electronics

MDPI

Article

Personal Identity Proofing for E-Commerce: A Case Study of Online Service Users in the Republic of Korea

Jongbae Kim

Department of IT Engineering, Sejong Cyber University, Seoul 05000, Republic of Korea; jb.kim@sjcu.ac.kr

Abstract: The rapid expansion of non-face-to-face e-commerce services in the Korea has significantly increased the importance of personal identity proofing (PIP) for verifying users in online transactions, such as payments, refunds, membership registrations, and access to age-restricted products. Currently, personal identity proofing agencies (PIPAs) indiscriminately provide all of a user's personal information to internet service providers (ISPs), leading to substantial privacy concerns and preventing users from selectively disclosing only the necessary information. The objective of this paper is to enhance the safety, convenience, and security of PIP services by proposing a method that empowers users to control the personal information they disclose while enabling digital identity integration for both online and offline applications. To achieve this, an extensive overview and analysis of the current PIP systems in Korea is presented, including methods. The strengths and weaknesses of these systems are critically examined, revealing limitations in privacy protection, user convenience, and security. Based on this analysis, a new method is proposed that introduces differentiated levels of PIP means according to authentication strength, allowing for the minimal necessary disclosure of personal information. The proposed method aims to improve the stability and reliability of the PIP service environment by addressing current privacy concerns and enhancing user control over personal information. This approach can be applied to e-commerce services in Korea and other countries facing similar challenges, contributing to the development of safer and more reliable online services.

Keywords: personal identity proofing services; digital identity; e-commerce; identity verification; internet service providers

Citation: Kim, J. Personal Identity Proofing for E-Commerce: A Case Study of Online Service Users in the Republic of Korea. *Electronics* **2024**, *13*, 3954. https://doi.org/10.3390/electronics13193954

Academic Editor: Aryya Gangopadhyay

Received: 14 September 2024
Revised: 5 October 2024
Accepted: 6 October 2024
Published: 7 October 2024

1. Introduction

The rapid advancement of information technology has significantly transformed the landscape of commerce, leading to a proliferation of non-face-to-face e-commerce services worldwide. Personal identity proofing (PIP) has become essential for verifying users' identities in online transactions such as payments, refunds, membership registrations, and access to age-restricted products. Traditionally, personal identifiable information (PII) provided by credible third parties such as social security numbers, driver's licenses, and passports has been used to identify individuals [1–3]. However, the online environment presents unique challenges in protecting user privacy while ensuring secure authentication. Despite the development of various PIP methods, including knowledge-based authentication, biometric verification, and digital certificates, existing systems often face issues related to privacy concerns, user convenience, and security vulnerabilities. The indiscriminate collection and use of sensitive personal information have led to social problems such as identity theft and infringement on individual privacy. In some cases, the misuse of unchangeable personal identifiers exacerbates these issues. There is a pressing need for improved PIP methods that balance security, privacy, and user convenience, while empowering users with control over their personal information. For personal identification purposes, all citizens in Korea are assigned a 13-digit resident registration number (RRN) at birth [4,5]. The structure of the RRN, as utilized in Korea's National ID system, is shown in Figure 1. The first six digits

indicate the date of birth, the first digit after "-" represents the gender, the next five digits represent the birth area code, and the final digit is a check digit used for error detection. In Korea, individuals can obtain a physical National ID card starting at the age of 17 [6,7].

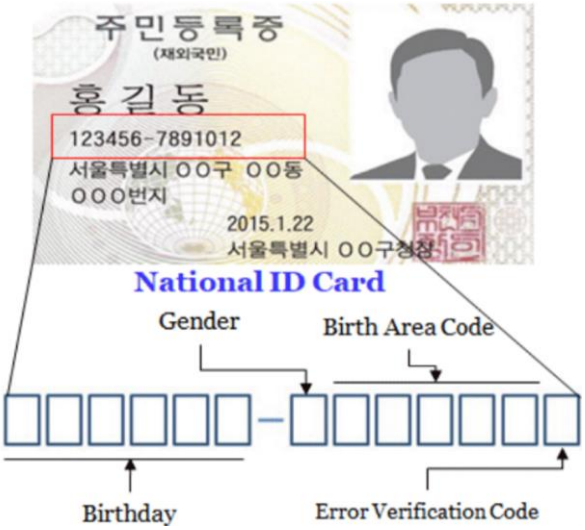

Figure 1. Resident registration number composition system included in Nation ID in Korea.

In Korea, the RRN is used as PII; each individual is assigned an RRN at birth, and this number is included in the National ID card. Identification can be directly verified in face-to-face settings by comparing the photo on the National ID with the individual's appearance. The RRN is uniquely assigned to an individual and is used as a personal identifier in most organizations. In some cases, it is also used for personal authentication. Additionally, once issued, the RRN is unchangeable, making it a comprehensive, unique, and permanent personal identifier. However, the indiscriminate use of these characteristics has led to social problems such as infringement on individual privacy. Since 2012, legislation has been enacted to prohibit the collection and processing of RRNs, except in cases permitted by law [8]. RRNs have traditionally been used to uniquely identify individuals in e-commerce and other contexts. However, due to changes in data collection practices, this method is no longer feasible. Therefore, new authentication methods are needed to verify individuals' identities online [9,10].

Authentication is the process of verifying an individual's identity to confirm their legitimacy as a user. This is achieved through an authentication element, which is unique information used to identify the individual [11]. Authentication is necessary in non-face-to-face online transactions to confirm the user's identity. In both face-to-face and non-face-to-face e-commerce environments, verifying the identity of the transaction party is essential. When purchasing age-restricted items such as alcohol, firearms, or medicine, it is crucial to verify the buyer's identity. In face-to-face transactions, the buyer's identification card should be examined. However, in non-face-to-face environments, electronic authentication methods must be used to identify and authenticate users since physical identification documents cannot be presented [12].

Table 1 shows the differences between identifying and authenticating users in e-commerce. The identification and authentication processes detailed in Table 1 verifies the identity of the transaction parties in both face-to-face and non-face-to-face transactions.

Table 1. Differences between identification and authentication.

	Definition	Tools
Identification	• Procedures for verifying user information • Activities of subjects who supply information to verify themselves in authentication services	Username, ID, account number, PIN, etc.
Authentication	• Proof activities to verify the identity of the data subject • Procedures for the system to confirm that it is the user who claims to be the person and then acknowledge that it is the user	PW, token, smart card, biometric authentication (including fingerprint, vein), etc.

The PIP process involves verifying and certifying that the user has agreed to legal and reasonable procedures [9,10]. Identity authentication, on the other hand, confirms that the user is indeed the actual user through electronic information provided by the online service [13–15]. PIP requires providing publicly available information to a subject who will identify a specific user among multiple users. To ensure the legitimacy of the proprietary information presented by the user, a verification process is performed. Authentication, which involves combining the verification process with the user's personal information, is then necessary to confirm that the individual presenting the information is a legitimate user.

Therefore, PIP involves identifying, verifying, and authenticating information owned by oneself. The importance of PIP lies in its ability to provide legitimate user verification and identification. Creating a PIP for each user is similar to the process of online operators creating non-overlapping user accounts.

According to research by Zviran and Erlich [16], identification refers to both the username and the user's identity, i.e., "who are you?". However, this identification information alone cannot definitively establish the user's identity. The presented information is selectively generated and requires the owner to prove their identity through a process of confirmation or verification by a third party [17,18]. Authentication mechanisms employ various methods, such as user-selected passwords, system-generated passwords, passphrases, question-and-answer passwords, tokens, and various biometric characteristics. This process prevents unauthorized users from accessing restricted systems.

The purpose of this paper is to enhance the safety, convenience, and security of PIP services by proposing a method that empowers users to control the personal information they disclose, enabling digital identity integration for both online and offline applications. To achieve this, an exhaustive overview and analysis of current PIP systems are conducted, with a particular focus on the Republic of Korea as a case study, given its advanced e-commerce environment and existing challenges in PIP practices. The methodology involves critically examining existing PIP methods including i-PIN, accredited certificates, mobile phone authentication, and credit card-based verification. By identifying the strengths and weaknesses of these methods in terms of privacy protection, user convenience, and security, the aim to uncover the limitations that necessitate a new approach.

Building upon previous research that has highlighted limitations in current PIP methods, such as privacy concerns arising from indiscriminate sharing of personal information and a lack of user control, this paper introduces a novel approach that differentiates levels of PIP means according to authentication strength. In contrast to previous studies, which have concentrated on technical enhancements to authentication mechanisms, this research places the onus on user empowerment, enabling the disclosure of only the minimum necessary personal information in accordance with the security level of the authentication method employed. This approach addresses current privacy concerns and enhances user control over personal data, thereby contributing to the development of safer and more reliable online services.

This paper makes two primary contributions to the field. First, through a critical analysis of existing PIP methods in Korea, it identifies key areas where privacy, security, and user convenience are compromised. Second, it proposes a practical solution that can be applied to e-commerce services. This solution differs from previous studies by focusing on user empowerment and practical implementation rather than solely on technical enhancements. Implementation these improvements will enable stakeholders to more effectively safeguard user privacy, enhance trust in digital transactions, and cultivate a more secure e-commerce ecosystem.

The remainder of this paper is organized as follows. Section 2 provides background information and a comprehensive overview of the current PIP systems in Korea. Section 3 presents a critical examination of the strengths and weaknesses of these systems, identifying areas for improvement. Section 4 presents the proposed method for enhancing PIP services, outlining its implementation, benefits, and how it addresses the identified issues. Section 5 discusses the potential implications and applications of this approach in Korea facing similar challenges, including considerations for policy and technology adoption. Finally, Section 6 concludes the paper and suggests directions for future research, emphasizing the importance of ongoing efforts to balance security, privacy, and user convenience in PIP systems.

2. Overview of Personal Identity Proofing

PIP methods involve authenticating identities through either face-to-face or non-face-to-face verification processes. To establish personal identity, authentication methods must meet the criteria outlined in Table 2 [19–22].

Table 2. Criteria for personal identity proofing.

Criteria	Definition
Applicability	must be usable anywhere
Convenience	must be developed to be easy to use
Economics	must be low-cost to use and maintain
Security	must be guaranteed security level
Compatibility	must be easy to manage.
Versatility	must be operated various communication channels

As shown in Table 2, the criterion for PIP is applicability, ensuring that users can utilize PIP methods across multiple devices, such as PCs and smartphones, without dependence on a specific medium or environment. Secondly, PIP methods should be user-friendly to guarantee convenience. Thirdly, the cost of implementing and using PIP should be economical. The fourth criterion is that the PIP system must effectively defend against various malicious security attacks, including phishing, hacking, and man-in-the-middle attacks, to ensure the trustworthiness of the authentication technology. Fifth, it is crucial that PIP can be easily integrated and expanded with other websites, security systems, and application software to manage the costs associated with authentication methods. For example, internet service websites that currently utilize a particular PIP method should be able to easily switch to other PIP methods without difficulty. Sixth, when using PIP methods via the internet, they should be accessible across various communication environments and not be limited to specific internet-connected devices.

The process of creating, authenticating, and approving a digital PIP method is presented in Figure 2, as described in the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) technical document [23].

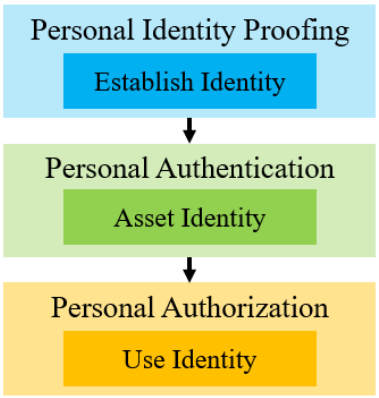

Figure 2. Flowchart of the authentication and authorization steps after creating a digital personal identity proofing means.

The PIP system enables users to assert ownership of their credentials by verifying them through a trusted third party and generating an authentication method exclusive to the user. Identity proofing methods can be categorized as either face-to-face or non-face-to-face. While face-to-face methods have the advantage of directly identifying users, they are limited by factors such as time and space.

Identity proofing is typically conducted through face-to-face methods by public institutions, banks, and telecommunication companies. In contrast, non-face-to-face methods, such as online authentication, are utilized in services like electronic finance and online transactions. The methods employed to verify an individual's identity can be divided into electronic and non-electronic media.

In Korea, there has been a rapid increase in personal information infringement issues due to the indiscriminate misuse of the 13-digit RRN assigned for citizen identification. To address this, the collection of RRNs has been prohibited since 2012, unless legally permitted. As a result, the personal identity proofing service (PIPS) has emerged as a replacement for the RRN. To generate PIP means in Korea, a state-issued identity certificate must be presented to the personal identity proofing agency (PIPA). After verifying the correct person, the PIP means is generated. The PIPA is designated by the government after comprehensively evaluation of reliability, accuracy, and safety. The PIP means used in non-face-to-face e-commerce in Korea include i-PIN, accredited certificate, mobile phone, and credit card [10,24]. PIP means are issued based on verification of the national ID cards such as driver's licenses and passports presented by the applicant. Non-face-to-face issuance requires a mobile phone, an accredited certificate, and a credit card obtained through face-to-face verification.

The PIPA identifies individuals through face-to-face verification and issues the PIP means based on the presented national ID card. Additionally, the PIPA collects and stores authentication information that is known only to the applicant.

When an online service provider requests a user's identification from the PIPA, the PIPA verifies the consistency of the user's PIP means and authentication information. If confirmed, the PIPA provides the personal information presented by the issuing applicant to the online service provider. Figure 3 shows the process of issuing PIP means in Korea.

Figure 3 shows that, to obtain PIP means for use in a non-face-to-face environment, an individual must first be identified through face-to-face verification using a government-issued identification document. After confirming the authenticity of the identification document presented by the user, the PIPA authenticates the PIP means using exclusive information known only to the user, thereby proving the user's ownership of it.

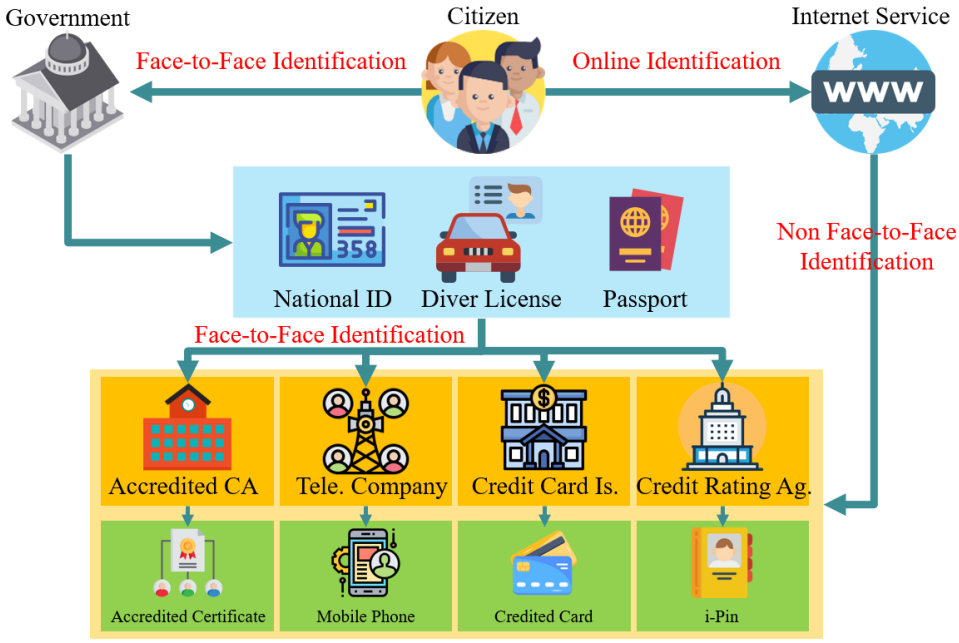

Figure 3. Offline and online personal identity proofing means in Korea.

Figure 4 shows the online user identity proofing methods used in Korea. In Korea, PIPAs include accredited certification authorities (CAs), mobile communication companies, credit card companies, and i-PIN companies. The PIP means include accredited certificates, mobile phones, credit cards, and i-PIN.

Figure 4. Types of online personal identity proofing means.

The Korean RRN is a 13-digit identification number assigned for administrative purposes to identify residents. It includes the individual's date of birth, gender, and serial number [4,5,25]. The national ID card containing the RRN includes a face photo, name, address, date of issue, and thumbprint. Therefore, in face-to-face identification, the personal identity can be verified by comparing the actual face of the holder's actual face with photo on their national ID card.

In non-face-to-face identification, the national ID card's RRN, name, and date of issuance were collected and verified for authenticity. However, indiscriminate online collection of RRNs has led to their misuse and abuse, resulting in their prohibition except when legally permitted. Therefore, alternative identification methods are necessary to replace RRNs for user identity proofing.

In 2005, the Korean government developed an alternative to the RRN with safety, convenience, and legal security in mind. Table 3 shows the conformity criteria for PIP means in Korea. These criteria are universal, valid, and do not change over time. They are designed to be safe and convenient, applicable to all devices. The RNN alternative means satisfies the criteria for uniquely identifying users online, as outlined in Table 3.

Table 3. Suitability criteria for PIP means in Korea.

Items	Criteria	Contents
Essential criteria	Universality	The means should be owned by anyone
	Persistence	The means should not change over time
	Uniqueness	The means should have the only characteristic of the user
Realistic criteria	Convenience	The means must be portable and easy to use, so that it can be easily used anytime, anywhere
	Safety	The means must be able to prevent illegal transactions in response to new hacking technologies
	Applicability	The means must be suitable for use in new environments such as smart phones
	Economics	The means must be able to reduce usage costs

3. Types of Personal Identity Proofing Means in Korea

In non-face-to-face e-commerce, verifying the identity of the transaction parties is essential. In Korea, PIPSs utilizing alternative methods to the RRN are mandated. The PIPA is designated as the authority responsible for issuing alternative methods to replace the RNN. The PIPA verifies and confirms the user's identity, generates and issues the PIP means, incorporates the user's authentication information into the means, ensures their consistency, and maintains the PIPS.

Alternative methods to the RRN include i-PIN, mobile phone, credit cards, and electronic signature-based accredited certificates. After verifying personal identity with a PIPA, the PIPS provides the connected information (CI) generated by the PIPA, along with the user's personal information (such as name, date of birth, gender, mobile phone number, etc.) to the internet service provider (ISP) [9,10,14]. The CI is an 88-byte encrypted unique identifier that matches 1:1 with the RRN. The CI is a one-way encrypted value generated by applying a hash function to the RRN and a secret key known only to the PIPA. This mechanism enables the online system to uniquely identify users, maintaining a 1:1 correspondence with the RRN presented by the user during the issuance of the PIP methods. Figure 5 illustrates the process of generating the CI.

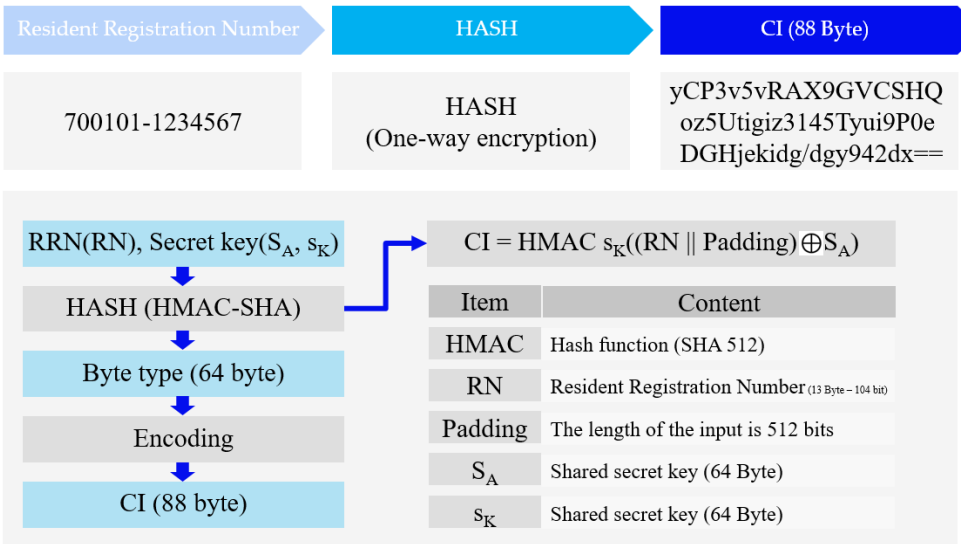

Figure 5. Flowchart of connected information generation based on resident registration number.

3.1. i-PIN

The internet personal identification number (i-PIN) is a knowledge-based PIP method that uses an ID and password. This method was introduced in 2005, and credit rating companies were designated as PIPAs to issue i-PINs. Internet users can obtain an i-PIN by providing their identity information to the PIPA that issues the i-PIN and verifying their identity either in person or remotely using a mobile phone or public certificate. To enhance the security of the service, the PIPS requires a secondary password in addition to the ID and PW [26–28]. Table 4 presents an overview of i-PIN services.

Table 4. Overview of i-PIN -based PIPSs.

Items	Contents
Concept	PIP using ID and PW
User verification	Face-to-face and non-face-to-face identity verification (using mobile phone and accredited certification)
Issuance	Online and in-person issuance
Agency	SCI/NICE/KCB
Authentication	i-PIN ID and 1st/2st password
Advantages	Easy to use with knowledge-based method
Disadvantages	High risk of ID/PW exposure

3.2. Accredited Certification

Public key infrastructure (PKI) is a security technology that confirms the identities of transaction parties and ensures the secrecy of transactions on the internet [29–31]. In 2000, the Korean government designated five PKI-based accredited certification authorities to issue accredited certificates and provide technical support for asymmetric key encryption and decryption. Accredited certificates issued by these agencies are commonly used in both financial and non-financial fields, such as electronic civil services, year-end tax settlements, housing subscriptions, and electronic tax invoices. Accredited certificates are preferred over knowledge-based user authentication methods that use ID and PW due to their higher security. Digital authentication has a non-repudiation function in e-commerce and has been applied to various non-face-to-face electronic transactions, including internet banking (since September 2002) and online stock trading (since March 2003). Initially applied to internet banking and online securities, digital authentication is now being used for various non-face-to-face electronic transactions, such as housing subscriptions, electronic civil complaints, income reports, and electronic procurement. According to the Korea Internet & Security Agency (KISA), the number of public certificates issued increased from 35.44 million in 2016 to 37.92 million in 2017, and reached 43.19 million in 2021 [9].

An overview of electronic signature-based accredited certificates is shown in Table 5. However, existing accredited certificates have technical limitations in terms of safety, convenience, and diversity. Accredited certificates are stored in a specific folder called NPKI when issued. This storage method poses a risk of leakage through folder copying during hacking attacks. Additionally, it is inconvenient of carry the certificate at all times. To improve convenience, certificates are now being stored and utilized on a cloud server for authentication purposes. This eliminates the need for users to carry physical certificates at all times. While certificates provide higher security, they may be less convenient compared to other authentication methods such as passwords or newer technologies. Legal limitations have also hindered the development of new technologies, which are often restricted to electronic signatures. Additionally, there is a growing trend towards authentication services that incorporate biometric or blockchain technology for simpler authentication [30,32].

Table 5. Overview of the accredited certification-based PIPS.

Items	Contents
Concept	PIP using the PKI-based electronic signature
User verification	Face-to-face identity verification
Issuance	Online issuance
Agency	Signgate, Coscom, KFTC, Crosscert, TradeSign
Authentication	Digital signature certificate and private key
Advantages	Adopting international standardized technology, high reliability and safety
Disadvantages	Difficult to apply offline, various means of identification are not provided, complex issuance procedures, etc.

3.3. Mobile Phone

A mobile phone-based PIPS sends a one-time identity verification code as a text message to the mobile phone number registered in the user's name. The user's identity is then verified by entering the code received in the text message. In Korea, face-to-face verification with proof of identity is required when a user obtains a mobile phone number. However, the identity verification service is not available for basic calling services, such as prepaid phones. An overview of mobile phone-based PIPSs is shown in Table 6.

Table 6. Overview of mobile phone-based PIPSs.

Items	Contents
Concept	PIP using subscriber personal information and received text messages of the mobile phone
User verification	Face-to-face and non-face-to-face identity verification (using accredited certificate)
Issuance	Online/off-line issuance
Agency	SKT, KT, LG U+
Authentication	Subscriber's personal information and authentication number received via text message
Advantages	Conveniently available anytime, anywhere
disadvantage	Available only to mobile phone subscribers

3.4. Credit Card

A credit card-based PIPS is a method of authentication that uses a credit card. The user is identified by providing the credit card number and expiration date, and the user is authenticated by requesting automated response system (ARS) authentication via mobile phone and entering the credit card payment password [33,34]. An ARS is a system where a company sends a pre-recorded voice message to a customer's phone and automatically receives the requested information from the user. Credit card numbers typically consist of 16 digits, divided into four sets of four digits. In a credit card-based PIPS, the user does not enter the entire card number but provides the eight numbers in the third and fourth sets, the expiration date, and the credit card issuer. If the card is valid, the credit card issuer initiates and ARS call to the subscriber's mobile phone number, requesting the first two digits of the credit card payment password. The ARS authentication is only attempted when the mobile phone subscriber and the credit card holder match. To ensure the safety of a credit card-based PIPS, this method only receives eight digits of 16-digit card number through the internet network. Additionally, only the first two digits of the four-digit payment password are received through the phone network to confirm identification. An overview of credit card-based PIPSs is shown in Table 7.

Table 7. Overview of credit card-based PIPSs.

Items	Contents
Concept	PIP using personal information and payment password presented when issuing a credit card
User verification	Face-to-face identity verification
Issuance	Offline issuance
Agency	8 credit card issuers
Authentication	Card number, payment password
Advantages	High reliability and versatility
Disadvantages	High risk of information exposure

4. Comparative Analysis of PIP Means

The characteristics, strengths and weaknesses, and considerations are analyzed by comparing Korea's PIP means as follows.

4.1. i-PIN-Based PIPS

The i-PIN-based PIP method is not dependent on a specific medium and authenticates the user using only an ID and password. i-PIN has the advantage of allowing the user ID to be easily changed. However, there are no measures in place to address inconvenience during the registration process or in the case of password loss after i-PIN issuance. To address this issue, it is recommended to implement a secondary password for password recovery, utilize two-factor authentication methods such as biometric identification, and enhance user experience by prioritizing safety and employing simple authentication that incorporates biometric data.

Figure 6 shows the PIPS flow based on i-PIN. When an e-commerce user accesses online services, ISPs request personal identity proofing. (1) The ISP presents an i-PIN-based PIPS authentication web page to the user's web browser. (2) On the authentication web page, the user enters their i-PIN ID and primary and secondary passwords, agrees to provide personal information, and requests that the PIPA verify their identity. (3)–(4) The PIPA verifies whether the user is registered and generates the CI using the RRN provided during user registration for the i-PIN. (5) The PIPA provides the user's personal information, including name, date of birth, gender, nationality, CI, etc., to the ISP. (6) Once the PIPS session is complete, it is terminated.

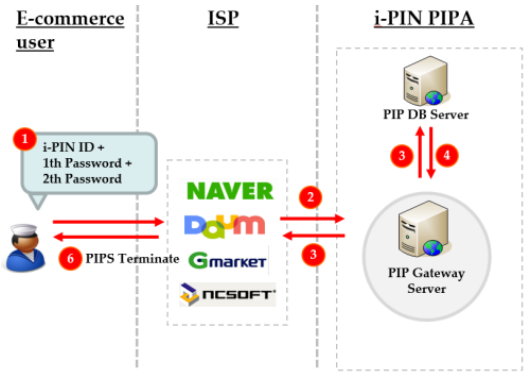

Figure 6. Flow of an i-PIN-based PIPS.

4.2. Accredited Certification-Based PIPS

An accredited certification-based PIP means encrypts transmitted and received data using a public key algorithm according to the public key infrastructure (PKI) and authenticates the user through a digital certificate. This method is highly reliable as it generates

certificates according to international standards and is widely used in the electronic finance field. Storing certificates in cloud storage reduces the inconvenience of carrying electronic files and the risk of hacking and leakage. This approach addresses the aforementioned issues. Additionally, certificates are updated annually, making them highly reliable and safe. However, this method is an accredited certificate-based and knowledge-based authentication method. Therefore, it is necessary to apply two-factor authentication to prevent theft by others due to illegal leakage.

Figure 7 shows the flow of a PIPS based on accredited certificates. In a PIPS, CI is used to uniquely identify online users. To prevent the secret key and algorithm used to generate CI from being exposed, only i-PIN PIPAs can create CI. Therefore, the accredited certificate-based PIPA encrypts the RNN and provides it to an i-PIN PIPA to obtain CI. The registration agency (RA) is an agency that links ISPs with accredited certificate-based PIPAs.

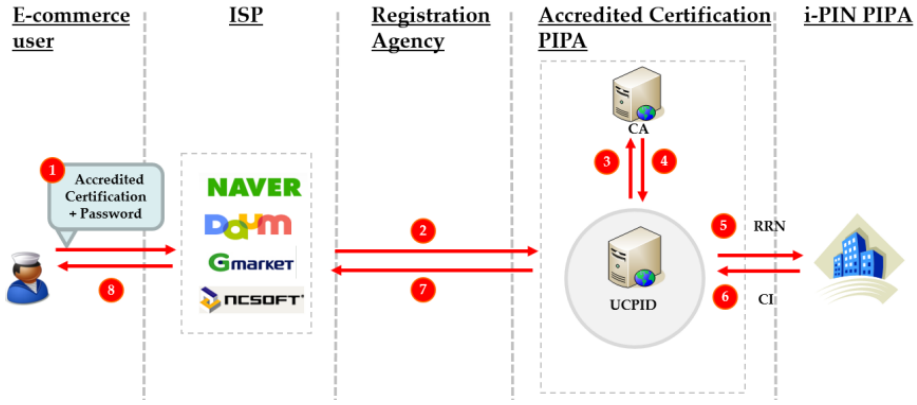

Figure 7. Flow of an accredited certification-based PIPS.

4.3. Mobile Phone-Based PIPSs

The mobile phone-based PIP method is convenient to use. Users simply enter their date of birth, name, gender, and mobile phone number and authenticate by entering a code received via text message. It can be used anytime within areas with mobile phone coverage. Additionally, users must have an active mobile phone number and carry their phone for safety purposes. The advantage of this method is its ease of use, as there is no need to memorize anything. However, there are some issues with its usage. The use of this method is limited to when the mobile phone is in operational, and identity authentication cannot be confirmed if the phone is lost. Additionally, there is a risk of unauthorized identity authentication by others. To enhance security, measures should be taken to quickly block authentication in case of theft or loss, and two-factor authentication should be implemented to prevent unauthorized access.

Figure 8 shows the flow of PIPSs based on mobile phones. (1) On the PIPS's authentication web page, the user enters their name, date of birth, gender, and the name of their subscribed telecommunications company and phone number. (2) The mobile phone-based PIPA verifies the user's subscription status and sends a one-time 6-digit random number (one-time password, OTP) via text message to conform that the mobile phone is in the possession of the user. (3) The user then enters the OTP received via text message into the PIPS authentication web page. (4) The mobile phone-based PIPA transfers the user's RRN to the i-PIN-based PIPA to convert it into the CI. (5) The mobile phone-based PIPA then provides the CI and the user's personal information to the ISP to verify their identity.

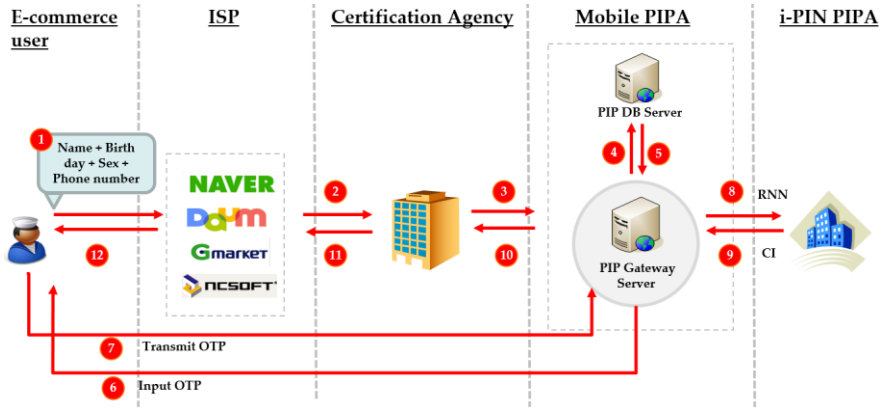

Figure 8. Flow of a mobile phone-based PIPS.

4.4. Credit Card-Based PIPSs

The credit card-based PIP method verifies identity by using the card number, payment password, and ARS authentication via a mobile phone registered under the same name as the card owner. This service offers authentication services through ARS calls, smartphone app authentication, and website membership registration to enhance security and user-friendliness. Additionally, the user must possess a registered phone number and have their phone with them. The phone's safety is guaranteed, and there is no need to memorize anything, making it easy to use. However, there are some limitations. It can only be used when the mobile phone is operational, and identity authentication cannot be confirmed if the phone is lost. Furthermore, this PIP method can be used on behalf of others, which may raise security concerns. Therefore, it is recommended to implement two-factor authentication to prevent unauthorized access in case of theft or loss.

Figure 9 shows the flow of a PIPS based on credit cards. (1) The user inputs the specified eight digits of their credit card number and their mobile phone number on the PIPS authentication web page. (2) The credit card-based PIPA verifies the user's subscription status. Then, the user is requested to confirm ownership of the credit card via an ARS call to their mobile phone. (3) The user must enter the two-digit identity proofing password, registered in advance, into the ARS system via their mobile phone. (4) The credit card-based PIPA transfers the user's RRN to the i-PIN-based PIPA to generate the CI. (5) The credit card-based PIPA provides the user's CI and personal information to the ISP to verify identity.

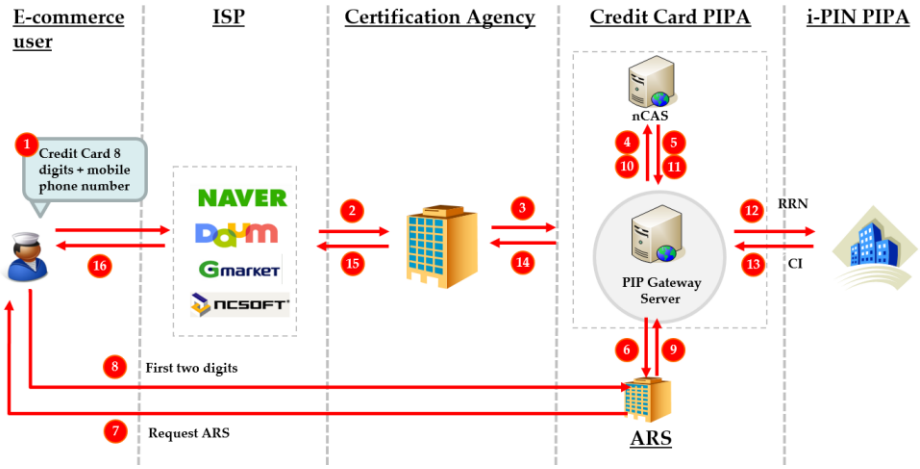

Figure 9. Flow of a credit card-based PIPS.

5. Proposed Methods to Strengthen the Safety of PIPSs

Currently, various technical methods are emerging for identifying and authenticating users when providing online services. Mobile authentication using smartphones, in particular, is becoming mainstream. This method involves confirming personal proofing through face-to-face verification when signing up for a mobile phone. It has the advantage that users always carry their mobile phone, making it a convenient option. However, most countries require identity verification when signing up for a mobile phone, either for crime prevention or electronic notification purposes. Additionally, some mobile phone subscriptions do not require identification and are solely used for making calls.

Traditionally, PIPSs that rely on knowledge-based user identification and authentication are experiencing various problems [17,35]. Users are verified through personal information questions, but if this information is leaked, there is a risk of personal data breaches.

Attackers in cyberspace can attempt social engineering attacks to obtain answers to knowledge-based questions from users of online PIPSs [36]. Answers can be obtained through social media or publicly available information. However, a significant challenge is that users may forget their authentication information. If the user does not frequently use the PIPS, they may not accurately remember the authentication information set in the past, making PIP difficult. Frequent changes to PIP information may have adverse effects, such as users reusing the same authentication information across multiple online services to remember it more easily.

Given the issues with knowledge-based user identification and authentication, it is crucial to supplement knowledge-based PIP and investigate more secure and efficient methods. Therefore, to enhance the safety of knowledge-based PIP methods, it is necessary to strengthen the PIP process by combining biometrics, quantum cryptography, and multi-authentication methods.

Due to the global spread of COVID-19, it became urgent to track the movements of infected individuals, making user identification more important than ever for administering vaccine to prevent infectious diseases. Countries without online identification methods are developing PIP methods and implementing legislation to regulate them. However, mandating the provision of unique identification information to individuals by law may raise concerns about personal privacy infringement.

Currently, the use of citizen identification information is limited. It is recommended to only use this information when necessary for medical and educational benefits, tax collection, driver's license issuance, and bank account opening. However, there is a growing need to uniquely identify users due to the rapid expansion of online services and the emergence of social phenomena, such as the spread of infectious diseases.

In order to receive online services for public purposes, users must sign up or present an identification document containing their unique identification information. In some countries, including Estonia, India, Singapore, and the UK, digital IDs are issued to identify and authenticate users on online services. These are mobile identification documents rather than physical ones [37–40]. The development of IT technology has led to a trend of proposing methods to ensure safety through the user of technologies such as blockchain, biometrics, and electronic certificates [41,42]. However, unlike Korea's PIPSs, PIPSs in other countries, such as Estonia and the UK, apply different levels of identity proofing assurances.

5.1. Trends of Digital Identity Proofing

The Digital Identity Guidelines from the U.S. National Institute of Standards and Technology (NIST) provide important guidance on digital identity management and identity proofing [43]. The guide presents a framework and recommendations for identity proofing procedures, which are detailed in the SP 800-63-3 document. First, user identity verification on online services is divided into three stages: the user enrollment stage, the identity proofing stage, and the authentication stage. The guidelines describe three levels of identity verification.

Level 1 (low assurance) only verifies the user by matching the password or PIN set during sign-up, without confirming their true identity. At Level 2 (moderate assurance), the user's true identity is verified and authenticated by matching the password or PIN along with additional verification methods. At Level 3 (high assurance), the user's true identity is verified through multiple authentications and robust identity proofing processes to ensure consistency and accuracy. The NITS guide follows a three-level identity authentication process. The process begins with basic identity verification and progresses to verification of address or date of birth. Finally, social security number verification is used for enhanced security.

The European Electronic Identification, Authentication, and Trust Services (eIDAS) regulation [44,45] was enacted in the European Union (EU) in 2014 with the purpose of strengthening the digital single market and increasing the efficiency and reliability of electronic transactions. It covers three main areas: electronic identification, which provides standards to support the electronically verifiable identity of individuals, enabling them to digitally prove their identity. Electronic authentication is the process through which users verify their identity when accessing electronic services. Trust services standards cover digital trust services, including electronic signatures, electronic authentication, time stamps, registered electronic delivery services, etc. The eIDAS regulation aims to unify standards and promote efficiency for electronic transactions and digital services within the EU. Each EU member state is required to implement this regulation by incorporating it into national law, enabling the provision of safe and reliable digital services across national borders.

eIDAS 2.0 is the EU's legal and regulatory framework that provides regulations and standards for electronic identification, authentication, and trust services [46]. The framework aims to simplify the process of verifying a user's identity by utilizing biometrics and multi-factor authentication on mobile devices. Additionally, it aims to improve international cooperation among EU countries to ensure seamless identity verification across borders. Furthermore, users will have increased control over their personal data to strengthen consent and privacy protection. Ultimately, eIDAS 2.0 is designed to enable service users to independently decide whether or not to provide their personal information based on the level of assurance or personal information required by the service provider. This is an international trend driven by the strengthening of individual control over personal information.

5.2. Improvement of PIPSs in Korea

In Korea, there are various methods of PIP, but the authentication level for each method is the same. This includes knowledge-based identity proofing methods such as i-PIN and credit card combined with ARS authentication. After authentication using various PIP means, a PIPA provides the user's personal information to the ISP without distinction.

In the United States, personal information is classified based on the level of assurance, while in the EU, there is a trend to towards strengthening user consent procedures for providing personal information in accordance with policies that promote user sovereignty [41,47]. However, in contrast, PIPSs in Korea provide user personal information to ISPs without distinction. Korea's PIPSs provide user personal information in batches without differentiation. However, Korea's PIPSs do not allow for selective provision of personal information to minimize excessive disclosure of personal information. A problem arises when personal information is transmitted through network communication unnecessarily, and ISPs collect and store personal information without the user's knowledge. When implementing PIPSs to identify and authenticate transaction parties in online e-commerce, it is necessary to incorporate the following safety measures.

First, differentiating the security strength of PIP means—it is necessary to establish PIP means with varying authentication levels. When issuing PIPS means, they are differentiated according to the security strength of the proof means presented to the PIPA for user identification purposes is provided. For example, when a user requests the PIPS on an online service, providing their name and a knowledge-based authentication method grants them

access to a limited range of online services. Furthermore, if they provide their name, date of birth, and a secondary authentication method, they can use online adult authentication services and more. Finally, if a user provides their PIP means through unique identification information and enhanced secondary authentication, such as biometric authentication, they can access all online services without restrictions.

Second, providing the minimum necessary personal information—when using PIPS, it should be possible to provide only the minimum personal information that the user has agreed to share with the ISP. However, in Korea's PIPSs, the PIPA provides the user's personal information to ISPs regardless of the security level of the authentication method presented by the user. Currently, PIPAs provide all personal information of PIPS users to ISPs. The ISP selectively collects and stores the personal information of the PIPS user, as provided by the PIPA.

ISPs should only request personal information that is necessary for the service from users, and PIPAs should only provide ISPs with personal information that users have agreed to provide. This ensures that users have control over their personal information and that ISPs are not collecting unnecessary data. Therefore, if an ISP requests access to all of a user's personal information, the PIPA should only provide it if the user has been issued a PIP method with the highest security level.

Therefore, when issuing a PIP means, it is important to consider the security of the user's presented identity verification means. Differentiated PIP means have the advantage of enabling users to selectively consent to the provision of personal information, giving them control over the sharing of their personal information.

Third, PIPSs can be provided by national or centralized organizations—in Korea, private businesses are designated as PIPAs and provide PIPSs. Private PIPAs incur costs for maintaining and managing information systems to provide PIPSs, and charge PIPS fees to the ISPs. This process includes the cost of the user's online purchase of goods and the cost of the PIPS. It is important to consider whether the government should provide frequent PIPSs, such as simple identification or age verification.

In the United States, Europe, and the United Kingdom, governments provide PIPSs to the public [13,36,37,43,44,46]. However, in Korea, private PIPAs such as mobile carriers and credit card companies provide PIPSs online without government intervention. The government issues the RRN at birth, which is necessary for confirming the individual's identity. Therefore, PIP should be handled by the government or a centralized system. In Korea, most of the citizen's personal information is held by the Ministry of the Interior and Safety, the National Tax Service, the National Health Insurance Service, and the National Police Agency. This allows for the provision of various PIPSs.

Fourth, unifying PIPS usage—Korea's PIP means increases user convenience by providing PIPSs through various means. However, ISPs are required to provide various PIP means, such as i-PIN, mobile phone, credit card, and accredited certificates, for users to access web pages. As each PIP method requires a different authentication method, it can be inconvenient to install and manage each authentication SW module. Therefore, unifying the system based on an integrated UI can reduce the inconvenience for PIPS users and ISPs.

6. Conclusions

This paper conducted a comprehensive analysis of PIPSs utilized by online service users in Korea's e-commerce sector. With the rapid expansion of non-face-to-face e-commerce services, the necessity for secure and efficient online user identification and authentication methods has become increasingly paramount. The traditional reliance on the RRN for user identification has raised significant privacy concerns due to indiscriminate collection and potential misuse of personal data, underscoring the necessity for alternative identity proofing methods. The current PIP methods currently employed in Korea, including i-PIN, accredited certificates, mobile phone authentication, and credit card-based verification, were examined and evaluated based on criteria such as applicability, user convenience, cost-effectiveness, security robustness, integration capability, and accessibility

across different devices and networks. The analysis revealed several limitations within the current PIPS framework.

Firstly, all PIP methods provide a uniform level of authentication without consideration the varying security strengths inherent in each method. This lack of differentiation may not adequately address the diverse security requirements of different online services, potentially leaving some services under-secured while overburdening others with unnecessary authentication complexity. Secondly, PIPAs provide users' personal information to ISPs without differentiation, thereby increasing the risk of unnecessary exposure of sensitive data and raising significant privacy concerns. Thirdly, the reliance on private entities for PIPS provision can result in additional costs for users and may result in inconsistencies in service reliability and standardization. Lastly, the existence of multiple PIP methods necessitates that ISPs support various authentication modules, which can increase system complexity and potentially cause inconvenience for both service providers and users.

To address these issues, several improvements are proposed to enhance the safety and efficiency of PIPS in Korea. The implementation of differentiated authentication levels based on the security strength of each PIP method can provide a more tailored approach, allowing online services to select the appropriate level of verification according to their specific needs. This stratification enhances overall security by aligning authentication strength with service sensitivity. The design of PIPSs is based on the principle of data minimization, which entails providing ISPs with only the minimum necessary personal information. This approach enhances user privacy and aligns with global privacy standards such as the GDPR. By limiting the disclosure of personal data, users retain greater control over their information, and the potential impact of data breaches is reduced. The design of PIPSs is based on the principle of data minimization, which entails providing internet service providers (ISPs) with only the minimum necessary personal information. This approach enhances user privacy and aligns with global privacy standards, such as the General Data Protection Regulation (GDPR). By limiting the disclosure of personal data, users retain greater control over their information, and the potential impact of data breaches is reduced.

The findings of this paper have significant implications for policymakers, ISPs, and users alike. By adopting the proposed improvements, the security and efficiency of the PIPS framework in Korea can be enhanced, thereby strengthening user trust and ensuring compliance with evolving privacy regulations. Furthermore, these recommendations also offer valuable insights for other countries aiming to develop or refine their own online identity proofing systems, especially those grappling with similar challenges in balancing security, privacy, and user convenience.

However, this paper is focused on the Korea, and there are limitations to its generalizability. Future studies should consider cross-country comparisons to evaluate the applicability and effectiveness of the proposed recommendations in different legal, cultural, and technological environments. Investigating user perceptions and acceptance levels of various PIP methods can provide deeper insights into the design of user-centric identity proofing services that cater to diverse user needs and preferences. Additionally, exploring the integration of emerging technologies such as biometrics, blockchain, and quantum cryptography into PIPS could contribute to the development of more secure, efficient, and innovative identity verification processes.

In conclusion, enhancing the safety and efficiency of Personal Identity Proofing Services is crucial in today's increasingly digital landscape. The implementation of the aforementioned enhancements may result in the establishment of a more robust and user-friendly PIPS framework in Korea. This advancement will not only protect personal information and prevent fraud but also support the sustainable growth of e-commerce and other online services, both domestically and internationally. By ensuring that PIPS are secure, efficient, and user-centric, greater trust among users can be fostered, compliance with stringent privacy regulations can be achieved, and adaptation to the dynamic demands of the digital economy can be facilitated.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data is contained within the article.

Conflicts of Interest: The author declares no conflicts of interest.

References

1. Wilbanks, L. The Impact of Personally Identifiable Information. *IT Prof.* **2007**, *9*, 62–64. [CrossRef]
2. Wu, N.; Tamilselvan, R.; Tayyab, T. A Study on Personal Identifiable Information Exposure on the Internet. In Proceedings of the 2022 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 14–16 December 2022; pp. 813–818.
3. Majeed, A.; Ullah, F.; Lee, S. Vulnerability and Diversity Aware Anonymization of Personally Identifiable Information for Improving User Privacy and Utility of Publishing Data. *Sensors* **2017**, *17*, 1059. [CrossRef] [PubMed]
4. You, J.H.; Jun, M.S. A Mechanism to Prevent RP Phishing in OpenID System. In Proceedings of the 2010 IEEE/ACIS 9th International Conference on Computer and Information Science, Yamagata, Japan, 18–20 August 2010; pp. 876–880.
5. Song, Y.; Kim, H.; Huh, J.H. On the Guessability of Resident Registration Numbers in South Korea. In *Information Security and Privacy: 21st Australasian Conference, ACISP 2016, Melbourne, VIC, Australia, July 4–6, 2016, Proceedings, Part I 21*; Springer: Cham, Switzerland, 2016; Volume 9722, pp. 128–138.
6. Pak, H.; Kim, C.; Choi, H. Preparation a study on the use of the Resident Registration Number and Alternatives for RRN. *World Acad. Sci. Eng. Technol.* **2012**, *611*, 3123–3126.
7. Kim, S.J.; Lee, K.H. A Comparative Study on Reforming the Resident Registration Number. *J. Korea Inst. Inf. Secur. Cryptol.* **2015**, *25*, 673–689.
8. RESIDENT REGISTRATION ACT. Available online: https://elaw.klri.re.kr/eng_service/lawView.do?hseq=40157&lang=ENG (accessed on 10 September 2024).
9. Kim, J.B. Improvement of Digital Identity Proofing Service through Trend Analysis of Online Personal Identification. *Int. J. Internet Broadcast. Commun.* **2023**, *15*, 1–8.
10. Kim, J.B. A Study on Improvement of Digital Personal Information Identification Service using Various Authentication Methods. *Test Eng. Manag.* **2019**, *81*, 2329–2336.
11. Zukarnain, Z.A.; Muneer, A.; Ab Aziz, M.K. Authentication Securing Methods for Mobile Identity: Issues, Solutions and Challenges. *Symmetry* **2022**, *14*, 821. [CrossRef]
12. Yu, Y.; He, J.; Zhu, N.; Cai, F.; Pathan, M.S. A new method for identity authentication using mobile terminals. *Proc. Comput. Sci.* **2018**, *131*, 771–778. [CrossRef]
13. Ferraiolo, H.; Mehta, K.; Francomacaro, S.; Gupta, S. *Interfaces for Personal Identity Verification—Part 1: PIV Card Application Namespace, Data Model and Representation*; NIST Special Publication 800-73-4; Computer Security Resource Center: Gaithersburg, MD, USA, 2015.
14. Kim, J.B. Study on the Quantified Point System for Designation of Personal Identity Proofing Service Provider based on Resident Registration Number. *Int. J. Adv. Smart Converg.* **2022**, *11*, 20–27.
15. Sinigaglia, F.; Carbone, R.; Costa, G.; Zannone, N. A survey on multi-factor authentication for online banking in the wild. *Comput. Secur.* **2020**, *95*, 101745. [CrossRef]
16. Zviran, M.; Erlich, Z. Identification and Authentication: Technology and Implementation Issues. *Commun. Assoc. Inf. Syst.* **2006**, *17*, 90–105. [CrossRef]
17. Ahituv, N.; Lapid, Y.; Neumann, S. Verifying the Authentication of an Information System User. *Comput. Secur.* **1987**, *6*, 152–157. [CrossRef]
18. Furnell, S.M.; Papadopoulos, I.; Dowland, P.S. A Long-Term Trial of Alternative User Authentication Technologies. *Inf. Manag. Comput. Secur.* **2004**, *12*, 178–190. [CrossRef]
19. What Is Strong Customer Authentication? Available online: https://www.fraud.com/post/strong-customer-authentication (accessed on 10 September 2024).
20. *ISO 29003:2018*; Information Technology—Security Techniques—Identity Proofing. International Organization for Standardization (ISO): Geneva, Switzerland, 2018.
21. Smith, R.E. *Authentication: From Passwords to Public Keys*; Addison-Wesley Longman Publishing Co., Inc.: Boston, MA, USA, 2001.
22. Augot, D.; Chabanne, H.; Clémot, O.; George, W. Transforming Face-to-Face Identity Proofing into Anonymous Digital Identity Using the Bitcoin Blockchain. In Proceedings of the 2017 15th Annual Conference on Privacy, Security and Trust (PST), Calgary, AB, Canada, 28–30 August 2017; pp. 25–2509.
23. ITU-T, Identity and authentication, ITU-T Focus Group on Digital Financial Services. 2017. Available online: https://www.itu.int/en/ITU-T/focusgroups/dfs/Pages/default.aspx (accessed on 10 September 2024).
24. Han, M.J.; Jang, G.; Hong, S.; Lim, J.I. A Study on reforming the national personal identification number system: The unconnected random personal identification number system. *J. Korea Inst. Inf. Secur. Cryptol.* **2014**, *24*, 721–737.

25. Lee, Y.G.; Ahn, J.H. A Study of the Alternative Means of Korean Resident Registration Number using the Authorized Certificate. *J. Korea Soc. Digit. Ind. Inf. Manag.* **2014**, *10*, 107–117.
26. Song, J.; Lee, H.; Shin, D.; Jung, H.C. OpenID Based Personal Information Management System. *Int. Inf. Institute. Inf.* **2013**, *16*, 1873–1886.
27. Ghazizadeh, E.; Zamani, M.; Ab Manan, J.L.; Pashang, A. A survey on security issues of federated identity in the cloud computing. In Proceedings of the 4th IEEE International Conference on Cloud Computing Technology and Science Proceedings, Taipei, Taiwan, 3–6 December 2012; pp. 532–565.
28. Kim, J.Y. Efficiency of Paid Authentication Methods for Mobile Devices. *Wirel. Pers Commun.* **2017**, *93*, 543–551. [CrossRef]
29. Ramadan, M.; Du, G.; Li, F.; Xu, C. A survey of public key infrastructure-based security for mobile communication systems. *Symmetry* **2016**, *8*, 85. [CrossRef]
30. Shi, J.; Zeng, X.; Han, R. A Blockchain-Based Decentralized Public Key Infrastructure for Information-Centric Networks. *Information* **2022**, *13*, 264. [CrossRef]
31. Zhou, Y.; Li, N.; Tian, Y.; An, D.; Wang, L. Public Key Encryption with Keyword Search in Cloud: A Survey. *Entropy* **2020**, *22*, 421. [CrossRef]
32. Rodday, N.; Cunha, Í.; Bush, R.; Bassett, E.; Rodosek, G.D.; Schmidt, T.C.; Wählisch, M. The Resource Public Key Infrastructure (RPKI): A Survey on Measurements and Future Prospects. *IEEE Trans. Netw. Serv. Manag.* **2023**, *21*, 2353–2373. [CrossRef]
33. Balepin, I.; Maltsev, S.; Rowe, J.; Levitt, K. Using specification-based intrusion detection for automated response. In *Recent Advances in Intrusion Detection: 6th International Symposium, RAID 2003, Pittsburgh, PA, USA, September 8–10, 2003. Proceedings 6*; Springer: Berlin/Heidelberg, Germany, 2003; Volume 6, pp. 136–154.
34. Ghasemi, M.; Asgharian, H.; Akbari, A. A cost-sensitive automated response system for SIP-based applications. In Proceedings of the 2016 24th Iranian Conference on Electrical Engineering (ICEE), Shiraz, Iran, 10–12 May 2016; pp. 1142–1147.
35. Wu, G.; Wang, J.; Zhang, Y.; Jiang, S. A continuous identity authentication scheme based on physiological and behavioral characteristics. *Sensors* **2018**, *18*, 179. [CrossRef] [PubMed]
36. Sslahdin, F.; Kaabouch, N. Social engineering attacks: A survey. *Future Internet* **2019**, *11*, 89. [CrossRef]
37. GOV.UK. Available online: https://www.gov.uk/ (accessed on 10 September 2024).
38. e-Estonia. Available online: https://e-estonia.com/solutions/e-identity/id-card/ (accessed on 10 September 2024).
39. Aadhaar. Available online: https://uidai.gov.in/en/ (accessed on 10 September 2024).
40. SingPass. Available online: https://www.singpass.gov.sg/main/ (accessed on 10 September 2024).
41. Ahmed, M.R.; Islam, A.M.; Shatabda, S.; Islam, S. Blockchain-based identity management system and self-sovereign identity ecosystem: A comprehensive survey. *IEEE Access* **2022**, *10*, 113436–113481. [CrossRef]
42. Mekruksavanich, S.; Jitpattanakul, A. Biometric user identification based on human activity recognition using wearable sensors: An experiment using deep learning models. *Electronics* **2021**, *10*, 308. [CrossRef]
43. Digital Identity Guide. Available online: https://pages.nist.gov/800-63-3/ (accessed on 10 September 2024).
44. eIDAS. Available online: https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation (accessed on 10 September 2024).
45. Gregusova, D.; Halasova, Z.; Peracke, T. eIDAS Regulation and Its Impact on National Legislation: The Case of the Slovak Republic. *Adm. Sci.* **2022**, *12*, 187. [CrossRef]
46. eIDAS 2.0. Available online: https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/eIDAS-Node+version+2.0 (accessed on 10 September 2024).
47. Vo, T.H.; Fuhrmann, W.; Hellmann, K.P.F.; Furnell, S. Identity-as-a-service: An adaptive security infrastructure and privacy-preserving user identity for the cloud environment. *Future Internet* **2019**, *11*, 116. [CrossRef]