Multi-Service Operator Service Delivery Platforms (MSO- SDP) and Policy Based Access Control (PBAC)

August 2011

V2.1

Alan Lloyd

Alan.lloyd@wwite.com

Foreword:

This paper is for discussion purposes only and invites feedback. The paper is of a general nature based on design and operational experience with MSO SDPs and PBAC. This paper is not a design specification.

Policy based access control (PBAC) is an emerging engineering methodology in large scale online systems. PBAC represents an outcome of identity and access management (IDM and IAM) developments that been occurring in a evolutionary fashion over the last fifteen to twenty years . MSO SDPs have been evolving over this period too and developing via directory enabled customer centric information system designs, IDM and IAM functionality as per the PBAC methods.

The rationale behind the paper is that many believe that applying new authorization models integrated with customer centric Business Process Modeling (BPM) methods are required in the emerging online marketplaces. The paper presents views in order to create awareness and discussion within your business units, IT planning, security and business process teams.

Contents

Foreword: 1
Executive Summary: 3
Introduction 4
Definitions: 4
AC Contexts: 4
Rule based Access Controls 4
Role Based Access Control - 4
Policy Based Access Controls 4
PBAC and Service Delivery: 5
Contextual Tips. 6
Authentication and Authorization Problem Case Studies: 7
Identity Management 7
The x2x Issues 7
Governance 8
Service Dimension and Self Care Costs 8
Conclusion 9
The New Emerging Authorization Paradigm 9
MSO SDPs and PBAC 9
Implementing PBAC 10
Customer Touch Points 10
PBAC and the SDP Information Model 11
PBAC - the information engineering 12
PBAC - Policies 13
Summary 14
About the Author 14

Executive Summary:

A new authorization paradigm is emerging called "PBAC" (Policy Based Access Control). PBAC allows for the creation of fine grained authorization policies using roles as well as service specific related attributes that define who can access what and when on a system under different situations.

The development of Multi Service Operator – Service Delivery Platforms, where converged personalized self care services are required, have embraced PBAC on the basis that multi faceted, dynamic role based access controls does not serve well in regard to system agility, management and cost

The paper provides the background to:

- customer centric service delivery systems and the way in which Access Control (AC) methods are evolving,
- high level system design scenarios that illustrate how certain system design contexts (without PBAC) can create issues both in system operation and revenue generation and
- why perhaps traditional identity and access management products serve well in some situations, but may not address the larger scale service delivery platform situations.

While it may be considered this paper may be seen as applicable to a multi service operator (MSO) or a CSP, we note that in today's world, governments, the financial sectors, ehealth, outcare, smart energy, smart city, smart transport systems (of scale) all share the same service delivery and user authorization issues. We therefore suggest the PBAC to user authorization should be considered as generalized solution to user management and service delivery issues.

The paper also recommends the use of information and identity engineering doctrines with a focus on governance methodologies and service management functions. While standard data interchange and AC techniques as provided by SOA design methods and XACML (eXtensible Control Markup Language) definitions can be used for service delivery systems, this paper recommends that the overall service delivery and user entitlement designs (PBAC methods) provides the foundation system design elements on which the application of SOA and/or XACML interface technologies can be made.

This paper begins by describing existing application and contexts for Rule Based Access Control (RuBAC) Role Based Access Control (RoBAC) and why PBAC is now required. Several solution design scenarios are then provided to illustrate how service delivery agenda problems could be encountered by not including PBAC capabilities and then finally the paper provides back ground to SDPs and the application of PBAC (service based entitlements).

Introduction

Definitions:

A number of key terms are used in this paper. Terms used in IT can be open to considerable debate, particularly when they are non-technical and represent day to day life styles and subject matter. Therefore the definitions used are as per the English dictionary and are provided here for information. Of note is that service delivery, governance and policy based control systems are used and managed by real people, therefore it is a design requirement with customer centric systems that the language taxonomy used in their software design and implementation reflects the language as used and understood by human users.

- behavior: (n) the manner in which a living organism or physical substance acts under specified circumstances
- entitlement: (n) something to which one is entitled; enable; a right; a privilege
- governance: (n) government; rule; control
- policy: (n) a plan of action; a way of management
- preference: (n) the action of favouring; selection; election
- role: (n) (sociology) the actions or behavior expected from an individual re their group position
- subscriber: (n) one who gives consent, approval or support to (the delivery of services)

AC Contexts:

While Access Control method descriptions can vary, the basic descriptions used by this document are

Rule based Access Controls – A rule, the determination of a processing path based on input conditions and predicates – e.g. If (x = 1) THEN { a, b, c} ELSE { d, e, f} .There is no need to externally measure a rule's performance or its quality, its either determines one thing or another. Rule processing generally underpins higher level AC methods.

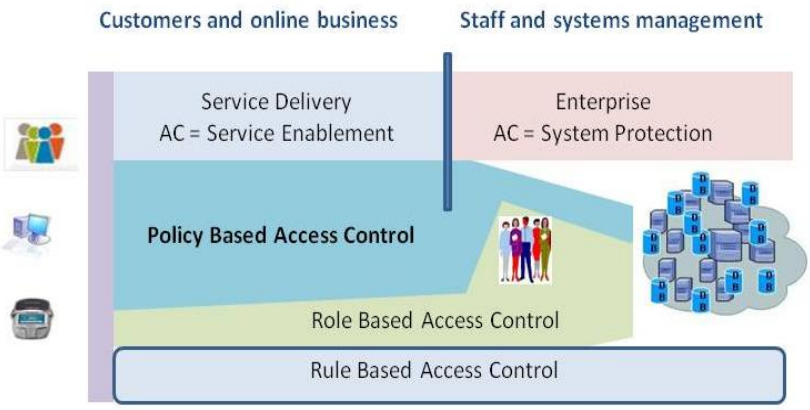
Role Based Access Control - The responsibility assigned to something instantiates their Role, which is then used, governed and tested by other Role based agents (the group). Activity of the role is tested with RoBAC. Roles are useful when the Role in terms of responsibility and performance and the means by which it is measured are stable. Within the CSP-MSO world a critical role is the "account holder" as the creation , management and responsibility of this "role" has considerable amount of personnel process and IT systems support . Managing the "account role" within a CSP-MSO attracts both CAPEX and OPEX.

Multiple role assignments in complex dynamic situations present systems engineering, business process and systems and personnel management issues.

Policy Based Access Controls Allow for the expansion of AC methods into many areas of IT system application be they static or dynamic, for security management or for customer facing functions. PBAC in the context of service delivery for example, allows us to tie service design and service management to

what an online business is trying to achieve with its online customers. Perhaps the critical difference with PBAC is that it requires a system wide approach to how its applied as uniformity of the policy framework means significant cost and implementation efficiencies.

The diagram (right) represents a high level view of AC method contexts and identifies that customer focused service delivery applies PBAC and possibly Role based methods to deliver services, that Role Based AC is generally applied to staff governance and system protection where procedural responsibilities are measured; and that Rules Based AC, because its context is very much "computational", can be applied in any situation.



We note in the diagram that traditionally AC systems are used to protect IT resources, whereas PBAC allows us to enable or entitle services to users and devices even to unknown users and devices.

We also note that the PBAC approach is not competing with Rules based AC and Roles based AC as each AC method has a distinct operational context , it design methods , business management and costs.

PBAC and Service Delivery:

PBAC is applied in the service delivery context for the following reasons.

- An online business needs to attend to governance and accountability to meet privacy, content rating, advertising, disclosure, customer age conditions, customer language, disposition and disability.
- A online business needs to provide services to unknown users and devices, known users, profiled and loyal users and allow for self-care, parental controls and the convergence of online help systems with voice / human supported customer centres.
- An online business system needs to relate to the real world, a world that is overflowing with device, user, content and situational identities, personalisations and governance methods.

For these reasons the design methods surrounding policies relating to access control have come to the fore. The real question might be is; when do they apply and what are the best systems engineering methods for their implementation.

Contextual Tips.

The following contextual tips are provided to assist the application of PBAC in a service delivery environment.

Point of Presence – the user and the system in question.

- In role based AC systems, the point of presence must ensure the role context is kept in order.
- In a customer centric world the application of roles to online customers should be minimal, perhaps the role is only that of an account holder because they are responsible for paying that account. It is widely recognized how much cost, resource and effort goes into looking after and managing the "account holder" of a CSP-MSO.
- Additionally the use of PBAC might say; we don't know the customer as of yet or completely, but if they use some of our services and as time progresses we will get to know each other for mutual benefit.

Governance, Identity and Naming.

- A key aspect of PBAC is that it applies to named items such as services and users or devices or even content. PBAC means the policy itself must have a name under its governance regime and what it enables or protects must also have a name, as does the policy originator (the governance function – the Business Process Management name) and the policy recipient (the governed entity). It follows that defining coherent identity engineering practices across BPM / BRMS and PBAC methods, reduces data mapping and self-care confusion around what the human business processes and the IT systems are and do.

Roles vs Entitlement.

Later in this document we associate information structures with PBAC, the main data structure being Entitlements and the other Preferences. Entitlements list the services a user is allowed to consume from a system. Again this approach amplifies the difference between Roles and PBAC meaning that Roles indicate a measured responsibility, whereas entitlements indicate the services a user or device is allowed to consume as and when they need to. Each AC method has different governance and systems design and service delivery agenda meaning that the information model required for each AC method will depend on where it is applied in the system and why.

PBAC Architectures.

Before designing PBAC architectures at the detailed level, its best to list the common functions and policies across the areas of the governance regime of interest. With SDP's for example, SDPs contain

functions such as self care, service assignment, parental controls, single view, presence and preference management, each of which can apply sub-set policies related to security, entitlement processing, service infrastructure configuration, status management . These sub-set policies require management to as they are explicitly or implicitly associated with the users entitlement – attribute sets.

Authentication and Authorization Problem Case Studies:

In this section we characterize system solution scenarios and their outcomes and why we think PBAC considerations may have assisted the implementation and revenue earning outcome.

Identity Management

Illustrates: Focused design around specific user processes and transaction types.

The company wanted to optimize user and access management and instead of looking at what the online outside-edge of the organization, it used the internal process view in that the CRM contained all the user's information and therefore the architecture proposed was to feed the IDM and IAM services from the CRM.

However, an evaluation of the organisation's outside edge showed that there were account management executives, retailers, third party service providers and devices, all of which authenticated and authorized to many and varied online services. In addition the IDM solution did not include functionality to define services that enabled new users to progressively engage with the organization as a potential customer.

The original design focus dealt with the "user" in an existing account context and how the IDM technology is used to provide user registration management and session control functions.

The x2x Issues

Illustrates: Focused design around specific application architectures and technologies.

The company developed an online business system around a particular application type. Many core applications have been developed to provide a wide range of functional and process management features in order to demonstrate their capability. But in terms of the non-functional areas such as scale, extensibility and throughputs, some new applications have to be upgraded to suit.

The application in question was then supplemented with gateways for the B2B partners and for the public user at large, they were considered as a " transactional users "- a simple transaction type.

The issue of B2B or B2C or C2C or all of the above raised its head because of poor system performance and reliability. Typically in a B2B system where 100 companies may be talking with each other, the transaction volume is low, but the transaction value high. In the B2C model there might be 1 million

users where the transaction volume is high and the transaction value medium to low. In a C2C environment, a social network or online auction system, the information elements run into the millions, the transaction numbers are very high, the value of many transactions are zero and the productive transactions margins quite small.

Examination from a PBAC and end user entitlement perspective may have indicated that the system design at its outset, should have included all of the x2x capabilities.

Governance

Illustrates: Focused design that the business is managing the customer's, regardless.

The solution architecture portrayed product management functions, CRM, Billing, web servers, identity store, IVR, asset management, a data warehouse, and "a customer". Of note is that both the governance and the identity engineering requirements were not shown. Experience is showing that up to 50% of the software in a solution is to deal with its governance. Probably indicating that 50% of the IT budget must directed at the solution's management and AC functions. This software code base might be critical system governance functions such as self-care, single view, online help, auditing. Needless to say the project went over budget, usability came into question and governance from a customer and operator perspective-problematic.

Who is accessing, managing and using the "solution" can addressed by the PBAC design methodology.

Service Dimension and Self Care Costs

Illustrates: A design ideal that all users are "crash dummies and customer care does not matter".

A technology decision was made to buy a " simple solution" and grow that as the user demand increased.

But as demand increased the services crashed under load, meaning that many users experienced the service failure. Sometimes it is assumed that additional hardware solves scaling problems, but that is not always the case. Poor information systems design remains that way regardless of the hardware being used. Continual failures meant that customers became upset (after all they are running their own business too), so they lodged complaints. The initial, solution cost probably $50k. However, the cost and time of the complaints over several years, were much, much larger.

Today, it's not that hard to understand what users do on systems and how many may use the system at one time. Defining service dimensions and using information and identity engineering and PBAC methods provide this perspective of the system and the same time reduce risk in its implementation.

Conclusion

Most of our larger systems such as cars, aircraft, theatres, buses, ships, buildings, etc , are designed for the real world and to accommodate people, a seating capacity and the delivery of services to those seats.

While one might need to know the names and roles of some users there are times when that is not the case, as per the customers in a shop. In all cases though, we simply need to know of their service requirements. This design methodology is applied with multi service operator – service delivery platforms (MSO-SDPs) and its application of PBAC.

The New Emerging Authorization Paradigm

MSO SDPs and PBAC

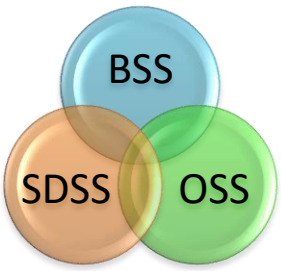
PBAC is generally based on **"Person ⇔ Operational Contexts ⇔ Permissions"** or within the SDP world as **User ⇔Personalised Services ⇔Entitlements ⇔Governance**

In the CSP-MSO domain governance is seen normally in two major contexts .

- BSS - Billing Support Systems
- OSS - Operational Support Systems

This paper applies a third context namely:

- SDSS - Service Delivery Support Systems (MSO-SDPs)



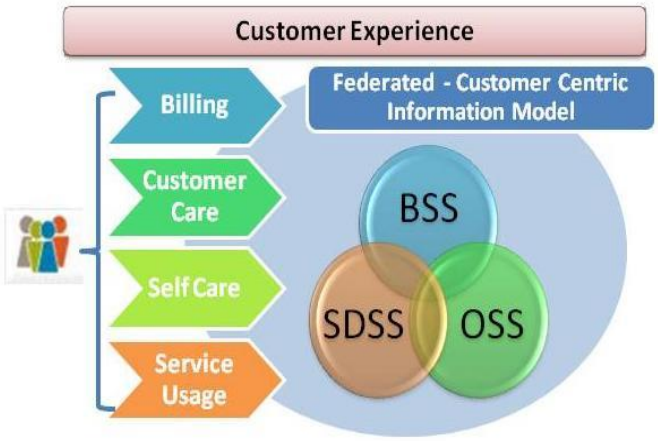
The SDSS governance context is focused on:

- The business and how it delivers online services to customers and business partners in the operational world
- The system's governance being given (in part) to customers under self-care and single view regimes
- That multiple billing, pricing, loyalty offers are made depending on the market situation
- The regulatory needs that operators need to consider how their systems manage emergency services, content classifications, privacy, advertising campaigns, fraudulent use and denial of service and virus threats

- That within the service delivery context there are customer characteristics such as financial status, language, gender, age, disability, location, device types and preferences to consider

Implementing PBAC

PBAC implementation within the service delivery context initially evaluates the outside of a company in terms of customer experience desires and expectations, the customer-organisation **touch points**, the logical and organizational governance structure of the business and the need to work with a federated **information taxonomy** which embraces the services delivery language and the PBAC methods. This language should also align to the organisation's product catalogue(s) and overall operational governance contexts.



The federated language taxonomy is essential as it will be language of the system that the customer's see and use and it will be the language used within the PBAC and service management systems by its implementers.

The diagram highlights the major constructs. The logical governance entities shown are the **Service Delivery support systems**, the **Billing support systems** and the **Operational support systems**

Customer Touch Points

Customers experience their service providers through for example, four touch points. Critical to revenue, cost and growth is the way these touch points are made seamless to the customer and scale. Touch points are not distinct in terms of design, implementation or business and operational dependencies. For example all customer accesses to the operator rely on network services and the billing system relies on the network services for charging records. Self-care, customer care functions can be inter-winded under particular circumstances. For this discussion we describe the four touch points below. Noting that direct access is via interactive web services and indirect access involves voice communication with one or more of the operator's agents.

Direct or indirect access to Account and Billing services

Indirect access to personal information, activation, disconnection, fault resolution procedures, complaints or product purchases

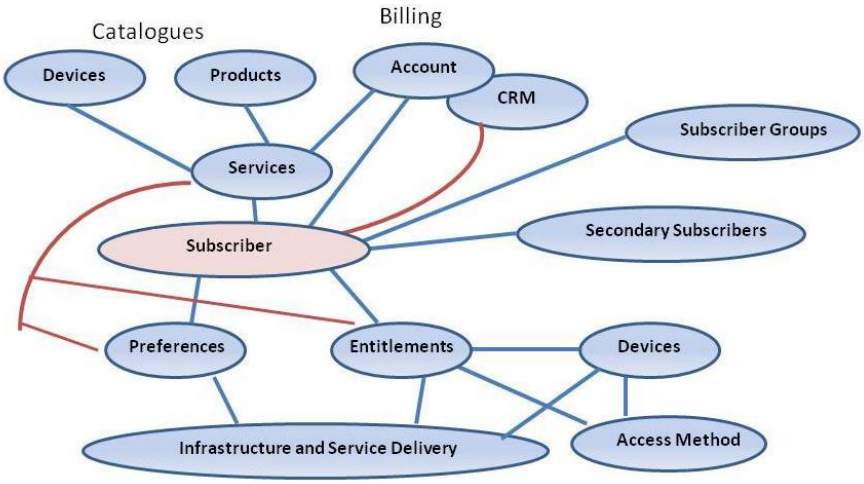
Direct access to L4 services within the operator -e.g. IP service authentication, authorization, web hosting, 3rd party, mail, parental controls, on demand purchasing, catalogues, guides, presence, smart apps, "My Account" services, device management and online help

Access and network services, voice, fixed, cable, mobile, telecoms, IP services , DNS, DHCP, (and SIP), Satellite.

PBAC methods can be used to deal with each touch point for unknown and potential customers, customers that are known that are not directly account holders and customers that are account holders and can verify their identity.

PBAC and the SDP Information Model

Within a MSO SDP a federated "retail specific" information model is applied. This information is designed to represent all the resources and users of the system and is applied to engineering that can scale and perform to the online capacity of the business. A typical and generalized SDP information model is shown in the diagram below . There are other information entities held in an SDP for example name management and product view entities, service event processing and application interface handlers.



The diagram identifies that :

- services are derived from product catalogues, which can include device oriented products,
- that account status from billing can control the service agenda
- that a CRM is made aware of the environment including self-care activities
- that subscribers and possibly groups of subscribers use the system
- that preferences and entitlements are really ordained from services
- that services that are enabled (via entitlements) and the access methods
- that entitled services are used or delivered over the infrastructure

Taking these related into the operational design can mean that:

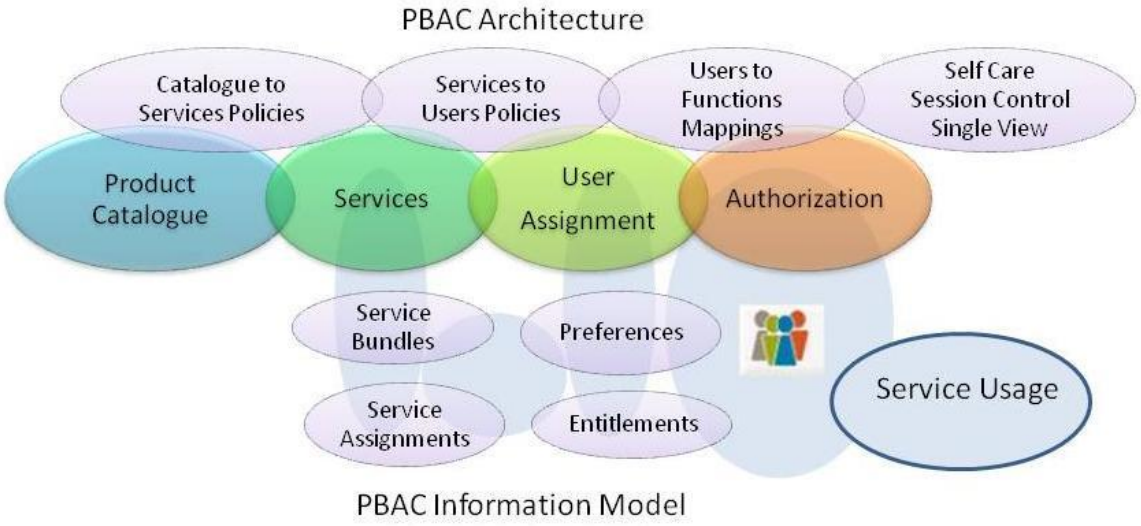
- That product catalogues should also contain information on how services are constructed and how the self-care agenda applies to them.
- That products-services can be for unknown users, specific touch point contexts or user contexts
- That an authorization engine is a design element of a SDP as is its ability to ingest catalogue and service definition information and to understand the system infrastructure on which services are managed and delivered.
- That services also include self-care purchasing, single view services, parental controls, authorization processes and service delivery assignments*.

*Service delivery assignment is the need to place particular users onto particular “physically placed servers” in order to attend to location or capacity requirements.

PBAC - the information engineering

PBAC enables system specifications to include policy entities that are governed, named, described, have behavior, have conditional elements and relational elements. In its most abundant form, a PBAC specification could be applied to every attribute type and value, meaning that with the sophistication of self care converged services systems today both the preference and entitlement information structures should have every attribute related to a PBAC definition. The governance aspects of such definitions are derived from the service and service delivery specifications which in turn are derived from product , device and content catalogues.

The diagram below identifies the linkages from a Product Catalogue through to services, users , authorization and usage. In this diagram service policies of bundling and infrastructure assignment are shown. Service policies are carried through to the users Preferences and Entitlements which in turn are used as Authorization (Access Control) and then service usage.



PBAC - Policies

Policies can be implemented implicitly (in line code) or as part of a policy management architecture that is governed and relates to the linkages of the entities as defined above. Policies if architected have the benefit of being applied in a common way across the whole service delivery dimension of the CSP-MSO, which reduces customized and dedicated developments, code paths, data values, policy constructions..

The diagram (right) provides the major policy definition constructs. Each and every construct can be engineered implicitly as in line code or explicitly as a well defined information processing methodology.

In regard to MSO SDPs and PBAC – these policy entities relate to the services, entitlements, preferences and processes of the authorization and session functions as applied to the users and devices. They are driven from a federated information model, namely the business products and services catalogues.

Summary

This paper has provided several scenarios which highlighted typical issues that enterprises encountered when trying to develop systems where service provisioning and user authorization was required and PBAC was not considered to the fullest.

Businesses in today's environment must adjust their authorization and user and service provisioning strategies to allow for contextual provisioning and authorization and the market place agenda. The architecture for this requires strong business unit support in creating and maintaining the provisioning and service authorization polices. We believe that the use of BPM (Business Process Management) and BRMS (Business Rule Management Systems) tied to self-care Service Delivery functions will become commonplace to drive the creation and maintenance of the PBAC authorization rules over time.

About the Author

Alan Lloyd, Owner, Director and CTO of wwite p/l (Australia). He is a long time player in identity, access and information engineering and has 30+ years experience with international standards and large scale service delivery systems for Defence, Telco/MSO and government infrastructures. Alan has developed a next generation service delivery platform which incorporates entitlement (IAM and PBAC) processing and customer centric governance functions. Alan can be reached at +61 418 536 749 or on alan.lloyd@wwite.com