Applicability

Authentication of a server certificate is provided by a "trusted third party" called a Certificate Authority (CA) which issues and manages security credentials. As part of a public key infrastructure (PKI), a CA verifies information provided by the requestor of a digital certificate with a registration authority (RA). Certificate request information usually includes the owners public key, name, domain, and dates of validity. If the RA verifies the information the CA will digitally sign and issue a separately controlled server (host) certificate.

The Infrared Processing and Analysis Center (IPAC) is required to distribute and collect information that must have a traceable line of integrity and validity. Access to this information is controlled by passwords in most cases. To insure the confidentiality of the information, and the passwords themselves which are sent over open networks belonging to multiple organizations, some type of encrypted transmission is required. The use of Secure Sockets Layer (SSL) to secure web transactions is convention for internet web based tools. In order to initiate this process in these tools the server host must present a valid (authenticated) server certificate to the client software. The validation, and the ability to verify the authenticity of a server certificate is fundamental to the security of this system. Once accepted by the user, which is often implicit, the use of the CA certificate to verify the authenticity of server certificates is usually automatic. A more detailed discussion of the operation of a CA is beyond the scope of this document.

This document describes the creation of a public key Certificate Authority (CA) for the Infrared Processing and Analysis Center at the California Institute of Technology. The CA provides a traceable authentication of IPAC server certificates to enable secure web transactions over the Secure Sockets Layer (SSL) or other "public key" system. While certificates may be purchased from commercial enterprises like Verisign, IPAC will follow the example of the University of Waterloo, Canada, Massachusetts Institute of Technology and others in establishing a private certificate authority for IPAC.

The purpose of operating an internal certificate authority is to allow the deployment of network based applications that use SSL to encrypt the network session information (such as passwords) in transit. It is important to note that the object of using a commercial certificate signing services such as Thawte, Verisign and the like, is to provide authentication of the server (IPAC in this case) to the client so that the client may have confidence that they are engaged in a transaction with the organization the server claims to represent and so feel more comfortable sending sensitive or confidential information (e.g. credit card numbers) to the server. Use of a private/internal certificate authority does not reduce the functional security of the SSL transactions. IPAC users are expected to derive confidence in the authenticity of the IPAC services by independently verifying the CA certificate and strict application of this standard.
The current role of the IPAC CA is to sign host certificates that enable SSL for IPAC web servers. IPAC CA will not sign certificates for other sites. At this time the IPAC CA will not be used to sign user certificates (SSL client certificates for S/MIME, PGP, GPG encrypted E-mail, Virtual Private Network authentication etc.), for ActiveX objects, for Java applets, etc. However, this CA may be extended to include these services should IPAC determine the need to support them.

**Practice**

**Certificate Authority Creation**

The IPAC CA will be created using OpenSSL v0.9.6 operating on a specially secured workstation located in an IPAC Operations facility which has limited access and physical access controls. The workstation will be dedicated to operating CAs and only approved CA operators will have access. The workstation will not be networked. The Public/Private key pair will be generated on this workstation and the private key will be encrypted.

While the Public certificate must be available to all that would use any certificate that is signed by the CA, access and use of the private key must be carefully controlled. The public certificate will be presented to as the official certificate for identifying IPAC internal restricted accessed services. The CA private key will be escrowed and access controlled by the IPAC Security Engineer.

The IPAC CA will use a 2048 bit RSA digital key, encrypted with triple-DES. This value is arrived at by following common practice of established certificate authorities both commercial and private. The current estimated usable life of such a key is measured in decades. The IPAC CA certificate will be created with a lifetime of 5 years.

**CA Identification - X.509 Entity**

The collection of fields in the X.509 standard header must uniquely identify the entity to which the certificate belongs. The field names in a public certificate conform to the ANSI X.509 standard and follow PKCS guidelines.

The IPAC CA will be identified as follows:

<table>
<thead>
<tr>
<th>X.509 Field</th>
<th>Description</th>
<th>IPAC CA value</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>Country Name (2 letter code)</td>
<td>US</td>
</tr>
<tr>
<td>ST</td>
<td>State or Province Name (full name)</td>
<td>California</td>
</tr>
<tr>
<td>L</td>
<td>Locality Name (eg, city)</td>
<td>Pasadena</td>
</tr>
<tr>
<td>O</td>
<td>Organization Name (eg, university)</td>
<td>California Institute of Technology</td>
</tr>
<tr>
<td>OU</td>
<td>Organizational Unit Name (eg, dept)</td>
<td>Infrared Processing and Analysis Center</td>
</tr>
<tr>
<td></td>
<td>Second Organizational Unit Name</td>
<td>IPAC</td>
</tr>
<tr>
<td>CN</td>
<td>Common Name</td>
<td>IPAC Certificate Authority</td>
</tr>
<tr>
<td>Email</td>
<td>Email Address</td>
<td><a href="mailto:security@ipac.caltech.edu">security@ipac.caltech.edu</a></td>
</tr>
</tbody>
</table>
CA Operation

An advantage of operating a private CA is that new keys can be generated, signed and installed very quickly in the event that new services must be brought online quickly. However, to maintain the integrity of the CA - its value as a trusted entity - the conditions of use (often called "policies") must be established and adhered to. In addition to the information used to create the CA, the following will be the operational policy of the IPAC CA.

CA Certificate Publication

The CA Certificate is required to validate the signature on digitally signed server certificates. The IPAC CA Certificate may be installed in IPAC installations of web browser clients - Netscape, Windows IE, Mozilla etc. The CA certificate may also be published separately such as from an IPAC web server.

Since users of the software, and anyone accessing the secured servers should be able to independently verify the validity of the certificate, at the very least, a checksum (aka "Fingerprint") of the CA Certificate should be available to the user community from a protected site.

Server Certificate Eligibility

Only host/server certificate signing requests (CSR) for certificates to be used on IPAC ISG operated servers providing access to IPAC services with authorization to process from IPAC Management will be signed by this CA.

The IPAC CA will verify with the IPAC Information Systems Group Supervisor, Security Engineer and/or IPAC management the authorization to process and the validity of the CSR, and that the certificate meets presentation criteria before signing or issuing any certificate.

Presentation of CSR

The identification of server entity must match the C, ST, L, O, OU fields of the CA. (Note this is an exact, including all spaces and punctuation, case-sensitive match.)

The CN (Common name) for a host certificate must be the fully qualified domain name of the host (e.g. www.ipac.caltech.edu). The CN must be in the ipac.caltech.edu domain, and the name must be registered with the Infrared Processing and Analysis Center (IPAC) domain authority.

The email address in the certificate request must be a valid IPAC email address corresponding to the operator of the service. Server certificate requests should not use security@ipac.caltech.edu as the email address.

Certificate Signing Requests requests must be sent to the IPAC CA at security@ipac.caltech.edu or delivered to the IPAC Security Engineer by hand on physical media. The CSR must be in Privacy Enhanced Mail (PEM) format and the file must follow the naming convention:

```
hostname_ipac_caltech_edu-csr.pem
```
That is, the CN with dots replaced by underbar followed by the dash, then "csr.pem"

CSRs that don't conform to these presentation criteria will not be signed.

Terms of signed certificates
Another advantage of operating a private CA for IPAC is that the policies encoded in the signed certificates such as period of validity (lifetime) can be determined by the organization. However, good practice for managing certificates indicates certificate lifetimes should not exceed about 2 years. The IPAC CA will sign certificates for one year by default, but requests for up to 2 year lifetimes with concurrence of the IPAC Security Engineer may be granted. Many client software verification policies will refuse to validate a server certificate after the CA certificate has expired even if the server certificate itself is still valid. Therefore, no server certificate will be given a term longer than the current version of the IPAC CA certificate used to sign the request. Note that this implies a second generation CA certificate will need to be generated within about 3 years of the first.

As it is often useful to have certificates for testing new servers shortly before deployment, beta-testing etc. Test CSRs may be presented and will be given a term of 30 days, but in no case more than 60 days. Test certificates may only be used on servers with access limited to within the IPAC domain.

**Protection of server private keys**

Disclosure of a server private key can result in the complete compromise of the services and all the client/user information transmitted in sessions using that key. Protection of the server private keys is the responsibility of the user of the key. Server private keys for IPAC servers should not be written to backup tapes or stored in accessible areas such as on an engineering/development CM system.

**Acronyms**
C - DN Country (Standard 2 letter abbreviation)
CA - Certificate Authority
CN - DN common name (in the case of a server certificate this is the host name)

CSR - Certificate Signing Request
DER - Distinguished Encoding Rules
DN - Distinguished Name
IPAC - Infrared Processing and Analysis Center
ISG - Information Systems Group
L - DN Locality - usually the city component of a Distinguished Name
O - DN Organization (University or other corporate entity name)
OU - Organizational Unit (Division or Department)
PEM - Privacy Enhanced Mail - an encoding format for including binary, possibly encrypted, information in email messages
PKI - Public Key Infrastructure

RA - Registration Authority
SSL - Secure Sockets Layer
ST - DN State or Province

History:

This revision: Version: 1.1/R. Ebert
Effective Date: 2002.11.23
Authority: R. Ebert/IPAC Security Engineer
Description: First issue