Honeywell

SwiftDecoder™ SDK

Security Manual

Disclaimer

Honeywell International Inc. and its affiliates, subsidiaries, and other entities forming part of Honeywell group (“HII”) reserves the right to make changes in specifications and other information contained in this document without prior notice, and the reader should in all cases consult HII to determine whether any such changes have been made. The information in this publication does not represent a commitment on the part of HII.

Honeywell warrants goods of its manufacture as being free of defective materials and faulty workmanship during the applicable warranty period. Honeywell’s standard product warranty applies unless agreed to otherwise by Honeywell in writing; please refer to your order acknowledgment or consult your local sales office for specific warranty details. If warranted goods are returned to Honeywell during the period of coverage, Honeywell will repair or replace, at its option, without charge those items that Honeywell, in its sole discretion, finds defective. **The foregoing is buyer’s sole remedy and is in lieu of all other warranties, expressed or implied, including those of merchantability and fitness for a particular purpose. In no event shall Honeywell be liable for consequential, special, or indirect damages.** While Honeywell may provide application assistance personally, through our literature and the Honeywell web site, it is buyer’s sole responsibility to determine the suitability of the product in the application. Specifications may change without notice. The information we supply is believed to be accurate and reliable as of this writing. However, Honeywell assumes no responsibility for its use.

Web Address: automation.honeywell.com

For patent information, refer to www.hsmpats.com.

Honeywell Data Policy: www.honeywell.com/privacy-statement.

TABLE OF CONTENTS

Chapter 1 - Security 1

Intended Audience 1
Prerequisites 1
Product Summary 1
Secure Development Life Cycle Process 2
Third-Party Cooperation and Certification 3
SwiftDecoder SDK External Connections 3
Security Checklist 3
Technical Assistance 5

CHAPTER

1 SECURITY

Intended Audience

This manual is intended for use by developers which are employed by the customers who are managing an implementation of the SwiftDecoder™ solution into mobile applications other devices include hand-held scanners, manual presentation scanners, and fixed station automation scanners using two-dimensional area sensors.

Prerequisites

This manual assumes a high degree of technical knowledge and familiarity with SwiftDecoder and their respective security practices.

Product Summary

SwiftDecoder is a barcode decoding Software Development Kit (SDK)— not a barcode scanner—packaged for developers, Independent Software Vendors (ISVs), and other Original Equipment Manufacturers (OEMs) that develop barcode scanning apps or custom barcode scanning solutions. SwiftDecoder offers the "M" version for mobile platforms, including Apple® iOS®, Android™ and Windows™ UWP (Universal Windows Platform), and the "S" version for non-mobile platforms, including Windows™ Desktop, Linux Foundation™, and Embedded OS. SwiftDecoder SDK is available under license from Honeywell.

Developers are looking for a barcode decoding solution that rivals the best commercial scanners. They need a decoding SDK that is easy to integrate and offers many configuration options to fit their applications. They require an SDK that will adapt to support the latest development environments as smart phones and operating systems get updated. Many developers can benefit from software integration support.

Secure Development Life Cycle Process

Honeywell has developed a robust system for considering security at the outset of product conception and during development, as well as responding to potential vulnerabilities in existing products. This system, Honeywell's Secure Software Development Life cycle (SSDLC) initiative, has evolved and grown even more robust over the past few years.

Honeywell takes product security seriously. Our products go through a robust and comprehensive penetration testing regimen. In some cases, additional independent security testing is conducted. The criteria for this additional testing as well as which products or offerings are selected for this are closely held proprietary information.

We have a robust and comprehensive Secure Development Life Cycle (SDLC) based on best practices and industry standards that includes the following:

- Security Risk Assessment based on the threat environment faced by a particular product or offering as well as the technical features and customer needs
- Security Requirements and security controls based on industry standards and others depending on the product or offering and the Security Risk Assessment
- Privacy Impact Assessments
- Threat Modeling
- Secure by Design, Privacy by Design and Secure Coding standards and practices
- Static Application Security Testing (SAST, also known as source code scanning) to enforce secure design and coding practices. We scan for OWASP Top 10 and SANS Top 25 vulnerabilities as well as for language-specific quality measures. Current SAST tools include SonarQube and Coverity depending on product and language needs.
- Binary scanning to identify open-source usage and potential vulnerabilities.
- A formal Risk Management Policy that requires specific mitigation timelines based on severity
- Review and approval of cybersecurity by senior leadership prior to product shipment

An audit team of Honeywell performs checks to ensure that security deliverables required under Honeywell's Secure Development Life Cycle processes are completed.

Honeywell completes training programs for its employees on the company's security process and on specific cybersecurity concerns and solutions. All software engineers in Honeywell receive formal training on the Secure Development Life Cycle process and general cyber/product security topics.

Third-Party Cooperation and Certification

Like Honeywell, companies across industries have become more sophisticated about cybersecurity, and the set of resources and tools available to improve and assess security programs likewise has grown dramatically. Honeywell uses the experience, tests, and certifications of third parties to manage its supply chain from the cybersecurity perspective, specifically tracking vulnerabilities associated with the software and hardware components provided by outside vendors. Increased awareness can help Honeywell identify where and how to apply security measures.

SwiftDecoder SDK External Connections

SwiftDecoder SDK barcoding scanning solutions is basically a licensed software. The SDK activates license using the specific license key provided to customers. The license activation process mainly involves communication to a license server. This license server could be in cloud or on premise based on customer requirement. Both cloud and on-premises solutions are supported by the SDK.

Activation using Cloud Server

The communication to the cloud license server is strictly over HTTPS channel which handles the required security for transferring the license key to the sever and get the activation response.

Activation using On Premise Server

For on premise installation Honeywell provides the complete server installation package. Usually, this on-premises server is termed as “Local License Server” while communication to customers. Current release of SwiftDecoder SDK communicates to server over a non-secure (HTTP) channel. Customers installing this local sever for license activation should have required security restrictions to local area network in which devices are connecting to server. Future version of SDK is planned to bring in the support for secured (HTTPS) connection to the local license server. The expectation of Honeywell is that the customer should have some form of network monitoring in place and devices accessible to the network should be handled responsibly. Only authorized devices should have access to the network.

Security Checklist

Securing SwiftDecoder License Key

You are responsible for keeping the license key safe and will bear responsibility for any misuse of the license key or unauthorized transfer to any third party.

Android Minimum and Target SDK Version Updates

From the 6.0 SDK releases specific to Android, the minimum Android SDK version is updated to 29 and the target Android SDK version is updated to 34 for increased cyber security. We recommend using targets with Android SDK version 29 to be the minimum SDK version as Google has stopped support for earlier Android SDK versions. We allow our customers greater flexibility for older devices by setting the minimum requirement lower in the SwiftDecoder SDK, however end application developers are advised to follow best practices as indicated by Google to avoid any security issues.

Infection by Malicious Software Agents

- Ensure virus protection is installed, signature files are up-to-date, and subscriptions are active on all machine hosting Honeywell Products.
- Allow only digitally signed software from trusted sources to run.
- Use a firewall at the interface between other network and Swift Decoder solution components.

Security Updates and Service Packs

- It is critical to keep the latest patches and software versions on all operating systems that support components of your Swift Decoder solution.

Unauthorized Internal Access

This threat encompasses unauthorized access from people or systems with direct access to a Swift Decoder solution component. This threat is most difficult since attackers may have legitimate access to part of the systems are simply trying to exceed their permitted access

- Do not allow the use of unauthorized removable media on Swift Decoder solution components.
- Monitor system access of the application.
- Implement strong password protection on Swift Decoder solution components and include a password lifetime management policy, reuse policy and strength of policy for passwords

Accidental System Change

This threat encompasses inadvertently changes to executables or configurations files

- Set the minimum level of privilege for all accounts, and enforce a strong password policy.
- Ensure string access controls are in place on the file system, directory, and file shares.
- Ensure user account control is enable on relevant operating systems.
- Maintain regular server and database backups.

Inter-Domain Trusts

- It is important to limit inter-domain trust, that is not to trust other domain users to log on unless necessary, if no trust exists, administrators can be assured that no access to systems resources can be accessed for users from other domains.
- If trust is necessary, then the “least access” principle should be followed: that is only have the trusts that are required. Use a one-way trust if possible. Explicitly trust can be configured between systems domains.

Third Party Applications

- In instances where a third-party application must be added to the Swift Decoder, always verify the following with the vendor.
    - Secure Development Life cycle (SDL) practices were used when writing the software.

Technical Assistance

Refer to the respective Software Integration Guide document packaged along with SDK for details on integration, references, and troubleshooting.

Honeywell
855 S. Mint St.
Charlotte, NC 28202

automation.honeywell.com