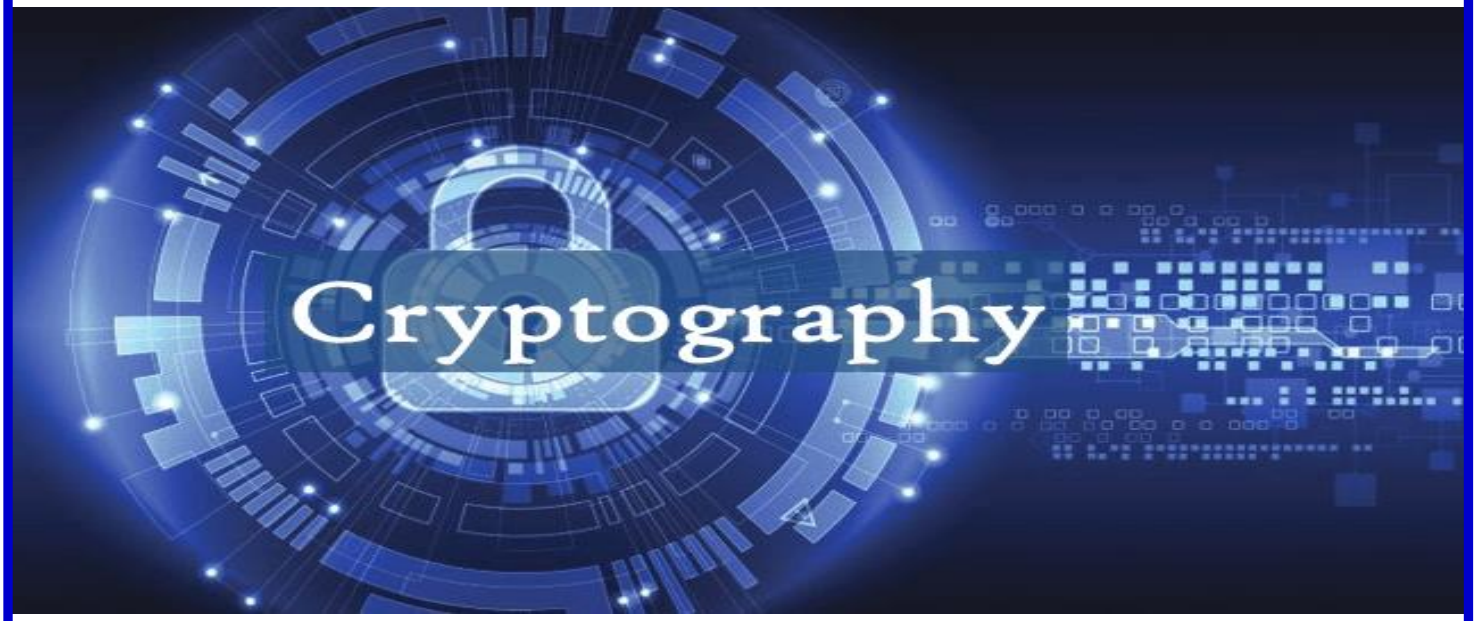
Transmission Corporation of Andhra Pradesh Limited



CRYPTOGRAPHY POLICY

File No. ENE51-ITOSEC/7/2021-ACICSU (Computer No. 1485830)
Generated from eOffice by BALAJI MITTINTI, DEE(MB), DEPUTY EXECUTIVE ENGINEER, AP Transco on 02/01/2025 04:36 pm

9705313/2024/ACIDO GICU

Confidentiality Statement

This product or document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form, by any means electronic, mechanical, photographic, optic recording or otherwise without prior consent, in writing, of the information owner.

Document Control

Document Name	Cryptography Policy
Document Reference Number	APTRANSCO/ISMS/CP/1.0
Classification	Internal
Version Number	D1.0
Date	25-Nov-2024
Reviewed by	IT Wing/ GICU Division
Approved by	

Revision History

Date	Version	Description	Created by
25-Nov-2024	D1.0	Initial Draft Release	GICU Division/ IT Wing

File No. ENE51-ITOSEC/7/2021-ACICSU (Computer No. 1485830)
Generated from eOffice by BALAJI MITTINTI, DEE(MB), DEPUTY EXECUTIVE ENGINEER, AP Transco on 02/01/2025 04:36 pm

9705313/2024/ACIDO GICU

TABLE OF CONTENTS

File No. ENE51-ITOSEC/7/2021-ACICSU (Computer No. 1485830)
Generated from eOffice by BALAJI MITTINTI, DEE(MB), DEPUTY EXECUTIVE ENGINEER, AP Transco on 02/01/2025 04:36 pm

9705313/2024/ACIDO GICU

1. Introduction

A cryptography policy outlines the rules and guidelines for the use of cryptographic techniques to secure data. It encompasses the selection of cryptographic algorithms, key management practices, implementation protocols, and compliance measures. This policy is designed to protect the confidentiality, integrity, and authenticity of information.

Purpose

The purpose of a cryptography policy is to ensure that all cryptographic measures are implemented consistently and effectively across an organization, mitigating risks and complying with legal and regulatory requirements.

Scope

It delves into the essential components, best practices, and considerations for developing and maintaining a robust cryptography policy.

2. Objectives of a Cryptography Policy

The primary objectives of a cryptography policy include:

- **Confidentiality**: Ensuring that sensitive information is accessible only to authorized individuals.
- **Integrity**: Protecting information from unauthorized modification.
- **Authentication**: Verifying the identity of users and systems.
- **Non-repudiation**: Ensuring that actions or transactions cannot be denied by the parties involved.

3. Key Components of a Cryptography Policy

3.1. Scope and Applicability

Define the scope of the policy, including which systems, applications, and data are covered. Specify the departments, personnel, and third parties that must comply with the policy.

3.2. Cryptographic Algorithms and Protocols

Specify the approved cryptographic algorithms and protocols for different purposes, such as:

- **Symmetric Encryption**: AES, 3DES
- **Asymmetric Encryption**: RSA, ECC
- **Hash Functions**: SHA-256, SHA-3
- **Digital Signatures**: RSA, ECDSA
- **Key Exchange**: Diffie-Hellman, ECDH
-

File No. ENE51-ITOSEC/7/2021-ACICSU (Computer No. 1485830)
Generated from eOffice by BALAJI MITTINTI, DEE(MB), DEPUTY EXECUTIVE ENGINEER, AP Transco on 02/01/2025 04:36 pm

3.3. Key Management

Outline the lifecycle management of cryptographic keys, including:

- **Key Generation**: Methods and standards for secure key generation.
- **Key Distribution**: Secure methods for distributing keys to authorized entities.
- **Key Storage**: Secure storage mechanisms, such as Hardware Security Modules (HSMs).
- **Key Rotation**: Regularly scheduled key changes to mitigate risk.
- **Key Revocation**: Procedures for revoking compromised or expired keys.
- **Key Destruction**: Secure deletion methods for decommissioned keys.

3.4. Implementation and Usage Guidelines

Detail the proper implementation and usage of cryptographic tools and techniques:

- **Data Encryption**: Guidelines for encrypting data at rest and in transit.
- **Authentication Mechanisms**: Use of cryptographic methods for user and device authentication.
- **Digital Signatures**: Procedures for signing and verifying digital documents.
- **Certificate Management**: Handling of digital certificates and Public Key Infrastructure (PKI).

3.5. Compliance and Legal Requirements

Ensure the policy aligns with relevant legal, regulatory, and industry standards, such as:

- **GDPR**: Data protection and encryption requirements.
- **ISO 27001**: Information security management standards.

3.6. Roles and Responsibilities

Define the roles and responsibilities of individuals and teams involved in implementing and maintaining the cryptography policy, including:

- **CISO (Chief Information Security Officer)**: Overall responsibility for the policy.
- **IT Infra and IT Application Team**: Implementation and monitoring of cryptographic controls.
- **GICU Team**: Ensuring adherence to the policy and regulatory requirements.
- **End Users**: Understanding and following the guidelines for cryptographic practices.

File No. ENE51-IT0SEC/7/2021-ACICSU (Computer No. 1485830)
Generated from eOffice by BALAJI MITTINTI, DEE(MB), DEPUTY EXECUTIVE ENGINEER, AP Transco on 02/01/2025 04:36 pm

9705313/2024/ACIDO GICU

4. Best Practices for Cryptography Policy

4.1. Regular Policy Review and Updates

Regularly review and update the cryptography policy to address new threats, vulnerabilities, and technological advancements. Ensure that the policy remains relevant and effective.

4.2. Education and Training

Provide ongoing education and training for employees on the importance of cryptography and proper implementation practices. This helps in building a security-aware culture within the organization.

4.3. Incident Response Plan

Develop and maintain an incident response plan specifically for cryptographic incidents, such as key compromise or algorithm vulnerabilities. This plan should include steps for containment, mitigation, and recovery.

4.4. Risk Assessment

Conduct regular risk assessments to identify and evaluate potential threats to cryptographic systems. Use the findings to improve the policy and enhance security measures.

4.5. Monitoring and Auditing

Implement continuous monitoring and regular auditing of cryptographic systems and practices to ensure compliance and detect anomalies. Use automated tools where possible to streamline these processes.

5. Key aspects related to cryptography policy in India

1. **IT Act, 2000:** The Information Technology Act, 2000 (IT Act) and its subsequent amendments provide the legal framework for electronic transactions and digital signatures in India. Section 84A of the IT Act empowers the government to prescribe modes or methods for encryption.
2. **Encryption Guidelines:** The Ministry of Electronics and Information Technology (MeitY) has issued guidelines on the use of encryption in India. These guidelines specify the methods and standards for encryption that entities, including government agencies and private organizations, should adhere to when securing sensitive data and communications.
3. **Key Management:** The guidelines also emphasize the importance of proper key management practices to ensure the security and integrity of encrypted data. This includes guidelines on the generation, storage, distribution, and destruction of cryptographic keys.

File No. ENE51-ITOSEC/7/2021-ACICSU (Computer No. 1485830)
Generated from eOffice by BALAJI MITTINTI, DEE(MB), DEPUTY EXECUTIVE ENGINEER, AP Transco on 02/01/2025 04:36 pm

9705313/2024/ACIDO GICU

4. **Data Localization:** As per the draft Personal Data Protection Bill (PDPB), certain categories of sensitive personal data must be stored and processed only within India. This has implications for the use of encryption to protect data within the country's borders.
5. **Regulatory Compliance:** Various sectors, such as banking, financial services, telecommunications, and healthcare, have their own regulatory requirements concerning encryption and data protection. These sectors must comply with sector-specific guidelines and standards while implementing encryption measures.
6. **Security and National Interest:** The Indian government reserves the right to regulate encryption and cryptographic technologies in the interest of national security and public order. This may include restrictions on the export/import of cryptographic products and services.
7. **International Standards:** India aligns its encryption policies and standards with international best practices and standards, ensuring interoperability and compatibility with global encryption technologies.

6. Challenges and Considerations

6.1. Balancing Security and Performance

Cryptographic operations can introduce performance overhead. Balance the need for strong encryption with the impact on system performance and user experience.

6.2. Interoperability

Ensure that cryptographic solutions are interoperable with existing systems and future technologies. This is particularly important in heterogeneous environments with diverse hardware and software.

6.3. Quantum Computing

Prepare for the potential impact of quantum computing on current cryptographic algorithms. Stay informed about post-quantum cryptography developments and plan for future migrations.

6.4. Vendor and Third-Party Dependencies

Assess and manage the risks associated with third-party cryptographic solutions and services. Ensure that vendors comply with the organization's cryptography policy and security standards.

By implementing a well-defined cryptography policy, organizations can significantly enhance their security posture and protect against the growing landscape of cyber threats.

= END=

File No. ENE51-ITOSEC/7/2021-ACICSU (Computer No. 1485830)
Generated from eOffice by BALAJI MITTINTI, DEE(MB), DEPUTY EXECUTIVE ENGINEER, AP Transco on 02/01/2025 04:36 pm