

## Encrypted VoIP Security

### *Advancing Safe Communications for Digital Voice*

Cost-saving benefits of VoIP come with expensive tradeoffs, including ID spoofing, hijacking, and fraudulent activity against users' credentials, phone numbers, and accounts. VoIP is an easy target of hacker eavesdropping, which feeds on proprietary information, trade secrets, and other critical intelligence.

Data tunnels and VPN constraints often work against productive business process, pushing enterprises to resort to the public Internet.

MerlinCryption's dynamic Embedded Encryption Platform protects against the risks of VOIP-based communication, making collaboration through voice, webinar, and streaming video seamless *and* secure.

Embedded encryption protects over any protocol, protecting the call-signaling packets that set up the call, as well as the media stream that carries the "voice."

### **Key Advantage: Stay Ahead of the Curve**

Other encryption vendors negotiate key exchange with hack-ridden protocols such as SDES or DTLS. MerlinCryption requires *no* key exchange, circumventing MiTM and other key-compromising attacks.

Patented random data generation outputs keys and passwords that are 'generated-used-destroyed-recreated' on demand, making key/password transfer between end points unnecessary. There is no key storage or certificates required. *PKI is eliminated.*

Unlike other encryption vendors, MerlinCryption initiates keys and passwords in varying lengths. Keys and passwords, including their sizes, are determined by the client, and can change from session to session or more often. Keys are scrubbed at the end of the session.

These forward-thinking innovations underscore unpredictability to hackers, and derail attack against the key.

### **Outmaneuver Attack: Dynamic 4-Factor Authentication**

MerlinCryption's dynamic, variable, changeable, smart-authentication empowers VoIP service providers and developers to take control of security. Authentication is typically based on something you know, something you have, and/or something you are. MerlinCryption's embedded encryption platform secures authentication to the next level by incorporating an additional category based on dynamic

"temporary" factors. This unexpected category includes non-linear factors, aptly detecting more subtle attacks. The indomitable power behind this solution is not only in the *number* of factors available, but also in the ability to customize each client with factors that are unique to their business environment. Competing 1- and 2-factor offerings pale to MerlinCryption's 4-factor options.

### TECHNOLOGY HIGHLIGHTS

#### SECURE VOIP COMMUNICATIONS

- *No* VPNs or tunnel necessary
- *No* Key Exchange necessary...*No* PKI
- Works with *any* Communications Protocol
- Embedded, Under-the-Hood Security for Invisible End-User Experience
- Total Protection Across All Layers of Risk

#### TECHNOLOGY SPECS & STATS

- Defeats Cryptanalysis, Phoneme-Parsing, MiTM, and other VoIP attack vectors
- Encryption speed more than twice as fast as AES
- Highly efficient minimal overhead code:
  - Platform = 200K
  - Low Overhead Platform = 55K
  - Encryption Engine as small as 22K
- Portable to any CPU
- Encrypted Payloads transmitted by any communications protocol and on any network
- 1 Patent, 1 Patent pending, multiple patents in process
- Eliminates PKI, Cert Authorities, and Key Depositories

*The Smart-World's Smart-Encryption®*

# Encryption Innovation: *Stealth in Today's Precarious VoIP Environment*

The embedded cryptosystem is fortified with Anti-Statistical Block Encryption (ASBE). No two encryptions are alike: Each encryption process always results in a different cyphertext, even when repeating the same key, password, and plaintext to encrypt. The platform contains special components that dynamically alter the generated data, exponentially increasing security

MerlinCryption Embedded Encryption Platforms defeat Cryptanalysis, Phoneme Parsing, and other VoIP attack vectors to support secure critical infrastructures, PBX, gateways, proxies, registrar and locator servers, and end-points.

*MerlinCryption secures diverse VoIP infrastructures and configurations. Encryption security adapts to any or all interoperable elements and system layers.*



Security Matters	MerlinCryption	Other Solutions
<b>Key Exchange</b>	<b>No Exchange Needed</b>	<b>Use SDES, DTLS &amp; other compromised exchange</b>
<b>Key Length</b>	<b>Variable Keys</b> (changes, as desired by User)	<b>Constant Keys</b> (fixed, as dictated by program)
<b>Key Transmission &amp; Storage</b>	<b>NO Transfer, No Storage, No PKI</b>	<b>Sent &amp; Stored Use PKI</b>
<b>Authentication</b>	<b>4-Factor</b>	<b>None to 2-factor</b>
<b>Attack Vectors</b>	<b>Defeats Cryptanalysis, Phoneme Parsing, MiTM</b>	<b>At Risk</b>

## Game Changers

- ASBE is more than twice as fast as AES
- Encryption engine as small as 22KB, low overhead platform is 55KB, and platform is 200KB.
- Encrypted Payloads are transmitted by *any* communications protocol and on *any* network
- The encryption software is portable to any CPU
- Two Embedded Encryption Platform SDKs streamline easy implementation

### THE SMART-WORLD'S SMART-ENCRYPTION

MerlinCryption develops invincible smart-world solutions that protect VOIP and streaming video against eavesdropping, packet spoofing, masquerading, and hijacking. Leading-edge technology secures dynamic end-to-end encryption for military, government, enterprise, healthcare, financial, and legal industries.

Unprecedented Embedded Encryption Platforms protect data as it is created, viewed, edited, shared, stored, and moved securely across communications channels and through the Cloud.

**MerlinCryption Is Changing The Way The World Protects Data**



PO Box 160284 | Austin TX 78716  
512-348-SAFE  
www.MerlinCryption.com