Abstract

This paper addresses an elegant and probably unique divisible Wireless E-cash Transfer System in distributed environment. The proposed Wireless E-cash Transfer System solves most of the crucial problem with existing wired e-cash and untraceable e-cash proposals. A distributed computing environment can support multiple platforms, multiple servers and some open networking infrastructure such as Internet. One of such distributed computing architecture is Common Object Request Broker Architecture (CORBA), which is object-oriented, scalable and is based on open specification. We used MICO CORBA and implemented (MIWCO) Wireless CORBA extension for MICO. We had to modify the MICO Core to implement MIWCO. Wireless CORBA architecture has been used in the development and transfer of the e-cash system. In our system we also used LiDIA library for bigint, which is used for security purposes. We used to start Naming Service, Event Service & create Home Location Agent, Access Bridge, Terminal Bridge in implementing the Wireless E-cash Transfer System. The computational complexity of this system is O(n^2). We have used binary tree approach to construct a divisible e-cash and at each transfer coin authentication and denomination revelation is checked.
A Divisible Transferable E-Cash in Wireless Distributed Environment

References


SECURECOMM 2012, Padus, Italy, 3-5 September.
Index Terms

Computer Science

Security

Keywords

Divisible transferable electronic cash  binary tree  double spending  security

anonymity

blind signature

digital signature

unlinkability

untractability