ANCHOR SECURITY ARCHITECTURE FOR CMMC 2.0

Simple architecture for CMMC compliance with Anchor Endpoint Platform (version 8)

Abstract

We provide a brief introduction to the basic requirements of the CMMC 2.0 and how Anchor can be used to reduce the cost and effort to become CMMC certified. To that end, we provide a security architecture that is broad and easy to implement for a variety of organizations. We provide examples of IT infrastructures and how the architecture can fit custom to each. Lastly, we provide a detailed mapping exercise, clearly illustrating the domains and sub-domains that are covered by the Anchor platform independently or with the support of other solutions.

Anchor compliance documents

support@datanchor.io

Table of Contents

Introduction

The **Cybersecurity Maturity Model Certification (CMMC)** is a certification, contractors need before they can perform work for the Department of Defense. All suppliers including small and medium sized businesses must implement CMMC 2.0 level 2 or higher to maintain business within the Department of Defense supply chain. The CMMC framework is built on the NIST 800-171 foundation, which the Defense Industrial Base (DIB) has been attesting to, since 2017 for their contracts.

This document explains the key aspects of the CMMC and how Anchor can be used to reduce the cost and effort to become CMMC certified.

What is different in CMMC 2.0?

- Move from 5 levels to 3 levels of data sensitivity.
    - Level 1 (Foundational) only applies to companies that focus on the protection of Federal Contract Information (FCI).
    - Level 2 (Advanced) is for companies working with Controlled Unclassified Information (CUI).
    - Level 3 (Expert) is focused on reducing the risk from Advanced Persistent Threats (APTs).
- From an absolute Pass/Fail system of the original CMMC, there is a composite, 1, 3, and 5-point scoring system for controls.
- CMMC 2.0 requirements can be in contracts as soon as March 2023
- The Department of Justice offers monetary incentives for whistle-blowers. False attestation to the original NIST controls will lead to penalties, 20% of which is passed on to the whistle-blower.

What Is a System Security Plan?

A security plan simply describes what an organization does in order to be secure. How do you know your organization is secure? Because you do the things in your security plan.

As for CMMC, your **System Security Plan (SSP)** describes how you protect sensitive information from the government such as Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).

From CMMC CA.L2-3.12.4:

“A system security plan (SSP) is a document that outlines how an organization implements its security requirements. An SSP outlines the roles and responsibilities of security personnel. It details the different security standards and guidelines that the organization follows.”

Being certified for CMMC means having an auditor review your organization’s SSP to ensure it meets all of the requirements for the CMMC level at which you’re being certified, and verifying that your organization is actually doing everything you claim in your SSP.

What Is a Covered Contractor Information System?

A **Covered Contractor Information System** defines the boundaries of connected network of computers and devices that process sensitive data from the government such as FCI and CUI.

Anything that contains or processes this kind of information is part of the covered contractor information system. Your SSP must thoroughly cover your entire covered contractor information system. Limiting and reducing the scope of devices that can process FCI and CUI reduces the size of your covered contractor information system and therefore simplifies the SSP needed to protect it.

The simpler your SSP, the easier it is to create, implement, and audit. Easier means faster and at a lower cost. The formula to reduce your cost and effort to be CMMC certified is:

1. Limit and reduce the scope of your covered contractor information system.
2. Create a simpler SSP to protect that covered contractor information system.
3. **Save on cost and effort implementing your SSP and getting CMMC certified.**

What Is a Security Architecture?

A **Security Architecture** is the technical design of your covered contractor information system, including what is in it, how it all fits together, and how it enables controls to implement your SSP.

Security Architecture

In this section, we provide the proposed security architecture with the Anchor platform. The architecture is simple and broad; it applies to a variety of business scenarios, covering a wide range of industries with different IT infrastructure, from very elementary to sophisticated and hybrid.

The proposed architecture is illustrated in Figure 1. With Anchor, the “system” is the set of Anchor-enabled devices containing CUI. Anchor simplifies CMMC compliance by reducing the system boundary from a complex network to a narrow set of Anchored files that are end-to-end encrypted by Microsoft CNG modules with FIPS-validated cryptography [CMVP].

The High-Level Architecture

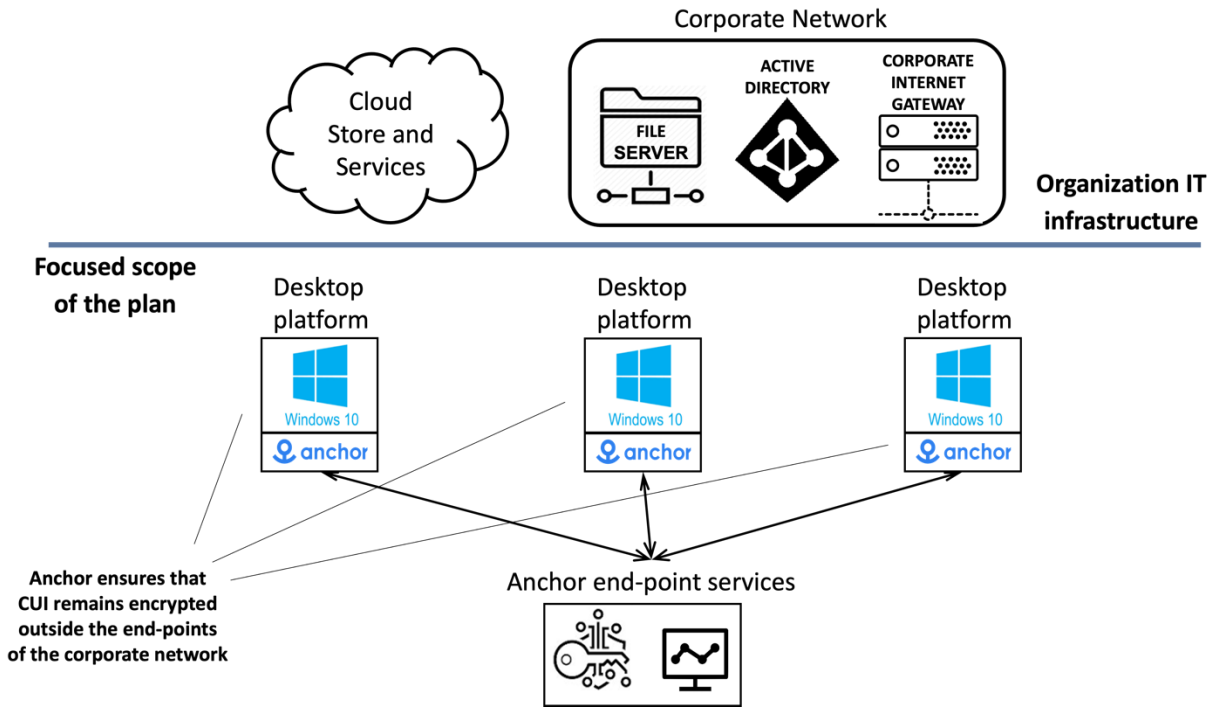

Figure 1: Anchor simplifies CMMC compliance by reducing the system boundary to a narrow set of Anchored files that are accessed and processed at the Anchor-enrolled endpoints (below the blue line). CUI is end-to-end encrypted by Anchor with FIPS-validated cryptography. The compliant architecture is independent of the IT infrastructure (above the blue line). Thus, the mapped domains are covered for a broad set of organizations with various sophistication.

At the heart of our architecture lies the fact that Anchored CUI can only be consumed at Anchor-enabled endpoints due to the robust end-to-end encryption system integrated into the desktop platform built by Anchor. The key management, and audit logging services are both provided by the Anchor platform, external to the desktop agent. These services provide the secure access management and audit log creation in coordination with the desktop platform, with components orthogonal to the rest of the organization IT infrastructure (above the blue line in Figure 1), making the implementation of the security plan **simpler, lower cost, and more robust**.

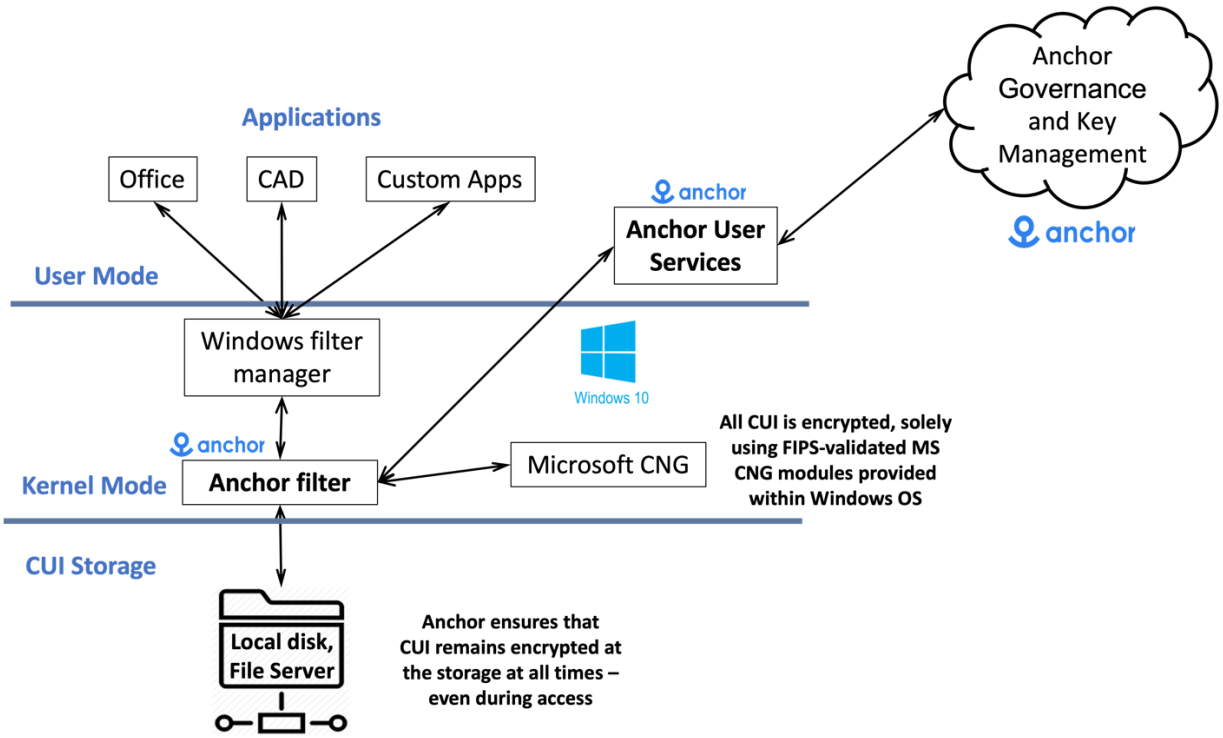

Figure 2: CUI is accessed in plaintext only from endpoints. All CUI remains encrypted at the storage at all times, even during access by applications. Encryption is only done by FIPS-validated Microsoft CNG Modules. Anchor operates in FIPS-mode and it merely conducts the data flow between the store and the applications to enforce CMMC controls. No module outside of MS CNG deals with encryption or decryption of CUI.

End-point users are managed by Active Directory (local or Azure). The CUI files can be stored on a network drive or a local store, but they cannot be decrypted on those drives due to end-to-end encryption. As the CUI is always encrypted at rest, each device containing CUI is treated as a mobile device. The end-point architecture is illustrated in Figure 2.

FIPS Compliance

All encryption and decryption are done via FIPS-Validated Microsoft CNG modules and the Anchor conducts the flow of data in accordance to the CMMC controls. The Microsoft CNG Modules provide encryption via the Federal Information Processing Standard (FIPS) 140-2 mode. FIPS 140 is a cryptographic security standard used by the federal government and others requiring higher degrees of security in order to comply with NIST requirements for data protection.

Anchor only utilizes the certified and unmodified encryption modules available within the Microsoft Operating Systems within desktop and server. Consequently, Anchor **will not** show up in the NIST Cryptographic Module Validation Program vendor lists. When the FIPS mode is enabled via the registry, encryption in all Anchor filter workflows use FIPS-approved algorithms during the encryption and decryption of CUI passed back and forth between the applications and the storage. At the time of this writing, the active certificate is #4536 which has a sunset date of 09/21/2026.

Examples of IT Infrastructures

In this section, we provide a few IT architectures with relevant use cases. As discussed in the last section, end-to-end encryption provided over the Anchor platform supports the security architecture for internal collaboration over a variety of use cases (illustrated in Figure 3).

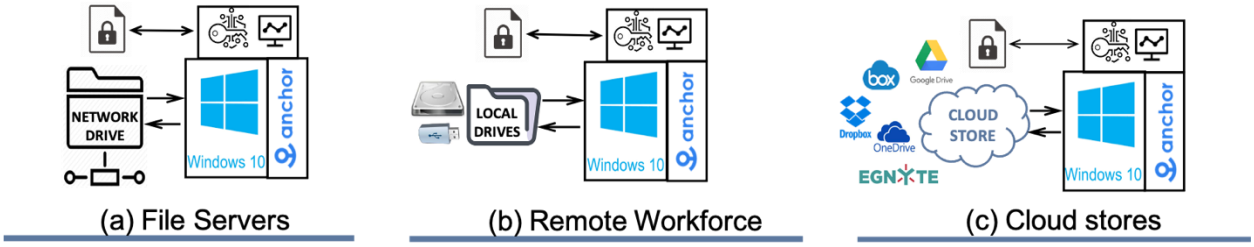

Figure 3: End-to-end encryption across endpoints makes it possible to collaborate on unstructured data over a variety of data stores.

(a) Many organizations keep CUI internally within their network at local file servers (mainly over Windows Server OS). For example, **manufacturing**, **construction**, and **high-tech engineering** organizations, building products and IP for the DoD use a variety of file types and applications, including CAD and Office. Anchor keeps the designs, associated IP, contracts, and calculations encrypted in the file server, while enabling access from the desired applications, a few of which are shown in Figure 4, without a change in the workflow or the application itself. Directories and CUI files are stored on a network drive but cannot be decrypted on that drive due to end-to-end encryption. As the CUI is always encrypted at rest, each device containing CUI is treated as a mobile device.

Figure 4: Anchor platform has support for a wide variety of applications that encompass CAD and Office. It enables secure and no-friction access and collaboration on the associated files.

As a result, CUI is protected automatically as per CMMC, while the organization does not lose any efficiency in processing the data.

(b) With the pandemic, organizations have a considerable amount of its workforce needing to access CUI remotely. In such cases, files are downloaded to the local drives for processing. This is sometimes despite the policies on VPN use, due to the performance issues associated with remote consumption. Such local store and access inflate the attack surface and makes the CUI policies difficult to enforce.

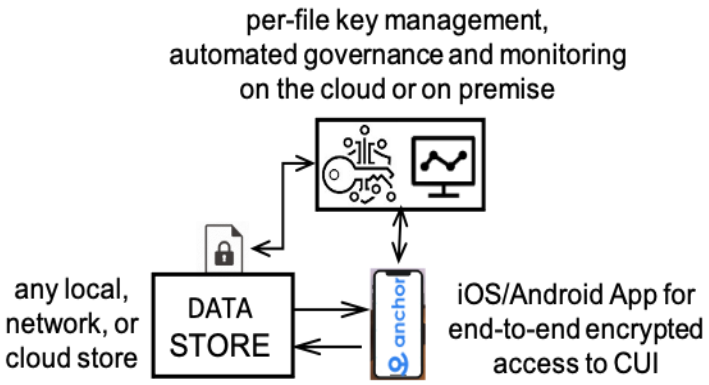

Figure 5: Anchor platform extends its end-to-end encryption to the mobile platforms including iOS and Android. As a result, files can be viewed from smart phones and tablets.

With the Anchor platform, this would not pose a problem. An admin can simply include the local drive as a protected area and make sure that the CUI remains safe, even when accessed remotely by the employees or contractors. Furthermore, Anchor's protection extends to a Mobile App for **iPhone and Android platforms**, as shown in Figure 5. As a result, CUI can be accessed from smart phones and tablets.

(c) Organizations are moving to a hybrid IT infrastructure with cloud applications and data stores involved in everyday processes. Most organizations will have certain processes handled over FedRAMP High government clouds such as Microsoft GCC High. However, it is likely that there will be applications and processes involving CUI on commercial cloud as well. Anchor platform provides the flexibility of protecting data on commercial cloud due to its robust end-to-end encryption integrated.

DFARS 7012 and **ITAR** have additional requirements, such as information must not be exported out of the United States. This creates an obstacle to using commercial cloud storage because commercial clouds store data outside the US and are administrated by people outside the US. However, they carve out an exception when the information end-to-end encrypted with FIPS-validated cryptography. With Anchor end-to-end encryption you can store data on commercial clouds and still be compliant.

Data Flow Diagram

For the Anchor security diagram given in the previous section, a detailed data flow diagram is provided in Figure 6. The diagram illustrates the data structures and types that are exchanged across the components of Anchor. All CUI access happens within the CUI access points, where the encryption and decryption of the CUI takes place. Anchor eliminates the possibility of any CUI content to be taken out of the access point. The only communication outside involves policy and key exchange, both of which are executed over an end-to-end encrypted (via Microsoft TLS modules) channel.

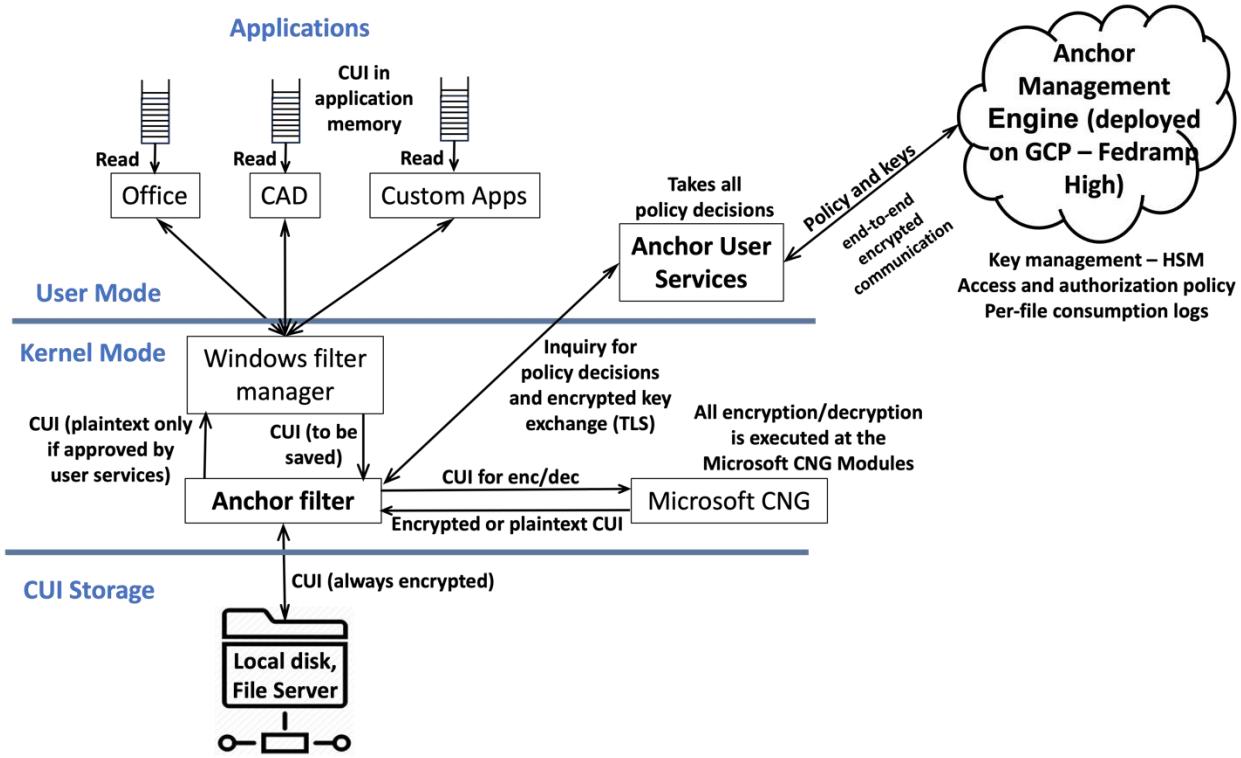

Figure 6: Anchor data flow diagram. This diagram details the data structures and types exchanged across different blocks within the security architecture.

CMMC Mapping

Assuming the security architecture described above, we provide a breakdown of the CMMC Level 1 and 2 practices by whether and how they can be covered with Anchor. We also provide supplemental text that can be used in your SSP as a template.

Each practice is labeled as one of:

Anchor Security Architecture Covered	The Anchor security architecture described above effectively implements the practice.
Shared Coverage	The Anchor security architecture described above contributes to implementing the practice, but complete coverage will require additional contribution from the customer.

Anchor Security Architecture Covered	The Anchor security architecture described above effectively implements the practice.
Customer Responsibility	The customer is responsible for implementing the practice entirely.

You can find the complete controls mapping in the Anchor CMMC SRM Table spreadsheet.

Conclusion

This document introduced the CMMC and its key points at high level. It described a model security architecture based on Anchor and Windows 10/11 that applies to a broad range of Department of Defense contractors and their business environments. Finally, it mapped the CMMC 2.0 Level 1 and 2 practices to the model Anchor Security Architecture and provided templates that can be used when creating your organization's SSP, reducing the time and effort to get CMMC 2.0 Level 2 certification.