



# Signal Identity Manager™

## Complete PKI & Token Management for Microsoft® Windows® Server 2003

Signal Identity Manager provides a policy-based, auditable workflow for lifecycle management of client hardware security devices (USB tokens and smart cards) and certificates that integrates seamlessly with Windows Server 2003 Certificate Services, database services, and Active Directory.

Role-specific modular consoles control enterprise-wide identity management functions. The Administrator Console defines enterprise security policies using Business Rules Templates to include registration, enrollment, and approval process for issuing security devices and certificates within specific communities of interest and Hydra PC enclaves.

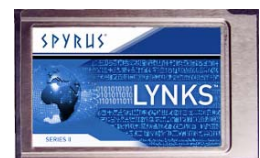
The Operator Console remotely manages Registration Authority (RA) operations such as end-user enrollment, biometric image capturing, Hydra PC enclave assignment, and lifecycle management of all issued security devices and digital certificates within defined Business Rules. Custom Operator Consoles can be configured using flexible Business Rules for specifically defined roles. Roles can operate within designated enclaves and security groups across one or more Microsoft Certification Authorities (MSCAs) in multiple locations within an enterprise.

The Audit console allows for independent review, analysis, and reporting on Signal IM operations based on an enterprise wide Audit Log.

The Client Console permits security device users to remotely manage their own PIN and certificate.

### Benefits and Features

- ▲ Modular console design with user role separation confines enterprise credential management control to those with direct accountability, wherever they are geographically located, providing both higher security and error reduction.
- ▲ Adds scalability, flexibility, security device management, end-user enrollment, and transaction audit capability to Windows Server 2003 Certificate Services and Active Directory.
- ▲ Provides flexible deployment through integration with other identity management functions such as biometric enrollment, and card printing.
- ▲ Custom Request Handlers can be created to implement interfaces to proprietary databases and other directories, such as human resources databases.
- ▲ Business Rules Templates enable custom configuration and enforcement of enterprise security policies and rules of operation, enhancing standard MSCA security policies and certificate templates.
- ▲ The LYNKS Series II Hardware Security Module (HSM) provides a hardware solution to enable management of end user security device keys and ensure business continuity.
- ▲ Consoles integrate seamlessly with Windows.
- ▲ Configurable Evidence of Identity and enrollment functions.
- ▲ Key archiving and recovery.
- ▲ User remote PIN recovery for Rosetta security devices.
- ▲ Full, signed secure audit records.
- ▲ Biometric template enrollment.
- ▲ Token Management Service facilitates central token management with inventories of all credentials stored on each security device.
- ▲ Supports MSCAPI-compliant security devices (SPYRUS security devices recommended: Hydra PC, Rosetta Smart Card or USB, LYNKS USB)



LYNKS HSM  
PCMCIA or USB



# Technical Specifications

## Software Compatibility

- |                                  |  |
|----------------------------------|--|
| ▲ Signal Administration Console  | Windows Server 2003 SP2<br>Windows XP Professional SP2                     |
| ▲ Signal Audit Console           | Windows Server 2003 SP2<br>Windows XP Professional SP2                     |
| ▲ Signal Client Console          | Windows Server 2003 SP2<br>Windows XP Professional SP2                     |
| ▲ Signal Operator Console        | Windows Server 2003 SP2<br>Windows XP Professional SP2                     |
| ▲ Signal Web Request             | Internet Explorer 6.0 or later   |
| ▲ Signal Databases               | Microsoft SQL Server 2000 Enterprise Edition SP4                           |
| ▲ Microsoft Certificate Services | Enterprise Root CA or Subordinate CA configured on Windows Server 2003 SP2 |
| ▲ Microsoft Active Directory     | Windows Server 2003  |

## Hardware Security Devices

- ▲ Client security devices use Crypto Service Providers (CSP) supporting the Microsoft CAPI interface
- ▲ Signal Operator Console requires a LYNKS HSM for hardware-based central key generation and to enable key archiving
- ▲ For higher assurance, Microsoft Certificate Services requires a LYNKS HSM to protect root keys



## SPYRUS, Inc.

For additional details about SPYRUS products, visit [www.spyrus.com](http://www.spyrus.com) or contact us at:

- ▲ USA +1 408 392-9131 [info@spyrus.com](mailto:info@spyrus.com)
- ▲ Australia +61 7 3220-1133 [info@spyrus.com.au](mailto:info@spyrus.com.au)

