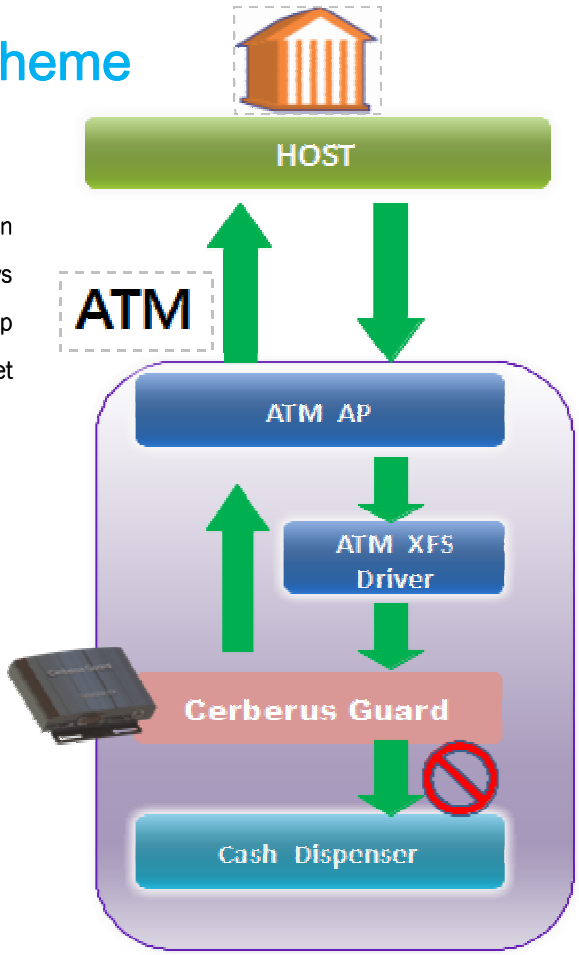
Hardware Security Encryption Scheme

HSM 安全機制

With the stricter requirements of data protection and correctness of transaction information, the standard security hardware (HSM) can be used to secure keys and calculate various cryptographic algorithms. Panorama software has deep technical capabilities and HSM integration application performance to meet customer needs and meet regulatory requirements.



Features

- Cerberus Guard protect the Cash Dispenser.
- HSM Cryptography Secure the transaction/ Command data Confidentiality、Authentication、Integrity、Non-repudiation.
- Cerberus Guard Algorithm to generate security token for ATM transcation.
- Secure Token diversify and Authorized by HOST & Cerberus Guard, protect ATM AP.
- THE ATM will be authorized by the Secure Token and then it will initial the XFS Driver and command to Dispenser of issuing note.
- Cerberus Guard against the forged command and protect the Host and terminal communication is consistent with authentication & integrity.
- Ensure that each issuing-note is authorized by the central Host, and that the hacker attack or abnormal commands will be blocked. And interrupt to all terminal or cash dispenser execution and alert ATM and Host on time.

Specification

- Secure Hardware 3DES/ AES/RSA Encryption, FIPS140 standard.

Dimension: 95*160*(H)30mm
ARM linuxOS