CYBER STANDARD DOCUMENT

Cryptography Standard

ABSTRACT:

This standard sets out the Cryptographic Algorithms to be used within policing. A list of algorithms are provided initially followed by applications and the associated cryptography required for each application. Finally the standard provides some commentary on the emerging cryptography for post quantum computing and lightweight computing.

This standard adheres to the National Policing Community Security Policy Framework and is a suitable reference for community members, notably those who build and implement IT systems on behalf of national policing.

ISSUED	May 2023
PLANNED REVIEW DATE	May 2024
DISTRIBUTION	Community Security Policy Framework Members

STANDARD VALIDITY STATEMENT

This document is due for review on the date shown above. After this date, the document may become invalid.

Members should ensure that they are consulting the currently valid version of the documentation.

Document Information

Document Location

PDS - National Policing Policies & Standards

Revision History

Version	Author	Description	Date
0.1	James Hyde	Initial version	10/3/2023
0.2	James Hyde	Minor revisions following NCPSWG approval	14/04/23

Approvals

Version	Name	Role	Date
1.0	NCPSB	National Cyber Policy & Standards Board	25/05/23

Document References

Document Name	Version	Date
ISF - Standard of Good Practice (for Information Security)	v2022	07/2022
ISO 27002:2022 - Information security, Cybersecurity and privacy protection – Information security controls	v2022	02/2022
CIS Controls	v8	05/2021
NIST Cyber Security Framework	v1.1	04/2018
CSA Cloud Controls Matrix	v4	01/2021
10 Steps to Cyber Security - NCSC.GOV.UK	Web Page	05/2021

Contents

Community Security Policy Commitment

National Policing and its community members recognise that threats to policing information assets present significant risk to policing operations. National Policing and its community members are committed to managing information security and risk and maintaining an appropriate response to current and emerging threats, as an enabling mechanism for policing to achieve its operational objectives whilst preserving life, property, and civil liberties.

This standard in conjunction with the National Policing Community Security Policy Framework and associated documents sets out National Policing requirements.

Introduction

This standard is intended to provide a baseline for the use of cryptography in policing. Cryptography has had to evolve as technology and computing power has increased to circumvent vulnerabilities in cryptographic algorithms. This document should assist those seeking to protect information using encryption to choose suitable algorithms and protocols to ensure confidentiality, integrity, authenticity and non-repudiation of data either in transit or at rest.

The standard outlines the cryptographic algorithms, key exchange algorithms, authentication methods in the first sections. Subsequent sections provide protocols that rely on cryptography and the common applications that use cryptography.

The final sections provide some commentary on emerging cryptographic standards particularly post quantum cryptography and lightweight cryptography.

The document does not provide a history of cryptography but focuses on the current standards that are relevant to policing systems and assumes that the reader is familiar with cryptographic principles.

Owner

National Chief Information Security Officer (NCISO).

Purpose

The purpose of this standard is to establish a set of cryptographic algorithms and protocols for use in specific applications for the transmission and storage of Police Data up to the classification of OFFICIAL. The requirements are the minimum acceptable levels of encryption and are aligned to the NIST and NCSC frameworks and are applicable to cloud environment, on premises environments and the data networks that interconnect them.

Cryptography relies heavily on the use of keys and this document does not provide a standard for key management which is documented elsewhere, but it must be borne in mind that even the most secure cryptographic solutions are only secure if the keys are sufficiently random, rotated regularly and protected against unauthorised access.

Computing power is continually increasing and any cryptographic algorithm can be compromised given enough time and sufficiently fast computing power, most cryptographic solutions rely on being sufficiently complex that the time taken even with the fastest computers is sufficiently long to discourage any attempt at compromise by brute force. This standard will need to be reviewed regularly to ensure that the algorithms remain suitable to protect police data see Review Cycle

.

Audience

This standard is aimed at:

- Staff across PDS and policing who build, implement and maintain ICT systems, either on behalf of National Policing or at a local force level.
- The user community, including those who have escalated privileges to provide administrative functions.
- Suppliers acting as service providers or developing products or services for PDS or policing.
- Auditors and penetration testers providing assurance services to PDS or policing

Scope

1. This standard is to cover systems handling data within the OFFICIAL tier including OFFICAL-SENSITIVE special handling caveat of the Government Security Classification Policy (GSCP). National policing IT systems, applications, or service implementations falling within this category will be subject to the requirements specified within this security standard. The requirements will be applied to new and existing installations.

2. The security control requirements laid out in this standard are vendor agnostic and applicable for all IT systems, applications, or service implementations that are provisioned for policing community of trust use.
3. Cryptography relies heavily on the use of Keys to secure encryption. This document does not include standards for key management.

Requirements

This section details the minimum requirements for cryptographic algorithms to protect policing data. Consideration must be given to Confidentiality, Authenticity, Integrity and Non-repudiation when selecting combinations of cryptographic algorithms, cryptographic keys, hash functions and authentication methods to ensure that sufficient end to end security is achieved.

Symmetric Key Block Cipher

Symmetric Key Block ciphers use a key that can be used to encrypt and decrypt data hence they are symmetric. They are suited to encrypting data blocks rather than continuous streams of data.

Reference	Minimum requirement	Control / Standard reference	Compliance Metric
Block Cipher	Advanced Encryption Standard (AES)	ISF TS.2, NIST CSF SC-8, SC-28, PR.DS-1, PR.DS-2 / FIPS 197,	Penetration testing, Configuration check, vulnerability assessment
Key length	128 bits		
Mode of operation	Galois Counter Mode (GCM)		
Authentication	Galois Message Authentication Code (GMAC) Hash-based Message Authentication Code (HMAC)		

Symmetric Key Stream Cipher

Symmetric Key Stream ciphers are used to encrypt and decrypt a stream of data and also use the same key to decrypt and encrypt data hence they are symmetric.

Reference	Minimum requirement	Control / Standard reference	Compliance Metric
Stream Cipher	ChaCha20	ISF TS.2, NIST CSF SC-8, PR.DS-2 / RFC 8439	Penetration testing, Configuration check, vulnerability assessment
Authentication	Poly1305		

Public Key Algorithms

Public Key Algorithms rely on a Public key infrastructure to manage keys. They consist of private keys that must be kept secret as they can be used to decrypt data and public keys which are shared and allow data to be encrypted but cannot decrypt the data. This is often referred to as one way encryption or asymmetric encryption as there are different keys used for encryption and decryption. They are most commonly used as a mechanism to share keys over a public network or to create unique digital signatures.

Reference	Minimum requirement	Control / Standard reference	Compliance Metric
Digital Signatures	Rivest Shamir Adleman (RSA) with a 2048 bit strength, Elliptic Curve Digital Signature Algorithm (ECDSA), Edwards-curve Digital Signature Algorithm (EdDSA)	ISF TS.2, NIST CSF SC-8, SC-28, PR.DS-1, PR.DS-2 / FIPS 186	Penetration testing, Configuration check, vulnerability assessment
Key exchange	Rivest Shamir Adleman (RSA) with a 2048-bit strength, Elliptic Curve Diffie Hellman Exchange (ECDHE) Group 19	ISF TS.2, NIST CSF SC-8, PR.DS-2 / SP 800-56A, SP 800-56B, RFC 8418	Penetration testing, Configuration check, vulnerability assessment

Cryptographic Hash Functions

Hash functions are used to map an arbitrary length string of bits to a string of fixed length. They are used in many applications such as message authentication, password storage and digital signatures. They can be further secured by adding additional padding to the input value before hashing which prevents rainbow table attacks. This is known as adding a salt.

Reference	Minimum requirement	Control / Standard reference	Compliance Metric
Hashing Algorithm	Secure Hash Algorithm 256 (SHA-256)[1]	ISF TS.2, NIST CSF SC-8, SC-28, PR.DS-1, PR.DS-2 / FIPS 180	Penetration testing, Configuration check, vulnerability assessment
Password Hashing	Secure Hashing Algorithm 256 (SHA-256) with unique random 128bit minimum salt for each hash	ISF TS.2, NIST CSF SC-8, SC-28, PR.DS-1, PR.DS-2 / NIST 800-132	Penetration testing, Configuration check, vulnerability assessment

[1] SHA3 is also now available as a complimentary algorithm to SHA 2 and NIST certified as FIPS 202

Security Protocols using Cryptography

There are several security protocols that are linked to cryptography and are used to underpin secure communications locally or over the internet. These are the minimum required versions that must be implemented. These protocols must be configured to use at least the minimum cryptography standards defined in the previous sections.

Reference	Minimum requirement	Control / Standard reference	Compliance Metric
Transport Layer Security	Transport Layer Security (TLS) 1.2[2]	ISF TS.2, NIST CSF SC-8, PR.DS-2 / RFC 5426, NCSC Guidance on TLS profiles	Penetration testing, Configuration check, vulnerability assessment
Internet Key Exchange	Internet Key Exchange (IKE) v2 preferred, v1 acceptable.	ISF TS.2, NIST CSF SC-8, PR.DS-2 / RFC 7296	Penetration testing, Configuration check, vulnerability assessment
Secure Shell	Secure Shell (SSH)-2	ISF TS.2, NIST CSF SC-8, PR.DS-2 / RFC 4251	Penetration testing, Configuration check, vulnerability assessment
Kerberos	Version 5	ISF TS.2, NIST CSF SC-8, SC-28, PR.DS-1, PR.DS-2 / RFC 4120	Penetration testing, Configuration check, vulnerability assessment
Security Architecture for the Internet Protocol	IPsec	ISF TS.2, NIST CSF SC-8, PR.DS-2 / RFC4301	Penetration testing, Configuration check, vulnerability assessment

[2] TLS 1.3 is now available, so consideration should be given to migration to TLS1.3, however 1.2 is the minimum standard at this point

Applications using Cryptography

Reference	Minimum requirement	Control / Standard reference	Compliance Metric
Site to Site Virtual Private Network (VPN)	IPSec, IKEv2, AES128GCM, HMAC-SHA256, Diffie-Hellman (DH) Group 19	ISF TS.2, NIST CSF SC-8, PR.DS-2	Penetration testing, Configuration check, vulnerability assessment
Remote Access VPN	IPSec, IKEv2, AES128GCM, HMAC-SHA256, DH Group 19	ISF TS.2, NIST CSF SC-8, PR.DS-2	Penetration testing, Configuration check, vulnerability assessment
SSL VPN	TLS1.2	ISF TS.2, NIST CSF SC-8, PR.DS-2	Penetration testing, Configuration check, vulnerability assessment
Database Encryption	Transparent Database Encryption (TDE) with AES128	ISF TS.2, NIST CSF SC-28, PR.DS-1	Penetration testing, Configuration check, vulnerability assessment
Whole Disk Encryption	AES128 with GCM	ISF TS.2, NIST CSF SC-28, PR.DS-1	Penetration testing, Configuration check, vulnerability assessment
File system Encryption	AES128 with GCM	ISF TS.2, NIST CSF SC-28, PR.DS-1	Penetration testing, Configuration check, vulnerability assessment
Web access	HTTPS using TLS1.2	ISF TS.2, NIST CSF SC-8, PR.DS-2	Penetration testing, Configuration check, vulnerability assessment
Email	TLS1.2 for email transport and Secure/Multipurpose Internet Mail Extensions (S/MIME) for individual message encryption	ISF TS.2, NIST CSF SC-8, PR.DS-2	Penetration testing, Configuration check, vulnerability assessment
Data transfer	Secure Copy(SCP) or Secure File Transfer Protocol (SFTP) using SSH-2	ISF TS.2, NIST CSF SC-8, PR.DS-2	Penetration testing, Configuration check, vulnerability assessment

Lightweight Cryptography

The National Institute of Standards and Technology (NIST) has announced that ASCON is the winning bid for the "lightweight cryptography" program to find the best algorithm to protect small IoT (Internet of Things) devices with limited hardware resources.

Small IoT devices are becoming increasingly popular and omnipresent, used in wearable tech and other applications on small devices. However, they are still used to store and handle sensitive data, financial details, and more.

Implementing a standard for encrypting data is crucial in securing data. However, the weak chips inside these devices call for an algorithm that can deliver robust encryption at very little computational power**.**

This area of cryptography is evolving and as more IoT devices are deployed it is important to remain vigilant to the cryptography capabilities of these devices and the data that is stored within them particularly while we wait for standardisation to be implemented.

Post Quantum Cryptography

Quantum computing threatens current asymmetric cryptography which relies on the difficulty in factoring large prime numbers.

Shor's algorithm can significantly improve the factorisation time using a quantum computer and therefore threatens traditional encryption algorithms.

Grover's algorithm could brute-force a 128-bit symmetric cryptographic key in roughly 2^{64} iterations, or a 256-bit key in roughly 2^{128} iterations. As a result, it is suggested that symmetric key lengths be doubled to protect against future quantum attacks

Although Quantum computers are not yet available at sufficient complexity to use these algorithms to decrypt, attackers could already be capturing encrypted data streams with a view to decrypting them once they have the capability.

NIST has called for proposals for post quantum algorithms for cryptography and there have been 4 rounds of submissions resulting in selected algorithms for 2022 being published.

The Selected Algorithms are currently as follows:

Public-key Encryption

- CRYSTALS-KYBER

Key-establishment Algorithms

- CRYSTALS-DILITHIUM
- FALCON
- SPHINCS+

It is essential that planning and adoption begins as soon as possible to incorporate post quantum cryptography into roadmaps to ensure that there is sufficient time to protect data once implementations are available and reduce the threat to existing data that may have been intercepted.

Communication approach

The Cryptography standard will be communicated as follows:

1. Internal peer review by the members of the National Cyber Policy & Standards Working Group (NCPSWG), which includes PDS and representatives from participating forces.

2. Presentation to the Nation Cyber Policy & Standards Board (NCPSB) for approval.

3. Formal publication and external distribution to PDS community, police forces and associated bodies.

For external use (outside PDS), this standard should be distributed within IT teams to help complete an initial gap analysis which can inform any implementation plan. This implementation plan can be shared with force SIROs / Security Management Forum. Consideration should also be given to raising awareness amongst force personnel of the implementation of this standard where it may affect them.

Measurables generated by adopting this standard can also form part of regular cyber management reporting.

Review Cycle

This Policy will be reviewed at least annually (from the date of publication) and following any major change to Information Assurance (IA) strategy, membership of the community, or an identified major change to the cyber threat landscape. This ensures IA requirements are reviewed and that the policy continues to meet the objectives and strategies of the police service.

Document Compliance Requirements

(Adapt according to Force or PDS Policy needs.)

Equality Impact Assessment

Forces should consider local impacts as a result of this standard being applied.