Method of Design Public Key Infrastructure for Secure Audio Information Transmission in Multimedia Systems

Snezhana Pleshkova, Dimitar Kinanev

Snezhana Pleshkova, e-mail: snegpl@tu-sofia.bg
Dimitar Kinanev, e-mail: dimitarkinanev@gmail.com

***Abstract*— The importance to protect from non-authorized access of audio information transmission in multimedia systems is very high. [1] There are a lot of methods and algorithms suitable for the general case to secure transmission of all kind of data, including video and audio as a part of the multimedia information [2] In this article is proposed a special methodological approach to design and implementation of Public Key Infrastructure (PKI) in order to secure the transmission of audio information and protect it from unauthorized access through encryption keeping its confidentiality and integrity.**

Keywords—audio, security, certificates, pki, encryption.

I. INTRODUCTION

There are variety of benefits which makes Public Key Infrastructure best solution when securing audio information during its transmission between two communication points. [3] The Smart-Card Logon ensures two-factor authentication which implements the two main aspects of securing audio information - something you have, the private key the person owns, and something you know, the PIN with which the smart-card could be accessed in order the private key to be used. The digitally signing ensures the originator of data, who have sent it. The recipient of the data can verify the signature of the sender which provides three important benefits: the communication did come from the sender and from nobody else, there has been no change made during transmission of the audio information, and finally, the sender cannot deny having sent it. The encryption of audio information ensures that only the intended recipients can decrypt the message and the confidentiality of sensitive audio information which should not be shared.

One of the most common implementations of the process of asymmetric cryptography used by the PKI systems, is the RSA algorithm which add more benefits of using it. [4] One of those benefits is that the RAS algorithm provides simplification of the problem of key management which exists in symmetric encryption the number of keys required to allow n entities, where n is the number of users, to communicate is proportional to n2. Whereas in asymmetric encryption each participant needs two keys; therefore, the total number of keys required is simply 2*n. The growth in the number of keys with the growth in the number of users is linear and therefore manageable even when there are a large number of users. The other main benefit is that the security of the keys itself is highly increased. Every user must have a pair of keys that he/she generate for himself/herself. The secret key must not be shared with anyone and so the problem of transmitting it does not arise, nor do the problems of secure channels and their management; the secret key really is secret, since it is shared with nobody. The public key, however, is shared with everyone, for example in a catalog, which it can be transmitted using the most convenient method, and therefore does not pose any problems regarding its privacy.

II. DEVELOPMENT OF METHOD FOR PUBLIC KEY INFRASTRUCTURE (PKI) DESIGN TO SECURE AUDIO INFORMATION TRANSMISSION IN MULTIMEDIA SYSTEMS.

The two main perspectives which could be used to categorize the considerations taken into account when designing PKI solution in order to secure the transmission of audio information are business perspective which contain all the factors which will have influence on the cost of implementing such solution and technical perspective which defines all mandatory technical parameters. The both perspectives along with the steps which needs to be followed when designing PKI system are show on Figure 1.

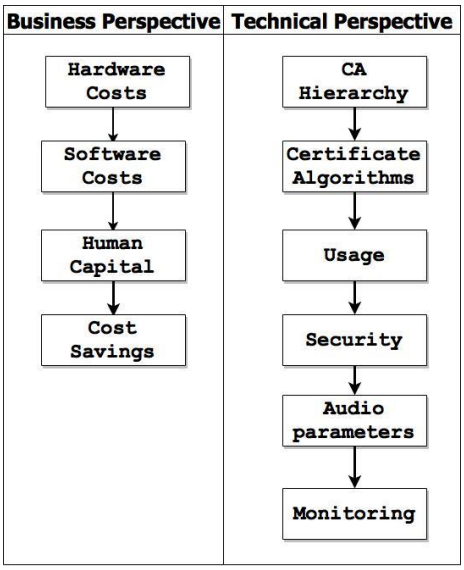

Fig. 1. Method for Public Key Infrastructure (PKI) design to secure audio information transmission in multimedia systems.

III. TECHNICAL PERSPECTIVE

A. Certificates Authority (CA) hierarchy

Define Certificate hierarchy planning is one of the most important aspects of PKI design because the design will affect how certificates are validated and used by PKI-enabled solutions that is why the planning of the technical perspective starts with this consideration. This section introduces a number of recommendations for designing a certificate hierarchy that can be used to meet today's pressing business needs as well as future needs that may not yet be identified.

A single tier Hierarchy consists of one CA. The single CA is both a Root CA and an Issuing CA. A Root CA is the term for the trust anchor of the PKI. Any applications, users, or computers that trust the Root CA trust any certificates issued by the CA hierarchy. The Issuing CA is a CA that issues certificates to end entities. For security reasons, these two roles are normally separated. When using a single tier hierarchy they are combined.

A two tier hierarchy is a design that meets most company's needs. In some ways it is a compromise between the One and Three Tier hierarchies. In this design there is a Root CA that is offline, and a subordinate issuing CA that is online. The level of security is increased because the Root CA and Issuing CA roles are separated. But more importantly the Root CA is offline, and so the private key of the Root CA is better protected from compromise. It also increases scalability and flexibility.

Specifically the difference between a Two Tier Hierarchy is that second tier is placed between the Root CA and the issuing CA. The placement of this CA can be for a couple different reasons. The first reason would be to use the second tier CA as a Policy CA. In other words the Policy CA is configured to issue certificates to the Issuing CA that is restricted in what type of certificates it issues.

B. Certificate Algorithms

When designing certificate hierarchy, it should be used only secure cryptographic algorithms and associated key lengths in PKI CAs. It should be strictly avoided the use of weak cryptographic algorithms (such as MD5) and key lengths. Here we need to take into account the length of time data needs to be kept secure. This is where CA certificate validity period plays its role. The validity period defines how long CA certificates will be trusted because the key length for CA certificates relates to both the security level that needs to be provided and the required duration of the key's validity. With a longer validity period, plan for a higher security level of crypto algorithms. With these considerations in mind, the recommended subordinate CAs key length must be at least 2048 bits for RSA. For any CA that has certificate expiration more than 15 years in the future, the CA key length that uses RSA must be 4096 bits or greater.

C. Usage

The intended scope of usage for a private key is specified through certificate extensions, including the Key Usage and Extended Key Usage (EKU) extensions in the associated certificate. The cryptographic use of a specific key is constrained by the Key Usage extension in X.509 certificates. All certificates should include key usage as a critical extension. The other important certificate extension that controls what a certificate is trusted for is the Extended Key Usage (EKU) extension. The Key Usage Extension has an indirect dependency with the EKU extension, so these two extensions need to align. These extensions are usually populated according to RFC 5280 and corresponding certificate usage recommendations - for example, in the Transport Layer Security protocol or for smart card logon.

D. Security

The security of PKI system is provided by HSM device. While it is technically possible in many cases to migrate an existing software-based key to an HSM, in general it is not the preferred approach. One of the benefits in using an HSM is the knowledge that the key has never been stored or used outside the secure HSM. Even if no compromise has occurred or is suspected, with a software-based key there is no real assurance that other copies of the key do not exist. In the event that you have an existing PKI and want to begin leveraging HSMs, consider a migration to a new infrastructure with new keys that are generated within the HSM.

E. Audio parameters

When designing PKI system for protecting audio information needs to be taken into account the time for encryption and the time for decryption [5]

$$T_{ENC} = T_C \tag{1}$$

$$T_{DEC} = T_{C^d} \tag{2}$$

which will directly affect the transmission of audio information live through the communication channel, as for example in VoIP systems which are extremely bandwidth- and delay-sensitive. For VoIP transmissions to be intelligible to the receiver, voice packets should not be dropped, excessively delayed, or suffer varying delay (otherwise known as jitter).

The ITU G.114 [6] specification recommends less than 150 millisecond (ms) one-way end-to-end delay for high-quality real-time traffic such as voice. (For international calls, one-way delay up to 300 ms is acceptable, especially for satellite transmission. This one-way delay takes propagation delay into consideration—the time required for the signal to travel the distance.)

The size of the fragment from the whole audio message is also important in the planning. For example, for a link speed of 64 kbps and MTU size of 1500 bytes, we have [7]:

$$Delay = \frac{(1500bytes * 8bits/byte)}{64000bits/\sec} = 187{,}5ms \tag{3}$$

F. Monitoring

Because the Certificate Authority is a very important part of the system, monitor it closely for abnormal activity is very important for its work. [8] There two major events categories to monitor, standard events which are typically the same for such kind of systems and specific events that could be seen only in this specific system. Table I illustrates some of the activities that should be monitored to help detect compromise of a system based PKI:

TABLE I
MONITORING ACTIVITIES OF CERTIFICATE AUTHORITY

Standard events	Specific activity
Successful and failed logons	Unauthorized changes to CA security settings
Addition, removal, or deletion of user accounts	Revocation of a significant number of certificates during a short time period
Changes to membership in the local administrators group	Changes to the audit filter settings for the CA
Usage of the built-in administrator account	Issuance of certificates that contain restricted usages (Enrollment Agent, Key Recovery Agent)
Changes to system time outside a defined threshold (changes greater than ten minutes)	Changes to the active Policy Module on the CA
Abnormal startup or shutdown events	Changes to the configured Key Recovery Agents
Clearing of event logs	Changes to role separation settings if role separation is enabled
Disabling or modification of antivirus and antimalware software	Addition of certificate templates that are not normally issued by the CA
Antivirus or antimalware action taken (quarantine, etc.)	Addition or deletion of certificates from the CA database
Installation of new services	Usage of the CA private key outside of certsrv.exe (certutil.exe, custom executables or scripts).
Unknown processes starting or stopping	Suspicious use of accounts belonging to registration authorities. For example, if a smart card management system uses a specific service account to request certificates from the CA and that account makes certificate requests from systems that are not part of the smart card management system.
Addition, removal, or deletion of user accounts	Revocation of a significant number of certificates during a short time period
Changes to membership in the local administrators group	Changes to the audit filter settings for the CA
Usage of the built-in administrator account	Issuance of certificates that contain restricted usages (Enrollment Agent, Key Recovery Agent)
Changes to system time outside a defined threshold (changes greater than ten minutes)	Changes to the active Policy Module on the CA

IV. BUSINESS PERSPECTIVE

In the practice main decision driving component is the cost for implementing Public Key Infrastructure which is the reason why it takes a major place into this proposed approach for designing those systems. There are several major types of costs which should be considered when designing a PKI system and based on them it could be concluded the expression (4) of the total costs (TC)

$$TC = HC + SC + HC + T + S \tag{4}$$

where Hardware Cost (HC) is the cost for the needed servers, Hardware Security Modules (HSMs), Backup Devices, Backup Media; The Software Cost (SC) is the cost of the software, for example licenses or any other subscriptions, needed for the running infrastructure; The Human Capital (HC) is the cost which should be considered for day-to-day support of the infrastructure in order to ensure 100% availability; The Tokens (T) is a parameter which influences the total cost considering the hardware devices where the certificates for the user will be securely stored; The Subscription (S) represents the money that should be set aside for the yearly availability of certificates which usually is 3 years;

V. EXPERIMENTAL RESULTS

Table II represents an example configuration of the parameters from the technical perspective according to the needs of medium size company. Based on those parameters it will be calculated the total cost of the PKI solution for protecting audio information while its transmission.

TABLE II
TECHNICAL PERSPECTIVE PARAMETERS

PARAMETERS	
CA hierarchy	2 Tier hierarchy (Hybrid)
Certificate Algorithms	RSA/3DES/SHA2
Usage	Encryption, 10000 Users
Security	HSM device
Audio parameters	Link with speed 64 kbps/ MTU 1500 bytes
Monitoring	Software
CA hierarchy	2 Tier hierarchy (Hybrid)
Certificate Algorithms	RSA/3DES/SHA2
Usage	Encryption, 10000 Users
Security	HSM device
Audio parameters	Link with speed 64 kbps/ MTU 1500 bytes
Monitoring	Software
CA hierarchy	2 Tier hierarchy (Hybrid)
Certificate Algorithms	RSA/3DES/SHA2
Usage	Encryption, 10000 Users

Table III represents the cost of each module from expression (4) on yearly basis. The resulted total cost considering the technical parameters is 250 000 Euro.

TABLE III
COST CALCULATION

	COST (EURO)
Hardware Cost (HC)	10 000
Software Cost (SC)	10 000
Human Capital (HC)	20 000
Tokens (T)	10 000
Subscription (S)	20 per User

Total Cost	250 000

VI. CONCLUSIONS

The proposed special methodological approach to design and implementation of Public Key Infrastructure (PKI) to secure the transmission of audio information in multimedia systems is described as the necessary sequence of the steps and their monitoring to detect compromise in the designing of a system based PKI for secure transmission of audio information Therefore, it can be concluded, that the goal in this article to propose and develop of method for security in multimedia systems using in design and implementation both specific characteristics of transmitted audio information and Public Key Infrastructure (PKI) system is completed and can be use and applied in the real practical implementations.

Based on expression (3) the delay limitation for transmission of audio information is 187.5ms which means that we cannot use RSA algorithm since the estimated experimentally average time for encryption/decryption is 700ms. As per the estimated average times for encryption/decryption of symmetric algorithms [9] are from 20ms to 40ms which satisfy the limitation but it is less secure and expose the information at risk. This is the reason why the modern PKI systems are hybrid which is also used in the proposed method subject of this article.

Based on the calculations in Table III we can conclude that the cost of a PKI solution could be increase or decrease depending on the technical parameters chosen for the solution. This is the reason why in the common design case, we need first to consider the technical parameters and then to calculate the total cost. If needed the technical parameters could be reconsidered in order the total cost to be decreased if it doesn`t fit in the forecasted budget.

ACKNOWLEDGMENT

This work was supported by Technical University – Sofia inner program to research projects under 172PD0032-07:"Algorithms for the study of methods for improving the security of information through audio infrastructure for encryption with public key in multimedia communications computer systems and networks".

REFERENCES

[1] B. Furht, E. Muharemagic, and D. Socek, "Multimedia encryption and atermarking Series: Multimedia systems and applications", Springer, Vol. 28, 2005.

[2] Omar M.Barukab, Asif Irshad Khan, Mahaboob Sharief Shaik, MV Ramana Murthy and Shahid Ali Khan, "Secure communication using symmetric and asymmetric cryptographic techniques", I.J. Information Engineering and Electronic Business, 2012, 2, pp. 36-42.

[3] Stephen Wilson, "The importance of PKI today", China Communications, 2012.

[4] Suranjan Choudhury, Kartik Bhatnagar, Wasim Haque, "Public Key Infrastructure Implementation and Design", M&T Books, 2002

[5] X.509 Internet Public Key Infrastructure Online Certificate Status Protocol. http://www.networksorcery.com/enp/data/x509.htm

[6] Pleshkova Sn., Kinanev D. "Method for security enhancement of audio information in communication multimedia systems and networks applying encryption algorithm with public key," CEMA'2016, Athens

[7] ITU-T Recommendation G.114. "Series g: Transmission systems and media, digital systems and networks," May 2013.

[8] Cisco, "Quality of Service for Voice over IP recommendation," http://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/qos_solutions/QoSVoIP/QoSVoIP.html

[9] Microsoft Knowledge Base, https://technet.microsoft.com

[10] Pleshkova Sn., Kinanev D. , "Method for comparative performance analyze of encryption algorithms used in Public Key Infrastructure for secure transmitting of audio information", (to be published) ISSE, 2017.