Technical Disclosure Commons

Defensive Publications Series

September 06, 2017

Self Configuration Of Wireless Devices For Cloud Deployments

Frédéric BRUNNER
ALE International

Jean-Michel LAURIOL
ALE International

Docket Number	**FR82017004**
Title	**"Self Configuration Of Wireless Devices For Cloud Deployments"**
Contributors	**Frédéric BRUNNER, Jean-Michel LAURIOL**
Company	**ALE International**

Description of the technical solution:

In a context of Cloud deployments, we need to find a way for "out of the box" devices with no MMI (Man to Machine Interface) capabilities to easily discover the Cloud Service Provider and Application Server instance they are attached to.
These devices "MMI less" are devices without input (e.g. keyboard) or output (e.g. Display) allowing user to type any characters or read information on the screen, typically wireless DECT (Digital Enhanced Cordless Telecommunications) Base Station or WLAN (Wireless Local Area Networks) Access Points.

This problem is typically relevant in the context of Unified Communication as a Service (UCaaS) Solution offered from the Cloud by Cloud Service Provider.
Basically a Communication solution for corporate environment consists of equipments such as communication servers (e.g. telephony servers) and terminals including softphones (e.g. desktop, mobile) and hardphones (called also deskphone). All these equipments interwork together and need to be configured. In case of mass deployment of devices, the configuration procedure consists of an automatic downloading of a configuration file from a repository server (which can be part of not of the communication servers).

For these devices having a local MMI deployed in a cloud environment, some solutions exist today based on a Vendor Redirection Server with the following methods:

- MAC address based
- activation code based.

The principle of the Vendor Redirection server is to provision first for each device the final Configuration Repository Server address based on device identifier such as the MAC address or an activation code. The Redirection Server address is embedded in each device during the manufacturing process.
Then, when the device boots the first time, it requests to the Redirection Server its Configuration Repository Server. In case of "activation code" method, the user is prompted once to enter the activation code he received before in a secure way from the Cloud Service provider.

The key point to address in the cloud environment, is how the DECT base station learns the Configuration Repository Server address the first time it is started with an empty "out of the box" configuration, using the "activation code based" method but having no MMI to enter an activation code directly in the base station.

Several existing solutions can be considered appropriate in specific contexts, but all face limitations with respect to the key objectives described above:

1) Pre-configuration of terminals by the terminal vendor or by the CSP (Cloud Service Provider):

Consist in a pre-configuration of the device with the CSP address where the device will find its configuration file. This operation is done before the device is shipped to the end user. The end user then has to plug the device that directly connects to the right CSP address, and ask a user for some identification information so the device is authorized on the Application Server.
This pre-configuration can be performed:

- Either by the vendor before devices are shipped to the CSP or CSP end customers, meaning a specific manufacturing/logistics step has to be added by the vendor for devices that will be deployed by any CSP. The vendor has to track each CSP business projections to finely manage inventory of devices for each CSP ;
- Or by the CSP, that has to build a specific procedure for customizing devices, requiring CAPEX (Capital Expenditure) and OPEX (Operational Expenditure) for people training, logistics aspects, investment in the infrastructure enabling this specific step.

In summary, this solution requires costly operations before the terminals can be delivered to the end customer, and highly impacts the operation and logistics costs for the service provider or vendor.

2) Vendor Central Server Tracking every deployed device:

Most of the vendors implement a central server accessible on the internet and delivers the configuration for all the vendor's terminals deployed by various customers. This however implies high operational costs for the vendors to maintain the database of all deployed/sold terminals (typically by tracking MAC addresses of shipped terminals), to keep customers' related parameters up to date. It also has the drawback that the vendor remains involved in the terminals network flows and the customer is never totally independent of the vendor's service.

3) Relying on DHCP (Dynamic Host Configuration Protocol):

Using DHCP to provide the Configuration Repository server URL (Uniform Resource Locator) is a possibility, that requires configuring the DHCP server of the network where the end user will install his device, so it delivers a specific DHCP option containing the server location.
This solution however requires that the user or the CSP controls the DHCP server of the network the device will be deployed on. This is consequently not relevant for a lot of cases, typically:

- Not applicable when the user connect from a network where the DHCP server is not manageable by the end-user and neither by the CSP (unless the CSP is also the Network Access Provider, which cannot be taken as general assumption). A typical example is deployment on the home network of a user.
- Not applicable if several devices of different CSP, or different AS (Application Server) of the same CSP, are deployed on the same network and therefore served by the same DHCP server.

4) Configuring the terminal using Web Based Management:

The terminals embedding a Web server can be accessed by a Web browser. The activation code can be entered in the base station by this way. In order to be able to connect to the base station, its IP address should be known. This is the difficulty as the terminal doesn't have any mean to display its IP address. A solution exists to get the IP address using a DECT handset and after used it with the Web browser, enter the Web based management credential (i.e. login and password) and select the correct menu to enter the activation code.

Compared to existing vendor cloud manager solution the advantages of the new solution are the following:

- Simplification of vendor operation: No specific supply chain operations, devices shipped to CSP are generic "out of the box" devices. Other solution need to handle CSP devices specifically, for example by tracing each device with an unique identifier (e.g MAC address) to route the device configuration request toward the appropriate vendor/CSP configuration repositories.

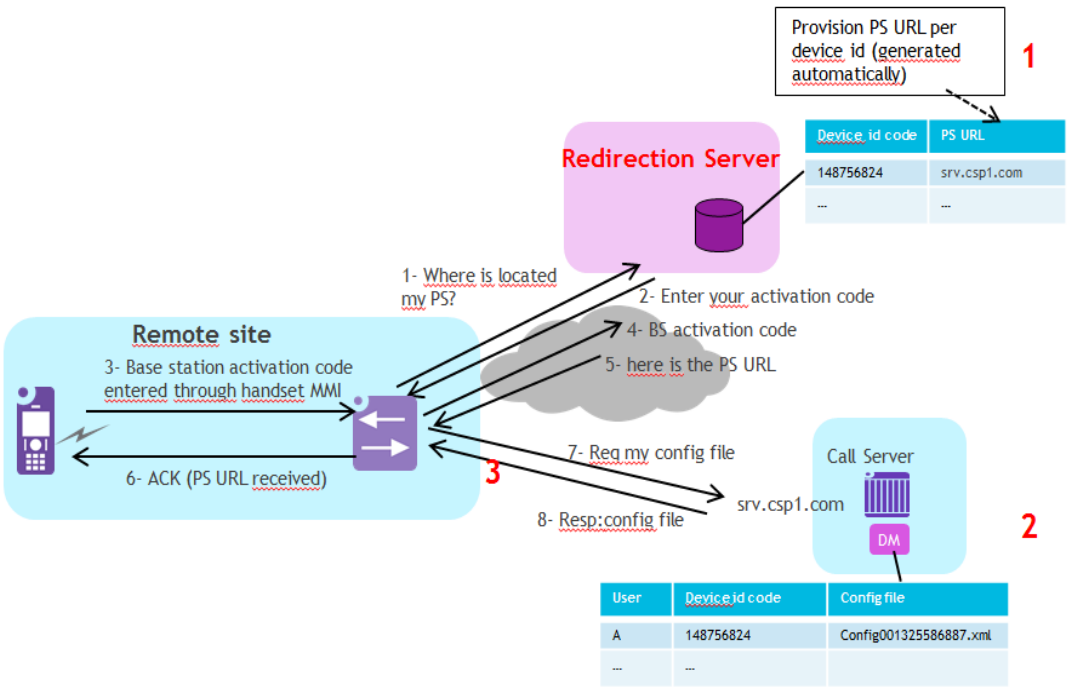
- Automation of the Cloud Service Provider infrastructure: At the end of the user subscription, the CSP can automate the generation of end user ID and the association end user ID with the configuration repository. Other solution requires to associate the device ID (e.g MAC address) to a configuration repository, action that is manual.
  For one device the saving can be up to five minutes (i.e. time for the CSP admin to create the device in the vendor database and associate it with the right configuration repository).

- Easiness of the end user's deployment: Other solutions may request the end user to enter the configuration repository address manually which is difficult when the device only have numeric pad. The benefit here is that there is only a numeric activation code to be entered by the end user from an handset.

The added value brought in that new invention is the capability to enter an activation code through an external wireless handset without being registered with the Base Station or Access Point (secure registration of a handset on a base requires an action of both sides, pressing a button on the base for example, but physical access to the base could not be easy to perform when the base is already mounted).

A. Architecture:

The main architecture is depicted below.

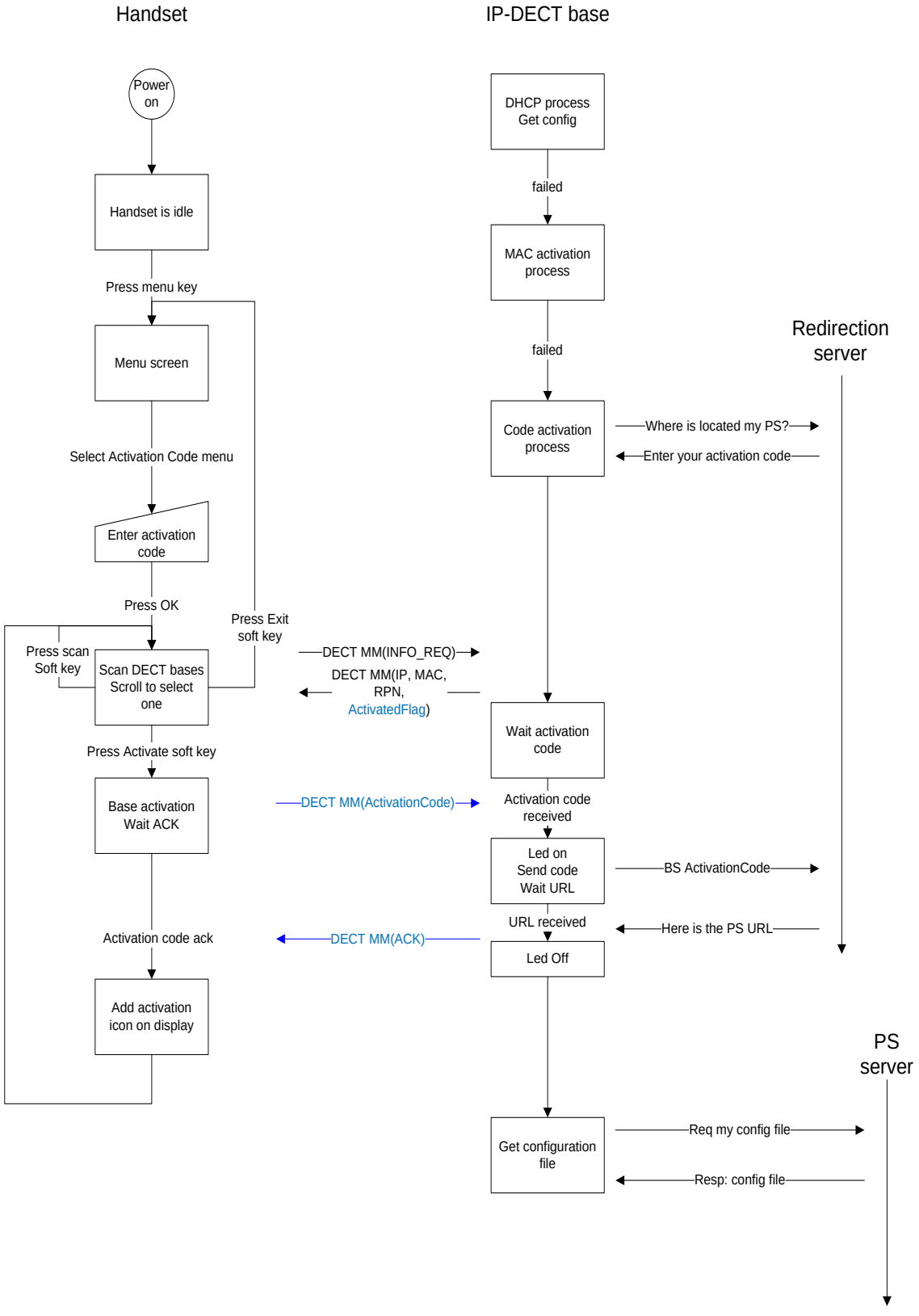


B. Principle:

The principle is the following:

- Same method as wired phones (activation code or MAC @ based) using Redirection Server allowing to retrieve the PS (Provisioning Server) address.
- Using DECT handset as interface to provision a "base station" activation code in an IP-DECT base station.
- Need proprietary DECT MM (Mobility Management) message to allow DECT handset connection to the base (and not to the call server) without any authentication nor subscription process. The DECT handset is able to send this proprietary message, which is by definition not a standard DECT handset, but a proprietary handset with a specific MMI to enter the activation code with the handset keyboard and then sends it to the base station this activation code using this proprietary MM message. The term of proprietary MM message means a standard DECT MM message in which specific vendor information has been added staying DECT compatible message. When receiving this proprietary message the base escapes the standard authentication procedure asking the handset to authenticate. There is no security risk to use this non-registered handset to make a call for example. Any tentative to make a standard connection will be checked by the base and will request the handset to authenticate. The proprietary connection without registration/authentication allows only to enter the activation code in the base. A bad activation code will not allow to configure the base station as it is checked by the redirection server, the base station will not useable as it has not received its configuration file.
- Need IP- DECT radio part being activated early during the initialization phase (using European DECT frequency band).
- The base station will directly connect to the redirection server to get its provisioning server address first and then request the configuration file from the DM (Device Management).
- The activation code could be the same for all IP-Base Station in a deployment and is entered by the end user.
- DECT handset offering the activation code menu is available in all DECT handsets to be deployed for end user (no need to be a dedicated configuration DECT handset for an installer).

C. Algorithm and workflows in handset and base station:



This above diagram on the left part shows the DECT algorithm in which the activation code is the same for all the DECT Base stations of the installation. For different activation codes, this algorithm has to be modified .

D. Solving the allowed DECT radio frequency band before getting the configuration file:

The radio part of the DECT base station must be activated during the activation code process with the handset. At this step, the base station has not yet downloaded the configuration file from the PS defining the allowed DECT radio frequency band for the country in which the base station is deployed. Therefore, during this step the DECT radio part should started with a frequency band matching the country area in which the Base station is located. Problem to solve is how the base station can find its geolocation?

Several solutions are possible:

- Having several commercial references for the different frequency bands
- Exchanging country info between handset and base station over wireless link
- Geolocation based on public IP address of the router

➢ 1) Having several commercial references for the different frequency bands:

There are several possible frequency bands. Given the market where the base station is sold it is preconfigured with the correct frequency band in manufacturing. This means that there is one base station commercial reference for each possible frequency band.

➢ 2) Exchanging country info between handset and base station over wireless link:

The radio frequency band to use is entered by the end user in a specific DECT handset menu and after that the handset will act as a base station. The handset broadcasts permanently, over the allowed frequency band, a proprietary message giving the frequency band to use.
The base station not knowing the frequency band to use, starts the DECT part in receiving mode and scans the radio environment. The base station acknowledges the reception of the frequency band to the DECT handset. This one will stop to act as a base station and behaves now as a classical handset. The base station can start its radio to transmit at the correct frequency. The activation code can then be entered in the handset as described earlier.

➢ 3) Geolocation based on public IP address of the WAN router:

The IP address of the WAN (Wide Area Network) router is found thanks to the IETF standards STUN/TURN or a cooperation with the Redirection Server.

- With STUN (Simple Traversal of UDP through NAT) / TURN (Traversal Using Relays around NAT): The DECT base station embeds a STUN/TURN client with the pre-defined address of the STUN/TURN server (address flashed during manufacturing like the Redirection Server one).
- With the Redirection server: Redirection server is able to find the public IP address of the WAN router by extracting the IP source address of the message sent from this router and initiated by the DECT base station. Then, the server can return this IP address to the DECT base station through a dedicated message. Once the DECT base station retrieves the public IP address, it performs an IP-based geolocation mechanism. IP-based geolocation is a mapping of an IP address to the real world geographical location of devices connected to Internet, including country, region, latitude/longitude, ISP (Internet Service Provider). Commercial and

freely available geolocation databases exist and can be reached through API (e.g. ARIN Whois). When the DECT base station gets the country information from this geolocation database, it determines the right DECT radio frequency band based on an embedded mapping table. This method applies mostly for remote office with a local WAN router/proxy located in the same country as the deployed DECT base station.