Secure Commnication Made Easy

Domain Identity Registry Server

The Sixscape *Domain Identity Registry* Server runs on Windows Server 2008 or better. It consists of three components:

- PKI_Tool: A GUI Windows app for doing manual operations, such as creating a certificate hierarchy, issuing requested certificates, creating certificates directly, creating PKCS #12 packages, revoking certificates, etc.
- The DIR Database: This contains all information for the users, certificates, PKCS #12 packages, etc.
- IRP_Server: A multithreaded server application that accepts incoming connections from IRP-enabled clients (e.g. SixChat) and implements the Sixcape *Identity Registration Protocol* (IRP).

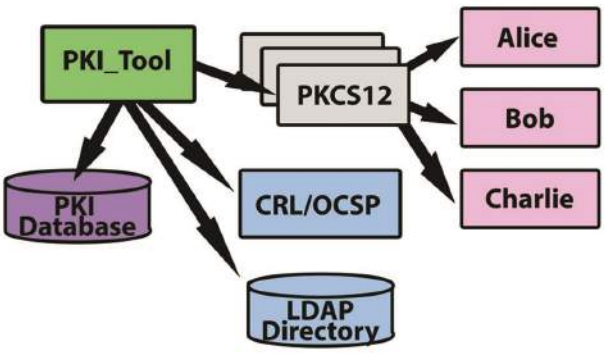
Vendors interested in using IRP in their products should enquire about our IRP SDK product (not included with DIR). Optional DIR components include:

- An OCSP server for legacy clients to determine certificate revocation status
- A connector to publish issued certs in any LDAP compliant directory server (such as Microsoft's Active Directory)
- An Automated CRL Generator
- An Automated Registration Authority function (for the distributed PKI model)
- An Automated Certificate Issuer (for the centralized PKI model)

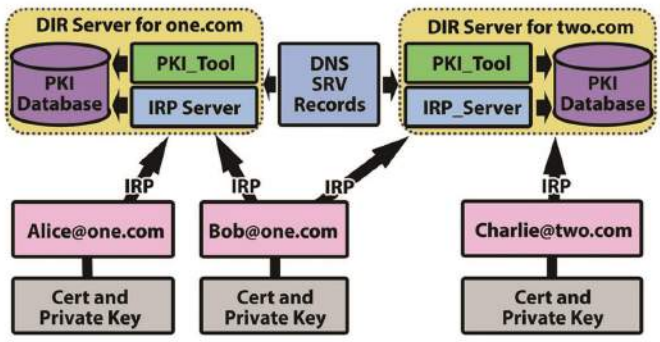
These last two components must be customized for a given organization, and typically require access to the organizations HR or customer database.

DIR is a client/server design, and will run over IPv4 and/or IPv6 (it can accept incoming connections over either IP version).

Centralized PKI (Just PKI_Tool)



Distributed PKI (Add DIR Server)



Sixscape

www.sixscape.com

Since the security of the certificates depends heavily on protecting the CA root and intermediate private keys, we can provide a FIPS 140-2 compliant Hardware Storage Module for the protection of these private keys. These are like a grown-up version of USB security tokens, but can do a large number of public key operations per second, so are suitable for use on a server.

PKI_Tool and IRP_Server are designed to work with the AEP Keyper HSM, but we can add support for other HSMs on a custom basis. We do not recommend running a commercial PKI without this kind of protection for root and intermediate keys.

DIR is licensed to issue a specific number of client certs. Packages are available at various levels, for different sized organizations. We can help you determine hardware requirements for a given number of IRP-enabled clients.

Organizations with customers who need to authenticate to a sensitive website (e.g. banks) can run their own in-house DIR for their customers. Corporates or Government agencies can run their own in-house DIR to provide certificates and secure communications for their employees.

We expect Telco's and ISP's to run public DIR servers on a subscription basis, for users that want to use IRP, much like DNS service is provided today. Also like DNS, the sum total of deployed *Domain Identity Registry* servers constitutes a *Global Identity Registry*. IRP-enabled clients can locate the DIR for any IRP domain (via DNS SRV records) and use it to obtain or verify certs issued by it. DIR helps make password-less authentication and true End2End secure communications practical.

DIR can generate two types of digital certificates: Server Certs and Client Certs

Server certs bind the public key to a device nodename (e.g. www.sixscape.com). They enable SSL/TLS on a server including key exchange for privacy, and provide server to client authentication. Public Server CAs (like VeriSign) can easily verify the information in a server cert (they only need to check your rights to use the domain name and company name). Only one server cert is needed per secure server.

Client certs bind the public key to a person's name and email address. They are issued to people, not devices. Today, client to server authentication is usually accomplished with username/password (which is no longer viable). Client certs allow cryptographic authentication in web based systems, which is far stronger against hacking attacks than username/password. Each user needs a client cert to provide client to server authentication (called "strong client authentication") without any need for passwords. So far more client certs must be issued and managed than server certs (maybe hundreds to millions of client certs for a single secure server).

Distributed PKI Function

What a bank is interested in is not your name and passport, but your identity *as their customer*. An employer is interested in your identity *as one of their employees*. Vetting name and address by an online CA by submitted documents is very expensive (e.g. $150 per applicant). Even then it may not be of value to a bank or employer. They need to verify you as a customer or an employee of theirs. Only they have the databases to verify that information.

We have distributed the PKI function so this information vetting can be done by the people in the best position to do it. We also can handle far larger volumes of certificates by distributing the PKI function, rather than trying to have a single giant CA issue and manage certificates for the entire world. Imagine one giant DNS server trying to provide address resolution for the entire Internet. The volume of server certs is small enough for one centralized CA to handle. Client cert volume is simply too massive for one central CA to handle.

The current online CA's are lacking a single comprehensive PKI protocol. We have created IRP to allow the CAs to be distributed, all over the Internet, in a manner similar to DNS.

Sixscape's IRP makes it possible to embed PKI functionality in applications. This includes obtaining a cert, checking validity and revocation status, renewing a cert, backing up your key material in encrypted form and getting other users' certs to send them encrypted objects. This allows hiding complexity from the user, so less knowledge and training is required. For example, we will be releasing an add-in for Microsoft Outlook that will make it far easier to use S/MIME, compared to using it without our add-in and DIR.

IRP is a major breakthrough in PKI technology, as the first really comprehensive protocol that allows the PKI function to be distributed and embedded in applications. OCSP (one of the few existing PKI protocols) provided a way to check revocation status, but no other PKI functionality. Finally we integrated a scalable address registry into IRP to enable End2End Direct connectivity over IPv6.

SIXSCAPE COMMUNICATIONS PTE LTD

67 Ubi Road 1 Oxley Bizhub #07-10/11
Singapore 408730

Tel | +65 6509 8070 Fax | +65 6509 9667
Email | sales@sixscape.com
URL | www.sixscape.com

Sixscape