

# White Paper



## Distribution of Sensitive or Valuable Data

Protecting digital content from producer to consumer

Author	Adrian Waller
Date	03/06/04
Reference	NET040604
Issue	2

# Abstract



As the information world converges on an open, shared communications infrastructure the protection of sensitive digital content increasingly becomes the responsibility of the originator or distributor. In this White Paper we highlight the shortcomings of the conventional approaches to this problem. We describe TRT (UK) work on defining a solution that operates above the communications infrastructure, and can offer many advantages compared to the conventional approaches.

## Keywords

Security, Privacy, Confidentiality, Infosec, Information Assurance, Digital Containers, Digital Rights Management, Encryption, Microtransactions, Micropayments, Access Control

### Thales

Thales is a world leader in mission-critical information systems covering three major markets: Aerospace and Space, Defence, and Security. We are present all along the value chain, providing equipment and systems, systems integration, prime contracting and services. Thales meets the communications, information and security needs of people in countries throughout the world with operations in more than 50 countries and 68,000 employees worldwide.

### Thales Research and Technology (UK) Limited

Thales UK's Reading-based research & technology facility is the UK arm of the Thales corporate research centre. Its activities focus on providing solutions: Security and Communication Systems, Galileo and Position-Based Systems, and Enhanced Digital Environments. These are based on the key technologies of IP Networks and Network Security, Wireless Communications, Sensors and Signal Processing, and Navigation and Positioning. The facility offers a wide range of consultancy and development services to European Government Agencies and to industry throughout the world.

Thales Research and Technology (UK) Limited  
Worton Drive, Worton Grange  
Reading, Berkshire, RG2 0SB, UK

Company Registration No. 774298

<mailto:scs.trtuk@thalesgroup.com>

## The Problem

The information world is converging on an open, shared communications infrastructure. Underlying networks are becoming more heterogeneous in nature. There is a move from static and centralised systems to more open, dynamic, mobile and distributed systems. The client/server model of large producers serving many consumers is being extended as more devices become producers of content - even those that are severely limited in processing capabilities. In such an environment, the secure distribution of digital content from producers to consumers requires new and innovative solutions.

In this White Paper we describe TRT (UK) work on defining a security architecture suitable for this situation. We show how this architecture can be applied to a wide variety of scenarios, ranging from the distribution and control of classified information to payment for "Infotainment" services.

## The conventional solution

The conventional solution for secure content distribution is to set up a secure channel between the producer and the consumer. The most commonly used technologies of this type are SSL and IPsec.

One major drawback of this approach is that the significant overhead involved in setting up the secure channel limits its scalability. For example, handling the near simultaneous set-up of a large number of connections on an SSL server or gateway is a significant problem. If the amount of content to be transferred is small (a "microtransaction"), this overhead is especially significant.

Scalability can also be adversely affected since the protection is applied as part of the process of content delivery. Sending the same data to a large number of consumers simultaneously or at a high data rate represents a significant computational load.

A third major drawback is that the producer must be directly involved in authorising the consumer to receive the content. As

networks become more distributed and dynamic, the task of authenticating and authorising consumers is becoming harder to manage and implement. Not only is this a burden on the producer, but it has implications for privacy and security. Consumers may need to provide sensitive details to producers as part of the authorisation process, which would imply that producers have to be relatively highly trusted.

## An alternative solution

### Securing the content

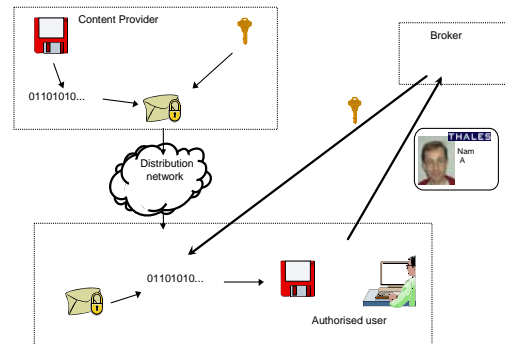


Figure 1 - Digital container system

An alternative to the conventional solution is to apply protection directly to the content, which removes the need for a secure session. This is the approach taken in "digital container" systems, as illustrated in Figure 1. In such a system, the content is encrypted and appropriate header information, containing rules for the use of the content, is attached to form a digital container. This container can then be delivered to any number of consumers without further processing by the producer. On receipt by a consumer, a third party broker has to be contacted in order to obtain the decryption key. This will only be returned after the broker has authenticated the user and checked their authorisation to use the content, based on the rules that were attached to the container by the producer.

### Advantages of this approach

This approach has many advantages. In terms of scalability, protection can be applied once, offline, for any number of consumers. This means that potentially expensive cryptographic operations do not need to take place in real-time or be repeated by the producer for each use. It

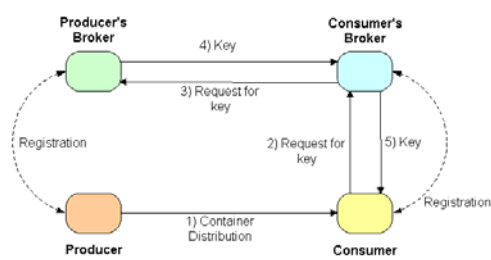
also protects the content while it is in storage at the producer. For these reasons, digital containers are particularly suited to store and forward applications.

The content may also be delivered through any distribution channel without a requirement for additional security. This makes it ideal for heterogeneous or dynamic networks.

The architecture separates the delivery of content from authorisation to use it, thus freeing producers from this potentially difficult and expensive task. Authorisation decisions are made at a central point, the broker, which can be specifically designed to handle them. Furthermore, consumers do not have to reveal potentially sensitive details to producers to obtain content. In fact, consumers can be anonymous to the producers with this approach.

## TRT (UK) approach

### SIBIS



**Figure 2 - Digital containers architecture with broker network**

TRT (UK) made a significant contribution to the development of a digital containers architecture as part of the SIBIS project. SIBIS was a DTI Link/EPSC sponsored project looking at efficient solutions for microtransactions. The architecture selected for implementation was based on the digital containers architecture. A key feature of the solution was the adoption of a broker network, as illustrated in Figure 2.

With this solution, each consumer registers with one broker, which will not, in general, be the same as the producer's broker. After registration, the consumer only ever needs to deal with their own broker. Keys are obtained from the producers' brokers by the consumer's own broker.

This architecture inherits all of the previously mentioned advantages of a digital containers architecture. In addition, the authentication and authorisation issues

are simplified since the consumer only ever has to deal with one broker. The number of brokers the consumer has to provide potentially sensitive details to is also reduced to one, and this can be one of their choosing.

The SIBIS architecture has been validated by implementing it as Java software components and running user trials.

### Summary of advantages

Protection applied once to content for end to end transfer

- *Can use any, potentially insecure, delivery channel*
- *Ideal for heterogeneous or dynamic networks*
- *Multiple 'hops' do not require multiple encryptions.*

Pre-preparation of content is possible

- *Content secured once for multiple end users.*
- *Containers provide secure storage at producer.*

Centralised authorisation and access control

- *Producer freed from handling authentication and authorisation of consumers.*
- *Centralised decisions and simplified auditing.*

Broker network

- *Consumers contact one broker only*
- *Scalability. Users set up one secure connection which can handle all further key requests.*
- *Privacy. One broker holds sensitive user details.*
- *Control. In a business domain, one broker controls all accesses by users.*

Microtransactions

- *Architecture specifically designed to have low overhead for microtransactions.*

Content neutral

- *Handles any digital content (e.g. documents, audio, video etc.)*

Consumer anonymity is possible

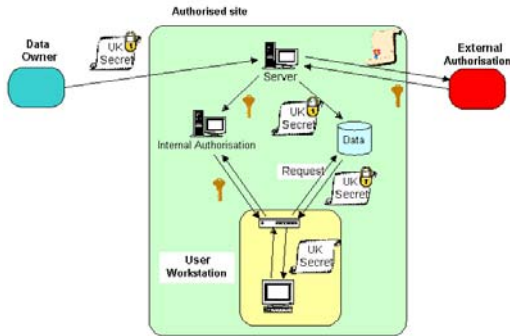
- *Consumers provide no details of themselves to producers.*

## Applications

### Classified data management

For a classified data management application, digital containers could contain documents (text, still pictures, web pages

etc.) or real-time data (e.g. sensor data, voice, video etc.). The rules attached to the encrypted data in the digital container could be as simple as a classification label, but could also contain more sophisticated rules for the release of the data. Access control to the data could be based on user authentication (e.g. biometrics, smart-card etc), user role/identity and entitlements.



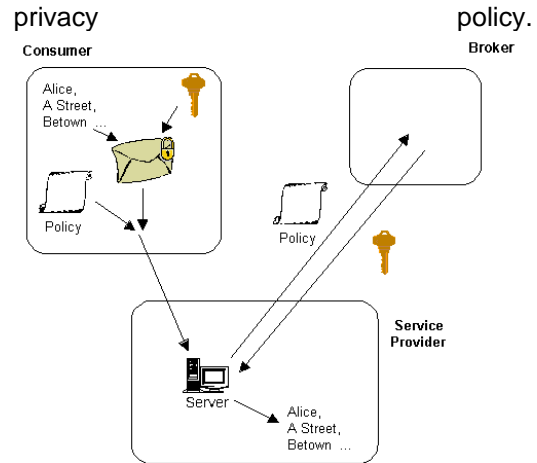
**Figure 3 - Classified data management**

The example in Figure 3 shows a hierarchy of brokers. The "External Authorisation" broker is responsible for releasing data to secure sites, and a separate "Internal Authorisation" broker performs fine-grained access control within the site. The actual decryption of content is handled by an assured device located at each user's workstation. In this environment, the centralised logging and auditing of access to classified data that this architecture provides would be a significant advantage. In addition, storing of data in encrypted form reduces the risk of exposure and the architecture potentially provides cryptographic separation for multilevel security on the same network.

## Privacy management

The need to protect consumer privacy on the Internet is becoming an increasing concern. It is now commonplace for consumers to have to provide personal information to service providers to receive their services. However, there is clearly the potential for service providers to use this personal information against the consumer's wishes and thus compromise their privacy.

Figure 4 illustrates the use of the digital containers architecture to control access to sensitive consumer details. In this case, the rules attached to the encrypted data in the digital container specify the consumer's



**Figure 4 - Privacy management**

When a service provider requests the decryption key, the broker will check to make sure that they satisfy the consumer's policy before granting access to the data. The broker may also keep a record of this access as a deterrent against misuse.

## "Infotainment" charging

A digital containers architecture can be used for distributing of and charging for "Infotainment". The content may be audio and video, streamed live events (e.g. a football match) or even stock market quotes or web pages. The architecture is used as shown in Figure 1, with the exception that consumers provide payment information to their broker in addition to identification information. Payments between consumers and content providers are cleared using the broker network.

For this application, the broker network is particularly attractive as it allows efficient account based billing to be used. Consumers hold an account at their broker, and payment for content involves the broker altering the balance for this account (with a corresponding alteration being made at the content provider's broker). This can make even very low payments (micropayments) feasible.

## Summary

In this White Paper, we have described the problems with the conventional approach for secure content distribution and shown how an alternative approach based on "digital containers" can be used. The digital containers approach has many advantages, particularly in terms of scalability and by freeing producers from having to deal with potentially complicated authentication and

authorisation decisions. Further advantages can be obtained by making use of a "broker network" for key management. TRT (UK) have helped develop an architecture based on these approaches and which has many applications, including classified data management and payment for "Infotainment" services.

## Further Information

For further information on the work by TRT (UK) described in this paper please contact [networks@thalesgroup.com](mailto:networks@thalesgroup.com).

THE INFORMATION IN THIS DOCUMENT IS SUPPLIED "AS IS" WITHOUT ANY EXPRESS OR IMPLIED WARRANTY WITH RESPECT TO THE ACCURACY, COMPLETENESS, OR USEFULNESS OF ITS INFORMATION AND IN PARTICULAR WITHOUT ANY WARRANTY AS TO FITNESS OF SUCH INFORMATION FOR THE INTENDED PURPOSE.

THALES NOR ANY PERSON ACTING ON ITS BEHALF:-

A) MAKES ANY WARRANTY OR REPRESENTATION, EXPRESS OR IMPLIED, THAT THE USE OF THE INFORMATION IN THIS DOCUMENT MAY NOT INFRINGE THIRD PARTY RIGHTS;

OR

B) ASSUMES ANY LIABILITIES, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE) OR OTHERWISE, WITH RESPECT TO THE USE OF, OR FOR DAMAGES RESULTING FROM THE USE OF ANY INFORMATION IN THIS DOCUMENT.

NO RIGHT OR LICENCE IS GRANTED TO THE RECIPIENT IN RELATION TO ANY INFORMATION IN THIS DOCUMENT.