BMBAD BJESR Mühendislik Bilimleri ve Araştırmaları Dergisi
Journal of Engineering Sciences and Researches

Java Card Tabanlı Platform Bağımsız Mobil İmzalama Sistemi

Java Card-Based Platform-Independent Mobile Signing System

[1]Ömer YILDIZ, [2]Ahmet Remzi ÖZCAN

[1]TÜBİTAK BİLGEM, UEKAE, Kocaeli, Türkiye

[2]Bursa Teknik Üniversitesi, Mühendislik ve Doğa Bilimleri Fakültesi, Bursa, Türkiye

[1]omer.yildiz@tubitak.gov.tr, [2]ahmet.ozcan@btu.edu.tr

Araştırma Makalesi/Research Article

ARTICLE INFO

Article history

Received : 13 May 2025
Accepted : 24 June 2025

Keywords:

Java Card, Digital Signature, NFC Communication, Secure Element, Cross-Platform Security

ABSTRACT

Secure storage of private keys is a fundamental requirement for cryptocurrency users in managing digital assets. However, existing hardware wallets (e.g., Ledger, Trezor) face limitations in terms of widespread adoption and integration due to their high cost, limited mobile compatibility, platform dependency, and closed-source nature. In particular, the lack of hardware-level support for iOS devices adversely affects user experience.

This study presents a platform-independent and application-free digital signature system developed using Java Card technology and the NFC-based NDEF standard. The proposed system features a dual-applet architecture running in isolation on Java Card: one applet parses NDEF messages, while the other performs cryptographic operations at the hardware level. Experimental validation using a React Native mobile client compatible with both Android and iOS confirms that the system delivers stable communication, high performance, and a user-friendly interaction model.

MAKALE BİLGİSİ

Makale Tarihleri

Gönderim : 13 Mayıs 2025
Kabul : 24 Haziran 2025

Anahtar Kelimeler:

Java Card, Dijital İmza, NFC Tabanlı İletişim, Güvenli Donanım Birimi, Platformlar Arası Güvenlik

ÖZET

Kripto para kullanıcıları için özel anahtarların güvenli biçimde saklanması, dijital varlık yönetiminin temel gereksinimidir. Ancak mevcut donanım cüzdanları (Ledger, Trezor vb.), yüksek maliyet, sınırlı mobil uyumluluk, platform bağımlılığı ve kaynak kodlarının kapalı olması nedeniyle yaygın kullanım ve entegrasyon açısından sınırlılıklar taşımaktadır. Özellikle iOS cihazlarla donanımsal entegrasyon eksikliği, kullanıcı deneyimini olumsuz etkilemektedir.

Bu çalışmada, Java Card teknolojisi ve NFC üzerinden NDEF standardı kullanılarak geliştirilen, platformdan bağımsız ve uygulama gerektirmeyen bir dijital imzalama sistemi sunulmaktadır. Sistem, Java Card üzerinde izole çalışan iki applet'ten oluşmakta; biri NDEF mesajlarını ayrıştırmakta, diğeri ise kriptografik işlemleri donanım düzeyinde gerçekleştirmektedir. Android ve iOS cihazlarla uyumlu geliştirilen React Native mobil istemci üzerinden yapılan testlerde, sistemin kararlı iletişim, yüksek performans ve kullanıcı dostu etkileşim sağladığı gözlemlenmiştir.

ORCID ID: [1]0000-0002-7163-4313
[2]0000-0002-4093-1059

1. GİRİŞ

Kripto paraların ve diğer dijital varlıkların finansal sistemlerdeki artan rolü, bu varlıkların güvenli biçimde saklanması ve yönetilmesini önemli bir ihtiyaç haline getirmektedir. Merkeziyetsiz yapıları gereği, bu sistemlerde kullanıcıların sahip olduğu özel anahtarlar, varlıklar üzerinde tam kontrol sağlayan tek unsurdur. Ancak geleneksel finansal yapılardan farklı olarak, merkezi bir otorite bulunmadığından, kimlik bilgilerinin kaybı ya da yetkisiz işlemler gibi durumlar geri alınamamaktadır. Bu nedenle, özel anahtarların güvenli şekilde saklanması dijital varlıkların korunması açısından hayati öneme sahiptir. Anahtarların kaybedilmesi ya da üçüncü tarafların eline geçmesi durumunda, kullanıcılar sahip oldukları varlıkları kalıcı olarak kaybetme riskiyle karşı karşıya kalmaktadır.

Günümüzde birçok yatırımcı, dijital varlıklarını merkezi borsalar veya çevrimiçi cüzdan servisleri aracılığıyla yönetmektedir. Ancak bu tür hizmetlerde özel anahtarlar hizmet sağlayıcıların kontrolünde bulunduğundan, kullanıcıya gerçek anlamda sahiplik sunulmamaktadır. Özellikle son yıllarda yaşanan büyük ölçekli siber saldırılar, borsa iflasları ve sistem açıkları, merkezi yapılara duyulan güveni zedelemiş ve kullanıcıları dijital varlıklarını kendi denetimleri altında saklayabilecekleri alternatif çözümlere yönlendirmiştir. Bu noktada, özel anahtarların yalnızca kullanıcı tarafından tutulduğu ve işlemlerin güvenli donanımlar üzerinde gerçekleştirildiği self-custody (kendi kendine saklama) yaklaşımları ön plana çıkmaktadır. Bu tür çözümler hem sahiplik bilincini güçlendirmekte hem de kullanıcıları üçüncü taraf risklerinden koruyarak dijital varlık güvenliğinin temel yapı taşlarından biri hâline gelmektedir.

Self-custody yaklaşımını destekleyen en yaygın çözümlerden biri, özel anahtarların çevrimdışı ve izole bir ortamda tutulmasını sağlayan donanım cüzdanlarıdır. Bu cihazlar, özel anahtarların güvenliğini sağlamak amacıyla tasarlanmış fiziksel aygıtlar olup, kriptografik işlemleri cihazın içinde gerçekleştirerek, anahtarların dış dünyayla temasını tamamen engellemektedir. Böylece, hem yazılımsal saldırılara karşı dirençli bir yapı sunulmakta hem de işlemlerin yetkisiz müdahaleye kapalı bir ortamda gerçekleştirilmesi sağlanmaktadır. Ancak pratikte yaygın olarak kullanılan geleneksel donanım cüzdanları (Ledger [1], Trezor [2] vb.), USB veya Bluetooth gibi belirli bağlantı yöntemlerine bağımlı çalışmakta; bu durum, özellikle mobil cihazlarla kullanımda çeşitli kısıtlamalara yol açmaktadır. Geleneksel donanım kripto cüzdanlarının mobil cihazlarla entegrasyonunda yaşanan zorluklar, özellikle iOS desteğinin olmaması, Bluetooth gibi ek yapılandırmalar gerektirmesi ve genellikle kapalı kaynak olmaları kullanıcıların bu cihazları yaygın ve esnek biçimde kullanmalarını engellemektedir. Ek olarak, bu cihazlar yüksek maliyetli ve enerji tüketen yapıları nedeniyle erişilebilirlik sorunu yaratmaktadır. Tüm bu nedenlerle, platformdan bağımsız çalışan, açık iletişim protokollerine dayanan, sade ve sürücü gerektirmeyen alternatif çözümlere olan ihtiyaç giderek belirginleşmektedir.

Günümüzde dijital imza işlemlerinin hem bireysel kullanıcılar hem de kurumsal sistemler tarafından güvenli ve pratik biçimde mobil cihazlar üzerinden gerçekleştirilebilmesi kritik bir ihtiyaç hâline gelmiştir. Mobil cihaz kullanımındaki artış ve dijital varlıkların yönetimine yönelik talepler doğrultusunda; platformdan bağımsız, uygulama gerektirmeyen ve açık iletişim protokolleriyle çalışan çözümler öne çıkmaktadır. Bu çerçevede, NFC teknolojisinin yaygınlaşması ve Java Card platformunun sunduğu donanım temelli güvenli anahtar saklama altyapısı, söz konusu ihtiyaca cevap verebilecek etkili bir çözüm potansiyeli taşımaktadır.

Donanım tabanlı güvenli anahtar saklama ihtiyacına yönelik çözümler arasında Java Card teknolojisi, düşük maliyeti, açık standartlara dayalı yapısı ve yüksek güvenlik özellikleriyle öne çıkmaktadır. Java Card, sınırlı donanım kaynaklarına sahip akıllı kartlar üzerinde çalışan, minimal Java Sanal Makinesi sunmakta olup, “bir kez yaz, her yerde çalıştır” ilkesini güvenlik odaklı sistemlere taşımaktadır [3]. Bu teknoloji, birden fazla uygulamanın aynı kart üzerinde birbirinden izole şekilde çalışmasına imkân tanırken, donanım düzeyinde sunduğu kriptografik modüller sayesinde özel anahtarların kart içinde oluşturulmasına, güvenli biçimde saklanmasına ve dışarı çıkarılmadan imzalama gibi kritik işlemlerde kullanılmasına olanak tanımaktadır. Böylece, geleneksel donanım cüzdanlarında olduğu gibi özel anahtar hiçbir zaman cihaz dışına çıkmadan güvenli işlem ortamı sağlanmaktadır. Ayrıca platformdan bağımsız yapısı, geliştirici dostu açık kaynak ekosistemi ve endüstri standartlarıyla uyumlu çalışma prensibi sayesinde, kapalı ve üreticiye özgü sistemlerin ötesinde esnek bir alternatif sunmaktadır. NFC destekli Java Card modelleri sayesinde bu teknoloji, modern mobil cihazlarla doğrudan iletişim kurabilmekte böylece taşınabilir ve platformdan bağımsız çözümler geliştirmek için güçlü bir temel oluşturmaktadır.

NFC (Yakın Alan İletişimi) teknolojisi, mobil cihazların temassız akıllı kartlarla doğrudan ve platformdan bağımsız biçimde iletişim kurabilmesine olanak tanımaktadır. Kısa menzilli kablosuz veri aktarımını mümkün kılan bu protokol hem Android hem de iOS cihazlarda donanımsal ve yazılımsal olarak desteklenmektedir. NFC üzerinden çalışan ve veri iletişimi için standartlaştırılmış bir yapı sunan NDEF (NFC Data Exchange Format), cihazlar arasında metin, bağlantı veya özel komut iletimi gibi işlemler için kullanılmaktadır. Mobil işletim sistemlerinin bu formatı yerel olarak desteklemesi sayesinde, akıllı kartlarla sürücüsüz veri iletişimi gerçekleştirilebilmektedir. Java Card’lar NDEF uyumlu şekilde yapılandırıldıklarında mobil cihazlardan gelen mesajlar yorumlanarak kart üzerindeki appletler tetiklenebilmektedir. Bu yaklaşım, mobil cihazın yalnızca bir kullanıcı arayüzü ve komut iletim aracı olarak görev yaptığı; buna karşın imzalama gibi güvenlik açısından kritik işlemlerin tamamen Java Card üzerinde, izole bir donanım ortamında yürütüldüğü bir mimariyi mümkün kılmaktadır.

Bu çalışmada, mobil cihazlarla platformdan bağımsız olarak, ek sürücü ve özel sistem entegrasyonu gerektirmeden etkileşim kurabilen, Java Card tabanlı güvenli bir dijital imzalama sistemi önerilmektedir. Önerilen sistem, Java

Card üzerinde çalışan iki ayrı applet'ten oluşan katmanlı bir mimariye sahiptir. İlk applet, NDEF protokolünü yöneten bileşen olup, mobil cihazdan gelen mesajları karşılamakta, içeriğini ayrıştırmakta ve ilgili komutları ikinci applet'e iletmektedir. İkinci applet ise, anahtar üretimi, imzalama ve özet alma gibi temel kriptografik işlemleri güvenli donanım ortamında gerçekleştirmektedir. Bu çok katmanlı yaklaşım sayesinde, dış dünya ile iletişimi yöneten ve kriptografik işlemleri gerçekleştiren birimler birbirinden ayrılarak işlem güvenliği artırılmakta ve sistemin modülerliği sağlanmaktadır. Önerilen mimarinin doğrulanması ve platformlar arası etkileşimin test edilmesi amacıyla, Android ve iOS cihazlarla uyumlu bir React Native mobil uygulama geliştirilmiştir. Mobil uygulama, kullanıcıdan aldığı girdiler doğrultusunda belirli bir iş akışını izlemekte ve buna göre ilgili komutları içeren NDEF mesajlarını oluşturarak Java Card ile NFC üzerinden haberleşmeyi başlatmaktadır. Karttan gelen yanıtları işleyen uygulama, işlem sonucunu kullanıcıya iletmekte ve sistem ile kullanıcı arasında güvenli, sade bir etkileşim katmanı görevi görmektedir. Böylece güvenlik açısından kritik işlemler donanımsal olarak izole bir ortamda gerçekleştirilirken, mobil uygulama yalnızca komut iletimi ve kullanıcı etkileşimini yönetmektedir.
Sunulan sistem, açık standartlara dayalı, harici uygulama gerektirmeden ve platformdan bağımsız bir mimariyle donanımsal güvenliği mobil ortama taşımaktadır. Java Card üzerinde önerilen çift katmanlı yapı ve NDEF tabanlı iletişim mekanizması sayesinde, güvenli imzalama işlemleri iOS ve Android cihazlarda sürücü kurulumu gerektirmeksizin gerçekleştirilebilmektedir. Bu yönüyle çalışma, Java Card altyapısının mobil ortamlarda uygulanabilirliğini ortaya koymakta ve benzer güvenlik ihtiyaçları için taşınabilir ve platformdan bağımsız çözümler geliştirilmesine olanak sağlamaktadır

2. İLGİLİ ÇALIŞMALAR

Java Card teknolojisi, 1990'lı yılların sonlarından itibaren bankacılık, kimlik doğrulama ve telekomünikasyon gibi güvenlik odaklı alanlarda yaygın şekilde kullanılmaya başlanmıştır. ISO/IEC 7816 ve ISO/IEC 14443 protokolleriyle uyumlu bu platform, düşük kaynak tüketimi ile donanımsal güvenlik özelliklerini bir araya getiren kompakt bir sanal makine ortamı sunmaktadır [4]. Uygulamaların izole biçimde çalışması, firewall mekanizması, CAP dosya yönetimi ve GlobalPlatform desteği gibi özellikler, bu teknolojiyi ödeme sistemleri ve kamu e-kimlik altyapılarında yaygınlaştırmıştır.
Zamanla dijital varlıkların güvenli yönetimi ihtiyacı arttıkça, bu güvenlik prensipleri kripto para ekosistemine de taşınmıştır. Başlangıçta bu alandaki ihtiyaçlar, masaüstü, mobil ve web tabanlı yazılımsal cüzdanlarla karşılanmaya çalışılmıştır [5]. Ancak internete sürekli bağlı olan bu uygulamalar, kötü amaçlı yazılımlar ve ağ tabanlı saldırılar karşısında savunmasız kalmıştır. Bu nedenle donanımsal güvenlik yaklaşımlarına dayanan çözümler giderek daha fazla önem kazanmıştır [4]. Ayrıca yazılımsal cüzdanların PIN girişleri gibi hassas bileşenleri hedef alan saldırılar (örneğin MinidriverSpy) da donanım cüzdanlarına geçişi hızlandıran önemli etkenlerden biri olmuştur [6].
Bamert vd. çalışmalarında Bitcoin işlemleri için geliştirilen açık kaynaklı yazılım cüzdanı BlueWallet'i önermektedir [7]. Uygulama, kullanıcıya ait özel anahtarları yalnızca cihaz üzerinde şifreli biçimde saklamakta ve Lightning Network desteğiyle zincir dışı işlemleri de desteklemektedir. Açık kaynaklı mimarisi sayesinde şeffaflık ve denetlenebilirlik sunan sistem, yalnızca yazılımsal güvenliğe dayandığı için donanım temelli tehditlere karşı sınırlı bir koruma düzeyi sağlamaktadır.
Yazılımsal güvenliğe dayalı bir başka çözüm, Popchev vd. [8] tarafından önerilen masaüstü tabanlı sıcak cüzdan uygulamasıdır. Çalışmada, blokzincir cüzdanlarının sistematik bir sınıflandırması sunulmuş ve ERC-20/721 tokenlarını destekleyen, biyometrik kimlik doğrulama özellikli bir yazılım cüzdanı geliştirilmiştir. Uygulama, anahtar yönetimini macOS işletim sisteminin güvenli alanı (Secure Enclave) içerisinde gerçekleştirerek, kullanıcıya ait özel anahtarların dışarı çıkarılmasına izin vermemektedir. Ancak, donanımsal güvenlik yerine yazılımsal önlemlere dayanan bu tür çözümler, gelişmiş tehdit modelleri karşısında sınırlı bir koruma sağlayabilmektedir.
Houy vd. kripto cüzdan güvenliğine çok katmanlı bir bakış sunan kapsamlı incelemelerinde; bellek, yazılım, donanım, ağ, kullanıcı arayüzü ve blokzincir protokolü gibi altı temel katmanı ayrı ayrı analiz etmiş ve her bir katman özelinde karşılaşılan saldırı vektörlerini sistematik olarak sınıflandırmıştır [9]. Mevcut savunma mekanizmalarının bu tehditlere karşı etkinliği değerlendirilmiş, özellikle yazılımsal güvenliğe dayanan çözümlerin fiziksel ve donanımsal saldırılar karşısında yetersiz kalabildiği vurgulanmıştır. Bu bağlamda çalışma, donanım tabanlı çözümlerin güvenlik açısından sağladığı avantajlara dikkat çekmektedir.
Ledger ve Trezor gibi ticari donanım cüzdanları, milyonlarca kullanıcıya, özel anahtarlarını donanımsal olarak koruma imkânı sunmaktadır [10]. Ancak bu cihazlar genellikle USB veya Bluetooth gibi bağlantı arayüzlerine bağımlı çalışmakta, bu da mobil cihazlarla doğrudan kullanımda sınırlamalara neden olmaktadır. Örneğin, Trezor cihazları iOS ile doğrudan çalışmazken; Ledger Nano X modeli Bluetooth desteği sunmakta, ancak bu da eşleştirme, batarya kullanımı ve ek yapılandırma gibi gereksinimler doğurmaktadır.
Java Card ortamında dijital imzalama işlemlerine yönelik ilk akademik girişimlerden biri, Elo ve Nikander tarafından sunulan ve ECDSA algoritmasının yazılımsal olarak Java Card üzerinde uygulanmasına dayanan merkeziyetsiz yetkilendirme sistemidir [11]. Bu çalışmada temel güvenlik işlevlerinin kart üzerinde dağıtık biçimde gerçekleştirilmesi hedeflenmiş olsa da mobil uyumluluk, donanımsal hızlandırma ve kullanıcı etkileşimi gibi güncel gereksinimler göz önüne alınmamıştır. Günümüzdeki kullanım senaryoları açısından bakıldığında, bu tür erken dönem prototiplerin donanımsal verimlilik ve pratiklik yönünden sınırlı kaldığı görülmektedir.

Sejfuli-Ramadani vd. çalışmalarında çeşitli donanım cüzdanlarının çevrimdışı kullanım ve NFC entegrasyonu açısından karşılaştırmalı bir analizini sunmuştur [12]. Söz konusu çözümler de benzer donanımsal sınırlamalar veya protokol bağımlılıkları taşımaktadır. Örneğin, Tangem kartları kullanıcı arayüzünü sadeleştiren fiziksel kart formunda sunulmakta, NFC üzerinden çalışmakta ve işlem onaylarını doğrudan kart üstündeki tuş ile sağlamaktadır. Ancak Tangem, tüm işlem geçmişi ve uygulama kontrolünü kendi bulut altyapısı üzerinden yürütmesi nedeniyle merkezî güvenlik riskleri barındırmaktadır. SafePal ise Bluetooth üzerinden bağlanan, QR kod ile işlem doğrulayan çok varlıklı bir donanım cüzdan sunmakta, ancak bağlantı kurulumu ve uygulama bağımlılığı gibi kullanım zorlukları gözlenmiştir.

OneKey cüzdanları açık kaynak kodlu donanım/yazılım sunması açısından geliştiriciler için avantaj sağlasa da, mobil platform desteği bakımından halen iOS tarafında sınırlı kalmaktadır. Cypherock X1 ise anahtarların Shamir Secret Sharing ile bölünerek USB-C destekli dört donanım parçasına dağıtılması fikrine dayanmaktadır; bu güvenliği artırmakla birlikte, taşınabilirlik ve kullanıcı dostu arayüz açısından karmaşıklık doğurmaktadır.

Ticari çözümlerin sahip olduğu bu tür donanımsal ve yazılımsal kısıtlamalar, geliştirici topluluklarını daha açık, sade ve platformlar arası çalışabilir sistemler geliştirmeye yönlendirmiştir. Bu doğrultuda, Java Card altyapısını kullanan açık kaynaklı çözümler ön plana çıkmaya başlamıştır. SatoChip, YubiKey Neo ve TapSigner gibi projeler, kullanıcıya özel anahtarlarını Java Card benzeri donanımlar üzerinde tutma imkânı sunarken, farklı kullanım senaryoları için tasarlanmıştır. SatoChip, açık kaynaklı firmware ve mobil uygulama aracılığıyla Bitcoin işlemlerine olanak sağlarken, YubiKey Neo çoklu kimlik doğrulama sistemleri için tasarlanmıştır. TapSigner ise NFC üzerinden çalışmasına rağmen yalnızca Nunchuk gibi belirli mobil uygulamalarla uyumludur ve NDEF protokolünü doğrudan desteklememektedir.

NFC destekli Java Card çözümlerinin bir kısmı, temel kullanıcı etkileşimi için NDEF protokolünden faydalanmaktadır. Örneğin, bazı projelerde Java Card üzerinden HMAC tabanlı OTP üretimi gerçekleştirilmekte ve bu değerler NDEF üzerinden mobil cihaza URL olarak aktarılabilmektedir. Bununla birlikte, bu uygulamalar çoğunlukla tekil işlevlerle sınırlıdır ve platformdan bağımsız, genel amaçlı imzalama altyapısı sunmamaktadır. NFC ile çalışan sistemlerin güvenlik analizi, yeniden oynatma saldırıları ve mesaj sıralama açıklarına karşı ek protokol katmanlarına ihtiyaç duyulduğunu göstermektedir [6].

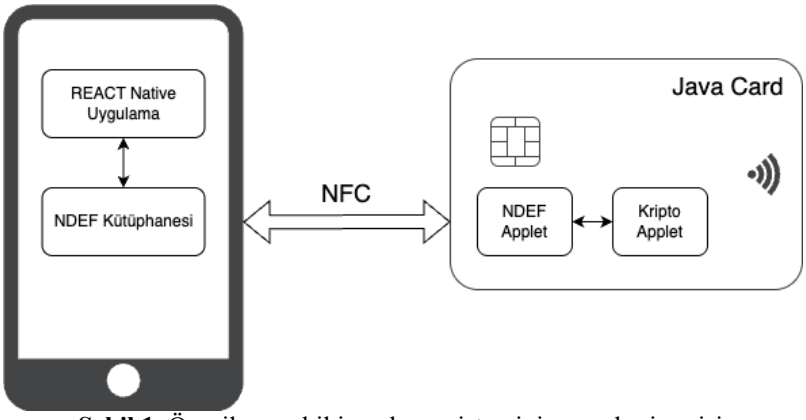
Donanımsal güvenliğe odaklanan farklı mimari yaklaşımlar arasında, özel anahtarların güvenli biçimde saklanması ve yedeklenmesi amacıyla Intel SGX tabanlı, Shamir Secret Sharing destekli bir mimari sunan CryptoVault [13] öne çıkmaktadır. Crypto Terminal [14] ise Java Card'ı merkezde tutan, açık kaynaklı ve donanımsal olarak özelleştirilebilen bir terminal çözümü önermektedir. Her iki sistem de kullanıcıdan bağımsız olarak güvenli işlem ortamı sunmayı hedeflemektedir. Benzer şekilde, deterministik alt-cüzdan yapıları üzerine yapılan çalışmalar kullanıcı varlıklarının kontrollü biçimde bölünmesini sağlayarak hem güvenliği hem de gizliliği artırmayı amaçlamaktadır [15]. Bu tür yaklaşımlar, önerilen sistemin mobil cihazdan ayrık işlem güvenliği sağlayan ve modüler mimariye sahip yapısıyla örtüşmektedir.

Donanım tabanlı dijital imzalama sistemlerinin başarısı, yalnızca mimari yapı ve kullanıcı etkileşimi ile değil, aynı zamanda seçilen kriptografik algoritmaların sınırlı kaynaklara sahip donanımlar üzerinde verimli biçimde uygulanabilmesine de bağlıdır. Bu bağlamda, Avanzi ve Lange tarafından yürütülen çalışmada, Twisted Edwards eğrileri üzerinde tanımlı bir dijital imza algoritması, Java Card üzerinde optimize edilerek başarıyla uygulanmıştır [16]. Çalışma, bellek kısıtlı ortamlarda elliptic curve tabanlı imza algoritmalarının hesaplama süresi, bellek kullanımı ve genel uygulanabilirliği açısından ayrıntılı değerlendirmeler sunmaktadır.

Tanrıkulu vd. [17] tarafından geliştirilen donanımsal kripto cüzdan uygulaması, AKiS işletim sistemi üzerine tasarlanmış ve BIP-32, BIP-39, BIP-44 protokollerine uygun şekilde, tek bir tohum değeri üzerinden çok sayıda anahtar türetebilen hiyerarşik deterministik (HD) cüzdan mimarisi sunmaktadır. Sistem, secp256k1 eğrisi üzerinde ECDSA imzalama desteği başarıyla çalıştırılmış, AKiS içerisinde deterministik anahtar üretimi ve APDU tabanlı iletişim modülü ile bütünleşik bir yapı olarak geliştirilmiştir.

Fritsche vd. özel anahtarların fiziksel olarak ayrık ve müdahaleye dayanıklı ortamlarda saklanmasını esas alan, Java Card tabanlı açık kaynak bir donanım cüzdan prototipi geliştirmiştir [18]. Geliştirilen sistemde, hem dokunmatik ekranlı hem de NFC destekli versiyonlar değerlendirilmiş; iletişim kanallarının güvenliği, SRP gibi parola ile kimlik doğrulamalı protokollerle sağlanmaya çalışılmıştır. Uygulama mimarisi, Java Card üzerinde çalışan applet yapısı, APDU protokolü ile iletişim, donanımsal doğrulama mekanizmaları ve kullanıcı arayüzü iş akışları detaylı biçimde açıklanmıştır.

Mevcut çözümlerin büyük bir kısmı, belirli platformlara, uygulamalara veya üreticiye özgü donanım ve yazılımlara bağımlı çalışmaktadır. Önerilen sistem, NDEF standardını kullanarak mobil cihazlarla doğrudan iletişim kurmakta ve herhangi bir uygulama, sürücü veya özel entegrasyon gerektirmeden hem Android hem de iOS platformlarında sade ve taşınabilir bir imzalama altyapısı sunmaktadır. Bu yönüyle çalışma, yaygın bağımlılıkları ortadan kaldırarak güvenli dijital imzalama için açık ve erişilebilir bir alternatif ortaya koymaktadır. Önerilen sistemin literatürdeki öncü çalışmalarla donanım güvenliği, mobil uyumluluk, iletişim protokolü, uygulama gereksinimi ve platform bağımsızlığı gibi açılardan karşılaştırmalı değerlendirmesi, Tablo 1 ve Tablo 2'de sistematik bir biçimde sunulmuştur.



Şekil 1. Önerilen mobil imzalama sisteminin genel mimarisi.

Tablo 1. Literatürdeki yöntemlerle önerilen sistemin donanım ve uyumluluk açısından karşılaştırması.

Sistem / Çalışma	Donanım Güvenliği	Mobil Uyum (iOS/Android)	NDEF Desteği	Açık Kaynak	Uygulamasız Kullanım
Ledger Nano X	EAL5+	Android & iOS (Bluetooth)	Yok	Kısmen	Hayır
Trezor Model T	Sertifikasyon Yok	Android (USB)	Yok	Evet	Hayır
TapSigner (Coinkite)	Güvenli Çip	Android (Nunchuk App)	Kısıtlı	Hayır	Kısmen
YubiKey Neo	Donanım Temelli	Android (Yubico App)	Kısıtlı	Kısmen	Hayır
SatoChip	Java Card tabanlı	Android (USB)	Yok	Evet	Hayır
Fritsche vd.[18]	Java Card (EAL5+)	Android (NFC)	Evet	Evet	Kısmen
Popchev vd. (macOS Wallet)[8]	Yazılımsal Güvenlik	macOS (Secure Enclave)	Yok	Evet	Evet
CryptoVault	Intel SGX tabanlı	Sınırlı (PC temelli)	Yok	Kısmen	Hayır
Crypto Terminal [14]	Java Card + Güvenli Donanım	Android & PC	Kısıtlı	Evet	Hayır
AKiS (Tanrıkulu vd.)[17]	AKiS OS EAL4+	Android (USB)	Yok	Kısmen	Hayır
Tangem	EAL6+	Android & iOS (NFC)	Kısıtlı	Hayır	Evet (kısıtlı)
SafePal S1	Donanım (QR Kamera) EAL6+	Android & iOS	Yok	Hayır	Kısmen (QR ile)
OneKey 1S	Güvenli Donanım EAL6+	Android	Yok	Evet	Hayır
Cypherock X1	Güvenli Donanım + EAL6+	Yok	Yok	Kısmen	Hayır
Önerilen Sistem	**Java Card (EAL6+)**	**Android & iOS (NFC)**	**Evet**	**Evet**	**Evet**

3. YÖNTEM

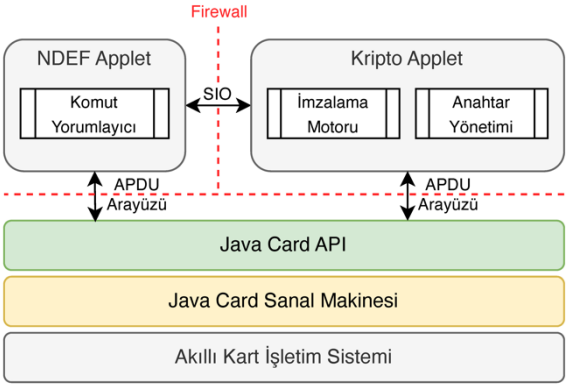
Bu bölümde, önerilen güvenli imzalama sisteminin genel mimarisi sunulmakta; Java Card üzerinde geliştirilen applet yapısı, NDEF standardı üzerinden gerçekleştirilen veri iletim süreci ve mobil uygulama ile sağlanan platform bağımsız etkileşim detaylı şekilde açıklanmaktadır.

Önerilen yöntem, mobil cihazlarla platformdan bağımsız ve sürücüsüz bir biçimde güvenli dijital imzalama ihtiyacını karşılamak amacıyla geliştirilmiştir. Mevcut donanım cüzdanlarının platform kısıtları, uygulama bağımlılığı ve kapalı ekosistem yapısı; açık standartlara dayalı, donanım tabanlı ve harici uygulama gerektirmeden çalışan sistem tasarımlarına olan ihtiyacı ortaya koymaktadır. Bu ihtiyaç doğrultusunda, Java Card'ın izolasyon temelli mimarisi ile NFC'nin doğal platformlar arası desteği birleştirilerek, kullanıcı dostu ve güvenli bir çözüm hedeflenmiştir.

3.1. Genel Sistem Mimarisi

Önerilen sistem, mobil cihazlar ile Java Card tabanlı akıllı kart arasında, NDEF standardı üzerinden sürücüsüz ve platformdan bağımsız bir etkileşim sağlayacak şekilde tasarlanmıştır. Şekil 1'de genel mimarisi sunulan sistem, Java Card üzerinde çalışan çift applet yapısı, bu yapıyla mobil cihaz arasında NDEF protokolü üzerinden veri haberleşmesini sağlayan iletişim katmanı ve Android ile iOS platformlarında çalışabilen React Native tabanlı mobil uygulamadan oluşmaktadır. Java Card tarafında görev ayrımını sağlamak amacıyla, NDEF mesajlarını karşılayarak komut ayrıştırma işlevini üstlenen bir NDEF applet ile, anahtar üretimi, imzalama ve özet alma gibi kriptografik işlemleri gerçekleştiren bir kripto applet geliştirilmiştir. Bu iki applet, Java Card ortamında APDU

komutları aracılığıyla dolaylı olarak iletişim kurmakta; bir applet diğerine komut yönlendirerek iş akışını sürdürmektedir. Bu mimari, dış dünya ile etkileşimi yöneten katman ile güvenlik açısından kritik işlemleri gerçekleştiren bileşeni birbirinden ayırarak hem işlem güvenliğini artırmakta hem de sistemin modülerliğini desteklemektedir. Mobil uygulama, kullanıcı girdilerine göre belirli bir işlem akışını izlemekte ve NDEF formatında komutlar oluşturarak kart ile NFC üzerinden haberleşmektedir. Bu haberleşme, sistemin komut bazlı işleyişini yöneten özel bir protokol tarafından düzenlenmektedir.



Şekil 2. Java Card üzerinde önerilen katmanlı applet mimarisi.

Tablo 2. Literatürdeki yöntemlerle önerilen sistemin yetenek, bağımsızlık ve uygulama gereksinimleri açısından karşılaştırması.

Sistem / Çalışma	Platform Bağımsızlık	Komut Genişletilebilirliği	Pil Bağımlılığı	Önerilen Sistemle Karşılaştırma
Ledger Nano X	Kısıtlı	Sınırlı	Var	Ek uygulama gerekir; iOS'te Bluetooth eşleşmesi ve pil bağımlılığı vardır.
Trezor Model T	Kısıtlı	Evet (Trezor Suite)	Yok (USB'den)	iOS desteği yok, masaüstü bağımlılığı yüksek.
TapSigner (Coinkite)	Kısıtlı	Hayır	Yok	Uygulamaya bağımlı; NDEF sınırlı destekleniyor.
YubiKey Neo	Kısıtlı	Hayır	Yok	OTP/U2F odaklıdır, genel imza altyapısı sunmaz.
SatoChip	Kısıtlı	Kısmen	Yok	USB gerektirir, NFC uyumu bulunmaz.
Fritsche vd. [18]	Kısıtlı	Hayır	Yok	Akademik prototip; genişletilebilirlik sınırlı.
Popchev vd. [8]	Kısıtlı (macOS özel)	Kısmen	Yok	Donanım güvenliği zayıf, platforma özel bağımlılık var.
CryptoVault [13]	Sınırlı	Kısıtlı	Var	SGX bağımlılığı nedeniyle taşınabilirlik düşük.
Crypto Terminal [14]	Kısmen	Kısmen	Yok	Geliştirici odaklı, genişletilebilir ama kullanıcı dostu değil.
AKiS (Tanrıkulu vd.) [17]	Kısıtlı	Kısmen	Yok	Mobil platformlarda sınırlı uyum; genişleme potansiyeli yüksek.
Tangem	Kısıtlı	Hayır (ön tanımlı)	Yok	İşlem geçmişi bulutta, fiziksel onaylı; merkezi risk barındırır.
SafePal S1	Kısmen	Hayır	Var (şarjlı)	QR ile uygulama bağımlı çalışır; bağlantı hızı düşüktür.
OneKey 1S	Kısıtlı	Kısmen	Var	Açık kaynaklı, iOS'te sınırlı uyum; yazılım/USB bağlılığı var.
Cypherock X1	Sınırlı	Kısmen	Yok	Bütünleşik olmayan bir yapı, taşınabilirlik zayıf.
Önerilen Sistem	**Tam**	**Evet**	**Yok**	**Harici uygulamasız, sürücüsüz, açık formatlı, çift applet'li yapı sunar.**

3.2. Java Card Applet Mimarisi

Java Card üzerinde uygulanan mimari, işlevsel ayrım ve güvenlik gereksinimlerini karşılamak üzere iki bağımsız applet bileşeninden oluşmaktadır. NFC üzerinden mobil cihazlarla haberleşmeyi sağlayan NDEF Applet, NDEF mesajlarını karşılayan ve komutları ayrıştırarak uygun işlem birimine yönlendiren bir kontrol bileşeni olarak

yapılandırılmıştır. Komutların işlenmesi ve güvenlik açısından kritik tüm operasyonların yürütülmesi ise kriptografik işlemci applet tarafından gerçekleştirilmekte olup, bu iki applet yapısı fiziksel olarak izole biçimde çalışmaktadır.

NDEF Applet, kartın NFC arayüzünü NFC Forum Type 4 Tag standardına uygun şekilde yapılandırmakta ve mobil cihazlarla NDEF üzerinden metin tabanlı veri iletişimine olanak tanımaktadır [19]. Mobil uygulama tarafından oluşturulan NDEF mesajları karta iletilmekte; burada NDEF Applet tarafından algılanmakta ve içerdiği komut metni yorumlanarak kripto applet'e APDU komutu olarak yönlendirilmektedir. Kripto işlemci applet, güvenlik açısından hassas tüm kriptografik işlemleri gerçekleştirmektedir. Bu işlemler arasında anahtar üretimi, anahtar yönetimi, dijital imzalama, imza doğrulama ve açık anahtarın dış ortama aktarımı gibi işlevler yer almaktadır. Kripto applet doğrudan mobil cihazla iletişime geçmeyip; yalnızca NDEF Applet tarafından yönlendirilen komutlara tepki vermektedir. Bu görev ayrımı, özellikle dış dünya ile etkileşimde bulunan bileşen ile gizli verileri yöneten bileşeni ayırarak saldırı yüzeyini daraltmakta ve sistem güvenliğini artırmaktadır. Java Card üzerindeki katmanlı mimari ve appletler arası iletişim, Şekil 2'de gösterilmektedir.

Appletler arasındaki kontrollü iletişim, Java Card platformunun desteklediği Sharable Interface Object (SIO) mekanizması aracılığıyla sağlanmaktadır. Güvenlik duvarı prensibi gereği her applet yalnızca kendi belleğine erişebilirken, SIO arayüzünden türetilmiş nesneler üzerinden belirli işlevler diğer applet'ler tarafından erişilebilir hale getirilmektedir. Bu çalışmada, NDEF Applet yalnızca kripto applet'in sunduğu yetkilendirilmiş paylaşılabilen arayüz fonksiyonlarına erişim sağlayacak şekilde yapılandırılmıştır. Böylece iki applet arasında doğrudan değil, yalnızca tanımlı işlemlere izin veren bir geçit üzerinden güvenli iletişim kurulmuştur. Bu yaklaşım hem bileşenler arası bağımlılığı azaltmakta hem de güvenliğin sürdürülebilir şekilde korunmasına olanak tanımaktadır.

Mobil uygulama, kart ile etkileşimi NDEF formatındaki *well-known text record* yapısını kullanarak gerçekleştirmektedir [20]. Her işlem, bir metin kaydı üzerinden insan tarafından okunabilir şekilde tanımlanmaktadır; örneğin "prepkey" komutu kartın belirli bir anahtarı hazırlamasını sağlarken, "generatekey" komutu yeni bir anahtar çifti üretmesini tetikler. Çok aşamalı imzalama işlemleri için "signinit", "signupdate" ve "signfinal" komutları sırasıyla imzalama sürecini başlatma, imzalanacak veriyi parça parça gönderme ve imzanın tamamlanmasını ifade eder. Bu yapı, özellikle büyük veri bloklarının imzalanması gerektiğinde işlem akışının parçalara bölünerek güvenli şekilde yürütülmesine olanak tanımaktadır.

Komutların NDEF metin kayıtları içinde açık biçimde ifade edilmesi, sistemin hata ayıklama, test ve uygulama geliştirme süreçlerinde önemli kolaylıklar sağlamaktadır. Ayrıca bu yaklaşım, geliştirici ve kullanıcı açısından protokolün daha kolay anlaşılmasını ve uyarlanmasını mümkün kılmaktadır.

3.3. NDEF ile Veri Haberleşmesi

NDEF protokolü, mobil cihaz ile Java Card tabanlı akıllı kart arasında komut bazlı ve sürücüsüz bir etkileşim sağlamak amacıyla kullanılmıştır. Bu yapı sayesinde Java Card, NFC Forum Type 4 Tag gibi davranmakta ve standartlaştırılmış bir protokol üzerinden sürücüsüz iletişime olanak tanımaktadır. Her işlem adımı, mobil uygulama tarafından oluşturulan bir NDEF mesajı aracılığıyla karta iletilmekte; kart ise gelen mesajı ayrıştırarak uygun kriptografik işlemi tetiklemektedir.

NDEF mesajları, tür (type), uzunluk (length) ve içerik (payload) alanlarından oluşan kayıtlar (records) dizisidir. Önerilen sistemde, kayıt türü olarak NFC Forum tarafından tanımlanan Text (T) tipi kullanılmış ve içerik alanında metin tabanlı özel komutlara yer verilmiştir. Örneğin, "prepkey", "generatekey", "signinit", "signupdate" ve "signfinal" gibi komutlar, sırasıyla anahtar hazırlama, yeni anahtar üretme ve çok aşamalı imzalama işlemlerini temsil etmektedir. Bu komutlar, NDEF applet tarafından algılanarak, karşılık gelen APDU komutları aracılığıyla kripto applet'e yönlendirilmektedir.

Mobil uygulama, kullanıcıdan aldığı girdiye bağlı olarak işlem akışını belirlemekte ve NDEF formatında uygun komutu oluşturarak kart ile haberleşmeyi başlatmaktadır. NFC etkileşimi süresince, uygulama tarafından tetiklenen işlemler doğrultusunda gerekli NDEF mesajları ardışık biçimde karta yazılmakta ve karttan yanıt okunmaktadır. Metin tabanlı, açık ve standartlara dayalı bu iletişim yapısı yalnızca platform bağımsızlık avantajı sunmakla kalmamakta, aynı zamanda hata ayıklama, test ve uygulama geliştirme süreçlerinde yüksek düzeyde şeffaflık ve esneklik sağlamaktadır.

Bu iletişim modeli, işlem akışının uygulama tarafından adım adım yönlendirilmesini mümkün kılmaktadır. Mobil cihazın kartın menziline girmesiyle birlikte bir NFC oturumu başlatılır; kullanıcı uygulama arayüzü üzerinden "Veriyi İmzala" benzeri bir komutu tetiklediğinde, ilgili NDEF komutları sırasıyla karta iletilir. Kart, her bir komutu NDEF applet aracılığıyla algılayarak uygun şekilde ayrıştırır ve kriptografik işlem için kripto applet'e yönlendirir. Oluşan yanıt ise, yine NDEF formatında uygulamaya geri aktarılır. Bu yapı, mobil cihaz ile akıllı kart arasında dönüşümlü yazma/okuma işlemlerine dayalı, standartlara uygun ve sürücü gerektirmeyen bir etkileşim mekanizması sağlamaktadır. Bu süreç, aşağıdaki adımlarla ilerlemektedir:

- Mobil uygulama, kartın NDEF belleğine "signinit" komutunu içeren bir Text tipi NDEF mesajı yazar. Bu mesaj, NDEF applet tarafından algılanarak imzalama oturumunu başlatacak APDU komutu ile kripto applet'e yönlendirilir.
- Uygulama, imzalanacak veriyi parçalara ayırarak her birini "signupdate:<data>" biçiminde ayrı NDEF mesajları ile karta gönderir. Kart bu verileri dahili tamponda birleştirerek imzalama algoritmasına aktarır. Veri boyutu büyükse, bu adım birden çok kez tekrarlanır.

- Verinin tamamı iletildikten sonra, uygulama “signfinal” komutunu içeren son NDEF mesajını yazar. Kart bu komutu yorumlayarak imzalama işlemini tamamlar ve sonucu hazırlanan bir NDEF yanıtı olarak belleğe yazar.
- Uygulama, kartın belleğinden bu NDEF mesajını okur ve içeriğinde yer alan imzayı (örneğin Base64 kodlu) kullanıcıya sunar veya doğrulama için dış servislere iletir.

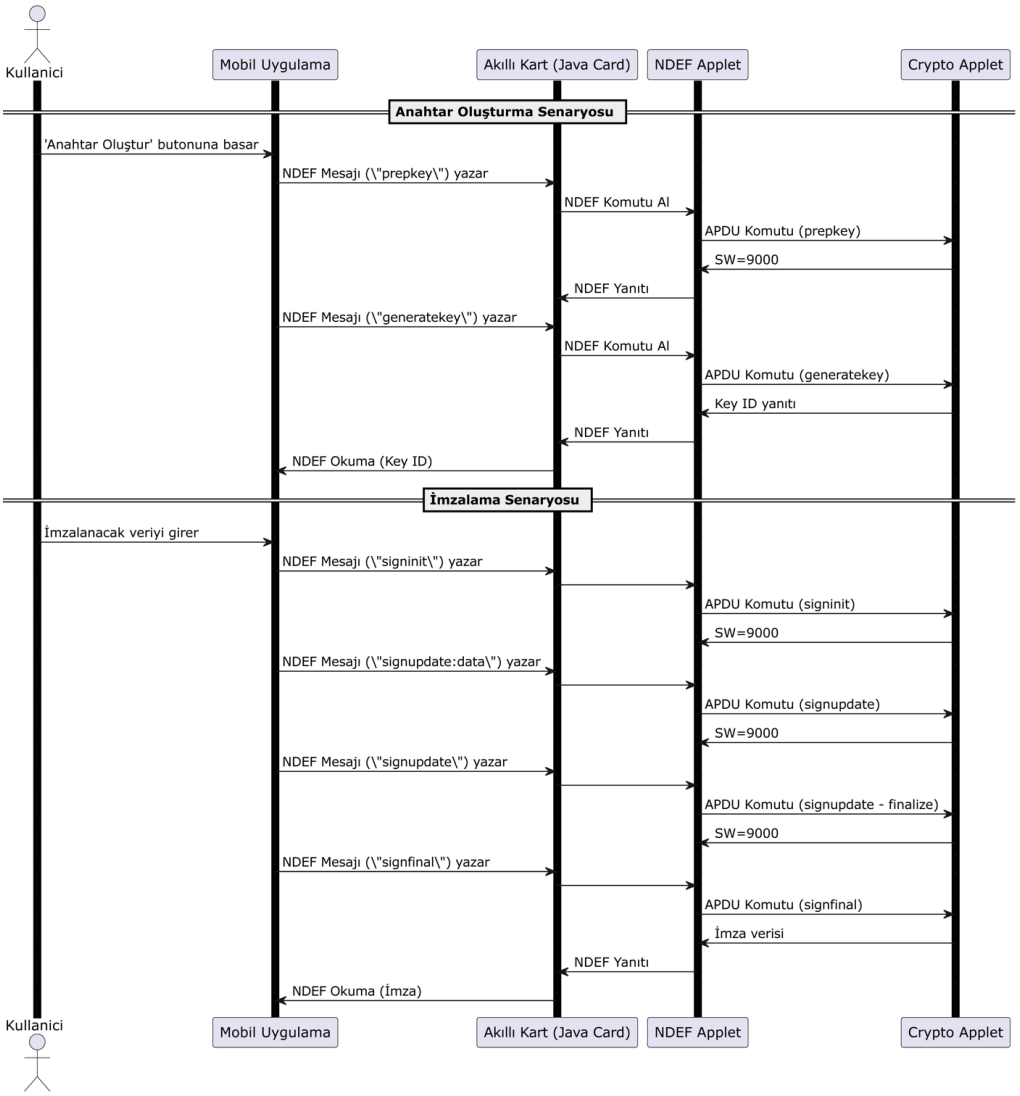
NDEF üzerinden gerçekleşen bu iletişim modeli, yarı çift yönlü (half-duplex) bir protokol yapısı sergilemektedir. Mobil cihaz ve Java Card, dönüşümlü olarak NDEF mesajları yazarak ve okuyarak işlem adımlarını sıralı biçimde yürütmektedir. Bu yaklaşım, NFC Forum Type 4 Tag standardının sunduğu mevcut okuma/yazma mekanizmasına dayandığı için ek sürücü gereksinimi olmaksızın hem Android hem de iOS platformları tarafından doğal olarak desteklenmektedir. Ancak güvenliğin sağlanabilmesi için iletilen mesajların sırası, bütünlüğü ve içerik doğruluğu son derece önemlidir. Bu nedenle hem kart tarafında hem de mobil uygulama tarafında durum makineleri tasarlanmış ve beklenmeyen durumlara karşı hata denetimleri entegre edilmiştir.

4. UYGULAMA DETAYLARI

Bu bölümde, önerilen sistemin uygulama düzeyindeki teknik detayları sunulmakta; özellikle kriptografik işlem akışı, kullanıcı arayüzü bileşenleri ve güvenliği artırmaya yönelik uygulama içi önlemler ayrıntılı olarak ele alınmaktadır.

4.1. ECC Anahtar Üretimi

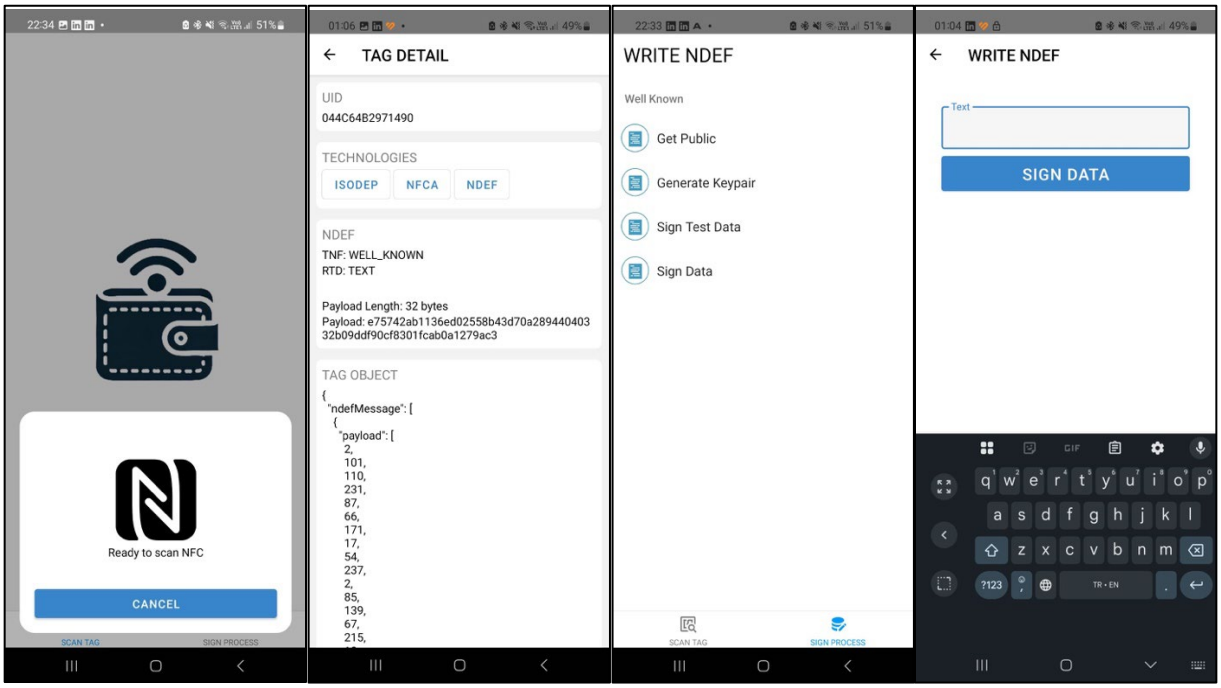
Sistemde gerçekleştirilen dijital imzalama işlemleri için Eliptik Eğri Kriptografisi (ECC) tabanlı iki farklı algoritma desteği sağlanmaktadır: Ed25519 (EdDSA ailesi) ve ECDSA (örneğin secp256r1 eğrisi). Ed25519, kısa anahtar ve imza boyutları ile yüksek işlem verimi sunması nedeniyle tercih edilmekte; ECDSA’ya kıyasla modern uygulamalarda daha sık kullanılmaktadır [21].



Şekil 3. Uygulama, kart ve applet katmanları arasında gerçekleşen anahtar oluşturma ve veri imzalama işlemlerine ait etkileşim sekans diyagramı.

Java Card ortamında Ed25519 algoritması, Java Card 3.1 sürümü ile standart olarak desteklenmeye başlanmış olsa da bu çalışmada kullanılan kartın Java Card 3.0.5 sürümüne sahip olması nedeniyle donanımsal destek bulunmamaktadır [22]. Bu nedenle, sistemin mimarisi gerektiğinde yazılımsal bir Ed25519 gerçekleştirimine uyum sağlayacak şekilde kurgulanmıştır. Ancak, bu tür yazılımsal yaklaşımların donanım hızlandırmalı çözümlere göre daha sınırlı performans sunabileceği göz önünde bulundurulmalıdır.
Kart kişiselleştirme aşamasında, Kripto Applet içerisinde varsayılan olarak Ed25519 algoritmasıyla bir ECC anahtar çifti oluşturulmaktadır. Bu işlem, mobil istemciden gönderilen "prepkey" ve "generatekey" komutları doğrultusunda tetiklenmektedir. Mevcut anahtar güvenli biçimde silinmekte ve yerine yeni bir anahtar çifti üretilmektedir. Bu yapı sayesinde, anahtar yenileme ve gerektiğinde çoklu anahtar desteği gibi işlevler sistem kapsamında desteklenebilir hale getirilmektedir.
Üretilen açık anahtar, mobil uygulama tarafından NDEF protokolü üzerinden okunarak kullanıcıya sunulmakta ve gerekli durumlarda dış sistemlere (örneğin blok zincir cüzdan adresi oluşturmak amacıyla) aktarılabilmektedir. Özel anahtar ise yalnızca kart üzerinde saklanmakta ve imzalama işlemleri bu güvenli donanım ortamı içerisinde yürütülmektedir. Bu sayede, özel anahtarların dış ortama çıkarılması engellenmekte ve kriptografik güvenlik bütünlüğü korunmaktadır.
Anahtar yönetimi, birden fazla anahtar çiftine destek verecek şekilde genişletilebilir olarak tasarlanmıştır. Her anahtar çifti, kendine özgü bir kimlik (key ID) ile etiketlenebilmekte ve bu kimlik, komutlara parametre olarak iletilerek aktif anahtarın dinamik olarak belirlenmesine olanak tanımaktadır. Bu çalışmada yalnızca tek bir aktif anahtar çifti kullanılmakla birlikte, söz konusu genişletme potansiyeli sistemin modüler yapısına katkı sunmaktadır.

4.2. Veri İmzalama ve Doğrulama



(a) (b) (c) (d)

Şekil 4. Mobil uygulama arayüzünde (a) NFC kart tarama ekranı, (b) kart bilgi ekranı, (c) işlem menüsü ve (b) imzalama ekranı.

Sistemdeki imzalama işlemleri, önceki bölümlerde tanımlanan çok adımlı protokol yapısı aracılığıyla yürütülmektedir. Kullanıcının mobil uygulama arayüzü üzerinden dijital imzalama komutunu seçmesiyle birlikte, kullanıcıdan alınan veri (örneğin serbest metin, dosya özeti veya belirli bir protokol mesajı), uygulama tarafından ön işleme tabi tutulmakta ve gerekiyorsa parçalanarak ardışık NDEF mesajları hâlinde karta iletilmektedir. Bu süreçte uygulama, sırasıyla "signinit", bir veya daha fazla "signupdate:<data>" ve ardından "signfinal" komutlarını içeren NDEF mesajlarını karta yazarak protokolün adımlarını ilerletmektedir.
Kripto Applet, kendisine aktarılan verileri dahili bir tamponda birleştirerek bütünsel veri yapısını oluşturur. Ardından "signfinal" komutunun ulaşmasıyla birlikte, seçilen algoritmaya bağlı olarak (örneğin Ed25519 ya da ECDSA/secp256r1) dijital imzayı üretmektedir. Oluşturulan imza, algoritmanın gereklerine uygun şekilde (örneğin Ed25519 için 64 baytlık sabit uzunlukta, ECDSA için DER formatında) hazırlanır ve NDEF Applet aracılığıyla dışarıya aktarılır. Mobil uygulama, bu imzayı NDEF üzerinden okuyarak kullanıcıya genellikle HEX veya Base64 formatında sunmaktadır.
Bu yapı, sadece küçük veri bloklarını değil; aynı zamanda daha büyük içeriklerin imzalanmasını da

desteklemektedir. Örneğin, bir akıllı sözleşme kodu, dosya özeti ya da işlem yığını gibi geniş veri yapıları, uygulama tarafından otomatik olarak parçalara ayrılmakta ve birden fazla "signupdate" komutu ile karta iletilmektedir. Bu sayede, Java Card'ın sınırlı bellek yapısına rağmen bütünlük korunarak imzalama işlemi başarıyla tamamlanabilmektedir.
Kullanıcı etkileşimi ile başlayan ve kart üzerinde tamamlanan bu işlem akışı, ardışık NDEF komutları ve APDU yönlendirmeleri ile modellenmiştir. Şekil 3, önerilen sistemde anahtar oluşturma ve veri imzalama senaryolarına ilişkin olarak, mobil uygulama, akıllı kart ve applet katmanları arasındaki etkileşimi ayrıntılı biçimde göstermektedir. Diyagram, her bir katman arasında gerçekleşen mesaj akışını, işlem sırasını ve protokolün temel yapı taşlarını görselleştirerek sistem işleyişini açıklamayı amaçlamaktadır.

4.3. Mobil Uygulama Arayüzü

Geliştirilen mobil istemci uygulaması, önerilen sistemin kullanıcı tarafından etkileşimli biçimde kullanılmasını mümkün kılan bir arayüz sunmaktadır. Arayüz, kullanıcı deneyimini artırmak amacıyla sade, yönlendirici ve çok adımlı bir yapı ile tasarlanmıştır.
Ana ekran, kullanıcının gerçekleştirebileceği işlemleri açık ve erişilebilir biçimde sunan bir işlem menüsü olarak yapılandırılmıştır. Şekil 4'te gösterilen bu menü aracılığıyla kullanıcı, sistemin sunduğu temel işlevler olan *Anahtar Oluştur*, *Veriyi İmzala* ve *Açık Anahtar Al* seçeneklerine erişebilmektedir. Her bir işlem seçeneği, kullanıcıyı ilgili veri giriş ekranına yönlendirmekte ve işlemi başlatmak için gerekli bilgilerin girilmesini talep etmektedir.
İmzalama ekranında, kullanıcıdan serbest metin girmesi istenmektedir. Giriş tamamlandığında, uygulama otomatik olarak NFC etkileşim oturumunu başlatmakta ve kullanıcıyı kartı cihaza yaklaştırması yönünde bilgilendirmektedir. Kart algılandığında, sistem işlem akışını arka planda yürütmekte ve dijital imza üretildikten sonra sonucu kullanıcıya sunmaktadır. Oluşturulan dijital imza, genellikle HEX veya Base64 biçiminde gösterilmekte ve gerektiğinde dışa aktarılabilmektedir.
Uygulama, işlem sürecinin her aşamasında kullanıcıya durum mesajları aracılığıyla geri bildirim sağlamaktadır. Örneğin, NFC oturumu başlatıldığında "Kartı telefona yaklaştırın", imzalama süreci başladığında "İmzalama başlatıldı", işlem başarıyla tamamlandığında ise "İmzalama başarıyla tamamlandı" gibi mesajlar gösterilmektedir. Kartın algılanamaması, zaman aşımı veya yanıt hatası gibi durumlarda kullanıcı açık biçimde bilgilendirilmekte ve işlem gerektiğinde yeniden başlatılabilmektedir. Bu yapı hem kullanıcı deneyiminin sürekliliğini hem de işlemlerin güvenli yürütülmesini desteklemektedir.

4.4. Güvenlik Önlemleri

Çalışmada güvenlik, Java Card tarafındaki applet mimarisi ile mobil istemci uygulaması arasında çok katmanlı biçimde ele alınmaktadır. Amaç, yetkisiz erişimi engellemek, işlem sırasını doğrulamak ve kullanıcı deneyimini sekteye uğratmadan anahtar bütünlük ve gizliliği korumaktır.

Kart erişim kontrolü: Java Card ortamında, uygulama yükleme ve yönetimi için kullanılan *GlobalPlatform* güvenlik anahtarları (Secure Domain key'leri), ilk kurulum aşamasında değiştirilmiş; bu sayede izinsiz applet yükleme veya silme işlemleri engellenmiştir. Komut kabulü yalnızca NDEF arayüzü üzerinden sınırlandırılmış, diğer fiziksel arabirimler devre dışı bırakılmıştır.

Hata yönetimi ve bildirim mekanizması: Kart üzerindeki applet'ler, protokol dışı kullanım veya beklenmeyen durumlarda standart *Status Word* hata kodları döndürmektedir. Mobil istemci bu kodları yorumlayarak kullanıcıya anlamlı mesajlar sunar. Örneğin, imzalama işlemi başlatılmadan "signfinal" komutu gönderildiğinde kart "6A86" kodunu üretir; uygulama ise bu durumu "İşlem sırası hatası" olarak kullanıcıya iletir. Bu bildirimler, hata ayıklama sürecini kolaylaştırmakta ve kullanıcıyı yönlendirmektedir.

Zaman aşımı ve oturum yönetimi: NFC tabanlı haberleşme, özellikle iOS platformlarında 800ms gibi kısa zaman aşımına sahip oturumlarla sınırlıdır. Bu nedenle her bir NDEF mesajının yazılıp okunması işlemi, oturum süresine sığacak şekilde optimize edilmiştir. Büyük verilerin imzalanması gibi uzun işlemler, "prepkey" ve "signupdate" gibi parçalara ayrılarak yürütülmektedir. Android cihazlardaki donanımsal farklılıklar nedeniyle, bazı modellerde ek bekleme süreleri ve yeniden deneme mekanizmaları uygulanmıştır.

Veri bütünlüğü ve komut kimlik doğrulama: NDEF mesajlarının radyo frekanslı ortamda iletilmesi, potansiyel aktarma saldırılarına açık bir kanal oluşturabilir. Bu duruma karşı, kritik işlemler için opsiyonlu olarak mesaj bütünlüğü denetimi (örneğin önceden paylaşılan bir PIN ile birlikte hesaplanan HMAC) uygulanabilecek şekilde sistem mimarisi tasarlanmıştır. Bu özellik aktif olarak kullanılmamakla birlikte, güvenlik modelinde yer almakta ve gelecekteki sürümlerde devreye alınabilecek biçimde yapılandırılmıştır.
Uygulama ve kart tarafında alınan bu güvenlik önlemleri, kullanıcı etkileşiminde doğrudan görünür olmamakla birlikte, işlem sırasının bütünlüğünü, anahtar gizliliğini ve sistemsel tutarlılığı mimari düzeyde garanti altına alacak şekilde bütünleşik olarak uygulanmıştır.

5. DENEYSEL SONUÇLAR

Geliştirilen sistem, çeşitli test senaryoları kapsamında değerlendirilmiştir. Yapılan deneyler, sistemin performansını, NDEF tabanlı iletişimdeki güvenilirliği, mobil platformlar arası uyumluluğu ve önerilen çözümün mevcut donanım cüzdanlara kıyasla avantajlarını ortaya koymayı amaçlamaktadır.

5.1. Sistem Yapılandırması ve Test Ortamı

Önerilen sistem mimarisi, JCOP v3.0.1r3 tabanlı, NXP'nin SmartMX3 ailesine ait P71D321 güvenlik kontrolcüsünü içeren bir Java Card 3.0.5 Classic Edition destekli akıllı kart üzerinde gerçekleştirilmiştir. Kart, ISO/IEC 14443 Type A uyumlu olup, Common Criteria EAL6+ (PP0084) sertifikasına sahiptir ve ödeme, erişim kontrolü ve kimlik doğrulama gibi yüksek güvenlik gerektiren uygulamalara yönelik geliştirilmiştir [23].
Donanımsal özellikler açısından kart, AES (128, 192, 256-bit), DES/3DES, SHA-1/2/3, RSA (4096 bit'e kadar) ve ECC (521 bit'e kadar) gibi modern simetrik ve asimetrik algoritmaları donanım hızlandırmalı olarak desteklemektedir. Sistemimizde ECC (secp256r1) tabanlı dijital imza işlemleri, kartın yerleşik kriptografik ortak işlem birimi üzerinden gerçekleştirilmiştir. Ayrıca kart, AIS31 uyumlu donanımsal True Random Number Generator (TRNG) ve deterministic RNG modlarını desteklemektedir. Yazılım geliştirme süreci, Java SE Development Kit 8 (JDK 1.8) ortamında, JCIDE geliştirme ortamı kullanılarak gerçekleştirilmiştir. Geliştirilen applet, GlobalPlatform 2.3.1 standartlarına uygun olarak tasarlanmış ve kart üzerine GlobalPlatformPro aracıyla yüklenmiştir.
Mobil cihaz tarafında testler, Android 12 işletim sistemine sahip bir Samsung Galaxy Note 10 Lite (SM-N770F/DS) modeli üzerinde gerçekleştirilmiş olup, cihazda NDEF tabanlı iletişim sağlayan özel bir test uygulaması kullanılmıştır. Cihazda NXP Smart Card Reader API (v3.3) kullanılmıştır. NFC iletişimi doğrudan NDEF (NFC Data Exchange Format) mesajları üzerinden gerçekleştirilmiştir. Kart üzerindeki kontrol bileşeni, gelen NDEF mesajlarını ayrıştırarak ilgili kriptografik işlemleri gerçekleştirmek üzere yönlendirmektedir.
İmzalama testleri kapsamında, sistem tarafından 32 bayt uzunluğundaki SHA-256 hash değerleri ve 1KB'a kadar ham veriler (dummy veriler), NDEF mesajı formatında karta iletilmiş ve hem ECDSA (secp256r1) hem de Ed25519 algoritmalarıyla dijital imza çıktıları üretilmiştir.

5.2. Kriptografik İşlem Süreleri

Sistem performansı, temel kriptografik işlemlere ilişkin süre bazlı analizlerle değerlendirilmiştir. Bu kapsamda gerçekleştirilen deneysel çalışmalar, 32 bayt uzunluğundaki veri özetleri üzerinde yürütülen dijital imzalama ve anahtar üretim süreçlerini temel alarak işlem sürelerini nicel olarak ortaya koymaktadır. Gerçekleştirilen tüm deneysel ölçümler, işlem türüne, algoritma çeşidine ve veri boyutuna göre detaylandırılarak Tablo 3'te özetlenmiştir.
İmzalama işlemleri için Ed25519 ve ECDSA (secp256r1 eğrisi) olmak üzere iki farklı ECC algoritması değerlendirilmiştir. Ed25519 algoritmasıyla gerçekleştirilen bir imzalama işlemi, NXP JCOP4 [24] tabanlı Java Card üzerinde ortalama 752 milisaniyede tamamlanmıştır. Aynı işlem, ECDSA-P256 algoritması ile yaklaşık 386 milisaniyelik bir sürede gerçekleştirilmiştir. ECC anahtar çifti üretimi ise ortalama 800 milisaniye sürmüştür. Tüm işlem süresine NFC üzerinden yürütülen NDEF iletişim katmanının katkısı incelendiğinde, komut ve yanıt paketlerinin düşük boyutlu olması nedeniyle toplam süreye etkisinin sınırlı kaldığı görülmektedir. Ed25519 algoritmasının, mevcut Java Card 3.0.5 platformunda yalnızca yazılımsal olarak desteklenmesi nedeniyle işlem süresi görece yüksek kalmaktadır. Java Card 3.1 ile birlikte Ed25519 donanımsal hızlandırma desteği kazanmıştır. Bu sayede daha güncel kartlarla yapılacak uygulamalarda, işlem sürelerinde önemli iyileştirmeler elde edilmesi mümkündür. Deneysel ölçümlere göre, NDEF mesajlarının iletimi yalnızca birkaç milisaniyelik bir ek süre oluşturmakta ve böylece toplam işlem süresi açısından ihmal edilebilir düzeyde kalmaktadır.
İmzalanacak veri miktarının artması durumunda, sistem tarafından uygulanan parça bazlı iletim mekanizması ("signupdate" komutlarının ardışık kullanımı) doğrusal zaman artışına neden olmakta, ancak bu durum kullanıcı deneyimini olumsuz etkilemeyecek düzeyde kalmaktadır. Örneğin, 1KB boyutunda bir veri kümesi için toplam işlem süresi yaklaşık 700ms olarak ölçülmüştür. Elde edilen bu sonuçlar, kaynak kısıtlı Java Card ortamında dahi güvenli imzalama işlemlerinin, mobil cihazlarla etkileşim içinde makul sürelerde gerçekleştirilebildiğini ortaya koymaktadır.
Bu bağlamda, önerilen sistemin güçlü yönü; mobil senaryolarda pratik kullanım için yeterli işlem süreleri sunmasıdır. Bununla birlikte, donanımsal Ed25519 desteğinin bulunmadığı kartlarda yazılımsal implementasyona ihtiyaç duyulması, işlem süresinde kısmi artışa neden olan sınırlayıcı bir unsurdur.

5.3. NDEF Mesajlarının Güvenilirliği

NFC üzerinden gerçekleştirilen NDEF tabanlı iletişim, gerçekleştirilen deneysel çalışmalarda yüksek güvenilirlik düzeyi sergilemiştir. Farklı üreticilere ait Android cihazlarla yapılan testlerde, NDEF mesajlarının okuma ve yazma işlemleri sırasında herhangi bir kritik hata veya iletim kaybı gözlemlenmemiştir. Android işletim sisteminin sağladığı otomatik etiket algılama ve tetikleme özellikleri sayesinde, kullanıcı müdahalesi gerektirmeden işlemlerin ardışık biçimde yürütülmesi mümkün olmuştur.

Tablo 3. Kriptografik işlem süreleri ve performans karşılaştırması.

İşlem Türü	Algoritma	Veri Boyutu	Ortalama Süre	Açıklama
Anahtar Üretimi	ECDSA (secp256r1)	-	800 ms	Kart içi ECC anahtar çifti oluşturma. Donanım hızlandırma mevcut.
Donanımsal İmzalama	ECDSA (secp256r1)	32 Bayt (SHA-256)	386 ms	Donanım hızlandırmalı imzalama
Yazılımsal İmzalama	ED25519	32 Bayt (SHA-256)	752 ms	Java Card 3.0.5 ortamında yazılım tabanlı Ed25519. Donanım hızlandırma olmadığından ortalama süre uzamaktadır.
İmzalama (Büyük Veri)	ECDSA (secp256r1)	1 KB	~700 ms	Bu işlem signinit, birden fazla signupdate, signfinal akışıyla yapılmaktadır. Veriler birleştirilip edilip özet alma işlemi 300 milisaniye civarında sürmektedir. İmza 386 ms civarındadır.
NDEF Mesaj İşleme	-	Tek Kayıt	<5 ms	Okuma/yazma süresi, işlem süresine etkisi ihmal edilebilir düzeydedir

NFC teknolojisinin fiziksel sınırlılıkları kapsamında, kart ile mobil cihaz arasındaki mesafe ve hizalama koşulları da sistemin güvenilirliği açısından değerlendirilmiştir. Yapılan ölçümlere göre ideal okuma/yazma mesafesi yaklaşık 1~cm olarak belirlenmiş; bu mesafenin aşılması durumunda, özellikle metal telefon kılıfı gibi çevresel etkiler nedeniyle bağlantı kararlığında azalma gözlemlenmiştir. Bu durumu dengelemek ve kullanıcı deneyimini iyileştirmek amacıyla, mobil uygulama arayüzüne yönlendirici bir görsel rehber (örneğin telefonu karta yaklaştırmayı gösteren animasyon) entegre edilmiştir.
Sistemin yeniden deneme ve hata toleransı kabiliyetleri, 50 ardışık okuma/yazma işlemiyle yapılan testlerde değerlendirilmiştir. Testlerde nadiren de olsa karşılaşılan iletim hataları, uygulamanın yerleşik hata algılama ve yeniden deneme mekanizmaları sayesinde kullanıcıya yansıtılmadan otomatik olarak yönetilmiştir. Bu bağlamda, NDEF tabanlı haberleşme mekanizmasının hem güvenilirlik hem de etkileşim hızı açısından, mobil cihazlarla çalışan dijital imzalama uygulamaları için yeterli düzeyde olduğu sonucuna varılmıştır.
Bu kapsamda değerlendirildiğinde, önerilen sistemin güçlü yönü NDEF üzerinden sürücüsüz, güvenilir ve kararlı iletişim sağlamasıdır. Ancak sistemin sınırlı yönü, NFC hizalamasına olan duyarlılığı nedeniyle bazı cihaz/kılıf kombinasyonlarında iletişim performansının etkilenebilir olmasıdır.

5.4. Platformlar Arası Uyumluluk

Sistemin platformlar arası çalışma yetkinliği, farklı mobil işletim sistemleri ve cihaz üreticileri üzerinde gerçekleştirilen kapsamlı deneysel çalışmalarla analiz edilmiştir. Hem Android hem de iOS tabanlı mobil cihazlarla gerçekleştirilen testlerde, sistemin istikrarlı ve tutarlı bir şekilde çalıştığı gözlemlenmiştir. Uygulama, *React Native* çerçevesiyle geliştirilmiş olup, kod tabanının büyük bir bölümü her iki platformda ortak biçimde çalışacak şekilde yapılandırılmıştır. NFC erişiminde ortaya çıkan platforma özgü farklılıklar, soyutlama katmanları aracılığıyla giderilmiş ve sistemin tutarlı çalışması sağlanmıştır.
Sistem davranışı, yalnızca normal işlem akışlarıyla değil, aynı zamanda olası sınır durumlar ve hata senaryolarıyla da değerlendirilmiştir. Kullanıcının ardışık işlemler gerçekleştirmesi durumunda (örneğin birden fazla imzalama işlemini kısa sürede başlatması) sistem her isteği bağımsız bir oturum olarak ele alarak başarılı şekilde işleyebilmiştir. Ayrıca, kartın etkileşim sırasında erken uzaklaştırılması, protokole uygun olmayan komutların iletilmesi gibi durumlarda, sistem bu hataları güvenli biçimde işleyerek, kilitlenme yaşamaksızın yeni işlemlere hazır hâle gelmiştir.
Bu deneysel gözlemler, sistemin farklı cihaz ve platform konfigürasyonlarında kararlı çalıştığını, platformlar arası geçişlerde güvenilirlik sağladığını ve kullanıcı deneyimini sekteye uğratmadan çeşitli senaryolara adaptasyon sağlayabildiğini ortaya koymaktadır. Tüm bu değerlendirmeler ışığında sistemin güçlü yönü, iOS desteği sayesinde mevcut donanım cüzdanlara kıyasla platform bağımsızlık açısından önemli bir avantaj sunmasıdır. Bununla birlikte, iOS işletim sisteminde NFC oturum süresinin sınırlı olması, büyük boyutlu verilerin dikkatli biçimde bölünmesini ve yönetilmesini gerektirmektedir. Ayrıca, Apple'ın NFC erişimiyle ilgili API'lerinde zaman zaman yaptığı değişiklikler, mevcut uygulamanın kararlılığını ve çalışabilirliğini etkileyebilecek potansiyele sahiptir. Özellikle NFC oturum süresine ilişkin yapılacak olası kısıtlamalar, uygulamanın iOS üzerinde çalışmasını sınırlayabilir veya tamamen engelleyebilir. Bu tür platforma özgü değişikliklere rağmen, önerilen sistem mimarisi Android, Linux ve Windows işletim sistemlerinde sorunsuz çalışmakta olup, mobil cihazlar dışında kart okuyucular aracılığıyla da geniş uyumluluk göstermektedir.

5.5. Donanım Cüzdanlarıyla Karşılaştırma

Çalışmada önerilen mimari, günümüzde yaygın olarak kullanılan donanım cüzdanları ile çeşitli yönlerden karşılaştırmalı olarak analiz edilmiştir. Bu karşılaştırma; platform bağımsızlığı, kullanım kolaylığı, güvenlik düzeyi, işlem performansı ve geliştiriciye yönelik özelleştirme olanakları başlıkları altında sunulmaktadır.

Platform Bağımsızlığı: Mevcut donanım cüzdanları genellikle masaüstü uygulamaları veya sınırlı mobil destek ile entegre şekilde çalışmaktadır. Örneğin, Trezor cihazları iOS platformlarında doğrudan kullanılamamakta, yalnızca Android tabanlı cihazlarla uyum sağlamaktadır. Ledger Nano X modeli Bluetooth bağlantısıyla iOS desteği sunsa da bu destek batarya seviyesi, cihaz eşleşmesi ve bağlantı istikrarı gibi ek bağımlılıklar içermektedir. Öte yandan, önerilen Java Card tabanlı çözüm, pasif bir NFC cihazı olması nedeniyle herhangi bir pil gereksinimi olmaksızın doğrudan mobil cihazlardan enerji alarak hem Android hem de iOS platformlarında sorunsuz şekilde çalışabilmektedir.

Kullanım Kolaylığı: NFC temelli "yaklaştır ve işlem yap" etkileşim modeli, kullanıcıya hızlı ve sezgisel bir deneyim sunmaktadır. Örneğin, kullanıcı sadece kartı telefona yaklaştırarak işlem başlatabilmekte; bu süreç özel bir bağlantı kurulumu veya kullanıcı doğrulaması gerektirmemektedir. Buna karşın, donanım cüzdanlarında genellikle kablolu bağlantı, arayüz navigasyonu veya fiziksel onaylama gibi ilave adımlar bulunmaktadır. Bu bağlamda sunulan yaklaşım, günlük kullanımda pratiklik ve ergonomi açısından avantaj sağlamaktadır.

Güvenlik: Java Card platformu, özel anahtarların kart dışına çıkarılmadan güvenli biçimde saklanmasını ve tüm kriptografik işlemlerin donanım içinde yürütülmesini sağlamaktadır. Kullanılan JCOP4 kartı, EAL6+ güvenlik sertifikasına sahip olup, donanım cüzdanlarında yaygın olan EAL5+/EAL6+ güvenlik seviyeleriyle karşılaştırılabilir niteliktedir. NFC tabanlı iletişim kanalının açık doğası, belirli tehdit faktörlerini beraberinde getirse de; yalnızca filtrelenmiş ve sınırlandırılmış bir NDEF komut setine izin verilmesi, protokol dışı erişimin engellenmesi ve kartın yalnızca yetkilendirilmiş komutları kabul etmesiyle bu riskler minimize edilmiştir. Ayrıca, sistem mimarisi gelecekte PIN tabanlı doğrulama ve erişim kilitleme gibi mekanizmaları entegre edebilecek biçimde tasarlanmıştır.

Performans: Gerçekleştirilen ölçümler, geliştirilen sistemin imzalama süresi açısından donanım cüzdanlarıyla karşılaştırılabilir seviyede olduğunu ortaya koymaktadır. Örneğin, ECDSA-P256 ile imzalama süresi ortalama 386ms olarak ölçülürken, Ed25519 algoritması için bu süre 752ms civarındadır. Bu değerler, örneğin Ledger Nano S gibi donanım cüzdanlarının tipik işlem süreleri (500ms) ile paralellik göstermektedir. Ayrıca, Bluetooth üzerinden bağlantı kuran cihazların işlem başlatma süresindeki gecikmelere kıyasla, NFC iletişimi düşük gecikmeli ve daha az kullanıcı müdahalesi gerektiren bir alternatif sunmaktadır.

Açık Format ve Özelleştirilebilirlik: Geliştirilen sistemin bir diğer güçlü yönü, iletişim katmanında açık standart olan NDEF protokolünü kullanması ve uygulama yazılımının açık kaynak biçiminde geliştirilebilir olmasıdır. Bu durum, akademik araştırmalar, özelleştirilmiş kriptografik iş akışları ve prototipleme süreçleri açısından ciddi bir esneklik sağlamaktadır. Donanım cüzdanlarında ise genellikle üretici tarafından kapalı kaynaklı sistemler ve sınırlı yapılandırma seçenekleri sunulmaktadır.
Bu karşılaştırmalı değerlendirme, sunulan yaklaşımın mobil uyumluluk, erişim kolaylığı ve özelleştirme esnekliği açısından donanım cüzdanlarıyla karşılaştırılabilir nitelikte bir alternatif oluşturabileceğini göstermektedir.

6. SONUÇ

Bu çalışmada, Java Card platformu ve NDEF standardı kullanılarak geliştirilen, mobil cihazlarla uyumlu dijital imzalama sistemi sunulmuştur. Sistem, platform bağımsız çalışabilmesi, açık standartlara dayalı iletişim modeli, mobil cihazlarla doğal etkileşim sunması ve güvenli anahtar saklama yetenekleri ile dikkat çekmektedir. Kullanıcıların özel anahtarlarını güvenli donanım üzerinde saklayarak mobil cihazlar aracılığıyla işlem gerçekleştirebilmeleri, sistemin hem güvenlik hem de kullanılabilirlik açısından dengeli bir yapı sunduğunu göstermektedir.
Önerilen sistem, kripto varlık yönetiminde mobil uyumlu ve donanımsal güvenliğe sahip bir dijital imzalama altyapısı sunarak mevcut çözümlerin sınırlı kaldığı alanlara katkı sağlamaktadır. Sistemin başlıca yenilikleri şunlardır: (i) NFC üzerinden NDEF iletişim formatının kullanılması sayesinde platformdan bağımsız, harici uygulamasız ve sürücüsüz bir çalışma imkânı sunulmuştur; (ii) "Tap-and-sign" temelli sezgisel kullanıcı etkileşimi ile işlem süreci sadeleştirilmiş ve kullanıcı dostu hâle getirilmiştir; (iii) Java Card üzerinde izole çalışan applet mimarisi sayesinde, özel anahtarların hiçbir zaman kart dışına çıkarılmadan güvenli biçimde yönetilmesi sağlanmıştır; (iv) Gerçekleştirilen testlerde imzalama süresinin ortalama ~752 ms ve ~386 ms seviyesinde olduğu gözlemlenmiş ve sistemin kararlı, hızlı çalıştığı doğrulanmıştır; (v) Açık kaynaklı ve modüler mimarisi sayesinde, sistemin farklı kullanım senaryolarına kolaylıkla entegre edilebileceği ve geliştirilebileceği ortaya konmuştur.
Sunulan yaklaşım, literatürde sınırlı sayıda örneği bulunan mobil uyumlu donanım cüzdan mimarilerine katkı sunmakta hem Android hem de iOS platformlarında çalışabilmesi ile mevcut çözümlerden ayrışmaktadır. Deneysel analizler, sistemin işlem süresi, güvenilirlik ve platformlar arası uyumluluk açısından başarılı sonuçlar verdiğini göstermiştir. Donanım cüzdanlarıyla yapılan karşılaştırmalar, özellikle erişilebilirlik ve esneklik bağlamında önerilen sistemin rekabetçi olduğunu ortaya koymaktadır.
Mevcut sistem mimarisi, kullanıcı kimlik doğrulaması gibi ek güvenlik katmanlarını destekleyecek biçimde tasarlanmıştır. Ancak mevcut prototip, PIN tabanlı erişim kontrolü mekanizmasını henüz içermemektedir. Bu çalışmanın temel amacı, uçtan uca çalışan tam bir ürün geliştirmekten ziyade, donanım tabanlı dijital imzalama işlemleri için açık standartlara dayalı, genişletilebilir ve platformdan bağımsız bir mimari çerçeve sunmaktır. Bu bağlamda, PIN doğrulama ve benzeri güvenlik katmanları, sistemin gelecekteki sürümlerinde kolaylıkla entegre

edilebilecek şekilde mimari tasarım kapsamında öngörülmüştür. Gelecek çalışmalar, sistemin güvenlik modelini daha da güçlendirmek amacıyla PIN tabanlı erişim kontrolü ve oturum yönetimi gibi ek mekanizmaları entegre etmeyi hedeflemektedir. Ayrıca, FIDO2/WebAuthn protokol desteği entegre edilerek, kartın dijital imzalama dışında kimlik doğrulama senaryolarında da kullanılabilmesi amaçlanmaktadır. Buna ek olarak, mobil uygulama ile kart arasındaki iletişimin şifrelenerek güvenliğinin artırılması amacıyla Secure Channel (Güvenli Kanal) protokolünün entegrasyonu planlanmaktadır. Özellikle açık NFC haberleşmesinin kullanıldığı bir ortamda, APDU komutlarının şifreli olarak iletilmesi, veri gizliliği ve bütünlüğü açısından kritik bir katkı sunacaktır. Secure Channel kullanımı, şifreli iletişim sırasında NDEF mesajlarının segmentlenmesi, MAC hesaplama ve veri şifreleme/çözme işlemleri gibi ek adımlar gerektirdiğinden, işlem süresine yaklaşık 100–200 ms düzeyinde bir ek süre yükü getirmesi beklenmektedir. Bu etki, ilerideki sürümlerde hem deneysel ölçümlerle hem de farklı güvenlik seviyeleriyle birlikte değerlendirilerek sistemin performans-güvenlik dengesi daha kapsamlı şekilde optimize edilecektir.

Mobil uygulamanın kullanıcı deneyimini geliştirmek üzere arayüzde işlem geçmişi görüntüleme, çoklu hesap desteği, imzalı belge kontrolü gibi özelliklerin eklenmesi hedeflenmektedir. Son olarak, kart üreticileri ile yapılacak iş birlikleri sayesinde donanım seviyesinde optimizasyonlar (örneğin özel NFC komutları veya artırılmış NDEF alanı gibi) gerçekleştirilmesi mümkün olacaktır. İleri düzey senaryolar kapsamında, kart üzerinde yer alacak bir onay tuşu ve E-Ink ekran gibi donanımsal yeniliklerle, imza sürecinin görselleştirilmesi ve işlemlerin kullanıcı tarafından fiziksel olarak onaylanması olanaklı hale getirilebilir.

Bu çalışma, düşük güçlü güvenli donanım birimlerini mobil cihazlarla entegre ederek güvenli, taşınabilir ve kullanıcı dostu bir dijital imzalama çözümü sunmaktadır. Sunulan mimari, halihazırda bilinen kriptografik algoritmaların donanım destekli, platformdan bağımsız ve açık standartlara dayalı bir yapı içerisinde uygulanmasını mümkün kılan bütüncül bir çözüm ortaya koymaktadır. Java Card platformunun sunduğu donanımsal güvenlik özelliklerinden yararlanan sistem; kriptografik işlemler, güvenli anahtar saklama ve mobil cihazlarla doğal etkileşim gibi kritik işlevleri güvenli ve standartlara uygun biçimde gerçekleştirebilmektedir. Ayrıca sistem, ödeme, e-kimlik ve erişim sistemlerinde yaygın olarak kullanılan ve Common Criteria EAL6+ gibi yüksek güvenlik sertifikalarına sahip Java Card donanımlarla doğal uyumluluk sağlayacak şekilde tasarlanmıştır. Bu da önerilen yaklaşımın hem güvenlik açısından gerekliliğini hem de pratikte yaygınlaştırılabilirliğini desteklemektedir. Bu yönüyle, platforma özel sürücü ya da uygulama gerektirmeyen, NDEF tabanlı iletişim modeliyle çalışan sistem hem teknik erişilebilirlik hem de güvenlik açısından özgün bir denge sunmaktadır. Bu yönüyle çalışma hem akademik hem de endüstriyel uygulamalarda uygulanabilir olup, gelecek çalışmalarla birlikte daha da kapsamlı hale getirilebilir. Bu yaklaşımın, dijital dünyada güvenli ve kullanıcı dostu imzalama uygulamalarına yönelik önemli bir adım olduğu değerlendirilmektedir.

Yazar Katkıları

Bu çalışma, her iki yazarın eşit katkılarıyla yürütülmüş olup, problem tanımı, sistem tasarımı, deneylerin gerçekleştirilmesi, analizlerin yapılması ve makale metninin yazımı süreçlerinde ortak sorumluluk alınmıştır.

Çıkar Çatışması

Makale yazarları aralarında herhangi bir çıkar çatışması olmadığını beyan ederler.

KAYNAKÇA

[1] Ledger SAS, “Ledger Nano X Security Target,” ANSSI, Security Target, 2023. Available: https://cyber.gouv.fr/sites/default/files/document_type/ANSSI-cible-CSPN-2023_17en.pdf

[2] C. Christen and M. Lafon, “Why Secure Elements Make a Crucial Difference to Hardware Wallet Security,” Ledger Donjon, Tech. Rep., 2025.

[3] Oracle Corporation, “Java Card Platform Security – Technical White Paper,” Oracle Corporation, 2001. Available: https://www.oracle.com/a/otn/docs/java/javacardsecuritywhitepaper-149957.pdf

[4] H. Rezaeighaleh, “Improving Security of Crypto Wallets in Blockchain Technologies,” Ph.D. dissertation, Dept. of Computer Science, Univ. of Central Florida, Orlando, FL, 2020.

[5] S. Suratkar, M. Shirole, and S. Bhirud, “Cryptocurrency Wallet: A Review,” in Proc. 2020 4th Int. Conf. Computer, Communication and Signal Processing (ICCCSP), Chennai, India, 2020, pp. 1–7.

[6] H. Rezaeighaleh and C. C. Zou, “New Secure Approach to Backup Cryptocurrency Wallets,” in Proc. 2019 IEEE Global Communications Conf. (GLOBECOM), Waikoloa, HI, USA, 2019, pp. 1–6.

[7] D. Bamert, C. Decker, R. Wattenhofer, and S. Welten, “BlueWallet: The Secure Bitcoin Wallet,” in Proceedings of the 3rd IEEE International Conference on Mobile Secure Systems, 2020.

[8] M. Popchev, I. Mirchev, and T. Stoyanova, “Towards Blockchain Wallets Classification and Implementation,” in Proceedings of the 17th International Conference on Computer Science and Education in Computer Science (CSECS), 2023.

[9] S. Houy, P. Schmid, and A. Bartel, “Security aspects of cryptocurrency wallets—A systematic literature review,” ACM Computing Surveys, vol. 56, no. 1, pp. 1–31, 2023.

[10] I. Homoliak and M. Perešíni, “SoK: Cryptocurrency Wallets–A Security Review and Classification Based on Authentication Factors,” in Proc. 2024 IEEE Int. Conf. Blockchain and Cryptocurrency (ICBC), Dubai, UAE, 2024, pp. 1–8.

[11] M. Elo and J. Nikander, “Decentralized Authorization with ECDSA on a Java Smart Card,” Helsinki Univ. of Technology, Telecommunications Software and Multimedia Laboratory, Tech. Rep. TML-C5, 2000.

[12] N. Sejfuli-Ramadani, F. Idrizi, V. Angelkoska, and A. Risteski, “A comparative analysis of offline wallets and their integration with NFC for practical offline payments,” J. Nat. Sci. Math. UT, vol. 9, no. 17–18, pp. 354–360, 2024.

[13] N. Lehto, K. Halunen, O.-M. Latvala, A. Karinsalo, and J. Salonen, “CryptoVault–A Secure Hardware Wallet for Decentralized Key Management,” in Proc. 2021 IEEE Int. Conf. Omni-Layer Intelligent Systems (COINS), Barcelona, Spain, 2021, pp. 1–4.

[14] P. Urien, “Crypto Terminal: A New Open Device for Securing Blockchain Wallets,” in Proc. 2020 IEEE Int. Conf. Blockchain and Cryptocurrency (ICBC), Toronto, Canada, 2020, pp. 1–3.

[15] H. Rezaeighaleh and C. C. Zou, “Deterministic Sub-Wallet for Cryptocurrencies,” in Proc. 2019 IEEE Int. Conf. Blockchain (Blockchain), Atlanta, GA, USA, 2019, pp. 419–424.

[16] N. Duif, Smart card implementation of a digital signature scheme for Twisted Edwards curves, M.S. thesis, Dept. of Mathematics and Computer Science, Technische Universiteit Eindhoven, Eindhoven, Netherlands, 2011.

[17] A. Tanrıkulu, H. Yüce, and E. Ölçer, “Blokzincir Tabanlı Donanımsal Cüzdan ve Akıllı Kartlar,” Afyon Kocatepe Üniversitesi Uluslararası Mühendislik Teknolojileri ve Uygulamalı Bilimler Dergisi, vol. 4, no. 1, pp. 37–48, 2021.

[18] R. V. Fritsche, L. M. Palma, and J. E. Martina, “Recommendations for Implementing a Bitcoin Wallet Using Smart Card,” Tech. Rep., Dept. of Informatics and Statistics, Federal University of Santa Catarina (UFSC), Florianópolis, Brazil, 2020.

[19] NFC Forum, “NFC Forum Type 4 Tag Operation Specification,” NFC Forum, Inc., Technical Specification, 2021. Available: https://nfc-forum.org/build/specifications/type-4-tag-specification

[20] NFC Forum, “NFC Data Exchange Format (NDEF) Technical Specification,” NFC Forum, Inc., Technical Specification, 2020. Available: https://nfc-forum.org/build/specifications/data-exchange-format-ndef-technical-specification/

[21] D. J. Bernstein, N. Duif, T. Lange, P. Schwabe, and B.-Y. Yang, “High-Speed High-Security Signatures,” J. Cryptographic Eng., vol. 2, no. 2, pp. 77–89, 2012.

[22] Oracle Corporation, “Java Card 3 Platform: Version 3.0.5 Classic Edition – Specification,” Oracle Corporation, Technical Specification, 2019. Available: https://docs.oracle.com/en/java/javacard/3.0.5/index.html

[23] NXP Semiconductors, “P71D321 Secure Element for eID and Mobile ID,” NXP Semiconductors, Fact Sheet, 2022. Available: https://www.nxp.com/docs/en/fact-sheet/P71D321.pdf

[24] NXP Semiconductors, “JCOP 4 Secure Identification Platform,” NXP Semiconductors, Tech. Rep., 2020. Available: https://www.nxp.com/docs/en/brochure/JCOP4SECIDAPPA4.pdf