Crypto Agility – The How

In the era of evolving cyber threats and quantum computing, Crypto Agility (the ability to swiftly switch between cryptographic algorithms and protocols) has become essential. It is no longer just about compliance. It is a strategic advantage that boosts resilience against cyberattacks, quantum risks, and regulatory demands.

This extensive introduction outlines a structured path to Crypto Agility, starting with Cryptographic Asset Management: inventorying artefacts using scanning tools and centralized repositories for visibility and control. It emphasizes assessing and tracking cryptographic use, aligning strategy with priorities, and addressing technical and process constraints. Key steps include defining roles, strategic planning, execution, and continuous improvement.

By embedding agility into cryptographic practices, organizations can future-proof infrastructure, maintain resilience, and mitigate emerging threats.

Capgemini NMWP. The Innovation Engineers.

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Table of Contents

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

1 Crypto Agility – Introduction

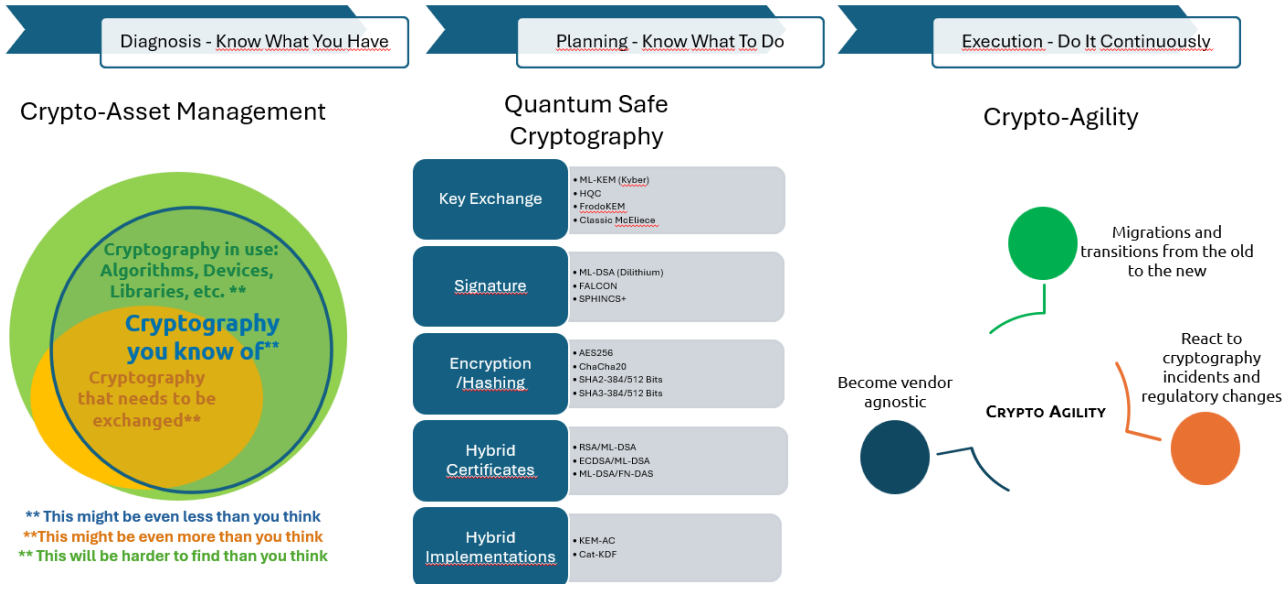


Figure 1: Crypto Agility - The How

Crypto Agility refers to the ability and flexibility to react in a timely manner and to adapt quickly in the cryptography landscape (algorithms, processes, vendors, libraries, etc). The IT landscape should be able to adapt quickly to new algorithms, standards and regulatory changes in response to evolving threats regarding quantum computing.

For example, a A 829 bit key (RSA-250) [1] was broken in 2020, offering a glimpse into what increasing computational power can achieve. Also, there are well-known attacks against RSA implementations e.g. the Coppersmith attack [2][3]

NIST [5] defines crypto agility as “the capabilities needed to replace and adapt cryptographic algorithms for protocols, applications, software, hardware, and infrastructures without interrupting the flow of a running system in order to achieve resiliency, “which must be considered for each specific implementation environment.

Or more specifically:

1. the ability for machines to select their security algorithms in real time and based on their combined security functions, for example in TLS.
2. the ability to add new cryptographic features or algorithms to existing hardware or software, resulting in new, stronger security features; and
3. the ability to gracefully retire cryptographic systems that have become either vulnerable or obsolete [6]

Thus Crypto Agility defines the need for flexibility to transition from deprecated or known Dates of expired Algorithms by BSI, ANSSI, NIST, etc. and broken crypto methods to newer and more secure alternatives reducing the risk from significant operational disruption due to awareness and implementation of a process to react to cryptography

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

changes effectively and timely and evolve the organization's security posture to obtain secure and quantum safe cryptography.

And there are many challenges in cryptographic transitions. Not only discovering all assets in the organization´s environment and assessing associated risks and the constant need for tracking and transition. We face organizational and technical challenges like considering resources, processes, having a crypto agility maturity model in place, backward compatibility, interoperability, technical and performance restrictions and complexity. [7]

So we need to find a way to smoothly migrate the current cryptography to modern and quantum safe algorithms and implement crypto agility to be able to switch to alternative algorithms, vendors, libraries and processes. But more agility comes with a higher complexity. Known as the coffin corner in Aviation we must individually identify the specific point of agility with the maximum complexity, which is still practical enough for an organization. [8]

In August 2024 the US National Institute of Standards and Technology (NIST) published the first PQC standards. [9] Various organizations and regulatory bodies worldwide are preparing and implementing PQC-related legislation [10] or have already started the PQC migration. Thus it´s a common understanding on the urgency of this topic and the need of well-coordinated efforts to achieve the development of a precise PQR migration roadmap. But especially in Europe we are facing additional challenges, since the member states must align in a joint process.

The QPrEP project aims for the Identification of requirements and common interests between the stakeholders, especially in the public sector, to enable systematic work and consolidation to transfer into a comprehensive roadmap of PQC for leading the way to quantum-safe IT in the European public sector and beyond.

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

2 Cryptography Asset Management

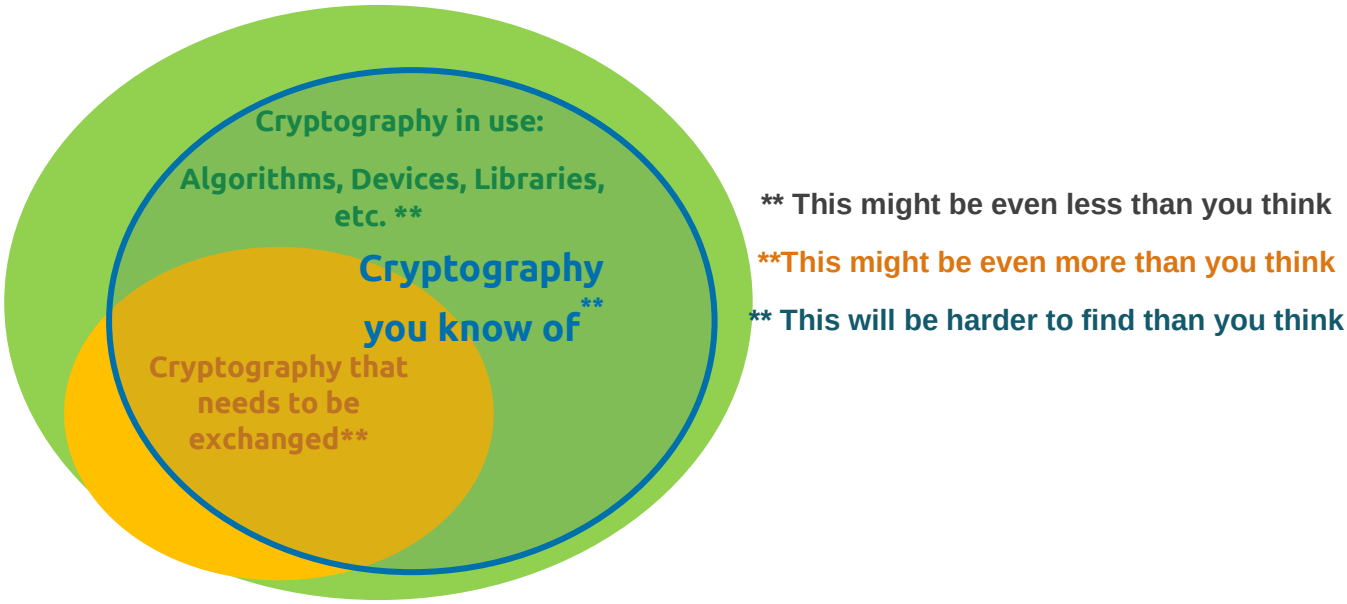


Figure 2: Cryptography Asset Management visualization

Involves a systematic discovery process, accurate inventory management, monitoring and life cycle management of crypto assets (keys, certs, algorithms, and related policies) within an organization. Maintaining an accurate cryptographic inventory is essential for gaining full visibility into all cryptographic assets.

For identifying the systems and components that need to be migrated, gaining a clear view of the organization's crypto landscape is crucial. Since advances in cryptoanalysis could compromise any algorithm – regardless from PQC – the ability to adapt and implement rapid changes is a necessity.

The more assets that are managed, the better the complete cryptographic overview is and the better the cryptographic maturity can be tracked. More managed assets mean more overhead, thus there should be an evaluation of what artefact types need to be assed to the cryptographic asset management repository.

→ Your goal is to find and optimize ALL artefacts.
→ Adversaries need only the ONE artefact you missed.

2.1 Artefacts – What cryptographic artefacts do we have

Capturing a cryptography asset inventory involves a systematic approach to identify, classify, document, track, update and maintain all cryptographic artefacts used across applications, infrastructure, and networks. This capturing procedure can be manual,

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

automated or a hybrid procedure. While a manual process can be suitable for small-scale applications or isolated environments to document object type, usage, location, dependencies, and responsible parties, it won´t be feasible for complex enterprise environments due to the time-consuming nature, possible human errors and the potential for inaccuracy. [12]

Cryptography assets can be any of the following artefacts:

- **Algorithms** for Encryption/Decryption, Signature/Verify, Authenticate, Padding (also deprecated algorithms)
- **Data-at-Rest** which includes Backups, Encrypted Files, Hashed and encrypted Passwords, etc.
- **Data-In-Transit** which includes protocols and processes like TLS, VPN, IPSec, etc.
- **Public-Key-Infrastructure and HSM** which includes all PKI-Components, CAs (Certificate Authorities), HSMs and HSM-Keys used by PKI.
- **Products, Libraries and Implementations** which includes all products using cryptography, as well as products, libraries and implementations that produce cryptographic primitives.
- **Keys** which include all cryptographic material including Private Keys, Public Keys, Symmetric Keys, and SSH Keys.
- **Digital Certificates (**TLS/SSL, Signing Certificates, S/MIME).

2.2 Scanning Tools – Products, processes & procedures

Scanning for cryptographic artefacts, means looking everywhere in the IT-landscape for usages of cryptography, which can include scanning networks, computers, network and storage devices, firewalls, applications, key- and trust stores, digital certificates, security tokens and many more.

The methods of the scanning tools include passive/static vs. active/dynamic and the general differentiation between open source vs. proprietary.

The challenge here is finding the right tool for your use cases and the balance between effort, overhead and costs vs. accuracy and completeness.

When choosing a tool you should consider the following aspects:

- **Effort** = implementation, execution and reporting
- **Overhead** = performance penalty on system because of the scanning process
- **Costs** = tool price and service price and integration costs
- **Accuracy** = quality and amount of found artefacts as well as low false positive rates
- **Completeness** = complete IT landscape coverage with low false negative rate

To choose the right tools suitable for your organization, requirements need to be defined e.g.:

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

- **Scope**: What do I need to scan, from file systems, data in transit, key stores, ports, digital certificates, etc.
- **Location**: Do I want to scan on on-premise networks, all world-wide networks, virtual networks or cloud networks.
- **Integration**: Do I want the scanning tools to be stand-alone tools, only running for the purpose of scanning for cryptographic artefacts, or do I want to integrate these scanning tools into existing tools and reports.
- **Agents**: Do I want to scan remotely, use stateful or even stateless agents or a mixture of them.
- **Logs**: The one consideration is whether I want to scan logs for any cryptographic artefacts and the other consideration is whether I want to log all scanning activities.
- **CBOM ingestion**: CBOM (Cryptography Bill of Materials) can be used as a guideline, and scanning tools reporting using CBOM-formats can be an advantage for interoperability with other scanning and reporting tools.
- **Scan frequency**: Regular scanning can deviate from hourly to monthly and can be either full scans or delta scans depending on the tools and the type of infrastructure that is being scanned.
- **Accuracy**: It is important that scanning tools are accurate and reliable.

Examples of scanning artefacts:

Category	Name	OSS	Restriction / comments
Port	Nmap with NSE Scripts	✅	Port scanning and service discovery incl. weak cipher/protocol detection
	Masscan	✅	Port scanner for large networks (lacks deep crypto analysis)
	OpenVAS	✅	Network vulnerability scanner with TSL/SSL checks, detects vulnerabilities, misconfigurations and outdated software across networks and systems. Does compliance scanning (SCAP, CIS)
	Nessus		Vulnerability scanner incl. crypto checks, can identify vulnerabilities, misconfigurations and compliance risks (NIST, CIS, PCI-DSS) in networks, systems and applications.
Network	Wireshark	✅	Network protocol analyzer. Can inspect TLS/SSL handshakes, extract certificates/keys and detect weak crypto (supports live capture and offline analysis)
	Superscan	✅	Scans, network, servers, applications and cloud environments and detects SSL/TLS certificates, SSH keys, cryptographic libraries, weak or deprecated algorithms, expired certificates and misconfigurations. Can generate centralized inventory

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Keystores	Key Store Explorer	✅	GUI for managing Java keystores (JKS, PKCS#12)
	KeyTool (JDK)	✅	CLI for keystore management
	Portecle	✅	Java-based cross-platform keystore (supported JKS, JCEKS, PKCS#12) and certificate management tool, limited HSM & smartcard support (PKCS#11)
	IBM Keyman		Key management and discovery tool (supports HSMs, PKCS#11)
TLS/SSL	*OpenSSL	✅	CLI tool for certificate/key inspection and cipher checks
	Testssl.sh	✅	Checks SSL/TLS config, weak ciphers and certificate issues/flaws
	SSLyze	✅	Python based SSL/TLS scanner incl. ciphers, certificates, vulnerabilities (supports TLS 1.3)
	SSL-Scan	✅	SSL/TLS scanner with cipher prioritization
	OpenSSL	✅	Supports basic PKI features like CSR (Certificate Signing Requests), certificate generation, no native HSM support (needs PKCS'11 engine), not FIPS-validated by default. Useful for development, testing and custom crypto implementation, debugging TLS and certificate converting
PKI/Secrets Management	Hashicorp Vault	✅	Advanced secrets management and can discover unsecured keys (Vault requires paid subscription.)
	Keywhiz	✅	Secrets management with discovery capabilities
	HashiCorp Vault		Advanced secrets management with discovery
	Key factor		PKI and certificates discovery and inventory
	Cert+ AppViewX		Certificate life cycle automation (discovery, issuance, renewal with multi-cloud support)
	DigiCert CertCentral		Centralized life cycle management of digital certificates (TLS/SSL, code signing, S/MIME). Discovers and inventories certificates across networks. Supports integration with DevOps tools CI/CD pipelinens and cloud
	Cert+		Certificate and key discovery/management with focus on compliance and PKI
	Venafi		Certificate and key lifecycle management with compliance focus
	Keywhiz	✅	Secrets management with discovery capabilities
File System	TruffleHog	✅	Scans for secrets, crypto keys in files/Git repos
	Ripgrep (rg)	✅	File/content search
	Strings+grep	✅	CLI commands to find/extract keys/certs from binaries
	YARA	✅	Pattern-matching tool for identifying keys/certs in binaries/files
	GitLeaks	✅	Scans Git repos for exposed secretes/keys

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

	Binwalk		Firmware/disk image analysis, can extract certs/keys
SSH keys	SSH-scan	✅	SSH config and weak cipher scanner
	LinPEAS	✅	Linux privilege escalation scanner checks SSH keys and sensitive files
	SSH-Audit	✅	SSH-server configuration auditing (weak algorithms, keys)
	OpenSCAP	✅	Compliance scanning incl. crypto checks
	Lynis	✅	Security auditing tool checks crypto configs and systems
	SSH Keychain		SSH Key Management and discovery tool
	Qualys SSL Labs		SSL/TLS Scanning and cipher analysis
	Tenable		Vuln scanning including crypto checks
	Rapid 7		Asset discovery and crypto protocol scanning
Active Directory	pingCastle	✅	AD security auditing tool. Checks misconfigurations, privilege escalation paths and weak cryptographic settings (e.g. Kerberos encryption types)
	Bloodhound	✅	AD attack path mapping tool. Can visualize privilege escalation paths (e.g. certificate abuse, Kerberos trusts etc.)
	Purple Knight	✅	AD attack path mapping tool. Helps discover IoCs (indicators of compromise) and IoEs (indicators of Exposure). Supports AD, Entra ID and Okta assessment.
	MSCA/ADCS		Software-based PKI, manages digital certificates in AD environments, RBAC-based, can integrate nCipher/Ultimaco for key storage (if not used software-based storage NO HSM)
SAST	SonarQube	✅	Static Application Security Testing Tool (also proprietary) for code analysis. Can detect vulnerabilities e.g. hardcoded secrets, weak crypto etc.)
HSM	Thales Luna		Discovers and manages hardware-backed keys (FIPS-compliant)
	Entrust nCipher/nShield (now part of Thales)		Cryptographic key generation, storage and management, secures CAs (certification authorities), SSL/TLS certificates, secures software signing keys supports AWS, Azure, Google Cloud (via payShield, codeSafe); FIPS 140 2/3 certified
	Utimaco		Available as HW, virtual or cloud HSM, FIPS and CC (Common Criteria Certified)
Cloud	Azure Key Vault Analytics		Discovers and audits keys/certs in Azure
	AWS Certificate Manager ACM		Discovers and manages SSL/TLS certificates in AWS

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

	Google Cloud Key Management		Discovers and manages keys in GCP
SIEM/Logging	Splunk		Correlates logs to track certificate expirations, key usage and anomalies
	IBM QRadar		Log Analysis for cryptographic artefacts (e.g. unauthorized key access etc.)
Container	Anchore		Scans container images for exposed keys/certs and misconfigurations
Network	F5 BIG-IP		Decrypts/inspects TLS traffic to identify rogue certificates

2.3 Repository Tools - Products, processes & procedures

All cryptographic artefacts should be placed in an inventory or repository, that serves as a central point of reference for all cryptographic artefacts.

This repository should also have a person responsible for each artefact that can be contacted in case these artefacts become deprecated or compromised.

Cryptographic Asset Repository
One can either implement a single repository for all company assets, that also includes the cryptography artefacts, but these might not be able to capture all the necessary information for cryptographic artefacts.

Using multiple repositories where a dedicated repository captures all information on cryptographic artefacts has the disadvantages that these multiple repositories must be kept in sync.

This repository should also contain cryptographic processes, if possible, since even processes (like signing certificates, generating random numbers and saving private keys in key stores might become deprecated or vulnerable.

Asset Lifecycle Management
The asset lifecycle management means that all artefacts in the repository should be kept up to date and should be re-checked regularly to make sure that the owner of the asset hasn't changed, the asset is still used, the information about the asset is still valid and that the asset does not contain or use deprecated or broken cryptography.

CBOM Cryptography Bill of Materials (CBOM)
Cybersecurity Bill of Materials (CBOM) is a security-focused extension of the SBOM that helps organizations identify and mitigate vulnerabilities in software components.

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

2.4 Scanning Processes

The processes around scanning are addresses in chapter 4, crypto agility. Scanning should be regularly and controlled and the reposts should be evaluated.

All possible cryptography artefacts, like algorithms, products, digital certificates, keys, libraries and anything related to cryptography asset management should be scanned.

Chapter 2.1 has examples for artefacts that can be captures, and chapters 2.2 and 2.3 mention the tools for scanning and the repositories.

2.5 Asset Management Assessment

In addition to asset lifecycle management, all cryptographic assets should be assessed and analyzed based on the current state of the artefact, about the probability of compromise and the damage upon compromise, based on normal risk management tables.

Cryptographic processes and procedures should also be regularly assessed, to make sure that they are still contemporary, compliant and secure.

Examples of weaknesses and vulnerabilities that might be an indicator that the cryptographic artefacts need to be optimized:

- **Broken and Weak Algorithms**
  - Some algorithms and implementations (like SHA1, PKCS1 v1.5 padding, DES, RC4, CBC) be weak or broken and the list of vulnerable algorithms and implementations grows continuously.
- **Non-Quantum Safe Algorithms**
  - Most classical cryptographic algorithms, especially asymmetric algorithms, are vulnerable to quantum computers, using either Shor's or Grover's algorithms.
  - As quantum computers become stronger (more stable qubits and better error correction) current classical cryptography becomes more vulnerable.
- **Broken and Weak Implementations**
  - Due to the high numbers of cryptographic algorithms and the many different parameters and modes they use, implementation errors might occur causing secure products and libraries to have weak and vulnerable versions that should be avoided.
  - These products and libraries should also be used according to implementation guidelines and should not be customized or used with non-secure parameters.
  - Due to the complexity of implementing these algorithms, it is also not advisable to implement your own cryptographic algorithms.

Most countries have central institutions that can give advice and guidelines on cyber security, which also covers cryptography and quantum safe cryptography.

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

2.6 Technical and Regulatory Limitations and Restrictions

Technical Limitations
When scanning, searching or discovering cryptographic artefacts, protocols, libraries and products, there might be limiting factors preventing you from finding all the cryptographic artefacts.

Examples of technical limiting factors:
- **Tool-dependent coverage**: some tools might not be able to scan all operating systems, all network protocols or all file system types.
- **Permissions and access restrictions**: some tools might be prevented from scanning certain network drives, folders on a hard drive or even some networks. This might be caused by insufficient access, firewalls, blocked interfaces or they may be off-limits due to compliance and policies.
- **Segmentation barriers**: Some networks might be air-gapped and others might be behind VPNs or Wi-Fi access points and therefore not reachable.
- **Scanning with operational constraints**:
    - Scanning might be limited to time slots, where the networks are not busy or when no critical workload is being processed, which might cause certain artefacts to be skipped.
    - Scanning in cloud environments might be limited and different compared to scanning data centers.
    - Scanning OT and IoT devices are known to produce unexpected results and might cause problems or even down-time if certain devices and networks cannot handle the requests from the scanning tools.
- **Workload limitations**: Scanning should be throttled is possible to reduce workload impact and to limit unnecessary workload costs.

Regulatory Limitations and internal constraints

Internal **IT priorities** might affect the scanning and discovery of cryptographic artefacts. Usually implementing new features and other IT processes might be prioritized higher than security.

IT processes might also be slow and tedious, causing the scanning and discovery processes to take an excessive amount of time.

Internal change management, problem management and information security management should be involved to streamline the processes of capturing cryptography artefacts.

Some regulations might also limit the scanning of certain artefacts, since some artefacts should not be visible for such access, like HSMs, which should probably be scanned manually.

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

3 Cryptography Use Cases

Cryptography is the foundation of our modern digital security, enabling confidentiality, integrity, authentication and non-repudiation across various applications. Cryptography is like the invisible shield that protects our digital world and is safeguarding our digital interactions. It secures everything - from web traffic (TLS) to digital identities (PKI) or encrypting transactions. There are many different algorithms and tools—each designed for specific purposes.

Just like we use different keys for our car, house, or office, computers use different cryptographic algorithms and methods depending on the situation.

Below is a high-level view of the basic cryptographic primitives and use cases:

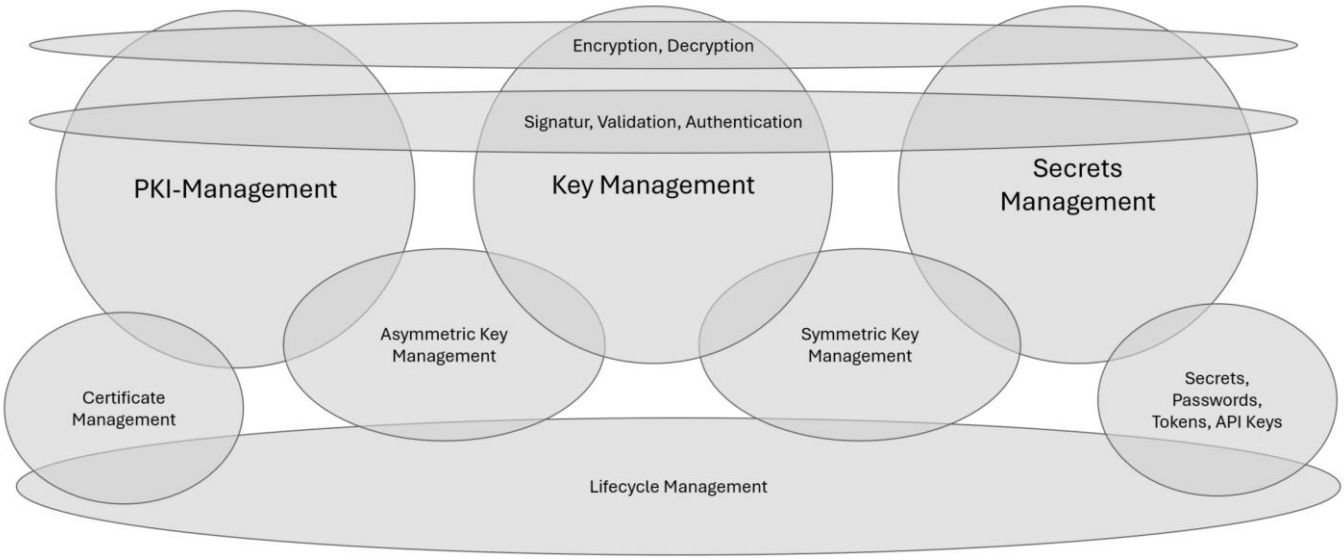


Figure 3: Cryptography Use cases I

Cryptography can get complicated quickly as the different use cases, different algorithms and different implementations are combined in an IT-landscape. To handle this complexity a systematic process for generating, storing, use, rotation and deprovisioning/retiring cryptographic keys and certificates is essential. Just with proper cryptographic Life cycle management a robust security across an organization can be maintained.

Below is a more detailed view of most of the cryptographic components in an IT-landscape.

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

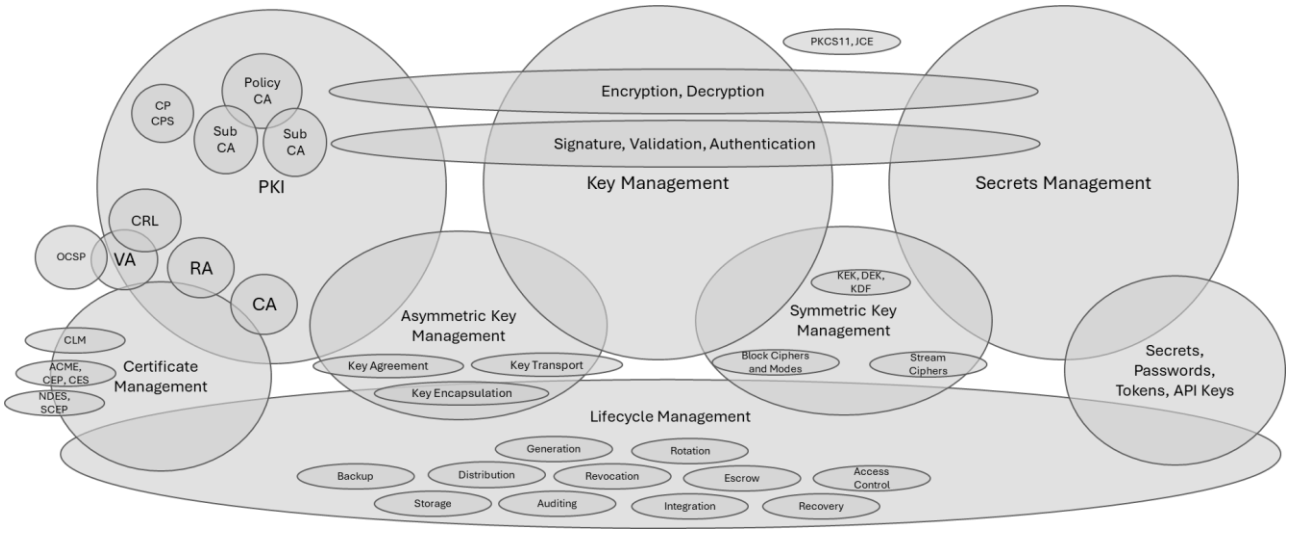


Figure 4: Cryptography Use cases II

3.1 Quantum Safe Cryptography

The following are current (May 2025) recommended quantum safe algorithms and implementations. These recommendations are different between countries and industries.

The following video gives a summary of the implementation and security of post quantum cryptography algorithms: https://www.youtube.com/watch?v=6qD-T1qjtKw

Key Exchange between Parties

For the exchange of symmetric keys, the current recommendation is to switch over from all current procedures to Key Encapsulation Methods. This means moving away from quantum unsafe methods like key agreement (DH, ECDH) and key transport (RSA) to the following algorithms:

- ML-KEM: CRYSTALS-Kyber
- HQC: Hamming Quasi-Cyclic
- FrodoKEM
- Classic McEliece

Digital Signatures

For signing documents, code, authentication tokens, digital certificates and other artefacts, the current recommendation is to switch from quantum unsafe algorithms like ECDSA, EdDSA, DSA and RSA to the following quantum safe algorithms:

- ML-DSA: CRYSTALS-Dilithium
- FN-DSA: FALCON
- SLH-DSA: SPHINCS+

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Encryption /Hashing

Current hashing and symmetric encryption algorithms and cipher modes are considered quantum safe, if the key lengths are adequate. For encryption the key lengths show be at least 256 bits, and for hashing at least 384 or 512 bits:

- Symmetric Encryption:
  - AES-256
  - ChaCha20
- Hashing:
  - SHA2-384/512 Bits
  - SHA3-384/512 Bits
  - BLAKE2, Whirlpool

Hybrid Certificates

Due to the importance of digital certificates (authentication, non-repudiation and integrity) it is recommended to switch from using just one algorithm for signing certificates to using 2 algorithms. This can be a combination of classical and quantum safe algorithms but might in future include 2 different quantum safe algorithms.

Using hybrid certificates is a recommendation from certain countries and governments only, and although other European countries and NIST do not recommend using hybrid certificates, they do mention the advantages of using them.

Examples of algorithm-combinations for hybrid certificates:

- RSA/ML-DSA
- ECDSA/ML-DSA
- ML-DSA/FN-DSA

3.2 Use cases: Key Agreement, Key Encapsulation, Key Transport and Key Exchange

Term	Goal	Shared Key Origin	Communication Direction	Authentication Involved
Key Agreement	Two/more parties jointly derive a key	Derived from inputs	Interactive (usually)	Optional
Key Encapsulation (KEM)	Securely send a key using public key crypto	One party generates, other party receives	One-way	Optional

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Key Transport	One party generates and securely sends a key	One party generates	One-way	Optional
Password-Authenticated Key Exchange (PAKE)	Derive a key using a shared password	Derived from password	Interactive	Yes (via password)

Table 1: This table shows a comparison of the different key exchange use cases and their differences.

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

4 Crypto Agility – The How to achieve Crypto Agility

NIST [11] proposed a strategic plan to transition the organization to Crypto Agility identifying key activities to integrate Crypto Agility into the organization's existing governance function adopting a data-centric approach by automating the identification, assessment, characterization, enforcement, and monitoring to identify gaps and develop a prioritization list and a strategy and actions based on prioritization. These key activities need to be repeated continuously to mitigate existing and emerging crypto risks enabling the enhancement of the crypto agility posture within the organization.

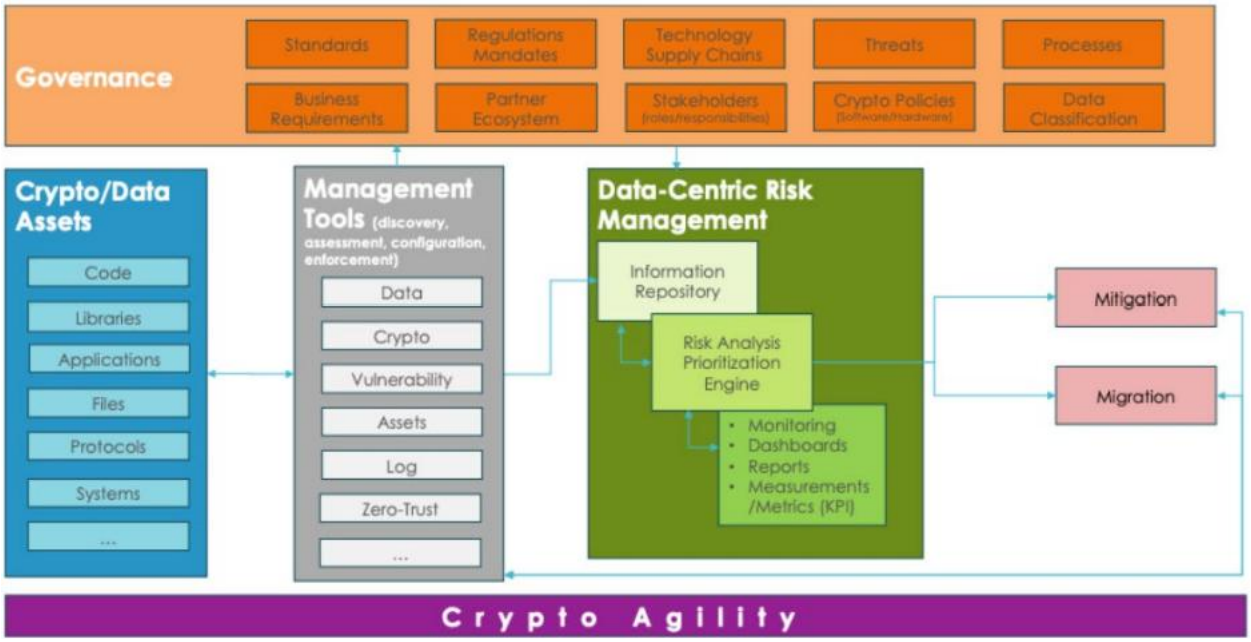


Figure 5: Crypto Agility Ref.: NIST March 5, 2025 Cybersecurity White Paper NIST CSWP 39 ipd: Considerations for Achieving Crypto Agility
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.39.ipd.pdf

4.1 Defining roles and responsibilities for the tasks and deliverables (RACI)

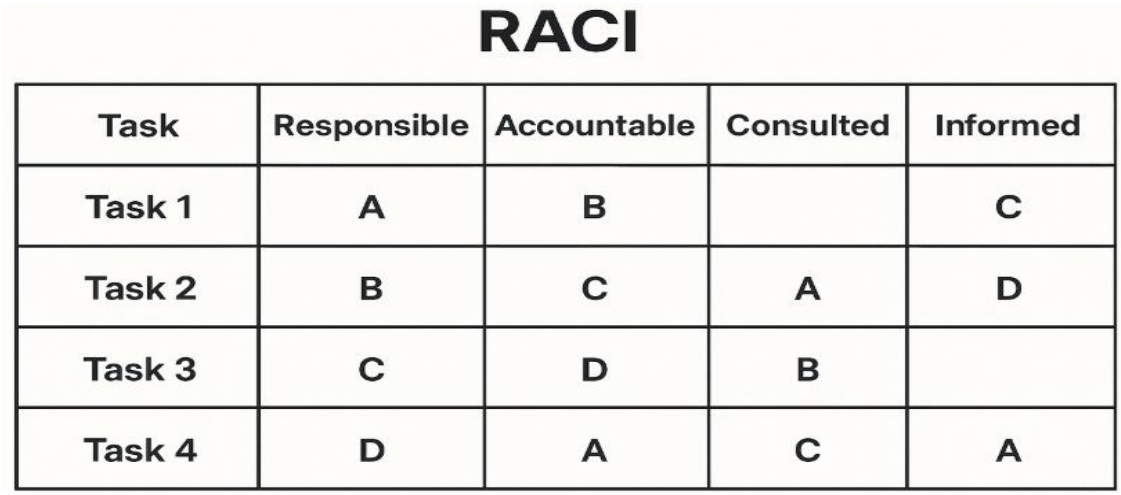
For all cryptographic artefacts and all processes involved in the quantum safe journey, there should be named personnel who are responsible for the actual doing, accountable for the results, consulted when help is needed and informed if they are in some way affected.

This requires implementing a risk management process and RACI to define who is Responsible, Accountable, Consulted and Informed and involve all the different stakeholders within the organization in the planning.

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE



RACI

Task	Responsible	Accountable	Consulted	Informed
Task 1	A	B		C
Task 2	B	C	A	D
Task 3	C	D	B	
Task 4	D	A	C	A

Figure 6: This illustration shows an example RACI matrix

Ownership
The cryptographic asset management and assessment processes should have dedicated roles and responsibilities assigned to dedicated people, who should involve and inform the needed stakeholders.

There should also be an escalation path to address and mitigate and alleviate the limitations and other problems in the asset management and assessment processes.

4.2 Planning

The planning for the crypto agility journey should include the following aspects: stakeholders, costs, timelines, deadlines and general flexibility.

Stakeholders are not only the people working in the project or the people implementing quantum safe cryptography, but everyone who is involved, affected, consulted and informed.

- **Internal management**: this is where the journey starts. Management should be aware of the risks of not implementing crypto agility and quantum safe cryptography. They should be the driving force being the program and usually plays a big part in organizing the needed budged. Some laws in the EU and in some countries are stiving to make C-level management personally responsible for the consequences of not implementing quantum safe cryptography. Examples are article 20 of NIS2, article 32 of GDPR, DORA as well as country specific laws like Germany's IT-Security Law 2.0 and France's LPM law.
- **Internal IT-Operations**: IT operations are working on the IT systems daily, and knows the cryptographic assets the best, and can also judge the effects of changing or migration cryptographic assets to different cryptographic products, algorithms and implementations. They are also the direct contact people if changes in cryptographic assets cause problems or downtimes.
- **Internal IT-Security**: IT Security should regulate the use of cryptography assets and should be informed about current and future safe cryptography artefacts. They

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

should help with the capture as well as the assessment of cryptographic artefacts, since they can usually best assess the probability and damage of security breaches and should be up to date with current vulnerabilities and weaknesses in cryptography.

- **Internal IT-Architects**: Architects have an overview of the IT landscape and can help with their overview of cryptographic usage and with the interconnections and dependencies between components. They should also be able to have an overall overview of the effects of implementing new cryptographic algorithms, products and implementations.
- **Internal Developers**: These developers either implement cryptography libraries or configure cryptographic implementations to develop and deploy their applications. They can also help with the capture and assessment of cryptographic assets. They and their applications are also affected by changes in the cryptographic landscape.
- **External Vendors**: External vendors provide hardware and software and have an overview of the cryptographic artefacts within their products. They can also provide information about the supported cryptographic implementations within their products as well as a roadmap of future cryptographic updates and improvements.
- **External Service Provider**: External service providers might be used for different use cases within a company and depending on these use cases they might have valuable information about the currently used cryptographic artefacts as well as the effects of implementing new algorithms and products. They might also have experience from other clients, where they might already have worked on implementing new cryptographic algorithms, frameworks and products.

The costs of crypto agility cover the whole life cycle from asset management, through the migration and transition to new cryptography, as well as the continuous efforts thereafter to maintain secure cryptography. The costs also cover the workforce, compute power, the products and their licenses.

The asset management process of scanning and assessment can be once off, which also includes the search for the right tools as well as the implementation, scanning for assets and reporting of these tools.
The scanning for assets and the assessment of these assets should be at least a once of event, but for crypto agility, these actions should be repeated regularly, meaning these costs should also be included in the planning. The costs for continuous scans can be reduced, by limiting reoccurring scans to prioritized assets.

Internal timelines and hard cryptographic deadlines should be considered in the planning, due to the fast-evolving landscape of cryptography. Effective roadmap planning therefore also hinges on these factors to be able to swiftly adapt to new algorithms, standards and security requirements that is critical for long-term resilience.

As crypto graphic standards shift (e.g. known dates of expired algorithms, deprecation dates or new compliance guidelines evolve), organizations must align internal projects

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

and release cycles with these deadlines to avoid disruptions. This requires continuous direct communication and alignment with Change and Release Management.

Since rigid roadmaps can backfire and cybersecurity needs to react fast because of unforeseen vulnerabilities or for example because of delays in 3rd party dependencies, flexible and adaptable strategies need to be implemented.
Balancing predictable deadlines, deliveries and proactive timeline management ensures timely and sustainable crypto transitions without sacrificing operational efficiency.

The flexibility factor should not be neglected. It might be necessary to replan everything completely due to planned and implemented cryptographic artifacts being broken, compromised or even exploited.

4.3 Implementation

A normal implementation of new cryptographic artefacts should still follow the normal cycles for implementing new software or hardware, from the test stages, through the change management and security management processes up to the implementation, where also problem management should be involved.

There should also be a backup plan and a fallback plan.

The integration of the implementation of cryptographic artefacts is more complex, since there are no new applications or servers being deployed, but applications and servers, currently running in production, are migrating and transitioning to new cryptography algorithms, libraries or products.

4.4 Continuous Improvement / Reflection / Lessons Learned

Achieving Crypto agility and a smooth and seamless transition between cryptographic technologies, standards and regulations requires more than just switching the technology or adopting new algorithms. It demands a culture of continuous improvement, adjusting tested procedures and processes and structured reviews.

Like in other IT disciplines, every cryptographic migration offers critical lessons. Some procedures and processes succeed while others reveal gaps in planning, testing, implementation or stakeholder communication. By systematically analyzing what went well and what failed, organizations can refine their procedures and processes, update risk assessments and adjust timelines.

Documenting lessons learned, optimizing workflows and iterative process improvements can transform cryptographic transitions from reactive challenges into proactive and repeatable successes. Whether the organization addresses training shortfalls,

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

unexpected compatibility issues or vulnerabilities or delays in vendor support or simply failed rollouts, all these insights can drive smarter processes and more resilience.

Regular reviews and embracing a culture of transparency and reflection ensures that each step and evolution strengthens – rather than disrupts the security posture and helps to evolve the maturity level of the organization.

4.5 Process Continuity / Repetition

Processes
For maintaining sustainable crypto agility, a continuous, repeatable process must be systematically integrated into IT operations. However, competing internal IT priorities – such as new feature development or infrastructure upgrades etc. – might affect the scanning and discovery of cryptographic artefacts.

Since these priorities deprioritize cryptographic scanning and discovery, they are leaving organizations exposed to outdated or vulnerable algorithms. Additionally, slow and tedious processes might delay critical visibility into cryptographic assets which cause investment of excessive amounts of time and can lead to creating compliance risks and security gaps.

Organizations must establish a well-structured and cyclic approach that includes:

- Involvement of change management, problem management and information security management to streamline processes
- Conducting periodic discovery scans (dependent on the organizational needs e.g. monthly, quarterly etc.)
- Maintaining an up-to-date cryptography asset inventory with proper status tracking mechanisms
- Regularly evaluating scanning and repository tools for effectiveness
- Regularly assessing discovered artefacts for cryptographic risks

By embedding these steps into routine operations, businesses can balance competing IT demands. A critical pillar therefore is not just identifying weak or obsolete cryptographic assets, but actively tracking their migration status to ensure timely risk remediation. Being able to report on the current status of the risk with a weaker cryptographic asset maintains visibility and accountability – and prevent prolonged exposure to vulnerabilities or potential breaches when IT priorities shift focus away from cryptographic upgrades.

By integrating a measurable and auditable process alongside other IT initiatives and maintaining real-time oversight of cryptographic risks, organizations are enabled to proactively manage threats instead of handling cryptographic risks ad hoc.

Continuity
Crypto agility is not a once off task but should be a continuous process. Scanning and discovering cryptographic artefacts as well as the assessment of these artefacts should be a regular and continuous process.

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Basically, crypto agility should be a part of life like patch management of software updates.

Some processes like complete scanning, assessment and reporting can be a yearly exercise, and for certain more critical assets or known vulnerable assets, these scans, assessments and reporting can be more regularly.

A tracking system should be used to track the status of weak and broken assets as they are being migrated to use more secure cryptography, to be able to report on the current status of the risks associated with the weaker cryptography.

Roadmap

From Start to Finish and Beyond

Choose the right steps and building blocks for you….

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

5 Appendix A: Public Key Encryption Use Cases

5.1 Key Agreement

Key agreement is a fundamental process in Public Key cryptography, that allows two or more parties to securely establish a shared secret key over an insecure communication channel. This enables secure sessions in web communication, VPNs and messaging apps. [14] [15]

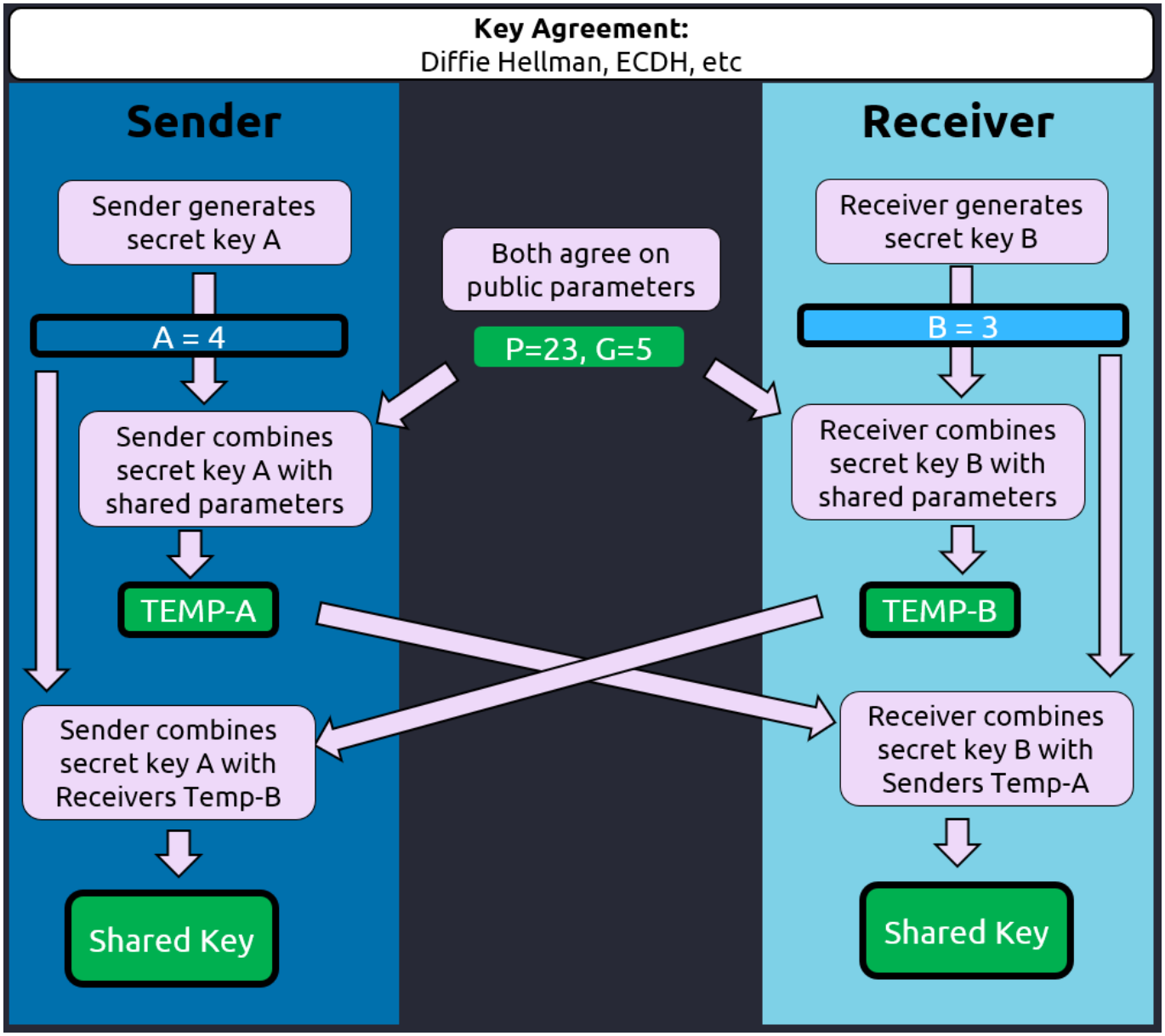


Figure 7: Key Agreement visualization

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

→ Example Walkthrough

- Both parties contribute input to derive a shared key
- Neither side knows the final key alone before the exchange
- Alice and Bob each generate private/public keys
- Both exchange public parts
- Both compute the same shared key

→ Compact and efficient

- Advantage: Ensures neither party decides the key alone
- Disadvantage: Needs further authentication to prevent on-path attacks (MitM)

→ Classical: Diffie Hellman (DH), Elliptic Curve Diffie-Helman (ECDH)

5.2 Key Encapsulation Mechanism (KEM)

A KEM [16] is a cryptographic primitive used to securely establish a shared secret between parties over an insecure channel. Unlike traditional key agreement protocols (like DH), KEM separates the key generation and encapsulation process, and also implements a quantum safe algorithm for encryption and decrypting the shared secret.

A KEM specializes for securely wrapping (encapsulating) a random symmetric key and it is used in hybrid encryption systems: Encrypt data with symmetric key, encrypt that key with KEM

→ Example walkthrough:

- Sender: generates a random key, encrypts (encapsulates) it using receiver's public key
- Sender: sends ciphertext and encapsulation to receiver
- Receiver: decapsulates the decapsulation to get the key
- Receiver: encrypts with the decapsulated key.

→ Compact and efficient

- Advantage: Used in post-quantum cryptography. KEMs have been around for decades.
- Disadvantage: Only one party generates, but with defined rules.

→ Classical: RSA-KEM, ACE-KEM, ECIES-KEM and PSEC-KEM

→ Quantum Safe: ML-KEM, HQC, FrodoKEM

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

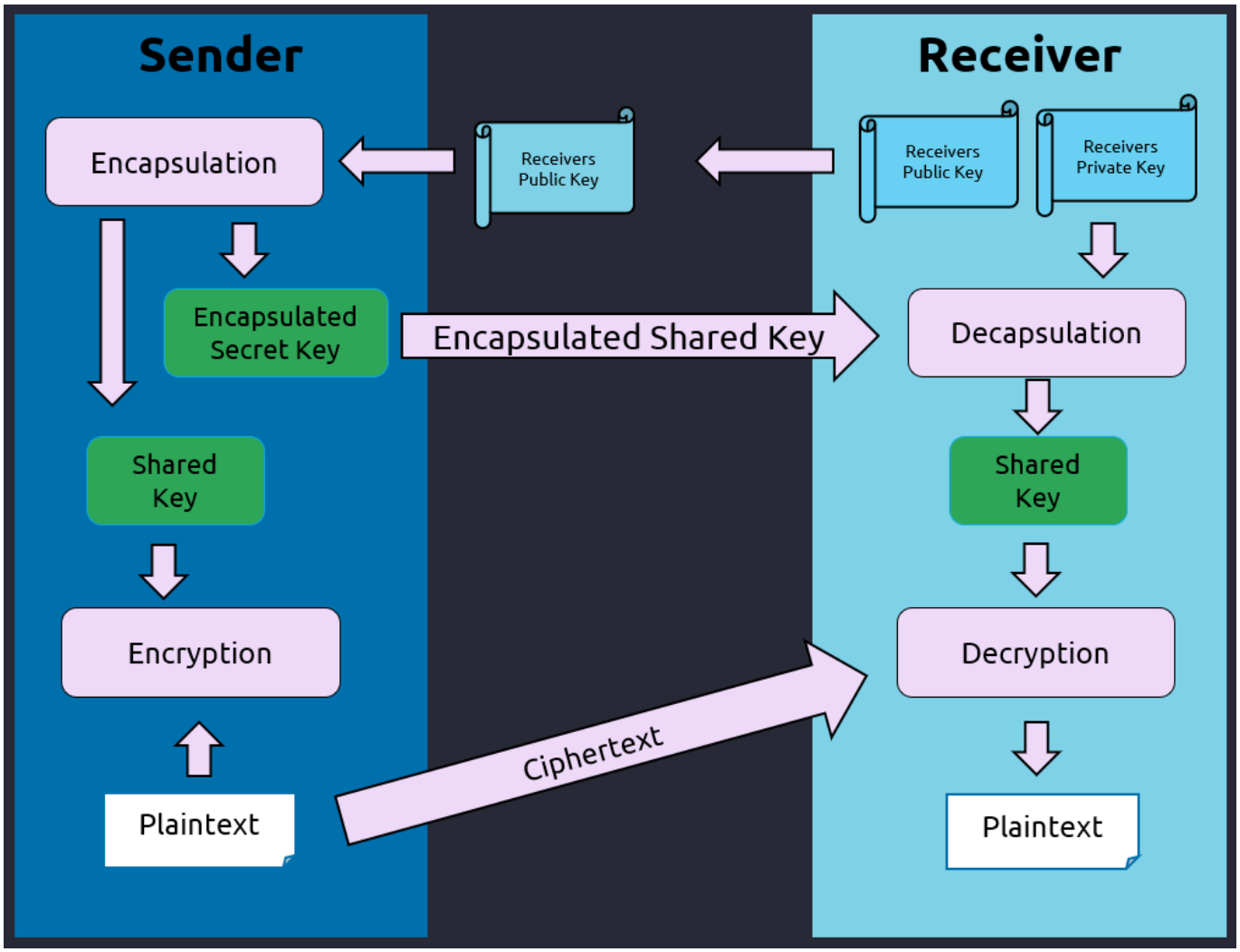


Figure 8: KEM Visualization

5.3 Key Transport (not considered Key Exchange)

Key transport is a simple process where one party generates a secret, without any parameters from the second party. It then encrypts this generated secret with the second party's public key, so that only that party can decrypt the new shared secret.

There is no control over the generation, the randomness or the entropy of this generated key.

Example walkthrough:

- Alice generates a session key
- Alice encrypts the session key with Bob's public key
- Alice sends Bob the encrypted session key
- Bob decrypts the session key with his private key

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

- Alice and Bob exchange messages, encrypted and decrypted with the new shared secret.

→ Simple to implement

- Disadvantage: Only one party controls the secret and its generation.
- Disadvantage: Not ideal when fairness or joint control is needed.
- Disadvantage: There is no control over the secret generation, its entropy or randomness.

→ *Classical: RSA*

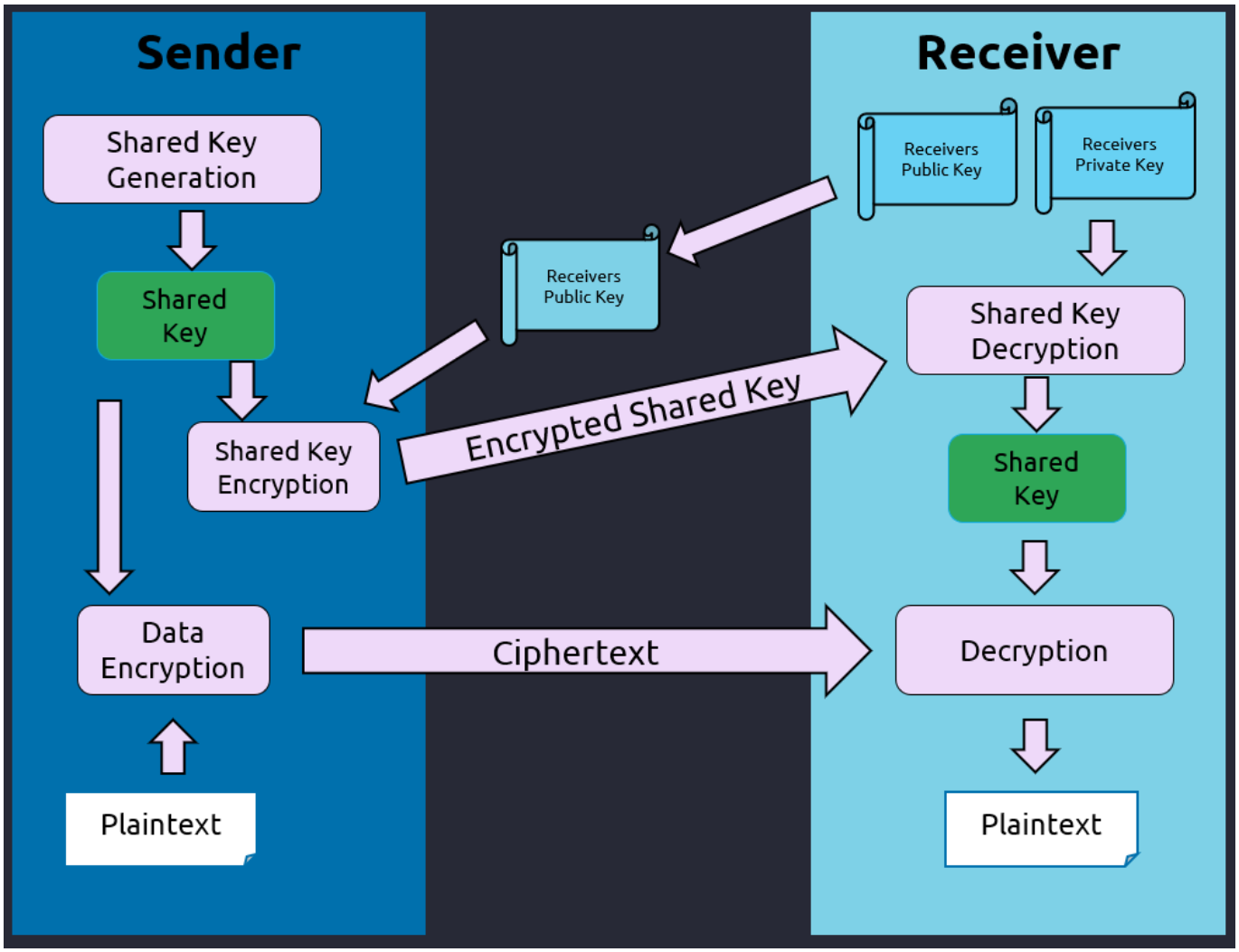


Figure 9: Key Transport visualization

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

5.4 Public Key Authentication - Digital Signatures

Digital certificates, documents, data, code and other artefacts can be digitally signed, to guarantee their authenticity. This means that there is proof of the integrity of that artefact and that is has not been manipulated.

The process of signing an artefact consists of generating a cryptographic hash of the artefact, which the sender then encrypts with its private key. The result is called the signature.

The process of validating an artefact consists of two steps:

- The receiver generates a local hash of the artefact.
- The receiver also decrypts the signature with the sender's public key, which should produce the same result as the local hash of the artefact.

This process covers multiple use cases:

- Authentication: Confirms the signer is who they claim to be.
- Integrity: Detects any tampering in the message containing the artefact.
- Non-repudiation: Signer cannot deny having signed the artefact.

Algorithm	Key Size(s)	Signature Size	Secure (2025)?	Notes
RSA-PSS	≥2048 bits	≈ key size	✅ Yes	Probabilistic variant of RSA; better than PKCS#1 v1.5
ECDSA	256–521 bits	~64–132 bytes	✅ Yes	Based on elliptic curves; used in TLS, Bitcoin
EdDSA (Ed25519)	256 bits	64 bytes	✅ Yes	Fast, secure, deterministic; used in OpenSSH, DNSSEC
DSA	1024–3072 bits	~40–64 bytes	⚠️ Aging	Standardized by NIST; less used today
SPHINCS+	256-1024 bits	17–50 KB	✅ Yes (Post-Quantum)	Stateless hash-based signature scheme
Dilithium	1952-4896 bits	2–4 KB	✅ Yes (Post-Quantum)	NIST PQC finalist, part of ML-DSA
Falcon	897-1793 bits	666-1793 Bytes	✅ Yes (Post-Quantum)	Fast, compact; requires floating point and complex implementation

Table 2: PKI algorithms

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

6 Appendix B: Hashing and Encryption

6.1 Hashing

Cryptographic hashing is a mathematical algorithm that takes data of any input size, and produces a fixed-size output (hash, message digest or fingerprint). The same input data always produces the same hash when using the same key and algorithm.

Cryptographic hashes are irreversible, meaning that it's computationally infeasible to reproduce the original input data from a hash value.

Hashes are used in the following use cases:

- Digital signatures, where the message is hashed, and the hash is signed.
- Digital Integrity, to verify that the data hasn't been tampered with.
- Password hashing, passwords are never stored, only the hashed passwords.
- HMAC, for message integrity, where the data is hashed using a secret key
- Key derivation, where hashed of secrets and passwords are used to generate keys

Algorithm	Output Size	Year	Safe in 2025?	Notes
SHA-1	160 bits	1995	❌ Broken	Collision attacks proven (Google, 2017)
SHA-2	224–512 bits	2001	✅ Yes	Strong, widely used (e.g., SHA-256, SHA-512)
SHA-3	224–512 bits	2015	✅ Yes	Keccak-based; good alternative to SHA-2
BLAKE2	256/512 bits	2013	✅ Yes	Very fast, secure, supports keyed hashing
BLAKE3	256 bits	2020	✅ Yes	Even faster, parallelizable, constant-time
RIPEMD-160	160 bits	1996	⚠️ Aging	No known attacks, but slower and older
MD5	128 bits	1991	❌ Broken	Collisions found; don't use for security

Table 3: Hash algorithms

Recommended Hash Algorithms (May 2025):

Application	Algorithm
General Purpose	**SHA-256**, **SHA-512**, **SHA3-256, SHA3-512**
Fast & Secure Applications	**BLAKE2b**, **BLAKE3**
Password Hashing	Use a **KDF** (e.g., **bcrypt**, **scrypt**, **Argon2**)
MAC/HMAC	**HMAC-SHA256**, **HMAC-BLAKE2**

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

The following Hash Algorithms should not be used:

- **MD5** – collisions easy to generate
- **SHA-1** – proven to be insecure
- **RIPEMD-160** – aging, but still not broken

6.2 Symmetric Encryption

In symmetric encryption, the same secret key is used for both encryption and decryption of data.
The main advantage is symmetric encryption is its speed and efficiency. The main disadvantage is the key distribution between the different parties.

Advantage: Fast and efficient
Disadvantage: Requires secure key sharing

There are 2 different types of symmetric encryption namely block ciphers and stream ciphers.
Block ciphers encrypt data in fixed-length blocks (e.g., 64 bits, 128 bits or even 256 bits), whereas stream ciphers encrypt data bit-by-bit or byte-by-byte, like a stream of data.

Feature	Block Cipher	Stream Cipher
Data unit	Block (fixed-size chunks)	Bit or byte stream
Speed	Generally slower, secure	Often faster, lower latency
Modes needed	Yes (ECB, CBC, GCM...)	No (self-streaming)
Error propagation	Affects full block (in CBC)	Affects only a small part
Use cases	File encryption, disk encryption	Voice/video calls, IoT, VPNs
Secure Ciphers*	AES, Camellia, Twofish	ChaCha20, Salsa20, Trivium and AES-CTR
Insecure Ciphers	DES, 3DES, GOAT	RC4

Table 4: Block Ciphers vs. Stream Ciphers

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Cipher	Type	Block Size	Key Size(s) (bits)	Secure (2025)?	Notes
AES	Block	128 bits	128, 192, 256	✅ Yes	NIST standard, widely trusted
ChaCha20	Stream	–	256	✅ Yes	Modern, fast, used in TLS/SSH
Salsa20	Stream	–	256	✅ Yes	Predecessor of ChaCha20
Camellia	Block	128 bits	128, 192, 256	✅ Yes	ISO/IEC standard, AES alternative
SM4	Block	128 bits	128	✅ Yes	Chinese government standard
SEED	Block	128 bits	128	✅ Yes	South Korean standard
3DES	Block	64 bits	112, 168	❌ Deprecated	Slow, meets-in-the-middle attack
DES	Block	64 bits	56	❌ Broken	Easily brute-forced today
RC4	Stream	–	40–2048	❌ Broken	Biases in keystream; deprecated
Trivium	Stream	–	80	✅ Yes (for constrained use)	Lightweight; good for IoT
Grain-128	Stream	–	128	✅ Yes (lightweight)	Part of eSTREAM project
HC-128	Stream	–	128	✅ Yes	Fast in software
Twofish	Block	128 bits	up to 256	✅ Yes	AES finalist; secure but less used
Serpent	Block	128 bits	128, 192, 256	✅ Yes	Conservative design, AES finalist
PRESENT	Block	64 bits	80, 128	✅ Yes (lightweight)	For RFID, smartcards
LEA	Block	128 bits	128, 192, 256	✅ Yes	Korean lightweight cipher

Table 5: Symmetric Encryption algorithms

The current algorithms are generally considered secure and are actively used:

- AES-GCM, ChaCha20-Poly1305 are recommended for general-purpose use.
- Camellia, Twofish, and Serpent are also secure alternatives.
- Trivium, Grain, PRESENT are suitable for constrained devices (e.g., IoT)

6.3 Stream Cipher

Stream ciphers encrypt data bit-by-bit or byte-by-byte, like a stream of data. The encryption is done with a keystream, which is continuously generated based on a symmetric key and a nonce/IV.

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

The IV or initialization vector is added to generate entropy and randomness. The encryption is basically the keystream being XORed with the plaintext.

Stream ciphers are considered faster and better for real-time or low-memory environments, but is considered less secure than block ciphers.

Currently accepted stream ciphers are ChaCha20, Salsa20, Trivium, and AES-CTR

The following streams ciphers are insecure and should not be used: RC4

6.4 Block Ciphers

Block ciphers encrypt data in fixed-length blocks (e.g., 64 bits, 128 bits or even 256 bits). The data is divided into fixed-length blocks, which are then encrypted with a secret key, which is usually the same size (e.g. 64, 128 or 256 bits).

Block ciphers are usually used for file, disk and message encryption, and is slower than steam ciphers. Block ciphers also need padding, to fill up blocks that aren't full, but it is generally more secure than stream ciphers.
The main Block Ciphers in use today: AES, Camellia, Twofish

The following Block Ciphers are considered broken and should not be used: DES, 3DES

6.5 Block Cipher Modes

Block ciphers encrypt and decrypt fixed-size blocks and there are multiple modes being used, some faster and some slower, some more secure and other not secure at all.

Mode	Full Name	Authenticated?	IV/Nonce Required?	Secure (2025)?	Notes / Usage
ECB	Electronic Codebook	❌ No	❌ No	❌ Insecure	Leaks patterns; never use with real data
CBC	Cipher Block Chaining	❌ No	✅ Yes	⚠️ With caution	Requires padding; IV must be random
CFB	Cipher Feedback	❌ No	✅ Yes	✅ Yes	Self-synchronizing; stream-like output
OFB	Output Feedback	❌ No	✅ Yes	✅ Yes	Resistant to transmission errors
CTR	Counter Mode	❌ No	✅ Yes	✅ Yes	Very fast; secure if nonce is unique
GCM	Galois/Counter Mode	✅ Yes (AEAD)	✅ Yes	✅ Yes	High-performance AEAD; used in TLS, IPsec
CCM	Counter with CBC-MAC	✅ Yes (AEAD)	✅ Yes	✅ Yes	Used in constrained environments (IoT)

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

XTS	XEX with Tweaked CodeBook	❌ No	✅ Yes (tweak)	✅ Yes	Disk encryption (e.g., BitLocker, LUKS)
OCB	Offset Codebook Mode	✅ Yes (AEAD)	✅ Yes	✅ Yes	Fast AEAD mode; patented in past

Table 6: Block Cipher Modes

- OCB was previously patented but is now freely available for open-source and non-commercial use. It's very fast and secure.
- **Authenticated:** Indicates whether the mode provides message authentication (AEAD).
- **IV/Nonce**: Initialization vector or nonce must be unique per encryption to ensure security.

Recommended Cipher Modes (May 2025):

- GCM: Best general-purpose AEAD mode.
- CTR: Fast and secure if used correctly (ensure nonce uniqueness).
- OCB: Excellent but not as widely supported.
- XTS: Best for full disk encryption (FDE).

Use with Care Block Cipher Modes:

- CBC: Still used in legacy systems but must use unpredictable IVs and padding carefully.
- CCM: Slower than GCM; suitable for constrained devices.

Deprecated and insecure Block Cipher Modes:

- ECB: Leaks structure and patterns; do not use for any sensitive data.

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

7 References

[1] F. Boudot, P. Gaudry, A. Guillevic, N. Heninger, E. Thomé, and P. Zimmermann, June 11, 2020: Comparing the difficulty of factorization and discrete logarithm: a 240-digit experiment*: https://arxiv.org/pdf/2006.06197

[2] Coppersmith, D.: Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities. Journal of Cryptology 10(4), 233–260 (Sep 1997

[3] Nemec, M., Sys, M., Svenda, P., Klinec, D., Matyas, V.: The return of coppersmith's attack: Practical factorization of widely used rsa moduli. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. p. 1631–1648. CCS '17, Association for Computing Machinery, New York, NY, USA (2017). https://doi.org/10.1145/3133956.3133969 , https://doi.org/10.1145/3133956.3133969

[4] V. Gheorghiu and M. Mosca, 6 Feb 2019: Benchmarking the quantum cryptanalysis of symmetric, public-key and hash-based cryptographic schemes: https://arxiv.org/abs/1902.02332

[5] NIST: Information Technology Laboratory - Computer Security Resource Center: Crypto Agility: https://csrc.nist.gov/projects/crypto-agility

[6] Lily Chen, Information Security and Privacy Advisory Board (ISPAB) March 2024 Meeting: Crypto-Transition and Agility https://csrc.nist.gov/csrc/media/Presentations/2024/cryptographic-agility-and-transition-rd-and-plans/Chen-Day2-Crypto-Agility_and%2BTransition_R_and_D_Plans.pdf

[7] Sandip Dholakia, May 06, 2025: Review & Commentary: NIST Whitepaper Achieving Crypto Agility https://www.rsaconference.com/library/blog/review-commentary-nist-whitepaper-achieving-crypto-agility

[8] Stefan-Lukas Gazdag, Sophia Grundner-Culeman, September 24, 2024: The transition to post-quantum cryptography, metaphorically https://eprint.iacr.org/2024/1487.pdf

[9] NIST, August 13, 2024: Announcing Approval of Three Federal Information Processing Standards (FIPS) for Post-Quantum Cryptography: https://csrc.nist.gov/News/2024/postquantum-cryptography-fips-approved

[10] ENISA, may 03, 2025, v2: Post-Quantum Cryptography: Current State and Quantum Mitigation https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation

[11] NIST March 5, 2025 Cybersecurity White Paper NIST CSWP 39 ipd: Considerations for Achieving Crypto Agility https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.39.ipd.pdf

[12] NÚKIB: 1, February 2025: Minimum requirements for cryptographic algorithms: https://nukib.gov.cz/download/publications_en/Minimum%20Requirements%20for%20Cryptographic%20Algorithms.pdf

[13] IEEE, 31 January 2024: A Framework for Migrating to Post-Quantum Cryptography: Security Dependency Analysis and Case Studies https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10417052

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

[14] Whitfield Diffie and Martin e. Hellman in IEEE Transactions on Information Theory, Vol. IT-22, No. 6, November 1976: New Directions in Cryptography: https://www-ee.stanford.edu/~hellman/publications/24.pdf

[15] NIST SP 800-56A Rev. 3 20018 Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography: https://csrc.nist.gov/pubs/sp/800/56/a/r3/final

[16] Reference implementations of PQC KEMs https://github.com/open-quantum-safe/liboqs

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Disclaimer

This document does not represent the opinion of the European Union or European Commission, and neither the European Union nor the granting authority can be held responsible for any use that might be made of its content.

Neither the Q-PREP consortium as a whole, nor a certain party of the Q-PREP consortium warrant that the information contained in this document is capable of use, nor that use of the information is free from risk and does not accept any liability for loss or damage suffered by any person using this information.

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE