Casambi Whitepaper

Wireless lighting control for: **Casambi System Security**

CASAMBI

Introduction

Casambi's technology provides lighting designers and manufacturers with the ability to wirelessly link devices together enabling the creation of customizable smart lighting networks that are configured and controlled using the Casambi App. The solution is based on Bluetooth® Low Energy (BLE), a wireless technology built to communicate data within a short range.

Since its introduction to the market, BLE has succeeded to become a wireless standard and can be found in all smartphones and tablets today. In fact, growth forecasts predict that more than six billion Bluetooth-enabled devices will ship annually by 2025; 96% of which are expected to include BLE radio by the same year. Owing to its low-power mode, BLE is being used in a wide range of applications such as lighting, beacons, industrial sensors, fitness, medical devices, and others where sensitive information is being transferred over short distances up to several hundred meters.

When we speak of transferring data over radio waves, questions of wireless security quickly come to the fore. Data is valuable, and therefore becomes the target for costly hacks and consequent reputation damage.

Casambi is aware of the importance of cybersecurity to be successful as a lighting control solution provider and places it at the center of its strategy and mindset. Although Casambi has a solid reputation for continuously strengthening its security posture against any potential threats, the work never ends - the company remains vigilant and poised to adapt when needed.

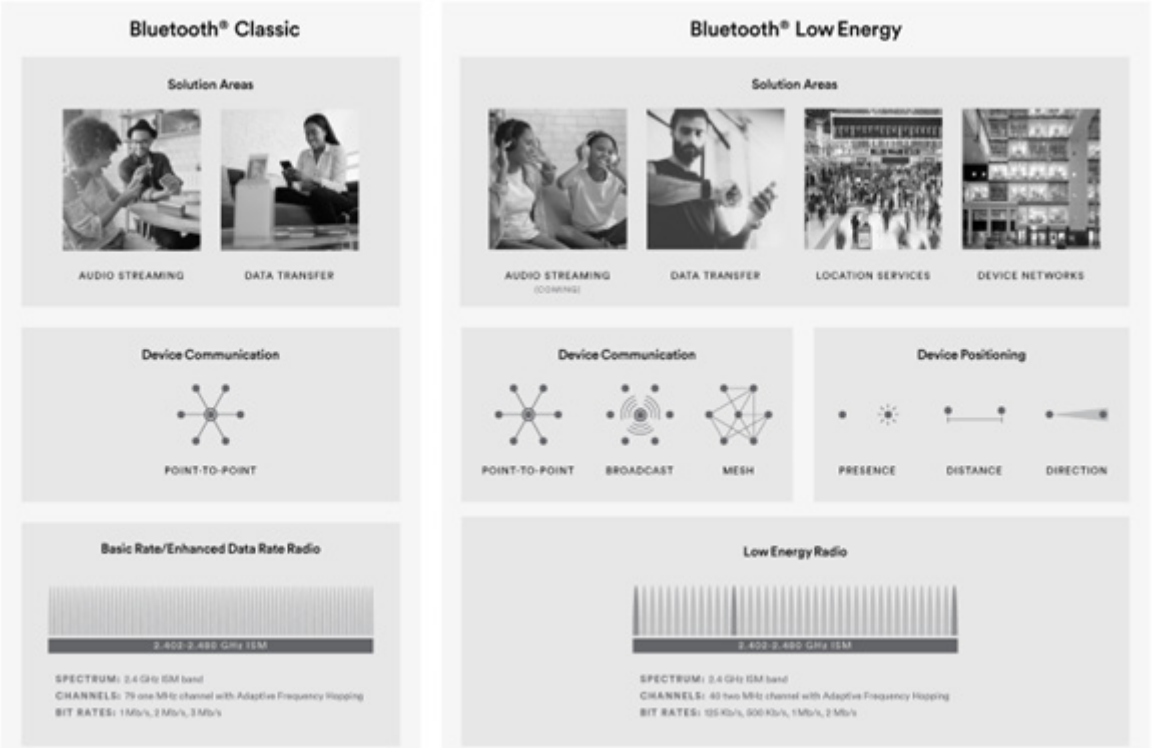
BLE and vulnerability

What Is BLE?

Bluetooth is a short range wireless techology standard that operates in the ISM band from 2.402 GHz to 2.480 GHz. There are two different types of Bluetooth technology: Bluetooth® Classic (Bluetooth BR/EDR) and Bluetooth® Low Energy.

Bluetooth® Classic is the technology that supports point-to-point device communication and is used to enable wireless audio streaming and data transfer across relatively short distances. It is commonly used in wireless speakers, keyboards, headphones, and in-car entertainment systems.

Bluetooth® Low Energy is designed for very low power operation and to transmit small data packages over 40 channels. BLE supports multiple communication topologies such as point-to-point, broadcast and mesh.



Bluetooth classic vs. Bluetooth Low Energy. [Extracted from Bluetooth website.]

Both are Bluetooth technology, however they are nearly completely independent protocols. The focus of this document is the Casambi mesh and how it communicates with smart devices using BLE.

We are using within our own internal mesh network different sub channels to the standard BLE. This means that we don't get interference even from the standard BLE channels. However, we also support the standard BLE channels. So we are fully compatible with the latest BLE 5.3 standard.

Types of cyberattacks facing BLE

The main ways in which hackers can exploit a BLE network are: passive eavesdropping, man in the middle (MITM) attacks and identity tracking.

Passive eavesdropping is the attack by which a third device passively listens to the data being transmitted between two paired devices.

A Man-in-the-middle attack occurs when a third device pretends to be a legitimate device in order to trick other devices into connecting to it. In this way, the attacker can take control over the entire network, intercept all the data being sent and inject false data into the communication. Identity tracking is when a third device is able to associate the address of a BLE device with a specific user and then physically track that user based upon the presence of the BLE device.

BLE Security

Bluetooth® Low Energy is a secure wireless communication protocol, but only if it is specified and implemented properly. The definition of security mode, security level and the pairing method is crucial to guarantee the security properties.

There are many security measures that can be used against potential threats: multiple device pairing schemes, encryption, authentication of connections, and address randomization.

Casambi Topology

Casambi's technology forms a mesh network ('Casambi Mesh'), which enables node-to-node communication inside a lighting network. The Bluetooth® Low Energy protocol enables communication between a mobile device (or the control device) and the Casambi platform. The mesh topology is self-healing, which means that, if a device fails, the signal flow automatically reroutes through other devices, ensuring that data has multiple routes to its destination. This increases reliability through multiple nodes and redundancy of nodes. Therefore, there is no single point of failure because no single critical element that stores the information is needed for the proper functioning of the network or part of it.

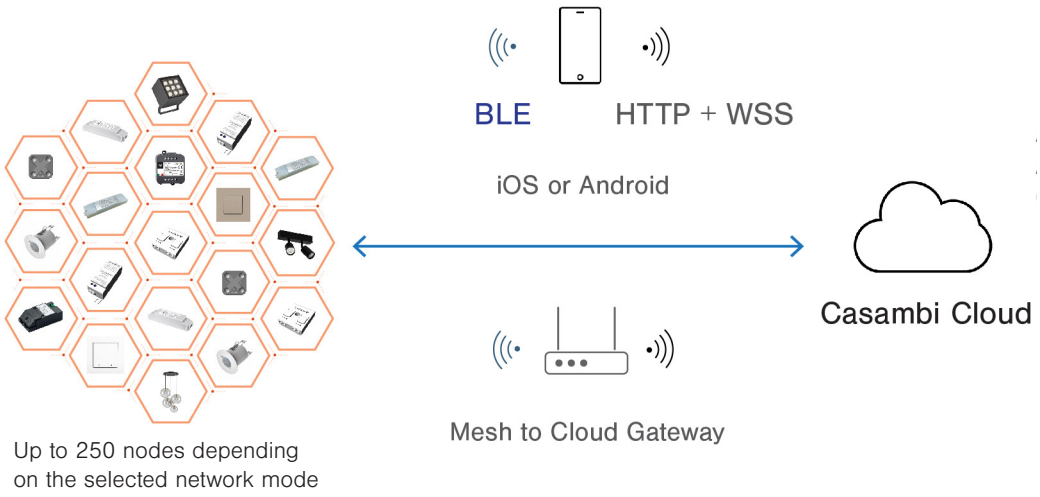
No special wiring for lighting controls is needed and all hardware complexity is reduced to a minimum because no central units such as routers, controllers or gateways are needed for the operation of a Casambi network. A Casambi network can contain up to 250 devices and each one is independent and has a backup of the entire network, i.e., all nodes of the mesh network carry the complete system intelligence.

Casambi Stand-alone mesh network

All system configurations and end user controls are managed via the Casambi App on mobile devices. No additional network connectivity is needed during normal operation; a Casambi network can function without being connected to the internet.

Casambi devices, and the Casambi mesh network they form, are not internet-facing. They don't have IP addresses. Casambi uses a proprietary protocol over which the Casambi nodes can communicate across the Bluetooth bandwidth.

An internet gateway can be used if it is required to have remote control over the network or to interface building management systems via a cloud connection. As this is internet-facing, great attention is paid to keep the Casambi security configuration up to date.



Casambi wireless mesh network with internet gateway

Network accessibility

With Casambi, it is possible to control access rights to your network and to define who interacts with the lights. The mesh network has 4 security levels that can be chosen and modified directly from the app:

- Open – free and open access for anyone without requiring a password. Modifications require an administrator password.
- Not shared – network details stored only on device used to create the network. Other devices cannot access the network.
- Password protected – possible to use and edit network with a visitor password, except sharing settings.
- Administrator only – only administrator(s) can access with an administrator e-mail and password.

When the network is in ‘Not shared’ mode, there is no cloud communication. When the network is in ‘Administrator only’, ‘Password protected’ or ‘Open’ mode, the Casambi mobile application will send a (backup) copy of the network configuration to the Casambi cloud.

Security is about working in layers – it’s about adding additional barriers to entry. Casambi’s system architecture has been built to maximize resiliency against attack. In most cases the system security essentially boils down to the credentials of users. The only way to access the data is if you have the proper credentials. As an additional measure to manage security and the integrity of data, Casambi provides different levels of access for users:

- **Admin**: Has full control of all network aspects.
- **Manager**: Can configure the network (i.e., change programming), but not create new user accounts.
- **User**: Can only use the network but cannot make any programming changes.

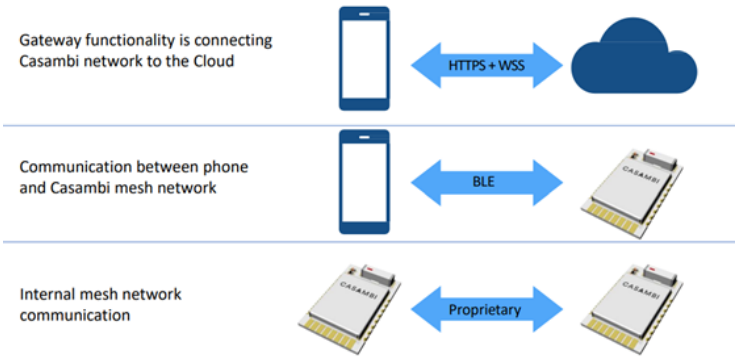
Up to 10 access tokens can be set for either User, Manager, or Administrator roles. On the network level, other accessible possibilities are also provided:

- Device lock to prevent unpairing (without administrator access).
- Update of firmware can also be disabled to prevent any changes occuring at the firmware level
- Network configuration can be backed up to the cloud via a mobile phone app.
- The network can be hidden from other users.

Communication channels and security

Each Casambi network contains 3 main communication channels:

- Communication between gateway and cloud (only if cloud connection is required)
- Communication between mobile and unit/mesh network
- Communication from unit to unit in mesh network



Casambi communication channels

Communication from unit to unit in a mesh network

Unit-to-unit communication in a mesh network uses only encrypted packets and the initialization vector for each message consists of network ID, unit ID and rolling code.

In order to prevent replay attacks (whereby an attacker intercepts and fraudulently resends network data packets that don't belong to them), each unit performs bi-directional challenge/response authentication with all neighboring units.

Communication between mobile and unit

Casambi uses industry standard well-known algorithms for encryption: ECDH with secp256r1 curve, AES-128 symmetric cryptography and SHA-256 digests. Full encryption between the mobile device and the units is provided, where both sides (mobile and unit) generate a new public/private key pair for each connection.

Communication between gateway and cloud

The connection between a mobile device/gateway and the cloud is secured by TLS (Transport Layer Security).

All communications are done via HTTPS (Hyper Text Transport Protocol Secure) and WSS (Web Services Security) which is a trusted end-to-end communication process. This prevents hackers from sniffing out passwords and hijacking user accounts.

Full encryption

All communications channels are encrypted, which means that the information is converted into secret code that hides the information's true meaning, preventing unauthorized third parties from accessing the data.

Since Casambi has different communication channels and offers a multitude of solutions – from APIs, mobile apps, and different solutions that participate in how we manufacture devices – the company uses various encryption algorithms and techniques for securing data:

- AES-128: Symmetric encryption cipher.
- AES-CMAC: Message authentication algorithm for data integrity.
- ECDH: Elliptic curve key exchange.
- ECDSA: Elliptic curve digital signature algorithm.
- Full encryption between mobile device and units. New encryption key for each connection, derived with ECDH.
- 10 changeable passwords.

Over-the-air updates allow Casambi to push new security features and software patches out to the entire fleet of installed devices at once.

Preventions

Different methods are used to prevent different types of cyber-attack:

- **Prevention of replay attacks**: using rolling codes for packets, and two-way authentication between units to validate initial rolling codes.
- **Prevention of eavesdropping**: fully encrypted communication. Unit-to-unit communication is even impossible for network administrators to decrypt.
- **Prevention of man-in-the-middle attack**: two-way authentication between mobile device and unit, and unit-to-unit.
- **Prevention of trash-can attack**: mobile device verifies the authenticity of the unit before it is added to network.
- **Prevention of tampering**: strong message integrity checks.

Cloud Security

Casambi services are hosted on the Microsoft Azure cloud platform. Microsoft Azure is a cloud computing platform that provides multi-layered security and unique threat intelligence to help identify and protect against rapidly evolving threats.

The cloud requires username and password, that allows an access token to a local “Bluetooth network”. Passwords are stored using one-way hash algorithms. With an access token, only a local network can be accessed. An access token is a cryptographically verifiable opaque key identifying its bearer and it allows role based access to the network for one mobile device. When network passwords are changed all affected access tokens are invalidated.

Only information related to network configurations and system performance is stored in the Casambi cloud. This data can only be accessed by Casambi for troubleshooting, debugging the system, or optimizing system performance. This analysis is always done in an aggregated format. Data Aggregation is the process of collecting data about the usage and performance of the software to analyze and improve system performance. During this process, all personal data is anonymized, and no part of the information is shared with other third parties. Casambi is committed to protecting its customers data privacy with industry leading security.

ioXt Certification

Casambi has received ioXt Alliance cybersecurity certification for its system, affirming its ongoing commitment to network security for customers and stakeholders.

Casambi’s wireless lighting control system has tested positively against the alliance’s eight guiding principles:

- No Universal Passwords – Unique security credentials are required for operation.
- Secured Interfaces – Product interfaces are appropriately secured.
- Proven Cryptography – System security uses strong, proven, updateable cryptography.
- Security by Default – System security is appropriately enabled by default.
- Verified Software – The system only supports signed software updates.
- Automatic Security Updates – Established strategy for applying timely security updates.
- Vulnerability reporting program – Actions encouraging the responsible reporting of suspected vulnerabilities or weaknesses in the system.
- Security Expiration Date – Transparency on end-of-life policies and the provision of security updates.

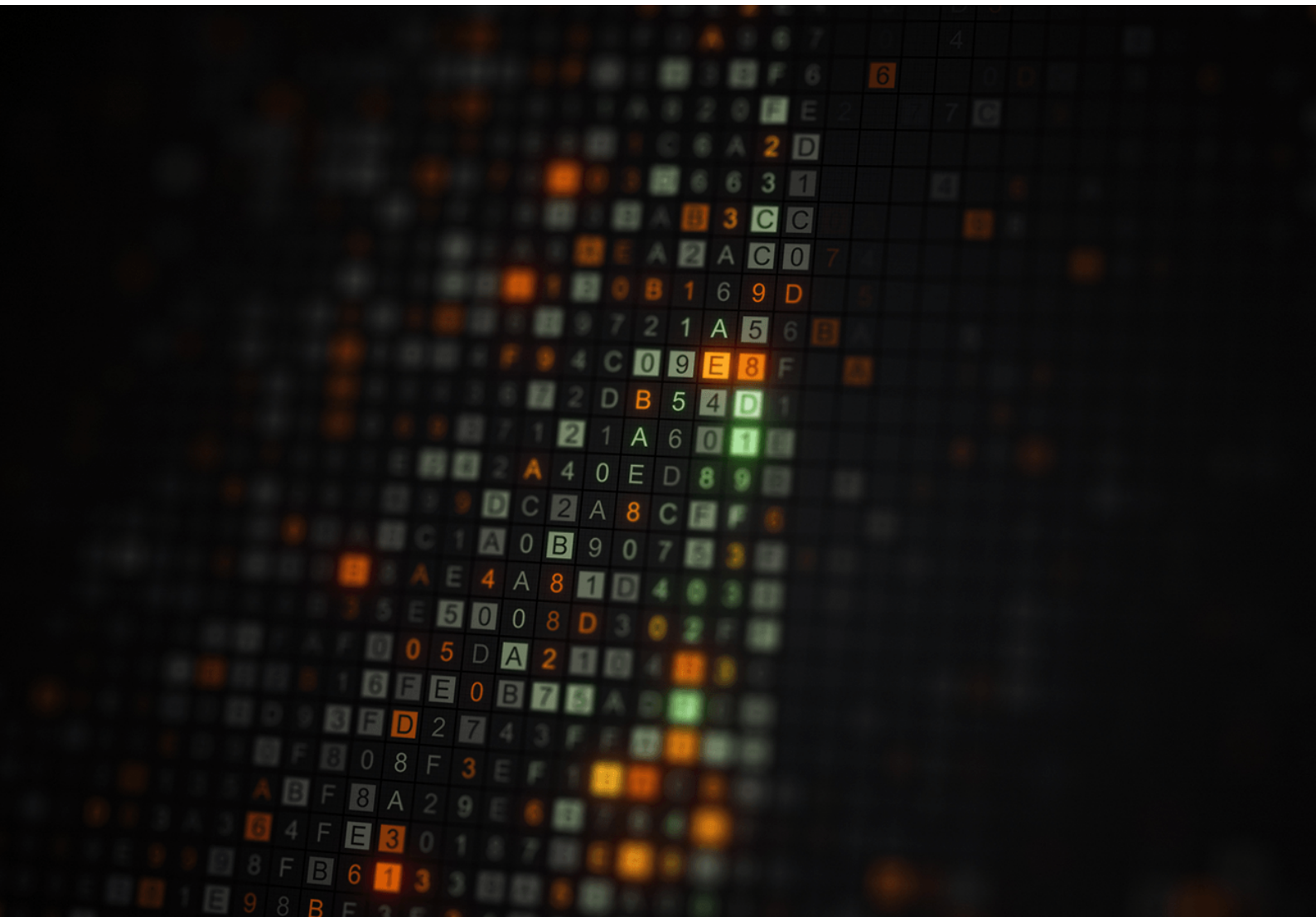
Engaging the ethical hacker community

Casambi highly values the work that security researchers and ethical hackers undertake in good faith to secure the cyber world. As security is a prime concern, Casambi has a **Vulnerability Disclosure Policy**, which provides clear guidelines for conducting vulnerability discovery activities and for the process of reporting potential vulnerabilities in Casambi systems.

For more information, please access *https://casambi.com/vulnerability-disclosure-policy/*

Casambi in highly sensitive environments

Casambi is deployed in highly sensitive environments, such as in hospitals and airports, where reliability and security of communication are critical. Such cases bear testimony to the hardiness of the technology and supporting services. The system is robust in design and has been certified as cyber-secure in accordance with global standards.



Case studies

Ulster Hospital

The Casambi control solution covers all the hospital lighting, namely the bedrooms, nurses' stations, corridors, plant rooms, offices, and all exterior lightings around the perimeter and the roof.

A particular function that Casambi provides is in the patients' bedroom, where several sensors monitor such things as "out of bed movement" (alerting nurses if a patient is out of bed) and daylight, which in turn adjusts the lighting accordingly. The bedrooms' lights can also be controlled from the nurses' station in such events as an emergency. Additionally, many of the bedrooms' scenes provide, via a bedside handset, different scenes for such things as reading or watching TV.

Site: Ulster Hospital, Acute Services Block

Location: Belfast, United Kingdom

Casambi nodes: 9 000+

BBC

The BBC's output reaches more than 400 million people worldwide every week, and its 24/7 TV news operation is the biggest in the world. In 2020, the organization decided to bring the same forward-thinking approach to its buildings, which house numerous TV and radio studios, data centers, and offices.

The BBC installed Casambi's wireless lighting control system at nine of its buildings across the UK.

Choosing Casambi gave the BBC team access to the entire Casambi Ready ecosystem of thousands of interoperable sensors and control devices. Sensors from Tridonic and Danlers have been installed to enable presence/absence detection and daylight dimming, ensuring lights are only on when they're needed. Energy-harvesting wireless switches from EnOcean are also being used, which provide another easy way for staff to control the lights. EnOcean's wireless switches are particularly well suited to Casambi because Casambi's is the only lighting control system in which they can be paired with the whole network, rather than just the nearest individual node, ensuring reliable commissioning and operation.

The installation at Broadcasting House was carried out during late evenings, and each area being upgraded had to be ready the following morning when staff returned to their desks, so there would be no disruption.

Site: New Broadcasting House (London), Wogan House (London), Energy Centre (London), Mailbox (Birmingham), Glasgow Pacific Quay (Belfast), Manchester Media Centre, BBC Oxford, and BBC Radio Nottingham.

Location: United Kingdom

Casambi nodes: 10.000+

Helsinki Airport

Project objectives were to find a long-lasting, high-quality lighting solution that would be wireless for sections of Terminal 1, including the high ceilings, the maintenance corridors on the bottom floor, and the corridors connecting terminals T1 and T2. Additionally, unique scene-setting abilities for the different areas and improved energy efficiency overall were also set as high priorities.

Airport terminals require 24/7 optimized illumination, all year round. At Helsinki Airport, this has been achieved with Casambi Ready daylight sensors that adjust the lighting levels as needed when there is a plentiful amount of sunlight coming through the terminal's large windows. General lighting at the boarding gates has been assigned to ensure a calm and cozy atmosphere. Commercial spaces within the vicinity (each with its brand guidelines) also have more apt lighting.

Site: Helsinki Airport

Location: Vantaa, Finland

Casambi nodes: 2500

Terminology

AES - Symmetric encryption cipher
AES - CMAC – AES Cipher based Message Authentication Code
API – Application Programming Interface
BLE – Bluetooth® Low Energy
ECDH – Elliptic Curve Diffie-Hellman key exchange algorithm
ECDSA – Elliptic Curve Digital Signature Algorithm
HTTPS - Hyper Text Transport Protocol Secure
ID - Identification
ISM band – Industrial, Scientific, and Medical Radio Band
MITM – Man in the midle
TLS - Transport Layer Security
WSS - Web Services Security

CASAMBI

casambi.com