

S.R0032-0 v1.0

**3GPP2 S.R0032**

*Version 1.0*

*Version Date: December 6, 2000*



**3RD GENERATION  
PARTNERSHIP  
PROJECT 2  
"3GPP2"**

# **Enhanced Subscriber Authentication (ESA) and Enhanced Subscriber Privacy (ESP)**

---

***COPYRIGHT***

*3GPP2 and its Organizational Partners claim copyright in this document and individual Organizational Partners may copyright and issue documents or standards publications in individual Organizational Partner's name based on this document. Requests for reproduction of this document should be directed to the 3GPP2 Secretariat at [secretariat@3gpp2.org](mailto:secretariat@3gpp2.org). Requests to reproduce individual Organizational Partner's documents should be directed to that Organizational Partner. See [www.3gpp2.org](http://www.3gpp2.org) for more information.*



# Table of Contents

1	Scope.....	1
2	References .....	1
3	General Description .....	1
4	Enhanced Security .....	1
	4.1 Cryptographic Strength.....	1
	4.2 Export Considerations.....	2
5	Enhanced Subscriber Authentication (ESA) .....	3
	5.1 Root Authentication Keys.....	3
	5.2 Secondary Authentication Keys .....	3
	5.3 Minimum Standard of Service .....	3
	5.4 Enhancements if Security is Compromised .....	4
	5.5 Mobile Station Capabilities.....	4
	5.6 Network Capabilities .....	4
	5.7 Air Interface Capabilities.....	4
	5.8 Backwards and Forward Compatibility .....	4
	5.9 Applicability to Telecommunications Services .....	5
	5.10 Normal Procedures With Successful Outcome .....	5
	5.11 Normal Operation With Successful Outcome.....	5
	5.12 Exception Procedures or Unsuccessful Outcome .....	6
	5.13 Alternative Procedures.....	7
	5.14 Interactions With Other Wireless Services .....	7
6	Enhanced Subscriber Privacy (ESP).....	11
	6.1 Privacy Keys.....	11
	6.2 Minimum Standard of Service .....	11
	6.3 Enhancements if Security is Compromised .....	11
	6.4 Backwards and Forward Compatibility .....	12
	6.5 Air Interface Capabilities.....	12
	6.6 Network Capabilities .....	12
	6.7 Applicability to Telecommunications Services .....	12
	6.8 Normal Procedures With Successful Outcome .....	12
	6.9 Normal Operation With Successful Outcome.....	13
	6.10 Exception Procedures or Unsuccessful Outcome.....	13
	6.11 Alternative Procedures.....	14
	6.12 Interactions With Other Wireless Services .....	14



# 1 Scope

---

This document defines requirements for the cdma2000 Air Interface to support Enhanced Subscriber Authentication (ESA) and Enhanced Subscriber Privacy (ESP). ESA provides enhanced security in authentication and ESP provides enhanced privacy of user data.

Selection of cryptographic algorithms is outside the scope of this feature description.

# 2 References

---

TIA/EIA Interim Standard IS-124, Cellular Radio-Telecommunications Intersystem Non-Signaling Data Communications (DMH); Telecommunications Industry Association; 1993.

# 3 General Description

---

ESA provides mutual-authentication between the MS and the serving BS/network.

ESP provides encryption to prevent user traffic or signaling traffic from unauthorized disclosure.

# 4 Enhanced Security

---

The purpose of this section is to define enhanced security capabilities for wireless networks and mobile stations. The enhanced security capabilities address:

- a. Unauthorized use (i.e., theft) of service, and unauthorized communications to the MS (i.e., unauthorized base stations attempting to control the MS or retrieve any information from the MS)
- b. Unauthorized monitoring of subscriber traffic (i.e., unauthorized eavesdropping)

The security capabilities that address these problems are:

- a. Enhanced Subscriber Authentication – by means of a cryptographically-generated challenge-response, enhanced subscriber authentication (ESA) provides corroboration that a subscriber requesting service and the base station is authorized.
- b. Enhanced Subscriber Privacy – by means of encryption across the air-interface, enhanced subscriber privacy (ESP) protects subscriber traffic (bearer data and signaling) from unauthorized eavesdropping.

From the end user perspective, the enhanced security requirements are independent of the air interface. Thus, the enhanced security capabilities are applicable to all digital air interfaces.

## 4.1 Cryptographic Strength

---

The cryptographic strength of the ESA process is independent of the cryptographic strength of the ESP process. Compromise of the ESP process does not weaken the ESA process.

## **4.2 Export Considerations**

---

ESA and ESP meet the requirements of U.S. export laws and regulations, currently the Export Administration Regulations (title 15 CFR parts 730 through 774 inclusive.).

## 5 Enhanced Subscriber Authentication (ESA)

---

ESA provides methods for determining the authenticity of any request for service made on an air interface. In addition, ESA provides methods for determining the authenticity of the BS. ESA is supported on all wireless channels and in all MS states in which access to services can be requested. On the control channels, ESA provides the ability to authenticate every message transmitted by a MS or the base station, that may compromise the subscriber's security. On dedicated channels, ESA authenticates any message that a MS transmits to request new or different network resources, and any message that a BS transmits that may compromise the ESA security.

ESA uses challenge-response authentication (not a mandate); wherein the challenge is random and the response is generated by correspondingly keyed cryptographic algorithms within the MS and the network. The authentication procedure prevents replay attacks by minimizing the likelihood that authentication signatures are reused.

ESA verifies that the MS contains data representing a valid subscription (IMSI or MIN). ESA also verifies the authenticity of the base station. The authentication process permits subscriber identity authentication independent of the MS identity (ESN or IMEI).

### 5.1 Root Authentication Keys

---

The root authentication key (equivalent of A-key) is known only to the MS and to the home system Authentication Center.

Methods for the installation of root authentication keys include means to prevent compromise of the keys.

The authentication procedures permit the distribution of root authentication keys in removable UIMs. The authentication procedures may permit the operation of a removable UIM in multiple terminals.

The authentication procedures permit proper authentication of the MS only when the UIM is present in the mobile equipment.

### 5.2 Secondary Authentication Keys

---

Secondary authentication keys may be generated in the MS and the home system Authentication Center, and may be transmitted to visited systems for use in authentication.

Compromise of secondary authentication keys does not compromise the root authentication key. The secondary authentication keys can be modified in the MS under the control of the home system.

### 5.3 Minimum Standard of Service

---

ESA provides the maximum possible protection against unauthorized access to wireless services, subject to the message size and similar constraints imposed by the air interfaces. The contribution of ESA to call drops and call attempt failures is negligible.

The ESA algorithm shall be publicly disclosed and commercially available, and shall have been sufficiently studied by the cryptographic community, with strengths and weaknesses thoroughly understood.

## 5.4 Enhancements if Security is Compromised

---

ESA provides a mechanism to enhance the ESA algorithm(s), key generation procedures, or both, in the event the security of ESA is compromised.

## 5.5 Mobile Station Capabilities

---

The MS should reject messages from an authentication-capable base station, which can not be successfully authenticated by the mobile station. (TSG-C may at their own discretion, develop a list of messages that should be rejected )

## 5.6 Network Capabilities

---

The home system can share authentication key data with visited systems to enable the visited system to perform authentication procedures, thereby minimizing network signaling traffic.

Broadcast (global) challenges can be used for pre-call authentication of service requests on control channels.

Individual challenges of an MS can be used on dedicated (bearer and signaling traffic) channels.

Privacy and encryption keys are generated as part of the authentication procedure.

MS authentication of the network (i.e., base station) is used to ensure the authenticity of the base station.

The home system can revoke MS access to service at any time, regardless of the location of the MS.

## 5.7 Air Interface Capabilities

---

All air interfaces providing access to services include a means to verify the authenticity of the subscriber making the request and the base station.

## 5.8 Backwards and Forward Compatibility

---

Air interface and network protocols allow mutual identification of the authentication procedure version or versions supported by the MS and by the network equipment so that a mutually supported authentication procedure can be negotiated. Negotiations of authentication options are under the control of the network based on the capability information provided by the base station. MS access to service may be rejected if an acceptable authentication option can not be negotiated. The MS may reject the services offered by the base station if an acceptable authentication option can not be negotiated.

ESA is a significant modification of the existing authentication methodology and may not be supported by older wireless systems. However, an ESA-capable MS should function in a non-ESA-capable system,

using the authentication algorithm currently specified in the Common Cryptographic Algorithms (CCA), and shall also function in systems in which authentication has not been implemented. An ESA-capable system is expected to support the present authentication methodology, thus preserving the capability to authenticate a current non-ESA-capable MS. Air interface and network protocols should allow for the possible introduction of new authentication algorithms during the expected lifetime of ESA.

## **5.9 Applicability to Telecommunications Services**

---

ESA is applicable to all telecommunications services (e.g., voice, data and signaling).

## **5.10 Normal Procedures With Successful Outcome**

### **Authorization**

---

ESA is provided to all subscribers.

### **De-Authorization**

---

None identified.

### **Registration**

---

ESA has no registration.

### **De-Registration**

---

ESA has no de-registration.

### **Activation**

---

ESA is always active.

### **De-Activation**

---

ESA has no de-activation.

### **Invocation**

---

ESA is invoked upon any MS access for service (e.g., registration, origination, page response).

## **5.11 Normal Operation With Successful Outcome**

---

ESA is invoked upon an MS access for service.

When ESA is invoked, the subscriber identity information (IMSI or MIN) contained in the MS is verified using cryptographic algorithms. If the subscriber identity information is verified, the MS service access is allowed.

If the subscriber identity information is not verified, the MS service access may be refused.

When ESA is invoked, the identity of the BS is verified using cryptographic algorithms. If the identity of the BS is verified, communications to the BS is allowed.

If the identity of the BS is not verified, the MS may refuse to further communicate with the BS.

### **Call Detail Record**

---

None identified.

## **5.12 Exception Procedures or Unsuccessful Outcome**

### **Registration**

---

None identified.

### **De-Registration**

---

None identified.

### **Activation**

---

None identified.

### **De-Activation**

---

None identified.

### **Invocation**

---

None identified.

### **Exceptions While Roaming**

---

None identified.

### **Exceptions During Intersystem Handoff**

---

None identified.

## 5.13 Alternative Procedures

---

None identified.

## 5.14 Interactions With Other Wireless Services

### Asynchronous Data Service (ADS)

---

ESA takes precedence over an MS access for ADS.

### Call Delivery (CD)

---

ESA takes precedence over an MS access for CD (e.g., page response).

### Call Forwarding—Busy (CFB)

---

None identified.

### Call Forwarding—Default (CFD)

---

None identified.

### Call Forwarding—No Answer (CFNA)

---

None identified.

### Call Forwarding—Unconditional (CFU)

---

None identified.

### Call Transfer (CT)

---

ESA takes precedence over an MS access for CT.

### Call Waiting (CW)

---

ESA takes precedence over an MS access to initiate CW.

### Calling Name Presentation (CNAP)

---

None identified.

### Calling Name Restriction (CNAR)

---

None identified.

**Calling Number Identification Presentation (CNIP)**

---

None identified.

**Calling Number Identification Restriction (CNIR)**

---

None identified.

**Conference Calling (CC)**

---

ESA takes precedence over an MS access for CC.

**Data Privacy (DP)**

---

None identified.

**Do Not Disturb (DND)**

---

None identified.

**Emergency Services (9-1-1)**

---

ESA shall not affect the ability for an MS to access emergency services.

**Emergency Services Reconnect (9-1-1 RC)**

---

None identified.

**Enhanced Subscriber Authentication (ESA)**

---

Not applicable.

**Enhanced Subscriber Privacy (ESP)**

---

ESP is only invoked if ESA is performed successfully.

**Flexible Alerting (FA)**

---

ESA takes precedence over an MS access for FA (e.g., page response)

**Group 3 Facsimile (G3 Fax)**

---

ESA takes precedence over an MS access for G3 Fax (e.g., page response).

**Incoming Call Screening (ICS)**

---

None identified.

**Message Waiting Notification (MWN)**

---

None identified.

**Mobile Access Hunting (MAH)**

---

ESA takes precedence over an MS access for MAH (e.g., page response)

**Network Directed System Selection (NDSS)**

---

None identified.

**Non-Public Mode Service (NP)**

---

None identified.

**Over-the-Air Service Provisioning (OTASP)**

---

ESA may have an impact on OTASP.

**Password Call Acceptance (PCA)**

---

None identified.

**Preferred Language (PL)**

---

None identified.

**Priority Access and Channel Assignment (PACA)**

---

ESA takes precedence over an MS access for PACA.

**Remote Feature Control (RFC)**

---

None identified.

**Selective Call Acceptance (SCA)**

---

None identified.

### **Service Negotiation**

---

None identified.

### **Short Message Services (SMS)**

---

ESA takes precedence over an MS access for SMS.

### **Speech Option Selection (SOS)**

---

None identified.

### **Subscriber Confidentiality (SC)**

---

None identified.

### **Subscriber PIN Access (SPINA)**

---

None identified.

### **Subscriber PIN Intercept (SPINI)**

---

None identified.

### **Three-Way Calling (3WC)**

---

ESA takes precedence over an MS access to initiate 3WC.

### **User Group ID (UGID)**

---

None identified.

### **Voice Controlled Services (VCS)**

---

ESA takes precedence over an MS access for VCS.

### **Voice Message Retrieval (VMR)**

---

ESA takes precedence over an MS access for VMR.

### **Voice Privacy (VP)**

---

None identified.

## 6 Enhanced Subscriber Privacy (ESP)

---

ESP provides encryption across the air interface to protect subscriber traffic, both voice and data, as well as certain signaling messages, from unauthorized disclosure.

ESP shall be activated for all subscribers on digital channels.

### 6.1 Privacy Keys

---

Keys for ESP may be based on the root authentication key.

Keys used for ESP are cryptographically decoupled from the keys used for authentication. Compromise of a privacy key does not compromise authentication.

Compromise of privacy keys does not compromise the root authentication key. The privacy key can be modified in the MS under control of the home system.

Keys for ESP are changed with each new security association.<sup>1</sup> Privacy keys for each call are established at the time of authentication of an MS service access. Privacy keys for control channel encryption are established at the time of MS system access, after a successful authentication.

### 6.2 Minimum Standard of Service

---

In order to recover the traffic protected by ESP, the cryptanalysis requires no less than  $10^4$  hours using commercially available computing equipment costing under \$10,000 and expected to be available in the year 2007.

The ESP algorithm shall be publicly disclosed and commercially available, and shall have been sufficiently studied by the cryptographic community, with strengths and weaknesses thoroughly understood.

### 6.3 Enhancements if Security is Compromised

---

ESP provides a mechanism to easily enhance the algorithm (or algorithms), key generation procedures, or both, in the event the security of ESP is compromised.

---

<sup>1</sup> A Security Association (SA) is established when the mobile station and the base station successfully authenticate one another. Time duration of a Security Association depends on security requirements for specific services, and could span the length of a registration session, or the length of a single or multiple calls. There could be more than one Security Association established at any given time allowing individual ESP keys for multiple subsequent communication sessions.

## 6.4 Backwards and Forward Compatibility

---

Air interface and network protocols allow mutual identification of the privacy procedure version or versions supported by the MS and by the network equipment so that a mutually supported privacy procedure can be negotiated. Negotiations of privacy algorithms are independent of the negotiation of authentication algorithms. Negotiation of privacy algorithms is under the control of the network. MS access to service may be rejected if an acceptable privacy option cannot be negotiated.

Air interface and network standards allow for the introduction of new privacy algorithms during the expected lifetime of the standard.

ESP is a significant modification of the existing privacy scheme and may not be supported by an older wireless system. However, an ESP-capable MS should function without privacy and encryption in a non-ESP-capable system, with an indication to the user that ESP is not active. An MS may also implement multiple privacy modes to enable the MS to provide privacy using older algorithms. Likewise, infrastructure may support multiple privacy modes, thus allowing privacy for an MS with different capabilities.

## 6.5 Air Interface Capabilities

---

ESP is supported on all digital wireless channels and in all MS states in which access to services or access to systems can be provided. ESP is supported on control channels, as well as on traffic channels.

All digital air-interfaces that support ESP support a method of maintaining cryptographic synchronization.

## 6.6 Network Capabilities

---

The ESP process includes means for the home service provider to allow or deny provision of ESP service at any time, regardless of the location of the MS. The ESP process includes means for serving systems to provide ESP locally, without interaction with the home system, whenever the MS is registered in the serving system, after the mobile station is successfully authenticated.

## 6.7 Applicability to Telecommunications Services

---

ESP is applicable to all telecommunications services (e.g., voice, data and signaling).

## 6.8 Normal Procedures With Successful Outcome

### Authorization

---

ESP is provided to all subscribers.

### De-Authorization

---

None identified.

## Registration

---

None identified.

## De-Registration

---

None identified.

## Activation

---

ESP is always active. The MS provides an indication that ESP is in operation.

## De-Activation

---

None identified.

## Invocation

---

ESP can be invoked for user data traffic independently during a call session(s) (e.g., concurrent calls active in the MS). ESP for signaling traffic can be invoked separately.

ESP is invoked if all of the following are true:

- a. There is an active call that requests ESP
- b. ESP is supported by the current serving system
- c. ESA has been performed successfully (i.e., subscriber identity information contained in the mobile stations and the authenticity of the base station have been verified)

## 6.9 Normal Operation With Successful Outcome

---

When ESP is invoked for signaling, most signaling traffic is encrypted. When ESP is invoked for a particular call, all the user data traffic of that call is encrypted.

## Call Detail Record

---

The system should record call detail information for the following:

- a. ESP usage duration for each system involved.

See *TIA/EIA-124* for the specific information to be included for each element.

## 6.10 Exception Procedures or Unsuccessful Outcome

### Registration

---

None identified.

### **De-Registration**

---

None identified.

### **Activation**

---

None identified.

### **De-Activation**

---

None identified.

### **Invocation**

---

The MS may provide an indication that ESP is not in operation, possibly with a reason given.

### **Exceptions While Roaming**

---

ESP may not be supported by all systems.

### **Exceptions During Intersystem Handoff**

---

ESP may not be supported by all systems.

## **6.11 Alternative Procedures**

---

None identified.

## **6.12 Interactions With Other Wireless Services**

### **Asynchronous Data Service (ADS)**

---

ADS may be denied if ESP is required but is not supported by the serving system.

### **Call Delivery (CD)**

---

None identified.

### **Call Forwarding—Busy (CFB)**

---

None identified.

### **Call Forwarding—Default (CFD)**

---

None identified.

**Call Forwarding—No Answer (CFNA)**

---

None identified.

**Call Forwarding—Unconditional (CFU)**

---

None identified.

**Call Transfer (CT)**

---

None identified.

**Call Waiting (CW)**

---

None identified.

**Calling Name Presentation (CNAP)**

---

None identified.

**Calling Name Restriction (CNAR)**

---

None identified.

**Calling Number Identification Presentation (CNIP)**

---

None identified.

**Calling Number Identification Restriction (CNIR)**

---

None identified.

**Conference Calling (CC)**

---

None identified.

**Data Privacy (DP)**

---

None identified.

**Do Not Disturb (DND)**

---

None identified.

**Emergency Services (9-1-1)**

---

None identified.

**Emergency Services Reconnect (9-1-1 RC)**

---

None identified.

**Enhanced Subscriber Authentication (ESA)**

---

ESP is only invoked if ESA is performed successfully.

**Enhanced Subscriber Privacy (ESP)**

---

Not applicable.

**Flexible Alerting (FA)**

---

None identified.

**Group 3 Facsimile (G3 Fax)**

---

G3 Fax may be denied if ESP is required but is not supported by the serving system.

**Incoming Call Screening (ICS)**

---

None identified.

**Message Waiting Notification (MWN)**

---

None identified.

**Mobile Access Hunting (MAH)**

---

None identified.

**Network Directed System Selection (NDSS)**

---

None identified.

**Non-Public Mode Service (NP)**

---

None identified.

**Over-the-Air Service Provisioning (OTASP)**

---

ESP may have an impact on OTASP.

**Password Call Acceptance (PCA)**

---

None identified.

**Preferred Language (PL)**

---

None identified.

**Priority Access and Channel Assignment (PACA)**

---

None identified.

**Remote Feature Control (RFC)**

---

None identified.

**Selective Call Acceptance (SCA)**

---

None identified.

**Service Negotiation**

---

None identified.

**Short Message Services (SMS)**

---

None identified.

**Speech Option Selection (SOS)**

---

None identified.

**Subscriber Confidentiality (SC)**

---

None identified.

**Subscriber PIN Access (SPINA)**

---

None identified.

**Subscriber PIN Intercept (SPINI)**

---

None identified.

**Three-Way Calling (3WC)**

---

None identified.

**User Group ID (UGID)**

---

None identified.

**Voice Controlled Services (VCS)**

---

None identified.

**Voice Message Retrieval (VMR)**

---

None identified.

**Voice Privacy (VP)**

---

None identified.