Market Models in the European Digital Identity Wallet Ecosystem

Timm Bauer, Stefan Genchev*
*Chair of Network Architectures and Services
School of Computation, Information and Technology, Technical University of Munich, Germany
Email: timm.v.bauer@tum.de, genchev@net.in.tum.de

***Abstract*—The European Digital Identity (EUDI) Wallet creates new opportunities for issuing verifiable digital diplomas as Qualified Electronic Attestations of Attributes (QEAA). This paper explores and compares market models for QEAA-based diploma issuance and verification. The models under consideration include university-operated Qualified Trust Service Providers (QTSPs), outsourcing to external providers, government-supported schemes, pay-per-verification, and industry-sponsored approaches. By examining stakeholder incentives and dependencies, this paper highlights benefits and limitations per model. The analysis reveals that there is no dominant market model, as the optimal strategy depends on the use case and stakeholders. Hybrid approaches can help adapt and apply models to specific use cases, and an adoption phase may help gaining trust and experience at a lower initial investment.**

***Index Terms*—EUDI wallet, QEAA, eIDAS 2.0, verifiable credentials, digital diplomas, market models**

1. Introduction

The European Digital Identity (EUDI) Wallet, introduced in the eIDAS 2.0 framework [1], is changing how digital credentials are issued, stored, and verified. One key application is the issuance and verification of Qualified Electronic Attestations of Attributes (QEAA) [2], such as higher education diplomas. This process involves multiple stakeholders, each with distinct roles and incentives.

Although the wallet infrastructure is evolving, there is a lack of analysis regarding sustainable market models, particularly for the use case of digital university diplomas. Actors here are universities, graduates, Qualified Trust Service Providers (QTSPs), and employers [3], and their interaction affects the sustainability and accessibility of the EUDI wallet. This paper examines market models that could govern the issuance and verification of QEAA-based diplomas within the EUDI wallet ecosystem.

Section 2 provides an use-case-independent overview of the legal and technical foundations. Section 3 delves into the use case, by describing the problem and examining stakeholders, their roles, and incentives. By analyzing incentives and funding mechanisms, Section 4 explores applicable models, considering university-, government-, and verifier-centric approaches. Using the QEAA-based diploma use case as a representative scenario, this paper aims to identify which market models can sustainably support the issuance and verification of QEAA, while balancing incentives, accessibility, and financial obligations.

2. Background and Regulatory Framework

Regulation (EU) No. 910/2014 [4], known as eIDAS, established a legal framework for electronic identification, authentication, and trust services across the EU. Aimed at enabling cross-border interoperability of services such as eID, signatures, and seals, it faced limited adoption due to restricted user control and lack of support for attribute issuance [5], [6]. Additionally, its inflexibility with respect to supporting diverse use cases caused it to be "unable to respond to new market demands for Identity Management" [7, p. 439]. These issues led to its 2021 revision and introduction of eIDAS 2.0 [1], which mandates that Member States provide citizens an EUDI Wallet [8].

2.1. European Digital Identity Wallet Ecosystem

The EUDI Wallet is a standardized and user-centric digital wallet proposed by the European Union. Its main objective is enabling citizens and organizations to store, manage, and verify digital certified attributes [9]. This wallet is related to the concept of *Self-Sovereign Identity* (SSI), a model where users fully control their identity data and can selectively share verified credentials issued by trusted entities [10]. In the EUDI ecosystem, Trust Service Providers (TSPs) are trusted entities that issue Personal Identification Data (PID), a person's core identity attributes like name and date of birth. Comparable to the SSI approach, the ecosystem is based on a trust triangle betweet its participants, with the roles depicted in table 1:

TABLE 1: Digital Identity Ecosystem Participants [9]

Participant EUDI	SSI Equivalent	Description
PID Provider	Issuer	Issues identity attributes
End User	Holder	Wallet user who stores and presents credentials
Relying Party	Verifier	Validates credentials

In this relationship, TSPs issue verified credentials to users, who share them with a relying party to prove their identity or attributes [10]. Wallet users control what information they present to the relying party for verification. This concept is referred to as *Selective Disclosure* [9].

2.2. Electronic Attestations of Attributes

In the EUDI Wallet Ecosystem, electronic attributes refer to verified pieces of information, belonging to a person or organization, that can be stored, shared, and

 doi: 10.2313/NET-2025-11-3_11

verified digitally. The attestation of attributes, such as certificates, licenses, and professional or educational qualifications can be issued by TSPs or public authorities [2]. Based on the required level of assurance, a distinction is made between different types of attribute attestations, affecting their issuance and legal recognition [11]:

- **Qualified Electronic Attestations of Attributes** (QEAA) are issued by QTSPs which must be accredited according to the eIDAS 2.0. Examples of QEAA include education diplomas, and their legal effect is equivalent to paper documents [12].
- **Public Electronic Attestations of Attributes** (Pub-EAA) are attributes originating from official government records, for example driver's licenses [11]. Issuers are public authorities, and the legal effect is also equivalent to paper documents.
- **Electronic Attestations of Attributes** (EAA), also called non-qualified EAAs, do not have to be issued by a QTSP as they do not require the same level of assurance. Issuers can be non-qualified TSPs, but the legal effect is not equivalent to paper documents. Examples of non-qualified EAAs include gym membership attestations [12].

2.3. Monetization Strategies

One of the core requirements outlined in the eIDAS 2.0 regulation is that the EUDI Wallet should be provided to citizens free of charge [9]. Additional costs may arise for the other ecosystem participants based on the services they provide, particularly for QTSPs due to strict qualification requirements and regular conformity assessment [8], [13]. Developing sustainable business models and monetization strategies for attribute attestations is essential for the successful implementation of a self-sustaining wallet ecosystem [14]. Castaldo et al. [14] identify three different pricing models, given that the system architecture incorporates fitting verification and attribute management methods to support the corresponding model:

- **Issuance-based**: In a *pay-per-issuance* fashion, the user covers the cost of receiving a verified attribute [15].
- **Verification-based**: Contrary to the above model, the relying party would be required to *pay-per-use* upon verifying a presented credential [15].
- **Free of charge**: Neither the wallet user nor the verifier have to pay. To ensure sustainability, this would most probably require external funding such as government subsidies [13].

With the foundational principles established, this paper now focusses on the issuance and use of digital university diplomas as a representative use case of QEAA.

3. Use Case: QEAA for University Diplomas

This section showcases how the abstract technical components and ecosystem participants translate into real-world implementations, namely digital university diplomas. Graduates typically need to prove their qualifications for employment or further study. Paper-based verification is slow, error-prone, and susceptible to fraud [13], [16], with additional challenges in cross-border recognition [17]. The EUDI Wallet provides an opportunity for an interoperable, and user-oriented verification of educational qualifications [18]. Diplomas as QEAA are legally recognized, cross-border operational [12], and can be seamlessly integrated into digital workflows, e.g. supported by the EU's Single Digital Gateway, which aims to streamline access to public services across Member States [19]. In a sustainable ecosystem, participants require financial compensation for provided services. This paper therefore explores market models for issuing digital diplomas in the EUDI ecosystem.

3.1. Stakeholders and Roles

The stakeholders are the degree-awarding institution, a QTSP, the graduate, and the employer or higher education institution the graduate is applying to [3], [18]. The university acts as the issuer, but might partner with an external TSP instead of fulfilling that role exclusively itself. [3]. The graduate acts as the wallet user and the employer as the relying party.

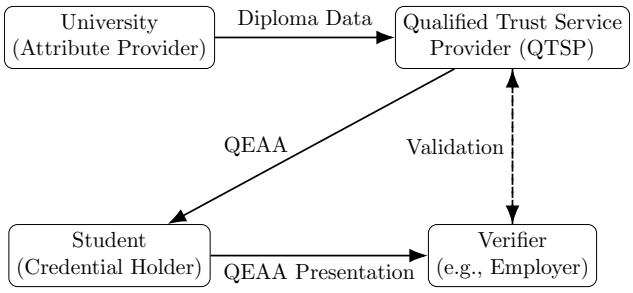

Figure 1: Attribute Issuance Workflow

Figure 1 shows the workflow for issuing and verifiying QEAA diplomas. Solid arrows indicate attribute data flow, and the dotted arrows the verification process. The university transfers the diploma information to the QTSP via a secure channel. Upon receiving the information and identifying the student, the QTSP issues a QEAA for the diploma to the student's wallet. Within an application process, the student presents these credentials to the employer, who verifies them via the QTSP's signature [3].

3.2. Incentive Structure and Value Gain

To identify applicable market models for the presented use case, it is necessary to understand the stakeholders' incentives, especially their potential financial benefits. This is important when considering the central question of who is willing to pay for the attribute attestation.

- Issuing universities may benefit from improved process efficiency, enhanced reputation, and compliance with EU digital standards [3].
- Graduates gain portable, verifiable credentials that improve cross-border access to jobs and education [18].
- Employers can reduce hiring costs and impede fraud through digital verification [16].
- QTSPs directly monetize their services through their attestation business models [14].

 doi: 10.2313/NET-2025-11-3_11

3.3. Related Work

Vaziri et al. [3] analyze the use case of universities issuing digital diplomas, considering the regulatory and operational challenges under the eIDAS 2.0 regulation. A comparison of the approaches of diplomas as QEAA as opposed to qualified sealed documents, reveals that "QEAA offers superior interoperability and holder binding, [but] it faces regulatory uncertainty and implementation complexities" [3, p. 183]. Vaziri et al. explore scenarios where the university becomes a QTSP, outsourcing to an external QTSP as shown in Figure 1, university alliances, and a "bring-your-own-QTSP" [3, p. 189] model. Vaziri et al. [3] and Seegebarth et al. [2] also explore the possibility of credentials electronically signed as qualified electronic seals (QSeals) according to eIDAS 1.0, to ease adoption until QEAA are fully applicable in the market.

4. Market Models for QEAA-Based Diploma

Having established the operational dynamics of digital diplomas in the EUDI ecosystem, we now focus on the market models that could emerge to support, govern, and monetize such use cases. Understanding the value exchange mechanisms and the economic and social implications for each market model is important for assessing the benefits and limitations for stakeholders. Implementing QEAA-based diplomas requires upfront investment and ongoing compensation. Strong incentives for stakeholders, in the form of substantial value gains, are necessary to promote stakeholders' willingness to pay. Network effects also play a role, as a full transition from paper-based to QEAA diplomas depends on widespread issuance and employer adoption of digital application processes. While graduates do benefit, as outlined in Section 3.2, their benefits are not financial and their willingness to pay is low, as a consequence [16]. Additionally, as the EUDI Wallet is intended to be free for users [13], market models must focus on other stakeholders.

This section presents five models, based on either the university, the government, or the verifier bearing the primary cost. As the academic literature regarding formalized market models for QEAA is scarce, these models are mainly adopted from SSI-related monetization strategies, or transferred from related trust services.

4.1. University-Centric

Similarly as proposed by Vaziri et al. [3], the university-centric approach considers both the possibility of the university becoming a QTSP and enlisting an external QTSP.

4.1.1. Internal QTSP. In this market model, the university itself becomes a QTSP and directly issues QEAA for diplomas. This model provides a high level of trust, since the university acts as both the authentic source of the academic credential and is responsible for its authenticity [3]. For verifiers, this direct issuance simplifies trust relationships as there is no dependency towards external issuers. The university's motivations might include the ability to exercise full control over credential issuance and remaining the technical authority for authenticity, which is also visible in the attribute attestation [3]. This approach could also help avoid vendor lock-in by reducing reliance on third-party infrastructure.

To gain and maintain the qualification status, universities must meet strict requirements and regularly face conformity assessments. Vaziri et al. [3] conclude that the regulatory and financial requirements are too high, especially for smaller universities. University alliances, such as EuroTeQ [20], could reduce the operational cost per university. This approach could be considered a hybrid version of the internal and external QTSP model.

4.1.2. External QTSP. In the external QTSP model, universities enlist an already accredited QTSP. The university maintains its role as the authentic source, while delegating the technical processes of credential creation, signing, and lifecycle management to the external QTSP [3]. The primary benefit in comparison to the internal approach is that universities can implement eIDAS-compliant credentials without substantial upfront investments. For verifiers, trust in the credential depends on both the external QTSP, and the university that is referenced in the QEAA as the attribute source [3]. However, it introduces a long-term dependence on the external service provider.

The university's financial gain depends on the price for issuing a QEAA-diploma compared to a paper-diploma, and whether the paper-based process can be replaced entirely. As of now, there is no standard price for QEAA in the European market. Since both services are regulated trust services under eIDAS, the pricing model might be similar to that of remote qualified electronic seals, allowing for an estimate. Sign8 is a German QTSP, that charges approximately 2.50 EUR per signature, within a volume-based pricing model [21]. In the year 2023, the Technical University of Munich (TUM) had 9 541 graduates [22]. Assuming no more than 12 000 graduates per year, TUM would be charged up to 30 000 EUR per year by Sign8.

4.2. Government-Centric

In the use case of QEAA diplomas, the government was not considered a stakeholder so far, despite its significant role in the EUDI ecosystem. It plays a crucial part either by directly providing the wallet infrastructure or by enabling private providers to do so in a competitive market [13]. This role was neglected in the previous consideration because the infrastructure provider does not significantly influence the presented market models. However, given the government's involvement, government-supported market models will also be considered.

External funding via direct subsidies could reduce the financial barrier for the issuance of digital diplomas by making the outsourcing model more financially sustainable, especially for smaller universities. Alternatively, state-operated TSPs could be established, issuing the diplomas on behalf of universities free of charge, comparable to the issuance of PuB-EAA [11]. At the same time, this could introduce bureaucratic burdens, slow down innovation cycles, and may raise concerns about institutional autonomy. Nonetheless, government-supported issuance could enhance accessibility to QEAA diplomas for all universities and support financial sustainability, if the ecosystem is not self-sustaining.

4.3. Verifier-Centric

Long-term self-sustainability in the EUDI Wallet ecosystem can also be achieved if the verifier contributes to the financial compensation. As verifiers, such as employers, benefit from improved credential verification processes, making manual verification obsolete and preventing fraud, they have an incentive to invest [13], [16]. Similarly as for the university-centric models, the willingness to pay depends on the opportunity cost compared to current paper-based verification processes.

4.3.1. Pay-Per-Verification. The Pay-Per-Verification model is based on the verification-based monetization strategy on the side of the QTSP. This model is transferred from market models for digital identification services, such as know-your-customer processes, in which the relying party pays an identity provider per user identification [23]. In this analogy, the QTSP corresponds to the identity provider and the employer to the relying party.

Universities collaborate with external QTSPs, which employ a verification service that charges the verifier to establish a usage-based monetization [14]. Cost for universities and students would be eliminated and transferred to the employer. However, if different universities use different QTSPs without a unified verification interface, this could introduce process inefficiencies as employers have to adapt to the corresponding interfaces.

Additionally, privacy concers arise from tracking verification requests for billing purposes. This tracking could potentially lead to exposure of information regarding the verification of credentials by specific parties. Depending on the implementation, service providers could potentially link users and credentials to verification requests, and ultimately to the verifier [14], [16]. However, Castaldo et al. [14] suggest a verification approach that would maintain user anonymity and eIDAS compliance, even considering a verification-based monetization strategy.

4.3.2. Sponsored Attestation. Academic credentials are typically static, therefore they would be issued once and potentially verified multiple times [13]. The pay-per-verification model has the potential to establish long-term sustainability and support ongoing maintenance of the trust infrastructure. However, frequent verification fees might discourage adoption from the employer's side.

In the Sponsored Attestation model, companies that directly benefit from the academic training of students cover the costs of issuing eIDAS-compliant digital diplomas. This model is particularly interesting when empirical evidence indicates that a significant proportion of university graduates are likely to apply to a particular employer. Examples of this use case could be dual study programs or university-industry partnerships, such as those between TUM and SAP [24].

Similarly to government funding, universities would benefit due to the reduced financial demand while strengthening institutional ties with partners. However, this approach could potentially result in unequal access, where students of universities without industry partners might lack digital academic credentials. This could lead to a heterogeneous credential ecosystem and negative network effects.

Nonetheless, this model could support the adoption of QEAA and a self-sustainable ecosystem by aligning financial responsibility with financial benefits for the employer. These employers could also benefit from this model if it is implemented in the early stages when digital credentials are not yet established as market standard. This would give them early access to the benefits of digitally verifiable academic credentials.

4.4. Adoption Phase

The implementation of verifiable credentials in business processes is subject to network effects [13]. Integrating QEAA into processes requires substantial investments in infrastructure and system integration, while the return on investment depends on the usage rate. This effect could hinder the use of QEAA-diplomas in the early stages of EUDI ecosystem development, as the potential return on investment may seem too low.

Seegebarth et al. [2] suggest splitting the transition towards QEAA into two phases, whereas the first phase represents an adoption phase. During this phase, verifiable credentials would be implemented as eIDAS compliant qualified sealed documents [2], [3]. The infrastructure for this approach is already implemented and stakeholders could gain trust and experience with the technology at a lower cost, before QEAA will be fully utilized in the second phase. Ultimately, QEAA are superior to the QSealed document approach due to higher interoperability, seamless process integration, and selective disclosure features [3].

5. Conclusion

As eIDAS 2.0 facilitated the widespread adoption of the EUDI wallet and QEAA-based credentials, the question of how market models will shape the issuance and verification of digital diplomas becomes increasingly critical. The models explored in this paper differ in funding, monetization strategy, and stakeholder dependencies and obligations, based on their respective incentive structures.

The internal QTSP approach provides the university with maximum institutional control, but it requires the university to meet strict conformity requirements, which introduces high costs, making it not viable especially considering smaller universities. Outsourcing to external QTSPs offers better operational efficiency but introduces dependencies on third parties.

Government-supported models would improve accessibility independent of the university's size and budget. Public funding may also support adoption, as network effects limit stakeholders' willingness to invest during early stages with low returns. Both direct subsidies and central public services could support equity and adoption but might reduce flexibility and institutional autonomy.

The pay-per-verification and sponsored attestation approaches would directly link costs to verifiers' benefits but could introduce privacy risks or unequal access. The willingness to pay for both the issuing universities and employers depends on the transition cost and operational cost compared to paper-based diplomas.

 doi: 10.2313/NET-2025-11-3_11

Further work could include comparative analyses regarding the cost and effort between paper-based and digital credential issuance and verification. Hybrid approaches could also be applied since it is unlikely that one single model will universally fit all educational contexts. Ultimately, the success and sustainability of QEAA-diplomas will depend on balancing financial sustainability, privacy, and institutional autonomy.

References

[1] European Parliament and Council of the European Union, "Regulation (eu) no 1183/2024 amending regulation (eu) no 910/2014 to establish the european digital identity framework," https://eur-lex.europa.eu/eli/reg/2024/1183/oj, 2024, [Online; accessed 07-June-2025].

[2] C. Seegebarth, P. Bastian, and M. Kraus, "Enabling attribute attestations: Road from verifiable credential to qeaa," *Datenschutz und Datensicherheit-DuD*, vol. 48, no. 4, pp. 237–240, 2024.

[3] A. Vaziry, L. Vetter, and A. Küpper, "eidas 2.0: Evaluating the issuance of digital university diplomas," in *Open Identity Summit 2025*. Gesellschaft für Informatik eV, 2025, pp. 183–190.

[4] European Parliament and Council of the European Union, "Regulation (eu) no 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing directive 1999/93/ec," https://eur-lex.europa.eu/eli/reg/2014/910/oj, 2014, [Online; accessed 07-June-2025].

[5] European Commission, "Study to support the impact assessment for the revision of the eidas regulation - final report," https://digital-strategy.ec.europa.eu/en/library/study-support-impact-assessment-revision-eidas-regulation, 2021, [Online; accessed 07-June-2025].

[6] C. Busch, *eIDAS 2.0: Digital Identity Services in the Platform Economy*. Centre on Regulation in Europe, 2022.

[7] J. Inza, "The european digital identity wallet as defined in the eidas 2 regulation," in *Governance and Control of Data and Digital Economy in the European Single Market: Legal Framework for New Digital Assets, Identities and Data Spaces*. Springer Nature Switzerland Cham, 2025, pp. 433–452.

[8] S. Schwalm, "The possible impact s of the eidas 2.0 digital identity approach in germany and europe," in *Open Identity Summit 2023*. Gesellschaft für Informatik eV, 2023, pp. 109–120.

[9] N. Urbach, T. Guggenberger, H. Pfaff, J.-C. Stoetzer, S. Feulner, M. Babel, M. Principato, and J. Lautenschlager, "Eu digital identity wallet - anwendungsfälle, nutzungspotenziale und herausforderungen für unternehmen," Projektgruppe Wirtschaftsinformatik des Fraunhofer-Institut für Angewandte Informationstechnik FIT, Bayreuth, 2024.

[10] J. Strüker, N. Urbach, T. Guggenberger, J. Lautenschlager, N. Ruhland, V. Schlatt, J. Sedlmeir, J.-C. Stoetz, and F. Völter, "Self-sovereign identity - grundlagen, anwendungen und potentiale portabler digitaler identitäten," Projektgruppe Wirtschaftsinformatik des Fraunhofer-Institut für Angewandte Informationstechnik FIT, Bayreuth, 2021.

[11] Potential, "What are the 3 types of electronic attestations of attributes (eaa)?" Apr 2025, [Online; accessed 07-June-2025]. [Online]. Available: https://www.digital-identity-wallet.eu/news/what-are-the-3-types-of-electronic-attestations-of-attributes-eaa/

[12] European Commission, "Eu digital identity wallets for issuers," [Online; accessed 07-June-2025]. [Online]. Available: https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/Wallet+for+Issuers

[13] K. Degen and T. Teubner, "Wallet wars or digital public infrastructure? orchestrating a digital identity data ecosystem from a government perspective," *Electronic Markets*, vol. 34, no. 1, p. 50, 2024.

[14] L. Castaldo, G. Cortese, S. Izzo, and F. Balsamo, "Electronic attestation of attributes extended validation services," *TDI 2025: 3rd International Workshop on Trends in Digital Identity*, 2025.

[15] M. Panfilio, "Possible architectures of digital european wallets: national certifications and the roles of key stakeholders," Namirial, Feb 2025, [Online; accessed 07-June-2025]. [Online]. Available: https://www.namirial.com/en/inspiration/possible-architectures-of-digital-european-wallets/

[16] M. Kubach and H. Roßnagel, "Economically viable identity ecosystems: Value capture and market strategies," in *Open Identity Summit 2024*. Gesellschaft für Informatik eV, 2024, pp. 27–38.

[17] Your Europe, "Recognition of academic diplomas," [Online; accessed 09-June-2025]. [Online]. Available: https://europa.eu/youreurope/citizens/education/university/recognition/index_en.htm

[18] P. Herbke and H. Yildiz, "Elmo2eds: transforming educational credentials into self-sovereign identity paradigm," in *2022 20th International Conference on Information Technology Based Higher Education and Training (ITHET)*. IEEE, 2022, pp. 1–7.

[19] Bundesministerium für Digitales und Staatsmodernisierung, "Die single digital gateway-verordnung (sdg)," [Online; accessed 23-August-2025]. [Online]. Available: https://www.digitale-verwaltung.de/Webs/DV/DE/onlinezugangsgesetz/info-sdg/info-sdg-node.html

[20] EuroTeQ, "About euroteq - how six universities engineer the future," [Online; accessed 20-June-2025]. [Online]. Available: https://euroteq.eurotech-universities.eu/about-us/

[21] SIGN8, "Volumenbasierte modelle - digitale unterschriften sign8," [Online; accessed 10-June-2025]. [Online]. Available: https://sign8.eu/volumebased/

[22] TU München, "Tum in zahlen 2023," [Online; accessed 10-June-2025]. [Online]. Available: https://mediatum.ub.tum.de/doc/1774468/1774468.pdf

[23] V. Schlatt, J. Sedlmeir, S. Feulner, and N. Urbach, "Designing a framework for digital kyc processes built on blockchain-based self-sovereign identity," *Information & Management*, vol. 59, no. 7, p. 103553, 2022.

[24] TU München, "Sap@tum collaboration lab," [Online; accessed 20-June-2025]. [Online]. Available: https://www.ioc.tum.de/sap-colab/startseite/