

FILIGRANE – A Copyright Management System for Mobile Code

Mehrdad Jalali

Introduction

Intelligent software agents are a new class of software that acts on behalf of the user to automate complex tasks. A mobile intelligent agent can move to different agent servers to be executed there to perform some tasks. The mobile agent is completely exposed to the server on which it is executed. This is called a Malicious Host problem. Casual fraud is therefore a major concern, and the advent of the agent code coupled with ubiquitous platforms is a huge potential threat to content originators. Relevant security issues encompass several aspects:

- mobile software IPRs guaranteeing software right holders the rightful use of their production,

- security mechanisms authenticating mobile software origin and authorized user,
- security mechanisms certifying software integrity,
- secured protocol for the support of software download from server to user (PC, NC or smart card),
- mechanisms to trace the software during its entire life cycle from development to its use by authorized users,
- users' protection against software with malicious behavior.

FILIGRANE merges a number of different security blocks to a functioning framework and defines an integrated secure Web architecture for it.

German Abstract

Copyright Schutz ist ein Schlüsselement bei der Entwicklung der mobilen Agenten Technologie. Dies ist begründet durch die bewegliche Natur dieser Art von Software und der Macht von Servern. Die Abwesenheit von Schutz wird das Risiko von Piraterie zu einem Punkt bringen, daß die Wirtschaft dieses Sektors schwächen sogar zerstören würde. Zusätzlich zu den gesetzlichen Maßnahmen ist technologischer Schutz ein wichtiges Element in der Entwicklung dieses neuen Marktes. Im Verlauf des ESPRIT Projekts FILIGRANE (FlexibLe IPR for Software AGent ReliANcE) entwickelten wir eine sichere Web Architektur und einen assoziierten Sicherheitsrahmen sowie Protokolle für das Handeln des mobilen Codes im Internet.

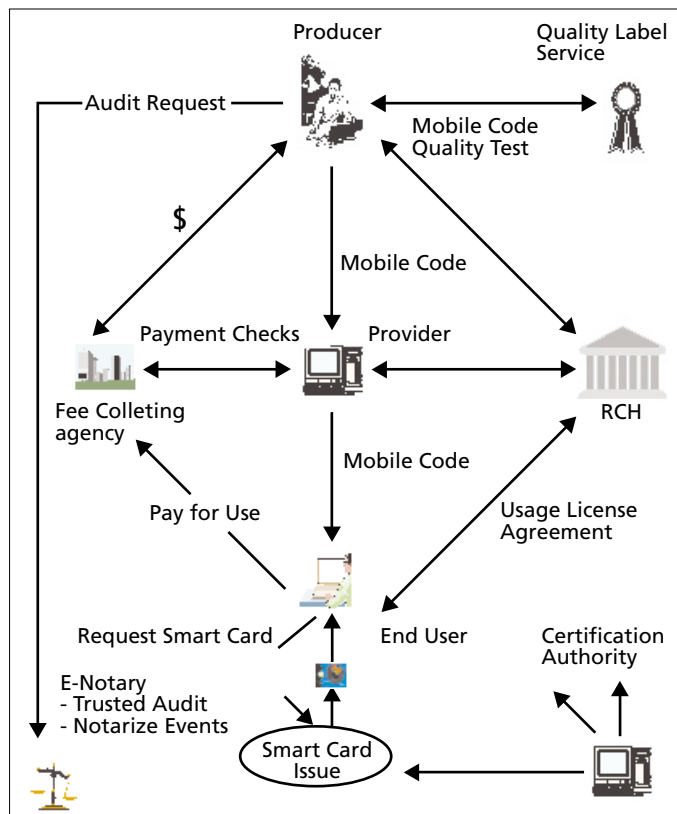


Figure 1: FILIGRANE Functional Model

FILIGRANE functional Model

The FILIGRANE system consists of the following actors:

- Certification Authority (CA): a Trusted Third Party (TTP), providing services for the creation and distribution of electronic certificates for producer, end user, provider and the Rights Clearing House (RCH);
- Producer: a software developer or company, offering the mobile code to an e-commerce provider;
- Provider: actor providing goods such as software, services or information. The provider sells services and/or electronic delivery of commercial items such as software. The provider negotiates the contract conditions for the use of services electronically;
- End user: an authorized holder of a certificate supported by a CA, and registered to perform software download by the FILIGRANE system;
- Rights Clearing House: The FILIGRANE Rights Clearing House organizes definition and redistribution of rights between the actors of the system as the result of a transaction;
- Fee Collecting Agency: this actor is responsible for the collection of funds as the result of financial transactions and will redistribute them proportionally to the various actors of the system according to the conditions of the associated contracts.
- Quality Label Service: this optional actor can enter the system qualifying the mobile code to be distributed with various quality labels recognized by potential purchasers;
- E-Notary: this actor will notarize all transactions of the system and act as a trusted repository for all actors.

FILIGRANE Security Blocks

By combining a number of security blocks we provide a secure framework for the commerce of the mobile code. These security blocks are presented below:

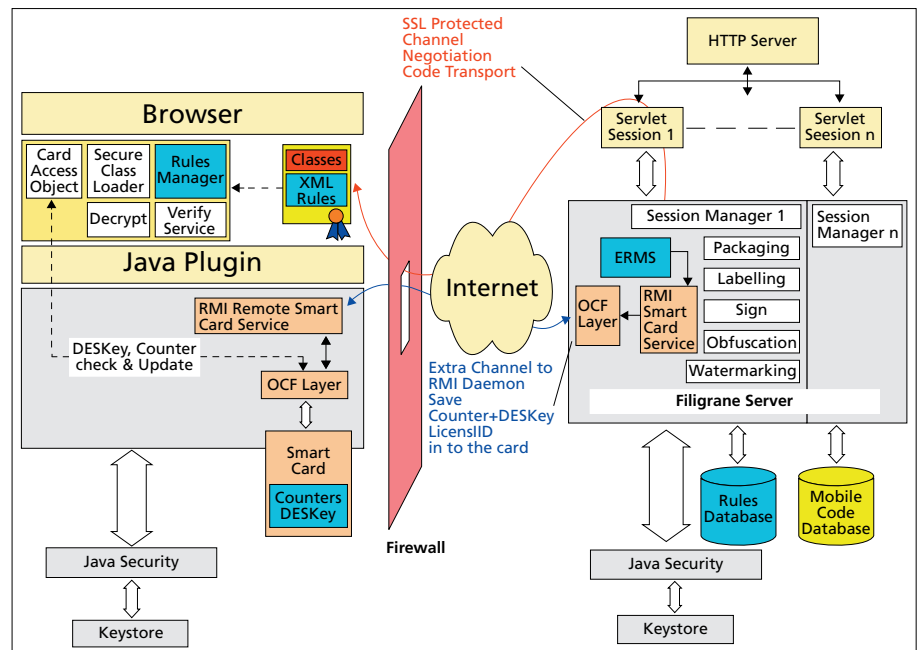


Figure 2: FILIGRANE Web Design

- Signature: The mobile code could be signed by different parties. The signature can secure origin and integrity of the mobile code.
- Encryption: An encryption of the mobile code has two objectives. The first is to avoid decompilation/reverse engineering. The second is to control parts of the execution/ read rights of the customer.
- Rules: are associated with the mobile code. These rules will describe parts of the contract between producer, provider and end-user. The rules will be checked by the FILIGRANE execution environment to avoid any breach of the contract.
- Watermarks: Another stage of protection is the presence of watermarks embedded within the mobile code.
- Obfuscation: Intuitively, an obfuscation of the code will insert modifications into the compiled code to prevent reverse engineering.
- Labeling: A tag is an important data. It permits the identification of the mobile code (name, version, author, date ...).
- Code Envelope: All these protection mechanisms are compiled in one single package.

Figure 2 illustrates the integrated secure Web architecture of FILIGRANE. This architecture realizes the following phases of an e-commerce transaction: browsing, item selection, ordering, contract handling, authorization, confirmation, Smart Card initialization, software delivery.

Point of contact

Mehrdad Jalali-Sohi
 Fraunhofer IGD, Darmstadt,
 Germany
 Email: jalali@igd.fhg.de