# Key Management for Updating Crypto-keys over AIR

**Nagaraj Hediyal**
Vice President-Technical, SystemsAids, Bangalore-560043

**Abstract*:***
In modern security, the need for safe cryptographic algorithms with sophisticated key management is of great importance. The need for updating crypto keys over AIR is inevitable due to proliferation of large number of encryption systems across huge communication networks. The main objective of this paper is to emphasis on the various aspects of the key management and updating of crypto keys over air to avoid any time delay involved in bringing up the network to the life. In this paper, a new approach to the Key Management for Updating Crypto-Keys over Air has been presented. Paper also provides an insight into the design of a secure key data transceiver (SKDTR), secure key data carrier (SKDC), and network architecture. The generic requirements, managerial issues, policies, guide lines of key management has been dealt. The other objectives of the paper are to provide a generic, low cost, low power, flexible hardware and easy maintenance of the solution.

***Key words:***
*Security, Crypto system, Cryptographic Keys, Key Encrypting Keys, Authentication, Signature, Algorithm, Policy, Guidelines, Secure Data Transceiver.*

## 1. INTRODUCTION

**S**ecurity is a factor of an increasing importance in the design of modern communication systems [1].Cryptography, indeed is the only practical means of exchanging information over an insecure channel, be it telephone line, microwave, or satellite links [2]. Cryptography provides the necessary tools for accomplishing private and authenticated communications. Although, there are many good algorithms with different usages and key management characteristics, not all of them can be characterized fully secure [3]. In all the communication systems, the need for safe cryptographic algorithms with sophisticated key management is of great importance. There has been a great need for the ***transfer of keys over air*** due to the proliferation of Encryption systems across the various communication networks spread all over the country, especially the networks used by the major defense forces. Due to many security reasons, non-existence of proper procedure, policies to transfer the keys over air were not thought off. It was also felt that the personal courier is the best way to handle the distribution of cryptographic keys when the numbers of systems were limited.

There are inherent risks if proper key management procedures, policies are not followed because of the complexity involved in distributing keys to all the systems across the communication network used by various users. The loss or theft or compromise of the cryptographic keys could affect the integrity, confidentiality of the communications [4]. If the proper guidelines or procedures are not followed while handling the cryptographic keys during their life cycle, the keys can be modified, or disclosed by the unauthorized authorities that could then disturb or intercept the communication.

In order to update the key information in various encryption systems spread over the network periodically, the key management technique must be powerful, failsafe and easy to handle [5].

In this paper, all these issues are considered in detail and given suggestions for good implementations. Section 2 deals with generic requirement of key management. Section 3, deals with Non technical but managerial issues, Section 4, deals with the proposed design of Efficient Key management system, algorithms to be used and methodology needed to implement a good key distribution system are introduced. Section 5, deals with the proposed SKDTR design and NW Link architecture and process of key transfer and receive. Section 6 summarizes the recommendations.

## 2. GENERIC REQUIREMENTS

Key management plays a fundamental role in cryptography as the basis for securing cryptographic techniques providing confidentiality, entity authentication, data origin authentication, data integrity, and digital signatures. The goal of a good cryptographic design is to reduce more complex problems to the proper management and safe keeping of a small number of cryptographic keys, ultimately secured through trust in hardware or software by physical isolation or procedural controls. Reliance on physical and procedural security (E.g. secured rooms with isolated equipment), tamper resistant hardware, and trust in a large number of individuals is minimized by concentrating; trust in small number of easily monitored, controlled and trustworthy elements.

Key management is the set of techniques and procedures supporting the establishment and maintenance of keys between authorized parties. Key is the state where in communicating entities share common data to facilitate cryptographic techniques.

Manuscript received January 5, 2011
Manuscript revised January 20, 2011

This data may include public or secrete keys, initialization values, and additional non secret parameters. Key management encompasses techniques and procedures supporting:

a. Initialization of system users within a domain.
b. Generation, distribution and installation of keys.
c. Controlling the use of keys.
**d.** Update, revocation and destruction of keys.
**e.** Storage, backup, recovery and archival of keys.

## 3. NON_TECHNICAL /MANAGERIAL ISSUES

This section highlights the physical mechanisms that need to exist and some of the points of concern are as follows.

a. Avoiding the frequent movement of the physical courier.
b. Updating of the keys in all equipments at all places at once.
c. Bringing back the network fast to live state in case of any eventuality with the key erasure, key mismatch during operation/use.
d. Establishment of the proper control, and procedure to avoid any compromise of confidentiality, authenticity of Key Encrypting Keys and Cryptographic keys.
e. Avoiding the unauthorized use of Key Encrypting Keys and cryptographic keys.
f. Establishing the procedural controls for handling the Key Encrypting Keys and Cryptographic keys.
g. Facilitating the ways means of securing and storing the transmitted cryptographic keys.
h. Providing the guidelines on how to protect the Key storage devices from unauthorized access.

## 4. PROPOSED DESIGN OF EFFICIENT KEY MANAGEMENT SYSTEM

Proposed design of Key Management for Updating Crypto-Keys over Air is devised based on the following assumptions:

### 4.1 Assumptions

i. A dedicated line/link of required data rate say, 16 Kbps/64Kbps is available as and when required to update the crypto keys.
ii. Always key transfer takes place from a designated Key Updating Centre (KUC) to all the sites of the network.
iii. Crypto keys and Key Encrypting Keys are generated and collected from a designated key management approval authority.
iv. Crypto keys are encrypted and decrypted on line.
v. The cryptographic keys are transferred and stored on to the respective crypto systems.
vi. Specifically designed secure key data transceiver (SKDTR) is being used to achieve the key transfer over air along with a secure key data carrier (SKDC).
vii. Crypto keys present in SKDTR and SKDC are erased immediately after the key transfer.
viii. All the cryptosystems have the unique ID option to facilitate the authentication and identification of the requisite crypto system.

### 4.2 Devised Key Management System

The most important starting point is complete knowledge about the network environment where in such an application is to be implemented. The key management should have:

i. Authentication mechanism for sender and receiver.
ii. Algorithm with key to encrypt and decrypt the Crypto Keys while transferring on air.
iii. Generation and Transportation of Crypto Keys.
iv. Mechanism to store the Crypto Keys.
**v.** Mechanism to address the tampering, copying, of the Crypto Keys.

#### 4.2.1 Authentication of the sender and Receiver

Authentication by itself has little meaning other than to convey the idea that some means has been provided to guarantee that entities are who they claim to be or that unauthorized parties have not manipulated information. Authentication is specific to the security include access control, entity authentication, message authentication, data integrity, non-repudiation, and key authentication. Authentication is one of the important of all information security objectives.

Authentication depends on appropriate policies, procedures and controls. An effective authentication method should have customer acceptance, reliable performance, scalability to accommodate growth and interoperability with existing systems and future plans. Authentication methods that depend on more than on

factor are more difficult to compromise than single factor methods. Accordingly, properly designed and implemented multifactor authentication methods are more reliable and stronger.

For example, consider a hardware device that holds a cryptographic key. The key might be activated by a password or any other means like biometric etc. Such a device is considered to be effectively provided two factor authentications, although the actual authentication protocol between the verifier and the claimant simply proves possession of the key. Symmetric and Asymmetric Encryption provides source authenticity along with message integrity. Also both methods provide secrecy of the messages. Recipient can check whether meaningful message and authentication data are obtained after decryption. Changes to cipher are likely to result in meaningless message and authentication data. These are depicted in fig 1 and 2 below.

**Symmetric:** Key shared between sender & receiver.

**X** encrypts message 'P' and authentication data 'A' using algorithm ALG with symmetric key 'K' to obtain cipher data 'C' as shown in fig1.a below.

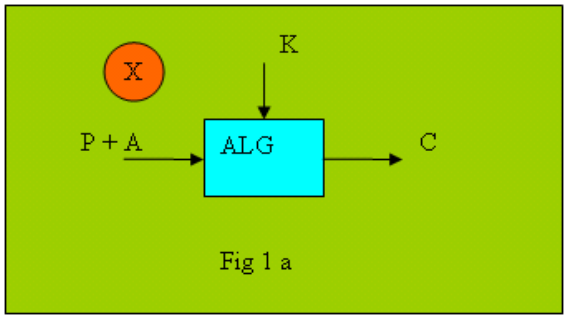


Fig 1 a

**Y** decrypts cipher data 'C' using algorithm ALG with symmetric key 'K' to obtain message 'P' and authentication data 'A' as shown in fig1.b below. B checks authentication data and authenticates the sender.

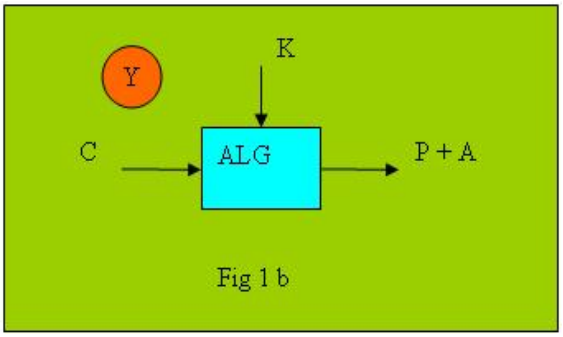


Fig 1 b

**Y** decrypts cipher data 'C' using algorithm ALG with symmetric key 'K' to obtain message 'P' and authentication data 'A' as shown in fig1.b below. B checks authentication data and authenticates the sender.

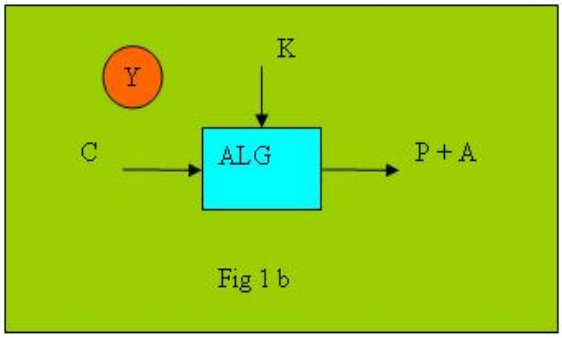


Fig 1 b

**Y** decrypts cipher data 'C' using the algorithm ALG with key 'Pub (K)' to obtain the message 'P' & authentication data 'A' as shown in fig 2.b below. B checks authentication data and authenticates the sender.

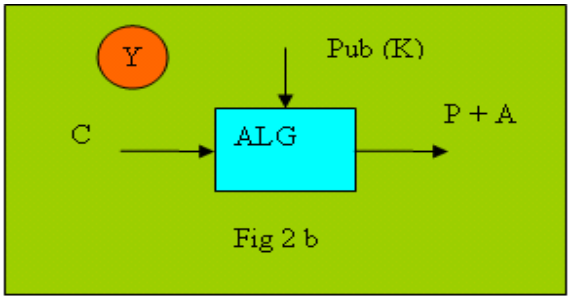


Fig 2 b

### 4.2.2 Algorithm to secure the Cryptographic Keys.

The requirement of the transfer of cryptographic keys from a designated distribution center to any sites (where number of encryption systems are in use) over air is essential to avoid the loss of communication due to expiry of the life of the existing keys life or corruption of the existing keys etc. Under such circumstances it is necessary to update the keys and bring back the network to live condition immediately. These cryptographic keys have to be updated at the earliest without compromising or loosing or modifying to safe guard the information that is being communicated over this network.

It is essential that the cryptographic keys have to be safely distributed to the respective sites other wise the compromise of these keys results in stoppage of the communication over that link or network. In order to protect these cryptographic keys while transferring over air on any required network there is a need for unique algorithm with sufficient cryptographic strength. The complexity and strength of the algorithm depends upon the amount of key data to be secured. Consider the technique presented in fig.3 using three linear feedback

shift registers and two-to-one multiplexer called as Geffe generator.

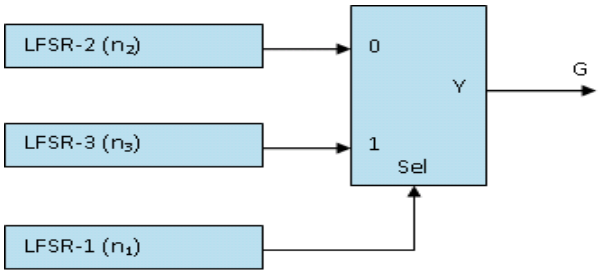



Fig. 3 Geffe Generator

If the primitive polynomials of LFSR-1, LFSR-2, and LFSR-3 have degrees $n_1$, n2 & $n_3$, respectively, the generator will have linear complexity:

$$LC = n_3 n_1 + (n_1 + 1)n_2 \quad \text{---------- (1)}$$

And period:

$$T = lcm(2^{n_1} - 1, 2^{n_2} - 1, 2^{n_3} - 1) \quad \text{---------- (2)}$$

For example, if $n_1$= 31, $n_2$=43, $n_3$= 59 then,

$$T = lcm(2.147 \times 10^9, 8.79 \times 10^{12}, 5.76 \times 10^{17}) \quad \text{--------- (3)}$$

There fore, the key data amounting to period (T) can be safely encrypted and transferred over the link. But the generator needs a modification to avoid being cracked. This unique algorithm (Complexity depends on the requirement) is used in association with a key called **key encrypting key**. In the above algorithm, if each LFSR has 8 primitive polynomials and out bit is tapped from a four to one multiplexer then totally 3 + 2 bits are required to operate an LFSR on one of the polynomial. Hence, totally 15 bits of key encrypting key is required for all of them. These keys have to be kept very safely as their usage is very limited. It all depends on the frequency of changing or updating of cryptographic keys. Obviously the frequency of the utilization of these keys depends upon the life of the cryptographic keys. Key encrypting keys can be either distributed manually by sending a personal courier to the sites wherever the device (SKDTR) is located or the device itself can be sent to the key management center/key generation center to update these keys. The frequency of updating the key encrypting keys depends on how often the cryptographic keys have to be transported over air to the respective sites. It means that the life of the cryptographic keys decides the frequency of updating the key encrypting keys. Generally the life span of the key encrypting keys can be very large ie, a year. This requires that the device (SKDTR) has to be stored in the very safe place with all cryptographic controls. The loss or theft of this device may result in collapse of the communication or the working network needs to be stopped immediately.

#### 4.2.3 Generation and transportation of Crypto keys:

Since the Cryptographic keys are generated at different place other than the designated key updating center a secured key data carrier is necessary. Secured data carrier could be Compact Disc (CD), Floppy Disc (FD) or Pen Drive (PD) etc depending on the availability of means. Cryptographic keys are generated at the key generation centre which is highly secured, restricted place and only authorized officials can only be allowed. These Cryptographic keys are encrypted either by Transformation Tables (TT's) or Substitution Boxes (SB) etc and then transferred on to CD, FD or PD as the case may be. These are transported by a secured physical courier on a designated date and time.

#### 4.2.4 Mechanism to Store the crypto keys.

The design of all the crypto systems should be such that the sufficient memory space for both current and future crypto keys is provided. All crypto systems will be using the keys from the current memory space during net work operation. Crypto keys stored in future memory space will be transferred to the current memory space in case of emergency or on expiry of the life of the currently used crypto keys. Then the new set of crypto keys will be transferred over air on a pre-designated date and time. These keys will be stored in memory space provided for future crypto keys.

#### 4.2.5 Mechanism to address tampering, copying etc.

Since all the crypto systems caters appropriate size memory space for both current and future crypto keys, the accessibility to be restricted. In any case the key data should never be able to retrieve from either of the memory space. Systems should be able to transfer or copy the crypto keys from future memory space to the current memory space only when the authorized personnel authenticates himself/herself with the crypto system and initiates such a command. The crypto keys stored in future memory space should be in encrypted form. System should be protected both electronically & mechanically. Electronic protection can be using multi level password and lock & key for mechanical access control.

## 5. Proposed Secured Key Data Transceiver (SKDTR) design.

Secure Data Transceiver is a critical device to be designed and developed for the purpose of updating keys over air. This needs a careful attention in deciding the

capablities, operating conditions, interfacing details while designing and developing. It should have the features such as:

i. Small, compact, weight less, handy.
ii. Cost effective, and easy to use.
iii. An appropriate algorithm to secure Crypto keys.
iv. Appropriate size memory for temporary storage of crypto keys.
v. LCD and Key pad interface for diagnostic and user control.
vi. Password protection for access and operation control at various levels.
vii. Appropriate standard protocol for cryptographic key data transfer to various equipments connected.
viii. Appropriate interface such as RS232C, RS485C, LAN, USB etc as the case may be.
ix. Any one or two authentications methods discussed in section 4.2 for user, source/destination and systems etc.
x. Option for reconfiguration/change of algorithms etc.
xi. Unique ID generation/allocation to systems, sites etc.
xii. RTC option for the purpose of time stamp, day, date etc.

## 5.1 Block Diagram of the proposed SKDTR

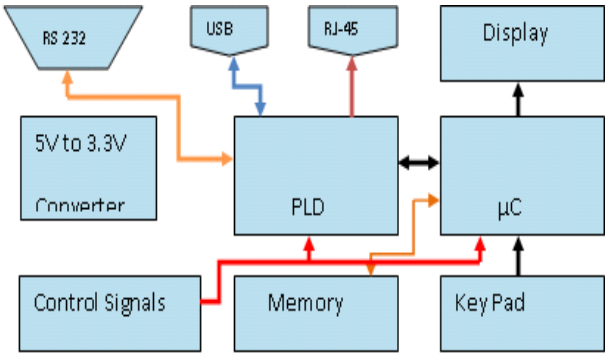



Fig.4 Block diagram of SKDTR

Fig.4 shows the block diagram of the proposed SKDTR. The hardware used in this solution contains various sections; 5V to 3.3 V converter section, CPLD section, µC section, RS 232,USB, RS465 communication section, Key pad and Display section and other control signal generation switches section. The LT 1963 regulator converts 5V input voltage down to 3.3 V. This 3.3V is extended to CPLD section, µC section for their operation. The CPLD section generates the necessary pseudo random bit sequences (PRBS) for the purpose of encryption and decryption of the crypto keys. The algorithm presented in section 4.2.2 has been implemented successfully. The µC section receives the command to load the necessary key encrypting key for the generation of PRBS to secure the crypto keys. It also updates and erases the crypto keys based on the command issued. The display section is used to display the various actions being carried out while transferring/receiving the crypto keys on the network.

The communication section consists of RS232C, USB and also RS485 serial communication transceiver to communicate with the computer and the net work. The control signal generation section generates the load signal, transfer signal etc for µC. The proposed structural view of the secure data transceiver is shown in fig 5 below.

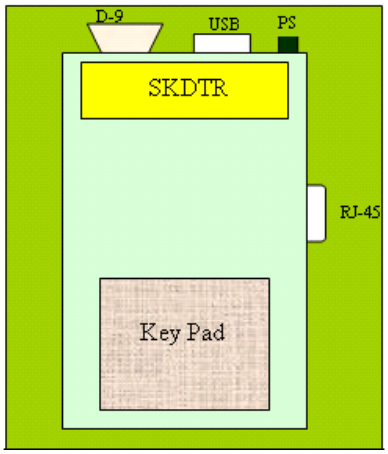



Fig.5 Structural View of SKDTR

## 5.2 Link Network Architecture design and Key transfer process.

The proposed network link architecture at the key updating center and at the remote locations is shown in fig 6(a) and fig 6(b) below and is self explanatory.

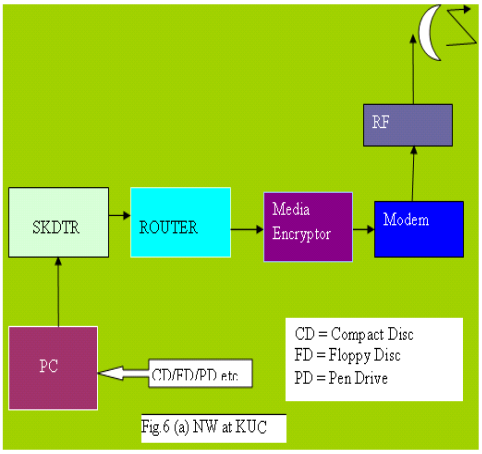



Fig.6 (a) NW Link structure at KUC.

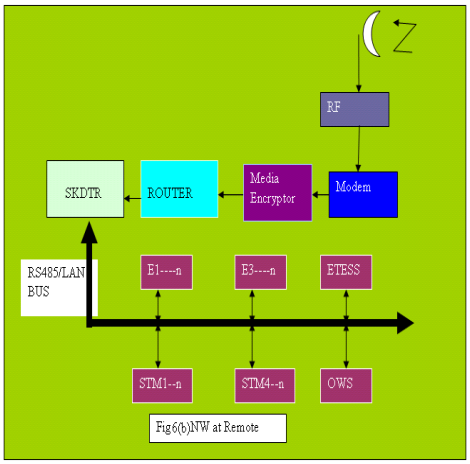
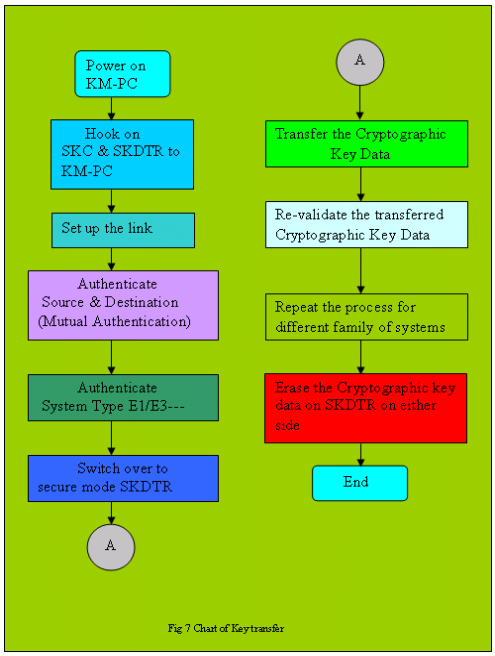



Fig.6 (b) NW link structure at remote site.

### 5.3 Process of key transfer

The chart shown in fig 7 details the process used for key transfer to the required sites.




SKC=> Secured Data Carrier,
KM-PC=> Key management Personal Computer.

## 6. RECOMMENDATIONS

The generic requirements, managerial issues (non technical), proposed efficient key management design, SKDTR, NW Link architecture aspects have been detailed in sections 2, 3, 4 and 5 respectively. Taking into account, all these aspects of key management, the recommendations for updating cryptographic keys over air are detailed in this section.

### 6.1Key Management Policy

Key management is usually provided within the context of a specific security policy. A security policy explicitly or implicitly defines the threats a system is intended to address. The policy may affect the stringency of cryptographic requirements, depending on the susceptibility of the environment in question to various types of attack. Security policies typically also specify the following:

a. Practices and procedures to be followed in carrying out technical and administrative aspects of the key management, both automated and manual.
b. The responsibilities, accountability of each party involved.
c. Types of records (audit trail information) to be kept, to support subsequent reports or reviews of security related events.
d. Integrity of the keys shall be ensured during generation, distribution, storage, entry, use, and destruction.
e. Keys shall be controlled and distributed during its lifetime to prevent unauthorized disclosure, modification, substitution or destruction etc.
f. Keys should be destroyed immediately after their intended period of life to prevent unauthorized disclosure.
g. Key access requirements should be reviewed on a periodic basis by a concerned authority.
h. Key generation equipment and storage devices shall be protected from unauthorized access through physical and electronic access controls.

### 6.2 Key Management Guidelines.

Key management guidelines are developed based on the established key management policies. Guidelines must explicitly explain/provide instructions on how to handle and protect keys. Typically guidelines must specify the following.

a. A strategy to establish data link between key updating center to the remote site to which the keys to be transmitted.
b. Appropriate proprietary algorithm with required cryptographic strength.

c. Source of key generation, mode of transport of keys from source of generation to key updating center.
d. Frequency/ period of change of both key encrypting keys and cryptographic keys.
e. Bases on which the frequency/ period of change of both keys to be determined.
f. Means and methods of keys destruction and their maintenance.
g. Type of training to be provided to the officials responsible for key generation, distribution, maintenance.
h. Types of electronic controls such as Smart card authentication, password authentication, biometric authentication.
i. Physical control access such as lock & key arrangement and many more.

## 7. EXPERIMENTAL SET UP, RESULTS AND ANALYSIS

The experimental set up used to simulate and verify the aspects of the updating of crypto keys is as shown in figure 8.

Figure 8 PC and SKDTR simulator

The SKDTR simulator is as shown in figure 9.


Fig.9 Proto type Board used as SKDTR

The algorithm presented in section 4.2.2 has been implemented in CPLD MAX II device (Altera make). This algorithm was used as the unique algorithm to secure the crypto keys while updating over AIR to the corresponding encryption systems working across the links of the network. Algorithm size complexity depends on the requirement of the security, amount of crypto key data to be secured etc. The data rate to communicate with PC was at 9.6 Kb/s and the interface used was RS232. The aspects of authentication between the key management PC and the SKDTR were done with simple pass word mechanism instead of the special type of algorithms detailed in section 4.2.1 to simplify the testing mechanism. Then the communication between the KM-PC and SKDTR was established successfully. Then KM-PC was also used as a crypto system to verify the data transfer from KM-PC- SKDTR-Crypto System. This was simulated by re routing the data from SKDTR to KM-PC. The key data required to operate the algorithm implemented in the CPLD was predefined within the circuit. VHDL code was used in the implementation of the algorithm. The communication was established using the microcontroller and the KM-PC. The interfacing between the CPLD and the microcontroller for the various activities such as authentication, data encryption was fast enough to verify the objective of the paper.

The total time required to establish the authentication, communication process was almost instantaneous between KM-PC and SKDTR. The total time taken to complete authentication of SKDTR with the KM-PC, SKDTR-Crypto System is about 5 ms plus the few ms for data (Crypto Key File) transfer. When the system is utilised over the network the time would be 5ms+ network delay+ time for Crypto Key file transfer.

The devised system is very flexible as it has microcontroller with in circuit serial port interface (ICSPI) and the PLD with JTAG interface there by avoiding

sophisticated programmer and programming cable for the purpose. Since the author has limited resources to simulate the actual field conditions the time to deduce the correct actual field timing was difficult. It is certain that the described protocol would be self sufficient in achieving the goal of updating the crypto keys over AIR without any compromise.
The simulated SKDTR is only 4" x 2.5" in size,. It is compact, low cost, low power and low weight. There fore the solution is very cost effective. The performance of the SKDTR still can be tried with actual network field conditions. Method explained is a new technique by itself. It would definitely prove to be an achievement if it is adopted and tried on any of the network.

## 8. CONCLUSION

The aim of the paper has been to describe and propose the efficient key management technique to achieve the failsafe, secure key transfer to the various encryption equipments spread across the huge communication networks. The design of proper and smart Secure Key Data Transceiver has been presented. Also the possible key areas, procedure guide lines along with a network structure for updating cryptographic keys over Air has been discussed. The secured data carriers, secured data transceiver, preparation, procedure and authentication of source destination, system types etc have been discussed. Desirable features of the secured data transceiver are also discussed. The few authentication algorithms used in practice are also detailed in this paper. Further the size of the prototype can still be reduced and it can be made to fit into the packet without compromising any of the security aspects of the key management discussed in this paper.

## REFERENCES

[1] Konrad Wrona "Distributed Security: AD Hoc Network and Beyond", AD Hoc Network Security PAMPAS Workshop, RHUL, Sept 16-17, 2002
[2] K.Zeng,CH Yang,DY Wei, and T.R.N.Rao "Pseudorandom Bit Generators in Stream-cipher Cryptography" 0018-9162/0200-008 1991 IEEE.
[3] Bruce Schneier,"Applied Cryptography- Protocols, Algorithms & Source Code in C", John Wiley and Sons, 2nd Ed New York 1996.
[4] A. Menezes, Paul C. Van Oorschot, Scott A. "Hand Book of Applied Cryptography", CRC, Press 1996.
[5] Public safety wireless Network October 2001
[6] Lidong Zhou and Zygmunt J. Hass "Security Adhoc Networks". IEEE Nov/Dec 1999
[7] Chai Keong Toh. "A novel distributed routing protocol to support Adhoc Mobile computing" IEEE1996.
[8] Frank Stajano and Ross Anderson Springer Verlag Berlin "Security Issues for Adhoc Wireless Networks", 1999
[9] H J Becker and Fred C Piper"Secure Speech Communications", Academic Press, 1985.
[10] Man Young Rhee "Cryptography and Secure Communication" Mc Graw Hill Book Co 1994.

**Nagaraj Hediyal** was born in India in 1966. He received his BE and M.Tech degree in 1989 and 2008 from Bangalore and Visvesvaraya Technological Universities. Presently, he is working as Vice President-Technical, and Heading R &D, Production at Systems Aids, Bangalore. He was Divisional Head and Deputy General Manager- R & D, Manatec Electronics Pvt Ltd, Puducherry. Formerly, Technical Manager, CG-CoreEl Programmable Solutions Pvt Ltd, Bangalore. He was Head of the Section (Encryption), Core R & D, ITI Ltd, Bangalore-16He authored and coauthored number of proprietary encryption algorithms for Indian defence such as Army, Navy and Airforce. He successfully designed and developed many encryption systems, for which ITI, Army presented appreciations for his rendered service.. He is a fellow of IETE. His research interests are Cryptography, VLSI, Embedded systems etc.