Managed Encryption Service
An Overview
Chris Greengrass
Encryption and Cryptography

The use of encryption/decryption is as old as the art of communication. In wartime, a cipher could be employed to keep the enemy from obtaining the contents of a transmission. Simple ciphers include the substitution of letters for numbers, and the rotation of letters in the alphabet; this latter technique goes back to Roman times and is sometimes known as the Caesar Cipher.

In today's systems, much more complex ciphers work according to sophisticated computer algorithms that rearrange the information so as to make it unreadable to anyone that intercepts the data or signals.

In order to easily recover the contents of encrypted data or signals, the correct decryption key is required.

There are two basic types of encryption methods, symmetric and asymmetric. A symmetric method relies on a single private key used to encrypt and decrypt data thus requiring all parties to have possession of that private key to be able to send and receive messages. Essentially the problem is one of how to securely distribute and store the private key, without it being compromised by non-authorised people or systems.

An asymmetric method uses two keys, a private key that is used to decrypt messages, and a public key, which is used to encrypt messages. This method has many benefits for an encryption system; firstly, the decryption (private) key does not have to be shared. Secondly, the encryption key can be, and indeed is, shared with as many parties as possible so that they can secure data or signals sent to the owner of the private key.

Important, the possession and ownership of a private key is the intrinsic point of trust of in both systems.

Typically, asymmetric methods are used to establish secure channels of communication over open systems such as the Internet whilst symmetric methods are employed to encrypt data on more restricted channels.

These two basic methods of encryption, or combinations thereof, are used throughout modern computer and communications systems to secure data within those systems. They are used extensively in financial and government systems for everything from on-line banking to secure mobile phone communications.

What are the benefits of cryptography?

As well as the many obvious benefits of keeping data secret, either when it is at rest on a computer disc or when traversing untrusted networks such as the Internet cryptography can be used to authenticate all communicating entities, be they machine or human, so long as all either possess or have access to a private key which is intrinsically trust.

The data we encrypt may be sensitive for a number of reasons from medical data, financial records or indeed financial transactions. It may also contain information relating to national security.

What are the problems with cryptography?

Despite the numerous advantages of cryptography, as a technology it has yet to deliver its real benefits to businesses. Here are some of the reasons why:

- Cryptography can quickly become very complex;
- The encryption algorithms have to be implemented without error to be effective;
- Algorithms ‘age’ and do not offer the same degree of protection over their entire lifetime because the longer they are in use the more vulnerable they become to attack and compromise;
High assurance cryptography has to be done in trusted environments using specialised hardware such as the Trusted Platform Module (TPM) found in laptops and other client-side devices, and/or the Hardware Security Module (HSM) in data centres, smartcards, phones and credit cards;

The protection of any cryptographic system is only as strong as the protection used to secure the encryption/decryption keys;

Deploying enterprise-level cryptography can quickly become very costly;

Specialised hardware and software are often required;

Specialist full time staff will be needed to manage an enterprise cryptographic service;

Regulatory compliance costs can be very high e.g. within the financial services sector;

Year on year support costs are high.

Cryptographic devices often represent a single point of failure in an infrastructure;

Maintenance often requires significant downtime for business critical systems;

It is difficult (if not impossible) for cryptographic systems to match modern Data Centre operational capacity levels;

Cryptography is very demanding of computer resources and current devices do not scale well to increasing demand;

Cryptography vendor lock in, i.e. it can be very difficult to change, or even upgrade, a cryptographic device or system once a particular hardware vendor or certain interfaces have been selected;

Cryptography is not “plug and play” friendly: application programming interfaces are diverse and often proprietary in nature, and they don’t adapt or extend;

It can be difficult to detect when illegitimate encryption is being used to bypass system security;

Cryptography does not currently fit well into the cloud computing model.

Current industry practise means that cryptographic systems are deployed on a project by project basis, with each project picking up the capital expenditure to deploy a cryptographic system. Applications have to manage encryption keys as well as the complexity of existing API’s (e.g. PKCS #11) which frequently results in poor and ineffective implementation.

Furthermore, project by project deployment in large data centres often means that where the full capacity of a cryptographic device is not used, there will be excess capacity that cannot be shared with other projects within the same enterprise.

In summary there are substantial obstacles for the adoption of wide scale cryptography in an enterprise, despite its obvious benefits. Clearly in order for the benefits to be widely realised, all of these hurdles must be overcome.

What is a Managed Encryption Service?

In order to address the issues with cryptography and to meet the demands and realise the benefits of cloud computing, a new approach to cryptography deployment and application integration is needed.

Instead of being centred on devices and projects, effective enterprise encryption must be based on a service oriented approach which provides cryptography as a managed utility or commodity service, much in the same way as broadband access is provided.

This approach allows enterprises to gain the full advantages of cryptography:

- No capital expenditure, bought as a service from day one;
- Purchase a defined service with guaranteed capacity and level of assurance;

---

Centralised management of cryptographic devices via a Cryptographic Network Operations Centre (CNOC);
Scalable cryptographic resources, not limited by the capacity of any single device;
High Availability configuration, no single point of failure in service;
Keys managed securely within the service and NOT by applications;
Encryption algorithms selected by the service and under the control of a user-defined policy; can be updated transparently to the application;
Vendor neutral interfaces, no vendor lock in to any supplier(s);
A variety of industry standard API’s;
A highly abstracted business oriented API allowing rapid integration for bespoke applications (removes the need for application developers to have knowledge of cryptography);
A variety of assurance levels for cryptographic devices;
Extensive and secure audit, compliance and attestation records;
Policy based access to cryptographic resources allowing exquisite control over who and what is encrypted and decrypted;
RIPA compliance services;
Reduced environmental impact (less power consumption, better utilisation).

Amethyst Cryptographic Services Ltd (ACS) Managed Encryption Service (MES) provides a highly scalable enterprise encryption service. Because the core cryptographic devices are stateless in operation, additional devices and capacity bandwidth can be added without disruption to service continuity.

What does a Managed Encryption Service look like?

This diagram shows the components of the service. The ACS trusted boundary is either the ACS data centre or an appliance boundary within a client data centre that will be remotely managed from the ACS data centre depending upon the enterprise requirements.
With managed encryption it is possible to limit the visibility of the encryption keys purely within the ACS trusted boundary. This abstraction allows the application to focus on the business at hand and be completely unaware of the complexities of the algorithms and keys used to protect the data. It also allows the service to rollover the keys without interruption to the application.

In order to make full use of the managed service, access to the encryption resources is granted by means of authentication credentials and by the enforcement of cryptographic policy by the service management layer.

The authentication can be:

- Username/Password authenticated by LDAP or Microsoft Active Directory;
- Remote Authentications Dial in user Service (RADIUS);
- Digital certificate challenge.

The cryptographic policy defines the detailed cryptographic policy to be used, the encryption key algorithm and the access rights assigned to the user or entity requesting access.

As the service is the only point which has access to the application keys and the devices under which the cryptography (encryption and decryption) takes place, it is able to produce extensive audit and compliance information. This log is digitally signed for integrity and non repudiation.

**Managed Encryption Service Integration**

There are a variety of industry standard interfaces to cryptography, some are proprietary products and some are open standards. The ACS MES integrates with a wide range of OS platforms, middleware and applications including: Oracle; SQL Server; MS SharePoint; and bespoke applications. The service can also include a scalable SSL acceleration engine for all data in transit.

One of the major advantages of the ACS MES is that the API is non-proprietary and extensible in nature, so any new commands can be added to the service without impacting the underlying service.

The ACS MES integrates with HSM’s from the following vendors:

- Safenet;
- AEP, (Commercial and CAPS approved);
- Thales;
- nCipher

In addition, the ACS MES can provide a High Performance Software Security Module (SSM) for development and test during system integration phases.

**A Managed Encryption Service for all Sectors**

The ACS MES can be configured and operated to meet the needs of specific sectors. For HMG and MOD, the ACS MES incorporates CAPS Baseline and Enhanced Hardware Security Modules. This service provides protection for protectively marked IL2, IL3 and IL4 data. The CNOC is staffed by staff with DV security clearance.

For other sectors, including financial services, the MES provides unique flexibility and resilience.

**Business Benefits**

The ACS MES delivers a number of business benefits:

- It can be used to provide a technical control against aggregation of data, which can otherwise lead to expensive enhancements to data centre infrastructure or limitations on use of the application system;
It allows the use of shared SAN disc arrays within a data centre, if used in conjunction with Transparent Disk Encryption (TDE), as it provides segregation between application data. Whilst TDE provides a blanket encryption of the data within a database, the ACS MES also provides exquisite control over the data that users can share;

It can be deployed as a gateway between two systems working at different Impact levels so that information traversing such systems is re-keyed with different keys, denying users in the lower domain visibility to protected data in the higher domain. This is enforced centrally by cryptographic policy;

It supports the HMG G-Cloud initiative by providing a centrally managed encryption service to applications running in virtual machine on clustered data centres.

Service Levels

Our service levels mirror those that are typically provided by the leading providers of data centre hosting services. Please contact us for details.

Contact

Amethyst Cryptographic Services Ltd
Worting House
Church Lane
Basingstoke
Hampshire RG2 8PX

Email: sales@amethystcrypto.com
Tel: 01256 345612