Sixscape™ CERTIFICATE MANAGER

The Sixscape Certificate Manager^{TM} is a fully functional Certificate Authority (CA) for implementing a local Public Key Infrastructure. It can function in a centralized mode, with all processes done on the server by admins, or in a decentralized model, using the Sixscape SixWallet client that allows end-users or agents to request and retrieve certificates via IRP. The private keys can be protected by a Thales HSM (Hardware Security Module).

IRP (Identity Registration Protocol) is the first authenticated, secure certificate management protocol (similar to CMP or SCEP, which have no authentication). IRP was allocated port 4604 by IANA. IRP supports both Username/Password authentication and strong client authentication. Our Secure Messaging Applications can do fully automated certificate management via IRP.

The Sixscape Certificate Manager^{TM} is implemented in C#.Net and runs on Windows Server. It is not written in Java, and it is not Open Source. We also avoid web based protocols wherever possible (e.g. for certificate request and retrieval) for higher security. We are working on a FreeBSD based hardware appliance with the same functionality. Our major differentiator is support for IRP, which allows you to hide the complexity of PKI from the end users (e.g. in applications).

Our Certificate Manager^{TM} supports manual RA (Registration Authority) and CA (Certification Authority) mechanisms by separate administrators. We have automated CRL generation and publishing (via HTTP and LDAP), posting of certificates into LDAP, IRP account creation, as well as the RA and CA roles. It is very easy to fully automate even very large and complex CA scenarios. Since we are not implemented as a web application, we can easily create custom deployments and integrate into your existing systems. Most functionality is implemented as Windows services (like UNIX daemons). It is all based on PostgreSQL, either running on Windows Server, or on external nodes (even in redundant deployments). Our IRP allows partially decentralized schemes such as having account execs in a bank provide customers in a branch with soft token or hard token certificates, while the CA is actually located at HQ.

We support creation and management of many kinds of digital certificates, including E-mail S/MIME, XMPP S/MIME (for SixChat), client certs for Strong Client Authentication, Windows Smartcard login, IPsec, etc.

We support any PKCS #11 compliant HSM, but we recommend Thales, for its superior performance, support of newer asymmetric algorithms, and ability to backup and restore key material.

Supported IETF Standards

- X.509 v3 Public Key Digital Cert (RFC 5280)
- PKCS #1 (RFC 3447)
- PKCS #5 (RFC 2989)
- PKCS #7 (RFC 2315)
- PKCS #10 (RFC 2986) – CSR (Certificate Signing Request)
- PKCS #11 and #11 v2.20 – Cryptographic Token and HSM interface
- PKCS #12 (RFC 7292) – Certificate Archive File Format (PFX)
- PEM (Privacy Enhanced Mail) certificate format
- CRLv2 (RFC 5280) - Certificate Revocation List
- OCSP (RFC 5019) - Online Certificate Status Protocol
- RFC 3851 S/MIME v3.1 – Secure Multipurpose Internet Mail Extensions
- RFC 4511 – LDAP v3 – Lightweight Directory Access Protocol

Supported X.509 Certificate Types

- Server cert (on XMPP Server, including server to client authentication)
- Client cert (client to server authentication, S/MIME signing and encryption)

Cryptographic Algorithms

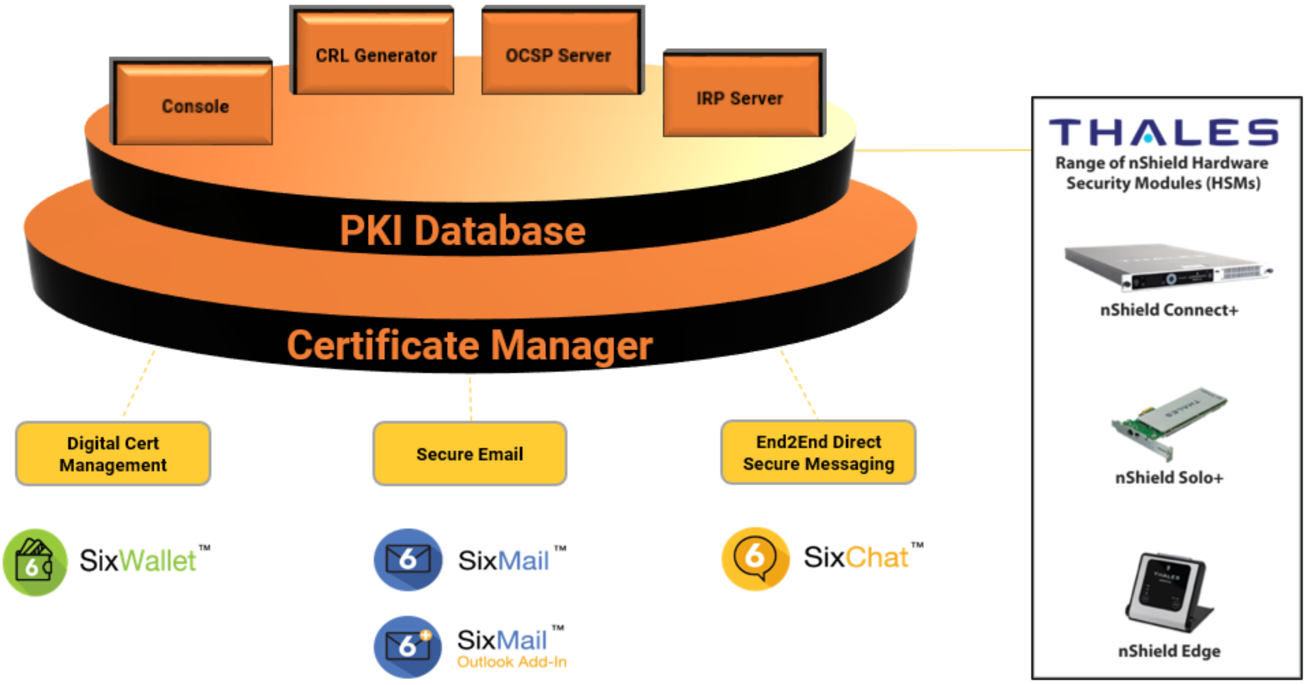
- RSA, ECC/DSA/ECDSA, AES, Camellia, Serpent, SHA1, SHA2, SHA3

Others

- Well suited for enterprise on the Intranet and Extranet
- Works well on both IPv4 and IPv6 infrastructures
- S/MIME v3.1 (with Compressed Data) for reduced transmission size and time

Supported Operating Systems

- Windows Server 2012 R2 or later


CRL Generator
OCSP Server
Console
IRP Server
PKI Database
Certificate Manager
Digital Cert Management
Secure Email
End2End Direct Secure Messaging
SixWallet™
SixMail™
SixChat™
SixMail™ Outlook Add-In
THALES
Range of nShield Hardware Security Modules (HSMs)
nShield Connect+
nShield Solo+
nShield Edge