

## Business Language

	<b>AcousticPay</b>	<b>LISNR</b>
RSA Encrypted Payload	Yes	Yes
TLS Encrypted Payload	Yes	Yes
Hacking / Spoofing Detection	Yes	No
Unauthorized Transaction Detection	Yes	No
Data Transfer Speed	2,000 / second	1,000 / second
Unauthorized Transaction Request Tagging	Yes	No
High Range Ultrasonic Data Transmission	Yes	Yes
Medium Range Near Inaudible / Ultrasonic Data Transmission	Yes	No
TLS 1.3 (Transport Layer Security)	Yes	TLS 1.2

## More detail

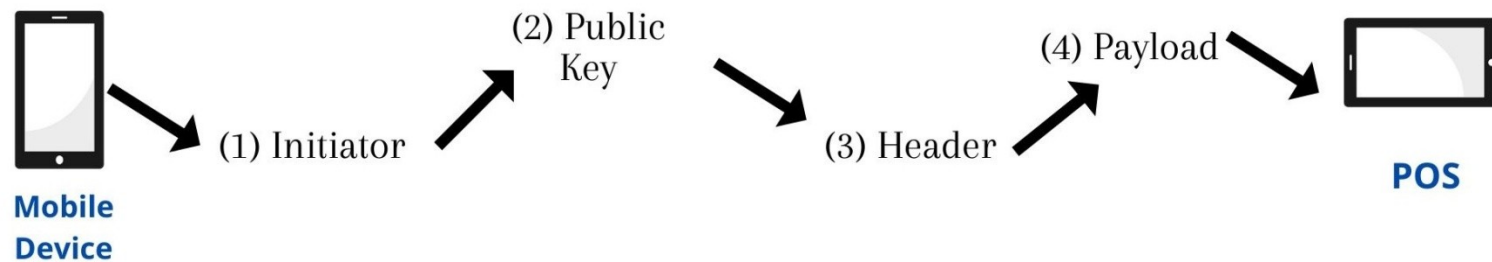
	AcousticPay	LISNR
RSA Encrypted Payload	Yes	Yes
TLS Encrypted Payload	Yes	Yes
Deep Learning based Audio Source Separation for Spoofing Issue	Yes	No
Deep Learning based Unauthorized Transaction Detection	Yes	No
Data Transfer Speed	2,000 / second	1,000 / second
Unauthorized Transaction Request Tagging	Yes	No
Ultrasonic Data Transmission ( > 20k)	Yes	Yes
In Audible Data Transmission (>19k < 20k)	Yes	No
TLS 1.3 (Transport Layer Security)	Yes	TLS 1.2

## How AcousticPay works?

A client having AcousticPay application initiates a mobile payment through their mobile device. Using the State of the Art technology of AcousticPay, ultrasonic or in-audible data transmission occurs, through, a secure tri-communication among the mobile device, server and POS (Point of Sale) terminal via microphone and speaker.

Mobile device and POS terminal sends and receives encrypted data between devices. AcousticPay uses UTAB technology, complete throughput of 2,000 bit per second to send and receive encrypted audio data.

Each audio message has four parts, the Initiator, PublicKey, Header and Payload.



- Initiator: The initiator tone announces the presence of an audio tone to start SDK demodulation.
- Public Key: Audio tone of Public Key.
- Header: The header contains the metadata regarding the payload.
- Payload: The main or actual data containing portions of the audio.

The development kit of AcousticPay allows different types of devices to utilize the power of inaudible and ultrasonic audio technologies.

Currently AcousticPay supports the follow platforms:

- Raspberry Pi
- POS Operating Systems (4690 OS, MS Windows POSReady, SUSE Linux POS 11, TCX Sky)
- Android
- iOS
- Linux
- Windows

### How AcousticPay Ultrasonic/Inaudible Payment Work?

AcousticPay technology bi-directional approach to exchange sensitive payment credentials. In this approach, both party uses same levels of security, Transport Layer Security.

### RSA-Encrypted Payload Approach

In RSA-Encrypted Payload Approach the mobile device gets Public Key (Public RSA Key) of Payment Terminal and creates an audio data message which contains encrypted credit card credentials (data encrypted by Public RSA Key). Then mobile device broadcast these data. The payment terminal receives the data and decrypt the audio message.

Payment terminal decrypts the data, sends to server, gets response from server and then responds another audio message containing ProcessingComplete status. ProcessingComplete status may convey success, failure, or any other issues. This approach provides high level security because only Payment Terminal knows the Private Key and can decrypt the data.

### TLS Payload Approach

In TLS Payload Approach, utilizes a full handshake to transfer data. Here, a ciphersuite used to encrypt the communication between mobile device and Payment terminal.

Client		Server
ClientInit	----- >	

		ServerInit
		Certificate
		ServerKeyExchange
	<-----	ServerInitDone
ClientKeyExchange		
ChangeCipherSpec		
Finished	----- >	
		ChangeCipherSpec
	<-----	Finished
TranscationData	<----- ----- >	Transactin Data