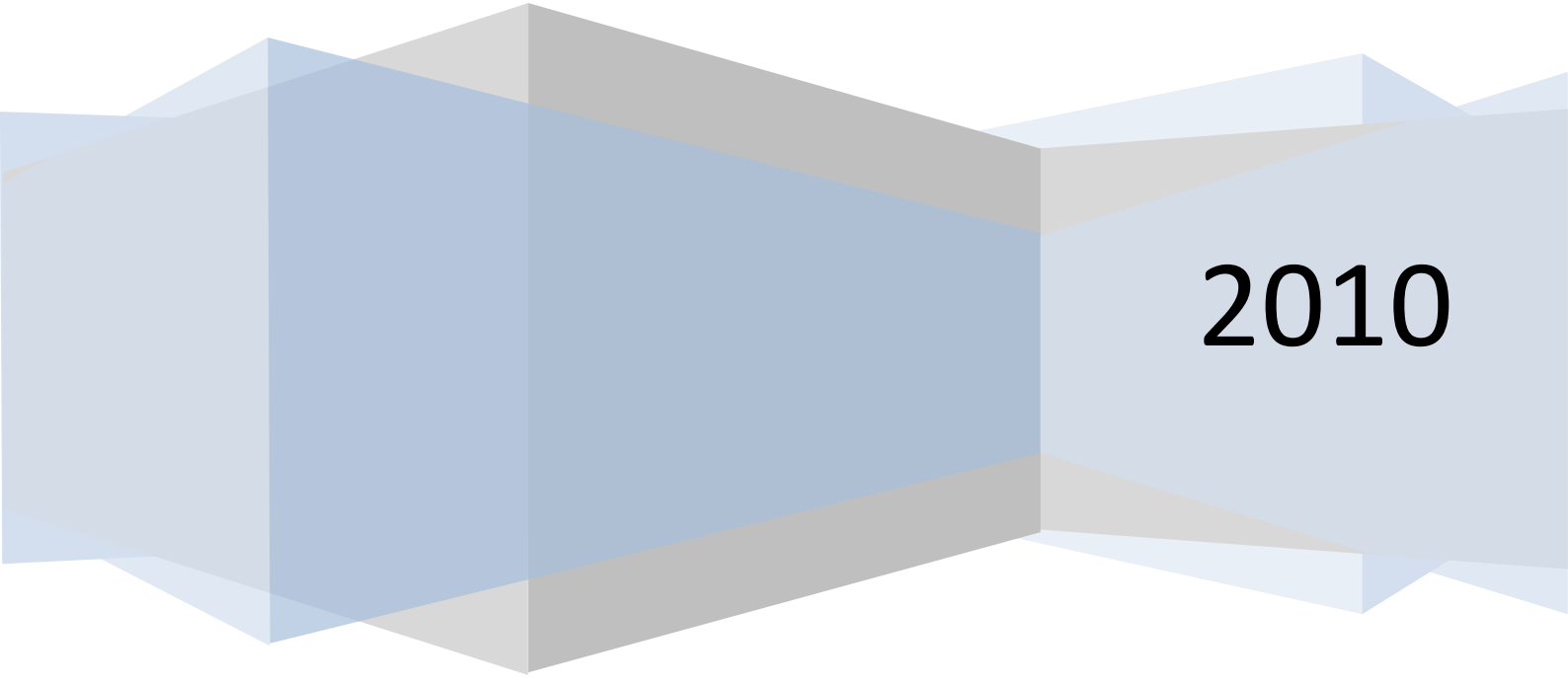
BSTTech Consulting Pty Ltd

Policy Based Security

The implementation of ABAC Security through trusted business processes (policy) and enforced metadata for people, systems and information.

Bruce Talbot



2010

Executive Summary

The creation of a computer based solution for the presentation of information across multiple information compartments[1] (Multi-Level Security) in a federated environment requires the amalgamation of several traditional security technologies and the close coupling of technology and business. In particular, federation requires the establishment of detailed 'agreements' regarding the information to be shared and the meta information[2] that can be provided.

As is further described in this document; an essential element of a complete solution to meet these requirements is the development of a structured set of metadata elements that can be used to describe the critical attributes used to allow access to information. A metadata based approach, coupled with the identification and codification of the business processes for the management and release of information is often referred to as Attribute Based Access Control (ABAC).

ABAC provides scope for a highly scalable access control regime, which can be applied beyond the traditional enterprise level, based on a defined trust-relationship among providers and consumers over and above the traditional system-to-system logon. ABAC seeks the provision and matching of specific attributes between users and information for each access. Examples of these attributes could include items such as citizenship, organisation, geographic location, association with law enforcement, etc which ABAC systems test against well defined policy requirements and enforce to determine access to data.

This paper discusses the conceptual metadata requirements and business logic approaches necessary for the implementation of a Commercial of the Shelf (COTS) based ABAC authorisation approach to information security.

[1] Within a military environment these are often referred to as Communities of Interest (COI)
[2] Meta Information, descriptive information about or concerning the object under discussion which could be a person, application, system, device, document or database record.

Table of Contents

Table of Figures

Trusted Management of Information

Attribute Based Access Control (ABAC)

Attribute Based Access Control is an access control methodology that assesses known (and trusted) information about every individual attempting to access information within a system against the attributes (metadata) required by policy (business rules) for each business compartment. ABAC provides highly scalable access control, beyond an enterprise level, based on a trust-relationship among providers and consumers which goes well beyond the traditional system-to-system logon. It uses specific trusted attributes for each access such as citizenship, organisation, geographic location, association with law enforcement, etc and tests these attributes against policy and enforcement requirements to determine access to data. This vetting by policy/business rule to look for the necessary attributes before granting access means two different users can access an information site and receive distinctly different sets of data, depending on their individual attributes for a particular session. Additionally, by allowing external agencies to participate in the trusted environment the concept is infinitely scalable.

To implement ABAC requires a well defined information management regime to allow the classification of what services or information can be presented to which users based on which attribute sets. Additionally, to be managed by an ABAC capability, information needs to be 'marked' with the appropriate metadata and controlled by well defined business processes to ensure release of information based on the resultant policy decision.

Purpose

The purpose of this document is to present the results of the BSTTech Consulting Pty Ltd (BSTTech) research into how ABAC can be practically achieved in a federated environment. The document presents the approach to developing the appropriate metadata set(s), and the resulting metadata standard, to achieve controlled information sharing in a distributed and federated environment. In addition the document discusses the underlying technology and federation issues that are required to provide a practical path to implementation.

Background

Prior to discussing the ABAC concepts, the following table covers the descriptions of terms used throughout this paper.

Term	Definition / Usage
Authentication	Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. In computer networks (including the Internet) authentication is commonly done through the use of logon passwords. Knowledge of the password is assumed to guarantee that the user is authentic. Many transactions require a more stringent authentication process such as biometrics or digital certificates. The use of digital certificates issued and verified by a Certificate Authority (CA) as part of a public key infrastructure is considered likely to become the standard way to perform authentication on the Internet.
Authorisation	Authorisation is the process of giving someone permission to do or have something. In multi-user computer systems, a system administrator defines for the system which users are allowed access to the system and what privileges of use (such as access to which file directories, hours of access, amount of allocated

Term	Definition / Usage
	storage space, and so forth). Assuming that someone has logged in to a computer operating system or application, the system or application may want to identify what resources the user can be given during this session. Thus, authorization is sometimes seen as both the preliminary setting up of permissions by a system administrator and the actual checking of the permission values that have been set up when a user is obtaining access.
Access Control	Access Control is any mechanism by which a system grants or revokes the right to access some data, or perform some action. Once a user has logged in to a system, using some Authentication system, the Access Control mechanism controls what operations the user may or may not make by comparing the User ID to an Access Control database. Access Control systems include: • File permissions, such as create, read, edit or delete on a file server. • Program permissions, such as the right to execute a program on an application server. • Data rights, such as the right to retrieve or update information in a database.
Trusted	Firm reliance on the integrity, ability, or character of a person or thing.

Access Control in Legacy Systems

Traditionally, access control for data sharing in modern applications and system has been Role-based Access Control (RBAC). With RBAC, individuals log on to a system in an assigned role (i.e., user, administrator, etc.) which has been authorised by the appropriate system manager. If a user's credentials allow access to a system, they have access to any information on that system within their role and that does not require an additional logon. The use of RBAC has limited capability because of the number of roles that can be defined and practically managed, and because roles are mostly application specific.

As previously noted, RBAC is based on roles which have been created for particular job functions. The permissions to perform certain operations are assigned to specific application or system roles and then users are assigned these roles, and through these role assignments acquire the permissions to perform particular system functions. Since users are not assigned permissions directly, but only acquire them through their role (or roles), management of individual user rights becomes a matter of simply assigning appropriate roles to the user. While this simplifies common operations, such as adding a user, or changing a user's department, it constrains significantly the access granularity that can be achieved.

The traditional representation of RBAC is shown in Figure 1, where users are assigned to one or more roles and roles may also derive one or more roles (role hierarchy). Figure 1 also shows the extensions to RBAC to cater for dynamic roles.

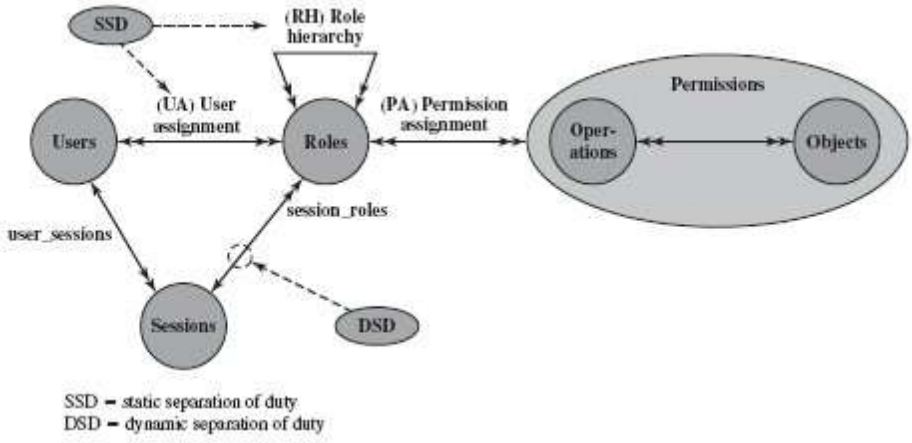


Figure 1 - RBAC Model (Derived from NIST)

RBAC differs from access control lists (ACLs) used in the older Discretionary Access Control (DAC) and Mandatory Access Control (MAC) systems in that it assigns permissions to specific operations with meaning in the organization, rather than to low level data objects. The assignment of permission to perform a particular operation is meaningful, because the operations are granular with meaning within the application. RBAC has been shown to be particularly well suited to Separation of Duties (SoD) requirements, which ensure that two or more people must be involved in authorizing critical operations. An underlying principle of SoD is that no individual should be able to effect a breach of security through dual privilege. By extension, no person may hold a role that exercises audit, control or review authority over another, concurrently held role.

Implementing ABAC

The adoption of ABAC as an information release and management capability requires a significant shift in how information is stored, managed and accessed. Current computer applications and operating systems do not support the management of information in this manner. Traditional operating system access control is based on group membership which is associated with defined functional roles. Because of this limitation to group based access, new information access and storage systems are required to be developed and fielded.

For this paper, a conceptual system based on the use of an Identity Management System, Enterprise Service Bus (ESB), Content Repository and Business Process Management suite has been designed. The concept system allows policy based decisions to be made on the release of information to end users, based on their individual user attributes, rather than just their group membership. A high level visualisation of this concept system is represented in Figure 2.

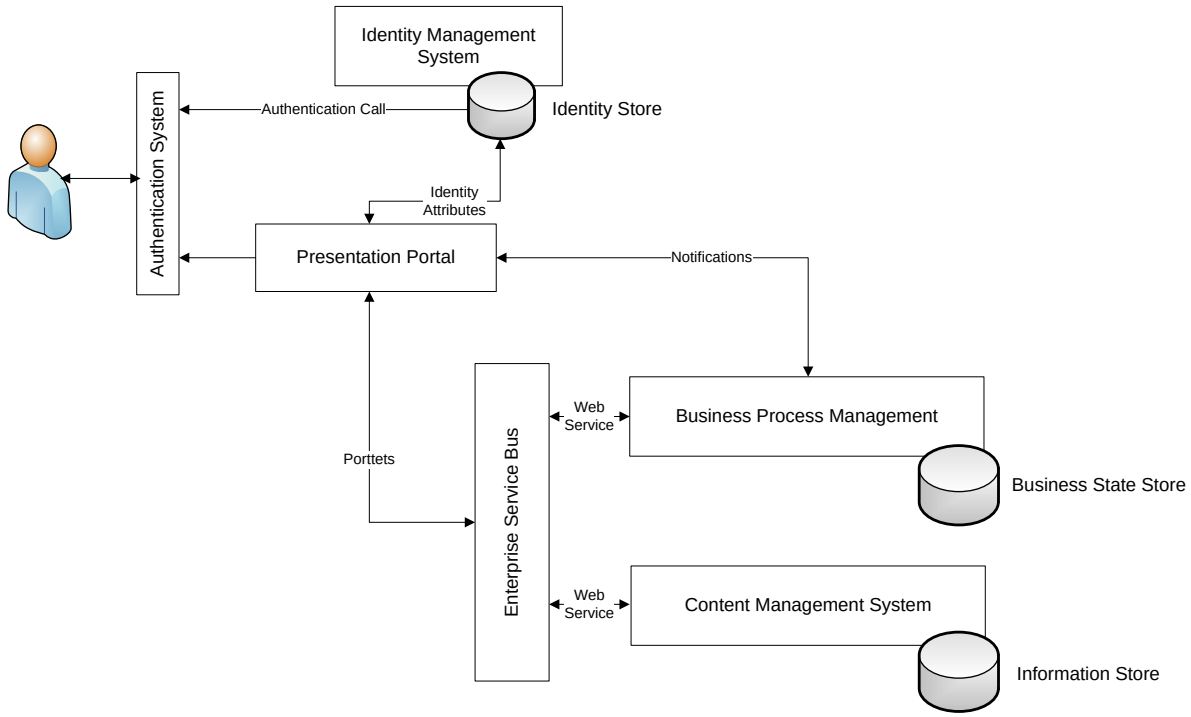


Figure 2 - Conceptual System Diagram

The representative concept system relies on:

1. An Identity Management Capability to register and manage users and to add trusted metadata information to individual records (Authorisation);
2. An Identity store to securely contain identity records and metadata;
3. An Authentication System to ensure that a user is correctly identified to the capability;
4. An Information Content Management system (supported by a database) to store both the actual information and the additional metadata for information;
5. A Business Process Management system to supply the business data (processes) for consumption by the presentation system (portal);
6. A Portal that contains one or more portlets linked to business processes and logic to display information; and
7. An Enterprise Service Bus to act as the orchestration system and service descriptors for the individual elements in the system.

Identity Management Sub-System

The Identity Management Sub-System ensures that people (users) can be dynamically assigned to business defined 'groups' or Communities of Interest. This is done through the collection of 'trusted' information about users. This is in the form of particular metadata (data about data) that characterises a person. In a government environment this will include information about a person such as: citizenship, nationality, security clearance, functional position, role, security briefings etc.

As sensitive information will be released to individuals based on this information, a high level of trust in the process that captures this information is required. Information must be supplied by trusted sources or through trusted processes, stored in a secure identity management repository and validated prior to being published.

In a federated[3] environment, the trust associated with user attributes or metadata is established through the agreement of Federation Agreements, which establish the access protocols, information structure and information releasability of identity information.

Identity Store

As noted in Figure 2, identity information within the local system is required to be controlled by a secure identity store. Traditionally this is through a read-only LDAP directory controlled by an Identity Management (IdM) sub-system. The IdM sub-system controls all write level access to the identity store and ensure that attributes (identity metadata) are controlled and appropriately authorised prior to publication. This may use secondary trusted information stores (a trusted Security Clearance database) or a 2 person integrity process that ensures that any identity changes are entered and authorised by separately authorised users (Separation of Duties).

Figure 3 provides further detail on a IdM Sub-System concept for an ABAC implementation.

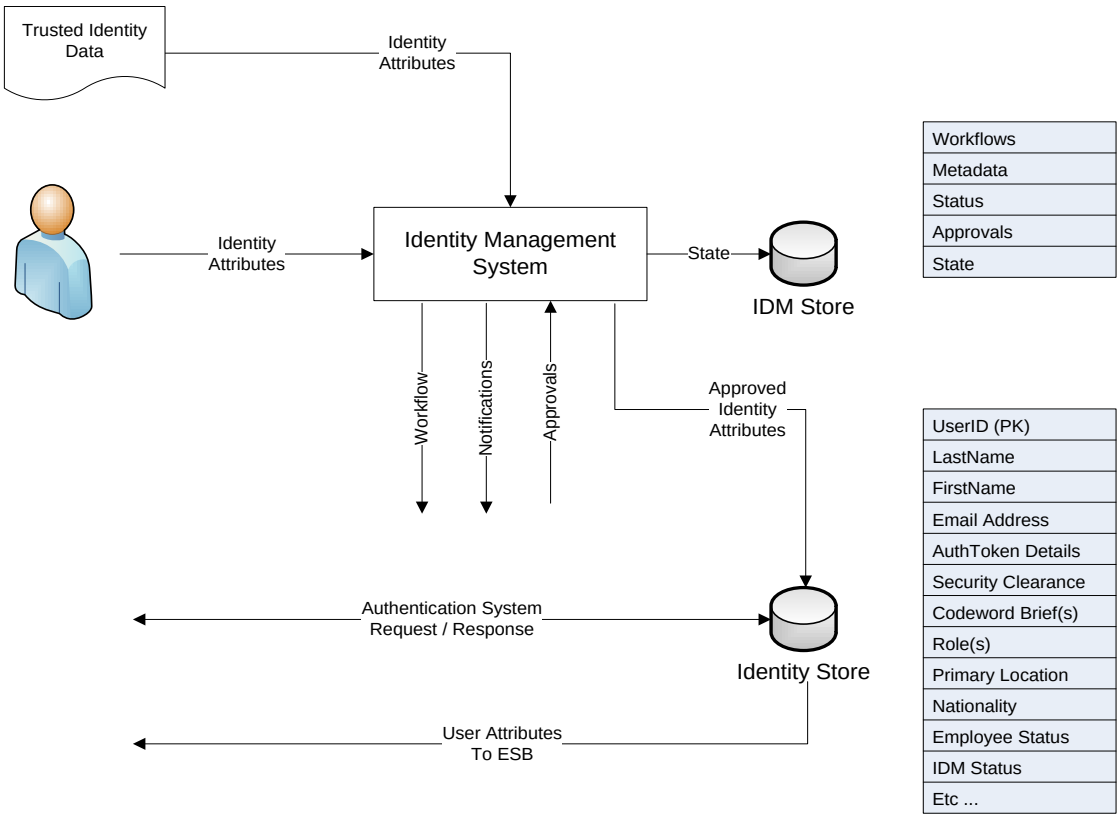


Figure 3 - IdM Concept Diagram

[3] Federated identity, or the "federation" of identity, describes the technologies, standards and use-cases which serve to enable the portability of identity information across otherwise autonomous security domains. The ultimate goal of identity federation is to enable users of one domain to securely access data or systems of another domain seamlessly, and without the need for completely redundant user administration. Identity federation comes in many flavours, including "user-controlled" or "user-centric" scenarios, as well as enterprise controlled or B2B scenarios. Federation is enabled through the use of open industry standards and/or openly published specifications, such that multiple parties can achieve interoperability for common use cases. Typical use-cases involve things such as cross-domain, web-based single sign-on, cross-domain user account provisioning, cross-domain entitlement management and cross-domain user attribute exchange.

Several CoTS solutions already support SoD for identity management and hold accreditation to suitable trust levels (Common Criteria[4] EL 4 or higher) for their workflow and approval processes. These solutions will require additional configuration and the addition of the required attribute information to support the provision of ABAC like information structures.

Authentication Sub-System

An Authentication sub-system will use the information credentials supplied by a user and compare them against the trusted Identity Store (or Identity Federation system) to provide coarse-grained access to system functions and the overall information repository. The Authentication sub-system is the 'gate-keeper' to the information presentation system. The authentication sub-system provides a matching to a preconfigured high level role structure to ensure that a user only receives access to the system resources and functions appropriate to the combined attributes and subsequent derived virtual role.

In a Federated environment, the external user credentials and authentication information will be compared to the information and business processes noted in the registered Federation Agreement. The Federation Agreement will detail the remote authentication source, the mapping information and availability of external metadata and any limitations on the releasability of information or information transformation required. For example; the US Government does not recognise the security classification of RESTRICTED which is in wide use within the Australian Government as a National Security Classification. The US alternative classification is For Official Use Only (FOUO). Within a federated information and identity environment that could exist between the US and Australia, these information fields will need to be dynamically transformed for user access to provide the appropriate metadata information as per the federation agreement. Thus the US will see documents marked as RESTRICTED as a FOUO document and vice versa.

Information / Content Management Sub-System

The Information / Content Management sub-system (CMS) is the overall repository for all information submitted for management and release by the capability managing multi-domain information. The CMS is the solution component that provides a number of critical information management functions or services through the Enterprise Service Bus. These functions must include:

- Storage of collected information metadata in a structured format;
- Controlled search of information and metadata;
- Decomposition of documents and information into semi-structured information based on pre-defined business and information formatting rules;
- Partitioning of decomposed document elements into separate information items with the

[4] Common Criteria. Common Criteria is an accreditation framework in which computer system users specify their security functional and assurance requirements, which vendors implement and/or make claims about the security attributes of their products. Common Criteria accreditation is performed by testing laboratories which evaluate the products to determine if they actually meet the claims. Common Criteria provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard manner.

appropriate metadata and document identity information;

- Presentation of documents and information based on defined business processes / rules; and
- Recreation (re-composting) of documents based on supplied business logic.

The CMS is a critical part of an ABAC capability in that whilst an Identity Management sub-system provides the trusted capture and storage of attributes about users, the CMS does the same for information. Like the IdM sub-system, the CMS is required to be integrated with Business Process Management and the Enterprise Service Bus (ESB). However, the CMS is also required to carry out a wide range of other functions in achieving this collection of attribute information. These include gathering document attribute information from the provided document(s), deconstructing documents to separate paragraphs of different security conditions and re-composting documents to meet display conditions.

Figure 4 depicts a conceptual CMS and the interactions.

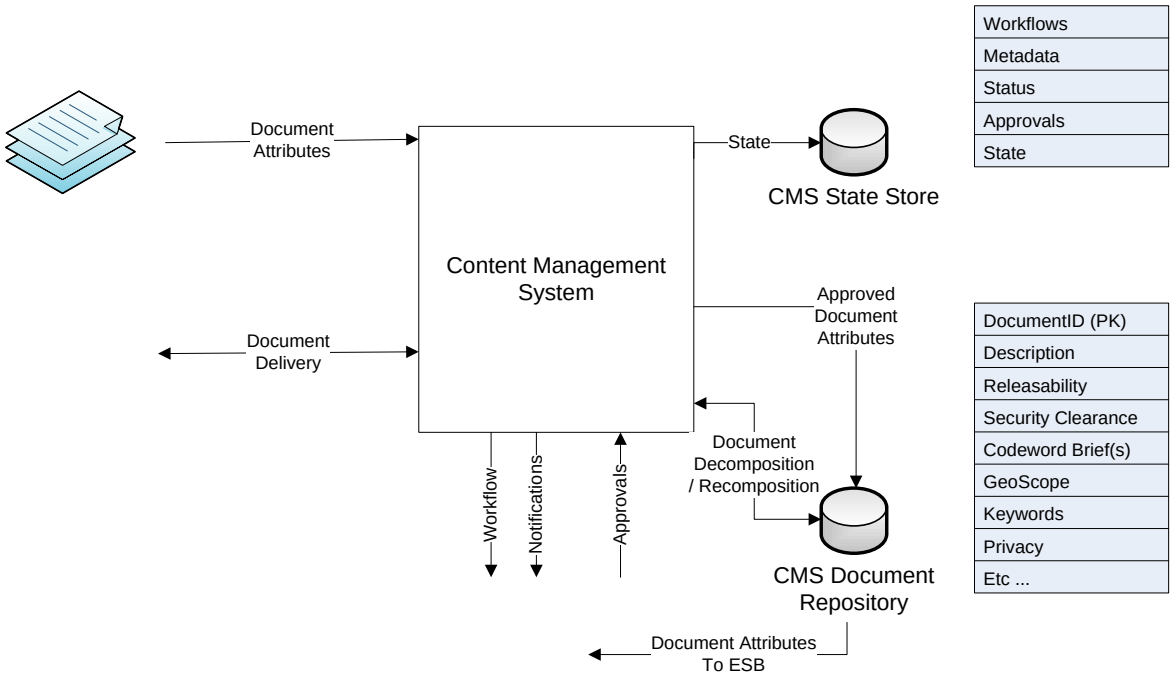


Figure 4 - CMS Conceptual Sub-system

Business Process Management Sub-System

With the separation of access control functionality from a group based structure into a metadata based ABAC structure, defined business processes are the resultant security mediation layer that provides the fine-grained access control to information resources within the Information / Content Management sub-system. Business processes are required to be a positive function where only a complete match with the requirements of the business definition (Community of Interest [CoI] or Information compartment) permits the return of information to the presentation sub-system. To achieve this control the developed business processes must be trusted, controlled, unique and managed.

The concept system presented within this paper is based on a business process sub-system within an Enterprise Service Bus. The business processes are individually created to match the information compartment definitions specified by a series of unique meta-data elements which are then matched by the business process to users within the Identity Store and the information within the CMS. Business processes are validated against specific metadata structures that define a unique information compartment or release structure. A sample business flow is depicted in Figure 5.

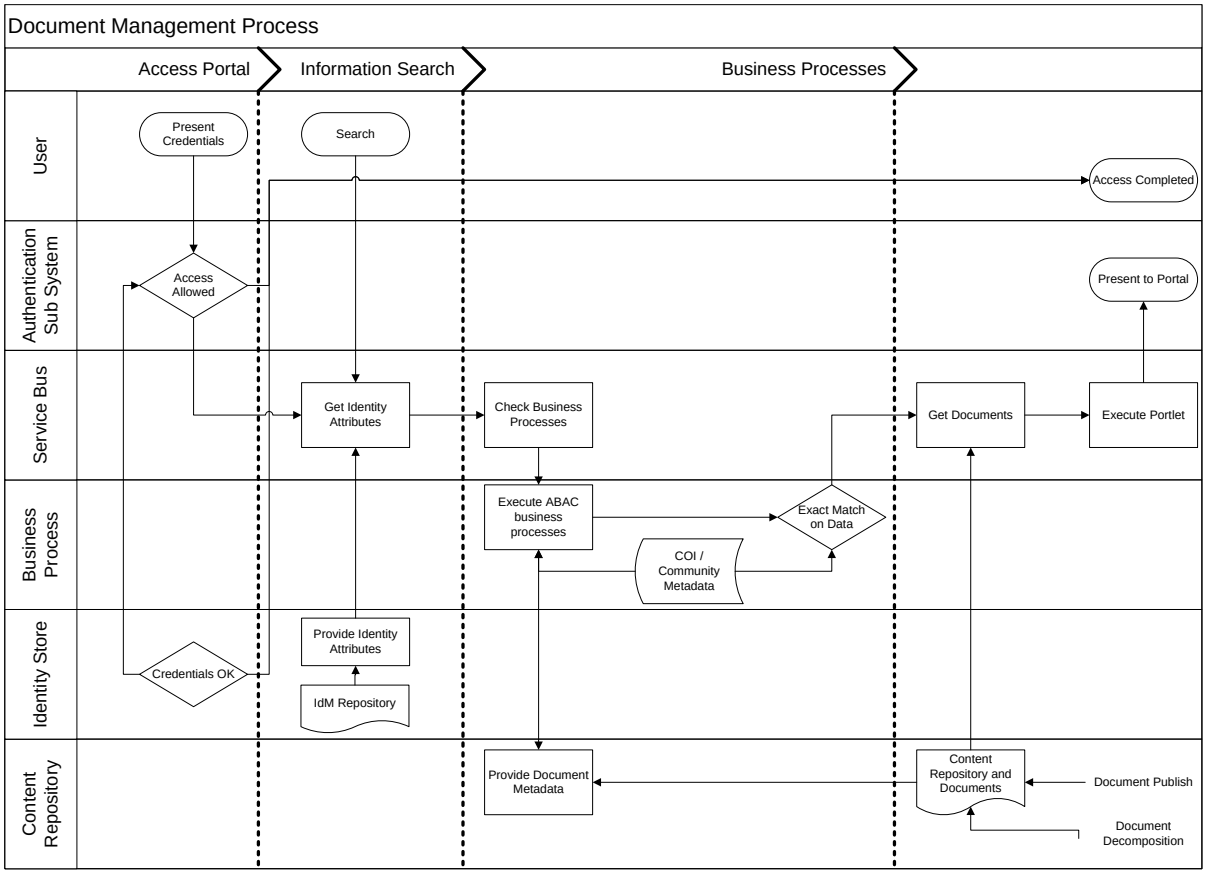


Figure 5 - Document Metadata Matching

The Business Process sub-system supports all of the necessary business logic and workflow management to support the trust required for ensuring that basic identity information and the required metadata are collected and managed.

Business processes can be interactive (requiring user input and action) and derivative (providing control to ESB services). The document matching capability is a derivative process whereby no defined user interaction is required and the ABAC business processes (based on the metadata match of Users and Information) will provide document information to the ESB and Portal. The IdM workflow is an interactive process whereby specific users are notified and required to provide authorisation to enable the completion of the workflow. Another example of an interactive workflow is the document publishing process which will require approval from either the compartment / CoI manager or Security Officer prior to a document being viewable.

A representative diagram for the Identity Management requirements is shown in Figure 6.

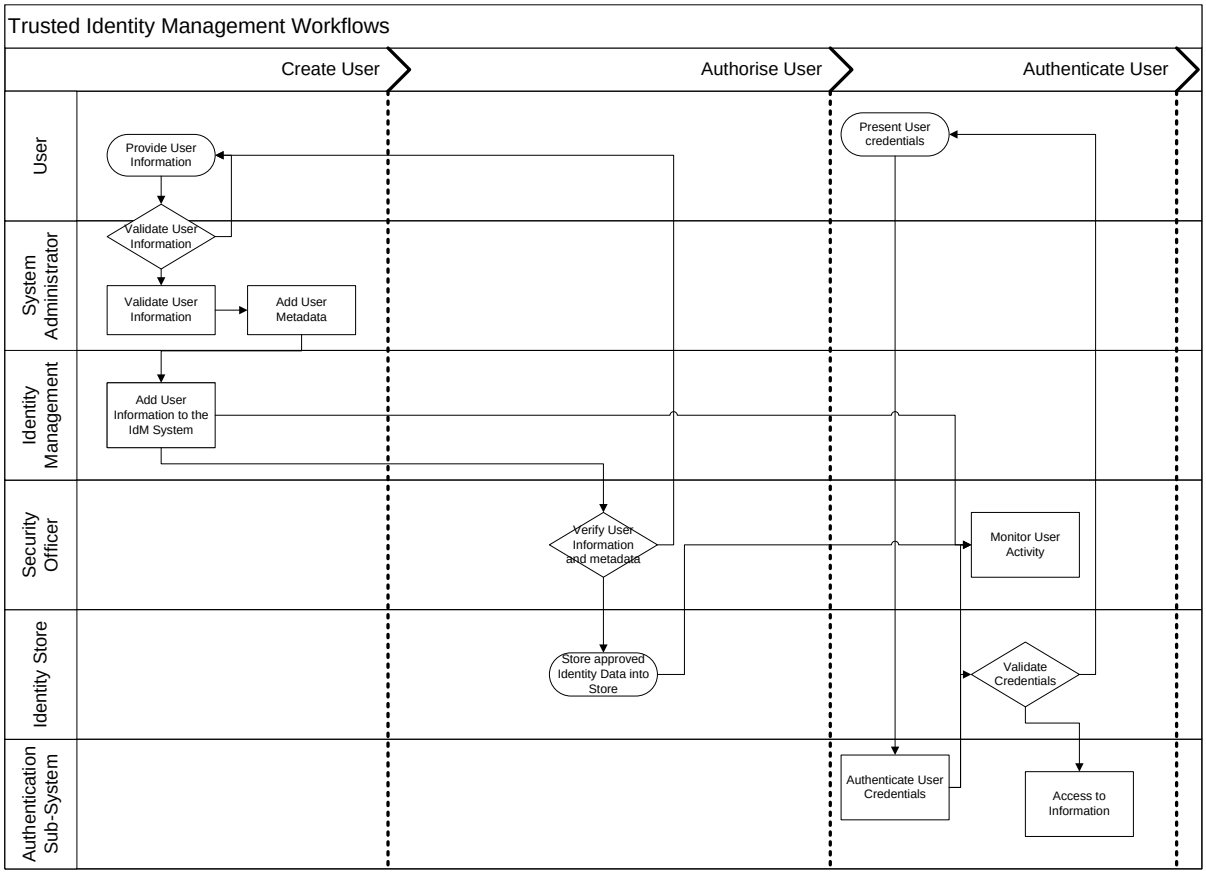


Figure 6 - Identity Management Workflows

Enterprise Service Bus

The component that performs the structured management of information and business processes is the Enterprise Service Bus[5] (ESB). The ESB is the component that provides inter-application messaging, workflow management, business process control, event and message orchestration and application presence management. Within the conceptual ABAC environment, the ESB is a critical functional component as it provides the control for the business processes and ensures that the matching of attributes between people and information is carried out in accordance with the policy.

The ESB will provide the ABAC capability for control of information to users and systems through policy / business processes. As the gatekeeper for cross application information flows, the ESB uses the business process policies to match information from the major sub-system and provide the infrastructure components for the presentation system based on a structured web portal. A diagram showing these concepts is shown in Figure 7.

Expansion of the ESB capabilities would include metadata and information transformation for cross enterprise functionality, integration with messaging systems such as email, IM and VOIP and the federation of systems with multi-language and multi-policy capabilities.

[5] An ESB represents the piece of software that lies between different business applications and enables communication among them. The ESB replaces all direct contact with the applications on the bus, so that all communication takes place via the bus. In order to achieve this objective, the bus must encapsulate the functionality offered by its component applications in a meaningful way.

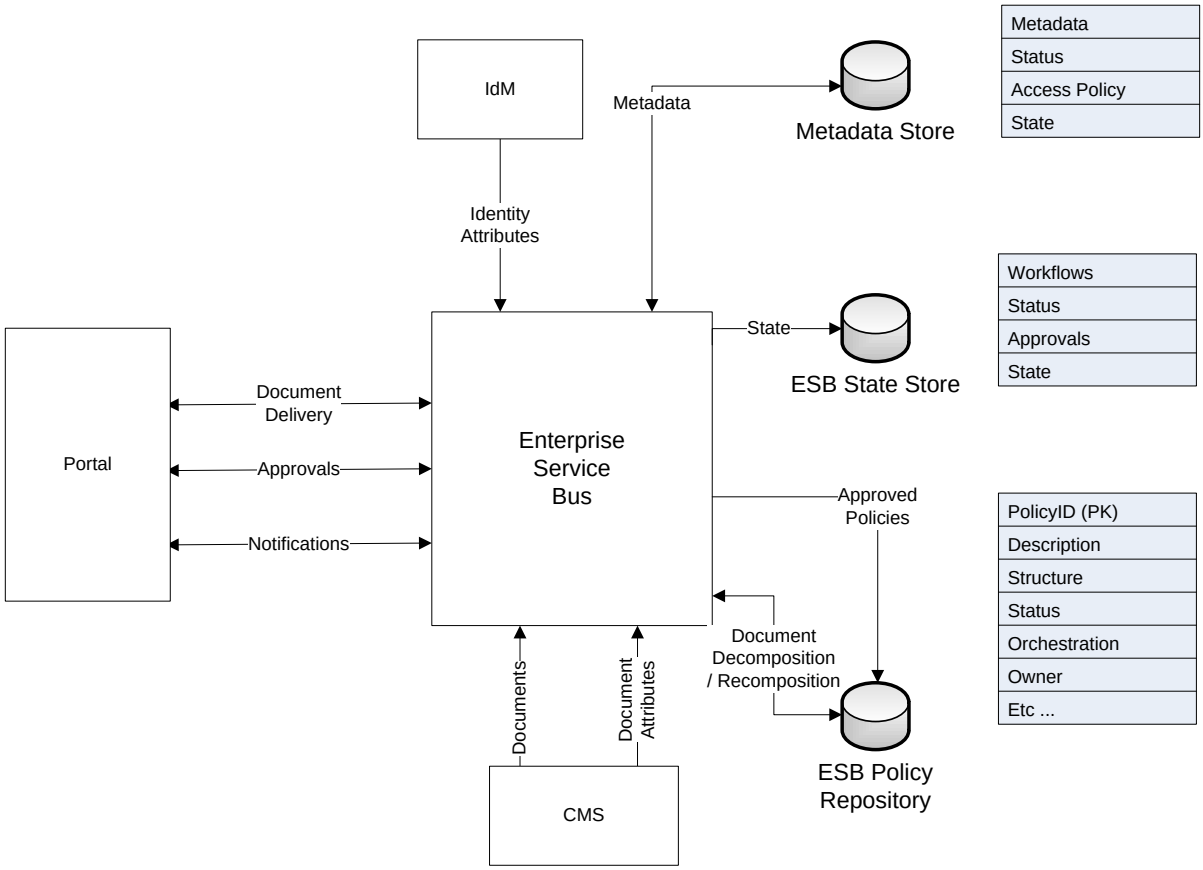


Figure 7 - ESB Conceptual Sub-system

Portal / Presentation Sub-System

The display of information from the ESB is through information portlets displayed within a web portal[6] framework. The portal system virtualises the CMS information and presents the authorised information from the CMS in a standardised manner based on the policy decision contained in the business processes of the ESB.

Attributes (Metadata)

From the descriptions of the overall concept system above, metadata is a critical element which is used by most of the system components to create the environment to allow ABAC. BSTTech has developed a metadata standard that supports nationally classified information within the Defence and Intelligence communities based on the existing Australian Government requirements and US standards including:

- Australian Government Record Keeping Metadata Standard;
- US Department of Defense Metadata Standard (DDMS2); and
- US Intelligence Community Metadata Standard (ICS2).

[6] A web portal presents information from diverse sources in a unified way. Web portals offer services such as search, e-mail, news, stock prices, information, databases and entertainment. Portals provide a way for enterprises to provide a consistent look and feel with access control and procedures for multiple applications and databases, which otherwise would have been different entities altogether.

Whilst this standard provides the overall baseline for ABAC within the Australian Government, additional attributes / elements may well be required to allow true business decisions to be derived and created which will support the dynamic assignment of information to support other Government and Non-Government enterprises. The accurate documentation of these extensions to the metadata standard is an essential element of any trusted information management capability. BSTTech provides consulting services to support the derivation, documentation and implementation of metadata elements to meet these diverse business requirements.

Information Compartments

Because ABAC does not use groups to structure information, a different approach is required. Within this document and the concept system, information is presented in 'compartments' which are defined as a discrete set of information (metadata) elements and the defined taxonomy that is required to be met. Multiple compartments may exist and people can access information based on the resultant metadata set. Figure 8 shows three examples of an Information Compartment definition.

Figure 8 - Information Compartment examples

Conclusion

The ABAC Access Management solution, described in this document, is able to provide highly scalable and structured information management, with a policy based release of information to users, based on a matching of metadata elements between users and information. When properly architected and designed, an ABAC solution is able to provide highly secure (based on a positive match only) information access solution to a wide range of business needs.

Critical to the successful management of information through an ABAC solution is:

1. A defined and structured metadata standard that supports the objectives and aims of the business;
2. The codification of business access policy into an ESB based Business Process/Rule Management system;

3. The integration of Identity Management and Content Management sub-systems with an ESB based Business Process Management system; and
4. The construction of web portlets, based on the business policies coded in the ESB, for the presentation sub-system.

BSTTech provides specialised consulting services and documentation to support the development of an ABAC system for your business. We can document your business processes, discover your information assets and create the infrastructure components for a highly scalable, robust and secure ABAC system.

BSTTech Consulting is an acknowledged specialist in designing, building and managing secure information processing systems. With a number of highly cleared consultants providing a range of services including Project Management, Business Analysis, Systems Architecture and Technology implementation, BSTTech is a one-stop shop for all of your secure information management and sharing needs. A specialist in the design of secure computing and information management, BSTTech Consulting is able to advise and provide systems architectures and implementation strategies to secure critical information.

For more information please visit our website (www.bsttechconsulting.com) or contact us by phone on +61 2 6247 3372.