



IT security for smaller businesses

Michel Kamel, Abdelmalek Benzekri, François Barrère, Bassem Nasser
Université Paul Sabatier – IRIT
Toulouse, France

+33 (0)5 61 55 60 86
{mkamel, benzekri, barrere, nasser} @irit.fr



IRIT Involvement

- **The domains of interest of IRIT within the VIVACE project are the design of solutions that should be deployed to ensure connectivity and security within the Virtual Organisation (VO).**
- **Concepts such as authentication, authorisation, access control, security policies and security practices within a VO environment are being considered in order to deploy an infrastructure supporting the secure share and exchange of information between partners within the VO. Aspects, relevant to third tier suppliers for supporting the supply chain members are studied deeply.**

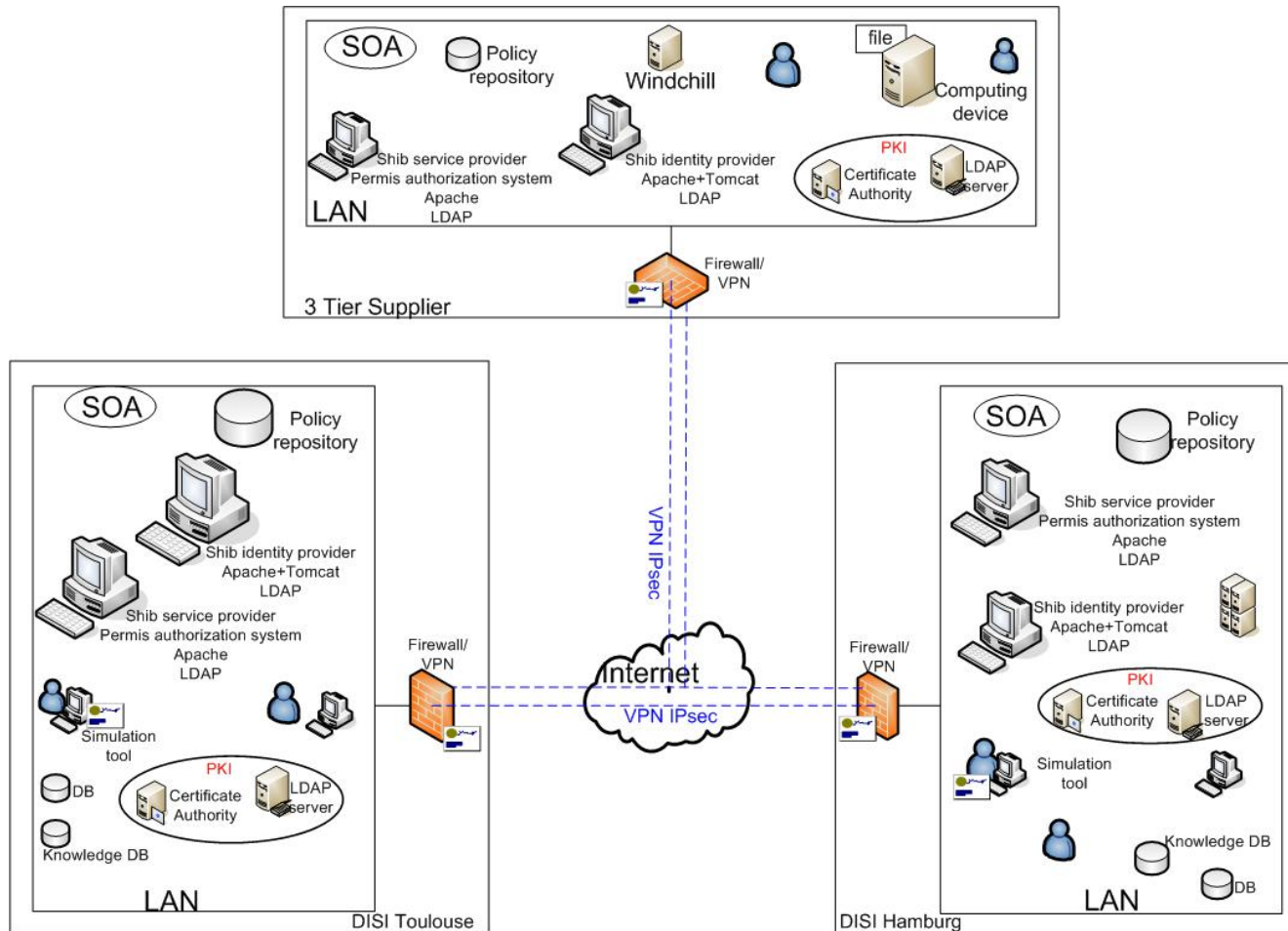


The “Virtual Organisation” Type of collaboration

- **ICT mediated business organisation**
- **Needs for the pooling of more than one core competencies within small ‘specialists’ companies**
- **Memorandum of Understanding = Contractual Agreement**
 - **Common understanding/common vision and work towards shared goals**
 - **Sophisticated ICT infrastructures and mutual confidence**
 - **efficiency determined by the speed and efficiency with which information can be exchanged and managed among business partners.**



The VO concept and the 3TS support





The VO security policy

- **A global security policy should be deployed within the VO network. This security policy is not a new one but should be considered as an extension of the different security policies defined on each partner's site.**
- **The Common IT Security approach within the VO is intended to merely enable organisations to extend their IT Security Policy in the leanest and most efficient way. This security policy must ensure privacy and security for 3TS.**



VO IT infrastructure base services

- **The shared IT infrastructure deployed to support the VO type of networks must guarantee these base services:**
- **Security services:**
 - **Confidentiality and integrity**
 - **Authentication**
 - **Authorisation**
 - **Single Sign On**
- **Control and management services:**
 - **Identity management**
 - **Access control management**
 - **Audit and log management**
 - **Network management using tools such as firewalls, routers, NIDS, etc.**



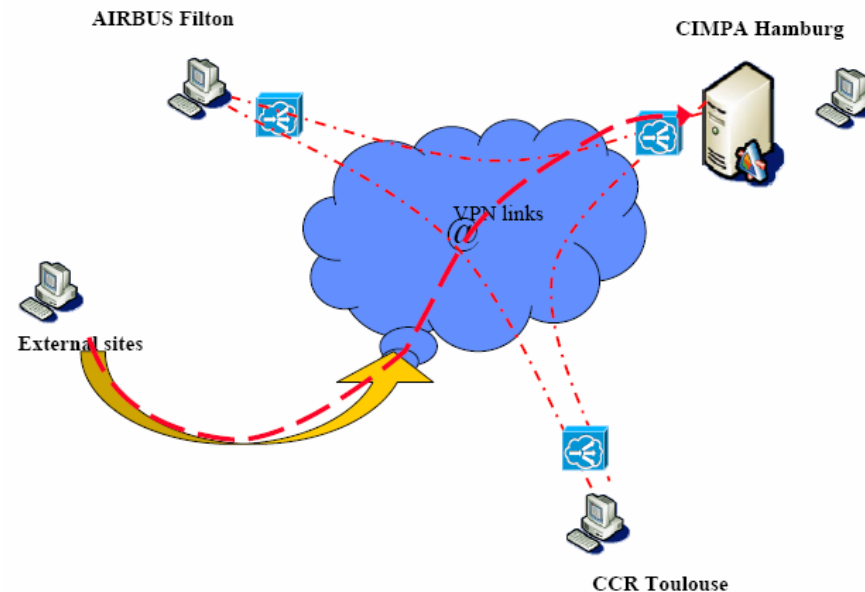
VO confidentiality and integrity services

- **Confidentiality and integrity services are ensured using security protocols (IPsec, SSL, etc.) and security equipments (firewalls, routers, IDS, etc.).**
- **Protocols:**
 - IPsec
 - SSL
 - ...
- **Equipments:**
 - Firewalls and routers
 - IDS
 - ...



VO confidentiality and integrity services

- A VPN IPsec solution can be deployed to ensure an encrypted tunnel between separated sites; this tunnel will be used to transmit data securely between the partners' sites.





VO access control service

- **Access control is realized through two security services: authentication and authorisation.**
- **A formal approach must be adopted to specify an access control policy. Access control models such as RBAC or OrBAC could be used. Once modelled, the access control policy must be enforced.**
- **For access control policy enforcement, infrastructures for identification, authentication and authorisation must be used. PKIs are satisfactory for identification and authentication, but they don't provide a solution for authorisation.**



VO access control service

- **During all the VO lifecycle, security problems are faced. The interconnection of partners' information systems must preserve that each partner keeps control on its own resources.**
- **An access control policy suitable for a dynamic trans-organisational environment should be deployed. A distributed management infrastructure should be implemented.**
- **Users roles must be defined and managed**



Information Security management process

- **Definition of an information security management process; this process will ensure a secure exchange and share of information between partners. It will guarantee these properties:**
 - **information confidentiality,**
 - **information integrity,**
 - **information availability, and**
 - **Information non-repudiation**
- **Security practices implemented must be parts of the global VO's information security policy and must guarantee that this policy is respected by different users and partners.**



Information Security management process

- **The Information Security Management process that we adopt in order to deploy a secure shared IT infrastructure for the VO type of networks is:**
 - **Use risk management methods such as Ebios, Mehari, etc.**
 - **Use the ISO/IEC 17799 and the ISO/IEC 27001 standards to build, operate, maintain and improve an ISMS (Information Security Management System).**
 - **Define a tool that allows SMEs administrators to evaluate the security practices' maturity level implemented within their infrastructures to ensure Identity and Privilege management, business continuity, etc. The evaluation will be realized compared to the ISO/IEC 17799 directives. This tool provides a solution to quantify trust between partners.**



Thank You

Any Questions ?

