



www.galaxkey.com



SECURE COMMUNICATIONS

For Service Members of the Armed Forces



In the current climate, it is important to maintain communications with friends and family. This is especially important when a service member is deployed abroad and is physically absent from family members for extended periods (weeks, months and even years). This white paper highlights how Galaxkey can help our valued Armed Forces to stay securely connected to their family without compromising data security.

The Challenge

Staying connected with friends and family is important – especially in today’s climate. And this connection becomes paramount for service members who are deployed away from home for extended periods of time - weeks, months and sometimes even years. It has been proven that frequent communications enhance morale for both service members and their families back home. Maintaining connection and remaining involved in each others daily lives helps to provide the much-needed support and strength needed by all parties to keep them thriving. It makes the distance and time spent apart more bearable.

It is often challenging to communicate when deployed abroad particularly under diverse and harsh conditions. Deployments are always different and restrictions on communications vary from one deployment to the next. This places parameters on the conversations that can be had and information that can be communicated - which leads to limited openness of communication. Privacy is fundamental within a family unit and the fear of a lack of privacy and security also limits communications from both sides. Adding to this complex situation, working conditions of those deployed service members can be highly sensitive.

Moreover, due to the extended timeframe in which some service members find themselves away from home, it is often the case that they need a means to communicate securely with, and send information to, family members back home (and vice versa). There are times where privacy and security are essential for matters to be communicated and resolved efficiently.

Technology Improvements

Times have changed and technology has improved the manner in which service members can stay in contact with their families.

Sending letters and parcels is still an option but it's not the only way. In the current era, communication usually takes place over email, video, phone, social media and instant messaging.

The methods of communication accessible are dependent on the deployment type and on which communications are allowed.



Phoning home may not always be possible and when it is, is likely to be a costly option.



Social media may be prohibited for certain deployments.



Email is a reliable option and a form of communication that is frequently used, and often service members choose to take their own laptops and devices to use. However, internet access may only be available publicly (for example at home-base or an internet café) and with varying degrees of reliability. Because of this reliance on public connections, security is lacking.

These advancements in technology have offered multiple ways to stay in touch, however, none are guaranteed secure ways to communicate. The data communicated is handled in diverse ways and treated with wide-ranging levels of privacy and security. However, further advancements are now enabling communications in situations like these to be secure and private too.

Family and Operational Security

Service members and their loved ones should be able to communicate openly and be safe in the knowledge that their communications are as secure and private as can be.












Service members and their families should feel assured that their communications are reliable, confidential and protected, and that they remain private - only being seen by those intended.

Deployments abroad are never the same. Countries differ with each deployment. Service members and their families need to be assured that no matter the country of deployment, their secure communication will be unaffected and that their information will remain secured and governed in a country of their choice that they have confidence in.

It is a given that the safety of service members is prioritised when working under deployed conditions, and communications is a means where compromise could occur - with detrimental ramifications to operational security. Secure communications for service members and families should be supported to ensure communications are maintained as well as the confidentiality of information and thus operational security.

The Operational Security Challenges Faced

Geographical location, remoteness, facilities, devices, compliance issues and criminal activity are all challenging the communications of service members when deployed abroad. There are consequently operational challenges for those responsible for ensuring the ongoing safety of those service members who need to understand that:

-  The data is highly valuable
-  The data can be highly sensitive and may be personally identifiable
-  The risk of attack is high, as the adversary is aware of the high value attributed to the data
-  Operational sensitivity is high
-  It is challenging to manage communications
-  It is challenging to manage the type of data being communicated
-  A variety of personal devices and laptops may be used
-  Mobile and remote manner of functioning is on the rise
-  Geographic locations of deployment are always different
-  Facilities of deployment are always different
-  Limited IT budgets impose constraints when trying to ensure a good security posture is achieved by all

The Challenging environment

The environment is one that is challenging to secure. Service members deployed abroad communicate with families back home in a multiple of ways. This is often dependent on the deployment and the mission as well as the available facilities at the time of deployment. Restrictions may also apply.

Communications that are not secured and not properly managed may present potential security risk.

A balance needs to be achieved between operational sensitivity and safety, and private and reliable communications for service members and their families.

Data misuse, compromise and theft

Lack of operational security is detrimental to the mission as well as the safety of service members and civilians.

Communications and data can be used by adversaries for malicious purposes. Photographs or details pertaining to the deployment and mission that are communicated insecurely (linking the location for example) could jeopardise operational security.

Service members and family members regularly communicate data via email (back and forth) including: photographs, documents and accounts of everyday

On a more personal level, service members abroad, being away from home for extended periods, may need to communicate sensitive, personal data with family members back home. This data can potentially be compromised if not communicated securely.

Mobility, cloud and remote functioning

Service members often take their own devices on deployment to have a guaranteed method of communication with family members back home.

By this very nature, this means that devices are not uniform. Furthermore, the devices used by family members back home are also diverse and many. Moreover, many choose to store their data in the cloud or share it in a manner that utilises cloud services. The adoption of mobile device usage is also on the rise. Cloud platform utilisation is becoming common practice and this growing trend expands the security risk and the attack vector.

Data communicated is shared and stored across an array of devices: desktop computers, laptops, mobile devices, as well as in the cloud. There is also the risk of devices being misplaced, lost and/or stolen. The data communicated is challenging to manage and to control access to.

Data traversing geographical boundaries

Deployment locations are always different. Furthermore, family members are more likely than not to be located elsewhere.

Data is traversing boundaries - physical, virtual and geographical. All these are potential areas of security risk. Data crossing geographical boundaries brings its own set of unique challenges. Potential access by foreign entities, who have free rein to access data assets, due to binding laws within certain jurisdictions, is a growing concern. A lack of security with regards to who has access to data and can infiltrate the communications is high. The location of the data will determine the laws that will govern that data.

How Galaxkey can help

The challenges faced point directly to data security, and by securing this valuable data many of these challenges can be met.

The main concerns involve securing data (in all its forms), managing access to data, conforming to strict data regulations for data privacy and security, and achieving this within a varied and mobile environment that crosses all boundaries physical, virtual and geographical. Service members require a reliable, private and secure means to communicate whilst operational security must be maintained. The confidentiality, integrity and availability of communications and data created, sent, received and stored must be achieved. Through effectively securing these communications, potential threats to the security and integrity of the information is prevented. Moreover, accidental disclosure of sensitive data is thwarted and thus operational security maintained whilst communications remain best supported.

Galaxkey addresses these challenges:



SECURE ACCESS CONTROL



DATA SECURITY
email, documents, cloud data, removable media and transfer systems



COMPLIANCE



MOBILE AND MULTIFACETED ENVIRONMENT



SUPPORTS ALL POPULAR DEVICES
and all internet connected platforms

WHAT DOES GALAXKEY SECURE



Galaxkey secures entire data content: email, documents, cloud data, removable media and transfer systems (in any file and in any format), regardless of the recipient, external party or third party. Achieving the same level of security whether communicating internally or to an external party.

Moreover, Galaxkey works on all mobile device platforms and through web access.

GALAXKEY IS AN INNOVATIVE AND FLEXIBLE SOLUTION



Galaxkey integrates seamlessly within any existing framework and works on all devices and platforms on premise and in the cloud. It provides complete platform and mobile support and is highly scalable.

Galaxkey lets the Armed Forces maintain sole rights to their encryption keys alleviating any concerns of third party access to their data.

Galaxkey has no backdoors, thus foreign entities are unable to gain access to the encrypted data. The data remains the sole asset of the organisation.

SECURE NO MATTER THE LOCATION



Galaxkey offers a geo-fencing feature (Geofence) whereby the user can ensure that their data resides in the country of their choice and under the jurisdiction that they choose. The user gains comfort from always knowing exactly where their data is and this safeguards against foreign entities potentially gaining rights to the data (if it were stored within a foreign jurisdiction).

The user can be confident in knowing the laws that govern their data by choosing a jurisdiction that they are comfortable with.

SECURE DATA AND ACCESS CONTROL



Galaxkey is designed to secure data within sensitive environments in a manner that is easily integrated into the existing operations and is easily managed.

The identity-based encryption solution achieves exceptional data security and access control while alleviating any convoluted key management concerns. Additionally, complete key control remains with the Armed Forces. The solution offers an automated key management system, easing any key management complexities. The identities are secured with user provided credentials, ensuring secure user access only.

The encrypted data remains the asset of the Armed Forces at all times, wherever it is transmitted or stored. The solution, user access and the data can be easily managed via centralised control.

ENCRYPTING DATA AFTER CLASSIFICATION



Through the use of classification systems, Galaxkey is able to encrypt on policy once an email or file has been classified. Thereby making it easier to ensure data is protected.

Galaxkey ensures the data is encrypted and access is controlled at creation, adding security.

GALAXKEY AIDS COMPLIANCE



Galaxkey contributes to the achievement of privacy and regulatory security compliance and the solution is compliant with the government standard. Data is managed through audited access, ensuring compliance.

Conclusion

Much emphasis is placed on data security. Where such an abundance of valuable and sensitive data exists, the opportunity for attack is heightened and the security risk enhanced. Threats to sensitive data have reached a critical point and the sophistication and frequency of attacks are escalating.

Like other industries, The Armed Forces continues to transition to a more electronic and mobile environment, in which service members can sustain contact with their family members back home. The security challenges and risks to both operational security and personal service members' security through communications must be addressed to ensure that data is always secure.

It is in the Armed Forces best interest to ensure that their service members are getting the support that they require to ensure that their communications are always secure and that the valuable data asset is properly secured. This is essential in sustaining operational security for optimal quality and safety whilst reducing the probability of risk to sensitive data.

About Serbus



Formed in 2010, Serbus are specialists in secure communications, data and personnel security

“Securing the remote worker”, with secure communications, was born out of the recognition that business continues no matter where in the world you and your team may be. Have you sent that vital email or message before you board your flight? Did you use the public hotspot? Who else was listening?

Serbus Secure is the answer to continuing your business in a secure manner.

Our expertise in commercial and defence secure communications, combined with operational experience, enables our clients to operate safely and securely in remote and hostile environments worldwide.

Serbus draw upon the extensive military and commercial experience of its team, ensuring the quality services are delivered in a well considered and professional manner.

Our team are selected predominantly from UK Special Forces (land and maritime) and include:

- Security consultants and instructors
- Specialist communications consultants
- Information security consultants

Appropriate staff hold security clearances (SC / DV)

About Galaxkey

Galaxkey is a UK based company that provides an easy to use encryption platform for files and emails. Galaxkey provides the flexibility for either cloud or on-site management of encrypted data and keys.

Partnering with a Global leader (Thales) in the key management sector, Galaxkey are able to provide a high assurance encryption platform, underpinned with government and banking grade encryption processes. This ensures compliance and security best practices for any organisation.

Using Galaxkey, organisations and users are able to secure data at the click of a button- this includes emails, files on FTP servers, end points and cloud storage, to name a few. Galaxkey can be used to secure data and control access to data regardless of its location.

For more information:

www.galaxkey.com
+44 (0) 333 150 6660
info@galaxkey.com

Galaxkey Ltd, 2 Falcon Gate, Shire Park, Welwyn Garden City,
Hertfordshire, AL7 1TW