

Innovation Reports

ROLE-ID

(ITEA 2 ~ 08007)

It's not who you are
but what you do that counts

TIMMO-2-USE

(ITEA 2 ~ 09033)

Getting more for less
More predictable development, less time to market

ROLE-ID

(ITEA 2 – 08007)

Aline Andrillon, Cassidian Cybersecurity,
France

It's not who you are but what you do that counts

Use of information and communications technology (ICT) has grown enormously in every sector of business and public services in recent years. The economic well-being of enterprises in Europe has come to depend increasingly on instant access by all companies and their customers to an unlimited flow of information based on interoperable public networks and information technology (IT) systems. Weaknesses and vulnerabilities in these networks and systems pose an increasingly serious threat to the proper functioning of key value chains in Europe. The magnitude of this threat increases with the growing number of network users and the value of the transactions they carry out. Identification is therefore a key element, and security a vital strategic aspect of European e-business.

ROLE-ID has developed an organisation-oriented identity extension of role-based access control, built on a role-centred vision. It provides a set of innovative and modular security components and processes that will enhance role management within the infrastructure identity level and provide innovative role functionalities. The concepts were demonstrated in three application domains: healthcare, public safety and cyber defence.

INNOVATIVE CONCEPT OF FUNCTION IN IDENTITY

Identity control currently centres on a user-centred approach: e-administration concentrates on the citizen, while e-business is focused on the private customer. However, while organisations also have a crucial need for identity control, several specific issues

had not been satisfactorily addressed, prompting a shift towards role-based access control (RBAC) that breaks down each task into its component parts. For organisations, the two main issues concerned:

1. Managing great complexity – a large number and a disparity of users, teams, divisions, enterprises, applications, services, intranet, extranet, roles, job functions, etc.
2. Continuous change – frequent reorganisations, mergers and acquisitions, people changing jobs, international, European or national regulation changes, etc.

To address these issues, ROLE-ID developed an organisation-oriented identity extension to RBAC

based on a role-centred vision by introducing an innovative concept of function in identity. The aim is to improve notions of context sharing and delegation, create a new concept of virtual user to enable rich dynamic role attribution, develop new means for organisations to model a great complexity of identities and roles, adapt and improve existing methodologies to administrate a complex organisation identity database, and provide enhanced tools for identity provisioning that are relevant to real-life constraints.

EXTEND AND ENHANCE

Briefly, ROLE-ID adds the notion of function and virtual role to user identity. In essence, ROLE-ID simplifies the identification management process in

large, complex organisations through context-based filtering – Mr Smith as purchasing manager or as software engineer rather than Mr Smith as opposed to Mr Jones or Mrs White – so that information commensurate with that particular function, rather than the individual, is accessible. In organisations where personnel change or turnover is regular or sudden, a role defined identifier provides both optimum access and security.

The purpose was not to develop a completely new identity framework but to work from identity products, standards and concepts already developed by the different partners in the consortium and extend them. In addition, existing theoretical concepts and methodologies from around the world were also used and extended, and implemented in actual existing products. Furthermore, some innovative concepts were introduced in the field of identity management along with several new organisation-oriented identity modules that have been proved through demonstrators in the three main application domains addressed: healthcare, public safety and cyber defence.

The technological achievements and general results have been incorporated in concrete applications that are directly supported by users' partners or indirectly tested by developers' partners. Information security was emphasised in every phase of the development lifecycle through testing and reviews including design, implementation and business logic.

BUSINESS IMPACT ON HEALTHCARE

The innovative approach of role identity has been demonstrated in the field of healthcare and in generic use cases whereby identity is validated on the basis of self-accreditation from external credentials. In the event of an accident, for instance, the data and information concerning the accident itself and any persons involved are disseminated according to role identity. A journalist may have access to accident details specific to his public reporting needs whereas for the requirements of the emergency services, for instance, information about a person's medical history and condition may be vital to ascertaining treatment on the spot.

In the ORBAC model that set out to define a conceptual and industrial framework to meet the needs of information security and sensitive healthcare communications, information sensitivity, integrity and confidentiality are key parameters. ROLE-ID offers a way of facilitating the transfer of a confidential patient file and delegating the responsibilities of individuals involved in patient care and treatment.

BUSINESS IMPACT ON E-GOVERNMENT

The collaboration and cooperation within the consortium of French and Finnish partners enabled the problems and challenges to be addressed and value to be added in a variety of applications and sectors. For example, the formalisation of specific options and constraints across various e-gov services and the establishment of the semantics and syntax of user attributes for the (Finnish) public sector federation. Dissemination came through 21 conference articles and 5 journal papers along with 5 PhD doctoral dissertations and 7 Master theses.

The added value for organisations (public safety, healthcare and commercial) comes through lower user management costs and higher employee efficiency, increased levels of security and more user-friendly system use by end users. Citizens and society benefit from better public organisation efficiency and greater trust in privacy protection while sharing more information (right to know). The project partners have improved their solutions and will use the results in the next versions of their solutions, with some having already deployed some of the results.

FAST EXPLOITATION OF RESULTS

The results of the ROLE-ID have already been implemented and/or are being planned for implementation among many of the partners. For instance, a partnership initiated between the large Cassidian company and Ilex SME qualifies for 'research as a business development tool' given the partnership's drive to get a solution to market. This solution in the form of new role management software has already been sold to customers, such as the French ministry of security.

Other examples of quick exploitation of the results include the incorporation of ROLE-ID by Telecom Bretagne to improve versions of MotOrBAC tool and the OrBAC API that allow easy web service integration and a new plug-in. Ubisecure is an instance of how the deeper knowledge gained on role-based models has been incorporated to extend the functionalities of handling roles/identity attributes. In fact, project results have now been included in five major and sixteen minor Ubisecure product version upgrades, with several commercial installations in place. Entr'ouvert has gained extended knowledge in access control centralisation, session management centralisation, role and attribute-based access control to implement new features in its main products: a centralised access control administration point and a centralised decision point module in Authentic 2. Insta is developing service concepts in Identity and Access Management areas with the prospect of including these concepts in public safety development work.

POWERFUL YET PRAGMATIC

The fruits of the ROLE-ID project have created new market opportunities with new products and solutions, thereby strengthening the competitive position of European industry in the selected sectors, based on its improved capacity to implement and deploy powerful yet pragmatic identity and security mechanisms and solutions, mandatory for business operations in these sectors.

MORE INFORMATION:

www.roleid.org

