Journal of Digital Convergence
Vol. 17. No. 9, pp. 161-171, 2019

ISSN 1738-1916
https://doi.org/10.14400/JDC.2019.17.9.161

# mNPKI for Mobile Government in Developing Countries

Hyunsung Kim[1,2]
[1]Professor, Department of Cyber Security, Kyungil University
[2]Visiting Professor, Department of Mathematical Sciences, University of Malawi

# 개발도상국의 모바일 정부를 위한 mNPKI

김현성[1,2]
[1]경일대학교 사이버보안학과, 교수, [2]말라위대학교 수학과, 방문교수

Abstract Government transactions over wireless electronic devices are not safe and hence the messages are prone to attack. Thereby, devices supporting wireless Internet must assure the same level of security and privacy as the wired network. National public key infrastructure (NPKI) for electronic government used in the wired environment is not suitable for wireless environment for mobile government (mGovernment) because of the limitations of computing power, memory capacity and restricted battery power. This requires the development of a new NPKI for mGovernment, denoted as mNPKI, to developing countries, which provides the same security level as the wired NPKI. For the wireless environment requirements, mNPKI is based on short lived certificates. Analysis shows that mNPKI is well suited to wireless Internet and provides the same security requirement from the wired NPKI.

Key Words : Information Security, Electronic Government, Mobile Government, Public Key Infrastructure, National Security, Digital Certificate

요 약 무선 전자 장치 상에서 전자 정부의 행정 처리는 안전하지 않으므로 메시지들이 공격에 취약하다. 따라서 무선 인터넷을 지원하는 장치는 유선 네트워크와 동일한 수준의 보안과 프라이버시가 보장되어야 한다. 유선 환경에서 사용되는 전자 정부의 국가 공개키 기반 구조(NPKI)는 컴퓨팅 성능, 메모리 용량 및 제한된 배터리 전력의 한계로 인해 모바일 전자 정부를 위한 무선 환경에 적합하지 않다. 이를 위해서는 유선 NPKI와 동일한 보안 수준을 제공하는 개발도상국을 위한 모바일 국가 공개키 기반구조(mPKI)의 개발이 필요하다. 무선 환경에서의 mNPKI 요구사항은 짧은 시간 한계를 갖는 인증서를 기반으로 한다. 분석 결과 mNPKI는 무선 인터넷에 적합하고 유선 NPKI와 동일한 보안과 프라이버시를 제공함을 확인하였다.

주제어 : 정보보호, 전자정부, 모바일전자정부, 공개키기반구조, 국가보안, 디지털인증서

## 1. Introduction

The emergence of information and communication technologies (ICTs) has led a lot of changes to the way things are done in the world. These changes affect across the spectrum at large, which are that the way private companies do business, the way governments provide services to their citizens and the way they interact with stakeholders. Especially, governments are under pressure to deliver at the right time and quality with the growing demands

*This research was supported by NRF funded by the Ministry of Education (NRF-2017R1D1A1B04032598)
*Corresponding Author : Hyunsung Kim(kiu.ac.kr)
Received May 27, 2019 Revised June 28, 2019
Accepted September 20, 2019 Published September 28, 2019

of citizens and changing global rules and regulations. Many governments are trying to support the demand by reengineering their processes by adopting ICT solutions [1−4]. Electronic government (eGovernment) is slowly gaining ground across the world due to the transformation of existing government service paradigm to cater for ICT. However, providing public sector information and services online also has various issues to be solved especially focused on security and citizens' trust in governments, including threats to privacy and data systems.

Public key infrastructure (PKI) has been recognized as a key element for supporting secure and reliable eGovernment service delivery [5,6]. Several countries have implemented, or are in the process of implementing, national PKI (NPKI) for internal purposes such as Federal Bridge Certification Authority in USA, European Bridge Certification Authority in European Union, DFN−PKI in Germany, SignKorea in the Republic of Korea and others [7−10].

Many least developed countries (LDCs) cope with difficulties to implement eGovernment due to lack of strategy, technology, policy and organization [11]. In 2011, two thirds of the participants indicated that eGovernment services failed to develop in African countries as anticipated, which are among LDCs [12]. Especially for LDCs, the wide use of mobile phone networks has changed the way of communications. It has also allowed LDCs to skip the landline stage of development and jump right to the digital age [13]. Thereby, mobile government (mGovernment) was initiated as a method to communicate with the general public in country where eGovernment failed. mGovernment uses wireless Internet infrastructure and mobile devices. Mobile devices include smart phones, mobile phones, personal digital assistants, laptop computers, table PCs and other related devices. They do not have the same computational power and storage capacity as the desktop PC and wireless communication has lower bandwidth than its wired counterpart. They have lack of computing capabilities of NPKI services and memory size of storing certificate and certificate revocation list (CRL).

To guarantee security of mGovernment over wireless Internet, a new NPKI should be developed suitable for wireless environment requirements. The wireless environment has two different elements that need to be considered : mobile device and wireless Internet. First of all, mobile device must provide functionalities related with public key operations, especially digital signature. Based on the certificate, mobile device user must authenticate himself (or herself) to any service provider and could establish secure channel for mGovernment service.

This paper points out the necessity of developing a new NPKI framework for eGovernment and mGovernment, and discusses to what extent they really can fulfill their intention in acting as guiding frameworks in the implementation of mGovernment based on mobile devices. After that, we propose a new NPKI for mGovernment (mNPKI) for LDCs, which is based on short lived certificates to support mobile devices' limitations and provide the similar security level as the wired NPKI. Furthermore, we devise detailed security schemes for mNPKI by using smart cards or universal subscriber identity module (USIM) to cope from the limitations on mobile device and wireless Internet.

## 2. eGovernment and mGovernment Security

eGovernment is at the most important position of current public sector reform policies over the world where the use of ICTs to digitalize transactions and deliver public services is thought as a major leverage of public sector

innovation [14,15]. United nations (UN) report noted that already, a decade ago, 91% of UN members had eGovernment web sites [16]. However, many such services on eGovernment involve sensitive personal information, which needs to be exchanged electronically.

Transactions involving sensitive information are likely to require greater security assurances than the simple security solutions, such as requiring passwords to access to a system. For any given application, government agencies are responsible to make good decisions on the type of online transactions to be conducted over Internet and the security services needed to protect those transactions [17]. Many government information security experts believe that sensitive government transactions cannot be safely managed through purely electronic means until a full package of security and privacy features are enabled [18].

Public administrations are becoming more and more mobile, and are supported in this respect by mobile communication facilities, through which persons, data, objects and processes can be reached. There are as many definitions of mGovernment as there are various publications on this topic. However, this paper only considers the definition that mGovernment denotes the utilization of mobile technologies for eGovernmental services combined with the development of new solutions using mobile approaches [19,20]. mGovernment uses wireless Internet infrastructure and mobile devices. Wireless communication has lower bandwidth than its wired counterpart and mobile devices do not have the same computational power and storage capacity as the desktop PC. Specially, mobile devices have lack of computing capabilities of NPKI services like key generation, certificate validation, digital signature generation and verification and CRL verification.

Without devising and applying special security features, electronic transactions over eGovernment or mGovernment are much more easy to fraud and abuse than traditional government transactions, which are based on paper. In addition, eGovernment or mGovernment transactions will take place in an environment of security and privacy weaknesses. Known information technology vulnerabilities on computer system and network are increasingly being made publicly available. This offers attackers having less technical skill and knowledge the opportunity to cause a great damage to the system and network.

According to National Institute of Standards and Technology at USA, individuals or entities interacting with government agencies electronically over eGovernment or mGovernment where there requires for a secure transaction should have four security assurances [21-24].

- *Identification and authentication* are the confirmation that both of the information sender and the recipient will be identified uniquely so that they both know where the data is coming from and where it is going
- *Confidentiality or privacy* is the belief that the data will be protected from unauthorized access
- *Data integrity* is the proof that data have not been accidentally or deliberately modified
- *Nonrepudiation* provides the assurance of integrity and origin of data that can be verified by a third party. It may provide important evidence in the event of a dispute.

Most security techniques in common use today provide only a subset of these security features. However, for many sensitive eGovernment or mGovernment transactions, this level of security and privacy is not enough to support the needs of the stakeholders. Especially, they may want some kinds of irrefutable electronic method to prove that the transaction was submitted by the end user and received by the government.

## 3. Overview of NPKI

A PKI uses certificate to bind public keys to entities, makes other entities to verify public key bindings and supports the services required for ongoing management of keys in a distributed system, especially eGovernment or mGovernment. The emerging approach to address these security needs for eGovernment or mGovernment makes use of the scalable and distributed characteristics of NPKI [25].

NPKI is a system comprised of a set of people, organizations, constraints, policies, procedures and etc. NPKI collects, processes and stores customer data, and transforms this data to data used for identification and authentication, confidentiality, privacy, data integrity and nonrepudiation in electronic services through complex operations.

Certificate holders will obtain their certificates from different certificate authorities (CAs), depending on the community or organization in which they are a member. A NPKI is composed of many CAs linked by trust paths, which link a relying party with one or more trusted third parties. The initial challenge is deploying a NPKI that can be used throughout an enterprise, a company or government agency. There are two traditional PKI or NPKI architectures to support this goal, which are hierarchical and mesh enterprise architectures. More recently, an enterprise, a company or government agency are seeking to link their own PKIs or NPKIs to those of their business partners. Bridge CA architecture is a third approach, which has been developed to consider this problem. They are described as follows [26]

- *Hierarchical*: Authorities are formed hierarchically under a root CA that issues certificates to subordinate CAs. These CAs could issue certificates to CAs below them in the hierarchy, or to users. Every relying party in a hierarchical PKI could know the root CA's public key. Any legality of certificate could be checked by validating the certification path of certificates from the root CA.
- *Mesh*: Independent CA's cross certify each other, which results in a general mesh of trust relationships between peer CAs. A relying party could get the public key of a nearest CA, generally the one that issued his (or her) certificate. The relying party verifies certificate by checking a certification path of certificates that leads from that trusted CA. CAs could certify with each other, that is they issue certificates to each other, and combine the two in a cross certificate pair.
- *Bridge*: It was designed to connect enterprise PKIs or NPKIs, hierarchical or mesh, regardless of the architecture. It is possible by introducing a new CA, called a bridge CA, whose purpose is to establish relationships with enterprise PKIs or NPKIs. Note that, the bridge CA does not issue certificates directly to users. Different from a root CA in a hierarchy, it is not intended for use as a trust point. All PKI and NPKI users could think the bridge CA as an intermediary. The bridge CA sets up peer-to-peer relationships with different PKIs or NPKIs. These relationships can be used to form a bridge of trust connecting the users from the other PKIs or NPKIs.

There are many issues in making such an NPKI infrastructure trustable and practically feasible to deploy. These issues and solutions on them are the subject of the rest of this paper.

## 4. mNPKI for Mobile Government

The objective of mNPKI for mGovernment that we propose is to facilitate secure exchange of information through wireless devices, especially using mobile phone. The main actors in this process will be government bodies and citizens.

Both the governmental employee and the citizen will have digital certificates stored on their smart cards or USIMs, which will be used to secure communications.

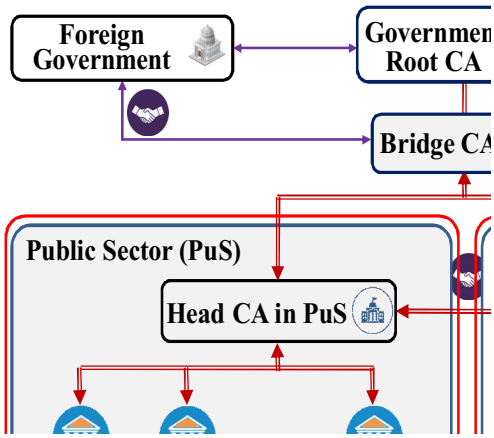


Fig. 1. Bridge mNPKI architecture between wired and wireless

By building a CA for each major government agency or ministry, denoted as public sector (PuS), we can construct a nationwide mNPKI as shown in Fig. 1, which will not have only a single failure. Since each of these authorities will have a CA, denoted as $G_{CAi}$, trust on PuS will be established by cross certifying each with the root CA. Citizens will not receive a certificate from any of $G_{CAi}$ but from accredited CAs ,$C_{CAi}$, which are private companies, denoted as private sector (PrS), which offer certification services. For a trust relation between a public officer at PuS and a citizen at PrS, a cross certification is necessary by helping of the root CA via a bridge CA.

For simplicity, it is assumed that mNPKI uses short lived certificate and every certificate is stored on a smart card or USIM. When this card or USIM is used, the holder of it provides the correct password or personal identification number (PIN) and thereby authorizing use of the certificate. With proper implementation, a secure mNPKI solution with USIM will be

- User friendly, which will encourage stakeholders to increase usage
- Interoperable, adding value through cross-functional use in different areas
- More secure, increasing the trust of citizens in their government.

## 4.1 Goal of mNPKI

The development of mNPKI based infrastructure in LDCs public administration is suited under a number of key issues, which are concerning ability of providing a secure and efficient government to government (G2G), government to business (G2B) and government to citizen (G2C) communication and operational design choices. mNPKI system is designed to achieve the following aspects

- *Flexibility*: Special measures should be taken to handle problems producing from the heterogeneity that features PuS and PrS. Therefore, both lower and higher levels of the infrastructure need to be designed to confront with the obstacles. For lower level example, the hardware and software should interoperate and adhere to international standards. On higher level, designing efficient organizational structures should be carefully considered as well as security models, which support secure interoperation between different organizations even to PrS. Systems must set up the technical functions of a mNPKI, including positively identifying internal and external users, generating keys, issuing them digital certificates, and managing the exchange and verification of certificates.
- *Scalability*: The adoption and support of more and more mGovernment services as well as the citizen's participation raise continuously the demands for introducing more and secure services. A mNPKI should be able to accommodate these increased demands.

- *Interoperability*: In order to develop an interconnected government wide system, mNPKIs will have to work seamlessly with each other. The compliance of the infrastructures with international standards is the only choice towards this direction.

We adopt the bridge model of NPKI where the bridge CA will establish a relationship with the root CA. There is only one legally recognized root CA, two head CAs in both of PuS and PrS, a bridge CA between two head CAs, unlimited number of government CAs under in PuS and unlimited number of accredited CAs in PrS. Root CA does not issue certificates directly to users but issue to CAs including $G_{CAi}$ and $C_{CAi}$.

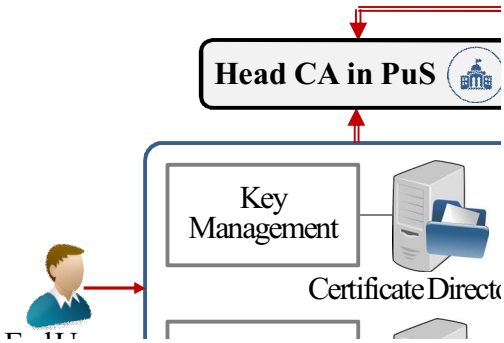


Fig. 2. Configuration of the head CAs and the root CA with repository

## 4.2 Entities and Their Roles

mNPKI follows a bridge model as shown in Fig. 1 with the configuration of the system at Fig. 2. CAs in the bridge comprise a chain that leads up to the root CA or trusted anchor as shown in Fig. 1 and has the following roles

- *Root CA*: It generates certificates for intermediate CAs and also for all systems in Fig. 2. Root CA is kept offline as a compromise of it would compromise the trust in all certificates issued by CAs. For the simplicity of the architecture configuration, it is assumed that root CA is composed of CA, policy CA and issuing CA.
- *Registration authority* (RA): It is an entity to register or vouch for the identity of users to mNPKI. It is intermediate between user and CA. RA does the main rolf of user's identifications. After RA submits the certificate requests to the CA, it verifies certificate contents for the CA. RA could also throw back information provided by a third party. The level of trust could be determined with the quality of this authentication process, which can be placed in the certificates.
- *Card management system* (CMS): It checks the smart card or USIM status including valid, reported as stolen, reported as lost, and so on and invokes verification systems that decide on the certificate status.
- *Repository*: It is a database of active digital certificates. The main role of it is to provide data that makes users to confirm the status of digital certificates for entities that receive digitally signed messages. CAs post certificates and CRLs to repositories.
- *Archive*: It is a database of information to be used in settling future disputes. The business of it is to store and protect sufficient information to determine whether a digital signature on an old document should be trusted or not.
- *Certificate revocation list* (CRL): It is used for PuS to revoke a certificate before it has expired. This is required because of the private key having been lost, stolen or compromised. When a certificate is revoked and the reason for revocation is included in the CRL.
- *Online certificate status protocol* (OCSP): It is used for PrS to provide the timely status of identified certificates instead of using CRL.
- *Certificate authority* (CA): It is also called certificate issuer, which is used to issue the certificate. A certificate is a data structure formed of both the public key and the identified information that belongs to the

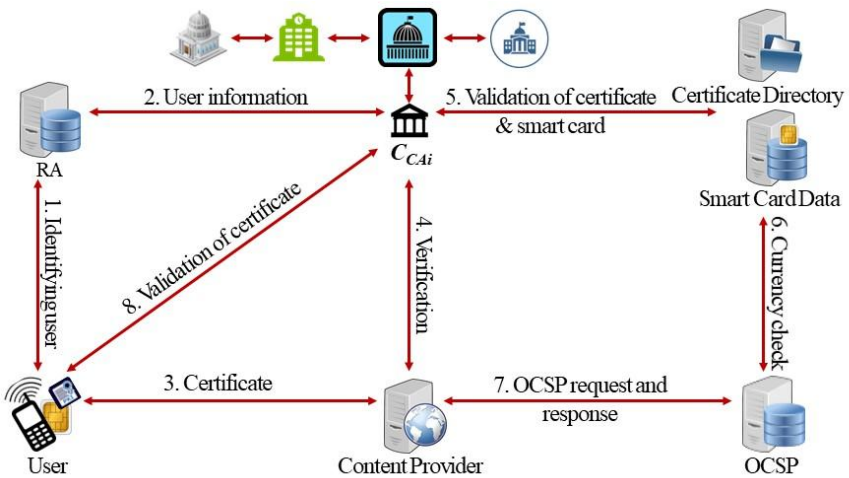


Fig. 3. Scenario of mNPKI

holder of the corresponding private key. Each certificate based on short lived X.509 certificate is issued to an individual and has a digital signature of the issuing CA. The certificate of the proposed system has short life compared to the wired Internet service. The certificate could be revoked for several reasons including loss of the private key, compromise of the key or the expiration of lifetime of the certificate. There are multiple revocation mechanisms and they need to be timely and efficient.

- *Users*: They are organizations or individuals that use the mNPKI, but do not issue certificates. They rely on the other components of the mNPKI to obtain certificates, and to verify the certificates of other entities that they do cooperate with. End entities contain the relying party, who counts on the certificate to know, with certainty, the public key of another entity and the certificate holder, that is issued a certificate and can sign digital documents. Note that an entity could be both a relying party and a certificate holder for various services.

## 4.3 Functions

mNPKI is primarily focused on simplifying routine G2G, G2B and G2C transactions. To support various applications including electronic identification, electronic passports, health and insurance cards, electronic tax systems and so on, the main operations of these applications are briefly discussed.

- *Enrollment*: It collects data for an individual or an organization to conform to a set of predefined criteria. This procedure may be different for each individual RA and is usually related to the certificate use cases. At the end of the enrolment process, a customer should have a smart card, a digital certificate stored in the smart card and a PIN associated with the certificate. For example, an individual may be asked to provide his (or her) identity by presenting authentic documents, such as an identity card, tax record number, proof of residence and bank account details for the tax authority's RA.
- *Identity verification and validation*: The operations are usually processed through validating and verifying the certificate contained in the smart card or USIM. Validation or verification is done when the owner of the certificate inputs the smart

card into a reader and gives the correct PIN when prompted to do so for PuS. However, for PrS, application accesses the USIM and performs proper operations on it after providing the proper PIN. The operation is performed by CMS that checks the card status and then invokes verification systems, which decides the certificate status. The validity of the certificate is performed via OCSP, which is updated hourly with a certificate's status, or just with short lived certificate for PrS. This process ensures that both the card and the certificate are associated and are valid at the time of use.

## 4.4 Short Lived Certificates

mNPKI uses short lived certificates for mobile devices. A short lived certificate is the same as a regular certificate, except using short validity period. Short lived certificates are an alternative to traditional certificate checking methods by shortening certificate lifetimes ranging anywhere from 24 to 96 hours [27,28]. This shortened certificate validity period would make inclusion of OCSP information unnecessary, since any stolen or misused certificates are set to expire before browsers would check for OCSP status and before a major attack could be completed [29]. Because servers do not have to check for certificate status, short lived certificates enable faster web load times. Similarly, by not relying on receiving an OCSP response, short lived certificates are not vulnerable to a sophisticated man-in-the-middle attack that would block responses. On the performance side, for many large consumer facing sites, every millisecond matters, and the balance with security is difficult to reach with current methods. Short lived certificates help eliminate this concern. Some of the reasons to use short lived certificates in mNPKI include smaller handshakes with no call backs to CAs, no online certificate status checks and certificate expiration within a few days that limits the use of the compromised certificate.

## 4.5 Scenario and Analyses

Fig. 3 shows a scenario of mNPKI between user in PrS and government agency in PuS. Short lived standard X.509 certificate is applied to mobile phone. Verification of the certificate of mobile phone is just by using the certificate itself otherwise OCSP is used by server for the performance reasons. $C_{CAi}$ issues a certificate, publishes it on directory, and sends a digital certificate stored in the smart card of mobile phone. When user wants to use any government service, he (or she) sends certificate information to content provider. The service provider easily accesses $C_{CAi}$ and validates the certificate. OCSP is used to delegate the validation of the certificate via $C_{CAi}$ if mobile phone needs to verify any certificate, which could reduce the overhead of mobile phone and put efficiency on it. We need to adopt the feature of short lived certificate in [27-29] for the security and privacy reasons. It does not have extensions that are used for certificate path validation, which could avoid the burden of CRL. For the short lived certificate, mobile phone only validates the certificate by verifying signature and the valid period in the certificate. After the successful transaction, the system should keep the transaction record as the irrefutable electronic receipt to prove that it was actually submitted by the user and received by the government.

Digital signature is one of the most important and expensive operation of NPKI, which affects overall system performance. Thereby, the proposed system recommends the ECC based digital signature algorithm (ECDSA) with 163 bits key, which has the same security level with RSA with 1024 bits key.

Table 1. Comparison of NPKI Features

| Property \ NPKIs | Wired NPKI | mNPKI |
|---|---|---|
| Basic communication | Wired communication | Wireless communication |
| Basic device | Personal computer with smart card | Mobile phone with USIM |
| Architecture | Bridge model | Bridge model between wired and wireless |
| Certificate | X.509 | X.509 (Short lived certificate) |
| Certificate size (X.509, short lived) | (949 Bytes, -) | (819 Bytes, 181Bytes) |
| Number of communications for certificate validation | 7 | 3 |
| Digital signature algorithm (generation, verification) | ECDSA on PC (3ms, 3.6ms) | ECDSA on mobile phone (1200ms, 2500ms) |
| Total module size | 1.6 MBytes | 200 KBytes |

Table 1 shows a comparison for properties between the wired NPKI on RFC 2511 and RFC 2510 and the proposed mNPKI [30-31]. Especially, the communication overhead is very apt to wireless Internet and total module size requirements are good for mobile phones. The overall communication requires 8 steps for mNPKI as shown in Fig. 3, which includes authentication, certificate delivery and certificate verification. It only requires 3 steps for certificate verification, which is much smaller than the wired NPKI case.

### 4.6 Further Considerations

There are more challenges to mGovernment with mNPKI readiness, ranging from human capacity to set up and maintain the system to other drawbacks in reproviding certificate for each transaction in terms of user friendliness, among others which include the following

- Insufficiency in the investment for rural network infrastructure, caused by inadequate budgets and foreign exchange that affect procurement of networking tools
- Lack of infrastructure for electronic transactions in LDCs and institutional configurations
- Unfriendly organizational bureaucratic tendencies that impedes the leadership to modify the processes of business undertakings to accommodate mobile phones
- Poor quality of data and lack of coordinated user focused service approaches
- Absence of partnership between private sector and government in dealing with issues of common interest
- Mobile technology appropriate legislation is also falling short of effective regulation in its utilization

All the challenges in the research are quite similar to challenges found in other studies on mGovernment in LDCs [32].

## 5. Conclusion

LDCs are struggling to implement eGovernment due to lack of strategy, technology, policy and organization. Especially for LDCs, mGovernment was started as a method to communicate with the general population in country where eGovernment failed. To guarantee security of mGovernment via wireless Internet, this paper has been proposed a new NPKI, mNPKI, for mGovernment. mNPKI supports two different elements' requirement over wireless environment: mobile device and wireless Internet. First of all, mNPKI based on short lived standard X.509 certificates supports mobile devices' limitations and provides the similar security level as the wired NPKI. Furthermore, the proposed security schemes for mNPKI by using smart cards or USIM could cope from the limitations on mobile device and wireless Internet.

The proposed mNPKI could be used for the implications of the applications mentioned in [33,34] but there are no restricted applications of

it. It should be noted that each nation with its government has its distinct structure, departing from its unique geography, history and culture. Thereby, efforts and initiatives to devise NPKI need to aim at fulfilling the individual goals, taking into consideration on their specific national contexts and priorities.

## REFERENCES


[1] A. Das, H. Singh & D. Joseph. (2017). A longitudinal study of e-government maturity.*Information & Management*, 53, 415-426.

[2] H. Kim & H. Choi. (2016). *Research on* Deployment Strategy of Public Key Infrastructure for Developing Country: Focused on Malawi. *Journal of Digital Convergence, 14(10),* 45-51.

[3] J. Jo & S. Choi. (2016). Firm's Market Value Trends after Information Security Management System(ISMS) Cerficiation Acquisition. *Journal of the Korea Convergence Society, 7(6),* 237-247.

[4] D. Kang, M. J. Park, D. H. Lee & J. J. Rho. (2017). Mobile services with handset bundling and governmental policies for competitive market. *Telematics and Informatics*, *34,* 323-337.

[5] A. Jansen & S. Olnes. (2016). The nature of public e-services and their quality dimensions, Government *Information Quarterly, 33,* 647-657.

[6] C. E. V. Madhavan & P. K. Saxena. (2003). Recent Trends in Applied Cryptology. *IETE Technical Review, 20(2),* 119-128.

[7] National Institute of Standards and Technology. (2000). *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*.

[8] *Solution Profile-U.S. Federal Bridge Certification Authority (FBCA)*, European Federated Validation Service Study, 2009.

[9] *DFN-PKI Certificate Policy - Security levels: Global, Classic and Basic*, Deutsches Forschungsnetz, 2006.

[10] J. Kim, S. Park, H. Cho, J. Kim & J. Y. Choi. (2017). Public trust in a mobile device and service policy in South Korea: The Mobile Device Distribution Improvement Act. *Telematics and Informatics, 34,* 540-547.

[11] W. Lam. (2005). ZBarriers to e-government integration, *Journal of Enterprise Information Management, 18(5),* 511-530.

[12] Informata. (2001). Mobilizing public services in Africa: The m-government challenges, 1-12.

[13] J. Poushter & R. Oates. (2015). Cell Phones in Africa: Communication Lifeline-Texting Most Common Activity, but Mobile Money Popular in Several Countries, Pew Research Center.

[14] S. F. Verkijika & L. D. Wet. (2018). A usability assessment of e-government websites in Sub-Saharan Africa. *International Journal of Information Management, 39,* 20-29.

[15] M. Z. I. Lallmahomed, N. Lallmahomed & G. M. Lallmahomed. (2017). Factors influencing the adoption of e-Government services in Maturittius. *Telematics and Informatics, 34(4),* 57-72.

[16] Z. Li & F. Yang. (2016). The E-government Information Model Based on GPR. *Government Information Quarterly, 33(2),* 291-304.

[17] United Nations. (2005). Global E-Government Readiness Report 2005.

[18] OMB Memorandum M-00-10. (2000). *OMB Procedures and Guidance on Implementing the Government Paperwork Elimination Act*,

[19] European Parliament. (2013). Security of eGovernment System Final Report, Science and Technology Options Assessment, IP/A/STOA/FWC/2008-096/LOT4/C1/SC10.

[20] I. Marin, N. A. J. Al-Habeeb, N. Goga, A. Vasilateanu, I. Pavaloiu & C. Boiangiu. (2017). *Improved M-Government based on Mobile WiMAX*, in *Proc. of 2017 21st International Conference on Control Systems and Computer Science*, Bucharest, Romania, 37-42.

[21] S. Hong. (2014). Research on Wireless Sensor Networks Security Attack and Countermeasures: Survey. *Journal of Convergence for Information Technology. 4(4),* 1-6.

[22] NIST Special Publication 800-25. (2000). *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*.

[23] H. Kim. (2013). Privacy Preserving Security Framework for Cognitive Radio Networks. *IETE Technical Review, 30(2),* 142-148.

[24] S. H. Lee. (2015). Cloud computing Issues and Security measure. *Journal of Convergence for Information Technology, 5(1),* 31-35.

[25] NIST Special Publication 800-57. (2013). *Recommendation for Key Management Part 3: Application-Specific Key Management Guidance*.

[26] W. Shanks & H. Khiabani. (2013). *Building and managing a PKI solution for small and medium size business*, The SANS Institute.

[27] B. Payne. (2016). *PKI at Scale using Short-lived Certificates*, in *Proc. of USENIX Enigma* 2016, San Francisco, CA.

[28] H. Jin & P. Papadimitratos. (2016). *Proactive*

*certificate validation for VANETs*, in *Proc. of 2016 IEEE Vehicular Networking Conference*, (pp.1-4). USA: IEEE.

[29] J. Rowley. (2016). *How Short-Lived Certificates Improve Certificate Trust, Digicert blog*, https://blog.digicert.com/short-lived-certificates/.

[30] IETF RFC 3280. (2002). *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.

[31] Y. Lee, J. Lee & J. Song. (2007). Design and implementation of wireless PKI technology suitable for mobile phone in mobile-commerce. *Computer Communications, 30,* 893-903.

[32] C. Marufu & K. A. Maboe. (2017). Utilisation of mobile health by medical doctors in a Zimbabwean health care facility. *Health SA Gesondheid, 22,* 228-234.

[33] B. Klievink, A. Neuroni, M. Fraefel & A. Zuiderwijk. (2017). *Digital Strategies in Action-a Comparative Analysis of National Data Infrastructure Development*, in *Proc. of the 18th Annual International Conference on Digital Government Research*, (pp. 129-138). New York : ACM.

[34] I. K. Rohman & L. Veiga. (2017). *Against the Shadow: the Role of e-Government*, in *Proc. of the 18th Annual International Conference on Digital Government Research*, (pp. 319-328). New York : ACM.

김 현 성(Hyunsung Kim) 정회원

· 2002년 2월 : 경북대학교 컴퓨터공학과 (공학박사)
· 2002년 3월 ~ 현재 : 경일대학교 사이버보안학과 교수
· 2010년 2월 ~ 2018년 8월 : 정보융합보안연구소 소장
· 2015년 12월 ~ 현재 : 말라위대학교 수학과 방문교수

· 관심분야 : 인지무선네트워크 보안, 네트워크 보안, 암호 프로토콜, 암호구현, 정보보호
· E-Mail : kim@kiu.ac.kr