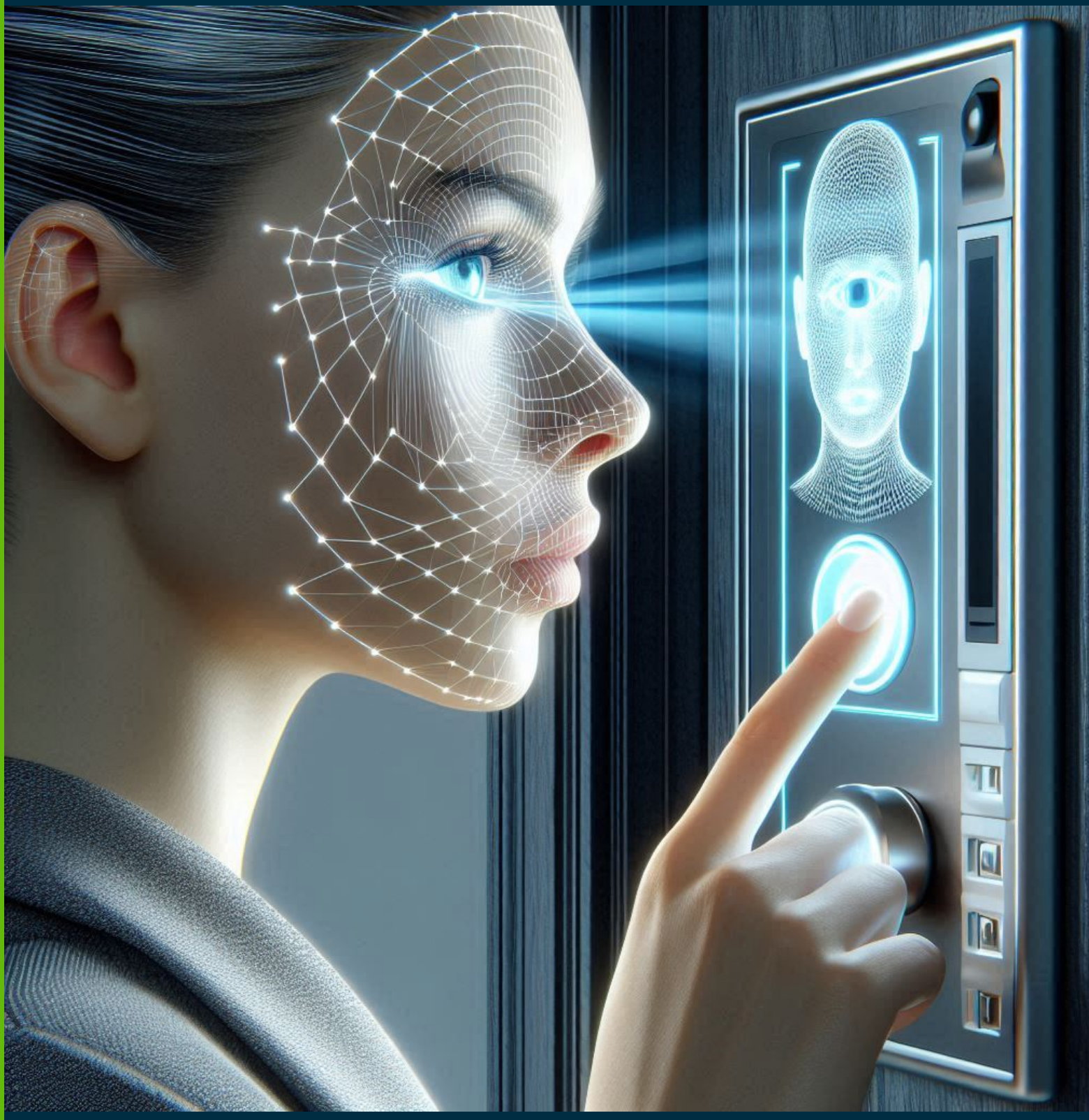
ID-BIOMETRIC ACCESS CONTROL

Multi-modal Biometric Integration Platform



IDENTITY MATTERS

Access Control with Biometric Attendance

Solution Technical Summary

ID-INTEGRATE allows the use of any biometric capture/authentication device (as well as RFID cards) to be used with existing or future time and attendance systems.

ID-INTEGRATE bridges the gap where your selected or existing time and attendance system lacks the interoperability or, where required, you need biometric matching capability.

We can support most of the main capture and authentication devices on the market with or without biometric components. These can be USB enabled devices on a tablet (Android or Windows) and Windows PCs, Network enabled devices using server based or stand alone biometric matching, and even E-gates and boom gates.

For initial testing we used the CMITech EF-45NC was selected and used to build and test the ID-INTEGRATE (a key component of our Access Control Solution).

ID-INTEGRATE allows a quick and easy connection between your biometric and identification devices and on-premise and cloud-based solutions via web services.

It provides a built-in ANSI/NIST-ITL standard interface for exchanging demographic and biometric data with enterprise application servers in your domain or with other external agencies.

ID-INTEGRATE runs on Windows and Android platforms as a background service and user interface. It uses an encrypted database to fill the gaps when your back-end systems do not meet your biometric requirements.

ID-INTEGRATE will dynamically load a library (built by us or you) that hooks into your identification device's SDK. This library communicates via standardised tasks and queues to communicate to the back-end. This eliminates the need to build a system from scratch.

ID-INTEGRATE can communicate with a time and attendance back end over an API layer (again built on predefined tasks and queues). We have integrated NCheck (developed by Neurotechnology) which provides a robust biometric attendance application. Together with ID-INTEGRATE and NCheck we provides a fully functional service.

With its onboard matching the EF-45NC will allow continued, logged, secure access when the back office systems are not available while local power is available. ID-INTEGRATE will distribute the required biometric data to all registered devices for a user - ensuring simplified management of users access.

ID-INTEGRATE will provide on-server matching and authentication where multiple biometrics may be registered - providing different access requirements.

NCheck

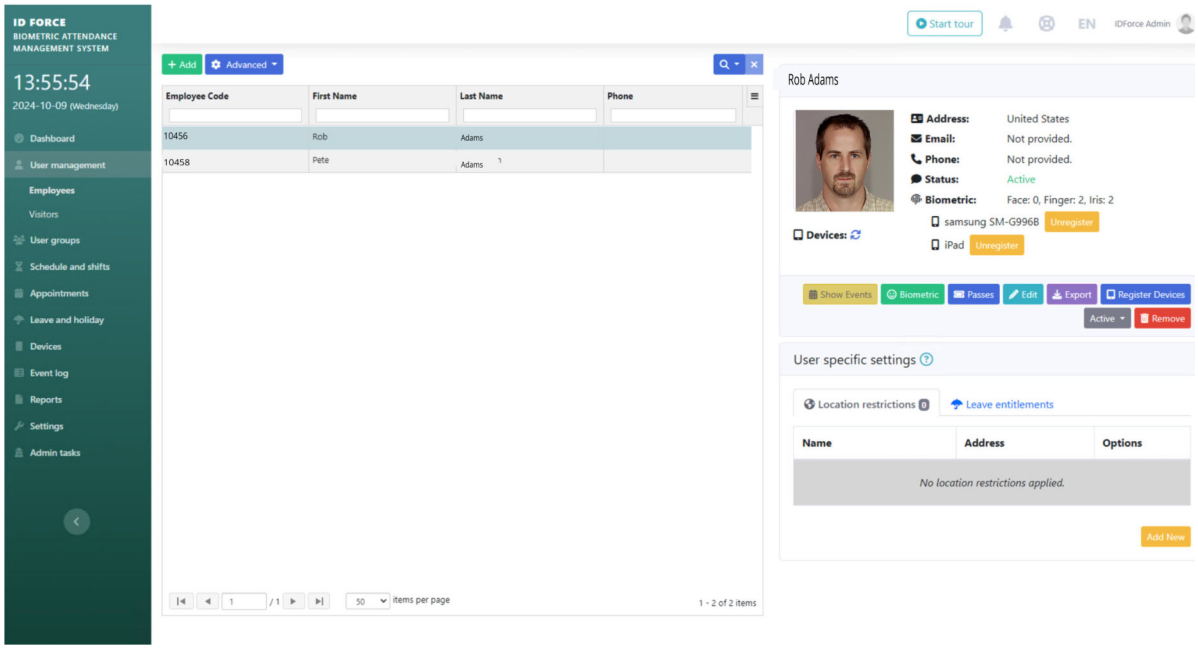
Provides an events and user management feature. It supports schedules, shifts, and appointments. You can create user access passes as well as calendars and schedules with leave and holidays. Through the management console, you can add a number of different devices depending on the requirements.

NCheck has a Windows client that can power any USB-connected devices or using ID-INTEGRATE we communicate directly to the preferred device.

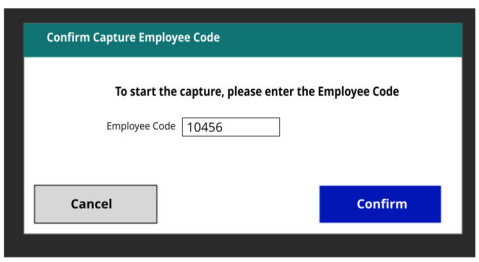
All operations have an event logged and provide logging-in and logging-out information. This can be viewed in real time when you may have logged in to a fingerprint device and logged out with an Iris device.

Operational Process

Admin - User Management Screen

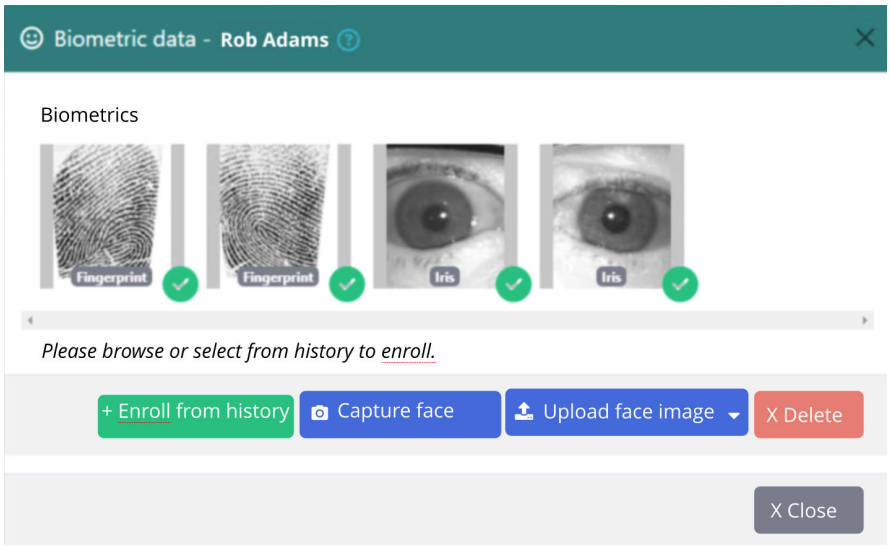


User Enrolment



After entering allocated employer code you capture the biometric modalities* selected. In this case we capture dual Iris's and Fingerprints.

***NOTE** *ID-INTEGRATE allows our system integrators and/or customers to easily add biometric devices and provide a connection back to the NCheck Time and Attendance solution.*



For this explanation, we will use the EF 45NC IRIS and Fingerprint scanning devices to show the enrolment process. The EF NC45 can capture left and right irises and a face photo that is compliant with NIST standards.

The NCheck enrolment management desk will ask for a user/employee code, name, and details, and once this is done you can connect to the selected device (in this case ER 45NC). Location information is also added to the person's record.

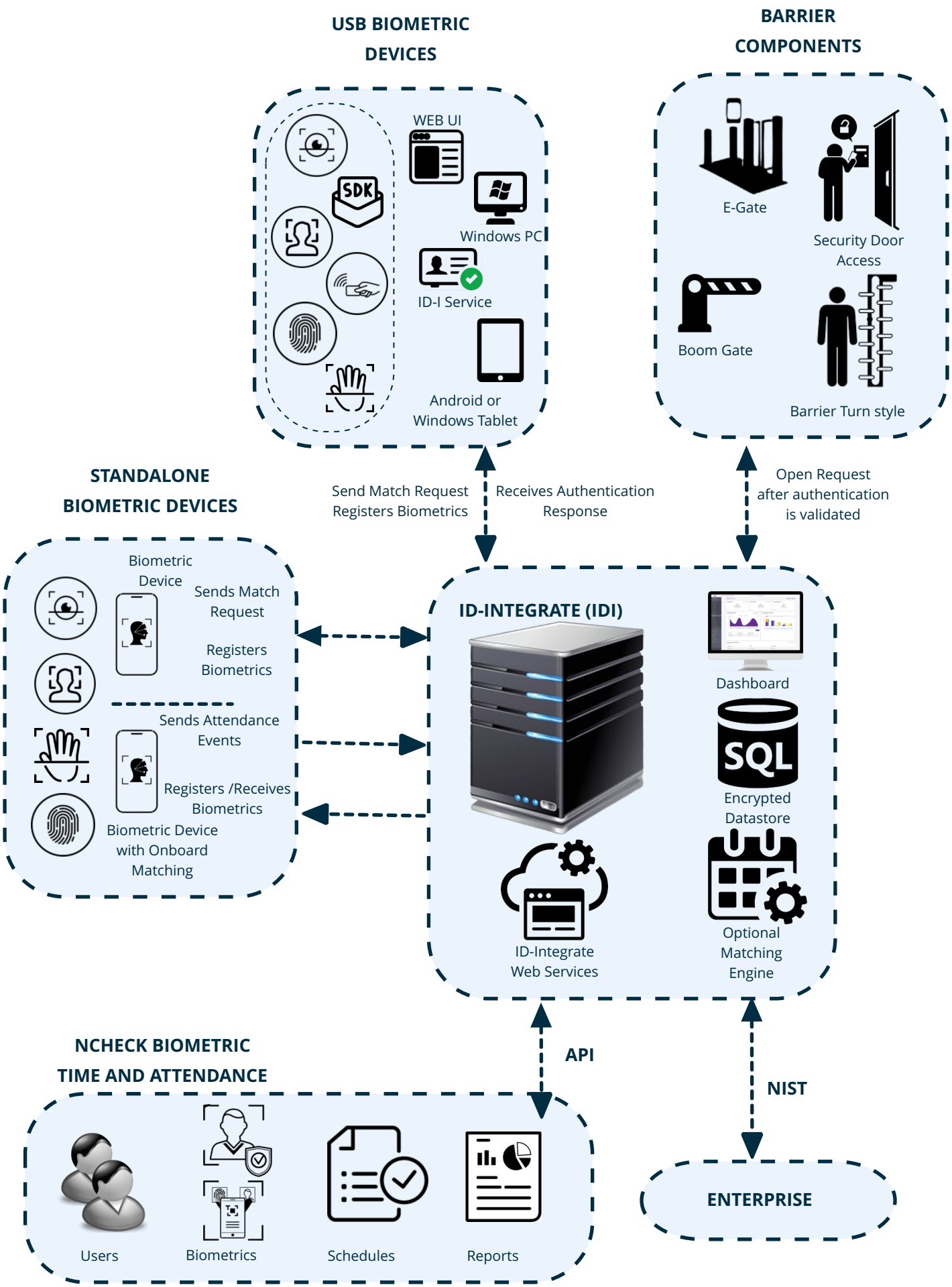
Once a new biometric device has been registered then we can use it for login and logout ents or use a different device for both.

This solution will seamlessly integrate into many access facilities – doors, e-gates & turnstiles, and barriers.

If the biometric device has storage capabilities we can push the biometric information out to all devices on the network.

All authentications are done via web services on the device (i.e. Master Mode) or back to the server (Client Mode) depending on the use case and the biometric device capabilities to match on-board.

ID-INTEGRATE APPLICATION TOPOLOGY
NCHECK BIOMETRIC TIME AND ATTENDANCE



Road Map Enhancements Planned	Status
Unified employee and visitor management	in progress
Pricing per use (both employees and visitors)	in progress
Registration from mobile device (admin and self)	in progress
Personal report updates	in progress
New user interface (fewer steps/barriers)	in progress
Access control integration (can now open gates)	Done
ALPR - Automatic License Plate Recognition	Done

Contact info@idforce.io

ID Force International Pty Ltd
Suite 705, 11 Railway Street
Chatswood NSW 2067 Sydney,
Australia