Guidance on becoming cryptographically agile

CANADIAN CENTRE FOR CYBER SECURITY
MAY 2022 | ITSAP.40.018

Cryptographic agility is a concept of best practice that enables cryptographic algorithms used in applications and protocols to be interchanged easily to ensure systems remain secure if new cryptographic vulnerabilities are discovered. This is done primarily through configuration without requiring major software or hardware updates. Agile products must have streamlined software and firmware upgrade capabilities to support cases where all configuration options have been exhausted. To enable a phased transition, agile products should retain interoperability with other systems. Agile products should retain any and all applicable validations and certifications, subject to configuration. Agility relies upon organizational processes and policies that maintain an inventory of locations and uses of cryptographic algorithms and products within an organization to facilitate quick, easy, and complete transitions as needed.

Why is cryptographic agility important?

Over time, breakthroughs in cryptographic research and computing can leave cryptographic algorithms with less strength than their intended design. Legacy applications may employ weak cryptography that can be difficult to upgrade. Vendors with existing support contracts may be unable to react quickly enough to implement and deploy new cryptographic algorithms in response to Common Vulnerability and Exposures (CVE) reports.

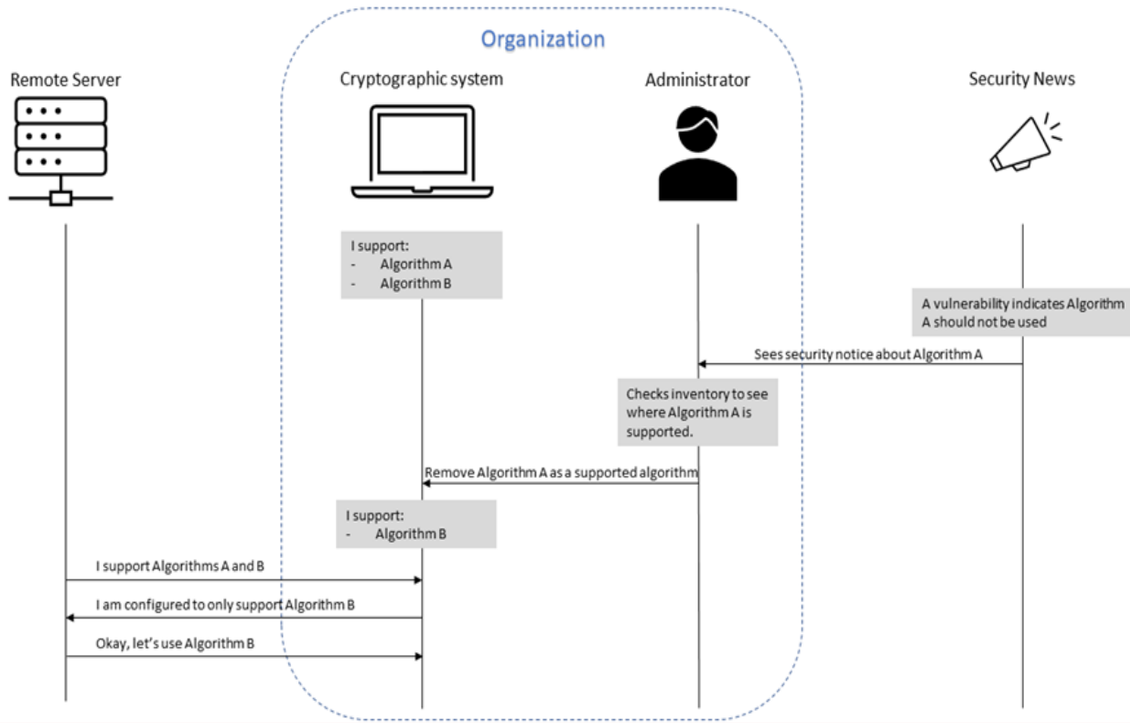
A major cryptographic transition is expected in the near future to mitigate against the threat of quantum computers. Much of the public key cryptography in use by products today will be vulnerable to a sufficiently powerful universal quantum computer. Cyber security products that support cryptographic agility can help your organization through this transition.

How does cryptographic agility work?

Cyber security products that are-designed with cryptographic agility in mind have access to multiple cryptographic algorithms and allow system owners to configure the product to use or prefer certain algorithms. When configuration options are exhausted, these security products have streamlined software and firmware upgrade processes that provide new configuration options. Cryptographically agile systems also have policies and processes in place to ensure configuration changes, as well as software and firmware updates, are quickly identified.

Network security protocols often negotiate which cryptographic algorithms to use, thus allowing endpoints to be configured differently. The ability to set preferences in product configuration for cryptographic algorithms allows for a phased approach to migrating equipment and applications which maintains interoperability.

Cryptographic agility in action



For more information on the quantum threat, see *Addressing the Quantum Computing Threat to Cryptography* (ITSE.00.017) and *Preparing Your Organization for The Quantum Threat to Cryptography* (ITSAP.00.017).

Communications Security Establishment
Centre de la sécurité des télécommunications

Canada

Cryptographic agility

CANADIAN CENTRE FOR CYBER SECURITY

MAY 2022 | ITSAP.40.018

What cryptography should I be using now?

When selecting a vendor, ensure they use standardized cryptography with an implementation certified under an independent assurance program (e.g. Cryptographic Module Validation Program [CMVP] and Common Criteria [CC]). Guidance on cryptographic algorithms and protocols can be found in two publications from the Cyber Centre: Cryptographic Algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information (ITSP.40.111) and Guidance on Securely Configuring Network Protocols (ITSP.40.062). These documents will provide guidance on the transition to quantum-safe cryptography once it is standardized.

Does my organization support cryptographic agility?

To determine whether the products currently deployed in your organization are cryptographically agile, you should complete the following actions:

1. Create an inventory of your products that use cryptography.
2. Ask your product vendors how they support cryptographic agility. If they do not, request details on their plans to implement agility in future releases.
3. Confirm whether your vendors use standardized, validated cryptography (e.g. validated modules under the Cryptographic Module Validation Program) in current and future agile products.
4. Determine if your organization has policies and procedures in place in your IT change management activities to support cryptographic agility.

Creating an inventory of all the cryptography used in a large enterprise may be challenging. There is likely cryptography within products that you aren't aware of.

Some vendors offer products for enterprises that can scan systems or networks and report on cryptography that may need to be replaced. Standard security considerations and practices should be followed when deploying tools that monitor sensitive components like those employing cryptography.

Becoming cryptographically agile

We recommend your organization take the following steps to help become cryptographically agile:

1. Inventory your products that use cryptography.
2. Implement new policies and procedures in your IT change management activities to maintain this inventory on an on-going basis and manage any configuration changes related to cryptographic agility.
3. Ask the vendors of your cryptographic products if they support cryptographic agility. Understand their software and firmware upgrade policies and procedures for any necessary large agility updates.
4. Develop a transition plan for any non-agile products, including any legacy cryptography, to upgrade to products that support cryptographic agility.
5. Create a procurement policy to ensure cryptographic agility is considered in future purchases.
6. Ensure your agility plan uses standardized cryptographic algorithms such as those recommended in ITSP.40.111 and ITSP.40.062 and that the implementations of the cryptographic algorithms have been validated under the Cryptographic Module Validation Program.

Learn more

If you want to learn more about cyber security topics, please check out the following publications on our website (cyber.gc.ca).

- *Using Encryption to Keep Your Sensitive Data Secure (ITSAP.40.016)*
- *Preparing Your Organization for The Quantum Threat to Cryptography (ITSAP.00.017)*
- *Preventative Security Tools (ITSAP.00.058)*
- *Implementation Guidance: Email Domain Protection (ITSP.40.065)*
- *Cyber Security Considerations for Consumers of Managed Services (ITSM.50.030)*

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada