BV TECH: Privatewave, crittografia e comunicazioni sicure

privatewave
secure communication solutions

BV TECH

Indice

- Breve presentazione della società e del Gruppo BV TECH
- Comunicazioni sicure: la soluzione Privatewave
- Privatewave:
  - Protocolli di sicurezza per il VoIP
  - Vantaggi della soluzione
  - Principali funzionalità

BV TECH – chi siamo

BV TECH è un gruppo innovativo, fondato nel 2005, interamente italiano, composto da società di ingegneria, servizi informatici e telecomunicazioni. Nel 2019 il Gruppo, che comprende oltre 900 professionisti altamente qualificati, raggiungerà un fatturato totale di circa 100 milioni di euro.

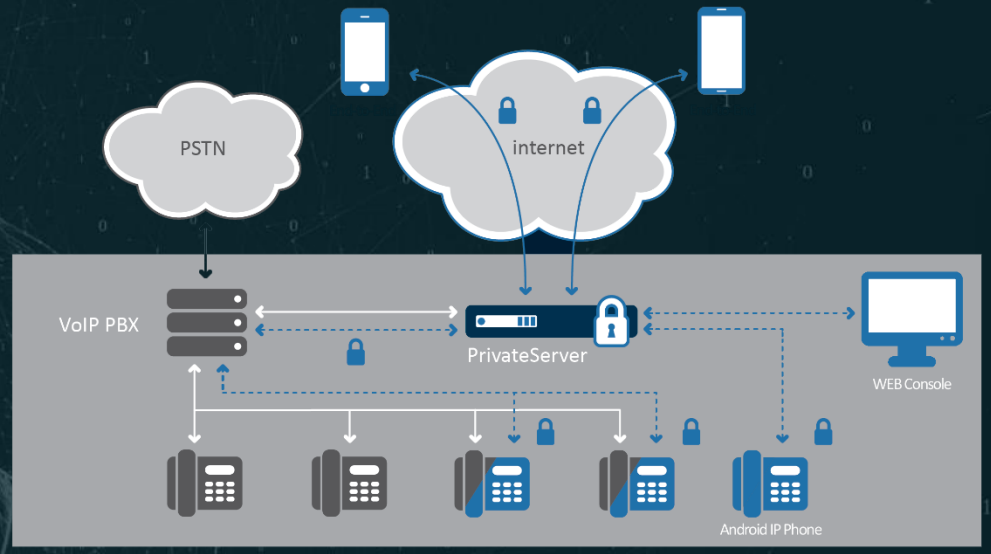
Grazie alla sua esperienza, a costanti attività di formazione e aggiornamento, e al supporto di professionisti specializzati, BV TECH si pone tra le principali protagoniste del panorama nazionale del settore dell'Information & Communication Technology, della Gestione Documentale, della Consulenza Direzionale per i settori della Difesa, della Sicurezza, del Finance, dell'Industria, della Pubblica Amministrazione e della Sanità.

Nel 2015 BV TECH ha ottenuto la certificazione **ELITE**, l'iniziativa di Borsa Italiana rivolta alle imprese di alto profilo.

BV TECH è tra i soci fondatori del consorzio internazionale Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity del Massachusetts Institute of Technology per il miglioramento della sicurezza cibernetica delle infrastrutture critiche.

BV TECH – Privatewave

Privatewave è una soluzione di comunicazione sicura basata sull'uso di protocolli standard di cifratura e sull'utilizzo di componenti software open source, in grado di mettere in sicurezza il contenuto delle conversazioni telefoniche in tutte le sue declinazioni (mobile-mobile, fisso-mobile, fisso-fisso), dei messaggi di testo e degli allegati, con cifratura di grado militare.



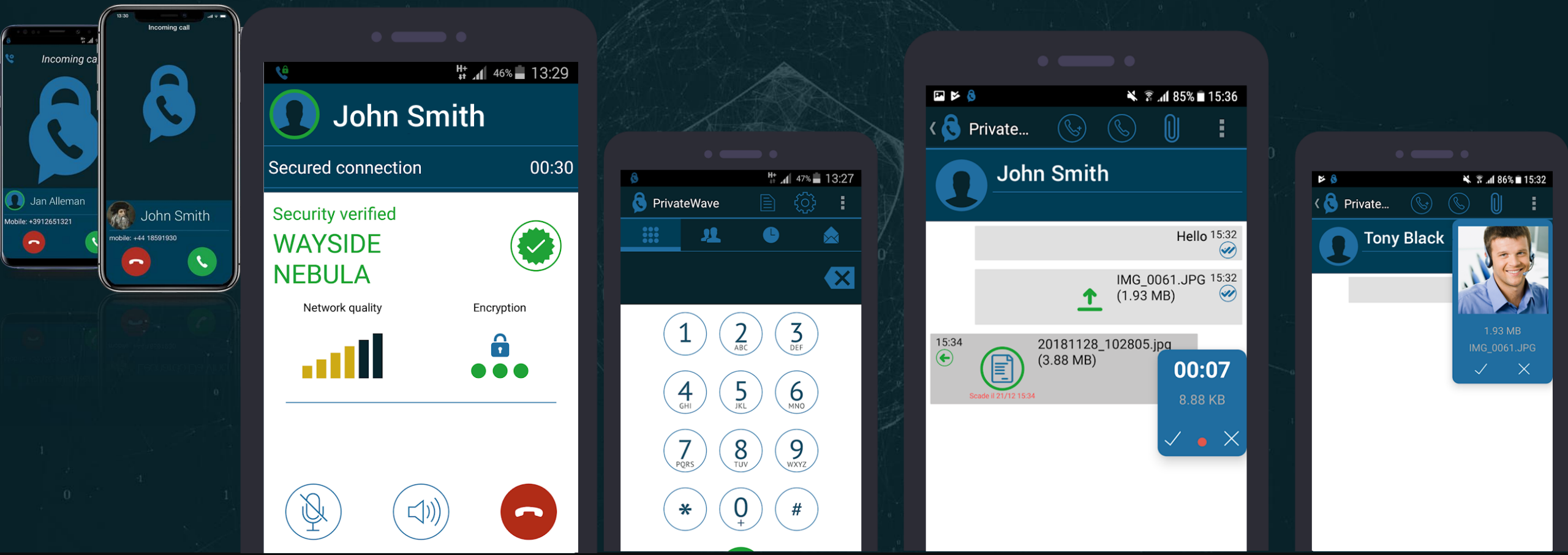
L'evoluzione della piattaforma è garantita da una continua ricerca dell'eccellenza con un approccio volto ad anticipare i veloci cambiamenti del mondo delle telecomunicazioni.

Tutte le attività di sviluppo sono realizzate presso la software factory BV TECH. Il prodotto è totalmente made in Italy e nessuna delle attività nell'ambito del prodotto sono realizzate in outsourcing o con società esterne.

BV TECH – Phone call – SMS / Attach – Voice sms

Available on the App Store

GET IT ON Google play

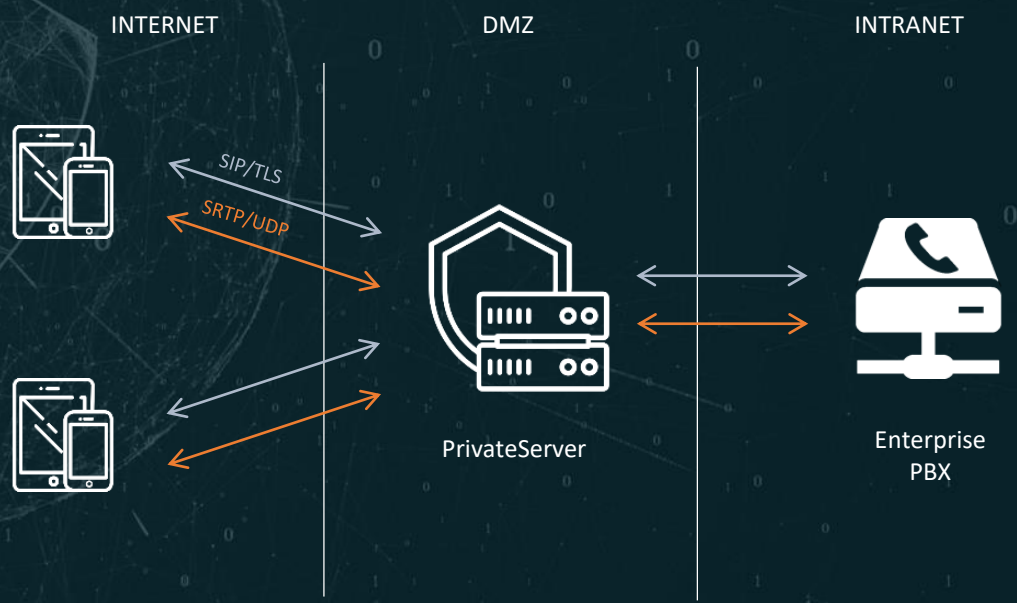


privatewave
secure communication solutions

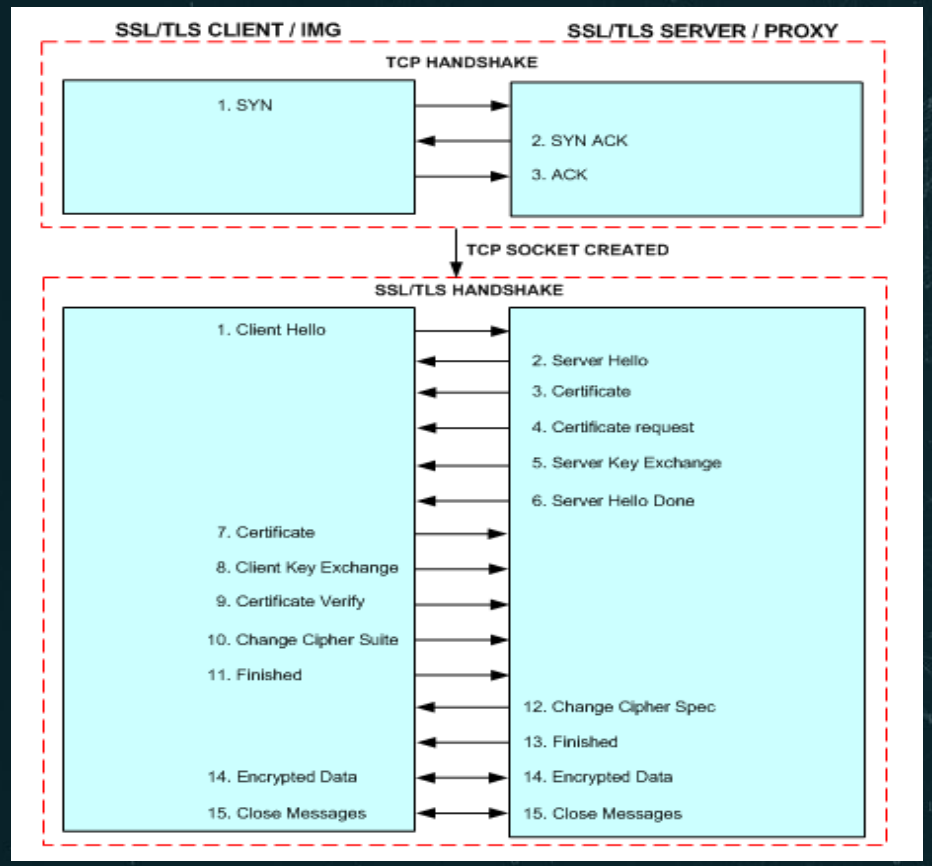
BV TECH

PrivateWave – Protocolli di sicurezza per il VoIP

- Session Initiation Protocol (SIP): protocollo ASCII usato per la segnalazione
- Real-time Transport Protocol (RTP): per l'instaurazione di sessioni media (audio)
- Segnalazione SIP cifrata con TLS (come i browser con HTTPS) per garantire la confidenzialità dei metadati
- SRTP con payload autenticato e cifrato simmetricamente con AES-256-CTR: garantisce confidenzialità delle comunicazioni contro attacchi di tipo CCA, CPA e Replay



PrivateWave – Protocolli di sicurezza per il VoIP, SIP/TLS



SIP/TLS handshake e standard di cifratura

- Certificato digitale per validare l'identità del server
- Certicate pinning per protezione da attacchi MITM
- Possibilità di autenticazione del client mediante certificato x509 (mutua autenticazione)
- Policy TLS rigide per garantire la sicurezza:
  - Scambio chiavi: Diffie-Hellman Ephemeral (DHE), Elliptic Curve Diffie-Hellman Ephemeral (ECDHE), RSA
  - Autenticazione/Firma digitale: RSA, ECDSA
  - Cifratura simmetrica: AES256, AES128 (IP-PBX legacy)
  - Hashing: SHA256, SHA384
- Negoziando cipher suite di tipo DH la segnalazione SIP acquisisce la proprietà di Forward Secrecy

PrivateWave – Protocolli di sicurezza per il VoIP, SRTP

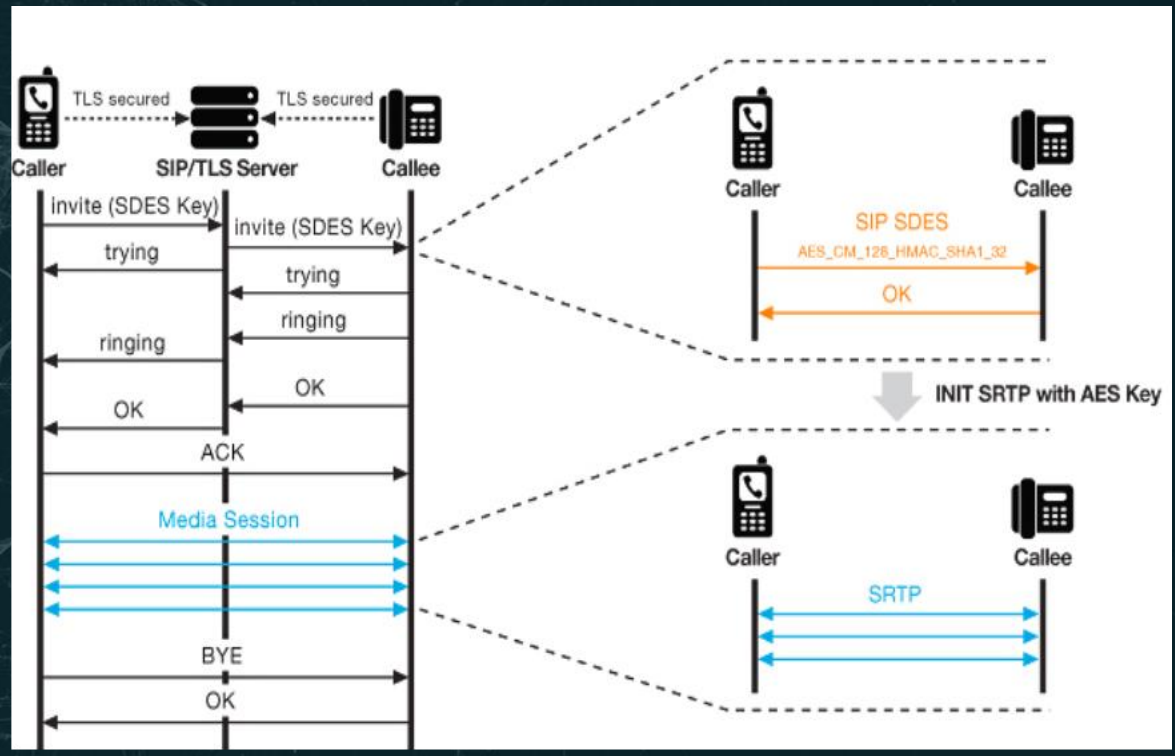
Caratteristiche di SRTP e standard di cifratura

- SRTP garantisce la confidenzialità e l'integrità dei pacchetti RTP
- È uno standard IETF dal 2004 (RFC3711 and RFC6188)
- Supporto alla cifratura simmetrica:
  - AES-256-CTR: utilizzato dai client PrivateWave
  - AES-128-CTR: utilizzato da alcuni IP-PBX legacy
- Controllo di integrità mediante algoritmo HMAC-SHA1
- Due modelli di sicurezza per la negoziazione delle chiavi di sessione SRTP:
  - End-to-Site: fuori banda nel canale SIP/TLS con protocollo SDES. In questo modello il server è una "trusted party" e può erogare funzionalità aggiuntive come 3-way call, conference room e l'integrazione con l'infrastruttura telefonica enterprise.
  - End-to-End: in banda nel canale RTP con protocollo ZRTP. Al di fuori dei due client coinvolti nella chiamata, nessuno può decifrare il traffico. Questo modello è disponibile solo per comunicazioni mobile-mobile
- La versione Enterprise di PrivateWave implementa entrambi i modelli di sicurezza e li applica in modo adattativo su base chiamata allo scenario richiesto (Multi Level Security)

PrivateWave – Protocolli di sicurezza per il VoIP, negoziazione delle chiavi con il modello End-to-Site

Scambio chiavi secondo il modello End-to-Site: protocollo SDES

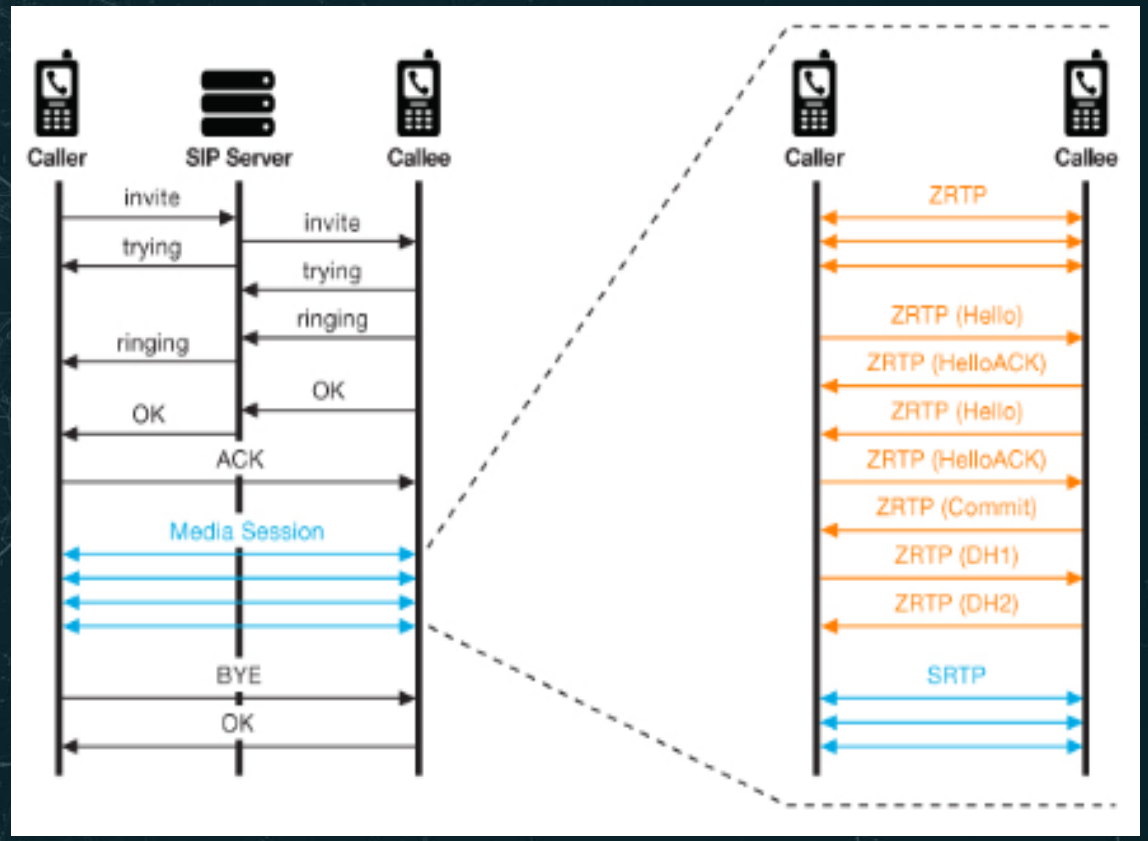
- Cifratura client-server con verifica del certificato digitale
- Stessa architettura di sicurezza di HTTPS
- Basato su certificati digitali e Public Key Infrastructure (PKI)
- Chiamato e chiamante si scambiano le chiavi di sessione attraverso PrivateServer (trusted 3° party) su canale sicuro SIP/TLS
- Standard IETF (RFC4568)
- Diffuso tra i maggiori produttori di apparati VoIP:
  - Cisco, Avaya, Asterisk, Snom
- Standard «de facto» per la telefonia sicura Enterprise



PrivateWave – Protocolli di sicurezza per il VoIP, negoziazione delle chiavi con il modello End-to-End

Scambio chiavi secondo il modello End-to-End: protocollo ZRTP

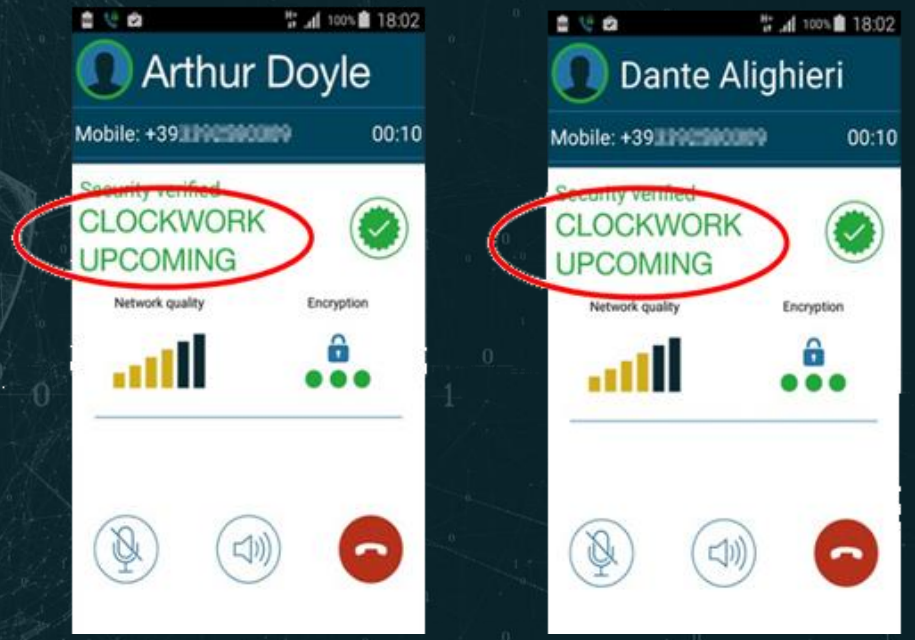
- Cifratura end-to-end con protezione da attacchi MITM
- Inventato nel 2006 da un gruppo di crittografi internazionali guidati da Philip Zimmermann
- Standard IETF (RFC6189)
- ZRTP utilizza la crittografia a Curve Ellittiche ECC (P-384 / P-521)
- Rilevazione a runtime di curve ECC deboli
- Implementato in codice open source
- Algortitmo di cifratura simmetrica: AES-256 (CTR)
- Algortitmo di cifratura asimmetrica: ECDH-384/521 (P-384/521)
- Forza di cifratura equivalente: RSA 7680/15360
- Perfect Forward Secrecy (PFS): nel caso sfortunato di perdita del telefono non vengono compromesse le chiavi utilizzate nelle sessioni precedenti



PrivateWave – Protocolli di sicurezza per il VoIP, autenticazione ZRTP

Autenticazione ZRTP

- I client PrivateWave forniscono autenticazione di tipo umano con generazione automatica e scambio e delle chiavi basato su ZRTP
- *Short Authentication Strings (SAS)*
  - Le parti verificano verbalmente due parole chiave mostrate ad entrambi gli end-point
  - Le SAS sono hash crittografici delle chiavi Diffie-Hellman: usate per verificare la presenza di un attacco MITM
- *Key Continuity*
  - Cache delle chiavi di sessione precedenti: verifica della presenza di MITM dopo il primo scambio di chiavi
  - Verifica delle SAS richiesta solo alla prima chiamata, in seguito verificate automaticamente



BV TECH – Privatewave, i vantaggi delle soluzione

- Applicazione multipiattaforma su smartphone e tablet commerciali per la protezione di telefonate e messaggi mobile-mobile e/o mobile-fisso.
- Server in cloud oppure dedicato e completamente gestito dal cliente.
- Comunicazioni mobili con crittografia end-to-end e cifratura di grado militare.
- Garanzia di riservatezza.
- Estrema semplicità di utilizzo.
- Attivazione Over-The-air per una distribuzione facile e veloce senza necessità di configurare il terminale.
- Prestazioni eccellenti con tutte le tecnologie di rete: LTE, UMTS, EDGE, GPRS, WIFI.
- Possibilità di integrazione con l'infrastruttura telefonica aziendale.

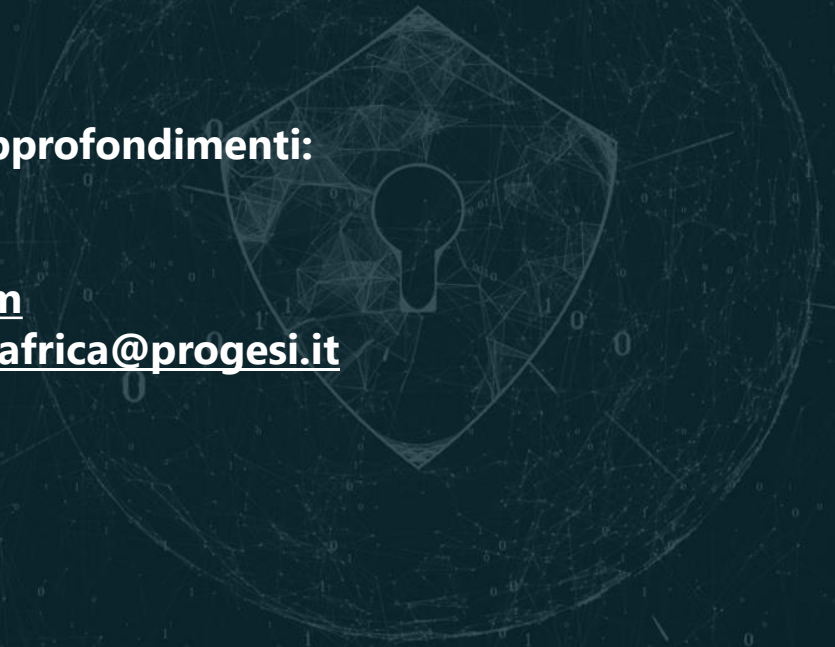
BV TECH – Privatewave, principali funzionalità

Principali funzionalità	Release	
	Professional	Enterprise
Telefonate – SMS (fino a 1000 caratteri) – SMS vocale	✓	✓
Allegati (pdf, word, audio, video, ecc.)	✓	✓
Conference Call/Room	✗	✓
Servizi di chiamata avanzati (chiamata a tre, trasferimento di chiamata, integrazione PBX aziendali)	✗	✓
SIP Proxy (Denial-Of-Service prevention)	✓	✓
SSL Certificate Pinning	✓	✓
Mutua Autenticazione tramite Certificato X.509	✓	✓
Modello di sicurezza	End-to-End (ZRTP)	End-to-End (ZRTP/SDES)
Multilevel Security (modello di sicurezza adattativo ZRTP/SDES)	✗	✓
Mascheratura presenza on-line	✓	✓
Scadenza programmabile dei messaggi con PIN attivo	✓	✓
PIN di sicurezza per accesso all'APP – PIN di sicurezza sotto minaccia	✓	✓

BV TECH – Privatewave, principali funzionalità

Principali funzionalità	Release	
	Professional	Enterprise
Offuscamento anti blocco VoIP	✓	✓
Tastiera virtuale Anti key logger	✓	✓
Utilizzo esclusivo della risorsa microfono su piattaforma Android	✓	✓
Rubrica aziendale centralizzata separata dalla rubrica del telefono con gestione di gruppi e protetta all'interno dell'app	✓	✓
Supporto SELinux (framework di sicurezza secondo linea NSA)	✓	✓
Inserimento nuovo utente in rubrica direttamente dall'APP	✓	✓
Attivazione	Self-Registration/1-click	1-click
Attivazione con autenticazione a 2 fattori (SMS/E-MAIL)	✓	✓
Supporto Push Notification	✓	✓
Compatibilità terminale GrandStream GXV3275	✓	✓
Localizzazione	Italiano, Inglese, Francese, Tedesco, Spagnolo, Portoghese, Turco, Russo, Arabo	

GRAZIE



Per eventuali informazioni e approfondimenti:

Email:

support@privatewave.com
v.mafrica@bv-tech.it ; vmafrica@progesi.it

Cell.: +39 340 5818242