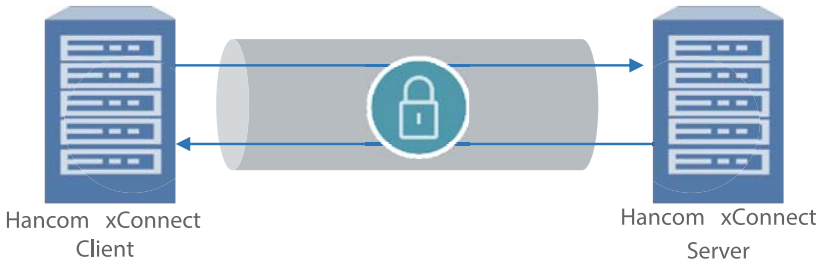
model:Hancom xConnect

Cryptography for Cyber Security solution

Product guideline

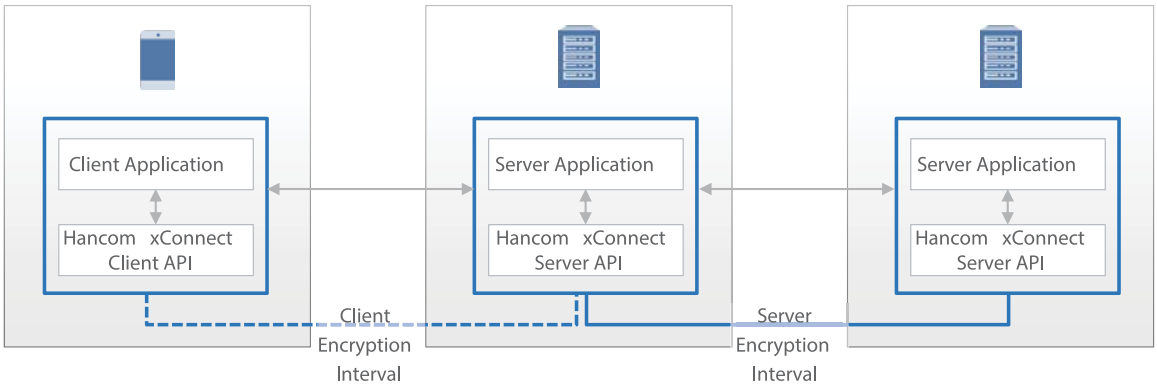
HancomxConnect is a wired and wireless communication interval encryption solution that ensures security through interval encryption and electronic signature for sensitive information.



1) Wired/Wireless Communication Interval Production
   (1) Mount the Cryptographic Module Validation Program of the NIS(CMVP)
   (2) Support Encryption/Decryption, Electronic Signature, Digital Envelope
   (3) Support for Replay Attack protection technology

2) Support Various Environments
   (1) System Requirements : PDA, CD/ATM, Server, etc.
   (2) System Programming: C, C++, Java, Delphi, VB, PB, etc.
   (3) Use SCP protocols that simplify the complexity of SSL and Strengthen Structure

Product consist



Type	Content	Performance Procedures
Hancom xConnect Client	Client End Encryption	1. Secure session key exchange using Challenge-Response method 2. Intercommunication of client-side and server-side transactions using session keys 3. Quick encryption processing interlink APP and API methods
Hancom xConnect Server	Server End Encryption	

※HancomxConnect has passed the Financial Supervisory Service's security review and is in use by many financial institutions.

System requirements

- Support Requirements

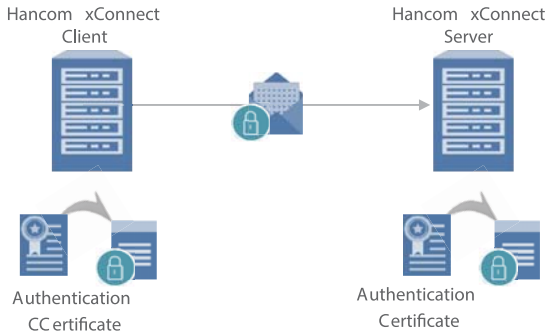
Type	Target	- Requirements
Client	O/S	- Hancom xConnect 3.0: DOS, 019 Java, WIPI, Windows 3.1/NT/2000/XP/2003 - Hancom xConnect 2.0: Embedded Linux, RTOS, WinCE3.0 above, Velos, Palm OS
	Support Programming language	- C, C++, Java, VB, Delphi, PB
Server	O/S	- Windows 7/10/2000/2003 - AIX 4.3 or later, Sun Solaris 2.6 or later - HP Itanium 11.23 , HP 11.0 or later - Linux Kernel 2.4 or later
	Support Programming language	- C, C++, Java, VB, Delphi, PB
Network	HTTP, TCP/IP, SNA, Serial, x.25, CDMA 2000 1X, 1x EV-DO, W-CDMA, etc Any Network Enviroment Support	

- Support Functions

Type	Support Function
Client/Server Library	- Security library to apply to client and server applications - Support RSA,KCDSA Signature, Cache Signature, Digital Envelope - Support Algorithm(Comply with PKIX and PKCS International Standards) - Publiuc Algorithm : RSA, DH, DSA, KCDSA, ECDSA, ECKCDSA, etc - Symmetric Algorithm : SEED 128, ARIA 128/256, AES 128/192/256, BLOWFISH, CAST128, DES, RC5, TDES, etc - Signature Algorithm : RSA, KCDSA - MAC Algorithm : SHA1, SHA256, SHA384, SHA512, SHA224, etc - Replay Attack Prevention Function ? Sequence Number Check

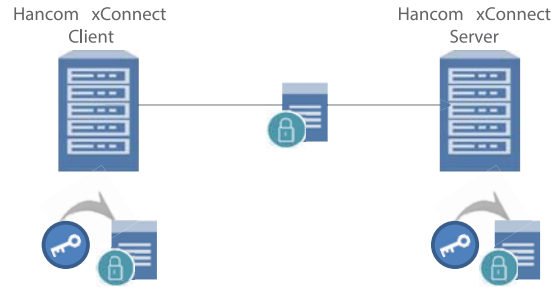
Main Function > Communication Interval Encryption

Digital Envelope Method



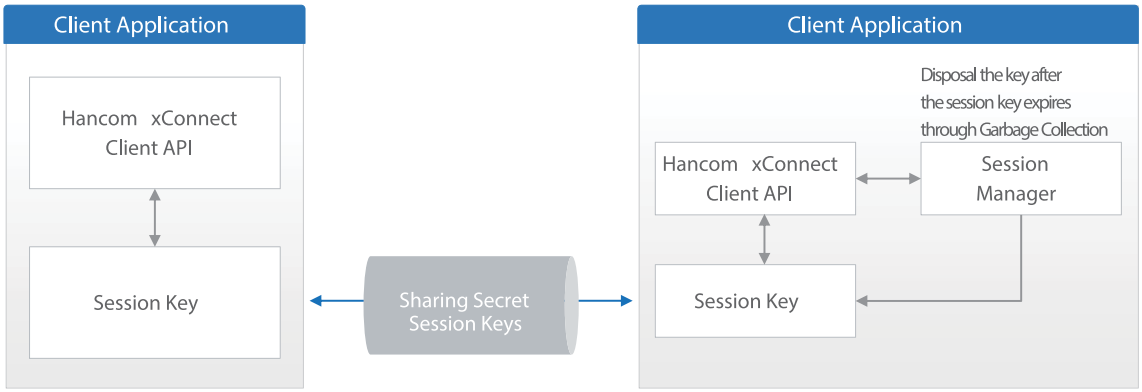
Encryption Method	Type	
Digital Envelope	Security	Very High
	Speed	General

Symmetric Key Method



Encryption Method	Type	
Symmetric Key	Security	High
	Speed	Fast

Main function > Key management



Self-developed Security Protocols

- Secure Capsule Protocol (SCP) independent development, a secure protocol for optimized secure communication
- Mutual authentication mode during encryption key sharing mode unables the availability of confidential information from other users even when certain values are exposed over the network interval

Prevent External Attacks

- Provides mutual authentication with Sequence Number Check to prevent external attacks such as Replay Attack, Man In the Middle Attack, and Session hijacking
- Symmetric key encryption and decryption are performed using secret session keys when communicating between server and client modules to avoid unnecessary RSA Operations

Specification

1. Software spec

Hancom xConnect : wired and wireless communication interval encryption software
• Communication Interval Encryption - Secure session key exchange using Challenge-Response method - Intercommunication of client-side and server-side transactions using session keys - Quick encryption processing interlink APP and API methods
• Cryptographic Module Validation Program of the NIS(CMVP)
• Support Encryption/Decryption, Electronic Signature, Digital Envelope
• Prevent External Attacks - Support for Replay Attack protection technology - Provides mutual authentication with Sequence Number Check to prevent external attacks - Symmetric key encryption and decryption
• 20 types of algorithm support - Publiuc Algorithm : RSA, DH, DSA, KCDSA, ECDSA, ECKCDSA, etc - Symmetric Algorithm : SEED 128, ARIA 128/256, AES 128/192/256, BLOWFISH, CAST128, DES, RC5, TDES, etc - Signature Algorithm : RSA, KCDSA - MAC Algorithm : SHA1, SHA256, SHA384, SHA512, SHA224, etc
• Support Various Environments - System Requirements : PDA, CD/ATM, Server, etc. - System Programming : C, C++, Java, Delphi, VB, PB, etc. - Use SCP protocols that simplify the complexity of SSL and Strengthen Structure
• Support System (Available by selecting from the OS below) - Windows 7/10/ 64Bit, CPU i3 above, Memory Min 4GB, Disk Min 100GB (Support for virtual machine) - AIX 4.3 or later, Sun Solaris 2.6 or later, HP Itanium 11.23 , HP 11.0 or later - Linux Kernel 2.4 or later
• No of License - 5 license keys (4 licenses for PCs and 1 license for Server)

2. Server PC spec (customer need to prepare the Server PC which is not included)
(Available by selecting from the OS below. user can select one OS from below)

- Windows 7/10 64Bit, CPU i3 above, Memory Min 4GB, Disk Min 100GB
(Support for virtual machine)
- AIX 4.3 or later, Sun Solaris 2.6 or later, HP Itanium 11.23 , HP 11.0 or later
- Linux Kernel 2.4 or later

3. Client Desktop PC spec (customer need to prepare the Client Desktop PC which is not included)

- Windows 7/10 64Bit, CPU i3 above, Memory Min 4GB, Disk Min 100GB
(Support for virtual machine)

4. Operating in same Network area : wired, or wifi

Training contents (Training -4 days)

Chapter 1. Information Security Overview.
- Concepts of Information Protection
- Fundamental elements of information protection

Chapter 2. Encryption Technology
- Encryption Overview
- Symmetric encryption algorithm
- Hash Encryption Algorithm
- Public key encryption algorithm

Chapter 3. Hancom xConnect
- Solution Overview
- Server Installation
- Installing Solutions
- Solution Practice

Component Lists

a) xConnect software CD (or, USB Dongle) : 1 copy (for 5 users)
b) License key (USB Dongle key) : 5 ea (Perpetual license key)
c) Manual book : 10 books