Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

CANADIAN CENTRE FOR
CYBER SECURITY

Recommended contract clauses for cryptography

Management

Canada

Foreword

This is an UNCLASSIFIED publication, issued under the authority of the Head of the Canadian Centre for Cyber Security (Cyber Centre). For more information, contact the Cyber Centre:

- Email: contact@cyber.gc.ca
- Phone: 613-949-7048 or 1 833 CYBER 88

Effective date

This publication takes effect on September 2025.

Revision history

Revision	Amendments	Date
1	First release.	September 1, 2025

D97-4/00-501-2025E-PDF
ISBN 978-0-660-78902-6

Overview

As your organization increases the use of cryptography to protect your infrastructure and data, there is a growing need to ensure that your organization purchases products and services that provide effective protection. Whether procuring a single-use product or contracting with a service provider such as a cloud service provider (CSP), your organization must consider certain elements to ensure that the product or service will meet your needs. This publication provides advice and guidance on what to consider when procuring products and services that use cryptography, including example clauses.

Table of contents

1 Introduction 5

1.1 Scope 5

2 Cryptographic considerations 6

2.1 Product considerations 6

2.1.1 Recommended cryptographic algorithms 6

2.1.2 Cryptographic agility 7

2.1.3 Cryptographic certification 7

2.2 Considerations for service providers and cloud services 8

2.2.1 Post-quantum cryptography 8

2.2.2 Configuration 8

2.2.3 Using validated cryptographic modules and algorithms 9

3 Terms and conditions 10

4 Conclusion 11

1 Introduction

The guidance in this publication highlights important security considerations for your organization when purchasing products and services that use cryptography. This includes but is not limited to service providers and cloud service providers (CSPs).

While vendors may present initial foundational terms and conditions, your organization's management team is responsible for demonstrating and validating that the terms and conditions and the contract's supporting security clauses address your organization's business security needs.

The terms and conditions should be adaptable for future modifications to safeguard the interests of your organization. The terms and conditions in the service contract should also provide your organization with the best possible business outcomes. Your organization must initiate proactive measures to ensure service provisions include cyber security mechanisms for identifying, communicating, mitigating and preventing risks.

This publication outlines cryptographic considerations that should be factored in alongside the primary functional and legal contracting aspects when working with a vendor.

The clauses outlined in this publication should not be considered legal advice. Rather, they offer context for your organization and can help your organization determine considerations and questions to ask when procuring cryptographic products and services.

1.1 Scope

The Cyber Centre provides advice and guidance on selecting and using cryptographic algorithms to protect the authenticity, confidentiality and integrity of sensitive information. This publication provides advice and guidance on what to consider when engaging with a vendor to purchase products or services that use cryptography for the protection of UNCLASSIFIED, PROTECTED A and PROTECTED B information.

Disclaimer: The Communications Security Establishment Canada (CSE) and its Cyber Centre do not recommend or endorse the use of any particular contracting clause listed in this publication. The example clauses provided are only intended to be a source of examples of contract clauses that may be useful for procuring products and service that use cryptography and are provided for informational purposes only. We recommend seeking legal and procurement advice when using these clauses to ensure that they meet your organization's requirements.

2 Cryptographic considerations

To protect the confidentiality, integrity and authenticity of your organization's data, you must ensure that all infrastructure effectively uses strong cryptography for both on-premises environments and service provider environments. This includes cloud environments.

The following sections present items that should be considered when engaging with vendors. The considerations discuss cryptographic algorithms, modules and parameters to support organizations in following Cyber Centre guidance.

Section 2.1 Product considerations outlines considerations to be taken when purchasing products and focuses on the requirements of the products being purchased. Section 2.2 Considerations for service providers and cloud services provides advice and guidance for engaging with service and cloud providers and focuses on how the vendor selects, configures and uses cryptography.

2.1 Product considerations

This section provides product considerations and example contract clauses to use when purchasing products that support cryptography. The clauses have been developed for products that have built-in cryptographic modules, such as virtual private networks (VPN) and other network appliances that support cryptography natively. These considerations can also be used to develop requirements for generic computing devices that will have software installed after purchase (for example, servers).

Note: The Cyber Centre publication Cryptographic algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B information (ITSP.40.111) is updated regularly as advice and guidance changes. Any clauses that are used to procure products and that reference ITSP.40.111 should specify the publication version.

2.1.1 Recommended cryptographic algorithms

Contractual clauses should ensure that cryptographic modules use algorithms recommended in ITSP.40.111 that meet your system requirements. Additionally, to avoid extra costs during the migration to post-quantum cryptography (PQC), we recommend that all newly procured cryptographic modules support appropriate PQC algorithms.

The following clauses recognize that some vendors do not currently support PQC and that some standards that will use the algorithms may still be under development. By specifying a date by which the vendor must provide PQC capabilities, your organization can purchase from the vendor when needed without waiting for the vendor to have PQC capable products. The vendor will be required to provide upgrades to the cryptographic modules on or before the date specified.

Example clause structure and language

- Cryptographic modules must use only CSE-approved cryptographic algorithms with cryptographic parameter sizes and key lengths as specified in Cryptographic algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B information (ITSP.40.111).
- By the end of 2026, cryptographic modules implementing key establishment schemes must support appropriate post-quantum cryptography compliant with Cryptographic algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B information (ITSP.40.111).

- By the end of 2026, cryptographic modules implementing digital signature schemes must support appropriate post-quantum cryptography compliant with Cryptographic algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B information (ITSP.40.111).

2.1.2 Cryptographic agility

Using systems that support cryptographic agility enables organizations to reconfigure or upgrade cryptographic technologies as needed. This is important because progress in cryptographic research, vulnerability research and computing can lead to cryptographic deployments with less strength than when they were initially deployed. Products should have the capability to modify parameters, such as key lengths, parameter sizes and key lifetimes, and to select cryptographic algorithms without replacing software or hardware components. This will reduce both the expense and time needed for purchasing new infrastructure. Products must also have the critical ability to securely patch systems that use cryptography to ensure that vulnerabilities are mitigated as they are discovered.

For more information on cryptographic agility, read our publication Guidance on becoming cryptographically agile (ITSAP.40.018).

Example clause structure and language

- Cryptographic modules must support cryptographic agility by providing cryptographic algorithms, parameter sizes, key lengths and crypto periods that are configurable.
- Cryptographic modules must support vendor-signed patches and updates.

2.1.3 Cryptographic certification

We recommend that all cryptographic modules be validated through the Cryptographic Module Validation Program (CMVP). The CMVP is jointly managed by the Cyber Centre and the National Institute of Standards and Technology (NIST). It ensures that vendors implement cryptography correctly in their products and that they follow Cyber Centre–recommended security best practices. To find validated modules, organizations can search the database of CMVP-validated modules, which is hosted by NIST. Cryptographic algorithms used in the modules should be validated by the Cryptographic Algorithm Validation Program (CAVP).

CMVP certification is specific to the details provided in the security policy available on the product certificate webpage. It is important that products use the cryptographic module according to that security policy. This ensures with a high degree of certainty that the module will provide the expected security services in the expected manner.

Example clause structure and language

- Cryptographic algorithms must be validated by the Cryptographic Algorithm Validation Program (CAVP) with a certificate listed on the CAVP validation list.
- Cryptographic modules must be validated by the Cryptographic Module Validation Program (CMVP) with an active CMVP certification and a certificate number listed on the CMVP-validated modules list.
- Cryptographic modules must be applied in accordance with the cryptographic module security policy listed on the CMVP-validated modules list, in either an approved or an allowed mode.

2.2 Considerations for service providers and cloud services

Organizations that outsource IT infrastructure or software solution management to cloud vendors or service providers must consider the cryptography used to protect the information. This section provides additional cryptographic considerations when contracting a service or cloud provider.

Your organization should ensure that contracting requirements obligate the contractor to maintain IT systems that are aligned with current cryptographic guidance. In addition to this publication, the Cyber Centre publication Recommended cyber security contract clauses for cloud services (ITSM.50.104) provides general procurement clauses and considerations when acquiring cloud-based solutions or services

Note: We recommend that contracts with service providers ensure contractors remain current with the latest versions of ITSP.40.111 and our Guidance on securely configuring network protocols (ITSP.40.062). As such, clauses that reference either ITSP.40.111 or ITSP.40.062 should not reference a specific version or publication date and should require contractors to remain aligned with current Cyber Centre recommendations.

2.2.1 Post-quantum cryptography

We recommend that all cryptographic modules support CSE-approved PQC algorithms as soon as they are available. The following clauses allow organizations to procure from service providers as needed, with the understanding that the cryptographic modules must be migrated to support PQC no later than the date specified. This approach provides flexibility to both the purchaser and the vendor while ensuring that the PQC migration is not delayed or more costly than necessary.

Example clause structure and language

- By the end of 2026, cryptographic modules implementing key establishment schemes must support appropriate post-quantum cryptography compliant with Cryptographic algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B information (ITSP.40.111).
- By the end of 2026, cryptographic modules implementing digital signature schemes must support appropriate post-quantum cryptography compliant with Cryptographic algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B information (ITSP.40.111).

2.2.2 Configuration

Cryptography should be configured to operate according to the advice and guidance provided in the Cyber Centre's publications ITSP.40.111 and ITSP.40.062. Following the most recent versions of these publications will help to keep your environment secure as cryptographic guidance evolves. Additionally, we recommend that cryptography is configured and operated in an approved or allowed mode found in the CMVP security policy.

Example clause structure and language

The Contractor must:

- configure systems to only permit use of cryptography in accordance with CSE-approved cryptographic algorithms and cryptographic parameter sizes, key lengths and key lifetimes, as specified in Cryptographic algorithms for

UNCLASSIFIED, PROTECTED A, and PROTECTED B information (ITSP.40.111) and Guidance on securely configuring network protocols (ITSP.40.062)

- ensure these policies remain consistent with any subsequent published versions

2.2.3 Using validated cryptographic modules and algorithms

Similar to Section 2.1.3 Cryptographic certification on procuring products, we recommend that only algorithms and modules that have been validated by CAVP and CMVP be used in cloud and service provider environments, respectively.

Example clause structure and language

- Cryptographic algorithms permitted to operate must be validated by the Cryptographic Algorithm Validation Program (CAVP) with a certificate listed on the CAVP validation list.
- Cryptographic modules must be validated by the Cryptographic Module Validation Program (CMVP) with an active CMVP certification and a certificate number listed on the CMVP-validated modules list.
- Cryptographic modules must be applied and operated in accordance with the cryptographic module security policy listed on the CMVP-validated modules list, in either an approved or an allowed mode.

3 Terms and conditions

A vendor or contractor may already have terms and conditions they use when selling their products and services. Many of the clauses recommended in this publication may be covered using different contractual language (for example, referencing NIST publications rather than Cyber Centre publications).

In these situations, we recommend that organizations carefully compare the recommended clauses with the ones presented by the vendor, as well as any documents that the vendor references. This will help to ensure that the product or service that your organization purchases will meet your cryptographic requirements. As with all situations, when dealing with legally binding contracts, we recommend seeking legal advice.

4 Conclusion

Cryptography provides an important means to protect your organization's IT environments, whether in the cloud or managed on premises. However, it is important to ensure that the cryptographic products that these systems use to protect your data are sufficiently strong and secure. Using products that meet the Cyber Centre's recommendations on cryptography, including validations by CAVP and CMVP, will help provide effective data confidentiality and integrity.

This guidance has been provided for general knowledge and guidance for any organization purchasing cryptographic products or using them in their environments. As indicated, this is not legal advice.