SYSTEM AND METHOD FOR PRIVACY PRESERVING DIGITAL SIGNATURE WITH HASHING AND SIGNING OPERATIONS PERFORMED IN DISTRIBUTED TRUSTED RICH EXECUTION ENVIRONMENTS

BACKGROUND

Field of Invention

[0001] This disclosure relates in general to the practice of affixing digital signature to an electronic file (a.k.a. File Signing) in order to certify content integrity and origin authenticity of that file. In particular, this disclosure discloses the architecture of a distributed trusted computing system including virtualized trusted execution environments instantiated in a network of computers and the information processing and interchanging methods employed by these virtualized trusted execution environments to perform a digital signature operation on an electronic file while preserving the content privacy of that file.

Description of Related Art

[0002] In the ecosystems of Internet of Things (IoT), Software Defined Networks (SDN), and Edge/Cloud Computing Systems, system and application software modules are often supplied by different software developers, each of which intends to preserve the proprietary ownership of their software while allowing their software to be integrated with those of the other developers and then deployed together through the Continuous Integration and Continuous Deployment (CI-CD) process in a Secure Development-Operation (DevSecOps) lifecycle. All the system and application software modules developed by the software developers in this lifecycle must be certified by trusted Certification