ERRATA

Section 3.3.8 contained incorrect statements concerning vertical- and horizontal key derivation. The errors have been corrected and a revised version of the section is provided. The new text should also clarify the concept of key chaining in general.

3.3.8 The AS Security Context and Key Derivation

The AS Security Context Root Key K_{eNB}

Before we proceed we need to explain a few things about the AS Security Context and the root key K_{eNB}. To start off with, the K_{eNB} key is always associated with a so-called Next hop Chaining Counter (NCC)[21]. Then there is a "next hop" (NH) intermediate key derived by the ME/MME from K_{ASME} (see Section 3.3.9). The NH and NCC form a pair. The NCC is incremented for each handover. For the first K_{eNB} derived subsequent to an EPS-AKA event there is no previous handover history and so the NCC is set to zero. At this stage there exists no corresponding NH. During handover there is a process of chaining in the derivation procedure. The chaining involves producing a new K_{eNB} key, called $K_{eNB}*$, from the intermediate key (NH) or from the current K_{eNB}. Subsequently the $K_{eNB}*$ becomes the current K_{eNB}. There are two distinctive types of K_{eNB} key derivation events:

- **Handover related key derivation**

  Handover events (intra-eNB, X2-handover or S1-handover) will cause a new K_{eNB} to be generated. This process is a *key chaining* event.

- **IDLE-to-CONNECTED mode transition**

  When a UE goes from a connected state (`ECM-CONNECTED`) to an idle state (`ECM-IDLE`) the eNB will delete all current AS keys, including the NH and the NCC. The ME and the MME will, however, keep the `NAS Security Context`. If the UE later goes back to ECM-CONNECTED state a new `AS Security Context` needs to be created. The associated K_{eNB} will be the "initial" K_{eNB}.

Model for Key Handling during Handover

Key handling during handover is referred to as key chaining in TS 33.401 [78]. Figure 3.14 depicts the key chaining model. The initial state is after the EPS-AKA where one has an entirely fresh `EPS Security Context` and an associated fresh K_{ASME}. A `NAS Security Context` is also derived at this stage.

Later, when an `AS Security Context` is needed the ME and MME/ASME will derive the initial K_{eNB}. This is depicted as the (upper left) starting point in the key chaining model (Figure 3.14). By then there will not be a handover history and the next hop chaining counter NCC is initialized to zero. The initial K_{eNB} key is bounded to the `NAS COUNT` (a NAS Security Context message counter). Having derived the initial K_{eNB} one also increments the NCC and derives a NH parameter. This "initial" $(NH, NCC = 1)$ pair is stored in the MME and ME. Subsequent K_{eNB} keys are derived with the physical cell id (PCI) and $EARFCN-DL$[22] as input parameter. The input key is then either the NH (*vertical key derivation*) or the current K_{eNB} (*horizontal key derivation*). Figure 3.14 illustrates the vertical/horizontal key derivation concept.

[21] It was ill-advised to call the parameter NCC since that abbreviation is already used for the Network Color Code concept, but within TS 33.401 NCC will only refer to the NH chaining counter.

[22] This is the number of the E-UTRAN specific physical downlink RF frequency used.

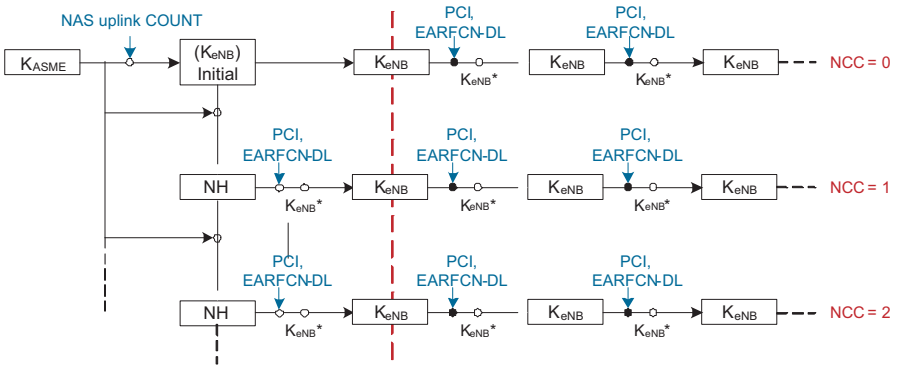

Figure 3.14: Handover Key Chaining

Intra-eNB Handover case

The eNB must compute the $K_{eNB}*$ key, and for this it will need either the NH or the K_{eNB} as the input key. If the eNB has access to an unused NH key (a (NH, NCC) pair really), which it will have gotten from the MME, it will use NH as the basis for deriving $K_{eNB}*$. This is depicted as *vertical key derivation* in the key chaining model (see Figure 3.14). If the eNB lacks an unused (NH, NCC) pair it will simply use the current K_{eNB} to derive the $K_{eNB}*$. This, with reference to Figure 3.14, is a *horizontal key derivation* case. For both cases, the derived $K_{eNB}*$ becomes the new K_{eNB} after the handover.

Inter-eNB Handover (X2-handover)

For this case the connection is transferred from a *source* eNB to a *target* eNB over the X2-interface. If the source has an unused (NH, NCC) pair available it will carry out vertical key derivation, otherwise it must use the current K_{eNB} (horizontal case). Either way, the source eNB computes $K_{eNB}*$ for the target channel and forwards the $(K_{eNB}*, NCC)$ pair to the target eNB (where the $K_{eNB}*$ becomes the K_{eNB}). Subsequent to HO the target eNB sends a `PATH SWITCH MESSAGE` to the MME, which allows the MME to update its copy of NCC and compute a new NH key. The MME then forwards the new (NH, NCC) pair to the target eNB. Note that the source eNB will know the keys used at the target eNB. Only after another HO will the (originating) source eNB loose track of the current AS key set.

Inter-eNB Handover (S1-handover)

This procedure is designed to be used when the UE leaves the current MME service area. For this case the source eNB requests the source MME to execute the handover procedure. The source MME will compute a fresh $\{NH, NCC\}$ pair and forward it to the target MME, together with the current K_{ASME} and $eKSI$. The target MME will forward the $\{NH, NCC\}$ pair to the target eNB, which then derives the new K_{eNB} (with radio channel info etc included). Thus, we only have vertical key derivation for the S1-Handover procedure. Note that while the S1-Handover procedure is primarily intended for inter-MME use, it is nevertheless permitted that the source- and target MME is the same MME.