International Journal of Business, Human and Social Sciences
ISSN: 2517-9411
Vol:6, No:11, 2012

Preparation a Study on the Use of the Resident Registration Number and Alternatives for RRN

Hyejin Pak, Changsoo Kim, and Healahng Choi

Abstract**—**The resident registration number was adopted for the purposes of enhanced services for resident convenience and effective performance of governmental administrative affairs. However, it has been used for identification purposes customarily and irrationally in line with the development and spread of the Internet. In response to the growing concern about the leakage of collected RRNs and possible abuses of stolen RRNs, e.g. identity theft, for crimes, the Korean Communications Commission began to take legal/regulatory actions in 2011 to minimize the online collection and use of resident registration numbers. As the use of the RRN was limited after the revision of the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc., online business providers were required to have alternatives to the RRN for the purpose of identifying the user's identity and age, in compliance with the law, and settling disputes with customers. This paper presents means of verifying the personal identity by taking advantage of the commonly used infrastructure and simply replacing personal information entered and stored, without requiring users to enter their RRNs.

Keywords**—**Resident Registration Numbers(RRNs), Alternative identification for RRNs.

I. Introduction

AFTER the Resident Registration Act was promulgated in 1962, the resident registration number (RRN) was issued to all individuals at or over the age of 18. The RRN, as a means of tracking demographic changes in the population, was adopted for the purposes of providing enhanced services for residents and performing the government's administrative affairs effectively [1]. Because of its convenient use for identification purposes, the RRN is used for other purposes, including banking and medical services; it is also required for online business transactions or membership sign-ups on web sites [2].

As the value of personal information increased, large leaks of personal information have been caused by hackers' attacks. In response to the growing concern about abuses of stolen information, e.g. spam, identify theft, voice phishing, etc., the Comprehensive Plan for Minimizing the Collection and Use of resident Registration Numbers has been implemented along with studies on alternatives to the RRN.

As personal data leaks have continued despite the efforts. The Korean Communications Commission (KCC) has pushed the plan aimed at limiting the use of the RRN on web sites to prevent the abuses of stole information [3].

To limit the online use of the RRN, it is necessary to ban the entry of the RRN for identification. This paper presents alternate means of identity verification that do not use the RRN. Section II discusses the use of the RRN for identity verification and the purposes of the verification means. Section III analyzes the utilization of existing identity verification methods. Section IV presents alternate means of identity verification that are transformed versions of the existing means of identity verification and do not use the RRN.

II. Use of the 'RRN'

Of the total web sites receiving over 10,000 visitors daily as of the fourth quarter of 2011[4][5][6], about 1,200 web sites, excluding public or non-profit organizations, were subject to the Act on Promotion of Information and Communications Network Utilization and Information Protection (the Act). With regard to the use of the resident registration number (RRN), 72.3% of about 1,200 web sites required visitors to enter their RRN when they signed up for site membership or checked their ID or password that had been forgotten.

The RRN was used for membership sign-up or password checking to prohibit the creation of multiple membership accounts by or for the same person or to handle membership management. The web sites required users to enter their RRNs for age and identity verification, as requested by the Act or for user identification to clarify who should be responsible in case a dispute occurs in relation to the purchase made by a user.

In case of inadvertently having multiple memberships, the user's identity can be verified by checking the user's e-mail address or telephone number, so a means of identity verification can be used instead of the RRN. However, for identity verification requested by the laws such as the Juvenile Protection Act and the Game Industry Promotion Act, a means of online identity verification is needed to confirm if the person claiming to be the user is the asserted identity.

Hyejin Pak is with Korea Internet Security Agency, Seoul, Republic of Korea (phone: 82-11-777-1054; fax: 82-2-405-5219; e-mail: idsaft@ kisa.or.kr).

Changsoo Kim is with Korea Internet Security Agency, Seoul, Republic of Korea (phone: 82-10-2683-4733; fax: 82-2-405-5219; e-mail: changsookim@ kisa.or.kr). T. C. Ms Haelahng Choi is with Korea Internet Security Agency, Seoul, Republic of Korea (phone: 82-01-2360-8415; fax: 82-2-405-5219; e-mail: hlchoi@ kisa.or.kr).

III. Current Means of Identity Verification

Identity verification is the process of providing real-time confirmation that 'the user is who s/he claims to be' by checking personal details about the asserted identity provided by the user at the time of sign-up [7].

The identity of the user can be proven in three ways: by something the user knows (Something you know), something the user possesses (Something you possess) or something the user is (Something you are).

For identity verification, a unique number or something else unique to the user, which is the RRN entered by the user or stored on the web site, is authenticated via a reliable agency, such as the National Information & Credit Evaluation, Inc. or the authorized certification agency, to assure the objectivity of the verification of the user's identity.

The means currently used to verify the personal identity online based on personal characteristics unique to the user include the real-name authentication based on the user's RRN and name, the i-PIN authentication using the ID and password, the mobile phone authentication done by sending the mobile number and the mobile verification code and the certificate authentication using the certificate and the password.

The real-name authentication is the process of providing the confirmation of the user's personal identity by a credit evaluation agency based on the information about the user's RRN and real name that is entered by the user. This method seems to be convenient because it is done quickly by entering the information that the user knows and pressing the OK button. However, it is very vulnerable to abusive uses, e.g. identity theft, because the RRN can be leaked and used by a wrong person; Massive leaks of personal information including the RRN have been already reported. For this reason, the Korean government announced the "Comprehensive Plan for Minimizing the Collection and Use of Resident Registration Numbers," under which public organizations and private companies are not allowed to use the real-name authentication service for personal identity verification [8].

The means of verifying the personal identify, such as an i-PIN, a mobile verification code and a certificate, assure the safety and objectivity of the verification because it is presumed that the personal identity has been confirmed offline, the confidential information that the user knows only is used, the data is encrypted for transmission and the trusted third party (TTP), under the control and supervision, handles the verification service.

The mobile phone authentication confirms the mobile phone information and personal information that the user knows through a mobile service provider and verifies the user's identity using the transmitted verification code, a kind of OTP (One Time Password). This authentication method proves the personal identity based on what the user knows (Something you know) or what the user possesses (Something you possess). Like the certificate authentication, however, this method uses the RRN for the verification of the user, checks the validity of the user's RRN stored on the web site or entered by the user by finding out the RRN in the user DB of the mobile service provider.

TABLE I
Means of Verifying the Personal Identify

Means	Authentication Ways
real-name authentication	Based on the user's RRN and name by a credit evaluation agency
i-PIN	Based on I-pin ID and password issued by a personal identify agency
mobile phone	Based on mobile company name, mobile phone number, name, RRN, OTP by a mobile service company
certificate	Based on certificate(connecting RRN), and password by a authorized certification agency
credit card	card type, card number, due date, password(in front of a two-digit), RRN by a credit card companny connecting payment agency(VAN, PG, etc)

The i-PIN authentication for identity verification does not require the user to enter the user's RRN, but the authentication based on the mobile verification code or the certificate requires for the RRN entered by the user or stored on the web site, not in compliance with the aim of the Comprehensive Plan for Minimizing the Collection and Use of Resident Registration Numbers.

The certificate authentication uses the hash value of the RRN stored in the certificate. The identity of the user is verified in the following process: ① the password for the certificate (passphrase for the private key) is entered, R (random sequence of numbers with a specified number of bits) is extracted from the decrypted private key, and R and the certificate are encrypted and sent to the web site; ② the validity of the certificate is proven by an authorized certification agency; and ③ VID is generated based on the RRN stored on the web site and the received R value (R⊙ RRN hash = VID) and compared with VID generated based on the hash value of the RRN and the R value (R⊙ RRN hash = VID')[9]. The authentication based on the certificate has the advantage of high safety and reliability because it confirms the personal identity using the passphrase that the user has and the certificate but requires for the RRN.

Fig. 1 Certificate authentication using RRN

Fig. 2 Mobile phone authentication using RRN

The means commonly used to verify the personal identity in Korea assure the safety and reliability but require for the use of the RRN. Therefore, it is necessary to introduce alternate means for identity verification for the tighter security of personal information.

IV. Means of Identity Verification without using 'SSN'

This paper presents the means of identity verification that meet such requirements as uniqueness to the user and the assurance of safety and reliability and can be adopted soon by making the most of the existing infrastructure.

The authentication method based on the mobile phone or the certification assures the safety and reliability and has a large pool of users. If their process for confirming the personal identity is enhanced a little, the user's identity can be verified without using the RRN.

The mobile phone authentication verifies the personal identity by checking the user's mobile number information, RRN and name in the use DB of the mobile service provider. The mobile service provider confirms the user's identity by checking the user's ID card, so identity verification can be achieved satisfactorily by using the date of birth instead of the RRN online based on the user DB. The personal identity can be verified in the following process: ① the user enters the user's mobile information, date of birth and name; ② the mobile service provider confirms the personal information entered by the user by checking it with the information stored in the DB; ③ the verification code is sent to the mobile phone number of the user if the personal information entered by the user is proven authentic; and ④ after checking if the user has entered the correct verification code, whether the user is who s/he claims to be is or not informed to the web site.

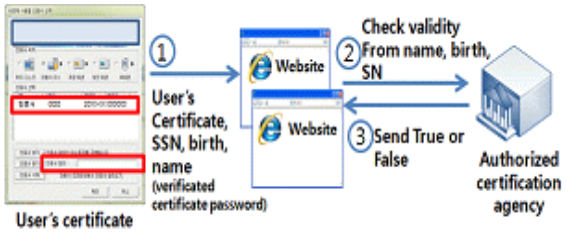

Fig. 3 Certificate authentication using birth

If only the user's name and birth of date are used for identity authentication, there could be more than one user with the same name and birth of date. However, the new mobile phone authentication method also uses the mobile information -- the mobile service company and the mobile phone number, so there cannot be more than one person with the same personal information. The identity of the possessor of the phone and the phone number can be also confirmed by checking if the verification code entered by the possessor is the same as the code sent to the possessor.

The identity authentication using the certificate can be improved by confirming the personal identity through an authorized certification agency because personal information separately proven on the web site is required for the existing method. The upgraded version of this method is processed in the following way: ① the user enters the passphrase for the user's certificate, it is checked if the user knows the correct passphrase and the certificate is transmitted safely; ② the SN (Serial Number) of the certificate and the user's date of birth and name are checked with those stored in the user DB of the authorized certification agency; and ③ the value determining if the user is who s/he claims to be is transmitted.

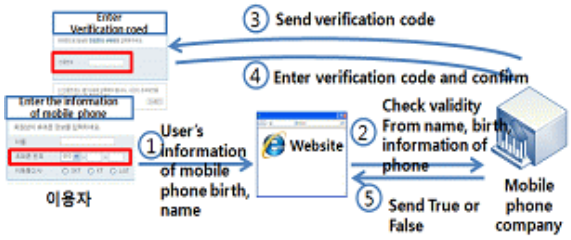

Fig. 4 Mobile phone authentication using birth

This method also uses the information available on the certificate but assures the safety or reliability only when the user knows the passphrase for the certificate because the information is sent to the authorized certification agency and confirmed by the TTP only when the user knows the passphrase for the certificate. Because only one SN is available for each certificate, one SN can be used to verify the identity of one person. The certificate-based authentication can be improved for use by using other information than the SN or changing the information about the certificate.

V. Conclusion

It is expected that the identity of the user can be confirmed without transforming the existing infrastructure much and using the RRN as presented above. That is, the personal identity can be proven without entering sensitive information, like the RRN.

However, it would be more important to minimize the request for identity verification by reviewing if identity verification is needed. It would be also necessary to cooperate with related agencies for verifying the personal identity without using the RRN. It is also necessary to seek other types of means

for identity verification that can help online business providers reduce authentication fees, and alternate means of offline verification for the use of the RRN must be also sought.

REFERENCES

[1] "Resident Registration Act", May 1962.
[2] NIA(National Information Society Agency), "Reaserch of Ways for minimizing collection and using RRN", Mar 2009.
[3] Revision of the Act on promotion of information and communicationcs network utilization and information protection for reinforcing privacy.
[4] Rankey-dot-com, http://www.rankey.com/
[5] Matrix, http://www.internetindex.co.kr/
[6] Koreanclick, http://www.koreanclick.com/
[7] Ant Allan "A Taxonomy of Authentication Methods, Update", Cartner, May 2011.
[8] Action plan of minimizing the collection and use of RRN in internet, Korea Communications Commission, June 2012.
[9] Technical standard for subscriber identification based on VID[v1.21], Korea Internet Security Agency, SEP 2009.