Ministry of the Interior and Kingdom Relations

Framework cryptography policy for the Central Government

Framework for drafting a cryptography policy

Building strong foundations. For the Netherlands and for the Kingdom.

Table of contents

1 Introduction 4
1.1 Introduction 4
1.2 Objective 4
1.3 Scope of application 4
1.3.1 Organisational scope 4
1.3.2 Substantive scope 4
1.3.3 Explanation of the application 5
1.4 Target groups 5
1.5 Document management 6
1.6 Reading guide 6

2 Context, vision and strategy 7
2.1 Context 7
2.2 Vision 7
2.3 Strategy 7
2.3.1 Specification of policy by organisations themselves 7
2.3.2 Framework for cryptography policy 7
2.3.3 List of technical aspects of cryptography 8

3 Framework for cryptography policy 9
3.1 Introduction 9
3.1.1 Objective 9
3.1.2 Target group 9
3.1.3 Scope of this policy 9
3.1.4 Policy coordination with other organisations 9
3.1.5 Policy management 9
3.1.6 Definitions and abbreviations 9
3.2 Frameworks 10
3.2.1 Normative frameworks 10
3.2.2 Informative frameworks 10
3.3 Principles and starting points 10
3.4 Responsible parties 11
3.4.1 Person with ultimate responsibility 11
3.4.2 Persons responsible for policy 11
3.4.3 Persons responsible for implementation 11
3.4.4 Persons responsible for assessing 11
3.5 Processes 11
3.5.1 Asset management 12
3.5.2 Design and development 12
3.5.3 Procurement and vendor management 12
3.5.4 Change management 12
3.5.5 Vulnerability management 12
3.5.6 Incident management 12
3.5.7 Logging, monitoring and anomaly detection 12
3.5.8 Business continuity management 12
3.5.9 Backup and recovery 13
3.5.10 Archiving 13
3.5.11 Auditing 13

3.6 Personnel 13
3.6.1 Screening 13
3.6.2 Qualifications and training 13
3.7 Use of cryptography 13
3.7.1 Applications of cryptography 13
3.7.2 General technical cryptography requirements 13
3.7.3 Application-specific cryptography requirements 13
3.8 Key management 14
3.8.1 Lifecycle of cryptographic keys 14
3.8.2 Other aspects of cryptographic key management 14
3.9 Use of certificates 14
3.9.1 Applications of certificates 14
3.9.2 Requirements for being able to rely on certificates 14
3.9.3 General technical requirements for certificates 14
3.9.4 Application-specific requirements for certificates 15
3.10 Certificate management 15
3.10.1 Lifecycle of certificates 15
3.10.2 Other aspects of certificate management 15
3.11 Preparation for future developments 15
3.12 Other aspects 16
3.12.1 Legal aspects 16
3.12.2 Physical aspects 16
3.12.3 Other aspects 16

4 List of technical aspects of cryptography 17

Appendix A: Chapter structure for cryptography policy 18

Appendix B: Policy requirements from BIO, ISO 27002 and NIS2 19

Appendix C: References 20

Appendix D: Abbreviations 21

1 Introduction

1.1 Introduction

This document presents the policy framework cryptography for the Central Government. Cryptography includes, among other things, encryption, digital signatures, cryptographic key management, and the use and management of certificates.

This document describes the generic aspects of preparing cryptography policies within the Central Government. It is intended to provide government bodies with relevant frameworks that guide the processes, architecture, and design principles surrounding cryptography.

This document is a prescriptive tool for preparing cryptography policy, but it is not an introduction to cryptography. The reader is expected to have a basic understanding of cryptography. In practice, preparing cryptography policy can be complex. This document will assist the reader in developing this policy and provides a framework for describing their own policy clearly and completely.

1.2 Objective

This government-wide policy framework for cryptography prescribes mandatory requirements for cryptography policy within the Central Government. The Interdepartmental Committee on Government Operations (ICBR) adopts this policy framework. The policy framework provides uniformity in policy and language regarding cryptography within the Central Government. Based on this framework, all government bodies can formulate their own policies.

As such, it serves as a tool for developing an effective cryptography policy. This allows organisations, among other things, to prepare in a timely manner for emerging threats and take appropriate measures.

1.3 Scope of application

1.3.1 Organisational scope

This policy framework applies to the Central Government. According to Section 2 of the Civil Service CIO Scheme Decree 2021 [*Besluit CIO-stelsel Rijksdienst 2021*], the Central Government comprises the core departments of the ministries and the units that fall under them. The cryptography policy of these organisations must align with this policy framework. This policy framework can be translated into organisation-specific cryptography policy, ensuring the policy framework fits within the system of the relevant department.

In addition, these organisations must impose the same requirements on their vendors when carrying out contracts for the Central Government. Other government organisations and private parties can use this framework within their own contexts. For these organisations, the framework can be used as a guideline, without any formal obligation.

1.3.2 Substantive scope

This policy framework is prescriptive for all applications of cryptography to achieve information security objectives – including confidentiality, integrity, authenticity, non-repudiation and authentication – for unclassified information and classified information up to and including the level '*Departementaal VERTROUWELIJK*', Dep.V, within the Central Government.

The policy framework applies to all processes and information systems in which cryptography is used. This includes the management of cryptographic keys and the use and management of certificates. It also covers, among other things, the configuration, development, management and procurement of hardware, software and outsourced services such as cloud services.

This policy framework is not prescriptive for applications of cryptography on classified information at the level '*Staatsgeheim CONFIDENTIEEL*', Stg.C, and higher. Various clear regulations apply to this, such as the Civil Service Information Security Classified Information Decree 2013 (VIRBI 2013), | and applying this policy framework would add little. Nevertheless, for the sake of comparability of policies and consistency in use of language, it is recommended that, where possible, this policy framework and in particular the given framework be used for such applications.

Adjacent aspects of information security, such as access control – including Identity and Access Management (IAM) and the management of secret authentication information (secrets management) – fall (largely) outside the scope of this policy framework. Where cryptography is used in such cases, that part does fall within the scope of this policy framework.

Where an organisation (unit) is bound by sectoral legislation and regulations that also contain requirements for cryptography, the said legislation and regulations apply primarily. No Comply or Explain policy is required here. These regulations may, for example, come from the Dutch government, the European Union, the ICAO (International Civil Aviation Organisation) or NATO (North Atlantic Treaty Organisation).

1.3.3 Explanation of the application

This policy framework focuses on the 'what', not the 'how', and identifies the aspects that must be included in the organisation's cryptography policy for the correct and effective application of cryptography.

Based on this framework, specific policies can be determined at the level of a department, organisation, or system. Existing departmental and organisational policies will need to be adjusted to align with this government-wide policy framework.

The aspects of the cryptography policy do not need to be described in a single, overarching policy document; it is in a free format. This means they can also be included in, or referenced from, various documents covering those aspects, such as lifecycle management or change management. This applies to both the departmental level and the levels below.

1.4 Target groups

This policy framework provides for a primary and a secondary target group.

The primary target group consists of:
- Departmental Chief Information Security Officers (CISOs);
- Cryptography policymakers within the Central Government; and
- Security Authorities (BVAs) and Security Coordinators (BVCs).

For the primary target group (within the Central Government, also refer to 1.3.1 Organisational scope), this policy framework is mandatory and they will have to translate this policy framework into their own policy.

The secondary target group consists of:
- Crypto custodians within the Central Government;
- Others who have to make choices or are interested in the application of cryptography within the Central Government; and
- Auditors who monitor the specifics and implementation.

This policy framework is intended to be informative for the secondary target group, and they can use it when making choices regarding cryptography or when organising their work.

Government bodies that do not fall under the Central Government, and other organisations are advised to follow this policy framework.

1.5 Document management

This document was prepared by representatives of:

- the Ministry of the Interior and Kingdom Relations (BZK);
- the Ministry of Finance (MinFin);
- the Ministry of Health, Welfare and Sport (VWS);
- Logius;
- ICT Implementation Service (DICTU);
- the Tax Administration;
- the Netherlands Police;
- the National Office for Identity Data (RvIG); and
- the Central Government Real Estate Agency (RVB).

This document was reviewed by representatives of:

- the Central Government Audit Service (ADR);
- the Netherlands Court of Audit (AR);
- the Ministry of Defence (MinDef);
- the Ministry of Justice and Security (JenV);
- the Employee Insurance Agency (UWV);
- the General Intelligence and Security Service (AIVD);
- the National Cyber Security Centre (NCSC); and
- the Netherlands Organisation for Applied Scientific Research (TNO).

This document is managed by BZK/CIO Rijk (BZK/CIO Government).

This document is adopted by the CIO-beraad (CIO Consultations).

This document is revised every two years.

This document is published at https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/quantumveilige-cryptografie/.

Please send an email with your questions and remarks to: QvC-NL@rijksoverheid.nl.

1.6 Reading guide

This policy framework contains a 'framework for cryptography policy' and a 'list of technical aspects of cryptography' about which choices must be made.

The core of this document can be found in Chapters 2 through 4:

- Chapter 2 explains how this framework and list can help organisations develop a robust cryptography policy of their own.
- Chapter 3 then describes the framework to be used when preparing organisation-specific cryptography policies.
- Chapter 4 contains a list of technical aspects of cryptography in respect of which an organisation must make choices and establish requirements.

Additional information can be found in the subsequent Appendices:

- The recommended chapter structure for cryptography policy, to facilitate collaboration, comparison, and testability.
- A summary of policy requirements from BIO, ISO 27002, and NIS2, along with an explanation of how, through proper application of the framework and the list, these requirements are adequately met.
- A list of references in which this document has been reviewed and to which references are made in this document.
- An overview of the abbreviations used in this document.

2 Context, vision and strategy

2.1 Context

Cryptography is used to achieve various information security objectives, such as confidentiality, integrity, authenticity, non-repudiation and authentication.

Organisations belonging to the Central Government are, based on the Government Information Security Baseline (BIO), required to develop and implement policies regarding the use of cryptographic control measures and key management policies. For most government organisations, a cryptography policy is also required under the Network and Information Security Directive (NIS2 Directive). In practice, this proves difficult to implement, often because it is unclear what exactly should be included in this kind of policy. This then results in policies that are limited in content, difficult to implement, or difficult to test.

At the same time, organisations within the Central Government must be prepared for future developments, both unexpected and anticipated. Examples of (sometimes unexpected) developments in the past include the MD5 and SHA-1 hash functions proving to be weak, the vulnerabilities that led to the Heartbleed, Spectre, Krack, or Efail attacks or the need to replace DigiNotar certificates. Expected future developments include changing requirements for TLS connections or preparing for the arrival of the quantum computer through quantum-safe cryptography.

The Central Government wants to continue connecting with national, European and global developments in the field of cryptography.

2.2 Vision

This policy framework was written with the vision that the Central Government has a grip on current cryptographic applications within government organisations and is able to respond promptly to relevant cryptographic developments.

2.3 Strategy

To achieve the above vision, substantively strong policy, good implementation thereof and assessment of both the policy and the implementation are required.

2.3.1 Specification of policy by organisations themselves

In line with the agreements in the CIO scheme, the actual specification of the policy is up to the departments and underlying organisations themselves. This allows for organisation-specific implementation. The policy framework therefore describes 'what' should be included in policy and provides direction where necessary, but leaves the implementation of the 'how' to the departments and underlying organisations.

The policy framework supports this implementation. It contains a 'framework for cryptography policy'. It also includes a list of technical aspects of cryptography in respect of which choices must be made. Based on this, an organisation can develop and implement its own policy.

2.3.2 Framework for cryptography policy

Central to the policy framework is a framework for cryptography policy. This framework contains the elements expected in the policies developed by the organisations. It also prescribes a (chapter) division of topics and provides a brief explanation of the expected specification for each topic.

Government organisations then develop cryptography policy based on this framework, or test existing policy against it.

The benefits of using the framework are:

- The policy maker knows which components should be included in the policy and what the expected implementation of each component is.
- Developed policies can be compared and exchanged between organisations, making it easier to develop high-quality policies.
- A uniform interdepartmental language is being created around cryptography, key management and certificates, which promotes mutual exchange of knowledge and support, and standardises communication with vendors.

- Auditing parties (such as the Central Government Audit Service and the Netherlands Court of Audit) can use the framework and policy framework to assess policy and implementation in a uniform manner. This also allows them to compare individual organisations using the same framework. It provides clear guidance on which components and principles are expected in policy and implementation, which auditors can then use to base their standards on. In addition, it becomes easier for government organisations to prepare for an audit, as it is clear which components and principles are expected in policy and implementation.

2.3.3 List of technical aspects of cryptography

When developing an effective cryptography policy, it is essential to make decisions about various technical options. This includes establishing a technical baseline with overviews of permitted cryptographic algorithms, key lengths, protocol settings, certificate types, the completion of certain certificate fields, and so on. These choices can be incorporated into the policy or determined by reference to relevant standards. The *Forum Standaardisatie* (Standardisation Forum) currently prescribes various cryptographic standards, without specifying the specific technical settings. For Transport Layer Security (TLS) and its use in HTTPS, various technical minimum requirements have already been established in the 'Secure Connections to Government Websites and Web Applications Decree' [*Besluit beveiligde verbinding met overheidswebsites en -webapplicaties*]. These regulations often lack clarity regarding suitable technical options for applications other than TLS. There is no clear (government-wide) baseline yet for several more common cryptographic options. Therefore, this policy framework contains a list of technical aspects that organisations should decide on in their policy or underlying documents.

The implementation of the 'how' regarding cryptography policy depends heavily on organisation-specific aspects. However, a technical baseline for cryptography can be largely the same for all government organisations. In addition, making such technical decisions requires (cryptographic) expertise that is limited within the departments and underlying organisations.

Therefore, such a baseline could eventually be established and managed for the Central Government. Once a government-wide technical baseline for cryptography is available, it could be imposed on an 'Comply or Explain' basis. Until a government-wide baseline exists, each organisation will have to determine its own technical choices based on reliable external standards. This policy framework proposes several suitable sources for this purpose.

3 Framework for cryptography policy

This chapter provides a framework for cryptography policy. It prescribes the topics that should be addressed in cryptography policy. For each topic, a brief explanation is provided of what is expected in the specification of the topic.

The following topics are mandatory in organisation-specific cryptography policies. It is recommended that you adopt the proposed chapter structure in 'Appendix A: Chapter structure for cryptography policy' in your own specifications.

The text below provides some guidelines for implementing these topics. However, the framework does not prescribe a precise implementation. When developing the organisation-specific cryptography policy, it is important to ensure that the requirements of the normative frameworks are met.

3.1 Introduction

This chapter provides an introduction to the policy.

3.1.1 Objective

This section describes the policy objective. It explains the importance and use of cryptography. Remember that by correctly and fully applying cryptography, the organisation can protect information at any desired or mandatory level, up to and including Dep.V, against loss of confidentiality, integrity, authenticity, non-repudiation, or authentication. Examples of derived objectives include:

- Managing, reducing, and mitigating risks related to data storage, transport, and processing.
- Protecting information and data in terms of availability, integrity, confidentiality, and non-repudiation, both now and in the future.
- Maintaining an overview of all cryptographic applications and cryptographic materials used by the organisation.
- Ensuring that the organisation complies with relevant legislation, standards, and guidelines regarding cryptography.
- Ensuring future-proofness by using appropriate forms of cryptography, including quantum-safe cryptography.
- Developing requirements and preferences for the procurement of information systems.
- Providing implementation guidelines, such as ensuring crypto agility and using standard crypto libraries.

3.1.2 Target group

This section describes the target group for the policy. It will usually align with the target group for the other information security policies of the organisation.

3.1.3 Scope of this policy

This section describes the scope of cryptography application within the organisation. This scope includes the application of cryptography for encryption and signing, the management of cryptographic keys, and the use and management of certificates.

3.1.3.1 Scope of cryptography application

This section clearly defines the scope of application covered by this policy. At a minimum, specify the organisational and substantive scope of the policy. Where possible, follow section 1.3, Scope of application, of this policy framework.

3.1.3.2 Limitations and exclusions

This section describes the limitations and exclusions to this policy. Consider, for example, the policy regarding the use of cryptographic resources for classified information from level '*Staatsgeheim CONFIDENTIEEL*', Stg.C, onwards; Such policies may be integrated into this policy or exist separately.

3.1.4 Policy coordination with other organisations

When communicating between different organisations, the policy must also be adopted mutually (in accordance with BIO 10.1.1.1 / BIO2 8.24.01).

3.1.5 Policy management

This section describes how the cryptography policy is managed. It includes where the policy can be found, how questions and comments on the policy can be communicated, when the policy is updated, and how the policy is approved and adopted.

3.1.6 Definitions and abbreviations

This section provides a list of definitions and abbreviations to clarify the policy for the target group where necessary.

3.2 Frameworks

This chapter addresses the normative and informative frameworks consulted in developing the policy.

3.2.1 Normative frameworks

This section contains a list of legislation and regulations related to cryptography that must be followed, and which were taken into account in developing the policy and implemented where necessary. Consider, for example:

- the organisation's information security policy;
- the organisation's cloud policy;
- legislation and regulations, such as:
  - (the Dutch Implementation Act for) the Network and Information Security Directive (NIS2 Directive);
  - the Civil Service Data Security 2007 (VIR 2007) [Voorschrift Informatiebeveiliging Rijksdienst 2007];
  - the Civil Service Data Security – Special Information 2013 (VIRBI) [Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013];
  - the Civil Service CIO Scheme Decree 2021 [*Besluit CIO-stelsel Rijksdienst 2021*];
  - the Civil Service Security Authority Scheme Decree 2021 [Besluit BVA-stelsel Rijksdienst 2021];
  - the Public Records Act [Archiefwet] (1995), followed by the Public Records Decree [Archiefbesluit] and the Public Records Regulations [Archiefregeling];
  - the General Data Protection Regulation (GDPR);
  - the European regulation regarding 'electronic IDentification, Authentication and trust Services' (eIDAS);
  - the Artificial Intelligence Regulation (AI Regulation); and
  - the Cyber Resilience Act (CRA);
  - the most recent version of the Government information security baseline (BIO);
  - the list of 'Comply or Explain' standards of the *Forum Standaardisatie* (Standardisation Forum);
  - the Secure Connections to Government Websites and Web Applications Decree' [Besluit beveiligde verbinding met overheidswebsites en -webapplicaties], and subsequently the ICT security guidelines for Transport Layer Security (TLS); and
  - National Communications Security Regulations (VBVs) of the National Communications Security Agency (NBV) of the AIVD;
  - other applicable (inter)national policies and standards for cryptography, key management and certificates of a mandatory nature.

3.2.2 Informative frameworks

This section contains a list of documents and standards that are not mandatory, but can serve as background information when developing the policy. Consider:

- the list of recommended standards of the Forum Standaardisatie;
- fact sheets, advice and guidelines from the National Cyber Security Centre (NCSC), if these are not mandatory;
- lists of approved crypto equipment on the website of the NBV of the AIVD and the public lists on the internet of approved crypto equipment of the EU and NATO;
- recommendations and guidelines from the German Bundesamt für Sicherheit in der Informationstechnik (BSI);
- recommendations and guidelines from the French Agence nationale de la sécurité des systèmes d'information (ANSSI);
- recommendations from the European Union Agency for Cybersecurity (ENISA);
- recommendations and guidelines from the American National Institute of Standards and Technology (NIST);
- standards of the European Telecommunications and Standardisation Institute (ETSI) in relation to electronic signatures and infrastructures;
- recommendations from the Open Worldwide Application Security Project (OWASP) in the field of cryptography; and
- the PQC Migration Handbook of the AIVD, TNO and CWI (National Research Institute for Mathematics and Computer Science in the Netherlands);
- other relevant (inter)national policies and standards for cryptography, key management and certificates with an informative nature.

3.3 Principles and starting points

This chapter outlines the principles and starting points behind the policy. Possible principles and starting points include: *'the policy complies with the stated normative frameworks (compliance)'* and *'the choices made in the policy are risk-based.'* The implications of these principles and starting points may be further elaborated in this chapter.

3.4 Responsible parties

This chapter describes the responsibilities surrounding cryptography and the handling of cryptographic materials (such as keys and certificates). Cryptography is made possible by technology, but organisational aspects are also crucial for the successful application of cryptography. An appropriate organisational structure, in which agreements were made and recorded, such as the design of processes, procedures and responsibilities for cryptography should be described.

Describe how responsibilities and authorities within the crypto organisation are established and assigned. Link this to government-wide frameworks and schemes (e.g., BIO, CIO scheme, BVA scheme). Also specify the roles and positions of the (official) management, directors, and officers.

3.4.1 Person with ultimate responsibility

This section describes who is ultimately responsible for the correct and effective use of cryptography to protect the confidentiality, authenticity, and/or integrity of information. Follow the standards of the CIO and BVA schemes.

3.4.2 Persons responsible for policy

This section describes who is responsible for cryptography policy.

At a minimum, include: who drafts the policy, who approves it, the policy's validity, who is responsible for keeping it up to date, and who is responsible for implementing the policy (in accordance with BIO 10.1.1.1). Ensure this aligns with the implementation of section 3.1.5, Policy management.

3.4.3 Persons responsible for implementation

This section describes who is responsible for implementing the cryptography policy. Indicate which roles are recognised, with a description of each role and its responsibilities.

Clearly describe how the roles for creating, modifying, and delivering cryptography, cryptographic keys, and certificates are assigned within the organisation. Identify who is responsible for the registration, application, (physical) delivery, and verification of cryptography, keys, certificates, and other related items.

Describe the roles for key management and certificate management: for example, make the line manager responsible for ensuring that each key and certificate is assigned an owner (also refer to the considerations regarding key and certificate management in the BIO, regarding key management in ISO 11770, and regarding certificate management in RFC 3647). Where necessary, consider the separation of duties and the four-eyes principle.

If applicable, describe the role of the crypto custodian.

Also describe the role of the end user. Describe the responsibilities of cryptography end users. For example: Users must check the crypto assets in their possession on a daily basis.

3.4.4 Persons responsible for assessing

This section describes who is responsible for assessing the policy specification and its implementation (compliance). This includes the following aspects: who assesses the policy specification and implementation (compliance), who performs audits (also refer to Auditing under the Chapter Processes), and who is responsible for the assessment of the specification of and the compliance with the cryptography policy.

3.5 Processes

This chapter outlines the processes needed to properly manage cryptography and ensure that the organisation is in control of all aspects of cryptography. To achieve this, organisations must achieve the prescribed or desired levels of protection, depending on the type of information involved, and ensure that appropriate processes are followed to guarantee the corresponding level of reliability.

The provisions in this chapter must explicitly not lead to parallel or intersecting processes that conflict with existing processes within the organisation. In cases where existing (more general) processes are affected, it must be described how cryptographic aspects should be incorporated into those processes.

3.5.1 Asset management

This section describes how cryptography and cryptographic materials (such as keys and certificates) are part of asset management. Cryptography in asset management is about how an organisation has insight into the cryptography used within it and how it can release information when needed and dispose of it when it is no longer needed. This also includes the use of techniques and standards (such as algorithms), and the cryptographic material (such as the keys and certificates in use).

3.5.1.1 Inventory

This section describes how the organisation ensures transparency regarding the use of cryptography and cryptographic materials (such as keys and certificates). It may be identified here which information should be collected manually and which should be collected automatically. Due to the volume of information to be collected, automation is recommended.

For every application of cryptography and for every use of cryptographic material, at least the following aspects must be recorded:

- Where the cryptography is applied or where the cryptographic material is used and/or stored (including, for example, applications, storage locations, Hardware Security Modules (HSMs), and software libraries).
- The purpose for which cryptography is used (such as encryption or signing).
- What cryptography is used or what properties the cryptographic material has (such as protocols, versions, algorithms, key lengths and parameters).
- What the current security level is and what the quantum security level is, the latter expressing the extent to which the cryptography used is resistant to attacks with a quantum computer.

The above results at least in a register of keys and a register of certificates.

More information about why and how to create an inventory of the cryptography used is described in the PQC Migration Handbook of the AIVD, TNO and CWI.

3.5.1.2 Cryptography throughout the entire lifecycle

This section describes the most important procedural measures within life cycle management (LCM) for the correct handling of cryptography and cryptographic materials. It also describes the secure deactivation and destruction of cryptographic materials.

3.5.2 Design and development

This section describes how cryptography is taken into account in design and development.

3.5.3 Procurement and vendor management

This section describes how cryptography and policy requirements are taken into account during the procurement process and vendor management.

At a minimum, address the following aspects:

- Procurement requirements: based on the normative framework, procurement must take place – new systems to be procured must technically be sufficiently future-proof.
- Vendor management: require the vendor to comply with the normative framework and the organisation that adopts it periodically.

3.5.4 Change management

This section describes how the relevant aspects of cryptography are arranged within change management.

3.5.5 Vulnerability management

This section describes how the relevant aspects of cryptography are arranged within vulnerability management.

3.5.6 Incident management

This section describes how the relevant aspects of cryptography are arranged within incident management.

3.5.7 Logging, monitoring and anomaly detection

This section describes how the use and management of cryptography and cryptographic material (such as keys and certificates) is logged, how the security surrounding cryptography and the storage of cryptographic material is monitored, and how anomalies can be detected.

3.5.8 Business continuity management

This section describes how the relevant aspects of cryptography are arranged within business continuity management (BCM).

3.5.9 Backup and recovery

This section describes how cryptographic material (such as keys and certificates) is included in backup and recovery processes.

3.5.10 Archiving

This section describes how all relevant cryptographic material (such as keys and certificates) is also included in archiving, so that encrypted or signed archived information can still be viewed or verified.

3.5.11 Auditing

This section describes how the policy and implementation regarding cryptography are audited. At a minimum, it describes which audit is conducted by the internal organisation and which external audit takes place.

3.6 Personnel

This chapter addresses the personnel aspects surrounding the use of cryptography.

3.6.1 Screening

This section describes which roles related to the use and management of cryptography and cryptographic materials require additional personnel screening and what that screening consists of. Consider the mandatory level of security screening for personnel who come into contact with certain cryptographic or key materials. Consider the applicable screening levels and authorisations for each role. Where necessary, relate this to the internal, national, or international classification levels of the underlying information. Also indicate how it is ensured that personnel have undergone appropriate screening and that screening is repeated regularly.

3.6.2 Qualifications and training

This section describes how to ensure that personnel are properly qualified to use and manage cryptography and cryptographic materials. Also specify how personnel are trained and continue to be trained. List the relevant training and certifications.

3.7 Use of cryptography

This chapter specifies the requirements for the use of cryptography.

3.7.1 Applications of cryptography

This section describes the applications (at an abstract level) for which cryptography should be used. Where applicable, a distinction is made between various required or desired levels of protection or the classification of the information to be protected. Attention is paid to the use of cryptography for both storage and transmission of information.

3.7.2 General technical cryptography requirements

This section describes the general technical cryptography requirements. These include the required security strength expressed in bits and the associated key lengths, algorithms, and so on. Ideally, the requirements should be referenced to a relevant, clear standard. Such a standard can be developed internally (organisation-specific) or externally. For each topic, it must be clear which options are recommended, permitted, to be phased out, or not permitted.

Refer to Chapter 4 List of technical aspects of cryptography for a list of topics that should be covered at a minimum in such a standard.

Also specify requirements for cryptographic implementations in applications, operating systems, and software libraries, as well as implementations in hardware.

Where possible, also consider the quantum security of the cryptography used.

3.7.3 Application-specific cryptography requirements

This section describes the application-specific technical cryptography requirements. They include requirements for symmetric and asymmetric encryption, signing using message authentication codes and digital signatures, connection security using TLS and IPsec, and so on.

Preferably, the requirements should be referenced to relevant, clear standards. Such standards can be developed internally (organisation-specific) or externally. For each topic, it must be clear which options are recommended, permitted, to be phased out, or not permitted.

Refer to Chapter 4 List of technical aspects of cryptography for a list of topics that should be covered at a minimum in such a standard.

3.8 Key management

This chapter describes how the organisation handles cryptographic key management.

3.8.1 Lifecycle of cryptographic keys

This section describes the implementation of (the most important) operations on cryptographic keys throughout their lifecycle, as described in ISO 11770-1.

At a minimum, the following operations must be described: generation, storage, archiving, retrieval, distribution, revocation, and destruction. Rotation (renewal) of key material must also be described. Also describe the requirements for the storage and processing of cryptographic keys, such as in which situations the use of a Hardware Security Module (HSM) or Trusted Platform Module (TPM) is required.

3.8.2 Other aspects of cryptographic key management

This section describes other aspects of cryptographic key management. It describes, among other things, how operations on keys are recorded and which operations require additional safeguards such as the 'four-eyes principle.'

3.9 Use of certificates

This chapter specifies the requirements for the use of certificates.

3.9.1 Applications of certificates

This section describes for which applications (at an abstract level) certificates should be used. Where applicable, a distinction is made between different levels of protection or the classification of the information to be protected.

Describe which type of certificate is required for each application. Certificates can be broadly divided into three applications: authentication, encryption (for confidentiality), or signing (for integrity, authenticity, and non-repudiation). Examples of certificate types include: certificates for authenticating web servers (TLS or QWAC certificates), certificates for signing software code (Code Signing certificates), and certificates for signing email (S/MIME certificates).

For each certificate type, determine whether it is for internal or external use.

In addition, specify the level of trust required, including the scope of the trust (internal, national, within the EU or international) and whether the certificate must be qualified (with associated legal validity). Within (central) government, the use of PKIoverheid certificates is recommended due to their high level of reliability at national, European, and international levels, and the recognisability of the State of the Netherlands. If a different level of trust is chosen, specify how the reliability and recognisability of the certificates used are guaranteed.

3.9.2 Requirements for being able to rely on certificates

This section describes the requirements for certificates, the certificate management process, and the provider before a certificate can be trusted. It also describes the criteria used to add a root certificate to the trust list of an application or system, and how to prevent certificates from untrustworthy parties from being trusted inadvertently. Make a distinction between publicly trusted external certificates, other external certificates (such as vendor-specific certificates or certificates from the PKIoverheid private root) and internal certificates.

Also describe how self-signed certificates should be handled, in which exceptional cases their use may be permitted, and what additional measures should be taken in such situations.

3.9.3 General technical requirements for certificates

This section describes the general technical requirements for certificates. This includes the types of certificates to be used, requirements for completing certificate fields, requirements for certificate providers, and so on. Ideally, the requirements should be specified by reference to a relevant, clear standard. Such a standard can be developed internally (organisation-specific) or externally. For each topic, it must be clear which options are recommended, permitted, to be phased out, or not permitted.

Refer to Chapter 4 List of technical aspects of cryptography for a list of topics that should be covered at a minimum in such a standard.

3.9.4 Application-specific requirements for certificates

This section describes the application-specific technical requirements for certificates. These include requirements for digital signature certificates, TLS certificates, IPsec certificates, and so on. Ideally, the requirements should be specified by reference to a relevant, clear standard. Such a standard can be developed internally (organisation-specific) or externally. For each topic, it must be clear which options are recommended, permitted, to be phased out, or not permitted. An example of this is that when applying for and using TLS certificates, the level of reliability must be taken into account, whereby the use of the lowest reliability level, 'domain validated' (DV), is not permitted for (central) government organisations.

Refer to Chapter 4 List of technical aspects of cryptography for a list of topics that should be covered at a minimum in such a standard.

3.10 Certificate management

This chapter describes how the organisation handles certificate management.

3.10.1 Lifecycle of certificates

This section describes how to implement all operations on certificates as described in RFC 3647. The following operations are described: application, application processing, issuance, acceptance (deployment), (key pair and certificate) usage, renewal, re-key, modification, revocation, and suspension.

In this section, an organisation describes at least the following components:

- The applicable requirements.
- The manner in which the identification and authentication of the applicant is performed.
- The manner in which certificates can be applied for and accepted.
- The manner in which certificates are processed by a trusted party (process).
- The manner in which certificates are distributed.
- A description of the key pair and certificate use.
- A description of renewing and/or modifying a certificate.
- The revocation process for certificates or placing them on hold.
- The manner in which issued certificates are registered, including the status of a certificate.
- A description of the termination of an agreement between the issuing and receiving party.
- The manner in which key material is transferred to a third party for management.
- Recovery procedures.
- How physical, procedural, and organisational protective measures are implemented.
- How to handle crisis situations (with a view to business continuity).
- How conformity assessments and security screenings are organised.
- Financial responsibilities and liabilities.

In addition, specify how the description of the policy pursued will be published, preferably in the form of a Certification Practice Statement (CPS) and Certificate Policy (CP) and on a website that is accessible to all parties who need to be able to rely on the certificates in question.

3.10.2 Other aspects of certificate management

This section describes the remaining aspects of certificate management. Also refer to the other considerations in RFC 3647. For key management related to the certificates used, including the secure storage and use of the related keys, refer to the specification in section 3.8 Key management.

3.11 Preparation for future developments

This chapter outlines how the organisation prepares for expected and unexpected future developments. Unexpected future developments may include sudden weaknesses in cryptographic algorithms or protocols, or the discovery of cryptographic implementation errors. Expected future developments include the arrival of a cryptographically relevant quantum computer, developments in the application of cryptography in cloud computing, the development of 'zero trust' and 'continuous authentication', or the trend to increasingly shorten the lifespan of certificates.

In addition, it must at least be stated how the organisation applies 'crypto agility' (cryptographic agility), for example by applying cryptography in a modular manner.

For advice on implementing this, see, for example, the ‘Make your organisation quantum secure’ guideline or the PQC Migration Manual.

3.12 Other aspects

This chapter identifies other relevant aspects of cryptography.

3.12.1 Legal aspects

This section describes the legal aspects relevant to cryptography, including privacy or the protection of personal data (including the interaction between privacy and encryption), intellectual property, liabilities, and terms of use. It outlines the requirements for Dossier Agreements and Procedures (DAPs), Service Level Agreements (SLAs), and contracts or covenants.

3.12.2 Physical aspects

This section describes the physical aspects relevant to cryptography, including physical security measures.

3.12.3 Other aspects

This section describes the other aspects relevant to cryptography, if applicable.

4 List of technical aspects of cryptography

A cryptography policy or associated standard for cryptography must contain requirements regarding the technical aspects of cryptography listed below. It is recommended describing the most common options and indicating which options are recommended, permitted, to be phased out, or not permitted.

Reliable sources must be used as the basis for the choices made. They may include the NCSC ICT security guidelines for Transport Layer Security, the BSI TR-02102 series on Cryptographic Mechanisms, and NIST SP 800-57 part 1, SP 800-131A, and SP 800-175B. Refer to Appendix C: References.

The resulting policy or standard must cite the sources used.

Where different requirements apply to different application areas, the trade-off framework for choosing between the various technical options for the specific context in which the cryptography is to be used must be clearly described.

General

- Security levels (security strength expressed in bits)
- Key lifetimes

Symmetric cryptography

- General
- Key lengths
- Encryption
- Algorithms
- Modes of operation for encryption
- Message authentication (via a Message Authentication Code, MAC)
- Modes of operation for message authentication
- Authenticated encryption

Asymmetric cryptography

- General
- Key lengths
- Finite field groups
- Elliptic curves
- Hybrid constructions
- Key exchange (via a Diffie-Hellman key exchange protocol or a Key Encapsulation Mechanism, KEM)
- Algorithms
- Parameters
- Forward secrecy and backward secrecy
- Authentication of key exchange
- Encryption
- Constructions (using an integrated encryption scheme (IES) based on a combination of key exchange and symmetric encryption)
- Digital signature
- Algorithms
- Parameters
- Constructions (using a signature scheme)

Hashing

- Algorithms

Cryptographic material

- Key generation requirements (by type/algorithm)
- Key derivation and key stretching
- Random number generation requirements
- Initialisation vector and salt requirements

Certificates

- Certificate types
- Subject fields
- Public keys
- Signature algorithms

Quantum-safe cryptography

- Quantum security levels
- Algorithms
- Key lengths
- Combining classical and quantum-safe algorithms (hybrid cryptography)

Implementation

- Required measures against side-channel attacks
- Requirements for the quality of cryptographic code
- Requirements for the origin of cryptographic code

Various cryptography applications must meet the requirements for the items listed above. Where necessary or desirable, the organisation can develop application-specific options in its policy or by developing organisation-wide templates.

Examples of cryptographic applications include TLS, IPsec, SSH, and password storage. The Forum Standaardisatie prescribes or recommends various cryptographic standards.

Appendix A: Chapter structure for cryptography policy

The chapter structure below is recommended for developing cryptography policy. It follows the structure of the framework described in Chapter 3, Framework for cryptography policy.

Introduction

- Objective
- Target group
- Scope of this policy
- Scope of cryptography application
- Limitations and exclusions
- Policy coordination with other organisations
- Policy management
- Definitions and abbreviations

Frameworks

- Normative frameworks
- Informative frameworks

Principles and starting points

Responsible parties

- Person with ultimate responsibility
- Persons responsible for policy
- Persons responsible for implementation
- Persons responsible for assessment

Processes

- Asset management
- Inventory
- Cryptography throughout the entire lifecycle
- Design and development
- Procurement and vendor management
- Change management
- Vulnerability management
- Incident management
- Logging, monitoring and anomaly detection
- Business continuity management
- Backup and recovery
- Archiving
- Auditing

Personnel

- Screening
- Qualifications and training

Use of cryptography

- Applications of cryptography
- General technical cryptography requirements
- Application-specific cryptography requirements

Key management

- Lifecycle of cryptographic keys
- Other aspects of cryptographic key management

Use of certificates

- Applications of certificates
- Requirements for being able to rely on certificates
- General technical requirements for certificates
- Application-specific requirements for certificates

Certificate management

- Lifecycle of certificates
- Other aspects of certificate management

Preparation for future developments

Other aspects

- Legal aspects
- Physical aspects
- Other aspects

Appendix B: Policy requirements from BIO, ISO 27002 and NIS2

The Government Information Security Baseline (BIO), the ISO 27002 and the NIS2 Directive specify requirements for developing cryptography policy. Government organisations must comply with one or more of these frameworks. Below is a brief overview of how this government-wide policy framework can use cryptography as a tool to meet these requirements.

Government Information Security Baseline (BIO, version 1.04zv)

The Government Information Security Baseline (BIO) stipulates that a government organisation must develop and implement policies regarding the use of cryptographic control measures and key management. Several topics must be addressed within the cryptography policy. It must also be ensured that cryptographic applications comply with appropriate standards. Furthermore, there are several key management policy considerations regarding certificates. The BIO sets requirements for the use of cryptography in several measures.

The framework for cryptography policy and the list of technical aspects of cryptography provided in this policy framework can be used as a tool to meet these BIO requirements.

When developing an organisation-specific cryptography policy, it must be checked – if required – whether all cryptography requirements from the BIO are met.

ISO 27002:2022

The 2022 edition of the ISO 27002 standard addresses the need for proper cryptography application in various controls. Control 8.24, Use of cryptography, also provides guidance on developing policies for cryptography in general and for key management (including key certificates) in particular.

The framework for cryptography policy and list of technical aspects of cryptography provided in this policy framework do not address all these requirements, but it does offer the opportunity to implement them all and to include them in a logical place in the organisation's cryptography policy.

When developing an organisation-specific cryptography policy, it must be checked – if required – whether all cryptography requirements from ISO 27002 are met.

NIS2 Directive

Article 21, paragraph 2(h), of the NIS2 Directive requires organisations subject to this directive to develop and implement policies and procedures regarding the use of cryptography.

Cryptography can also be a factor in the other types of policies that must be developed and implemented according to Article 21, paragraph 2.

The framework for cryptography policy and the list of technical aspects of cryptography provided in this policy framework can be used as a tool to meet these requirements of the NIS2 Directive.

When developing an organisation-specific cryptography policy, it must be checked – if required – whether all cryptography requirements from NIS2 Directive are met.

Appendix C: References

This document was reviewed against the requirements from the following sources:

- Government Information Security Baseline (BIO), version 1.0.4zv. https://bio-overheid.nl/media/13kduqsi/bio-versie-104zv_def.pdf.
- Civil Service CIO Scheme Decree 2021 [Besluit CIO-stelsel Rijksdienst 2021] https://www.rijksoverheid.nl/documenten/besluiten/2020/12/22/besluit-cio-stelsel-rijksdienst-2021.
- ISO 27002:2022 (Control measures for information security). *Available for a fee only*.
- Network and Information Security Directive (NIS2 Directive)
- Consolidated version 27 December 2022, with references to the underlying legally binding documents: https://data.europa.eu/eli/dir/2022/2555/2022-12-27.

In addition, this document refers to the following sources:

- Civil Service Data Information Security Decree 2007 [Besluit voorschrift informatiebeveiliging rijksdienst 2007] (VIR 2007) https://zoek.officielebekendmakingen.nl/stcrt-2007-122-p11-SC81084.html.
- Civil Service Information Security Classified Information Decree 2013 [Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013] (VIRBI 2013) https://zoek.officielebekendmakingen.nl/stcrt-2013-15497.html.
- BVA Scheme Civil Service 2021 Decree [Besluit BVA-stelsel Rijksdienst 2021] https://www.rijksoverheid.nl/documenten/besluiten/2020/12/29/besluit-bva-stelsel-rijksdienst-2021.
- 'Comply or Explain' standards from the Forum Standaardisatie. https://www.forumstandaardisatie.nl/open-standaarden/verplicht.
- Recommended standards of the Forum Standaardisatie. https://www.forumstandaardisatie.nl/open-standaarden/aanbevolen.
- Secure Connections to Government Websites and Web Applications Decree [Besluit beveiligde verbinding met overheidswebsites en -webapplicaties]. https://wetten.overheid.nl/BWBR0048225/2023-07-01.
- ISO 11770-1:2010 (Framework for key management) *Available for a fee only*.
- RFC3647 (Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework). https://www.rfc-editor.org/rfc/rfc3647.
- NCSC ICT security guidelines for Transport Layer Security v2.1 (TLS) https://www.ncsc.nl/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1.
- BSI TR-02102 series regarding Cryptographic Mechanisms. https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html.
- NIST SP 800-57 part 1 revision 5 (Recommendation for Key Management: Part 1 – General) https://csrc.nist.gov/pubs/sp/800/57/pt1/r5/final.
- NIST SP 800-131A revision 2 (Transitioning the Use of Cryptographic Algorithms and Key Lengths). https://csrc.nist.gov/pubs/sp/800/131/a/r2/final.
- NIST SP 800-175B revision 1 (Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms). https://csrc.nist.gov/pubs/sp/800/175/b/r1/final.
- Guideline 'Make your organisation quantum secure' from the AIVD and NCSC. https://www.ncsc.nl/quantumveilige-cryptografie/maak-je-organisatie-quantumveilig.
- The PQC Migration Handbook from TNO, CWI and AIVD. https://www.aivd.nl/documenten/2024/12/3/het-pqc-migratie-handboek.

Appendix D: Abbreviations

The following abbreviations are used in this document:

ADR	Auditdienst Rijk - Government Audit Service
AI	Artificial Intelligence
AI Act	Artificial Intelligence Act - Verordening Kunstmatige Intelligentie
AIVD	Algemene Inlichtingen- en Veiligheidsdienst - *General Intelligence and Security Service*
ANSSI	Agence nationale de la sécurité des systèmes d'information
AR	Algemene Rekenkamer - *Netherlands Court of Audit*
BCM	Business Continuity Management
BIO	Baseline Informatiebeveiliging Overheid - *Government Information Security Baseline*
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVA	Beveiligingsautoriteit - *Security Authority*
BVC	Beveiligingscoördinator - *Security Coordinator*
BZK	(Ministerie van) Binnenlandse Zaken en Koninkrijksrelaties – *(Ministry of) the Interior and Kingdom Relations*
CIO	Chief Information Officer
CIO Rijk	Chief Information Officer Rijk - *Chief Information Officer of the Central Government*
CISO	Chief Information Security Officer
CISO Rijk	Chief Information Security Officer Rijk - *Chief Information Security Officer of the Central Government*
CP	Certificate Policy
CPS	Certification Practice Statement
CRA	Cyber Resilience Act
CWI	Centrum Wiskunde & Informatica - *National Research Institute for Mathematics and Computer Science in the Netherlands*
DAP	Dossier Afspraken en Procedures - *Dossier Agreements and Procedures*
Dep.V	Departementaal VERTROUWELIJK - *Departmental CONFIDENTIAL*
DICTU	Dienst ICT Uitvoering - *ICT Implementation Service*
DV	Domain Validated
eIDAS	electronic IDentification, Authentication and trust Services
ENISA	European Union Agency for Cybersecurity
ETSI	European Telecommunications Standards Institute
GDPR	General Data Protection Regulation
HSM	Hardware Security Module
HTTPS	Hypertext Transfer Protocol Secure
IAM	Identity and Access Management
IB&P	Informatiebeveiliging & Privacy - *Information Security & Privacy*
ICAO	International Civil Aviation Organisation
ICBR	Interdepartementale Commissie Bedrijfsvoering Rijk - *Interdepartmental Committee on Government Operations*
ICT	Information and communication technology
IES	Integrated Encryption Scheme
IPsec	Internet Protocol Security
ISO	Internationale Organisatie voor Standaardisatie - *International Organisation for Standardisation*
JenV	(Ministerie van) Justitie en Veiligheid - *(Ministry of) Justice and Security*
KEM	Key Encapsulation Mechanism
LCM	Life Cycle Management
MAC	Message Authentication Code
MD5	Message-Digest algorithm 5
MinDef	Ministerie van Defensie - *Ministry of Defence*

MinFin	Ministerie van Financiën - *Ministry of Finance*
NATO	North Atlantic Treaty Organisation
NBV	Nationaal Bureau Verbindingsbeveiliging - *National Communications Security Agency*
NCSC	Nationaal Cyber Security Centrum - *National Cyber Security Centre*
NIS2	Network and Information Security directive
NIST	National Institute of Standards and Technology
OWASP	Open Worldwide Application Security Project
PQC	Post-Quantum Cryptography
QvC Rijk	Quantumveilige Cryptography Rijk – *Quantum secure Cryptography Central Government*
QWAC	Qualified Website Authentication Certificate
RFC	Request for Comments
RVB	Rijksvastgoedbedrijf - *Central Government Real Estate Agency*
RvIG	Rijksdienst voor Identiteitsgegevens - *National Office for Identity Data*
S/MIME	Secure/Multipurpose Internet Mail Extensions
SHA-1	Secure Hash Algorithm 1
SLA	Service Level Agreement
SP	Special Publication
SSH	Secure Shell (Protocol)
Stg.C	Staatsgeheim CONFIDENTIEEL - *State Secret CONFIDENTIAL*
TLS	Transport Layer Security
TNO	Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek - *Netherlands Organisation for Applied Scientific Research*
TPM	Trusted Platform Module
TR	Technische Richtlinie - *Technical Guideline*
UWV	Uitvoeringsinstituut Werknemersverzekeringen - *Employee Insurance Agency*
VBV	Verbindingsbeveiligingsvoorschrift - *National Communications Security Regulations*
VIR	Voorschrift Informatiebeveiliging Rijksdienst - *Civil Service Data Security*
VIRBI	Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie - *Civil Service Information Security Classified Information*
VWS	(Ministerie van) Volksgezondheid, Welzijn en Sport - *(Ministry of) Health, Welfare and Sport*

Colophon

This brochure is a publication of:
Ministry of the Interior and Kingdom Relations

Owner	CIO Rijk (CIO Government)
Management	IB&P
To be adopted by	CIO-beraad (CIO Consultations)
Contact address	CISO-Rijk@minbzk.nl
Author 1st version	Werkgroep QvC-Rijk (Working group QvC Government)
Version number	1.0
Date	14 February 2025
Status	Final