

Context Based Access Control

An approach for implementing RBAC and beyond



Business Whitepaper

Context Based Access Control

An approach for implementing RBAC and beyond

Author: Hans Scholten

Editors: Peter Valkenburg, Danny De Vreeze

This document is copyrighted (2007) by Everett BV, Wiersedreef 5-7, 3430 ZX Nieuwegein, The Netherlands. Nothing from this document may be used, copied, multiplied, or (electronically) reproduced without prior written consent of an authorised Everett representative.

Contents

1	Introduction	4
2	The case for context based access control	5
3	Evolving from Identity to Role to Context	7
3.1	Identity Based Access Control	7
3.2	Role Based Access Control (RBAC)	7
3.3	Context Based Access Control	8
3.4	CBAC Implementation Considerations	9
4	CBAC Services Architecture	10
4.1	Context Modelling Services	10
4.2	Context Mapping Services	13
4.3	Identity Provisioning Services	14
4.4	Deviation Management Services	14
4.5	Software Provisioning Services	14
4.6	Access Management Services	15
4.7	Logging Services	16
4.8	Auditing & Reporting Services	16
5	Seven frequently asked questions	18
6	Everett	22

1 Introduction

While organisations are becoming more open, regulations are getting tighter. The business landscape is more volatile than ever before and, at the same time, the need to keep ICT in line with business is increasing. Key challenge for ICT is managing the balance between business agility and compliance, within the organisation, but also beyond its boundaries.

Proper access control makes an organisation more agile, and at the same time enables it to comply seamlessly with regulations, whether internal or set by governing bodies. This can be enhanced when Identity & Access Management is implemented as a tactical instrument that looks at the broader context when determining user access rights. This goes beyond regular identity and role based access control.

This paper discusses how to utilise Context Based Access Control (CBAC) to get towards a flexible, yet controlled, ICT landscape. This includes a description of the services required to reach the necessary compliance level, while increasing responsiveness to business needs. It also illustrates a practical approach on how to implement CBAC, based on experience with identity and access management and role based access control.

This paper is primarily targeted at CIOs, CSOs, ICT managers and others that are responsible for aligning and controlling ICT and regulatory compliance. In addition, business management and ICT professionals that are new to access control challenges may find this whitepaper useful.

2 The case for context based access control

Developments in regulatory compliance and the requirement for flexible and cost efficient service access have increased the necessity to introduce a fine-grained approach towards managing access.

The first step in this process is often to make the current situation more manageable by introducing enterprise wide identities and on top of that role based access control. Although these are necessary steps, this does not address the context in which access to a resource is requested. As an example, a finance employee is allowed to access financial data, but not when using a PDA via an unsecured wireless network. To handle situations such as these effectively, context based access control (CBAC) is required. Some specific trends supporting the introduction of context based access control are:

REGULATORY COMPLIANCE: SOX, EUPD, CORPORATE GOVERNANCE

Scandals have led to a wide array of regulations, in particular from the US government and the European Union, that require increasing access control mechanisms. This is particularly the case for financial information and privacy of employee and client information. The Sarbanes–Oxley Act (SOx) for example makes CEOs and CFOs personally liable for producing financial reports that are verifiable and auditable and requires full disclosure of events that are material to business results. Consequently, CxOs need to install control mechanisms to prevent misuse of financial and privacy sensitive data. This brings up the need for tight access control to the relevant systems and, in addition, to create audit trails of all access requests to enable organisations to act effectively in case of any dubious events. As a result, organisations have started to implement identity management frameworks to manage identity data for the various systems. However, identity data alone is not enough. Enforcing the business policies and rules that determine someone's access is as important as providing the identity itself.

SECURITY

Besides regulatory compliance, organisations, particularly the responsible CIOs and Security Officers, are looking for means to improve access security to their systems and data. Boundaries of enterprise IT extend beyond company walls implicating that besides ('trust enforced') employees also clients, vendors and suppliers may have access to these systems from anywhere on the internet. This logically requires a transparent and robust security model around business data and transactions. For when security is compromised, an organisation's intellectual capital may be spread across the world within an instant. From an information security perspective, granting access should be

based on a valid organisational role and must take place in an acceptable context of use.

IMPROVING BUSINESS FACILITATION & SERVICE LEVELS

As markets are changing faster and faster, businesses also need to act faster and faster. This requires an agile ICT environment that can quickly respond to business changes at minimal cost, prompting the integration and optimisation of existing systems into a service oriented architecture. For example, when business is shifting to a multi-channel market approach, ICT should be able to converge and link all the existing separate channels and control access to them. Using an efficient and centrally managed infrastructure where customers and partners are provided with access across the available channels, while adhering to detailed policies of the context of use.

Each of these trends point to the need for both efficient and fine-grained access control. Moving the management of identity data and access policies away from the operational level and putting it on a centralised tactical level makes it more cost efficient. In addition, context based access control allows for the required flexibility while satisfying control requirements. This means that for defining and enforcing business policies one should not only look at what identity a person may have, but also:

- ▶ what roles are performed within the business process,
- ▶ from what location access is attempted,
- ▶ when the service is being accessed,
- ▶ how the service is being accessed (devices & applications used).

In short: one should look at the whole context rather than at a limited set of static user characteristics.

3 Evolving from Identity to Role to Context

The imperative for implementing a secure and flexible access control solution for the entire enterprise is clear. The solution is more complex. With the introduction of identity management it is often assumed that all issues are solved. However additional role based access control (RBAC) beyond straightforward identity based access control is often required. Even then, an important aspect may be missing, namely the context within the request for access is performed. This chapter describes the differences between identity, role and context based access control and explains why RBAC alone is not the silver bullet for solving the agility and compliance challenges in modern organisations.

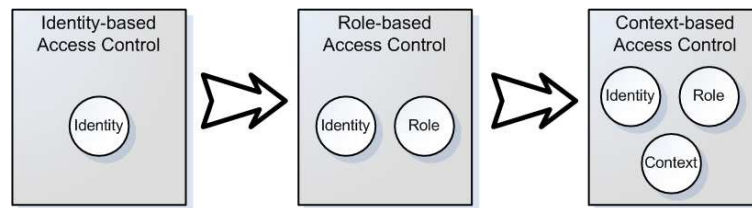


Figure A: The roadmap to context based access control

Figure A shows the roadmap that organisations typically take to implement a solid context based access control (CBAC) environment. Although it is possible to implement a CBAC environment from scratch, there are often too many organisational and technical hurdles to do that successfully. Therefore it is recommended to follow an organisation specific learning curve to keep the stakeholders aligned: business, management and ICT professionals.

3.1 Identity Based Access Control

The starting point for most organisations is to consolidate identity data and to automate the steps for provisioning identity data and access rights. This means that access to all the available systems is still provided on an individual basis, preferably in an automated manner. This is called identity provisioning and can be made as sophisticated as desired, including rules to determine who should have what access to which applications. Together with a coarse-grained, i.e. application level access management solution, this provides a basic identity management system. It could also support self service requests and workflow services to support the process. However, the decisions made during the process are typically based on individual and context-insensitive characteristics.

3.2 Role Based Access Control (RBAC)

The identity based access control described above has the major shortcoming that similar persons could have different access rights, while performing the same organisational role. For example, an inexperienced employee will 'collect' access rights over the years and by the time he leaves the company, as a manager, his successor probably inherits all these access rights for no other reason, than that his

predecessor previously held these rights. One step further, an RBAC approach supplies people with the access rights appropriate to their role, and in addition provides withdrawal of the access rights whenever an employee's role changes.

Another shortcoming of identity based access is that some access rights might conflict with another. For example, someone who is able to order new machines, is probably not the one who is allowed to approve the payment. By granting access on a role level, RBAC can be used to enforce segregation of duty.

A typical difficulty when implementing RBAC, is that the design of the role model is often crippled by a lack of knowledge and experience when translating 'business' roles into operationally relevant 'technical' roles before implementing those into a solution. This often frustrates RBAC implementations or at least lengthens their implementation significantly. Practical approaches for this are discussed in the next paragraph as part of the context modelling process.

3.3 Context Based Access Control

RBAC has many advantages above straightforward identity based access control, but is still lacking important aspects that are necessary for further agility and compliancy. These concern the actual context in which the access request is made. 'Context' includes the identity and role based information required for an access decision, but also describes the situation in which the request was made, for example:

- ▶ Who is requesting access?
- ▶ What role(s) does the requestor have?
- ▶ Which role(s) might conflict regarding this request?
- ▶ What access level is requested?
- ▶ When is the access requested?
- ▶ What device is used to request the access?
- ▶ What software is used to request the access?
- ▶ What is the number of concurrent sessions?
- ▶ From what location is access requested?
- ▶ What network security level is used to access the service?

Therefore the RBAC model needs to be extended with context information. On the access management side where the actual decision is made to grant or revoke access, all the context information needs to be available to make this decision. This typically means the required static information needs to be provisioned to the access management service(s) whenever it is created or updated. At the time of access the necessary dynamic information needs to be retrievable by these services. In addition, having access to particular services may require the distribution of specific software to the user in case of a service or access rights update.

The architecture and implementation of these context based access services is explained in the next chapter.

3.4 CBAC Implementation Considerations

The appropriate approach for implementing CBAC depends on the goals and the available identity management infrastructure. However, given that CBAC supports strategic goals, it is recommended to design for the future, which means planning big, but starting small.

Since CBAC can be quite challenging to implement, it is required that that the organisation, ICT and business, follow a defined learning curve starting with consolidating identity data. This makes it easier to implement more sophisticated topics like roles and context in the future.

It should be kept in mind that the market for context based access control is not mature, and that hence integrated software suites that contain all required services are not yet available. When choosing software, ensure that the architecture allows for missing components that can be filled in later with other products. The typical service components of a CBAC architecture are described below.

4 CBAC Services Architecture

While a large part of implementing context based access control is politics and culture, which has to be carefully managed throughout the implementation process, the solution requires an architecture that supports both the definition and enforcement of access control policies.

In the ideal world there is one Policy Administration Point (PAP) where all access policies and rules are defined, one Policy Decision Point (PDP) that decides on individual access requests and a set of Policy Enforcement Points (PEPs) that completely rely on these to allow or deny access. In the real world however, these administration, decision and enforcement services are spread across various products that overlap in functionality. Consequently, a component architecture is necessary to develop the CBAC service landscape.

In the paragraphs below, the various framework services that form a complete CBAC infrastructure (as depicted in fig. B) are described.

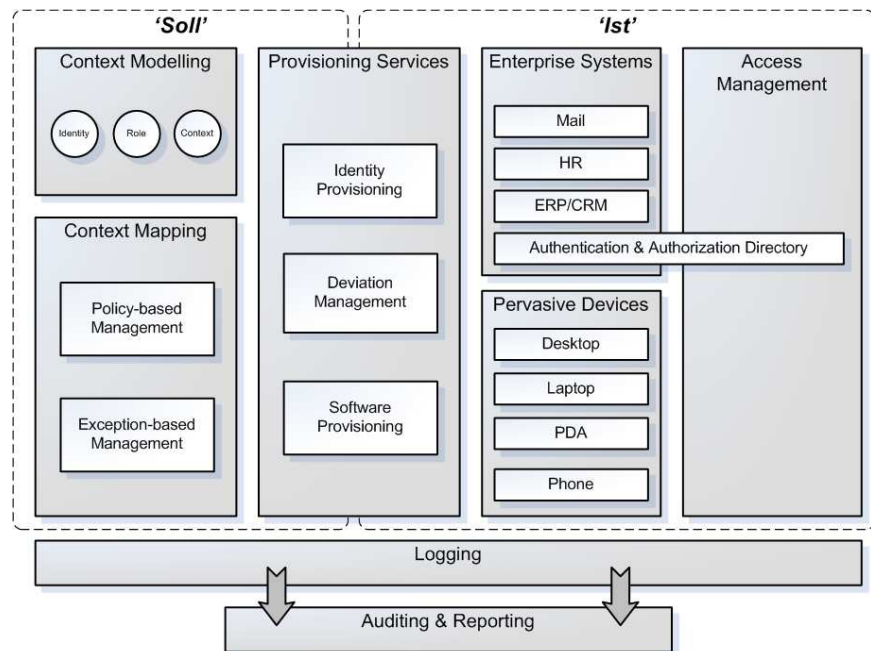


Figure B: The Context Based Access Control architecture including services that form the desired ('Soll') state and actual ('Ist') state of access control

4.1 Context Modelling Services

Context modelling services can be split into two categories: role modelling and context modelling.

Role modelling can be seen from a business angle as a process for determining which access rights a business role should have. Context modelling takes the counterview and looks at what context is required for accessing specific services. This means that 'Role A' only has access to 'Application B' when within the correct context. The example below shows this by comparing the results of an access request based on an identity, a role based and a context based scenario.

Situation: John Smith, CFO and Corporate Finance roles, wants to access one of the financial applications with his PDA over an insecure connection using a username and password.

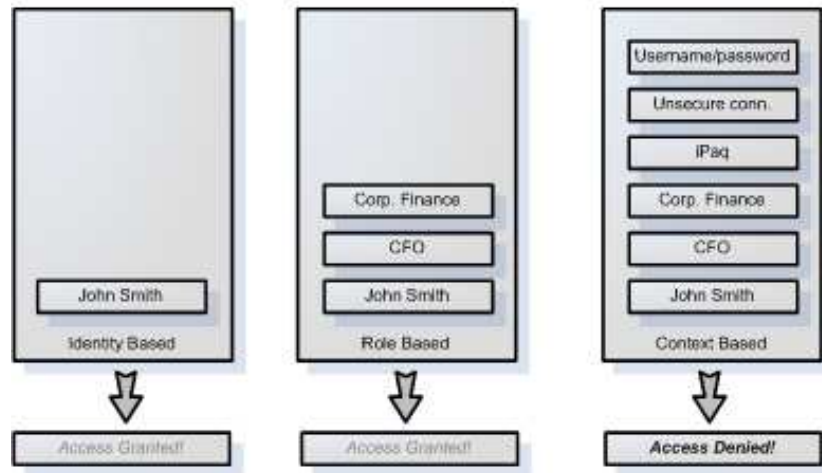


Figure C: Access control decision process

The example shows that a static user based policy (a CFO should have access to the financial application) is overridden with a dynamic device based policy (handhelds are not allowed to access financial data). In an identity or role based setup these are not even part of the decision process.

For modelling the roles one can choose to define roles top-down or bottom-up. Both scenarios have their advantages and disadvantages and a good way to start is to define business roles top-down along organisational lines. Every role inherits characteristics from its ancestor, while excluding any conflicting roles.

When coming down to the application level, one has to look which functions are used within the application. These functions need to be assigned to a specific role. For simple applications this can be done top-down, but for more sophisticated applications this can also be done by the service owner. This last option avoids managing every single access right assignment on an enterprise level. The table below shows an example of this.

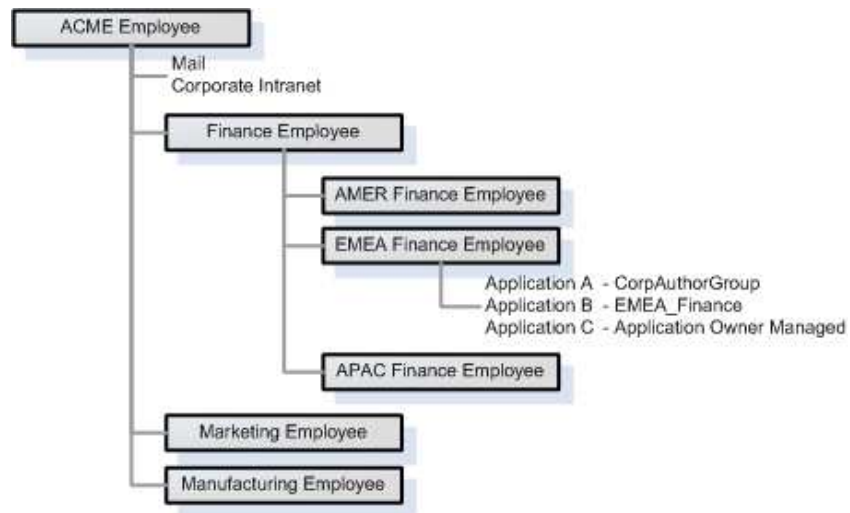


Figure D: Role Modelling Example

For employees that are in the EMEA Finance department, access will be granted to Mail, Corporate Intranet and they will be added to two application specific groups. For application C only the identity is synchronised and the application owner will define the granular access level.

For every role certain characteristics needs to be set in order to work context based, among which:

- ▶ The permissions per system that this role has;
- ▶ The role where this role is inherited from;
- ▶ The roles that conflict with this role and how these conflicts will be resolved (so-called static segregation of duty);
- ▶ The (time) constraints that this role has.

Context Modelling also covers, as mentioned, the application side. Per application it is determined which context characteristics are supported. The access management services will then combine the role information and the context information to decide if access may be granted or not. This is an authorisation process where all required context information is considered. The number of context variables used determines the complexity of this process. It is also possible that the context determines what a user will see. For example, from the internal network a user might see his whole HR profile, but from the internet only basic information is accessible. The example below shows how context (outside roles) might be modelled.

Applications	Corporate Intranet	Corporate Intranet (HR site)	Mail	File Servers	HR System	CRM System
Context						
Authentication	Not Required	Username/ Password	Username/ Password	Username/ Password	Username/ Token	Username/ Token
Channel Availability	Internal	Internal & Internet	Internal & Internet	Internal	Internal	Internal & Internet
Connection Security	Not required	SSL	SSL	Not required	Not required	SSL
Device Bound	Not restricted	Desktop, Laptop, PDA	Not restricted	Desktop, Laptop	Desktop, Laptop	Desktop, Laptop
Time Bound	Not restricted	Not restricted	Not restricted	Not restricted	07:00 – 19:00 mo-fr	Not restricted
Required Software	Internet Explorer 6, Firefox 1.5	Internet Explorer 6, Firefox 1.5	Internet Explorer 6, Firefox 1.5	CIFS	HR Client, Internet Explorer 6, Firefox 1.5	CRM Client, Internet Explorer 6, Firefox 1.5
Concurrent Sessions	Unlimited	Unlimited	Unlimited	Unlimited	1	1

Figure E: Context Modelling Example

Modelling of roles and context can be done using an automated tool or just a simple spreadsheet. Automated tools often help with a number of tasks, for example:

- ▶ provide insight in role-to-user or user-to-role assignments;
- ▶ provide insight in application-context assignments and vice versa;
- ▶ provide insight in role-to-context characteristic assignments and vice versa;
- ▶ provide insight in role-to-permission and permission-to-role assignments;
- ▶ provide insight in role hierarchies and inherited permissions;
- ▶ make it easy to activate/deactivate a role or context characteristic, for example when using time constraints or connection security;
- ▶ Compare and act on differences between the desired state ('Soll') and the actual state ('Ist').

The function of context modelling, whether done with a simple spreadsheet or a sophisticated context modeller, is to provide a Policy Administration Point (PAP) that delivers the input information for the identity provisioning services. These then deliver access rights to one or more Policy Decision Points (PDPs) where the actual access decisions will be made, which are typically individual applications or access management services, as explained below.

4.2 Context Mapping Services

In the context mapping services all the information comes together. The identity data from an authoritative source is mapped against the role information from the modelling services. This mapping is mainly based on business policies and rules and is performed automatically. However, there will always be exceptions to these rules and policies and these will be set and logged within the mapping services. This also applies to role mapping and to context mapping. The latter will be distributed to the

access management services, so these know which applications require which context characteristics.

4.3 Identity Provisioning Services

Identity provisioning services react upon changes in business policies and identity information that come in and execute workflows for distributing the data accordingly. They perform filtering, object/attribute mapping and other transformations to make the identity information suitable for the connected resource. To simplify processing, system connectors are used that are capable of talking to the connected system in a language the system understands. This allows uniform processing of events and allows the implementation to focus on the business policies instead of technology. These connectors are available for all kinds of systems e.g. directories, databases, operating systems or web services.

4.4 Deviation Management Services

It is crucial to have a robust provisioning system that is capable of distributing the desired ('Soll') state out to the various systems, and at the same time gathering the actual ('Ist') state from all these systems. Unless starting a new organisation, there will always be a difference between these two states. The deviation between these states needs to be managed as a known exception or should result in either automated or manual actions, like changing the access rights in the desired state. This needs to be a continuous management cycle as is shown in the figure below:

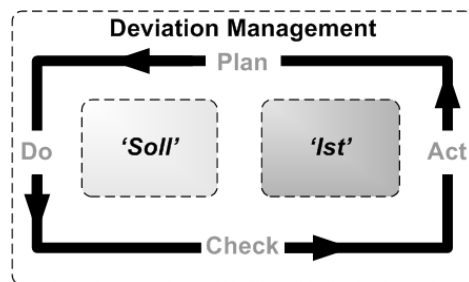


Figure F: The 'Soll' vs. 'Ist' management cycle

4.5 Software Provisioning Services

Besides provisioning of identities to give access to required systems, users often need to be provided with the necessary client software to access the resources they have permission for. This client software not only includes security software, like virus scanners and firewalls, but also configuration settings and security patches that comply with corporate policies. For every type of client (desktop, laptop, PDA) different software and settings may need to be distributed.

When users are assigned to new roles, which require the installation (or removal) of client side software, this can be dealt with automatically by the software provisioning environment.

4.6 Access Management Services

Access management services are available to grant or deny a specific access attempt to a service. In a full context based environment the access decision may be based on static information such as:

- ▶ user identity (username or derived from badge, token, etc.);
- ▶ authentication data (such as password, certificate or biometric information);
- ▶ group and role membership;
- ▶ the day and time the service is allowed to be accessed.

This information can be combined with dynamic information, e.g.:

- ▶ client application used to access the service;
- ▶ minimum patch levels installed
- ▶ the location of the user during the request (office or remote);
- ▶ network security level used (secured wireless, LAN, VPN);
- ▶ the day and time the service is accessed;
- ▶ the other roles of the user that might conflict with the applicable role (dynamic separation of duty);
- ▶ other details about the request (number of copies for printing, viewing of restricted data)

The static information is managed and distributed upfront, but the dynamic information needs to be evaluated every single time a request is made. This allows fine-grained access control, for example, finance employees may view financial data either using their office desktop and network or a PDA while on a holiday, but only when using a secured wireless network.

The access management services can be split up into two categories: client based and server based access management services.

Client side access management means that an agent is installed on the client device that intercepts authentication requests and performs authentication for the user without any intervention. All credentials are synchronised locally, so users are able to work offline.

Server side access management is usually composed of a central access management service that relies on an identity repository such as a directory, with various access management agents on every (web) server that is accessible by end users. If the solution only consists of a central access management module, then this service typically functions as a reverse proxy that includes the policy decision (PDP) and policy enforcement (PEP) functions; if additional agents are part of the solution

then these agents get their access information from the central machine and function as pure PEP components.

The principal component to enforce context based access control is this server side access management, especially for browser based applications or client-server applications that require a secure connection (VPN).

4.7 Logging Services

Even when both the business applications and the context based access control components are secured and access is restricted to authorised persons, it is still important to log security and usage events within the system(s). In case of a security breach, these services allow administrators and security officers to track and trace the problem. The events from all the components should be logged into a central store that can only be accessed by administrators with audit permissions. These will typically not be the same people as the administrators who manage other parts of the environment.

Since log data needs to be kept for a long period of time it is important that the logging data can be easily stored on non-expensive storage media, like tape or DVD. For example, the Sarbanes-Oxley law requires that event data is being stored for a period of 7 years. It is required that during all these years the data can be restored, so it should be independent of technology, product or protocol. Storage in ordinary plain text files is therefore often recommendable.

Because of non-repudiation, all the changes made to the logging database and configuration should also be logged. This makes the whole environment traceable.

4.8 Auditing & Reporting Services

Logging of data is one thing, but after that, the data needs to be transformed into a format, as required by different audiences in the security chain. Some examples of the type of information that needs to be extracted from the log files are:

- ▶ How many users have access to system x ?
- ▶ What users have what roles?
- ▶ Who has permission x on system y ?
- ▶ What are the administrative accounts of system x ?
- ▶ Who had write access to system x last Monday between 2 and 3?
- ▶ Who changed role x ?
- ▶ Who accessed document x in system y via portlet z ?
- ▶ How many users access rights in system x violate policy y ?

To get this kind of information, specific auditing tools can be used or the reporting can be incorporated into tools that are already in use within the organisation.

Important is that the log data is not only secured for write access, but it should also be restricted for read access. The information about all kinds of events in the system should be restricted to the compliancy officer, security officer and related administrators. The log data can be used for forensic research in the event of security or fraud issues.

5 Seven frequently asked questions

1: WHAT IS CONTEXT BASED ACCESS CONTROL?

Context Based Access Control is a process around giving people access to ICT resources. The concept is that people are relevant to an organisation by fulfilling a role that helps the organisation to reach its goals. This includes employees, clients, partners and suppliers.

The role determines what resources a person should have access to and the resource determines what software is required to access these resources. In addition, access control also depends on situation specific characteristics, such as the device, time of request, physical location, client software used, etc..

The combination of identity, role and context characteristics is what makes context based access control more useful in aligning ICT with business than identity based or role based access control alone.

2: HOW DOES CONTEXT BASED ACCESS CONTROL BENEFIT MY ORGANISATION?

The first benefit for any organisation is that access rights will be transparent throughout the enterprise and that the organisation's computing environment becomes more universally available.

Currently, most organisations manually assign access rights and the related software independent of each other and solely based on user ID instead of the role he or she fulfills within the organisation. The introduction of CBAC however, permits access rights or roles that are changing to be made available immediately for everyone and for every resource or application. In addition when people leave the organisation their access to all resources can be revoked instantly.

Another benefit is that ICT will be much more capable of following and supporting business. A change on the business side is immediately reflected in the ICT services without delay by administrator tasks. This not only applies to authorisations alone, but also the situations the company resources can be accessed. Context based access control is also one of the pillars for efficient corporate governance.

3: ARE THERE ANY OUT-OF-THE-BOX SOLUTIONS?

Software vendors are in the process of building suites that contain all of the components, however no single software suite contains all the components today. Market leading identity and access management

vendors have mostly come either from a provisioning or workflow background and they typically provide most of the functionality. The exceptions are typically role & context modelling and mapping components. These are still owned by niche players. To get a full suite including these components one has to integrate multiple vendor products or develop components to fill in all the functionality.

Another component that is lacking in most suites is an integrated software provisioning or software deployment component. Only a few identity management vendors have integrated software provisioning into their software suite. Often, third-party tools have to be introduced to fill this gap.

4: CAN I ACHIEVE COMPLIANCE WITH CONTEXT BASED ACCESS CONTROL?

CBAC is another means in the entire compliance process. Of course it depends on what type of compliance the organisation is trying to reach. For SOx for example, mostly financial systems are important, which results in only a subset of the available systems that have to be incorporated in the access management solution. These systems normally have specific access requirements that are difficult to manage on an organisational level. The solution that is discussed in this paper is to provision identity data down to the role level and let the application administrators perform the last piece of mapping. This implicates that part of the compliance may be difficult to achieve, since it is unknown who has what access rights within the particular system. To deal with this issue, one can identify the systems that are important for the regulations at hand and centrally manage these down to the access rights level instead of the role level or introduce a corporate auditing solution that is able to cope with these systems.

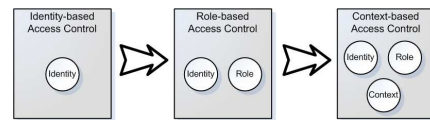
Context based access control makes compliance much easier, but it becomes essential when efficiency and service level are at stake. It is the combination of using automation for modelling roles, provisioning software and identities, workflow and auditing that makes context based access control almost required to have for compliance.

5: WHAT ARE THE BIGGEST PITFALLS DURING IMPLEMENTATION?

Politics and role proliferation. The technical side of context based access control is 'just' implementing software and configuring it according to business policies and roles, but defining these policies and roles and reaching agreement about enforcing these is the time consuming part. When it comes to which roles are required, organisations tend to end up with too many roles to manage. A strategy to control this process is to combine top-down organisational role and policy definition with a bottom-up approach that starts with existing systems and access rights.

6: WHAT DOES A PROJECT OUTLINE LOOK LIKE?

Although there are several ways to start a project or programme to implement context based access control, it is highly recommended



to start with defining a vision on what the end situation should look like. This results in a reference architecture that will be leading during the whole process.

Important aspects of realising context based access control are:

- ▶ **Blue print architecture:** defines the high-level long-term architecture of the identity and access management environment
- ▶ **Roadmap:** defines the steps how the organisation can reach the end situation in an optimal route;
- ▶ **Scoping:** to determine and document what is to be implemented in every single step and why certain choices are made.
- ▶ **Programme Management:** required to control the process of multiple 'independent' projects that are defined within the roadmap.
- ▶ **Transformation Management:** to manage the changes that an organisation will encounter during the programme and to keep all stakeholders aligned.

The actual execution of a project can be set up in different ways and depends on the chosen order in the roadmap. Typically the components can be divided into three implementation areas:

1. Role management
2. Provisioning
3. Access management

The central component is the provisioning component, especially identity provisioning, as this enables the integration of the other services. It is usually beneficial to start with an identity provisioning model to supply identity data to either role management tools or an access management component.

On top of provisioning, software distribution and access management may be added. To speed up the process, it is often recommendable to start role management in parallel as implementation often take time to complete.

As a rule-of-thumb it is recommended to start with a simple identity information model and extend it with role concepts and eventually with the context. As the services need to be auditable, logging typically needs attention from the start and is augmented as services are added.

7: HOW DO I START?

Context based access control is a complex area that touches both ICT and business. In most cases it is a multi-year programme that needs serious attention, not only from project management perspective, but also from business representatives and the CxO-level. The definition of a realistic programme will also benefit from experienced technical and process specialists.

CBAC is more than the introduction of new technology, and often requires a shift of paradigm from management and ICT professionals, in order to view identity and access control as central to the organisation. Consequently, formulation of a strategic vision and goals that identify the business benefits are a crucial first step.

6 Everett

Everett, formerly known as Webflex, is a systems integrator and consultancy firm with highly skilled professionals and unique hands-on experience. Our inspiration is connecting individuals and ICT services in a secure, personalised and demand-triggered way.

However, 'demands' are changing ever faster, requiring ultimate flexibility of ICT-systems. Providing access usually is in conflict with control, governance and privacy. Furthermore, corporate ICT should continuously reassess its past investments in the light of being potentially unique sources for new services, while balancing within the constraints of being auditable, cost-efficient and compliant. Our inspiration has therewith become a boardroom consideration, which will largely determine the success of the organisation.

Everett firmly believes in a middleware solution for this requirement for a controllable and agile ICT environment. New concepts and technologies in that area can provide your organisation with a sustainable -competitive- advantage, in terms of cost control as well as time-to-service. Over the years Everett has proven itself as a leading specialist on SOA integration frameworks and middleware in general and Portal, Secure Remote Access, Search, Identity & Access Management and Enterprise Application Integration technology in particular - an area of expertise that is subject to major new developments on a continuous basis.

We have therefore become a truly innovative company, embracing innovative concepts in the stage that they are 'fit for purpose', when they are *leading edge* rather than *bleeding edge*, however still early in their lifecycle.

We use our vision and knowledge capturing capability to identify which technologies will stand or fail, and which can contribute to an increase of the agility of your ICT services. We are organised in such a way that we know things earlier and better than others.

Since new technology and new concepts bring uncertainty we have adopted methods to absorb this while implementing. Our interactive and iterative methodology embraces change and channels it to the desired result. We will assist you in this process as your consultant, architect, project manager or engineer. As a temporary addition to your team or as a complete project team with a clear mission.

And after we deliver we will not back off. Everett's Advanced Technical Support centre will be available to assist with in-depth expertise to accommodate the appropriate SLA. We strive for thought leadership in our competence and we want to work as a trusted advisor with the early adopters in any industry.

Everett NL, Wiersedreef 5-7, 3430 ZX Nieuwegein, The Netherlands
Everett UK, 55 Station Road, Beaconsfield HP9 1QL, United Kingdom