PKWARE | SMARTCRYPT

CONTINUOUS DIAGNOSTICS AND MITIGATION WITH THE SMARTCRYPT PLATFORM

PKWARE's Smartcrypt is a data-centric audit and protection platform that automates data discovery, classification, and protection in a single workflow, managed from a single dashboard.

With Smartcrypt, government agencies can eliminate security gaps and maintain control over sensitive data, meeting the requirements of the Continuous Diagnostics and Mitigation (CDM) program and other data security objectives.

THE DATA CENTRIC APPROACH

Unlike outdated approaches that focus solely on perimeter protection, Smartcrypt enables the deployment of a business strategy directly related to protecting the data. Smartcrypt's integrated discovery, classification, and protection capabilities allow government departments and agencies to mitigate risk, drive data security behavior, enforce standards and apply best practices through policy.

Smartcrypt offers the ability to increase cybersecurity defenses by implementing controlled and persistent data-centric encryption that provides chain of custody visibility, consistent data protection practices, key management and key rotation, and emergency access to encrypted objects by security administrators and auditors, as needed.

SMARTCRYPT AND CDM

Smartcrypt's data-centric approach is aligned with the goals and strategies of the CDM program, and provides the capabilities government departments and agencies require in order to meet their data protection objectives.

Secure Data Exchange: Within each data enclave, Smartcrypt can apply persistent encryption to files before they are exchanged between enclaves or with outside partners and customers. This enables organizational control over sensitive information, regardless of how many times files are copied, backed up, or forwarded. This approach also allows users to exchange sensitive information through cloud services or protocols like email and FTP that provide little security on their own.

Auditing, Monitoring, and Reporting: Security administrators need the ability to detect inappropriate encryption or decryption activity, and to demonstrate departmental and agency compliance with data protection mandates. Smartcrypt's Data Security Intelligence capabilities provide visibility into what sensitive information is being protected and where it is transmitted or accessed.

Cross-Platform Protection: From mainframe to mobile, Smartcrypt provides data protection on every enterprise operating system. With integrations for common tools and applications, Smartcrypt can be used to protect information stored on end-user devices, network shares, and even file sharing services. Smartcrypt is also easily integrated into back-office and batch processing workflows.

Enhanced DLP: Government departments and agencies need flexible data security solutions that work with data loss prevention technology and processes within and between enclaves. Smartcrypt can be integrated with existing DLP strategies to facilitate access to encrypted documents and to protect unencrypted information before it leaves an enclave.

CDM PHASE 3:

MANAGE "WHAT IS HAPPENING ON THE NETWORK AND HOW IS THE NETWORK PROTECTED?"

Phase 3 of the CDM program includes Boundary Encryption (BOUND-E) capabilities that are necessary in order to protect data within data enclaves and as it travels beyond enclave borders. Smartcrypt's policy-based approach to data protection can help agencies and departments ensure that data remains safe from unauthorized use on and off the network.

CDM ELEMENT	SMARTCRYPT SOLUTION
MANAGED BOUNDARY ENCLAVES	A Smartcrypt implementation would provide persistent data protection for data at rest within an enclave and for data in motion between agencies, departments, or other enclaves. Smartcrypt provides consistent data protection and policy enforcement, as well as a consistent approach to data protection including key exchange and key usage across all areas of the organization.
REQUIREMENT V - 3.5.1 CRYPTOGRAPHIC ALGORITHM ELEMENT	Smartcrypt applies persistent AES-256 encryption, the strongest form of data protection, to sensitive data. Smartcrypt's cryptographic algorithms meet the requirements of FIPS 140-2 and all other applicable data security standards.
REQUIREMENT V - 3.5.3 KEY MANAGEMENT ELEMENT	PKWARE's innovative Smartkey technology takes the confusion and frustration out of encryption key management. A Smartkey is generated and utilized by the Smartcrypt application for a specific file, folder, or other protected asset. With Smartkeys, user access to protected files and folders can be added or revoked at any time—even if the files have been shared, copied, renamed, transferred, or emailed—ensuring full lifecycle protection. Smartcrypt also allows users to encrypt data for external parties such as vendors or partners. A cloud-based key server stores and distributes keys based on the organization's security policies, even for external users who are granted access after the encryption takes place. With Smartkeys, administrators can tailor encryption policies to meet your unique requirements, while streamlining the encryption and decryption process for end users.
REQUIREMENT V - 3.5.5 CERTIFICATE AUTHORITY ELEMENT	Smartcrypt also supports other common encryption key types, including X.509 certificates, OpenPGP certificates, and passphrases.
REQUIREMENT V - 3.5.6 APPLICATION PROTOCOLS ELEMENT	Smartcrypt integrates with Microsoft Outlook and other Office applications to keep data safe from internal and external cyber threats.

CDM PHASE 4:

MANAGE "HOW DATA IS PROTECTED ON THE NETWORK?"

Smartcrypt provides more capabilities on more operating systems than any other data protection platform, allowing each organization to create a tailored solution that meets its unique operational needs and compliance requirements.

CDM ELEMENT	SMARTCRYPT SOLUTION
C.4.3.4.1 MICRO-SEGMENTATION	Smartcrypt is transparent to and supports micro-segmentation. Keys and policies follow the data so that if placed in a micro-segmentation environment they would persist.
C.4.3.4.2 DIGITAL RIGHTS MANAGEMENT	Smartcrypt detects the presence of sensitive data immediately on capture or creation and applies persistent protection that prevents unauthorized use inside or outside the organization. When unauthorized access is attempted, the attempt is blocked and administrators are alerted of inappropriate activity. Data is protected with AES 256 keys, with available full-entropy random number generation technology.
C.4.3.4.3 ADVANCED DATA PROTECTIONS: (DATA LIFECYCLE MANAGEMENT) DLM is the automated movement of critical data to online and offline storage and protections applied to maintain confidentiality, integrity and availability of that information in the various locations for the specified purpose. Relevant capabilities include: • Encryption and key management • Data masking • Backup and recovery of data	Smartcrypt provides strong data-level encryption and streamlined key management, with support for every enterprise operating system. Organizations can choose from multiple protection and remediation options for sensitive data, including encryption, data masking, quarantine, and file deletion. Files protected by Smartcrypt are compressed before encryption, reducing storage costs for data backups.
C.4.3.4.3 ADVANCED DATA PROTECTIONS: (INFORMATION LIFECYCLE MANAGEMENT) ILM is the strategy for understanding the value of information and protecting important information assets. Relevant capabilities include: • Discovery and classification of data • Data labeling • Data masking and subsetting • Monitoring of data access • Normalized repository of auditing data	Smartcrypt is the only data protection solution that combines discovery, classification, and data protection into a single integrated workflow. Smartcrypt scans servers and endpoints for files containing sensitive data, applies classification labels, and protects data with strong encryption, data masking, or other methods, according to the organization's policies. All encryption and decryption events are logged, and data usage and access/denials are normalized to facilitate reporting via SIEM down to the document, user, and path.

SMARTCRYPT

COMPLETE ENTERPRISE DATA PROTECTION

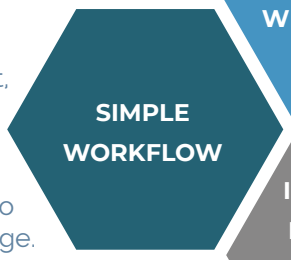
PKWARE's Smartcrypt eliminates security gaps by finding, classifying, and protecting sensitive data across the entire enterprise. Smartcrypt provides capabilities no other product can match, allowing each organization to create a tailored data protection solution.

Smartcrypt agents are installed anywhere sensitive data might be created or stored: laptops and desktops, mobile devices, file servers, even midrange and mainframe systems. Smartcrypt agents apply your organization's policies each time data is created or moved, ensuring that you always have control over your sensitive information.

THE SMARTCRYPT DIFFERENCE

The Smartcrypt Enterprise Manager provides a single point of control for data protection activity across the entire organization.

Smartcrypt works on every enterprise operating system and provides persistent protection that remains with data even when it's copied or shared outside the organization.



With Smartcrypt, data protection is automated for end users and easy for administrators to manage.

Smartcrypt supports a variety of deployment options, enabling organizations to implement their data protection solution without time-consuming changes to infrastructure or workflows.

No other solution has the capability to find, classify, and protect data in a single automated workflow.

Organizations can take a policy-based approach to data protection and choose from actions including persistent encryption, quarantine, masking, and deletion.

PKWARE®

www.PKWARE.com

PKWARE provides a data-centric audit and protection platform that automates policy-driven discovery, classification, and encryption wherever sensitive data is used, shared, or stored.

CORPORATE HEADQUARTERS
201 E. Pittsburgh Ave.
Suite 400
Milwaukee, WI 53204

+ 1 866 583 1795

EMEA HEADQUARTERS
79 College Road
Suite 221
Harrow HA1 1BD

+ 44 (0) 203 367 2249