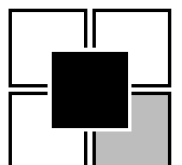
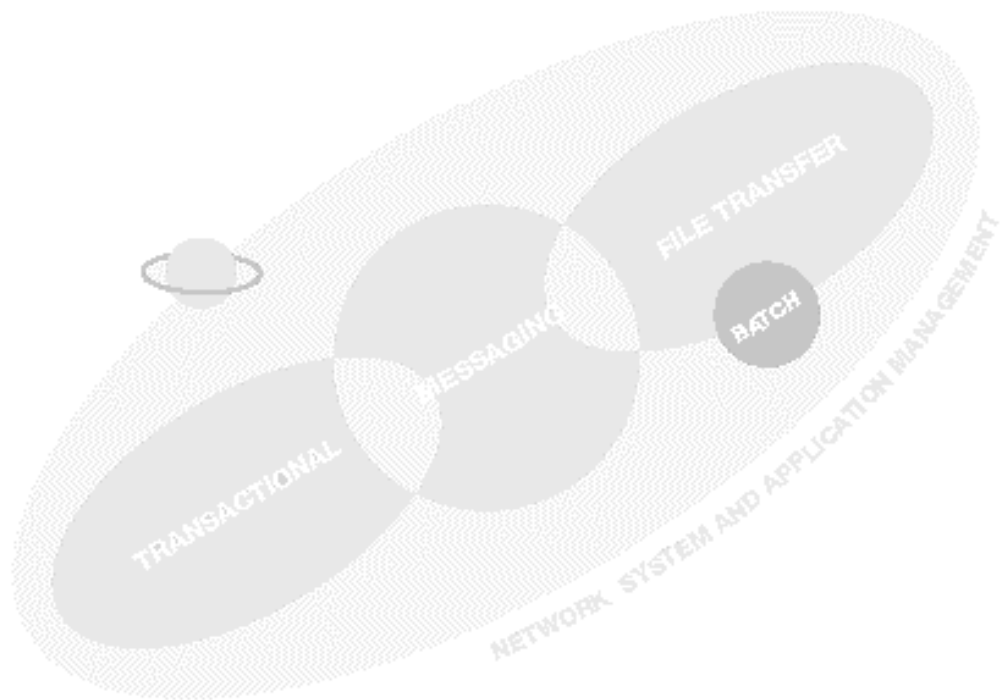


SPAZIO Data Secure

by Cesare San Martino (Primeur Security Consultant)

EWP004/01

July 2002



Contents

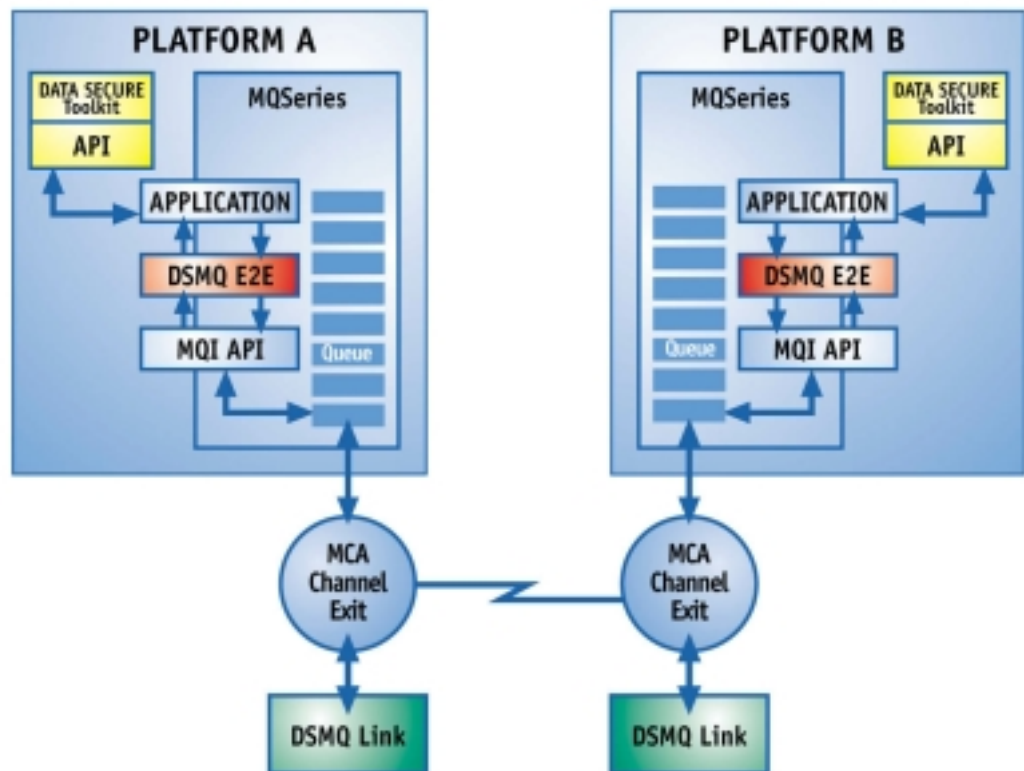
Chapter 1	Introduction	2
Chapter 2	Data Secure Services	4
Chapter 3	Data Secure Architecture and Functionality	5
3.1	Data Secure toolkit	5
3.1.1	Data Secure API	5
3.1.2	Data Secure Token Editor	7
3.1.3	Correspondent DB	7
3.2	Data Secure stand alone	7
3.3	Data Secure for MQSeries	7
3.4	External Technologies	8
Chapter 4	Data Secure Algorithms	9
Chapter 5	Data Secure for MQSeries	10
5.1	Background	10
5.2	Product features	10
Chapter 6	Data Compress for MQSeries	13
Chapter 7	Platform availability	14

Chapter 1 Introduction

Data Secure offers a wide range of powerful and modern cryptographic techniques, to achieve security of data in a very wide environment. Data Secure is currently available in 3 different versions:

- **DATA SECURE Toolkit (DSTK)**. A multiplatform set of APIs, that allows the developer to use security functionality in any context.
- **DATA SECURE for MQSeries Link (DSMQ Link)**. A product specifically written for the IBM MQSeries environment, aimed at securing messages over an MQSeries network at the channel level.
- **DATA SECURE for MQSeries End To End (DSMQ E2E)**. A product specifically written for the IBM MQSeries environment, aimed at securing messages at the application level, being transparent from the application itself.

The difference between the three* can be better appreciated by looking at the following diagram:



- DSMQ Link is a link oriented solution. Its point to point security module (DSMQPPS) is hooked into the MQ Channel exit and will therefore secure anything below that i.e. the link. DSMQ thus offer security “on the wire”, by providing the following functionality:
 - Peer Entity Authentication
 - Privacy
 - Integrity
 - Compression

The above functions can be individually switched on or off, to achieve e.g. authentication only, or authentication and integrity or all of the services together.

- DSTK is an end to end solution. It provides a higher level since it is positioned at a higher level in the architecture and can therefore protect anything below the application, including MQSeries queues. The programmer is required to code the appropriate calls within the application. DSTK is applicable to any environment, including MQSeries.
- DSMQ E2E is an end to end solution specifically aimed at the MQSeries environment. It provides a higher level since it is positioned at a higher level in the architecture and can therefore protect anything below the application, including MQSeries queues. DSMQ E2E is application transparent and therefore requires no code change.

Chapter 2 Data Secure Services

Data Secure offers a comprehensive series of security services, described in this section.

Standard Service	S/MIME	PKCS#7	PEA X.509
Privacy	x	x	x
Integrity	x	x	
Authentication	x	x	
Non Repudiation	x	x	
PEA			x

Chapter 3 Data Secure Architecture and Functionality

SPAZIO Data Secure has a modular architecture, that lets you choose from a wide range functionality provided at various levels, depending on the context in which you wish to use these services.

3.1 Data Secure toolkit

The toolkit is the central element of Data Secure. The Toolkit provides access to the functionality of the product in the widest and most complete way.

3.1.1 Data Secure API

The Data Secure APIs are the core of the Data Secure Toolkit. They are available for MVS, UNIX and Windows NT platforms. The following functions can be implemented through the API:

PKCS#7 Support

Support for the PKCS#7 standard is support for the widest range of cryptographic techniques based on RSA public key encryption. In particular, this includes handling the generation of signed messages and “digital envelopes” as supported by this standard.

PKCS#10 Support

This functionality allows the generation of standard X.509v3 certificate requests, to be submitted to a Certification Authority, in accordance with the PKCS#10 standard. The generation of RSA keys is executed internally. Certificates can be managed and Certificate Revocation Lists accessed.

PKCS#11 Support

This standard allows the management of Cryptographic Tokens. Cryptographic tokens are used to protect and manage data that is sensitive from a security viewpoint. The token is normally implemented on a specific hardware device, such as a smart card. Data Secure also allows a software implementation, that is more useful in certain cases (large systems).

The Data Secure software token, as well as storing encrypted keys, as supported by the PKCS#11 standard, is protected from fraudulent modifications by a special function.

More specifically, Data Secure manages a “Cryptoki”: Cryptographic Token Interface.

The Data Secure Cryptoki manages the following objects:

- X.509 certificates
- Public and private RSA keys
- DES, 3DES and RCx secret keys

In addition, a software module (Win32 platform) called the Token Editor is supplied with Data Secure for interactive token management.

Cryptographic tokens are currently considered the safest way to store the critical elements of a security system and are quickly being established as the standard method for storage of keys, replacing traditional solutions such as storage in hidden files or internally in the system.

The implementation of the PKCS#11 standard guarantees the widest possibility of interoperability with applications based on the standard. Data Secure can interoperate with external Tokens and CryptoKis.

S/MIME Support

Allows the generation (and subsequent extraction) of cryptographic messages signed and/or packed according to the S/MIME standard.

X.509 Standard 3-way Peer Entity Authentication Support

This allows the mutual authentication of communicating entities using the X.509 standard, in its 3-way form (the most secure), which does not presume the availability of synchronized clocks on the network.

3.1.2 Data Secure Token Editor

The Token Editor is a Win32 application that allows the interactive management of cryptographic tokens. All the basic functions are provided for each object handled:

- Certificates: generation of requests to the CA, storing, import and export
- RSA keys: generation, storing, import and export
- Secret keys: generation, storing, import and export

Tokens are protected by a relevant PIN with a Password of configurable length.

3.1.3 Correspondent DB

The Correspondent Data Base, or CDB, is used to store security-related data on correspondents to whom you frequently connect in protected mode. Therefore, the CDB includes both certificates and the public keys they contain, to be used for a quick local consultation.

The CDB is loaded and consulted automatically by Data Secure when required. A management utility is also available for UNIX, Windows NT and MVS environments.

3.2 Data Secure stand alone

Data Secure stand alone is a Win32 application that allows the user to perform certain basic cryptographic functionality.

It lets you generate and open messages and files that are signed and/or encrypted, packed according to S/MIME or PKCS#7 standards. In addition, this utility lets you read the Correspondent Data Base, from which you can extract certificates and public keys.

3.3 Data Secure for MQSeries

Data Secure for MQSeries is a security software product especially for users of MQSeries. Paragraph 5 contains a complete description.

3.4 External Technologies

Data Secure is based completely on international standards and published algorithms. Data secure can therefore be integrated with other security technologies that adhere likewise to recognized standards. For example, Data Secure could communicate with interoperable applications based on differing software solutions on diverse, or with implementations based on Smart Cards or other cryptographic hardware devices.

Chapter 4 **Data Secure Algorithms**

The algorithms underlying Data Secure are constantly updated, keeping pace with the most recent discoveries and implementations in the area of cryptography. Data Secure currently implements its services using the following algorithms:

- Symmetric encryption: DES, T-DES, RC4
- Asymmetric encryption: RSA
- Hashing: SHA1, MD4, MD5, RIPEMD160

Chapter 5 Data Secure for MQSeries

5.1 Background

As an increasing number of companies rely on MQSeries to exchange data and integrate applications in their distributed environment, it is essential to be able to provide encryption capabilities for those applications that deal with sensitive data.

It is important for encryption to be transparent to the application, so that no changes to the source code need to be applied.

Data Secure for MQSeries provides the following security features:

- Peer Entity Authentication.
- Integrity (proof that the message has not been tampered with during the transport)
- Encryption (data transmitted over the network is protected against intrusions)
- Compression (optional)

5.2 Product features

The following capabilities are offered:

Cryptoki Editor

A utility to manage Public and Private keys on both ends. The user will be able to build and maintain a local crypto token according to the PKCS#11 standard, where he will maintain his sensitive data (private keys, symmetric (secret) keys, certificates etc.).

CDB Editor

A Correspondent Data Base editor is also provided to keep track of trading partners' certificates, public keys etc.

PEA

A Peer Entity Authentication mechanism (PEA). This is implemented at the channel exit level of MCA, using the X.509 3-way standard PEA (which does not assume the availability of synchronized clocks at both ends). This mechanism will mutually authenticate both ends, and dynamically establish a symmetric encryption session key for further use during the session.

Technically this functionality will be provided as an API to be used with MCA. PEA will also provide the functions of Authentication and implicitly non-repudiation.

Encryption

Based on the established session key. The RC4 algorithm is used as it is strong enough (128-bit key) but still gives good performance. Alternatively T-DES could be used, which has the same level of security but is significantly slower. Finally, also DES could be used, although it's not recommended for certain applications, as it has been shown not to be strong enough nowadays.

Integrity

A MAC (Message Authentication Code) is added to a message to ensure that there has been no tampering with it on the network (the message that arrives is exactly the same as the message that left the other end).

Application transparency

The above security services are offered as integrated services within MQSeries at the MCA exit level. The user will not need to make any further change to his applications or to his system.

Of course, if application transparency is NOT desired (i.e. application end-to-end security is needed) this can always be achieved by coding the Data Secure Toolkit API calls within the application.

MQSeries Server and Client availability

The above services are available for an MQSeries Server as well as for an MQSeries Client.

MQSeries Clustering compatibility

Data Secure Services. The above services are available also on a MQ clustering configuration, both with homogeneous and Heterogeneous clusters.

Chapter 6 Data Compress for MQSeries

As well as encryption, another very useful service is offered to MQSeries users: compression. This is based on the Primeur proprietary SPACOD engine. This is technically a variation of LZW, with compression ratios and performances similar to the standard ZIP algorithm. Data Compress for MQSeries can perform buffer oriented compression on the fly, with unlimited buffer length.

Data Compress for MQSeries will allow significant saving on the application throughput, since the average expected compression rate on standard data messages is anywhere from 50 to 90% (depending on the type of message and the message length).

The compression function is available both as:

- An API
- Integrated transparently with MQSeries at the MCA exit level

Data Compress for MQSeries may be used jointly with Data Secure for MQSeries, further enhancing the overall security of the messages exchanged, besides providing the saving in data transmission mentioned above.

Chapter 7 Platform availability

DSMQ and DSTK are currently available for the following platforms:

- OS/390 (DSTK, LINK, E2E)
- AIX (DSTK, LINK, E2E)
- SOLARIS (DSTK, LINK)
- HP_UX (DSTK, LINK)
- NT (Win 32) (DSTK, LINK, E2E)
- OS/2 (DSTK, LINK)
- TANDEM Guardian (DSTK, LINK)
- Open VMS on Alpha (DSTK, LINK)
- AS/400 (DSTK, LINK)