Time and Attendance Security and Data

Secure transfer of our time and attendance data is of the utmost importance to ClockedIn. The data transfer has a number of levels of protection to avoid issues of external data capture.

The data security measures are listed below:

- All the data is encrypted:
- To Protect our application from external threats, the API & database are encrypted using AES and RSA Cryptographic Algorithms.
- SL security on server
- Android Operating System is safer than other operating systems, at the operating system level the Android platform provides the security of the Linux kernel
- Secure inter-process communication (IPC) facility to enable secure communication between applications running in different processes.
- No lottery-themed and similar ADS that have the potential to interrupt and start using our device.
- The device itself is secured within a kiosk which is locked, this mitigates external threat of accessing ports such as Micro USB.
- The operating system is set to run the OnTime app in 'Kiosk' mode which means a user cannot navigate to other areas of the operating system. Only users with 'Super Admin access' can exit out of the OnTime application.
- Wi-Fi network firewall - customer internet policies would apply.

We maintain state-of-the-art technical and organizational measures in order to ensure data security, in particular for the protection of all Personal Data. These measures are updated from time to time in order to remain at the forefront of technology.

A typical user finger scan data string would be double encrypted – Sample Below

AwFjFYJN4ADAAMAAgACAAIAAgACAAIAAgADAAPAC//7//v/+//7//gAAAACCAgc5aUASBAAV
HQJVBFNeGQgoXl0JU349i5EeFgxPHnOREn51Gw9+HKHiXiYjY55MLeS+dAgUf06SEB9ml5D/EJt
hf3Aijj9VIs7/a5OQ3UehpR1Gm+Z6SxuOm00i5lsAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA==

ClockedIn
1C Uppingham Gate, Ayston road, Uppingham, Rutland, LE15 9NY
0845 4 903 901 | info@clockedin.co.uk | clockedin.uk

A typical user facial scan data string would be double encrypted – Sample Below

AID6RAAAnELpjgq+dpe6PVjhLD2GVzo86t8FvCt0yL3JqgY9cuQ7Pel5zr1GqPQ7IQO0vZvnQLwk
vKq8uP5nvaUq/rxkHHW8J7JyvNNdIT0Bd0C9jZJuPOVdpz0VxQ69tdEIPIMDJ73Mgzg+WaoZvN
fK
3j2/PKs9/Iz2PDgxSD2YXUi8bOKOPTYEjT3AO0S9ngzpPC0jW72tFuy8cmQGvGW2vb2vvAy9H1j
ive6N9Lx44n87zy8LvYaZJr3OScG8hcmuPdtyjj3uMVu9X1m/PH56DjxhKys9nP1Bu33ahj0xj1s9

These data strings can only be unencrypted by the algorithms created by ClockedIn

Data Size

The below are approximate data sizes of time and attendance events and biometric templates:

Attendance event (1 event) – 2-3Kb

Biometric Facial Template – 20-25Kb

Biometric Finger Template - 20-25Kb

ClockedIn
1C Uppingham Gate, Ayston road, Uppingham, Rutland, LE15 9NY
0845 4 903 901 | info@clockedin.co.uk | clockedin.uk