Open-source Secure NFC-based Physical Access Control System using EV2 Mutual Authentication

Brais Gómez-Espiñeira, Martiño Rivera-Dourado, Rubén Pérez-Jove, and Jose Vázquez-Naya

Grupo RNASA-IMEDIR. Departamento de Ciencias de la Computación y Tecnologías de la Información. Facultad de Informática, Universidade da Coruña, Elviña, 15071 A Coruña, Spain.
Centro de Investigación CITIC, Universidade da Coruña, Elviña, 15071 A Coruña, Spain.
Correspondence: brais.gomez2@udc.es

DOI: *https://doi.org/10.17979/spu.23.c41*

Abstract: Currently, physical access control is dominated by private and proprietary solutions that are closed, inflexible and often insecure. To address these shortcomings, this work presents an open-source, modular NFC-based access control system. The system consists of two modules. First, a hardware module, capable of reading NFC NTAG424 cards and unlocking a magnetic lock has been assembled. Second, a centralized management server, with an administration panel. The system supports Enhanced Version 2 mutual authentication protocol, time-based and role-based policies, allowing administrators to protect multiple zones within the same facility from a centralized management server. This open solution provides a secure and cost-effective alternative that seeks greater transparency and control.

1 Introduction

Access control systems allow controlling who can access a resource, either a physical building, a digital computer system or sensitive data (Cambridge, 2025). In the context of physical facilities, such as corporate offices, data centers, laboratories or manufacturing plants, access control systems integrate hardware and centralized management software to enforce entry rules and audit log events into their solutions (Nazri et al., 2023). Despite NFC's suitability for this purpose, most current systems are either closed, proprietary, or insecure, often using outdated technology like MIFARE Classic cards. These cards are vulnerable to cloning and replay attacks, making them unsuitable for sensitive environments (Arduino, 2024; Inc., 2025). Additionally, commercial systems tend to be unaffordable for SMEs and private users (Global, 2025; Honeywell, 2025; Suprema, 2025).

This work introduces a modular, open-source, and cost-effective physical access control system using NFC. Motivated by the lack of affordable, transparent solutions and the potential of NFC technology for securing physical facility entry, the developed system uses NFC cards, readers, and a web server to securely manage electronic locks and record entry events in real time. System administrators are able to configure user profiles, apply time-based permissions and centrally view a detailed access history through a web dashboard. In addition, the solution incorporates advanced cryptographic mechanisms (e.g., TLS or AES-128) to mitigate threats such as card cloning, unauthorized interception and data tampering (Azeez and Chinazo, 2018). Furthermore, regarding the physical layer, the system leverages a microcontroller

integrated with dedicated hardware modules, specifically designed for seamless interaction with NFC tags and secure communication with the web server (Dewanto et al., 2021; Ismailov, 2022).

2 State of the Art

In recent years, NFC has evolved from simple proximity identification to the foundation of multilevel security architectures. Three main approaches can be distinguished in NFC-based access control. The first relies on plain UID-based authentication, where the static identifier of the card is matched with an access list. While simple, this approach is highly vulnerable to cloning and replay attacks, particularly in legacy cards such as MIFARE Classic (de Koning Gans et al., 2008). To overcome these limitations, a second strategy combines UID authentication with an additional factor such as a PIN or biometrics, following the principles of multifactor authentication. Finally, the most robust approach is the adoption of mutual authentication protocols, particularly the EV2 scheme, which derives session keys from AES-128 and ensures that both the card and the reader prove knowledge of a shared secret. EV2, implemented by NXP in NTAG 424 DNA and MIFARE DESFire EV2/EV3 (NXP Semiconductors, 2019), protects against cloning, replay, and man-in-the-middle attacks, and has become the industry standard for secure NFC-based access control.

NFC communication is standardized under several ISO/IEC norms. ISO/IEC 14443 defines proximity cards, operating at 13.56 MHz, and their communication technologies (International Organization for Standardization, 2023). ISO/IEC 7816-4 specifies commands and data structures for integrated circuit cards, providing mechanisms for secure messaging and mutual authentication (International Organization for Standardization, 2020). ISO/IEC 7810 defines the physical characteristics of contactless identification cards (International Organization for Standardization, 2019).

From a cryptographic standpoint, AES-128 is widely adopted in secure NFC applications for symmetric encryption, offering strong resistance against brute-force attacks (Ratnadewi et al., 2017). In the proposed system, Hash-based Message Authentication Codes (HMAC) are used as a mechanism for key derivation, specifically HMAC-SHA256, which allows generating unique session or application keys from a MasterKey and a card-specific identifier, ensuring that each card interaction uses independent keys without exposing the root secret (Azeez and Chinazo, 2018).

3 System Architecture

The architecture design of the system is meant to provide secure and flexible physical access control via NFC. It aims to ensure that only authorized users can open doors or barriers, while centrally logging each access attempt. Also, it ensures consistency in access policies, the possibility of implementing updates and new functionalities without physically intervening on each device, and a high level of cryptographic security to protect both credentials and communication between the two domains. The system is composed of two main modules (see Figure 1):

- **NACU (NFC Access Control Unit):** Hardware module installed in a physical door to control access to the room. There can be more than one NACU protecting different facilities.
- **ACMS (Access Control Management Server):** Backend of the access control system, interacting with the NACU hardware modules. It provides an administration panel to register users and configure access policies. It is implemented as a web server in Django, and incorporates a Hardware Security Module (HSM) for NFC-based authentication.

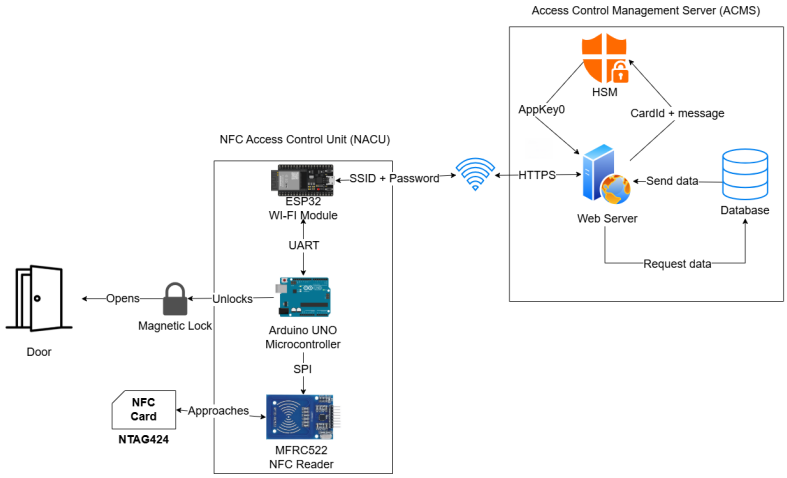

Figure 1: NFC Physical Access Control System Architecture. Left part of the figure repre sents the physical door with a magnetic lock, connected with the NACU module with an NFC Reader. The right part represents the ACMS server authentication module

3.1 Hardware Implementation: NACU

The NACU (NFC Access Control Unit) was designed based on low-cost and widely available components, chosen to ensure reproducibility and modularity. The objective was to integrate an NFC reader with a microcontroller capable of controlling the electronic lock, while providing wireless communication with the centralized management server. Special care was taken in the selection of each element to balance cost, performance, and ease of integration, allowing the construction of a prototype that could later be scaled to multiple access points.

- **Arduino Uno:** Controls NFC reader and magnetic lock.
- **MFRC522 Reader:** Communicates via SPI to read NTAG 424 DNA.
- **ESP32:** Sends card data to ACMS via Wi-Fi.
- **Magnetic lock:** Activated via relay controlled by Arduino.

Integration and Testing: Each component was tested iteratively. The reader and lock worked reliably when the UID was validated by the server. Mutual authentication and UID extraction via EV2 was successfully demonstrated.

3.2 Software Platform: ACMS

The Access Control Management Server (ACMS) was implemented as a web application using the Django framework. This platform acts as the central component of the system, providing administrators with a graphical interface to configure users, manage NFC credentials, and define access policies. Its modular design allows it to interact seamlessly with multiple NACU devices through a Django based RESTful API, while ensuring that authentication and authorization decisions remain centralized and consistent across the system.

The platform includes:

- Role and schedule-based access control
- User and card management
- RESTful API for NACU interaction

- Real-time email alerts for unauthorized attempts

The ACMS incorporates a role and schedule-based access control mechanism that allows administrators to define fine-grained policies for each registered user. Each cardholder is assigned a specific role, such as *administrator*, *staff*, or *visitor*, and an access schedule that defines the valid time windows for entry. When a card is presented to a NACU, the device forwards the authentication request to the ACMS. It evaluates the UID (unique card identifier), obtained after performing EV2 authentication, against these policies before granting or denying access. This approach ensures that possession of a valid NFC card is not sufficient for entry, but that contextual restrictions such as role privileges and temporal constraints are also enforced.

In addition to policy enforcement, the ACMS provides a notification mechanism to increase auditability and immediate responsiveness. Unauthorized access attempts are logged in the server database and immediately reported to system administrators via email alerts. This real-time feedback not only deters malicious behavior but also enables administrators to quickly identify anomalies, monitor system usage, and maintain a comprehensive audit trail of all failed access events.

3.3 Multi-NACU Deployment and Role-based Prototype

As shown in Figure 2, the system architecture allows more than one NACU module to be connected simultaneously to the same ACMS. This centralized management enables administrators to control access to multiple facilities from a single point, ensuring scalability and reducing administrative complexity. Each NACU communicates with the ACMS via secure RESTful API calls, so that authorization policies are always verified by the server before granting access.

Regarding the prototype of the role-based access control system, each user is assigned a role and an access schedule. This allows the ACMS to enforce fine-grained policies that combine both time and user privileges. For example, administrators may configure specific users to access only certain areas, while other roles, such as administrators, retain higher privileges. This approach enhances security by ensuring that access is not only tied to the possession of a valid NFC card, but also to contextual rules managed centrally in the ACMS.

4 Data Flow and Key Management

The EV2 mutual authentication protocol is designed to guarantee confidentiality, integrity, and resistance against replay or cloning attacks. As illustrated in Figure 3, NTAG 424 DNA cards rely on four application keys (`AppKey0`–`AppKey3`) that secure different memory areas. In this project, only `AppKey0` is used to establish the EV2 authentication process. Through this mechanism, the reader and the card prove knowledge of the shared key by exchanging AES-128–based encrypted challenges. Once the secure session is established, the `CardId` can be retrieved from the NDEF file, while the card's UID remains protected in a secure memory area, only accessible through the authenticated EV2 channel.

Upon card detection, the NACU sends the a custom card identifier to the ACMS over a TLS-secured connection. Inside the secure server environment, an HSM uses the MasterKey as the root of the key hierarchy to derive the unique SharedKey for that card through an HMAC-SHA256 operation:

$$\texttt{AppKey0} = \text{HMAC\_SHA256}(\texttt{MasterKey}, \texttt{CardId} \parallel \text{"READUID"}) \tag{32.1}$$

The derived key is returned to the NACU, which uses it to initiate EV2 mutual authentication with the card. This process establishes a secure channel for reading of the protected card identifier.

Once the UID is securely obtained, the NACU transmits it to the ACMS via a TLS-protected REST API. The ACMS verifies the UID, checks role-based and time-based access policies, and sends an authorization or denial response back to the NACU.

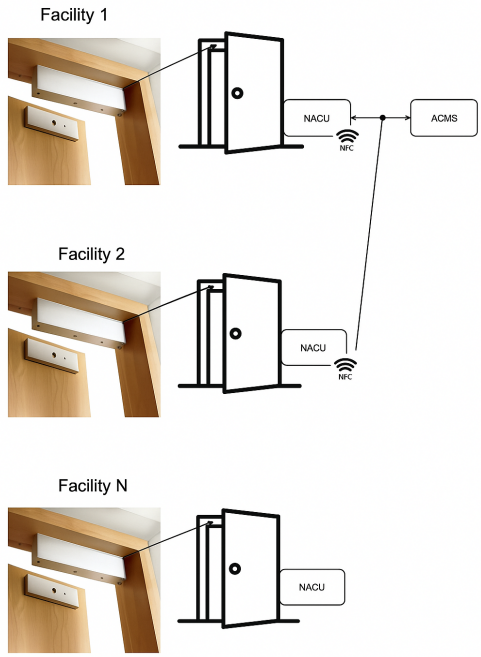

Figure 2: Diagram of multiple NACU modules connected to a single ACMS. Each facility is protected by its own NACU, which integrates an NFC reader and controls the magnetic lock of the door. All NACUs communicate over Wi-Fi with the centralized ACMS server, which manages authentication, access policies, and decision responses. This architecture allows scaling the system to multiple facilities while maintaining centralized control and coordination.

This design ensures that the MasterKey never leaves the HSM, each card uses its unique SharedKey, and all sensitive identifiers remain protected throughout the process.

5 Threat Analysis

This project is deeply focused on security, providing confidentiality, authenticity and integrity in identification systems, mitigating threats inherent to the technologies used and IoT environments. Identifying and analyzing these threats is essential to develop a secure NFC-based control access system.

One of the main threats to NFC is eavesdropping (Chattha, 2014). Communication between two devices over an NFC channel can be intercepted using several devices such as Flipper Zero or Proxmark 3 (Garcia et al., 2011), which are designed to exploit vulnerabilities in systems that use ISO 14443A NFC. Although the required physical proximity (less than 10 cm) limits the attack, the use of high-gain antennas or resonant couplings can extend the effective range.

Another risk, related to eavesdropping, is cloning or tag impersonation, which consists in an attacker uploading a stolen NFC tag in another device such as ChameleonMini (Beningo, 2020), trying to impersonate its legit owner.

The proposed system mitigates these security issues by combining EV2 mutual authentication with AES-128–based key derivation, ensuring that intercepted communications or cloned tags cannot be used for impersonation.

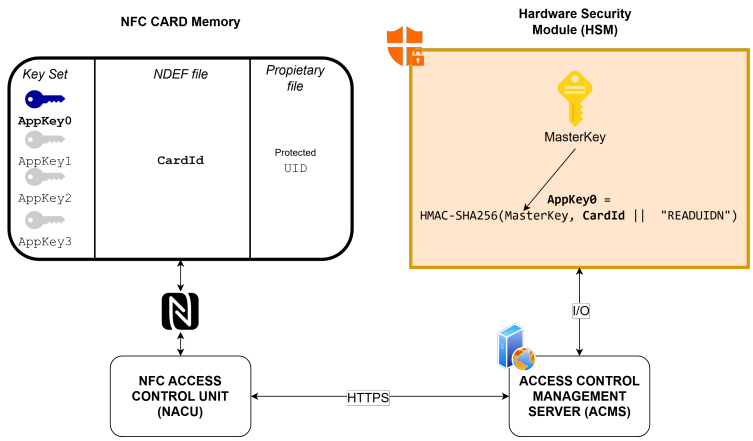

Figure 3: Diagram of the key hierarchy. On the top right, the MasterKey represents the root of the key hierarchy, from which the AppKey of each NFC card is derived. On the left, a representation of the memory card is shown, including the four AppKeys stored in the key set; the CardId stored in the NDEF file and the UID stored in the propietary file. Also, in the bottom it can be seen a representation on how NACU and ACMS interact between them, with card, and with the HSM.

There are also interference and denial of service (DoS) attacks that can affect this type of systems. Generating electromagnetic noise in the NFC band or saturating the reader with multiple requests can cause failures or crashes. However, using maglocks ensures that this attack would not let the attacker pass through the protected door. This is because voltage is constantly supplied to the lock, and in order to open it, a voltage cut-off is needed. If the reader were to be saturated, the door would not open because the reader itself would not be able to send the voltage cut-off signal.

In addition, one of the main physical threats is the manipulation of the wiring between Arduino and ESP32, which could lead to data leaks. As this system is designed for academic purposes, wiring is not protected. If this system needs to be installed in a real environment, a proper safe box must be used in order not to be easily manipulated. It is also important to highlight that no key is stored in any of these microcontrollers, as it is considered a poor security practice.

Related to the Access Control Management Server (ACMS), several attacks including SQL Injection, XSS in the API, TLS certificate theft, and DoS against the server could be performed. To mitigate these threats, the information that is stored in the Django model database is not critical or personal (e.g., NIF or keys). The NFC tag is stored in it but, again, in case of compromise, it would not be enough to authenticate in the system. Moreover, the MasterKey is stored in a Hardware Security Module to prevent these types of attacks from being effective.

6 Results and Discussion

The proposed system demonstrates the feasibility of implementing a secure and modular access control solution based on NFC using EV2 mutual authentication, meeting the objectives set at the beginning of the project. A functional prototype was developed, integrating both the hardware module (NACU); see Figure 4, and the centralized management platform (ACMS), and validating the complete authentication and authorization workflow.

A major achievement was the successful implementation of EV2 mutual authentication with NTAG 424 DNA cards, enabling the secure retrieval of the card UID through a protected channel. This protocol ensures confidentiality, integrity, and protection against replay and clone

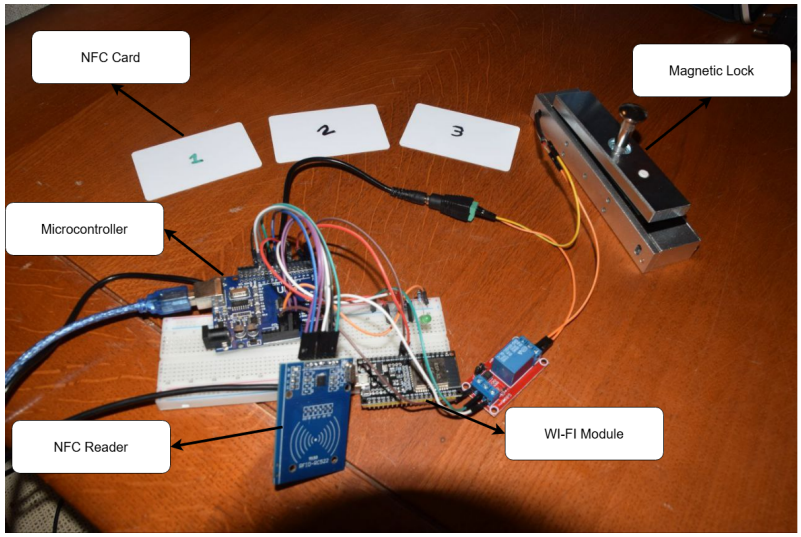

Figure 4: NACU and Test Cards. From left to right, the Arduino Uno, MFRC522, ESP32 and magnetic lock can be seen. Also, the three cards at the back were used in the system evaluation.

attacks, which represents a significant advance over traditional and insecure approaches such as MIFARE Classic. The project also incorporated a robust derivation of application keys using HMAC-SHA256, with the MasterKey remaining securely in the HSM, thus guaranteeing that card-specific keys are generated dynamically without exposing the root secret.

From the perspective of system integration, the NACU is able to reliably detect NFC cards, request shared keys from the ACMS, and control the magnetic lock based on the server's authorization response. Each component of the NACU was iteratively tested to confirm its proper operation within the complete architecture. The results confirmed that the hardware operated stably when interacting with the server and that unauthorized attempts were correctly denied.

On the software side, the ACMS platform provided an administration panel that enabled role-based and schedule-based access policies. This allowed defining access policies for each user and assigning different roles. Unauthorized access attempts were correctly logged and triggered alerts, validating the system's capacity to increase auditability and administrator awareness in real time. The availability of a RESTful API for communication with the NACU also guaranteed modularity and extensibility of the platform, following the open source approach.

The discussion highlights that this solution offers a real alternative to commercial access control systems, which are typically closed, costly, and often insecure. The use of open-source libraries, affordable hardware, and standard cryptographic mechanisms (AES-128, HMAC-SHA256, TLS) ensures transparency, flexibility, and maintainability. Furthermore, the modular design allows replicating the system across multiple facilities, centralizing their management in the ACMS.

Another relevant result is the demonstration of key hierarchy management, where the MasterKey remains confined to the HSM and card-specific AppKeys are derived per transaction. This design ensures that even if one key were compromised, it would not endanger the rest of the infrastructure. The evaluation confirmed that this mechanism significantly strengthens the resistance against cloning or replay attacks.

7 Conclusion

Finally, the project demonstrates that secure physical access control using modern NFC technology can be achieved with low-cost and open components. The combination of NTAG 424 DNA features, EV2 authentication, and centralized policy management provides a level of security and control previously limited to proprietary solutions. Therefore, the work contributes to bridging the gap between academic research and practical deployment of open, secure, and scalable access control systems.

Bibliography

Arduino. Httpclient library — arduino reference, 2024. [Online]. Available: *https://docs.arduino.cc/libraries/httpclient/*.

N. A. Azeez and O. J. Chinazo. Achieving data authentication with hmac-sha256 algorithm. *Computer Science & Telecommunications*, 54(2):34–43, 2018. URL *https://www.researchgate.net/publication/332182220*.

J. Beningo. Cómo usar trustzone para asegurar los dispositivos de iot con un mínimo de complejidad y costo de hardware, 2020. [Online]. Available: *https://www.digikey.es/es/articles/how-to-use-trustzone-to-secure-iot-devices* [Accessed: Jun. 10, 2025].

D. Cambridge. Access control, 2025. URL *https://dictionary.cambridge.org/dictionary/english/access-control*. Accessed: Apr. 10, 2025.

N. A. Chattha. Nfc — vulnerabilities and defense. In *2014 Conference on Information Assurance and Cyber Security (CIACS)*, pages 35–38, Rawalpindi, Pakistan, 2014. doi: 10.1109/CIACS.2014.6861328.

G. de Koning Gans, J.-H. Hoepman, and F. D. Garcia. A practical attack on the mifare classic. In *Proc. 8th Smart Card Research and Advanced Application Conf. (CARDIS)*, volume 5189 of *Lecture Notes in Computer Science*, pages 267–282. Springer, 2008. [Online]. Available: *https://link.springer.com/chapter/10.1007/978-3-642-12510-2_18* [Accessed: Jun. 13, 2025].

S. A. Dewanto, M. Munir, B. Wulandari, and K. Alfian. Mfrc522 rfid technology implementation for conventional merchant with cashless payment system. *Journal of Physics: Conference Series*, 1737(1):012012, 2021. doi: 10.1088/1742-6596/1737/1/012012.

F. D. Garcia, G. de Koning Gans, and R. Verdult. Tutorial: Proxmark, the swiss army knife for rfid security research. In *Proc. of the 5th USENIX Workshop on Offensive Technologies (WOOT '11)*, San Francisco, CA, USA, 2011. [Online]. Available: *https://www.usenix.org/conference/woot11/workshop-program/presentation/Garcia*.

H. Global. Powering trusted identities of the world's people, places and things, 2025. URL *https://www.hidglobal.com/*. Accessed: Apr. 14, 2025.

Honeywell. Home, 2025. URL *https://www.honeywell.com/us/en*. Accessed: Apr. 14, 2025.

F. D. Inc. Flipper zero documentation. *https://docs.flipper.net*, 2025. Accessed: Jun. 5, 2025.

International Organization for Standardization. Iso/iec 7810:2019 - identification cards — physical characteristics. Technical report, ISO, 2019. URL *https://www.iso.org/obp/ui/#iso:std:iso-iec:7810:ed-4:v1:en*.

International Organization for Standardization. Iso/iec 7816-4:2020 - identification cards — integrated circuit cards — part 4: Organization, security and commands for interchange. Technical report, ISO, 2020. URL *https://www.iso.org/obp/ui/#iso:std:iso-iec:7816:-4:ed-4:v1:en*.

International Organization for Standardization. Iso/iec 14443 - cards and security devices for personal identification — contactless proximity objects — parts 1 to 4. Technical report, ISO, 2023. URL *https://www.iso.org/standard/73596.html*.

A. Ismailov. Study of arduino microcontroller board, 2022. URL *https://www.researchgate.net/publication/359502443_Study_of_arduino_microcontroller_board*. Accessed: May 19, 2025.

T. A. A. Nazri, N. M. Saad, A. A. Zaidel, S. K. Syed-Yusof, and N. A. M. Radzi. Smart access control system using face recognition, nfc and otp. *IEEE Access*, 11:28838–28851, 2023. doi: 10.1109/ACCESS.2023.3255519.

NXP Semiconductors. Nt4h2421gx: Ntag 424 dna – secure nfc t4t compliant ic. Technical report, NXP, 2019. URL *https://www.nxp.com/docs/en/data-sheet/NT4H2421Gx.pdf*. Accessed: May 24, 2025.

R. Ratnadewi, I. Riadi, and L. A. Nugroho. Implementation and performance analysis of aes-128 cryptography method in an nfc-based communication system, 2017. URL *https://www.researchgate.net/publication/318528672_Implementation_and_performance_analysis_of_AES-128_cryptography_method_in_an_NFC-based_communication_system*. Accessed: May 19, 2025.

Suprema. Security & biometrics, 2025. URL *https://www.supremainc.com/en/*. Accessed: Apr. 14, 2025.