

The Iris system is not just a stand alone camera that can only do peer to peer communications and have a restricted feature sets.

Both our 2G and 3G cameras have the following structure- i.e. the cameras are clients to a middleware server, no public IPs are required, large numbers of cameras can be supported and we support live video 'call in' to the camera at any time.

A technical Overview

The WDC system consists of a camera, client software for a mobile phone and server middleware which allows connections to be established between the camera and the mobile phone.



The camera is equipped with a GPRS module which permits a connection to be made through a private APN to the server running the middleware. An instance of the client software establishes a connection to the same server using a GPRS connection via the chosen operator's public APN. The server handles issues of security and dynamic IP resolution, as well as monitoring and recording traffic for billing purposes etc.

Camera Function

When the unit is turned on, the camera firmware establishes a connection to the middleware server via the APN. The firmware extracts the unique hardware ID from the GPRS module and uses this to identify itself to the server. The server verifies that the ID belongs to a valid account. The camera and server then intermittently exchange short keep-alive messages to ensure that the connection between them is maintained as 'always on'. If the camera does not receive a message from the server within the timeout period, the firmware automatically forces a reconnection attempt.

In response to client activity or according to a pre-programmed schedule, the server may send a message to the camera requesting that it begin to capture and send images back to the server.

Images will be encrypted before transmission using a hash based on the unique hardware ID of the GPRS module and the PIN number selected by the user.

In response to activation of the passive infra-red sensor, the camera may send an alert message to the server, and optionally may also capture and send images to the server for a pre-determined period.

Client Function

The client software will be initially compiled for a range of different Java-enabled mobile phones. Running the software will require the entry of a PIN number, which can be selected by the user at the time the software is registered. Once running, the client application establishes a connection to the middleware server via the internet APN of the user's chosen network provider. The client sends authentication information which includes the PIN used to activate the software, the hardware ID of the phone, and the SIM ID number. These IDs will have been given to the service provider at the time of software registration. This method prevents a stolen phone and/or stolen SIM being used to obtain unauthorised access to a camera.

Server Middleware Function

The server middleware maintains a database of registered users which contains authentication details for clients, cameras, and the relationships between them. One client may have access to multiple cameras. One camera may be accessible to multiple clients.

The middleware maintains two lists which change dynamically, one list of currently connected and authenticated cameras, and a second list of currently connected and authenticated users. Connections are logged, and the volume of data transferred is also recorded for each transaction. This data is used to support the billing function, as well as providing management information.

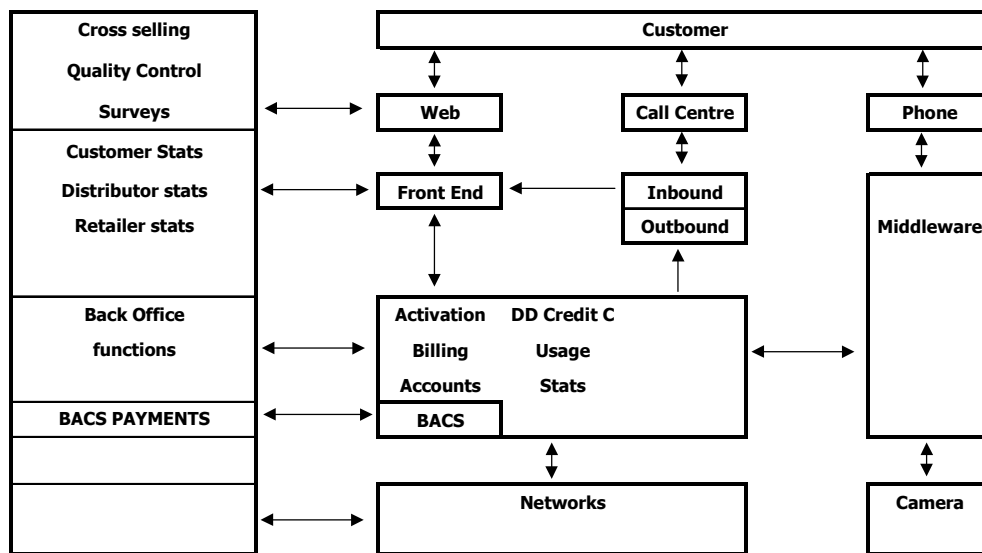
When encrypted images are received from the camera, each record will have a timestamp added to it, and the combined package will be tamper-proofed using a CRC or similar mechanism.

In response to an alert message from a camera the server can send an SMS message, via an SMPP link, to one or more registered client phones selected by the user. The system can also send the alert message via emails.

Customer and system support

Wrapped around the camera system are the customer support processes and systems. The diagram below gives an overview of the system design and the linkage between the main elements.

Overall system design



Note that the Camera and phone communicate via the Mobile network

The customer support system offers the customer the ability to self manage their camera and handset set-ups. This is achieved by setting up an internet based account system that gives customers access to all the management functions of the system related to their cameras and handsets.

By using best of class partners for the customer management with the domestic camera solution a quality lead solution provider can be established that will enable significant numbers of the public to enjoy increased security and lower their fears of crime.

Understanding the Technology Involved – what the end customer needs to know

From the user point of view operation of the camera is very simple. There are 3 items to use:

1. **The Camera:** Plug it in and switch it on via the single button located on the front of the camera. Point it at what you want to see or mount it on the wall with the bracket included.
2. **The Customer's Phone:** Install the Iris Player (the application used to view the camera) on the phone by following the simple instructions sent via text message, literally just a couple of button clicks. Then access the camera from their phone at will.
3. **The Web:** Customers can log on to the 3rdisecure website to manage all aspects of their account, from adding extra phones to view their camera, adding extra cameras, viewing their bill and all sorts of other fun things to come.

One Time Requirement

When the customer first uses the camera they will need to register with 3rdisecure to activate the Mobile Data Connection with the camera. They will need seven pieces of information before they start:

1. The IMEI number for the camera (found on the label of the box the camera was delivered in or behind the battery in the battery compartment).
2. The serial number for the camera (found next to the IMEI number).
3. Their mobile phone make and model number.
4. Their mobile phone number.
5. Their mobile service provider (e.g. Orange, T-Mobile etc)
6. Payment details, either credit card or bank details for direct debit, for monthly airtime usage charges.
7. A memorable PIN number which they will enter every time they log on their camera.

There are two choices, either call the 3rdisecure Customer Service centre, and one of our highly trained and super helpful staff will talk them through the registration process, or log on to the 3rdisecure website and follow the simple online registration process entering the information they have collected above.

But what actually happens when the customer registers?

Although from the customers perspective the whole process will seem easy and seamless there is actually some very clever techie stuff going on. Here is a brief overview which will help you understand what happens and will assist you with customer questions.

When the customer registers either by phone or on our website we take all billing information to activate their account. Also during the process by collecting their mobile phone number and make & model we then WAP push data settings to their phone. Obviously they need to be able to send and receive mobile data on their phone in order to view mobile content and most users do not have data access set up on their phone.

This WAP push arrives as a SMS text message which contains simple instructions to allow the settings to be automatically set to their phone. These settings are specific to the model of the phone and the network they use.

Now that the phone is able to connect to the mobile data network we then send another WAP push via SMS text which is a link to the java application, Iris Player, which allows them to view the camera. These settings are again specific to their phone and matched to their account only allowing access to the cameras on their account, this is part of the security built in to our system to protect users.

The user again just follows the instructions in the message which will just be a couple of confirmation button clicks and the application will be installed and ready to use.

The Iris Player is then accessed on the phone, normally through the applications or games menu.

Every time the Iris Player is started the user will need to agree to a data protection license statement which reads:

I agree to use this software in accordance with all applicable local laws governing privacy, data protection, digital media rights & viewing of content.

Once they have agreed to the statement they will be requested to enter the PIN number they gave at registration. This protects the user from other people viewing their camera or recordings in the event of the mobile phone being lost or stolen.

The connection is then made with one of the 3rdisecure web servers which will allow access to recordings already stored on the server or relay a link live to the camera. It is this type of link to the camera that uses the GPRS data connection which forms part of the monthly airtime bill the customer pays to 3rdisecure.

Full instructions are included in the box with the camera.