Digital Infrastructures for the Future of Space: Enhancing Security, Intelligence, and Resilience

Ulpia-Elena BOTEZATU[1,2], Cristina-Gabriela GHEORGHE[1], Sorin SOVIANY[1]
[1]National Institute for Research and Development in Informatics – ICI Bucharest, Bucharest, Romania
[2]Romanian Space Agency, Bucharest, Romania
ulpia.botezatu@ici.ro, cristina.gheorghe@ici.ro, sorin.soviany@ici.ro

Abstract: Secure satellite communications underpin the resilience of governmental missions across the European Union. This paper presents the results of the DK-PEX project (SOL-2024-20), which developed APEX, Romania's national access system to the EU GOVSATCOM programme and a stepping stone towards IRIS². We report the demand analysis of eighteen institutional user categories, the redundant and modular system architecture, its hardware and software implementation, and an evidence-based testing and validation framework built on requirement–test–evidence traceability. The results demonstrate how digital infrastructures combining virtualization, next-generation firewalls, multi-factor authentication, TEMPEST-protected processing and post-quantum readiness consolidate national participation in European secure connectivity.
Keywords: secure satellite communications, GOVSATCOM, IRIS², digital infrastructures, cybersecurity, quantum key distribution, resilience, national access system.

INTRODUCTION

During recent years, the European Union (EU) has elevated space-based secure communications to the status of a critical component of its strategic autonomy and resilience agenda. The Union Space Programme, established by Regulation (EU) 2021/696, introduced GOVSATCOM as a dedicated component whose purpose is to ensure the long-term availability of reliable, secure and cost-effective governmental satellite communications services by pooling national and commercial satellite capacities and sharing them among authorised institutional users (European Union, 2021). This "pooling and sharing" logic was subsequently extended by Regulation (EU) 2023/588, which established the Union Secure Connectivity Programme for the period 2023–

https://doi.org/10.54851/v8i2y202608

2027 and initiated IRIS² (Infrastructure for Resilience, Interconnectivity and Security by Satellite), a multi-orbital constellation to be realised through a public–private partnership between the European Commission and a concessionaire consortium, gradually absorbing the European Quantum Communication Infrastructure (EuroQCI) initiative for quantum key distribution (European Union, 2023; European Commission, 2024). In parallel, EuroQCI is being developed with the European Space Agency to integrate quantum key distribution (QKD) over terrestrial fiber and space links, reinforcing the cybersecurity of governmental networks against both classical and quantum-enabled adversaries (European Commission, 2025; The European Space Agency, 2025). According to the planning documented during the project, the initial operational capability of GOVSATCOM was foreseen for the end of 2025, while that of IRIS² is currently foreseen for the end of 2030.

The relevance of these programmes is not merely institutional. The EU Agency for the Space Programme (EUSPA) estimates that the use of satellite communications supporting crisis management, surveillance and key infrastructure in the EU will grow by a factor of fourteen between 2025 and 2040, reaching approximately 186 Gbps of fixed satellite service demand by 2040 (European Union Agency for the Space Programme, 2023). At the same time, the emergence of quantum computing threatens the asymmetric cryptographic primitives on which current secure communications rely, a risk crystallised in the "harvest now, decrypt later" scenario highlighted by the United States National Institute of Standards and Technology in its post-quantum migration guidance (National Institute of Standards and Technology, 2024c). Secure satellite communications must therefore be conceived as layered digital infrastructures in which network security, identity management, cryptographic agility and physical resilience are engineered jointly rather than sequentially. This emphasis on resilient and coordinated security architectures is consistent with the analysis by Petcu and Barbu (2022), who situate Romania's cybersecurity policy within evolving geopolitical risks, critical-infrastructure vulnerabilities and European security priorities.

In this context, Romania launched in 2024 the project "*Development of the 'pooling and sharing' participation capacity in EU programmes for secure satellite communications*" (DK-PEX), funded under the National Plan for Research, Development and Innovation PNCDI IV (UEFISCDI, 2024; ICI-Bucharest, 2024). The general objective of DK-PEX is to increase Romania's capacity to participate in the European programmes for secure satellite communications by strengthening national components and creating a system architecture that ensures the continuity of national activities and the transition to Secure Connectivity. Its specific goals encompass the analysis and evaluation of Romania's existing components for secure satellite communications, the improvement of national capabilities, the design of a national architecture integrating domestic infrastructure with EU assets (GOVSATCOM, EuroQCI and the planned European constellation), and the testing and validation of a national secure-communications access system built on these components.

The central technical result of the project is APEX (*Acces la Programele Europene de Comunicații Satelitare Securizate/Access to the European Secure Satellite Communications Programmes*), the national system through which authorised Romanian institutions request, obtain and use access to GOVSATCOM services in a controlled, traceable and secure manner. This paper consolidates the project's findings across its analytical, architectural, implementation and validation phases. It extends a simplified version presented at

the International Astronautical Congress (IAC) 2025 by incorporating the evidence-based validation methodology developed within DK-PEX. The remainder of the paper is organised as follows. The section entitled *Secure satellite communications as a layered digital infrastructure* synthesises the technological and programmatic background. The *Methods* section describes the research and engineering methodology. The *Discussion* section presents the results across four dimensions: user requirements, system architecture, implementation, and testing and validation. The *Conclusions* section discusses the implications, limitations, and future directions, and concludes the paper.

SECURE SATELLITE COMMUNICATIONS AS A LAYERED DIGITAL INFRASTRUCTURE

The project's state-of-the-art analysis documented a profound transformation of the satellite communications sector, driven by new market entrants and the emergence of multi-orbital constellations serving fixed, mobile, aeronautical and maritime applications. In the space segment, the most consequential trends identified were the growth of throughput via frequency reuse in multiple spot beams, which moved satellites from a few Gbps to tens or hundreds of Gbps; the rapid deployment of non-geostationary (NGSO) constellations, expected to represent roughly seventy percent of satellite demand by unit count over the next decade and exemplified by Starlink, OneWeb and the Chinese Guowang filing for 30,000 satellites; the advent of fully software-defined satellites whose coverage, power and frequency plans can be reconfigured in orbit; the adoption of higher frequency bands (Ka for user links, Q/V for feeder links); and the introduction of optical communications, including optical inter-satellite links and direct-to-Earth laser links, which combine very high data rates with improved interception resistance.

In the ground segment, the analysis emphasised the convergence between satellite and fifth-generation (5G) terrestrial networks. Multi-orbit and multi-band user terminals enable seamless handover between GEO and NGSO systems; the DVB-S2X standard currently dominates commercial links while 5G non-terrestrial network (NTN) protocols are expected to become a second major standard; virtualization allows ground infrastructure to scale with constellation capacity; and network slicing offers the ability to prioritise crisis-communications traffic over dispensable flows—a capability of direct relevance for governmental users. The same analysis warned that cyber threats increasingly target the space industry across both segments, and that quantum technologies simultaneously create opportunities (QKD) and threats (cryptanalysis) for the current generation of communications security. More broadly, Barbu (2019) examines scalable Big Data processing and analytics approaches, offering a conceptual reference for assessing future information-management and monitoring requirements in data-intensive satellite ground infrastructures.

Much of today's widely deployed public-key cryptography—including RSA, Diffie–Hellman and elliptic-curve schemes—relies on the computational difficulty of integer factorisation or discrete logarithm problems. A cryptographically relevant, fault-tolerant quantum computer could solve these problems efficiently using Shor's algorithm or closely related variants. Two complementary approaches are central to the European response. The first is infrastructure-based: EuroQCI is designed to combine a terrestrial component (TerrQCI), using new and existing fibre-optic networks to connect strategic sites within and across Member States, with a space component (SpaceQCI), comprising quantum-communications satellites and associated ground infrastructure. According to the proposed architecture, the latter

includes satellite and mission control centres, a security operations centre and SpaceQCI access nodes, while a Quantum Hub coordinates service requests and resource allocation. The first EuroQCI services will be based on quantum key distribution (QKD), which uses quantum-mechanical properties to enable two endpoints to establish shared secret key material. Attempts to eavesdrop on the quantum channel introduce disturbances that can be detected under the protocol's security assumptions. In present-generation multi-hop QKD networks, each quantum link establishes key material only between directly connected nodes; consequently, end-to-end key relay depends on intermediate "trusted nodes", whose security and accreditation constitute central design requirements for EuroQCI.

The second path is algorithmic. In August 2024, NIST finalised the first post-quantum cryptography standards: FIPS 203 for key encapsulation and FIPS 204 for digital signatures (National Institute of Standards and Technology, 2024a; 2024b). Symmetric cryptography such as AES remains largely unaffected by the quantum threat, so the migration effort concentrates on replacing RSA, Diffie–Hellman and elliptic-curve primitives in key exchange and authentication. The DK-PEX conceptual analysis accordingly framed the national secure-communications system as a layered architecture—access, transport, processing and storage, control and security, management and monitoring—governed by Zero Trust principles and designed for cryptographic agility, so that both QKD-derived keys and post-quantum algorithms can be introduced without re-architecting the system.

Technologically, Romania has developed the Romanian National Quantum Communication Infrastructure, aimed to build the country's first quantum communications network of interconnected nodes using quantum devices, as the national segment of EuroQCI (RoNaQCI, 2025). The infrastructure comprises a unified national backbone and six metropolitan QKD networks connecting institutional nodes through quantum and classical security technologies (RoNaQCI, 2025). Prior work examined the simulation of point-to-point QKD links for cybersecurity applications, establishing the analytical basis for estimating expected performance and setting feasible performance targets for QKD-enabled security applications (Soviany, Gheorghe & Gheorghe-Moisii, 2024; Botezatu, 2023). At the institutional and operational level, however, a separate gap remained: the need for a national mechanism capable of facilitating and coordinating eligible Romanian institutions' access to European secure satellite communications programmes. DK-PEX addresses this need through the development of APEX, the national platform designed to support access to those programmes. The development of this national access and coordination layer constitutes the contribution reported here.

Publicly available national arrangements indicate that the common EU GOVSATCOM competent-authority model is being implemented through different institutional configurations. In Sweden, the national Competent GOVSATCOM Authority function is assigned to the Civil Defence Agency (*Myndigheten för civilt försvar*), which coordinates the national implementation of GOVSATCOM and the process through which eligible Swedish users obtain access to EU secure satellite communication services (Myndigheten för civilt försvar, 2025). In Czechia, the National Cyber and Information Security Agency (NÚKIB) performs the competent-authority function for GOVSATCOM and secure connectivity, in cooperation with the National Security Authority, the Ministry of Transport, the national telecommunications regulator and the Armed Forces (NÚKIB, n.d.). Poland illustrates a more distributed

institutional-development approach, in which the Polish Space Agency (POLSA) and the Office of Electronic Communications (UKE) have supported the Ministry of the Interior and Administration in establishing the national Competent GOVSATCOM Authority (POLSA, 2024). These examples illustrate that, while the EU regulatory framework establishes a common set of functions concerning user authorisation, access management and security compliance, Member States retain discretion regarding the institutional location and supporting arrangements of the competent authority. Against this background, the specificity of APEX lies not in creating a separate governance model, but in operationalising Romania's national implementation through a dedicated access and coordination layer integrating institutional onboarding, request validation, access control, traceability and interaction with the GOVSATCOM service layer.

For clarity, QKD and post-quantum cryptography are treated in this paper as forward-looking architectural reference points for cryptographic agility and future migration, rather than as capabilities implemented or experimentally validated within APEX.

METHODS

The project employed a structured, multi-phase engineering methodology in which each phase produced auditable deliverables that conditioned the next.

The first phase comprised a comprehensive analysis of the current technological state and of the existing national capabilities and needs. The consortium reviewed the EU programmatic and technological baseline—GOVSATCOM user requirements, the IRIS² regulation, the EuroQCI architecture and EUSPA's market and technology assessments—and catalogued the methods, technologies and elements available for secure communications in Romania. A central instrument of this phase was a structured user-needs survey. Eighteen categories of potential governmental and institutional users of secure satellite communications were identified across six mission domains (border surveillance and external action, the maritime community, police missions, civil protection and public health, environmental monitoring, and critical infrastructure monitoring), and a thirty-two-item questionnaire covering current usage, mission types, coverage, environmental constraints, security expectations, frequency bands, data rates and cost criteria was administered; thirteen institutions responded. In parallel, the applicable regulatory corpus for classified information protection was synthesised at national level (Romanian Law No. 182/2002, Romanian Government Decision No. 585/2002, and Romanian Government Decision No. 353/2002), at EU level (Council Decision 2013/488/EU, Commission Decision (EU, Euratom) 2015/444, Regulation (EU) 2023/588) and at NATO level, together with the derived INFOSEC, COMSEC and TEMPEST requirements. A complementary conceptual study established the cryptographic foundations of the system, reviewing symmetric and asymmetric primitives, their post-quantum limitations and migration strategies.

The second phase translated these requirements into an integrated architectural design for the national access system, APEX. The architecture was specified around two principles stated in the project proposal: redundant and secure communications between the entities of interest, and distributed application logic. The design documentation covered network topology, the security perimeter, identity and access management, the handling of GOVSATCOM credentials, the classified-information processing chain and the environmental support infrastructure, and it explicitly

reserved interfaces for future EuroQCI/RoNaQCI quantum key distribution and for IRIS² services.

The third phase comprised implementation, testing and validation. Hardware was procured in accordance with specifications derived from the system architecture, while the software platform was developed and configured. A testing and validation methodology was also established, covering the system's functionality, performance, security, availability and interoperability.

A distinguishing methodological feature was the rigorous evidentiary framework applied throughout the validation process. Each test case was linked to a source requirement through a requirement–test–evidence traceability matrix, and test verdicts were limited to "PASSED", "FAILED", "BLOCKED" and "NOT APPLICABLE". A "PASSED" verdict could be assigned only when the expected result was expressed in objectively verifiable terms and supported by appropriate technical evidence. The configuration baseline was frozen and documented before each test campaign. Test evidence was limited to what was necessary and anonymised or redacted where appropriate, with passwords, one-time password secrets, cryptographic keys and authentication tokens expressly excluded.

Nonconformities were classified as critical, major or minor, and any unresolved critical nonconformity precluded a finding of operational readiness. Finally, the findings and technical specifications were consolidated into the final technical documentation for the national system. This documentation explicitly distinguished among components that had been procured and installed, functions that had been configured and validated through technical evidence, functions that had been designed but not yet validated, and potential areas for further development, including integration with IRIS², quantum key distribution, post-quantum cryptography and advanced anomaly-detection capabilities.

Throughout these phases, coordination with Romanian stakeholders and EU structures ensured alignment: the architecture was developed against the GOVSATCOM Hub concept operated by EUSPA, the survey engaged the national user community in line with EUSPA's user-network model, and the interoperability constraints of the European platform—including IP-address-based access restriction and manual credential provisioning—were incorporated as design inputs.

User requirements for secure satellite communications in Romania

The user-needs survey provides an aggregated view of demand among 13 respondents. All considered a permanent national satellite communications service useful. Eleven reported prior use of satellite communications, whereas twelve reported no prior benefit from services provided through EU agencies. The most frequently reported requirements included operation under adverse environmental conditions (13/13), field-to-base connectivity (12/13), emergency-response applications (8/13), national coverage (8/13) and permanent availability (8/13). Cost was the leading procurement criterion for all respondents, while capacity and robustness were identified as relevant criteria by twelve and seven respondents, respectively (Agenția Spațială Română et al., 2025d).

These findings indicate demand within the surveyed group for accessible and resilient satellite connectivity. Given the small and targeted sample, however, they should not be interpreted as representative of all Romanian public institutions or as evidence that no national or European access mechanisms previously existed.

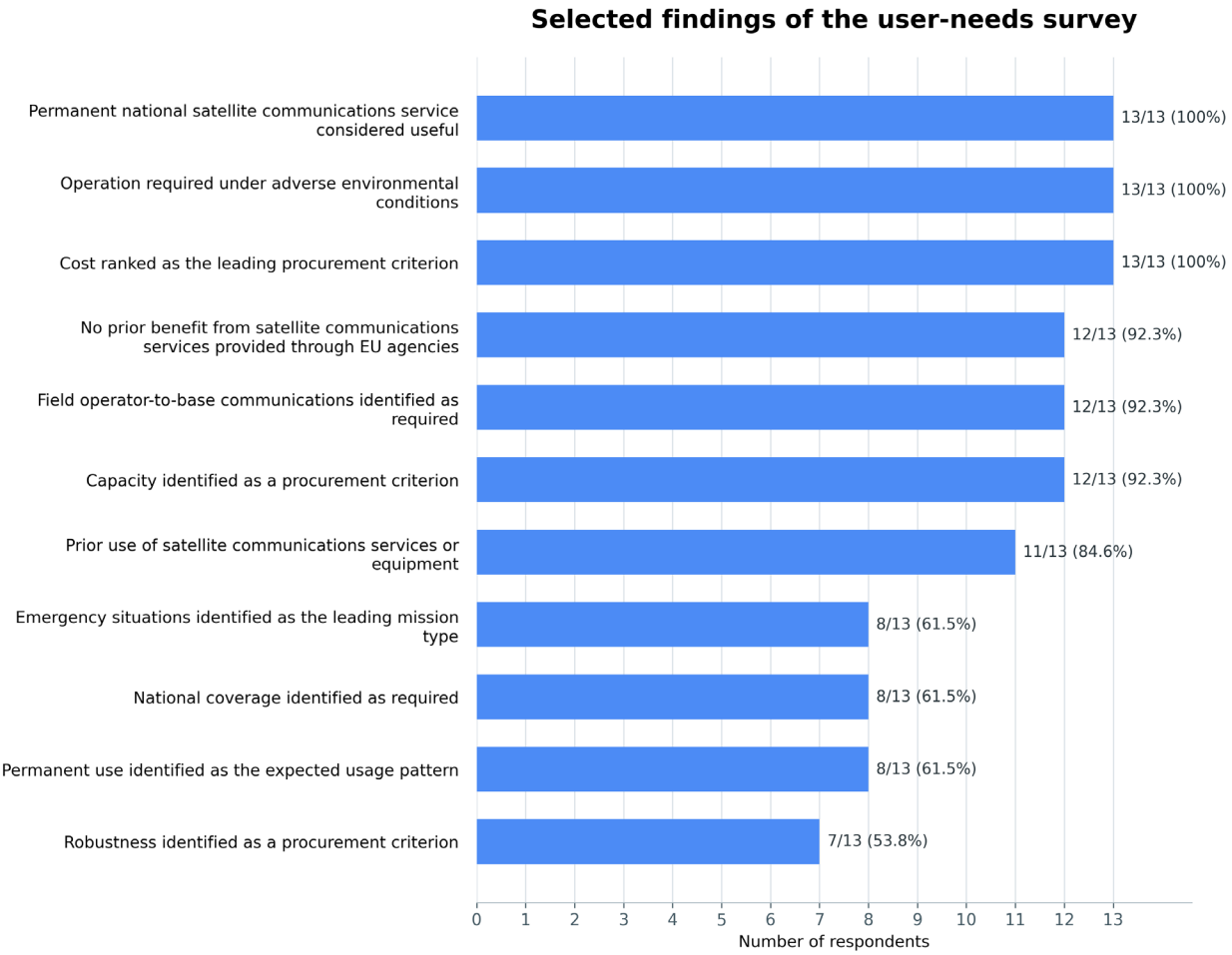


Figure 1. *Selected aggregated findings of the DK-PEX user-needs survey (n = 13 respondents).*
Source: authors' elaboration Agenția Spațială Română et al. (2025d)

The APEX system

Within DK-PEX, APEX is conceived as a national access and coordination layer for authorised Romanian users of EU GOVSATCOM services, rather than as a system that creates or allocates satellite capacity. Its role can be described functionally as receiving and validating service requests, applying access controls, maintaining traceability and interfacing with the European GOVSATCOM service layer. Service matching and resource allocation remain functions of the GOVSATCOM Hub under Union procedures (Agenția Spațială Română et al., 2026b; European Commission, 2023).

This division is consistent with Regulation (EU) 2021/696, under which each GOVSATCOM participant designates a competent authority, and with Commission Implementing Decision (EU) 2023/1054, which places that authority between authorised users and the GOVSATCOM Hub. At a conceptual level, the architecture therefore comprises three domains: authorised national users, the national access layer and the Union GOVSATCOM service layer.

The stated design objectives include controlled access, traceability, separation of responsibilities and service continuity

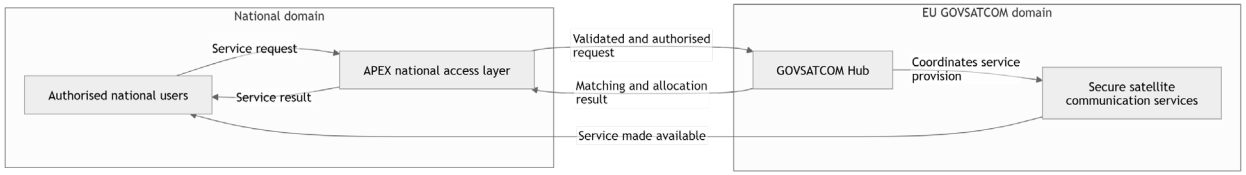


Figure 2. *Public, functional representation of the APEX national access layer. The arrows represent institutional functions and service-request processing, not physical network connections.*
Source: authors' elaboration based on Regulation (EU) 2021/696, Commission Implementing Decision (EU) 2023/1054 and Agenția Spațială Română et al. (2025c; 2026b)

(Agenția Spațială Română et al., 2025c; 2026b). Detailed topology, security controls, communications arrangements and procedures for handling classified information are intentionally excluded from this public description. QKD, post-quantum cryptography, IRIS² interoperability and AI-supported functions should be presented only as potential evolution paths unless their implementation and validation have been formally documented. NIST's ML-KEM and ML-DSA standards provide relevant reference points for future cryptographic migration but do not establish their current implementation within APEX (National Institute of Standards and Technology, 2024a; 2024b).

Implementation: procured infrastructure and the national software platform

During the third stage of DK-PEX, technical infrastructure was procured and a national software platform was developed to implement the APEX access-layer concept. For public reporting purposes, the infrastructure can be described by function rather than by manufacturer or configuration: protected connectivity and access management, computing and data hosting, operational continuity, and system administration (Agenția Spațială Română et al., 2026b).

The software platform supports institutional onboarding, role-based administration and the national service-request lifecycle, including request submission, verification and consultation of approved service information. Documented security controls address authentication, authorisation, auditability and credential lifecycle management. The platform supports the intermediary role of the national competent authority, while service matching and resource allocation remain functions of the GOVSATCOM Hub under Union procedures (European Commission, 2023).

Public documentation should distinguish clearly between infrastructure that has

Table 1. *Functional components of the APEX implementation*
Source: authors' elaboration based on Agenția Spațială Română et al. (2026b)

Implementation domain	Public description
Protected connectivity and access management	Supports controlled interaction between authorised institutions, the national access layer and the European service interface.
Computing and data services	Hosts the application, data-management and administrative functions of the national platform.
Operational continuity	Provides the technical basis for service availability, recovery and continuity.
National software platform	Supports institutional onboarding, role administration and processing of service requests.
Security governance	Applies documented requirements for authentication, authorisation, auditability and credential lifecycle management.

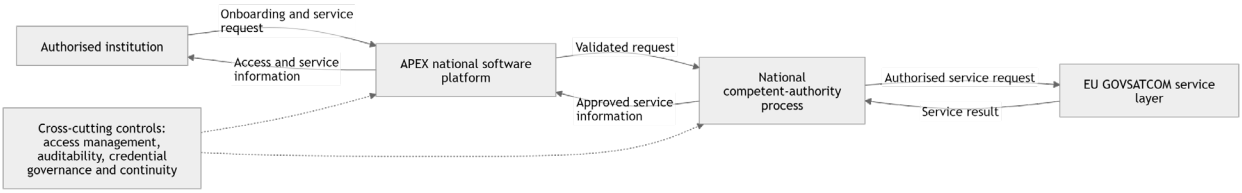


Figure 3. *Public functional representation of the implemented national access platform.*
Source: authors' elaboration based on Agenția Spațială Română et al. (2025c; 2026b)

been procured and installed, software functions that have been implemented and validated, and functions that remain dependent on the evolving European service interface. Equipment inventories, network configurations, protective measures, credential-handling procedures and arrangements for classified information are outside the scope of this public description. As a prospective security enhancement, adaptive threat intelligence could draw on the work of Rotună, Sacală and Alexandru (2025), who combine registry, DNS and TLS-related features for machine-learning-based .ro domain reputation assessment; no such capability is claimed as implemented or validated within APEX.

Testing and validation: an evidence-based framework

DK-PEX approached validation as an evidence-based and scope-limited assessment rather than as a binary claim concerning the system as a whole. Each test case was linked to a source requirement through a requirement–test–evidence traceability matrix and executed against a documented configuration baseline. Changes introduced during a test campaign were recorded, and the affected tests were reassessed. Verdicts were limited to "PASSED", "FAILED", "BLOCKED" and "NOT APPLICABLE", with a "PASSED" result requiring objective acceptance criteria and appropriate technical evidence (Agenția Spațială Română et al., 2026a).

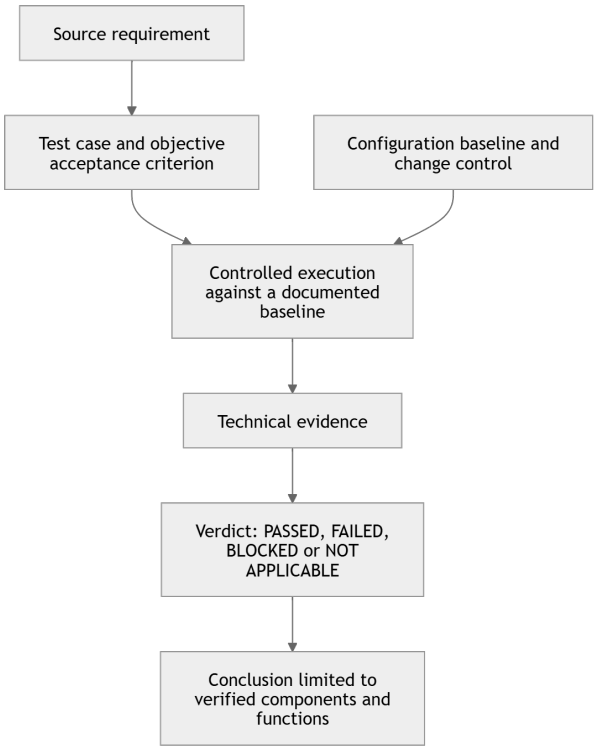


Figure 4. *Evidence-based validation chain used for public methodological reporting*
Source: authors' elaboration based on Agenția Spațială Română et al. (2025c; 2026b)

Testing addressed five broad areas: functionality, performance, security, availability and recovery, and interoperability. Security and end-to-end tests were conducted only within authorised and controlled environments and were expressly non-intrusive. Detailed configurations, test thresholds, security scenarios and technical evidence are excluded from this public description.

A central methodological distinction was maintained between simulated and externally executed tests. A successful simulation demonstrates only the internal functions and flows reproduced in that environment; it does not establish operational integration with an external European system. Validation conclusions were therefore limited to the components and functions that had been configured, tested and supported by evidence. Blocked, simulated or unexecuted capabilities were not treated as operationally validated, and detailed results and remediation records remained within the dedicated project documentation (Agenția Spațială Română et al., 2026a; 2026b).

DISCUSSION

The results illustrate how a targeted national research project can translate identified institutional demand into a structured access-layer concept and an evidence base for future participation in European secure satellite communication services. All 13 survey respondents considered a permanent national satellite communications service useful, while 12 reported no prior benefit from satellite communications services provided through EU agencies (Agenția Spațială Română et al., 2025d). Given the size and targeted composition of the sample, these findings demonstrate demand within the surveyed group but cannot be interpreted as a representative assessment of all Romanian public institutions or as proof of a nationwide access gap.

Against this background, the principal contribution of DK-PEX is the combination of three elements: an assessment of institutional requirements, the development of APEX as a national access-layer concept, and an evidence-based framework for testing and documenting the resulting system. APEX supports national functions associated with request handling, validation, access control and traceability, while service matching and satellite-resource allocation remain functions of the GOVSATCOM Hub. This division is consistent with Regulation (EU) 2021/696 and Commission Implementing Decision (EU) 2023/1054, which place competent national authorities between authorised users and the European service infrastructure.

This functional alignment is relevant in the evolving European context. GOVSATCOM Hub initial operations began in January 2026, using pooled governmental satellite capacity, while services associated with IRIS² are expected to become available from 2029 onwards (European Union Agency for the Space Programme, 2026). APEX may provide a national basis for adapting to this evolving service environment. The project results do not, however, demonstrate current integration with IRIS² or guarantee compatibility with interfaces and service arrangements that have not yet been finalised.

The treatment of quantum and post-quantum technologies must be interpreted with similar caution. QKD was not experimentally validated within DK-PEX, and the project does not demonstrate operational deployment of post-quantum algorithms. Compatibility with RoNaQCI, EuroQCI and future quantum-secure services therefore remains a prospective development path. The publication of ML-KEM and ML-DSA by NIST in 2024 provides a relevant reference point for future cryptographic migration, but it does not establish their implementation within APEX (National Institute of Standards and Technology, 2024a; 2024b). The project contribution in this area is consequently best understood as architectural planning for future cryptographic adaptability rather than as a demonstrated quantum-secure capability.

The validation results are also necessarily bounded. Simulated end-to-end testing can demonstrate the internal APEX workflow reproduced within the test environment but cannot establish operational integration with the external GOVSATCOM infrastructure. Such a conclusion requires authorised testing

against the relevant European environment. More generally, validation claims apply only to components and functions that were configured, executed and supported by technical evidence. Functions that were simulated, blocked, not executed or retained as future design options cannot be reported as operationally validated (Agenția Spațială Română et al., 2026a; 2026b).

The most transferable outcome of DK-PEX may therefore be methodological. Its documentation model links institutional requirements, technical specifications, test cases, evidence and bounded validation conclusions, while distinguishing among procured infrastructure, implemented functions, validated capabilities and prospective developments. This approach can support national coordination and future engagement with European services without overstating the maturity of the underlying system. Broader effects—such as reduced institutional compliance costs, enhanced national resilience or a contribution to collective European capacity—should be presented as anticipated impacts requiring subsequent operational evidence, rather than as results already demonstrated by the project.

CONCLUSIONS

This paper has presented the principal results of DK-PEX (SOL-2024-20), a national research and development project intended to strengthen Romania's capacity to engage with European programmes for secure satellite communications under the pooling-and-sharing model. The project combined an assessment of the technological and regulatory context, an analysis of institutional user requirements, the development of APEX as a national access layer, the implementation of supporting technical and software infrastructure, and an evidence-based testing and validation framework.

The user-needs survey identified clear demand within the targeted group. All 13 respondents considered a permanent national satellite communications service useful, while 12 reported no prior benefit from satellite communications services provided through EU agencies (Agenția Spațială Română et al., 2025d). These findings describe the surveyed institutions and should not be generalised to the entire Romanian public sector.

APEX addresses the national functions required for structured interaction with EU GOVSATCOM services, including institutional onboarding, request validation, access control, traceability and service coordination. It does not allocate satellite capacity or control European service-provision decisions, which remain within the EU GOVSATCOM framework. At the public level, its implementation can therefore be described as a combination of functional infrastructure and a national software platform supporting controlled access, request management, auditability and service continuity (Agenția Spațială Română et al., 2025c; 2026b).

The most transferable project outcome is its evidence-based validation methodology. By linking requirements, test cases, evidence and verdicts, the framework limits validation conclusions to functions that were configured, tested and technically demonstrated. It also distinguishes internal simulation from operational integration with an authorised external environment, thereby preventing simulated, blocked or prospective capabilities from being presented as operational results (Agenția Spațială Română et al., 2026a; 2026b).

Compatibility with QKD infrastructures, migration to post-quantum cryptography and future interaction with RoNaQCI, EuroQCI and IRIS² remain possible evolution paths rather than validated project outcomes. NIST's ML-KEM and ML-DSA standards provide relevant reference points for future cryptographic migration but do not establish their present implementation within APEX (National Institute of Standards and Technology, 2024a; 2024b).

GOVSATCOM Hub initial operations began in January 2026, while IRIS² services are currently

expected from 2029 onwards (European Union Agency for the Space Programme, 2026). In this evolving context, DK-PEX provides a documented basis for further authorised testing, institutional coordination and adaptation to future European service interfaces. It should therefore be understood as a structured step towards Romania's participation in the European secure-connectivity ecosystem, rather than as the completion of a fully operational national capability. Any wider contribution to national resilience, European strategic autonomy or collective secure-communications capacity remains an anticipated impact that will require subsequent operational evidence.

ACKNOWLEDGEMENTS

This work was supported by the project SOL-2024-20 (DK-PEX), "Development of the 'pooling and sharing' participation capacity in EU programmes for secure satellite communications", funded under PNCDI IV and coordinated by the Romanian Space Agency, with the National University of Science and Technology POLITEHNICA Bucharest, RARTEL S.A., ICI Bucharest, the Institute of Space Science (ISS–INFLPR), the Military Technical Academy "Ferdinand I" and IFIN-HH as consortium partners. A simplified version of this work was presented at the International Astronautical Congress (IAC) 2025.

REFERENCE LIST

Agenția Spațială Română, Universitatea Națională de Știință și Tehnologie POLITEHNICA București, RARTEL S.A., Institutul Național de Cercetare-Dezvoltare în Informatică – ICI București & Institutul Național de Cercetare-Dezvoltare pentru Fizică și Inginerie Nucleară "Horia Hulubei" (2025a) LVB I.1 – Raport privind stadiul actual de dezvoltare tehnologică și a sistemelor relevante existente. Project DK-PEX (SOL-2024-20) deliverable. Bucharest, Romanian Space Agency, internal document.

Agenția Spațială Română et al. (2025b) LVB I.3 – Raport privind metodele/echipamentele/sistemele/tehnologiile/mijloacele și conceptele destinate comunicațiilor securizate. Project DK-PEX (SOL-2024-20) deliverable. Bucharest, Romanian Space Agency, internal document.

Agenția Spațială Română, Universitatea Națională de Știință și Tehnologie POLITEHNICA București, Institutul Național de Cercetare-Dezvoltare în Informatică – ICI București & Institutul de Științe Spațiale – Filiala INFLPR (2025c) LVB II.2 – Raport tehnic privind arhitectura sistemului de comunicații securizate. Project DK-PEX (SOL-2024-20) deliverable. Bucharest, Romanian Space Agency, internal document.

Agenția Spațială Română, Universitatea Națională de Știință și Tehnologie POLITEHNICA București, RARTEL S.A. & Academia Tehnică Militară "Ferdinand I" (2025d) LVB I.2 – Raport privind metodele/tehnologiile/elementele destinate comunicațiilor securizate în România. Project DK-PEX (SOL-2024-20) deliverable. Bucharest, Romanian Space Agency, internal document.

Agenția Spațială Română et al. (2026a) LVB III.1 – Documentație tehnică referitoare la testarea/validarea funcțională a sistemului național bazat pe infrastructurile existente. Project DK-PEX (SOL-2024-20) deliverable. Bucharest, Romanian Space Agency, internal document.

Agenția Spațială Română et al. (2026b) LVB III.3 – Documentația tehnică definitivată a sistemului național destinat comunicațiilor securizate. Project DK-PEX (SOL-2024-20) deliverable. Bucharest, Romanian Space Agency.

American National Institute of Standards and Technology (2024a) FIPS 203: Module-Lattice-Based Key-Encapsulation mechanism standard. Gaithersburg, NIST. [Online] Available at: https://doi.org/10.6028/NIST.FIPS.203. [Accessed: 22nd July 2026].

Barbu, D.-C. (2019) 'Big Data Processing Solutions', Romanian Journal of Information Technology and Automatic Control, 29(2), pp. 35–48. Available at: https://doi.org/10.33436/v29i2y201903 [Accessed: 19 October 2026].

Ulpia-Elena BOTEZATU, "Attempted Cyber Security of Systems and Operations in Outer Space: an Overview of Space-

based Vulnerabilities", Romanian Cyber Security Journal, ISSN 2668-6430, vol. 5(1), pp. 67-76, 2023. https://doi.org/10.54851/v5i1y202306

Council of the European Union (2013) 'Council Decision 2013/488/EU of 23 September 2013 on the security rules for protecting EU classified information', Official Journal of the European Union, L 274, 15 October, pp. 1–50. Available at: https://eur-lex.europa.eu/eli/dec/2013/488/oj/eng [Accessed: 24 July 2026].

Council of the European Union (2022) Council and European Parliament agree on boosting secure communications with a new satellite system. [Online] Available at: https://www.consilium.europa.eu/en/press/press-releases/2022/11/17/council-and-european-parliament-agree-on-boosting-secure-communications-with-a-new-satellite-system/ [Accessed: 22nd July 2026].

European Commission (2015) 'Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information', Official Journal of the European Union, L 72, 17 March, pp. 53–88. Available at: https://eur-lex.europa.eu/eli/dec/2015/444/oj/eng [Accessed: 24 July 2026].

European Commission (2024) IRIS²: the new EU secure satellite constellation – Infrastructure for Resilience, Interconnectivity and Security by Satellite. [Online] Available at: https://defence-industry-space.ec.europa.eu/eu-space/iris2-secure-connectivity_en [Accessed: 22nd July 2026].

European Commission (2025) European Quantum Communication Infrastructure – EuroQCI. [Online] Available at: https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci [Accessed: 22nd July 2026].

European Commission (n.d.) GOVSATCOM | Satellite Communications. [Online] Available at: https://defence-industry-space.ec.europa.eu/eu-space/govsatcom-satellite-communications_en [Accessed: 28th August 2025].

European Union (2021) Regulation (EU) 2021/696 of the European Parliament and of the Council of 28 April 2021 establishing the Union Space Programme and the European Union Agency for the Space Programme. Official Journal of the European Union. L 170, 12.5.2021, 69–148. [Online] Available at: https://eur-lex.europa.eu/eli/reg/2021/696/oj/eng [Accessed: 22nd July 2026].

European Union (2023) Regulation (EU) 2023/588 of the European Parliament and of the Council of 15 March 2023 establishing the Union Secure Connectivity Programme for the period 2023–2027. Official Journal of the European Union. L 79, 17.3.2023, 1–39. [Online] Available at: https://eur-lex.europa.eu/eli/reg/2023/588/oj/eng [Accessed: 22nd July 2026].

European Union Agency for the Space Programme (2023) EUSPA Secure SATCOM: Market and User Technology Report. Luxembourg: Publications Office of the European Union [Online] Available at: https://www.euspa.europa.eu/sites/default/files/external/publications/euspa_secure_satcom_report_2023.pdf [Accessed: 22nd July 2026].

European Union Agency for the Space Programme (2025) GOVSATCOM. [Online] Available at: https://www.euspa.europa.eu/eu-space-programme/secure-satcom/govsatcom [Accessed: 22nd July 2026].

European Union Agency for the Space Programme (2026) 'Cyprus completes first operational use of EU GOVSATCOM Hub services, marking a major milestone in European secure connectivity', 10 March. Available at: EUSPA [Accessed: 24 July 2026].

Institutul Național de Cercetare-Dezvoltare în Informatică – ICI București (2025) SOL-2024-20 – Development of the "pooling and sharing" participation capacity in EU programs for secure satellite communications (DK-PEK). [Online] Available at: https://ici.ro/en/current-projects/national-plan-for-research-development-and-innovation-pncdi-IV/sol-2024-20-development-of-the-pooling-and-sharing-participation-capacity-in-eu-programs-for-secure-satellite-communications-dk-pek/ [Accessed: 22nd July 2026].

Ministry of Research, Innovation and Digitalization, The Executive Unit for Financing Higher Education, Research, Development and Innovation (UEFISCDI), (2024) [Online] Available at: https://uefiscdi.gov.ro/sol-2023-dezvoltarea-capacitatii-de-participare-pooling-and-sharing-la-programele-ue-privind-comunicatii-stelitare-sigure [Accessed: 22nd July 2026].

Myndigheten för civilt försvar (2025) *Säker och robust satellitkommunikation*. Available at: https://www.mcf.se/sv/amnesomraden/beredskap-for-kris-och-krig/beredskap-for-aktorer/rymdsakerhet/eus-rymdprogram/saker-och-robust-satellitkommunikation/ [Accessed: 22 July 2026].

National Cyber and Information Security Agency (NÚKIB) (n.d.) GOVSATCOM, Příslušný orgán GOVSATCOM (CGA). Available at: https://nukib.gov.cz/cs/galileo-prs/govsatcom-prislusny-organ-govsatcom-cga/ [Accessed: 22 July 2026].

National Institute of Standards and Technology (2024b) FIPS 204: Module-lattice-based digital signature standard. Gaithersburg, NIST. [Online] Available at: https://doi.org/10.6028/NIST.FIPS.204. [Accessed: 22nd July 2026].

National Institute of Standards and Technology (2024c) NIST IR 8547: Transition to post-quantum cryptography standards (initial public draft). Gaithersburg, NIST. [Online] Available at: https://doi.org/10.6028/NIST.IR.8547.ipd. [Accessed: 22nd July 2026].

Petcu, I. & Barbu, D.-C. (2022) 'The New Challenges of Romania's Cyber Security Policy', Romanian Cyber Security Journal, 4(1), pp. 57–67. Available at: https://doi.org/10.54851/v4i1y202207 [Accessed: 19 October 2026].

Polish Space Agency (POLSA) (2024) POLSA podpisała porozumienie z UKE. 7 May. Available at: https://polsa.gov.pl/wydarzenia/polsa-podpisala-porozumienie-z-uke/ [Accessed: 22 July 2026].

Romania (2002) Law No. 182 of 12 April 2002 on the protection of classified information [Legea nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate]. Monitorul Oficial al României, Part I, No. 248, 12 April. Available at: https://legislatie.just.ro/Public/DetaliiDocument/35209 [Accessed: 24 July 2026].

Romania (2002a) Government Decision No. 585 of 13 June 2002 approving the National Standards for the Protection of Classified Information in Romania [Hotărârea Guvernului nr. 585 din 13 iunie 2002 pentru aprobarea Standardelor naționale de protecție a informațiilor clasificate în România]. Monitorul Oficial al României, Part I, No. 485, 5 July. Available at: https://legislatie.just.ro/Public/DetaliiDocument/37319 [Accessed: 24 July 2026].

Romania (2002b) Government Decision No. 353 of 15 April 2002 approving the Rules on the Protection of Classified Information of the North Atlantic Treaty Organization in Romania [Hotărârea Guvernului nr. 353 din 15 aprilie 2002 pentru aprobarea Normelor privind protecția informațiilor clasificate ale Organizației Tratatului Atlanticului de Nord în România]. Monitorul Oficial al României, Part I, No. 315, 13 May. Available at: https://legislatie.just.ro/Public/DetaliiDocument/35977 [Accessed: 24 July 2026].

RoNaQCI (2025) About RoNaQCI. [Online] Available at: https://www.ronaqci.upb.ro/about-ronaqci [Accessed: 22nd July 2026].

Rotună, C. I., Sacală, I. Ș. & Alexandru, A. (2025) 'Towards Proactive Domain Name Security: An Adaptive System for .ro domains Reputation Analysis', Future Internet, 17(10), article 478. Available at: https://doi.org/10.3390/fi17100478 [Accessed: 19 October 2026].

Soviany, S., Gheorghe, C.–G. & Gheorghe-Moisii M. (2024) Quantum Networks and Cyber Security. A Simulation Case Study for Point-to-Point QKD Links. Romanian Cyber Security Journal. 6(2), 27-43. https://doi.org/10.54851/v6i2y202403.

The European Space Agency (2025) ESA and European Commission to build quantum-secure space communications network. [Online] Available at: https://www.esa.int/Applications/Connectivity_and_Secure_Communications/ESA_and_European_Commission_to_build_quantum-secure_space_communications_network [Accessed: 22 July 2026].



This is an open access article distributed under the terms and conditions of the
Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.