How Entrust Helps Address CMMC

ENTRUST
SECURING A WORLD IN MOTION

Access Control (AC)

Capability	Practices Addressed by Entrust	Products
C001 Establish system access requirements	AC.1.001, AC.2.005, AC.2.006	Entrust Identity as a Service Entrust Identity Enterprise Entrust PKI Entrust nShield HSMs Entrust DataControl Entrust CloudControl
C002 Control internal system access	AC.1.002, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.3.017, AC.3.018, AC.3.019, AC.3.012, AC.3.020, AC.4.023, AC.4.025	Entrust Identity as a Service Entrust Identity Enterprise Entrust PKI Digital Certificates Entrust nShield HSMs Entrust CloudControl Entrust DataControl
C003 Control remote system access	AC.2.013, AC.3.014, AC.3.021, AC.4.032	Entrust Identity as a Service Entrust Identity Enterprise Entrust PKI Digital Certificates Entrust nShield HSMs
C004 Limit data access to authorized users and processes	AC.1.003, AC.2.016, AC.3.022	Entrust Identity as a Service Entrust Identity Enterprise Entrust PKI Digital Certificates Entrust CloudControl Entrust DataControl

Entrust PKI & Digital Certificates: PKI and certificates provide the ability to restrict access to data by providing secure access credentials for authentication and data management platforms, as well as a means to sign data for integrity and encrypt data for privacy. The PKI allows users to exchange data securely and validate that signatures on data are legitimate. PKI also provides a means to distribute keys/certs used for data protection to devices and users in an automated way.

For controlling internal system access, much of the requirement relates to setting up and enforcing policy around data access. PKI and certificates provide a method to enforce the policies by providing every participant with a credential that can be used to enforce the defined access policies. Typically, the path is via a corporate directory like Active Directory (AD) – access to resources is set and group policies will push users into access groups leveraging certificates for authentication. Credentials placed on access cards, in AD, or on other user devices via MDM are governing access controls. Remote system access can be VPN, secure auth, MFA – these are all backed by crypto keys and certificates.

How Entrust Helps Address CMMC

When it comes to limiting data access to authorized users and processes, device certificates and MDM are applicable based on encryption certificates being deployed to devices. User certificates are provided by the PKI via an MDM allowing content to be decrypted/encrypted by users so they can view it on their devices seamlessly. PKI enables the credentials to be distributed to many endpoints. Full disk encryption solutions like Microsoft and BitLocker leverage certificates and keys deployed to endpoints to carry out disk encryption/decryption. Containers can be similar through the use of code signing and secrets managers like HashiCorp Vault.

Entrust Identity: Entrust Identity applies an identity to ensure the right level of access to the right applications through a set of centrally managed policies with the ability to inject real-time contextual information with adaptive risk-based authentication. Administrators can easily set access and entitlement rules based on attributes such as user group membership.

Entrust Identity provides visibility into who has access to which data and specific applications. Defined users can be assigned to established groups and provided access to applications and services by group. Privileged users can be placed into a group and control around accounts and resources can be provided within this group.

Entrust Identity allows IT admins to manage unsuccessful log-on attempts in accordance with the organization's policy. Entrust Identity automatically monitors session activity and allows IT administrators to centrally manage organizational policy for session timeout and re-authentication processes. Session termination rules can be established as well as unlock processes using time out or help desk intervention.

Entrust Identity's advanced multi-factor authentication (MFA) offers a non-disruptive, non-intrusive, easily integrated solution that works with your virtual private network (VPN), Remote Desktop Protocol (RDP), and Secure Shell (SSH).

Entrust Identity maintains logs for monitoring and the ability for initial access with MFA for remote sessions. Entrust Identity can verify and control connections to external systems but may not limit those connections.

Entrust nShield HSMs: The Entrust nShield Security World provides a specialized key management framework that spans the entire nShield family of general purpose HSMs. This architecture provides a unified administrator and user experience and guaranteed interoperability whether the customer deploys one or hundreds of devices.

Administration and operation functions are separated using different and unique sets of smart cards, created using a k-of-n quorum that utilizes the Shamir secret sharing method. The creation of the k-of-n quorum of smart cards provides the inherent ability to enforce separation of duties and multi-party control.

Our flexible Security World architecture provides three different methods of key protection, isolation, and access control: Operator card set (OCS) for physical token with passphrase-protected keys, softcard protection for passphrase-protected keys, and module protection. There are no logical limits to how many of these key protection mechanisms can be used, and your application keys are cryptographically separated using these key protection mechanisms, which can effectively be used to achieve cryptographic boundaries for multi-tenancy.

With strict process isolation controls, once a key is loaded into the HSM, only the application/session that loaded the key can access it in the HSM memory.

How Entrust Helps Address CMMC

Entrust CloudControl: Entrust CloudControl enforces least privilege access model and separation of duties across the environment to mitigate the risk of intentional/unintentional misuse. Specific functionality includes automated secondary approver, temporary access requests via root password vaulting, and two-factor authentication. Privileged access administration for groups/individuals leverages Active Directory.

Entrust DataControl: Entrust DataControl provides platform independent data-at-rest encryption and KMIP compliant key management (FIPS certified). The encryption policy travels with the workload to always ensure data is protected. This agnostic solution allows customers to administer/track/monitor workloads wherever they reside (on-prem or in the cloud) via a single, easy-to-use interface. DataControl limits user and group access to encrypted workloads allowing for secure multi-tenant configurations.

Asset Management (AM)

Capability	Practices Addressed by Entrust	Products
C005 Identify and document assets	—	—
C006 Manage asset inventory	AM.4.226	Entrust Certificate Hub Entrust nShield HSMs Entrust CloudControl

Entrust Certificate Hub: Certificate Hub's Discovery Scanner can identify and discover components that have certificates in your organization. Certificate Hub can also distribute certificates to endpoints. Additionally, CEG modules and Admin Services provide mechanisms to distribute certificates to assets via protocols.

Entrust nShield HSMs: It is possible to find the HSM firmware and appliance software version of an Entrust nShield HSM from an authorized client.

Entrust CloudControl: Entrust CloudControl may be used to inventory VMware vCenter and see all objects that have been created.

How Entrust Helps Address CMMC

Audit & Accountability (AU)

Capability	Practices Addressed by Entrust	Products
C007 Define audit requirements	AU.2.041, AU.3.045, AU.3.046	Entrust Identity as a Service Entrust Identity Enterprise Entrust PKI Entrust nShield HSMs Entrust CloudControl Entrust DataControl
C008 Perform auditing	AU.2.042, AU.2.043, AU.3.048	Entrust Identity as a Service Entrust Identity Enterprise Entrust PKI Entrust nShield HSMs Entrust CloudControl Entrust DataControl
C009 Identify and protect audit information	AU.3.049, AU.3.050	Entrust PKI Entrust nShield HSMs Entrust CloudControl Entrust DataControl
C010 Review and manage audit logs	AU.2.044, AU.3.052, AU.4.054	Entrust PKI Entrust CloudControl Entrust DataControl

Entrust PKI: All PKI functions inside of Entrust Certificate Authority carry auditable logs. More importantly, certificates provide non-repudiation and a means by which user access can be traced when the certificates are used for functions within applications. A secure certificate-based identity provides a strong credential that can be traced back through vetting and enrollment processes established on the Certification Practice Statement (CPS). Audit logs are created and signed to ensure tampering is not possible. Logs are integrated with syslog and security information and event management (SIEM) tools for integration into corporate systems.

Entrust Identity: Entrust Identity records system events related to your organization in order to provide an audit trail that can be used to understand platform activity and to diagnose problems. Entrust Identity requires unique user IDs assigned to individuals.

How Entrust Helps Address CMMC

Entrust nShield HSMs: Entrust nShield HSM connections can be traced using logs both on the HSM (i.e. which application server made the connection) and on the application server (which user/process initiated the connection). The nShield Connect HSM (network-attached) appliance can also synchronize its internal clock with a trusted NTP server. Additionally, specific key operations can be audited if enabled during generation of the Security World and/or in the access control lists (ACLs) of a given key. These logs can also be sent to a syslog server for further analysis, alarm triggers, and long-term retention.

If audit logging is enabled when generating a new Security World, critical audit log messages are digitally signed by the HSM. This capability provides:

- Logs generated and signed on the nShield HSM
- Tamper detection
- Deletion detection
- Administrative operations are logged
- Key lifetime events are logged
- Per key usage events are optionally logged
- Optional key usage logging
- Public key verification of audit logs
- Compatibility with syslog and SIEM tools

Entrust CloudControl & DataControl: Both feature audit-quality logging and alerting. This advanced logging captures complete audit trails tied to privileged users' actions and events taking place in the environment (including both allows and denies). Inalterable logs can be automatically sent, in real-time, to syslog/SIEM tools for broader security monitoring and further analysis.

Configuration Management (CM)

Capability	Practices Addressed by Entrust	Products
C013 Establish configuration baselines	CM.2.061, CM.2.062	Entrust CloudControl
C014 Perform configuration and change management	CM.2.064, CM.2.065, CM.2.066, CM.3.067, CM.3.068, CM.5.074	Entrust PKI Digital Certificates Entrust nShield HSMs Entrust CloudControl

Entrust PKI & Digital Certificates: Code signing certificates and toolkits and gateway can be used to ensure that updates to systems and configurations can be validated by those systems and made tamper-proof.

Entrust nShield HSMs: Cryptographic signatures and signed hashes ensure the integrity and authenticity of software and protect against unauthorized changes to code. nShield HSMs provide FIPS 140-2 Level 3 certified protection of the signing keys that underpin cryptographic signatures and hashes.

How Entrust Helps Address CMMC

Entrust CloudControl: This may be used to inventory VMware vCenter and see all objects that have been created. The solution can also continuously assess and remediate against most common configuration standards while reporting any deviations from the established baseline. This rapid ROI solution is template-driven and spans hundreds of controls from standard regulatory requirements such as NIST 800-53 and 800-171, DISA STIG, CJIS, etc., including OEM hardening guides (VMware ESXi). Assessments and/or remediation can be scheduled or continuous with enterprise-wide status/metrics available via executive dashboard.

Identification & Authentication (IA)

Capability	Practices Addressed by Entrust	Products
C015 Grant access to authenticated entities	IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.2.082, IA.3.083, IA.3.084, IA.3.085, IA.3.086	Identity as a Service Identity Enterprise Entrust PKI Entrust nShield HSMs Entrust CloudControl Entrust DataControl

Entrust PKI: Entrust's PKI services can sync certificates for users and devices into Active Directory, LDAP, and MDM Services. IoT, IT devices, and users can be issued unique cryptographically verifiable credentials to allow mutual certificate-based authentication and provide seamless access to organizational websites and applications through digested authentication.

Digital certificate authentication employs replay-resistant mechanisms; for example, TLS 1.2 tunnels natively have reply technology. Digital certificates provide an encrypted tunnel that obscures feedback of authenticated information. Digital certificates issued from PKI can provide logical access in support of users' processes to authenticate and access.

Entrust Identity: Entrust Identity acts as an identity provider so organizations can onboard users and devices, configure their registration process, set password complexity rules, use MFA, and deploy single sign-on (SSO). Entrust Identity can solve IAM control challenges by centralizing identity integration with Active Directory and LDAP and apply workflow orchestration to verify and manage users accessing corporate resources.

Entrust Identity includes a session logout after a defined period in accordance with the organization's policy.

Entrust Identity's centralized management console allows IT professionals to adjust password lengths and complexities and update schedules in keeping with current NIST guidelines.

Password policies can be established to ensure a user does not match previous passwords in accordance with the organization's policy guidance. Using common password detection can help you meet compliance guidelines by detecting and preventing users from defining weak or breached passwords. Policy guidance is set by the organization, but Entrust Identity's flexible policy framework allows for step-up authentication to verify users before they access accounts and services.

Entrust Identity's adaptive risk-based authentication affords intelligent, contextual access based on the defined user groups. Entrust Identity's adaptive risk-based authentication supports a variety of factors such as one-time password, mobile push, physical tokens, and biometric factors.

How Entrust Helps Address CMMC

Entrust Identity enables replay-resistant mechanisms using a variety of credentials including mobile smart credentials, physical smart cards, FIDO2, and push notifications.

Entrust nShield HSMs: Administration and operation functions are separated using different and unique sets of smart cards, created using a k-of-n quorum that utilizes the Shamir secret sharing method. The creation of the k-of-n quorum of smart cards provides the inherent ability to enforce separation of duties and multi-party control.

Administration functions are authorized using the administrator card set (ACS), and operation functions (such as loading application keys) are authorized using an operator card set (OCS) or softcard. ACS and OCS are physical smart card sets, whereas softcards are HSM-protected logical tokens that require a passphrase to unlock.

ACS (management) and OCS (operation) cards can be used either locally or remotely for two-factor authentication by defining a passphrase per card.

Diffie-Hellman-based transport layer security, combined with mutual authentication, help protect client-to-HSM communications against man-in-the-middle and replay attacks.

The nShield HSM also provides the capability for properly enrolled Windows-based servers to use the HSM for strong authentication to Microsoft Active Directory domain environments, effectively using the HSM as a hardware-based authentication token. This is similar to how a user would use a PIV or PIV-I smartcard to authenticate to a Microsoft Windows domain. This capability enables a variety of use cases such as those found in robotic process automation applications.

Entrust CloudControl & DataControl: Provide comprehensive identity and access controls, including MFA, to further enforce user security.

Maintenance (MA)

Capability	Practices Addressed by Entrust	Products
C021 Manage maintenance	MA.2.112, MA.2.113, MA.2.114	Entrust PKI Entrust nShield HSMs Entrust CloudControl Entrust DataControl

Entrust PKI: Logical authentication from remote networks and establish maintenance sessions can be done via digital certificates, for example using personal identity verification (PIV) and derived PIV.

Entrust nShield HSMs: Certain maintenance activities, such as firmware upgrades, can be performed with intervention from authorized administrators (ACS holders). Only firmware that is signed by Entrust nShield HSM manufacturing systems can be installed.

To prevent malicious actors from circumventing security controls, if newer firmware is installed that fixes critical bugs or other issues, the firmware contains a version serial number that prevents it from being downgraded to a previous version. However, if the newer firmware only introduces new features, the firmware can usually be downgraded back to the previous version. This provides a safe but flexible method of validating newer firmware prior to production upgrades.

Entrust CloudControl & DataControl: Each provides a means to upgrade the system. The upgrades are provided by Entrust and include application and OS patches/upgrades.

How Entrust Helps Address CMMC

Media Protection (MP)

Capability	Practices Addressed by Entrust	Products
C022 Identify and mark media	—	—
C023 Protect and control media	MP.2.119, MP.2.120	Entrust PKI
C024 Sanitize media	MP.1.118	Entrust DataControl
C025 Protect media during transport	MP.3.124, MP.3.125	Entrust PKI Entrust nShield HSMs Entrust DataControl

Entrust PKI: PKI and digital certificates can be used to encrypt data placed on media. PKIs, when leveraged with policy controls, can also be used to securely encrypt/decrypt data. We achieve this through PKI integration with AD group policies as well as enforcement with our Certificate Agent on Windows and Mac. The agent ensures that content can be securely encrypted/decrypted or signed/verified through the use of certificates and keys. Certificates can be used during "transport" to secure TLS as well as traditional file encryption and disk encryption for physical devices transferring information.

Entrust nShield HSMs: Entrust Shield HSMs provide FIPS 140-2 Level 3 certified generation and protection of cryptographic keys, which can be used to protect sensitive encryption and/or digital signature keys for critical applications. These applications can include PKI, secure web servers, secrets management applications, and more, which protect CUI data with HSM-backed cryptographic keys.

Additionally, all nShield HSMs can be sanitized by way of factory reset functionality built-in to the firmware and client tools. This sanitization is compliant with our NIST FIPS 140-2 Level 2 and 3 certifications on all nShield HSM models.

Entrust DataControl: Entrust DataControl can be used to encrypt a virtual machine. These virtual machines would remain encrypted regardless of where they reside (on-prem, cloud, etc.); backups are encrypted as well. Access to the keys/data is only available via the Entrust DataControl appliance.

How Entrust Helps Address CMMC

Physical Protection (PE)

Capability	Practices Addressed by Entrust	Products
C028 Limit physical access	PE.1.131, PE.1.132, PE.1.134	Instant ID Issuance VMaaS Entrust PKI Entrust nShield HSMs

Entrust PKI: Certificates are used in access cards and tokens to authenticate users into physical spaces.

Entrust nShield HSMs: Entrust nShield HSMs are tamper-resistant devices, certified to FIPS 140-2 Level 3 and Common Criteria EAL4+ (EN 419 221-5). They are also shipped to customer facilities in tamper-evident packaging.

Instant ID Issuance: ID badge issuance to plastic cards or mobile devices, which can be inspected by a security guard to confirm that a person should have access to a building or a space. ID badge issuance to smart chip-enabled plastic cards that can be integrated with physical access door reader systems.

Instant ID on premises can issue printed plastic cards with or without smart chip capabilities. Instant ID as a Service can issue plastic cards without a smart chip (smart chip coming in the fall) or to mobile using the Apple/Google wallet systems on iOS and Android.

Entrust VMaaS: The VMaaS solution allows an organization using the solution to check in visitors and issue them physical badges. When these badges are displayed by a visitor, the organization can mandate that the visitor be escorted and can control the areas that the visitor goes to.

How Entrust Helps Address CMMC

Recovery (RE)

Capability	Practices Addressed by Entrust	Products
C029 Manage backups	RE.2.138	Entrust PKI Entrust nShield HSMs Entrust DataControl
C030 Manage information security continuity	RE.5.140	Entrust PKI Entrust nShield HSMs

Entrust PKI: Encryption of backups and access controls can be provided through the use of certificates. Entrust Managed PKI secure facilities and data centers would meet organization-defined information security continuity, redundancy, and availability requirements.

Entrust nShield HSMs: Entrust nShield HSMs are extremely simple to cluster by simply deploying additional HSMs and then enrolling client applications with them. All key management, synchronization, failover, and load balancing is monitored and handled by the nShield Security World client software.

Additionally, the nShield Connect HSM (network-attached appliance) is very easy to back up and restore. Configuration data is automatically backed up to its accompanying support system ("RFS server"), which can subsequently be used to quickly restore the HSM or an appropriate replacement.

nShield HSM application key material is automatically encrypted during the generation process inside the HSM and can only be decrypted inside the confines of the HSM's FIPS boundary. The encrypted key material can afterwards be backed up by any standard backup tool, requiring no additional hardware. Administrator and operator smartcards (see the Identification and Authentication (IA) section) are backed up by design using the k-of-n approach to creating smart card quorums (e.g. make 'n' sufficiently large enough to have extra backup smart cards).

Entrust DataControl: Provides capability to take backups of the appliance via a GUI interface, NFS share, or an API. Any of these methods may be used to back up the appliance.

How Entrust Helps Address CMMC

Systems & Communications Protection

Capability	Practices Addressed by Entrust	Products
C038 Define security requirements for systems and communications	SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.1.83, SC.3.184, SC.3.185, SC.3.186, SC.3.187, SC.3.188, SC.3.189, SC.3.190, SC.3.191, SC.4.197, SC.4.228, SC.5.198, SC.5.230	Entrust PKI Digital Certificates (S/MIME, TLS/SSL) CryptoCoE Entrust nShield HSMs
C039 Control communications at system boundaries	SC.1.175, SC.1.176, SC.3.192, SC.4.199, SC.4.202, SC.4.229, SC.5.208	Entrust PKI Digital Certificates Entrust nShield HSMs Entrust CloudControl Entrust DataControl

Entrust PKI: Secure onboarding of devices to networks can be managed with MDM/EMM solutions that leverage PKI for security. When it comes to implementing IDPS/WAFs, they usually require the use of HTTPS/web proxies, which are typically tied to enterprise PKI to support re-encryption of user browsing. Ties to https proxies, IDPs, and WAFs often need special interactions with PKIs (SubCAs) and certs distributed to end-users/devices. To ensure the separation of networks and data, that could be considered role-based access control (RBAC) and certificates could be used as a form of authentication and data protection through encryption. Providing step-up authentication or high assurance validation on a task is often done with strong credentials such as certificates or tokens, which are both available in the PKI portfolio and can be managed in concert with the PKI (via Entrust Certificate Agent, formerly Entelligence).

Implementing cryptographic mechanisms to prevent unauthorized disclosure of controlled unclassified information (CUI) is an encryption use case, and it could be one for signing as well. Certificates and keys are relevant here, specifically things like PIV play a role in the FedSSP to achieve this. Key Recovery Server once encryption is implemented is important for the ability to recover old keys that protect data. For remote connections and transmission of data, HTTPS proxying is an example of what can be done 'securely' via encrypted pipes that need to chain back to PKIs. For terminating a connection, if the connect is secured using authentication, that allows for revocation of credentials. This would then break the connection. To do this, certificates and validation of certificates is needed. To control and monitor the use of mobile code, digital certificates are often used for this type of DRM/license enforcement. SIP devices and VOIP use certificates for encryption and for RADIUS-based authentication for users onto the network, so typically you need a PKI connection.

Digital Certificates (S/MIME & TLS/SSL): Both protect the authenticity of communications sessions through identity and encryption. DNSSEC and DMARC can be used in conjunction with S/MIME and other certificates for secure communication. We also have partners like Agari and Valimail who are in this space and can use our certificates.

Cryptographic Center of Excellence: Our PKI Health Check and consulting will assess and then provide guidance to ensure the customer's security environment is architected and operated to best practices and meets compliance requirements, promoting effective information security within organizational systems. It can also help organizations gain visibility into their cryptographic inventory to ensure they have proper algorithms and management in place.

How Entrust Helps Address CMMC

Entrust nShield HSMs: As a best practice, any application or system that can make use of cryptographic material should have its keys protected by an HSM if possible. Entrust nShield HSMs provide FIPS 140-2 Level 2 and 3 certified generation and protection of cryptographic keys, which can be used to protect sensitive encryption and/or digital signature keys for critical applications. These applications can include PKI, secure web servers, secrets management applications, and more, which protect CUI data with HSM-backed cryptographic keys.

The nShield Inter-Module Path (abbreviated 'IMPATH') protocol provides a secure channel connection, mutually authenticated, between enrolled client and HSM, and between nShield HSM. Negotiation of the session is based on a Diffie-Hellman style key exchange. IMPATH provides the following properties:

- Messages sent through the IMPATH can't be read except by the modules at either end
- A message not sent by one of the modules won't be accepted as valid by either
- A replay of a previous valid message won't be accepted as valid by either module

IMPATH can be used to communicate cryptographic shares, key data, and other sensitive information. ACLs associated with data items such as keys or shares can specify limits on the kinds of IMPATH over which the data may be transmitted. Secrets used to secure an IMPATH connection are never revealed.

Entrust CloudControl & DataControl: Entrust CloudControl limits privileged access to specific systems; Entrust DataControl is leveraged to secure virtual machines via data-at-rest encryption. Entrust BoundaryControl is a combination of these two products that sets policies so that virtualized applications can only run on proven, trusted hosts that are physically located within the defined parameters. This can significantly reduce the potential for theft or misuse of sensitive data, or violation of regulatory compliance laws.

System & Information Integrity (SI)

Capability	Practices Addressed by Entrust	Products
C040 Identify and manage information system flaws	—	—
C041 Identify malicious content	SI.1.211, SI.1.212, SI.5.222	Digital Certificates (Code Signing)
C042 Perform network and system monitoring	SI.2.217, SI.5.223	Entrust Certificate Hub Entrust CloudControl Entrust DataControl
C043 Implement advanced email protections	SI.3.219	Digital Certificates (S/MIME & VMCs)

Entrust Digital Certificates (Code Signing, S/MIME & VMC): Entrust Code Signing Certificates authenticate a software publisher's identity and verify code integrity with a tamper-proof seal for software downloads.

S/MIME can help prevent email forgery by signing emails to prove authorship of the email, whereas VMCs can do this from a corporate level, providing organizational ownership with a registered mark in the email (for Gmail users).

How Entrust Helps Address CMMC

Entrust Certificate Hub: Discovery Scanner with Certificate Hub can find certificates with weak algorithms or key lengths. Certificate Hub now integrates with Tenable and InfoSec Global scanners to capture certificate data from those system scanners.

Entrust CloudControl & DataControl: Both feature audit-quality logging and alerting. This advanced logging captures complete audit trails tied to privileged users' actions and events taking place in the environment (including both allows and denies). Inalterable logs can be automatically sent, in real-time, to syslog/SIEM tools for broader security monitoring and further analysis.