Reliable Modern Credentials

Faiz Ahmad
College of Engineering,
Bharati Vidyapeeth University,
Pune-411043(India).
nststsn@hotmail.com

Rajesh Jalnekar
Vishwakarma Institute of
Technology,Pune-411037(India).
ph:+919922432291
rajesh-jalnekar@yahoo.com

ABSTRACT

This paper describes an efficient and reliable modern credentials that support a secure and fast access for various kinds of online applications like e-commerce, online banking, or e-government. The modern credentials are designed with respect to developed pseudonymous digital signature to sign a special type of the X.509 attribute certificate. In such certificate the holder field is replaced by a public unique pseudonym field which uniquely and globally identify the certificate holder. The credentials are signed by issuer's private key and it combine the security and privacy aspects in reliable functionality to serve the growing needs in the online applications and services.

Categories and Subject Descriptors

D.4.6 [Security and Protection]: Access controls, Authentication, Cryptographic controls.

General Terms

Reliability, Security.

Keywords

Modern Credential, Access Control, Certificate, Privacy.

1 INTRODUCTION

With the rapid increase in the number of online users, and corresponding increases in the number of online applications and services, the number of online security threats has significantly increased. Most of these attacks target end user applications, and it has affected user trust in security sensitive online services, such as online banking and electronic commerce. The nature of attacks on online users varies from a simple user profiling attack using tracking cookies, to more sophisticated attacks on cryptographic algorithms and security protocols[11]. Pseudonymous interaction with online services offered by most pseudonym systems [10,16] could be a right solutions to protect a user privacy and prevent such security threats. The vulnerability to some attacks and the weak reliability of the pseudonymous credentials implemented with such systems in terms of high cost of issuing and management of credentials and the complexity to proof possession with verifying organizations, makes a great demands for reliable credentials to resolve the existing problems.

Pseudonyms help to protect a users privacy; they also change the way conventional security properties like confidentiality, integrity and availability are guaranteed. These properties are often based on a long term relationship between the user and the organisation that wants to enforce the properties. In general term, pseudonyms are identifiers of subjects. A subject is pseudonymous if a pseudonym is used as identifier instead of one of its real names. Depending on the scope of the context there are different pseudonym types[8]:

- The users public key can act as a person pseudonym.
- A user could derive role pseudonyms from his secret key and use it with different organisation whenever he wants to act in a certain role.
- Unique pseudonyms are organisation wide relationship pseudonyms.
- Normal pseudonyms used only in a specific role are role relationship pseudonym.
- By creating a new pseudonym for a new transaction the user establishes a transaction pseudonym.

In this paper we proposed a flexible mechanism to generate pseudonyms which are adopted to serve in reliable credentials. The next section explains how the centralized third party generates for every registered player a public unique pseudonym and related private pseudonym where the player updates his related private pseudonym whenever needed locally in his personal security environment.

The rest of this paper is organized as follows: The next section describes the generation of pseudonyms. Subsequently, Section 3 explains the enhanced RSA digital signature. Sections 4 describes reliable credentials. Finally, the paper concludes in Section 5.

2 GENERATION OF PSRUDONYMS

The root pseudonyms are generated based on the following assumption: **Assumptions.** for any trusted centre with an RSA modulus $n \in Z_n^* \; : \; n = p \cdot q$ (p, q are two prime numbers with approximately of k-bits length each) and the related Euler's totient function $\phi(n)$ =(p-1)(q-1), it is always possible to generate a secret random integer $r \xleftarrow{R} \mathrm{Z}_{\phi(n)}$, and the related public integer $s \in Z_{\phi(n)}$ such that r : 2 < r < ϕ (n) and s= ϕ (n)-r, where $\exists$ g$\in Z_n^*$ and the following condition must be hold:

$$g^{\phi(n)} \equiv 1 \bmod \phi(n) \tag{1}$$

Similarly to [4], according to this assumptions every player (e.g. users and organizations) registered with TTP will obtains two root pseudonyms : a unique public root pseudonym $s \equiv ID_p$, and private root pseudonym $r \equiv ID_v$. A player's unitary pseudonymous identity denoted by ID_u :

$$ID_u = ID_p + ID_v = k \cdot \phi(n)$$

Where *k*-random integer number.

It is assumed that no two player registered with a trusted third party have the same root pseudonyms under the given RSA modulus. More generally, a pseudonym ID_v is generated by use of a function *f* parameterized with two parameters: the player's unitary pseudonymous identity ID_u and a unique public pseudonym ID_p. Hence the pseudonym ID_v results in:

$$ID_v = f(ID_u, ID_p) = k \cdot \phi(n) - ID_p$$

More precisely, the TTP generates unique pseudonym ID_p for the player while the player responsible for updating private pseudonym ID_v in his personal security environment such that:

$$ID_v = f(C \cdot ID_u, ID_p) = C \cdot ID_u - ID_p \qquad (2)$$

According to the above assumptions the player's public and private exponents are calculate respectively as follow:

$$E \equiv (g^{ID_P}) \bmod \phi(n) \qquad (3)$$

$$D \equiv (g^{ID_V}) \bmod \phi(n) \qquad (4)$$

Then the player's public and secret keys $[pk_p(E,n), sk_p(D,n)]$.

The registered player upon completion of registration phase will obtains a pseudonymous certificate uniquely identified by public exponents E which acts as a player public pseudonym. Basically, it is similar to the X.509 attribute certificate except that the holder field is replaced by public exponents E field and a new field, named peudonymity revocable, is added to indicate that a third party can unveil a subject's identity under well specified Conditions. The certificate is signed by issuer's private key (TTP).

3 ENHANCED RSA SIGNATURE

Consider the protocol is a session between a user $U[UIP_P, UID_V; pk_U(E_U, n), sk_U(D_U, n)]$ wants to access some services with an organization $O[OIP_P, OID_V; pk_O(E_O, n), sk_O(D_O, n)]$. Where the public and secret keys for each player (e.g. users and organizations) are generated by TTP as described in previous section.

3.1 Signing Algorithm

Sign(D_U, E_O ,M**).** This algorithm takes as input a signer's secret pseudonym(user) D_U, a destination's public pseudonym(organization) E_O, and a message $M \in \{0,1\}^*$ and signs the message as follow:

$$S_U(M) \equiv [(M^{D_U})^{E_O}] \bmod n \qquad (5)$$

3.2 Verification Algorithm

Verify(S_U *(M)*, D_O, E_U **).** The verification algorithm takes as input signer's public pseudonym E_U, a verifier's secret pseudonym D_O, and a purported signature S_U *(M)*, and proceeds as follow :

$$M \equiv [(S_U(M)^{E_U})^{D_O}] \bmod n \qquad (6)$$

If the message *M* equal to decrypted one the signature is accepted and the organization ensured that the signer belongs to trusted pseudonymous user from the same trusted domain, then the user is granted access to the intended service.

3.3 Implementation of Enhanced RSA

We use a key generation time, signature / verification time as indicators of a signature scheme's performance to make direct comparisons between Enhanced RSA and original RSA schemes for one single player.

Table 3. The test results on enhanced and original RSA

Enhanced RSA	Message M =4096 char		Block size = 8	
Modulus N, bit	1024	1536	2048	4096
Key Gen. Time, MS	109	359	468	2527
Enc./Dec. Time, MS	2886	5757	9719	38532
Original RSA	Message M =4096 char		Block size = 8	
Key length, bit	1024	1536	2048	4096
Key Gen. Time, MS	297	2013	6037	62197
Enc./Dec. Time, MS	1545	2948	5054	19375

3.4 Key Generation Time

All the times recorded in (Table 1) have been measured on a AMD Turion(tm) 64x2 Mobile technology TL- 50 1.60 GHz processor, using the time measurement functions offered by the

Java library on a Windows Vista platform. The table1. shows the key generation times for enhanced and original RSA schemes which were recorded with various bit-strengths. Here we have to mention that for enhanced RSA algorithm the key generation time not includes the time of generation of modulus N, because it generated only once by a trusted third party. Figure 1, describes the curve of key generation time when the lengths of modulus changed. It seem that enhanced RSA key generation time is very small and approximately the same for all tested values of N, where the original RSA key generation time is increases proportionally with modulus size.

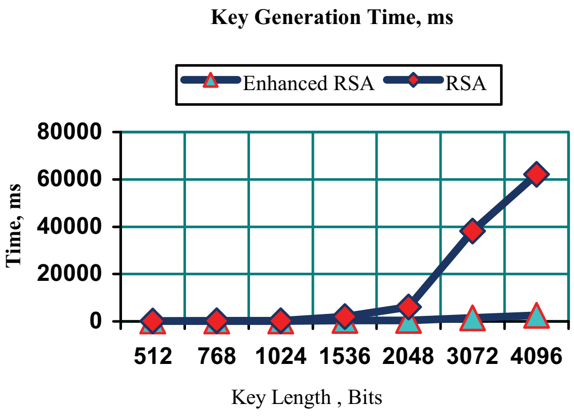

Figure 1. The key generation time with various bit-strengths of modulus N.

3.4.2 Encryption/Decryption Time

Figure 2, describes the curve of encryption/decryption time with the same input file (4096 char) and various key lengths as it recorded in table1.

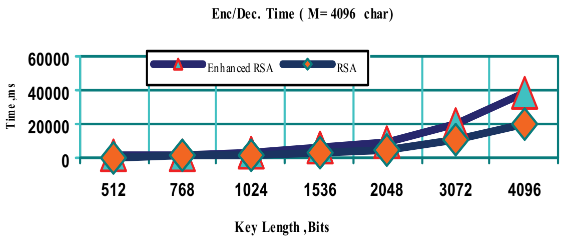

Figure 2. Encryption/decryption time with the same input file (4096 char)

The test results shows that the enhanced RSA a little slower in term of encryption / decryption time, this is due the security improvement in key generation techniques made in section 2, which equalizes the values of public and private exponents in size. In our framework we are concern to encrypt small messages(hash function) to proof possession of credential and grant access to online services, so in our opinion the 4096-bit modulus is a good balance between speed and security for enhanced RSA with reasonable cost.

4 RELIABLE CREDENTIALS

Credentials are statements about an individual that are signed by the issuer and can be shown to other organisations. Pseudonymous credentials are used for pseudonymous service access. A credential from an organisation can be shown to other organisations (to which the user is known under a different pseudonym) without revealing the pseudonym under which the credential was originally established. Where any credential can be used under any pseudonym, but there are still no clear protocols to establish pseudonyms[16].

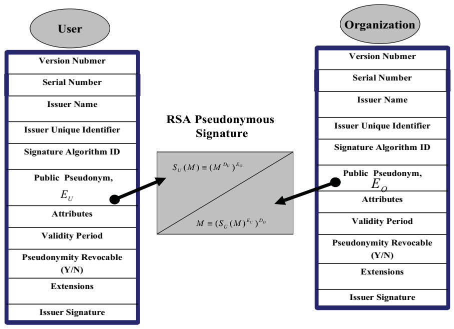

Figure3. Reliable pseudonymous access control

In our framework there are a distinct and flexible organization /user- centric protocol to establish pseudonyms, issue credentials and show credentials to organisations. The root organization(TTP) responsible for generate root pseudonyms and their related public and private exponents in addition to long lived pseudonymous certificates. The control is transferred then to the player who will have full sovereignty to update his pseudonyms and consequently generates the required related type of pseudonyms. Figure3, simplify the framework of pseudonymous interactions between user and organization that provides internet services.

The credential multi-show protocol implies the proves possession of RSA pseudonymous signature(by the prover and verifier). The verifier does not learn anything about the prover's credential, except that it is valid and belong to pseudonymous user from trusted domain.

The reliability of the framework includes in the following advantages :

- *Pseudonymity Support and Enhanced Privacy*: multi use authorisation pseudonyms keys are used directly without reference to the names of the key owners. It becomes difficult to correlate different tasks/activities of a single user over time because the private keys, which are engaged in the activities, are frequently updated by user itself. Using separate private keys when communicating with different entities, or when performing different unrelated tasks, prevents the easy combination of gathered information for a single entity. In this way, the properties of pseudonymity and untraceability are achieved.
- *Effective Pseudonymous Environment*: A trust relationship created between two entities without relying on the support of trusted third parties. This eliminates the cost of running a Certificate Authority for centralised key management (e.g. key distribution and revocation) as in traditional X.509[6].The ownership of the key can be verified pseudonymously without a trusted third party. Since the

key is used as the identifier, there is no need to use a global naming scheme.

- *Great Security:* RSA pseudonymous signature very secure and fast in term of key generation as compared to original RSA as described earlier. An adversary cannot compute secret pseudonym for legitimate player in the system from publicly available information.
- *Simplicity and Flexibility*: The design simplify the management of keys and credentials while it has great flexibility to be modified and used for different kinds of applications.

5 CONCLUSIONS AND FUTUREWORK

This paper describes an efficient and highly secure enhanced pseudonymous RSA signature based on strong mechanism for generation and building pseudonymous environment. Reliable pseudonymous credentials are developed accordingly to fulfil the security, privacy and functional requirements of modern online services and applications. The trust established by proposed credentials could be a proper solutions for the most problems still unresolved in current pseudonym systems.

6 REFERENCES

[1] R.L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, vol. 21, no. 2, pp 120-126, February 1978.

[2] Dan Boneh and Matthew Franklin. Efficient Generation of Shared RSA Keys. Journal of the ACM, Vol. 48, No. 4, July 2001

[3] Aleksandra Nenadiæ, Ning Zhang, Barry Cheetham, Carole Goble. RSA-based Certified Delivery of E-Goods Using Verifiable and Recoverable Signature Encryption. Journal of Universal Computer Science, vol. 11, no. 1 (2005), 175-192.

[4] Faiz Ahmad, Rajesh Jalnekar. Modern Credential Access Control Approach Based On Pseudonymous Signature. IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.10, October 2007, pages 129-134.

[5] E. R. Verheul. Self-blindable credential certificates from the Weil pairing. In C. Boyd, editor, Proceedings of Asiacrypt 2001, volume 2248 of LNCS, pages 533–51. Springer-Verlag, Dec. 2001.

[6] Richard Au, Harikrishna Vasanta, Kim Kwang Raymond Choo, Mark Looi. A User Centric Anonymous Authorisation Framework in Ecommerce Environment. ICEC'04, Sixth International Conference on Electronic Commerce, ACM, pages 138-147.

[7] S. Chow, C. Boyd, and J. Gonzalez. Security-mediated certificateless cryptography. In *PKC 2006*, volume 3958 of *Lecture Notes in Computer Science*, pages 508-524. Springer-Verlag, 2006.

[8] C. Diaz (Ed.), H. Dekeyser, X. Huysmans,' Advanced Applications for e-ID Cards in Flanders'. ADAPID Deliverable D7,pages 1-79. September 2007.

[9] B. Pftzmann. Privacy in enterprise identity federation - policies for Liberty 2 single sign on. *Information Security Technical Report*, 9(1):45-58, January-March 2004.

[10] J. Camenisch and A. Lysyanskaya. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In *EUROCRYPT 2001, LNCS 2045*, pages 93–118, 2001.

[11] Adil M. Alsaid,' Enhancing End User Security -Attacks & Solutions'. Ph.D thesis , Pages 30-40,2006.

[12] Ernest F. Brickell, Jan Camenisch, and Liqun Chen. Direct anonymous attestation. *Proceedings of the 11th ACM Conference on Computer and Communications Security, CCS 2004*,pages 132-145, Washington, DC, USA, October 2004. ACM.

[13] ITU-T Recommendation X.509. In Informationtechnology - Open systems interconnection – the directory: Public-key and attribute certificate frameworks, 2000.

[14] B. Friedman, P.H. Khan, and D.C. Howe. Trust Online. In Communications of the ACM, volume 43,pages 34–40, 2000.

[15] R. Clarke. Identified, Anonymous and Pseudonymous Transactions: The Spectrum of Choice. In Proceedings of User Identification & Privacy Protection Conference, 1999.

[16] Walt Teh-Ming Yao. Trust Management for Widely Distributed Systems. Ph.d thesis, February 10th, 2003.

[17] R. Song, L. Korba, and G. Yee. Pseudonym technologyfor e-services. In G. Yee, editor. Privacy Protection for E-Services. National Research Council Canada, Canada, Idea Publishing Group,200