nCIPHER

www.ncipher.com

Code Signing Gateway

Service Description

For organizations that need an enterprise-grade, controlled software signing approval process, the Code Signing Gateway provides a range of flexible and centralized workflow automation functions that help software development organizations meet strong security requirements. The Code Signing Gateway is a customer hosted server that runs nCipher code signing workflow applications.

The Code Signing Gateway manages authorization workflow, accepts requests, notifies approvers via email, manages time-outs, acknowledges approvals, logs activity, and delivers signed code to the staging area. The solution utilizes nCipher HSMs and the root of trust – securing all signing keys in a FIPS 140-2 certified HSM. This prevents the potential loss of valuable signing keys – the keys to your code's authenticity and integrity.

The Code Signing Gateway integrates with your Microsoft Active Directory environment to provide user authentication, and manage approval groups.

The Code Signing Gateway can be accessed through a traditional web-based portal, of through a RESTful API, allowing integration into automated build process, or customer workflow engines.

- The Code Signing Gateway offering supports the signing of the following code types:
- Microsoft Windows - .exe, .dll, *.ocx, *.vbs, *.msi, *.html, and all types supported by Microsoft's signtool
- Java – Java archive (.jar), and .cab files
- Generic hash signing

Signature algorithms are limited to those supported by the nCipher nShield HSM. Other platforms and signing utilities are available under a custom Statement of Work, including:

- Android applications – through apksigner
- iOS/iTunes
- Custom firmware/device signing

Integration with existing automated build platforms, workflow engines, ticketing systems, or reporting products is available under a Custom Statement of Work.

Purchase of the Code Signing Gateway ("CSGW") Service (PS-DEV-CSGW) includes the following components:

- Onsite installation of the CSGW on customer supplied hardware
- Integration of the service with the customer's Active Directory environment
- Integration of the CSGW with an existing nCipher HSM environment (requires Security World v. 12.10 or greater)
- Configuration of sample workflows and signing profiles
- Training of up to 4 code signing administrators

This engagement provides the following deliverables:

- A pre-engagement planning meeting to review the customer requirements and environment. Pre-requisites required by the customer will also be reviewed
- Code Signing Gateway Administrators Guide
- Code Signing gateway API Guide
- Installation of Code Signing Gateway application
- Training for up to 4 Code Signing Gateway administrators
- Sample profile configuration (up to 4 sample profiles)

nCipher submits the deliverables to you in electronic format, specifically a Microsoft Word document compatible with MS Office 10 or higher within five (5) business days after the end of deployment. You have five (5) business days to review the deliverables, edit and/or append comments, and return them to nCipher. Upon receipt of those edits, nCipher prepares a final deliverable submission.

nCipher typically performs this service on-site. Any travel, lodging, or sustenance expenses for on-site service delivery are NOT included in the scope or price of this service offering. The Customer agrees to reimburse nCipher for reasonable travel costs incurred during the execution of this Service Offering.

Successful deployment requires the following customer activities and resources:

- Existing nCipher HSM environment for storage of signing keys, with Security World 11.72 or greater installed. A cluster of two or more HSMs is recommended.
- Customer must supply and Windows 2012r2 (or greater) server with the .NET framework installed. This can be a virtual machine.
- Customer must supply a SQL Server 2012 sp4 (or greater) instance for storage of request metadata. This can be a virtual machine.
- Customer must supply a network file share for the purpose of storing signing code.
- Customer must configure firewall rules to allow access from the CSGW to the HSMS, and the CSGW to the SQL server. In addition, users must be able to access the CSGW.
- Customer must provide access to their Microsoft Active Directory instance to provide the CSGW with the ability to authenticate and read/manage groups.
- Customer ensures systems are available to nCipher during the scheduled professional services hours of 8:30 am to 5:00 pm in the Customer's time zone, unless alternate hours are agreed to in advance. Alternate hours may impact scheduling and travel costs.
- Customer ensures access to all deployment related key personnel, including:
  - System administrators
  - Network administrators

This Service Description incorporates by reference and is governed by all of the terms and conditions contained in the Professional Services Terms and Conditions, which can be obtained from **go.ncipher.com/rs/104-QOX-775/images/nCipher-PS-Terms-and-Conditions-January-2019-Final.pdf**, unless the Customer has an existing Master Services Agreement ("MSA"), in which case the terms of that agreement shall govern.

This Service Description is the property of nCipher; the contents herein are the intellectual property and copyright of nCipher. Disclosure of this document and its contents herein does not grant or construe any transfer or other rights in relation to nCipher intellectual property.

SKU: PS-DEV-CSGW

Copyright ©2019 nCipher Security, Inc. All Rights Reserved.