I. J. Computer Network and Information Security, **2017, 8, 23-31**
Published Online August 2017 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2017.08.04

Mutual Authentication and Session Key Establishment for Secure Communication using Generalized Digital Certificate

Balaji V Durgawad
Department of Computer Engineering, Gramin Polytechnic, Vishnupuri, Nanded
E-mail: balajidurgawad007@gmail.com

Mohammed Aijaz Ahmed
Research Scholar, Department of Computer Science and Engineering, GITAM University, Vishakapatnam
E-mail: mohd_aijaz@yahoo.com

Dr. D. Rajya Lakshmi
Professor, University College of Engineering, Vizainagram, JNTU Kakinada
E-mail: rajyalakshmi.cse@jntukucev.ac.in

Dr. Sayed Abdul Sattar
Professor,Nawab Shah Alam Khan College of Engineering & Technology, JNTU Hyderabad
E-mail: syed49in@yahoo.com

Received: 16 April 2017; Accepted: 13 June 2017; Published: 08 August 2017

***Abstract*—**Public–key digital certificates are being used in public key infrastructure to provide authentication of the user's public key. Public key digital certificates like X.509 are used to bind a public key to its user. This kind of certificates cannot be used for user authentication. Such use may lead to forgery of user's identity. Lein et al proposed a authentication scheme based on Generalized Digital Certificates (GDC). A GDC consists of user's public information like digital birth certificate, digital identity, etc. and the digital signature of trusted third party generated from that public information. The GDC based scheme provides user authentication and allows for session key establishment. The scheme is secure against forgery of user's identity but it does not provide mutual authentication. The scheme proposed in this paper not only provides mutual authentication and session key but also it preserves the security strength of Lein et al's GDC based scheme.

***Index Terms*—**PKI, public key digital certificate, generalized digital certificate, identity forgery, authentication and session key.

I. INTRODUCTION

Public key digital certificate consists of a public key of certificate holder, name, period of validity, algorithm, etc. and digital signature generated for this public key [18]. The digital signature is generated by trusted third party normally certifying authority (CA). "X.509" is an example of public key digital certificate [1]. In PKI X.509 certificate is widely used to provide authentication of Certificate holder's public key. If a certificate holder proves that he has knowledge of the private key associated with the public key specified in the X.509 digital certificate the certificate holder is authenticated otherwise not.

But there is a security flaw identified in this mechanism. As all fields present in public key digital certificate are public, if a malicious receiver obtains public key digital certificate, then he can forge the identity of the certificate holder. If a certificate holder H needs to send a message M to J, then H will create a message M and put his digital signature $SIGN_H$ on it using private key PR_H and encrypts it by using the public key PU_J and then forwards this digitally signed and encrypted message to J. J will decrypt it using J's private key PR_J. Then J will verify the digital signature $SIGN_H$ of certificate holder H. For this J needs a public key PU_H of H which is obtained from public key digital certificate of H. If the digital signature $SIGN_H$ of H verified correctly, then J comes to know that the message received is really coming from H. If receiver J is not trustworthy, then he can encrypt the digitally signed message by H using public key PU_X of other user X and forwards this message to X. Then X will decrypt it using its private key PR_X. X finds a digital signature $SIGN_H$ and needs to verify the digital signature $SIGN_H$ of certificate holder H. For this J needs a public key PU_H of H which is obtained from public key digital certificate of H. If the digital signature $SIGN_H$ of H verified correctly, then X comes to know that the message received is really coming from H. But it is not true. Thus the identity of certificate holder H is forged by malicious receiver J. The certificate holder H has no complete control over his signature and privacy of certificate holder is not achieved. It is clear that public key digital certificates cannot be used for authenticating certificate holder. This issue is addressed Generalized Digital Certificate (GDC) based scheme [2].

Generalized digital certificates are used to authenticate the certificate holder and establish a secret session key at each end of communication using any type of digitized general certificate like digital unique identity certificate, digital passport, digital school certificate, etc. A GDC consists of general and public information of the certificate holder and digital signature of this public information generated by certifying authority. GDC is never sent to the receiver and the signature of GDC will not be sent to the receiver in plain text. Rather GDC holder will have to respond to the challenge sent by the receiver.

In the GDC based scheme [2], only GDC holder is verified and a secret session key gets established upon successful authentication for subsequent communication. But there is no provision for sender to check the authenticity of the verifier. The proposed scheme described in this paper uses the concept of GDC and achieves mutual authentication along with session key establishment.

Digital Certificate application involves following three entities.

i. *Certifying Authority (CA):* is a third party which can be trusted by all others. CA can be an organization or a person who can create a digital signature using its private key PR_{CA}. The X.509 public key digital certificate contains the public key of the certificate holder and digital signature of CA for this public key. The GDC consist of public information of certificate holder in the general form of certificate like digital unique identity certificate, digital passport, digital school certificate etc. and digital signature of CA for this public information. But there will be no public key present in GDC.

ii. *GDC-Owner:* is a person who receives the GDC for his public information from a trusted CA through a secure communication. In order to get authenticated and establish a secret session key this GDC-Owner needs to present a valid response to the challenge generated by GDC-verifier.

iii. *GDC-Verifier:* is a person with whom GDC-Owner wishes to establish a secure communication. GDC-Verifier sends a challenge to the GDC-Owner and verifies the response using received public information from GDC-Owner and public key of the CA.

The entire GDC is never sent to the GDC-Verifier instead the GDC-Owner will simply send the public information for which he or she obtained the digital signature from the CA. The digital signatures of GDC need not to be sent to the GDC-Verifier. The digital signature becomes a security factor on the basis of which user can be authenticated [2].

The rest of the paper is organized as follows. In section II an overview of the related work is given. Section III consists of proposed DL-based scheme and its security analysis. In Section IV the proposed IF-based protocol and its security analysis is discussed. Section V consists of the conclusion which is followed by references.

II. Related Work

Authentication is one of the most important services of security. Managing a key is also an important aspect of establishing a secure communication. A number of efforts have been taken to improve these services. Most of the techniques make use of public key digital certificates.

A receiver can validate the authenticity of a received message by validating the digital signature of the receiver. For this purpose Public key digital certificates are used. But this scheme may violate the privacy of a signer if receiver decides as explained previously.

Efforts have been taken for solving this issue with the introduction of signature scheme that will not depend on digital certificates for the verification of signatures [10], [11], [12], [13], [14]. In [15] concept of signatures that do not require certificates are proposed which uses benefits of ID based cryptography and it can be widely used in applications where there is less bandwidth like wireless applications [16]. This scheme has a drawback of the key escrow problem.

Another attempt was made to solve the issue of privacy violation in [8] with the help of Identity based cryptography in which identity of user like name or email address will be used as a public key. But it is limited to the situation in which user knows the identity of his communication partner.

Introduction of Generalized digital certificate [2] solves the problem of violation of user’s privacy. It is used to authenticate the certificate owner and establish a session key with communication partner. Generalized digital certificate consist of public information like digital birth certificate, school certificate, identity etc. of GDC-owner. The Generalized digital certificate is used to authenticate the GDC-owner by using challenge and response mechanism in which information of digital signature will be passed as a secret token. Generalized digital certificates provide only one way authentication. Both communication partners can’t be authenticated at once. If we authenticate a GDC-owner and after successful authentication if the same procedure is used by the user at the other end, then for his successful authentication it will take again four steps of the protocol described in [2]. For this step of the protocol in [2] will be doubled. At the end there will be two session keys.

Attempts have been taken in improving the Generalized Digital Certificate based communication [4-6]. In [4] there is improvement in strengthening session key created for each message being exchanged. It treats the session key as a key1. Key1 will be used to send a message first time only. For the second time key2 will be obtained as

Key2= key1 XOR M1
Key3= key2 XOR M2

This will be continued until the session expires. But this scheme also works to achieve one way authentication.

In [5] data security is increased by use of AES. It is also based on one way authentication. Similar kind of work is found in [6] with an additional security feature but it is again based on one way authentication.

The proposed work consists modifications to Lein et al's Discrete log based scheme (DL-based scheme) and Integer Factorization based scheme (IF-based scheme) in order to provide mutual authentication and subsequent session key establishment.

III. DL-Based Scheme

In day to day life individuals are identified on the basis of ID-card issued by a trusted authority. The ID-card consists of name, date of birth, address etc. and photograph. The authority put a stamp and signature on photograph and ID-card. If a person produces an ID-card and matches with the photo on the card, then he or she is successfully identified. In this scheme, it is very difficult to forge signatures. So owning an ID-card (paper certificate) is the key factor in the process of identification.

The schemes described in this paper introduce a similar approach for identification of both individuals (one who is being verified and the other who is verifying). In the digital world, both individuals one who is being verified and other who is verifying present at far ends so authentication of both parties becomes important. In this new scheme, there is no need to transfer entire GDC to each other for authentication of each other rather a valid response to received challenge needs to be generated. Finally, on successful authentication of both individuals a secret session key is generated.

Like GDC the proposed protocol is based on the combination of traditional discrete log based ElGamal digital signature [3] and the famous Diffie-Hellman Assumption [9].

A. *ElGamal Digital Signature*

In the ElGamal scheme [3] a large prime number Q and its primitive root α is supposed to be shared by all the users [20]. The signer selects at random a private key X such that $X \in [1, Q-2]$ and computes corresponding public key $y = \alpha^X \ mod\ Q$.

The signer then selects a random secrete k excluding 1 and Q-1 such that $k \in Z_Q^*$ and computes $R1 = \alpha^k \ mod\ Q$ [19]. Then S1 is solved by using the signer's secrete X, and k, as

$$S1 = K^{-1}\big(D - (R1 * X)\big) mod\, (Q-1) \qquad (1)$$

Where D represents the message digest of the message Msg. The digital signature of the message Msg is defined as a pair (R1, S1). The signature is verified by checking whether "(2)" holds true.

$$\alpha^D = Y^{R1} * R1^{S1} mod Q \qquad (2)$$

The parameter R1 is computed offline which depends on random integer k. It is independent of the message Msg. So there will be no harm in making it public, but the parameter S1 depends on the user's statement Msg. So S1 should be kept secret. There are a number of variants of ElGamal Signature [17].

B. *Diffie-Hellman Assumption*

Assume U and V have their private keys X_U and X_V. Their corresponding public keys are $Y_U = \alpha^{X_U} mod\ Q$ and, $Y_V = \alpha^{X_V} mod\ Q$ respectively, where Q is a large prime number and α is its primitive root such that $\alpha \in Z_n^*$ of order Q. Only U and V can compute a shared secret key as DL-Based protocol for Authentication of the user and Establishment of Key

$$K_{U,V} = Y_U{}^{X_U} modQ = Y_V{}^{X_V} modQ = K_{V,U} \qquad (3)$$

Diffie-Hellman Assumption refers to the assumption that is computation of key $K_{U,\ V}$ from public key Y_U or Y_V, without knowledge of corresponding X_U or X_V is computationally infeasible. However, solving the private key X_U or X_V from the corresponding Y_U or Y_V is equivalent to solving the discrete logarithm problem.

C. *Review of DL-based Authentication and Key Establishment*

The scheme consists of two phases [2]:

i. *Registration at Certificate Authority:* Let O and V are the GDC-owner and GDC-Verifier. In order to get Authenticated O needs to be registered at Certifying Authority. O will send his public information M_O like digital identity to the Certifying Authority and as a result O will receive a Generalized Digital Certificate having digital signature of Authority. Digital signature consists of a pair ($R1_O$, $S1_O$) created by using ElGamal digital signature and private key of certificate Authority. As stated earlier R1 is made public, but S1 depends on public information M_O. So it must be kept secret during and after the process of authentication. The protocol for authenticating and establishing a key is as described below.
ii. *Authentication and Key Establishment Protocol:* The protocol takes four steps to complete described as follows:

Step 1:

The user O needs to compute secrete token from digital signature of receiving Generalized Digital Certificate. It is calculated as below

$$\$_O = R1_O{}^{S1_O} \; mod \; Q \qquad (4)$$

User O passes his public information M_O and pair ($R1_O$, $\$_O$) to the GDC-verifier V

Step 2:

After receiving these, verifier needs to verify whether the token received $\$_O$ is really generated from the digital signature of Generalized Digital Certificate of O. This can be done by checking whether the following "(5)" holds true.

$$\alpha^{D_O} = Y^{R1_O} * \$_O \; mod \; Q \qquad (5)$$

Where Y is the public key of the certificate authority. If inequality 5 doesn't satisfy then authentication will fail and protocol stops otherwise V will select a random integer Z_V such that $Z_V \in [1, Q-2]$ and computes a challenge $CH_V = R1_O{}^{Z_V} \; mod \; Q$ and sends CH_V to the user O.

Step 3:

The user O uses secret S1 and computes Diffie-Hellman Key $K_{O,V} = CH_V{}^{S1_O} mod \; Q$ and obtains$K'_{O,V} = D(K_{O,V})$, where $D(K_{O,V})$ represents a key derivation procedure with $K_{O,V}$ as an input. O selects a random integer Z_O such that $Z_O \in [1, Q-2]$ and computes a challenge $CH_O = R1_O{}^{Z_O} \; mod \; Q$ and computes $ACK = h(K'_{O,V}, CH_V || CH_O)$, where $h(K'_{O,V}, CH_V || CH_O)$ represents a one way keyed hash function with $K'_{O,V}$ as an input key. The user O then sends CH_O and ACK.

Step 4:

User V will receive CH_O and ACK. User V uses his secrete Z_V and computes Diffie-Hellman Key $K_{V,O} = \$_O^{Z_V} \; mod \; Q$ and obtains $K'_{O,V} = D(K_{O,V})$, and checks whether $ACK = h(K'_{V,O}, CH_V || CH_O)$ is true. If this satisfies then GDC-owner O is successfully authenticated by GDC-verifier V. Otherwise, authentication fails, and protocol stops. On successful authentication a session key is created.

$$S_K = CH_O{}^{Z_V} modQ = CH_V{}^{Z_O} modQ \qquad (6)$$

D. Proposed Dl-Based Scehme

The proposed DL-based scheme provides mutual authentication on the basis of their public information like digital driving license, digital passport, or any digital identity. The proposed scheme consists of two phases:

- Registration at Certificate Authority
- Mutual Authentication and Key Establishment

This new scheme is based on discrete logarithm [7]. Solving the problem of discrete logarithm is computationally infeasible.

Select a large prime Q such that Q-1/2 is also a prime number [21]. Find its primitive root α. Prime number Q and α is supposed to be shared by all.

i. Registration At Certificate Authority

Initially, both users need to be registered at certificate authority. Certificate Authority will produce Generalized Digital Certificate for the received public information $M_{O,}$ and M_V of user O and V respectively. O receives a signature pair ($R1_{O,}$ $S1_O$) and V receives a signature pair ($R1_{V,}$ $S1_V$) for their public information $M_{O,}$ and $M_{V.}$ The values $S1_{O,}$ $S1_V$ depends on public information so need to be kept secret.

ii. Mutual Authentication and Key Establishment phase

Authentication and key establishment protocol take five steps as shown below.

Step 1:

The user O needs to compute secrete token from digital signature of receiving Generalized Digital Certificate.

$$\$_O = R1_O{}^{S1_O} \; mod \; Q \qquad (7)$$

User O passes his public information M'_O and pair ($R1_O$, $\$_O$) to the GDC-verifier V.

The user V also computes his secret token from the information received during registration.

$$\$_V = (R1_V)^{S1_V} mod \; Q$$

Step 2:

The verifier needs to verify whether the token received $\$_O$ is really generated from the digital signature of Generalized Digital Certificate of O. This can be done by checking whether "(8)" holds true.

$$\alpha^{D_O} = Y^{\, R1_O} * \$_O \; mod \; Q \qquad (8)$$

Where Y is the public key of the certificate authority. If inequality (8) doesn't satisfy then authentication fails and protocol stops otherwise V selects a random integer Z_V such that $Z_V \in [1, Q-2]$ and computes a challenge

$$C_V = R1_O{}^{Z_V} \; mod \; Q. \qquad (9)$$

User V sends C_V, M'_V, ($R1_V$, $\$_V$) to O.

Step 3:

User O checks the validity of receiving credentials. This can be done through "(10)".

$$\alpha^{D_V} = Y^{\, R1_V} * \$_V \; mod \; Q \qquad (10)$$

Where Y is the public key of the certificate authority. If inequality (11) doesn't satisfy then authentication of V fails and protocol stops otherwise the user O randomly selects $Z_O \in [1, Q-2\,]$ and computes

$$C_O = (R1_O)^{Z_O} \, mod \, Q \quad (11)$$

$$CH_O = (R1_V)^{Z_O} \, mod \, Q. \quad (12)$$

User O uses secret $S1_O$ and computes Symmetric key using DHA

$$K_{O,V} = CH_V{}^{S1_O} mod \, Q = R1_V{}^{Z_V S1_O S1_V} \, mod \, Q \quad (13)$$

User O obtains, $K'_{O,V} = D(K_{O,V})$ where $D(K_{O,V})$ represents a key derivation procedure with $K_{O,V}$ as an input. O computes acknowledgement using

$$ACK = h\,(K'_{O,\,V},\, C_V \| C_O). \quad (14)$$

O sends an ACK, C_O, and CH_O to V

Step 4:

V computes symmetric key using DHA $K_{V,O} = \$_O{}^{Z_V} \, mod \, Q$ and obtains $K'_{V,O} = D(K_{V,O})$, where $D(K_{V,O})$ represents a key derivation procedure. Owner O is authenticated if

$$ACK = h(K'_{V,O},\, C_V \| C_O) \quad (15)$$

Otherwise, the authentication fails and protocol exits. V computes a key

$$K_{V,O1} = CH_O{}^{S1_V} \, mod \, Q \quad (16)$$

Obtain*s* $K'_{V,O1} = D(K_{V,O1})$. Comput**e** a new ACK1, $ACK1 = h(K'_{V,O1}\,,\, CH_V \| CH_O \| K_{V,O})$ V sends $ACK1,\, CH_V$ to O.

Step 5:

User O computes $K_{O,V1} = \$_V{}^{Z_O} \, mod \, Q$ and O derives another symmetric key $K'_{O,V1} = D(K_{O,V1})$ which is used to compute $ACK1$ which is used to authenticate V using "(17)".

$$ACK1 = h(K'_{O,V1},\, C_V \| C_O \| K_{O,V}) \quad (17)$$

O creates a session key

$$S_K = (C_V)^{Z_O} mod \, Q = (R1_O)^{Z_O Z_V} \, mod \, Q \quad (18)$$

Otherwise, the authentication fails and protocol exits. Meanwhile, user V creates session key

$$S_K = (C_O)^{Z_V} mod \, Q = (R1_O)^{Z_O Z_V} \, mod \, Q$$

Where S_K is a shared session key between O and V. In order to get authenticated successfully each user needs to compute the secret token and send public information along with a pair ($R1_X$, $\$_X$) to each other. The validity of the digital signature will be checked with the help of "(2)". In which $R1^{S1}$ is replaced by secrete token of another user. As every term in "(2)" is public, anyone can validate it, but for successful authentication of user received ACK and computed ACK must match each other and this is possible if and only if ACK is generated by genuine user who have authentic Generalized Digital Certificate because ACK is computed by using a key $K'_{V,O}$ and $K'_{O,V}$ which requires secret $S1_V$ and secret $S1_O$ respectively. And only GDC-Holder can compute session key as security provided by Diffie-Hellman. In this way both parties can authenticate each other.

If a malicious user somehow manages to obtain the public information of V then there is no possibility of forgery attack on the identity of V because V sends challenge in step 2 which is obtained from the use of secret parameters of digital signature of the generalized digital certificate. And computation of secret $S1_V$ from $\$_V$ is a discrete logarithmic problem which is infeasible. Also, the computation of session key requires the use of secret parameter S1 of public information M_V and this is possible for only genuine user V who owned generalized digital certificate for his public information M_V from certificate user.

E. Security Analysis Of Proposed Dl-Based Scehme

The security analysis of the newly introduced scheme is described in this section. The proposed scheme depends on Diffie-Hellman in combination with ElGamal digital signature. The security of his scheme depends on the security of Diffie-Hellman and security of ElGamal scheme. The proposed protocol satisfies the property of unforgeability, one-wayness, and non-transferability.

a) *Unforgeability:* User who knows the digital signature of Generalized Digital Certificate can generate a valid response only. In order to perform a forgery attack, an attacker needs to compute ($R1_X$, $\$_X$). If somehow attacker manages to get this pair and his digital signature gets validated by using "(8)" or "(10)". This is possible because all values are public in these equations, attackers need to find out the secrete power S1 of from token \$. This is infeasible because of the security provided by discrete logarithm. Then in order to get successfully authenticated attacker needs to present a valid ACK which is infeasible. Only GDC-Holder can obtain the secret parameter S1 from certificate authority which is kept as a secret. Thus UNFORGEABILITY is achieved through the security of Diffie-Hellman in combination with ElGamal digital signature. In this way, the new proposed scheme is secure against Forgery attacks.

b) *One-wayness:* Based on the interactions nobody can derive the digital signature of the certificate. The digital signature of the generalized digital certificate consists of a pair (R1, S1). GDC-Holder is not sending the generalized digital certificate to anybody, S1 will be secure. Instead of sending secret parameter token generated from secret parameter is passed. The computation of secret parameter S1 from \$ is infeasible because this is equal to solve problem of discrete logarithm and which is infeasible. If attacker can't obtain secret parameter S1 then he can’t respond with correct ACK and protocol stops. In this way the proposed protocol satisfies the property of one-wayness.

c) *Non-transferability:* A response produced for one GDC-Verifier should not be transferred in response to the other GDC-Verifier. Because this will lead to the impersonation of a user. Because of Diffie-Hellman a valid response ACK is generated by GDC-Holder, who knows secrete parameter s1 or by a user who knows the random secret of random challenge. As the user selects a random challenge each time, the response validity is for only one session.

GDC-Holder is not sending the generalized digital certificate to anybody its digital signature will be safe and nobody can transfer complete generalized digital certificate to any other user. In this protocol, there is no problem of privacy intrusion. Therefore a valid response ACK cannot be passed into other GDC-Verifiers challenge.

Step	USER O	USER V
1	Creates a Secret Token $\$_O = (R1_O)^{S1_O} mod\ Q$ M'_O and pair $(R1_O, S1_O)$ $\longrightarrow$	Creates a Secret Token $\$_V = (R1_V)^{S1_V} mod\ Q$
2	$\longleftarrow$	$IF\ \alpha^{D_O} \neq Y^{R1_O} * \$_O\ mod\ Q$ Then authentication fails and protocol terminates, otherwise Verifier randomly selects Z_V such that $Z_V \in [1, Q-2]$ and computes $C_V = (R1_O)^{Z_V} mod\ Q$ C_V, M'_V, pair $(R1_V, \$_V)$
3	$IF\ \alpha^{D_V} \neq Y^{R1_V} * \$_V\ mod\ Q$ Then authentication fails and protocol terminates, Otherwise, O randomly selects $Z_O \in [1, Q-2]$ compute $C_O = (R1_O)^{Z_O}\ mod\ Q$ and $CH_O = (R1_V)^{Z_O}\ mod\ Q$ computes $K_{O,V} = C_V{}^{S1_O}\ mod\ Q$ and obtains $K'_{O,V} = D(K_{O,V})$ computes $ACK = h(K'_{O,V}, C_V \Vert C_O)$ ACK, C_O, CH_O $\longrightarrow$	
4	$\longleftarrow$	computes $K_{V,O} = \$_O{}^{Z_V} mod\ Q$ and obtains $K'_{V,O} = D(K_{V,O})$ IF $ACK = h(K'_{V,O}, C_V \Vert C_O)$ then owner O is Authenticated and computes $K_{V,O1} = CH_O{}^{S1_V}\ mod\ Q$, obtain $K'_{V,O1} = D(K_{V,O1})$ Compute $ACK1 = h(K'_{V,O1}, CH_V \Vert CH_O \Vert K_{V,O})$ Otherwise, the Authentication fails and protocol terminates $ACK1$
5	computes $K_{O,V1} = \$_V{}^{Z_O} mod\ Q$ and obtains $K'_{O,V1} = D(K_{O,V1})$ If $ACK1 = h(K'_{O,V1}, C_V \Vert C_O \Vert K_{O,V})$ then V is Authenticated and Creates a session key $S_K = (C_V)^{Z_O} mod\ Q$ $S_K = (R1_O)^{Z_O Z_V}\ mod\ Q$ $S_K = (C_O)^{Z_V} mod\ Q = (R1_O)^{Z_O Z_V}\ mod\ Q$ Otherwise, the Authentication fails and protocol terminates	

Fig.1. DL-based Mutual Authentication and Key Establishment Protocol

IV. IF-BASED SCHME

This section describes a mutual authentication protocol which is based on the trapdoor hash based online- offline signature scheme and Diffie-Hellman assumption generalized modulo composite number (GDHA) [2], [22-23]. The online-offline scheme makes use of the trapdoor hash function that satisfies the property of unforgeability, one-wayness and Non Transferability.

A. Review of IF-based User Authentication And Key Establishment

The protocol consists of two phases [2]:

i. Registration At Certificate Authority
ii. Authentication and Key Establishment

i. Registration at CA:

Certificate owner O sends his public information for registration to the certificate authority (CA). CA creates a GDC by putting his signature, which will be converted into the online-offline signature of the public information received. The CA sends GDC consisting of online-offline signature defined by

$$Sig_{sign\_key}\left(hash_{hash\_key}(M', R')\right), SEC,\ hash_{hash\_key}(M', R')$$

The owner is required to keep the SEC secret from others. For verification owner sends a secret token computed from secret parameter SEC.

ii. Authentication and key establishment protocol

Step 1:

The user O needs to compute secrete token from digital signature of receiving Generalized Digital Certificate. It is calculated as $\$_O = g_O{}^{SEC_O}\ mod\ n$

User O passes his public information M_O and $Sig_{Sign\_key}\left(hash_{hash\_key}(M', R')\right), \$_O,\ hash_{hash\_key}(M', R')$ to the GDC-verifier V

Step 2:

After receiving these, verifier needs to check the authenticity of the received token and information Initially, V checks the validity of the digital signature of

CA received by owner O. Verify $Sig_{sign\_key}\left(hash_{hash\_key}(M',R')\right)$ using Sig_{verify_key} of CA, if it is verified then V check the

$$hash_{hash\_key}(M_O,R_O) = hash_{hash\_key}(M'_O,R'_O) \quad (19)$$

If above inequality doesn't satisfy then authentication fails and protocol stops otherwise V will select a random integer Z$_V$ such that $Z_V \in [1,N-1]$ and computes a challenge $CH_V = {g_O}^{Z_V} \; mod \; N$ and sends CH_V to O.

Step 3:

The user O uses secret SEC and computes Diffie-Hellman Key $K_{O,V} = {CH_V}^{SEC_O} mod \; N$ and obtains $K'_{O,V} = D(K_{O,V})$, where $D(K_{O,V})$ represents a key derivation procedure with $K_{O,V}$ as an input. O selects a random integer Z$_O$ such that $Z_O \in [1,N-1]$ and computes a challenge $CH_O = {g_O}^{Z_O} \; mod \; N$ and computes $ACK = h(K'_{O,V}, CH_V || CH_O)$, where $h(K'_{O,V}, CH_V || CH_O)$ represents a one way keyed hash function with $K'_{O,V}$ as an input key. The user O then sends CH_O and ACK.

Step 4:

V will receive CH_O and ACK. V uses his secret Z_V and computes Diffie-Hellman Key $K_{V,O} = \$_O^{Z_V} mod \; N$ and obtains $K'_{O,V} = D(K_{O,V})$, and checks whether

$$ACK = h(K'_{V,O}, CH_V || CH_O) \quad (20)$$

If this satisfies then GDC-owner O is successfully authenticated by GDC-verifier V. Otherwise, authentication fails, and protocol stops. On successful authentication a session key is created.

$$S_K = {CH_O}^{Z_V} mod \; N = {CH_V}^{Z_O} \; mod \; N \quad (21)$$

B. Proposed IF-based Scheme

The new scheme consists of two phases:

i. Registration at CA:

Initially, both users need to be registered at certificate authority. CA will produce Generalized Digital Certificate for the received public information M_O , and M_V of user O and V respectively. O and V receive GDC having digital signature of the CA described as

$$Sig_{sign\_key}\left(hash_{hash\_key}(M',R')\right), SEC_O, hash_{hash\_key}(M',R')$$

and

$$Sig_{sign\_key}\left(hash_{hash\_key}(M',R')\right), SEC_V, hash_{hash\_key}(M',R')$$

respectively. The value SEC_O, SEC_V depends on public information so need to be kept secret.

ii. Mutual Authentication and key establishment protocol

Figure 2 shows the mutual authentication protocol for user authentication and key establishment.

Step 1:

The user O needs to compute secrete token from digital signature of receiving Generalized Digital Certificate. It is calculated as $\$_O = {g_O}^{SEC_O} \; mod \; n$ User O sends his public information M$_O$ and

$$Sig_{sign\_key}\left(hash_{hash\_key}(M',R')\right), \$_O, \; hash_{hash\_key}(M',R')$$

To the GDC-verifier V.

User V also uses his information received from the CA during the registration phase and computes his secret token $\$_V$, such that $\$_V = (g_O)^{SEC_V} mod \; N$

Step 2:

After receiving these, verifier needs to check the authenticity of the received token and information. Initially, V checks the validity of the digital signature of CA received by owner O. Verify $Sig_{sign\_key}\left(hash_{hash\_key}(M',R')\right)$ using Sig_{verify_key} of CA, if it is verified then V check the $hash_{hash\_key}(M_O,R_O) = hash_{hash\_key}(M'_O,R'_O)$

If above inequality doesn't satisfy then authentication fails and protocol stops, otherwise V selects a random integer Z$_V$ such that $Z_V \in [1,N-1]$ and computes $CH_V = {g_O}^{Z_V} \; mod \; N$ V sends to O challenge CH_V and

$$CH_V, M_V, Sig_{sign\_key}\left(hash_{hash\_key}(M',R')\right), \$_O, \; hash_{hash\_key}(M',R')$$

Step 3:

The user O uses secret SEC and computes symmetric key using GDHA $K_{O,V} = {CH_V}^{SEC_O} mod \; N$ and obtains $K'_{O,V} = D(K_{O,V})$, where $D(K_{O,V})$ represents a key derivation procedure with $K_{O,V}$ as an input. O selects a random integer Z$_O$ such that $Z_O \in [1,N-1]$ and computes a challenge $CH_O = {g_O}^{Z_O} \; mod \; N$ and computes $ACK = h(K'_{O,V}, CH_V || CH_O)$, where $h(K'_{O,V}, CH_V || CH_O)$ represents a one way keyed hash function with $K'_{O,V}$ as an input key. The user O then sends CH_O and ACK.

Step 4:

V will receive CH_O and ACK. User V uses his secret Z_V and computes symmetric Key $K_{V,O} = \$_O^{Z_V} mod \; N$ and obtains $K'_{O,V} = D(K_{O,V})$, and checks

$$ACK = h(K'_{V,O}, CH_V || CH_O) \quad (22)$$

Step	USER O	USER V
1	Creates a Secret Token $\$_O = (g_O)^{SEC_O} mod\ N$ $Sig_{sign\_key}\left(hash_{hash\_key}(M',R')\right), \$_O, hash_{hash\_key}(M',R')$, M_O →	Creates a Secret Token $\$_V = (g_O)^{SEC_V} mod\ N$
2	← $M_V, Sig_{sign\_key}\left(hash_{hash\_key}(M',R')\right), \$_O, hash_{hash\_key}(M',R')$	Verify signature $Sig_{sign\_key}\left(hash_{hash\_key}(M',R')\right)$ and $hash_{hash\_key}(M_O,R_O) = hash_{hash\_key}(M'_O,R'_O)$ If authentication fails then the protocol terminates, otherwise Verifier randomly selects Z_V such that $Z_V \in [1, N-1]$ and computes $CH_V = g_O{}^{Z_V} mod\ N$
3	Verify signature $Sig_{sign\_key}\left(hash_{hash\_key}(M',R')\right)$ and $hash_{hash\_key}(M_O,R_O) = hash_{hash\_key}(M'_V,R'_V)$ If authentication fails then the protocol terminates, otherwise user O randomly selects Z_O such that $Z_O \in [1, N-1]$ and computes $CH_O = g_O{}^{Z_O} mod\ N$ and computes $K_{O,V} = CH_V{}^{SEC_O} mod\ N$ and obtains $K'_{O,V} = D(K_{O,V})$, computes $ACK = h(K'_{O,V}, CH_V \|\| CH_O)$ CH_O and ACK →	
4	← $ACK1$	computes $K_{V,A} = \$_O{}^{Z_V} mod\ N$ and obtains $K'_{V,O} = D(K_{V,O})$ IF $ACK = h(K'_{V,O}, CH_V \|\| CH_O)$ then O is Authenticated and computes $K_{V,A,1} = CH_O{}^{SEC_V} mod\ N$ and obtains $K'_{V,O1} = D(K_{V,O1})$ and Computes $ACK1 = h(K'_{V,O1}, K_{V,O1} \|\| K_{V,O})$ and sends ACK1 to the O
5	computes $K_{O,V1} = \$_V{}^{Z_O} mod\ N$ and obtains $K'_{O,V1} = D(K_{O,V1})$ IF $ACK1 = h(K'_{O,V1}, K_{O,V1} \|\| K_{O,V})$ then V is Authenticated and Creates a session key $S_K = (CH_V)^{Z_O} mod\ N = (g_O)^{Z_O Z_V} mod\ N$ $S_K = (CH_O)^{Z_V} mod\ N = (g_O)^{Z_O Z_V} mod\ N$ Otherwise, the Authentication fails	

Fig.2. IF-based Mutual Authentication and Key Establishment Protocol

If this satisfies then GDC-owner O is successfully authenticated by GDC-verifier V. Otherwise, authentication fails, and protocol stops. V again computes a new asymmetric key $K_{V,A,1} = CH_O{}^{SEC_V} mod\ N$ and obtains $K'_{V,O1} = D(K_{V,O1})$ Computes and sends ACK1 to O

$$ACK1 = h(K'_{V,O1}, K_{V,O1} \| K_{V,O}) \tag{23}$$

Step 5:

To check the authenticity of the received information the owner needs to derive a symmetric key which is obtained as $K_{O,V1} = \$_V{}^{Z_O} mod\ N$ and obtains $K'_{O,V1} = D(K_{O,V1})$ Create $h(K'_{O,V1}, K_{O,V1} \| K_{O,V})$ and compare it with $ACK1$ If it matches, and then V is authenticated and creates a session key

$$S_K = (CH_V)^{Z_O} mod\ N = (g_O)^{Z_O Z_V} mod\ N \tag{24}$$

Otherwise, the Authentication fails and the protocol terminates. Meanwhile V creates a session key

$$S_K = CH_O{}^{Z_V} mod\ N = CH_V{}^{Z_O} mod\ N \tag{25}$$

C. Security Analysis of Proposed IF-Based Scheme

The IF-based protocol makes use of the GDHA, RSA signature, and online-offline signature based on the hash function. So the security of the scheme depends on the security of the GDHA, RSA signature and online-offline signature scheme. Similar to the security analysis given in section III E for the DL-based protocol, the IF-based scheme also satisfies the property of unforgeability, one-wayness and non transferability.

V. Conclusion

Public key digital certificates are used for authenticity of public key of a user but it cannot be used for user authentication. Lein et al proposed generalized digital certificates based scheme which can be used to authenticate a user and establish session keys for secure communication. But it does not provide mutual authentication which is essential for many applications. The proposed work consists of modifications to DL-based and IF-based schemes. The proposed schemes not only achieve mutual authentication but also preserves the security strength of the original schemes.

References

[1] Network Working Group, “Internet X.509 public key infrastructure certificate and crl profile, RFC: 2459," Jan. 1999.

[2] LeinHarn and JianRen, “Generalized Digital Certificate For User Authentication And Key establishment for secure communication,” *IEEE Trans. on wireless communication,vol.,10,No.7,July2011.*

[3] T. A. ElGamal, “A public-key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. Inf. Theory, vol. 31, no. 4,pp. 469-472, 1985.*

[4] Bismin.V.Sherif and Andrews Jose, “Secure Communication using generalized Digital Certificate”, International Journal of Computer Applications Technology and Research, Volume 2-Issue 4,396- 399, 2013.

[5] M.V.Kishore, G.Pandit Samuel, N.AdityaSundar, M.Enayath Ali, Y.LalithaVarma “A Novel Methodology for Secure Communications and Prevention of Forgery Attacks,” *International Journal of Computer Applications (0975 – 8887) Volume 96– No.22, June 2014.*

[6] SharinaToor, KesavaRaoSeerapu, Y.Rameshkumar, “A

Novel Secured Data Communication and Prevention of Forgery Attacks Using Digital Certificates,” *international Journal of Computer Science and Information Technologies, Vol. 5 (5), 2014, 6410-6415.*

[7] en.wikipedia.org/wiki/Discrete-logarithm

[8] A. Shamir, “Identity-based cryptosystems and signature schemes," in *Advances in Cryptology: Proc. Crypto’84, Lecture Notes in Computer* Science vol. 196, (Berlin), pp. 47-53, Springer-Verlag, 1985.

[9] W. Diffle and M. E. Hellman, “New directions in cryptography," *IEEE Trans.Inf. Theory*, vol. 22, pp. 644-654, 1976.

[10] W. Diffle and M. E. Hellman, “New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. 22, pp. 644-654, 1976.

[11] M. Jakobsson, K. Sako, and R. Impagliazzo, “Designated verifier proofs and their applications," *Advances in Cryptology - EUROCRYPT*, pp. 143-154, 1996. LNCS Vol 1070.

[12] C. Schnorr, “Efficient signature generation by smart cards," *J. Cryptology*, vol. 4, no. 3, pp. 161-174, 1991.

[13] F. Laguillaumie and D. Vergnaud, “Designated verifier signatures: anonymity and efficient construction from any bilinear map." *IACR eprint.*

[14] R. Steinfeld, L. Bull, H. Wang, and J. Pieprzyk, “Universal designated verifier signatures," in *Asiacrypt’03*, vol. LNCS 2894, pp. 523-542, 2003.

[15] L. Harn, J. Ren, and C. Lin, “Design of DL-based certificateless digitalsignatures," *J. Syst. Software*, vol. 82, pp. 789-793, 2009.

[16] Al-Riyami, S., Paterson, K, “Certificateless public key cryptography,”Advancesin Cryptology – AsiaCrypt, LNCS, vol. 2894. Springer-Verlag, pp. 452–473, 2003.

[17] L. Harn and Y. Xu,“Design of Generalized ElGamal type digital Signature scheme based on discrete Logarithm," ELECTRONICS LETTERS, vol. 30 , no. 24, 1994,2025-2026.

[18] Rivest R. L.Shamir A. and Adelman L, “A Method for obtaining digital signatures and public key cryptosystems,"*commun. SCM, 1978, 21, (2), pp.120-126.*

[19] R. Lidl and H. Niederreiter, *Finite Fields.* Cambridge University Press, 2000.

[20] Rashmi singh, shiv kumar “Elgamal‟s Algorithm in Cryptography” International Journal of Scientific & Engineering Research Volume 3, Issue 12, December-2012.

[21] Pohlig, S. and M.E. Hellman, “An improved algorithm for computing logarithms over GF (p) and its cryptographic significance,” *IEEE Transactions on Information Theory, vol. IT-24, 1978, pp. 106-110.*

[22] A. Shamir and Y. Tauman, “Improved online/offline signature schemes," in *Proc. 21st Annual International Cryptology Conf. Advance Cryptology*, p. 355-367, Springer-Verlag, 2001.

[23] H. Krawczyk and T. Rabin, “Chameleon signatures," in Proc. Symp. Netw. Distributed Syst. Security (NDSS00), (Internet Society), pp. 143-154, Feb.

[24] Dr. S. Santhosh Baboo,K. Gokulraj, “An Enhanced Dynamic Mutual Authentication Scheme for Smart Card Based Networks,” I. J. Computer Network and Information Security, 2012, 4, 30-38.

Authors’ Profiles

Balaji V Durgawad has received his bachelor of engineering degree in computer science and engineering from Mahatma Gandhi Mission’s College of Engineering, Nanded (M. S.), India in 2009. He received his Master of Engineering in the department of computer science and engineering in Mahatma Gandhi Mission’s College of Engineering, S.R.T.M. University, Nanded (M. S.), India in 2017. He is working as a lecturer in the Department of computer Engineering, Gramin Polytechnic,Vishnupuri, Nanded. His research interests are focused on cryptography and network security.

Md. Aijaz Ahmed received his B.E. Degree in Computer Science & Engineering from, M.B.E.S’ College of Engineering, Ambejogai, (M. S.), India in 2003; He has obtained M.E. in Computer Science & Engineering in 2007 from, M.G.M’s College of Engineering, S.R.T.M. University, Nanded,(M.S.), India. He is currently pursuing Ph.D. in Computer Science & Engineering from GITAM University Vishakapatnam, (A. P.), India. His area of interest includes Network Security and Cryptography, Discrete Mathematics, Automata.

Dr. D Rajya Lakshmi was awarded Ph.D. in CSE from JNTU, Hyderabad. She is presently working as a professor in the Department of Computer Science & Engineering, University College of Engineering Vizianagram, JNTU Kakinada, A.P., INDIA. She has 25 years of teaching experience. Her research areas include Image processing and soft computing, Data mining, Network security. Her areas of Interest are Data Mining, Network Security, Image Processing and Soft computing.

Dr. Syed Abdul Sattar received B.E. (Electronics) from Marathwada University, Aurangabad, Maharashtra, India , in 1990. He received M.Tech. in Digital system and Computer Science from J.N.T. University, Hyderabad, Andhra Pradesh, India, in 2002. He received Ph.D. in Electronics & Communication Engg. from J.N.T. University, Hyderabad, in 2007. His area of interest include Computer Communications, Network Security, Image Processing.

How to cite this paper: Balaji V Durgawad, Mohammed Aijaz Ahmed, D. Rajya Lakshmi, Sayed Abdul Sattar,"Mutual Authentication and Session Key Establishment for Secure Communication using Generalized Digital Certificate", International Journal of Computer Network and Information Security(IJCNIS), Vol.9, No.8, pp.23-31, 2017.DOI: 10.5815/ijcnis.2017.08.04