Intelligence Community Public Key Infrastructure (IC PKI)
# Intelligence Community Public Key Infrastructure (IC PKI)

**Report Date:** 2002

**Type of Report:**

**Dates Covered:** 00-00-2002 to 00-00-2002

**Title and Subtitle:**

Intelligence Community Public Key Infrastructure (IC PKI)

**Performing Organization:**

MITRE Corporation, 202 Burlington Road, Bedford, MA, 01730-1420

**Distribution/Availability Statement:**

Approved for public release; distribution unlimited

**Supplementary Notes:**

The original document contains color images.

**Security Classification of:**

- **a. Report:** unclassified
- **b. Abstract:** unclassified
- **c. This Page:** unclassified

**Limitation of Abstract:** unclassified

**Number of Pages:** 19

---

*Standard Form 298 (Rev. 8-98)*

Prescribed by ANSI Std Z39-18
Outline

- The US Intelligence Community
- Why is PKI needed on CLASSIFIED networks?
- What is in an IC PKI Certificate?
- Current IC PKI Status
- Notional IC PKI Topology
- MITRE IC PKI/FSD Laboratory
- Certificate Validation
- IC PKI Requirements and Issues
- Conclusion
The US Intelligence Community

Ref: CIA website http://www.cia.gov/ic/contents.html
Why is PKI Needed on CLASSIFIED Networks?

- The ability to establish more secure areas on CLASSIFIED networks is essential to wider release and dissemination of data to the end users
  - Data dissemination that needs to be tracked and controlled
  - Data restricted to those with a “need to know”
  - Compartmented data (beyond the level of the network)
  - Originator-controlled data
  - Data restricted to those on a “by name” access control list
Why is PKI Needed on CLASSIFIED Networks? (cont)

- PKI-enabled applications can include:
  - Secure messaging applications
    - Who sent me that message?
  - Secure Web access and Communities of Interest (COIs)
    - How do I keep other people from viewing this data?
  - Release authorities and disclosure procedures
    - How do I know I can release this information?
  - Mobile Code and object signing
    - Who authored this applet and can it be trusted?
  - Virtual Private Networks (VPN)
    - How can I have a (more) secure connection?
  - Collaborative toolkits
    - Can we establish a (more) secure VTC?
Why is PKI Needed on CLASSIFIED Networks? (cont)

- In addition, agencies are allowed to use the IC PKI certificate for internal purposes
  - Approval documents
  - Electronic workflow applications
  - Restricted access directories and documents
  - Financial forms
# IC Communities of Interest

<table>
<thead>
<tr>
<th>Network Access Control Level</th>
<th>Description</th>
<th>Access Control Mechanism</th>
<th>Server Management</th>
<th>Certificate</th>
<th>Technical Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>General Access</td>
<td>None</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Information available to all network users</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Controlled Access (Simple I &amp; A)</td>
<td>Access may be controlled by non-certificate based controls</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Authenticated (Certificate based I&amp;A)</td>
<td>Valid Community certificate required</td>
<td>Community</td>
<td>SSL</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Restricted Membership - Distributed Control</td>
<td>COI access decision is managed according to rules approved by data owners and the decision process may be centralized or decentralized</td>
<td>Per data owner's consent</td>
<td>Community</td>
<td>SSL</td>
</tr>
<tr>
<td>5</td>
<td>Restricted Membership - Data Owner Controlled</td>
<td>COI access decision is managed by the data owner</td>
<td>Data Owner</td>
<td>Community</td>
<td>SSL</td>
</tr>
<tr>
<td>6</td>
<td>Restricted Membership - Self-Protecting Data</td>
<td>COI access decision is managed by the data owner</td>
<td>Data Owner</td>
<td>Data Owner designates Certificate Authority (Community or other)</td>
<td>Self-Protecting Data -- Data are encrypted in transit and at-rest and are only accessible by authorized user</td>
</tr>
</tbody>
</table>
What is in an IC PKI Certificate?

### Signature Certificate (required elements)

<table>
<thead>
<tr>
<th>Basic Certificate</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Version</strong></td>
<td>V3(2)</td>
</tr>
<tr>
<td><strong>Serial Number</strong></td>
<td>Unique integer</td>
</tr>
<tr>
<td><strong>Issuer Signature Algorithm</strong></td>
<td>sha1WithRSAEncryption</td>
</tr>
<tr>
<td><strong>Issuer Distinguished Name</strong></td>
<td></td>
</tr>
<tr>
<td>Country Code</td>
<td>C</td>
</tr>
<tr>
<td>Organization</td>
<td>O</td>
</tr>
<tr>
<td>Organizational Unit 1</td>
<td>OU1</td>
</tr>
<tr>
<td>Organizational Unit 2</td>
<td>OU2</td>
</tr>
<tr>
<td>Common Name</td>
<td>CN</td>
</tr>
<tr>
<td><strong>Validity Period</strong></td>
<td>012400ZMAY00-012400ZMAY03</td>
</tr>
<tr>
<td><strong>Subject Distinguished Name</strong></td>
<td></td>
</tr>
<tr>
<td>Country Code</td>
<td>C</td>
</tr>
<tr>
<td>Organization</td>
<td>O</td>
</tr>
<tr>
<td>Organizational Unit 1</td>
<td>OU1</td>
</tr>
<tr>
<td>Organizational Unit 2</td>
<td>OU2</td>
</tr>
<tr>
<td>Common Name</td>
<td>CN</td>
</tr>
<tr>
<td><strong>Subject Public Key Information</strong></td>
<td>1024 RSA key modulus, RSA encryption</td>
</tr>
<tr>
<td><strong>Issuer's Signature</strong></td>
<td>sha1WithRSAEncryption</td>
</tr>
</tbody>
</table>
### What is in an IC PKI Certificate (cont)?

#### Signature Certificate (required elements)

<table>
<thead>
<tr>
<th>Extensions</th>
<th>Key Usage</th>
<th>Certificate policies</th>
<th>Subject Alternative Name</th>
<th>Subject Directory Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>email signing certificate:</td>
<td>id-US-level3 ::= {id-certificate-policy 7}</td>
<td>macgari@cia</td>
<td>Nationality=US</td>
</tr>
<tr>
<td></td>
<td>digitalSignature set</td>
<td></td>
<td></td>
<td>EmployeeType=Contractor</td>
</tr>
<tr>
<td></td>
<td>non-repudiation set</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>keyEncipherment not set</td>
<td></td>
<td></td>
<td>Citizenship of user</td>
</tr>
<tr>
<td></td>
<td>Permits use for authentication and non-repudiation only when used with newer S/MIME clients</td>
<td></td>
<td></td>
<td>Employment status of user</td>
</tr>
</tbody>
</table>

“Many legacy S/MIME clients do not enforce functional separation so both the digitalSignature and keyEncipherment flags may be set in some certificates. Since newer S/MIME clients that enforce functional separation are beginning to become available, the IC PKI shall require one S/MIME certificate with the digital signature and non-repudiation bits set and a second certificate with the key encipherment bit set for those clients.” (IC PKI Certificate Policy)

**Note:** fields in red italics mean required but “non-critical” fields
Current IC PKI Status

- Overarching Policy signed October 1999
- IC standup effort currently underway
  - Root: Interim Authority to Operate (IATO) on 24Jul00, final ATO issued 08Aug00
  - NSA: Interim Approval to Test (IATT) Aug00, IATO Sep00
  - CIA: IATT Apr01, ATO Jun01
  - Common Services (IMO) (incl NIMA): IATT Jun01, IATO Sep01, ATO Dec01
  - DIA: IATT August 2001, IATO October 2001, planned ATO Feb02
  - NRO: Planned IATT Mar02(?), planned ATO May02(?)
To ensure certificate validity, certificates must be verified
- Applications may check expiration dates but other checks are not automatic
- Certificates may be revoked for the following reasons:
  ● identifying information or attributes in the end entity’s certificate changes before the certificate expires;
  ● the certificate subject can be shown to have violated the CP or the CPS of the CA who issued the certificate;
  ● fraudulent use or suspected compromise; or
  ● the user or other authorized party (as defined in the CA's CPS) asks for his/her certificate to be revoked
- Two approaches are supported today:
  ● Certificate Revocation Lists (CRLs)
  ● Online Certificate Status Processing (OCSP)
Certificate Validation (cont)

- Certificate Revocation Lists (CRLs)
  - A list of revoked certificates issued by an IC PKI CA
  - Each CA issues their own CRL
  - CRLs are periodically issued to reflect revoked certificates
    - CRLs work on a “push/pull” basis (an issuing CA periodically “pushes” the information out; other CAs periodically “pull” this information in)
    - IC PKI CP mandates a new CRL every 28 days
      - Nonroutine revocations are issued within six hours
    - CRL retrieval is based on organizational need/processes
      - Community applications that understand CRLs must retrieve a CRL at least every 72 hours
    - CRLs need a central distribution point or points
Certificate Validation (cont)

- **Online Certificate Status Processing (OCSP)**
  - OCSP means that a CA automatically attempts to validate a certificate each time the certificate is used.
  - Each CA must maintain an OCSP lookup point wherein the relevant information is located.
  - OCSP works in real time but must as a minimum meet the same mandated deadlines as CRLs (28 days/6 hours).
  - OCSP options:
    - A CA may “push” the CRL to the OCSP responder.
    - A CA may “push” the CRL to the FSD and the responder “pulls” it from there.
    - Some CAs have built-in responders that automatically “pull” the needed data from the issuing CA.
  - Few applications currently use OCSP.
IC PKI Requirements and Issues

- Lack of common IC directory
  - Extensive installed base precludes single common directory
  - Federated approaches make directory-based functionality more complex and may impose more processing overhead
  - Directory is not yet operational even though IC PKI has reached IOC

- Desire to avoid separate operations and maintenance infrastructure
  - Most O&M costs for PKI are labor-related (registration and revocation are manpower-intensive)
  - IC PKI structure mirrors DoD structures as much as possible to allow reuse of already-planned support organizations and procedures
IC PKI Requirements and Issues (cont)

- Absolute need for key escrow
  - Required for counterintelligence purposes
- Auditing and Malicious Code Detection Policies
  - Should an encrypted message be logged and scanned at the gateway?
- Foreign (allied) national access
  - US users of foreign allied networks have a need to access US resources
- PKI deployment and training issues
  - We need good user training materials
IC PKI Requirements and Issues (cont)

- We have a real requirement for “group” certificates with individual audit capability
  - Ease of operations makes it imperative that some messages be sent and received from common addresses and accounts
    - A virus warning would be “signed and sent” from an agency CIRT desk to prove its authenticity; a user would not have to identify John Doe as being the watch officer
    - A watch officer comes on duty to relieve another watch officer and wants to be able to read all emails sent and received from the position during that duty day
    - A question arises about a warning sent by a duty officer position six months ago; who was the individual who sent that official message?
Conclusion

- IC PKI is on schedule to complete infrastructure deployment this year

- In 2002 IC PKI is moving toward
  - PKI enablement of applications
  - Updating original hardware and software configurations
  - User training and education
  - Interim directory deployment
  - Vendor interoperability issues