KEYWATCHER
AUSTRALIA

AUSTRALIAN SECURITY TECHNOLOGY PTY. LIMITED
TRADING AS **KEYWATCHER AUSTRALIA**
ABN: 68 002 952 936
PO BOX 345
SEVEN HILLS, NSW, 1730
☎ (02) 8020 5555
SALES@KEYWATCHER.COM.AU
WWW.KEYWATCHER.COM.AU

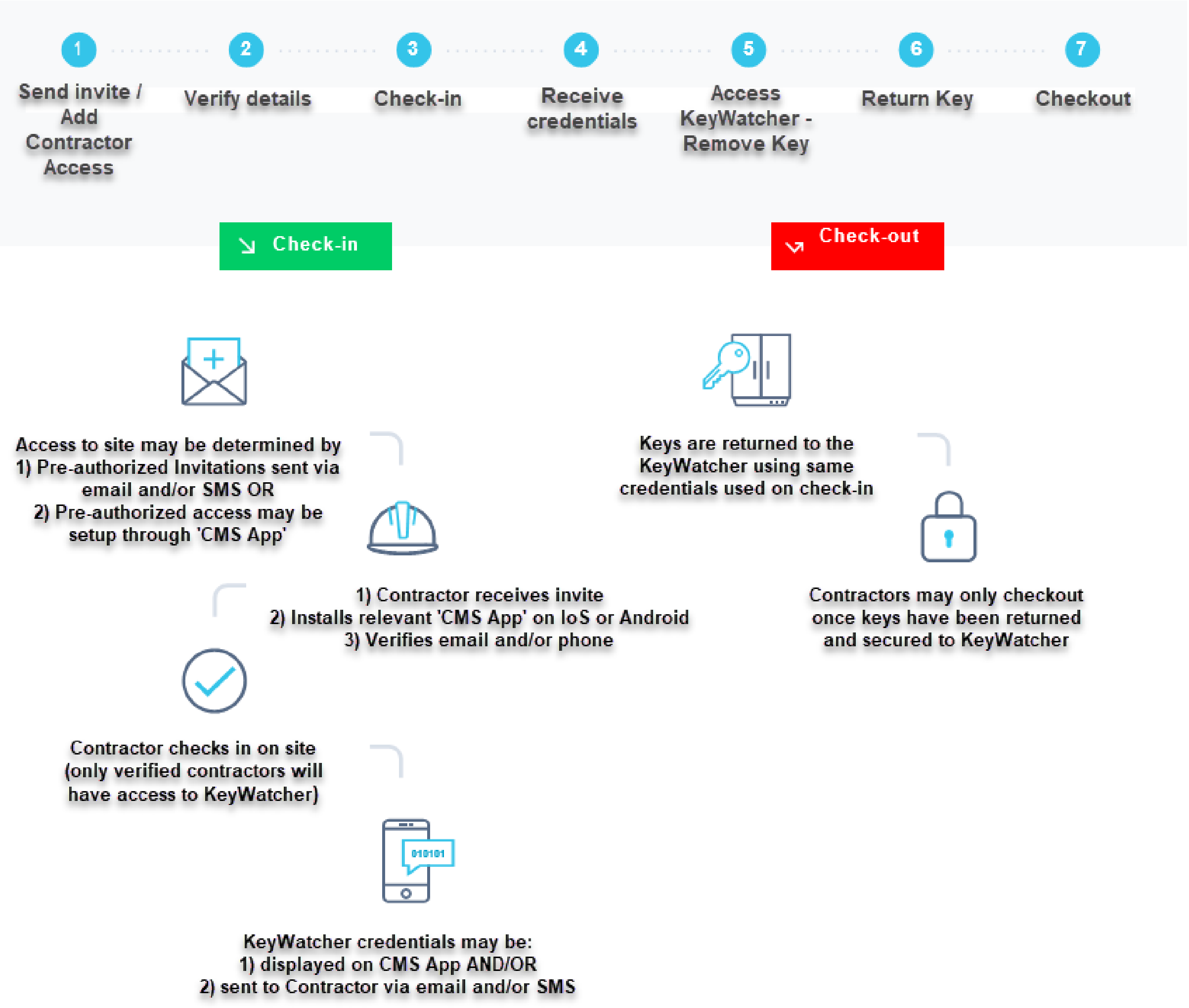
KeyWatcher & Contractor Management Interface Specification

Introduction

This document captures the requirements for a successful interface between the KeyWatcher (KW) product and a Contractor Management Solution (CMS).

Summary

The desired outcome will provide a Facilities Manager with the ability to closely control access to site without having to manually handle on site inductions and the issuance of property keys and assets. Contractors and Visitors may receive invitations to attend site through the CMS and would have the ability to remove and return keys via the CMS on site induction process. Successfully checking out of the CMS would ensure that all property keys are secured on site so that no property keys leave site.



1 Send invite / Add Contractor Access

2 Verify details

3 Check-in

4 Receive credentials

5 Access KeyWatcher - Remove Key

6 Return Key

7 Checkout

Check-in

Check-out

Access to site may be determined by
1) Pre-authorized Invitations sent via email and/or SMS OR
2) Pre-authorized access may be setup through 'CMS App'

1) Contractor receives invite
2) Installs relevant 'CMS App' on IoS or Android
3) Verifies email and/or phone

Contractor checks in on site (only verified contractors will have access to KeyWatcher)

KeyWatcher credentials may be:
1) displayed on CMS App AND/OR
2) sent to Contractor via email and/or SMS

Keys are returned to the KeyWatcher using same credentials used on check-in

Contractors may only checkout once keys have been returned and secured to KeyWatcher

Compatible Hardware and Requirements

- ***'KeyWatcher Touch (KWT)'*** model provides a touch screen access point
- ***'KeyWatcher Illuminated (KWILL)'*** model provides a two-line LCD and metal keypad access point
- ***'GPO (electrical power-point)'*** is required for either model. A standard 10amp GPO may be fitted and terminated inside the cabinet so as not to be tampered with. Templates for the various sized cabinets may be supplied to outline where in the cabinet this service may be fitted.
- ***'Android or IOS device'*** may be used for CMS App
- ***'Wireless Comms'*** equips the KeyWatcher with a ***'4G modem'*** and an ***'IPSEC VPN'*** for added security
- ***4G Signal'*** at the location where the KeyWatcher is fitted should provide at least 1 bar of reception. If 4G reception is NOT achievable then a '***Data cable'*** will need to be supplied and run to a location on site where 4G reception is available and where the 4G modem may be installed.
- ***'Secure KeyRings & Accessories'*** should be used when attaching property keys and assets with the KeyWatcher SmartKey
- ***'Biometric Access'*** is available with the KeyWatcher *'Touch'* model only. Provides added security and replaces the requirement for UserID/PIN credentials.
- ***'Galaxy or BiLock'*** Cam and Barrell replacements for KeyWatcher override and service access may be supplied to suit on site master keying system

Compatible Software and Requirements

- ***'KMaaS'*** abbreviated for *'Key Management as a Service'* provides a REST API for CMS providers to interface with the KeyWatcher product. Also provides the administrator with management tools for the KeyWatcher hardware such as Database management and audit reporting & notifications. Please refer to documentation labelled *'KeyMaaS - Integration Guide v3+'*
- ***'Contractor Management System (CMS)'*** should have the ability to integrate using a '***SOAP or REST'*** based API. Should have the ability to communicate via ***'webhooks'*** or similar. Can provide access to contractors / visitors via personally owned Android and/or IOS device or provide an on-site Android and/or IOS tablet.

  Note: *all entries managed at the CMS 'app' should have the ability to create/modify/delete entries in the KMaaS app using an integration method such as webhooks. Manual marrying and dual data entry should not be acceptable*
- ***'AWS or Azure'*** cloud environments provide added security for data integrity and protection

Features / Functionality

- ***'Access to site for contractors/visitors or employees'*** may be managed in a few different ways.
  - Deployed via an invitation through the CMS administration 'app' where an email and/or SMS is sent to contractor/visitor outlining on site attendance requirements and pre-approving KeyWatcher access

  - Setup 'ad-hoc' in the CMS administration 'app' when required
  - Setup in the KMaaS 'app' would bypass the CMS process. Normally done for employees and permanent site staff

- ***'Check-in & Check-out Devices'*** may be either IOS and/or Android.
  - If a fixed asset on site is used, the device should be allocated within the vicinity of the KeyWatcher.
  - If a personally owned IOS and/or Android is to be used the ability to check-in and check-out should be made available only when in vicinity of the KeyWatcher or when on site. Typically, a geo-fenced location may be used.
- ***'KeyWatcher credentials'*** should be provided to the contractor upon successful check-in on site. Instructions on how to remove and return keys from the KeyWatcher should be provided with the delivery of the credentials and which may be either:
  - Displayed on the CMS IOS/Android device OR
  - Sent to the contractor/visitor via email and/or SMS

  The KeyWatcher credentials should only be valid whilst the contractor/visitor is signed into the CMS. This will prevent users from re-using the credentials at another time and should always prompt the user to access keys through the CMS process.
- ***'Removing & Returning Keys'*** When credentials are presented at the KeyWatcher, the user may be presented with the option to remove or return keys.
  - When removing keys, the front door of the KeyWatcher should unlock and illuminate the slot of the set of keys which are to be removed. All other keys sets should be locked in place.
  - When returning keys, the front door of the KeyWatcher should unlock and allow the user to return the key to 'any' available and empty slot in the cabinet. All other keys sets should be locked in place. The ability to return keys to any available slot adds security to the site though preventing others from learning where keys are in the cabinet (in fixed locations)
- ***'Instant Key Release Functionality'*** should allow the contractor/visitor to simply type in a 9-digit number (KWILL) or an 11-digit number (KWT) at the KeyWatcher access point to remove and return keys. The cabinet should automatically identify the key-access programmed against the credentials and open the front door of the KeyWatcher and illuminate the slot of the set of keys which are to be removed. This functionality prevents the need to navigate through the KeyWatcher remove/return key menus.
- ***'Property Keys & Assets'*** should remain on site at all times. The contractor/visitor should not be able to check-out of the CMS till all 'checked-out' Keys/Assets have been returned to the KeyWatcher. This prevents important property keys and assets being removed from site and posing as a security concern
- ***'Notifications'*** around the movement and overdue use of property keys should be automated and distributed via Email and/or SMS. Notifications should be 'Escalatable' till the alert is rectified.
- ***'Reporting & Access'*** from both the CMS and KMaaS should be assigned to an individual and NOT against a Company profile. Ie: KeyWatcher credentials should be assigned to the contractor/visitor and not the organisation that the contractor/visitor represents. This allows the system to keep each contractor/visitor responsible for site access.