AT&T Encrypted Mobile Services provides mobility customers with end-to-end security features for confidential and sensitive calls and text messages. AT&T Encrypted Mobile Services transforms standard smartphones into protected communication devices, meeting government grade classifications for Controlled Unclassified Information, and Sensitive But Unclassified, and offering automatic FIPS 140-2 validation and AES-256 encrypted two-way sessions.

Greater Mobile Communications Capability
In today's environment, mobile phones handle voice and text communications that are often sensitive in nature. Breaches of mobile communications can impact a government agency's mission, public safety and security, a firm's stock price, mergers and acquisitions activity, Intellectual Property, cyber security, physical security and executive safety. AT&T Encrypted Mobile Services helps protect mobile communications, utilizing off-the-shelf smartphones.

How it Works: The Hardware Difference
The solution features a powerful hardware and software combination, supporting iOS, Android™, and BlackBerry® devices on the AT&T wireless data network and on Wi-Fi networks. Fully optimized with the AT&T Mobile Network, the combination of TrustChip®, TrustCall®, and TrustText® offers a hardened, two factor encryption solution. The purpose-built TrustChip is a fully hardened, self-contained crypto engine which users simply insert into the smartphone's microSD slot, or which is embedded in a dedicated sleeve for iPhone. The TrustChip can be shipped unbranded and includes an embedded AT&T TrustGroup hardcoded within the chip. The AT&T TrustGroup offers the strength of additional hardware authentication, and also provides potential for encrypted calling interoperability with other interagency AT&T Global TrustGroup users, sharing a common relay server. The TrustChip can be managed over-the-air and serves as a hardware anchor to the TrustCall and TrustText software applications which allow users to easily place and receive secured calls and SMS text messages. They integrate with the phone's standard operation and address book, providing users an intuitive and seamless security option. This on-demand protection delivers mutual authentication and end-to-end encryption for the duration of the call or text session.

Who Should Consider this Solution?
- Government users who communicate CUI (Controlled Unclassified Information)/SBU (Sensitive But Unclassified) information or whose operational success would be more likely if mobile communications could be used to handle CUI/SBU info.
- Government users who must communicate CUI/SBU information when normal operations are disrupted.
- International Travelers: Government and Enterprise Users whose staff or executives travel overseas to locations where “snooping” of cellular traffic may occur.
- Enterprises with business matters requiring a higher level of confidentiality.
- Legal firms handling sensitive information.

Potential Benefits
- Advanced Security Features – Two factor authentication to include both hardware and software encryption
- Global Reach – Increased security through over-the-air access to provide seamless encryption and wireless roaming to over 150 countries.
- Broad Coverage – Not limited by circuit switched data.
- Optimized for Performance on the AT&T Mobile Network.
- Rapid deployment and integration, with hardware to include AT&T TrustGroup.

Features
- Hardware Difference – Combination of hardware and software helps to deliver both strong security and an outstanding user experience.
- Enhanced Power Management – Application remains dormant when not in use so it limits the drain on the devices battery.
- Available for Android, BlackBerry, and iPhone devices from any carrier.

To learn more about AT&T Encrypted Mobile Services, visit www.att.com/critical-communications or have us contact you.
• Healthcare, financial services or other organizations where industry or regulatory policies require additional protection when transmitting sensitive information
• Anyone with additional security needs due to confidential, sensitive mobile calls

AT&T Encrypted Mobile Services Benefits
AT&T Encrypted Mobile Services Benefits include network optimization: the application has been enhanced and specially tuned for performance on the AT&T Mobile Network to reduce latency and set up time. Encryption is available across carriers and offers a two factor authentication, utilizing the hardware-anchored TrustChip coupled with encryption software. Its global reach can operate in more than 150 countries worldwide where AT&T provides data roaming (performance may vary). Its unique enhanced power management capabilities are also important, since the application remains dormant when not in use, so it does not drain the battery. In addition, AT&T Encrypted Mobile Services provide a single source for support and billing. A single monthly feature from AT&T incorporates both client software licensing and service costs, plus provides a single contact for care and billing. Finally, simple, cost effective, protected connectivity!

Optional equipment and services are also available. Data rates apply to Encrypted Mobile voice calls. When using your Encrypted Mobile Services outside the U.S., Puerto Rico, or U.S. Virgin Islands, international roaming rates also apply. Remember – your Encrypted Mobile Services application can use a significant amount of data and international data roaming can get expensive quickly.

For more information contact an AT&T Representative or visit www.att.com/encrypted-mobile-services.

Important Information
General: AT&T Encrypted Mobile Services is available only to enterprise and government customers with a qualified AT&T agreement (“Qualified Agreement”) and their respective CRUs. AT&T Encrypted Mobile Services is subject to the Qualified Agreement, applicable Sales Information, terms and conditions found at http://www.koolspan.com/terms-and-conditions/ (“Additional Product Terms”). For AT&T’s government customers on a Qualified Agreement: Any Additional Product Terms not allowable under applicable law will not apply, and the Qualified Agreement will control in the event of any conflict between the Qualified Agreement and the Additional Product Terms. May not be available for purchase in all sales channels or in all areas. Additional fees, charges, taxes and other restrictions may apply. Offer subject to change.

Encrypted Mobile Services Limitations/911: To make an Encrypted Mobile Services call, the receiving party must also have the Encrypted Mobile Services feature and be included on the CRU’s Encrypted Mobile Services contact list. Encrypted Mobile Services cannot be used to call public services such as 911. To place a 911 call the CRU must exit Encrypted Mobile Services and dial 911 as standard wireless voice call.

Requirements: Technical Information: Eligible voice and data plan and certified Android, iOS or BlackBerry smartphone device equipped with microSD capability are required. Additional hardware, software, services and/or network connection may also be required.

Coverage: Usage/Billing: Availability, security, speed, timeliness, accuracy and reliability of service are not guaranteed. Coverage is not available in all areas. AT&T wireless coverage maps are available at http://www.wireless.att.com/coverageviewer. Wireless service is subject to transmission, terrain, system, capacity and other limitations. AT&T Encrypted Mobile Services incur data usage. Measured usage incurred in connection with Encrypted Mobile Services will be charged as specified in the CRU’s associated voice and/or data plan. When using Encrypted Mobile Services outside the U.S., Puerto Rico, or U.S. Virgin Islands, international roaming rates also apply. Customer may cancel a CRU’s Encrypted Mobile Services at any time. Customer will be billed for all associated CRU voice and data usage up to cancellation of Encrypted Mobile Services.

Wi-Fi: Encrypted Mobile Services may not function on or be compatible with all Wi-Fi networks. Some Wi-Fi networks may not allow the use of the Encrypted Mobile Services. Some Wi-Fi networks may require users to authenticate on the Wi-Fi network before obtaining Wi-Fi access. Customer and its CRUs are responsible for paying any fees that may be required to access a Wi-Fi network. Customer and its CRUs are responsible for complying with the terms of service, acceptable use policies, legal terms and conditions, and similar documents, as applicable, for each Wi-Fi network over which the Encrypted Mobile Services service is used, including AT&T’s Wi-Fi network. Due to the nature of wireless signal propagation, transmission, reflection, diffraction, and degradation, Wi-Fi access may not be available everywhere within a venue with a Wi-Fi network.

Customer Personal Data: Customer Personal Data may be transferred to or accessible by (i) AT&T personnel around the world; (ii) third parties who act on AT&T’s or AT&T’s supplier’s behalf as subcontractors; and (iii) third parties (such as courts, law enforcement or regulatory authorities) where required by law. Customer will only provide or make Customer Personal Data accessible when Customer has the legal authority to do so and for which it has obtained the necessary consents from its end users, and will camouflage or securely encrypt Customer Personal Data in a manner compatible with this offer. As used in this Product Brief, the term Customer Personal Data includes, without limitation, name, phone number, email address, wireless location information or any other information that identifies or could reasonably be used to identify Customer or its end users. Customer is responsible for providing end users with clear notice of AT&T’s and Customer’s collection and use of Customer Personal Data obtained via this offer and for obtaining end user consent to that collection and use. Customer may satisfy its notification requirements as to AT&T by advising end users in writing that AT&T and its suppliers may collect and use Customer Personal Data by providing for end user review the relevant links to the Sales Information that describes the availability of optional goods, content or services and AT&T’s Privacy Policy at http://www.att.com/gen/privacy-policy?pid=2506.

Optional Services: Additional professional services, common relay servers, management and hosted services are optional and may be purchased separately. See applicable materials for details. Additional charges and other restrictions apply.

How Encrypted Mobile Services Users Can Minimize International Data Charges
• Purchase an international data package. An international data package can help significantly reduce the cost of using data abroad. AT&T now offers discount DataConnect Global international packages.

We also offer a discount data package to customers who frequently travel only to Canada or Mexico. See att.com/worldpackages for details, restrictions, terms and conditions.

• Utilize Wi-Fi® instead of 4G/3G/GPRS/EDGE: Wi-Fi is available in many international locations.

Share this with your peers

To learn more about AT&T Encrypted Mobile Services, visit www.att.com/critical-communications or have us contact you.

Scan this code to learn more.

09/04/14 AB-2885-01
© 2014 AT&T Intellectual Property. All rights reserved. AT&T and the AT&T logo are trademarks of AT&T Intellectual Property.