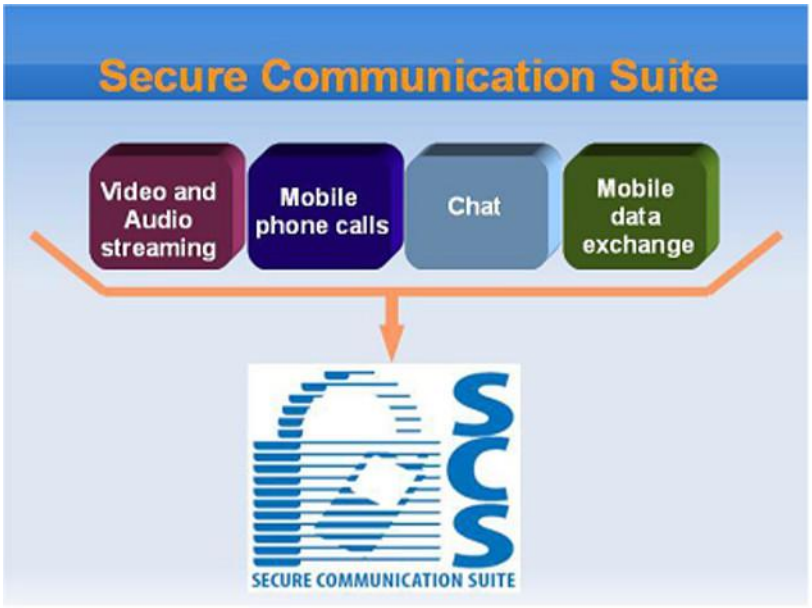
INTRODUCTION

The protection of information has become one of the most important activities to consider if we want to protect our privacy. The possibility of being constantly connected and having geographical independent access to information is a great advantage, but along with global access comes the issue of global security. There are three aspects that must be considered for information security.

- The security of the accesses to information sources: preventing non authorized entities access to the information sources
- **The security of the transmission channel**: it is possible that the transmission channel can be monitored by third parties when accessing the information source (or when performing an information exchange)
- **The security of the electronic devices used to access (exchange) information**: it is possible that the some devices (PC,Smartphone, etc.) have been hacked and are being controlled by someone else

The Secure Communication Suite (SCS) access to information sources (or performs information exchanges) in a secure way by solving the three issues as listed above.



SCS DESCRIPTION

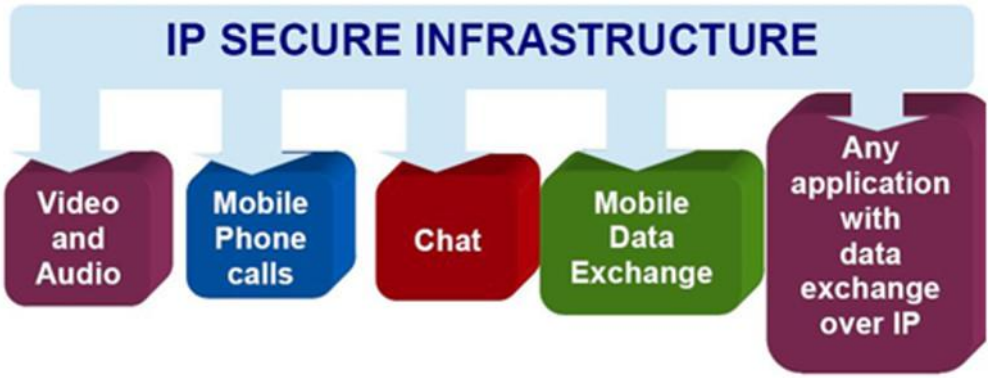
The SCS protects voice and data communications against wiretapping, interception and internet intrusion.It is a comprehensive solution for mobile communication security, which consists of client applications and server modules.

SCS client applications are made for end users' mobile phones and PCs.Server modules provide authorization and mutual connection between individual users.

SCS can be delivered as scalable solution which meets specific customer requirements. It's dedicated for government agencies.

Main features from user's point of view are:

- Secure Voice Communications
- Secure Text Communications
- Secure Data transfer
- Audio, Video and GPS streaming with real time viewing
- In general, any application with data exchange over IP

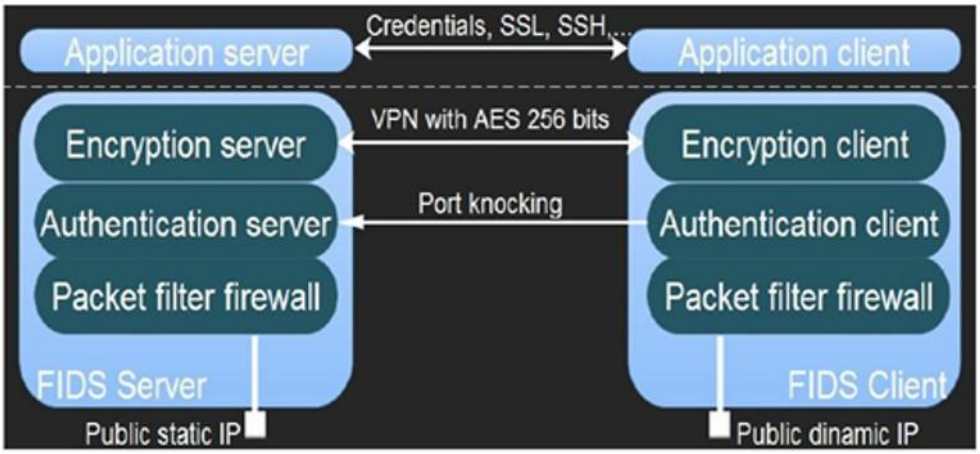


SCS client applications can be installed on a wide range of recent and ongoing devices for end-users (mobile phones and PDA with Android operating system, Computers and notebooks with Windows and Linux operating systems) and supports all the most used Internet Connections (GPRS, EDGE, UMTS, HSDPA, LTE, WiFi, LAN/WAN, IP satellite networks).

SCS ARCHITECTURE

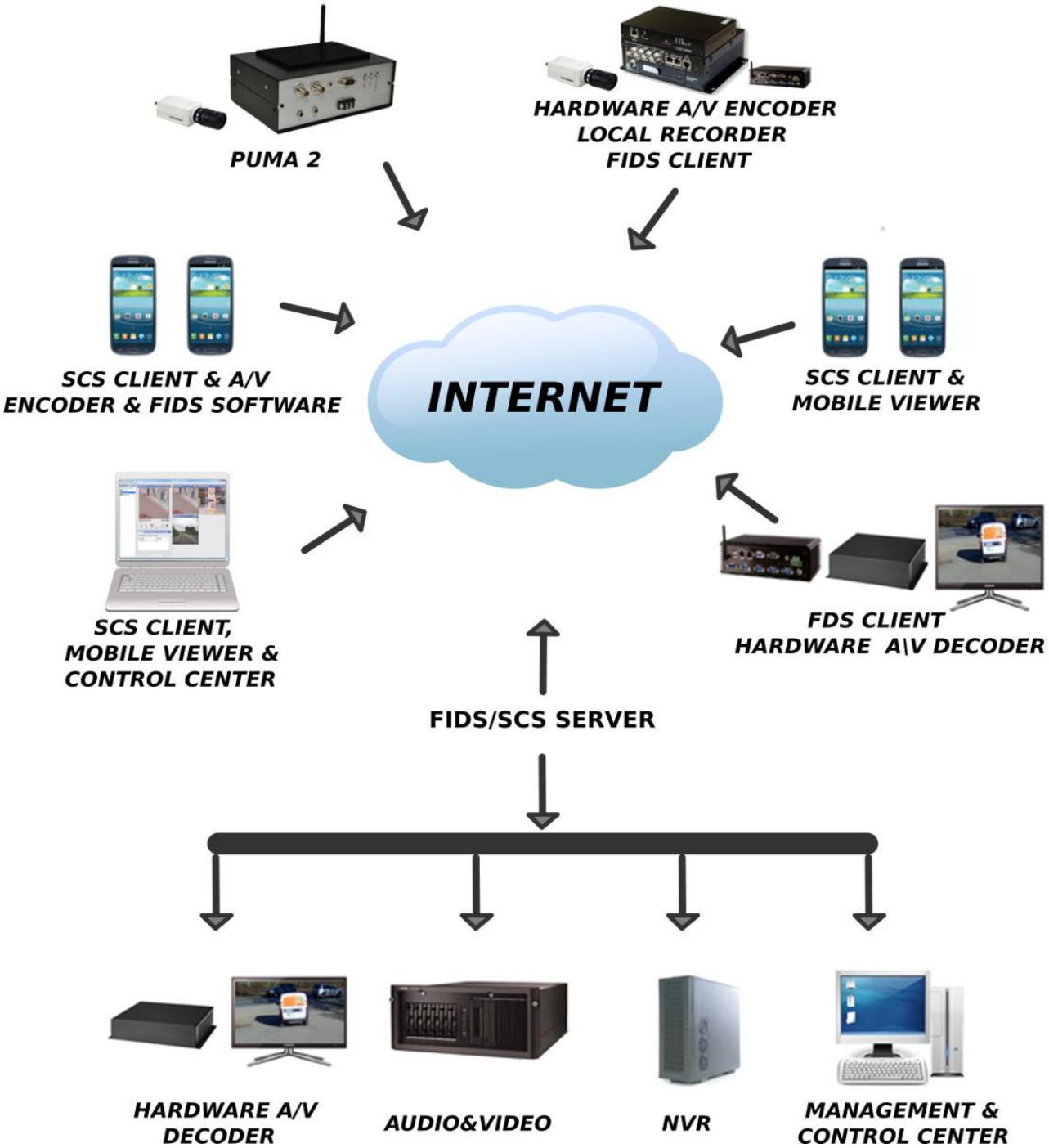
The SCS infrastructure is based on client-server principles and consists of client and server hardware and software modules:

- Firewall and Intrusion Detection System (FIDS) Server, which provide a secure communication environment to all those applications which make a data exchange in a WAN over IP protocol
- FIDS Client, which is the embedded hardware and software solution that realizes with the FIDS Server the secure IP environment



- SCS Communication Server, which is the server application representing the core part of the overall communication system
- A/V Server, which is at the centre of the wireless surveillance distribution architecture. Its primary function is to distribute the live video and audio streams from deployed encoders to any number of viewing clients, while ensuring reliable transmission through active channel management allowing dynamic bandwidth adaption. A/V Server has been specifically designed to ensure the most effective use of available network bandwidth, by keeping the amount of communication with deployed devices as 'light touch' as possible
- SCS Client for Android

- SCS Client for Windows
- SCS for Linux
- SCS Server is available in three editions – **Lite, Business and Enterprise** – respectively for 20, 100 and 1.000 users.


PUMA 2
HARDWARE A/V ENCODER
LOCAL RECORDER
FIDS CLIENT
SCS CLIENT & A/V
ENCODER & FIDS SOFTWARE
INTERNET
SCS CLIENT &
MOBILE VIEWER
SCS CLIENT,
MOBILE VIEWER &
CONTROL CENTER
FDS CLIENT
HARDWARE A\V DECODER
FIDS/SCS SERVER
HARDWARE A/V
DECODER
AUDIO&VIDEO
NVR
MANAGEMENT &
CONTROL CENTER