DRAFT NATIONAL ENCRYPTION POLICY

Under Section 84A of Information Technology Act, 2000 Rules are to be framed to prescribe modes or methods for encryption. In this regard, a draft National Encryption Policy as given under has been formulated by an Expert Group setup by DeitY based on which the Rules would be framed. Comments from the public are invited on the draft Policy. You can send your comments by 16/10/2015 to Shri A. S. A. Krishnan, Scientist 'G', Department of Electronics and Information Technology, Electronics Niketan, 6, CGO Complex, Lodhi Road, New Delhi: 110003, Email: akrishnan@deity.gov.in.

Preamble

Cryptography has emerged as a powerful tool that can help to assure the confidentiality, non-repudiability and integrity of information in transit and storage as well as to authenticate the asserted identity of individuals and computer systems. Encryption technology was traditionally deployed most widely to protect the confidentiality of military and diplomatic communication. With the advent of computer and Internet revolution and online applications as well as the recent innovations in the science of encryption, a new market for cryptographic products in E-commerce & E-Governance civilian applications has rapidly developed. Communication and E-commerce applications such as electronic mail and electronic fund transfer, which require secure means of communication, make extensive use of encryption for securing the information and authentication. The recognition of the need to protect privacy and increase the security of the Internet and associated information systems have resulted in the development of policies that favour the spread of encryption worldwide. The Information Technology Act 2000 provides for prescribing modes or methods for encryption (Section 84A) and for decryption (Section 69). Taking into account the need to protect information assets, international trends and concerns of national security, the cryptographic policy for domestic use supports the broad use of cryptography in ways that facilitates individual / businesses privacy, international economic competitiveness in all sectors including Government.

This policy is not applicable to sensitive departments / agencies of the government designated for performing sensitive and strategic roles. This policy is applicable to all Central and State Government Departments (including sensitive Departments / Agencies while performing non-strategic & non-operational role), all statutory organizations, executive bodies, business and commercial establishments, including public sector undertakings and academic institutions and all citizens (including Personnel of Government / Business performing non-official / personal functions).

I. Vision

To enable information security environment and secure transactions in Cyber Space for individuals, businesses, Government including nationally critical information systems and networks.

II. Mission

To provide confidentiality of information in cyber space for individuals, protection of sensitive or proprietary information for individuals & businesses, ensuring continuing reliability and integrity of nationally critical information systems and networks.

III. Objectives

i) To synchronize with the emerging global digital economy / network society and use of Encryption for ensuring the Security / confidentiality of data and to protect privacy in information and communication infrastructure without unduly affecting public safety and National Security.

ii) To encourage wider usage of Digital Signature by all entities including Government for trusted communication, transactions and authentication.

iii) To encourage the adoption of information security best practices by all entities and Stakeholders in the Government, public & private sector and citizens that are consistent with industry practice.

IV. Strategies

1. **Category of Users**: Based on the nature of transactions that require encryption the users in the Policy are classified as:

   G Govt. – All Central and State Government Departments (including sensitive departments / agencies while performing non-strategic and non-operational role).
   B All statutory organizations, executive bodies, business and commercial establishments, including all Public Sector Undertakings, Academic institutions.
   C All citizens (including personnel of Government / Business (G/B) performing non-official / personal functions).
   G2G Government to Government users
   G2B,G2C,B2G & C2G Government to Business & Government to Citizen users
   B2B Business to Business users
   B2C & C2B Business to Citizen users

2. Use of Encryption technology for storage and communication within G group of users with protocols & algorithms for Encryption, key exchange, Digital Signature and hashing will be as specified through notification by the Government from time to time.

3. Use of Encryption technology for communications between G group and B / C groups (i.e. G2B and G2C sectors) with protocols and algorithms for encryption, key exchange, Digital Signature and hashing will be as specified through notification by the Government from time to time.

4. Users / Organizations within B group (i.e. B2B Sector) may use Encryption for storage and communication. Encryption algorithms and key sizes shall be prescribed by the Government through Notifications from time to time. On demand, the user shall be able to reproduce the same Plain text and encrypted text pairs using the software / hardware used to produce the encrypted text from the given plain text. Such plain text information shall be stored by the user/organisation/agency for 90 days from the date of transaction and made available to Law Enforcement Agencies as and when demanded in line with the provisions of the laws of the country.

5. B / C groups (i.e. B2C, C2B Sectors) may use Encryption for storage and communication. Encryption algorithms and key sizes will be prescribed by the Government through Notification from time to time. On demand, the user shall reproduce the same Plain text and encrypted text pairs using the software / hardware used to produce the encrypted text from the given plain text. All information shall be stored by the concerned B / C entity for 90 days from the date of transaction and made available to Law Enforcement Agencies as and when demanded in line with the provisions of the laws of the country. In case of communication with foreign entity, the primary responsibility of providing readable plain-text along with the corresponding Encrypted information shall rest on entity (B or C) located in India.

6. Service Providers located within and outside India, using Encryption technology for providing any type of services in India must enter into an agreement with the Government for providing such services in India. Government will designate an appropriate agency for entering into such an agreement with the Service provider located within and outside India. The users of any group G,B or C taking such services from Service Providers . are also responsible to provide plain text when demanded.

7. Users within C group (i.e. C2C Sector) may use Encryption for storage and communication. Encryption algorithms and key sizes will be prescribed by the Government through Notification from time to time. All citizens (C), including personnel of Government / Business (G/B) performing non-official / personal functions, are required to store the plaintexts of the corresponding encrypted information for 90 days from the date of transaction and provide the verifiable Plain Text to Law and Enforcement Agencies as and when required as per the provision of the laws of the country.

8. Algorithms and key sizes for Encryption as notified under the provisions in this Policy only will be used by all categories of users.

V. Regulatory Framework

1. **Registration:** All vendors of encryption products shall register their products with the designated agency of the Government. While seeking registration, the vendors shall submit working copies of the encryption software / hardware to the Government along with

professional quality documentation, test suites and execution platform environments. The vendors shall work with the designated Government Agencies in security evaluation of their encryption products. Complete confidentiality will be maintained in respect of information shared by the vendors with designated agency. The vendors shall renew their registration as and when their products are upgraded. Mass use products like SSL / TLS are exempted from registration.

2. The Government will notify the list of registered encryption products from time to time, without taking responsibility for security claims made by the vendors.

3. The vendors of encryption products or service providers offering encryption services shall necessarily register their products / services with Government for conducting business in the country.

4. Government may review this policy from time to time and also during times of special situations and concerns.

5. Encryption products may be exported but with prior intimation to the designated agency of Government of India. Users in India are allowed to use only the products registered in India.

6. Government reserves the right to take appropriate action as per Law of the country for any violation of this Policy.

VI. Promotion of Research and Development in Cryptography

1. Research and Development programs will be initiated for the development of indigenous algorithms and manufacture of indigenous products for Encryption, hashing and other cryptographic functions. These will be carried out by Public and Private Sector / Government Agencies and Academia. Continuous intensified R&D activities in the niche areas of technical analysis and evaluation of Encryption products will be strengthened.

2. Testing and evaluation infrastructure for Encryption products will be set up by the Government.

3. **Technical Advisory Committee**: The technology is advancing at a fast pace. New forms of applications / products are emerging which employ encryption as integral part of the product. Many newer forms of communications with an intent to hide / protect information including social network based communication, peer-to-peer communication etc are already becoming very popular. The encryption deployed in such communication applications / devices uses both fixed and dynamic key algorithms for key exchanges and Encryption. Government agencies constantly identify these new forms of communication. A Technical Advisory Committee will monitor the technology development in the area of Cryptography to make appropriate recommendations on all aspects of Encryption policies and

technologies. It will carry out a continual follow-up of the National and International activities in basic and applied research in the science and technology of Encryption.

DRAFT

Annexure

Draft Notification on modes and methods of Encryption prescribed under Section 84A of Information Technology Act 2000

1. Definitions – In these Rules/Policy, unless the context otherwise requires, -

(a) The following definitions Cryptography, Encryption, Hash, Key, Public Key Cryptography/Asymmetric Cryptography, the meaning of aforesaid definitions has already been provided under Information Technology Act 2000, Rules and Regulations made there under.

(b) Symmetric Encryption is a method of encryption where the same key is used for both Encryption and Decryption. The key must be kept secret, and is shared by the message sender and recipient.

2. Symmetric Cryptographic/Encryption products with AES, Triple DES and RC4 encryption algorithms and key sizes up to 256 bits are prescribed by the Government for use for protecting information by stakeholders.

3. Asymmetric Cryptographic/Encryption products as prescribed under Information Technology Act 2000, Rules and Regulations made there under shall be used for Digital Signature purposes by stakeholders.