B U L G A R I A N A C A D E M Y O F S C I E N C E S
INSTITUTE OF INFORMATION AND
COMMUNICATION TECHNOLOGIES

Iliyan Grozdanov Iliev

ABSTRACT

of a dissertation submitted for the award of the educational and scientific degree "Doctor"

OPTIMIZING THE TRANSITION FROM ASSET MANAGEMENT TO SERVICE MANAGEMENT IN COMPLEX FEDERATED SYSTEMS IN THE PUBLIC SECTOR

under the doctoral programme "Computer Systems, Complexes and Networks"
professional field 5.3. "Communication and Computer Engineering"

Scientific Supervisor: Assoc. Prof. Dr. Velizar Shalamanov

Sofia, 2026

Contents

GENERAL CHARACTERISTICS OF THE DISSERTATION

The dissertation is devoted to optimizing the transition from asset management to service management in complex federated systems in the public sector. The study considers digital transformation not as the introduction of isolated technologies, but as a comprehensive architectural and organizational rearrangement of the way digital services are planned, delivered, and managed.

The relevance of the topic is determined by the growing dependence of the public sector on distributed digital services that must operate reliably in a heterogeneous infrastructure, under budget constraints, high security requirements, and a need for interoperability among autonomous participants. In this context, the service-centric model is viewed as the necessary next step after the traditional resource-oriented approach.

Author	Iliyan Grozdanov Iliev
Scientific Supervisor	Assoc. Prof. Dr. Velizar Shalamanov
Doctoral Programme	"Computer Systems, Complexes and Networks"
Professional Field	5.3. "Communication and Computer Engineering"
Dissertation Length	153 pages, 49 figures, 6 tables, 127 references

Relevance of the Research

Performance management systems in public sector networks face specific challenges arising from distributed governance, participant heterogeneity, and dynamically changing public and political priorities. The broad deployment and combination of digital technologies across all spheres of social and economic life leads to an overall digital transformation that necessitates a transition from asset management to service management.

This transition also has a deeper historical logic. In earlier stages of the development of communication systems, it was sufficient to provide the end user with a transmission medium through which they could reach a central computing resource. In such a model, data processing, storage, and management are concentrated at the center, while the network performs the role of an input and output channel. As data volumes grow and requirements for service quality, security, and

latency sensitivity increase, this model begins to reveal limitations that cannot be overcome merely through even greater centralization.

Contemporary digital transformation in the public sector is not limited to the deployment of individual technologies, but represents a rethinking of the way digital services are planned, delivered, and managed. This transition is especially complex in federated systems, where multiple autonomous administrative, communication, and computing domains must interact under different governance rules, a non-uniform infrastructure, and limited control over connectivity, security, and capacity.

In the traditional centralizing model, the emphasis is placed on the infrastructure itself and on maintaining individual technical components. In the service-oriented model, the focus shifts to the value for the end user, the quality of the service delivered, and the system's ability to use the available assets in a flexible, coordinated, and scalable manner. In such an environment, the main question is no longer only which technologies are used, but how they are organized so that the end result is a reliable, secure, and economically justified service capable of operating beyond the logic of absolute centralization.

The dissertation examines four representative classes of digital services: adaptive multimedia distribution through HLS, GPU-based computing services through API and WebSocket, VoIP architectures with direct media exchange, and a federated AIS cloud for edge collection and processing of real-time telemetry. These case studies differ in application, but share common architectural problems: separation between the control and information layers, operation in a heterogeneous and often NAT-constrained environment, protection of identities and data, and efficient use of limited network and computing assets.

Within the present study, optimization is understood as the engineering and organizational improvement of the transition to a service-oriented model according to several basic criteria: reducing latency and improving service responsiveness; increasing reliability and resilience in distributed operation; protecting communication, content, and personal data; using shared assets more efficiently; and ensuring applicability in the conditions of the public sector, including limited budgets, legacy infrastructure, and distributed responsibility.

Object, Subject, Goal, and Tasks

The object of the dissertation is complex federated systems in the public sector, in which multiple autonomous administrative, communication, and computing domains interact in the provision of digital services.

The subject of the dissertation is the set of approaches, architectural models, and technological mechanisms for optimizing the transition from asset management to service management in such systems, examined through representative case studies in the fields of multimedia distribution, high-performance computing, real-time communication, and federated telemetry.

The main goal of the dissertation is to develop approaches for optimizing the transition from asset management to service management in complex federated systems in the public sector.

The following tasks have been set in order to achieve this goal:

1. **To analyze the prerequisites for the transition from asset management to service management in the public sector, including the historical, technological, and organizational factors that determine the need for such a transition in federated environments, and on this basis to formulate general principles and an architectural model for service management in complex federated systems applicable to different classes of digital services in the public sector.**
2. **To analyze the cryptographic risks in computer systems with a view to increasing the security and reliability of communication services.**
3. **To develop methods for secure access to protected content and for protecting personal data in the provision of digital services.**
4. **To develop an architecture for providing administrative and computing services on demand for processing large volumes of data in the public sector.**
5. **To develop a hybrid architecture for providing a communication service in an environment with infrastructural constraints.**
6. **To propose an architectural solution for real-time telemetry in complex federated environments.**

Research Methods

The following research methods were used to achieve the stated goal and tasks:

- systematic and comparative analysis of existing technologies, architectures, and models for delivering digital services;
- historical and contextual analysis of the development of communication and digital infrastructure;
- architectural modelling of services and interactions among autonomous domains in a federated environment;
- analysis of the security and reliability of communication and computing solutions;
- design and study of practically applicable solutions based on actually developed and deployed services;
- generalization of the results into an overall model for the transition to service management.

Length and Structure of the Dissertation

The dissertation is structured into five chapters, an introduction, a conclusion, a bibliography, and appendices. The first chapter examines the historical, technological, and organizational prerequisites for the digitalization of services in federated systems in the public sector. The second chapter analyzes the security and reliability of communication services in a distributed environment. The third chapter is devoted to methods for accessing protected content and to the protection of personal data in video distribution. The fourth chapter examines the transition to the provision of digital services in the public sector through administrative, computing, and federated telemetry services. The fifth chapter proposes architectural solutions for optimizing the transition from asset management to service management in real-time communication and telemetry environments.

The dissertation contains 153 pages, 49 figures, 6 tables, and 127 references.

BRIEF PRESENTATION OF THE DISSERTATION

Chapter 1. Digitalization of Services in Federated Systems in the Public Sector

The first chapter examines the historical, technological, and organizational prerequisites for the transition from asset management to service management. The study begins with the historical evolution of the communication environment in Bulgaria and traces how the accumulated infrastructural deficits in North-Eastern Bulgaria turn into a telling example of a regional digital divide. Emphasis is placed on the difference between the visible manifestations of digitalization - e-services, registers, platforms - and the deeper infrastructural and organizational basis without which these services cannot function reliably.

The transition from the analogue telephone network, dial-up access, and the early forms of Internet connectivity to DSL, LAN access, coaxial networks, and the later development of FTTH/PON is traced. The analysis shows that in a number of remote areas modernization remained economically unprofitable for operators for a long time, which caused the lag to accumulate simultaneously as low capacity, high latency, and limited organizational ability to provide modern digital services. In this context, both the technical characteristics of the environment and the socio-economic consequences - migration, weakening of local capacity, and delay in digital transformation - are examined.

It is shown that global factors such as the COVID-19 pandemic and the war in Ukraine accelerate the reassessment of broadband connectivity as a condition not only for convenience, but for resilient civil-military and administrative infrastructure. Within this framework, the new submarine and terrestrial optical projects in the Black Sea region are also analyzed, as well as their significance for overcoming the accumulated lag. The conclusion is that physical infrastructure remains an irreplaceable foundation, but real public value arises only when coordinated digital services are organized on top of it.

On this basis, the chapter derives the transition from the management of communication assets to the management of services. In the traditional model, the focus is on individual technical resources - lines, servers, routers, receivers. In the service-oriented model, the focus shifts to the way these assets are combined and managed so as to provide a reliable, secure, and scalable service. This requires a clear separation between the control plane and the data plane, as well as a new perspective on latency, security, and efficiency.

The first chapter defines the four representative classes of services used as analytical case studies in the dissertation: HLS adaptive multimedia distribution; CUDA analyses through API/WebSocket as "GPU as a Service"; VoIP direct P2P as real-time communication; and a federated AIS cloud for collecting and processing telemetry. The comparative analysis among them shows that, although they differ in application, all require architectural separation of functions, security mechanisms, resilience under connectivity constraints, and the possibility for available resources to be provided as a service rather than as a locally owned asset.

Particular attention is paid to federated systems as a natural response to the limitations of absolute centralization. The chapter summarizes their basic properties - autonomy of participants, interoperability, secure exchange of information, and more efficient use of resources. As a practically significant example, the AIS environment is examined, in which multiple coastal stations, platforms, and operators interact without a single central owner of all assets. It is shown that precisely here the need arises for an intermediate federated layer for normalization, deduplication, and coordinated delivery of data.

At the end of the chapter, the criteria for optimizing the transition to service management are formulated: latency and responsiveness, reliability and resilience, security, efficiency in the use of assets, and organizational applicability. These criteria serve as a general framework for the following chapters, in which the individual technological implementations are examined. The conclusion is that it is not the individual technology, but the architectural model, that determines whether a given digital environment will remain a set of resources or will turn into a service delivery system.

For the purposes of the present dissertation, optimizing the transition from asset management to service management is considered a multi-criteria task involving interrelated engineering and organizational improvements.

The first criterion is service latency and responsiveness, which is particularly important in real-time communication, video streaming, and interactive computing requests.

The second criterion is reliability and resilience, understood as the system's ability to maintain the service under infrastructural constraints, failures of individual nodes, and variable network conditions.

The third criterion is security, including protection of communication, content, identities, and personal data, as well as limiting the consequences of compromise of individual components.

The fourth criterion is efficiency in the use of assets, that is, the possibility for the available network, computing, and organizational assets to be combined and delivered in such a way as to achieve higher service value under limited resources.

The fifth criterion is organizational applicability, which is particularly important in the public sector, where solutions must operate in conditions of legacy infrastructure, limited budgets, distributed responsibility, and the need for interoperability among autonomous participants.

On the basis of these criteria, the proposed architectural solutions are evaluated in the following chapters, and the way in which they contribute to optimizing the transition from asset management to service management in different classes of digital services is traced.

The first chapter traced the historical development of communication infrastructure and identified the reasons why, in the contemporary digital environment, a transition from asset management to service management is necessary. It was shown that historical infrastructural divides, limited regional connectivity, rising requirements for latency, capacity, and security, as well as the need for interoperability among autonomous participants, make the classical centralizing model increasingly insufficient.

The analysis of the examined service classes showed that, regardless of their differences, they share common architectural problems: the need for a clear distinction between control and information functions, protection of identities and data, efficient use of communication and computing assets, and the ability to provide functions as services rather than merely as locally owned resources.

On this basis, federated systems emerge as a natural architectural direction for development, since they allow a combination of autonomy, coordination, and service sharing among different domains. It is precisely in this context that the following chapters successively examine the cryptographic foundation of trust, the secure provision of protected content, on-demand computing services, and architectural solutions for communication and federated real-time telemetry.

Chapter 2. Methods for Ensuring Reliability in the Management of Communication Services

The second chapter is devoted to the reliability and cyber-resilience of communication services under conditions of uneven digitalization. The thesis is advanced that, with the accelerated

penetration of digital technologies in the public sector, a cyber-security divide emerges alongside the infrastructural one. Therefore, the reliability of digital services must be considered not only as a matter of connectivity and capacity, but also as a matter of choosing an appropriate cryptographic foundation.

The main analytical focus is on the weaknesses of RSA when random number generators operate with low entropy. Examples and studies are examined that show how improper generation of randomness can lead to predictable cryptographic parameters, common divisors among different RSA keys, and practical compromise of systems using an otherwise "strong" algorithm. It is shown that the problem lies not only in the mathematical model of RSA, but in the real computational environment in which it is applied.

The second chapter examines in detail the importance of entropy sources, the role of PRNG and TRNG, and the limitations of Linux-based systems during early boot, when system randomness has not yet been sufficiently accumulated. The possibilities for using hardware entropy mechanisms, including Intel Secure Key, are analyzed as a practically applicable measure for increasing the reliability of cryptographic processes.

On this basis, the transition from RSA to ECC is argued as a more suitable cryptographic foundation for the services examined in this dissertation, which function in distributed and resource-constrained environments. It is shown that ECC provides a comparable level of security with substantially shorter keys, lower computational load, and better applicability to edge devices and embedded platforms. ECDSA and ECDH over NIST curves are examined as a practically applicable framework for authentication and key agreement in the future architectures developed in the dissertation.

The chapter also outlines the perspective for development toward post-quantum resilience. Although this is not the subject of an independent development in the dissertation, the analysis shows that the choice of a cryptographic scheme should not be seen as a one-off decision, but as a stage in a longer cycle of adaptation to new risks. Thus, the second chapter builds the cryptographic and authentication foundation of the entire dissertation and prepares the following chapters, in which security is already considered as part of the service model itself.

Where development has been inconsistent, fragmented, or for a long time subject to partial and delayed solutions, not only connectivity and capacity constraints accumulate, but also vulnerabilities in security. In this sense, the escalation of cybercrime, violations of personal data, financial abuse, loss of information, and extortion related to it are not merely side effects of the

broader use of technology, but indicators that digital transformation often proceeds under conditions of unevenly built cyber-resilience. This shows that alongside the infrastructural divide there is also an interconnected divide in cyber security that requires not isolated measures, but a consistent architectural approach to the reliability and protection of communication services. (Jang-Jaccard and Nepal, 2014), (Kostadinov and Atanasova, 2019), (Dineva and Atanasova, 2019).

Compliance with cyber-security requirements is a prerequisite for the security and safety of IT infrastructures, digital resources, and the protection of personal data. In this regard, the topics of cryptography and sufficiently reliable generation of random numbers, which are at the core of every encryption system, are of special interest (Shalamanov, 2020).

For the needs of modern cryptography, two types of random number generators are used - true random number generators (TRNG) and pseudo-random number generators (PRNG) (DiCarlo, 2012).

A true random number generator (TRNG) is used when the RNG must generate values at a given moment that must be unique and must not repeat in subsequent RNG invocations (Carr, 2003), (L'Ecuyer, 2007). The numbers obtained through this type of RNG are applied to operations that require unique, non-repeating numerical values generated over time. (Jin, 2004), (Camara, 2019) An example of such a situation is the generation of a cryptographic key for encoding/decoding data, initialization vectors, initial numerical values (seed) for controlled RNGs, and similar cases. (Ergun, 2015), (Ryabko et al., 2016)

A pseudo-random number generator (PRNG) uses an initial random number from the micro or macro world (seed) as its basis, and a mathematical formula is used for the subsequent numbers. From the initial value, through the application of a specific algorithm, all subsequently generated random numbers are derived. The subsequent values are reproducible in order. The only unexpected and secret value that must be as unpredictable as possible is the initial number, which is the "root" at the base of the sequence and initiates the generation of the entire numerical series. Technologies such as one-time-password authentication (OTP), the generation of cryptographic keys derived from a master root key (used in the construction of wallets in blockchain, i.e. distributed ledger technology), HMAC-based authentication, and others are based on this principle.

Problems with the random number generator (RNG) are at the root of the flaw in the digital certificate of a Taiwanese citizen. Bernstein, Chang, Cheng, Chou, Heninger, Lange, and van Someren presented a report during Asiacrypt 2013 (Bernstein et al., 2013), in which they showed that the official smart cards for citizen identification issued by the Taiwanese government were

defective. Their results were based on the study by Heninger et al. (2012) on low-entropy security keys. In that work, the researchers investigated low-entropy security keys and whether similar defects could be discovered in Taiwan's "Citizen Digital Certificate" database. The researchers examined 2 million 1024-bit RSA keys from that database and established that 184 of these keys were trivial to compute within a few hours. They attributed these weak RSA keys to a fatal flaw in the hardware random number generator (RNG). The randomness used to generate the RSA keys had insufficient entropy and created predictable patterns for RSA primes.

An article published in 2012 (Heninger et al., 2012) showed a weakness in TLS (Transport Layer Security) and SSH (Secure Shell) servers involving weak security keys. The authors revealed that improperly functioning random number generators (RNGs) led to low entropy in the randomness used for RSA and DSA server keys, which in turn caused compromised cryptography. The researchers pointed out that this vulnerability was due to an entropy gap in the RNG (/dev/random and /dev/urandom). During boot, /dev/random uses data left over from the previous boot for the entropy pool. But when the system has been powered off for a long time and memory has returned to its baseline state, these data become predictable.

The RSA algorithm is considered slower. RSA keys are commonly 2048 or 4096 bits in length. From the standpoint of RSA security, 2048-bit RSA keys are no longer considered fully secure. This is why most organizations are currently moving to 4096-bit keys. Many organizations, however, avoid RSA encryption because of the slow key generation and algorithmic operations, as well as because of the high consumption of machine resources.

P and Q are publicly known. The secret (the private key) is the scalar d in the equality $Q = d \cdot P$. Computing Q from (P, d) is easy, but recovering d from (P, Q) is hard when the parameters are correctly chosen and the order of the group is sufficiently large; in mathematics this is known as the elliptic-curve discrete logarithm problem. ECDLP is a fundamentally hard mathematical problem on which the security of modern elliptic-curve cryptography (ECC) rests. For the "reverse direction" in ECC (finding d from $Q = d \cdot P$), the standard argument for hardness is that in the generic model any attack against the discrete logarithm requires at least $\Omega()$ group operations, where p is the largest prime divisor of the order of the group - that is, in practice it grows like the square root of the group size and becomes infeasible with properly chosen parameters (Shoup, 1997).

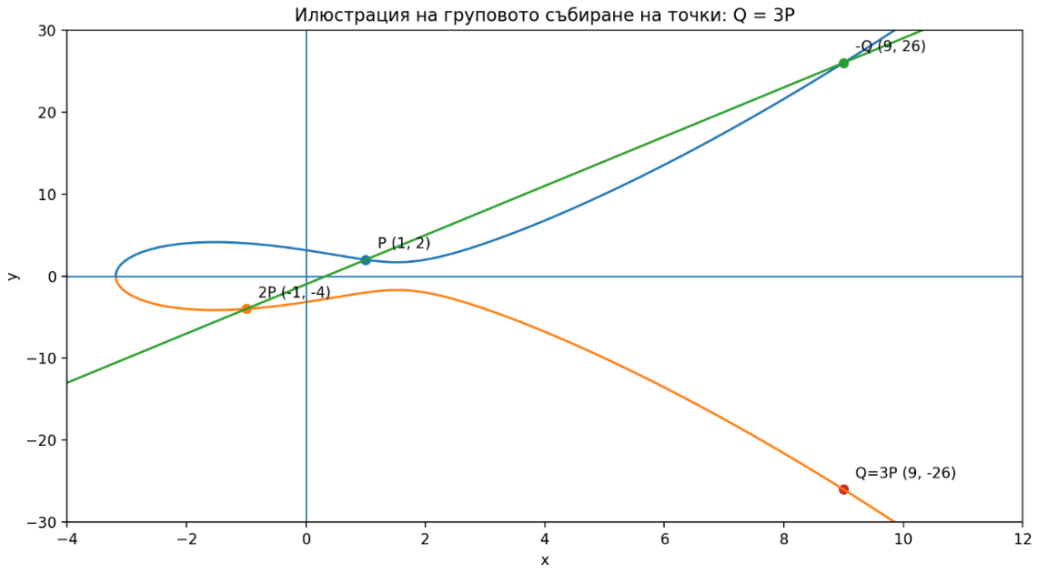

Fig. 2.2. Illustration of point addition: Q = 3P.

For autonomous systems in the federated AIS cloud, which often operate on embedded devices (Raspberry Pi, edge receivers/forwarders), it is important for asymmetric operations to be fast and not to "inflate" the traffic. Algorithms based on elliptic-curve cryptography - ECDSA for signatures and ECDH for key agreement - provide equivalent cryptographic strength with significantly shorter keys and signatures than RSA, which is practical for end-to-end protection during transport between nodes in the cloud.

The NIST Digital Signature Standard (FIPS 186-5) defines ECDSA and the established "NIST curves" P-256, P-384, and P-521, which are widely supported in standard cryptographic libraries and hardware modules.

According to recommendations for equivalent security strength (for example SP 800-57 Part 1), P-256 is a typical choice for approximately 128-bit strength: public keys and signatures are compact (tens of bytes), whereas RSA for a similar level requires keys on the order of 3072 bits, which increases latency, certificate size, and the load during signing and verification.

Similar principles - signing AIS content for authentication and integrity while preserving backward compatibility - are also demonstrated in Protected AIS (pAIS), where a cryptography-compatible scheme is used to address known AIS vulnerabilities and preserve interoperability with unmodified AIS devices (Gary Kessler, 2020).

Chapter 3. Methods for Accessing Protected Content

The third chapter examines methods for accessing protected content and possibilities for limiting the leakage of personal data when delivering multimedia services. The starting point is that, in modern web streaming, protection of communication and protection of the user's identity should be regarded as different, though interrelated, functions. On this basis, the chapter proposes an architectural approach in which content distribution is separated from the process of authenticating the end user.

A typical scheme for video distribution via upstream RTMP and HLS to the end user is examined (Fig. 3.3). A web streaming service is essentially a combination of protocols for upstream transmission to the streaming server and downstream transmission to end users, with the most commonly used set being RTMP + HLS. This division of protocols has emerged over the years because of the specifics of user connectivity. Under HLS, the video stream is divided into chunks, and a text playlist in standardized M3U format describing the chunks available for download is periodically retrieved and read. In order to achieve service reliability, load distribution, and low latency toward the end user, the streaming platform is built as a CDN scheme with multiple geographically distributed nodes.

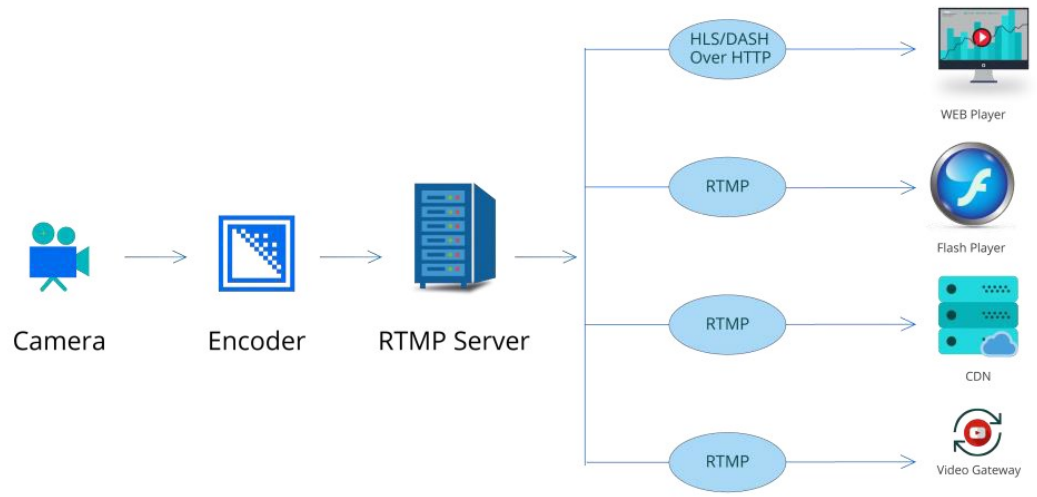

Figure 3.3. Diagram illustrating the RTMP streaming process (source: synopi.com).

It is shown why HLS is practically suitable for broad consumer distribution - support in browsers and HTML5 players, operation over HTTP(S), better resilience in home and mobile networks, and the ability to apply standard authentication and authorization mechanisms. At the same time, it is argued that protecting RTMP communication between the studio and the server is

more reliable when done through a pre-established cryptographic tunnel than when relying solely on RTMPS on endpoint devices with limited security capabilities.

A substantial contribution of the chapter is the idea of separating content from authentication. A test model has been developed in which the video distributor does not process sensitive personal data, while user authentication and token issuance are assigned to a separate trusted service. As a result, even if the streaming infrastructure is compromised, the risk of leakage of personal and payment data is significantly limited. Thus, security is not achieved solely through encryption, but through a functional separation of responsibilities.

The chapter also examines the possibility of regional and local redistribution of protected video content in an environment of small and regional Internet providers. The thesis is advanced that, where local PON infrastructure exists and external Internet connectivity is limited, the operator can receive one high-quality incoming stream and redistribute it within its own network, thus reducing external traffic and improving service quality for subscribers. This logic is placed in a regulated environment of access control and key-material protection, unlike the historical practices of unregulated LAN file sharing.

The conclusion of the third chapter is that the secure provision of content does not amount to the basic encryption of video fragments, but requires a complete service model in which transport, authentication, issuance of key material, and local distribution are organized coherently. In this way, the cyber-resilience of the service is increased, dependence on the limitations of external Internet connectivity is reduced, and the transition to more complex administrative and computing services in the next chapter is prepared.

Here comes the second aspect of the study, which concerns the video distributor and examines the protection of video content against end users. Since the specific video content is intended for a strictly defined group of users, it follows that the HTTPS server must first be configured in accordance with security best practices (https://www.ssl.com/guide/ssl-best-practices/). Mechanisms for authenticating users must then be implemented.

For the purposes of the study, a simulator of such processes has been developed in the backend, functioning between the "bare" HLS service of nginx and the end user, which is responsible for providing the user with a token in a cookie after valid authentication and, accordingly, for validating the tokens from client requests. If the token is not provided or is invalid (expired), the backend returns 401 Unauthorized (Mueller, 2015).

The possibilities for obtaining a token are numerous and varied. They depend primarily on the managerial decisions of the organization or group of organizations.

In this dissertation, a simple SSO login service has been developed for demonstration purposes.

After the SSO service is invoked (Fig. 3.6) and the authentication process is successfully completed, an application user session is started with a randomly generated cryptographically protected identifier, and the session cookie is returned in the response to the client.

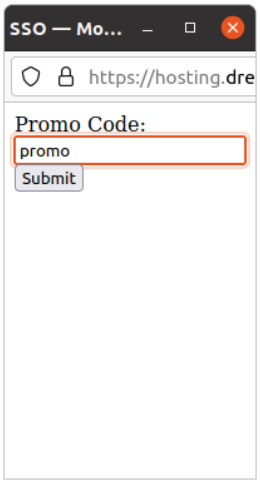

Fig. 3.6. Form for obtaining an authorization token.

The client is required to provide the token in order to keep the session active (Fig. 3.7). The time window during which the token is valid, as well as the time for re-issuance, are subject to definition at the managerial rather than the technical level.

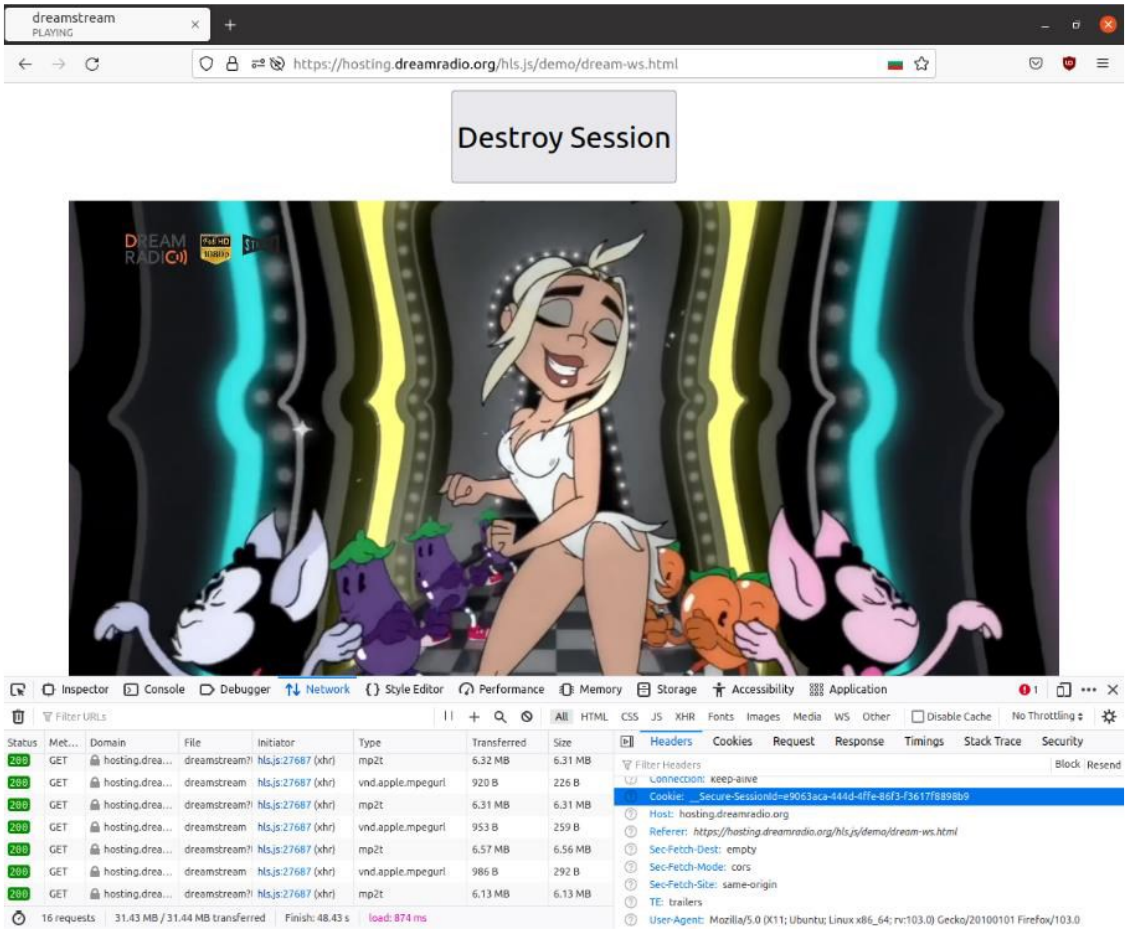

Fig. 3.7. Authorization to a streaming session using cookies

The implementation of this SSO service is intended to demonstrate that the distribution of video itself and the authentication of users can be separated among different organizations. This means that the broadcasting organization and the trust provider can be completely separated.

An extended conditional-access model has also been developed (Fig. 3.13), in which the keys for decrypting the HLS streams are provided only after successful authentication and initiation of a user session. In this way, the logic of protected multimedia distribution is combined with minimizing the processing of personal data by the distributor itself. It is shown that this approach is practically applicable both to larger and to smaller streaming projects.

In this way, the download of each key is protected by the application's user session against unauthorized retrieval.

Initially, the user is identified before an authentication-service provider integrated with the system, which creates a profile for the user. Usually, identification is carried out remotely, and the profile is accessible through a mobile application.

The streaming service encrypts the AES key each time with the public keys of each x509 certificate subscribed to the live stream and sends the encrypted AES keys to the repository.

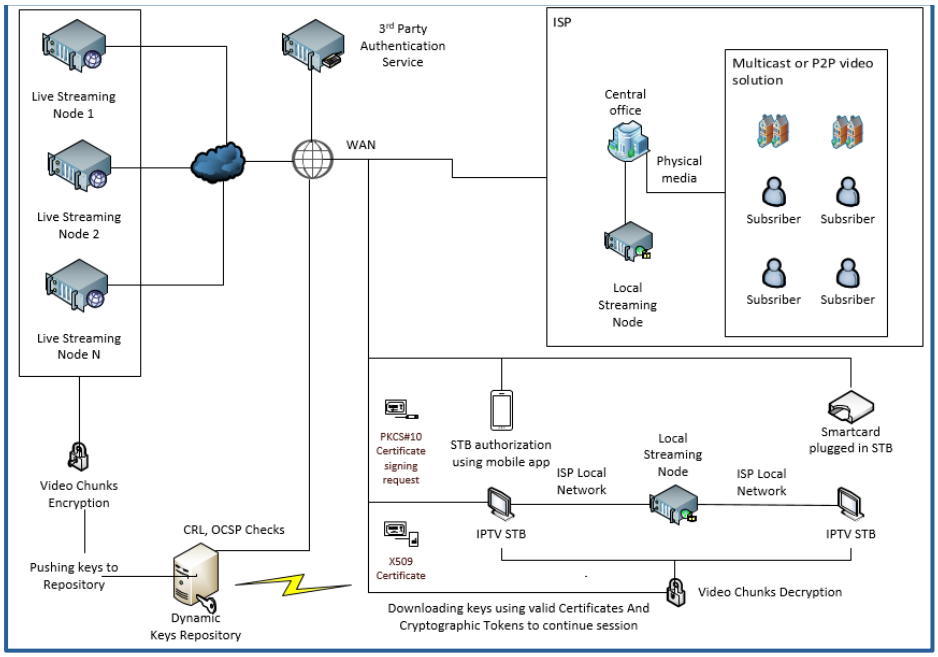

Fig. 3.13. General scheme for distributing live streaming in a local Internet environment

In this way, the dissertation examines the possibilities for protecting the communication between the streaming studio and the RTMP server, on the one hand, and the HLS communication between the video distributor and the end user, on the other, while proposing the implementation of a user-authentication portal provided by an authentication-service provider that relieves the video distributor of processing personal data and payment instruments. For the purposes of the research, the proposed approach was implemented on a test server, from which the results of the study were presented. The advantage of the proposed approach to protecting streaming content is that it can be applied to any kind of high-budget or low-budget project. In addition, content distributors are not required to take care of administering users' personal data. This leads to even higher cyber-resilience of the proposed solution, because even in the event of a server security breach, there are no personal data that can be stolen.

Chapter 4. Service Management in Complex Federated Systems in the Public Sector

The fourth chapter examines service management in complex federated systems in the public sector through three interrelated directions: administrative services, on-demand computing services, and a federated service for collecting and pre-processing streaming telemetry. The general idea is that the transition to a service-oriented model may be realized either through centralized computing services or through distributed federated mechanisms, depending on the nature of the task.

In the first direction, it is shown that complex analytical and administrative functions can be provided as a service instead of being duplicated locally in every office or administration. An architecture has been developed and implemented with an HTTP API for receiving files and tasks, reverse WebSocket signalling for real-time notification, and a standalone insightd daemon that performs GPU-accelerated processing through RAPIDS. Thus, the API/WebSocket layer functions as an intermediate service layer between the consumers of the analyses and the computing service itself.

The analysis of geospatial data is a key factor for digital transformation and regional development in the case of urban planning, solving traffic-related problems and serving as a clear direction toward smart cities (Erskine et al., 2014). It is also of essential importance to commercial organizations for decision-making in cases such as network coverage planning, investment studies, risk assessment, and market analysis (Wickramasuriya et al., 2013). So-called online analytical processing services (OLAP) are becoming increasingly necessary (Rivest et al., 2005), since they provide various mechanisms for geodata analysis in remote digital environments, enabling this to be performed entirely automatically. Human history has repeatedly shown that every change or revolution is difficult, painful, and unfolds over a long period of time. There is no exception here. Today, the workflow is still not automated despite all the practical requirements of current computer technology development.

The main practical problems of digital transformation in administrations have been analyzed: lack of sufficient IT skills, partial and unsynchronized transformation, high costs for specialized hardware, and difficulties in integration among different systems. The proposed model solves these problems by centralizing heavy computations and providing a stable interface to internal and external users. This means delivering online services for the analysis of geospatial data (Fig. 4.1). At the same time, partner organizations are increasing their interest in this area by creating cutting-edge products.

Moreover, most of them would not wish to create a complex infrastructure for this activity and would refrain from developing their own software, which requires in-depth knowledge of multidimensional data processing. Consequently, they would focus on developing higher-level software and services for their business, and in this case the provision of an online analytical service would be an excellent opportunity for this.

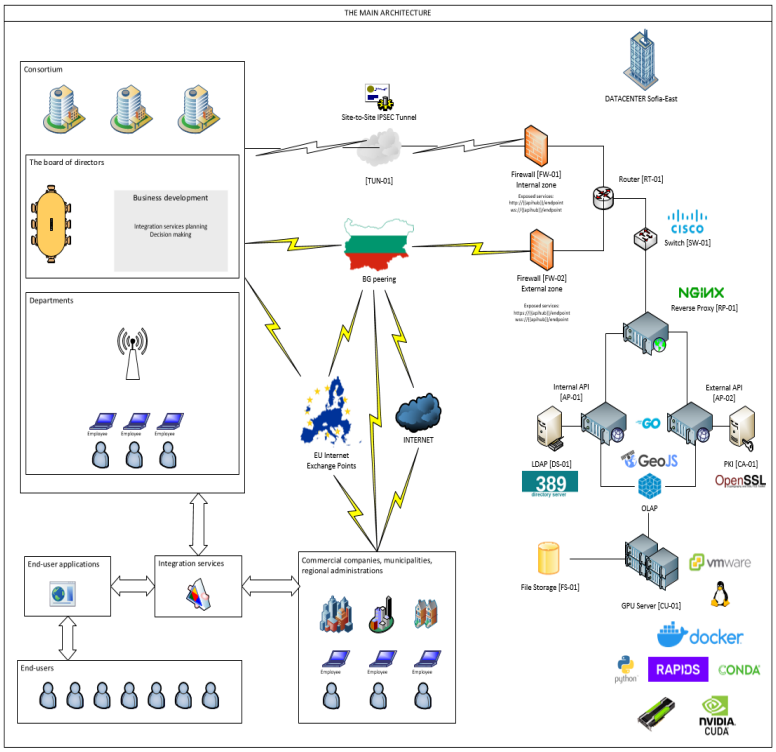

Fig. 4.1. Presentation of the main architecture of the platform developed in this dissertation.

The purpose of providing the API service is, on the one hand, to enable integration with potentially interested organizations that can benefit from a centralized data-analysis service (de Castro Lima, 2018), and, on the other hand, to ease their technical tasks compared to undertaking the construction of their own data-analysis services. An important point to mention is that the tasks of integration are not exhausted merely by building API services, because they do not represent a one-off action in time, but are subject to changes and improvements. In this regard, it is necessary to emphasize CI/CD approaches that follow established principles, while for organizations lacking highly qualified personnel this may be especially challenging.

The second line in the chapter is related to the federated AIS cloud. Here, parallelism is not understood as speeding up a single centralized task, but as the simultaneous existence of multiple

streaming processes for reception, normalization, deduplication, routing, and delivery. It is shown that the AIS environment requires a different architectural approach: data arrive continuously, from multiple sources, and require immediate pre-processing close to the place of reception.

On this basis, an architectural model of a federated AIS cloud is proposed (Fig. 4.7), with a clear separation between the control plane and the data plane, as well as the roles ingress, transit, dedup, and egress. An important characteristic of this model is that the same autonomous system may perform different roles for different logical flows, while its internal implementation remains autonomous as long as it supports the agreed interface toward the other participants. In this way, the service is built upon a federation of operators rather than upon a central owner of all reception points.

The internal architecture of each AS is fully autonomous (it may be a single process or a large cluster), while the overall behaviour is formed through a standard external interface: identity (with asymmetric cryptography mechanisms), functional capabilities, pairing rules, and accountability.

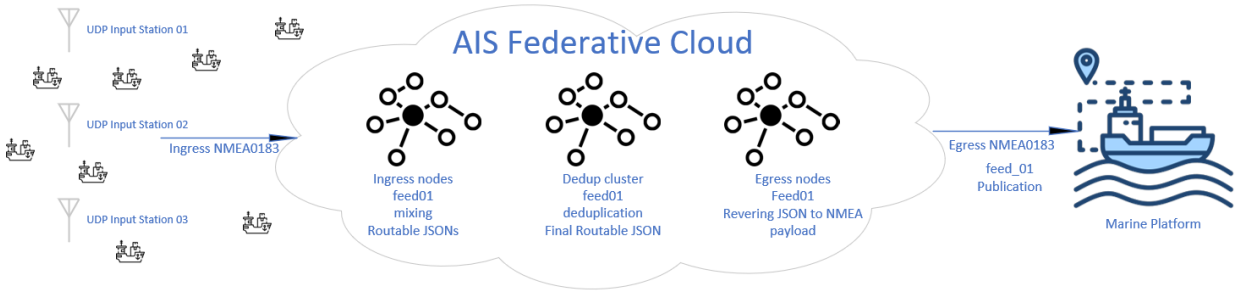

Fig. 4.7. General architectural scheme of the AIS federated cloud proposed in this dissertation

The roles Ingress, Transit/bridge, Dedup/aggregator, and Egress are not fixed for a given AS. The same AS may perform different roles for different logical flows. The federated character comes from the fact that the system does not impose one "correct" software stack; each operator may choose a technological stack, provided that it supports the interface toward the others. From a practical point of view, the proposed model should simultaneously satisfy requirements for easy inclusion of new participants, compatibility with existing marine platforms, and sustainable growth in the number of nodes without concentrating processing in a single center.

The conclusion of the fourth chapter is that service management in complex federated systems does not imply a single architectural recipe. For some tasks, centralizing the computational burden and providing it as a service is more efficient, while for others a distributed federated organization close to the source of data is required. In both cases, however, clear separation of

functions, the possibility for coordinated management, and relieving end participants of possessing and maintaining all necessary local assets are decisive.

The normative specifications for AIS emphasize the real-time nature of the system: AIS is autonomous and self-organizing (without a master), and tactical information must be exchanged continuously (typically at least every 10 seconds, and on some routes every 2 seconds). To achieve such a "live" picture in coastal areas, the density of terrestrial receivers is crucial: each additional antenna/receiver point not only extends the geometric coverage, but also increases the probability of receiving weak or partially obstructed transmissions. The problem is that more receivers mean more repetitions of the same AIS reports, which "flood" the output toward the platforms. This is precisely where the federated cloud has systemic value: it allows a dense coastal reception network for real-time reception while at the same time performing deduplication and normalization before delivery to the platforms.

Inter-domain routing through BGP uses permanently established peering sessions for the exchange of routing information between autonomous systems (RFC 4271). MPLS offers a logical abstraction of the path through labels, which is useful as a metaphor for a "logical flow" and classes of traffic (RFC 3031). P2P DHT systems such as Kademlia (Maymounkov et al., 2002) show how decentralized nodes discover resources/paths without central control. In the mass target scenario, participants in the cloud are small operators. Paths may change dynamically for various practical reasons related to reconfigurations on the Internet provider's side, temporary interruptions, and so on. Central routing is anti-federated and often becomes outdated; therefore, searching in the local graph of connectivity is preferred. A typical algorithm is BFS over neighbours with a time-to-live (TTL), a hop limit, and a cache of the successful next hop.

The issues examined in the preceding chapters concerning asymmetric cryptography, the choice of lighter and more applicable elliptic-curve schemes, identity management, and transport-channel protection are directly relevant to the federated AIS cloud as well. Protection only at the transport level, for example through tunnelling or an encrypted channel between two points, is necessary, but not sufficient in an environment with multiple autonomous participants and with the possible passage of the flow through more than one node. In such an architecture, it is necessary for the origin and integrity of the data to remain verifiable beyond the specific transport segment. Therefore, application-level protection may be regarded as a natural complement to transport protection: the participant's identity is authenticated through asymmetric cryptography mechanisms,

and the payload data and accompanying metadata may be signed so that they remain verifiable along the entire path of the service. In this context, lighter elliptic-curve schemes are especially suitable because they allow practical protection in a distributed environment with limited resources. By analogy with the principle examined in the previous chapter of separating content from authentication, transport, identity, and the data themselves should here as well be regarded as distinct, though interrelated, layers of the service.

Chapter 5. Optimizing the Transition from Asset Management to Service Management

The fifth chapter is the culmination of the dissertation and presents two practically validated directions for optimizing the transition from asset management to service management: a hybrid VoIP solution for an environment of regional Internet providers and an architecture of a federated AIS cloud for providing navigational telemetry as a service.

In the first part, a real corporate scenario with offices in Varna and Balchik is examined, in which three main problems are present: insufficient capacity relative to contemporary needs, a lack of practice in providing extended L2/L3 services, and unusually high latency even between geographically close points. The analysis shows that under a classical centralized VoIP architecture, media traffic would have to pass through the central PBX, which unnecessarily lengthens the path of the audio and increases the risk of losses and fluctuations in quality.

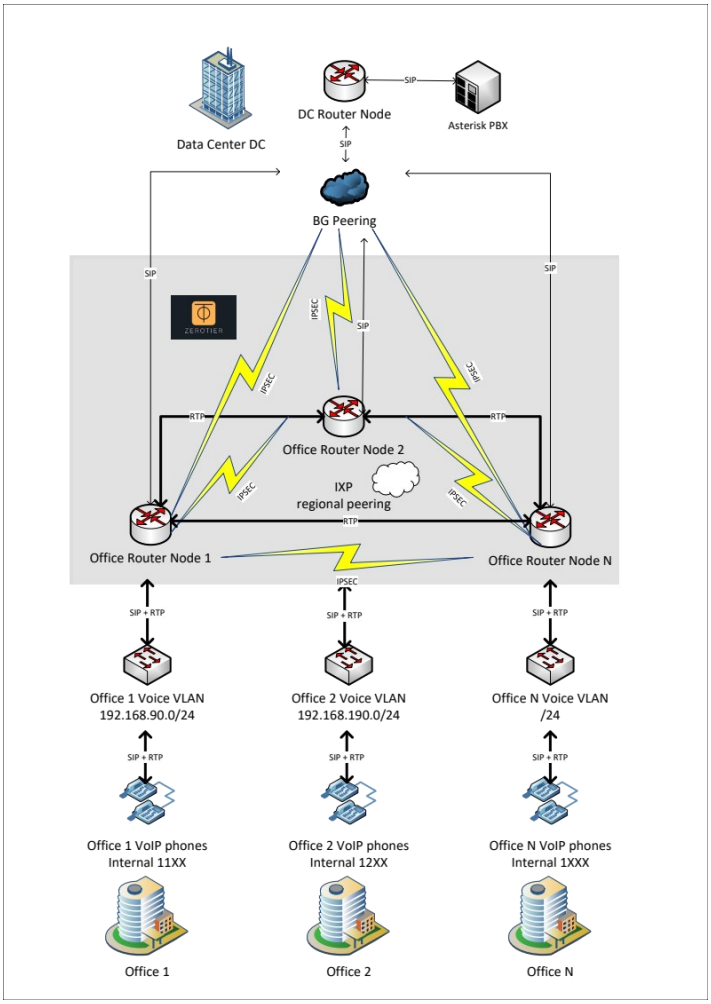

Fig. 5.5. Architecture of the solution

The proposed solution (Fig. 5.5) is a hybrid architecture in which the Asterisk PBX in the data center performs only the role of a central SIP signalling server, while RTP audio streams are transmitted directly peer-to-peer between the endpoints through ZeroTier overlay connectivity and additional IPsec protection.

The architectural meaning of this choice is twofold: on the one hand, central management of calls and rules is preserved; on the other hand, the payload traffic itself follows the shortest practically possible route between the participants.

It is shown how this architecture addresses all three main problems. Heavy audio traffic is not concentrated in the central "star", which relieves the channels toward the data center. The absence of public IP addresses is overcome through dynamic virtual connectivity, which makes it possible to build P2P channels even in a NAT-constrained environment. The most significant practical result is

the reduction of latency: instead of approximately 25 ms when relayed through the center, latency of about 15 ms is achieved with a direct media connection between the offices.

The effectiveness of the solution is validated through analysis of the signalling and media traffic with Wireshark. The registration of terminals to Asterisk, the SIP dialogue during call establishment, codec negotiation, and the subsequent direct RTP exchange between the local networks of the two offices are traced. These observations confirm that the PBX manages only the signalling, while the voice flow is exchanged directly, which is precisely the practical manifestation of the transition from management of a central resource to the provision of a service through a coordinated distributed architecture.

The services examined so far in this dissertation - video streaming, the on-demand GPU service, real-time VoIP communication, and the federated AIS cloud - represent different engineering regimes, but share a common architectural logic: separation of functions, control over latency, observability, and resilience when components fail. For this reason, the design of the federated AIS cloud should draw on proven practices from streaming systems, real-time communications, and federated cloud models, adapting them to the specifics of navigational telemetry and the multi-domain environment.

The second part of the chapter examines the federated AIS cloud no longer merely as a conceptual architecture, but as a means of optimizing the provision of telemetry as a service. A compact formalization of the resource effect under centralized and federated models is proposed.

Notation	Meaning
N	number of active receiver nodes
λu(N)	intensity of the useful unique stream of AIS events
ddup(N)	average duplication coefficient before local deduplication
dres(N)	residual duplication coefficient after local or regional deduplication
κ	relative weight of deduplication with respect to pure reception and transport

Cnf(N)	normalized central resource under a non-federated model
Cfed(N)	normalized central resource under a federated model
G(N)	architectural benefit of the federated approach as the ratio between the two resources

Table 5.1. Notation

If $\lambda u(N)$ denotes the useful unique stream of AIS events, and ddup(N) denotes the duplication coefficient, then under a non-federated model the central resource must absorb a raw stream $\lambda raw(N)=ddup(N)\cdot\lambda u(N)$. The normalized central resource may be written as $Cnf(N)=ddup(N)+\kappa\cdot(ddup(N)-1)$, where the second term expresses the additional burden of deduplication. Under a federated model, part of the cleansing is carried out closer to the source, and a stream with a residual coefficient dres(N) reaches the higher level, so that $Cfed(N)=dres(N)+\kappa\cdot(dres(N)-1)$. The ratio $G(N)=Cnf(N)/Cfed(N)$ expresses the architectural benefit of moving part of the processing to the lower levels of the federation.

This formalization does not claim to be an empirically calibrated model; rather, it serves to show the most essential relationship: under strong overlap of reception zones, the raw incoming stream toward a central node grows faster than the useful unique stream. Consequently, the centralized system pays a cost not only for transporting the data, but also for deduplicating them. Under a federated model, a substantial part of this burden is absorbed lower in the architecture through local deduplication, normalization, and preliminary processing.

Accordingly, the architectural benefit of the federated approach grows as the number of nodes increases and as the degree of local overlap rises. This shows that, in the absence of a federated cloud, an increase in the number of reception points leads to an equivalent increase in the required central resource, whereas under a federated organization part of that load is absorbed at a lower level through local deduplication and preliminary processing. Fig. 5.12 presents a schematic dependence between the number of reception nodes and the required central resource in two regimes: without a federated cloud and with a federated cloud. For illustration, it is assumed that the duplication coefficient before local deduplication grows according to $ddup(N)=1+0.07\cdot(N-1)$, and the residual coefficient after local or regional deduplication grows according to $dres(N)=1+0.012\cdot(N-1)$, with $\kappa=0.6$. The parameters are illustrative.

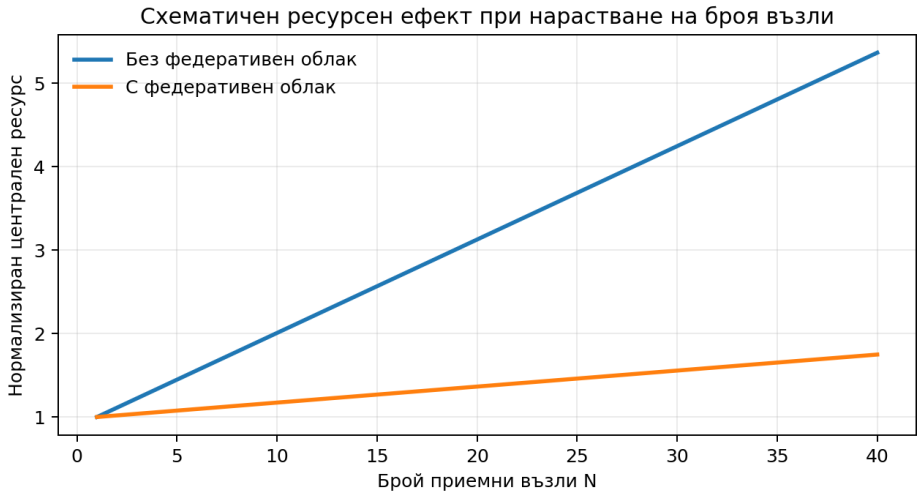

Fig. 5.12. Schematic resource effect as the number of nodes increases

The practical effect is organizational as well. The administrative user is not interested in which specific station received a given AIS message, but in obtaining a reliable picture for a specific operational section. For this reason, the dissertation proposes defining the service not with respect to physical assets, but with respect to the requested result - for example, a basic deduplicated and geographically limited stream for a specific stretch of the fairway. In this way, reception, cleansing, deduplication, and spatial limitation become a coordinated service rather than unrelated operations on fragmented assets.

Particularly illustrative is the Danube example of Ruse - Tutrakan - Silistra, in which individual reception points observe a partially overlapping AIS picture. Under a traditional model, the end user would receive a mixed stream from different stations and different river segments. Under the federated model, the logical order of processing is normalization, temporal ordering, deduplication, geographic limitation, and, where necessary, contextual enrichment with relevant non-positional messages. Thus, what reaches the end user is not a raw infrastructural mixture, but a selected and operationally meaningful service. Consequently, under the traditional model of delivering data according to physical assets, the end recipient does not receive a "clean" stream for the requested section, but a mixture of messages that also relate to neighbouring river segments (Fig. 5.13).

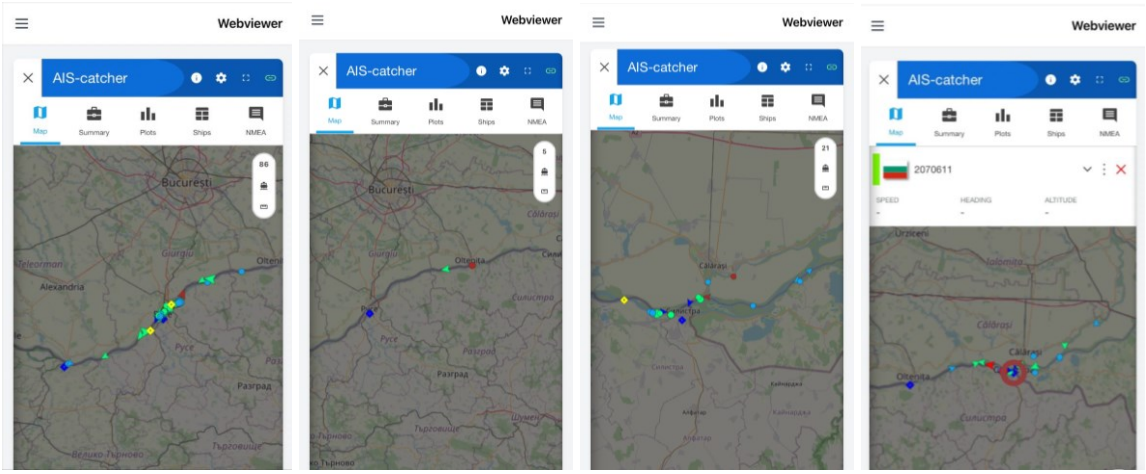

Fig. 5.13. AIS reception study in the area of Ruse, Tutrakan, Aydemir and Silistra

Mixing of streams, deduplication, and spatial limitation are performed in the federated environment, close to the place of reception, without the operator maintaining these functions locally. Traceability of reception, transit, deduplication, and delivery activities is also provided, without burdening the station operator with the management of these components.

The practical relevance of such an approach can also be seen in European initiatives for the integration of river information services. EuRIS is implemented as a common and centralized point of access that collects data from national infrastructures and provides services through a web portal and programming interfaces, with raw AIS data entering the environment through protected VPN connectivity (Zwicklhuber and Kaufmann, 2023). In this sense, the model proposed here does not reject such solutions, but builds upon them by shifting the emphasis from centralized collection of infrastructural flows to federated provision of a cleansed service according to a specific section and a specific administrative need. A similar direction is observed in DANRiSS and its planned upgrade DANRISS 2, where an integrated platform, avoidance of duplication among administrations, the use of sensors, data analysis, and artificial-intelligence solutions for improved monitoring and inspections are being pursued (Ministry of Transport and Communications, 2018), (Ministry of Regional Development and Public Works, 2026).

The fifth chapter shows that optimizing the transition from asset management to service management does not boil down to replacing one technology with another. In VoIP, it manifests itself as a separation between centralized management and direct transmission of payload traffic. In

the federated AIS cloud, it manifests itself as a separation between the control and information layers, edge collection, normalization, deduplication, and the provision of telemetry as a service instead of as static inheritance of individual physical stations. In this sense, the chapter concludes the dissertation with two practically validated models of service-oriented transformation for services with the highest sensitivity to latency, resilience, and environmental dynamics.

SUMMARY OF THE RESULTS OBTAINED

The obtained results confirm the main thesis of the dissertation, namely that optimizing the transition from asset management to service management in complex federated systems cannot be reduced to the choice of a single technology, but requires a comprehensive architectural approach. Such an approach does not diminish the importance of infrastructure, but places it in the proper systemic context.

In the field of security, the need for a transition to more modern authentication and protection mechanisms is substantiated. The analysis of RSA's dependence on the quality of entropy shows that the reliability of digital services depends not only on the algorithm itself, but also on the actual computational environment. On this basis, ECC is justified as a more suitable cryptographic foundation for modern distributed and resource-constrained environments, as well as the need for future development toward post-quantum resilience.

In the field of multimedia services, it is shown that protection of content and protection of personal data can be combined more effectively through the separation between content distribution and user authentication. In this way, the processing of sensitive data by the video distributor is limited and the cyber-resilience of the service is increased.

In the field of administrative and computing services, a practically applicable model for centralized provision of API/WebSocket-based and GPU-accelerated services for processing geospatial data has been validated, implemented through an intermediate layer for access and notification and through the standalone insightd daemon. This reduces the need for expensive local hardware, facilitates integration, and allows more efficient use of computing assets in the public sector.

In the field of real-time communication and telemetry, two practically significant models of service-oriented transformation are demonstrated: a hybrid VoIP architecture with centralized

signalling and direct P2P media transport, and a federated AIS cloud with separation between control and information functions, edge collection, normalization, deduplication, and coordinated delivery of data. In both cases, the focus shifts from ownership of individual resources to the provision of a reliable service with a clearly defined result.

The general conclusion is that infrastructure is a necessary foundation, but real digital value arises when coordinated services are built on top of it. Therefore, the service-oriented and federated approach represents not a temporary technological fashion, but the logical next step in the development of digital systems in the public sector.

CONTRIBUTIONS

The main scientific and applied-scientific contributions of the dissertation can be summarized as follows:

1. A **general model for the transition from asset management to service management** in complex federated systems in the public sector has been developed. The model integrates digital, network, and computing resources into integrated services with guaranteed quality. This optimizes the reliability and security of processes while at the same time improving their efficiency and organizational applicability in data management.
2. The choice of **ECC (Elliptic Curve Cryptography)** is argued as a more suitable cryptographic foundation for the distributed services with limited resources examined in the dissertation. This is achieved through a detailed analysis of the deficiencies of RSA under low entropy and the formulation of practical guidelines for increasing cryptographic resilience. With ECC, the entropy requirements for generating a secure key are substantially lower than with RSA (because of the smaller key size for the same security level), which is critical for IoT devices and edge services, where sources of true randomness are often limited.
3. Methods have been developed for the **secure provision of multimedia services** by separating the processes of content distribution from user authentication. This approach limits the processing of personal data by the distributor, ensures regulated redistribution, and increases the cyber-resilience of the service.

4. An architecture has been developed for providing a**dministrative and computing services on demand**. It includes API-based access to geospatial-data processing and a specialized insightd daemon for centralized GPU-accelerated computation. This approach minimizes dependence on expensive local hardware and significantly facilitates integration with external systems. The use of GPU-accelerated processing through a specialized daemon is a key advantage in the context of geospatial data (GIS). The combination of API access and a GPU daemon architecturally separates the management interface from the heavy computations. Because of the high requirements for parallelization in large arrays of spatial data, centralized structures offer substantially higher efficiency and computational power compared with the capacity of standard local workstations.
5. **A hybrid VoIP architecture** has been developed for communication services in environments with infrastructural constraints. The model combines centralized SIP signalling with direct transport of media traffic, which minimizes latency and eliminates the negative impact of technical limitations imposed by regional providers. This helps overcome NAT traversal problems or bandwidth limitations on the providers' side.
6. **An architecture of a federated AIS cloud** has been proposed for providing navigational telemetry as a service. It is based on a strict separation between control and information functions and introduces specialized roles for processing data streams. Mechanisms for deduplication, cleansing, and normalization are integrated, which guarantee the coordinated provision of reliable telemetry services. The federated cloud can combine data from different sources without forcing them into centralization. The normalization and deduplication module efficiently filters the "noise" generated by duplication of telemetry packets in dense sensor networks. This makes it possible to build a unified, consistent real-time picture of traffic.

In this way, the formulated contributions outline a comprehensive model for optimizing the transition from asset management to service management in complex federated systems in the public sector.

FUTURE RESEARCH

The results obtained in the dissertation outline a number of opportunities for future development and expansion of the proposed models and architectural solutions.

First, a logical continuation is the development of the federated AIS cloud through improvement of the mechanisms for aggregation, processing, and protected transport of telemetry streams. In this direction, approaches may be investigated for following routing policies according to NMEA v4 Tag Blocks, as well as schemes for transport encryption over insecure networks. A practical basis for such development is the AISMixer platform, intended for mixing signals from one area into a common stream.

Second, a promising direction is the extension of the model toward edge data processing through the integration of lightweight algorithms for local analysis in municipal and regional nodes. Such an approach would allow part of the processing to be performed closer to the data source, which could reduce latency, limit the load on the central infrastructure, and create prerequisites for more proactive digital services.

A fourth possibility is related to improving the mechanisms of trust, traceability, and inter-organizational interaction in environments with multiple autonomous participants. In this context, means may be investigated for event logging, tracing the data life cycle, and automated reporting of the quality of delivered services, including under agreed service parameters.

A promising direction for future research is the introduction of edge AI into the federated AIS cloud. This would allow part of the analysis to be performed already in peripheral nodes through early anomaly detection, preliminary risk assessment, and separation of significant events. Such an approach is also in line with current initiatives along the Danube, including DANRISS 2, where a combination of artificial intelligence, sensors, and data integration is already being sought.

The indicated directions do not change the main framework of the dissertation, but represent its natural extension toward a higher degree of autonomy, security, scalability, and intelligence of services in complex federated systems.

PUBLICATIONS RELATED TO THE DISSERTATION TOPIC

1. **I. Iliev,** I. Blagoev and Y. Terziev, "Hybrid VoIP Solution to Address Regional ISP Challenges," 2025 6th International Conference on Communications, Information, Electronic and Energy Systems (CIEES), Ruse, Bulgaria, 2025, pp. 1-6, doi: 10.1109/CIEES66347.2025.11300241.
2. **Iliev, Il.,** Blagoev I., Centralized Parallel Computing as a Cloud Service for Solving Digital Transformation Problems in Smart Cities. 2023 4th International Conference on Communications, Information, Electronic and Energy Systems (CIEES), IEEE, 2023, DOI:10.1109/CIEES58940.2023.10378756, 1-1-4-4
3. **Iliev, I.**, **Blagoev, I.**, An Approach to Improve Web Video Streaming Security and Prevent Personal Data Leakage. Information & Security: An International Journal, 53, 1, Procon, 2022, ISSN:1314-2119, DOI:10.11610/isij.5306, 78-88
4. Blagoev, I., Balabanov, T., **Iliev,** I. RSA Weaknesses Caused by the Specifics of Random Number Generation. Information & Security: An International Journal, 50, 2, Procon Ltd., 2021, ISSN:0861-5160, DOI:10.11610/isij.5028, 171-179, 2021
5. Blagoev, I., Balabanov, T**., Iliev,** I. The Randomness in Shared Web Hostings. Extended Abstracts of 16th Annual Meeting of the Bulgarian Section of SIAM, Fastumprint, 2021, ISSN:1313-3357, 9-10
6. Iliev, I., Blagoev, I. Security Considerations and Techniques for Video Streaming Distribution in Home ISPs (International Conference on Electronics, Engineering Physics and Earth Science (EEPES 2026) which will be held on 24th-27th June, 2026 in Bandirma, Turkey).

PARTICIPATION IN PROJECTS

National Research Programme "Security and Defence" (NRP SD).

RECORDED CITATIONS

Iliev, I., Blagoev, I., An Approach to Improve Web Video Streaming Security and Prevent Personal Data Leakage. Information & Security: An International Journal, 53(1), Procon, 2022, DOI: 10.11610/isij.5306. 78-88

Cited in:

1. Daniela Borissova, Milena Bankovska, Katia Rasheva-Yordanova, Zornitsa Dimitrova, Multicriteria Model for Evaluation of Learning Management Systems, WSEAS Transactions on Business and Economics, 2025, DOI: 10.37394/23207.2025.22.101.
2. Yinka Akintunde Fagbile, Nollywood, Film Streaming, and Ethical Practices, Integral Research, Vol. 02, No. 03, 2025.

BIBLIOGRAPHY

1. Julian Jang-Jaccard and Surya Nepal, “A survey of emerging threats in cybersecurity,” Journal of Computer and System Sciences 80, no. 5 (2014): 973-993.
2. Georgi Kostadinov and Tatiana Atanasova, “Security Policies for Wireless and Network Infrastructure,” Problems of Engineering Cybernetics and Robotics 71 (2019): 14-19.
3. Kristina Dineva and Tatiana Atanasova, “Regression Analysis on Data Received from Modular IoT System,” 33rd Annual European Simulation and Modelling Conference ESM’2019, Palma de Mallorca, Spain, December 2019.
4. Velizar Shalamanov, Vladimir Monov, Ivaylo Blagoev, Silvia Matern, Gergana Vassileva, and Ivan Blagoev, “A Model of ICT Competence Development for Digital Transformation,” Information & Security: An International Journal 46 (2020): 269-284, https://doi.org/10.11610/isij.4619.
5. David F. DiCarlo, “Random Number Generation: Types and Techniques,” Theses (Liberty University, Center for Computer and Information Technology, 2012).
6. James Carr, “Simple Random Number Generation,” Computers & Geosciences 29, no. 10 (2003): 1269-1275, https://doi.org/10.1016/j.cageo.2003.07.002.
7. Pierre L’Ecuyer, “Random Number Generation,” in Handbook of Simulation: Principles, Methodology, Advances, Applications, and Practice, edited by James E. Gentle, Wolfgang Karl Härdle, and Yuichi Mori (Berlin, Heidelberg: Springer, 2007), https://doi.org/10.1007/978-3-642-21551-3_3.
8. Andrew Jin, David Ling, and Alwyn Goh, “Biohashing: Two factor authentication featuring fingerprint data and tokenised random number,” Pattern Recognition 37 (2004): 2245-2255.
9. Carmen Camara, Honorio Martín, Pedro Peris-Lopez, and Muawya Aldalaien, “Design and Analysis of a True Random Number Generator Based on GSR Signals for Body Sensor Networks,” Sensors 19, no. 9 (2019): 2033, https://doi.org/10.3390/s19092033.
10. Salih Ergün, “Security analysis of a chaos-based random number generator for applications in cryptography,” 15th International Symposium on Communications and Information Technologies (ISCIT), Nara, Japan, 2015, 319-322, https://doi.org/10.1109/ISCIT.2015.7458371.
11. Boris Ryabko, Jaakko Astola, and Mikhail Malyutov, Compression-Based Methods of Statistical Analysis and Prediction of Time Series (Cham, Switzerland: Springer International Publishing, 2016).
12. D. J. Bernstein, Y.-A. Chang, C.-M. Cheng, L.-P. Chou, N. Heninger, T. Lange, and N. van Someren, “Factoring RSA Keys from Certified Smart Cards: Coppersmith in the Wild,” in Advances in Cryptology – ASIACRYPT 2013 (Proceedings, Part II), K. Sako and P. Sarkar, eds., Lecture Notes in Computer Science, vol. 8270, Bengaluru, India, Dec. 1–5, 2013, pp. 341–360. Springer, Berlin, Heidelberg, 2013, doi: 10.1007/978-3-642-42045-0_18.

13. Nadia Heninger, Zakir Durumeric, Eric Wustrow, and J. Alex Halderman, “Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices,” 21st USENIX Security Symposium, Bellevue, WA, Aug. 8–10, 2012, pp. 205-220.
14. V. Shoup, “Lower Bounds for Discrete Logarithms and Related Problems,” in Advances in Cryptology — EUROCRYPT ’97, W. Fumy, ed., Lecture Notes in Computer Science, vol. 1233, pp. 256–266, Springer, 1997, doi: 10.1007/3-540-69053-0_18.
15. Kessler, Gary C. “Protected AIS: A Demonstration of Capability Scheme to Provide Authentication and Message Integrity.” TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation (2020).
16. Synopi. “RTMP streaming process diagram.” Available at: https://synopi.com/.
17. SSL.com Support Team. “SSL/TLS Best Practices for 2023.” Available at: https://www.ssl.com/guide/ssl-best-practices/.
18. John Paul Mueller, Security for Web Developers: Using JavaScript, HTML, and CSS, 2015, ISBN-13:978-1491928646.
19. M.A. Erskine, D.G. Gregg, J. Karimi, and J.E. Scott, “Business Decision-Making Using Geospatial Data: A Research Framework and Literature Review,” Axioms 3 (2014): 10-30, https://doi.org/10.3390/axioms3010010.
20. R. Wickramasuriya, J. Ma, M. Berryman, and P. Perez, “Using geospatial business intelligence to support regional infrastructure governance,” Knowledge-Based Systems 53 (2013): 80-89, https://doi.org/10.1016/j.knosys.2013.08.024.
21. S. Rivest, Y. Bédard, M.-J. Proulx, M. Nadeau, F. Hubert, and J. Pastor, “SOLAP technology: Merging business intelligence with geospatial technology for interactive spatio-temporal exploration and analysis of data,” ISPRS Journal of Photogrammetry and Remote Sensing 60, no. 1 (2005): 17-33, https://doi.org/10.1016/j.isprsjprs.2005.10.002.
22. J. de Castro Lima, Computing Data Cubes Over GPU Clusters, Monografia, Federal University of Ouro Preto, Institute of Exact Sciences and Biology, Undergraduate Program in Computer Science, December 2018. Available at: https://www.monografias.ufop.br/bitstream/35400000/1527/6/MONOGRAFIA_ComputingDataCubes.pdf
23. Yakov Rekhter, Susan Hares, and Tony Li, “A Border Gateway Protocol 4 (BGP-4),” RFC 4271, January 2006, doi:10.17487/RFC4271.
24. Arun Viswanathan, Eric C. Rosen, and Ross Callon, “Multiprotocol Label Switching Architecture,” RFC 3031, January 2001, doi:10.17487/RFC3031.

25. Petar Maymounkov and David Mazières, “Kademlia: A Peer-to-Peer Information System Based on the XOR Metric,” in Revised Papers from the First International Workshop on Peer-to-Peer Systems (IPTPS ’01), Springer-Verlag, Berlin, Heidelberg, 2002, pp. 53–65.
26. Zwicklhuber, T., and M. Kaufmann, “EURIS (European River Information Services System) – The Central European RIS Platform: Introducing a Joint RIS System Among 13 European Countries,” in Li, Y., Hu, Y., Rigo, P., Lefler, F. E., and Zhao, G., eds., Proceedings of PIANC Smart Rivers 2022, Lecture Notes in Civil Engineering, vol. 264, Springer, Singapore, 2023, pp. 850–856, doi:10.1007/978-981-19-6138-0_75.
27. Ministry of Transport and Communications. "Bulgaria and Romania with a common regime for ship inspections on the Danube." 22.02.2018. Available at: https://www.mtc.government.bg/en/category/1/bulgaria-and-romania-common-regime-ships-inspections-danube
28. Ministry of Regional Development and Public Works. "A modern system will monitor pollution of the Danube from ships." 23.03.2026. Available at: https://www.mrrb.bg/bg/moderna-sistema-ste-sledi-za-zamursyavane-na-dunav-ot-korabi/.