1. 主要包括：① 认证请求 ② 挑战文本 ③ 加密的挑战文本 ④ 接入成功/失败

2. 选①④

A 认证：定义用户与网络的交互，以提供相互认证，并生成用于STA和AP之间无线通信的短期密钥。

B 访问控制：对认证功能的增强，能与多种认证协议协同工作。

C 带消息完整性的机密性：MAC数据与消息完整性校验码一起加密以提供机密性和完整性。

3

(1) 连接到AS：STA向它的AP发送一个请求以连接到AS。AP识别这个请求并给AS发送一个访问请求。

(2) EAP交换：这个交换让STA和AS相互授权。

(3) 密钥分发：一旦认证完成，AS和STA产生一个主会话密钥，此密也称为AAA密钥。STA和AP进行安全通信所需的加密密钥都从MSK产生。

4. 包含：① 用户身份认证 ② 用户身份保密 ③ 用户数据保密以及信令及数据保密。

6. 3GPP的总体安全结构为包含网络接入安全，网络域安全，应用域安全，安全特性的可视性及可配置能力。详细描述如下：

① 网络接入安全

提供安全的接入3G服务网的机制并抵御对无线链路的攻击。

② 网络域安全

保证网内信令的安全传送并抵御对有线网络的攻击。

③ 用户域安全

保证对移动台的安全接入。

④ 应用域安全

使用户域中与服务提供商域的应用程序间可以安全的交换信息。

⑤ 安全特性的可视性及可配置能力

主要指用户能获知安全特性是否在使用以及服务商提供的服务是否需要以安全服务为基础。

6、① 加强了网络接入安全，增加了非3GPP接入，同时增强了AKA协议。

② 面向垂直行业需求，新增了二次认证，增加了安全性。

③ 新增了SBA域的安全，考虑了服务化网元的安全交互

④ 是应用域安全，新增了空口可选的完整性保护手段。