

— **Technical Resources**

Document Ref : 8348

11_2018

Version: 2



©Eseye Limited

— IoT Security Explained



Version number	Date	Author	Changes
2	November 2018		

+ 44 1483 802501 | +1 512-813-0599 | +27 87 551 8200 | +33 9 87 67 53 36 | +61 8 9551 5200 | +61 400 435 1000 Eseye, AnyNet, AnyNet Secure and Eseye Logos are registered trademarks of Eseye Ltd © Eseye 2018 Limited. All Rights Reserved. enquiries@eseye.com | eseye.com

– Table of Contents

Prevention of unwanted communications	2
VPNs	2
Restricted access	2
Enable only the required services	2
SIM card theft deterrence	3
MFF Embedded SIMs	3
Modem locking	3
Location locking	3

Eseye's secure globally available infrastructure and managed connectivity provides access to numerous security features. These security features are designed to provide security without affecting the performance or usability of the device.

The two main security threats to IoT devices are: **unwanted communications**, and **SIM card theft**.

Prevention of unwanted communications

Unwanted and potentially malicious communication represents a significant risk to IoT devices. These interactions can result in devices racking up large bills or being compromised to an extent that they are not performing their designed functions. Ultimately resulting in expensive maintenance visits. To restrict the unwanted communications Eseye offers the following recommendations and services:

VPNs

Eseye recommends using VPNs. Virtual Private Networks provide secure tunnels for data to be transferred. Eseye provide VPNs from devices through to customers' systems. This prevents anyone else from accessing the data or interacting with a deployed device.

Restricted access

Eseye recommends using restricted points of access. Eseye offers this service through 'Access Control Lists' for data transmissions and 'white listing' and 'blacklisting' for SMS and voice services. This prevents anyone else from interacting with a deployed device.

Enable only the required services

Eseye only allow the requested services (data, SMS, USSD, etc.). For example, if customers are not going to use SMS then there is no value in being vulnerable to its risks. This removes the risks associated with unused and unrequired services.

SIM card theft deterrence

IoT devices are expected to be deployed unattended for long periods, this leaves them vulnerable to the SIM card being removed and used in other devices, resulting in unexpectedly large bills. To help protect against this Eseye offers the following recommendations and services:

MFF Embedded SIMs

Eseye recommends using embedded SIM cards (MFF2 standard). Using MFF2 SIM cards negates the cost, of the SIM card socket while preventing the SIM card from being usable in other devices. This prevents an end user from stealing and using the SIM card.

Modem locking

Eseye recommends using a modem lock. Eseye normally uses TAC locking although individual IMEI locking can be configured too. Modem locking ensures that only the correct device(s) register on the network. This prevents the SIM card from being usable in a different device.

Location locking

Eseye recommends location locking. Location locking prevents a device from being able to register on the network in unplanned regions. This prevents a SIM card or device from being used in unexpected regions.

Eseye's security looks after both your data and your finances.

With data secured, costs should not soar as a result of unwanted communications, or SIM card theft.