Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 2, February 2014, pg.862 – 868

RESEARCH ARTICLE

Enhanced Privacy ID for Remote Authentication using Direct Anonymous Attestation Scheme

Uma.R[1], Aravind.P[2]

[1]PG Student, [2]Assistant Professor

Department of Electronics and Communication Engineering, Kamaraj College of Engineering and Technology,Virudhunagar, Anna University, Tamilnadu, India.

[1] umabtech2012@gmail.com, [2] mcetarv@gmail.com

Abstract - Anonymizing networks such as Tor allow users to access Internet services privately by using a series of routers to hide the client's IP address from the server. The success of such networks, however, has been limited to the users employing this anonymity for abusive purposes such as defacing popular Web sites. A system in which servers can "blacklist" misbehaving users, thereby blocking users without compromising their anonymity. For example, As Cloud Services such as Google collect more and more personal data and store them in a centralized manner, the consequence of exposing or leaking an account's information could be nightmarish. It is desirable that some measures of data control are available on the part of users. In this paper, we introduce a new cryptographic scheme called Enhanced Privacy ID (EPID) for remote, anonymous authentication of a hardware device securely and privately.

Keywords: Direct anonymous Attestation, Security, Anonymity, Privacy, Trusted Computing

I. INTRODUCTION

Trusted Computing Group (TCG) [1], an industry standardization body that aims to develop and promote an open industry standard for trusted computing hardware and software building blocks, and was included in TPM specification version 1.2.Direct Anonymous Attestation (DAA) is a scheme developed by Brickell et al. [2] for remote authentication of a hardware module, called Trusted Platform Module (TPM), while preserving the privacy of the user of the platform that contains the module. In the DAA scheme, during the issuing of a DAA private key, the issuer obtains the identity of the TPM, but does not learn the DAA membership private key. If sometime after issuing, the issuer discovers that the TPM has been compromised, the issuer cannot revoke the DAA private key that has been issued to that compromised TPM.

EPID scheme can be seen as a new DAA scheme with enhanced revocation capabilities. An EPID scheme can be viewed as a special digital signature scheme. Unlike traditional digital signature schemes, one public key in the EPID scheme corresponds to multiple private keys. There are three types of entities in an EPID scheme: issuer, members, and verifiers. The issuer creates an EPID

public key and issues a unique EPID private key to each member. Each member can use this private key to digitally sign a message, and the resulting signature is called an EPID signature. The verifier can use the public key to verify the correctness of a signature, that is, to verify that the EPID signature was indeed created by a member in good standing with a valid private key. The EPID signature, however, does not reveal any information about which unique private key was used to create the signature. EPID can be used for secure on-line banking. On-line banking is increasingly popular and provides great convenience to end users. However, the security of on-line banking is a concern, not only to end users but also to the banks. If the end user runs a platform that has a trusted execution environment and trusted I/O, the end user can conduct business in a relatively secure environment. However, the bank does not know whether the user is running in a secure environment. An anonymous attestation from the user's platform to the bank would give the bank more confidence that the transaction is secure. For example, if a bank user performs some high volume transactions, the bank wants to make sure that the transactions are properly authorized. If the user runs a trusted execution environment, the user can use the EPID scheme to anonymously attest to the bank so that the bank can give a token to the platform for future transactions. The bank would know that the token was being secured in a trusted execution environment. In later transactions, the user enters a password into the trusted execution environment that unlocks the token so that the bank can authenticate the user's environment. This assures the bank of the authenticity of the transaction. This paper is organized as follows: Related work is presented in Section II. We present our privacy preserving enhanced privacy id scheme in Section III. Results and Performance Analysis is discussed in Section IV. We conclude in Section V.

The following notations are used in this paper. H(.) denotes the hash function ;$\{0,1\}^l$ denotes $\{0,1\ldots\ldots..2^l-1\}$.

II. RELATED WORK

The EPID scheme in this paper shares some properties with group signatures [3], [4], [5], [6], DAA [1], identity escrow [7], and anonymous credential systems [8], [9]. In fact, our scheme draws on techniques that have been developed in these schemes, e.g., building blocks from the DAA scheme [1] and the group signature schemes [3], [8], [10].The EPID scheme differs from the DAA scheme in that it adds additional revocation capabilities. Another work related to EPID is the pseudonym system of Brands [11].Brands' system provides efficient techniques for proving relations among committed values. However, the credentials in that system are linkable for multiple display, whereas the signatures in the EPID scheme are unlinkable.

III. PROPOSED SYSTEM

The System Architecture for Enhanced Privacy ID Scheme is shown in Fig.1.In an Enhanced Privacy ID scheme; there are several types of entities: an issuer, a revocation manager, users, and verifiers. The issuer and revocation manager could be the same entity or separate entities. Our EPID scheme builds on top of the DAA scheme [1] and uses the CL signature scheme [10] as underlying building block. Modified the DAA scheme in the following ways: 1) each user chooses a single secret f instead of two secrets, and 2) the signature operation is performed solely by the user, instead of split by two separate entities (e.g., TPM and host in the DAA scheme).An EPID scheme has the following operations:

- Setup. The issuer creates a public key and an issuing private key. The issuer publishes and distributes the public key to everyone (that is, to every member and every verifier).
- Join. This is an interactive protocol between an issuer and a member, the result of which is that the member obtains a unique private key.
- Sign. Given a message m and a SIG-RL, a member creates an EPID signature on m by using its private key.
- Verify. The verifier verifies the correctness of an EPID signature by using the public key. The verifier also checks that the key used to generate the signature has not been revoked in PRIV-RL or SIG-RL.

Algorithm

A. Key Generation

1. The issuer chooses prime number p and q such that q | (p-1).
2. The issuer calculate the modulus value N using RSA algorithm such that N=P*Q, P=2P'+1,Q=2Q'+1;
3. The issuer chooses the g' value such that, the group of quadratic residues modulo n.
4. The issuer chooses the random quadratic residues g, h, R, S, $Z \in Z_N^*$based on Camenisch Lysyanskaya Signature Scheme.

5. Calculate the value of u based on Decisional Diffie Hellman.
6. The issuer publishes the group Public Key (N,g',g,h,R,S,Z,p,q,u).

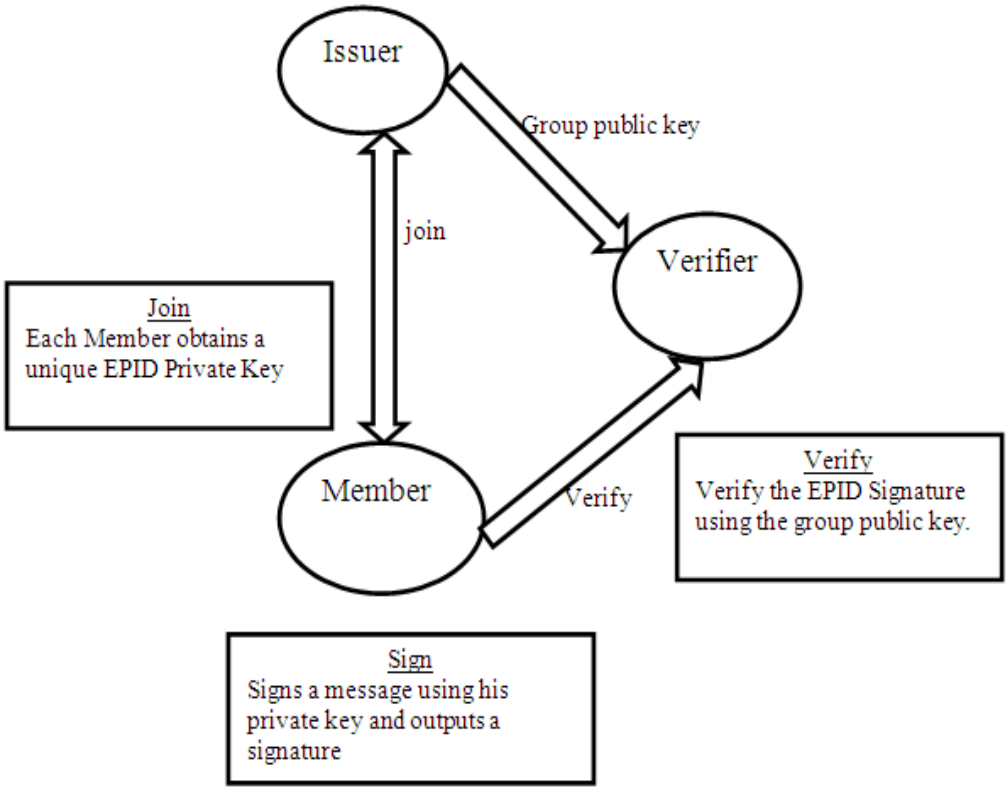

Fig.1. System Architecture

B. Join

1. The member chooses at random f and v' computes $K=B_I^f \bmod p$, $U=R^f S^{v'} \bmod N$.
2. The member sends (K,U) to the issuer and performs the following proof of knowledge to the issuer: $spk\{(f,v'): U \equiv R^f S^{v'} (\text{mod } N) \wedge K \equiv B_I^f (\text{mod } P) \wedge f \in \{0,1\}^L \wedge v' \in \{0,1\}^L\}$ (n_I)
3. The issuer chooses a random v" and random prime e and calculates: $A = (Z/US^{v''})^{1/e} \bmod N$.
4. The user calculates the v: v=v'+v".
5. The user obtains the private key (A, e, f, v).

C. Signature Generation

Let (A,e,f,v) be the member's private key, member randomly chooses the value w,r,ew,ee,er,n_v and message(m) from verifier. The member does the following:

SPK{(f,v,e,w,r,ew,ee,er) : $Z \equiv T1^e R^f S^v h^{-ew}$ (mod N) $\wedge$ $T2 \equiv g^w h^e (g')^r$ (mod N) $\wedge$ $1 \equiv T2^{-e} g^{ew} h^{ee} (g')^{er}$ (mod N) $\wedge$ $K \equiv B^f (mod\ p) \wedge f \in \{0,1\}^l\}$ ($n_v \| m$)

1. The member randomly chooses the $r_v, r_e, r_f, r_{ee}, r_w, r_r, r_{ew}$ value from the security parameters $l_N, l_f, l_e, l_{e'}, l_v, l_H, l_r$.
2. The member calculates the following value using public key parameters and randomly generated values

$\widetilde{T1}=T1^{re}\ R^{rf}S^{rv}h^{-rew}$ (mod N) ;

$\widetilde{T3}=T2^{-re}\ g^{rew}h^{ree}(g')^{re}$ (mod N) ;

$\widetilde{T2}=g^{rw}\ h^{re}(g')^{rr}$ (mod N); $\widetilde{\widetilde{K}} = B^{rf}\ (mod\ p)$

3. The member calculates the hash function for public key and calculates

$$C_1=H\left(\begin{matrix} N\|g'\|g\|h\|R\|S\|Z\|p\|\widetilde{T3} \\ q\|u\|B\|K\|T1\|T2\|T3\|\widetilde{T1}\|\widetilde{T2}\|\widetilde{T3}\|\widetilde{\widetilde{K}}\|m\|n_v \end{matrix}\right)$$

4. The member proves over the integers
   $S_v = rv+C_1 * v$; $S_e = re+C_1 * (e - 256)$; $S_{ew} = rew+C_1 * w*e$; $S_f = rf+C_1 * f$
   $S_r = rr+C_1 * r$; $S_w = rw+C_1 * w$; $S_{ee} = ree+C_1 * e^2$; $S_{er} = rer+C_1 * e*r$.
5. The member sets signature as

σ:=(B;K; T_1; T_2; C_1; S_v; S_f; S_e;S_r; S_w; S_{ew}; S_{ee}; S_{er}**)**

D. Authentication operation

1. The verifier verifies that message (m) and nonce (n_v) and sent to the prover as the challenge.
2. The verifier verifies that B, K subset of U.
3. The verifier verifies that prover private key has not been revoked in the revocation list. $K \not\equiv B^{f_1} \pmod p$

IV. RESULTS AND PERFORMANCE ANALYSIS

By adjusting and detailing the mathematical description of each of the protocol building blocks we have been able to implement all computational operations involved. The prototype development made using Java 7 (update 3) on a standard platform with the following processor: AMD Athlon(tm) 64 _ 2 Dual Core Processor2.2 GHz (18.500 MIPS). The computational analysis considers the number of mathematical operations required in each of the phases. The computational analysis of EPID Scheme is shown in Table .1.

TABLE 1: Performance Analysis

Operation	**Prover/Verifier**	**Computation cost**
Proof of membership	Prover	Constant time
	Verifier	
Verification based on private key	Verifier	n1
Verification based on signature	Verifier	6n2+3n3+c

Legend: n1, n2, n3: number of modular exponentiations, c: constant.

A. Simulation results

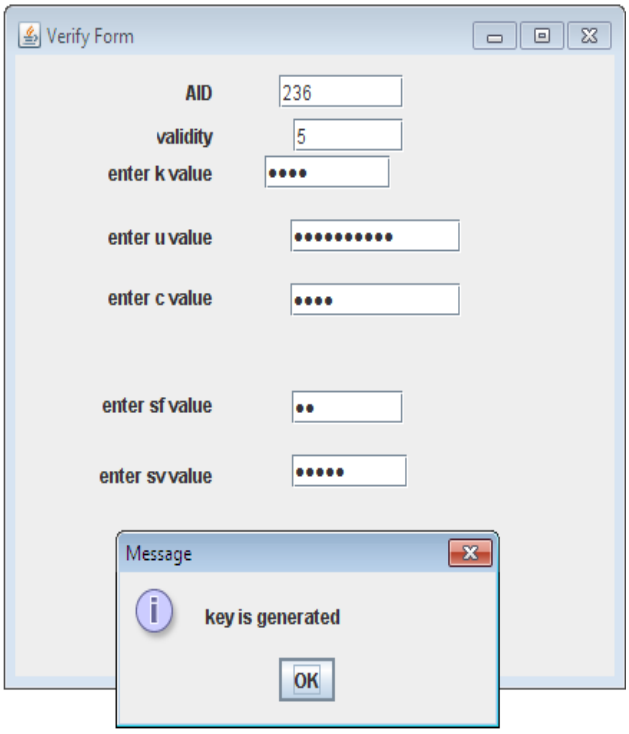

Fig.2. unique private key generation for each new user during join operation

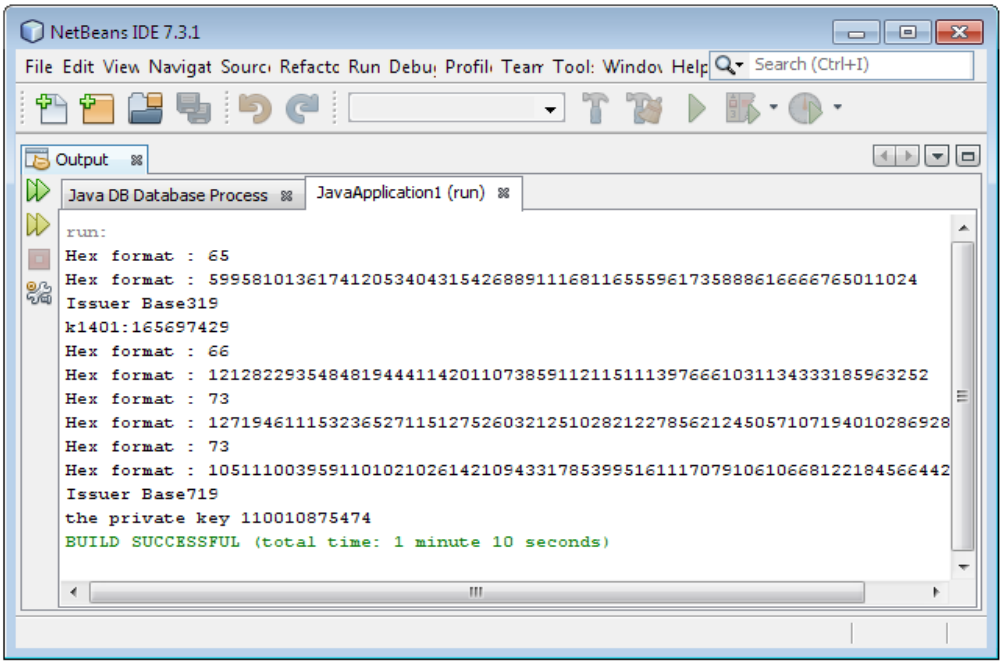

Fig.3.Value of Private Key for user after join operation

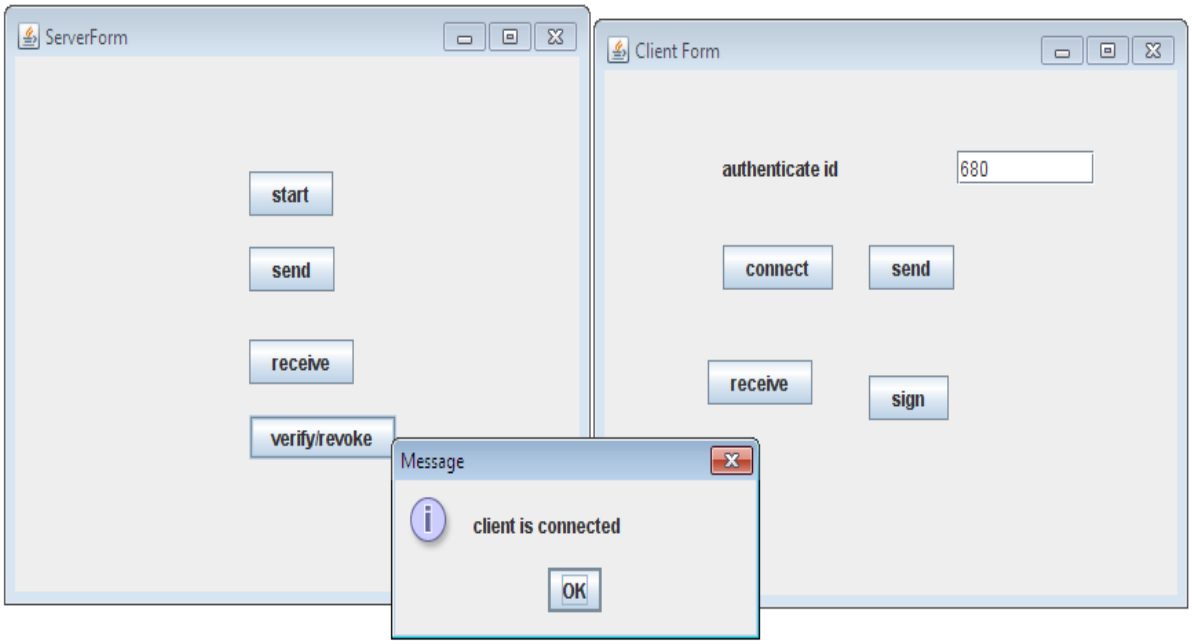

Fig.4. Client is connected to the server after authentication operation

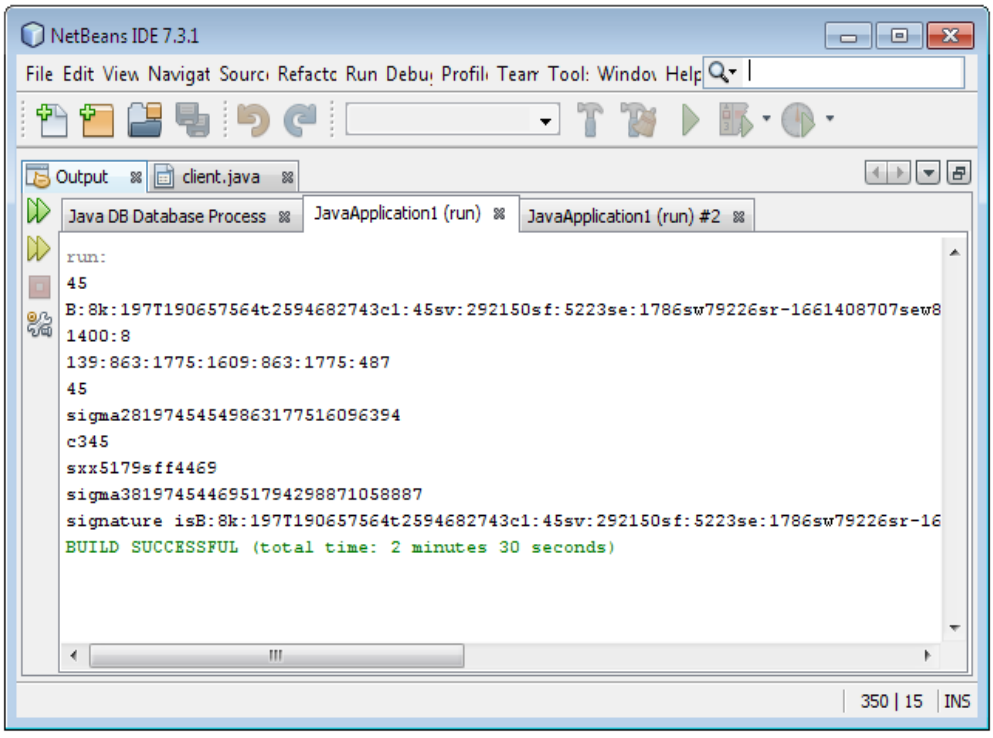

Fig.5. Signature generation operation

V. CONCLUSION

Thus the EPID Scheme gave an efficient construction for anonymous authentication and user privacy. EPID scheme provides the users to abilities of data sharing among his service accounts, proving the integrity of his platform to remote servers, and the most important of all, preserving anonymity of the user.

REFERENCES

[1] Trusted Computing Group websites http://www.trustedcomputinggroup.org, 2011.

[2] E.Brickell ,J.Camenisch ,and L.chen "Direct Anonymous Attestation ," Proc.11th ACM Conf, Computer and Commn.Security ,pp.132-145 ,2004.

[3] G.Attensie , J.Camenisch, M.joye, and G.Tsudik, "A Practical and Provably Secure Coalition-Resistant Group Signature Scheme, " Proc.Ann.Int'l Cryptology Conf, Advances in Cryptology(CRYPTO '00), pp. 255-270, 2000.

[4] D.Bonrh, X.Boyen, and H.Shacham, "Short Group Signatures, "Proc.Int'l Cryptology Conf. Advances in Cryptology(CRYPTO '04),pp. 41-55, 2004.

[5] J.Camenisch and M.stadler, " Efficient Group Signature Schemes for Large Groups," Proc. Ann. Int'l Cryptology Conf. Advances in cryptology (CRYPTO '97), pp. 410-424, 1997.

[6] D.Chaum and E.Van Heyst, "Group Signatures," Proc. Ann. Int'l Conf. Theory and Application of Cryptographic Techniques : Advanced in Cryptology (EUROCRYPT '91) , pp. 257-265, 1991.

[7] J.Killian and E.Petrank, "Identity Escrow," Proc. Int'l Cryptology Conf . Advances in Cryptology (CRYPTO '98) , pp. 169-185,1998.

[8] J.Camenisch and A.Lysyanskaya, " An Efficient System for Non-Transferable Anonymous Credentials with Optional Anonymity Revocation," Proc. Int'l Conf. Theory and Application of Cryptographic Techniques : Advances in Cryptology (EUROCRYPT '01), pp. 93-118, 2001.

[9] D.Cahum ,"Security without Identification: Transaction Systems to make Big Brother Obsolete," Comm. ACM, vol.28, no. 10,pp. 1030-1044, 1985.

[10] J.Camenisch and A.Lysyanskaya, " A Signature Scheme with Efficient Protocols ," Proc. Third. Conf. Security in Comm. Networking, pp. 268- 289,2002.

[11] S.A.BrandsRethinking Public KeyInfraStructures and Digital Certificates : Building in Privacy. MIT Press, Aug.2000

