

# nCipher keyAuthority™ Solution Suite

## PROVISIONING SYSTEM FOR ENTERPRISE KEY MANAGEMENT AND DISTRIBUTION

nCipher's keyAuthority™ Solution Suite delivers centralized cryptographic key management and automated key distribution to security applications deployed across large numbers of network-attached end-points. keyAuthority helps large organizations to:

- Deliver lower operational costs through central management and automation
- Manage risk by enforcing high-security policies
- Achieve regulatory compliance

### ENTERPRISE KEY MANAGEMENT

The use of cryptography is expanding rapidly as large organizations attempt to secure data wherever it is stored and whenever it moves within their extended enterprise. As more and more sensitive information is exchanged across open networks, cryptography provides a proven way to manage risk and meet regulatory requirements. It can protect high value information, communication channels and business processes through the use of encryption for confidentiality, digital signatures for non-repudiation and digital identities for stronger authentication. From SSL and VPN technology to XML security and database encryption, cryptography can deliver strong mutual authentication and content protection, the foundation stones of security for today's enterprise.

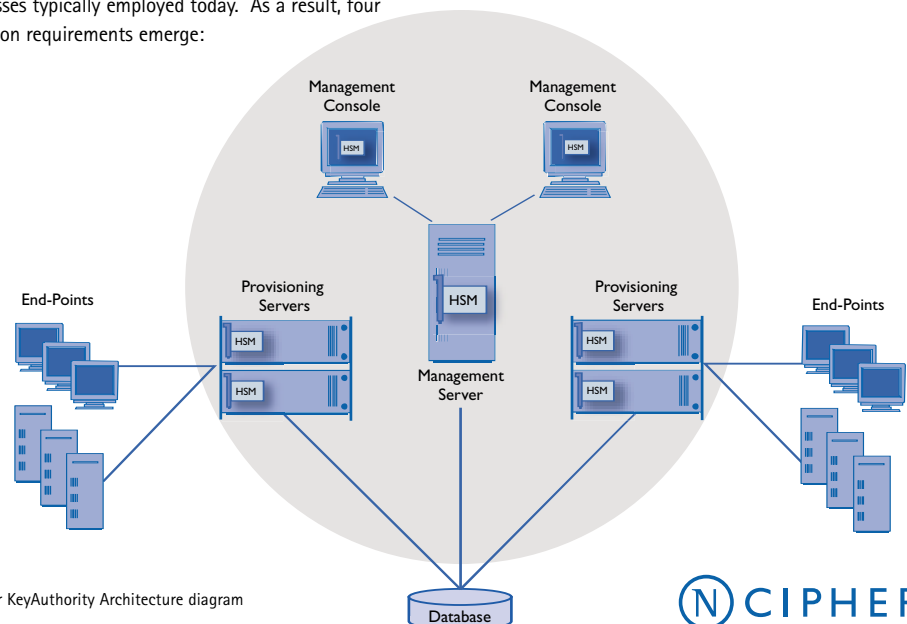
However, many organizations face deployment challenges and significant operational costs as they scale their systems. Providing lifetime management of the private keys and digital certificates across hundreds of applications and thousands of servers, end users and networked devices can easily overburden the manual processes typically employed today. As a result, four common requirements emerge:

- Seamless integration for all applications that support standard Crypto APIs and toolkits
- Automated and resilient distribution of keys and other credentials
- Centralized management, policy enforcement and audit
- Support for a wide variety of hardware end-points and operating systems

### nCIPHER KEYAUTHORITY

nCipher has applied its mature Security World™, Secure Execution Engine (SEE™) and Hardware Security Module (HSM) technologies to provide a solution for Enterprise Key Management – nCipher keyAuthority.

nCipher keyAuthority products allow keys and other security objects, configuration data and security policies to be generated and managed centrally, before distribution to cryptographic applications – on demand, anytime, anywhere.



nCipher KeyAuthority Architecture diagram

FEATURE	BENEFIT
SOPHISTICATED CENTRALIZED KEY MANAGEMENT FUNCTIONALITY	Generates, stores, archives, backs up and retrieves keys centrally. Provides key mobility, key escrow and automated key rolling. Delivers dynamic key and user revocation
RAPID DEPLOYMENT ACROSS DIVERSE SOFTWARE AND HARDWARE END-POINTS	Unified architecture and interface for key distribution that supports standard cryptographic algorithms and key lengths as well as standard security and cryptographic APIs to ensure minimal impact on servers and application software
SCALABLE ARCHITECTURE	Resilient key management and distribution to thousands of geographically-distributed end-points
HARDWARE-PROTECTED SECURITY ARCHITECTURE	FIPS 140-2 Level 3 compliant HSMs provides tamper-resistant security for each system component and supports two-factor, multi-party authentication for system administrators
MIGRATION ROUTE FROM SOFTWARE TO HARDWARE KEY PROTECTION	Future support for server-based hardware security modules (HSM) and next generation Trusted Platform Module (TPM) enabled computers
COMPLEMENTS EXISTING SECURITY INFRASTRUCTURES	Standards-based integration with existing IT infrastructure including PKI certificate authorities, databases, authentication servers, identity management systems and directory servers

## OVERVIEW OF KEYAUTHORITY SYSTEM COMPONENTS

The nCipher keyAuthority Management Server is the primary component of the system and is used to generate and archive keys, establish security policies and enroll end-points through a local management interface.

The nCipher keyAuthority Management Console provides a standalone management interface for the system. Multiple Management Console devices can be used remotely to support the needs of dispersed management teams or different operational functions.

The Database acts as a shared depository for wrapped keys and their associated policies. All interaction with the database uses the industry-standard ODBC interface.

The nCipher keyAuthority Provisioning Server securely distributes keys directly to end-points following a mutual authentication process. Multiple Provisioning Server devices can be deployed for resilience and to provide localized services to geographically-grouped end-points or to reflect a particular customer's internal management structure. Each Provisioning Server is intended to operate in an unattended manner.

## nCIPHER KEYAUTHORITY MANAGEMENT SERVER

Each key provisioning system contains a single nCipher keyAuthority Management Server to centralize the definition and manipulation of security data in relation to security and provisioning policies within the system. This centralized approach unifies control and provides policy enforcement to meet compliance demands.

The Management Server provides flexible and efficient mechanisms to specify which particular application may use a given key. This allows system-wide configurations to be changed rapidly and cost-effectively, for example to switch a business service between computers to meet changing loads or for revoking end-points that are known to have been compromised. The Management Server creates audit records for all changes on system data to facilitate regulatory compliance.

Each key is created with reference to a policy template that defines its lifetime properties, including the key's roll-over schedule. Typically, a security operator will construct standard, enterprise-wide policies that can unify, regulate and simplify the organization's use of cryptography.

The Management Server strongly maintains the integrity of policies, audit records, other data objects using hardware-protected cryptographic mechanisms. In particular, the binding of names to keys and other objects and the association between those objects, is strongly enforced. Integrity is protected by high-security logic that runs within an integral FIPS 140-2 Level 3 validated HSM.



## ENTERPRISE KEY DISTRIBUTION AND MANAGEMENT

### nCIPHER KEYAUTHORITY MANAGEMENT CONSOLE

The requirement for a Management Console arises from the fact that the central Management Server will often be located in a secure facility, making it inconvenient as a primary user interface. The use of one or more Management Consoles enables Security Operators to query and manage centralized data objects from a set of network-connected terminals across the enterprise.

The integral HSM within the Console is also used to enforce strong authentication to the system. A role-based, multi-party scheme is used where, if desired, more than one Security Operator must present their credentials and pass phrases in order to authorize an operation.

Each change to a data object is traceable to a set of credentials, enabling strong audit. Secure connections between a console and the Management Server, maintain security even over untrusted IP networks.

### nCIPHER KEYAUTHORITY PROVISIONING SERVER

To support 24x7 business services, applications deploying cryptography need to be able to request and receive key material with high reliability and resilience. However, most large enterprises operate their critical IT services over multiple, geographically distributed sites. Distributing keys securely in such environments, using traditional methods, is typically labor-intensive and error prone.

nCipher's Provisioning Servers addresses these needs by automating the secure distribution of keys.

For critical applications requiring resiliency, any end point can be configured to request data from multiple Provisioning Servers.

Provisioning Servers can be added to the system at any time as the needs of the enterprise grow. Once installed and commissioned, a Provisioning Server can operate in an unattended manner.

The key provisioning system is designed so that the system protects confidential keys, and other objects that it distributes, to the highest standards available today. Security-critical operations are executed within a FIPS 140-2 Level 3 HSM that is installed on each computer that runs a Provisioning Server. Moreover, the security model keeps the key material confidential from the Provisioning Servers themselves. Therefore, even if a Key Provisioning Server is compromised, these keys remain safe.

This approach allows a Provisioning Server to be located in a relatively insecure location, without compromising the confidentiality of the keys and credentials being provisioned.

## nCIPHER KEYAUTHORITY STARTER SYSTEM

To facilitate system development, integration, training and piloting, nCipher provides a compact version of the Key Provisioning System, called the nCipher keyAuthority Starter System.

The Starter System allows the Management Server, Provisioning Server and a console to be run on a single host computer. The Starter System provides all the functionality of the full system. However, it does not support resilient configuration and the number of end-points that can be enrolled is restricted.

A Starter System provides staff with a useful piloting and training resource:

- System Architects and Security Officers can use the Starter System to help design the operational security environment for the key Provisioning System and for drafting the associated security policies.
- Security Operators can prototype and test their security management environment (use of domains, regions, groups, policy templates, etc.) and train on the use of the Management Console.

A Starter System also allows software developers and system integrators and OEMs to prototype, implement and test applications that integrate with the key provisioning system:

- Make their own applications and end points key provisioning system-aware
- Generate custom reports on the key provisioning system database, for example to make audit logs
- Extend the database schema with custom tables
- Write programs to automate operations and to couple them to other management systems through the nCipher keyAuthority Key Provisioning Management SDK
- Write custom management user interfaces using the KPM SDK.

## END POINT SUPPORT

End-points run applications that use cryptographic keys distributed by the key provisioning system for strong authentication, digital signatures, channel protection e.g. SSL and data confidentiality through encryption.

Some applications will be standard commercial products, for example Web servers, e-mail packages and VPNs. Others may be custom developments that perform specific cryptographic functions.

In almost all cases the application will access cryptographic functionality through one of a standard set of APIs. nCipher keyAuthority supports end-point libraries that provide the following APIs:

- PKCS#11
- CSP for Microsoft CryptoAPI
- Java JCA/JCE CSP
- OpenSSL

keyAuthority also supports integration with other custom applications to enable requests to be made to the key provisioning system for key material and other non-cryptographic data such as passwords and integrity values.

## SYSTEM REQUIREMENTS

The different products in the nCipher's keyAuthority Solution Suite must be installed on a standard host computer that meets the following specifications:

- Windows 2000, 2003
- 2 GB free disk space
- 250 MB RAM
- Database client:
  - MS SQL ODBC client
  - Oracle ODBC client