9.0 **Security code information**

Each base and handset unit of the cordless telephone has a unique 17 bits ID code (FPN) to protect against unintentional access. The FPN ID code is generated randomly in manufacturing.

For electronic filing, security code information is saved with filename: security code information.pdf.

5.4 Power amplifier activation

5.4.1 External connection

The FP has one connection active at all times to make synchronization of the PP possible. In case a speech connection is active one slot will be active in down-link direction and one slot will be active from in up-link direction. The power amplifier will be active from start of sync field to the end of XZ field, which is slightly less than 1/12 of the total frame. In case dual slot diversity is active, two slots will be active equal to 2/12 of a frame.

5.4.2 Internal connection

Two handsets are able to make an internal connection. In this case two bearers will be active in the down-link direction from FP, and one bearer will be active from each handset. The two bearers in down-link direction are not correlated and uses different HoppingIndeOffset. Dual slot diversity is activated independently towards each handset, i.e. up to four bearers may be activated in down-link direction, and two bearer may be active in up-link direction.

5.5 Security

TW338/339 series security system is based on DECT ETSI standard ETS-300-175-6—Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 6: Identities and addressing. The core of radio security is a 40 bits MAC layer identity codes (RFPI), which will be described on following paragraphs. The 17bits Fix Part Number(FPN) of RPFI is generated randomly in manufacturing and stored in EEPROM.

5.5.1 General Description of FP and PP identities

Every radio FP broadcasts for its purpose a unique identity which contains a globally unique (to a service provider) Access Rights Identity (ARI). Every PP has both a Portable Access Rights Key (PARK) and an International Portable User Identity (IPUI). These operate as a pair. A PP is allowed to access any radio FP which broadcasts an ARI that can be identified by any of the portable access rights keys of that PP.

The IPUI is used to identify the portable in the domain defined by its related ARI. The IPUI can either be locally unique or globally unique.

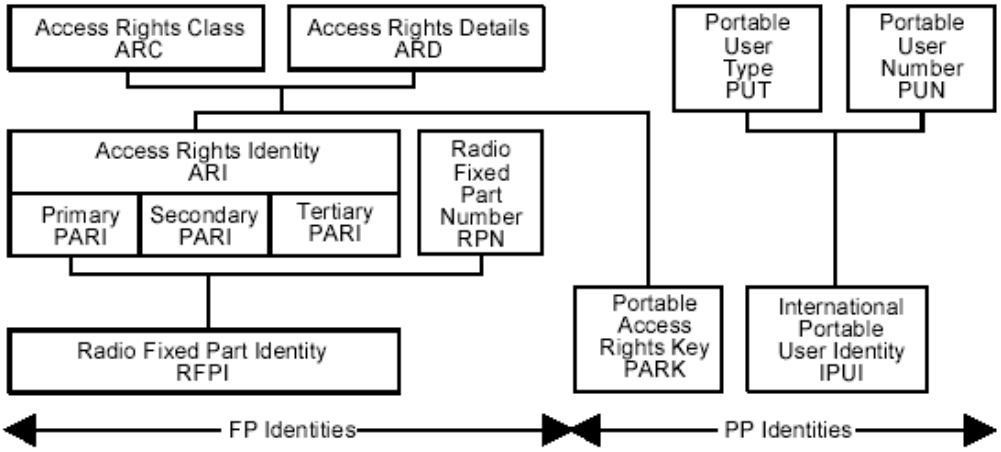

Figure 1 General identity structure

The common base for the DECT identity structure is the Access Rights Class (ARC) and Access Rights Details (ARD). These need to be known by both the FP and the PPs. In the FP the ARC and ARD are called Access Rights Identity (ARI), and in the PP they are called Portable Access Rights Key (PARK). The distinction between PARK and ARI is that each PARK can have a group of ARDs allocated, PARK{y}. "y" is the value of the PARK length indicator given in the PP subscription process.

Figure 2 Structure of PARK{y}

If the ARI is a primary ARI, i.e. PARI, it will form, together with a RFP number, the broadcast identity RFPI. ARIs can also be less frequently broadcast as Secondary Access Rights Identities (SARIs) and may also be available as Tertiary Access Rights Identities (TARIs), which are not broadcast, but are accessible upon request.

The PUT and PUN form the PP user's identity, IPUI. This identity can either be globally unique or locally unique. In addition to IPUIs, shorter temporary identities, TPUIs, may be used for paging.

A PP is identified by its pairs of PARK{y} and IPUI. A PP is only allowed to access a FP if one of its PARKs includes one of the ARIs of the FP, i.e. the PARI, a SARI or a TARI.

5.5.2 FP identities

FP identities are used to inform PPs about the identity of a DECT FP and the access rights to that DECT FP and thereby reduce the number of access attempts from unauthorized portables.

A DECT FP broadcasts this information on the NT-channel via all its radio FPs, at least once per multiframe. A PP needs to be able to interpret necessary parts of this broadcast information to detect the access rights to a system or even access rights agreements between

system operators, i.e. operators A and B have a bilateral agreement permitting their users to roam between their systems. These agreements can change and cannot therefore be stored in PPs without updating them frequently. Therefore the FP handles access rights information which is embedded in the identity structure.

The base for the identity structure is formed by the ARCs and the ARDs.

ARC: shows the type of access to a DECT network, such as public, private or residential.
ARD: this number is unique to the service provider. Its structure depends on the ARC. The ARC and ARD together form the basic identity, the ARI:
ARI: this identity is globally unique to a service provider, and shows the access rights related to this service provider. This identity may be applied to any number of FP installations. There are three categories of ARIs.
PARI: primary ARI has to be broadcast. This is also the most frequently broadcast ARI in order to give a higher grade of service to users with these access rights. The PARI is broadcast over the NT-channel. The PARI (in conjunction with RPN) also carries information about domains of handover and location areas.
SARI: secondary ARI. SARIs are less frequently broadcast than PARIs. They are sent as a SARI-list on the QT-channel.
TARI: tertiary ARI. The TARI is not broadcast at all and is only available as a (or in a) "TARI reply" message, which is an answer to a "TARI request" message including the relevant PARK{y}.

The classification of primary, secondary and tertiary access rights gives the possibility for operators or system owners to offer their subscribers/users an almost unlimited list of roaming agreements. This classification can be seen as an iceberg with the PARI visible on the top followed by a less visible SARI list and in the depth the invisible TARIs.

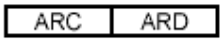

Figure 3 Structure of ARI

ARC: 8 available classes named A - H. Only classes A - E are currently defined.
ARD: details, depends on the ARC.
One ARI together with a radio FP number, forms the RFPI. The ARI embedded in the RFPI is the PARI.

The RFPI is frequently transmitted as bits a8 to a47 in the A-field using the NT-channel and has therefore a limitation of 40 bits.

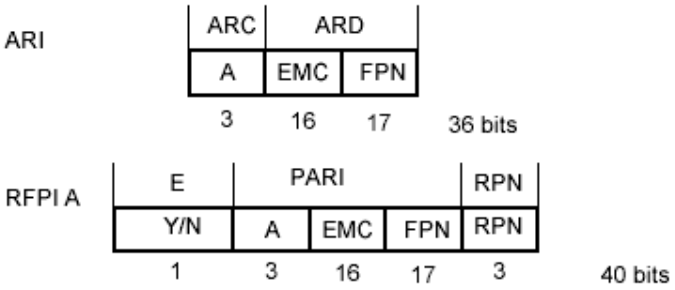

Figure 4 ARI and RFPI

E: this field indicates if there are any SARIs available. Value yes or no.
A: Access rights class A
EMC: Equipment Manufacturer's Code, set to 0 at manufacturing

FPN: Fixed Part Number, random generated at manufacturing. It has an upper limit of 131071, which gives a total of over 8.5 billion unique ARIs.
RPN: Radio fixed Part Number, this number is allocated by the manufacturer/installer and is used to separate a maximum of 7 different cells from each other. In case of single cell FPs, RPN = 0. This indicates for a PP that this FP does not have intercell handover, since there is only one RFP.

5.5.3 PP identities

PP identities have two main purposes, first to enable a PP to select a valid DECT FP and second to uniquely identify the PP within that DECT FP. For these purposes there are two identities defined.

These identities are the PARK, and the IPUI. A PP shall have at least one PARK{y} and an IPUI.

PARK: the PARK{y} defines the access rights for a PP. "y" is the value of its PLI. The structure of the PARK is same as an ARI.

PLI: associates a group of FP ARIs to the PARK, by indicating how many bits out of the ARC + ARD bits are relevant. The rest of the bits have "don't care" status. The PLI is programmed into a PP as part of the subscription process.

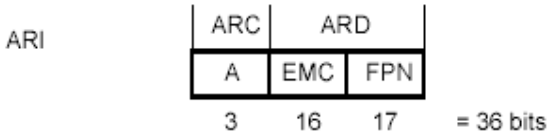

Figure 5 PARK structure