Software Design Specification

Z/IP LAN Security

Document No.:	SDS12938
Version:	
Description:	Z/IP LAN Security provides a framework for secure communication between Z/IP Clients and Z/IP Gateways
Written By:	JRM;AES;ABR;JFR;BBR
Date:	
Reviewed By:	JBU;MDUMBARE;AES;JRM;DCHOW
Restrictions:	Public

Approved by:

Date	CET	Initials	Name	Justification
2018-03-06	09:25:28	NTJ	Niels Thybo Johansen	

REVISION RECORD

Doc. Rev	Date	By	Pages affected	Brief description of changes
2	20160823	ABR	All	First revision for public release
3	20180306	BBR	All	Added Silicon Labs template

Table of Contents

1 ABBREVIATIONS

Abbreviation	Explanation
DTLS	Datagram Transport Layer Security
PSK	Pre-Shared-Key

2 INTRODUCTION

This document specifies a framework for secure communication between Z/IP Clients and Z/IP Gateways.

2.1 Terms used in this document

The guidelines outlined in RFC 2119, [1] apply.
Essentially, the key words "MUST", "MUST NOT", "REQUIRED", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

3 Z/IP LAN SECURITY

The Z/IP LAN Security framework provides a means of securing the communications path between:

- Z/IP Clients
- Z/IP Clients and Z/IP Gateways
- Z/IP Gateways

Starting with Z/IP Gateway 2.x, Z/IP UDP packets sent to and from the Z/IP Gateway MUST be secure. The same mechanism MAY be used to send secure Z/IP UDP packets between Z/IP Clients.

Z/IP UDP packets MUST be secured by wrapping ordinary Z/IP UDP packets in a DTLS 1.0 wrapper. DTLS is the datagram version of TLS. The default UDP port number for secure Z/IP communication MUST be 41230.

3.1.1 Supported Key Exchange Algorithms

The Pre-Shared-Key exchange algorithm MUST be used for key exchange.

The following ciphers MUST be supported:

3.1.1.1 Pre-Shared-Key Key Exchange

The Pre-Shared-Key Key (PSK) key exchange algorithm is based on a shared secret between two communicating parties. One end (the *Provider*) MUST provide the shared secret via at least one of the below methods:

1. A Sticker on the device
    a. The sticker MUST present a human readable PSK
    b. The sticker MAY present a machine readable code with PSK, such as QR code

2. A Display capable of displaying the PSK upon physical interaction with the device
    a. The display MUST present a human readable PSK
    b. The display MAY present a machine readable code with PSK, such as QR code

The PSK MUST be entered by the other party (the *Consumer*), either by means of human interactions or through a machine readable code, e.g. a QR code.

If the PSK algorithm is used for Z/IP security key exchange, the PSK MUST be the same for all Z/IP devices in the network.

- **Network with Z/IP Gateway capable of LAN Security**
    - A *Consumer* MUST perform the key exchange using the PSK provided by the Z/IP Gateway being the *Provider*.
    - If multiple Z/IP Gateways exist, there MUST NOT be more than one *Provider*.

- **Network with no Z/IP Gateway or where**
  LAN Security is not supported by the Z/IP Gateway
    - Any Z/IP Client in the network MAY become a *Provider* and provide the PSK, but all *Consumers* MUST perform the key exchange using the PSK provided by Z/IP Client being the *Provider*.

- **Network with two Z/IP Gateways**
  - A *Consumer* Z/IP Gateway MUST use the PSK given by the *Provider* Z/IP Gateway for, rather than the PSK presented on the sticker of the *Consumer* Z/IP Gateway.
  - A *Consumer* Z/IP Gateway MUST reject all connection attempts using its own PSK.

3.1.1.1.1 PSK Requirements

- A Z/IP Gateway MUST implement at least one of the following ciphers
  - PSK-AES256-CBC-SHA
  - PSK-AES128-CBC-SHA
- The Z/IP Gateway PSK MUST be at least 16 bytes.
- The Z/IP Gateway MUST NOT use PSK_identity and identity_hint messages [2].

3.2 Timeout and disconnect.

A Z/IP Client and server MUST implement a 60 second timer which is renewed whenever a datagram is sent or received over the DTLS connection. On timeout or disconnect, a Z/IP Client or Z/IP Gateway MUST send a “Shutdown” alert to its counterpart and close its session.

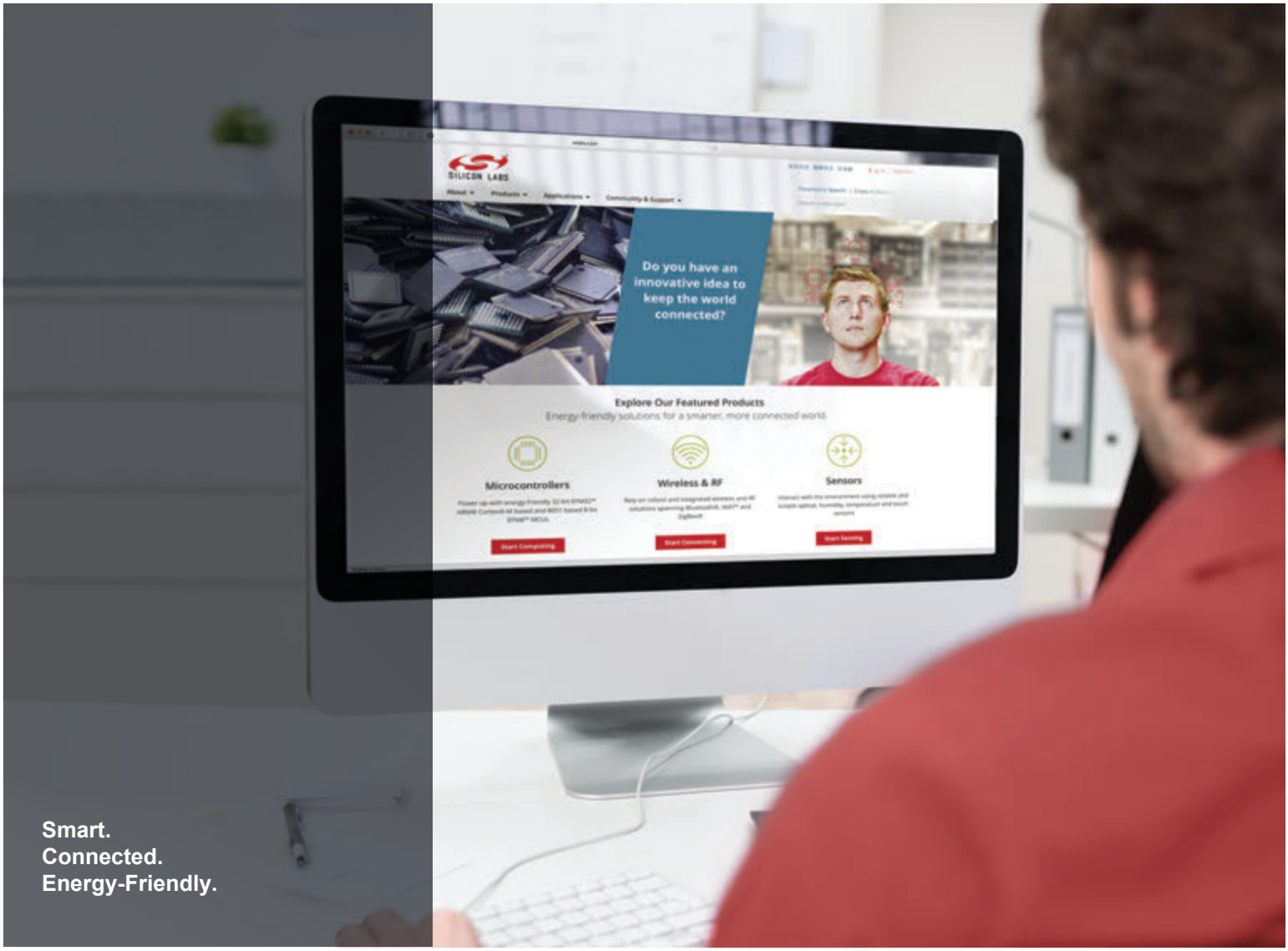
When a Z/IP client or a Z/IP Gateway shuts down its network connection it MUST send a Shutdown alert to close all its open sessions.

If a Z/IP Packet is transmitted with the Ack Request flag set, and no Z/IP Ack/Nack Waiting Response packet is received within 500ms, the sender MUST send a Shutdown alert and establish a new DTLS session.

Z/IP Keep Alive Commands MUST be used to monitor the health of a secure Z/IP LAN session.

REFERENCES

[1] IETF RFC2119, Key words for use in RFCs to Indicate Requirement Levels, March 1997.
[2] IETF RFC4279, Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)
[3]



Products
www.silabs.com/products

Quality
www.silabs.com/quality

Support and Community
community.silabs.com

SILICON LABS®

Silicon Laboratories Inc.
400 West Cesar Chavez
Austin, TX 78701
USA

http://www.silabs.com