] Peter Kairouz. “Federated Learning & Privacy“, given at the Summer School on Privacy-Preserving Machine Learning at ITU Copenhagen and Aarhus University (Denmark) in 2022. Slides available at: https://medialib.cmcdn.dk/medialibrary/7B031F9C-64B5-43B7-B5AC-D0DF772C7975/3743CF16-8E32-ED11-84B6-00155D0B0940.pdf

[12] INSPIRE-5gplus “D5.3 Complete 5G security testing infrastructure implementation and final results” Version: v1.0 available at: https://www.inspire-5gplus.eu/wp-content/uploads/2022/12/i5-d5.3_complete-5g-security-testing-infrastructure-implementation-and-final-results_v1.0.pdf

[13] MARSAL Consortium, "Deliverable D5.1 Initial report on decentralized framework for confidentiality and hardware-accelerated security mechanisms", 2021. Available at: https://www.marsalproject.eu/wp-content/uploads/2022/09/MARSAL_D5.1_V1.0.pdf

[14] ISO/TC 307/JWG 4 Joint Working Group. "Blockchain and distributed ledger technologies and IT Security techniques." Final Report, ISO/TC 307/JWG 4 N18, International Organization for Standardization, September 2021, https://www.iso.org/standard/76039.html.

[15] ASSURED Consortium, "Deliverable D6.2 first demonstrators implementation report, 2022. [Available] https://www.project-assured.eu/deliverables/

[16] European Telecommunications Standards Institute, “Zero-touch network and Service Management (ZSM); ZSM security aspects”, ETSI GS ZSM 014, 2024. [Available] https://www.etsi.org/deliver/etsi_gs/ZSM/001_099/014/01.01.01_60/gs_ZSM014v010101p.pdf

[17] European Telecommunications Standards Institute, "Network Functions Virtualisation (NFV); Trust; Report on Attestation Technologies and Practices for Secure Deployments ", ETSI GR NFV-SEC 007, 2017. [Available] https://www.etsi.org/deliver/etsi_gr/NFV-SEC/001_099/007/01.01.01_60/gr_nfv-sec007v010101p.pdf

Consortium

Space Hellas
www.space.gr

NCSR Demokritos
www.demokritos.gr

Telefonica I&D
www.telefonica.com

RHEA SYSTEM SA
www.rheagroup.com

INESC TEC
www.inesctec.pt

Infili Technologies PC
www.infili.com

UBITECH LTD
www.ubitech.eu

IQUADRAT R&D
www.ucm.es

ICCS
www.iccs.gr

FORSVARETS FORSKNINGSINSTITUTT
www.ffi.no

UNIVERSIDAD COMPLUTENSE DE MADRID
www.ucm.es

INSTITUTO POLITÉCNICO DO PORTO
www.ipp.pt

ERTICO ITS EUROPE
www.ertico.com

Contact Us
privateer-contact@spacemaillist.eu

Co-funded by the European Union
6GSNS

PRIVATEER has received funding from the Smart Networks and Services Joint Undertaking (SNS JU) under the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101096110