Résumé :

Les systèmes d'information répartis emploient de multiples processus autonomes et complémentaires qui coopèrent afin de remplir des tâches complexes. La plupart de ces systèmes ont recours à des protocoles aptes à rendre confidentiels les messages échangés. Cependant, peu d'entre eux prévoient la gestion des accès aux processus qui les composent.

L'objectif de ce travail est de proposer la modélisation UML d'un système réparti dont les processus sont des objets informatiques. Ce modèle repose sur les principes employés par l'architecture CORBA, tels que l'abstraction entre interfaces et traitements par le biais de l'Interface Description Language (IDL), la prise en compte de l'hétérogénéité des plates-formes et des langages de programmation ainsi que l'emploi de services communs. En complément de la confidentialité des échanges, les techniques de signature électronique sont employées afin d'assurer l'authentification forte des objets, l'intégrité des messages et la non répudiation des informations échangées. Dans ce sens, une grammaire d'un contrat IDL sécurisé (S-IDL) est proposée. La gestion des accès aux objets est en outre complétée par l'intégration de systèmes externes prenant en charge la surveillance des interactions entre les objets ainsi que l'audit des tâches réalisées.

Par ailleurs, le modèle ainsi élaboré s'accompagne d'une proposition relative à la définition d'un format de signature électronique issu de l'étude des standards existants et conforme aux exigences juridiques. Ce format est intégré à un protocole de communication entre objets, modélisé en Abstract Syntax Notation One (ASN.1) et UML. Un prototype valide le modèle proposé. Il est à l'origine d'une architecture répartie à grande échelle appelée « chaîne de confiance », composée de multiples tiers. La collaboration entre ces derniers permet de répondre aux recommandations d'acceptation par les juristes d'une signature électronique au même titre que son homologue sur support papier.

Cette chaîne est mise en relation avec des applications grand public qui font appel à ses services.

Mots-clés : système réparti objet, signature électronique, authentification forte, horodatage.

Abstract:

Nowadays information systems benefit from multiple autonomous and complementary processes that cooperate to provide end-users with elaborated services. Distributed object-oriented systems integrate the object concept in terms of services implementation. Although most of them make use of security protocols to achieve message transmission confidentiality, access control is reserved to a minority.

We suggest a UML model of a distributed object-oriented system, based on the CORBA standard main principles such as interface and implementation abstraction, using an Interface Description Language (IDL), environments and programming languages heterogeneity handling, and common services usage. This model allows distributed objects strong authentication and access control. It also offers confidentiality, supervision and audit mechanisms. The proposed control scheme makes use of a new secure IDL contract (S-IDL) grammar. S-IDL extends common IDL definitions to express security requirements. Electronic signature takes an important part of the proposed model as it testifies messages integrity and provides means for non repudiation.

This model comes along with a new signature structure proposal derived from existing standards, which takes into account legal recommendations. This format is integrated into an inter-object communication protocol described using Abstract Syntax Notation One (ASN.1) and UML languages. A prototype which contributes to a large-scaled "trust chain" implementation is designed according to the model. This chain is composed of a set of distributed third parties that interact with each other.

Beyond distributed computing, our ultimate goal is to contribute to make electronic signature accessible to the general public, providing tools that connect with the proposed distributed trust chain.

Keywords: object-oriented distributed system, electronic signature, strong authentication, time-stamping