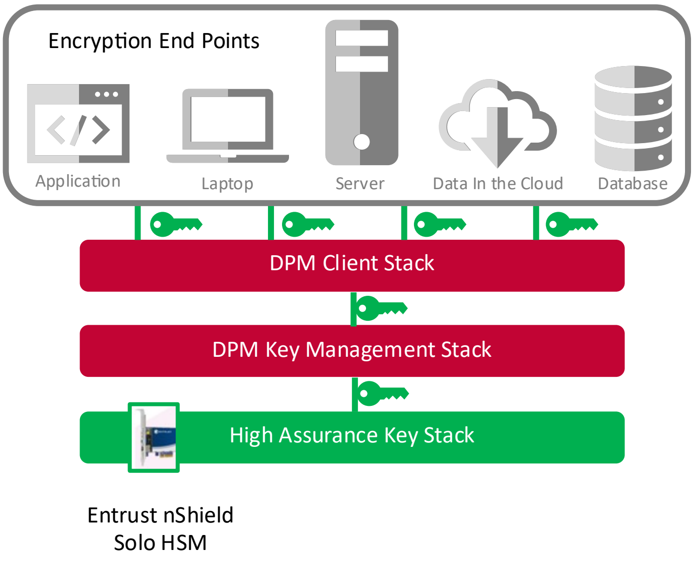
DATA PRIVACY AND COMPLIANCE ON PREMISES AND IN THE CLOUD WITH RANDTRONICS DPM AND ENTRUST HARDWARE SECURITY MODULES

Solution Benefits

- Enable comprehensive enterprise data protection using encryption, masking, tokenization and anonymization engines
- Deliver transparent deployment APIs for files, folders, databases, web, and application protection
- Provide centralized policy based control of cryptographic services
- Simplify security auditing and reduce compliance costs
- Store master keys in a FIPS and Common Criteria validated module

Randtronics and Entrust Deliver Scalable and Secure Enterprise Data Privacy Management



Entrust nShield HSMs safeguard and manages the cryptographic keys used by Randtronics DPM, providing a root of trust for the enterprise data privacy management program.

The Problem: Enterprise customers increasingly need to protect the privacy of both structured and unstructured sensitive data.

As enterprise customers maintain and use more sensitive data, the recurring cost of compliance with government and industry data security regulations can be significant. Added to the technical complexities associated with data protection schemes, cryptographic key management and support, the problem can burden businesses as they grow.

The Challenge: Scaling enterprise data protection on premises and in the cloud requires protecting sensitive cryptographic keys in a trusted manner.

Sensitive data can resides in many systems throughout the enterprise both inside and outside their physical perimeter. Businesses address the risk of compromise data through coordinated enterprise-wide data privacy management schemes. Using cryptographic mechanisms such as data encryption, masking, tokenization, as well as anonymization, risks can be properly mitigated. However, safeguarding and managing the underpinning keys that secure these processes is critically important to ensure the security of the entire ecosystem.

RANDTRONICS AND ENTRUST DELIVER SCALABLE AND SECURE ENTERPRISE DATA PRIVACY MANAGEMENT

The Solution: Randtronics and Entrust together deliver Enhanced security assurance, compliance scope reduction and transparent deployment

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. It is an inexpensive way to provide need -to-know access to internal and external users for ensuring data protection. Plug and play APIs for file, folder, databases, web, app and Entrust HSM provide easy deployment and on-going use. Policy based encryption, masking, tokenization and anonymization features facilitate defense in depth privacy options as enterprises progressively reduce security risk to expectations.

Combined with Entrust nShield hardware security modules (HSMs), the solution delivers trusted key protection and facilitates compliance and auditing. Integration of the DPM with nShield provides encryption and key protection to FIPS 140-2 Level 3 and Common Criteria EAL 4+, which enables organizations to deliver a high assurance environment in compliance with industry best practices.

Why use Entrust nShield HSMs with Randtronics DPM?

Encryption keys handled outside the cryptographic boundary of a certified HSM are significantly more vulnerable to attack, which can lead to compromise of critical keys. HSMs are the only proven and auditable way to secure valuable cryptographic material. Entrust nShield HSMs integrate with Randtronics DPM to provide comprehensive logical and physical protection of master keys. The combination delivers an auditable method for enforcing security policies of all cryptographic services.

Entrust nShield HSMs enables Randtronics customers to:

- Secure keys within carefully designed cryptographic boundaries that uses robust access control mechanisms, so master keys are only used for their authorized purpose
- Ensure key availability by using sophisticated management, storage, and redundancy features to guarantee they are always accessible when needed by the DPM
- Deliver superior performance to support demanding DPM applications

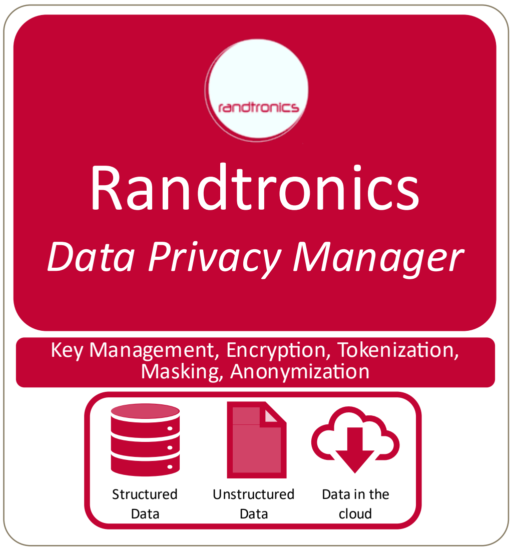
Entrust

Entrust nShield HSMs provide a hardened, tamper-resistant environment for performing secure cryptographic processing, key protection, and key management. With Entrust HSMs you can:

- Provide a tightly controlled tamper resistant environment for safekeeping and managing encryption keys
- Enforce key use policies, separating security functions from administrative tasks
- Interface with applications using industry-standard APIs

(PKCS#11, OpenSSL, JCE, CAPI, and CNG)

Randtronics



Randtronics DPM protects enterprise data anywhere. The solution offers privacy levels, SSO, MFA, auditing, high performance, transparent implementation, privileged user protection and high availability. With Randtronics DPM solution you can:

- Protect structured and unstructured data
- Easily deploy solution without code changes
- Reduce scope of compliance using tokenization

For more detailed technical specifications, please visit https://www.randtronics.com or https://entrust.com