NetGuard Certificate Lifecycle Manager
Automated Machine Identity Management

NetGuard Certificate Lifecycle Manager (NCLM) is a security management application which provides centralized, secure and cost-effective machine identity management of digital keys and certificates. NCLM helps security and IT operations teams manage and protect the hundreds-of-thousands of keys and certificates throughout an organization. NCLM improves network security posture by reducing risks arising from outdated or rogue digital identities, improves reliability by eliminating service outages due to expired certificates, and lowers operational costs through enhanced automation.

Digital certificates are the most common method for both users and machines to secure communication, authentication and authorization in proven technologies. Enterprises, communication service providers, cloud service providers, and IoT device manufactures are using certificates as fundamental building block within their security infrastructure. However, the increased reliance on keys and certificates may inversely heighten the risk for those businesses. Expired certificates can easily lead to costly IT outages and downtime, while weak and poorly-configured certificates can be used to hijack connections, eavesdrop on network traffic, or manipulate application data.

NCLM addresses these issues and gives security and IT teams full control over their certificate lifecycle management processes. It allows for seamless integration between various public certification authorities (CAs), such as Entrust, Symantec, or Digicert, and enterprise PKIs, like Microsoft CA, Insta Certifier, or Nokia’s NetGuard Certificate Manager. NCLM is an agnostic solution and provides unified management of every single certificate—regardless of the issuing source.

NCLM uses an open platform which supports plugins (or connectors), enabling a seamless integration with multivendor network elements and devices for centralized, single-step certificate deployment. Plugins can be rapidly developed by Nokia, or users can elect to develop their own deployment plugins.
Key features and benefits

Certificate enrollment: Enroll and renew a certificate on behalf of the target system

- Key pair management (generation and deletion)
- Certificate enrollment and renewal from different certification authorities via a plugin-based mechanism
  - Supported CAs: MS-CA, Entrust, NCM
- Certificate browsing and filtering
- Manual PKCS#12 import
- Template functionality to pre-populate certificate attributes or enrollment parameters
- Domain/FQDN whitelisting

Certificate deployment: Deploy and install certificates to a target system

- Configuration of deploy mechanism via plugin-based mechanism
- Automated or manual certificate and key installation and activation
- Deployment templates to pre-populate deployment parameters
<table>
<thead>
<tr>
<th>Certificate monitoring and validation</th>
<th>Status view of certificate enrollment and deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Certificate search and filter capabilities</td>
</tr>
<tr>
<td></td>
<td>Customizable email notification for certificate expiry and revocation status</td>
</tr>
<tr>
<td></td>
<td>Granular reporting and alerting</td>
</tr>
<tr>
<td></td>
<td>Customizable certificate metadata for enhanced asset management</td>
</tr>
<tr>
<td></td>
<td>GUI-based log viewer</td>
</tr>
<tr>
<td></td>
<td>Workflow-based certificate enrollment and deployment</td>
</tr>
<tr>
<td></td>
<td>Certificate benchmarking against “gold standard”</td>
</tr>
<tr>
<td>Certificate discovery</td>
<td>Network scans based on IP addresses or IP ranges</td>
</tr>
<tr>
<td></td>
<td>Service scanning and identification</td>
</tr>
<tr>
<td></td>
<td>Automatic import into NCLM for further certificate management</td>
</tr>
<tr>
<td></td>
<td>Email notification and reporting</td>
</tr>
<tr>
<td>Active directory integration</td>
<td>Active Directory group-based access mapping to target system groups or systems</td>
</tr>
<tr>
<td></td>
<td>Definition of granular access permissions (i.e. read-only, read-write, access to private key) based on user roles</td>
</tr>
<tr>
<td></td>
<td>Role-based access to enrollment and deployment plugin configuration</td>
</tr>
<tr>
<td></td>
<td>“Need to know” principle</td>
</tr>
</tbody>
</table>

**Technical specifications**

**Architecture**
- 3 Tier architecture: GUI / Application / Database
- Active/passive cluster providing high availability with geo-redundant deployment option
- Secure communication between system components

**Deployment modes**
- Bare metal on COTS HP hardware
- Virtualized on KVM or VMware
- Integrated into CloudBand and OpenStack

**Administration**
- Web administration UI with role-based access control
- Support for dual control and separation of duties
- Restriction of access to specific data and operations
- Integrity-protected event logging and audit trail

**SNMP support for monitoring and statistics**
**Email support for reporting and notification**
**Restful API allowing a seamless integration into existing business applications and workflow systems**

**Security features:**
- Workflow-based certificate enrollment including approval rights
- Certificate policies and pre-population templates
- Code signing of deployment plugins
- Certificate monitoring against security baseline

**Supported certificate authorities**
- Microsoft
- Entrust
- NetGuard Certificate Manager
**Supported network elements**
- Nokia service routers
- Cisco WLC, PIX, ASA, ACS
- Juniper routers and firewalls
- A10 load-balancers
- F5 load-balancers
- Microsoft Windows (via WinRM)
- Apache
- NGIX
- Microsoft IIS
- Java Key Store
- AWS
- vIDP cloud service
- and more

**Compliance**
- EU/ETSI qualified certificates
- ICAO Doc 9303, Part 12—Public Key Infrastructure for Machine Readable Travel Documents