

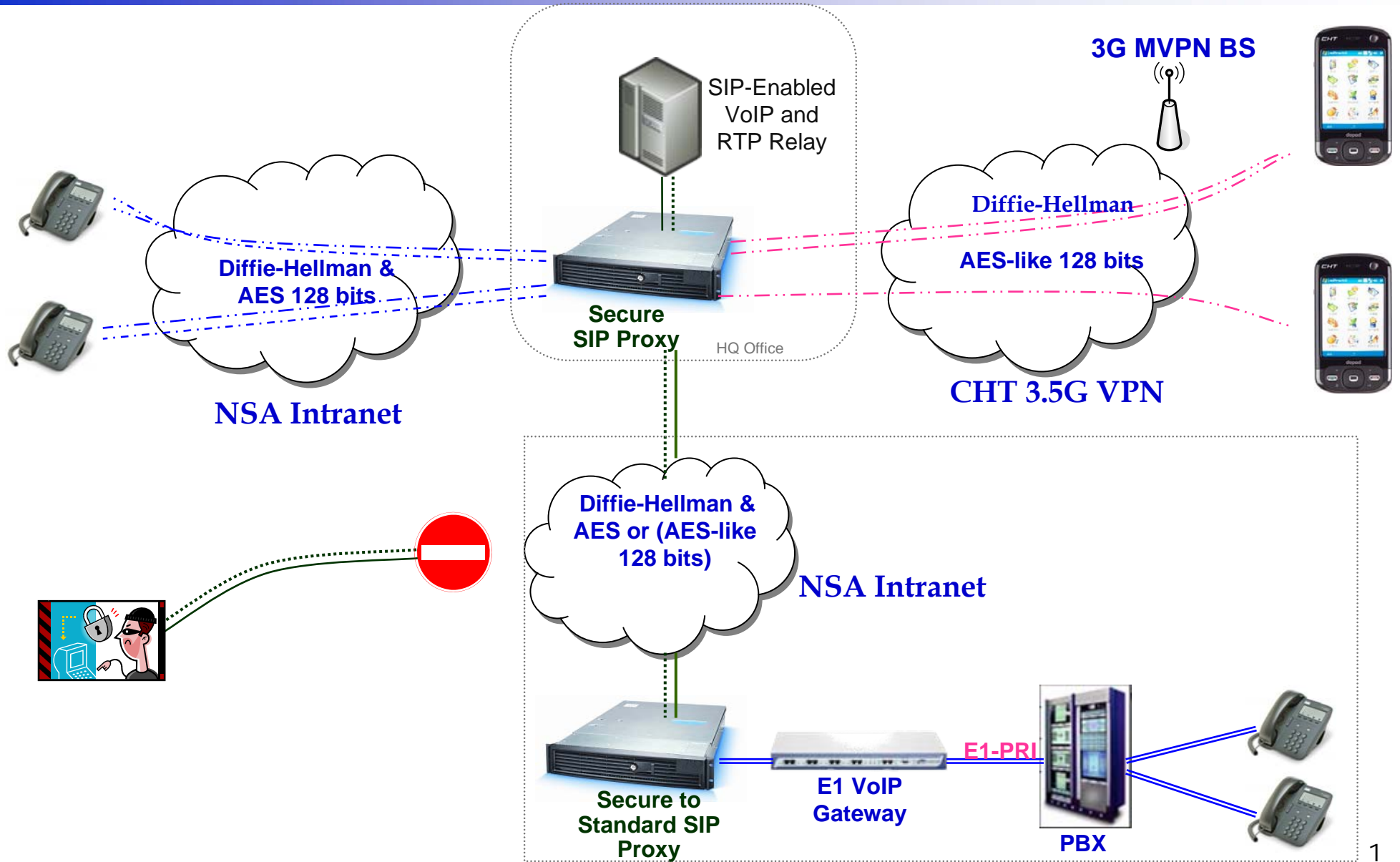
整合於HSDPA 與 IP 網路上之加密型 網路電話系統規劃

劉興華博士

網址：<http://www.hivocal.com.tw>

聲威網際科技股份有限公司

Secure VoIP Total Solutions



- **Secure IP Phone:** 使用 Diffie-Hellman & AES 128bits 安全加密演算法相互通訊
- **Secure PDA Soft Phone:** 使用 AES-like 128bits 演算法相互通訊
- **當 IP Phone 與 PDA 相互通訊時，會使用 AES-like 演算法互相通話**
- **當 IP Phone, PDA 與 PBX 相互通訊時，會透過 Secure to Standard VoIP Server 將加密演算法轉換成標準 SIP 協定與 PBX 通話，但還是在安全的 VPN 網路環境下**

(目前最佳支援平台CHT 9100)



- ◆ Windows Mobile 5.0 or 2003 Pocket Operate System
- ◆ 支援VoIP SIP通訊協定標準(SIP V1,V2, RFC3261,RFC3581)
- ◆ 相容於標準即時傳輸通訊協定(RTP, RFC3550) 及即時傳輸控制通訊協定(RTCP, RFC3551)
- ◆ 頻寬需求最小化,語音傳輸使用頻寬小於**28KB**
- ◆ 自行開發穿越NAT防火牆技術
- ◆ 支援Direct P2P(DP2P) 點對點通話之VoIP技術
- ◆ 介面研改：依需求單位加解密函式庫I/O介面修改並提供置換功能
- ◆ 獨家研發G.729壓縮簡化技術，最低CPU 166Mhz
- ◆ 支援802.11g/b
- ◆ 支援HSDPA模式上網
- ◆ MD5安全加密
- ◆ Deffie & Hellman (2048 bit) 金鑰交換演算法
- ◆ AES_Like(7 rounds) 192 bit 加密演算法

主要規格：

- 支援h.263視訊壓縮及G.729聲音壓縮格式
- 支援即時訊息傳送、檔案傳送
- 支援SIP標準通訊協定 (RFC3261,RFC3581)
- 支援Hivocal 穿越NAT/防火牆機制
- 電話簿功能：提供用戶電話簿管理功能
- 使用者線上狀態顯示
- 支援封包欄位設定Type of service (TOS) 以提升處理優先權
- 具備自動轉接功能
- 撥打計費電話，即時顯現通話餘額
- 通聯紀錄 (F_IP、T_IP、F_PhoneNo、T_PhoneNo...)
- 支援繁體中文及English語系切換

次要規格：

- 提供應用程式自動執行、耳機型式語音收發及百萬像素攝影功能
- 支援由需求單位內部網站連線(on-line)方式，直接下載更新版本功能
- 安全保護：應用程式自動執行啟動時先按鍵盤特定鍵，可設定成每次登入伺服器均須重新輸入帳號及密碼
- 電話簿功能：提供用戶電話簿管理功能，電話簿加密可儲存於隨身碟
- 支援802.11g/b
- MD5安全加密
- Diffie & Hellman (2048 bit) 金鑰交換演算法**
- AES_Like(7 rounds) 192 bit 加密演算法**



系統規格 伺服器

提供SIP Proxy Server、SIP Registrar Server、SIP Redirect Server、等功能。

SIP 具UPD與TCP通訊功能.

支援VoIP通訊協定標準(SIP,RFC3261,RFC3581)

通過工研院電通所SIP/ENUM相容性測試。

支援HA已達互相備援功能.

RTP (RFC1889) Relay

AAA (標準MD5認證)

相容於標準即時傳輸通訊協定(RTP, RFC3550)及時傳輸控制通訊協定(RTCP, RFC3551),提供G.723,G..729,G.711,等語音壓縮格式轉送功能.

防火牆/NAT：依需求單位網路環境以RTP Relay 機制來通過防火牆及NAT(Network Address Translation)

自行開發穿越NAT防火牆技術，非使用STUN或UPNP技術，雙方可直接穿越現今NAT的所有20種類型

具備帳號整批匯入功能.

提供即時通聯紀錄查詢暨產製報表功能.通聯記錄年限可依記憶體大小調整.

提供線上註冊狀況查詢。

提供支援通話監聽錄,語音信箱等功能.

金鑰交換：依需求單位金鑰機制設計以執行通話用戶間之金鑰交換功能

提供來電顯示、忙線回應、對方不在線上之通話管理功能.

提供Web-base或GUI管理界面.

支援偵測防禦用戶端密碼遭受暴力攻擊法登錄攻擊.

提供管理300000個使用者註冊,30000人同時通話容量

支援標準SIP之VoIP Gateway ;WiFiPhone註冊及通話服務.

本系統具有自動回復功能,當系統因故重新啟動時,原先SIP UA所註冊之Contact Address 等資料均可自動回復.

Server 具有Redundancy Function 1 + 2 Auto Routing.

支援用戶端管理：用戶帳號、密碼、基本資料(依需求單位定義欄位)登錄管理.

功能特點

- 1、通訊協定支持SIP (RFC2543、RFC3261)
- 2、64組來電號碼顯示64組撥出號碼查尋及存儲功能
- 3、100組電話本
- 4、免持撥號、通話自動計時顯示
- 5、來電回電查尋、刪除、重撥功能
- 6、拒接功能、保留功能、電話轉接功能
- 7、預撥功能
- 8、日期、時鐘顯示功能
- 9、PPPoE、乙太網點對點撥號協議
- 10、IP動態地址、靜態配置兼容
- 11、TCP/IP(ARP/RARP、IP/ICMP、UDP/TCP/IP、RTP/RTCP)
- 12、TFTP和Console功能
- 13、IEEE 802.1P/802.1Q/10BaseT/100BaseTX
- 14、DNS域名服務協議
- 15、三方通話功能
- 16、呼叫等待功能、呼叫轉移功能
- 17、半雙功方式、保證通話效果
- 18、可選擇模組、網路線供電(PoE)
- 19、**Deffie & Hellman (2048 bit) 金鑰交換演算法**
- 20、**AES 192 bit 加密演算法**



特殊保密功能

可依客戶需求,通話時以點對點方式執行密鑰交換模式,將通話封包加密,達到保密防諜的功能。(每通電話的密鑰都不相同).破解難度最高.

配合特殊加密型SIP Server,可隨時更換Client端電話之密鑰,由中央統一管理.達到組織保密防諜的功能.