



Contents

1. **Is DECLoop secure?**
2. **Voice and Data?**
3. **How does Authentication as a security measure apply to DECLoop?**
4. **Can someone impersonate a subscriber module?**
5. **How does Encryption work?**
6. **What about the security on the operator side?**

ACCESS BYTES

The abuse of communication services goes back centuries. In the days before postage stamps were invented, postage was paid by the recipient. Unsolicited mail became a huge problem (especially for famous people), so recipients were allowed to inspect a letter and reject it if they wished rather than paying for it.

In the 1950's, the operator in some systems had to listen for the sound of coins dropping on a metal plate to tell that a callbox customer had paid, so some people acquired the knack of hitting the coin-box with a piece of metal that struck the right note.

The attacks have continued ever since. At each stage, the defensive measures undertaken were not only very expensive but also tended to be inadequate for various reasons. But with time the security measures have been enhanced to be future proof and counter any possible attack.

This issue of @ccessbytes looks at the various **security measures deployed in the DECLoop architecture.**



Security in DECLoop

Question 1: Is DECLoop secure?

Yes. DECLoop is secure. DECLoop provides security at 3 levels to protect the not only the subscriber but the operator also. For security, DECLoop mainly uses the encryption algorithm as specified in the DECT standards. Provision is made for authentication, which allows curbing unauthorized use of the subscriber unit.

Security in the form of limited access to EMS and OMC consoles and traffic routing to EMS makes it secure on the operator side.

Question 2: Does it work for both voice and data sent over the network?

As such, DECLoop would not differentiate between voice and data as far as security over the air interface is concerned. The Security measure as far as Encryption is concerned, is applied to the user data that is transmitted over the air.

The DECLoop system provides complete security for the on-air transmission of data. This is being done through the following mechanisms:

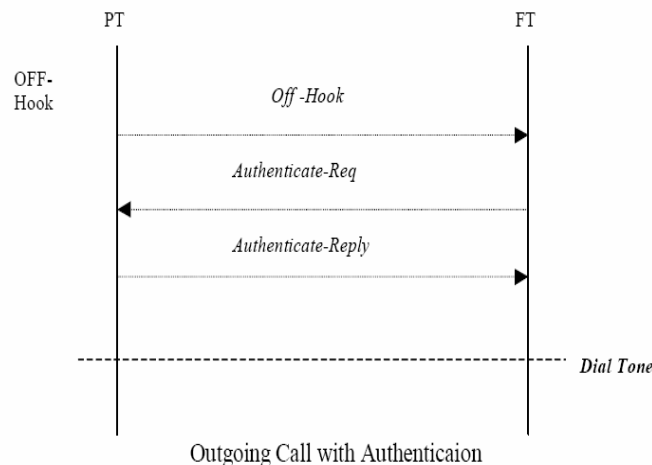
1. Authentication
2. Encryption
3. Anti-Cloning

Question 3: How does Authentication as a security measure apply in DECLoop?

DECLoop system employs authentication procedure in each outgoing and incoming call. The authentication keys are available at both CPE (SSU) and Switch (DIU). The authentication keys are obtained as part of the subscription process. These keys are not transmitted on air. DSAA (DECT Standard Authentication Algorithm) is used as authentication algorithm [ETSI ETS 300 175-7 96].

The authentication procedure ensures that the calls are originated or terminated from/to the correct portable. With this procedure the Switch (DIU) challenges the CPE (SSU) with a random number and the portable is supposed to give a response to the DIU based on the key and the random number using DSAA algorithm. The DIU calculates the result and cross-checks the result with that obtained from portable.

Whenever the authentication fails, the system automatically initiates Identity procedure to identify the misbehaved portable. The system does not allow the call to progress (dial tone is not fed in case of outgoing call and ring is not placed in case of incoming call) when the authentication fails, and such a failure is logged in log/mmerr.log file.





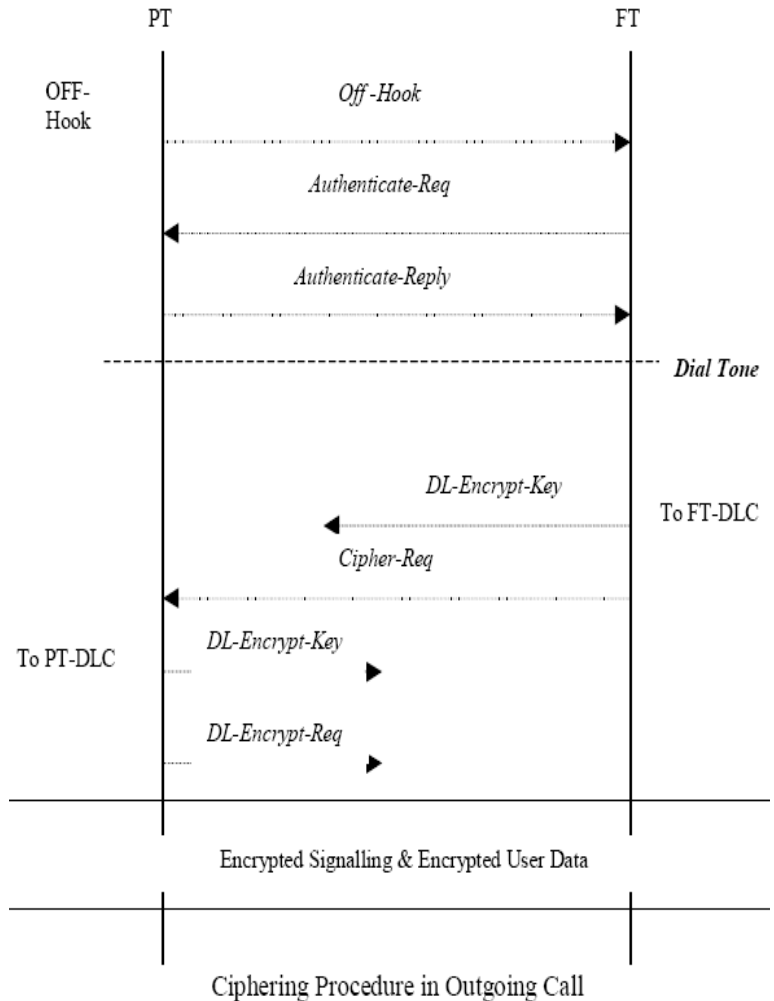
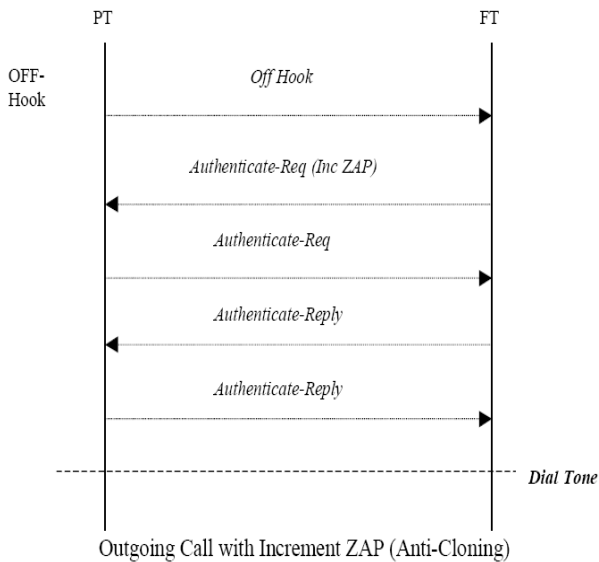
DECLoop News

Question 4: Can someone impersonate a subscriber module?

The system also provides an anti-cloning mechanism, by which impersonation of a portable is impossible. For this the system and the portable increment a counter (ZAP value) during each call. The value of this counter is checked in the authentication process, by FT. The CPE authenticates the DIU during this process. If the ZAP value does not match, the DIU does not allow the call to proceed and the system logs this information in log/mmerrr.log.

Question 5: How does Encryption work?

Apart from checking the authenticity of the portable, the DECLoop system also provides security for the user data (voice/data) that is transmitted on air. The system uses the encryption (ciphering) process for this security. Although static and dynamic authentication keys can be used for ciphering, we use dynamically generated keys, i.e., the cipher keys are dynamically generated for each call. The cipher procedure is a co-ordinated process between DIU and CPE [ETSI ETS 300 175-7 96]. The authentication and ciphering procedures are defined in DECT.





Question 6: How about the security on the Operator side?

The Operators owns and controls the Switch and softwares that control the Switches and the whole network i.e. the OMC and EMS.

EMS Security - All traffic between the GUI's and the agents on the DIU's is routed via a single corView manager that normally resides on one of the EMS workstations. This serves to improve the security and efficiency as each need only accept requests from one manager. In addition to this the access to the EMS can be controlled using User IDs and password for selected personnel.

On top of that the manager with a certain User ID and password for access cannot create or delete profiles. Only and Administrator with an "administrator User ID and password" can do that.

OMC Security - Security Password (up to 7 characters) for 10 different users in 3 different modes can be allotted.

OMC and EMS access is also controlled using Hardware locks and License files synchronized with those locks. Even if the locks are removed mid-way during use, the OMC / EMS will stop working.



We would appreciate any feedback / queries that you may have concerning this newsletter and it's contents. You may fill up a hard copy of the form below or click on ["ONLINE FEEDBACK FORM"](#). This will take you to an online feedback form which you can simply fill up and click submit to forward it to us.

Newsletter Feedback

▶ To get help us to improve on our newsletter and products, please fill the feedback form below.

Feedback Form

1. Your details:

Company name

Business nature OEM CM Stockist/Trader
 ODM Design House Others (please specify)

Country *

Salutation

Name *

Email address *

Contact number

Fax number

Address



2. Feedback details:

The information in the Newsletter should be :-

- More Technical
- Less Technical
- The current level is fine

Do you find the content informative ?

- Yes
- No

Which of the following elements of the newsletter do you think could be improved ?

- Content
- Layout
- Frequency of newsletter
- Others (please specify)

List the topics you would like to see contents in future issues of the newsletter:-

If you like to forward us your inputs on any aspects of the newsletter not covered above, please use the space provided below :-

Please contact me regarding the following matters

- | | | |
|---|--|---------------------------------|
| <input type="checkbox"/> DECLoop | <input type="checkbox"/> DECLoop 5000 | <input type="checkbox"/> IP-Max |
| <input type="checkbox"/> Network Planning | <input type="checkbox"/> Internet Access | <input type="checkbox"/> PBX |
| <input type="checkbox"/> Energy Meter | <input type="checkbox"/> Broadband | |

* Compulsory

Thank you for your time and valuable feedback.