



arkadin®

Cloud Collaboration Platform

Security White Paper

01/03/2013



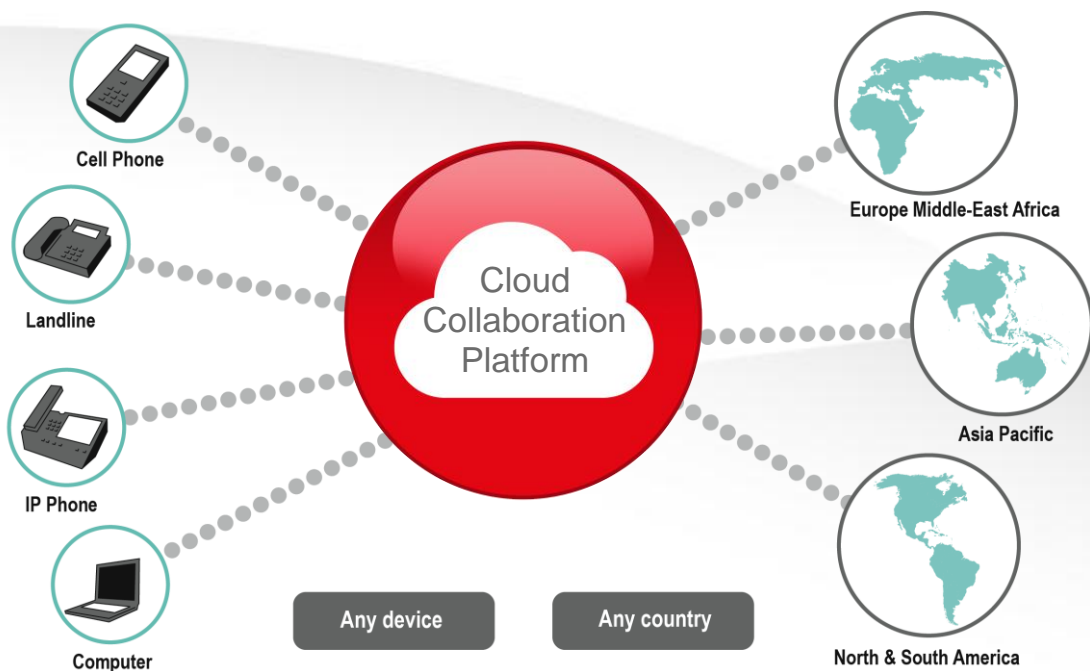
Introduction

Arkadin provides audio collaboration solutions to companies around the world for use by multiple applications across an enterprise including sales, marketing, training and events. This document describes the security features built into Arkadin Audio Cloud (including the online audio console for managing audio conferences).

ArkadinAnytime audio conferencing on the Arkadin Cloud Collaboration Platform

Arkadin has taken collaboration services to the next level with the launch of the **Arkadin Cloud Collaboration Platform**. Involving over two years of research and development, this new private IP network in the Cloud offers clients the best in **simplicity, quality** and **security** at an **increased ROI**.

The Cloud Collaboration Platform offers all the **benefits of Software as a Service (SaaS)**, with a hosted audio conferencing solution that requires no up-front investment and is easy to scale to a client's needs.



Arkadin's Cloud collaboration services make global conferencing **very simple** for customers; all employees use the same list of country access number regardless of their location or the location of their conferences. Administrators have just a **single list of numbers** to manage and deploy throughout the organization. In addition, participants benefit from the **Arkadin Client Care**, available at any time so all international conference participants can reach Arkadin operators for assistance in their own language.



With the Arkadin Cloud Collaboration Platform, there is no risk of audio degradation, ensuring **superior audio quality and reliability**. **Voice compression** and conversion protocol into the Cloud are not required and **Arkadin uses the latest audio technology to remove latency and acoustic echo**.

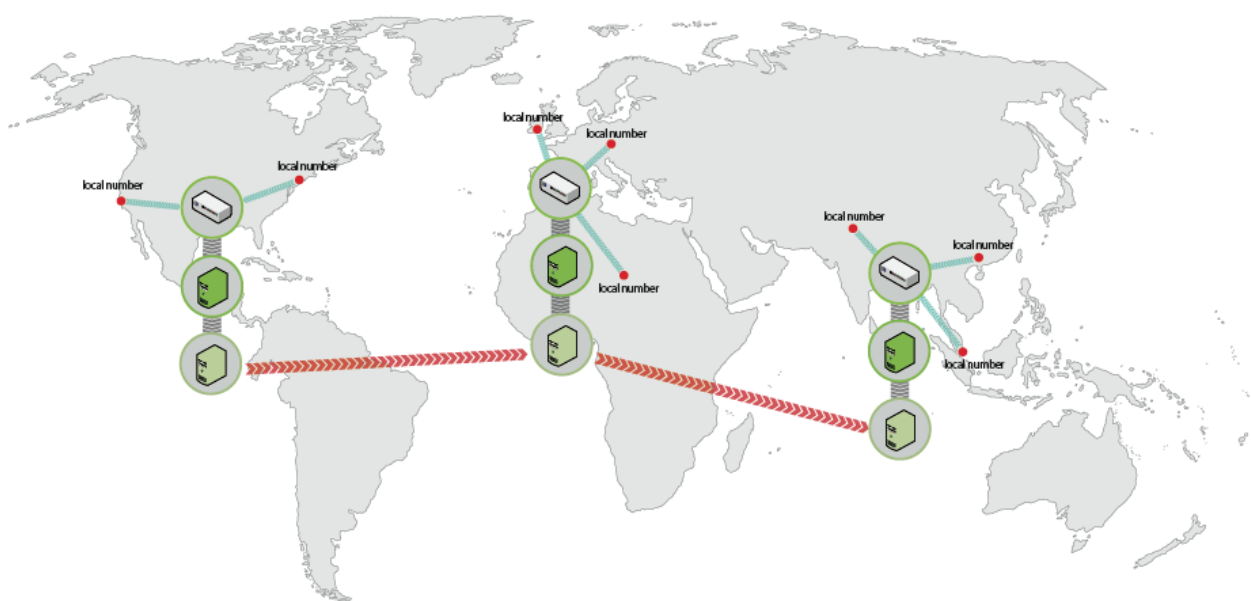
Arkadin Research and Development has designed a platform infrastructure that enables international calls to be routed **on a single bridge**. **Hosting the moderator and all the participants in the same meeting room optimizes the audio** quality, unlike other infrastructure designs which host an international conference on several bridges inter-connecting via an IP link that can delay the audio transmission.

For **maximum security**, voice data is transported through the Arkadin **private IP** network to maintain data integrity and each component of our network (software and equipment) is backed-up and our IP network is duplicated by design.

An **increased ROI** is also one of the benefits of the Arkadin Cloud Collaboration Platform which provides access to international conferences for the **price of local calls**. Thus companies with intensive global conferencing will see the most benefit from this **cost-effective solution**. Further savings can also be achieved through the integration of their corporate IP networks into Arkadin's via **SIP trunking** capability, bypassing all carrier access costs.

Combining the benefits of Software as a Service together with Arkadin's innovative architecture, the Cloud Collaboration Platform really is an essential element in the next generation of global collaboration.

Figure 1: Arkadin Cloud Collaboration Powered by Secure Private IP Network





Data Center Security Policy

All Arkadin platforms are housed in highly secure, world-class hosting data centers that provide 100% physical security guarantee. These data centers are purpose built for telecommunication service providers.

General Security Access

The data centers offer:

- 24 x 7 x 365 onsite security team
- CCTV monitoring
- Secure perimeter
- Rack mounting locker

Power

The data centers are equipped with:

- Dual feeds – diversely routed
- Redundant power components
- Racks with dual power feeding
- All the servers and hardware equipment have a dual PSU (Power Supply Unit) – see Network

Fire Protection

The data centers are protected by fire detection and protection equipment.

Network

All network equipment has a dual PSU. Each PSU is connected to a different power feed. Our internet access points have full redundancy. The internal Networks are protected by firewalls to prevent hacking and undesirable intrusion.

Environment

The data centers are equipped with:

- Separate cooling systems with alarms
- Temperature & humidity monitoring



Audio Infrastructure

Arkadin deploys the same platform across the world for all of our conferencing services.

Our platforms are monitored 24 x 7 x 365 by local IT teams based in Europe, North America & Asia Pac. System alerts are sent over the network to the Operations team in case of malfunction.

All the audio hardware used is fully redundant, modular, and equipped with dual power supplies. All systems have static cards that are hot-swappable, which means that any card replacement can be done without having to disconnect other cards, and without any customer-facing impact or disruption to conference calls already in progress.

The audio platforms are connected to multiple carriers so if there is a problem with one network we have alternatives for back-up.

The Local Area Network used for communication between the servers managing the audio service is redundant so the communication flow can use either network.

Arkadin's audio conferencing service is available 24x7, 365 days per year.

For occasional maintenance and upgrades, we deploy a backup platform that helps to ensure continuity of a full service. This backup platform is always available in case of major outage.

Security Audio Features

Meeting roles

2 key roles are defined in a an ArkadinAnytime audio conference: Moderator and Participant.

Moderator: joins the conference with a specific Moderator PIN which assigns management and control of the conference to the moderator.

The moderator has access to the following security features:

- The conference will not start until the moderator joins the conference (activated by default).
- The moderator can control when the conference is terminated by either selecting to end the conference at any time or through automatically terminating it by leaving the conference
- Find out how many participants are connected, and even their names if the option is selected
- Lock access to the conferencing, and thereby forbid any additional participants from joining

Participant: joins the conference with the Participant PIN. and has minimal responsibilities, typically only viewing session content.



Communication of Account Credentials

Personal PIN codes are only sent to Arkadin account holders ie moderators. The moderators are able to organize conferences, communicating just the access numbers and participant PIN to the attendees, not the moderator PIN.

Figure 2: sample of Welcome pack – only sent to the Moderator’s personal mailbox.



PIN Code & Login

The moderator PIN code is randomly generated and completely different from the participant PIN code associated with it. The moderator PIN code allows the moderator to manage the conference and access the call features.

The participant PIN code has very limited rights, just allowing access to the conference, self-mute, sub conference access and operator assistance.

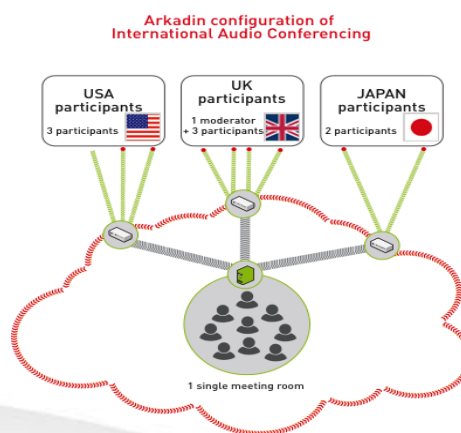
Arkadin strongly recommends that moderators do not share PIN codes, and that administrators perform regular usage checks and monitor turnover to correct any inaccuracies in the personal information we retain.



Audio Conference Hosting

By design, the cloud collaboration platform infrastructure is far more secure than other types of architecture; international conferences are hosted in one location not dispatched across a network and split across multiple hardware components.

Figure 3: example of international conference topology.



Audio Conference Management via the online Audio Console

Arkadin's unique online console provides a visual overview of conference calls. This incredibly powerful, yet simple and user-friendly tool allows moderators to view and manage audio conference calls in real time via an Internet browser.

At a glance, moderators can view the list of all attendees on the call and their telephone numbers (CLI) to monitor attendance. With this security feature, the moderator will be aware of any unexpected attendees. The moderator has control of conferencing features including muting, conference locking and the disconnection of one or multiple participants.

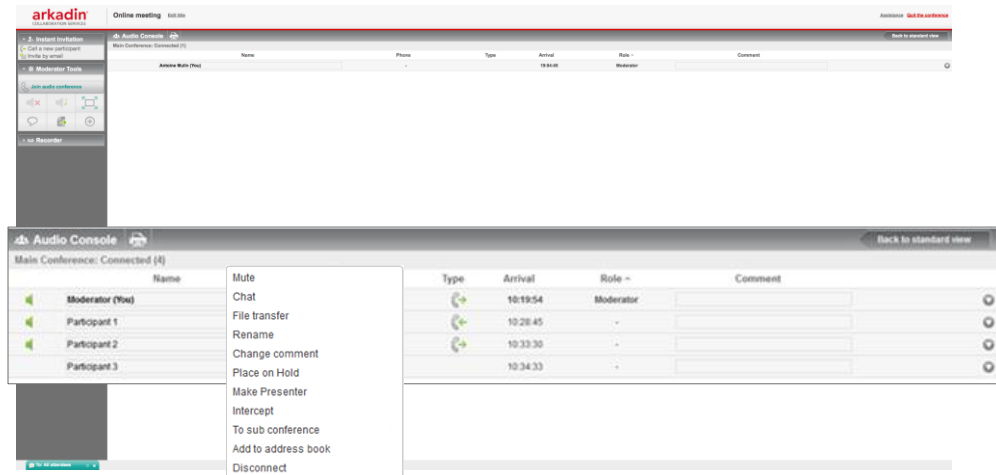
The Audio Console is accessed via ArkadinLounge:

- Login to ArkadinLounge®: [https:// anywhereconference.com](https://anywhereconference.com)
- Click on the Audio Console button and use it to:
 - View the list of participants
 - Mute all or individual participants
 - Record the call

The Moderator can also change which features participants can view or have access to. For example, the Moderator can disable the attendee list at any time during the conference for confidentiality. The list can also be disabled ahead of time or permanently. Conference settings such as chat, the right to save a shared document, transfer file, wait for moderator can also be enabled or disabled.



Figure 4: Audio Console Screenshot



Entry & Exit Information

The entry of a new participant during the conference call is identified by an ascending beep; easily distinguishable from the descending beep heard on exit.

For additional conference call security , Arkadin recommends selecting the Names-on-Entry / Names-on-Exit account option in advance. The name of each participant is requested, recorded and played to everyone present in the conference as they enter/leave.

Roll Call

At any time during the conference, the moderator can access roll call feature via the control menu. It provides the number of participants (CLIs) in the conference as well as the recorded names of the participants, if the option has been selected.

One-Time PIN Conference Access

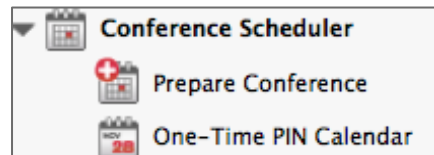
In addition to the permanent conference PINs, one-time use conferences can be scheduled via Arkadin Lounge portal for a specific date, time and duration. One-time PIN codes only allow entry to the conference during the scheduled time for increased security.

This system is easy to use and offers more secure conferences: the PIN codes protect entry to the virtual meeting room and can only be used once during the scheduled duration.



Moderators can schedule audio conferences online with the ArkadinLounge:

- Login to ArkadinLounge®: <https://lounge.anywhereconference.com>
- Click to 'Conference Scheduler' then 'prepare Conference':



- Click 'Next' on the following screen

- Select 'One Time Use', then schedule date/time
- A Unique PIN code will be generated which is required to enter the conference

Meet-Me Secure

This is the most secure conference profile. Each participant has their own individual and unique "Meet-Me Secure" PIN code or User ID. The participants must first dial participant the PIN code and are then asked to dial their individual "Meet-Me Secure" code to complete the secure access process. The system cross-checks the participant's "Meet-Me Secure" PIN against a list of people authorized to access this conference. If the PIN appears in the list, then the participant can enter. If not, they are automatically re-directed to an operator.

Security Level	Ease for Moderator	Standard Anytime access	One-Time PINs	Meet-me Secure
Good	One-click or one PIN	X		
Strong	Booking		X	
Strongest	PIN list management	X		X



Conference Locking

The moderator can lock the conference at any time using the telephone keypad or the Arkadin Audio console. When activated, this feature prevents from any new participant accessing the conference. A participant would be informed that the conference has been locked and that they will be disconnected.

For security, Arkadin recommend that moderators lock access to their conference once all participants have joined using the *4 keypad function.

Terminate Conference When Moderator Disconnects

This option is only available to moderators who can choose to disconnect all participants shortly after the moderator has left the conference. This will ensure that the attendees do not continue the conference without the moderator as well as enhance cost control as the conference automatically ends.

By default, the feature is not activated and can be triggered at any time during the conference by simply pressing *6.

Terminate Conference now

This option enables a moderator to disconnect all participants and moderators immediately by dialing *#1. The moderator is therefore able to ensure that everyone is disconnected, and attendees are unable to continue the conference, but also enhance cost control as the conference automatically ends.

Post Conference Report

A detailed Post Conference Report can be automatically sent to moderators by email after a conference. The report lists participants connected by phone number; connection time; and minutes connected (per participant and total).



Figure 5: example of a Post Conference Report email

Audio Conference Participants List	Conference Reference	500180600
xxxxx	Callers	2
Conference Started 2012-03-29 11:08	Minutes	2
	Billing Code	

Name	Dialed Number	Phone Number	Connect Time	Minutes
Moderator				
Robert	347242382993	33144652500	2012-03-29 11:08	2
Participants				
	347242382993	33144652784	2012-03-29 11:10	1

Second Level Pass Code

This option is an additional code set by the moderator at the beginning of the conference and then distributing it to invited attendees. Only attendees knowing the security code can join the conference.

After 3 wrong security code entries, participants are automatically routed to an operator for assistance.

The code is only activated for the conference in progress and is in addition to the standard PIN code.

Dedicated Dialing number

Dedicated Dialing numbers are a service option. If purchased, customized welcome message can be provided on the dialing number:

- If conference attendees dial the DDI, they hear the branded welcome prompt
- Callers entering a PIN code associated with the customer can join the conference.
- Callers without an appropriate PIN it is not associated with the customer's account cannot join the conference. This is to avoid fraud from persons dialing multiple PIN codes.

A caller (moderator or participant) can only enter a conference if the number dialed is appropriate for the PIN. In this case, the conference entry must match the coupled key: <DDI >+ <PIN>

The permitted PIN lists are therefore attached to the Dialing access number.

Conference Playback Security

1. Two security codes are required to listen to a recording via audio access
 - Conference Reference Number to access to a specific conference
 - Recording Reference Number to access to a single recording



To access all their recordings and to obtain Recording Reference Numbers the moderator follows these steps:

- Dial their Conference Playback Access Number
 - Enter the Conference Reference Number followed by #
 - Enter * then enter their Moderator PIN Code to identify themselves as a moderator followed by #.
 - Press 1 to listen to the last recording
 - Or press 2 to listen to a previous recording. Option 2 lists the date, time and a allocated range number from 1 to 6. Press the range number to listen to the preferred recording.
2. Recording available for a limited period
The conference reference number allows moderators to access their last 6 recordings for up to 30 days.

Security Network Policy

IP private Network

Voice data is transported through the Arkadin private IP network to maintain data integrity:

- Arkadin infrastructure uses equipment and networks from Tier-1 technology provider
- Identified partners are providing the global private network across all the regions

IP Transport Layers Security

Arkadin International traffic, for dialing access, is carried over a MPLS network on dedicated VPNs between hubs / regions. It is on private LANs operated by Arkadin within each site.

MPLS Transport

Multiprotocol Label Switching (MPLS) is a mechanism in high-performance telecommunications networks that directs data from one network node to the next based on short path labels rather than long network addresses, avoiding complex lookups in a routing table. The labels identify virtual links (paths) between distant nodes rather than endpoints. MPLS can encapsulate packets of various network protocols

MPLS is a highly scalable, protocol agnostic, data-carrying mechanism.

IP VPN

Secure VPNs use cryptographic tunneling protocols to provide:

- Confidentiality by blocking intercepts and packet sniffing, allowing sender authentication to block identity spoofing
- Message integrity by preventing message alteration



Technologic Partners

- **SIP trunks**

- Session Border Controller Provider
- Specialist on VoIP firewalls hardwares
- Market leader, Carrier-Class
- For Conferencing



- **Media Server Supplier**

- Specialist in Conferencing Media Server
- Same as competitors
- Good Signal treatment & QoS (echo cancelation, delays)
- To connect VoIP and audio pstn access



- **Media Gateway Supplier**

- Specialist in Audio, VoIP and Media gateway hardwares
- Carrier-Class



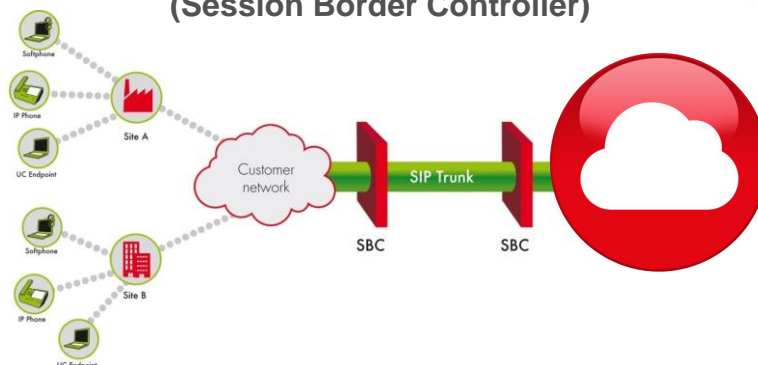
Security SIP trunk components

Dedicated VoIP trunk

All the conference data from the customer site to Arkadin will be carried across a direct network, without going via an intermediary or third-party (a carrier on a public PSTN).

The interconnection is from the customer site to Arkadin site so, the audio flow will be through a full managed network, control by the customer or Arkadin (depending on the option purchased).

**Figure 6: Secured SIP interconnection thanks to SBC installation
(Session Border Controller)**





Virtual Private Network

An IP VPN interconnection is setup between the customer and Arkadin.

Secure VPNs use cryptographic tunneling protocols to provide:

- confidentiality by blocking intercepts and packet sniffing, allowing sender authentication to block identity spoofing
- message integrity by preventing message alteration

Network-to-network tunnels often use passwords or digital certificates, as they permanently store the key to allow the tunnel to establish automatically and without intervention from the user.

A dedicated Virtual LAN (VLAN) tunneling is attributed per customer interconnection. It secures and guarantees the integrity of packets for the customer.

The protocol most commonly used today in configuring VLANs is IEEE 802.1Q.

The IEEE 802.1Q header contains a 4-byte tag header containing a 2-byte tag protocol identifier (TPID) and a 2-byte tag control information (TCI). The TPID has a fixed value of 0x8100 that indicates that the frame carries the 802.1Q/802.1p tag information. The TCI contains the following elements:

- Three-bit user priority
- One-bit canonical format indicator (CFI)
- Twelve-bit VLAN identifier (VID) - uniquely identifies the VLAN the frame belongs to

Session Border Controller

A session border controller (SBC) is a device deployed in Voice over Internet Protocol (VoIP) networks to exert control over the signaling and usually also the media streams involved in setting up, conducting, and tearing down telephone calls or other interactive media communications.

SBC role insures the security border between Customer VoIP network and Arkadin network.

SBC commonly maintains full session state, and offer the following security functions:

- Security – protect the network and other devices from:
 - Malicious attacks such as a denial-of-service attack (DoS) or distributed DoS
 - Toll fraud via rogue media streams
 - Topology hiding
 - Malformed packet protection
 - Encryption of signaling (via TLS and IPSec) and media (SRTP)



- Connectivity – allow different parts of the network to communicate through the use of a variety of techniques such as:
 - NAT traversal
 - SIP normalization via SIP message and header manipulation
 - IPv4 to IPv6 interworking
 - VPN connectivity
 - Protocol translations between SIP, SIP-I, H.323
 -
- Quality of service – the QoS policy of a network and prioritization of flows is usually implemented by the SBC. It can include such functions as:
 - Traffic policing
 - Resource allocation
 - Rate limiting
 - Call admission control
 - TOS/DSCP bit setting

In a SBC implementation, the term border refers to a point of demarcation between one part of a network and another. As a simple example, at the edge of a corporate network, a firewall demarcates the local network (inside the corporation) from the rest of the Internet (outside the corporation). A more complex example is large corporations where different departments have security needs for each location and perhaps for each kind of data. In this case, filtering routers or other network elements are used to control the flow of data streams. It is the job of a session border controller to assist policy administrators in managing the flow of session data across these borders.