

Cryptography Security Standard

Information Security Branch, Ministry of Central Services

Last revised: December 2018
Last reviewed: December 2018
Next review: December 2019

This document outlines the Government of Saskatchewan security standards for Cryptography.

Table of Contents

1. Cryptographic Controls	2
1.1. Standard for the Use of Cryptographic Controls.....	2
1.2. Key Management.....	2

Reference Documents

The following documents are available on the IT Security Services Taskroom:

- [Cryptography Security Policy](#)
- [Cryptography Security Specification](#)

1. Cryptographic Controls

1.1. Standard for the Use of Cryptographic Controls

The cryptographic controls used to safeguard an information system must be based on the sensitivity of the information and include consideration of:

- integrity requirements (e.g. financial payment instructions in excess of a specified amount);
- non-repudiation requirements;
- authentication requirements;
- other security requirements (e.g. proof of origin, receipt or ownership);
- legislation, regulations, standards or policies requiring the use of cryptography;
- restrictions on the export or use of cryptographic products; and
- risks related to long-term storage of electronic information (e.g. recovery of encrypted data, long-term key maintenance).

1.2. Key Management

No standards currently published.