www.galaxkey.com

GALAXKEY SECURITY

Technical white paper

galaxkey®

www.galaxkey.com

Contents

1 Introduction

The security strategy of an enterprise or an individual is usually multi-pronged having various security measures at different places of vulnerability. But at the heart of it, the most important element that needs to be secured is “Data”. Galaxkey helps customers take care of the security of data in the organisation using its state of the art, validated technology.

While security and usability are always at loggerheads with each other, Galaxkey makes sure that security is not compromised at any time while providing the best user experience. Security remains the primary focus throughout the life cycle of product management. This helps Galaxkey deliver the best security product that satisfies customer requirements by taking care of Confidentiality, Availability and Integrity.

This document provides details of the overall Galaxkey approach to security in design as well as deployment of the solution. The details are provided in following main sections:

GALAXKEY OFFERING AND ARCHITECTURE:
Provides overview of the Galaxkey offering and details of Galaxkey Architecture along with deployment types.

COMPONENTS AND THEIR SECURITY:
Lists some of the major components of the Galaxkey architecture and gives details of the security involved.

GALAXKEY STANDARDS AND CERTIFICATIONS:
Gives details of the standards used by the Galaxkey offering and technical security details.

GALAXKEY ARCHITECTURE

2.0

2.1 Galaxkey Solution

Galaxkey is an Identity based security solution that offers the following features to an enterprise or individual.

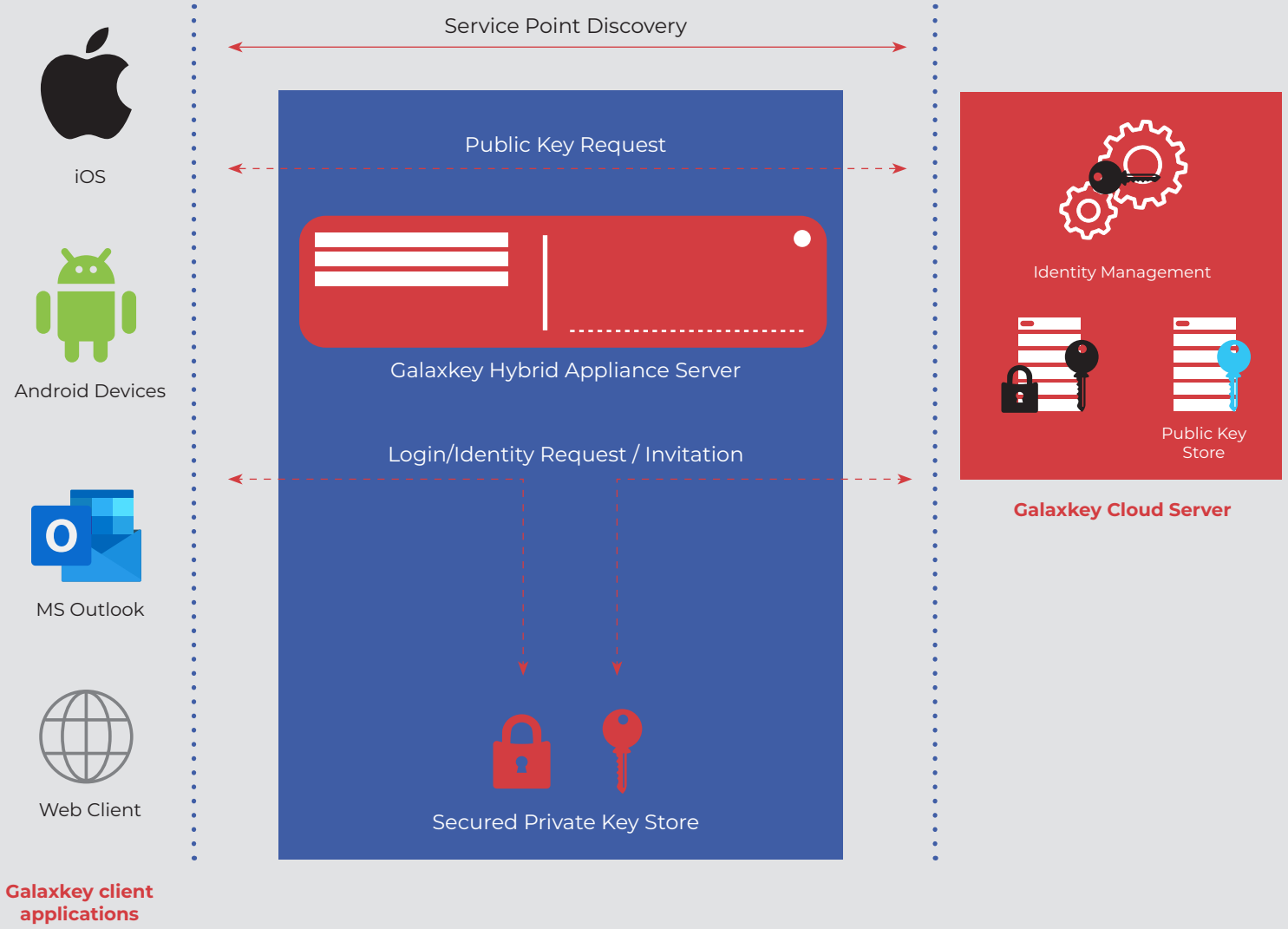
SECURE EMAIL COMMUNICATION:
Galaxkey provides end-to-end email security to its registered users. Email is secured for legitimate recipients and the sender before it is even handed over to the email server for delivery. The email remains secured throughout its transport and even when it reaches the recipient. Based on the security needs of the enterprise, the email security can be end-to-end or Gateway based.

SECURE COLLABORATION USING WORKSPACES:
Galaxkey provides a secure platform to collaborate with anyone and anywhere in the world. The platform also offers detailed access rights and other configurations to support the security needs of enterprise file sharing.

SECURE DOCUMENTS:
Galaxkey allows users to secure their document locally on demand or automatically based on the document location.

Galaxkey has a single identity associated with an email address that takes care of all the data security for that individual on all platforms. Galaxkey does the complete key lifecycle management for a user in the background. This allows the user to focus on their task at hand rather than worrying about the security of the data.

2.2 Galaxkey Architecture



2.2 Galaxkey Architecture

The Galaxkey solution consists of the following major components:

1. Galaxkey Server: This is the server component of the solution responsible for managing accounts and identities. This server provides the following functionality:

a. Self-service interface for identity
b. Corporate identities lifecycle and configuration management.
c. Access to audit logs and customisation templates.
d. Web access to Secured emails, Documents and Workspaces.
e. Web services for clients for key exchange.

---

2. Galaxkey Key and Data Store: This is the secure store used for storing the following data:

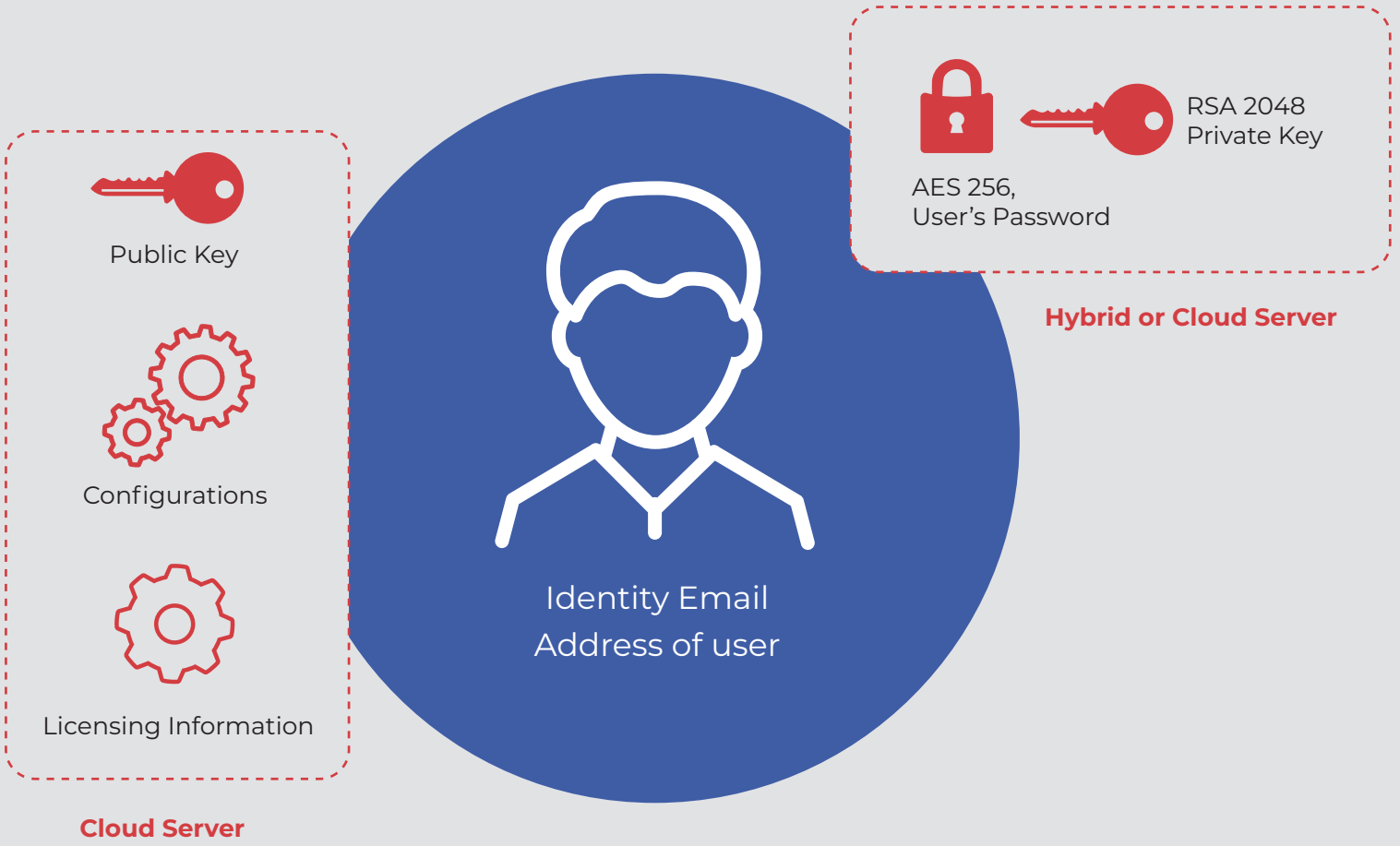
a. User keys
b. User secured emails sent, to make them available on Web access for no installation recipients.
c. Workspace files and folders for sharing with other users.

---

3. Galaxkey Client Application: Galaxkey clients are different end user applications that help the user achieve the email / data security tasks seamlessly. Some of the major client applications are:

a. Galaxkey Add-in for Microsoft Outlook: Used for sending and opening Galaxkey secured email from within Microsoft Outlook for Windows applications.
b. Galaxkey For Windows: Used for securing data on a windows desktop computer on demand or automatically using Galaxkey Vault.
c. Galaxkey Web Access: Zero installation web interface option for doing almost all activities within Galaxkey including Workspaces.
d. Galaxkey iOS: Galaxkey application for Apple mobile devices such as iPhone and iPad.
e. Galaxkey Android: Galaxkey application for mobile devices with Android operating system.
f. Galaxkey for OSX: Galaxkey application for Mac devices.

2.3 Galaxkey Identity



2.3 Galaxkey Identity

At the heart of the solution is Galaxkey Identity.
Galaxkey identity is made of the following components:

1. Keys: Each identity has a pair of keys for encryption (Public Key) and decryption (Private Key).
2. Configurations: Each identity has an associated configuration that allows or does not allow the user to perform various tasks. Configurations are managed by the corporate administrator in the case of a corporate account.
3. Licensing: A license is associated with an identity that decides the validity. Free users have perpetual validity with very limited functionality.

2.4 Security of the Galaxkey Identity:

Since Identity is the most vital aspect of the Galaxkey security, it is secured with the following mechanisms.

1. Keys are RSA 2048 Private and Public key pair.
2. The generated keys are secured using a derivative of the user password.
3. The password is not stored by Galaxkey, so ultimate control is with the end user.
4. Keys are always secured until they are needed to actually decrypt data.
5. Keys are always decrypted within the client application in ephemeral memory.
6. Access to the key is protected using multifactor authentication.
7. Galaxkey also allows “Yoti” based authentication which is a guarantee of identity verification of a user.
8. For password resets, we store a copy of keys secured using a derivative of the corporate administrator password.
   So, when the user forgets the password, the corporate admin can login and reset using his copy of the key. The actual password of the user is not stored.
9. Keys are stored in secured storage (See the following sections for details of key storage).

SECURITY OF GALAXKEY COMPONENTS

3.0

3.1 Galaxkey Deployment modes

The Galaxkey solution is designed, built, deployed, monitored and maintained with security as its prime focus. With its flexible deployment options, Galaxkey can cater to all sizes and types of customers ranging from an individual free customer to a multinational enterprise.

Based on the security and budgetary appetite of the enterprise, Galaxkey can be deployed in two modes:

1. Galaxkey full cloud mode: This is a hassle free, ready to use corporate account setup. There is no onsite setup involved in this and the user just needs to create a corporate account in the cloud. All the identities are managed by the Galaxkey cloud instance. This is an ideal solution for any corporate that has all of its services managed in the cloud.
2. Galaxkey Hybrid mode: This is the most secured option for an enterprise. In this mode, a Galaxkey virtual appliance is setup within the customer infrastructure with keys and data stored within that infrastructure itself. Galaxkey cloud is used only for managing licenses and configurations for corporate accounts.

Based on the deployment mode, the security of the Galaxkey server is taken care of either by Galaxkey or shared by the customer infrastructure team. We will take a look at both the aspects in the coming section.

3.2 Galaxkey Server (Cloud)

Galaxkey Cloud Server is responsible for managing cloud corporate accounts as well as free user individual accounts. As a cloud provider of platform, Galaxkey is responsible for managing security of the platform including the underlying infrastructure.

3.2.1 Infrastructure Security

Galaxkey, after careful consideration related to security, robustness and flexibility available decided to use Amazon AWS for its cloud instance hosting. Galaxkey leverages AWS infrastructure and native security and adds its security control over the service layer.

PHYSICAL SECURITY:

Galaxkey leverages Amazon AWS physical security for access to its physical servers. AWS data centers are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building entry points by professional security staff utilizing video surveillance, state-of-the-art intrusion detection systems, and other electronic means.

INSTANCE LEVEL SECURITY:

Galaxkey customizes its AWS Elastic Cloud Compute (EC2) instances and its Virtual Private Cloud (VPC) infrastructure to ensure security is maintained on multiple levels:

The virtual instance operating system or guest OS: Access to management of virtual instance requires multifactor authentication. All the accesses to the instance are logged and audited. Access to the administrative password is guarded using a certificate pair available only to authorised personnel. The virtual instance itself is locked down and completely controlled by Galaxkey.

The firewall: Galaxkey customises firewall configuration to allow only ports open that are necessary for providing the service, all other ports are disabled.

Secure isolation is also maintained at the instance level, and Galaxkey leverages AWS' Availability Zones to improve the service availability.

NETWORK SECURITY:

Galaxkey leverages the network security provided by AWS to mitigate the following threats

1. Distributed denial of service (DDoS) attack
2. Man in the middle attack (MITM)
3. IP spoofing
4. Port Scanning
5. Packet sniffing.

Galaxkey adds its own service level security measures that compliment the AWS provided security as follows:

a. All the communication to and from the Galaxkey server is over HTTPS with strong encryption algorithm and keys.
b. All sensitive data sent and received is encrypted in transport.
c. Connections use strong encryption algorithms such as TLS v1.2

AVAILABILITY AND MONITORING:

Each server in the Galaxkey environment is monitored for machine health metrics to track availability. These metrics include standard items such as network connectivity, CPU utilization, memory utilization, storage utilization, service status. Failures generate alerts that are pushed to the operational staff through prioritized channels.

3.3 Galaxkey Virtual Appliance (Hybrid)

In the hybrid mode deployment, Galaxkey installs a virtual appliance server in the customer infrastructure. The security of the server and network security of the appliance is managed as per the infrastructure and security strategy of the customer. Galaxkey recommends various security measures so that the high standard of security is maintained at the same level as the cloud server.

Galaxkey recommends the following:

1. Galaxkey appliance should be set in the DMZ.
2. The firewall should only open ports needed by Galaxkey.
3. Customers secure https traffic by providing SSL certificate with strong key (2048 RSA)
4. Network communication should be encrypted using TLSv1.2.
5. Physical and instance access to the server should be restricted to authorized personnel only and access should be audited.
6. High availability setup should be done to make sure the service is available.
7. Appropriate measures are in place to handle network attacks.
8. Server Guest OS is patched and updated to the latest version.
9. Server should be added as a critical resource to their monitoring system so that appropriate alarms are raised in case of fault and failure.
10. Galaxkey encourages clients to carry out independent Penetration testing regularly.

On top of the recommended policy, Galaxkey also gets notified by the appliance in case there is a service level issue. If the issue is related to the network or infrastructure, Galaxkey immediately alerts the customer contact to take appropriate action to fix it.

3.4 Galaxkey Key and Data storage (Cloud)

Galaxkey stores the following data for cloud customers to support its application

1. Identity Keys.
2. Identity Configurations.
3. Emails sent using Galaxkey platform.
4. Files and folders shared using Galaxkey Workspace.

3.4.1 Identity Keys storage and security

Identity keys are stored by Galaxkey in an instance of secured database in Amazon RDS.

In addition to security leveraged by Amazon, the access to the database is secured using the following measures:

1. Access to the database is strictly with authorization.
2. Access to the database is IP restricted so that only the application server can access it.
3. The database encryption is enabled which secures data at rest.
4. RDS instance is clustered for high availability.
5. On top of this security, the keys themselves are secured using a derivative of user's password as a symmetric key and stored in the database. The user password is not stored.
6. Public keys are also encrypted before storing in the database.

Identity configuration are also stored in a secure but different database in RDS.

3.4.2 Emails

Emails sent using Galaxkey secured platform are secured in Galaxkey's proprietary CPA certified file format ".gxk".

The email sending is end-to-end secured. The GXK is created using the recipient's identity when the email is sent. Once the email is sent, the GXK file associated is stored so that email can be accessed on a web portal without installing any client application.
The sent item GXK for cloud customers and individual users is stored in in Amazon S3. Access to S3 Bucket is restricted by authenticated user. Galaxkey, being a closed system does not expose any access to S3 bucket from any interface.

3.4.3 File and Folders for Workspace

Galaxkey allows its users to securely collaborate and share documents using its collaboration platform "Workspace".

For cloud customers, the data shared is stored in Amazon FSx storage. FSx is highly available and backed up storage provided by Amazon AWS with all of its intrinsic security measures in place.

Galaxkey manages security of data with the following controls:

1. The data is always stored secured for intended recipients in .gxk format. The securing is done using the identity of the owner and users with whom the file is shared.
2. Access to the share is restricted based on IP.
3. Only the required port is opened to give access to data.
4. Data is regularly backed up and is available as highly available network share.

3.5 Galaxkey Client Applications

Galaxkey supports securing and accessing secured data on a variety of platforms using its native client applications.

Galaxkey makes sure security of the applications using the following measures:

1. Galaxkey For Windows / Galaxkey Add-in:

a. Application is obfuscated after build to make it difficult to reverse engineer.

b. Application is signed using a signing certificate.

c. All the components used are strong named.

d. SHA 256 Hash of the installable is provided on downloads page.

e. Tampered installable fails.

f. All the communication with server is encrypted and over https.

g. The identity keys are stored secured in memory unless required for decrypting.

h. Cached identities are stored in user's profile in a secured format.

2. Galaxkey Device clients (iOS, Mac, Android):

a. Device clients are distributed only from official app stores.

b. Device applications are properly reviewed and signed using application certificate provided by the platform.

c. For best security, all client applications are developed using native code.

d. All the communication with the server is encrypted and over https.

e. The identity keys are stored secured in memory unless required for decrypting.

f. Cached identities are stored in the user profile in a secured format.

GXK FILE FORMAT

4.0

4.0 GXK File Format

Galaxkey stores secured files in a proprietary file format with extension ".gxk".

GXK file format makes use of both Symmetric and Asymmetric encryption to get the high speed and high security encryption.

Following are silent features of the CPA certified file format.

1. Uses RSA 2048 public keys and AES 256 symmetric key to secure data.
2. Each document / email gets secured using a random AES 256 key.
3. AES 256 Symmetric key is in turn secured using recipients public key.
4. File format open to changes and can accommodate any future changes to encryption algorithm required.
5. File format has self-integrity check and decryption fails if file is tampered with.
6. File format is cross platform and is supported on all Galaxkey client applications.
7. File format secures whole file / email and not its parts thus making it immune to the sort of attacks that can happen on S/MIME.

GXK file format has gone through extensive pen-testing and scrutiny for CPA and has obtained CPA certification through the National Cyber Security Centre (NCSC).

Galaxkey uses the recommended and standard encryption algorithms for Official communication. All algorithms used by Galaxkey are FIPS compatible

GALAXKEY STANDARDS

5.0

Federal Information Processing Standards (FIPS) is standardization developed by the US federal government for use in computer systems by all non-military government agencies and government contractors. Under the FIPS heading there are many standards defined by the US government such as Personal Identity Verification (201), Minimum security requirement for Federal Information (200). The standard of interest in Galaxkey context is FIPS 140.

5.1 FIPS Standards in Galaxkey

Advanced encryption standard (AES): AES used in Galaxkey for symmetric encryption is fully FIPS compliant under publication FIPS 197 (Certificate number: 1168). Galaxkey uses 256 as its key size for encryption.

RSA: RSA algorithm libraries used in Galaxkey for asymmetric encryption is also fully FIPS compliant under publication FIPS 186-2 (Certificate number: 560). Galaxkey uses 2048 as its key size for RSA.

Secure Hash Algorithm (SHA): SHA algorithm used in Galaxkey is FIPS compliant under publication FIPS 180-3 (Certificate number:1081). Galaxkey SHA 512 for its hashing.

5.2 Other Standards

TLSv1.2: All the communication between Galaxkey clients and server are secured using TLS v1.2 which is the latest protocol as of now for secure communication.

Simple object access protocol (SOAP): Galaxkey uses SOAP for its communication with server. SOAP is widely accepted as a standard for communication with a webservice. The SOAP communication over TLSv1.2 makes the communication very secure.

As a security platform, Galaxkey has gone through rigorous testing through certification process to make sure its offering is validated by the best authorities in the region.

GALAXKEY CERTIFICATIONS

6.1 Commercial Product Assurance (CPA) by NCSC UK

Commercial Product Assurance is the certification given by National Cyber Security Centre (NCSC) UK. NCSC is the regulatory authority that certifies a product to be suitable to be purchased by public sector or governmental organisations.

CPA certification is a thorough process of evaluation that checks not only the application for vulnerabilities but also the associated build process. Following are details of the testing methodology in a nutshell:

The evaluation process takes place in 3 stages:

1. Build Process Validation: Build process validation evaluates the processes and security controls in place for making sure the organisation has taken care of security at every step of the software development and distribution. NCSC has comprehensive requirements for build process validation that checks the following aspects:

a. Physical security of the premises and infrastructure in which software is developed.
b. Personnel security responsible for development and management.
c. Source code control and its security.
d. Build process and its ability to trace changes.
e. Change management.
f. Defect management.
g. Support process.
h. Client communication and providing updates.
i. Risk assessment and management.
j. Disaster Recovery and Continuity management

6.1 Commercial Product Assurance (CPA) by NCSC UK

2. Assurance Plan: Assurance plan outlines details of how Development, Verification and Deployment risks are mitigated in a product. It gives details of how they can be evaluated in given products documentation, testing and deployment recommendations. This is a comprehensive document submitted to NCSC that forms the basis for evaluation of the product. The plan includes open ended Fuzzy testing of protocols along with functional and encryption testing.

3. Evaluation testing: This is actual testing of the product as per the assurance plan. If any of the tests fail, the CPA is rejected. Galaxkey is proud to say that it has got CPA certification for its most vital components:

1. GXK file format.
2. Communication with server from client.
3. Galaxkey Outlook Add-in.

6.2 Other Certifications / Testing.

Galaxkey has also gone through various other certifications and testing such as:

1. Cyber Essentials certification for its development centre in UK.
2. Pen Testing for Galaxkey for Windows by BSI.
3. NCSC Web Check for Galaxkey Workspaces. (https://www.ncsc.gov.uk/information/web-check)

HELPFUL LINKS

7.0

7.0 Helpful Links

1. **CPA evaluation process details:**
   https://www.ncsc.gov.uk/files/CPA-Process_for_performing_foundation_grade_evaluations_2-5.pdf

2. **Galaxkey CPA Listing:**
   https://www.ncsc.gov.uk/products/galaxkey

3. **FIPS details:**

a. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
b. http://technet.microsoft.com/en-us/library/cc750357.aspx
c. http://csrc.nist.gov/publications/fips/archive/fips186-2/fips186-2.pdf
d. http://csrc.nist.gov/publications/fips/fips180-3/fips180-3_final.pdf

4. **Galaxkey Support:**
   https://support.galaxkey.com
   email: support@galaxkey.com