Case study

Engage BlackVault HSM and Randtronics DPM protect enterprise wide sensitive data – on premise and in the cloud

The requirement: protection of encryption keys and sensitive data as a priority for enterprise customers

Information is “power”. Today, organizations are collecting more information about their employees, suppliers, competitors and customers. That means today’s criminals do not break into banks: They engage highly skilled professional hackers to access vulnerable information - that is, unprotected encryption keys and unencrypted data. Organizations must prioritize their security based on encryption of data and protection of keys as their highest priority because it provides a true ‘last line of defense’.

The challenge: trust and scalability required for protecting cryptographic key material

Enterprise-wide data privacy management systems enable businesses to protect structured and unstructured data on premises and in the cloud. Data encryption, masking, tokenization and anonymization are the cryptographic mechanisms used for data privacy protection. However, underlying cryptographic keys have to be securely stored and managed. This prevents theft or loss of the key material and the ability for a stranger to decrypt previously “securely” encrypted data. Otherwise, the security of the enterprise-wide ecosystem and end points might be at risk.

The solution: hardware-enabled protection for sensitive data

Randtronics Data Privacy Manager (DPM) provides comprehensive data protection for sensitive information to facilitate data privacy and compliance on premises, in the cloud, or in hybrid cloud infrastructures. DPM offers an easy and effective way to provide need-to-know access to internal and external users for ensuring data protection. Plug and play connectors and or APIs for files, folders, databases, web, app and the Engage BlackVault Hardware Security Module (HSM) provide easy deployment, use and maintenance. Features such as policy-based access control, auditing, encryption, masking, tokenization and anonymization facilitate compliance with company-internal as well as government and industry security policies.

Integrated with the FIPS140-2 Level 3 BlackVault, Randtronics data privacy protection solution provides security and compliance.

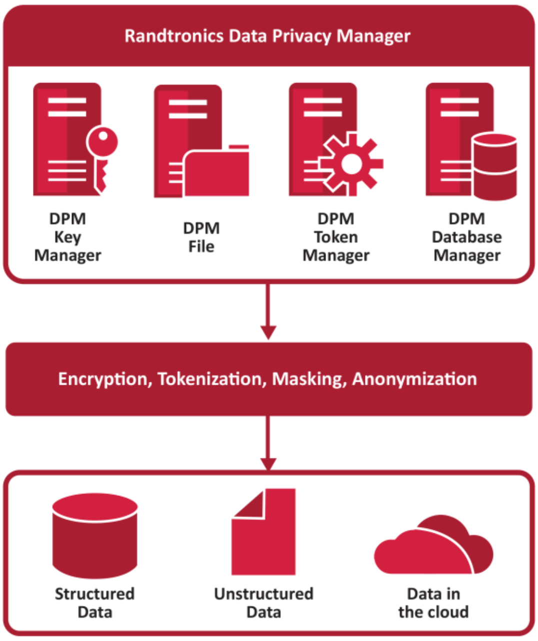
The technical solution

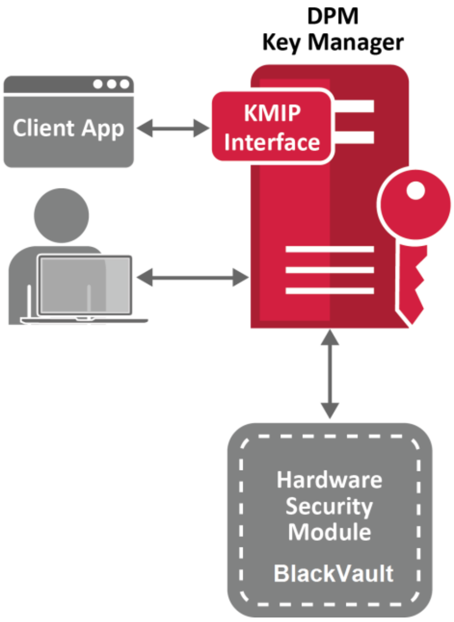
As inherent Root of Trust for their data privacy management program, Randtronics relies on BlackVault HSM to generate, store and manage cryptographic keys safely.

The DPM solution receives cryptographic keys from the DPM Key Manager, which in turn offers options of auto-generating keys in software or within the BlackVault HSM for highest security assurance. The HSM is the source of Master Key, System Keys, Key Encryption Keys and Data Encryption Keys.

Randtronics DPM runs on any Windows or Linux platform using standard hardware and software and commonly available databases such as MySQL, MS SQL Server and Oracle.

The architecture: keys managed in an HSM for maximum security





The solution benefits: comprehensive, transparent, centralized & compliant

The BlackVault HSM and Randtronics DPM enables enterprise customers to:

- Securely manage their cryptographic keys by means of role-based access control mechanisms; only authorized users can access master keys for designated purposes
- Guarantee keys are securely and readily accessible whenever needed by DPM and non-DPM clients via policy-based plug and play connectors and API features
- Ensure segregation of duties between DPM clients and the DPM Key Manager, which integrates with the HSM for external hardware key generation
- Provide highest performance to support DPM performance requirements

About Randtronics

Founded in 2002, Randtronics is a worldwide supplier that develops encryption solutions to protect against malicious intent from external hackers, internal employees and outsource contractors. Randtronics DPM protects enterprise data anywhere. The solution offers privacy levels, single sign-on, multi-factor authentication, auditing, high performance, transparent implementation, privileged user protection and high availability. With Randtronics DPM solution you can: protect structured and unstructured data, easily deploy solutions without code changes and reduce scope of compliance using tokenization. For more information, visit www.randtronics.com

About Engage Black

Since 1989, Engage has developed innovative products and solutions that help organizations across the globe deploy and operate cost-effective and reliable communications, and meet their data security needs. We combine an experienced and responsive engineering team, highly scalable manufacturing resources, and a “whatever it takes” customer service philosophy to meet the demanding needs of our customers.

Engage Black, in particular, provides solutions that address the growing sophistication of cyber attackers, both within and outside of organizations, by securing and protecting cryptographic keys, data at rest, and data in motion. For more information, visit www.engageblack.com