



EPP™

Enclave Processing Platform

The path to CMMC 2.0

Getting a company CMMC ready is a complex journey. The solution to this is an Enclave Processing Platform (EPP™), which meets all DoD cybersecurity compliance requirements.

EPP™ is an enclosed solution used to process DoD data

EPP™ is an isolated ecosystem called an enclave. Its intended use, is to process data in relation to contracts with the US Department of Defense (DoD) under DFARS 252.204-7012. Employees log on to dedicated terminals within the enclave and are here able to send/receive emails, share files and attend or host virtual Teams meetings with other parties while being in compliance with CMMC 2.0 and NIST 800-171.

Built on Microsoft Government Community Cloud

EPP™ is built on Microsoft Government Community Cloud High (GCC High). GCC High is a version of the Microsoft 365 Cloud service, which most companies already utilize today. The difference compared to Commercial 365 is that GCC High solely resides on datacenters within Containments of the United States (CONUS), and all support personnel are cleared US nationals. GCC High is approved by FEDRAMP, which is a requirement when using cloud services under DFARS 252.204-7012 (D) Clause, and processing Controlled Unclassified Information (CUI). It is also possible to process ITAR data on the platform.

GCC High has all the familiar applications just as commercial Microsoft 365

With GCC High, you get all the applications we all know and are used to working with. This introduces an almost non-existing learning curve when employees start using the platform. The main difference is the increased security systems built into the platform, and the usage of these.

Connecting the on-premises infrastructure

EPP™ is connectable to the headquarter and production network (OT) within the local country. This leverages selected employees access to DoD data from mobile devices, and computers locally on-site. Examples of this can be, emails, technical drawings and/or configuration files targeted to CNC or other production equipment.

We handle all the practical tasks

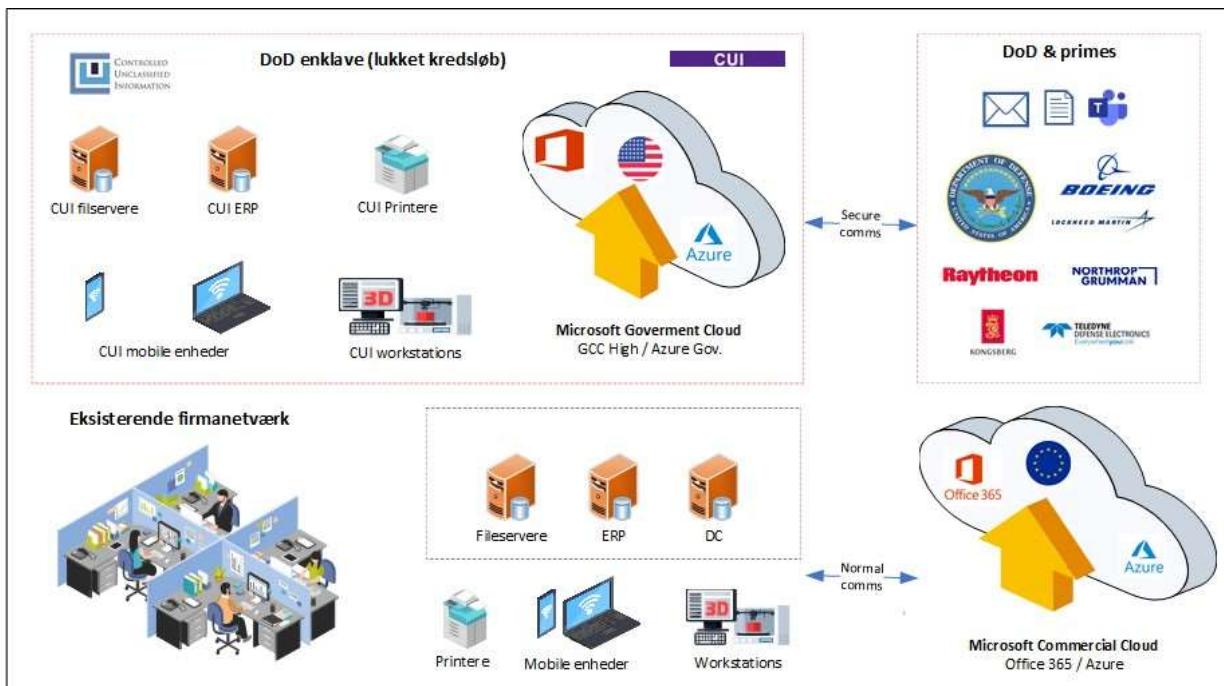
We handle all the practical tasks related to running the platform and being in compliance with CMMC 2.0 and NIST 800-171. The result of this, is that the company will at any given time be in compliance with the cybersecurity requirements set by DoD.

Extended requirements prior to being CMMC 2.0 ready

Prior to being CMMC 2.0 certification ready, several activities need to be in place. Policies, procedures, and controls need to be developed and all gathered in a Systems Security Plan (SSP), this typically takes anywhere from 12-18 months. With an EPP™ this time span is dramatically reduced, due to the nature of the platform initially being CMMC 2.0 Level 2 and NIST 800-171 compliant.

Advantages of EPP™

- Safe – closed ecosystem used to process DOD data (CUI & ITAR)
- Efficient – makes it manageable to comply CMMC 2.0 Level 2 & NIST 800-171
- Turn-key – we handle everything: setup, support, and maintenance
- Flexible – additional users are easily enrolled / disenrolled onto the system



DoD enclave example

Enclave Processing Platform (EPP™) is delivered in corporation with e-ducators and Qvist IT. Both companies have a long track record within the NIST 800-171 framework, which CMMC 2.0 is based on. We are the first to deliver complete turnkey solutions within the Nordic to be CMMC 2.0 level 2 certified.



NIST 800-171

Cost & pricing

An example of a turnkey solution which is required to be (and stay) NIST 800-171 and CMMC 2.0 Level 2 compliant, ready for certification.

Pricing will vary, based on the number of users, custom adjustments etc. final prices are calculated in connection with a specific solution for a company.

Startup cost

Development of the System Security Plan (SSP).

CMMC policies, procedures, and controls.

Customization of the EPP™ (equipment within the company).

CMMC awareness training and testing

Certification guidance

Project management

Enclave setup - 5 users - (data migration etc.).

Indicative price (dependent of the number of users)

Contact us.

Maintenance (monthly)

Enclave maintenance incl fair-use

Goal management, controls, training, and policy adjustments.

Microsoft GCC High licenses (5. pcs.)

Indicative price.

Additional cost (Purchased by the customer)

Enclave Pc's - 5. pcs

Certification cost /C3PAO.

N/A

Contact us for specific project and maintenance pricing.

*Pricing on US C3PAO certification is yet to be determined.

**Fair-use support includes, user creations/deletions, forgotten passwords and basic enclave system use.

Q & A

Who owns the enclave?

Your company does. We handle setup, configuration and maintenance and ascertains that the system is in continuous compliance with CMMC 2.0 and NIST 800-171 and an upcoming certification.

Is support included with the enclave?

Yes, we render full support on the enclave within business hours, based on a fair-use** principal.

Is CMMC certification included in the price?

No. This can only be performed by an accredited C3PAO (CMMC 3rd Party Assessment Organization). We assist in establishing contact with one.

Where is data stored?

All data is stored within the Microsoft GCC High datacenter within CONUS (Continental USA). We do not store any customer data locally.

Are support personnel working with EPP™ security cleared?

Yes, all employees working with the enclave is security cleared by the Danish authorities. Within the US, Microsoft clears all US personnel.

Can mobile devices be used?

It is possible to add mobile devices such as tablets and smart phones. EPP™ currently supports Apple devices (iPhone and iPad)

Is printing possible from the enclave?

Yes, connecting a regular printer to an EPP™ devices is possible.

How long does a maintenance contract run?

We have a minimum initial maintenance contract of 12 months, after this the maintenance contract can be terminated with 4 months notice.

What is the estimated implementation time?

We have an estimated implementation of 3 months from start to end.

Does an EPP™ comply with NIST 800-171

Yes, an EPP™ is in full compliance with NIST 800-171

**Fair-use support includes user creations/deletions, forgotten passwords and basic use of enclave connected devices.