A trust-based virtual collaborative environment

Michel Kamel, Romain Laborde, François Barrère and Abdelmalek Benzekri
IRIT/SIERA – University Paul Sabatier
{mkamel, laborde, barrere, benzekri}@irit.fr

Journal of Digital Information Management

ABSTRACT: *The concept of Virtual Organisation (VO) is a natural outcome of networks evolution and collaborative work tools growth. In the VIVACE and TSCP projects, we have studied the different issues when setting VOs up. In this paper, we expose requirements and characteristics of VOs through a use case, which was proposed by these two consortiums. Then, we present a secured collaborative environment, which combines attribute based access control models, privilege management infrastructure and identity federation, we have deployed to deal with VO security constraints. This architecture allows organisations to externalise processes such as authenticating remote users to their partners (the users' home organisations). The establishment of such a decentralised management solution implies these organisations to be sufficiently mature to deal with such delegated tasks. We consider the maturity of the security practices deployed within each organisation to choose the trustee organisations between the potential partners. We provide a tool that helps organisations to evaluate their maturity.*

Keywords: : Virtual Organisation, identity federation, PMI, ABAC, ISO/IEC 27000, maturity level

1. Introduction

The concept of virtual organisation (VO) is a direct consequence of the evolution of networks and tools that promote collaborative work. The multipartite projects need to federate experts on different areas and information systems in order to complete the common objective. Building infrastructures needed for the communication between the parties brings many security issues when administrators have to unlock some of the security doors of their information systems.

Bultje et al. have enumerated characteristics of VOs in [1]. VOs are characterised by a network of independent organisations which are geographically fragmented. The characteristic of independence implies the used technologies to allow both human resources and information systems to be shared within a VO and these resources to be fully controlled by the owning organisation. In addition, Bultje et al. complete this definition stating a VO is also characterised by a unique identity and a cooperation based on trust and information technologies shared between the members. As a consequence, a VO is the result of a trust relationship explicitly specified within a closed context, which is the common project/activity.

VO collaborative environments should provide enough flexibility for people to be able to work with it, and security services to allow each organisation to control its assets at any step of the collaborative process, as well. We are currently developing a secure collaborative environment for VO between aeronautical members. This environment should allow people to design specification documents. This work is part of a cooperation between the VIVACE[1] European project and TSCP[2] .

In our solution, we are combining attribute based access control (ABAC) models, privilege management infrastructures (PMIs) and identity federation. This architecture allows organisations to externalise processes such as authenticating remote users to their partners (the users' home organisations). The establishment of such a decentralised management solution implies these organisations to be sufficiently mature to deal with such delegated tasks. We consider the maturity of the security practices deployed within each organisation to select the trustee organisations between the potential partners. We provide a tool that helps organisations to evaluate their maturity and thus, to quantify the level of trust that they can have in their partners.

The rest of the paper is organised as follows. Section 2 describes the context and the requirements of the project. Section 3 presents the architecture of the solution. Section 4 describes the prototype. Within section 5, we introduce the concept of evaluating the maturity level of the security practices deployed within each organisation's Information System in order to identify the trustee partners on which we can rely within such a collaborative environment. Finally, section 6 concludes and states our future work.

2. Presentation of the use case

The use case was initially defined by industrial partners from both VIVACE and TSCP. It depicts a situation where people from different companies wish to collaborate in order to produce a technical aeronautic specification (Figure 1). Each organisation has people with specific skills and software to complete specific tasks. The technical document has to be created by a designer, analysed, and finally validated if no anomalies were detected during the analysis stage (if anomalies are detected, the document is sent back to the designer for correction). This sequence of tasks is structured in a workflow and managed by a conductor.

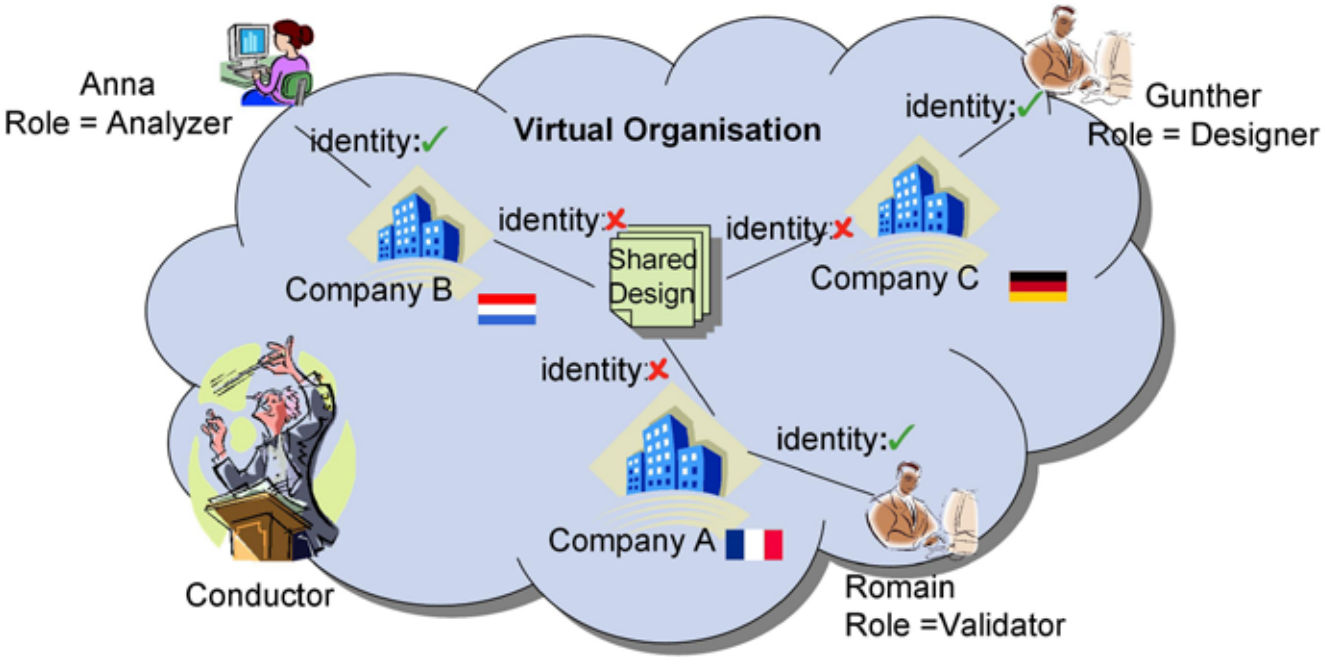
This collaboration is formalised by a contract that states:

- Company A provides analyzers,
- Company B provides designers,
- And company C provides validators.

The contract doesn't report anything about who should perform the job. Each company is responsible for managing its people. It also specifies the four access control policies that control accesses to the shared documents at each step of the design process:

1 Value Improvement through a Virtual Aeronautical Collaborative Enterprise, http://www.vivaceproject.com/
2 Transglobal Secure Collaboration Program, http://tscp.org/

- design-policy states that only designers can read and write on the shared design.
- analysis-policy states that only analyzers can read and write on the shared design.
- validation-policy states that only validators can read and write on the shared design,
- And end-policy states that any VO members, i.e. the designers, the analyzers or the validators, can read the final results.



A WorkFlow Engine (WFE) acts as a conductor. During the design step, it enables design-policy and disables the other policies. When this task is completed, it disables design-policy and enables analysis-policy. Etc. Finally, when the process terminates, the workflow engine informs the participants and grants read access to the shared documents to all of them by enabling end-policy. The WFE is hosted by Company B. 3. Data Generation Process

3. The use case analysis

The Secure Collaborative Environment (SCE) has to integrate the VO characteristics defined in [1]. Thus, it should allow each organisation, member of the VO, to keep control on its assets, i.e., control on the people participating to the VO and control on the resources put at their disposal too. However, if each organisation keeps control on its assets, it has also the associated responsibility (e.g. legal issues).

Consequently, a SCE must provide the tools allowing:

- The specification of the access control policy: in order to implement the policy, the specification language must be flexible so it can take into consideration the concept of roles, largely adopted today, in addition to any other characteristic related to security issues.
- Each organisation to keep control on its assets: on one side, organisations providing human competencies must be able to decide who participates to the VO. The scenario shows that the participating users are not identified by their names; only, their competencies are considered using roles. Only the users' home organisations have the ability to decide who may participate to the VO. Consequently, these organisations which have both authority and responsibility on their human resources within the VO environment, should manage the processes of authenticating and accrediting their people.
- To deal *with the problem of interoperability* between the different authentication and accreditation solutions adopted within organisations: it is not very probable that all organisations use the same technologies or that all these technologies are compatible.

We combine three concepts to respond to these three problems. First, we specify access control policies using the ABAC model. Then, we guarantee the authority and responsibility of each organisation on its assets using the concepts provided by the PMI. Finally, the interoperability problems are treated using the concept of identity federation.

3.1 Policy specification

We apply the ABAC model [18] to specify the access control policy. Contrary to classical models such as Identity Based Access Control (IBAC) [8] or Role Based Access Control (RBAC) [6], ABAC allows the definition of rights based uniquely on attributes. An attribute is any characteristic, relevant in terms of security, associated to a subject, an action, a resource or the environment. This approach brings to the access control solutions more flexibility and extensibility. It is more adequate to the needs of open and distributed systems where the users' identity is no more the unique characteristic taken into consideration for access control.

Thus, the access control policy of our scenario consists of four rules corresponding respectively to design-policy, analysis-policy, validation-policy and end-policy (S, A and R represent respectively the Subject, the Action and the Resource). We provide the design-policy and the end-policy as examples:

role(S) = designer $\wedge$ voagreement(S) = vocontract $\wedge$ (name(A) = read $\vee$ name(A) = write) $\wedge$ name(R) = specification-document $\wedge$ status (R) = await-design means that a user can access the document specification-document with read or write permission if he has the role designer defined within the contract vocontract and the document status is await-design.

role(S) = any ∧ voagreement(S) = vocontract ∧ name(A) = read ∧ name(R) = specification-document ∧ status (R) = validated means that a user can access the document specification-document with read-only permission if he has the role any (here, we are using the concept of role hierarchy where the role any is a sub role of designer, analyzer and validator, i.e. any permission affected to any is also affected to designer, analyzer and validator) defined within the contract vocontract and the document status is validated.

Thus, we are using an attribute called status which will be modified by the WFE. This mechanism allows the WFE to activate or deactivate the access control rules. It is important to use the same mechanisms of access control to protect the document/service allowing only the WFE to modify the status of the document. So, we add the following rule:

role(S) = WFE ∧ voagreement(S) = vocontract ∧ (name(A) = read ∨ name(A) = write) ∧ name(R) = status- specification-document.

3.2 Access control implementation

ABAC policies offer a high flexibility of specification. However, the associated access control mechanisms must be able to control who assigns the attributes values. For example, only Company A can assign the role analyzer in our scenario described in section 2.

Version 4 of the X.509 standard has developed the concept of PMIs. The major component of this specification is the attribute certificate (AC). An AC generalises the identity certificates managed within the Public Key Infrastructures (PKIs) by linking an attribute (a user's identity or its role) to a public key. An AC is signed by an Attribute Authority (AA). The concepts of PMIs and AAs are very relevant in the context of VOs because they offer the means to control the organisations authority and responsibilities:

- The organisations providing human resources by acting as AAs can assign attribute values to their employees and give a guarantee to the organisations providing resources about the fact that they have assigned these attributes to these employees.
- The mechanisms of access control to resources may filter the attributes depending on the AAs that have affected them to users.

For example, Company A is an AA for the value analyzer of the attribute role and for the value *vocontract* of the attribute *voagreement.*

Concerning the status attribute, two possibilities are considered:

- The WFE is the AA because it modifies the value of the attribute status, or,
- The AA is the mechanism controlling the modifications realised by the WFE.

The choice about who the AA is, depends on a strategic level based on the concepts of both authority and responsibility of partners. It must be defined within the contract.

3.3 Harmonising the information of authentication and accreditation

One of the major problems related to VOs consists in defining a harmonisation framework of the information needed for authenticating and accrediting users within this distributed environment. In fact, because a VO is composed of independent partners, each partner may have its own technology for managing/storing authentication and accreditation information that could be different from the one used by its partners. For example, authentication may be carried out by means of username/password couples, digital certificates, biometric techniques, etc using different protocols such as TACACS+, RADIUS, Kerberos, etc.

Traditionally, a site providing a service (SP- Service Provider) implements the authentication and accreditation mechanisms. Each time a user wishes to access a new resource provided by a new SP, a new user account should be created and managed. As a user may belong to an organisation that is different from the SP organisation, some information should be exchanged between the organisations administrators (the SP asks for information about the user, creates the user account, and sends connection information to the user). In addition, the user has to remember a number of passwords equal to the number of SPs managing the resources that he wishes to access, which complexifies the tasks of the users and the administrators.

A new concept, called identity federation, is adopted to harmonise the information of authentication and accreditation between partners. Identity federation is the sharing of digital identities to enable applications in different security domains to work together securely. Federation enables users and applications to work seamlessly as if they were part of the same security domain. It may be seen as a circle of trust between security domains where each domain accepts accreditations from other domains.

Mainly, two approaches exist for this information exchange. The first approach is developed by the Liberty Alliance Consortium [15]. The second approach, developed by Internet2 within the framework of the Shibboleth project [17], distinguishes two entities: the Identity Provider (IdP) and the SP. The users' accounts are managed uniquely by their home organisations, i.e., their IdPs. When a user is authenticated against its IdP, the IdP informs the SP by sending him a proof of the user authentication and his accreditations. These two specifications use the Security Assertion Markup Language (SAML) defined by the OASIS [16] as a protocol to exchange security information.

Shibboleth is the best solution in our context because it is based on the SAML standard and its approach responds to the structure needs where users have to remain dependent of their home organisations.

4. The prototype

The secure environment we have deployed exploits two technologies: Shibboleth provides a harmonisation of authentication and accreditation information, and, PERMIS as the PMI.

4.1 Shibboleth

Shibboleth is standard-based open source middleware software, which provides Web Single Sign On (SSO) across or within organisational boundaries. It provides mechanisms for users to access remote resources via authentication at their home site and authorisation via a set of user attributes provided by the home site (Figure 2).

Shibboleth includes a framework that allows the members of a VO to authenticate once to the VO (via their home site), and then to move between the different computer systems and services of the VO, that may be physically located at different members sites, without needing to authenticate again. In addition, Shibboleth allows a user's attributes to be retrieved from the home site, and for these to be used in authorisation decisions at remote sites. Figure 2 shows the information exchanges within the Shibboleth architecture allowing the web service to take the authorisation decision. The web service could make use of software such as PERMIS to determine which privileges to grant to the user, based on his attributes.

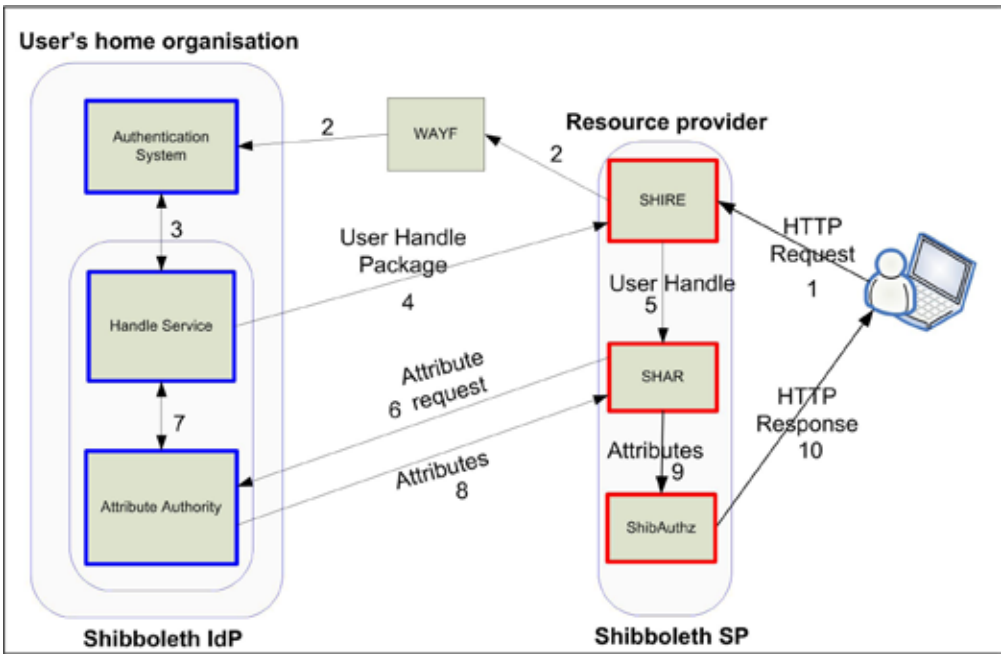


Figure 2. The Shibboleth authentication and authorisation framework

4.2 PERMIS

PERMIS is a PMI developed by the ISSRG team of the University of Kent [3]. The core of PERMIS is mainly composed of two entities: the PDP (Policy Decision Point) making access control decisions according to a given policy and the PEP (Policy Enforcement Point) implementing the decisions taken by the PDP (Figure 3).

The PERMIS project provides a higher-level policy and authorisation framework for the creation and management of a distributed authorisation infrastructure using X.509 standard ACs to hold users' roles. PERMIS implements hierarchical RBAC as defined in the NIST RBAC model, whereby superior roles inherit the privileges of subordinate roles. Administrators at various sites in a VO may allocate roles (or other attributes) to their users, in the form of X.509 ACs, and store these in a local (or remote) LDAP directory.

The manager of a VO resource (the Target Manager) determines the authorisation policy for the target resources under his control. This authorisation policy is written in XML and stored within the target resource.

When a user attempts to access a target resource, the application gateway (typically a web server) traps the user's request; authenticates the user in an application dependent way and then call the PERMIS decision engine to find out if the user is authorised to perform the requested action on the target or not.

Access control decisions are made according to the authorisation policy currently in force, the roles currently valid for the user, the target being accessed, the action being requested, and environmental variables such as time of day.

PERMIS is not hard coded with the authorisation rules. Administrators can change the policy for an application, which in turn will change PERMIS authorisation decision results. Changing policies will not require any change of the applications implementation or any recompiling of the applications.

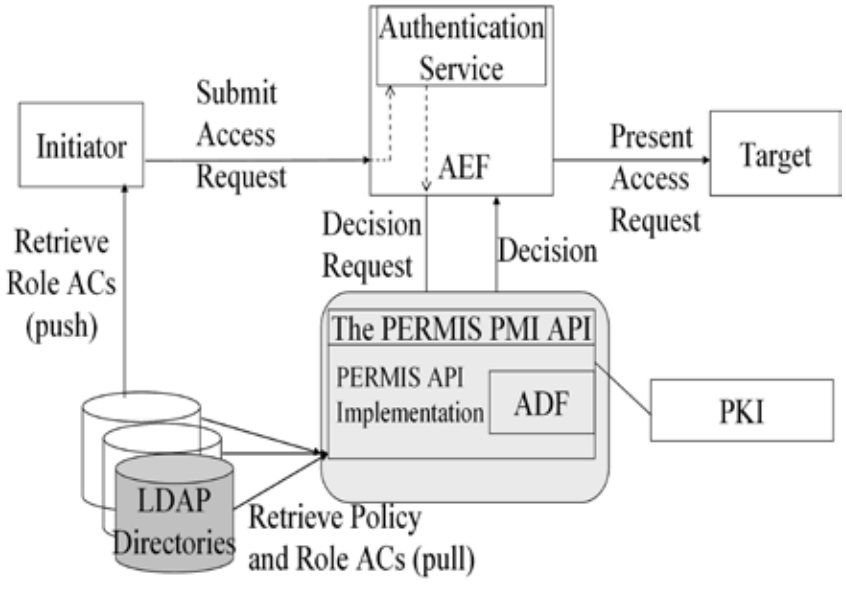


Figure 3: Case Study Implementation of data supplyment process

System administrators write policies, specifying what roles have what privileges, and what kind of credentials will be recognised by PERMIS. Attribute administrators will issue credentials containing users' attributes, telling what roles the users have.

On the request of accessing protected resources, the user's credentials are analysed by PERMIS (especially the AA), and only those that can be validated by the credential validation rules in the policy will be recognised. Then PERMIS uses the association of roles and privileges as specified in the policy, and the association of users and roles as specified in the recognised credentials, and the requested actions and the resource, to render an authorisation decision.

However, PERMIS being initially conceived to implement RBAC policies only recognises attributes that are the users' roles. Actually, the way roles have been implemented within PERMIS allows specifying any attributes for the users. But, PERMIS doesn't recognise resources attributes, which is required in our use case.

Thus, we extended PERMIS so that we can specify and implement ABAC policies. This new version of PERMIS takes into consideration any possible attribute of managed resources (in our example, the attribute status). Attributes of resources are specified in an XML file. Each element provides the name of the resource and the set of attributes. Figure 5 is the specification of the attributes of the resources in our use case. The first element MyResource states any files/ directories within http://sp.example.org/secure have one attribute, named status, and its current value is await-design. The second element is just an example that explains how to specify attributes of resources.

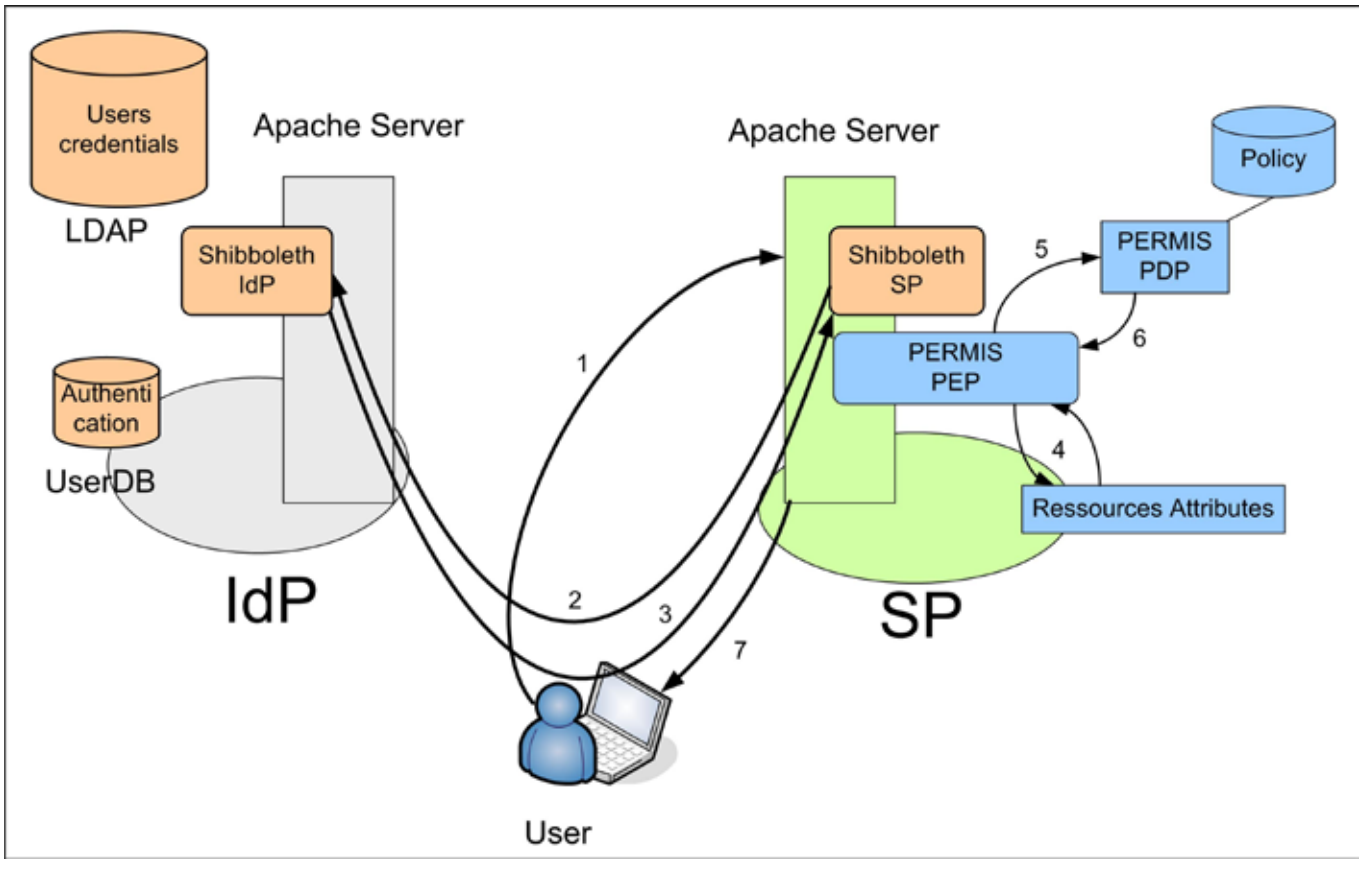


Figure 4. Architecture of the secured collaborative environment

```
<MyResource Id = http://sp.example.org/secure Attributes = {status=await-design;}/>
<MyResource Id = http://sp.example.org/other-dir/file.html
Attributes = {single-attribute=test1; multi-attribute={attr1, attr2, attr3};}/>
```

Figure 5. Definition of attributes of resources

4.3 The secured collaborative environment

In order to highlight the flexibility of our architecture, we have chosen a use case where the IdP manages authentication and accreditation information differently. The authentication is realised using the classical authentication module of Apache. The users' accreditations, protected within ACs, are stored within an LDAP repository. By signing these certificates, the administrator of the organisation, acting as the IdP, is considered as the AA. During the phase of access control on the SP side, the considered attributes are the only ones signed by trusted AAs which authority is recognised on these attributes.

Figure 4 illustrates the different messages exchanged when a user requests the access to a resource (user means real person or software):

1. The user requests access to resource R hosted by SP
2. The shibboleth SP module redirects the user to its IdP to authenticate itself. When SP knows only one IdP, this redirection is done automatically. In general, when SP

knows many IdPs, the redirection is done thanks to a Where Are You From (WAYF) module.

3. When the user is authenticated, IdP generates a SAML assertion that contains a statement indicating the user has been authenticated and the user's credentials inside an AC. This assertion is sent, through the user, to the shibboleth SP module that decodes the SAML assertion and forwards the credentials to PERMIS.
4. The PEP gets the attributes of resource R.
5. The PEP sends the request to the PDP. The request includes the attributes of the user, the attributes of resource R and the name of the action.
6. The PDP takes its decision according to the access control policy. For each attribute, it checks if the AA is known. Then, the decision is returned to the PEP.
7. Based on the decision of the PDP, the PEP makes Apache to accept or refuse the user's request.

Whatever the user is, the authentication/authorisation process is identical. We have written different PHP web pages for both:

- The shared environment (sp.example.org/secure) that contains all the specification documents created by the designers, analyzers and validators.
- The WFE administration interface that allows the workflow engine to modify the value of attribute status of the shared environment.

The current version of our collaborative environment is limited to the set of actions specified by the protocol HTTP [7]. Hence, action read is HTTP-GET and action write is HTTP-POST. The choice of HTTP and PHP web pages as well is due to some implementation issues.

4.4 Discussion

This solution provides flexibility to users management because SPs delegate both authentication and accreditation processes to IdPs, which means every organisation is responsible of its assets and SPs lose the entire control of who accesses their resources. As a consequence, SPs should trust IdPs and be sure they are implementing the necessary security practices (for authentication and accreditation) to not downgrade their own security. Based on the scenario provided in Figure 1, let us suppose that "Gunther" coming from "Company C" wants to access resources provided by "Company A and B". Thus, by adopting our solution based on identity federation and PMI, "Company C" acts as an IdP for its employees. But, what if "Company C" has a non mature identity management process where employees can have accounts without any vetting or proofing functionalities? How will "Company A" and "Company B" accept to open their information systems to the employees coming from "Company C"? In such cases, "Company A" and "Company B" would prefer to manage by themselves the users coming from "Company C". Thus, the organisations need to quantify the level of trust that they may have in their partners directly related to the security practices deployed within their information systems in order to decide how to deal with them. As a response, we defined a tool based on the ISO/IEC 27002 [12] and ISO/IEC 27001[2]. This tool calculates the maturity level of each partner in a VO.

5. Maturity level evaluation of partners

Many concepts are used in order to help organisations to respond to the question about if a potential partner is a trustee organisation. We have adopted the concepts of Information Security Management Systems (ISMS) [11], the ISO/IEC 27002 and 27001 standards dealing with information security and the maturity level concepts [13] [14].

5.1 Concepts related to maturity

5.1.1 ISMS

Today, new concepts allow organisations to address security as an integrated system named ISMS like the management systems used within organisations to develop their policies (quality, environmental, etc.) [2]. ISMS includes all the policies, procedures, plans, processes, practices, roles, responsibilities, resources, and structures that are used to protect and preserve information. It includes all of the elements that organisations use to manage and control their information security risks. When an organisation is part of a VO network, managing its ISMS becomes harder. Thus, international standards such as ISO/IEC 27001 and ISO/IEC 27002 and conformance to them allow setting up a common ISMS view and help to avoid security breaches.

5.1.2 ISO/IEC 27002

ISO/IEC 27002 (formerly known as ISO/IEC 17799) appeared in April 2007 as a part of the ISO/IEC 27000 series. ISO/IEC 27002 does not propose any changes to ISO/IEC 17799 unless the name of the standard. ISO/IEC 27002 is the code of practice for information security management. It lays out a well structured set of controls to address information security risks, covering confidentiality, integrity and availability aspects. This standard contains eleven main sections or security themes ("Security policy", "Organising information security", "Access control", etc.).

Because ISO/IEC 27002 does not say how to apply these best practices, ISO/IEC 27001 is adopted to instruct people in charge of the security within organisations how to manage an ISMS.

5.1.3 ISO/IEC 27001

ISO/IEC 27001 completes ISO/IEC 27002 and has the basic objective to help the administrators within organisations to establish and maintain an effective information management system using a continual improvement approach known as the Plan-Do-Check-Act model. Through this approach, ISO 27001 allows to establish, implement, review and enhance the organisation ISMS.

Neither ISO/IEC 27001 nor ISO/IEC 27002 does consider security levels. They do not allow expressing granularities when evaluating existing security practices. In order to evaluate the deployed security practices within each organisation, called here ISMS, we introduced the concept of maturity level integrated to the concept of security practices.

5.1.4 Maturity level

The maturity of security practices defines how well are the security issues treated within an organisation and evaluates the experience that the security administrators have. We have adopted the concept of levels to evaluate the maturity of the security practices. Thus, the concept of maturity level provides a way for evaluating the ISMS of organisations.

Reference models such as the Information Security Management Maturity Model (ISM3) [10] and the Capability Maturity Model Integration (CMMI) [4] treat the maturity level criterion. But, these models are adopting a process-oriented approach. We prefer to adopt the best-practices oriented approach based on the ISO/IEC 27002 standard so we can have more granularity by considering the security practices implemented and not the security processes adopted on a higher level within the organisation Information System. We propose five levels, ranging from 1 to 5, for the maturity of security practices in order to evaluate the efficiency of the

deployed practices in ensuring security services within the organisation network. The five defined levels are:

• Level 1 - Initial

The security level within the organisation network is very low: the level of risks the organisation assets are facing is very high which may cause their loss or their destruction.

• Level 2 - Minimal

The security practices deployed within the organisation allows it to benefit from a minimal level of security protecting its assets. Although some security practices are deployed, it is not sufficient for an organisation to consider that its infrastructure is protected from attacks.

• Level 3 - Acceptable

The security practices deployed within the organisation are at an acceptable level; we can say that the organisation assets are protected from attacks.

• Level 4 - Managed

The organisation administrators are effectively protecting the organisation network and assets. A high level of security is ensured within the organisation network. In other terms, the administrators are effectively managing security issues.

• Level 5 - Optimal

Level 5 indicates a very high level of security; the organisation has deployed the necessary security practices to protect itself from harmful attacks. Such a level of maturity reflects the administrators' high experience in security issues; it is reached only if the organisation considers security as a catalyst of its effective business strategy.

5.2 The maturity level evaluation tool

Based on the adopted concepts, we propose a tool that helps to evaluate the maturity level of the organisations security practices. Our approach consists of adapting the ISO/IEC 27002 and the ISO/IEC 27001 frameworks to VOs and defining the tool which is based on the ISO/IEC 27002 best practices. This tool is used as a decision support system helping the organisations to decide if their potential partners are trustee or not. This tool was defined in the context of the VIVACE project and its results evaluated by our partners.

Our tool is based on seven chapters of the ISO/IEC 27002 standard which are: 1) Security policy, 2) Organising information security, 3) Asset management, 4) Communication and operations management, 5) Access control, 6) Information systems acquisition, development and maintenance et 7) Compliance.

The tool is in the form of a questionnaire where each question proposes a statement about an ISO/IEC 27002 security practice that may be implemented, partially implemented or not implemented within an organisation. The questions intended to the administrators of organisations are associated to the five maturity levels depending on their criticality and the security issues they express. The more the security requirements expressed by the questions are strong, the higher the associated maturity level is.

For example, these three questions from chapter "access control" related to the security control "user registration" should be answered to decide if "Company C" may act as an IdP of its own employees in section 2 scenario:

- An access to the organisation information system is granted to a user (local or remote) only when he requests it. If so, the maturity level for the security control "user registration" is 1 or initial.
- Formal user registration (and de-registration) procedures are defined for granting (and removing) user access to all information systems and services. If so, the maturity level for the security control "user registration" is 3 or acceptable.
- To provide access to critical or sensitive information systems, users' roles (job function within the organisation) are used. If so, the maturity level for the security control "user registration" is 5 or optimal.

Using our tool, we will calculate the maturity level of "Company C" security practices through four steps:

Step 1: the administrators within "Company C" respond to the questions by '1' for « an implemented practice », '0' for « a not implemented practice » or '0.5' for « a partially implemented practice».

Step 2: the tool calculates the level of maturity for each security control adopted by the tool.

Step 3: the tool calculates the level of maturity per security theme. Two values are calculated: the minimal maturity level per theme "eval min" and the average maturity level per theme "eval average" (Figure 6).

Step 4: the tool displays values on a Kiviat graph (Figure 6). The calculated value for the maturity level is compared to an objective value "objective level" identified by the different partners as a minimal accepted level for trusting an organisation in the context of the specific VO.

5.3 Discussion

Figure 6 shows, for example, that Company C is mature in terms of managing its own assets and resources (the maturity level for the "asset management" theme is higher than the objective level) but it has some weaknesses in access control issues (the maturity level for the "access control" theme is lower than the objective level). Although "Company C" has good maturity levels for the "asset management" theme, its partners can not accept that it acts as an IdP for its own employees. This is because "Company C" does not have a good maturity level for the "access control" theme.

So, our tool allows organisations to quantify trust that they may have in their partners and decide if they are able to rely on them for managing their own users' accounts and accreditations. "Company A" and "Company B" will not accept to open their information systems to the employees of "Company C" unless they manage their identities and credentials.

Let us consider that both "Company A" and "Company B" have the required maturity level (objective maturity level) to act as IdPs. In this case, either "Company A" or "Company B" can manage the authentication and the accreditation tasks for "Company C" employees, i.e. can behave as an IdP for "Company C" employees.

Identity federation is not the panacea. The main issue is who can act as an IdP; our tool provides information to make a choice. When only one partner has the required maturity level, a centralised solution is the best choice. When more than one partner have the required maturity level, depending on context-specific criteria, a decentralised solution can be set up. When no partner has the required maturity level, they should subcontract this role (IdP) to a trusted entity.

Our tool can be used to decide who can store the shared resources. In our use case scenario, document is created by the cooperation of all the partners. If the partner that stores this private document is not mature enough (for example, there is no antivirus mechanism on the machine that hosts the resource), the whole security of the VO would be downgraded. Our tool includes the security control "access control policy" within chapter "access control" to evaluate this point.

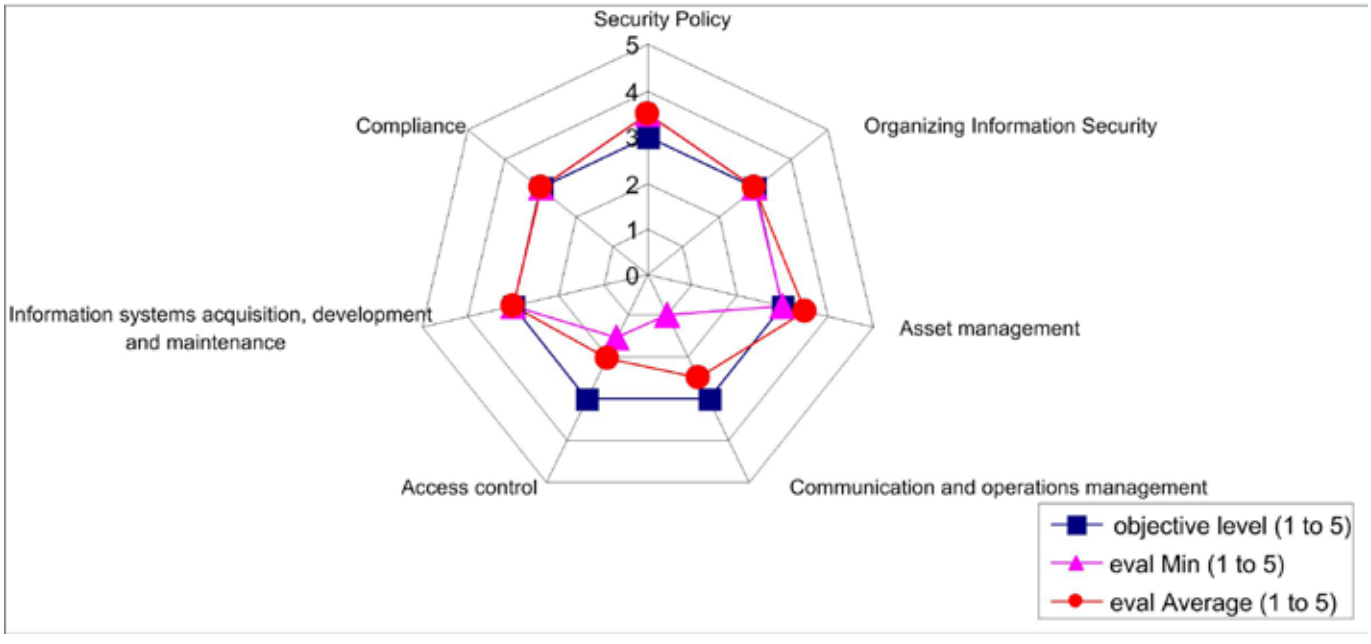


Figure 6. "Maturity level evaluation" graphic for Company C

T6. Related work

Currently, different tools provide collaborative workplaces and web-based content management functionalities such as Exostar [5], IBM Lotus Quickr [9] and, Xerox DocuShare [20]. Within the VIVACE project, we had some feedbacks on Exostar which has been used by some VIVACE members. The main issue concerning Exostar is that it necessitates an organisation to delegate the task of controlling access to its resources to an external entity, which manages the Exostar workspace (one of the partners or a third party). This issue has been pointed out in our analysis, especially when organisations share their critical resources. This is not mandatory in our environment because we have used the concept of identity federation.

IBM Lotus Quickr allows organisations to share content, collaborate and work faster online with teams from inside or outside the organisation. Xerox Docushare is a flexible Web-based content management solution that brings greater productivity to every knowledge worker. It allows organisation-wide information control without increasing demands on Information Technology. These two solutions provide secure workspaces for exchanging documents and information where a central authority is managing all the transactions between participating entities. Like Exostar, these solutions do not allow organisations providing resources to keep control on their resources.

Contrary to these products, we offer a technical solution that allows each organisation to keep control on its resources. This constitutes a big difference. An organisation can deny the access to its resources whenever it wants, even if this does break the original contract. In addition, organisations can manage their users that make the process of users account management faster. This makes our solution more flexible for a VO where dynamism and agility are a primary characteristic of such environments.

We also cover the organisational aspect by providing a tool that calculates the maturity level of the security practices of each partner. This information can be used when setting-up a VO to determine who is able to act as an IdP or an SP.

7. Conclusion

During the VIVACE project and the work with the TSCP program, we have captured the difficulties to merge minds and technologies when building a VO. Within a VO, contracts are established between partners who need to share and protect their know-how. Access management is a major concern to deal with. In our proposal, we cover both technical and organisational aspects of this issue.

First, our technical solution provides a secure collaborative environment based on three concepts: 1) the policy models based on attributes offer a good framework to specify access control policies, 2) the PMIs control the management of these attributes and 3) the identity federation harmonises the authentication and accreditation mechanisms. We have implemented these concepts within our collaborative environment using an enhanced version of PERMIS combined to Shibboleth.

This architecture provides high flexibility. But when setting-up a VO, the partners need to decide who will act as an IdP or an SP from the applicants. To tackle this issue, we have defined a tool based on the ISO/IEC 27002 best practices and the concept of maturity levels. The idea is to be able to evaluate the security practices of each partner to determinate that nobody will downgrade the security level of the others, i.e. the chain of trust is not broken. This tool has been validated in VIVACE.

Currently, we are working on enhancing our collaborative environment. We are replacing PERMIS, which provides a non-standardised policy language and where the interactions between the PEP and the PDP follow a proprietary protocol, by a PMI using the OASIS SAML and XACML [19] standards.

8. References

1. Bultje, R., van Wick, J (1998). Taxonomy of Virtual Organisations, Based on Definitions, Characteristics and Typology. VOnet Newsletter 2(3), 1998.
2. Calder, A (1996). Information Security Based on ISO27001/ISO17799, van Haren Publishing, 1996, 80 p., ISBN 9077212701

3. Chadwick, D., Zhao, G., Otenko, S., Laborde, R., Su, L., Nguyen, T-A (2006). Building a Modular Authorisation Infrastructure. The UK e-Science All Hands Meeting, 2006.
4. CMMI, http://www.sei.cmu.edu/cmmi/cmmi.html
5. Exostar, http://www.exostar.com/
6. Ferraiolo, D.F, Sandhu, R., Gavrila, S., Kuhn, D.R., Chandramouli, R (2001). Proposed NIST Standard for Role-Based Access Control. ACM TISSEC, 4(3):222--274, 2001
7. Fielding, R. et al (1999). Hypertext Transfer Protocol -- HTTP/1.1. RFC 2616, 1999.
8. Harrison, M.A., Ruzzo, W.L., Ullman, J.D (1976). Protection in Operating Systems. Communication of the ACM, 1976
9. IBM Lotus Quickr, http://www-306.ibm.com/software/lotus/products/quickr/
10. Information Security Management Maturity Model ISM3, 2007
11. ISMS, http://www.praxiom.com/iso-27001-definitions.htm
12. ISO/IEC 27002, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297
13. Kamel, M., Benzekri, A., Barrère, F., Laborde, R (2007). Evaluating the conformity of an access control architecture for Virtual Organisations with ISO/IEC 17799, IEEE GIIS 2007, Morocco, 2007
14. Kamel, M., Benzekri, A., Barrère, F., Grasset, F., Laborde, L (2007). VIVACE 0.3/3/IRIT/8-1.0, Deliverable N° D0.3.3_2v2, issue N° 1.0, 2007
15. Liberty Alliance, http://www.projectliberty.org/
16. SAML, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security
17. Shibboleth, http://shibboleth.internet2.edu/
18. Wang, L., Wijesekera, D., Jajodia, S (2004). A Logic-based Framework for Attribute based Access Control, 2nd ACM Workshop on FMSE, 2004.
19. XACML, www.oasis-open.org/committees/xacml/
20. Xerox Docushare, http://docushare.xerox.com/products/docushare.html

9. Author biographies

Michel Kamel is Ph.D. student in computer science at University Paul Sabatier, Toulouse, France. His research activities, conducted at IRIT (Institut de Recherche en Informatique de Toulouse), focus on the management of Virtual Organizations: validation and deployment of security policies. He participated to the European project VIVACE; his work consisted of the contribution to the deployment of a secure shared IT infrastructure used for the foundation of a secure Virtual Organization on a technical and an organizational aspects. Since September 2007, he has a temporary teaching and research position at University Paul Sabatier where he gives courses and practical works on networks.

Romain Laborde has been Maître de Conférence at University Paul Sabatier - IUT 'A' since September 2006. He is member of the IRIT laboratory. He received the PhD degree in computer science from University Paul Sabatier in 2005. Then, he was Research Associate in the Information Systems Security Group in the Computer Science Department, University of Kent at Canterbury, UK. His research interest includes formal methods for network security management, privilege and identity management, especially in the context of virtual organisation.

François Barrère is an Associate Professor. He received the Ph.D. degree in computer science from University Paul Sabatier, in 1987. He is member of IRIT. His research interest includes local area network protocols and design, network information security management, and digital rights management while building extended enterprises and virtual organizations. Since eight years he has been involved in different major European aeronautic research projects, where he participates to build secured network infrastructures. He is teaching network and security, in the Telecom Systems and Computer Network department in University Paul Sabatier.

Abdelmalek Benzekri is Professor at University Paul Sabatier – IUT 'A' since 1999 where he is director of a master degree on Information Systems Architecture. His research activities, conducted at IRIT, focus on systems and networks management and specifically on information security management. His last works address trans-organisational access control policies for virtual organisation formations. The results are assessed in the context of the aeronautical supply chain towards European research projects such as ENHANCE, CASH, IMAGE and VIVACE.