EAI Endorsed Transactions
on Scalable Information Systems

Research Article EAI.EU

Improved Authentication in Information Systems through a Mobile Identity Management Scheme (MoIdM-MSS) Utilizing Mobile Signature Service

Mohammadjavad Sharifpour[1,*], Mehdi Shajari[2] and Seyyed Amir Asghari Tochae[3]

[1]Department of Computer Engineering, Amirkabir University of Technology (Tehran Polytechnic), Tehran, Iran
[2]Ted Rogers School of Management, Toronto Metropolitan University, Toronto, Canada
[3]Department of Electrical and Computer Engineering, Faculty of Engineering, Kharazmi University, Tehran, Iran

Abstract

In today's digital economy, work processes are increasingly digitized using computer information systems. An essential aspect of employees' reliance on these systems is trust in their reliability. Mobile devices and apps play a vital role in this digital landscape, with Mobile Identity at the forefront. Mobile Identity extends the concept of digital identity through mobile networks, acting as a tool for login and transactions and as a crucial element in communication and interaction. This paper introduces a Mobile Identity Management Scheme based on the Mobile Signature Service for information systems. The scheme enables digital signatures on mobile devices for various purposes, enhancing security by leveraging the user's private key and the system's authentication challenge. Through this approach, authentication is ensured by permitting only users with the correct private key to sign the challenge, eliminating the necessity for traditional authentication methods such as usernames and passwords.

Furthermore, the scheme leverages mobile device security features like secure computing environments and biometric authentication to bolster authentication. By adding an extra layer of protection and focusing on user convenience, security is heightened without introducing unnecessary complexity. Evaluations conducted in local signing scenarios have demonstrated the scheme's effectiveness, acceptance, and potential, indicating promising results for its application in enhancing work process security.

Keywords: Mobile Identity Management, Mobile IdM, Mobile ID, Mobile Signature Service, MSS, Information Systems, Technology Acceptance Model, TAM

Received on 24 November 2024, accepted on 04 February 2025, published on 02 April 2025

doi: 10.4108/eetsis.9014

1. Introduction

In various aspects of life, a shift from a 'one size fits all' approach to a 'bring your own device' mentality is evident in the handling of official documents. People now seek to use their smartphones for tasks previously done with physical documents, such as their eID card, as they are accustomed to the convenience and versatility of this technology. For instance, many prefer accessing digital boarding passes and tickets on their smartphones rather than in print for activities like airport check-ins. Similarly, rail travellers can digitally store their tickets and railway cards on their phones [1].

Smartphones are becoming increasingly essential for identification and authentication, both online and in the physical world. Given their widespread use, storing identity data on smartphones is practical. However,

[*]Corresponding author. Email: m-javad.sharifpour@aut.ac.ir

ensuring the security of this data is crucial, as it contains vital information about individuals [1].

There has been a noticeable shift towards online transactions via mobile platforms in recent years. This trend has led to the development of mobile applications for various services such as smart parking meters, traffic management, public transit, healthcare, precision agriculture, building management, public monitoring, and petrol stations. These advancements have improved operational efficiency and user satisfaction [2]. The rise of global online commerce has also increased digital transactions significantly [3]. In today's digital age, having a secure mobile identity is essential as users depend on digital identities to verify their authenticity and access online services easily [4].

Mobile identity typically refers to using a SIM card to authenticate the owner of a mobile device. This involves verifying the user's identity attributes linked to the device for access authorization [5]. However, evolving mobile threats pose challenges with new features and detection avoidance techniques [6]. On the other hand, information systems involve various components like brainware, hardware, and software to organize and process data for decision-making and analysis [7]. While the progress in information systems benefits us, concerns around privacy and security have also emerged due to our systems' complex and decentralized nature [8]. Consequently, the mobile signature service allows users to sign documents or other information using a personal device's signing key. The term 'personal device' encompasses mobile devices and other general computing devices like personal computers, tablets, and laptops [9].

The Mobile Signature Service (MSS) offers a significant advantage as it leverages the widespread use of mobile phones, with 5.4 billion people having a mobile subscription in 2022 (GSMA [10]). This makes smartphones a compelling option for governments aiming to provide citizens with secure and convenient online services. Research suggests that global unique mobile subscribers will reach 6.3 billion by 2030 (Mobile Economy 2023 [10]), and over 3 billion individuals worldwide are expected to have a government-issued mobile ID app by 2024 (Juniper Research [11]).

This paper presents a mobile identity management scheme utilizing the mobile signature service (MSS) to address the issues discussed. Section 2 offers context on Mobile Signature Service and Mobile Identity Management. Section 3 covers existing research on mobile identity management, while Section 4 explains our scheme. Section 5 explores implementation approaches, followed by an acceptance and usage analysis in Section 6. Finally, Section 7 concludes the paper.

1.1 Our contributions

This article introduces a cutting-edge mobile identity management scheme that utilizes a mobile signature service to transform the authentication process for mobile users. Our innovative scheme enables users to securely create digital signatures on their mobile devices for various purposes, including authentication requests and identity verification. The primary goal of our scheme is to ensure robust and secure authentication using the user's private key and the system-generated authentication challenge, thereby eliminating vulnerabilities associated with traditional methods like usernames and passwords. Our scheme leverages the advanced security features of mobile devices, such as secure computing environments and biometric authentication, adding an extra layer of protection to the authentication process for maximum user security.

Additionally, our emphasis on user convenience and friendliness distinguishes our system. Users can easily verify their identity using their mobile devices, eliminating the necessity for extra authentication devices or intricate procedures. This seamless authentication approach provides both convenience and improved security while maintaining usability. Our system, which was developed as a mobile application, has been carefully designed and executed, with deployment results demonstrating its efficiency, effectiveness, and user acceptance. By providing a secure, convenient, and user-friendly authentication solution, we aim to empower users to authenticate themselves confidently and effortlessly.

2. Preliminaries

This section aims to provide the reader with the required context, detail, and concepts. Our proposed scheme is based on two concepts: The Mobile Signature Service and Mobile Identity Management.

2.1 The Mobile Signature Service

A mobile signature service functions like a traditional stamped signature to authenticate documents or data. Unlike a typical digital signature, which requires a token and special software, this service saves entrepreneurs' costs. It does not require software installations on multiple workstations and is accessible on any operating system or device, making it convenient, cost-efficient, and easily accessible [12].

The mobile certificate, developed in Finland in partnership with mobile network operators, is based on ETSI's Mobile Signature Service (MSS) standards [13]. MSS authorizes transactions initiated by users on their mobile devices, especially in financial contexts. The MSS manages the mobile signature process for both users and application providers. Mobile Signature Service Providers (MSSPs) offer MSS systems to service providers for authentication and content signing purposes in web service interfaces [14], [15]. Understanding MSS is crucial for network services utilizing mobile certificates. ETSI's Mobile Signature Service Standards include standards for mobile commerce (M-COMM [14], [15], [16], [17]) and standardizing digital signatures [9] on personal devices, as detailed in Table 1. This section is restricted to an overview of the relevant standards with a short description.

ETSI TR 102 203 [14] – "Mobile Signatures; Business Functional Requirements"
This standard defines the business and functional requirements for mobile signature service solutions that utilize smartcards, such as the GSM SIM card, and cryptographic techniques, specifically asymmetric cryptography used in public key infrastructure (PKI). These technologies are employed to streamline the implementation of electronic signature solutions.

ETSI TS 102 204 [15] – "Mobile Signature Service; Web Service Interface"
This standard outlines the methods that a mobile signature web service provider must offer. It describes the syntax of the messages exchanged between the server (MSSP) and the application providers (APs).

ETSI TR 102 206 [16] – "Mobile Signature Service; Security Framework": This standard comprises a framework of security requirements for a mobile signature service. In this respect, all stakeholders need to identify the level of security that an MSSP may, should, or must provide.

ETSI TS 102 207 [17] – "Mobile Signature Service; Specifications for Roaming in Mobile Signature Services"
This standard supports roaming for mobile signature services at the transaction level. It involves passing transactions through a linked Mobile Signature Service Providers (MSSPs) chain. The standard specifies technical interfaces over SOAP and HTTP for architectures that enable the roaming of mobile signature messages between the end-user and an application provider. Additionally, it facilitates the construction of an open model.

ETSI SR 019 020 [9] – "The framework for the standardization of signatures; Standards for AdES digital signatures in mobile and distributed environments"
This standard offers a framework to further standardize the creation and validation of AdES digital signatures (The term AdES refers to the result of serializing structures compliant with CAdES [18], XAdES [19], or PAdES [20].) in mobile and distributed environments with the assistance of remote servers. It recognizes the evolution of personal devices' capabilities, which are expected to increasingly overlap with those of other computing devices.

Table 1. ETSI MOBILE SIGNATURE STANDARDS

No	ETSI Mobile Signature Standards	
	Standard	Scope
1	Technical Report: ETSI TR 102 203	Mobile Commerce (M-COMM); Mobile Signatures; Business and Functional Requirements.
2	Technical Specification: ETSI TS 102 204	Mobile Commerce (M-COMM); Mobile Signature Service; Web Service Interface.
3	Technical Report: ETSI TR 102 206	Mobile Commerce (M-COMM); Mobile Signature Service; Security Framework.
4	Technical Specification: ETSI TS 102 207	Mobile Commerce (M-COMM); Mobile Signature Service; Specifications for Roaming in Mobile Signature Services.
5	Special Report: ETSI SR 019 020	The Framework for Standardization of Signatures; Standards for AdES Digital Signatures in Mobile and Distributed Environments.

2.2 Mobile Identity Management

Having a digital identity is crucial for using information systems. It involves using proper authentication methods to ensure the privacy, integrity, and security of the user's identity. Mobile identity is the umbrella term for using mobile communication to develop, enhance, and protect user identities, incorporating the following key features [21]:

1) Use of mobile communication, including mobile network, infrastructure, and distribution chain in:

- The establishment of citizen identity.
- The distribution, authentication, and verification of citizen identity.
- The provision of governmental, public, and social services.
- The provision of financial, private, and enterprise services.

2) Mobile phones are used as identification and authentication tokens.

Identity management (IdM) enables identification, authentication, and authorization in various digital processes involving humans. It is crucial for digital services, work processes, customer relationship management, telecommunications, and payment systems. Organizations depend on a specific IdM technology tailored to their needs for registration, credential issuance, and digital identity deployment [22].

Identity Management General Standards

The ISO/IEC 24760 series outlines a comprehensive framework for identity management, encompassing the entire life cycle of identity information. It defines key concepts and operational structures essential for effective identity management, aiming to facilitate information system management that ensures compliance with business, contractual, regulatory, and legal requirements [23].

- Part 1 of the standard clarifies identity management terminology and concepts to enhance understanding in the field [23].
- Part 2 of the standard outlines a reference architecture for an identity management system, detailing key architectural elements and their interconnections with various deployment models. It also lays out the requirements for designing and implementing an identity management system to ensure it aligns with stakeholders' goals in its deployment and operation [23].
- Part 3 of the standard introduces practices for identity management. These include ensuring the proper use of identity information, controlling access to this information and other resources based on identity, and implementing necessary objectives for establishing and maintaining an identity management system [23].

ISO/IEC 29115 outlines a framework for entity authentication assurance, encompassing the confidence in processes, management activities, and technologies to establish and oversee an entity's identity for authentication transactions [23].

ISO/IEC 29115 outlines four levels of entity authentication assurance and criteria for achieving each level. It also guides mapping different authentication schemes to these levels, exchanging authentication results, and implementing controls to mitigate authentication threats [23].

ISO/IEC 23220 Standards

This series of standards offers foundational elements for mobile eID system infrastructures and standardizes protocols, interfaces, and services for mobile eID applications and verification apps. It accomplishes this by defining generic system architectures, transaction flows, and lifecycle phases for mobile eID systems. A crucial component of this standard is the secure area of a secure device, which can be realized through various secure elements like embedded universal integrated circuit cards (eUICCs), embedded secure elements (eSEs), or Trusted Execution Environments (TEEs) [1].

3. Background and Related Works

Governments issue digital credentials, such as digital national insurance cards and mobile driver's licenses, for various reasons, aiming to enhance data accuracy, convenience, and security. These government-issued credentials verify legal identity through an identity resolution process, ensuring authenticity and uniqueness within the population. Transitioning to digital credentials involves using digital signatures to safeguard foundational identity information and biometric data, preventing fraud and ensuring data integrity. How governments manage digital credentials and data sharing impacts privacy outcomes significantly. The immediate motivations for issuing government digital identity credentials involve [24]:

1) Assisting individuals in asserting their identity online and in person, such as opening a bank account, buying age-restricted items, asserting rights to access government benefits, and travelling more smoothly.

2) Control fraud involves engaging in illegal activities, such as wrongfully collecting benefits or using false credentials to open financial accounts.

3) Assisting individuals in asserting their right to access age-restricted products or other services.

4) Ease of travel.

The government is issuing credentials for economy-wide use to safeguard individuals' access to benefits through digital identity verification. However, managing these roles simultaneously across various levels can be complex due to the need for coordination between local, national, and regional departments [24].

3.1 Specific Groups of Standards Providing Authentication Capabilities

Authentication Capability is the system's ability to verify the identity of devices or users before providing access to resources [25]. Common standards that offer authentication capabilities include TR-03110, ISO/IEC 18013, ITU-T X.509 | ISO/IEC 9594-8, eIDAS 2.0, Security Assertion Markup Language (SAML), OpenID Connect (OIDC), FIDO2, and Self-Sovereign Identity [23], [26].

International Civil Aviation Organization (ICAO) electronic machine-readable travel documents and the eIDAS token

ICAO establishes and upholds international standards. Its key belief is that public authorities should have a high level of trust in travel documents and inspection procedures to streamline the process for air travellers. By setting standardized specifications for travel documents and their data, ICAO aims to enhance this confidence [23].

A machine-readable travel document (MRTD) is an official document issued by a state or organization according to ICAO Document 9303 specifications. It is used for international travel, like a machine-readable passport, visa, or official travel document. The document includes required visual data and a machine-readable data summary format [23].

The basic MRTD is designed with optical character recognition for visual and mechanical reading. ICAO member states have recognized the need for standardization, understanding that adopting the Document 9303 standard formats for passports and travel documents offers benefits beyond automated clearance systems. These documents' physical characteristics and data security features protect against alteration, forgery, or counterfeiting. Additionally, using a standardized format for the visual zone of an MRTD streamlines inspection processes for airline and government officials, leading to quicker clearance of low-risk traffic, easier identification of issues, and improved enforcement [23].

Introducing biometric identification with data stored on a contactless integrated circuit (IC) enhances security, reduces fraud, and streamlines the process for legitimate document holders to obtain visas and pass through border inspections more efficiently [23].

The BSI and ANSSI have created the eIDAS token technical standards based on ICAO Document 9303, outlined in TR-03110. These specs facilitate the creation of customized electronic ID, authentication, and signature solutions that are seamlessly interoperable without using proxies, which aligns with the eIDAS middleware concept [23].

TR-03110's key features include user consent, two-factor authentication, strong authentication procedures, data minimization procedures, and an interoperable electronic logical data structure (LDS) encompassing all data fields used in European electronic identification infrastructures, with the ability to expand with new attributes effortlessly [23].

Mobile Driving Licence (mDL/mdoc) and Mobile eID

The mobile Driving Licence (mDL) is a popular initiative that transfers an ID to a smartphone. It is based on chip-based electronic driving licenses standardized in ISO/IEC 18013. This standard aims to streamline interface specifications for implementing a driving license in conjunction with a mobile device, focusing on the interface between the mDL and mDL Reader and the interface between the mDL Reader and the issuing authority infrastructure. The key function is accessing the smartphone's security anchor to authenticate the mDL data's origin and verify its integrity, which requires accessing the secure element used in the smartphone. As a result, the mDL incorporates protocols standardized in ISO/IEC 23220 for these purposes [1].

X.509 certificates

The Recommendation ITU-T X.509 | ISO/IEC 9594-8 standard defines public key infrastructure (PKI) and privilege management infrastructure (PMI) frameworks. Certification Authorities (CAs) issue X.509 public key certificates and often have Registration Authorities (RAs) and Validation Authorities (VAs) like Online Certificate Status Protocol servers. They provide certificate status information and may issue Certificate Revocation Lists (CRLs). Attribute Authorities (AAs) issue X.509 attribute certificates and maintain Attribute Revocation Lists (ARLs). Subscribers/subjects request and receive the certificates, while relying parties depend on them [23]**.**

Public key certificates can authenticate users for direct authentication, like in the TLS protocol, or for authentication before an IdP in an identity federation system. Certificates from an electronic identification scheme are acknowledged as electronic means of identification [23].

Public key certificates are utilized for server authentication, such as in TLS, and for generating advanced electronic signatures or seals. Those issued in the EU for electronic signatures, seals, and website authentication are governed by the eIDAS Regulation and are provided by trusted service providers. When utilized with an authentication method, Member States may acknowledge them as electronic identification tools [23].

Attribute certificates can assert users' identity attributes in authentication protocols and advanced electronic signatures or seals. Once approved, the eIDAS 2.0 regulation will regulate them as a trusted service for issuing electronic attestations of attributes [23].

Security Assertion Markup Language and the eIDAS regulation

The Security Assertion Markup Language (SAML) defines the syntax and processing rules for assertions made about a subject by a system entity. System entities using SAML may rely on other protocols to communicate about an assertion or its subject. The core SAML specification includes the structure of assertions and related protocols, along with rules for managing a SAML system [23].

OpenID Connect

The OAuth 2.0 Authorization Framework (IETF RFC 6749) and OAuth 2.0 Bearer Token Usage (IETF RFC 6750) specifications offer a framework for third-party apps to acquire and utilize restricted access to HTTP resources. While they outline ways to obtain and use Access Tokens for resource access, they do not establish standard approaches for identity information provision. Without profiling, OAuth 2.0 cannot provide information about an end user's authentication [23].

FIDO2

FIDO includes three sets of specifications for secure, passwordless user authentication: FIDO Universal Second Factor (FIDO U2F), FIDO Universal Authentication Framework (FIDO UAF), and Client to Authenticator Protocols (CTAP). Recommendation ITU-T X.1277 outlines the FIDO UAF, while ITU-T X.1278 covers the Client to Authenticator Protocol/Universal 2-factor framework [23].

Self-Sovereign Identity

Self-Sovereign Identity (SSI) is a new concept related to managing identity in the digital realm. Under the SSI approach, users can independently create and manage their identities without a central authority. SSI focuses on identity as a specific identifier that allows self-management, including authentication, self-assertion, and controlling and sharing third-party-asserted claims without relying heavily on a third party like a public or private identity provider. The ideological approach does not preclude the possibility that other parties may issue identity assertions that are not central to the identity itself [23].

3.2 Current projects around the world

Numerous projects have proposed solutions for managing mobile identities, including the ICAO DTC [1], OPTIMOS2 [1], Austrian ID Austria [27], Estonian Mobiil-ID [28], Finland Mobiilivarmenne [29], Belgian itsme® [30], identity management in cellular networks and GSM [31], federated identity management tools [32], [33], and mobile authentication solutions utilizing NFC-enabled national cards [34]. The increasing digitization of physical activities, like e-participation, online shopping, and e-banking, along with the prevalent use of smart devices with biometric features and connectivity, has led to a surge in the need for trustworthy mobile identity management solutions. This demand is projected to grow further in the coming years. Here, we delve into existing research on mobile identity management.

Digital Travel Credentials

In 2016, the ICAO New Technologies Working Group (NTWG) collaborated with the International Organization for Standardization (ISO) to establish a specialized subgroup aimed at standardizing digital travel credentials (DTC). These credentials, which can be issued or accessed digitally on smart devices or servers, represent a traveller's identity. A DTC can potentially replace a traditional passport temporarily or permanently. For a DTC to be effective, it should offer functionality and security features similar to those found in current eMRTDs. ICAO's responsibility is to develop policies and use cases, while ISO focuses on specifying technical guidelines in this area [1].

The main feature of the ICAO DTC is the ability for authorities to verify a digital passport data representation before the traveller's arrival, ensuring the data's integrity and authenticity. This capability provided by the ICAO DTC allows for [35]:

- Gathering precise and reliable information, including facial biometrics, in advance of travel improves screening abilities, such as travel authorization processing and pre-arrival screening.
- Enhancing border processes by broadening automated and biometric-enabled procedures for greater efficiency.
- Enhanced speed and convenience for travellers.

OPTIMOS 2

OPTIMOS 2 aims to create an open, user-friendly, and secure identity ecosystem for mobile services. The project aims to provide a platform for eID providers to offer mobile eID services at the "substantial" eIDAS level. Additionally, it aims to offer service providers a secure and privacy-friendly platform for mobile services at a certain security level. Access to a smart device's secure element ensures this security level. In this case, the holder data derived from the German ID card is securely stored in the smartphone's secure element. A Trusted Service Manager (TSM) provides access to the secure element, enabling secure and authentic storage of holder data [1].

The Austrian ID Austria and the Estonian Mobiil-ID

In Europe, especially in Austria and Estonia, user conversion rates of governmental mobile identity management solutions are on the rise if citizens have access to a dedicated ecosystem, as a study on mobile identity management solutions shows in [24]. The Austrian (“ID Austria” [27]) and Estonian mobile eID (“Mobiil-ID” [28]) can already be used for online authentication for electronic services (e.g., e-government, e-banking).

The Finland Mobiilivarmenne

In Finland, Mobile ID, a joint effort of three telecom operators (DNA, Elisa, and Telia), is experiencing an increasing market presence compared to the widely favored e-banking solutions used for online verification purposes, including access to e-government services [29].

The Belgian itsme®

A group of Belgian banks and telecom operators have utilized the secure technology of SIM cards to develop a secure mobile identity. Working alongside the Belgian government, they have created a mobile application called "itsme®" that supplements the existing national eID card. This app provides a convenient and mobile-friendly option for online public services [30].

Identity management in cellular networks and GSM: Examining standardized wireless communication technologies, like cellular networks and GSM, can provide insights into identity management and privacy protection. GSM, for instance, offers two key forms of identity management: The International Mobile Subscriber Identity (IMSI) and the International Mobile Equipment Identity (IMEI). The IMSI identifies the subscriber and is stored on the SIM card [31].

Federated identity management tools: Federated identity management models are efficient in handling identity administration. These models operate as overarching systems for identity management, with examples including Windows CardSpace [32] and Open ID [33]. These meta-systems allow for the effective organization and control of user identities.

Mobile Authentication Solutions Utilizing NFC-Enabled National Cards

Android phones provide open access to their NFC interface, allowing the government to utilize mobile technology for e-government services. In contrast, Apple only permitted access to their NFC interface with the launch of iOS 13 in September 2019 [34]. This milestone allowed Apple smartphones, including the latest models, to function as contactless smartcard readers. This granted Apple users access to a broader range of services and applications, enhancing the convenience and versatility of their devices.

4. Proposed Mobile Identity Management Scheme

Our proposed scheme for mobile identity management in information systems is implemented through the following steps:

- **Registration:** To access the mobile signature service, users must register their identities and mobile numbers with a trusted identity provider (IDP) or a mobile network operator (MNO) that supports the service. During the registration process, the user's identity is verified and associated with their respective mobile number. In our scheme, users are provided with digital certificates, which serve as credentials to authenticate themselves when accessing information systems through the mobile identity management system.
- **Mobile Signature Service Setup:** According to ETSI, the Mobile Signature Service (MSS) comprises protocols and technologies to create and validate digital signatures via mobile devices. MSS's role in our mobile identity management scheme is to offer a secure and convenient means for individuals to authenticate their identity and authorize transactions on their mobile devices. By utilizing digital signatures, MSS ensures that the data processed originates from a trusted source. It allows users to generate unique digital signatures tied to their mobile identity for use in Information Systems, ensuring data integrity and non-repudiation. Ultimately, MSS is crucial in mobile identity management, offering a reliable method for digital signatures and confirming user identities in mobile settings. Users need to install a mobile signature application, typically provided by the Identity Provider (IDP) or Mobile Network Operator (MNO) [9] [14] [15] [16] [17].
- **Authentication and Verification:** When a user tries to access an information system or verify themselves, the system sends an authentication challenge to the mobile signature service. The service signs the challenge with the user's key and returns it to the system for verification. Before sending the signed challenge to the system, the mobile signature service validates it through the Signature Validation Service Provider.
- **Authorization:** The information system verifies the provider's credibility before using a mobile signature service. Once the system receives the user's identity and verified digital signature, it grants access permissions or authentication.

Our scheme provides a secure and convenient way to manage user identities in information systems using a mobile signature service. It removes the need for traditional username-password combinations and improves authentication and data security.

4.1 Registration

To access the mobile signature service, users must go through a registration process. During this registration, users are required to provide their identities and mobile numbers. This information should be provided to a trusted identity provider (IDP) or a mobile network operator (MNO) that supports the service. Choosing a reliable and trustworthy IDP or MNO is essential, as they are crucial in facilitating access to the mobile signature service. The registration process for our mobile identity management scheme involves the following steps:

User Enrolment

The user must provide their personal information, including their name, email address, phone number, and occasionally additional verification details, such as date of birth or social security number. This information will be utilized to establish the user's mobile identity.

Identity Verification

Several verification methods, including email, SMS, and document verification, can be employed to ensure the user's identity. These methods play a crucial role in confirming the user's true identity.

Biometric Enrolment

In some cases, during the registration process, biometric data such as fingerprints or facial recognition may be collected. This data is collected to improve the security and authentication processes for our mobile identity management scheme.

Creation of Mobile Identity

Once the user's personal information and verification details are validated, a unique mobile identity is created for the user. This identity is usually stored securely on the user's mobile device and associated with their account.

User Consent

During the registration process, requesting users' consent to specific terms and conditions, privacy policies, and data usage agreements is customary. This ensures that users are fully informed about how their personal information will be utilized and safeguarded by the mobile identity management system.

Credential Provisioning

Users must be provided with credentials, which our scheme refers to as digital certificates. A Certification Authority (CA) issues and manages digital certificates for users.

User On boarding

The final step involves providing users with information and guidance on using and managing their mobile identities. This includes educating users about the system's benefits, explaining its various features and functionalities, and providing instructions on updating or revoking mobile identities as necessary.

4.2 Mobile Signature Service Setup

The following actors are defined in Mobile Signature Service Setups, as illustrated in Figure 1 [9] [14] [36]:

- **User with Mobile Signature App** (i.e. the signer)
- **Personal Mobile Device:** A networked mobile device is assumed to be solely controlled by an individual at the time of signing or validation.
- **Mobile Signature Service Provider (MSSP):** Provider of a mobile signature service (a facility that coordinates and manages the process by which an end-user can sign a document or other information using a signing key on or connected to a personal device)
- **Information System** (Application provider)
- **Validation Authority** (The signature validation service provider)

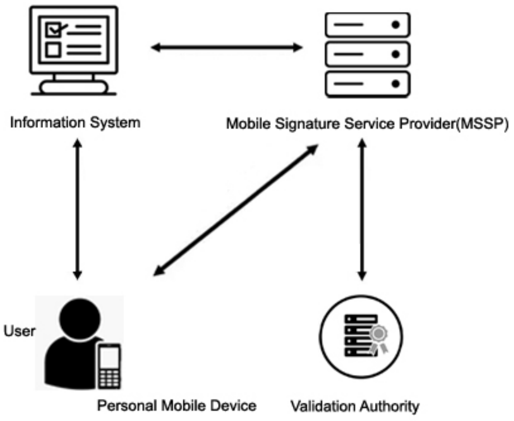

Figure 1. Mobile Signature Service Actors

User with Mobile Signature App

A user initiates the signing process using a mobile signature app to authenticate a challenge or transaction. The app serves as the core of our solution, acting as a Service Provider for qualified digital signatures. Its key features include a data processing library and a user authentication API.

Personal Mobile Devices

Mobile devices have quickly become the preferred method for hosting identity and signing keys. The widespread use of smartphones has solidified their position as the top choice for accessing the digital realm.

Using the secure computing environments within mobile devices: Various computing environments are integrated into mobile devices, enabling secure mobile identification and effectively storing and utilizing signing keys [37]. They encompass the following features:

- **Secure Elements:** A component soldered to the circuit board or within the system-on-chip and isolated from other computing environments [1]. Secure Element (SE) is crucial for establishing reliable identification and authentication. Capable of accommodating third-party applets for various purposes like identification, payment, and public transport, SE allows for independent installation of these applets by Trusted Service Managers (TSM). The management of applets, including loading, installation, and deletion, is facilitated through Trusted Service Management Systems (TSMS). Typically, the security of SE-hosted applets is verified through security certifications, with Common Criteria requiring a composite certification with the SE's Protection Profile. SE can host functionalities directly or provide a separate key storage/management backend. In either scenario, SE must hold a minimum EAL4+ certifications [1].

- **Secure Enclaves:** A secure enclave, which is a type of secure element, is now incorporated within the same chip as the main processor in Apple devices [38];
- **Trusted Execution Environments (TEE):** An isolated software environment is utilized for the secure execution of code [1]. A TEE-enabled mobile device comprises two execution environments, as illustrated in Figure 2: a TEE and a rich execution environment (REE). In both environments, applications can be installed and executed. Applications installed in the TEE, known as trusted applications, run in an isolated environment and can utilize trusted services provided by the TEE OS, such as the trusted user interface. Both environments' operating systems offer SE APIs that facilitate APDU communication with different types of SEs (SIM/UICC, smart micro SD, embedded SE) available on mobile devices.

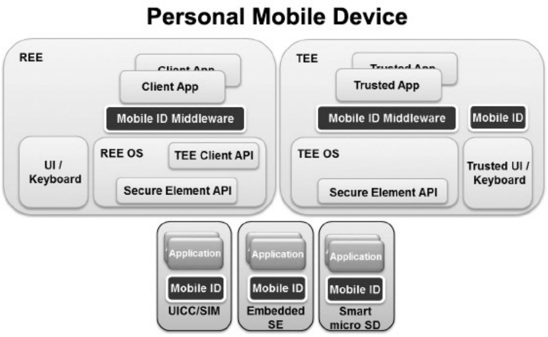

Figure 2. Computing environments incorporated within mobile devices [39]

These computing components are utilized to enable new types of SIM cards that are integrated within the mobile device itself:

- **Embedded SIM (eSIM):** Since 2017, some Android phones have been equipped with a SIM card that contains an embedded secure element within the mobile device [40];
- **Integrated SIM (iSIM):** A SIM card embedded within the secure enclave of a mobile device.

The new types of SIM cards offer a significant advantage by allowing users to download and use multiple profiles from different carriers wirelessly. This feature provides convenience and eliminates the need for physical SIM card swapping [41]. For example, users can have multiple accounts with telecom operators on their phones [42].

This functionality can also be utilized for mobile identification purposes, allowing users to download identity credentials from an identity manager [42]. These credentials, including certificates and cryptographic keys, are intended to be stored securely within a dedicated secure element or a trusted enclave. Subsequently, the applications utilized for authentication and identification would access these credentials from the secure storage and empower them within the trusted execution environment.

Mobile Signature Service Provider

All MSSP functions are implemented using a simple request-response message exchange pattern. The protocols outlined in the specification are generic and offer the flexibility to define an implementation that caters to the specific needs of the MSSP and the application providers.

Information System (Application Provider)

Information systems consist of brain-ware, hardware, software, communication networks, data sources, rules, and procedures for storing, displaying, changing, and deleting information within an organization. These interconnected components work together to collect, process, store, and distribute information to facilitate decision-making, coordination, control, analysis, and visualization within the organization [43]. In our proposed mobile identity management scheme, users initiate the authentication process when they want to access an information system. The information system sends an authentication challenge to the mobile signature service. The mobile signature service then uses the user's signing key to sign the challenge. Subsequently, the verified signature is sent to the information system.

Validation Authority

The validation authority, a signature validation service provider (SVSP), offers a qualified validation service for qualified electronic signatures [36].

4.3 Authentication and Verification

Authentication with a mobile signature service typically involves using the user's private key and the authentication request. Here are the steps involved in this process:

The user initiates an authentication request

The user initiates an authentication request by providing necessary information, such as the user's username or identification number, along with their credential, referred to as a digital certificate by our scheme, to the information system.

Information System generates a challenge

The Information System generates a challenge for the authentication process. This challenge is typically a random string of characters that will be used to authenticate the user. The information system sends this challenge to the mobile signature service.

Challenge is sent to the user's mobile device

The challenge is securely delivered to the user's mobile device through a channel, either a mobile app or SMS.

User signs the challenge with their private key

In order to verify their identity, users utilize their private key to sign the challenge received on their mobile device. This private key is securely stored on the mobile device.

The signature, produced using cryptographic algorithms, is unique to the user and specific to the content being signed.

The signed challenge is sent back to the mobile signature service

After signing, the challenge is securely sent back to the mobile signature service via a secure channel. This signed challenge provides irrefutable evidence that the user possesses the corresponding private key.

Verification

The specific verification process depends on the mobile signature service and the underlying technology but generally involves the following steps:

- **The MSS submits a signature validation request:** The MSS receives the signature and verifies its validity using the Validation Authority (the signature validation service provider). The mobile signature service requests a signature validation to the signature validation service server [36].
- **The signature validation service server performs the validation process:** The signature validation service provider (SVSP) conducts validation procedures based on constraints presented by either the mobile signature service or the service itself. In other words, this means that the SVSP verifies certain conditions or requirements set by either the mobile signature service provider or the service. These constraints can be related to various aspects, such as the signature format, the identification of the signer's certificate, the validation context initialization, the X.509 validation, the crypto validation, and the signature acceptance. The SVSP ensures that these constraints are met by conducting thorough validation checks [36].
- **The signature verification service server prepares and sends the validation response:** The response contains the validation report(s) and the service policy's OID (Object Identifier). It may also include the OID of the utilized signature validation policy [36].
- **Validation report presentation:** Based on the validation report, the mobile signature service decides whether it accepts the signature. If the signature successfully passes all the verification constraints, it is considered valid. On the other hand, if any of the verification steps fail, it indicates that the signature is either invalid or compromised [36].

It is important to note that this is a general overview, and the exact implementation details may vary depending on the specific mobile signature service, security protocols, and cryptographic algorithms used.

Signature Packaging

The mobile signature service combines the digital signature with other essential information, including the signed content, certificate details, and metadata. Typically, this package is formatted in XML or JSON.

Signature Transmission to Information System

The digital signature package is securely transmitted to the information system. This transmission can occur through various channels, such as the Internet, mobile networks, or dedicated secure connections.

Authentication status is confirmed

The information system verifies the user's authentication status based on the result of the signature process. If the signature is valid, the user is successfully authenticated.

This process ensures secure and reliable authentication by utilizing the user's private key and the challenge generated by the information system. It guarantees that only users possessing the corresponding private key can successfully authenticate themselves.

4.4 Authorization

Once the user's digital signature and identity have been verified, the information system can grant the necessary access permissions or authentication in various ways:

Role-based access control (RBAC)

The system can assign specific roles or groups to users depending on their job responsibilities or organizational hierarchy. Each role/group is associated with predetermined access permissions. Once the user's identity is verified, the system grants them the permissions linked to their assigned role.

Attribute-based access control (ABAC)

In ABAC, access permissions are granted based on several user attributes, including their job title, department, or location. The system evaluates these attributes against predefined policies to determine the user's access permissions.

Rule-based access control

The system operates based on predefined rules or conditions assessed after verifying the user's identity. The system will grant the required access permissions if the user meets the outlined criteria.

Multifactor Authentication (MFA)

In addition to verifying the user's digital signature and identity, MFA requires additional authentication factors like a one-time password (OTP), biometrics, or hardware tokens. The system grants access permissions once the user completes the other authentication steps.

Access control lists (ACLs)

The system lists particular resources and users who are granted or denied access. Once the user's digital signature and identity are verified, the system checks the ACLs to determine the necessary permissions. It gives access accordingly.

Single Sign-On (SSO)

Single sign-on (SSO) is a feature that enables users to authenticate themselves once, eliminating the need to re-authenticate when accessing multiple systems or applications. Once the user's identity is verified during the initial authentication process, the system provides access to various resources or applications without further verification. The specific method or combination of techniques employed depends on the design and implementation of the information system and the organization's security policies.

5. Implementation

The mobile signature service is commonly offered through a commercial agreement between a mobile signature service provider (MSSP) and individual or organizational information systems that use mobile signatures [14].

The deployment and application steps are crucial in helping information systems identify the requirements for their mobile signature services. Once these steps have been completed, information systems can begin creating the architecture essential for running their mobile signature services, taking into account credentials and authentications. They can also prepare to examine the services' security considerations and implementation scenarios.

Our scheme applies in cases where the mobile electronic signature is created by utilizing a signing key stored on the user's mobile device, such as within a secure element (SE). Personal mobile devices can include cryptographic capabilities specifically for computing the digital signature value.

Additionally, they can also construct the entire AdES structure. The term AdES pertains to the serialization of structures that comply with CADES [18], XAdES [19], or PAdES [20]. The various capabilities mentioned above are demonstrated through the following approaches:

5.1 MoIdM1. Digital signature value generation in personal mobile devices with information system / MSSP Interaction:

In this particular approach, referred to as the MoIdM1 approach, the authentication challenge exists in an information system, such as a dialogue generated with the user, which can interact with the MSSP (Mobile Signature Service Provider). The MSSP performs the digest computation, while the personal device handles the computation of the digital signature value. Additionally, the MSSP undertakes the construction of the AdES.

In this approach, it is the information system that initiates the activity of the MSSP, as illustrated in Figure 3:

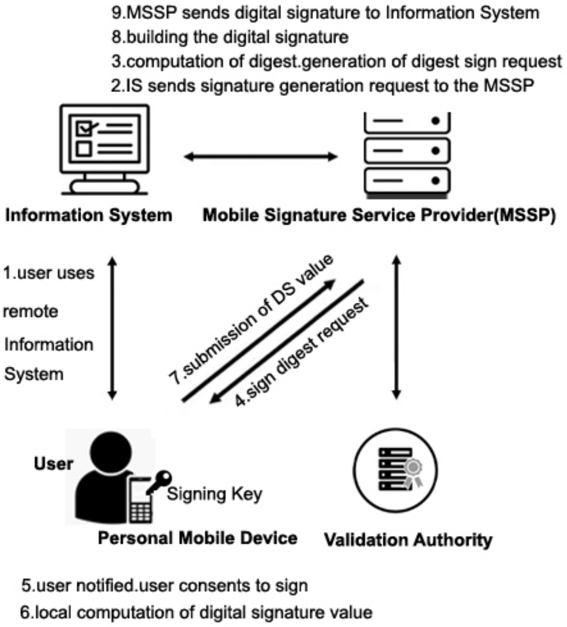
9.MSSP sends digital signature to Information System
8.building the digital signature
3.computation of digest.generation of digest sign request
2.IS sends signature generation request to the MSSP
Information System
Mobile Signature Service Provider(MSSP)
1.user uses remote Information System
7.submission of DS value
4.sign digest request
User
Signing Key
Personal Mobile Device
Validation Authority
5.user notified.user consents to sign
6.local computation of digital signature value

Figure 3. MoIdM1 Approach

5.2 MoIdM2. AdES is completely generated on a personal mobile device:

This approach referred to as the MoIdM2 approach, is an extension of the MoIdM1 approach. It presents a high-level approach to a case in which the personal device computes the digital signature value and generates the complete AdES, as illustrated in Figure 4:

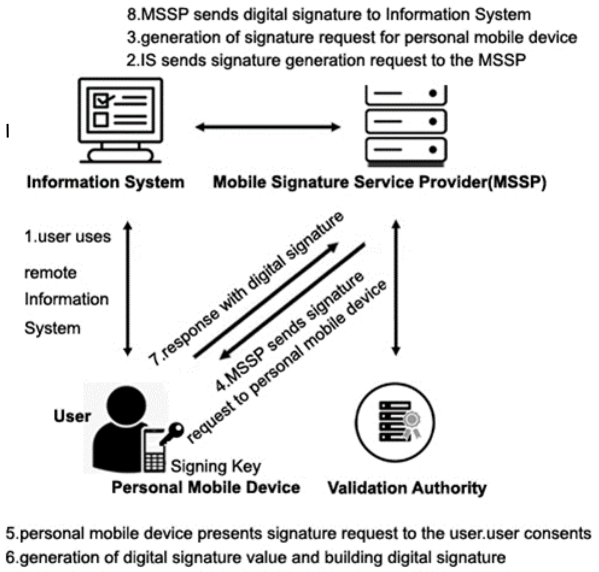
8.MSSP sends digital signature to Information System
3.generation of signature request for personal mobile device
2.IS sends signature generation request to the MSSP
Information System
Mobile Signature Service Provider(MSSP)
1.user uses remote Information System
7.response with digital signature
4.MSSP sends signature request to personal mobile device
User
Signing Key
Personal Mobile Device
Validation Authority
5.personal mobile device presents signature request to the user.user consents
6.generation of digital signature value and building digital signature

Figure 4. MoIdM2 Approach

6. Evaluation, Acceptance, and Usage Analysis

Our scheme offers multiple advantages:

1. It eliminates the need for traditional authentication methods, such as usernames and passwords, which can be easily compromised.
2. It utilizes mobile device security features, including tamper-resistant hardware and biometric authentication, to enhance the overall security of the authentication process.
3. It provides a convenient and user-friendly authentication method by allowing users to authenticate themselves using their mobile devices, which are typically carried with them at all times.

In the previous sections of this paper, we discussed two different approaches to implementing our mobile identity management scheme. These approaches use a mobile signature service for information systems.

- **MoIdM1. Digital signature value generation in personal mobile devices with information system / MSSP Interaction.**
- **MoIdM2. AdES is completely generated on a personal mobile device.**

This section will assess them based on various indicators, as outlined in Table 2:

Table 2. The evaluation results of two approaches for implementing our mobile identity management scheme

No	Indicators	The evaluation results	
		MoIdM1	MoIdM2
1	User sole control over the signature Creation.	√	√
2	The Authentication Challenge exists in information systems.	√	√
3	Steps relating to the completion of the AdES signature structure carried out on personal mobile devices.	×	√
4	Bind to a particular Personal Mobile Device.	√	√
5	The users prove their authentication by demonstrating their ability to utilize the private key stored in their mobile devices for signing an authentication challenge.	√	√

6.1 Acceptance and usage analysis:

The Technology Acceptance Model (TAM) is a popular framework for comprehending technology adoption and usage, such as mobile identity applications [44], [45]. TAM asserts that a technology's perceived usefulness and ease of use are crucial factors influencing its acceptance and usage. Utilizing TAM can aid in grasping the adoption and usage of our mobile identity management scheme and pinpointing the factors affecting user behavior [44]. By considering these factors, we can devise strategies to enhance the adoption and usage of our mobile identity scheme and the user experience. The proposed model is shown in Figure 5.

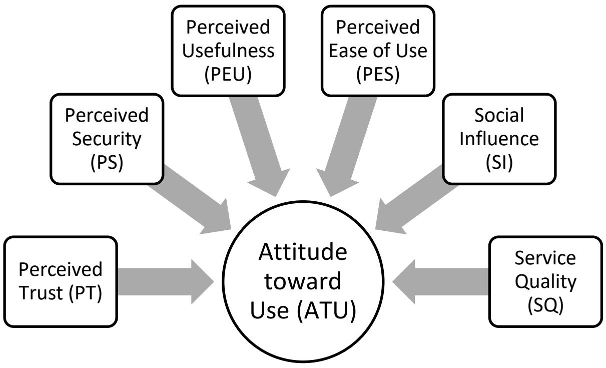

Figure 5. The proposed model for explaining the acceptance of our mobile identity management scheme

Perceived Trust (PT)

User trust is essential for the success of new technology, particularly in mobile identity management. Trust plays a crucial role in user usage and adoption of Mobile Signature Service Providers (MSSP) services through mobile signature applications. The absence of transactional risks and the delivery of benefits are key factors in establishing trust. Moreover, trust significantly impacts user loyalty, with untrusted mobile identity applications resulting in lower loyalty levels [46], [47]. In our study, we have incorporated a trust factor into the TAM model to assess the impact of perceived trust on user attitude towards mobile identity management schemes.

H1. Perceived trust has a positive effect on attitude toward the use of our mobile identity management scheme.

Perceived Security (PS)

Perceived security (PS) refers to how secure a user perceives a mobile identity application to be against risks. Ensuring the security of user services, transactions, privacy, and data through security measures is crucial for the success of mobile identity services [48]. This study assumes that enhancing security levels can boost user trust and increase positive attitudes toward mobile identity management schemes.

H2. Perceived security has a positive effect on attitude toward the use of our mobile identity management scheme.

Perceived Usefulness (PEU)

In this study, perceived usefulness refers to how much using a mobile identity app will benefit users in authentication transactions [49]. In our research, perceived usefulness is crucial in motivating information systems users to adopt and use our mobile identity management scheme, especially if they anticipate receiving benefits from the new technology.

H3. Perceived usefulness positively affects attitudes toward using our mobile identity management scheme.

Perceived Ease of Use (PES)

Perceived ease of use is the second predictor in the TAM model. In this study, it refers to the level of ease associated with using our mobile identity application. Users who perceive our app as user-friendly are likelier to adopt it. Moreover, if they find inter-actions with the app simple and straightforward, their intention to use it improves [50]. Perceived ease of use is vital in encouraging users to adopt and utilize our mobile identity management scheme in our research.

H4. Perceived ease of use has a positive effect on attitude toward the use of our mobile identity management scheme.

Social Influence (SI)

In this study, social influence refers to how family and friends can impact the intention to adopt new technology, like our mobile identity management scheme [51].

H5. Social influence has a positive effect on attitudes toward the use of our mobile identity management scheme.

Service Quality (SQ)

Ensuring the high quality of our mobile identity application is crucial for its success [52]. Our research emphasizes the significance of service quality in promoting the adoption of mobile identity management schemes among users who seek top-notch services.

H6. Service quality has a positive effect on attitude toward the use of our mobile identity management scheme.

Attitude toward Use (ATU)

This attitude is a critical predictor in TAM and other technology acceptance models such as UTAUT and TRA [53]. In our research, the user's attitude toward usage will be a key factor in predicting the adoption of our mobile identity management scheme.

H7. Attitude toward use positively affects the use of our mobile identity management scheme.

Data Collection and Participants

This study empirically examines social media users engaging with our mobile identity management scheme. Data was collected from four social media users through online questionnaires distributed during online chats.

Reliability Analysis

The quantitative research in our study was carefully planned and executed to produce valid and reliable results. We prepared model measurements, established a data collection method, and analyzed data characteristics. Pilot testing was conducted on all items, as outlined in Table 3, demonstrating high internal consistency and reliability. We selected measurement items based on prior research with similar frameworks to ensure relevance and suitability for our study's context [44]. This approach validated and maintained the reliability of our results. Cronbach's alpha was used to analyze reliability, with all constructs showing values above 0.70 in Table 3, meeting accepted standards for further analysis [54].

Table 3. Cronbach's Alpha values

No	Factors	Cronbach's Alpha values	
		Cronbach's Alpha value (Pilot Test)	Cronbach's Alpha value (Final Test)
1	PT	0.770	0.815
2	PS	0.703	0.851
3	SQ	0.701	0.870
4	SI	0.780	0.860
5	PES	0.710	0.859
6	PEU	0.777	0.885
7	ATU	0.790	0.922

Structural Model Analysis

The proposed model was tested using structural equation modeling (SEM) to analyze its hypotheses. The findings from the SEM test, displayed in Table 4, confirmed the acceptance of all seven hypotheses in the research model.

Table 4. Results of Structural Equation Modelling Analysis

No	Hypotheses Links	Results of Structural Equation Modeling Analysis		
		t-Values	p-Values	results
1	PT → ATU	4.533	P<0.001	Supported
2	PS → ATU	4.237	P<0.001	Supported
3	PEU → ATU	3.351	P<0.001	Supported
4	PES → ATU	3.214	P<0.001	Supported
5	SI → ATU	5.103	P<0.001	Supported
6	SQ → ATU	3.171	P<0.001	Supported
7	ATU → INU	3.221	P<0.001	Supported

Conclusions

Overall, a mobile identity management scheme based on a mobile signature service for information systems offers users a secure and convenient authentication method to access various information systems. Our main objective was to develop a scheme for mobile identity management in information systems while exploring the integration of digital certificates on mobile devices for business purposes. In this regard, we have successfully integrated a digital certificate on a mobile device and used it with the mobile signature service to authenticate users and establish secure connections with information systems. This scheme was developed in a closed and controlled environment but can be extended to more realistic situations.

Mobile identity management plays an increasingly vital role in various information systems such as government-to-citizen and government-to-government inter-actions, transaction processing systems (TPS), management information systems (MIS), decision support systems (DSS), executive support systems (ESS), enterprise resource planning (ERP) systems, customer relationship management (CRM) systems, knowledge management systems (KMS), supply chain management (SCM) systems, geographic information systems (GIS), expert systems, content management systems (CMS), business intelligence systems (BI), and many more. The deployment of mobile identity management encompasses a wide range of use cases.

While there are currently many applications, use cases, and deployments of mobile identity management, it is essential to note that the size and scope of these deployments are rapidly expanding. Ongoing large-scale deployments, innovation, and promises of security necessitate the support of standards-based technologies. One such technology, the mobile signature service, will continue to play a crucial role in the growth of the mobile identity management market. This paper highlights the existence of adequate technological resources for addressing mobile identity and digital signatures through the mobile signature service. The need for investment and effort to potentially trigger another significant boom in mobile communications remains.

Acknowledgments

We want to acknowledge that this paper is an extended version of the ' A Mobile Identity Management Scheme Based on Mobile Signature Service for Information Systems ' paper presented at the EAI MobiCASE 2024 Conference. We are grateful for the opportunity to expand upon our initial work and further explore the topic's intricacies. We sincerely thank the conference organizers and reviewers for their valuable feedback and support.

References

[1] Funke H. Digital and mobile identities. In: Open Identity Summit 2020 [Internet]. Copenhagen, Denmark; 2020. p. 27–33. Available from: https://doi.org/10.18420/ois2020_02

[2] Khan AR. National Identity Card: Opportunities and Threats. Journal of Asian Research. Journal of Asian Research. 2018 Mar 7;2(2):77. https://doi.org/10.22158/jar.v2n2p77

[3] Reddy AG, Suresh D, Phaneendra K, Shin JS, Odelu V. Provably secure pseudo-identity based device authentication for smart cities environment. Sustainable Cities and Society. 2018 Aug; 41:878–85. https://doi.org/10.1016/j.scs.2018.06.004

[4] Habib S, Hamadneh NN. Impact of Perceived Risk on Consumers Technology Acceptance in Online Grocery Adoption amid COVID-19 Pandemic. Sustainability. 2021 Sep 13;13(18):10221. https://doi.org/10.3390/su131810221

[5] Pöhn D, Grabatin M, Hommel W. eID and Self-Sovereign Identity Usage: An Overview. Electronics [Internet]. 2021 Jan 1;10(22):2811. Available from: https://www.mdpi.com/2079-9292/10/22/2811/html. https://doi.org/10.3390/electronics10222811

[6] SLA Digital Ltd. What is Mobile Identity? - SLA Digital [Internet]. SLA Digital. 2021. Available from: https://sla-digital.com/blog/what-is-mobile-identity/.

[7] Fatoni A, Adi K, Widodo AP. PIECES Framework and Importance Performance Analysis Method to Evaluate the Implementation of Information Systems. Warsito B, Sudarno, Triadi Putranto T, editors. E3S Web of Conferences. 2020; 202:15007. https://doi.org/10.1051/e3sconf/202020215007

[8] Dai HN, Maharjan S, Zheng Z, Hung PCK, Xu Q, Sun W. IEEE Access Special Section Editorial: Blockchain-Enabled Trustworthy Systems. IEEE Access. 2021; 9:67680–3. https://doi.org/10.1109/ACCESS.2021.3075115

[9] ETSI SR 019 020 V1.1.2: The framework for standardization of signatures; Mobile Signature Service; Standards for AdES digital signatures in mobile and distributed environments. ETSI; 2016. Available from: https://www.etsi.org/deliver/etsi_sr/019000_019099/019020/01.01.02_60/sr_019020v010102p.pdf

[10] The Mobile Economy 2023. GSMA and GSMA Intelligence; 2023 p. 1–50.

[11] Digital Identity: Solutions Assessment, Regional Analysis & Market Forecasts 2023-2027. Juniper Research Ltd; 2023 Feb.

[12] M. Singh, H. Kaur, A. Kakkar. Digital signature verification scheme for image authentication. In: 2015 2nd International Conference on Recent Advances in Engineering & Computational Sciences (RAECS), IEEE; 2015, p. 1–5. https://doi.org/10.1109/RAECS.2015.7453277

[13] FiCom's (The Finnish Federation for Telecommunications and Tele informatics) application guideline for ETSI's MSS standards: V2.1. FiCom; 2012.

[14] ETSI TR 102 203 V1.1.1: Mobile Commerce (M-COMM); Mobile Signatures; Business and Functional Requirements. ETSI; 2003.

[15] ETSI TS 102 204 V1.1.4: Mobile Commerce (M-COMM); Mobile Signature Service; Web Service Interface. ETSI; 2003.

[16] ETSI TR 102 206 V1.1.3: Mobile Commerce (M-COMM); Mobile Signature Service; Security Framework. ETSI; 2003.

[17] ETSI TS 102 207 V1.1.3: Mobile Commerce (M-COMM); Mobile Signature Service; Specifications for Roaming in Mobile Signature Services. ETSI; 2003.

[18] ETSI EN 319 122 (all parts): Electronic Signatures and Infrastructures (ESI); CAdES digital signatures. ETSI.

[19] ETSI EN 319 132 (all parts): Electronic Signatures and Infrastructures (ESI); XAdES digital signatures. ETSI.

[20] ETSI EN 319 142 (all parts): Electronic Signatures and Infrastructures (ESI); PAdES digital signatures. ETSI.

[21] Do T van, Feng B, Swafford C, Do VT, Khuong LH. Mobile Identity as a Tool to Develop Society. 2015 5th International Conference on IT Convergence and Security (ICITCS). 2015 Aug. https://doi.org/10.1109/ICITCS.2015.7292997

[22] Fritsch L. Identification collapse - contingency in Identity Management. In: Open Identity Summit 2020 [Internet]. Copenhagen, Denmark; 2020. p. 15–26. Available from: https://doi.org/10.18420/ois2020_01

[23] Alamillo I, Mouille S, Röck A, Soumelidis N, Tabor M. Digital Identity Standards [Internet]. ENISA; 2023 [cited 2024 Nov 30]. Available from: https://www.doi.org/10.2824/28598

[24] Kubach M, Leitold H, Heiko Roßnagel, Schunck CH, Talamo M. SSEDIC.2020 on mobile eid. Open Identity Summit. 2015 Jan 1;29–41. Available from: https://subs.emis.de/LNI/Proceedings/Proceedings251/29.pdf

[25] Alpern NJ, Shimonski RJ. Wireless Networking. Elsevier eBooks [Internet]. 2010 Jan 1;55–72. Available from: https://www.sciencedirect.com/topics/computer-science/authentication-capability.

[26] Ping Identity [Internet]. Pingidentity.com. 2024. Available from: https://www.pingidentity.com/en/resources/identity-fundamentals/centralized-identity-management/authentication-authorization-standards.html.

[27] ID Austria [Internet]. oesterreich.gv.at - Österreichs digitales Amt. 2023 [cited 2024 Nov 30]. Available from: https://www.oesterreich.gv.at/en/id-austria.html.

[28] Mobile-ID - ID.ee [Internet]. ID.ee. 2024 [cited 2024 Nov 30]. Available from: https://www.id.ee/en/mobile-id/.

[29] Etusivu - Mobiilivarmenne [Internet]. Mobiilivarmenne. 2024 [cited 2024 Nov 30]. Available from: https://mobiilivarmenne.fi/.

[30] itsme®, your digital ID [Internet]. itsme®. 2024 [cited 2024 Nov 30]. Available from: https://www.itsme-id.com/en-BE/.

[31] Mobile Identity Enabling the Digital World 2020 [Internet]. GSMA; [cited 2024 Nov 30]. Available from: https://www.gsma.com/solutions-and-impact/technologies/mobile-identity/wp-content/uploads/2020/07/Mobile-Identity-enabling-the-digital-world-report-Final-1.pdf.

[32] Introducing Windows CardSpace [Internet]. Microsoft.com. 2010 [cited 2024 Nov 30]. Available from: http://msdn.microsoft.com/en-us/library/aa480189.aspx.

[33] OpenID - OpenID Foundation [Internet]. OpenID Foundation - Helping people assert their identity wherever they choose. [cited 2024 Nov 30]. Available from: http://openid.net.

[34] Core NFC | Apple Developer Documentation [Internet]. Apple Developer Documentation. [cited 2024 Nov 30]. Available from: https://developer.apple.com/documentation/corenfc#overview.

[35] Machine Readable Travel Document High-Level Guidance: Explaining the ICAO Digital Travel Credentials [Internet]. 2024 [cited 2024 Nov 30]. Available from: https://www.icao.int/Security/FAL/TRIP/Documents/

High%20Level%20Guidance%20explaining%20ICAO%20DTC.pdf

[36] ETSI TS 119 441 V1.1.1: Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services [Internet]. ETSI; 2018 [cited 2024 Nov 30]. Available from: https://www.etsi.org/deliver/etsi_ts/119400_119499/119441/01.01.01_60/ts_119441v010101p.pdf

[37] eIDAS compliant eID Solutions | ENISA [Internet]. Europa.eu. ENISA Report; 2020 [cited 2024 Nov 30]. Available from: https://www.enisa.europa.eu/publications/eidas-compliant-eid-solutions.

[38] Secure Enclave [Internet]. Apple Support. Apple Platform Security; 2024 [cited 2024 Nov 30]. Available from: https://support.apple.com/guide/security/secure-enclave-sec59b0b31ff/web.

[39] Mobile ID: Realization of Mobile Identity Solutions by GlobalPlatform Technologies. GlobalPlatform [Internet]. 2015 Nov [cited 2024 Nov 30]; p. 1–52. Available from: https://globalplatform.wpengine.com/wp-content/uploads/2018/04/GlobalPlatform_White_Paper_MobileID.pdf

[40] Statt N. Google's Pixel 2 phones are the first to use built-in eSIM technology [Internet]. The Verge. 2017 [cited 2024 Nov 30]. Available from: https://www.theverge.com/2017/10/4/16424740/google-pixel-2-xl-esim-technology-project-fi-first-ever.

[41] Differences between SIM types - which SIM to choose? — 1oT [Internet]. 1oT. 2019 [cited 2024 Nov 30]. Available from: https://1ot.mobi/resources/blog/differences-between-sim-types-which-sim-to-choose.

[42] Mondato. eSIM: Fresh Paint for Mobile, Payments and Identity [Internet]. Mondato Insight. 2019 [cited 2024 Nov 30]. Available from: https://blog.mondato.com/esim-fresh-paint/.

[43] Fatoni A, Adi K, Widodo AP. PIECES Framework and Importance Performance Analysis Method to Evaluate the Implementation of Information Systems. Warsito B, Sudarno, Triadi Putranto T, editors. E3S Web of Conferences. 2020; 202:15007.

[44] Carlbäck J, Wong A. A Study on Factors Influencing Acceptance of Using Mobile Electronic Identification Applications in Sweden [Internet]. [JÖNKÖPING UNIVERSITY]; 2018 [cited 2024 Nov 30]. Available from: http://hj.diva-portal.org/smash/get/diva2:1214313/FULLTEXT01.pdf

[45] A. Berisca, S. Clive, J.A. Hardani, A.S. Hutabarat. Development of the TAM model of factors that influence the acceptance of mobile payments. JIMEA J.; 2024; Vol. 8; No. 2; pp. 42-66. https://doi.org/10.31955/mea.v8i2.3967

[46] Almaiah MA, Ayouni S, Hajjej F, Lutfi A, Almomani O, Awad AB. Smart Mobile Learning Success Model for Higher Educational Institutions in the Context of the COVID-19 Pandemic. Electronics. 2022 Apr 18;11(8):1278. https://doi.org/10.3390/electronics11081278

[47] Almaiah MA, Hajjej F, Lutfi A, Al-Khasawneh A, Shehab R, Al-Otaibi S, et al. Explaining the Factors Affecting Students' Attitudes to Using Online Learning (Madrasati Platform) during COVID-19. Electronics. 2022 Mar 22;11(7):973. https://doi.org/10.3390/electronics11070973

[48] Mohd Thas Thaker H, Mohd Thas Thaker MA, Khaliq A, Allah Pitchay A, Iqbal Hussain H. Behavioural intention and adoption of internet banking among clients of Islamic banks in Malaysia: an analysis using UTAUT2. Journal of Islamic Marketing. 2021 Feb 1; ahead-of-print(ahead-of-print). https://doi.org/10.1108/jima-11-2019-0228

[49] Patil P, Tamilmani K, Rana NP, Raghavan V. Understanding consumer adoption of mobile payment in India: Extending Meta-UTAUT model with personal innovativeness, anxiety, trust, and grievance redressal. International Journal of Information Management. 2020 Oct; 54:102144. https://doi.org/10.1016/j.ijinfomgt.2020.102144

[50] Ramos-de-Luna I, Montoro-Ríos F, Liébana-Cabanillas F. Determinants of the intention to use NFC technology as a payment system: an acceptance model approach. Information Systems and e-Business Management. 2015 May 29;14(2):293–314. https://doi.org/10.1007/s10257-015-0284-5

[51] Rodrick SS, Islam H, Sarker SA, Tisha FF. Prospects and Challenges of using Credit Card Services: A Study on the users in Dhaka City. AIUB Journal of Business and Economics. 2021 Dec;18(1):161–86.

[52] Lutfi A, Al-Khasawneh AL, Almaiah MA, Alshira'h AF, Alshirah MH, Alsyouf A, et al. Antecedents of Big Data Analytic Adoption and Impacts on Performance: Contingent Effect. Sustainability. 2022 Nov 22;14(23):15516. https://doi.org/10.3390/su142315516

[53] Trinh HN, Tran HH, Vuong DHQ. Determinants of consumers' intention to use credit card: a perspective of multifaceted perceived risk. Asian Journal of Economics and Banking. 2020 Aug 20;4(3):105–20. https://doi.org/10.1108/ajeb-06-2020-0018.

[54] Alhumaid K, Habes M, Salloum SA. Examining the Factors Influencing the Mobile Learning Usage During COVID-19 Pandemic: An Integrated SEM-ANN Method. IEEE Access. 2021; 9:102567–78. https://doi.org/10.1109/access.2021.3097753