

ABSTRACT

5 A cryptosystem having a secure Cryptographic Virtual Machine (CVM) protected by
a Tamper-Proof Virtual Layer (TPVL) for performing cryptography in software is
described. The CVM and TPVL allow software applications to store and process
cryptographic keys and data in a secure and tamper-proof manner, without requiring
the use of a Hardware Security Module (HSM).

10 Figure 2