AUDIT@eduroam: A Security Auditing Tool for the eduroam Infrastructure

Fabiano Losilla de Carvalho[1,2], **Luciana Pereira Oliveira**[1], **Erick Lazaro Melo**[2]

[1]Instituto Federal da Paraíba (IFPB) – Campus João Pessoa
Av. Primeiro de Maio, 720 – 58015-435 – João Pessoa – PB – Brazil

[2]Universidade Federal de São Carlos (UFSCar)
Rodovia Washington Luís, km 235 – 13565-905 – São Carlos – SP – Brazil

fabiano@ufscar.br, luciana.oliveira@ifpb.edu.br, erick@ufscar.br

Abstract. *The eduroam federation enables global academic mobility through IEEE 802.1X and RADIUS standards. However, non-compliance with RFC 7593 leaves user credentials vulnerable. To address this, AUDIT@eduroam introduces a three-stage automated framework: (1) data acquisition, (2) static client-side analysis of CAT profiles, and (3) dynamic server-side verification via RADIUS logs. Validation across 148 IdPs over three execution cycles revealed that theoretical compliance (39.86%) drops to just 2.70% in dynamic tests, with 81.08%-83.11% of institutions failing due to expired certificates and identity exposure. These findings underscore a state of insecurity within the infrastructure, highlighting the need for continuous, automated monitoring of the network.*

1. Introduction

Eduroam (education roaming) is a highly successful global federated Wi-Fi service designed specifically for the international research and education community. It enables students, researchers, and staff to securely access the internet at any participating institution worldwide simply by using the authentication credentials provided by their home organization. Since its inception, eduroam has expanded to a vast global scale, operating in over 100 countries and territories and facilitating millions of daily authentications across thousands of universities, research centers, and educational spaces, thereby becoming a fundamental infrastructure for global academic mobility.

The prominence of eduroam as the premier academic federated access solution is largely due to its foundational reliance on the IEEE 802.1X standard, the Extensible Authentication Protocol (EAP), and the RADIUS infrastructure. Consequently, the network benefits from the most robust encryption and authentication mechanisms available today.

Furthermore, eduroam's technical standard, RFC 7593 (The eduroam Architecture for Network Roaming), establishes strict security guidelines. These include verifying the server's identity via a Certificate Authority (CA), utilizing strong encryption for the RADIUS transport payload, and protecting user identity through pseudonymization [Wierenga et al. 2015].

However, practical experiments conducted within universities reveal significant challenges regarding adherence to the security recommendations outlined in RFC 7593 [Batista et al. 2025, Batista et al. 2024, Palamà et al. 2023, Palamà et al. 2022]. The study in [Batista et al. 2025] demonstrates that even in European countries—where

eduroam was originally conceived and technical maturity is generally higher—challenges in meeting these guidelines persist.

Recurring issues such as the failure to define an *Outer Identity*, incorrect EAP-TTLS/PEAP configurations, and the lack of proper server certificate validation are frequent causes of personal data leaks and Man-in-the-Middle (MitM) vulnerabilities [Batista et al. 2025, Daldoul and Berrima 2025, Oliveira and Silva 2024, Batista et al. 2024, Dekkar and Fiore 2021, Lima et al. 2021, Petrosyan et al. 2019].

Furthermore, compromised data can be exploited to breach sensitive academic systems or to orchestrate targeted social engineering attacks against users and their respective Identity Providers (IdPs). Because these exposures stem from preventable configuration weaknesses, they often constitute direct violations of stringent global data protection frameworks, such as the European General Data Protection Regulation (GDPR) and other equivalent national laws like the Brazilian LGPD.

These factors reinforce that eduroam's security depends not only on its underlying technology but also on the operational and organizational compliance of each participating IdP [Batista et al. 2025].

In light of this, the literature strongly emphasizes the fundamental importance of continuous auditing and monitoring within the eduroam network to ensure data security and identify vulnerabilities [Batista et al. 2025, Orús Comabella 2025, Batista et al. 2024, Júnior et al. 2024].

Current GÉANT monitoring focuses on the operational status of international and national servers, classifying reachability—via valid credentials—into states such as OK, Possible Problems, Wrong Response, or No Response [GEANT 2009]. However, this approach often excludes local IdPs and overlooks nuanced configuration vulnerabilities that compromise the privacy, trust, and integrity of end users.

To address the gap between theoretical security and practical implementation, this paper presents **AUDIT@eduroam**[1] . Grounded in the security directives of RFC 7593, this tool performs rigorous compliance audits using a tri-level qualitative classification system (APPROVED, AT RISK, and FAILED). The assessment methodology is systematically organized across three core pillars: (1) Trust, (2) Privacy, and (3) Integrity.

The proposed auditing framework operates in three sequential phases: (1) automated data acquisition and consolidation, which involves retrieving the list of IdPs and their respective eduroam Configuration Assistant Tool (CAT) profiles; (2) static auditing (client-side evaluation), which assesses the security parameters within the recommended eduroam CAT profiles [GÉANT 2011]; and (3) dynamic auditing (server-side evaluation), which analyzes RADIUS server logs produced by active authentication requests via the *eapol_test* utility. To empirically validate AUDIT@eduroam, this methodology was applied across three execution cycles to extract data and conduct security audits on all 148 Brazilian institutions registered in the eduroam CAT service.

It is important to emphasize that while the empirical validation was conducted exclusively within the Brazilian national network, this deployment serves primarily as a proof-of-concept. Because the framework's architecture is highly automated and re-

[1]Software registration currently in progress at the UFSCar Innovation Agency (AIn UFSCar).

lies on globally standardized data models provided by the eduroam CAT portal, AUDIT@eduroam is entirely geographically agnostic. Theoretically, the tool possesses the inherent capability to scale globally, enabling systematic compliance and security audits for any participating eduroam institution worldwide.

2. Theoretical Foundation and Related Work

The eduroam infrastructure is based on the IEEE 802.1X standard, a port-based network access control protocol involving three main actors, as illustrated in Figure 1: the supplicant (*Client*), the authenticator (*Access Point*), and the authentication server (*Home RADIUS*) [Wang et al. 2022].

The authentication process is divided into two phases. Phase 1, referred to as the *Outer Tunnel*, utilizes methods such as PEAP (*Protected* EAP) or EAP-TTLS (*Tunneled* TLS) to establish an encrypted TLS tunnel between the supplicant and the home authentication server [Daldoul and Berrima 2025].

Authentication traffic traverses a global hierarchy of servers until it reaches the user's home IdP [Yang et al. 2025, Palamà et al. 2022]. As shown in Figure 1, the process begins at Step 1, with traffic originating from the *Client* towards the *Access Point*. Next, in Step 2, the request is forwarded to the RADIUS server of the visited IdP network. In Step 3, the traffic is routed internationally until it reaches the *Home RADIUS* server of the destination IdP, which responds by sending its digital certificate back to the *Client*.

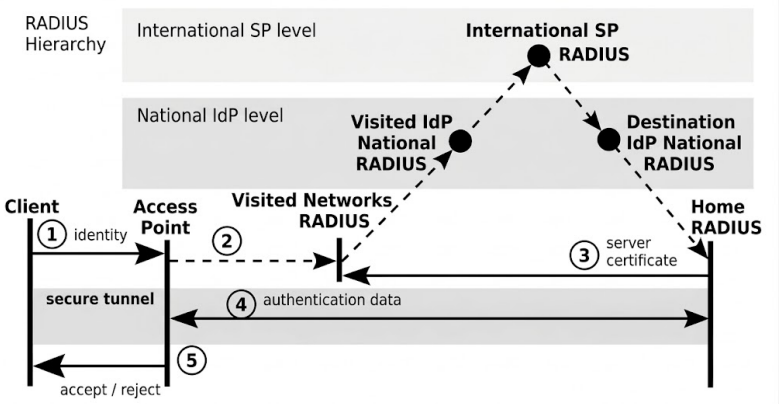

Figure 1. eduroam Infrastructure. Adapted from [Palamà et al. 2022]

The primary objective of this phase is to protect user credentials from network observers and allow the device to validate the identity of the *Home RADIUS* server via an X.509 digital certificate, verifying its validity and Subject Alternative Name (SAN) [Wang et al. 2022, Wierenga et al. 2015]. Furthermore, the user's real identity must remain hidden through the use of an *Outer Identity* [Batista et al. 2025, Wierenga et al. 2015].

Once the encrypted Phase 1 tunnel is established, Phase 2 begins. This phase, known as the *Inner Phase*, executes Step 4 of Figure 1 using MSCHAPv2 or PAP (*Password Authentication Protocol*). During this stage, the user's real identity (*Inner Identity*) and access credentials are transmitted [Daldoul and Berrima 2025].

In the case of MSCHAPv2, mutual authentication occurs between the *Client* and the *Home RADIUS*, followed by the transmission of a hash [Batista et al. 2025]. Conversely, PAP transmits the password in plaintext [Daldoul and Berrima 2025]. Both protocols are recommended by RFC 7593 [Wierenga et al. 2015]. Finally, in Step 5, the access request yields either an *accept* or a *reject* message.

Without adherence to the RFC 7593 security guidelines, eduroam becomes susceptible to various attack vectors. To mitigate these risks, it establishes five fundamental directives:

1. Server identity verification;
2. CA validation;
3. Strong payload encryption in RADIUS transport;
4. EAP server validation mitigation;
5. Prevention of user identifier exposure (pseudonymization).

To analyze the state-of-the-art and justify the approach of this research, related works were categorized by mapping these directives into three analytical pillars proposed by this study: **Trust**, **Privacy**, and **Integrity**.

2.1. The Trust Pillar (Directives 1, 2, and 4)

Trust relies on ensuring the user communicates with the legitimate IdP server. [Daldoul and Berrima 2025] address this challenge by proposing the *Robust Certificate Management System* (RCMS) to prevent evil twin attacks. They highlight that 802.1X lacks a practical method for users to validate the network certificate—a vulnerability RCMS aims to correct. Within the scope of identity validation, researchers in [Wang et al. 2022] emphasize checking the SAN and hostname on the supplicant side to prevent redirection to malicious domains.

Regarding the assurance of legitimate certificates via CAs, [Batista et al. 2025] emphasize the necessity of configurations tied to recognized entities (such as ICPedu in Brazil), while [Lima et al. 2021] propose the automatic installation of root certificates via a PAM module, mitigating user negligence. Furthermore, the research in [Goto 2025] advocates for the use of robust cryptographic parameters, such as HMAC and ECDH, to protect attributes in transit.

In a similar vein, [Rieckers 2021] identified inconsistencies in TLS implementations, and [Turner and Woodward 2006] historically pointed out the challenges of PKI management. While these works propose technical solutions or localized passive analyses, the present research focuses on actively verifying the real-world adoption of these practices (correct use of CAs, hash algorithms, and server validation) through eduroam CAT profiles.

2.2. The Privacy Pillar (Directive 5)

Privacy ensures that the user's identity is not exposed during Phase 1 authentication. [Batista et al. 2025] demonstrated that passive attacks could compromise the credentials of more than a third of the students evaluated at a Portuguese university due to a lack of pseudonymization.

Complementing this, [Batista et al. 2024] reinforce the mandatory nature of verifying and populating the *Outer Identity* to prevent the transmission of the real identifier.

Alternatively, [Okabe et al. 2024] suggests using a Chargeable User Identity (CUI) encrypted with AES128GCM for traceability without exposure, and [Caballero et al. 2016] propose implementing SAML pseudonyms generated by the home IdP.

Similarly, [Mazhar et al. 2021] analyzed thousands of institutions globally and revealed that 86% of the networks exhibited credential-capture vulnerabilities. Unlike these approaches, which focus on vulnerability exploitation or alternative infrastructures, this paper proposes the AUDIT@eduroam tool to proactively audit IdP configurations, verifying the mandatory use of the *anonymous* identifier.

2.3. The Integrity Pillar (Directive 3)

Integrity refers to the use of robust encapsulation and authentication methods to protect the RADIUS payload. The study by [Orús Comabella 2025] details the implementation of an autonomous server, highlighting the importance of EAPOL testing to validate the resilience of protocols like PEAP-MSCHAPv2.

To ensure communication integrity, [Daldoul and Berrima 2025] uses RCMS to confront verification codes and validate server matching, while [Palamà et al. 2023] warns of the need to monitor downgrade attempts to insecure methods.

In terms of alternative infrastructures, [Ahmed et al. 2020] suggest replacing traditional RADIUS transport with Blockchain and Intel SGX to protect logs in intermediate proxies, whereas [Oliveira and Silva 2024] implement N3IWF functions in the 5G Core to ensure RADIUS/EAP traffic is encapsulated in highly secure IPsec tunnels. The contribution of these studies is technical and prospective; in contrast, this research aims to dynamically audit authentication logs to verify whether the cryptographic and encapsulation methods suggested by standards are actually being enforced by IdPs.

Beyond strictly technical pillars, the literature highlights that infrastructure security is intrinsically linked to operational and institutional management challenges. The authors of [Dekkar and Fiore 2021] discuss the expansion of eduroam in Africa led by National Research and Education Networks (NRENs)—a context highly similar to the role played by RNP in Brazil. In the national scenario, [Torres et al. 2025] address the difficulty of configuration on mobile devices, reporting the development of a proprietary app by RNP to mitigate manual errors, while also proposing Quality of Service (QoS) monitoring architectures.

Overall, the analyzed studies show that eduroam's effectiveness depends as much on protocol robustness as on institutional compliance [Batista et al. 2025]. This paper differentiates itself precisely by systematically connecting these technical dimensions (Trust, Integrity, and Privacy) to operational reality. To bridge this gap, the AUDIT@eduroam tool is proposed, which is capable of actively evaluating the security maturity of institutions against RFC 7593.

3. The AUDIT@eduroam Tool

The AUDIT@eduroam tool was designed as an automated orchestration system, developed in Python, aimed at extracting data and auditing the eduroam service. To enable processing and technical analysis, the tool leverages the following libraries: *Selenium* and *Webdriver Manager* for web automation and dynamic driver management; *Pandas*

for data manipulation and structuring; and *Cryptography* for certificate security diagnostics.

Figure 2 illustrates the division of AUDIT@eduroam into three main modules: (1) the Orchestrator Module; (2) the Data Module (collection and preparation); and (3) the Audit Module (subdivided into static and dynamic auditing). These components are detailed in Sections 3.1, 3.2, and 3.3.

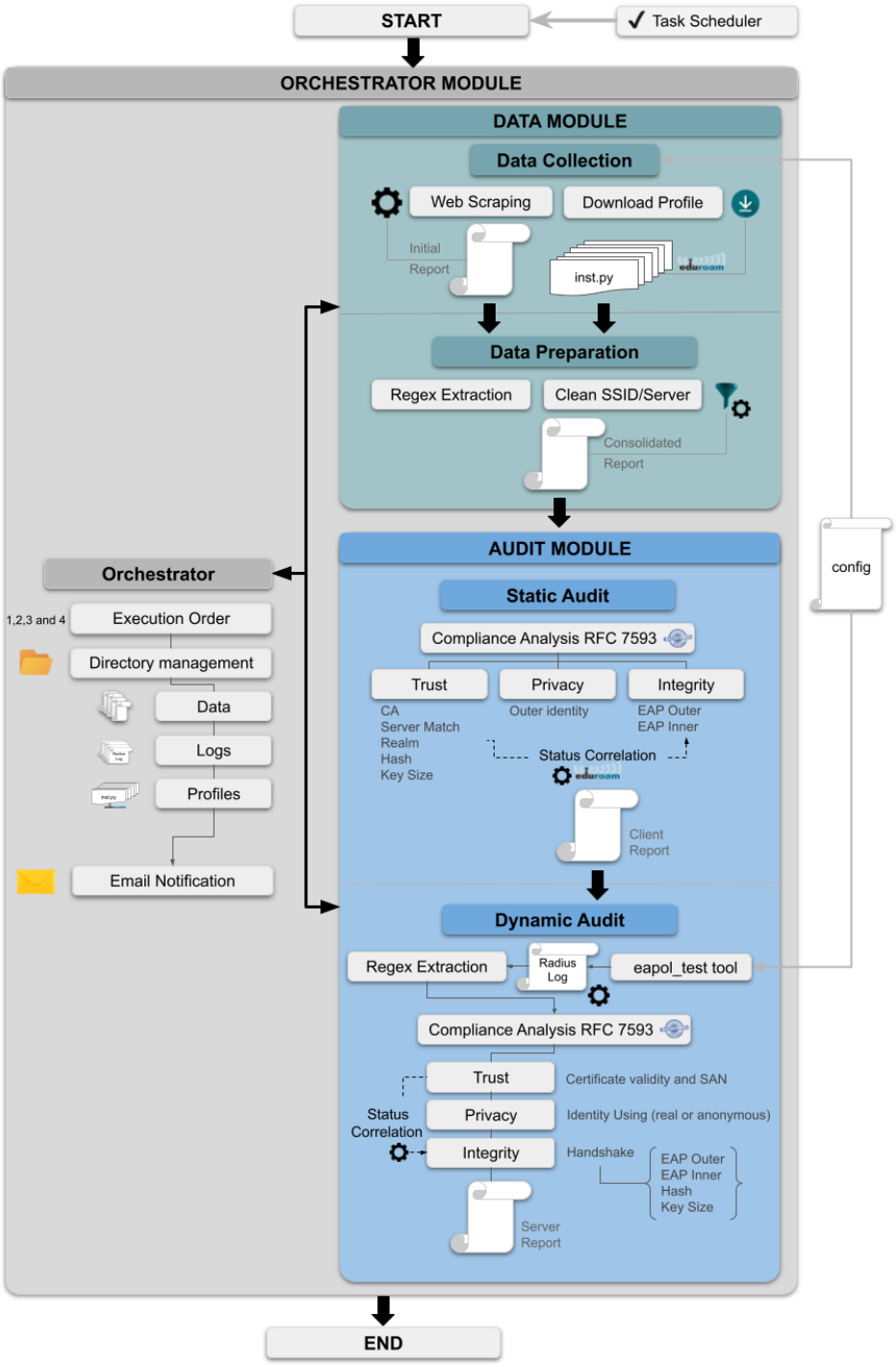

Figure 2. Operational Flow of the AUDIT@eduroam System

3.1. Orchestrator Module

The Orchestrator Module acts as the central intelligence and execution engine of AUDIT@eduroam, responsible for managing the complete lifecycle of large-scale audits. Its primary function is to coordinate transitions between system phases, eliminating the need for manual intervention by network administrators during intermediate steps and ensuring a strictly sequential and resilient workflow.

Upon initialization, the Orchestrator invokes the Data Module (Section 3.2), which provides the knowledge base required for the audit. The interaction between these modules is dynamic: the Orchestrator not only executes collection processes but also governs data persistence in directories defined via configuration parameters. This architecture allows the system to organize resulting artifacts—such as compliance reports, event logs, and institutional configuration profiles—in a logical and traceable manner.

To ensure the historical integrity of the diagnostics, the Orchestrator manages the local file system by creating an exclusive repository identified by a timestamp for each new execution. This allows past audits to be consulted for comparative security evolution analyses. Finally, the module integrates with the *Postfix* Mail Transfer Agent (MTA), automating administrator notifications regarding the operation's outcome, sending alerts for both successful completions and critical failures.

3.2. Data Module

This module contains the automation logic for acquiring eduroam CAT profiles and the intelligence for extracting metadata. The process begins by interacting with the eduroam CAT portal, a complex interface operating under a selection hierarchy (country $\rightarrow$ institution $\rightarrow$ profile) that utilizes Client-Side Rendering (CSR) technology. In such systems, the interface state and control elements—like the 'Continue' button, *profile_id* selectors, and profile redirects—are dynamically generated via scripts and event listeners, making traditional web scraping inefficient.

To overcome this technical barrier and ensure system resilience, the module uses structured JSON files that pre-map the list of countries and IdPs (Figure 3). This strategy allows AUDIT@eduroam to bypass the complexity of asynchronous visual navigation, directly generating profile download links and monitoring their capture. The obtained files are automatically renamed following the standardization $[ID_{inst}]Name[ID_{profile}] - eduroam.py$, which is crucial for the Orchestrator to maintain traceability between the technical file and the originating institution during subsequent phases.

Operational flexibility is a cornerstone of this module. Through a centralized configuration file, the administrator can define the audit scope via the *country_code* variable (allowing specific countries or the global database to be audited using the *all* parameter) and, crucially, fully customize the output directory tree. This parameterization ensures AUDIT@eduroam can be deployed across different server architectures without path or permission conflicts.

Additionally, the module manages the technical parameters of the RADIUS server (IP/FQDN, ports, and shared secrets) and the testing credentials. It is important to note that the validation of the Trust, Privacy, and Integrity pillars occurs during the handshake and the initiation of EAP Phase 2. This guarantees a technical audit without requiring real

Country Mapping

```
{"BR": {"name": "Brasil",
        "mainland": "América do Sul"}}
```

Institution Data (IdPs)

```
[{ "mainland": "América do Sul",
   "id_country": "BR",
   "country_name": "Brasil",
   "id_idp": "Code IdP",
   "idp_name": "Institution Name",
   "id_profile":"Code Profile" }]
```

Figure 3. Data structure extracted from the eduroam CAT interface.

user credentials. Upon completing its execution, this module generates a consolidated CSV report containing download statistics and reasons for any omissions, alongside the list of captured profiles and their respective execution logs. This logging procedure is replicated across all subsequent stages of AUDIT@eduroam, ensuring total transparency and traceability throughout the audit.

3.2.1. Data Preparation

Data Preparation acts as a sanitation bridge between collection and auditing. The system iterates through the initial report and extracts critical parameters from the downloaded profiles, such as: *server_match* (expected SAN), EAP methods (*Outer* and *Inner*), *user_realm*, pseudonymization (*anonymous_identity*), and CA certificates. The use of regex during this phase cleans inconsistent fields, resulting in a consolidated report that serves as the input for the audit engine.

3.3. Audit Module

To systematize Audit Module, the AUDIT@eduroam analysis engine was structured into three dimensions (Trust, Privacy, and Integrity) aligned with RFC 7593 guidelines. A key differentiator of the tool is the correlated Integrity analysis (indicated by the dashed line in Figure 2), which subordinates its approval status to the robustness of the Trust parameters.

3.3.1. Static Audit

Once Data Preparation is complete, the consolidated report is passed to the Audit Module, instantiating the Static Audit. In this phase, the client side (CAT profile) is evaluated. The consolidated report is read, and the iteration to evaluate each IdP begins. The creation of a control set for duplicate IdP registrations was necessary to avoid repeated analyses—such duplicates receive a DISCARDED classification. Furthermore, the Trust, Privacy, and Integrity pillars are initially set to APPROVED.

To evaluate the Trust pillar, technical parameters are first extracted, as shown in Figure 2. The *cryptography* library is used to read the CA text and expiration date. Subsequently, it verifies if the *Server Match* is a valid FQDN and contains the IdP's *Realm*. If criteria are unmet, Trust is classified as FAILED, and the reason is logged.

Still regarding the Trust pillar, the NIST security standard (SP 800-78-5) dictates that to ensure the integrity and authenticity of X.509 and CA certificates supporting the PIV system, cryptographic keys and hashes capable of maintaining a security strength of at least 112 bits must be used until the end of 2030. Therefore, the use of the *Rivest-Shamir-Adleman* (RSA) cryptographic algorithm with key sizes of 2048, 3072, or 4096 bits and a SHA-256 or SHA-384 hash algorithm, or the *Elliptic Curve Digital Signature Algorithm* (ECDSA) with curve P-256 and SHA-256 hash, or curve P-384 with SHA-384 hash [Ferraiolo and Regenscheid 2024], are recommended.

Following NIST recommendations, the Hash and Key Size defined in the CA are evaluated. They are extracted from the CA text and verified. Both the use of legacy hashes (SHA-1) and the use of short keys (under 2048 for RSA or under 256 for ECDSA) downgrade Trust to AT RISK if it was previously set to APPROVED.

The Privacy pillar focuses on evaluating the *Outer Identity*. The absence of a definition for this field results in an AT RISK classification, since lacking a pseudonym leads to the exposure of the user's real identity before a secure tunnel is established. "Conversely, using identities with a formatted string that does not contain the '@' character results in a FAILED classification, as it compromises the routing of Phase 1 EAP authentication when the user is roaming. Otherwise, the initial APPROVED value is maintained.

The final pillar, Integrity, is evaluated according to the systematic approach illustrated in Figure 2. First, the *EAP Outer* technical parameter is extracted and checked against RFC 7593 definitions. If the configured protocol deviates from EAP-TLS, EAP-TTLS, or PEAP, the pillar remains APPROVED.

Next, the *EAP Inner* is extracted for a correlation analysis with the Trust parameters (CA expiration date, Identity compliance via *Server Match* and *Realm*, as well as Hash and Key Size). This approach ensures the robustness of internal authentication is consistent with the protection provided by the TLS tunnel. The decision logic follows these guidelines:

- **APPROVED**: If the EAP-TLS method is used, or if MSCHAPv2 and PAP methods are in full compliance with RFC 7593 and NIST cryptographic standards (SP 800-78-5).
- **AT RISK**: If the authentication methods are recommended by RFC 7593, but the supporting cryptographic parameters (Hash or Key Size) do not meet the security strength levels required by the NIST standard (SP 800-78-5).
- **FAILED**: If legacy authentication methods (such as MD5 or GTC) are used, or if the Phase 2 method (MSCHAPv2 or PAP) operates over a compromised trust infrastructure (expired CA or server Identity failure).

The results are consolidated into the client report, integrating the Static Audit data with the preparation phase records. Additionally, the log file synthesizes the Trust, Privacy, and Integrity statuses alongside the analyzed technical values. This storage structure allows the administrator to conduct a detailed audit, tracing everything from the minutiae of intermediate processes to the final compliance diagnosis of each IdP.

3.3.2. Dynamic Audit

Once the Static Audit concludes, the Orchestrator instantiates the Dynamic Audit, which actively interacts with the eduroam infrastructure. This module executes RADIUS connection tests and extracts EAPOL logs to elaborate the final diagnosis of the Trust, Privacy, and Integrity pillars. As in the previous stage, the pillars and the final security status of the IdP are classified as APPROVED, AT RISK, or FAILED.

The Dynamic Audit begins by configuring the access credentials to the RADIUS server, enabling the operation of the EAPOL tool. The system reads the report generated in the Static Audit and ignores IdPs previously marked as DISCARDED. For the remaining IdPs, the test begins by retrieving the attributes from the eduroam CAT profile (*CA*, *EAP Outer*, *EAP Inner*, *Realm*, and *Outer Identity*), followed by the creation of temporary configuration files (*ca.pem* and *profile.conf*).

After executing the EAPOL test, the system applies regex methods to the generated logs to populate a data dictionary that maps:

1. Identity utilized - verifies whether the identifier is *anonymous* or *real*;
2. *CA* validation - confirms if the CA was read and the certificate chain validated (*chain*);
3. Connectivity - attests whether communication with the RADIUS server is operational;
4. *Handshake* - captures the success of the negotiation or the error that occurred;
5. The certificate signature algorithm - *Hash*, public key algorithm, certificate key size (*Key Size*), and the TLS version;
6. The certificate expiration date;
7. The server's *Subject Alternative Name* (SAN).

Once the dynamic data is mapped into the system's dictionary, the AUDIT@eduroam engine employs a structured decision matrix to assess the IdP's security posture. To ensure a systematic classification, result validation occurs across three hierarchical levels:

- **Level 1 (Cryptography):** evaluates *Hash*, *Key Size*, public key algorithm, and TLS version attributes against the guidelines of NIST SP 800-78-5 and NIST SP 800-52r2 (establishes guidelines for the selection, configuration, and use of TLS) [McKay and Cooper 2019]. Evaluation values can be APPROVED or AT RISK
- **Level 2 (Connectivity and Identity):** verifies whether the loaded CA has a valid *chain*, checks the temporal validity of the server certificate, and confirms if the expected *Server Match* is present in the provided SAN list. Evaluation values for this level can be be APPROVED or FAILED
- **At Level 3 (Pillar Decision)**, evaluation of Trust, Privacy, and Integrity is performed. Just as in the Static Audit, the qualitative result can be APPROVED, AT RISK, or FAILED.

At the final stage of the evaluation framework (Level 3), the system synthesizes the technical findings from the previous tiers to formulate a definitive qualitative verdict for each of the three foundational security pillars. The specific logical conditions for assigning the final status—APPROVED, AT RISK, or FAILED—are defined as follows:

- **Trust**: The classification depends on the connectivity and identity criteria (Level 2) being met. If all receive an APPROVED value, the final evaluation of this pillar depends on the cryptographic robustness obtained in hierarchical Level 1. Otherwise, the classification drops to FAILED.
- **Privacy**: Classified as AT RISK if the real identity is exposed or if the *Outer Identity* is undefined. It receives a FAILED value if there is an error in constructing the username (e.g., absence of the '@' character). An APPROVED classification requires the correct use of the defined pseudonym.
- **Integrity**: Evaluates whether the EAP methods adhere to RFC 7593 and if the *handshake* was successful. Approval of this pillar is conditional upon its correlation with the Trust pillar. Certificate or server identity failures result in a FAILED status, while purely cryptographic weaknesses result in AT RISK. Otherwise, the classification remains APPROVED.

The Final IdP Verdict consolidates the obtained diagnostics. The APPROVED classification is strictly reserved for institutions that demonstrated total compliance across all pillars in both audits (static and dynamic). The AT RISK status is assigned when there is at least one 'Warning' classification, provided there are no critical failures. Finally, the FAILED classification is mandatory if any pillar, in any phase, fails.

3.4. Ethical Considerations

Regarding ethical considerations, active probing during dynamic auditing rigorously replicates the behavior of a typical, legitimate user authenticating on the federated network. The evaluation is limited to standard protocol negotiation and certificate validation (TLS handshake), without the use of exploits or intrusive techniques. Furthermore, the audit process does not intercept, collect, or store any personally identifiable information (PII) or user credentials; the evaluation is strictly restricted to the metadata, configurations, and certificates of the institutional infrastructure.

Regarding the disclosure of identified vulnerabilities, the findings of AUDIT@eduroam will be formally reported to the Brazilian National Research and Educational Network (RNP), the national body responsible for the eduroam federation in Brazil. RNP maintains direct operational relationships with every participating IdP, making it the most effective channel to notify institutions and coordinate the necessary corrections. Additionally, the findings will be reported to the Federal Government's Cyber Incident Response Team (CTIR Gov), given that the majority of the audited institutions are federal public universities. This disclosure strategy ensures that the vulnerabilities identified reach the bodies with the authority and reach to drive effective remediation across the national academic network

4. Results and Discussion

The experimental audits were conducted on July 26, 2026, focusing exclusively on Brazilian Research and Education Institutions (country filter 'BR'). Across three execution cycles -— (1) from 10:43:35 to 11:03:32, (2) from 12:43:01 to 13:03:24, and (3) from 14:43:01 to 15:03:26 — the complete audit pipeline was executed successfully. The AUDIT@eduroam tool enabled a systematic analysis of the national infrastructure, demonstrating the feasibility of performing periodic, comprehensive audits that would be impractical using manual methods.

During the collection and preparation phases, the tool successfully processed 151 IdP records identified by the geographic filter. The data module retrieved 100% of the available eduroam CAT profiles for these institutions, consolidating a robust database for the subsequent stages. In the Static Audit phase, three IdPs were marked as DISCARDED—both due to a lack of configured profiles in eduroam CAT. This resulted in a net sample of 148 audited institutions.

It is important to highlight that the results of the Static Audit are fully replicable from the primary data provided. In contrast, the Dynamic Audit, by its empirical nature, portrays the operational state of the infrastructure at the exact moment of its execution, and may present variations in case of new tests (due to network instabilities or server updates). Nevertheless, all reports, logs, and profiles extracted during the simulations guarantee the traceability of the study and can be analyzed to attest to the veracity and accuracy of the findings presented here.

4.1. Static Audit Analysis

Across all three execution cycles, the Static Audits revealed an initial discrepancy between configuration availability and the theoretical security of the profiles. Due to the logical correlation between the Trust and Integrity pillars, non-compliance in server validation directly impacted the Integrity classification. In every run, only 59 IdPs (39.86%) achieved full compliance (APPROVED) in both pillars.

In contrast, 58 institutions (39.19%) were classified as AT RISK for operating with cryptographic parameters divergent from the NIST SP 800-78-5 standard. More critical, however, is the group of 31 institutions (20.95%) classified as FAILED, which exhibited multiple critical failures, as detailed in Table 1. A critical prevalence was observed in the combination of expired certificates and legacy cryptography, affecting 17.57% of the sample (26 IdPs). Notably, weak cryptographic hashing was the most pervasive vulnerability within this group, present in 19.59% of all institutions (29 IdPs). Conversely, Server Match misconfigurations were scarce, affecting 3.38% of the sample (5 IdPs).

Table 1. Breakdown of Security Failures in Failed IdPs

Failure Combination	**IdPs**	**%**
Exp. Cert. + Inv. Crypto	26	17.57
Server Match + Inv. Crypto	3	2.03
Server Match Only	2	1.35
Total Critical Failures	**31**	**20.95**

Failure Type	**IdPs**	**%**
Hash weak	29	19.59
Expired Certificate	26	17.57
Server Match Divergent	5	3.38

Simultaneously, in the Privacy pillar, non-compliance reached critical levels: 95.27% of the institutions (141 IdPs) failed to define an *Outer Identity*, exposing the user's real identity in cleartext before the establishment of a secure tunnel.

In summary, across all three execution cycles, the Static Audit results remained consistent, revealing that compliance within the Brazilian eduroam ecosystem is largely superficial. High reliance on eduroam CAT profiles without proper technical maintenance has created a scenario where fewer than half of the institutions (39.86%) consistently meet basic "on-paper" security requirements. This latent fragility in configuration files establishes a low ceiling for the federation's security, suggesting that failures found in the

static layer are merely a prelude to the operational vulnerabilities that manifest during real client-server interactions, as detailed in the following dynamic analysis.

4.2. Dynamic Audit Analysis

The Dynamic Audit, by confronting profiles with real-time RADIUS server responses via EAPOL, exposed vulnerabilities that static analysis alone could not detect. While theoretical cappproval in the static phase stood at 39.86%, real-time handshake validation reduced Integrity pillar approval to 18.24% (27 institutions across all three audit cycles). However, approval in one pillar did not guarantee systemic security: of the 27 institutions compliant in Integrity, 23 exhibited failures in other domains.

In the Trust pillar, between 92 and 95 IdPs (62.16%–64.19%) failed due to inconsistencies in the certificate chain or identity misalignment (SAN mismatch). Privacy, with only 7 IdPs (4.73%) achieving approval, aligning closely with the static audit. All others exhibited *Inner Identity* leakage, violating RFC 7593.

The Integrity pillar recorded between 97 and 100 failures (65.54%–67.57%) across the audit runs. Connectivity issues (RADIUS Offline/Timeout) accounted for 14–17 IdPs (9.46%–11.49%). Additionally, 7 IdPs (4.73%) failed prior to execution due to missing or invalid realm definitions in their CAT profiles, which prevented credential generation for the eapol_test tool. Among active TLS handshake failures, invalid or expired CA chains constituted the primary root cause, affecting 56–57 IdPs (37.84%–38.51%), closely complemented by Subject Alternative Name (SAN) mismatches against CAT profiles in 35–36 IdPs (23.65%–24.32%).

To consolidate these multi-pillar findings into a diagnostic hierarchy based on a worst-case severity rule, the results were structured into a four-level and summarized in Table 2, which synthesizes the operational status, connectivity failures, and security non-compliances detected across all pillars of the Dynamic Audit.

Table 2. Final Audit Verdict of Brazilian IdPs (n=148)

Level	Classification	Detailed Description / Primary Findings	Qty IdPs	%
1	APPROVED	**Total Compliance (NIST/RFC):** Full compliance across security, privacy, and integrity.	4	2.70%
2	AT RISK	**Configuration Weaknesses:** Non-critical issues (cleartext Phase 1 Outer Identity exposure or deprecated static crypto) in TLS handshake.	23	15.54%
3	FAILED	**Confirmed Vulnerabilities:** Handshake or trust chain failures in EAP Phase 1 (expired certs, missing CAs, or SAN mismatches).	97–100	65.54%–67.57%
4	NETWORK	**Availability Failure:** Socket timeout or unreachable RADIUS server status.	14–17	9.46%–11.49%
5	SKIPPED	**Configuration Pre-requisite Error:** Invalid or missing realm definitions in CAT profile preventing execution.	7	4.73%
Total		**Audited Institutions (Effective Sample)**	**148**	**100.00%**

These findings highlight a systemic structural challenge: the stark discrepancy between static profiles and dynamic performance proves nominal compliance fails under active testing. Operating largely below security baselines, the infrastructure requires automated tools like AUDIT@eduroam for continuous preventive monitoring.

5. Conclusion

This work presented the AUDIT@eduroam, an automated solution designed to audit the compliance and security of Identity Providers (IdPs). The motivation for this study arose from the realization that the ease of configuration provided by tools like eduroam CAT can mask security vulnerabilities in institutional servers.

The results obtained from the audit of the Brazilian infrastructure provide relevant insights into federated network security. The discrepancy observed between the Static Audit (where 39.86% of IdPs appeared compliant) and the Dynamic Audit (where actual approval plummeted to just 2.70%) proves that passive profile analysis is insufficient. Evaluating active configurations reveals a non-compliance rate between 81.08% and 83.11% (comprising 15.54% AT RISK and 65.54%–67.57% FAILED) — driven primarily by expired certificates, Subject Alternative Name mismatches, and real identity leakage-which highlights a critical gap in the security management of participating institutions. A detailed analysis of vulnerability patterns across different institutional profiles is the subject of ongoing work and will be addressed in a forthcoming study.

The primary contribution of this study is the demonstration that federated network security requires continuous oversight rather than static setup. The AUDIT@eduroam tool proved effective in conducting systemic diagnostics that would be impossible via manual methods, confirming that security in eduroam is an ongoing operational process.

As future work, we intend to expand the scope of the tool to a global audit, aiming to understand security challenges on a global scale and identify common vulnerability patterns across the international eduroam federation. We will formalize the consolidated findings of this national audit by formally reporting to key regulatory and operational authorities to drive necessary corrections. These include the Directorate of Privacy and Information Security (DPSI), linked to the Ministry of Management and Innovation in Public Services (MGI), the National Research and Education Network (RNP), and the Federal Government's Cyber Incident Response Team (CTIR Gov). This collaborative disclosure aims to guide technical corrections and strengthen the security posture of the national academic network.

The urgency of mitigating these configuration failures cannot be overstated. When an IdP operates with mismatched certificates or weak cryptography, it neutralizes defenses against Man-in-the-Middle (MitM) attacks, enabling malicious actors to deploy rogue Access Points ("evil twins") and intercept authentication requests. Due to the roaming nature of eduroam and its integration with central Single Sign-On (SSO) or synchronized corporate passwords, the threat extends beyond network access. A single compromised credential on a remote network can breach sensitive internal portals, financial systems, and research databases, escalating a localized wireless flaw into severe data leaks that compromise the university's entire corporate infrastructure.

Acknowledgments

The authors would like to thank the Instituto Federal da Paraíba (IFPB) – Campus João Pessoa for the financial support provided for the publication of this work, and the Federal University of São Carlos (UFSCar) for the support in the software registration process.

References

Ahmed, F., Li, X., Niu, Y., Zhang, C., Wei, L., and Gu, C. (2020). Uniroam: An anonymous and accountable authentication scheme for cross-domain access. In *2020 International Conference on Networking and Network Applications (NaNA)*, pages 198–205.

Batista, L. M., Gomes, H., and Almeida, J. R. (2024). A study of security issues of eduroam networks in portugal. In *13th Symposium on Languages, Applications and Technologies (SLATE 2024)*, pages 14:1–14:14. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

Batista, L. M., Gomes, H., and Almeida, J. R. (2025). Challenges and solutions for eduroam network security. *Procedia Computer Science*, 256:150–157. CENTERIS - International Conference on ENTERprise Information Systems / ProjMAN - International Conference on Project MANagement / HCist - International Conference on Health and Social Care Information Systems and Technologies.

Caballero, A., Garcia-Valverde, T., Pereniguez, F., and Botia, J. A. (2016). Activity recommendation in intelligent campus environments based on the eduroam federation. *Journal of Ambient Intelligence and Smart Environments*, 8(1):35–46.

Daldoul, Y. and Berrima, M. (2025). A robust certificate management system to prevent evil twin attacks in ieee 802.11 networks. *International Journal of Information Technology*, 17(6):3589–3599.

Dekkar, L. and Fiore, S. (2021). Africaconnect3: Connecting africa to unlimited possibilities. In *IST-Africa 2021 Conference Proceedings*. IST-Africa Institute and IIMC.

Ferraiolo, H. and Regenscheid, A. (2024). Cryptographic algorithms and key sizes for personal identity verification. Technical Report NIST Special Publication (SP) 800-78-5, National Institute of Standards and Technology (NIST), Gaithersburg, MD.

GEANT (2009). Report on introduction of monitoring system and diagnostics tools. Deliverable GN2-09-008v2, GEANT Association. Accessed: 2024-05-22.

Goto, H. (2025). Offline attribute sharing methods for authentication traffic reduction and functionality enhancement of wireless lan roaming systems. In *2025 IEEE 49th Annual Computers, Software, and Applications Conference (COMPSAC)*, pages 2224–2229.

GÉANT (2011). Configuration assistant tool. `https://cat.eduroam.org/`. Acessado em: 15 mar. 2026.

Júnior, C. A. J., da Rocha, L. F., Torres, R., and Silva, E. F. (2024). Monitoramento da última milha do eduroam com wifimon. In *Anais do XIV Workshop de Gestão de Identidades Digitais (WGID)*. Sociedade Brasileira de Computação (SBC).

Lima, M. L. G., Campos, P. H. L., and Matias, P. (2021). Módulo de autenticação via eduroam para o pluggable authentication modules. In *Anais do XI Workshop de Gestão de Identidades Digitais (WGID)*. SBC.

Mazhar, H., Kaiser, M., Smith, M., and Adams, C. (2021). All your credentials are belong to us: On insecure WPA2-Enterprise configurations. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (CCS)*. Acessado em: 26 mar. 2026.

McKay, K. A. and Cooper, D. A. (2019). Guidelines for the selection, configuration, and use of transport layer security (tls) implementations. Technical Report NIST Special Publication (SP) 800-52 Rev. 2, National Institute of Standards and Technology, Gaithersburg, MD.

Okabe, Y., Nakamura, M., and Goto, H. (2024). Dynamic vlan assignment for local users under external idp management in radius-based wi-fi roaming. In *2024 International Conference on Information Networking (ICOIN)*, pages 484–489.

Oliveira, L. A. and Silva, E. F. (2024). Evaluation of eap usage for authenticating eduroam users in 5g networks. *arXiv preprint arXiv:2402.10889*.

Orús Comabella, G. (2025). Autenticació segura en xarxes acadèmiques: Desplegament d'un servidor radius per eduroam. Master's thesis, Universitat Autònoma de Barcelona.

Palamà, I., Amici, A., Bellicini, G., Gringoli, F., Pedretti, F., and Bianchi, G. (2023). Attacks and vulnerabilities of wi-fi enterprise networks: User security awareness assessment through credential stealing attack experiments. *Computer Communications*, 212:129–140.

Palamà, I., Amici, A., Gringoli, F., and Bianchi, G. (2022). "careful with that roam, edu": experimental analysis of eduroam credential stealing attacks. In *2022 17th Wireless On-Demand Network Systems and Services Conference (WONS)*, pages 1–7.

Petrosyan, A. S., Petrosyan, G. S., Tadevosyan, R. N., and Arsalanian, K. K. (2019). Identity infrastructure boost concept for eduroam service. *Mathematical Problems of Computer Science*, 52:61–65.

Rieckers, J.-F. (2021). Passive security analysis of current TLS implementations and configurations in the eduroam EAP-TLS environment. Bachelor's thesis, Universität Bremen, Bremen, Alemanha. Acessado em: 26 mar. 2026.

Torres, R., Silva, E. F., and Júnior, C. A. d. J. (2025). Desenvolvimento de um App eduroam na RNP. In *Anais Estendidos do SBSeg 2025: WGID*.

Turner, P. and Woodward, A. (2006). Securing a wireless network with EAP-TLS: Perception and realities of its implementation. In *Proceedings of the 4th Australian Information Security Management Conference*. Edith Cowan University. Acessado em: 26 mar. 2026.

Wang, K., Zheng, Y., Zhang, Q., Bai, G., Qin, M., Zhang, D., and Dong, J. S. (2022). Assessing certificate validation user interfaces of wpa supplicants. In *Proceedings of the 28th Annual International Conference on Mobile Computing And Networking*, MobiCom '22, page 501–513, New York, NY, USA. Association for Computing Machinery.

Wierenga, K., Winter, S., and Wolniewicz, T. (2015). The eduroam Architecture for Network Roaming. RFC 7593.

Yang, X., Goto, H., and Suganuma, T. (2025). Route selection optimization for multihop radius proxies in wlan roaming systems. In *2025 IEEE 49th Annual Computers, Software, and Applications Conference (COMPSAC)*, pages 1553–1558.