iVEST SERVER 2.0

iVEST Server is a software that establishes secure Internet transactions through the use of PKI technology. It ensures the integrity and confidentiality of transactions. It consists of iVerify.

iVerify

iVerify consists of the iVerify Server and iVerify Client. The iVerify Server enables flexible retrievals of CRLs from a remote CA's repository server to the local database. It checks the validity of certificates by referring to certificate expiry date, certificate integrity and revocation.

iVerify Client provides an easy to use API for digital signatures and certificate verification. Web applications can use iVerify Client to verify digital signatures generated by Signing Module
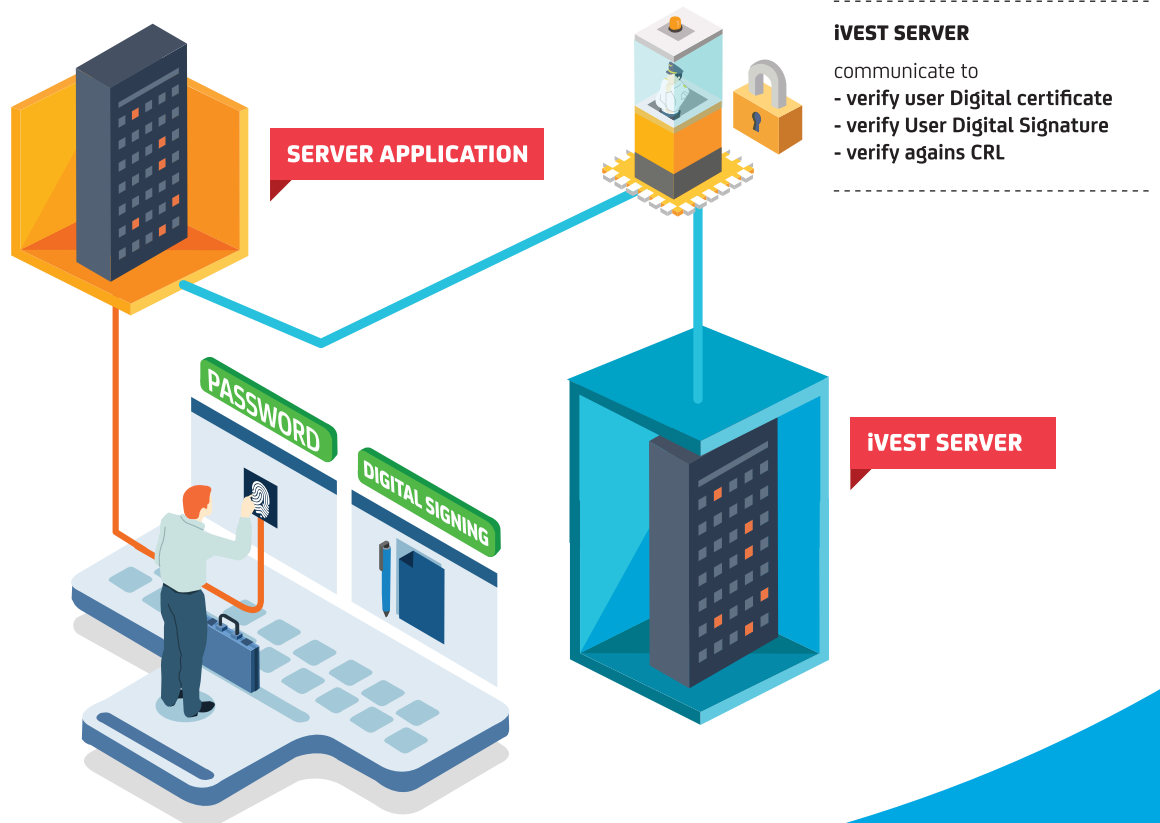
Suite of programs that enables :

Internet Communication

e-Commerce

SERVER APPLICATION

PASSWORD

DIGITAL SIGNING

iVEST SERVER
communicate to
- verify user Digital certificate
- verify User Digital Signature
- verify agains CRL

iVEST SERVER

Description

- **Easy to use API** to verify digital certificates and to access information in digital certificates.

- **Able to extract the following from digital certificates**: owner's name, email address, certificate serial number, unique identification number and digital certificate validity period. It can also extract digital certificate issuer name.

- **Able to check** for certificate revocation.

- **Easily uses API to verify** digital signatures.

- **Able to retrieve CRL automatically** after failing on first attempt.

Functionalities:

- Verifies PKCS#7 digital signatures generated by Signing Module.

- Verifies X.509 digital certificates.

- Provides API for extracting information from the X.509 digital certificate and PKCS#7 digital signature.

- Retrieves CRLs from any identified CA's certificate repository (LDAP server).

- Supports multiple entry in LDAP servers search.

- Supports flexible length of IC field in digital certificate.

- Supports both CRL version 1 & 2 from Digicert Sdn Bhd.

- Supports multiple CA procedures.

- Supports multi levels chain CA.

- Supports flexible distinguish name for CRL.

- Supports CRL retrieval using HTTP Server and local directory.

- CRL retrieval failure alert messaging

- Verify Signature supports the requirement of long term validity