Journal of Computer and Communications, 2026, 14(3), 17-26
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

The Development of Electronic Signature Processes in Türkiye and an Analysis of the Requirements for the Transition to Elliptic Curve Cryptography (ECC)

Mutlu Uysal[1*], Nursel Yalçın[2]

[1]Department of Computer Forensics, Institute of Informatics, Gazi University, Teknikokullar, Ankara
[2]Department of Computer and Instructional Technologies Education, Gazi Faculty of Education, Gazi University, Teknikokullar, Ankara
Email: *uysal.mutlu@gmail.com, nyalcin@gazi.edu.tr

How to cite this paper: Uysal, M. and Yalçın, N. (2026) The Development of Electronic Signature Processes in Türkiye and an Analysis of the Requirements for the Transition to Elliptic Curve Cryptography (ECC). *Journal of Computer and Communications*, **14**, 17-26.
https://doi.org/10.4236/jcc.2026.143002

Received: January 21, 2026
Accepted: March 2, 2026
Published: March 5, 2026

Abstract

This article mainly discusses the history of progress regarding the legislation and updates through scrutiny, its current architecture, and its standards applied around the world, such as eIDAS and eIDAS 2.0, which are used not only as technical but also as purely political standards. The penetration of the digital economy has largely promoted the evolution of cyber platforms for public and private use, so that e-signatures have become one of the pillars in the national IT architecture. 1) Legislation The e-signature operations in Türkiye are regulated by Electronic Signature Law No. 5070 and its secondary regulations. However, today, the infrastructure groundwork relies heavily on RSA-based cryptography. RSA is attracting greater and more debate these days, with concerns about whether it will continue to be useful given the increasing importance of security requirements for mobile devices, performance expectations, and the threat posed by quantum computing. This article also examines the extent to which Turkish law is compatible with the EU regulation of compliance. In this paper, we study whether the Turkish legislation complies with the European legislation. This covers security, performance, key size, and support for RSA and Elliptic Curve Cryptography (ECC) algorithms. This paper discusses technical, institutional, and legal requirements for the transition of the national e-signature infrastructure to ECC. Furthermore, ECC's contribution is evaluated in terms of Post-Quantum Cryptography (PQC), and a roadmap is suggested for transitioning to hybrid (ECC + PQC) architectures. Finally, policy and technical suggestions are proposed to facilitate international electronic and

mobile signature interoperability under eIDAS 2.0.

Keywords

Electronic Signature, Elliptic Curve Cryptography (ECC), eIDAS 2.0, Digital Identity, Post-Quantum Cryptography, Public Certification Authority

1. Introduction

In our digital age, electronic signatures have quickly become important instruments to ensure that transactions are secure and legally binding. Since the early 2000 s, various e-government initiatives and digital transformation projects in Türkiye have relied heavily on electronic signature systems [1]. As more people embrace digital communication, the need for efficiency, security, and legal certainty in our interactions has become paramount.

But this, of course, presents some challenges as of today. As the volume of transactions increases, we are becoming aware of some areas of our existing infrastructure that are not well-suited. In particular, new opportunities with mobile devices, as well as the Internet of Things (IoT), are opening doors, and there is a pressing need for the alignment of our systems with international standards. Finally, quantum computers represent a long-term threat to classical asymmetric cryptography, which makes it imperative to fully reassess our current cryptographic systems.

The primary focus of this research is to examine the development and current status of electronic signatures in Türkiye. We aim to explore the necessity and feasibility of transitioning from the existing RSA-based systems to elliptic-curve cryptographic (ECC) solutions.

This paper will address several key areas:

- We will assess Türkiye's Law No. 5070 in relation to the EU's eIDAS and eIDAS 2.0 legislation [1].
- We'll evaluate the performance of the RSA and ECC algorithms in terms of speed, safety, and overall effectiveness [2] [3].
- The study will investigate the adoption of ECC within both the public and private sectors in Türkiye, identifying any technical and institutional obstacles that may exist [4].
- We will analyze the significance of ECC in the context of post-quantum cryptography (PQC) design and propose hybrid architectures to enhance security [5].
- Lastly, we will suggest strategies for implementing digital identity wallets and mobile signatures in line with eIDAS 2.0 [6].

Through this research, we hope to contribute valuable insights into the future of electronic signatures in Türkiye and their alignment with global standards.

2. Material and Method

To this end, this research adopts a qualitative methodology, supported by document and literature reviews and comparative technical evaluation. This qualitative approach not only informs the study but also highlights how qualitative analysis can contribute to better public health. Legal texts, laws, and international conventions were reviewed comprehensively in the course of our research.

2.1. Data Sources

The main sources of data used in this study are as follows:

- **Source of Legal and Regulatory Text:** Electronic Signature Law No. 5070 [7], publications of Information Technologies and Communication Authority (BTK) regulations [8]-[10], and Prime Ministry circulars concerning the Public Certification Authority [11].
- **International Standards:** EU eIDAS and eIDAS 2 regulations [12] [13], ETSI standards (EN 319 4xx series) [14] [15], ISO/IEC 14888 [16], and ITU-T X.509 recommendations [17].
- **Technical Reports and Guides:** NIST and NCCoE publications, reports on PQC transition [1] [18], and Informatics and Information Security Research Center (TÜBİTAK BİLGEM) (Public Certification Authority) technical guides [19].
- **Academic Literature:** Research addresses comparisons of RSA and ECC effectiveness and the legal perspective of e-signatures in Türkiye [1]-[6] [20].

2.2. Analysis Method

Comparative analysis was applied to the collected dataset. Comparing Türkiye's legal framework with EU regulations revealed gaps. The technical performance parameters of the cryptographic algorithms were compared with respect to their theoretical security levels (bit strength) and practical performance indicators (signing speed and key size). Finally, a SWOT analysis was conducted to assess Türkiye's readiness for ECC transition.

3. Legal and Institutional Framework in Türkiye

3.1. Electronic Signature Law No. 5070

Since 2004, Law No. 5070 of Türkiye has been the backbone of the country's legal system for electronic signatures. It elaborates on the notion of a "secure electronic signature," "qualified electronic certificate" (QEC), and "time stamp," and accordingly states that a secure electronic signature receives the same legal significance that a handwritten signature does [7]. This regulation also governs Electronic Certificate Service Providers (ECSPs).

3.2. Secondary Regulations and the Role of the BTK

The Information Technologies and Communication Authority (BTK) is the agency responsible for regulating ESHS and establishing technical specifications. Second-

ary regulations, such as the "Electronic Signature and Certificate Services Regulation" [9], define ESHS responsibilities concerning key generation, storage, and key physical security. These regulations provide a stable, dependable infrastructure.

3.3. Public Certification Authority (Kamu SM)

Kamu SM, set up in TÜBİTAK BİLGEM, is the root certificate authority for all the public institutions in Türkiye. It issues qualified electronic certificates to public officials and manages the lifecycle of certificates in its e-government ecosystem [19].

4. European Union Framework: eIDAS and eIDAS 2.0

4.1. eIDAS Regulation

eIDAS (Regulation [EU] No. 910/2014) establishes standard rules for legal frameworks for electronic identification and trust services (including electronic signature, seal, timestamp, electronic delivery service, etc.) within the European Union [12]. Regulation (EU) 2015/1509 sets out minimum requirements for qualified electronic signatures and trust service providers [14].

4.2. eIDAS 2.0 and the European Digital Identity Wallet

eIDAS 2.0 (Regulation [EU] 2024/1183) defines the European Digital Identity Wallet, which will provide citizens with an opportunity to carry and make use of their digital identity assets within a secure environment using smartphones [15]. Through the stored secret in the hardware keys of such wallets, electronic signatures and identity authentication are completed [15].

4.3. Level of Compliance of Turkish Legislation with eIDAS

It is established that Türkiye's electronic signature laws, in general, are compatible with eIDAS, especially in connection with qualified electronic signatures, ESHS criteria, and legal aspects of electronic signatures [1]. Nevertheless, Türkiye needs to develop more legislation and technical infrastructure for the digital identity wallet, mobile signature, and cross-border recognition as defined under eIDAS 2.0.

5. Comparative Analysis of RSA and ECC Algorithms

5.1. Cryptographic Fundamentals

RSA security relies on the Integer Factorization Problem (IFP), whereas ECC depends on the Elliptic Curve Discrete Logarithm Problem (ECDLP). ECDLP is exponentially more challenging than IFP for the same key size, allowing ECC to offer similar security with far fewer keys than RSA.

5.2. Key Size and Security Levels

According to NIST recommendations, achieving a 128-bit security level (comparable to AES-128) requires a 3072-bit RSA key, whereas ECC requires only a 256-

bit key (e.g., the P-256 curve) [18]. This discrepancy becomes even more glaring at higher security tiers; at 256-bit security, RSA must use a practically impossible 15360-bit key, while ECC requires only 521 bits.

5.3. Performance Evaluation

ECC's efficiency compared to RSA has been demonstrated in multiple studies. As Table 1 shows, ECC takes less time for signing, retains keys far more efficiently, and uses less memory and storage than RSA [2] [3]. The data presented in the table have been derived from a compilation of the cited literature and various field tests.

Table 1. Performance comparison of RSA and ECC algorithms.

Parameter	RSA (2048 bits)	ECC (P-256)	Difference
Signing Time	35 ms	6 ms	~6 times faster
Verification Tim	9 ms	3 ms	~3 times faster
Key Storage Size	256 bytes	64 bytes	~4 times smaller
Memory Usage	12 MB	3 MB	~¼ reduction

The performance metrics of ECC demonstrate its effectiveness in resource-constrained environments such as mobile devices, smart cards, and Internet of Things sensors [4]. ECC is also advantageous for large-scale key generation operations. According to [3], minor key and signature sizes during the certificate lifecycle are said to be cost-effective for bandwidth and storage by diminishing the sizes of CRL and OCSP responses. RSA is the default in many legacy systems because it is older and more extensively used than the others. Nevertheless, current libraries and systems provide mature support for ECC. Mainly, web browsers and modern operating systems have native implementations of TLS certificates and code signatures based on ECC [1] [4].

6. Findings: Current Transition Status

Traditionally, the e-signature infrastructure in Türkiye has primarily adopted RSA in the past. RSA keys are widely used to establish root and sub-root certificates by Kamu SM and private ESHS [1]. In the PR, the ECC-based root certificates were developed by Kamu SM in 2019 and were intended to become operational by 2020. Testing began in 2019 with Kamu SM using e-signatures for large-scale public-sector applications, and was intended to focus on ECC algorithm-based e-signatures in 2020; regulatory amendments were considered.

Although the planning and transition schedule were clearly stipulated in the legislation, the actual transition could only be initiated in 2023 due to a multitude of factors. These included the delayed commencement of software compliance efforts within the specified timeframe, insufficient human resources, delays in software updates, and latency experienced in decommissioning legacy cards and tran-

sitioning to new ones following the requirement for card updates. Consequently, the production of e-signatures derived from ECC root certificates by the Public Certification Authority (Kamu SM) began in 2023. Furthermore, Kamu SM has been issuing ECC-based electronic seal certificates since 2024. Pilot studies conducted in public institutions utilizing Electronic Document Management Systems (EDMS) and Registered Electronic Mail (REM) systems have successfully achieved seamless ECC integration. However, while the transition in the public sector was accomplished within a five-year period, the transition among private Electronic Certificate Service Providers (ECSPs) remains incomplete due to challenges such as the lack of support for the required new cards across all field software and delays in the procurement of compatible tokens.

Despite these efforts, widespread adoption is hindered by incompatibility with legacy hardware (e-signature cards, HSM, Turkish ID cards) and the need for software updates in client-side applications. In truth, based on the reasons explained, the authority institution BTK has extended the transition period to new generation algorithms in the second paragraph of Article 6 of the Communique on Processes and Technical Criteria Related to Electronic Signatures, published in the Official Gazette of the Republic of Türkiye, dated October 4, 2025, and numbered 33037. The transition to the new generation is now extended until December 31, 2027.

7. Discussion

In Türkiye, the transition from RSA to ECC is not just a technical upgrade, but it is also a strategic necessity involving legal, institutional, and security aspects. In this section, we present the evidence-finding, the strategic status of Türkiye based on a SWOT analysis, the impact of post-quantum cryptography, as well as the roadmap for digital identity wallets.

7.1. Strategic Analysis of the Transition (SWOT)

A comparative SWOT analysis was performed, based on the existing system and regulatory infrastructure, to measure how the transition to the ECC would proceed.

- **Strengths:** Türkiye has a strong legal system characterized by a robust legal framework embodied in Law No. 5070 and the Central Public Certification Authority (Kamu SM) [11]. BTK and TÜBİTAK BİLGEM should provide the technical expertise upon which to base such a transition. Moreover, the rapid diffusion of new technologies is promoted by citizens' adoption of e-government services.
- **Weaknesses:** The law or technical circulars in force today rely predominantly on RSA, which results in regulatory lag. There are few staff trained in ECC and current cryptographic systems. Modern elliptic curves are not supported by hardware security modules (HSM) or smart cards today, which will then require expensive hardware upgrades.

- **Opportunities:** Adherence to eIDAS 2 can enable the European Digital Single Market. ECC performs better than other cryptographic techniques, which results in better end-user experiences for mobile applications. It also opens the way toward the development of domestic ECC libraries and crypto products and the phasing out of foreign technologies.
- **Threats:** One of the biggest threats to the development of the system is that there will exist a new threat of delay in the adoption of PQC (post-quantum cryptography), and it may potentially hinder the development of PQC. Lack of any focus on ECC individually could lead to a myth of long-term absolute security without consideration of the quantum implications. Rapidly changing cyber threats and the possibility of "collect now, solve later" attacks must be mitigated.

7.2. Post-Quantum Cryptography (PQC) and Hybrid Strategy

While it has all the advantages over RSA, ECC is susceptible to the Shor algorithm on fast quantum computers [5]. This poses an authentic conundrum: Should Türkiye adopt ECC now or wait for PQC standards to develop? The analysis of data shows that we are unable to support PQC due to the fast-paced, high-performance requirements of mobile/IoT systems, and this is compounded by the fact that PQC standards (e.g., CRYSTALS-Dilithium) continue to evolve and require larger key sizes than ECC [18]. ECC therefore acts as an essential "bridge" technology in the short- and medium-term (10 - 15 years).

We suggest a hybrid strategy:

1) Transition Period: Replace RSA with ECC (P-256/P-384); reducing the bandwidth and improving mobile performance.

2) Transition Period: Hybrid certificates containing both an ECC key and a PQC key should be implemented. These certificates incorporate both a classical ECC key and a quantum-resistant PQC key within a single certificate structure as a dual-key mechanism. This dual-key architecture enables systems to continue utilizing ECC signatures, which are efficient and compatible with current verification processes, while the PQC signature ensures long-term validity against future quantum attacks [15].

3) Long Term: The complete transition should be realized once standards, as well as support for the hardware technology, are mature and the PQC algorithms have been developed.

7.3. Digital Identity Wallets and eIDAS 2.0 Compliance

The "European Digital Identity Wallet" (EUDI Wallet) introduced by the eIDAS 2.0 regulation has changed from card-based to mobile digital wallets for identity information. The ecosystem in Türkiye depends on physical smart cards (Turkish ID Cards and Qualified Electronic Certificates on USB tokens). Türkiye needs to develop a "National Digital Identity Wallet" architecture to enable interoperability with the EU. The ECC framework is the de facto standard for mobile wallets

across all these, mainly because smartphones do not support the limited Secure Elements (SE) and Trusted Execution Environments (TEE). RSA keys are often too large to be produced and stored effectively in secure regions. As a result, it is essential to adopt ECC for a practical, interoperability-respecting national digital wallet. The wallet needs to fuse its National ID card, e-Government login details, and qualified electronic signatures into one mobile facility and be able to facilitate protocols, like OpenID Connect for federation [6].

7.4. Roadmap for ECC Integration

Based on this discovery, a roadmap is also suggested for the Turkish national infrastructure:

1) Policy and Regulatory Updates: Policy and Regulatory Updates: BTK should upgrade its secondary regulations to include ECC parameters and certificate profiles that are ETSI EN 319 412-5-compliant [15].

2) Root Authority Transition: All ESHSs and the Kamu SM should establish ECC root CAs, and not only the Kamu SM. To maintain backward compatibility, a parallel operational period (dual stack) is necessary, during which RSA and ECC certificates remain valid.

3) Client-Side Modernization: Middleware that is used in EBYS and KEP software, e-signature-creating applications, and libraries should be updated to process ECC keys.

4) Pilot Deployments: Pilot projects undertaken by the Kamu SM shall be extended to include mobile signatures and national ID card digital certificate functions.

5) PQC Readiness: A nationwide "Crypto Agility" inventory should be maintained to determine all crypto assets, which would allow for future upgrading of the PQC.

8. Conclusions

Nevertheless, the current study concluded that, although Türkiye has an excellent legal and institutional environment for electronic signatures, the RSA-based technology is becoming outdated. The move to Elliptic Curve Cryptography is essential to meet the performance requirements of today's mobile revolution, ensure compliance with national standards, and ensure it is in the right place and at the right time, as also set by international standards such as eIDAS 2.0.

Advantages of ECC:

- Smaller keys,
- Faster signing,
- Lower energy consumption.

Resolving the key bottlenecks in the current system.

That said, such a transition must be undertaken in a forward-looking way with post-quantum cryptography at the forefront. A hybrid strategy is currently being used in our country to manage the transition to e-signatures. However, ECC cer-

tificates cannot be loaded onto Turkish IDs or GSM lines at this stage, as existing card technologies are antiquated. Moreover, with years of experience and continuous work on the transition to ECC certificates, accelerating their issuance will be possible. With a progressive, modern legal framework to support digital wallets, the digital infrastructure can be built and integrated into the global digital economy. In its mission to comply with the eIDAS 2 regulatory framework, the technical and legal regulations our country will implement will ensure that the e-signatures it adopts are recognized and accepted across the European Union.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Seyirt, M., Özcan, T., Karabulut, B., Doğan, S.M. and Akman Harmancı, E. (2024) Elektronik İmza Standartlarındaki Güncellemeler ve Türkiye'deki Mevcut Durum. *Bilgi Yönetimi*, **7**, 1-15. https://doi.org/10.33721/by.1473545

[2] Gura, N., Patel, A., Wander, A., Eberle, H. and Shantz, S.C. (2004) Comparing Elliptic Curve Cryptography and RSA on 8-Bit CPUs. *Proceedings of the 6th International Workshop on Cryptographic Hardware and Embedded Systems* (*CHES*), Cambridge, 11-13 August 2004, 119-132. https://doi.org/10.1007/978-3-540-28632-5_9

[3] Kaya, A. and Türkoğlu, İ. (2023) Simetrik ve Asimetrik Şifreleme Algoritmalarının Performans Karşılaştırılması. *Fırat Üniversitesi Mühendislik Bilimleri Dergisi*, **35**, 891-900. https://doi.org/10.35234/fumbd.1296228

[4] Çekiş, İ.K., Toros, A., Apaydın, N. and Özçelik, İ. (2024) Performance Comparison of ECC Libraries for IoT Devices. *Eskişehir Technical University Journal of Science and Technology A—Applied Sciences and Engineering*, **25**, 278-288. https://doi.org/10.18038/estubtda.1427488

[5] National Cybersecurity Center of Excellence (NCCoE) (2021) Transitioning to Post-Quantum Cryptography (NIST SP 1800-36). NIST.

[6] Çimen, C., Akleylek, S. and Kılıç, E. (2023) Bilgi Güvenliği ve Kriptografi (5. Baskı). Papatya Bilim.

[7] Electronic Signature Law No. 5070 (2004) Official Gazette of the Republic of Türkiye, No. 25355. https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5070&MevzuatTur=1&MevzuatTertip=5

[8] Bilgi Teknolojileri ve İletişim Kurumu (2006) Güvenli Elektronik İmza Oluşturma ve Doğrulama Uygulamaları ile Güvenli Elektronik İmza Formatlarına Dair Usul ve Esaslar. https://www.btk.gov.tr/uploads/pages/guvenli-elektronik-imza-formatlarina-dair-usul-ve-esaslar-5a33fef63b234.pdf

[9] Bilgi Teknolojileri ve İletişim Kurumu (2020) Elektronik İmza Kanununun Uygulamasına İlişkin Usul ve Esaslar Hakkında Yönetmelik. Official Gazette of the Republic of Türkiye, No. 31523. https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=7224&MevzuatTur=7&MevzuatTertip=5

[10] Bilgi Teknolojileri ve İletişim Kurumu (2005) Elektronik İmza İle İlgili Süreçlere Ve Teknik Kriterlere İlişkin Tebliğ. T.C. Resmi Gazete, Sayı: 25692.

https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=8716&MevzuatTur=9&MevzuatTertip=5

[11] Mülga Başbakanlık (2006) Kamu Sertifikasyon Hizmetlerine İlişkin Usul ve Esaslar (2006/13). T.C. Resmi Gazete, Sayı: 2614. https://www.resmigazete.gov.tr/eskiler/2004/09/20040906.htm

[12] European Union (2014) Regulation (EU) No 910/2014 on Electronic Identification and Trust Services (eIDAS). *Official Journal of the European Union*, 57, L257.

[13] European Union (2024) Regulation (EU) 2024/1183 Establishing a Framework for a European Digital Identity (eIDAS 2.0). *Official Journal of the European Union*,1-56.

[14] ETSI (2021) Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers (ETSI EN 319 401). ETSI.

[15] ETSI (2024) Electronic Signatures and Infrastructures (ESI); Certificate Profiles Supporting ECDSA, Ed25519, and PQC Signatures (ETSI EN 319 412-5). Sophia Antipolis: ETSI.

[16] ISO (2020) Information Technology—Security Techniques—Digital Signatures (ISO/IEC 14888). ISO.

[17] ITU-T (2020) Information Technology—Open Systems Interconnection—The Directory: Public-Key and Attribute Certificate Frameworks (Recommendation X.509). ITU.

[18] NIST (2022) Recommendation for Key Management: Part 1—General (SP 800-57 Part 1 Rev. 5). NIST.

[19] TÜBİTAK BİLGEM Public Certification Center (n.d.) Qualified Electronic Certificate Certificate Policy (CP). https://kamusm.bilgem.tubitak.gov.tr/BilgiDeposu/KSM_NES_SI/KSM_NES_SI.pdf

[20] Koç, Ç.K. (2009) Cryptographic Engineering. Springer.