Abstract

Providing the security services (authenticity, integrity, confidentiality and non-repudiation) all together in mobile banking has remained a problematic issue for both banks and their customers. Both the public key infrastructure (PKI) and the identity-based public key cryptography (IB-PKC) which have been thought to provide solutions to these security services, have their own limitations. While the PKI suffers the scalability and certificate management problems, the identity-based cryptography suffers the key escrow problem. This paper proposes a secure web-based mobile banking scheme using certificateless public key cryptography. Within this scheme, the key generating center (KGC) has an offline connection with a public directory server. Both of the client and the bank's web-server use the identities of each other to obtain the public key of each from the KGC's public directory server. Then, each party computes an authenticated per-session shared secret symmetric key. By using this shared secret key, the client can encrypt his username and password to access his banking account and carry out signed banking transactions. As a result, the proposed scheme is secure in the standard model and provides authentication, confidentiality, integrity and nonrepudiation. Moreover, the scheme is secure against known key attack, resilient
against unknown key share and key-compromise impersonation, and secure against weak perfect forward secrecy

References

- Patrick Gallagher, Deputy Director Foreword, and Cita Furlani Director. Fips pub 186-3 federal information processing standards publication digital signature standard (dss), 2009.
A Secure Mobile Banking Scheme based on Certificateless Cryptography in the Standard Security Model

Springer-Verlag.

Index Terms

Computer Science

Security

Keywords

Certificateless cryptography
Key generating center
Mobile banking
Standard security model

Security services