



# Cryptographic Standards and RFCs

Version 2023.1  
2024-07-11

InterSystems®, HealthShare Care Community®, HealthShare Unified Care Record®, IntegratedML®, InterSystems Caché®, InterSystems Ensemble®, InterSystems HealthShare®, InterSystems IRIS®, and TrakCare are registered trademarks of InterSystems Corporation. HealthShare® CMS Solution Pack™ HealthShare® Health Connect Cloud™, InterSystems IRIS for Health™, InterSystems Supply Chain Orchestrator™, and InterSystems TotalView™ For Asset Management are trademarks of InterSystems Corporation. TrakCare is a registered trademark in Australia and the European Union.

All other brand or product names used herein are trademarks or registered trademarks of their respective companies or organizations.

This document contains trade secret and confidential information which is the property of InterSystems Corporation, One Memorial Drive, Cambridge, MA 02142, or its affiliates, and is furnished for the sole purpose of the operation and maintenance of the products of InterSystems Corporation. No part of this publication is to be used for any other purpose, and this publication is not to be reproduced, copied, disclosed, transmitted, stored in a retrieval system or translated into any human or computer language, in any form, by any means, in whole or in part, without the express prior written consent of InterSystems Corporation.

The copying, use and disposition of this document and the software programs described herein is prohibited except to the limited extent set forth in the standard software license agreement(s) of InterSystems Corporation covering such programs and related documentation. InterSystems Corporation makes no representations and warranties concerning such software programs other than those set forth in such standard software license agreement(s). In addition, the liability of InterSystems Corporation for any losses or damages relating to or arising out of the use of such software programs is limited in the manner set forth in such standard software license agreement(s).

THE FOREGOING IS A GENERAL SUMMARY OF THE RESTRICTIONS AND LIMITATIONS IMPOSED BY INTERSYSTEMS CORPORATION ON THE USE OF, AND LIABILITY ARISING FROM, ITS COMPUTER SOFTWARE. FOR COMPLETE INFORMATION REFERENCE SHOULD BE MADE TO THE STANDARD SOFTWARE LICENSE AGREEMENT(S) OF INTERSYSTEMS CORPORATION, COPIES OF WHICH WILL BE MADE AVAILABLE UPON REQUEST.

InterSystems Corporation disclaims responsibility for errors which may appear in this document, and it reserves the right, in its sole discretion and without notice, to make substitutions and modifications in the products and practices described in this document.

For Support questions about any InterSystems products, contact:

**InterSystems Worldwide Response Center (WRC)**

Tel: +1-617-621-0700

Tel: +44 (0) 844 854 2917

Email: [support@InterSystems.com](mailto:support@InterSystems.com)

# Table of Contents

Cryptographic Standards and RFCs.....	1
---------------------------------------	---



# Cryptographic Standards and RFCs

The following are standards and RFCs (requests for comment) that define the cryptographic primitives and algorithms used in InterSystems security:

- AES (Advanced Encryption Standard) encryption — FIPS (Federal Information Processing Standards) 197
- AES Key Wrap —
  - NIST (National Institute of Standards and Technology) document “Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping” ([https://csrc.nist.gov/CryptoToolkit/kms/AES\\_key\\_wrap.pdf](https://csrc.nist.gov/CryptoToolkit/kms/AES_key_wrap.pdf))
  - IETF (Internet Engineering Task Force) RFC 3394
- Base64 encoding — RFC 3548
- Block padding — PKCS (Public-Key Cryptography Standards) #7 and RFC 2040
- CBC (Cipher Block Chaining) cipher mode — NIST 800-38A
- Deterministic random number generator —
  - FIPS PUB 140-2, Annex C
  - FIPS PUB 186-2, Change Notice 1, Appendix 3.1 and Appendix 3.3
- GSS (Generic Security Services) API —
  - The Kerberos Version 5 GSS-API Mechanism — RFC 1964
  - Generic Security Service Application Program Interface, Version 2, Update 1 — RFC 2743
  - Generic Security Service API Version 2: C Bindings — RFC 2744
  - Generic Security Service API Version 2: Java Bindings — RFC 2853
- Kerberos Network Authentication Service (V5) — RFC 1510
- Hash-based Message Authentication Code (HMAC) — FIPS 198 and RFC 2104
- Message Digest 5 (MD5) hash — RFC 1321
- Password-Based Key Derivation Function 2 (PBKDF2) — PKCS #5 v2.1 and RFC 8018
- Secure Hash Algorithm (SHA-1) — FIPS 180-2 and RFC 3174
- Secure Hash Algorithm (SHA-512) — FIPS 180-2 and RFC 6234

All these documents are available online:

- [FIPS documents](#)
- [NIST documents](#)
- [RFCs \(IETF\)](#)

