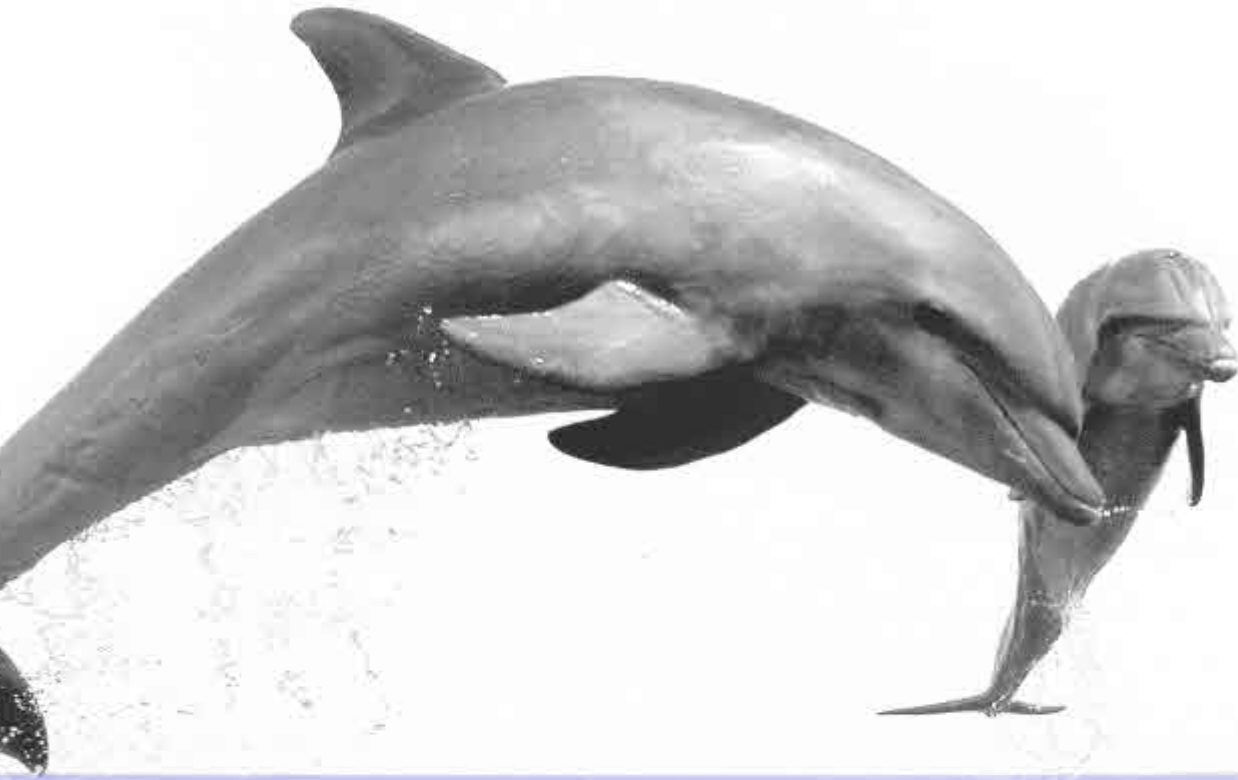


# CARiNA **Mobile**

Powered By

**obsidian**<sup>wireless</sup>



DELIVERING EXCELLENCE THROUGH TECHNOLOGY

**4net**  
TECHNOLOGIES



ComputerTel



# “Mobile Compliance”

## Enabling Risk Management for Mobile Communications by Ensuring Compliance”



ComputerTel's Carina Mobile, powered by Obsidian, enables organisations in the Financial Services industry to record mobile communications in a fully compliant manner, to ensure that users adhere to market regulations and also meet FSA, MiFID and BSI0008 standards.

Many FSA regulated organisations are already required to record all office based communications as standard. However, the FSA is currently developing procedures to consider the regulation of mobile devices. In the intervening period, much has been done to address this situation, and Obsidian is proud to be the first UK provider to be able to offer a truly compliant and effective Mobile Recording Compliance solution.

Carina Mobile takes mobile recording to a whole new level. Mobile compliance is not just about recording voice calls or even SMS, it's about the capture of deskbased communications which have been extended to mobile devices for example Instant Messaging, corporate email and webmail. All of these tools are now being used to conduct business via mobiles and as such, fall into the same category as the recording of office based communications.

This is why MCS™ has been developed with the ability to capture, monitor, store and retrieve all of the following forms of mobile electronic communications, whether they take place on corporate BlackBerry®, or other smartphone devices:

- Voice calls
- SMS
- Corporate email and webmail
- Instant Messaging
- Social networking sites
- BlackBerry® Mail and Messaging

Historically, because these forms of communication could not be recorded, many organisations have 'locked down' their corporate mobile devices so that messaging services cannot be accessed by their users. However, as technology develops, users now expect to be able to take advantage of all available communication methods, which they are familiar with using in the office and in their personal lives, and their customers also expect the same.

Taking SMS as an example, this is now seen as a mainstream tool both in business and for personal communication, but according to Sarbanes Oxley, SMS messages are classed as a business record and therefore must be archived in the same way as other such documents. So if organisations want to enable staff to communicate in this way, they must find a compliant way of recording and storing those messages. Future enhancements to MCS™ will also encompass new communication methods like Twitter and FaceTime as they become more widely used in a business context.

Mobile Compliance Suite™ has been designed to overlay existing devices, infrastructure and methodology, without causing interference or inconvenience to either the organisation or its users, or to those with whom they communicate. In addition, to minimise both power requirements and physical footprint, all Onsite elements of the Mobile Compliance Suite™ can operate from a single rackmounted server, which simply varies in size dependent upon the number of users required.

### Managing risk

Mobile Compliance Suite™ is as much about managing risk as it is about mobile compliance. The recording, storage and retrieval of mobile electronic communications ensures compliance with the necessary standards, but beyond this, organisations also need to manage the inherent risk which surrounds the use of mobiles. And that means being able to act upon the information gathered, in real time.

MCS™ makes Risk Management for mobiles a reality, by the use of Obsidian's optional Mobile Surveillance Module™. This monitors the electronic communication flow in real time and sends alerts, based on predetermined rules which each customer can specify, allowing them to act upon any information that has been identified, at that point in time. This can only be achieved by:

- Realtime recording of all mobile electronic communications
- Realtime rules based surveillance based on numbers, words, phrases or events
- Realtime onscreen alerts, or via text and email

For example, words, phrases or events which could be set to trigger an alert might include:

- The phrase 'off the record'
- The name of a competitor in an email address
- An instruction to call someone on their 'private mobile' number
- Confidential information
- Buyers and sellers contacting a specific person within a set timescale
- A message relating to an announcement on a news feed, even though the message was sent in the past

Without this capability, any information which is gathered cannot be acted upon in time to actually make a difference. What's the point of a fire alarm which goes off half an hour after the fire has started?

## How it works

The core elements of Carina Mobile Compliance are as follows:

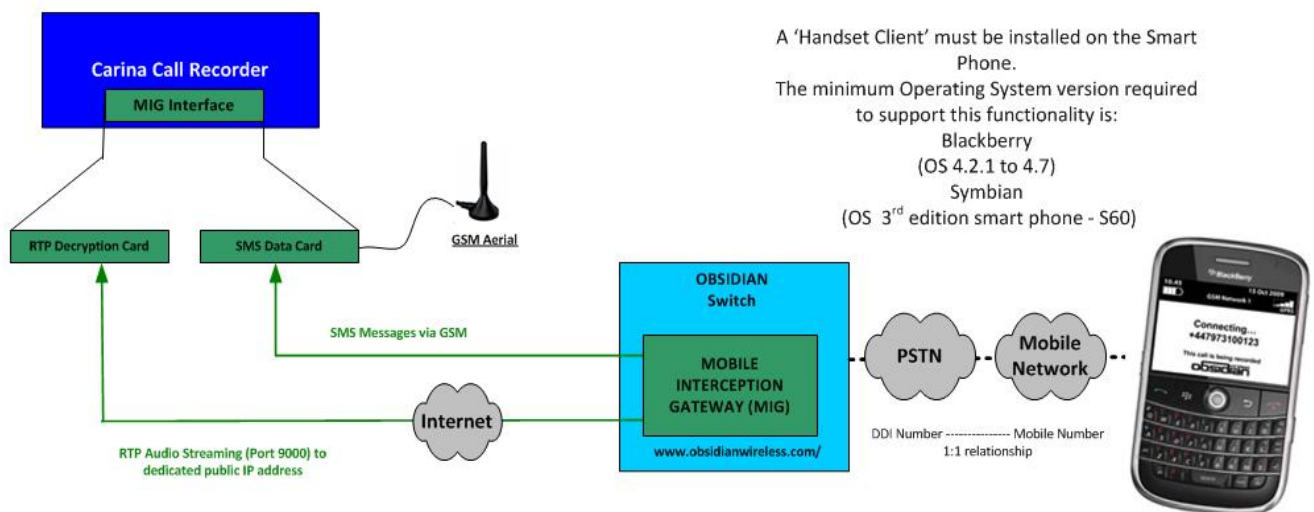
- Device based Capture Module
- Voice Services Platform
- Mobile Intercept Gateway™
- Compliance Engine
- Mobile Surveillance Module™
- C Store

Some of these are a fundamental part of the solution and some are optional depending on individual requirements, and on whether the customer wishes to record voice calls, electronic messages or both.

For either option, the first step is to load Obsidian's Capture Module onto each device. This can be carried out remotely, and there is no need to replace SIM cards, which keeps user disruption to an absolute minimum. The software runs in the background and reroutes all inbound and outbound calls or messages to their required locations, depending on whether it is a voice call or another form of mobile electronic communication.



## Mobile Compliance Suite



## Voice calls

- After capture, calls are rerouted to a Voice Services Platform, a carrier grade Class 5 exchange which is located at a data centre in London's Docklands. Please see the Security section for more details on this.
- Once received by the Voice Services Platform, all calls are subjected to 2048bit encryption. They are then 'packetised' into large format data packets and transmitted to the customer's site via a dedicated point to point data circuit which is provided by a Tier 1 carrier. At this stage the encrypted data can be sent to multiple locations if required.
- Encrypted calls are received by our Mobile Intercept Gateway™ (MiG™), which is located at the customer's site, and are then decrypted. This ensures absolute security as the data cannot be accessed until received by the MiG™.
- If present, the Mobile Surveillance Module™ scans all of the numbers which calls were made to or received from, and generates alerts as required based on customer specified rules.
- Calls are then streamed to the customer's preferred call recording and storage devices, including the option to send calls to multiple locations if preferred. This can be achieved from a single output in our exchange, by utilising the business continuity feature on the Exchange located equipment.

## Mobile electronic communications

- All other forms of communication are also captured by the software which is loaded onto each device.
- Messages are transmitted directly to our Compliance Engine at the customer's site in real time.
- If present, the Mobile Surveillance Module™ scans all messages and generates alerts as required based on Customer specified rules.
- Messages are then consigned to the customer's messaging vault for storage, archiving and retrieval, including the option to send messages to multiple locations if preferred.

DELIVERING EXCELLENCE THROUGH TECHNOLOGY



## Security

We understand the importance of data security, especially in the Financial Services industry. Our Voice Services Platform is a carrier grade Class 5 exchange, located at a highly secure data centre in London's Docklands. It has full built in resilience and redundancy and is the same platform that is used by many telecoms companies and global carriers for hosting and delivering their value added services. The platform is recognised by telecoms companies worldwide as one of the most secure in the industry and has interconnects with major UK and global carriers.

Existing customers already using generic services from this platform include Aon, Axa, Nationwide, ANZ Bank, Friends Provident and the Lloyds Banking Group, whilst telecommunications companies currently using the platform include BT, Cable & Wireless, Orange, Mitel and Sky.

## Cost Of Ownership

Some solutions use the customer's PBX to route voice calls, rather than using an external exchange like Obsidian's Voice Services Platform. But the problem here is not only with resilience, but also with bandwidth issues. Taking a worst case scenario, if every mobile user within an organisation was making or receiving a call at the same time, then the lines coming into a standard PBX would simply not be able to cope.

In order to maintain 1:1 integrity, any system which uses a customer's PBX will require an incoming line for every mobile user, thus incurring considerable ongoing line rental costs. Using an existing PBX would therefore require additional costly hardware upgrades or licenses in order to deal with the increased capacity. Our Voice Services Platform gives a 1:1 ratio of users to channels, and our fixed monthly tariffs are fully inclusive of all incoming and outgoing lines. In addition, because every call is encrypted and packetised before being forwarded to the customer's premises, this vastly reduces the amount of bandwidth required.

## Architecture, Routing and Connectivity

Whilst the call flow for the process of capturing voice calls remains generically the same in all environments, the system architecture can be adapted to suit the customer's specific requirements or those of the partner supplier.

## Partners

- If the service is being provided via a Mobile Network Operator (MNO), then this partner can integrate the call routing and encryption directly into their core infrastructure at the Mobile Switching Centre (MSC). This provides a number of benefits for the MNO and the customer, including reduced cost international roaming for voice and data.
- Alternatively MNOs can provide a dedicated VPN connection between the MSC and Obsidian's Voice Services Platform.
- If the service is being provided via a telecommunications carrier partner that possesses their own national and/or global fixed line switching infrastructure, then the partner can integrate Obsidian's platform at its core. This enables delivery of the calls via the carrier's own network and, as with MNO integration, can present a number of benefits for the carrier and its customers.

## Customers

- These partnering options, which enable mobile and fixed line carriers to integrate MCS into their networks, benefit the customer organisation by providing the option to acquire Obsidian's service via existing telecommunications providers.
- For organisations that wish to keep the capture of calls within their own data centre, we can provide a fully resilient in-house Voice Services Platform, rather than routing calls via our exchange. However, because a carrier class switching platform is required, this option is only likely to be suitable for organisations with more than 500 users.

## Global Reach

Organisations that need compliance solutions are very often global operations and likewise, regulation and compliance are global requirements.

We understand the importance of being able to satisfy these requirements and we know that our customers need to meet the specifications of organisations such as the Securities and Futures Commission (SFC), the Financial Services Authority (FSA), the Securities and Exchange Commission (SEC) in New York, the Financial Industry Regulatory Authority (FINRA), the Financial Services Board (FSB) in South Africa, the Office of the Superintendent of Financial Institutions (OSFI) in Canada, the Australian Securities and Investments Commission (ASIC), the Markets in Financial Instruments Directive (MiFID) and so on.

As such, through a series of alliances, Obsidian is able to offer and support Carina Mobile Compliance in all of the world's leading financial centres. This allows organisations to standardise on a global mobile compliance strategy in the same way that they would establish a global strategy for IP telephony networks and call recording platforms.

## 4Net Technologies

First Floor,  
3 Scholar Green Road,  
Cobra Court,  
Trafford Park,  
Manchester M32 0TR  
Tel: +44 (0) 8450556366  
Fax: +44 (0) 8450556377  
Helpdesk: +44 (0)8450556388

DELIVERING EXCELLENCE THROUGH TECHNOLOGY

