PROTELION
GOVERNMENT SOLUTIONS

# SECURE AUDIO CONFERENCING WITH AR MESSENGER

USE CASE

## The Growing Challenges of Audio Conferencing Security

From everyday life to commercial applications, audio conferencing has become crucial for businesses, government agencies, and individuals. Whether for remote work, international collaboration, or confidential discussions, virtual meetings have replaced traditional in-person gatherings. However, the increasing reliance on conferencing platforms has also led to growing security concerns. Hackers exploit vulnerabilities in popular conferencing tools, leading to eavesdropping, unauthorized access, and data leaks.

Cybercriminals use various tactics, such as man-in-the-middle attacks and credential theft, to intercept calls. Sensitive corporate discussions, classified government communications, and private business negotiations are all at risk. Organizations must prioritize secure communication solutions to mitigate these risks effectively.

## Project Specifications

Protelion AR Messenger provides a robust, secure alternative for traditional video calls, ensuring encrypted and private communication without compromising ease of use. Working in tune with Protelion VPN Technology, AR Messenger enables users to communicate over a secure VPN connection, shielding voice and video calls from cyber threats.

Organizations requiring high-security audio conferencing can rely on AR Messenger to maintain privacy and data integrity. It supports:

- **Voice calls** with Protelion users
- **Participation in multi-party audio conferences** using SIP servers
- **Secure messaging** with one or multiple users
- **File and audio message transmission** with advanced encryption
- **Full encryption of traffic** within the corporate VPN network (AES)
- **Optional integration with SIP server** for audio conference management
- **Authentication of participants** to prevent unauthorized access

## Implementation

**1.** The company should set up a Protelion Virtual Private Network (VPN), which will be built using Protelion Secure Management Center (SMC), Protelion Security Gateway Appliances (SGA) and Protelion VPN clients with Protelion Messenger. These core components will serve as the foundation for establishing a private, highly secure network infrastructure.

**2.** Deploy the SIP server and perform its initial configuration according to the company's infrastructure requirements. Configure SIP settings on the server and then configure them in Protelion Messenger to ensure correct client communication.

**3.** Configure SIP credential settings in Protelion Messenger for conferencing to work. Ensure that the VPN tunnel supports all SIP traffic and that clients are correctly registered on the SIP server and ready to establish connections.

**4.** Use Protelion Messenger to create a new SIP conference by assigning a unique identifier (e.g., PIN or password) and generating invitations for participants.

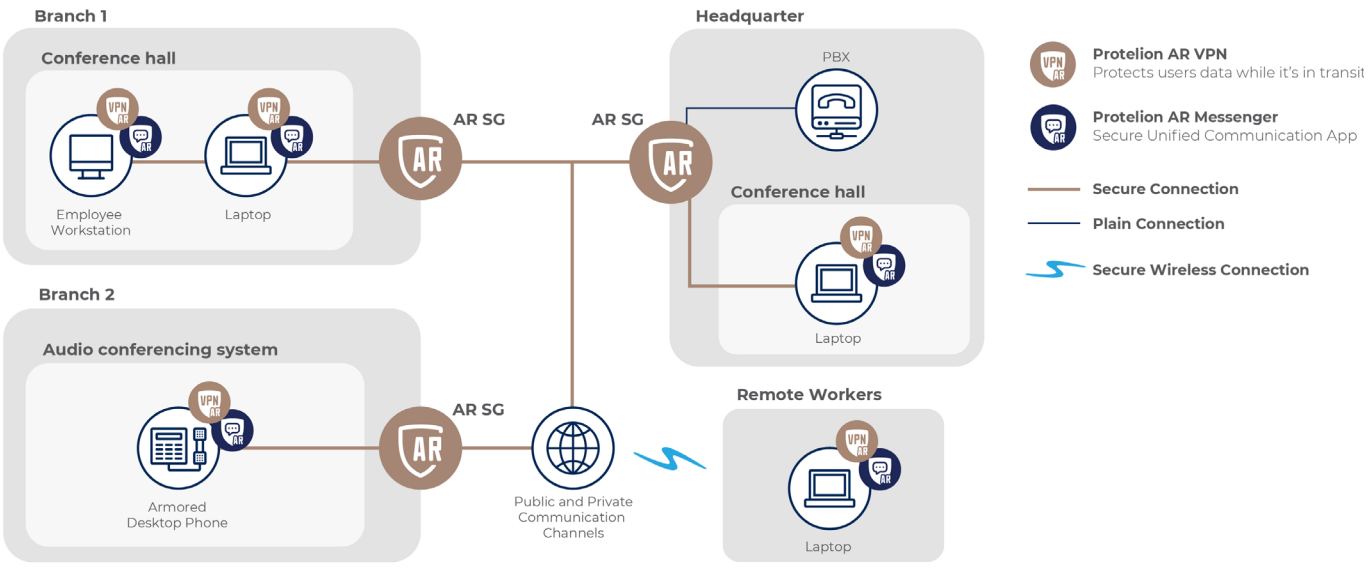
## Protelion Features

### Secure VPN link
All calls and messages are routed through a secure VPN, ensuring that the data remains encrypted and inaccessible to third parties even if intercepted.

### Cross-Platform Support
Available on Android, Windows, Linux, MacOS and iOS, ensuring compatibility across devices. expectations to the highest level.

### Centralized Contact Management
The Protelion Virtual Private Network administrator manages contact lists, minimizing unauthorized access and social engineering risks.

### Integration with existing infrastructure
AR Messenger seamlessly integrates with various VoIP and conferencing systems.




G.AC.25_v01_UCEng

PROTELION GOVERNMENT SOLUTIONS
Oberwallstr. 24
D-10117 Berlin,
Germany
+49 30 206 43 66-50
gov@protelion.com
gov.protelion.com