Cryptography-as-a-Service

Solution Brief

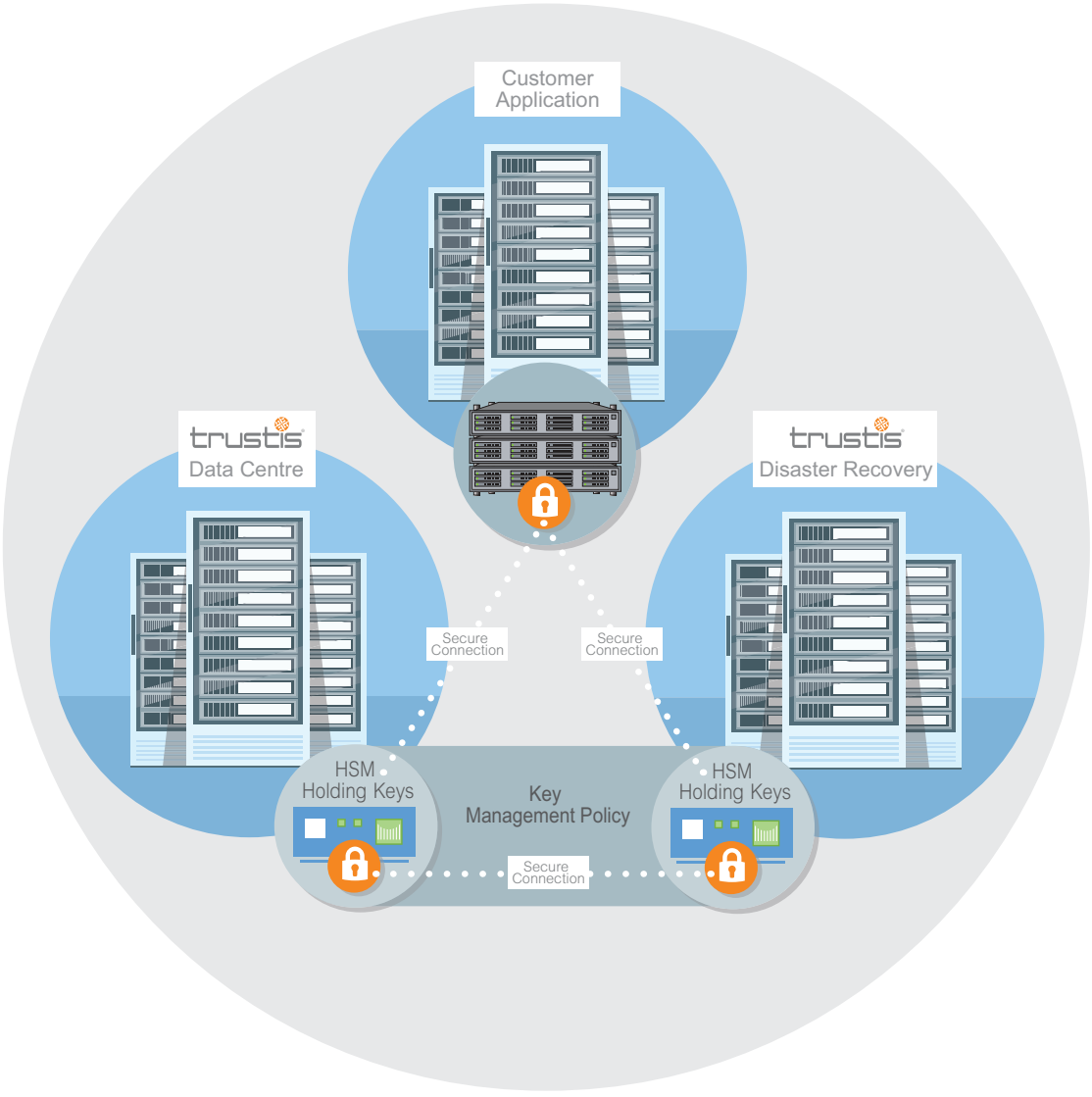
+44 (0)1635 231361
+44 (0)1635 231366
info@trustis.com
www.trustis.com

Cryptography-as-a-Service

Giving you complete control while protecting your data and systems

Key Points

- Cryptography-as-a-Service (CaaS) is an efficient, cost-effective means to protect your data and systems in the Cloud.
- It enables you to use certified, high-performance Hardware Security Modules (HSMs) without employing crypto experts or buying expensive hardware and having unused capacity.
- Hosted and expertly managed in the UK while you retain complete control over your encryption keys.



Keeping control of your cryptographic keys – the challenge

Cryptographic keys are a critical component for securing IT infrastructure, communications and applications. While mathematically they offer very strong protection, there is an assumption that these keys are kept secret and access to the keys is kept absolutely secure. This assumption is very difficult to guarantee, as without the proper controls, e.g. policy and audit, systems can be relatively easily compromised.

This problem is exacerbated when the IT infrastructure and applications are provided by Cloud Hosting Providers. In these cases, the customer is rarely in control of their own cryptographic keys and cannot guarantee that they won't be compromised.

Specialised management

Management of cryptographic systems and processes is a specialised function. To be effective it requires in-depth knowledge of processes, procedures and audit requirements which are specific to cryptography. Furthermore, even with the specialist skills to comply with security policies, the hosting provider may still control the cryptographic key material, giving them unrestricted access to sensitive data and/or cryptographic signing processes which is potentially a very high security risk.

The Trustis solution: Cryptography-as-a-Service

Trustis specialises in providing cryptographic services to Government and commercial organisations alike. Our CRYPTOGRAPHY-AS-A-SERVICE (CaaS) solution uses off-the-shelf HSMs certified to FIPS 140-2 Level 3 and EAL4+ validated which are configured in a cluster to provide resilient cryptographic processing power as needed.

CRYPTOGRAPHY-AS-A-SERVICE supports standard cryptographic calls to HSMs from application/storage programmes or infrastructure components that utilise a cryptographic interface. The key management procedures and policy can be tailored to fit your particular requirements and can be explicitly accredited by external parties (such as CESG) as required.

CaaS ensures that the cloud or 3rd party service provider does not have access to the key material even when key material needs to be revoked or updated for key rollover. Key management processes are performed by SC Cleared staff within the Trustis facility under ISO27001 certified defence in depth security controls.

Choose from two cloud service models:

- On Premise: Tamper-proof HSMs are placed at the customer (or their preferred Service Provider site) and remotely managed over secure links using HSM hardware from the Trustis Secure Facilities under strict policy controls. Backup of key material can either be on crypto hardware located at the customer or at Trustis.
- At Trustis: Tamper-proof HSMs are placed in the Trustis Secure Service Centres and connected to the customer applications via a secure connection. The HSMs are then managed under strict policy controls. Backup of key material can either be on crypto hardware located at the customer or at Trustis.

High availability

Trustis uses the highest-performing and fastest HSMs which are set up in a high-availability (active-active) architecture with a cluster in the Production site and an exact mirror in the DR facility. The HSMs load balance and failover between local units and sites for redundancy and thus we deliver very high availability aligned with the best cloud hosting providers.

Backup and restore

Encrypted key material is backed up onto a separate HSM Backup Device providing defence in depth and a keys-in-hardware strategy which delivers the strongest levels of key protection for application keys.

Benefits of Cryptography-as-a-Service

- Master control of customer cryptographic keys remains with the customer, where it should always be.
- Keys are always stored in FIPS 140-2 Level 3 certified and EAL4+ validated hardware.
- CaaS allows an organisation to consume cryptographic processing from multiple datacentre locations, either their own, from Trustis or their cloud hosting provider.
- It avoids unnecessary cryptographic hardware duplication and enables multiple customer systems to use as much or as little cryptographic processing as required.
- Over-capacity is avoided and yet, because it is cloud based, the ability to burst without loss of performance is accommodated.
- It enables the move from one hosting provider to another because cryptographic systems management is with a trusted and independent 3rd party.
- Bespoke KMS Policy is provided to suit each customer system(s).
- With a common, robust and accredited approach to cryptographic systems management, quality, reliability, security and performance is maximised.

Key Features and Technical Specifications

- FIPS 140-2 (Level 3) validated & EAL4+ certified Hardware Security Modules.
- Supports all the major algorithms and cryptographic APIs.
- HSMs located at Trustis or in your preferred cloud hoster.
- High-availability (active-active) architecture for resilience.
- High performance via load balancing and platform processing speed.
- Secure partitioning of key material for multiple requirements.
- Two-person control of sensitive cryptographic operations.
- Connectivity includes PSN (Public Services Network).
- Shared or dedicated secure backup of key material.

Contact:
Robert Hann • Commercial contact
robert.hann@trustis.com
+44 (0)7818 552411

Building 273, Greenham Business Park,
Thatcham, Berkshire RG19 6HN