

Mobile Security Innovation



VALUE SUMMARY

EZYPAY m-security innovative end-to-end security module eliminates the encryption exposure between SSL/WTLS and back-end authorization system. The m-security solution is flexible and scalable, enabling institutions and networks in exploiting secure payment over wired or wireless internet network.

As a versatile and flexible application, the system allows 'sensitive' transaction, such as a mPayment and secure message, to be enveloped under RSA or Triple-DES security technology.

With EZYPAY m-security, all key management operations, including keys generation, unwrapping, and derivation of a key, are secured in the tamper-resistant hardware, and can not be extracted in clear form.

SOLUTION OFFERINGS

- Bank grade end-to-end security.
- Adopt same PIN or Password based security principle as in Debit Card for user authentication and confidentiality.
- Fully end-to-end hardware encryption translation from mobile device for back-end authorization system.
- Hardware tamper-resistance keys management operations.

Bank Grade End-to-End Secure Mobile Transaction

The problem of protecting sensitive data over public networks (or even private networks) is not new. There are many technologies today that attempt to address this problem. In particular, the Secure Socket Layer (SSL) and Wireless Transport Layer Socket (WTLS) protocols were developed to aid in protecting the exchange of data between clients and servers. This protocol has been instrumental in the proliferation of ecommerce activities on the Internet.

SSL/WTLS, using non-export ciphers, provides an excellent means of cryptographically protecting sensitive data during transport between a client and a server. In practice, SSL/WTLS does a very good job of protecting data during transport but falls short in that once the data arrives at its destination - the data is obtainable in the clear.

EZYPAY has implemented a solution that couples existing technologies and protocols, to provide the additional level of protection required for Internet transactions. In essence, it provides a secure translation of

sensitive data between an WTLS session and a backend authorization system using Triple-DES and RSA PKI technology.

EZYPAY m-security utilizes the Bank Grade Hardware Security Module (HSM) as the secure device for performing the cryptographic functions at the wireless internet server location. The Security hardware is a tamper resistance external box or PCI card version that meets FIPS 140 level 3 and 4 certification.

For redundancy and scalability, multiple boxes or PCI cards are consolidated into a single network that connects, via Ethernet, to the customers application server. This configuration fits well into most environment and provides scalability by permitting the connection of additional devices to meet the required transaction volume.



EZYPAY is an innovator in secure mobile technology solutions that exploit and add value to the latest available mobile broadband communications. EZYPAY provides payment and secure exchange solutions that promise to be multi-network acceptance which enabling pervasive mobile transaction, and is payment instrument agnostic.