

ABSTRACT

COMPUTATIONALLY EFFICIENT METHOD FOR TRUSTED AND DYNAMIC DIGITAL OBJECTS DISSEMINATION

A computationally efficient method for trusted and dynamic dissemination of digital objects. Related digital objects of various types are grouped, based on their usage and functionality, by an information provider into distribution packages. Trustworthiness of objects contained in a distribution package are certified by a trusted certification authority in the form of a certificate which consists of a body and the certification authority's signature on the body based on a public-key digital signature scheme. The body further consists of the name of the information provider; name of the distribution package; and type, safety checking flag, and digest of each and every object. It is used by end users to verify the trust criteria of any individual or any subset of objects specified by the package. To verify whether a received object meets trust criteria certified by the certificate, the end user computes the digest of the object, compares it with the corresponding digest in the certificate, and examines the type and safety checking flag of the object contained in the certificate. The end user can dynamically download additional objects, check their trustworthiness without having to verify the certificate multiple times.

FIG. 3