Workflow Management Coalition

WfMC

The Workflow Management Coalition Specification

Workflow Management Coalition

Workflow Security Considerations - White Paper

Document Number WFMC-TC-1019

Document Status - Issue 1.0

Feb 98

Send comments to wmc_tc@fsc.ossi.com

Workflow Management Coalition
PO Box 165
2 Crown Walk
Winchester
Hants SO22 5XE
Tel: (+44 0) 1962 873401
Fax: (+44 0) 1962 868111
Email: wfmc@wfmc.org

Table of Contents

1. INTRODUCTION

1.1. Background

The Workflow Management Coalition is a non profit organisation with the objectives of advancing the opportunities for the exploitation of workflow technology through the development of common terminology and standards.

Within the WFM Coalition organisation, the Technical Committee is responsible for the development of appropriate technical specifications and related documents, which are approved for formal issue by the WfMC Steering Committee. Technical specifications are developed by these individual Working Groups, working within the overall framework of the WfMC Reference Model and following agreed common architectural principles.

A new technical area of work is normally started by the production of a White Paper, which is essentially a discussion document to identify alternative approaches. In the case of systems security, which is a pervasive topic potentially affecting all working groups, it is also important to scope work in other standardisation bodies to achieve as much harmonisation and adoption of other industry standards.

1.2. Purpose

This document is intended to stimulate discussion and identity a forward path for the incorporation of appropriate security services into the architecture and standards of the WfMC.

1.3. Scope

This document summarises a number of security services which may be important within a workflow system and relates them to a generalised model identifying different security domains within a heterogeneous workflow environment. It then identifies areas of potential work for the WfMC, concentrating on Workflow interoperability between different organisational domains.

1.4. Cross References

WFMC-TC-1003	Workflow Reference Model
WFMC-TC-1009	Workflow Client Application API (WAPI)
WFMC-TC-1012	Workflow Interoperability - Abstract Specifications
WFMC-TC-1015	Audit Data Specifications

1.5. Revision History

This issue is the first, unchanged from the earlier draft for comment.

2. OVERVIEW OF SECURITY SERVICES

The following services are of potential relevance within a workflow system or co-operating workflow systems. In some cases part, of all, of these security provisions may be provided by underlying software, such as the platform operating system or data communications services, rather than the workflow system itself.

It is not the intention to describe in detail the various security functions, nor to chronicle existing standards within the various areas, but to draw out those areas which are important for further consideration by the WfMC. In particular this concentrates on services required in the context of workflow interoperability, since this is where additional complexities arise due to the separation of security domains across different organisational boundaries and the probable use of public interconnection infrastructure between organisations. It is also known to be a priority area of requirements for the Japanese Standards Association (JSA) and of increasing interest to the Black Forest Group (BFG).

Note that where the use of various cryptographic algorithms is discussed, the author wishes to bring to attention the fact that the provision of cryptographic variables and the use of particular algorithms may be controlled by individual governments in the interests of both security and trade. In particular some algorithms are subject to export licence requirements if they are required to be used outside the country of origin. In addition, specific government restrictions and requirements may apply to any system in which government data is held.

The main implication of this is that the WfMC will need to adopt a policy of allowing alternative cryptographic algorithms to be specified to fulfil the same general functionality in different markets and countries. (In addition to the legal restrictions, users may also wish to use common algorithms already adopted as security infrastructure for other, non-workflow, applications.) This white paper is written on the assumption that the choice of particular algorithms should be an implementation issue, and should not be mandated by the WfMC.

2.1. Authentication

This is the process by which a computer system or a (human) system user unambiguously identifies themselves to another computer system, normally in the context of gaining access to various services which the authenticated party is authorised to use on that computer system.

In the context of workflow, the most common requirement is for the authentication of a user or systems administrator as part of the log-on activity prior to work assignment within a particular (single) workflow service. This typically occurs within a single administrative domain based upon the security services of the underlying platform or network service (e.g. via password log-on or the authentication of a token such as a smart card) and this aspect is not proposed as an area requiring immediate WfMC activity.

For simplicity it is assumed that all user access will use the authentication mechanisms within the local workflow domain even where access is granted to users within a different, but interoperating domain. This means that where users are required to interact with different workflow services they are required to be registered on each service and separately authenticate themselves to each domain. Thus the 2 workflow systems do not need to share a common model for user names and pass details of user credentials between themselves.

[This does not preclude the possibility of two or more workflow services adopting a common authentication model and authorisation - and for example using a “standardised” authentication service such as Kerberos or Sesame; however, it means that this is handled by mutual agreement between the parties outside the immediate workflow environment. Adoption of a more sophisticated approach may be an opportunity for further study in the longer term.]

A secondary requirement for authentication is to ensure that during a workflow interoperability exchange the two workflow systems initiating and responding to a command sequence can be assured of their mutual identities. In particular where such systems are operating in an asynchronous manner, with interconnection via email, this may require special provisions within the interoperability protocol, due to the relative insecurity of the underlying communications path with store and forward transfer through potentially insecure nodes and the probable use of public data communications infrastructure.

In some workflow scenarios, particularly those supporting electronic trading, this requirement may also be related to non repudiation of message origin, since one purpose of authentication of the originator is to assure the recipient that the originator cannot repudiate the business transaction which he has initiated.

Such authentication is normally based upon cryptographic algorithms; public key (asymmetric) techniques being adequate for proof of origin and private key (symmetric) techniques providing privacy and/or assurance between both parties. Some authentication models are based upon an ongoing session between the two parties with authentication occurring at session start; others allow for the authentication procedure to be periodically invoked. In the case of workflow interoperability by email, or other asynchronous mechanism, each exchange in effect constitutes a session requiring separate authentication. This particular requirement is further considered in Section 4.

2.2. Authorisation

Authorisation is the process of identifying to the computer system the various functions which a user (human and potentially a computer system) may undertake. In a workflow system users are often authorised to undertake a particular “role” defined within the process definition(s). Particular privileges may be associated with certain roles such as systems administrator.

Although various models of dynamic authorisation exist using a common authorisation service shared by a number of administrative domains it is not recommended that this be an immediate study area for the WfMC. In the first instance it is proposed that a simple model of authorisation be adopted based upon administrative functions local to a workflow domain.

Where interoperability is occurring between two different workflow domains, the shared workflow process definition is assumed to contain information which can be adequately interpreted by both domains. Thus any role based data within the process definition (or a sub-process definition) is assumed to have been established in conjunction with the user authentication and authorisation processes within each workflow domain.

[Again this does not preclude a common authorisation service across different workflow domains, but neither does it mandate it as a necessary element for interoperability. Generally similar considerations to 2.1 above apply.]

2.3. Access Control

Access control is the mechanism by which users are permitted access to various operations or data within a computer system, according to their identity (established by authentication) and associated privileges (established by authorisation). In the context of workflow systems, it may operate at the level of:
(a) log-on to the workflow service, and
(b) access to undertake particular activities or work items according to functional role and/or data sensitivity.

2.4. Audit

Audit provides the ability to maintain a history of system events and operations across the computer system to enable subsequent identification of events of interest or with particular security implications.

Audit may be thought of as having two constituent elements:
(a) Audit data recording, for which the WfMC has already published standards to enable consistent audit of process enactment across multiple workflow engines.
(b) Audit data retrieval and analysis, which is required to be locally provided on each workflow domain using the appropriate local tools and services.

The primary goal of WfMC in this area has thus already been reached, using specification WfMC-TC-1015, which defines standards for audit trail content and recording, thus enabling a consistent logical audit trail to be maintained across one or more different workflow domains.

2.5. Data Privacy

Data privacy services ensure that data transferred between users or computer systems or stored on such systems is confidential to the party (or often, parties) involved and cannot be viewed by a third party. In the context of workflow systems such data may comprise one or more of:

- Applications data,
- Workflow Relevant data, or
- (less likely) Workflow Control data.

Data privacy may be required within a single workflow domain, for example to ensure that sensitive case data relating to a particular process instance is confidential to those workflow participants authorised to operate on that process instance. In such cases the privacy mechanisms are specific to the workflow domain and may often involve a combination of access controls and data encryption. Again, it is proposed that the WfMC should not concentrate on this aspect as an immediate requirement, since the provision of value-added services such as security within a single (homogeneous) domain is not a WfMC objective.

It is also a common requirement to protect data transferred between different workflow domains from compromise by third party viewing during transfer. This is normally accomplished by cryptographic protection using a symmetric key known only to the two parties. Such techniques may be applied to all messages or to a subset, for example just those including sensitive application or workflow relevant data

2.6. Data Integrity

Data integrity services provide assurance that data transferred between parties has not been modified during the process of transfer. Several levels of integrity may apply:

- Basic protection against corruption or transposition errors during storage or transfer may rely on a relatively simple checksum style mechanism. Many data storage facilities and data communication protocols incorporate such mechanisms.
- Strong data integrity will normally rely on cryptographic algorithms, for example applied to a message hash computed by a strong one-way algorithm. Public key algorithms are often employed for this purpose using a verification of the message hash with the public key half, although symmetric key algorithms applied to a message hash may be equally applicable (although adjustments may be needed for the appropriate key lengths applied in each case).

Such data integrity mechanisms do not provide any message privacy protection since the message content is transferred in clear text and it is only the message hash to which the encryption is applied. Where a message is signed using an encrypted hash this also provides a mechanism for non-repudiation, due to the mathematical impossibility of decrypting the one way hash when signed with a different key.

Data privacy encryption using a symmetric key applied to the full message text may also provide a degree of data integrity. Whilst an inserted or modified message may decrypt to a valid bit string using the receiver's secret key, effective logical content stills depends upon original encryption using the secret key. In many situations where message content is changing relatively frequently, (for example financial authorisation messages from EFTPOS), symmetric key encryption is employed to provide both integrity and privacy protection.

Thus within a workflow service broadly similar considerations will apply to those under data privacy; the most important area for immediate consideration is the provision of message integrity protection during interoperability.

2.7. Non Repudiation

This has already been discussed above, within 2.1 and 2.6. In the context of workflow interoperability it may be a requirement when process interoperability has significant financial attributes, such as might be the case with various type of financial trading processes.

2.8. Security Management & Administration

Any security system relying on passwords, cryptographic keys and the like will require a security administration domain which must provide mechanisms for the allocation, distribution, secure storage and, in due course, replacement of the passwords / keys. For the purposes of this paper it is assumed that the boundaries of the workflow domain will normally coincide with those of the security domain, thus simplifying matters considerable and allowing whatever domain specific provisions are available to be applied in this area.

The one problem this leaves is that of key distribution between parties where cryptographically based security services are required during workflow interoperability. As workflow interoperability is defined in strictly bilateral terms (each message session is between exactly two parties) management of key material or passwords can be done relatively easily on a manual bilateral basis.

[Again this does not preclude the use of automated key distribution techniques, it just means that WfMC are not going to attempt to prescribe how such measures should be applied.]

Changing keys and distribution of the public key halves of asymmetric keys is, of course, much simpler conceptually than that for the symmetric private key. However, where secure interoperable workflow systems are established it is reasonable to assume that such interworking will be as the result of an agreed business process between the parties, within which such security provisions will be agreed and actioned.

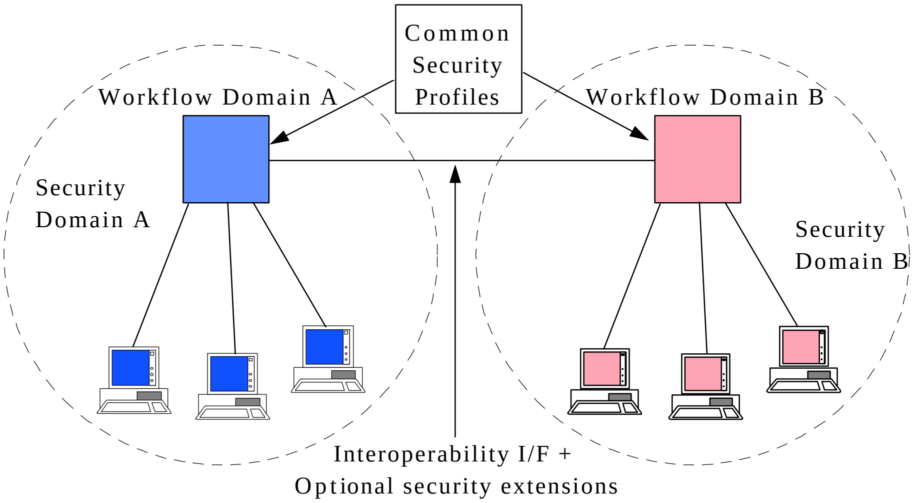
3. SIMPLE WORKFLOW SECURITY MODEL

3.1. Overview

The model following has been derived as a starting point for discussions on incorporating security services into the WfMC standards. It is based on a separation of security administration and support into individual workflow operational domains and the provision of optional security extensions to the interoperability protocol for operating inter-domain.

The initial WfMC security work should focus on interoperability since this is where the greatest market pressures lie. This introduces various security functions to be provided in a standardised manner within each domain (to support interoperability) as an integral element. However, there is also scope in the future to consider common security extensions to other interfaces local to a domain (such as process invocation) and the ability to introduce various security elements within the process definition to support process definition interchange.

This approach does introduce some important simplifications, in particular the alignment of workflow domains for administrative purposes (including assignment of security attributes) with those for interoperability purposes, but this should enable progress to be made quickly.



Security facilities may thus be considered in terms of those provided between security domains and those provided within each domain. [This is not intended to preclude the potential for establishing a single security domain across two interoperating systems, but reflects the practical requirement to support security services for interoperability between organisations or other entities, which will have their own individual security policies and procedures.

3.2. Cross Domain Interoperability Security Extensions

The following security operations are initially defined for use inter-domain:

- Authentication - at the level of peer workflow services
- Data integrity - on the data content of the interoperability protocol
- Data Privacy - on the data content of the interoperability protocol
- Audit - provision of consistent audit data (as per TC-1015 specifications)[1]

3.3. Security Profiles

It is proposed that the scope of security provisions required to be applied to any interoperability interface are defined in the form of a common security profile which is maintained consistently by both parties and which is used to control the way in which security is applied during interoperability.

The profile will identify the security services to be applied to interoperability between the two parties, along with the particular algorithm(s) and key(s) to be used for the cryptography. (it may also be the appropriate place to record any specific requirements for the provision of audit data for interoperability). The security profile may be thought of as an extension of other workflow interoperability data, for example alongside the Node Id and Email address of a particular workflow engine.

In addition to the information about security measures to be deployed, the profile should also contain information about when such measures should be used. Security services may need to be invoked under a range of circumstances:

- for specific type of process (e.g. identified by Process Definition Id)
- for specific process instances, for example according to client type where a common process exists for both "sensitive" and "non-sensitive" clients (e.g. represented through a workflow relevant data attribute of the process definition)
- by specific client application API call (e.g. WMAssignProcessInstanceAttribute or WMAssignActivityInstanceAttribute)

It is also likely that control information about authority for undertaking various operations may also need to be maintained. Such functions may need to include:

- Process initiation permissions - to define which external workflow domains are permitted to initiate processes on the target domain
- Control of Attribute usage - to define which process definition attributes are permitted to be externally modified or set (or, possibly, read) where a process is initiated remotely.
- Other administrative functions - for example to define what local operations are permitted on a remotely initiated process instance (for example should the initiator be able to prevent any local modification to particular workflow relevant data or other process attributes?)

[1] This is covered , in particular, by the Remote Process Operations Audit data

In such cases whenever a workflow engine (e.g. A) starts a workflow session with the remote engine (B) it always invokes security according to the defined security profile for A to B. Similarly the receiving engine, in this case (B), always expects incoming message exchanges to follow the defined security profile which have been preset on it for A to B.

The above scheme allows for asymmetry of security profiles between A to B and B to A, although details of both profiles have to be present on both machines. In particular it allows for the use of a pair of asymmetric keys between each party, avoiding the need for private keys being distributed. Where symmetric key operation is required, for example including privacy encryption, both A to B and B to A use the same key and algorithm information. However, the two separate profiles would allow different policies to be followed if required (e.g. authentication and specific message encryption A to B, authentication only B to A.

[It is for further consideration to assess whether a single symmetric profile would be adequate. In many practical situations it is likely that both parties exchanging data will be happy with a symmetric approach; however for the moment and in common with other asymmetric aspects of our interoperability model I have left the option open.]

In simple operational scenarios the security profile may be established by manual administrative procedures agreed between the two parties; in more complex scenarios (longer term) there may be automated support including negotiation of compatible profile options and distribution and installation of cryptographic keys. It is not proposed that WfMC moves to define specific security protocols for such purposes, but considers the work of other standardisation bodies.
As noted in the following section some data elements required in a security profile could be derived from the process definition and transferred as part of the process definition.

3.4. Security within a Domain

Each Security domain will normally be associated with a homogeneous product environment. In addition to the support for interoperability security extensions, it is expected that a range of local (within domain) security related facilities will be provided, such as:

- establishment of workflow user roles and associated privileges
- participant registration and role association
- authentication of participants
- administration of authorised operations via access control policy

Some of these facilities are likely to have commonality with the requirements for secure interoperability, for example process initiation and attribute modification may also need to be restricted to certain users or participant roles within a domain.

The existing WAPI specifications TC-1009 (Interface 2) already include the concept of different conformance classes and, by implication, different workflow user roles which may require different levels of authority for particular operations. In particular it identifies administrative functions and other operations which could be made subject to supervisory privilege where a particular implementation requires.

The Process Definition Interchange specification TC-1016 (Interface 1) does not include any security specific data, although the scheme for extended attributes and library functions would permit the definition of various security attributes as part of the process definition. However, this would need agreement on a useful and commonly accepted set of security related attributes which could be interpreted and supported in a meaningful way across heterogeneous systems

It has not been the policy of the WfMC to attempt to standardise security features within a single workflow product domain, since this has been seen as an area of product differentiation. Consideration, however, could be given to classifying various common levels of underlying required security capability within the process definition, e.g. which user role is permitted to create a process instance or whether certain process attributes can be manipulated in particular ways (approximately equivalent to read/write/execute permissions at the process instance level). It may also be feasible to specify a facility in general terms (e.g. “data integrity services required on the transfer of workflow relevant data”, whilst leaving the particular implementation of the security level as a product specified capability at execute time.

4. POTENTIAL WORK AREAS

4.1. Reviewing other relevant work

There is a very large amount of work done and being done on security by a range of industry bodies and formal standards institutions. Amongst the work likely to be directly relevant are standardisation activities within:

IETF	- RFCs on Security Services
OMG	- Security Services for CORBA interoperability
ISO	- Certification (X.509) and other related standards

Numerous cryptographic algorithms exist, some as formal standards (e.g. FIPS for DSA and SHA, the DES standards series), others as commercially available algorithms (e.g. RSA)

There has been some flux in the development of security services applicable to MIME objects and mail exchange operations, and which would be of direct relevance to the WfMC security interoperability requirements. Amongst the standards of potential use are:

- Security extensions using Multi-Part MIME bodies (providing basic rules for adding security elements to MIME body parts)
- MOSS, an object based set of security services applicable to MIME objects. This is perceived as rather complex and has not found widespread industry backing in product take up.
- S/MIME - a more recent standard aimed at providing Secure MIME services and with (currently) quite powerful industry backing.

In the immediate future it is suggested that RFC 1847 and S/MIME are worth more detailed assessment as the framework for developing interoperability security extensions.

4.2. Defining Security Profiles for Interoperability

From the earlier discussions it is possible to derive and postulate a number of security services which could be applied in increasing levels of security.

i) nothing
ii) simple authentication between the parties on message exchange
iii) authentication plus optional encryption of individual messages identified by message header, or on exchanges relating to particular process instances, where required
iv) authentication and encryption of all messages
v) etc..

The security profile would include the type of information discussed in section 3.3:

- the above information on level of security services required, by
- process type, or other criteria for invocation of the particular security level
- permission and authorisation data
- administrative data, e.g. algorithm and key details, etc.

There are several possible approaches to establishing the security profile:

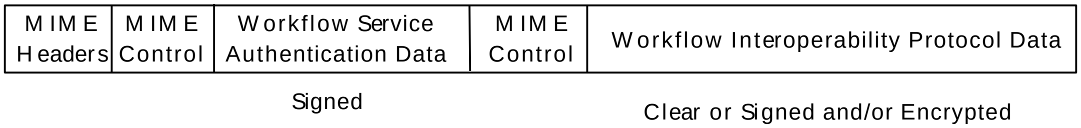
a) In the simplest approach it is externally (to the workflow interoperability exchanges) defined and both parties follow the pre-established profile. This is the simplest approach, using some external administration function, but does not offer the flexibility to dynamically negotiate or amend the profile, if required.
b) At session establishment some negotiation or notification of security requirements is passed between the parties. A fundamental problem with this in an asynchronous operational environment is that it does not easily allow negotiation where a number of individual messages are concatenated into a single email exchange. In these cases the session establishment message may be immediately followed by process creation and invocation messages to which the security profile may need to apply.
c) The security profiles are administered by a trusted third party and both systems obtain the information from this source.

The development of security profiles is an important element of the administrative procedures necessary to support security. The WfMC may not need to define an encoding standard for such security profile data (since such data may not need to be directly exchanged electronically) but it will be necessary to identify what data is required within the profile and what degree of flexibility is provided initially over invocation criteria. It is suggested that a simple approach is required for quick initial implementation, with more sophistication being capable of addition later.

4.3. Defining WfMC Interoperability Extensions

Extensions to the interoperability protocol are necessary to provide three security services. It is suggested that this could be handled by splitting the protocol into two components:

1. Workflow Service Authentication Data (covering the node id, domain id, and session id?)
This is used to identify the workflow service(s) involved in the exchange, and could be digitally signed to authenticate origin where required by the security profile, otherwise would be sent in clear as per the normal protocol
2. Workflow Interoperability Protocol Data (covering the specific interoperability commands/responses, etc.)
   This can be signed, and/or privacy encrypted, or sent in clear as required to meet the particular security profile considerations


MIME Headers
MIME Control
Workflow Service Authentication Data
MIME Control
Workflow Interoperability Protocol Data
Signed
Clear or Signed and/or Encrypted

This approach uses multi-part MIME bodies. Each component would be sent as a separate MIME body part, with its own MIME Control and MIME Header. This approach means that for simple peer authentication it is not necessary to hash and sign the complete message, merely the initial Service Header data. Security services to provide full data integrity will require the full message be signed and or encrypted.

An alternative approach for peer authentication on session establishment is attractive, where a connection oriented message transfer infrastructure exists. In this model the two parties can exchange secure tokens at session connection and periodically thereafter during the duration of the active session. (This approach is used by the CHAP authentication mechanism within PPP.) This model could be attractive where a permanent underlying connection supports email or CORBA interoperability. However, this model is not really applicable to most email based services which operate on an asynchronous store and forward basis and where the concept of a session based connection is not strictly relevant.

Each of the security services could be provided as follows

4.3.1. Authentication & Non-Repudiation

The simplest approach is by the use of signed body part on the protocol service data element. This is checked by the receiver using the public key. An alternative scheme using a private symmetric exchange is also feasible (as with CHAP).

4.3.2. Privacy

By private key encryption of the body part containing the message data, and decryption by the recipient. This may be done, if required, in conjunction with the public key signing of the body part. Certain public algorithms, notably RSA, allow the encrypted exchange of a private key using encryption by the public key and decryption by the private key.

4.3.3. Data Integrity

By signing the entire message using the private key half and verifying on receipt using the public key half.

4.4. Security Administration

It is envisaged that considerable future work could be done in this area, but that in the immediate future administration is likely to be largely manual or to use mechanisms defined by other bodies. It remains an area for future work by the WfMC, preferably in conjunction with other standards organisations.