Data Encryption - Traditional vs Innovation

Bob Adhar, Gary Lansdown, Gene Paschall and Nadia Vostrikov

Randtronics offers encryption innovation where compliance data can be encrypted without code changes and implements best practice guidelines for enforcing the security principles of policy based access control, separation of duties and auditing. For businesses, the days of encryption intimidation, the burden of encryption implementation and the absence of needed technical skills are over.

Data Encryption

Traditional vs Innovation

Cybersecurity – the problem of complexity

Bob Adhar, Gary Lansdown, Gene Paschall and Nadia Vostrikov

Randtronics offers policy based encryption innovation where compliance data can be encrypted without code changes and implements best practice guidelines for enforcing the security principles of access control, separation of duties and auditing. For businesses, the days of encryption intimidation, the burden of encryption implementation and the absence of needed technical skills are over.

The traditional approach to data security

The traditional approach to protecting encryption keys and data is to use a Hardware Security Module (HSM). There are many different HSM vendors and models and the core features common to all are the ability to provide encryption and decryption of data/keys and store the master key (a key that never leaves the HSM).

Applications can integrate with the HSM using APIs such as Java, PCKS11, KMIP or other protocols including HSM specific interfaces. Applications can send encryption and decryption requests to the HSM with the data they would like to encrypt or decrypt and the key ID to use. This data can also be keys controlled by the application, but encrypted with the HSM master key.

An organization has many types of data such as credit card data (numeric, 16 digits), address (alphanumeric or text), images, etc. Not all data types are suitable for sending to the HSM. Credit card numbers are small and are suitable for transport over LAN and processing inside an HSM. Full databases are gigabytes or more in size and are not suitable.

Databases implementing native encryption known as TDE (Transparent Data Encryption) can integrate with the HSM. In this case the flow is a little different from applications in that the database creates TDE keys which are encrypted with the HSM master key, but are stored within the database. When the database starts, it needs to connect with the HSM to decrypt the TDE keys using the HSM master key.

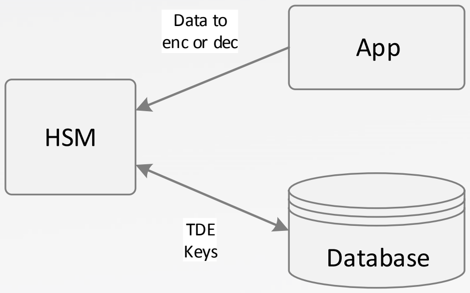


Figure 1 – HSM, applications and database key flows

While this traditional approach has been employed by companies for many years, it does have a number of drawbacks:

- Need to learn HSMs APIs
- Design and perform code changes to existing applications to make use of HSMs
- Migrate existing data when the HSM is initially put into place
- Database TDE is vendor specific

While HSMs are able to protect data, the primary technical issue is applications need to be modified in order to use them. This leads to a large development and test effort and project budget over runs often occur. Once the system passes QA and is deployed, then any change to a compliance standard, privacy enforcement or HSM vendor, requires a change to the existing application.

The big issue

By far the major issue with the traditional approach is the amount of code changes required to use the HSM. On initial analysis it might seem that these changes only require changing code to make use of the HSM to encrypt and decrypt data, but there are many more items to consider:

- Change code and add calls to the HSM to encrypt and decrypt sensitive data, including changes to application logic to identify sensitive data for encryption/decryption
- Need to maintain the relationship between encrypted data and a key ID that was used to encrypt data. If data is backed up, the relationship needs to be backed up as well so the data can be decrypted
- Implement logic to handle key rotation and key revocation – applications must be able to re-encrypt data using the new key values. Need to be able to keep track of all versions of the keys so the old backups could be decrypted in the future.
- Implement logic to manage access control of applications, separation of duties for system administrators
- Auditing and logging needs to be implemented for each encryption/decryption operation so that all access events can be tracked
- Securely store HSM access details so that only applications can access them

The innovative approach to data security

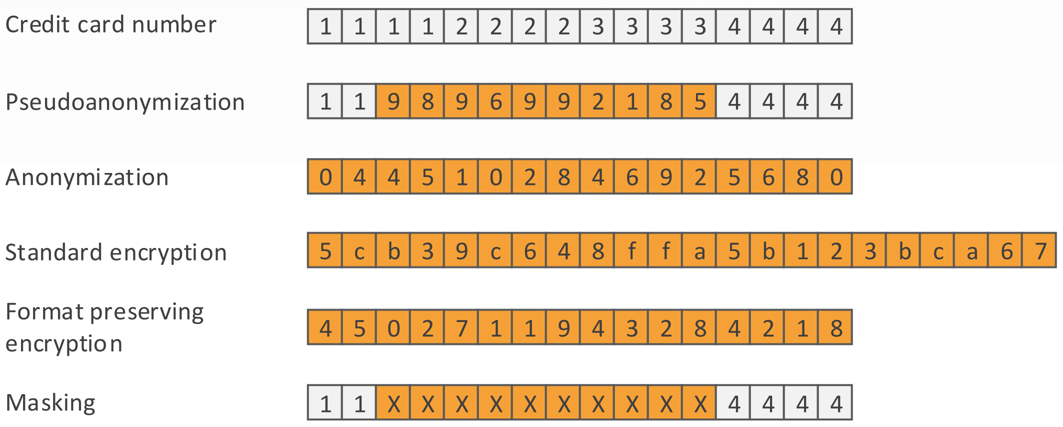
Many of the drawbacks of the traditional approach can be fixed by using the Randtronics out of the box DPM that features: no code changes, rich privacy options, multi-vendor HSM support and the appropriate security principles of policy based approach to data protection. Where optimization requires code changes the DPM APIs are middleware code which simplifies application integration to a few lines of coding as the middleware handles the best practice guidelines of security experts.

With Randtronics protection options there is no need to make code or application changes to encrypt your data in applications, files or databases. It saves time on learning 3rd party APIs and performing and testing code changes. It does not change the way of how a user or application accesses the data and it keeps the data secure. This results in a tremendous saving in development and testing costs. Key Management, storing master key in HSM, access control and auditing are taken care of using the Randtronics DPM product.

Policy based privacy – an approved security practice recommended by security experts

Policy based privacy allows users to set a policy that defines how data should be protected. It simplifies the approach to encrypting and protecting data. The policy is defined by the security and compliance team and governs the protection of the data. Policy settings include:

- How the data is protected (encryption, format preserving, masking, tokenization, pseudoanonymization, anonymization)
- What data is protected (files, folders, whole databases, columns and application data)
- Who is authorized to see the data in the clear (user and application)
- Time of day or other access day restrictions on when data can be retrieved
- What sort of keys are used for encryption



Credit card number	1	1	1	1	2	2	2	2	3	3	3	3	4	4	4	4						
Pseudoanonymization	1	1	9	8	9	6	9	9	2	1	8	5	4	4	4	4						
Anonymization	0	4	4	5	1	0	2	8	4	6	9	2	5	6	8	0						
Standard encryption	5	c	b	3	9	c	6	4	8	f	f	a	5	b	1	2	3	b	c	a	6	7
Format preserving encryption	4	5	0	2	7	1	1	9	4	3	2	8	4	2	1	8						
Masking	1	1	X	X	X	X	X	X	X	X	X	X	4	4	4	4						

Figure 2 – Rich data privacy flexibility

The policy based approach is designed to be flexible to meet the needs of customers. Once a policy has been defined it can then be enforced by Randtronics DPM Manager and its enforcement agents and connectors. DPM protects the data at file, application and database levels using the configured policy.

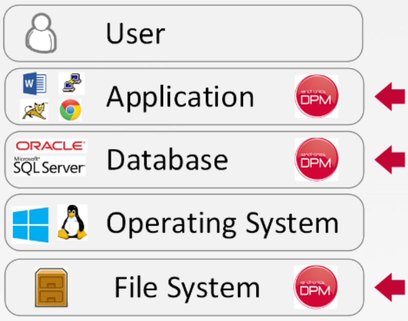


Figure 4 – Policy based integration layers

The policy based approach removes the need for applications to have to implement much of the security logic.

Multi-Vendor Flexible Key Generation

Randtronics protection options use encryption for data protection which require encryption keys. Encryption keys can be generated in software which can help keep costs low or the policy based approach can integrate with HSMs for higher key assurance. The flexibility in key generation allows a wide range of companies – from the smallest start-ups looking for basic security to large banks and defense organizations looking for maximum security.

Key generation is not locked to a specific HSM vendor as multiple vendors are supported. Policies can easily be configured for different HSM vendors or even quantum true random number generation can be incorporated for higher key entropy.

Separation of duties

The security policy can be defined and is under the control of the security team. Compare this to a traditional approach where the security team can advise application teams on how to integrate with the HSM, but leave it up to the application development teams to implement. Once implementation is done and the source code is compiled, it becomes a “black box” without visibility and control what has been done and how.

The policy based approach offers a true separation of duties. It allows visibility and control of what to protect and how. All policies can be viewed and easily audited by security team. It is easier for data owners to ensure compliance with policies.

Transparent data protection

There are many legacy applications used by enterprises and may be difficult or even impossible to perform code changes to integrate with an HSM.

File level and column level data protection policies can be achieved transparently to applications and users. No application changes or reconfigurations are required for existing applications. A workflow for applications, database, and end-users does not change after encryption is applied.

Flexible data protection options

Policy based approach to data protection allows a flexible choice of options for the protection of data. Policies can be configured to use any of the following:

- Encryption – data is encrypted with industry standard AES encryption
- Masking – replacing sensitive parts of data with a masking character to hide parts of data or the full data
- Tokenization (or pseudoanonymization) – replacing sensitive data with tokens or "spoofed" data that looks like the real data. Different from encryption in that the token is randomly generated
- Anonymization – replacing data with random tokens that cannot be detokenized, while maintaining the meaning of the data
- Format preserving encryption – similar to encryption, the cipher text matches the length and datatype of the original data

Policy based is vendor neutral

The policy based approach is vendor neutral. The same polices can be used to protect databases, whether they are Oracle, IBM DB2 or Microsoft SQL Server databases. Also any application data whether it is MS Office files, video files, images, or financial files can be protected.

Other benefits include:

- Initial data migration is handled once the policy has been put in place
- Applications do not need to implement key management or access control
- Full auditing of how data is accessed and which policy was enforced
- Backup of keys can be scheduled the same way as data backup using existing backup tools.

Policy based data protection makes it easier for companies to achieve compliance and data protection.

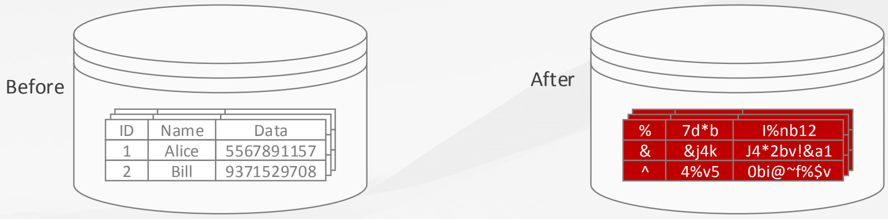
Example

A financial application manages various sensitive information about the customers, including bank account numbers, names, addresses, tax file numbers, etc. It writes data to a back-end MS SQL Server database as well as log files. A company security policy requires data to be protected using encryption.

The old approach:
To integrate with an HSM, encryption keys are created in the HSM and then encryption API calls are performed to encrypt data before it is written to the database and into the log file. When the data needs to be presented back to the screen, a decryption API call is performed to decrypt data.

The new approach:

a) The entire database is encrypted at a file level. Only a database service can access and decrypt/encrypt data. All data in the database are protected. Log files are also encrypted at a file level and only the financial application can access the files. Data is protected from OS users including privileged administrators. No code changes are required to be performed within the application or database.

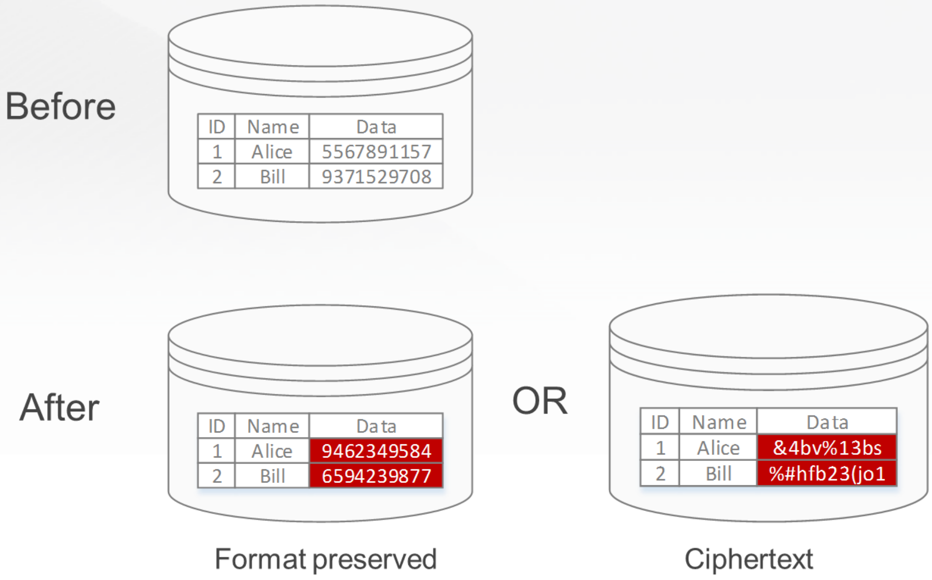


ID	Name	Data
1	Alice	5567891157
2	Bill	9371529708

%	7d*b	I%nb12
&	&j4k	J4*2bv!&a1
^	4%v5	0bi@~f%$v

Figure 5 – Before and after full database encryption

b) Alternatively, the database can be protected at a column level. Only columns that are required to be protected are tokenized or encrypted. Data is protected from OS or database users including privileged administrators and DBAs. Log files are encrypted at a file level and only the financial application can access the files.



ID	Name	Data
1	Alice	5567891157
2	Bill	9371529708

ID	Name	Data
1	Alice	9462349584
2	Bill	6594239877

ID	Name	Data
1	Alice	&4bv%13bs
2	Bill	%#hfb23(jo1

Figure 6 – Before and after column level database encryption

Conclusion

Randtronics DPM helps businesses protect compliance data easily with best practice security guidelines and without code changes. In today’s disruptive business environment where legacy applications are being replaced by newer applications businesses can substantially benefit from Randtronics DPM innovation. We add privacy without the pain and expenses.

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

Randtronics Pty Limited
ABN: 99 101 584 329

Suite 1, Level 1, 64 Talavera Rd
NorthRyde, NSW 2113, Australia

Phone:	(612) 8873 1999
Fax:	(612) 9870 8560

Randtronics LLC
303 Twin Dolphin Drive, Suite 600
Redwood City, CA 94062, United States

Phone: +1 650 632 4272
Fax: +1 650 591 9901

www.randtronics.com