Randtronics Data Privacy Manager

randtronics

Randtronics Data Privacy Manager

Securing your business

- A business that only encrypts their data is more secure than businesses with everything else
- Randtronics DPM de-risks businesses beyond the scope of meeting compliance

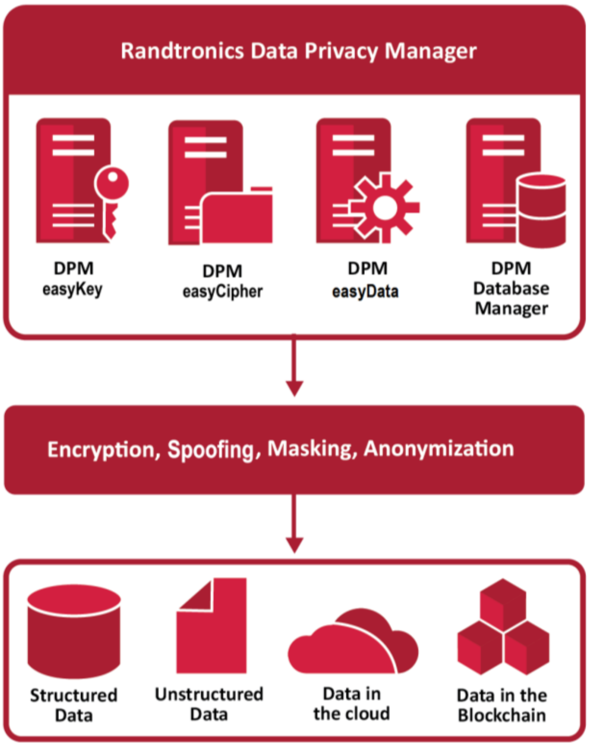
Randtronics is proud to have developed the Data Privacy Manager product, also known as DPM. DPM is a software based solution and enables users to easily protect data on any application, database or file. With DPM, users are able to encrypt their data without any software code changes.

DPM has the following features:

- Software based solution for protecting data
- Runs on Windows or Linux and is virtualization ready
- Can protect both structured and unstructured data
- Offers encryption, tokenization, masking and anonymization
- Flexible choice of encryption keys, software generated or integration with an HSM

DPM includes:

- **DPM easyCipher** – enables encryption and access control of files, folders, applications, databases stored on laptops, desktops and servers.
- **DPM easyData** – tokenizes, encrypts and anonymizes data using a web service interface. Allows creation of masking rules for unauthorized users.
- **DPM easyKey** – provides a central place for key management. Allows generation of keys internally or via a cluster of HSMs.
- **DPM Database Manager** – allows the masking of data stored in columns within databases. Integration with DPM easyData extends its features to tokenization, encryption and anonymization.



DPM easyKey

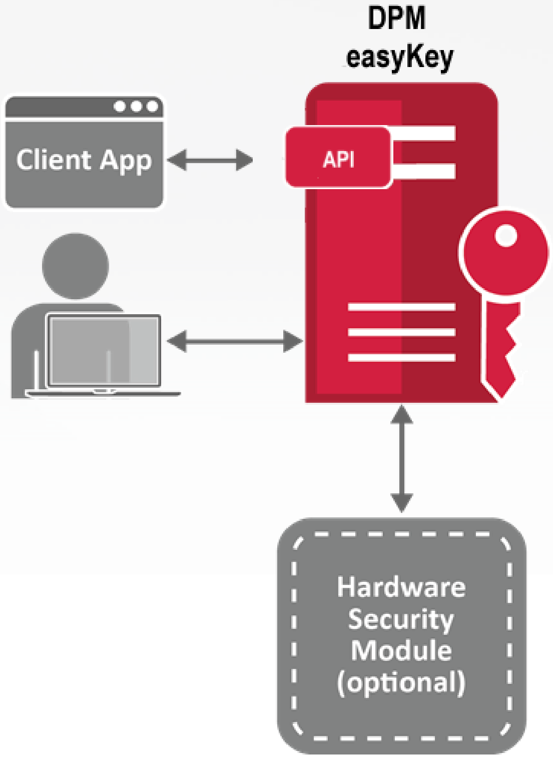
DPM easyKey provides a central place to manage encryption keys.

The product has the following features:

- Provides full key and certificate life cycle management (create, rotate, revoke, destroy)
- Support KMIP protocol for integration with client applications
- Integrates with DPM easyCipher and DPM easyData to provide key management
- Client integration connectors without code changes for database, file and folder
- Client integration APIs using RESTful, web services, Java and C/C++
- Create key generation and access control policies across client applications and multi-vendor HSMs
- Optionally integrates with a cluster of multi-vendor HSM for hardware key generation or cloud key services such as Microsoft Azure key vault

The software has a browser interface for administrators to maintain the encryption keys and a KMIP interface for client applications to use the encryption keys.

Encryption keys are either generated internally on the DPM easyKey, or Azure key vault or an HSM if optionally installed.



Supported databases:

- Microsoft SQL Server 2005, 2008, 2012 and 2014
- Oracle MySQL

Supported environments:

- Windows 7, 8, 10, Server 2008, Server 2012, server 2016
- Linux kernel 2.6 and up; CentOS kernel 2.6 and up
- SUSE kernel 2.6.32 and 4.4.21 and up

Supported client interfaces:

- File encryption key connectors for Windows and Linux based file servers, Laptops and Desktops
- Database encryption key connectors for Oracle, MySQL, MS SQL server, DB2, Cassandra, Informix, Teradata
- APIs using RESTful, SOAP, web services, Java, C/C++
- Tokenization connector for applications and database
- Multi-vendor HSMs (Utimaco, Gemalto, Thales, Fortanix and Engage) and Microsoft Azure key vault
- KMIP supported enterprise key manager

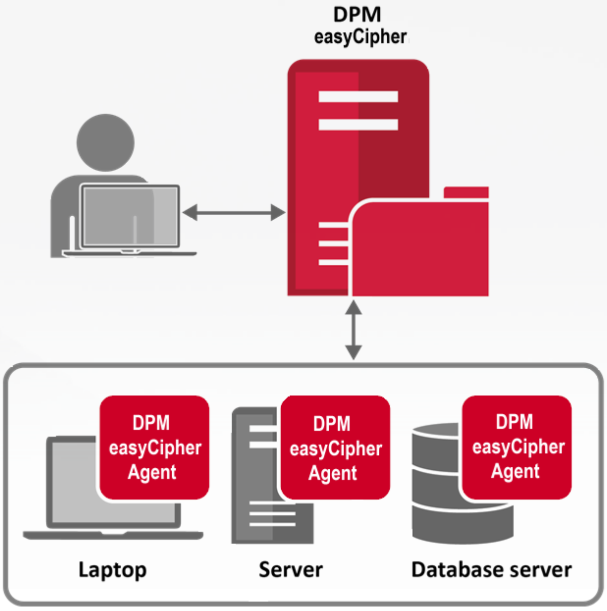
DPM easyCipher

DPM easyCipher allows users to secure files, folders, applications and databases in a Windows or Linux environment. The software is designed so that end users do not need to change their behavior in order to secure their files. The product has the following features:

- Runs in a Windows or Linux environment
- Provides transparent encryption of files on laptops and servers
- Allows encryption of database data files
- Security protection policies are managed from a central point by administrators
- Protection from unauthorized users and even system administrators/root users
- Application white and black list control to sensitive files
- Optionally integrates with DPM easyKey and or an HSM and or Azure key vault

The software has two components:

- **DPM easyCipher Manager** – provides a central place for administrator to configure security policies and to distribute those policies to end user agents.
- **DPM easyCipher Agent** – runs on each laptop, desktop or server in order to encrypt and enforce access control policy. Is designed to run in the background – users do not need to change anything in order to start using the software.



Supported backend databases:

- Microsoft SQL Server 2005, 2008, 2012 and 2014
- MySQL 5.6 and up

Supported environments:

- Windows 7, 8, 10, Server 2008 and Server 2012, Microsoft Hyper V
- Linux, CentOS kernel 2.6 and up, SUSE kernel 2.6.32 and 4.4.21 and up
- Any physical or virtualized environment

Supported clients:

- Any Windows and Linux based file servers, database servers, web and application servers
- Any Windows and Linux laptops and desktops
- Secure container with encryption and access control for master keys, configuration files, passwords
- Any application whitelist and blacklist enforcement module

DPM easyData

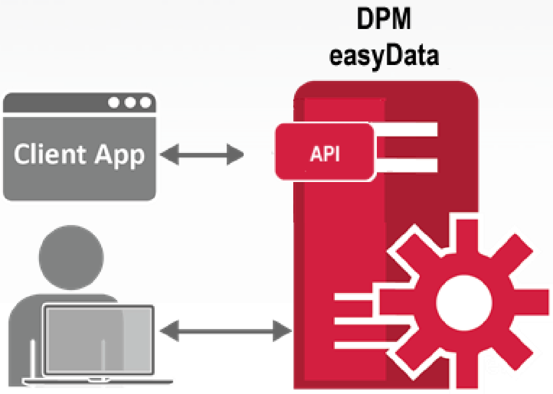
DPM easyData is a high performance data spoofing engine and front end console. Data spoofing or tokenization is the process of replacing whole or parts of sensitive data with a non-sensitive equivalent. DPM easyData allows web and app server applications and databases to tokenize and anonymize data and apply masking policies for unauthorized users when retrieving sensitive data.

The product has the following features:

- Pseudoanonymization or tokenization of data by replacing sensitive data with dummy “token” values
- Preserving the format of input data
- Policy based single use and multi-use tokens
- Multilanguage tokenization and anonymization
- High performance
- Web service API for client applications to perform tokenization/detokenization, encryption and anonymization
- Full auditing of all console operations and engine operations
- Performance monitoring and integration with syslog and email for performance alerts

DPM easyData is made up of two components:

- **Management console** - a browser based management console that allows users to configure policies, access and maintain tokens and administer the system.
- **Engine** – high performance engine to provide data spoofing such as tokenization and anonymization services and accessed using a web services API.



Supported backend databases:

- Oracle 10g, 11g and 12c
- MySQL 5 and up

Supported environments:

- Windows 7, 8, 10, Server 2008 and up
- Linux kernel 2.6 and up, CentOS kernel 2.6 and up, SUSE kernel 2.6.32 and 4.4.21 and up
- Physical and virtualized environments

Supported clients:

- Any legacy and current applications
- RESTful, SOAP and Web services, Java
- Oracle, MS SQL server and IBM iSeries DB2 Database connectors

DPM Database Manager

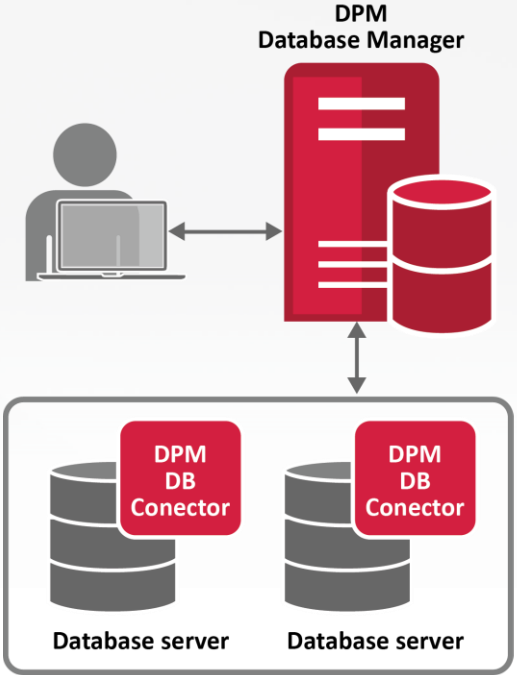
DPM Database Manager allows users to mask data stored in columns in a database. By integrating with DPM easyData it also can provide tokenization, encryption and anonymization of any sensitive data such as PII, HR and Financial. DPM Database Manager provides a way for users to protect data stored in databases, without having to make any application code changes.

The product has the following features:

- Masking, encryption and tokenization of column level data with no application code changes
- Protection from DBAs, software developers, outsourced workers, cloud administrators
- Dynamic tokenization, anonymization and masking rules
- Flexibility in number of columns that can be tokenized, anonymized or masked
- High performance

The software has two components:

- **DPM Database Manager** - a browser based management console that allows users to configure database column protection and perform migrations of column data.
- **DPM Database Connector** - runs on the database to provide the tokenization, anonymization or masking of column level data. Connectors performs real-time dynamic masking and tokenization. A connector is required on each database containing data to be protected.



Supported databases for DB Connector:

- Oracle 10g, 11g and 12c (excluding Express)
- Microsoft SQL Server 2005, 2008, 2012 and 2014
- IBM iSeries DB2

Supported backend databases for DPM Manager:

- Oracle 10g, 11g and 12c
- MySQL 5 and up

Supported environments for DB Connector:

- Windows
- Linux, SUSE
- HP-UX
- AIX, iSeries
- Solaris

Supported environments for DPM Manager:

- Windows 7, 8, 10, Server 2008 and up
- Linux kernel 2.6 and up, SUSE kernel 2.6.32 and 4.4.21, CentOS kernel 2.6 and up
- Physical and virtualized environments

Specifications are subject to change without notice.

Copyright Information

Contact Randtronics to arrange an evaluation download - **enquiry@randtronics.com**

Randtronics

America: Redwood City, CA 94065. Ph: +1 650 632 4272
Australia: North Ryde, NSW 2112. Ph: +614 1822 6234
South Korea: Seoul. Ph: +614 00 451 490

www.randtronics.com

randtronics