Prepaid Cellular Experience

with WPA2 and OCS

SigScale

What’s wrong with public Wi-Fi?

Legacy technology is holding us back!

Wi-Fi Consumers are Asking:

“Why can’t public Wi-Fi be as seamless and transparent as cellular?”

Wi-Fi Consumers are Asking:

“Why can’t my device connect automatically to public Wi-Fi?”

Wi-Fi Consumers are Asking:

“Why are public Wi-Fi networks not secure? Am I in danger of being hacked?”

Wi-Fi Service Providers are Asking:

“How can we gain more revenue from our installed base of access points?”

Wi-Fi Service Providers are Asking:

“How can we gain more revenue from our existing subscribers?”

Wi-Fi Service Providers are Asking:

“What impact will the Internet-of-Things (IoT) have on public Wi-Fi?”

Captive Portal

A solution to a 2004 problem is the industry's biggest problem today!

Wi-Fi HotSpot Captive Portal

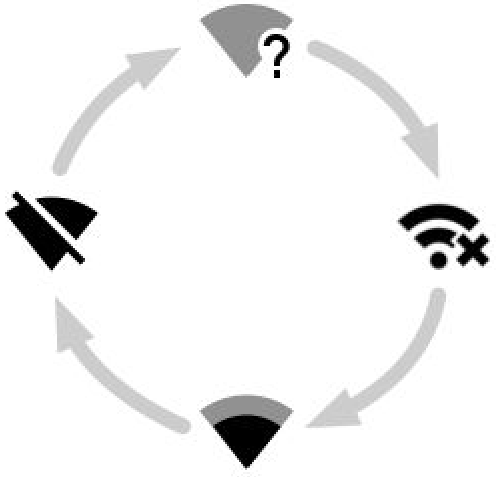
- Unsecured (“open”) 802.11 Wireless Local Area Network (WLAN)
- DHCP server assigns device an IP address and default gateway
- Default gateway does not route IP packets initially
- HTTP requests to any destination are answered by captive portal
- Captive portal answers with an HTML login page for the HotSpot
- A person must fill out a form (e.g. name, password, address, etc.)
- On sending complete form response the person is authenticated
- On success the MAC address of person’s device is authorized for access
- Default gateway enables routing of IP from MAC address to Internet

Four Wi-Fi Network States

1. **Wi-Fi Disabled**
2. **Network Selection**

   Waiting for manual selection from list of all available networks
3. **Connection Problem**

   Wi-Fi connected but Internet access blocked until user opens browser and completes captive portal registration
4. **Connected**



Drawbacks of Captive Portals

✘ Built on Lies

- DHCP: Here's a default gateway (a router that doesn't route!)
- DNS: "You want google.com? Yeah that's me!"
- Browsers reject spoofed secure (HTTPS) sites yet most sites now secure

✘ Cumbersome and Time Consuming for Users

- Requires people to open a web browser, navigate to a web form and type answers
- If multilingual it adds complexity, else impossible for people of other languages
- Thousands of browser versions and possible screen sizes makes incompatibilities likely

✘ Single Use Case Only

- Works only for devices with web browsers and human operators
- Most mobile traffic is from smartphone apps, people want to open their apps not browsers
- Rules out Internet-of-Things (IoT) entirely

✘ Security, Worse than None

- Effectively a man-in-the-middle attack, the acceptance of which weakens security practices
- Requires unsecured 802.11 wireless LAN
- MAC authentication is easily spoofed

WPA2

(Wi-Fi Protected Access)

An industry standard technology in use for a dozen years in enterprise and at home.

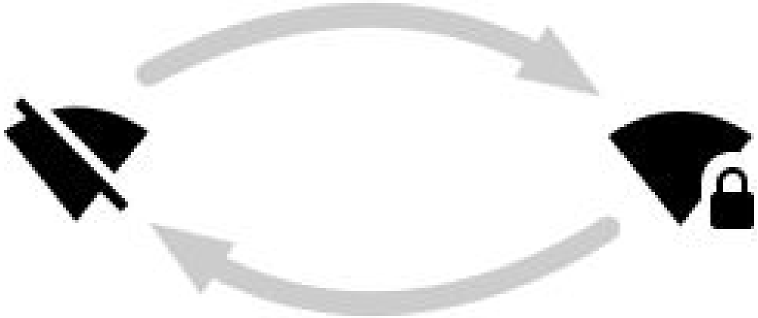
Wi-Fi Protected Access (WPA2)

Captive portals on **open** Wi-Fi networks have been used for over a decade however that technology was a hack, needed at the time, but not today.

All devices manufactured since **2006** are compatible with **WPA2** allowing secure wireless local area networks (WLAN) with **devices** which **authenticate themselves automatically**.

Two States: Off & Secure

With **WPA2** after enabling Wi-Fi the device scans for networks and when it recognizes one it has credentials for it automatically attaches with an encrypted secure connection.



Wi-Fi Protected Access (WPA2)

The original secure mode in IEEE 802.11 was **WEP** which turned out to be fairly easy to crack. The Wi-Fi Alliance developed **WPA** (2003) which introduced **TKIP** and **WPA2** (2004) (IEEE **802.11i)** which brought **AES** which is the preferred encryption method today and considered very secure.

Certification began in 2004 and from March 13, **2006** WPA2 certification is **mandatory for all new devices** to bear the Wi-Fi trademark.

WPA-Enterprise (IEEE 802.1x)

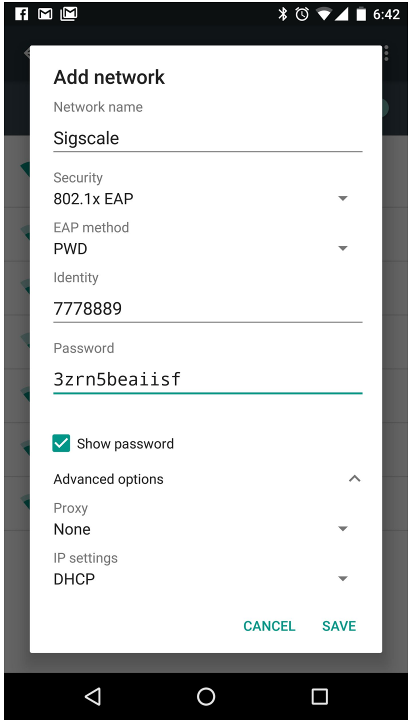
While WPA-**PSK** (Pre-Shared Key) uses a common secret for all wireless stations **WPA-Enterprise** utilizes the **802.1x** standard which allows a **AAA server** to uniquely authenticate the identity of each device.

The Extensible Authentication Protocol (**EAP**) is tunneled from Wi-Fi device over 802.11 and **RADIUS** to AAA server.

By **2005** Wi-Fi Alliance certification included several EAP methods including **EAP-TTLS**.

EAP Supplicants Replace Portal Login Forms

- ✓ Wi-Fi devices include a "**supplicant**", a built in **EAP** client which prompts user for authentication **credentials** required by the selected Wi-Fi network (SSID) first time
- ✓ Enter authentication credentials once
- ✓ Automatically attaches to network anytime within range without prompting user



Add network

Network name

Sigscale

Security

802.1x EAP

EAP method

PWD

Identity

7778889

Password

3zrn5beaiisf

☑ Show password

Advanced options

Proxy

None

IP settings

DHCP

Extensible Authentication Protocol (EAP)

Wi-Fi Alliance certification for **WPA2** requires support for either EAP-TTLS or EAP-TLS at a minimum.

EAP-TTLS uses an X.509 public key certificate on the server to establish a secure transport and then uses MSCHAPv2 to authenticate the client with a username and password.

EAP-TLS uses a unique certificate installed on the device to authenticate the client.

EAP-SIM and **EAP-AKA’** are also supported for authentication using credentials on SIM cards.

Many other **EAP methods** have been defined and may be used subject to **negotiation** between client and server:

EAP-PWD is a recent addition which authenticates using a username and password but without requiring certificates. It has very good security through the use of elliptic curve cryptography.

Android and Linux clients support EAP-PWD but iPhone and Microsoft currently do not.

SigScale OCS fully supports EAP-PWD.

Authentication, Authorization & Accounting (AAA)

The role of a **AAA** server is to **centralize** the functions related to securely identifying entities making access requests (**who?**), granting specific authorizations (**what?**) and keeping track of usage (**how much?**).

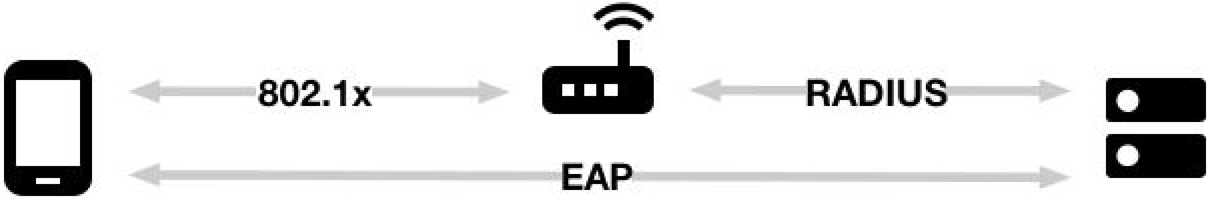
Network Access Servers (**NAS**), such as Wi-Fi access points, use the **RADIUS** protocol to send **Access-Request** messages to a AAA server. If the **identity** of the requester can be **authenticated** (e.g. correct username/password), and she is currently **authorized** to use the network (i.e. account not suspended), access is granted and parameters supplied (e.g. rate/time limit) to NAS.

Accounting-Request messages may be at session start, end and optionally periodically during a session.

Disconnect-Request message may be sent to NAS by AAA to **terminate** a session.

AAA Protocols

- access point relays access requests to AAA server
- EAP is tunneled inside of RADIUS
- 802.11 station authenticates directly with AAA server
- access point authorizes based on RADIUS request result



Prepaid

Online Charging System (OCS)

A secure dynamic centralized AAA server sets the stage for real time credit management.

Online Charging System (OCS)

An **OCS** is a AAA server which also performs **real-time credit management**. Authorization of a subscriber access request includes determining if their current **account balance** is sufficient to pay for the request.

When an Access-Request is allowed the OCS may include attributes which ensure Accounting messages are sent at periods sufficient to manage the available credit.

During an ongoing Wi-Fi access session interim accounting messages shall **decrement** a subscriber’s available credit balance.

When an account top-up is made the OCS will again authorize access.

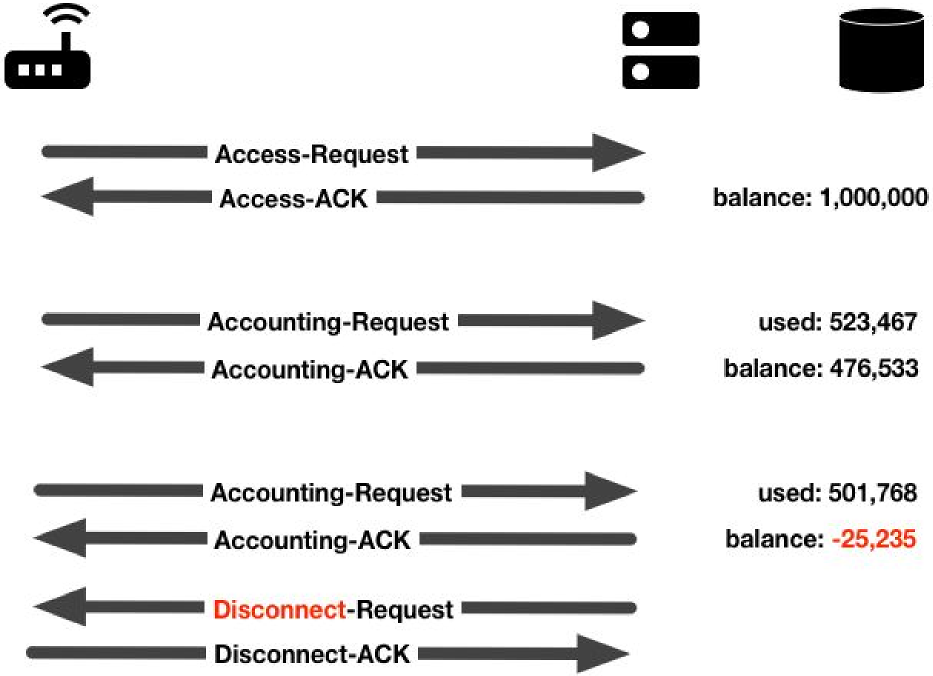
RADIUS Accounting & Disconnect

RADIUS accounting messages are sent at the beginning and end of a **session**. The NAS (AP) may also be configured to send Interim accounting messages at regular **intervals** during a session.

Accounting messages include **totals** for the number of **bytes** sent and received.

An Online Charging System (**OCS**) will check the subscriber's **balance** when access is requested and deny authorization when it is too low. The totals in **interim** accounting messages also compared to the subscriber's balance.

OCS sends a **disconnect** request when balance is too low to continue.



Question: What’s wrong with public Wi-Fi?

Answer:
Service providers not keeping up with technology curve.

Wi-Fi Consumers are Asking:

Q: Why can’t public Wi-Fi be as seamless and transparent as cellular?

A: With WPA2 your device prefers subscribed Wi-Fi networks whenever available and falls back to cellular when Wi-Fi is no longer available.

Wi-Fi Consumers are Asking:

Q: Why can’t my device connect automatically to public Wi-Fi?

A: With WPA2 your device connects while it is still in your pocket, you’ll find out Wi-Fi is available by notifications of incoming email and Facebook updates!

Wi-Fi Consumers are Asking:

Q: Why are public Wi-Fi networks not secure? Am I in danger of being hacked?

A: With WPA2 your device maintains a strongly encrypted wireless connection at all times. No known exploits exist to break AES cryptography.

Wi-Fi Service Providers are Asking:

Q: How can we gain more revenue from our installed base of access points?

A: By forcing subscribers to open a browser to manually connect a large portion of potential traffic is simply filtered out. WPA2 removes that filter!

Wi-Fi Service Providers are Asking:

Q: How can we gain more revenue from our existing subscribers?

A: Captive portals target the single use case of web browsing, but today most popular services use “apps”. WPA2 supports all apps, so more paid traffic!

Wi-Fi Service Providers are Asking:

Q: What impact will IoT have?

A: Smart watches, fitness monitors, e-readers, toys, cars, drones, security cameras, alarms, trackers, sensors, ... these devices need to connect automatically. It’s WPA2 or nothing!

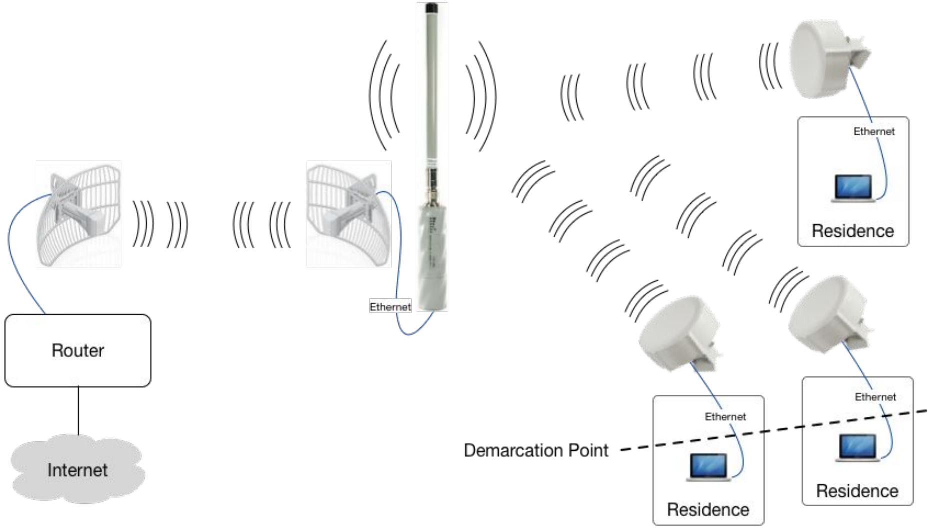
Case Study

Mexican Rural WISP

Taking the next step from fixed wireless to mobility and casual access.

Established Rural Wireless ISP in Mexico

- ✓ Started in 2005 to serve small towns where no Internet access (or cell phones) available
- ✓ Customer Premise Equipment (CPE): Mikrotik SXT2 Lite (STA) installed at each subscriber address
- ✓ Omnidirectional 2.4Ghz Mikrotik Groove (AP) on tower
- ✓ 5Ghz Wi-Fi backhaul
- ✘ Secure (WEP!) access for CPE only
- ✘ Subscribers receive wired Ethernet in home
- ✓ Arrangement repeated in hundreds of towns



Modernization Plan

Legacy

When this WISP started Wi-Fi was used only as an economical backhaul method to reach the subscribers who would usually have a traditional desktop PC.

Uniform price for flat rate monthly subscriptions.

Future Mode of Operation

Subscribers demand wireless service as they now have smartphones, tablets and notebooks.

Allow subscribers to use outdoor signal from existing towers and add more coverage areas.

New usage based, per device subscription packages available over the counter in town.

Network wide mobility.

Mikrotik: RADIUS AAA Server

The address of the AAA server (OCS) is given along with a shared secret to authenticate the AP.

```
    [admin@AP] > /radius add address=10.1.1.10 secret="dknpm6w3py28"
```

The AP will listen for incoming RADIUS Disconnect-Request and Change-of-Authorization from OCS.

```
    [admin@AP] > /radius incoming set accept=yes port=3799
```

Mikrotik: Security Profile

Define the authentication, authorization and accounting methods used by the AP.

```
    [admin@AP] > /interface wireless security-profiles add name=ocs
mode=dynamic-keys authentication-types=wpa2-eap radius-eap-accounting=yes
```

We’re also using OCS for the existing CPE subscribers using Mikrotik’s proprietary RADIUS MAC authentication and accounting.

```
    [admin@AP] > /interface wireless security-profiles add name=ocs-cpe
radius-mac-authentication=yes radius-mac-accounting=yes
```

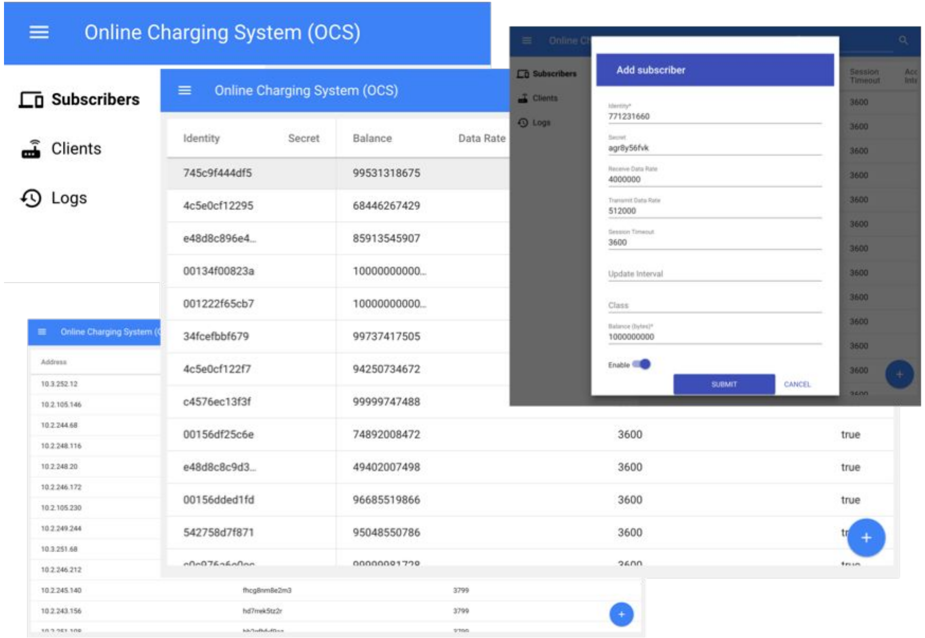
Mikrotik: Virtual Access Point

Virtual access points allows the AP to use multiple security profiles on the same WLAN interface.

```
[admin@AP] > /interface wireless add name=Red-Movil
default-authentication=no security-profile=ocs
```

SigScale OCS

- ✓ **Open Source**
  - ○ Apache 2.0 License
  - ○ Published on GitHub
- ✓ Graphical User Interface (**GUI**)
  - ○ Google Polymer Material Design
  - ○ Simple Guided Management
- ✓ **REST** API
  - ○ TM Forum Frameworx APIs
  - ○ OSS/BSS Integration
- ✓ Internet Protocol Detail Records (**IPDR**)
  - ○ TM Forum Interchange Standard
  - ○ Inter-Carrier Roaming Settlement
- ✓ Embedded **Distributed** Database
  - ○ Mnesia
- ✓ High Performance, **Scalable**, Resilient



Identity	Secret	Balance	Data Rate		
745c9f444df5		99531318675			
4c5e0cf12295		68446267429			
e48d8c896e4...		85913545907			
00134f00823a		10000000000...			
001222f65cb7		10000000000...			
34fcefbbf679		99737417505			
4c5e0cf122f7		94250734672			
c4576ec13f3f		99999747488			
00156df25c6e		74892008472		3600	true
e48d8c8c9d3...		49402007498		3600	true
00156dded1fd		96685519866		3600	true
542758d7f871		95048550786		3600	tr

Address		
10.3.252.12		
10.2.105.146		
10.2.244.68		
10.2.248.116		
10.2.248.20		
10.2.246.172		
10.2.105.230		
10.2.249.244		
10.3.251.68		
10.2.246.212		
10.2.245.140	fhcg8nm8e2m3	3799
10.2.243.156	hd7mek5tz2r	3799

Add subscriber

Identity*
771231660

Secret
agr8y56fvk

Receive Data Rate
4000000

Transmit Data Rate
512000

Session Timeout
3600

Update Interval

Class

Balance (bytes)*
1000000000

Enable ●

SUBMIT CANCEL

Point-of-Sale (PoS)

SigScale developed an embedded application for a mobile Point-of-Sale (**PoS**) terminal. At retail outlets clerks may accept a **cash payment**, key in amount, PoS updates **OCS** using our **REST API** over the air and **prints a receipt**. For a new subscriber an identity and password are printed on the receipt. For existing subscribers the clerk first keys in the identity (e.g. 7 digit number) then amount of the top-up.

- ✓ Keypad
- ✓ Colour LCD
- ✓ Thermal Printer
- ✓ Magnetic Card Reader
- ✓ Smart Card Reader
- ✓ Wi-Fi
- ✓ GPRS
- ✓ NFC

Wi-Fi Roadmap

Hotspot 2.0

Evolution of Wi-Fi

Wi-Fi Alliance - Passpoint^{TM}

Hotspot 2.0 R1 - Network Selection (2012)

Release 1 of the Hotspot 2.0 program introduced the Access Network Query Protocol (**ANQP**) which allows operators to advertise rich information about network capabilities which clients may use to select a network.

Hotspot 2.0 R2 - Online Signup & Policy Provisioning (2016)

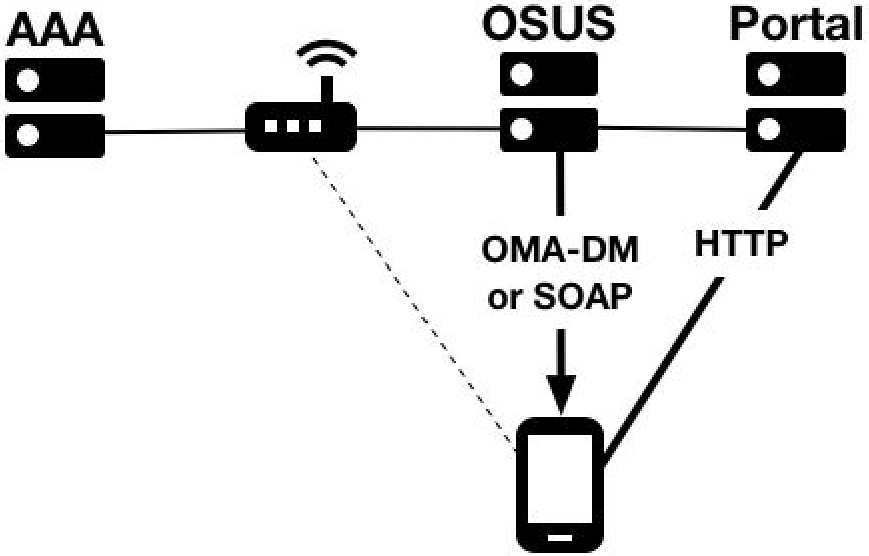
Release 2 of the Hotspot 2.0 program provides a standardized solution for online signup through an Online Signup Encryption Network (**OSEN**) and client credential and configuration provisioning.

Hotspot 2.0 - Online Sign-up and Provisioning

Access point advertises the URL of an Online Sign-Up Server (**OSUS**).

Client device authenticates anonymously, but securely, on the Online Sign-Up Server only Encrypted Network (**OSEN**) hidden SSID.

User browses the HTTP server of the OSUS to select a package to subscribe and configuration is pushed to the device.



SigScale
Level 26, World Trade Center
Echelon Square
Colombo 00100
Sri Lanka

Tel: +94117444186
Fax: +94117444556
info@sigscale.com
http://www.sigscale.com