Towards Legally Recognized Device Authentication in IoT M2M under eIDAS 2.0

1st Francesco Buccafurri
University Mediterranea of Reggio Calabria
Reggio Calabria, Italy
bucca@unirc.it

2nd Carmen Licciardi
University Mediterranea of Reggio Calabria
Reggio Calabria, Italy
carmen.licciardi@unirc.it

***Abstract*—The increasing adoption of Internet of Things (IoT) systems requires secure and scalable machine-to-machine (M2M) authentication. Current approaches, based on symmetric keys and X.509 certificates, provide strong cryptographic guarantees but lack a clear connection to legally recognized digital identities. At the same time, the eIDAS 2.0 framework defines a unified digital identity model in Europe, mainly targeting human and organizational actors.**

This paper investigates the gap between technical device authentication and regulated identity frameworks in IoT M2M scenarios. We outline a preliminary approach in which devices authenticate as representatives of legal entities through verifiable credentials issued by trusted authorities.

The proposed direction builds on decentralized identity principles and operates without user interaction at runtime. We discuss key design considerations and open challenges, including credential lifecycle management, secure device binding, and revocation. This work represents a first step towards integrating IoT authentication with legally compliant digital identity frameworks.

I. Introduction

The rapid growth of Internet of Things (IoT) systems is driving industries towards increasingly automated and interconnected environments, where devices interact without human intervention. In domains such as smart manufacturing, energy management, and logistics, machine-to-machine (M2M) communication has become the dominant interaction model, making authentication essential for secure and reliable operations.

Current IoT authentication mechanisms mainly rely on cryptographic solutions such as symmetric keys and X.509 certificates. While effective in verifying device identity at a technical level, these approaches are primarily designed to secure communication rather than to provide identities meaningful beyond the technical domain.

At the same time, the eIDAS 2.0 framework introduces a unified model for legally recognized digital identities in Europe, targeting individuals and organizations. Although particularly relevant for industrial scenarios requiring accountability and trust across organizational boundaries, eIDAS 2.0 does not explicitly address non-human entities such as IoT devices.

This creates a gap between IoT authentication mechanisms and regulated identity frameworks. IoT infrastructures provide efficient technical authentication, while emerging regulations require stronger guarantees in terms of identity, trust, and accountability. As a result, current IoT M2M solutions are not directly aligned with legally recognized identity models.

In this work, we investigate how concepts from regulated digital identity frameworks can be adapted to IoT M2M environments. We outline a preliminary approach based on decentralized identity principles and Verifiable Credentials, enabling devices to authenticate as representatives of legal entities without requiring user interaction at runtime.

The goal of this paper is not to provide a complete solution, but to identify the problem, define the main challenges, and propose a first conceptual direction. The main contribution of this work is the conceptualization of a bridge between conventional IoT authentication and legally recognized digital identity frameworks through a layered model combining technical authentication and verifiable identity semantics. Addressing this gap is essential for future IoT systems where technical security and legally recognized identities must coexist.

The remainder of this paper is organized as follows. Section II reviews the state of the art on IoT authentication and digital identity. Section III introduces a motivating scenario highlighting the limitations of current approaches. Section IV provides the necessary background on IoT M2M authentication and eIDAS-based identity frameworks, and clarifies the problem context. Section V presents the proposed approach, including its conceptual design and technical elements. Section VI discusses how the proposed solution differs from existing approaches. Section VII outlines the main design considerations, while Section VIII highlights open issues. Section IX focuses on revocation aspects and related trade-offs. Finally, Section X concludes the paper.

II. Related Work

Security and authentication in IoT systems have been widely studied, with several works highlighting the challenges of securing distributed and resource-constrained environments [1]. Existing approaches mainly rely on cryptographic mechanisms, such as key-based authentication and secure communication protocols, to ensure device identity and data protection [2], [3]. More recently, research on decentralized identity has introduced new models for managing digital identities in a distributed manner. Concepts such as self-sovereign identity and verifiable credentials enable entities to present cryptographically verifiable claims without

relying on centralized authorities [4], [5], [6]. Several recent studies have also investigated the adoption of decentralized identity and verifiable credential models in IoT ecosystems, mainly focusing on interoperability, privacy, and decentralized trust management. However, these approaches generally do not address the integration of IoT authentication with legally recognized identity frameworks and regulated trust infrastructures. In parallel, the eIDAS 2.0 framework aims to provide legally recognized digital identities and trust services across Europe [7]. However, it primarily targets human users and organizations, without explicitly addressing non-human entities such as IoT devices. Despite these advances, the integration of IoT authentication mechanisms with legally recognized identity frameworks remains relatively unexplored, especially in M2M IoT scenarios. This work aims to bridge this gap by proposing an approach that combines device-level authentication with verifiable, issuer-backed identities.

III. Motivating Scenario

Consider a smart manufacturing environment where multiple industrial devices, such as sensors, controllers, and robotic systems, interact across organizational boundaries. For example, a production line may include equipment provided and maintained by different vendors, while operational data is shared with external services for monitoring, optimization, or predictive maintenance. In such a scenario, devices continuously exchange data and commands in a machine-to-machine (M2M) fashion, without any human involvement at runtime. Authentication between devices is typically enforced using standard mechanisms such as TLS with X.509 certificates or pre-shared keys. These solutions ensure secure communication and verify that devices are authorized at a technical level. However, these mechanisms do not provide information about the legal or organizational identity behind a device. For instance, when a device sends data to an external service, it is technically authenticated, but it is not always clear which organization is responsible for that device, under which conditions it operates, or whether its identity can be trusted beyond the local system. This limitation becomes critical in industrial contexts where accountability, liability, and regulatory compliance are essential. For example, in case of incorrect data, malfunctioning behavior, or security incidents, it is important to determine which entity is responsible for the device and whether its identity can be linked to a trusted and verifiable source. At the same time, emerging frameworks such as eIDAS 2.0 aim to provide legally recognized digital identities and trust services across Europe. These frameworks enable strong guarantees in terms of identity, trust, and accountability, but are primarily designed for human users and organizations, not for autonomous devices operating in M2M environments. As a result, a gap emerges. On one side, IoT systems provide efficient and scalable authentication mechanisms, but lack a connection to legally recognized identities. On the other side, eIDAS 2.0 provides strong identity guarantees, but does not directly support non-human entities such as IoT devices. This gap raises a key question: how can IoT devices participating in M2M interactions be associated with legally recognized identities, enabling authentication mechanisms that are not only secure, but also aligned with trust and regulatory frameworks? In this work, we take a first step towards addressing this problem by exploring how concepts from digital identity frameworks can be extended to IoT devices, allowing them to act as representatives of legal entities in M2M interactions.

IV. Background and Problem Context

A. IoT M2M Authentication

Authentication in IoT systems is typically achieved through well-established cryptographic mechanisms, enabling devices to securely communicate in machine-to-machine (M2M) scenarios. Common approaches include symmetric key-based methods and public key infrastructures (PKI), often implemented through protocols such as TLS. These solutions ensure that devices can verify each other's identity and establish secure communication channels. However, device authentication in IoT is primarily focused on technical identity, that is, proving the possession of a cryptographic key. While this is sufficient to guarantee secure communication, it does not provide information about the entity behind the device, nor does it support notions such as accountability or legal responsibility. As a result, trust is typically confined within system boundaries and does not easily extend across different organizations.

B. eIDAS 2.0 and Digital Identity

The eIDAS 2.0 framework introduces a unified approach to digital identity and trust services within the European Union. It enables the use of legally recognized identities for individuals and organizations, supported by trust anchors such as qualified trust service providers and interoperable identity infrastructures. A key aspect of eIDAS 2.0 is the notion of identity with a defined level of assurance, allowing relying parties to evaluate the trustworthiness of an authenticated entity. In addition, the framework promotes the use of verifiable and portable credentials, enabling identity attributes to be securely shared across domains. Despite these advances, eIDAS 2.0 remains centered on human users and legal entities, and does not explicitly define how non-human actors, such as IoT devices, should be represented within the identity ecosystem. This limitation makes it difficult to directly apply eIDAS principles to M2M scenarios, where authentication occurs without user involvement.

C. Problem Context

The combination of these two perspectives highlights a fundamental mismatch. IoT authentication mechanisms provide strong technical guarantees but lack alignment with legally recognized identity frameworks. Conversely, eIDAS 2.0 provides robust identity and trust models, but does not directly support autonomous devices operating in M2M environments. This mismatch motivates the need for new approaches that can bridge technical authentication and legal identity, enabling IoT devices to participate in trust frameworks in a way that is both secure and meaningful beyond the system level.

V. Proposed Approach

A. Concept Overview

The proposed approach extends existing IoT authentication mechanisms by introducing an additional identity layer based on verifiable credentials, while preserving compatibility with standard communication protocols. In particular, authentication is performed using well-established mechanisms such as Transport Layer Security (TLS) or mutual TLS (mTLS), where devices prove possession of cryptographic material, typically associated with X.509 certificates or pre-shared keys. These mechanisms ensure secure communication and provide device-level authentication. On top of this layer, the proposed approach introduces identity semantics through the use of verifiable credentials compliant with the W3C Verifiable Credentials data model. These credentials bind a device to a legally recognized entity, such as an organization, and can be associated with decentralized identifiers (DIDs) as defined by the W3C DID specification. Importantly, the proposed approach does not replace existing PKI-based authentication mechanisms, but augments them. Verifiable credentials are exchanged at the application layer after the establishment of a secure channel, ensuring full compatibility with existing IoT infrastructures. This layered design enables devices to authenticate at a technical level while simultaneously providing verifiable information about the entity they represent, bridging the gap between cryptographic authentication and legally recognized identity frameworks.

B. Alignment with eIDAS 2.0

A key objective of the proposed approach is to align IoT device authentication with regulated identity frameworks such as eIDAS 2.0. In the eIDAS ecosystem, identity is associated with a level of assurance and is issued by trusted entities, such as qualified trust service providers. In this context, verifiable credentials can be used to represent device-related identity attributes issued by trusted authorities, potentially aligned with eIDAS trust anchors.

In particular, the issuer role defined in the proposed model can be mapped to regulated identity providers or trust service providers, ensuring that credentials are anchored to legally recognized entities. This enables relying parties to evaluate the trustworthiness of a device not only based on its cryptographic identity, but also based on the assurance level associated with the credential.

Although eIDAS 2.0 does not explicitly define device identities, the proposed approach leverages its trust model to extend identity concepts to non-human entities, enabling a consistent interpretation of trust across human and machine actors. In this context, the level of assurance associated with a credential can be interpreted in a way similar to eIDAS assurance levels, allowing relying parties to differentiate between devices based on the strength and trustworthiness of their associated identity. In this perspective, future developments may further investigate how different assurance levels could be associated with device identities, considering aspects such as hardware-backed key protection, trusted credential issuance procedures, and compliance with regulated trust service infrastructures.

C. System Model

The proposed model involves three main actors:

- **Device**: an IoT entity participating in machine-to-machine communication. The device authenticates using standard mechanisms such as TLS or mTLS, and holds both cryptographic credentials (e.g., X.509 certificates) and identity credentials (verifiable credentials).
- **Issuer**: a trusted entity responsible for issuing verifiable credentials that bind devices to legal entities. This role can be aligned with eIDAS trust service providers or other regulated identity authorities.
- **Verifier**: a system or service that interacts with the device. The verifier performs standard authentication (e.g., TLS handshake with certificate validation) and validates the presented credential using signature verification and trust anchor validation.

This model separates authentication (proof of key possession) from identity representation (credential-based), enabling greater flexibility and interoperability.

D. Authentication Flow

The authentication process combines standard TLS-based authentication with credential-based identity verification, following a layered approach:

1) The device initiates a connection with the verifier using a secure communication protocol, such as TLS or mutual TLS (mTLS).
2) During the handshake phase, the device performs standard cryptographic authentication, for example by presenting an X.509 certificate or by proving possession of a private key.
3) After the secure channel is established, the device presents a verifiable credential compliant with the W3C Verifiable Credentials model. The credential binds the device to a legal entity and may include attributes such as organization identifier, device role, or authorization scope.
4) The verifier validates the credential by verifying its digital signature, checking the issuer against trusted anchors, and optionally resolving decentralized identifiers (DIDs).
5) The verifier evaluates the credential according to its level of assurance and associated trust policies, potentially aligned with eIDAS assurance levels. Future extensions of the proposed approach may investigate stronger binding mechanisms between verifiable credentials and the underlying TLS session, for example through channel binding techniques or session-specific cryptographic proofs. This would further strengthen the association between the authenticated communication endpoint and the presented credential, mitigating potential replay or impersonation attacks in M2M environments.

6) If both the TLS-based authentication and the credential validation succeed, the device is authenticated as a representative of the associated legal entity.

This flow preserves compatibility with existing protocols while introducing a richer notion of identity and trust.

E. Discussion

The proposed approach provides a practical way to extend IoT authentication mechanisms towards models that incorporate identity semantics and legal accountability.

By combining established technologies such as TLS and X.509 with emerging standards such as W3C Verifiable Credentials and decentralized identifiers, the approach enables a gradual evolution of IoT systems without requiring disruptive changes.

At the same time, several challenges remain open. These include secure credential storage on constrained devices, binding between credentials and hardware (e.g., secure elements or TPMs), and the management of credential lifecycle and revocation in distributed environments.

Nevertheless, the proposed approach represents a first step towards integrating IoT authentication with regulated digital identity frameworks, enabling new forms of trust in machine-to-machine interactions.

VI. Comparison with Existing Approaches

Unlike existing IoT authentication approaches, which mainly focus on establishing technical trust between communication endpoints, the proposed model explicitly introduces legally meaningful identity semantics by linking devices to regulated digital identity frameworks and accountable organizational entities. Traditional IoT authentication mechanisms rely on well-established cryptographic techniques, such as symmetric keys and X.509 certificates, to ensure secure communication between devices. These approaches are effective in verifying device identity at a technical level and are widely adopted in industrial systems.

However, such mechanisms primarily focus on proving the possession of cryptographic material, without explicitly representing the identity of the entity behind the device. Although certificates may contain some identity-related information, they are typically bound to system-specific trust models and are not designed to convey legally recognized identities across organizational boundaries.

In contrast, the proposed approach introduces a clear separation between technical authentication and identity semantics. Cryptographic protocols, such as TLS, are still used to establish secure channels and verify device authenticity, while identity information is provided through verifiable credentials issued by trusted entities. This allows identity attributes to be managed independently from the underlying communication infrastructure.

Another key difference lies in the trust model. Traditional approaches rely on hierarchical PKI structures, where trust is anchored in certificate authorities that are often domain-specific. This limits interoperability across different systems and organizations. The proposed approach, instead, enables a more flexible trust model, where credentials can be issued by recognized authorities and verified across domains, in alignment with regulated identity frameworks.

Furthermore, the proposed model enables a stronger notion of accountability. By associating devices with legal entities through verifiable credentials, it becomes possible to trace actions performed in M2M interactions back to responsible organizations. This is particularly relevant in industrial and regulated contexts, where compliance and liability are critical.

Finally, the proposed approach supports greater extensibility. While traditional authentication mechanisms require modifications to certificate structures or trust configurations to include additional identity information, verifiable credentials allow new attributes to be added without changing the underlying protocols.

Overall, the proposed approach does not replace existing IoT authentication mechanisms, but extends them by introducing a complementary identity layer. This enables a transition from purely technical authentication towards a model where identity, trust, and accountability are aligned with legal and regulatory requirements.

VII. Design Considerations

The proposed approach extends traditional IoT authentication by introducing identity-related information linked to legal entities. This raises several design considerations.

- **Compatibility with existing protocols**: The approach should integrate with widely adopted mechanisms such as TLS, avoiding significant changes to current IoT infrastructures.
- **Credential format and verification**: The choice of credential format impacts both interoperability and performance. Lightweight verification mechanisms are desirable, especially for constrained devices.
- **Trust model**: The definition of trusted issuers and trust anchors is a key aspect. The reliability of the system depends on how trust relationships are established and maintained across domains.
- **Performance trade-offs**: Adding credential verification introduces overhead. The balance between stronger identity guarantees and system performance must be carefully evaluated.

These aspects influence the applicability of the proposed approach in different deployment scenarios.

VIII. Challenges and Open Issues

While the proposed approach provides a first step towards integrating IoT authentication with legally recognized identity frameworks, several challenges remain open.

- **Credential binding to devices**: Credentials must be securely bound to physical devices. Software-based storage is vulnerable to extraction and cloning, while hardware-based solutions (e.g., secure elements) increase cost and complexity.

- **Credential lifecycle management**: IoT deployments require scalable mechanisms for credential issuance, renewal, and revocation. Devices may operate for long periods or change ownership, making lifecycle management particularly challenging. Future developments should also investigate governance aspects related to issuer roles and ownership transfer scenarios, especially in multi-stakeholder industrial environments where manufacturing, operation, and maintenance responsibilities may belong to different entities.
- **Revocation and trust updates**: Efficient revocation is difficult in distributed environments with intermittent connectivity. Ensuring that compromised devices are quickly excluded from the system remains an open issue.
- **Scalability and performance**: Credential verification introduces additional overhead. This may impact constrained devices and latency-sensitive applications, requiring careful trade-offs.
- **Trust model and governance**: Defining trusted issuers and managing cross-domain trust relationships is complex, especially when multiple organizations are involved.

Addressing these challenges is essential to make the proposed approach practical in real-world IoT systems.

IX. Revocation Considerations

Revocation represents a critical aspect in the proposed approach, as it involves both traditional cryptographic credentials and identity-related credentials.

In standard IoT authentication mechanisms based on TLS and X.509, revocation is typically handled through mechanisms such as Certificate Revocation Lists (CRLs) or the Online Certificate Status Protocol (OCSP). While effective, these approaches may introduce privacy concerns. In particular, when using OCSP or similar online verification methods, the verifier may reveal information about which devices or credentials are being checked, enabling potential tracking or correlation of interactions.

In the proposed approach, revocation must also be considered for verifiable credentials. Emerging mechanisms, such as status lists or cryptographic accumulators, enable revocation checks that can be performed in a more privacy-preserving manner, reducing the need for direct interaction with centralized services.

Recent work has explicitly addressed this issue by proposing privacy-preserving revocation mechanisms for verifiable credentials, capable of protecting against curious verifiers while maintaining efficient validation procedures [8]. In particular, approaches based on advanced cryptographic primitives, such as attribute-based or hierarchical identity-based encryption, enable revocation checks without revealing which specific credential is being verified.

This leads to a dual revocation problem. A device may be cryptographically valid (e.g., its TLS certificate is still valid) while its associated identity credential has been revoked, or vice versa. Therefore, verifiers must evaluate both layers to correctly assess the trustworthiness of a device.

At the same time, the integration of revocation mechanisms must carefully balance security and privacy. While centralized revocation services provide strong guarantees of freshness, they may expose sensitive information about verification patterns. Conversely, privacy-preserving approaches improve unlinkability but may introduce additional complexity or computational overhead.

Efficiently addressing these trade-offs is particularly challenging in IoT environments, where devices may operate with intermittent connectivity and limited computational resources. As a result, designing revocation mechanisms that are both scalable and privacy-aware remains an open research challenge, especially in the context of regulated identity frameworks.

X. Conclusion

This paper explored the gap between technical authentication mechanisms in IoT M2M systems and legally recognized identity frameworks such as eIDAS 2.0. While current solutions provide strong cryptographic guarantees, they lack a clear connection to legal identity and accountability.

We outlined a preliminary approach in which devices can authenticate as representatives of legal entities using verifiable credentials issued by trusted authorities. This direction enables a richer notion of identity, extending beyond technical authentication towards trust models aligned with regulatory frameworks.

Although the proposed approach is still at an early stage, it highlights a promising direction for bridging IoT authentication and digital identity. Future work will focus on refining the model, evaluating its feasibility in real-world deployments, and addressing challenges related to scalability, revocation, and trust management.

XI. Acknowledgments

This work is supported by Agenzia per la Cybersicurezza Nazionale under the programme for promotion of XL cycle PhD research in cybersecurity – C36E24000080005. The views expressed are those of the authors and do not represent the funding institutions.

References

[1] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[2] R. Roman, P. Najera, and J. Lopez, "On the features and challenges of security and privacy in distributed iot," *Computer Networks*, 2013.

[3] R. Hummen *et al.*, "Delegation-based authentication and authorization for the ip-based internet of things," in *IEEE SECON*, 2013.

[4] A. Mühle *et al.*, "A survey on self-sovereign identity," *IEEE Communications Surveys & Tutorials*, 2018.

[5] W3C, "Verifiable credentials data model 1.0," https://www.w3.org/TR/vc-data-model/, 2019.

[6] ——, "Decentralized identifiers (dids) v1.0," https://www.w3.org/TR/did-core/, 2022.

[7] European Commission, "Proposal for a european digital identity framework (eidas 2.0)," https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation, 2021.

[8] F. Buccafurri and C. Licciardi, "Towards privacy-preserving revocation of verifiable credentials with time-flexibility," in *2025 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 2025, pp. 516–521.