Identity based Cryptography

** Sarvesh Tanwar*
*** Anil Kumar*

Abstract

Data security is one of the principle concerns today. Digital signature assumes an important role in guaranteeing authentication, non-integrity, and non-repudiation on a message. Digital signature can be computed using Rives, Shamir, and Adleman (RSA), and elliptic curve cryptography. It can be a simple signature in which hash of the message is encrypted with the private key of the sender. This private key and corresponding public keys are generated by Certificate Authority (CA), and public key is binded in the digital certificate. Another approach is Identity Based (ID) signature in which private keys are generated by Private Key Generator (PKG) and public key is derived from the user's identity. This is also known as certificate less communication. In ID based signature, there is no need to transmit public key over unsecure channel. Public keys are efficiently derived from the receiver's identity information such as name, email address, network address, IP address, and now Aadhar number. Unauthorized users can forge email addresses. Today, Aadhar number is used as a unique identity proof that can be used as ID to derive public key of the user. But ID based cryptography has an inherent key escrow because of its dependence on PKG that uses a single master secret key to generate a user's private key. Key escrow enables the PKG to decrypt all the messages of its domain. In this paper we have proposed a secure and efficient multiple signatures scheme based on Shamir's and Lein Harn's identity based signature that is secure against forgery and public key replacement attack and done a comparison between Public Key Infrastructure (PKI) and ID based cryptography.

Keywords: Aadhar number, digital certificate, digital signature standard (DSS), key escrow, private key generator (PKG)

I. INTRODUCTION

Public Key Infrastructure (PKI) is the primary means of deploying asymmetric key cryptography. It consists of encryption techniques, software and services for authentication implementation to protect the security of business transactions and communication over internet [16]. Certificates signed by CA offer authentication via digital certificates. Thus concept of PKI integrates public key cryptography, certification authority (CA), and digital certificates into network security architecture. It provides assurance of secure exchange of sensitive information over unsecure channels. The PKI is a technology which enables its clients to maintain a level of trust by providing security services [15].

Data and money can be sent securely by using PKI. It provides a digital certificate that is stored in public key directory or Lightweight Directory Access Protocol (LDAP). A PKI is also called a *trust hierarchy* [17]. CAs are basic source of trust.

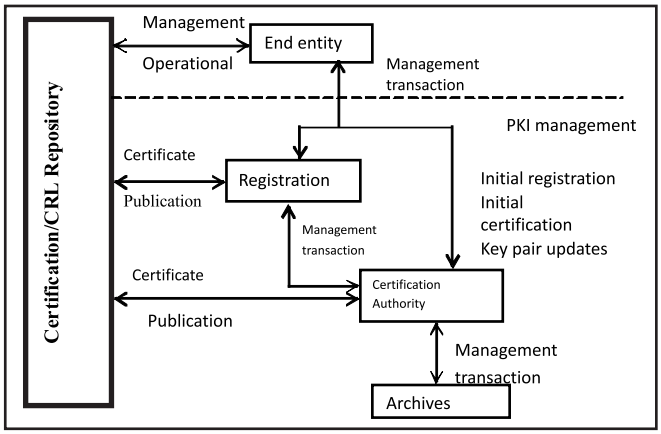
PKI is one of the building blocks of digital life. E-communication without security has little value in the competitive arena of business management and operations. A PKI is an infrastructure to support and manage public key based **digital certificates** where key can be generated either by CA or by client. If key pair is generated by client, he sends a copy of the public key of the CA for certification. The core components of PKI are:

A. Different CAs

- MTNL CA
- Tata Consultancy Services (TCS)
- The Institute for Development and Research in Banking Technology (IDRBT)
- SAFESCRYPT(SATYAM)
- nCODE Solutions
- National Informatics Centre (NIC)

Manuscript received May 21, 2017; revised July 13, 2017; accepted July 15, 2017. Date of publication August 6, 2017.
* S. Tanwar is with Department of Computer Science & Engineering, Mody University of Science & Technology, Rajasthan, India-332311 (email: s.tanwar1521@gmail.com)
** A. Kumar is with Department of Computer Science & Engineering, Mody University of Science & Technology, Rajasthan, India-332311 (email: dahiyaanil@yahoo.com)
Digital Object Identifier 10.17010/ijcs/2017/v2/i4/117850

Fig. 1. Core components of PKI

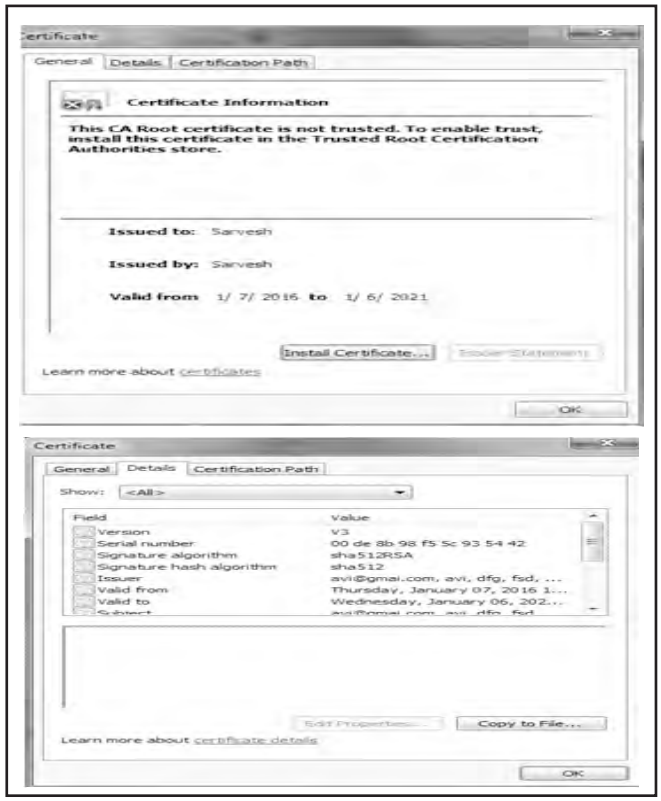


❖ Central Excise & Customs
❖ e-Mudhra

Every CA has a certificate to prove its identity. It is issued by a trusted CA. If it is Root CA , it has a self-signed certificate. Example of CAs are: VeriSign, GoDaddy, Entrust, and Thawte. CA is responsible for :

❖ Issuing certificates
❖ Revoking certificates
❖ Formulating a certificate policy
❖ Implementing the Certificate Practice Statement

Fig. 2. Format of PKI Certificate



B. Identity based Signature

In 1984, Shamir proposed the idea of identity based cryptosystem based on inter factorization problem to simplify key management procedures of PKI [14]. It is a public key system where public key can be represented by an arbitrary string such as name, contact number, email address, network or IP address. Instead of generating random private/public key, Shamir proposed mathematically generated recipient public key from receiver's identity information. Private Key Generator (PKG) has master public and private keys. Any user can generate a public key with reference to the identity ID by combing the identity attribute with master public key. He uses his master private key to generate the private key for the user with identity ID [1][6][20].

The main motivation to propose this approach was to eliminate the need of certificate and issues related to them such as validity of certificate, key/certificate revocation, trust on Certificate Authority (CA), and maintenance of public key directory. As the public key is derived from publically available information, there is no need for public key directory and certificate management.

In 2008 Harn [9] proposed efficient multiple signature based on discrete logarithm problem. In this scheme, the length and verification time of the signature are fixed [9]. To overcome this problem, all the signers must share the same modulus that was impossible in traditional public key system.

C. How ID based cryptosystem works

RSA based signature consists of three phases: Key Generation, Encryption, and Decryption.

Multiple signatures are digital signatures where a group of signers signs a message in such a way that the signature is valid if and only if it is determined by the signature of all and every single member of the group [13].

Suppose Alice wishes to send a message M to Bob [5]. The steps are:

1. PKG selects a random number to generate a master private key and master public denoted sk_{PKG} and pk_{PKG}.
2. First Alice authenticates herself to PKG and receives private key $sk_{IDAlice}$ to generate a signature σ for message M and transmits $M||\sigma$ to Bob.
3. PKG computes Bob's public key $Q_{ID}=H(ID_{Bob})$ [7] and the corresponding private key $SK_{IDBob}=s_0 Q_{ID}$. Bob checks whether σ is a genuine signature or not using Alice's identity ID_{Alice} and PKG's public $keypk_{PKG}$. Signature is

accepted if it is verified otherwise Bob rejects the message.

In this paper we have proposed a secure and efficient multiple signatures scheme based on Shamir's and Lein Harn's identity based signature that is secure against forgery and public key replacement attack.

II. IMPLEMENTATION OF ID BASED CRYPTOGRAPHY

ID based signatures are prone to key escrow problem [12][18]. PKG generates private key and is responsible for message communication. If PKG intentionally or maliciously uses private key of a person who does not belong to it, it leads to key escrow [11]. We provide a solution to remove the key escrow problem. We have proposed and implemented ID based cryptography in Java. Identity based signature uses the following algorithms:-

- ***Gen*(1,*k*):** On input security parameter k, this algorithm outputs the public parameter param and msk for the PKG.
- ***ExtractUser*(*ID*)**: This algorithm interacts with user and PKG. Upon successful execution of protocol, user obtains secret key with respect to identity ID.
- ***getStatus*(*ID*):** allows the public to determine whether PKG has generated signature on behalf of an honest user; returns 1 if Aadhar number and email id match else returns 0.
- ***Sign*(mID_S, ID_R, *t*) :** Outputs a signature on message with respect to identity ID.
- ***Verify*(*m*, ID_S, ID_R, *t*):** Verifies signature on message with respect to identity ID.

Any verifier can detect the malicious behaviour of the PKG by verifying ID and signature generated by a user and another signature generated by the PKG.

A. Design and Implementation

The signer is registered with PKG. PKG generates a secret key derived from the signer's identity. The generated secret key is used to sign the messages. The user's ID (only Aadhar number and email address) will be verified by the Unique Identification Authority of India (UIDAI). It ensures security and confidentiality of information by encrypting to prevent leakage in transit.

B. Signature Generation

If Aadhar identity is verified, PKG computes H(id). With private key *d* and corresponding public key *e*, secret key $g_j = id_j^d \bmod n$ is computed.

- If UIDAI verifies the Aadhar and email address, PKG computes H(id).
- Secret key $g_j = id_j^d \bmod n$ is computed using private key d and corresponding public key e.

C. Public key generation

```
public void set_key(String id){
RSA rsa = new RSA(id);
KEY = rsa.get_public_key();
n = rsa.getn();
public BigInteger get_public_key(String id){// Public
Key generator
BigInteger pk = BigInteger.valueOf(-1),sk
              = BigInteger.valueOf(-1);
boolean flag  = true;
try {
Scanner p = new Scanner(file);
String ID;
while(p.hasNext()){
ID = p.next();
pk = p.nextBigInteger();
sk = p.nextBigInteger();
n  = p.nextBigInteger();
if(id.compareTo(ID) == 0){// User is already registered
flag = false;
break;
   }
}
//PKG calculates the private key g using the master secret
key d.
Private key
public BigInteger get_private_key(String id){ // Private
Key generator
BigInteger x = BigInteger.valueOf(-1);
boolean flag = true;
try {
Scanner p = new Scanner(file);
String ID;
while(p.hasNext()){
ID = p.next();
x = p.nextBigInteger();
x = p.nextBigInteger();
n = p.nextBigInteger();
if(id.compareTo(ID) == 0){
        // User is already registered
flag = false;
break;
}
```

}

❖ Each signer with identity ID_j randomly selects a large integer number r_j and computes $t_j = r_j^e \bmod n$.

❖ Broadcast t_j to other signers.

❖ Then each signer computes

$t = \Pi_{j=1}^{l} t_j \bmod n$

$h = (m, t, id_R, e_{PKG}, L)$ Where $L = ID_j$, $j = 1,2,..n$

$s_j = g_j . r_j^h$

❖ Broadcast this s_j to remaining signers.

❖ After receiving of s_j where $j = 1, 2,\ldots n$ the multiple signature can be computed as follows:

$s = \Pi_{j=1}^{l} s_j \bmod n$

❖ The multiple signature is $\sigma = (t, s)$

D. Signature Verification

The receiver with ID i can verify the signature, signed by signers with identities $L = ID_1, Id_2.. ID_n$.

To verify multiple signatures σ whose ID is $ID_1, Id_2.. ID_n$.

$se = (j_1, j_2 .. j_l).t^{H(m,t,idR,ePKG,L)} \bmod n$

III. RESULTS

Fig. 3. Aadhar based signature generation

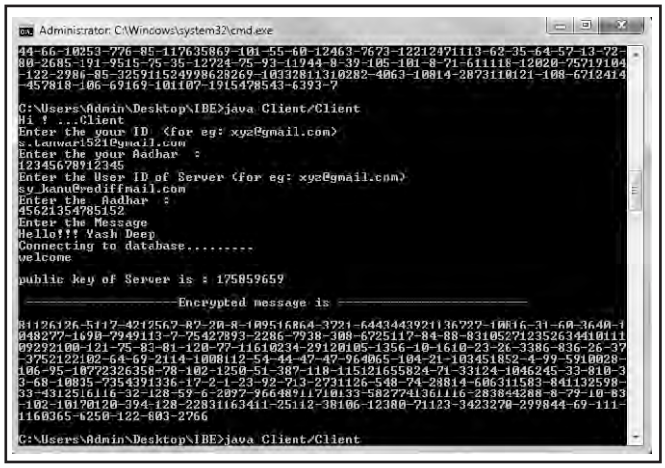
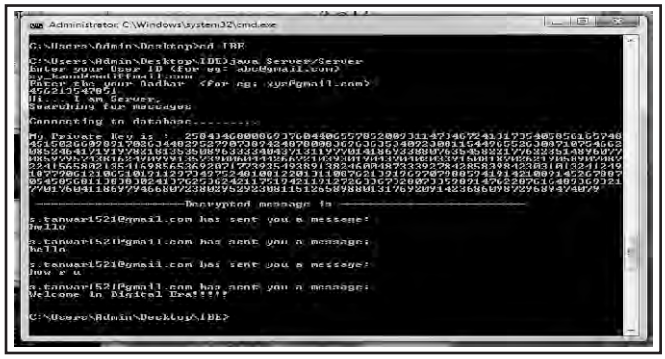


Fig. 4. Aadhar based signature generation



A. Verification

Figures 3, 4, and 5 show the output for ID based cryptography.

B. Database for ID verification

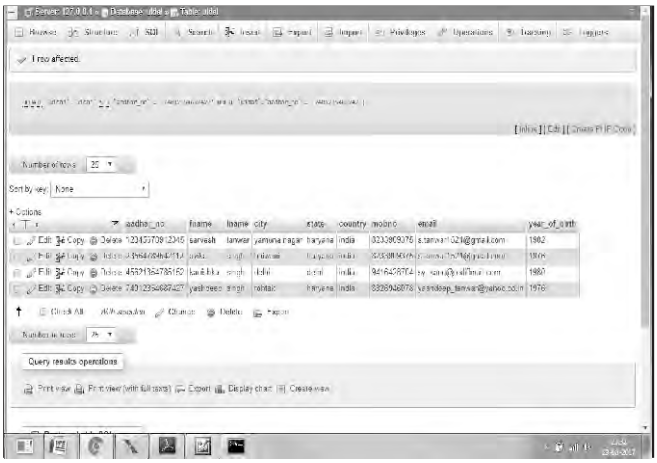
```
public String getStatus(String ID,String A,String
ID1,String A1)
{
int i=0;
try
{
Class.forName("com.mysql.jdbc.Driver");
    //STEP 3: Open a connection
System.out.println("Connecting to database.....");
con = DriverManager.getConnection("jdbc:
mysql://localhost/uidai","root","root1234");
prestat = con.prepareStatement ("select * from uidai
where aadhar_no=? and email=? ");
prestat.setString(1,A);
prestat.setString(2,ID);
result=prestat.executeQuery();
result.next();
if(result.getRow()>0)
{
i++;
}
prestat = con.prepareStatement ("select * from uidai
where aadhar_no=? and email=?");
prestat.setString(1,A1);
prestat.setString(2,ID1);
result=prestat.executeQuery();
result.next();
if(result.getRow()>0)
{
i++;
  }
}
catch(Exception evt)
{
System.out.println("error "+evt);
}
if(i==2)
return "Accepted";
else
return "Denied";
```

IV. PUBLIC KEY REPLACEMENT AND FORGERY ATTACK

❖ The proposed scheme avoids public key replacement and forgery.

❖ Public key of PKG can be replaced by attacker to make man in middle attack. But we are including both user id of the receiver and public key of the PKG so that both can be verified and it will avoid public key replacement attack.

Fig. 5. Database of identities



V. PKI vs. ID BASED APPROACH

Table I describes the key differences between ID based cryptography and PKI.

VI. CONCLUSION

ID based cryptosystem is mostly advantageous over traditional Public Key Infrastructure (PKI). ID based cryptosystem is used for key issuing to avoid problems of managing certificates in PKI. ID based signatures are more efficient as compared to PKI. PKI certificate is issued by CAs, whereas private key in ID based signature is generated by Private Key Generator (PKG). In PKI any user who wants to use a public key of receiver must verify its validity i.e. whether the certificate is valid or revoked. When many CAs are involved e.g. hierarchical PKI between two users [4], there must be trust relationship between them. It also suffers from key revocation and key management issues [2]. Key revocation requires storage and capacity is a big issue in PKI. Key management problem can be solved by ID based cryptography. But the disadvantage of this scheme is that signatures are more than twice as compared to the regular digital signature [10].

TABLE I.

KEY DIFFERENCES BETWEEN A CERTIFICATE BASED PKI AND AN ID BASED APPROACH

Basis	PKI	ID based approach
Private key generation	Either CA or Client itself	PKG
Public key generation	Either CA or Client itself	PKG
Key distribution		
Certification	Yes	No
Public key extraction	Yes	No
Key escrow problem	No	Yes
Key recovery	Must maintain key database	No key database is required
Scalability	Operational complexity	Yes
Server certificate	Yes	No server certificate requirement
Key Revocation	Online Certificate Status Protocol (OCSP),Certificate Revocation List (CRL)	No key revocation protocols required
Expensive	Expensive to deploy and run	No

Although ID based cryptography has advantage of public key management, it suffers from key escrow and identity revocation problems [3]. In this paper we have proposed Aadhar based ID based encryption scheme that does not suffer from inherent key escrow. Our proposed scheme eliminates key escrow by using online security server e.g. UIDAI server that provides privacy service to each user who receives key from PKG and simultaneously also supports fine grained revocation of identity.

REFERENCES

[1] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in Kilian, J. (eds) Advances in Cryptology - CRYPTO 2001. Lecture Notes in Comput. Sci., vol. 2139, Heidelberg : Springer, 2001, pp. 213-229. doi: 10.1007/3-540-44647-8_13

[2] C. Gentry, "Certificate-based encryption and the certificate revocation problem," in Biham, E. (ed.) EUROCRYPT 2003. Lecture Notes in Comput. Sci., vol. 2656, Heidelberg: Springer, 2003, pp. 272-293. doi: 10.1007/3-540-3920`0-9_17

[3] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in Laih, C.-S. (ed.) ASIACRYPT 2003. Lecture Notes in Comput. Sci., vol. 2894, Heidelberg: Springer, 2003, pp. 452-473. doi: : 10.1007/978-3-540-40061-5_29
[4] A. M. Al-Khouri, "PKI in government digital identity Manage. system," *Eur. J. of ePractice* , vol. 4, pp. 4-21, 2012.
[5] C. Youngblood, "An introduction to identity-based cryptography," *CSEP 590TU*, 2005.
[6] Ai-fen et al., "Separable and anonymous identity-based key issuing without secure channel," *Cryptology ePrint Archive, Rep.2004/322*, 2004. doi: 10.1007/11593980_22
[7] L. Chen, K. Harrison, D. Soldera, and N. P. Smart, "Appl. of multiple trust authorities in pairing based cryptoSyst.," in G. I. Davida, Y. Frankel, and O. Rees Eds. Infrastructure Soc., 2002. *Lecture Notes in Comput. Sci.*, vol. 2437, Heidelberg: Springer, 2002, pp. 260-275.
[8] A. R. Sattam and P. Kenneth, "Certificateless public key cryptography a full version", in Asiacrypt'03, *Lecture Notes in Comput. Sci. 2894*, vol. 20, no. 4, Heidelberg: Springer, pp. 452-473, 2003.
[9] L. Harn and J. Ren. "Efficient identity-based RSA multisignatures," *Comput. & Security*, vol. 27, no. 1, 2008, pp. 12-15. doi: https://doi.org/10.1016/j.cose.2008.03.003
[10] A. Jancic and M. J. Warren, "PKI-Advantages and obstacles", in *Proc. 2nd Australian Inform. Security Manage. Conf.: Securing the future*, Edith Cowan University, Perth, WA, 2004, pp. 1-9.
[11] Z. Cheng, R. Comley, and L. Vasiu, "Remove key escrow from the identity-based encryption system," *Found. of inform. technol. in the era of network and mobile computing*, 2004.
[12] B. Lee, C. Boyd, E. Dawson, K. Kim, J. Yang, and S. Yoo, "Secure key issuing in ID-based cryptography, in ACM 2nd Australasian Inform. Security Workshop, New Zealand, pp. 69-74, 2004.
[13] D. Raúl, H. Á. Fernando, H. E. Luis, and Q. D. Araceli, "A rev. of multisignatures based on RSA," 2010.
[14] A. Shamir. "Identity-based cryptoSyst. and signature schemes," In: G. R. Blakley, D. (eds) Chaum Advances in Cryptology. CRYPTO 1984. Lecture Notes in Comput. Sci., vol. 196. Springer, Berlin, Heidelberg Workshop on the Theory and Application of Cryptographic Techn. Springer: Heidelberg, 1985. doi: 10.1007/3-540-39568-7_5
[15] S. F. Al-Janabi and A. K. Obaid, "Develop. of Certificate Authority services for web appl.", Future Communication Networks (ICFCN), Int. Conf. on IEEE, 2012. doi: 10.1109/ICFCN.2012.6206857
[16] Z. Yu, "The scheme of public key infrastructure for improving wireless sensor networks security," Software Eng. and Service Sci. (ICSESS), *Proc. IEEE 3rd Int. Conf. on IEEE*, 2012. doi: 10.1109/ICSESS.2012.6269520
[17] J. Weise, "Public key infrastructure overview," Sun Blue Prints Online, August, 2001.
[18] J. Sayid, I. Sayid, and J. Kar, "Certificateless Public Key Cryptography: A Res. Survey," *Int. J. of Security and Its Appl.*, vol. 10, no. 7, pp. 103-118, 2016.
[19] M. C. Gorantla, R. Gangishetti, and A. Saxena. "A Survey on ID-Based Cryptographic Primitives." IACR Cryptology ePrint Archive 2005, p. 94, 2005.
[20] Kalyani, D., and R. Sridevi. "Survey on Identity based and Hierarchical Identity based Encryption Schemes." *Int. J. of Comput. Appl.* vol 134, no. 14, 2016.

About the Authors

Sarvesh Tanwar is a Research Scholar with Department of Computer Science & Engineering is College of Engineering & Technology (CET), Mody University of Science &Technology, Lakshmangarh (Rajasthan), India. She received her M.Tech Degree from Maharishi Markendeshwar University (MMU), Mullana with Distinction and is doing Ph.D from Mody University of Science &Technology (MUST), Lakshmangarh. Her research areas are Cryptography and Ad hoc networks. She has 11 years of teaching experience.

Dr. Anil Kumar is Professor and Head, Department of Computer Science & Engineering with College of Engineering & Technology (CET), Mody University of Science &Technology, Lakshmangarh (Rajasthan), India. His research areas are Network Security, Mobile Computing, and Big Data. He has published and presented 200 research papers in national and international journals and conferences. He has guided seven Ph. D. students and is guiding eight students at present. He is Senior Member, IEEE, ACM, and CSI. He has about 17 years of teaching and five years of industry experience.