



Call Recording within Wealth Management Institutions

White Paper

Management Summary

The Financial Services Authority (FSA) legislation introduced in March 2009 requires that some UK financial institutions record and store telephone conversations and electronic communications relating to client orders. For financial institutions looking to introduce new systems to meet this new legislation, there are considerations for security and a resilient authentication system. Encryption has to meet the FSA requirements, both on the platform and while transmitted, and the archiving system needs to be secure and easy to use.

This can be an opportunity to extend the system to cover the increasing number of mobile workers who need to make and receive calls on a mobile phone. It's also an opportunity, to meet the requirements of the growing number of employees making lifestyle choices for flexible working by introducing a recording system with the flexibility to use any handset - home, desk phone, or mobile.

There are additional priorities relating to the system infrastructure, such as the need to ensure the solution is based on a secure solution architecture offering high resilience and reliability levels. This paper provides information on the TeleWare hosted call recording service created specifically to meet the demands of the new FSA legislation.

The FSA Regulations

UK financial institutions have to record and store telephone conversations and electronic communications relating to client orders under new regulations introduced by the Financial Services Authority (FSA). From March 2009, firms involving client orders for the equity, bond and derivatives markets have to retain these files for six months. Electronic communication includes e-mail, instant messaging and faxes. The FSA regulations have been introduced in line with an EU review and are part of the FSA's efforts to combat market abuse, particularly insider dealing and market manipulation.

FSA compliance is the responsibility of the financial institution and does not simply relate to an FSA compliant product but to the entire process used within the institution. The institution is required to have policies and practices in place that ensure they, their staff and any supply agencies carry out their responsibilities to meet these requirements. TeleWare is able to act for the customer in delivering the call recording features and capabilities but our customers determine the rules under which we may manage it for them. The legislation proposes using Call Recording as a tool within the company policy framework.

The FSA rules take effect from March 2009 for companies who are undertaking the following activities:

- Receiving client orders
- Executing client orders
- Arranging for client orders to be executed
- Carrying out transactions on behalf of the firm or another person in the firm's group and which are part of the firm's trading activities or the trading activities of another person in the firm's group
- Executing orders that result from decisions by the firm to deal on behalf of its client
- Placing orders with other entities for execution that result from decisions by the firm to deal on behalf of a client.

For those firms affected, there is a transitional period of one year to give firms enough time to prepare and implement the necessary system changes.

The TeleWare Call Recording Service

The call recording service records and stores all inbound and outbound calls automatically. Calls can then be retrieved using the service's web interface.

Inbound Call Recording

Each user who wishes to record inbound calls is allocated an intelligent Number DDI (Direct Dial Inbound); any calls made to this DDI will be automatically recorded and the recording will be securely stored on the call recording hosted platform. The user owning the intelligent Number can register this DDI to route calls to any PSTN or mobile number, allowing them to receive recorded calls on existing phone equipment, provided the phone to where the user is registered has its own unique DDI, to allow the recorded call to be placed.

Registering the intelligent Number DDI to a phone is simple and secure. The user dials a pre-allocated number and enters their unique user ID and PIN. The user can register “here and now” in a single key stroke, if the number they are calling from is not recognised because there is no CLI they will be prompted to enter the DDI of the phone.

Once a user is registered, all calls to their intelligent Number DDI will be delivered to the registered number and will be call recorded automatically. On completion of the call, the recording of the call is securely stored on the call recording hosted platform.

Outbound Call Recording

The solution operates through a single DDI which allows users to enter an ID and a PIN which will then enable them to securely make an outbound call. This ID is also the secure reference when searching for recordings within the web call recording interface.

After entering the PIN, users are prompted to enter the number they wish to call; the call is then connected and recording starts automatically. As protection against hackers, there is an option to lock the account and require an administrator reset should multiple incorrect PIN numbers be entered.

On completion of the call, the recording of the call is securely stored on the call recording hosted platform.

Call Recording Access and Retrieval

Access to the stored call recordings is through a secure web interface housed on the platform. The web application utilises Secure HTTP as well as IP address filtering and two factor authentication. (See authentication section of this paper).

The IP address from which the log-in request is being made will be validated against a list of allowed addresses and the log-in request will be denied if the IP address is invalid.

When retrieving a call recording, the user is first directed to a two factor authentication screen for entry of validated details from a token fob; the user is then directed to the following web screen.

The web interface is accessed from a secure web URL which directs the user to the dedicated call recording portal.

Searches for call recordings can be filtered by inbound or outbound and can be based on date, status, time, user or team call recording ID and dialled number Caller Line Identifier (CLI).

Call recordings which match the



Search	
Date from	09-04-2009
Date to	09-04-2009
Time from	-- :--
Time to	-- :--
User / Team	1000
Dialled number	
CLI	01234567890
	<input checked="" type="checkbox"/> Exact match for CLI
iAB Application	
Minimum duration (secs)	
Maximum duration (secs)	
Status	All
Direction	Inbound and outbound
<input type="button" value="Search"/> <input type="button" value="Cancel"/> <input type="button" value="Reset"/>	

search criteria will be displayed and can be selected and played by clicking on any of the properties within the entry row.

The user selects the telephone to be used to listen to the playback of the selected recording from the 'Phone Number Request' screen.

To prevent calls from being directed to a destination where information can put the company at risk, the list of telephone numbers to which the call will be routed can be restricted.

Recordings List

								Modify Search
**Date & Time	User	Team	Duration (secs)	CLI	iAB Application	Dialled Number	Direction	
19-02-2009 11:37	5003		42	01234567890	1084	1234567	Inbound	
19-02-2009 11:36	5000		197	01234567891	1084	1234564	Inbound	
19-02-2009 11:26	5000		293	01234567892	1084	1234562	Inbound	
19-02-2009 11:24	5000		211	01234567893		1234567	Inbound	
19-02-2009 11:20	5003		208	01234567894	1015	1234568	Inbound	
19-02-2009 10:58	5003		472	01234567895	1084	1234567	Inbound	
19-02-2009 10:47	5000		111	01234567896		1234569	Inbound	
19-02-2009 10:00	1193		617	01234567897		1234565	Inbound	
19-02-2009 09:42	5003		598	01234567898	1015	1234563	Inbound	
19-02-2009 09:30	5000		235	01234567899		1234562	Inbound	
19-02-2009 09:22	5002		372	01234567900	1084	1234567	Inbound	

Cancel Only the first 500 matches have been displayed

Recordings can be downloaded from the secure platform using the call recording web application. All downloads are in encrypted form and download is over a secure HTTP connection. Software is provided to decrypt the recordings after they are downloaded. The decryption uses the customer's own unique key; this ensures that the recordings are never transited in unencrypted form and can only be decrypted by the customer who owns them.

Call recordings are stored on the platform for a period of 6 months after which they are then removed, unless a longer storage period has been previously agreed.

Encryption and Authentication – Delivering a Secure Service

The TeleWare Runtime provides a real-time call handling layer for all inbound and outbound calls on the platform and provides the call recording functionality. This enables a unique capability and strength, the ability to use the TeleWare Runtime to apply encryption during the recording process. This solution avoids the limitations of using an encrypted file server, where the same encryption key is used for all recording files on the server. The TeleWare Runtime allows each customer to be assigned a different encryption key, which can be changed at request from the customer.

For each call which transits the TeleWare platform, the Runtime encrypts the recording using the customer's symmetric 3DES key and signs the recording using its public/private key-pair associated with that key (the signature is based on the unencrypted content). The symmetric and public/private keys can be revoked / replaced on request. Revoked keys are kept on the Runtime's key ring for as long as there are recordings on the platform with those keys. The WAV header of the recordings will contain references to the signing public key and encrypting

symmetric key so that the Runtime knows which key to use for decryption and so that the signature can be verified.

Encryption Keys

Customers are provided with software to generate their own unique 2048 bit RSA signing and encryption keys. The solution uses three types of key: Master, Runtime and Decryptor. The Master key is first generated by the customer, should be retained securely by the customer on more than one computer and should never be distributed; it is used only to create new Runtime and Decryptor keys.

The Runtime encryption keys must be created and issued to TeleWare before any encrypted recordings can be made on the platform. Runtime keys allow the platform to encrypt the customer's recordings and allow them to be listened to on the telephone, via the call recording web application.

Decryptor keys are used to decrypt recordings downloaded from the secure platform, using the decryption software provided. The Decryptor keys will only decrypt the customer's own recordings and should be issued only to the customer's personnel who are permitted to decrypt recordings.

This system ensures that no one else with access to the platform can decrypt a customer's recordings.

Cryptographic Process

The TeleWare Runtime handles all telephony and media processing. This includes the mixing of 2 party audio, hashing and encrypting the mixed data and writing it to file. The Runtime uses Microsoft's Cryptographic API for all its encryption and signing functions. Microsoft allows 3rd party Cryptographic Providers to be used from their Cryptographic API. The solution uses Microsoft's Enhanced Cryptographic Provider, a widely accepted secure encryption interface.

Using the CryptoAPI, the Runtime will generate a 2048 bit RSA key pair which will be used for signing recordings and securely receiving symmetric keys for encryption.

Call Recording Storage

As additional security against hacking, no unencrypted data is stored, even on a temporary basis. All recordings are written and processed in real-time to the file server. When a recording is started, an empty WAV header is written, with space reserved for the standard WAV fields and TeleWare proprietary fields for basic call information for searching, a key reference and a signed hash of the recording.

While call audio data is being recorded, it is mixed down to mono and the data is hashed (MD5) and then encrypted (3DES) as it is written to file. When the Runtime plays an encrypted WAV file, it uses the key reference from the file to identify the correct decryption key to use for playback. The data in the file will then be decrypted and streamed in real-time. No decrypted data is stored, even temporarily.

Two Factor Authentication

Each user will be required to be authenticated through a CRYPTOCARD session, as well as through the secure login details associated with the TeleWare account (see access section above). These technologies form the two factor authentication. Failed authentication by either

will prohibit access. The two levels are independent, with no low level association of the technologies.

CRYPTOCard technology is implemented at the log-in page of the call recording web application. CRYPTOCard uses both the CRYPTO-Web and CRYPTO-MAS applications.

CRYPTO-Web is an ISAPI filter for Web servers. It sits in the data stream between the user's browser and the web call recording application residing on the hosted platform, intercepting all resource requests. It allows access to the requested resource only after authenticating the user and verifying that the user is authorised to receive the requested resource.

The user is presented with a CRYPTOCard Logon page.

If the user's credentials are valid and the user belongs to the validated group assigned to the web-based resource, they are redirected to the call recording URL where they then can enter their secure credentials to access the call recording archive. If the CRYPTOCard credentials provided are invalid, the user is presented with an Access Denied page.



CRYPTOCard's positive identification solutions support a broad range of authentication tokens. The token styles include both hardware tokens, such as the key chain style KT-1 token, and software tokens, that can be installed on a personal computer or a variety of portable devices, such as Blackberry's and PDAs. CRYPTOCard has the best token technology in the industry with tokens that are highly secure and durable.

The solution provided by TeleWare is a managed service solution, authenticated through the utilisation of tokens. This reduces the associated server costs and provides a commercial offering on a user-to-user basis based on a monthly or yearly fee.

Support for Mobile and Flexible Workers

The services can be delivered for inbound and outbound calls made from any designated phone irrespective of the network. This could be a mobile phone, a home phone or a desk phone.

This enables the system to seamlessly support the growing number of workers who use their mobile phone in preference to their desk phone, and the increasing number of home workers without requiring any special equipment at the home premise.

Reporting

Two standard reports are available from within the call recording web application:

1. Log Report – a report detailing web application log-in attempts, failed log-in attempts, what recordings were accessed / listened to.
2. Call Report – a report detailing call recordings; Call Recording Mailbox, Date of Call, Time of Call, Length of Call, CLI (Calling Line Identifier) and Number Dialed (for outbound calls)

Bespoke reports can also be created on request.

Network Architecture

The solution is provided as a hosted service run from the TeleWare secure data centre. This enables us to ensure the platform architecture is both resilient and secure and is provided with disaster recovery capabilities. (See separate white paper on the hosted platform architecture).

The networking architecture ensures that different partner networks do not have any direct access to core switching or application servers. All traffic is passed through the core router using secure network connections, such as VLAN or VPN, and is subject to security controls such as intrusion detection and rate limiting.

The hosted approach removes the requirement for any call recording specific hardware on site and so enables us to deliver the call recording service to distributed architecture and multi-site networks with common capabilities, irrespective of location or the hardware installed on the site. The hosted platform architecture has been designed to provide scalability and providing this solution as a hosted application ensures that, as new offices or users come online, there are no issues of system sizing or limitations imposed by the system.

Many multi-site organisations will have both IP and traditional TDM-based telephone architectures in place across their network. By using a centralised hosted solution, TeleWare is able to support both new and traditional architectures with identical capabilities and user interfaces.

Each customer has a designated secure tenancy within the hosted data centres based out of Harbour Exchange and Heathrow.

System design features include:

Access Control Lists (ACLs)

The core routers have specific rules as to which servers can communicate with the outside world (effectively a firewall)

Packet shaping

Although a method of improving QoS (Quality of Service), the core routers use packet shaping to block traffic generated by denial of service

Packet Filtering Rules

These are configured on each of the servers on the platform and serve to reinforce the Access Control Lists on the core routers

Strong Passwords

Each device is protected by complex administration passwords

Antivirus

Centrally managed on the platform with frequent updates

Intrusion Detection

Monitors all network traffic passing through the platform and uses rules to detect malicious traffic

Disaster Recovery (DR)

The primary call recording hosted platform is based in Harbour Exchange and a secondary solution is provided through the TeleWare data centre at Heathrow. In the event that a total loss of the primary data centre is experienced, then the calls will automatically be re-routed into the back-up data centre.

All important information, including user IDs and passwords and call recordings, are mirrored in real time, from the primary file server to the secondary file server, so that, in the event of a disaster, the secondary system will be up-to-date and up to the minute recordings will be accessible.

The primary service is accessed for outbound calls through a dedicated DDI. In the event of a disaster, the DDI will be re-pointed to the disaster recovery service based out of Heathrow. A single number is associated with both services providing continuity of service to the user. This service operates using Border Gateway Protocol (BGP) to manage inbound calls into the platform from two locations. If a primary link inbound is lost, then the calls will be re-routed via the secondary site, typically, within minutes.

If it is necessary to invoke DR, notification will be sent to a defined list of individuals informing them that DR has been invoked. Service Level Agreements will be in place between the customer and BT/TeleWare to ascertain acceptable levels of switchover time and downtime when DR is instigated.

For Further Information

- FSA Regulations - for a paper on the FSA regulations, visit http://www.fsa.gov.uk/pubs/policy/ps08_01.pdf
- Crypto card - for further information on this product, visit http://portal.cryptocard.com/documentation/TechDocs/CS6.4-CRYPTO-Web_IIS_QuickStart.pdf
- Secret Agent - for further information on this product, visit http://www.infosecorp.com/products/secretagent/sa_win.htm
- Hosted platform architecture - for a white paper on the hosted platform architecture, visit <http://www.teleware.com/resources/whitepapers.asp>
- TeleWare Call Recording - for further information on the call recording product, visit <http://www.teleware.com/products/intelligent-call-recording.asp>

call recording wp090401

Headquarters/Registered Office
TeleWare plc
TeleWare House, York Road, Thirsk,
North Yorkshire, YO7 3BX, UK
T: +44 (0) 1845 526830 F: +44 (0) 1845 522165

Asia Pacific Regional Sales Office
TeleWare NZ Ltd
Level 8, TeRenCo Finance House, 86 Victoria Street,
Wellington, PO Box 1956, New Zealand
T/F: +64 (9) 360 6881

Registered in England No 4756742

E: enquiry@teleware.com

W: www.teleware.com