GSM 系统在安全性方面采取了许多保护手段：接入网路方面采用了对客户鉴权；无线路径上采用对通信信息加密；对移动设备采用设备识别；对客户识别码用临时识别码保护；SMI 卡用 PIN 码保护。

(1) 提供三参数组

客户的鉴权与加密是通过系统提供的客户三参数组来完成的。客户三参数组的产生是在 GSM 系统的 AUC(鉴权中心)中完成，如图 3－38 所示。

①、每个客户在签约(注册登记)时，就被分配一个客户号码(客户电话号码)和客户识别码(IMSI)。IMSI 通过 SIM 写卡机写入客户 SIM 卡中，同时在写卡机中又产生一个与此 IMSI 对应的唯一客户鉴权键 Ki，它被分别存储在客户 SIM 卡和 AUC 中。

②、AUC 产生三参数组：

1> AUC 中的伪随机码发生器，产生一个不可预测的伪随机数（RAND）；

2> RAND 和 Ki 经 AUC 中的 A8 算法(也叫加密算法)产生一个 Kc(密钥)，经 A3 算法(鉴权算法)产生一个符号响应(SRES)；

3> 用于产生 Kc、SRES 的那个 RAND 与 Kc 和 SRES 一起组成该客户的一个三参数组，传送给 HLR，存储在该客户的客户资料库中。

③、一般情况下，AUC 一次产生 5 组三参数，传送给 HLR，HLR 自动存储。HLR 可存储 1～10 组每个用户的三参数，当 MSC / VLR 向 HLR 请求传送三参数组时，HLR 一次性地向 MSC / VLR 传 5 组三参数组。MSC / VLR 一组一组地用，用到剩 2 组时，再向 HLR 请求传送三参数组。

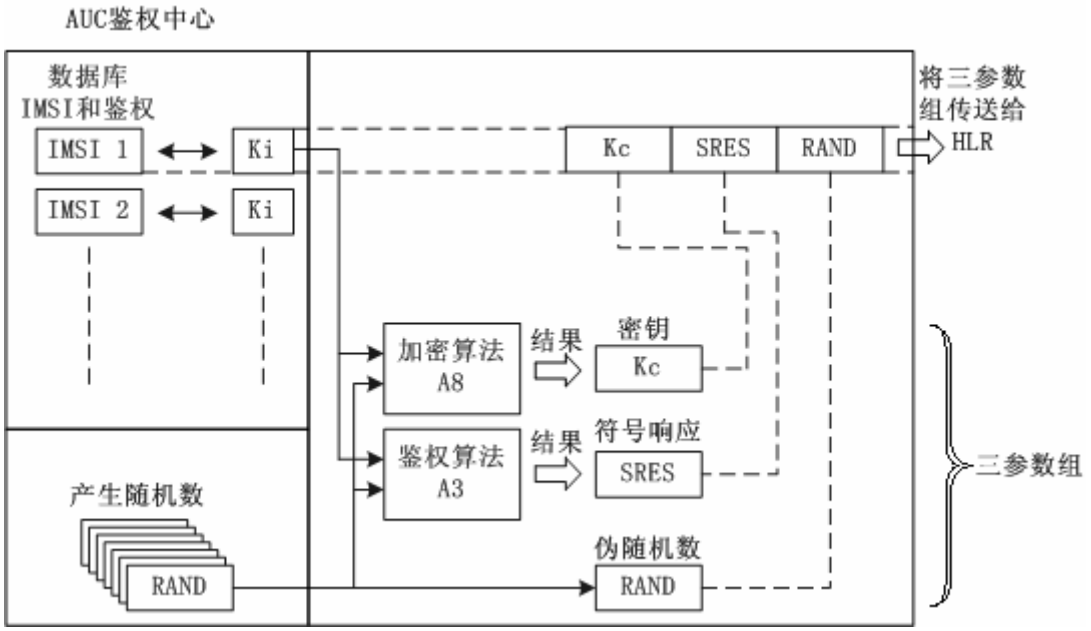

图 3－38　三参数组的提供

(2) 鉴权

鉴权的作用是保护网路，防止非法盗用。同时通过拒绝假冒合法客户的“入侵”而保护 GSM 移动网路的客户，鉴权的程序见图 3－39。

①、当移动客户开机请求接入网路时，MSC / VLR 通过控制信道将三参数组的一个参数伪随机数 RAND 传送给客户，SIM 卡收到 RAND 后，用此 RAND 与 SIM 卡存储的客户鉴权键 Ki，经同样的 A3 算法得出一个符号响应 SRES，并将其传送回 MSC / VLR。

②、MSC / VLR 将收到的 SRES 与三参数组中的 SRES 进行比较。由于是同一 RAND，同样的 Ki 和 A3 算法，因此结果 SRES 应相同。MSC / VLR 比较结果相同就允许该用户接入，否则为非法客户，网路拒绝为此客户服务。

在每次登记、呼叫建立尝试、位置更新以及在补充业务的激活、去活、登记或删除之前均需要鉴权。

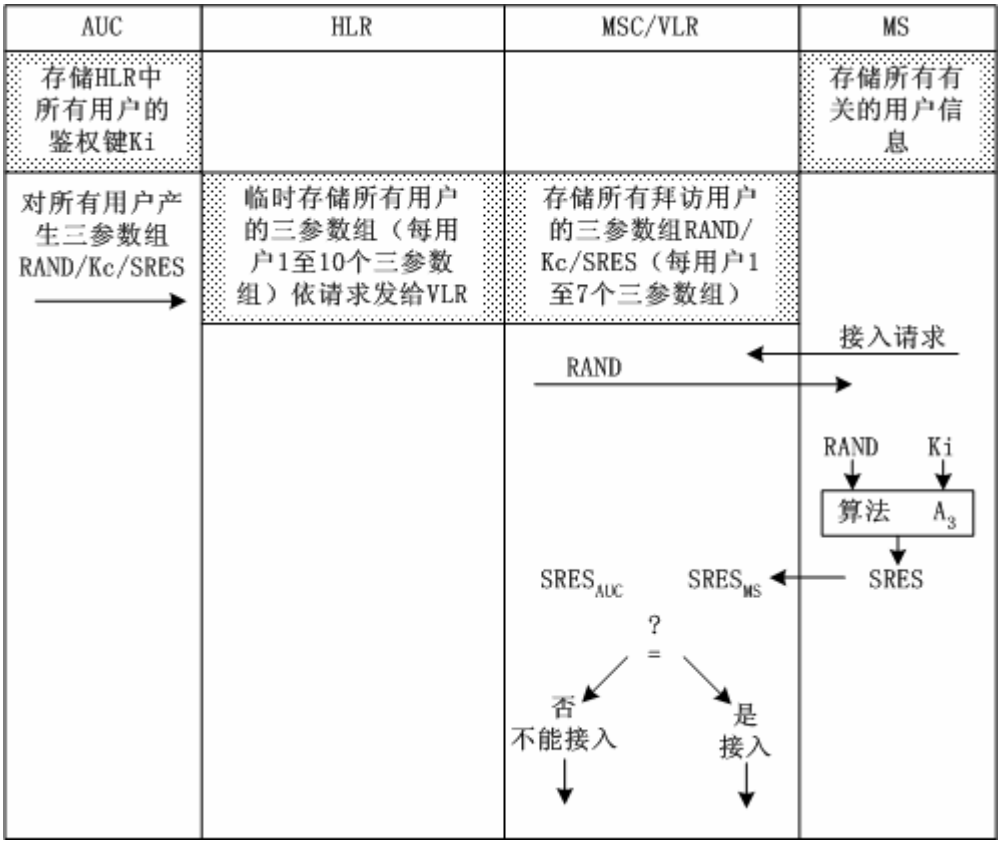

图 3－39　鉴权

鉴权的正常流程和异常情况流程见图 8－40、图 8－41 和图 8－42。

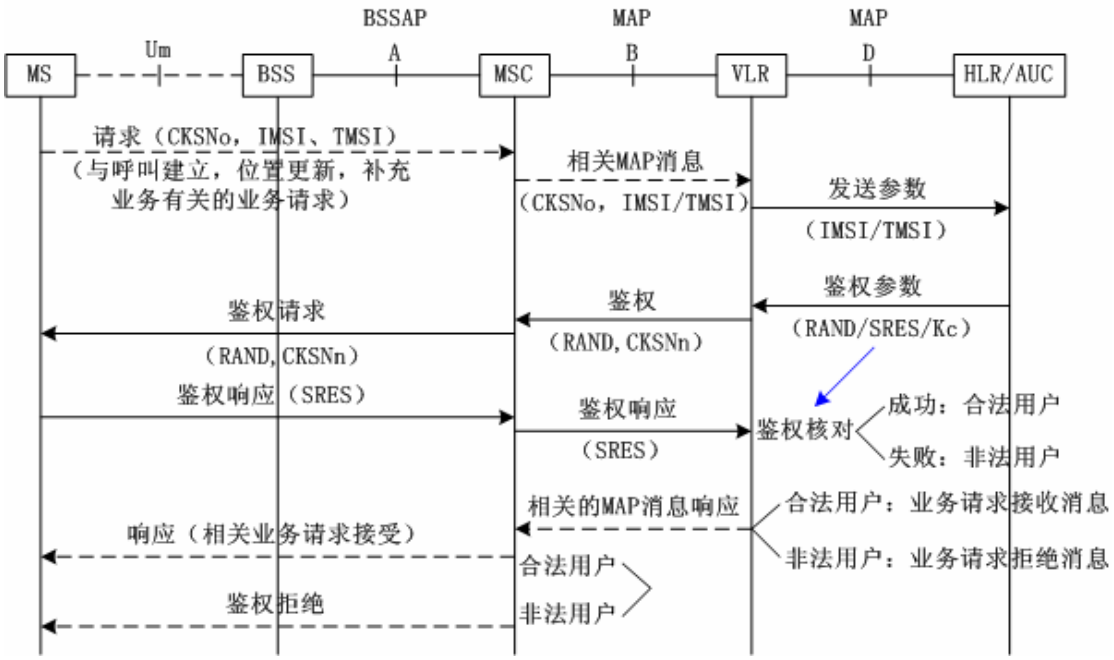

图 8－40　鉴权流程

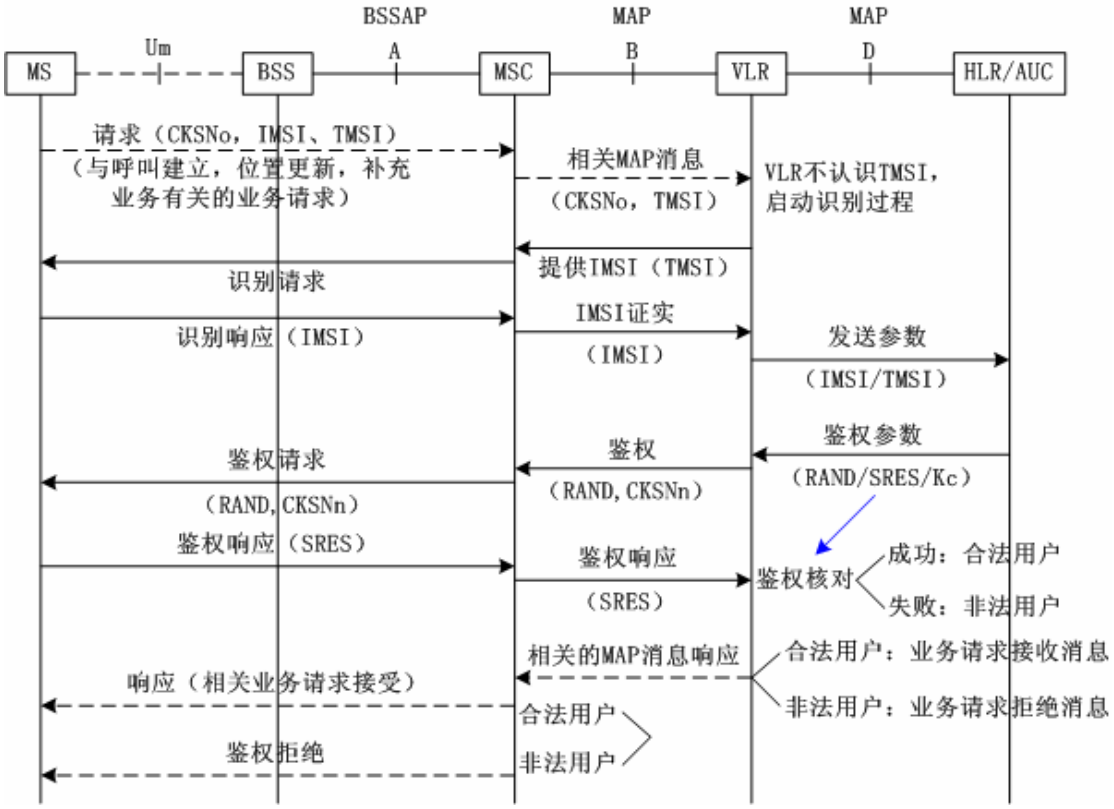

图 8－41　鉴权异常情况（一）VLR 不认识 TMSI

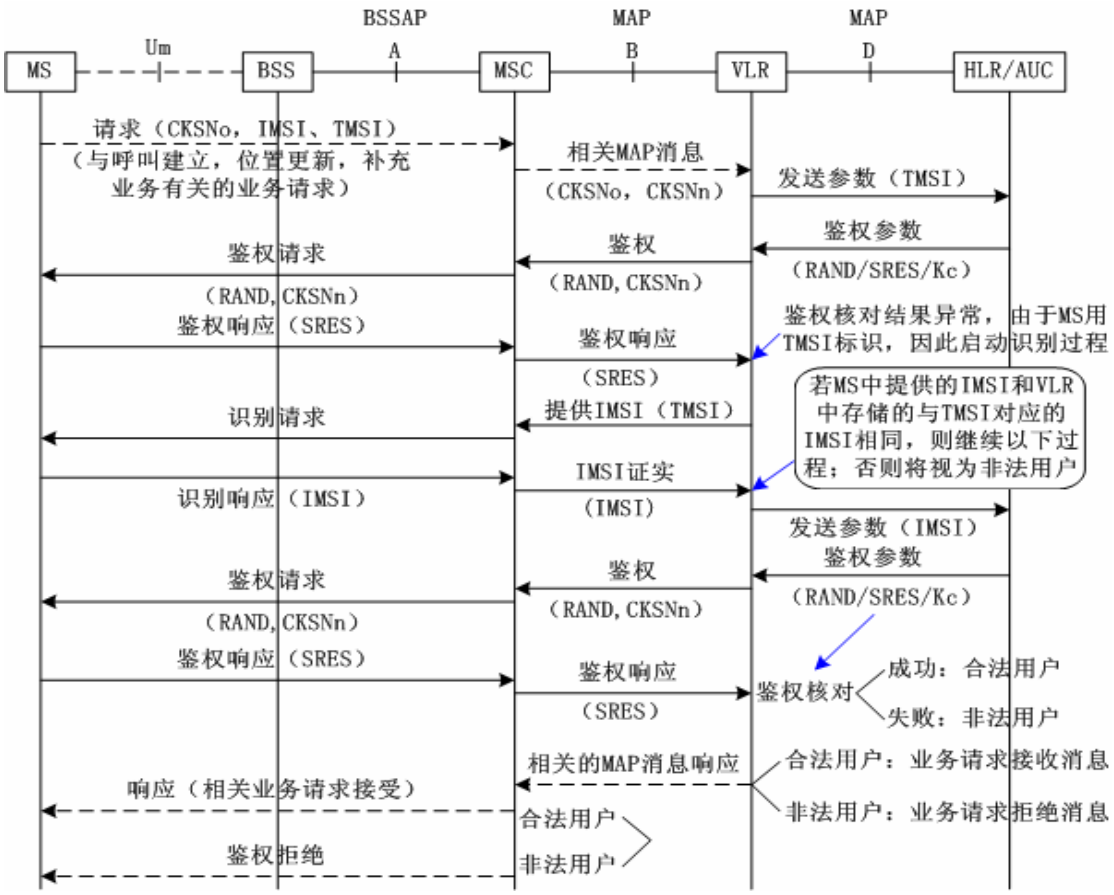

图 8－42　鉴权异常情况（二）MS 用 TMSI 标识时鉴权核对结果异常

(3) 加密

GSM 系统中的加密只是指无线路径上的加密，是指 BTS 和 MS 之间交换客户信息和客户参数时不会被非法个人或团体所盗取或监听，加密程序见图 3－43 所示。

①、在鉴权程序中，当移动台客户侧计算出 SRES 时，同时用另一算法(A8 算法)也计算出了密钥 Kc。

②、根据 MSC / VLR 发送出的加密命令，BTS 侧和 MS 侧均开始使用密钥 Kc。在 MS 侧，由 Kc、TDAM 帧号和加密命令 M 一起经 A5 算法，对客户信息数据流进行加密(也叫扰码)，在无线路径上传送。在 BTS 侧，把从无线信道上收到加密信息数据流、TDMA 帧号和 Kc，再经过 A5 算法解密后，传送给 BSC 和 MSC。

所有的语音和数据均需加密，并且所有有关客户参数也均需加密。

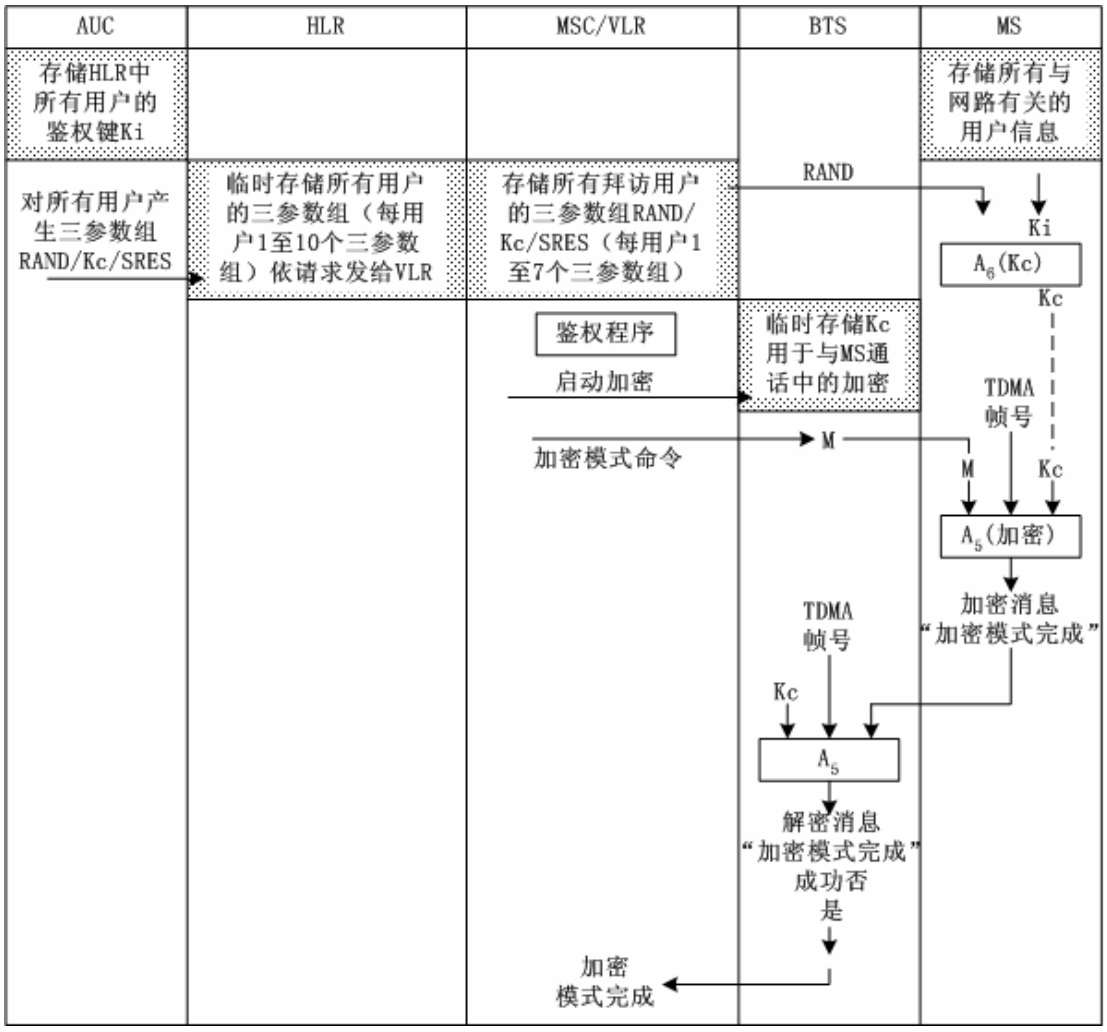

图 3－43　加密

(4) 设备识别

每个移动台设备均有设备识别码(1MEl)，移动台设备如允许进入运营网，必需经过欧洲型号认证中心认可，并分配一个十进制 6 位数字，占用 IMEI 15 位十进制数字的前 6 位设备识别的作用就是确保系统中使用的移动台设备不是盗用的或非法的。设备的识别是在设备识别寄存器 EIR 中完成。

EIR 中存有三种名单：

白名单--- 包括已分配给可参与运营的 GSM 各国的所有设备识别序列号码。

黑名单--- 包括所有应被禁用的设备识别码。

灰名单--- 包括有故障的及未经型号认证的移动台设备，由网路运营者决定。

设备识别的程序见图 3－44，MSC / VLR 向 MS 请求 IMEI，并将其发送给 EIR，EIR 将收到的 IMEI 与白、黑、灰三种表进行比较，把结果发送给 MSC / VLR，以便 MSC / VLR 决定是否允许该移动台设备进入网路。

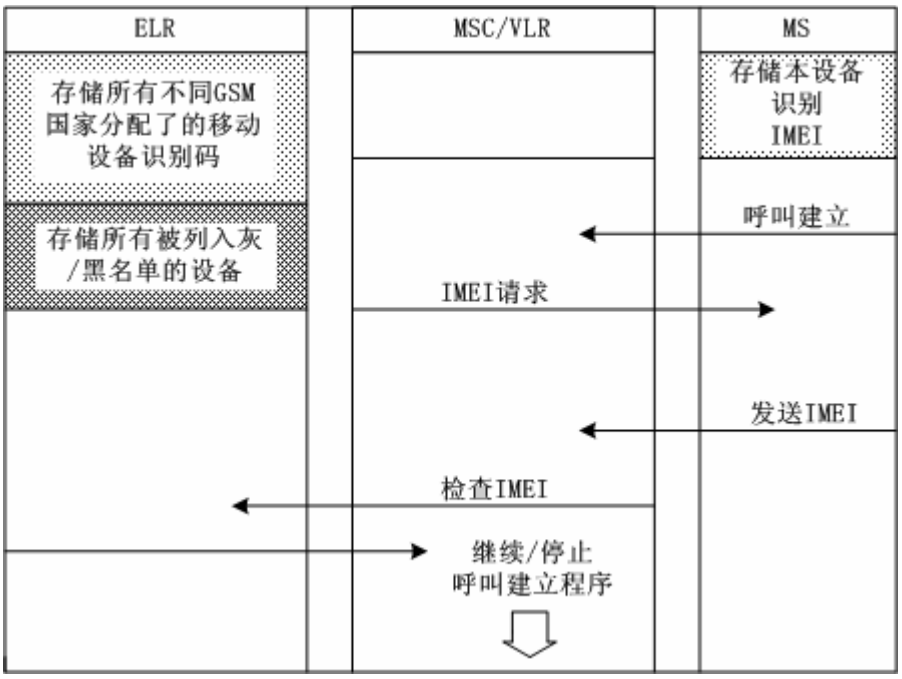

图 3－44　设备识别

何时需要设备识别取决于网路运营者。目前我国大部分省市的 GSM 网路均未配置此设备(EIR)，所以此保护措施也未采用。

(5) 临时识别码(TMSI)

临时识别码的设置是为了防止非法个人或团体通过监听无线路径上的信令交换而窃得移动客户真实的客户识别码(IMSI)或跟踪移动客户的位置。

客户临时识别码(TMSI)是由 MSC / VLR 分配，并不断地进行更换，更换周期由网路运营者设置。更换的频次越快，起到的保密性越好，但对客户的 SIM 卡寿命有影响。

客户识别码保密程序见图 3－45，每当 MS 用 IMSI 向系统请求位置更新、呼叫尝试或业务激活时，MSC / VLR 对它进行鉴权。允许接入网路后，MSC / VLR 产生一个新的 TMSI，通过给 IMSI 分配、位置更新 TMIS 的命令将其传送给移动台，写入客户 SIM 卡。此后，MSC / VLR 和 MS 之间的命令交换就使用 TMIS，客户实际的识别码 IMSI 便不再在无线路径上传送。

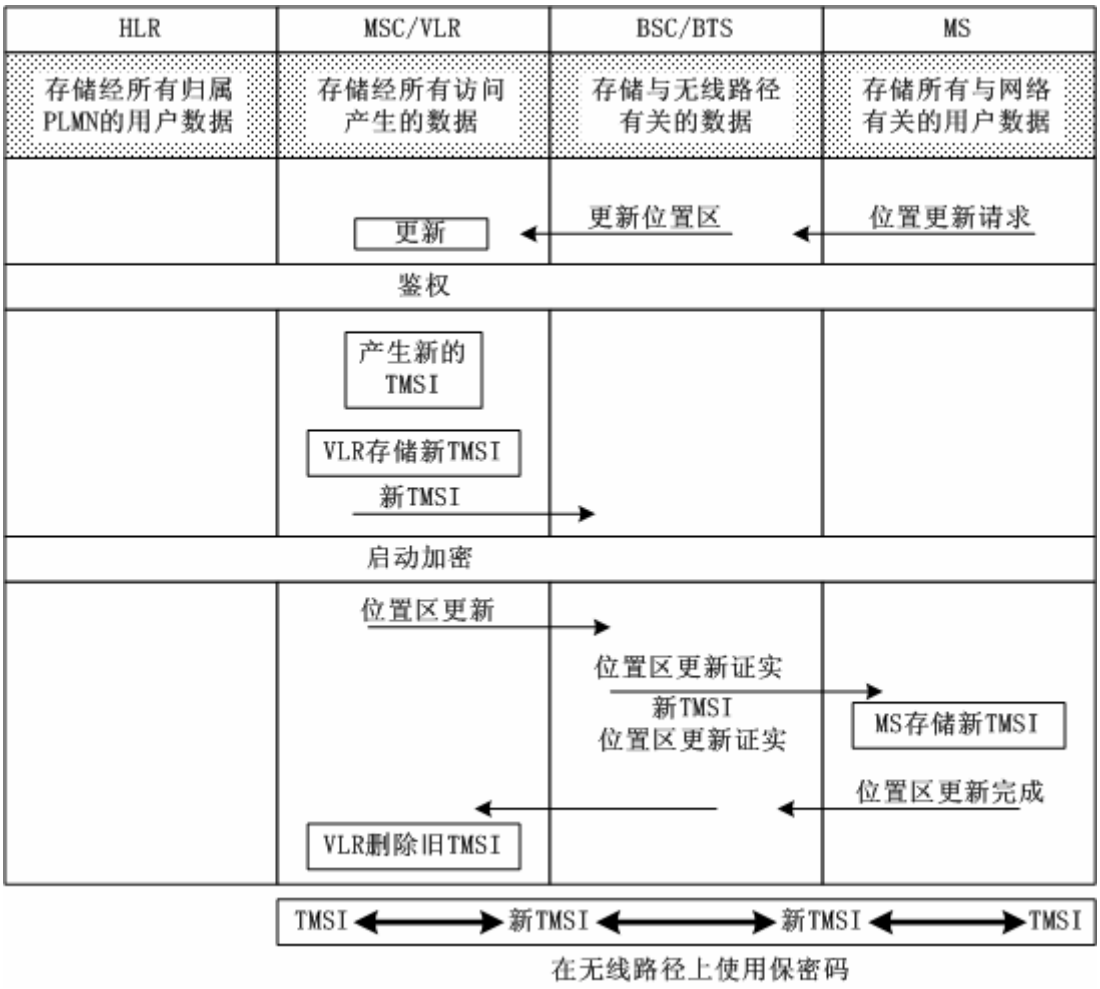

图 3－45　位置更新

(6) PIN 码

在 GSM 系统中，客户签约等信息均被记录在一个客户识别模块(SIM)中，此模块称作客户卡。

客户卡插到某个 GSM 终端设备中，便视作自己的电话机，通话的计费帐单便记录在此客户卡户名下。为防止帐单上产生讹误计费，保证入局呼叫被正确传送，在 SIM 卡上设置了 PIN 码操作(类似计算机上的 Password 功能)。PIN 码是由 4～8 位数字组成，其位数由客户自己决定。如客户输入了一个错误的 PIN 码，它会给客户一个提示，重新输入，若连续 3 次输入错误，SIM 卡就被闭锁，即使将 SIM 卡拔出或关掉手机电源也无济于事。闭锁后，还有个“个人解锁码”，是由 8 位数字组成的，若连续 10 次输入错误，SIM 卡将再一次闭锁，这时只有到 SIM 卡管理中心，由 SIM 卡业务激活器予以解决。