GPRS Security Guide for Users

Version 3.1

16 December 2014

This is a Non-binding Permanent Reference Document of the GSMA

Security Classification: Non-confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is confidential to the Association and is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Disclaimer

The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Antitrust Notice

The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

Table of Contents

Introduction

1.1 Purpose

1 This document presents the general security model of various GPRS connection types.

1.2 Scope

The scope of this document is limited to GPRS networks, however, general security issues will be presented with special reference to interconnection of other networks.

1.3 Audience

This document is intended as a security primer for users of GPRS services. It is not a formal training document, but provides security information based on a general knowledge of GPRS networks.

Definition of Terms

2

.1	APN	Access Point Name
.2	GPRS	General Packet Radio System
.3	SSL	Secure Sockets Layer
.4	WAP	Wireless Application Protocol
.5	GEA	General Encryption Algorithm
.6	WTLS	Wireless Transaction Layer Security

3 Capability

The GSM GPRS infrastructure provides a packet based network connection. Its greatest benefit is that of allowing an ‘always on’ mode, without the associated charges based on the duration of the connection.

For instance, it could allow a user to receive emails as they arrive, without the necessity of a periodic remote dial-up to check their inbox.

Note that GPRS is considered as a method of connection, not an application or service in itself, hence ‘WAP over GPRS’ is not a contradiction. The network is simply using GPRS as the connection medium, and connecting to a WAP service to provide visible content.

GSM Networks may offer a GPRS service to their customers that allows access to the Internet via WAP and as an Internet Service Provider (ISP) TCP/IP connection. It is the aim of GSM Operators to provide as highly reliable and secure service as possible with this service, but there are issues that customers need to be aware of in order for them to use this service securely.

3.1 General Security Principles

Ensuring proper security is not only a matter of deploying the right technology at the right place. Ensuring that proper procedures are adequately defined and continuously followed during operations throughout the entire chain is just as important. Security measures shall provide the following security features:

1. ***Continuous availability & operability***
   Both networks and node elements shall be able to sustain services under all conditions. Such measures shall prevent DoS attacks (Denial of Service), Distributed DoS or Replay attacks.
2. ***Data integrity***
   Network infrastructures shall ensure that the transiting data can not be tampered with in any way.
3. ***Authentication***
   Verification that all traffic coming from an identified source really originates from the claimed source shall be enforced.
4. ***Confidentiality***
   Sensitive information shall be protected from unauthorised disclosure. Close control of the sensitive information distribution and the isolation of the distribution infrastructure is the first step to guarantee confidentiality. The ultimate step being the encryption of information data into an unintelligible form before transmitting.
5. ***Non-repudiation***
   Prevents that a party to a transaction falsely denies that the transaction occurred or was authorised, after the fact.
6. ***Fraud Management***
   All procedures to respond to any security breach and restore normal service in the shortest delays shall be put in place in network infrastructures.

Security shall be ensured using security measures of several types, including physical security, logical security and personnel security, but also including risk assessment and compliance verification, contingency planning, security incident reporting and fraud management.

4 Handset and SIM Security

4.1 User Equipment

GSM customers use GPRS capable phones and devices. These devices are the property of the customer, and as such customers are free to do with them as they wish. In order to ensure the security of the terminal device, customers should ensure that any unauthorised person has not modified the terminal, either in terms of the hardware or software running on the device.

Customers connecting other devices to the mobile device such as laptop computers, personal organisers, and other devices also need to ensure the integrity of the software and hardware of these devices.

When using cables, infrared, bluetooth, or other services to connect devices together it is the customers' responsibility to ensure that these devices are set-up and operated in a secure manner together.

4.2 SIM Card and Network Subscription

All GSM devices capable of using GSM networks need a SIM card to be inserted into the device before it can connect to the network. This is either a credit card sized, or small factor chip card. The card contains the subscription identity for the network. Possession of this card gives the customer authority to incur charges on to the associated account.

Customers should keep this card in a secure manner and immediately notify their network operator if it is lost or stolen. All SIM cards have the capability of enabling a security PIN that is designed to help prevent unauthorised access and use of the SIM card. Customers are strongly encouraged to enable this security feature.

GPRS architecture security

5

5.1 Air Interface

The GPRS facility to encrypt data between the handset and the network is negotiated between the network and the handset. Most networks are currently enabled to use a GPRS encryption algorithm.

The standards bodies regularly release new security algorithms and network operators and handset manufactures make best efforts to implement them as soon as practical.

When a customer is roaming then the level of air interface encryption will be based on the capabilities of the visited network.

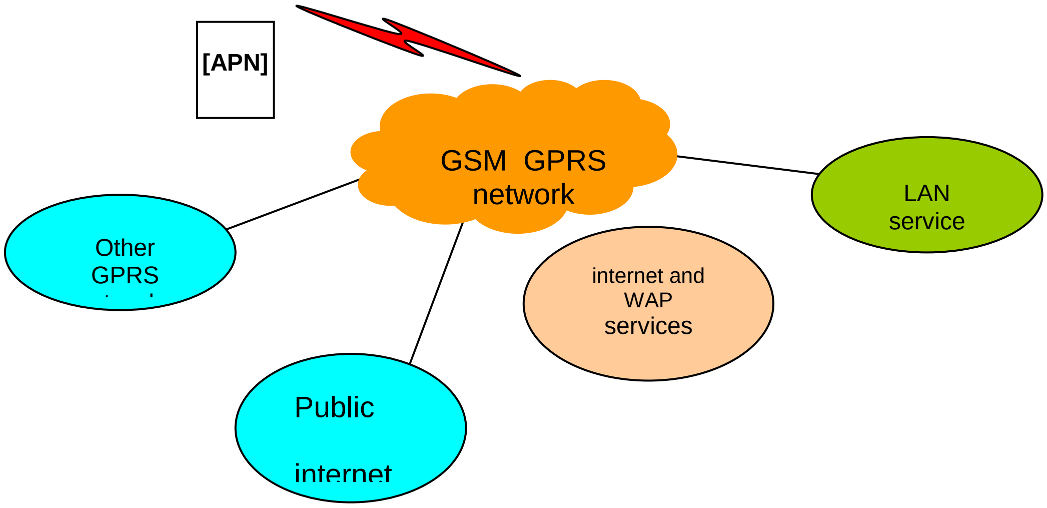
Recently, the GSM specifications required phones to have the capability to display the ciphering state of the connection but not all terminals support this capability at present. Some phones have the ability to warn the user when making a connection that the negotiation has resulted in the default unencrypted connection.

It is understood that the current level of encryption over the air is strong enough to withstand attacks using available tools and computing power, to ensure that the data is secure within a reasonable time frame.

5.2 Core network

The GSM GPRS core network allows connection from the base station to :-

- Internet and WAP services
- Public Internet and WAP services
- Other GPRS networks (considered as a roaming connection)
- Leased line connections to other networks (Business LAN)



In all cases, the connection between the user and the destination is transparent. i.e. no internal GPRS, or associated, nodes are visible to the user connection.

Also note, that there is no restriction on the type of service available to the user, e.g. http, ftp, irc, email and any existing (or future) internet service is available. However, users will not be able to run services that require external IP devices to establish connections to their terminal, such as a web server.

As with all internet connections, customers should take all the usual precautions when using the Internet against threats from email, downloaded programs and information entered on unsecured web pages.

GPRS users and internet users alike, are strongly advised to install anti-virus software and personal firewall software to protect their private connections.

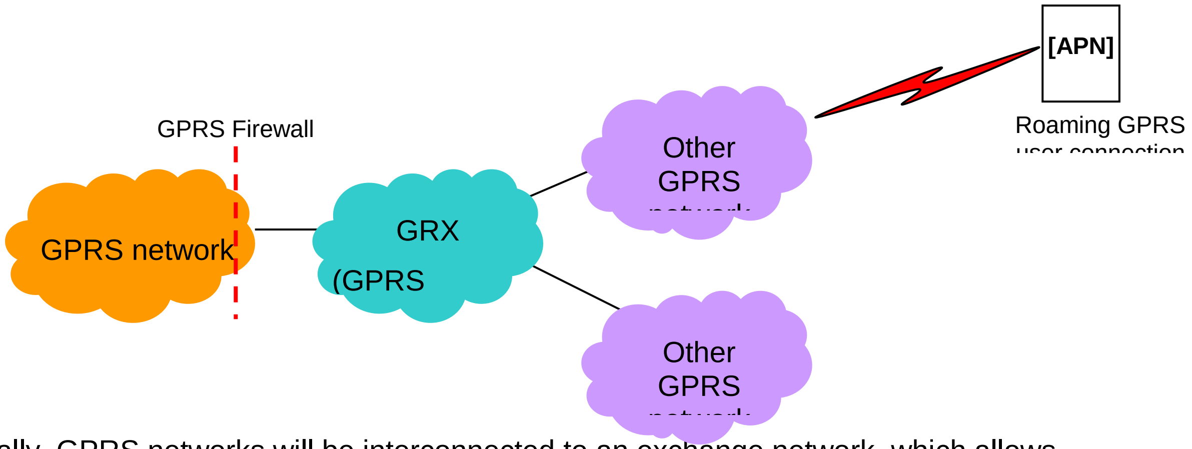
The nature of GPRS relies on the user obtaining an IP address from the serving network operator and making a subsequent onward connection. This indicates that a user is given a different IP address each time they create a new Context Activation (GPRS connection). Thus it is not possible to locate a user on IP address information in a reliable manner.

This mechanism has inherent security benefits, and it is recommended that unless it is necessary, or desirable, for a user to stay permanently connected to the GPRS network, that they are disconnected.

5.3 GPRS Roaming connections

GSM Operators are in the process of deploying roaming interconnections, which include GPRS aware firewalls.

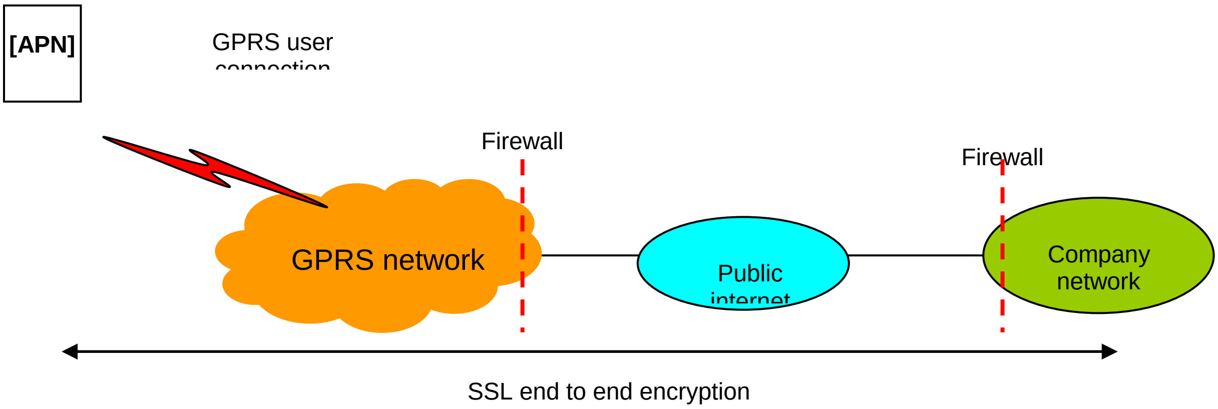
This allows the GSM / GPRS network operators to be protected against unwanted connections from other GPRS networks.



Typically, GPRS networks will be interconnected to an exchange network, which allows interconnection to other GPRS partners.

6 GPRS services

6.1 Business internet access over a GPRS connection



Because of the always on nature of a GPRS connection it is more likely that users will leave services connected and logged in for long periods. Users should enable facilities to lock the device during a period of inactivity, such as password protected screen savers.

All customary and necessary precautions, as suggested in section 4.2, should be deployed.

Regular business use of the internet implies that the information is company confidential and may be commercially valuable. It is the customers' responsibility to ensure that, if necessary, internet connections are SSL encrypted. This ensures that company servers cannot be 'replaced' by rogue copy servers, as well as ensuring that the information is encrypted to withstand eavesdropping over the internet.

It is usual business practice to ensure that any connection from the company to the internet is further protected by firewall infrastructure.

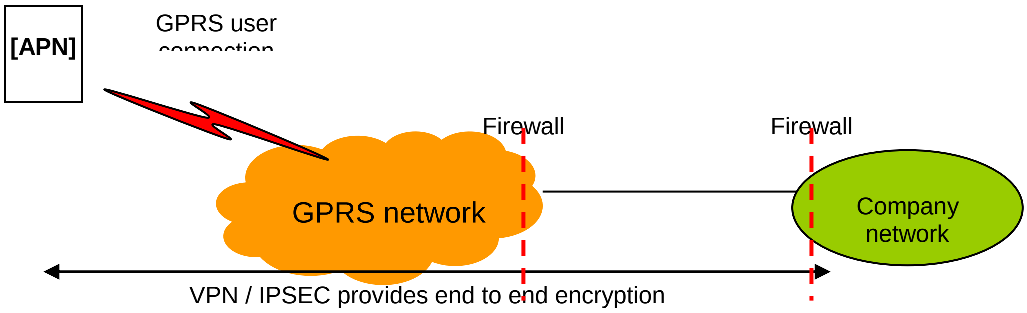
The IP address range associated with a company user can be set with a new APN. This is of great benefit when considering company firewall policy.

A new APN must be implemented by the operator in the core infrastructure.

6.2 Business LAN access to a GPRS connection

In this configuration, a leased line exists between the operator and the customers' company networks.

This provides dedicated bandwidth into the GSM / GPRS infrastructure. Additionally, it is possible to employ encryption across this leased line, between the company server and network operator.



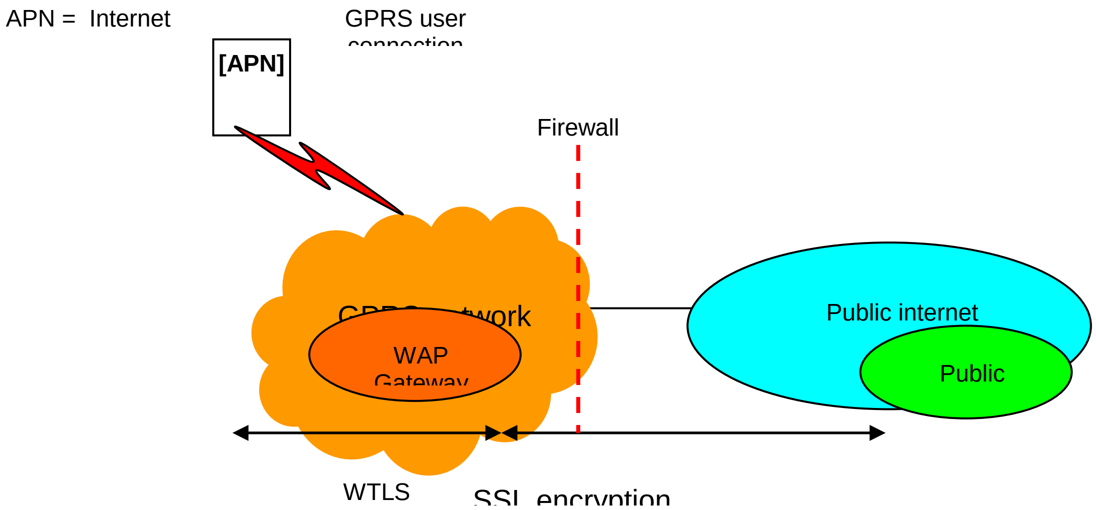
Appropriate protocols allow for an encrypted connection using a VPN or IPSEC.

In this scenario, SSL encryption would not be required.

It is recommended that the company LAN be protected by firewall infrastructure.

6.3 Consumer and general GPRS connections

In general, consumers should treat a GPRS connection in the same manner as any ISP Internet connection.



Note that for WAP access, GPRS provides no ‘extra security’ in itself, to a public service.

This can be provided by WTLS (an encrypted WAP connection), and is usually noted by an extra padlock symbol on the handset.

Public WAP services are available by entering the WAP bookmark in the handset, as would be the case for a circuit switched connection. If the padlock symbol is visible on the GPRS device when visiting a public WAP service, this indicates that an encrypted (SSL) connection is made between WAP Gateway and that public service.

This is with the proviso that the WTLS encrypted data is unencrypted at the WAP Gateway, before re-applying SSL encryption to the public service.

If, however, the WTLS encrypted session terminates at a WAP service on the operators WAP gateway, then encryption is ensured end to end.

7 Legal implications

7.1 Legal Interception

Networks in certain countries are required to provide interception of network traffic to suitably authorised government departments. Operators may also be obliged to ensure that information relating to an account and its activity is retained and passed to the relevant authority for the investigation of a crime.

7.2 Data Protection Legislation

Network operators may be bound by the terms of local data protection legislation and will not release any information on a customer account other than to those persons authorised to operate that account.

Annex A Document Management

A.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
3.1	12 Dec 2014	Transferred PRD from SG to FASG as SG.16 v3.1	FASG	David Chong, GSMA

Other

Type	Description
Document Owner	FASG
Editor / Company	James Moran, GSMA

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.