White Paper

Making Mobile Data a Reality

Brand 'Apollo' Mobile Data Security

Complete Wireless Data Protection including encryption features and endpoint data security

Brand Communications provides secure seamless mobility solutions including endpoint data security and encryption features and provides organisations with first class defence security. Brand ensures a secure means for accessing a private network and transferring sensitive data over public IP networks by employing authentication, data encryption and connection recovery.

White Paper Revision 2.1.1

BRAND COMMUNICATIONS

Trinity House, Ermine Business Park, Huntingdon,
Cambridgeshire, PE29 6XY, United Kingdom

Tel: +44 (0)1480 442100 Fax: +44 (0)1480 442153
http://www.brandcomms.com info@brandcomms.com

Table of Contents

Introduction

Meeting the Security Challenge

The next generation of mobile technology and mobility devices is now upon us. Mobility devices such as laptops, PDA's and Smart Phones are enabling mobile professionals access to e-mail, internet and mission critical applications anywhere at anytime. Mobile Data represents one of the most exciting opportunities for organisations to improve productivity and efficiency.

With more and more organisations rolling out mobile data solutions to their workforces, a major part of the mobile strategy should be to address the security of the systems and consider how the data will be protected over the mobile networks. Organisations are seeing more sensitive business critical data travelling with employees wherever they go and being accessed on laptops, handhelds, smartphones and removal storage devices such as USB devices.

Recently we have seen many press headlines such as "Data Fiasco leaves firms facing loss of contracts" and "Home Office has lost 43 laptops" which highlight the security risks posed by remote workers and data devices out in the field and proves that organisations cannot afford any possible infringement to their corporate data security.

Failure to protect sensitive and personal information on mobile devices can have serious consequences for the enterprise, including legal - under the Data Protection Act and also faced with increasing risks and costs associated with data losses, business compromises and the misuse of data. Companies also need to remember the loss of business reputation which can have a very damaging effect and can be a public embarrassment.

In this white paper, we explore the different security risks that must be recognised when deploying a mobile data solution and what can be put in place to safeguard your privileged data outside the organisations secure environment.

Information Commissioners Office (ICO) Official Guidance

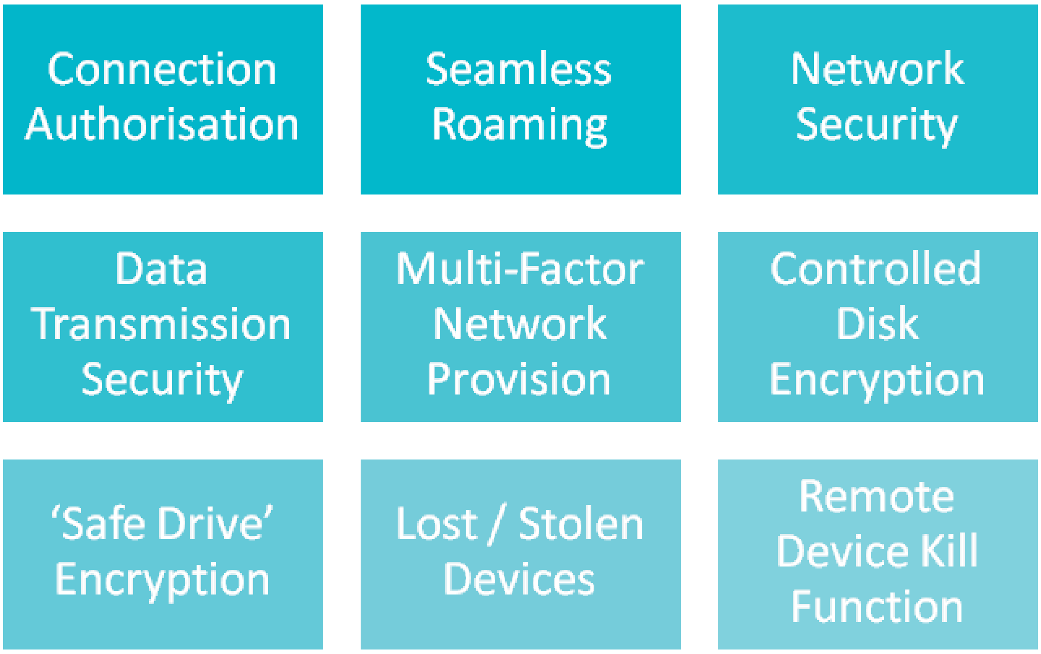
There have been a number of reports recently of laptop computers containing personal information which have been stolen from vehicles, dwellings or left in inappropriate places without being protected adequately. The Information Commissioner has formed the view that in future, where such losses occur and where encryption software has not been used to protect the data enforcement action will be pursued.

The ICO recommends that portable and mobile devices including magnetic media, used to store and transmit personal information, the loss of which could cause damage or distress to individuals, should be protected using approved encryption software which is designed to guard against the compromise of information.

Mobile Security Examined

Protecting company data requires many different issues being addressed and procedures put in place to reduce the risks. It is vital when designing your mobile system that security features are utilised and that the overall architecture of the system compliments those features. In doing so, a scaleable, secure and feature-rich platform can be built that is also simple to operate from both the user and administrator perspectives.

Mobile security generally includes the following areas:



Connection Authorisation

Seamless Roaming

Network Security

Data Transmission Security

Multi-Factor Network Provision

Controlled Disk Encryption

'Safe Drive' Encryption

Lost / Stolen Devices

Remote Device Kill Function

Solving the Security Challenge

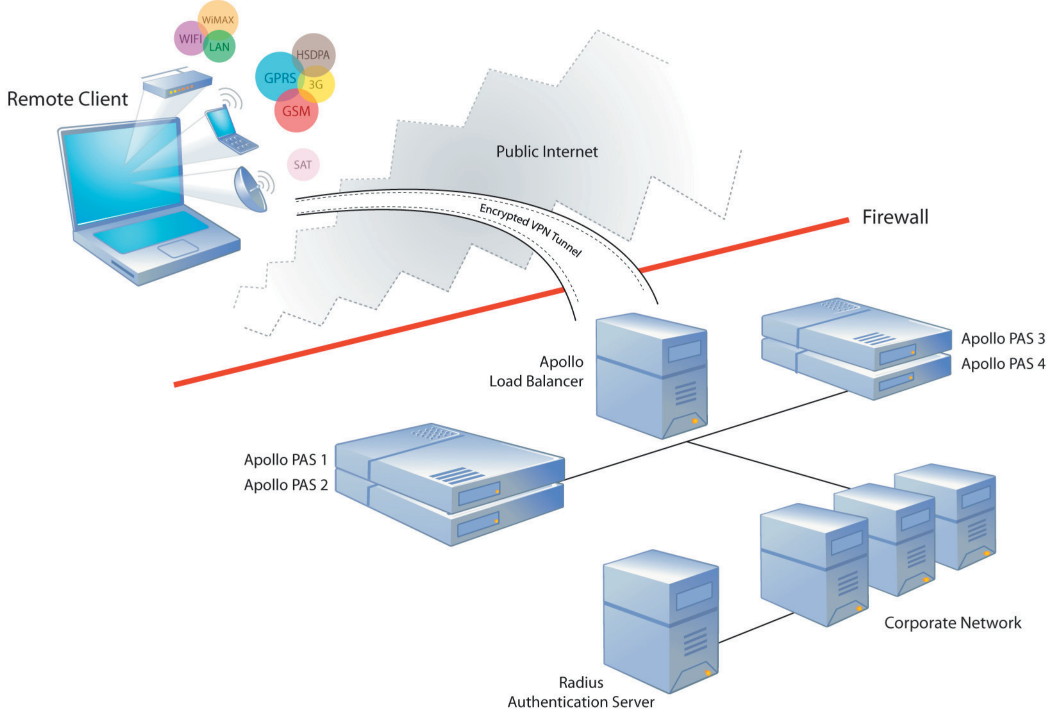
With Brand 'Apollo Anywhere' Secure Seamless Mobility

Security is greatly enhanced by Apollo. Brand's Apollo solutions transparently extend the LAN environment to any mobile device such as laptops, PDA's and other wireless devices, providing real time secure and reliable wireless connectivity for the mobile user, including endpoint data security and encryption features.

The Apollo solution is a remote access software, client server product, which provides a secure means for accessing a private network and transferring of sensitive data over public IP networks. The solution performs VPN IP encapsulation using L2TP protocol. Each client session establishes a unique Tunnel ID and Session ID which are used for traffic routing to a specific client. Beyond the L2TP layer we employ authentication, data encryption and compression protocols. Access to a private network will only be granted once authentication against an authentication server has been successful. Apollo makes the corporate network more secure and is renowned for it's ease of use.

Brand's Apollo also allows IT administrators to control and secure all mobility devices from a central position and takes the onus away from the employee. This gives complete management of the system and helps with user registrations, policy administration, system auditing and reporting, data encryption and recovery.

Figure 1 - Apollo Mobile Security Architecture



Connection Authorisation

Including Enhanced Security and Tunnelling

Access control is one of the most important factors of mobile data security. The ability to prevent unauthorised access is a definite 'must have' to any organisation implementing a mobile data strategy. The Apollo Server is the termination point / gateway for the VPN tunnels created by each of the client machines and handles the management of any tunnels that are linking to the corporate network.

Logging On

Most commonly when logging on, the user is presented with a login box requesting their user name and password. This user name and password would of been assigned by the network administrator. These user credentials are then checked with the Apollo Server to ensure that they are an authorised user. The user name and password are then checked during the VPN login process with the RADIUS (Remote Authentication Dial In User Service) server and also if required RSA SecurID (a Token Authentication System), other one time token passwords, domain server, directories or LDAP. Most VPNs use a common key taken from the network access server to secure their encryption, Apollo does not do this by instead uses a unique key for every user and every session with nothing passed in clear text. This makes the Apollo solution much stronger than other industry VPNs.

Another unique security feature of the Apollo system when logging on is the MAC address. By checking the MAC address with the Calling Station ID, the IT administrator is able to control a user by username and password and also MAC address (device). This allows the administrator to allow users to log in on any device or only specific devices.

Smartcards can also be used as part of the login process. Smartcards offer a high level of security by using certificates to authenticate the user's details against the corporate certificate server.

Apollo is also an extremely strong firewall and unlike other packet products has a RADIUS client to access the secure side of the network where the authentication server resides in a similar manner to switched circuit products. Most packet architectures require a hole in the firewall to allow the remote user to reach the authentication server at times when he hasn't been authenticated - which is a security risk. Using the RADIUS client, Apollo always has an absolute boundary that no un-authenticated packet can transverse, which ensures a much more secure environment.

Additional security procedures can also be added once the user is connected by requesting logins to the company network or domain and the application server if required.

Mac Address

Brand supplies all clients with a serial number. Within the serial number is encoded a MAC address, a globally unique identifier used within Ethernet routing to identify a network node. The Apollo Server checks the MAC address for uniqueness during the initial stages of a logon attempt. The client session which is logging in will only be granted access to the next stage of login if the MAC address is unique to the logon session on the Apollo Server. If the server has another client session using the same MAC address then both sessions will be terminated. This system avoids duplicate credentials, and provides a basis for client identification.

The Mac Address can also be identified through the customer care application - see Network Security section for more details.

Authentication

The authentication process uses Extensible Authentication Protocol (EAP) in conjunction with the Transport Layer Services (TLS) protocol. Together these protocols provide a means for mutual authentication of client and authentication server using digital certificates. Authentication is conducted immediately after an encrypted tunnel has been established. This means that none of the authentication packets are transferred in plain text.

So the system has full certificate sign on and can support many authentication schema including Certificate, SecureID, Soft Token, Active Directory, LDAP, RADIUS and many more. The system also supports device level authentication for managing layer2 access to bearers such as WiFi and WiMAX as well as PPPoE for bearers such as IP Wireless.

Re-Authentication

With seamless mobility the aim is to stay connected at all times. However, if one of your mobile devices was lost or stolen, this could create a possible security risk to your company's data network.

Brand's Apollo has the ability to set re-authentication time outs - which ensure the user has to verify their details at determined times to be able to continue with their session. This gives an added level of security and can also be used to activate the kill option of the device.

Certificate Management

The authentication certificate is stored at the client on a smartcard. Certificates can be revoked at any time or expire at a set time and date. In this case, the authentication process will fail unless the client has received a new valid certificate. Other certificate management features include single sign on for a user across multiple devices and networks, integration with Active Directory (Multiple X509 Certificate Management), Smart card auto logon/logoff, Windows Gina for device lockdown and full device security.

Smart Card Technology

More and more organisations are implementing Smart Cards as multi-function ID/ Photo cards for different workers across the organisation. The card is made up of a number of certificates and keys, which contain information required to access the organisations network and systems. To ensure data confidentiality, all information on the card can only be accessed by a pin-code. This authentication process brings an added level of security to organisations, securing both access to the device and subsequent connection to the IT network. If the card were lost or stolen it would be unusable without the user's pin, or should the pin be disclosed or the smart card compromised then IT Administration staff could simply revoke the user's certificates.

Figure 2: Security Card and Key

The benefits of the smart card technology is the high level of security they provide. Smart cards are an integral component in the infrastructure solution developed by Brand Communications, which through advanced authentication mechanisms enable wireless users to access network files and applications via any communication bearer in a secure and effective manner on any mobile data terminal.

The Apollo solution uses the EAP-TLS protocol to integrate with Microsoft Certificate Servers. The authentication protocol constructs a secure tunnel between the mobile client so that the authentication identities cannot be compromised. It is also recommended that Smart Card Authentication is used for secure Windows login. This process requires that the Windows user account is registered with the domain.

Seamless Roaming

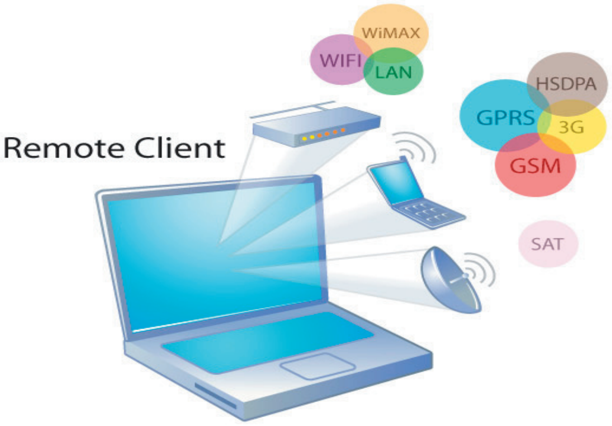
Across Bearers and Re-Connections

Connectivity is now available through so many different mediums, GSM, GPRS, 3G, WLAN (802.11b, 54G, N, MIMO, DSL, Cable and DVB are here today, others are arriving such as WiMAX (802.16) and HSDPA. These are giving the mobile user a huge range of choice for connectivity whilst out in the field and the ability to seamlessly roam between bearers without any disruption or compromise of security or data is now becoming a necessity.

The Brand Apollo solution provides mobile data users with the ability to "roam" across network boundaries whilst ensuring complete VPN security to the organisations data. It creates a highly secure, AES encrypted multi bearer roaming network solution that delivers a seamless access to the user which is agnostic to the transport mechanism. Apollo is a solution which can be used on a global basis and acts as an overlay to any network or combination of networks it traverses whilst keeping the VPN intact throughout any or all bearer changes. It overcomes many of the short comings of Mobile IP, reduces network management traffic and ensures a rapid transmission to one bearer to another whilst maintaining the session. This fast switching capability is by-directional (client to server - server to client) and is therefore ideal, if not essential for current and future data and perhaps more critically Voice over IP (VoIP) applications.

Seamless Roaming can allow the user to perhaps start a download on a Wireless LAN and then roam onto GPRS without intervention, meaning no need to keep logging in each time the session changes.

Figure 3 - Secure Seamless Capabilities Over Various Network Bearers



Network Security

Ensuring secure remote access to the organisation's network is essential as companies continue to move their business processes online and extend the enterprise boundary beyond the corporate firewalls. The Apollo Solution provides everything you need to ensure no threat is made to your network.

Firewall and IP Layer Access

The Apollo Solution tunnels IP packets between the Apollo client and server. This means that all user / application IP packets are encapsulated with a secondary IP packet. The protocol used is called L2TP (Layer 2 Tunnelling Protocol - RFC 2661). Client packets must therefore enter the corporate network on UDP port 1701 with a destination address of the Apollo Server. This information can be used as access control parameters on the corporate firewall. Apollo also has a built in firewall which gives added security benefits to the network.
The Apollo solution is fully capable of operating across networks employing network address / port translation which can be a useful system for protecting private networks. It handles the NAT (Network Address Translation), which is commonly found in GPRS and Public Bearer connections. The Apollo server hides the actual application layer IP addresses to give a more secure connection using VPNs.

VPN

Very few enterprise-level users now access networks remotely without using VPNs. Hence the extremely efficient and high performance AES VPN dynamic tunnelling employed by Brand that adds strengthened security to the network and data, ensuring no data is compromised or interfered with. It works with NAT and PAT environments and does not fail (like most) in out of coverage situations. Dynamic session keys ensure the highest level of security. The ultimate split tunnelling ability supports sessions over multiple simultaneous bonded bearers. The VPN has a extremely low overhead unlike IPSec solutions and as such is ideal for encrypting VoIP and Video protocols.

So how does it work? The Apollo VPN emulator is installed as an NDIS driver, which presents itself as an ethernet adapter to windows. The emulator can be configured to act in all respects exactly like a normal LAN card. The PC therefore believes that the Apollo emulator is a LAN connection, rather than a remote access or WAN connection, enabling the user to run any LAN application without modification.

The Apollo VPN uses a heavily modified L2TP tunnel with Brand vendor extensions. The extensions provide for faster TCP/IP recovery in case of packet loss, that can take place on congested internet links or the high packet loss environment that is found within a GPRS network, effectively making the unusable, usable.

Apollo ‘Anywhere’ Packet Access Server (PAS) Functions

The Apollo ‘Anywhere’ server is the termination point of the VPN tunnels created by each of the client machines and also handles the management of any tunnels that are linking any corporate or remote sites. As the PAS is the termination point of the user sessions and the start point of the corporate tunnels, it is possible to get an unencrypted snapshot or view of the data being passed through the server for all active sessions. Each Apollo PAS is able to have multiple services configured. Each of these services is able to have its own authentication rules and Radius servers using the built in Apollo ‘Triple A’ (AAA) mechanism.

VPN Server Services

A typical mobile data deployment will have many different users connecting to the solution. These users may use different numbers to dial in or have various packet bearers such as GPRS, 3G, HSDPA and may have different authentication servers which may have different timeouts or access perimeters and they will certainly want to route to different destinations. It is therefore important to be able to register, monitor and support these users individually.

Apollo has the ability to sub class each individual user as a profile for identification by IP address or smart name. Services can be assigned different IP pools. so that clients connecting to different services exist in different IP subnets. This allows routers and firewalls to control user access to different areas of the corporate network based on the connecting service.

Network Management

Network management encompasses a number of key functions: monitoring the network’s activity; evaluating its availability; measuring performance; and logging errors.

The Apollo Server provides event logging output which is sent to a monitoring application called Customer Care. Customer Care will log all authentication attempts whether success or failure, logon or log off events with date and timestamps. As the information is obtained direct from the Apollo Server, much more information about the client is visible than can be obtained from an authentication server log file. For example the unique MAC address would be displayed, along with the IP address of client, machine name, username, OS platform and IMEI number (a unique serial number assigned to GSM/GPRS devices), data volumes, access locations (including Wireless LAN. BSID, SSID and connections speed). This solution also supports full GPS transport layer including location, speed, direction and altitude, making it ideal for integration into GIS or lone worker implementations. All this information can be very useful in tracking down unauthorised users.

Data Transmission Security

To ensure data confidentiality, it is advisable to implement packet layer encryption software product such as Apollo which will ensure protection is given to all data that is transferred, including in-band control and authentication packet data.

Data Encryption

Data Encryption is addressed by Apollo. Once the Apollo session has been established, all data transferred is encrypted using block ciphers operating in the CBC (Cipher Block Chaining) mode. Symmetric Block Ciphers are used by Apollo to encrypt data as they are extremely fast and ideal for mobile working.

The Apollo encryption system offers protection against 'replay' attacks and 'man-in-the-middle' attacks and can be configured to use one of two possible block ciphers for each Apollo session, Blowfish or AES

Blowfish

Blowfish uses a 64bit block cipher with a 128 bit length key and 16 rounds of encryption. Key expansion converts the 128 bits into subkeys totalling 4168 bytes. Each packet sent carries an intialisation vector so that packets do not need to be sequenced and therefore avoiding any decryption problems with lost packets.

AES

AES is the latest encryption standard from NIST (FIPS 197) and is the DES approved replacement. AES is the Advanced Encryption Standard, which is the result of a three year competition sponsored by the U.S. Government's National Institute of Standards (NIST). This encryption method, also known as Rijindael, has been adopted by NIST as a Federal Information Processing Standard. AES like its predecessors, is a block cipher where "plain text" is encrypted in "blocks". Apollo uses AES 256.

Key Exchange

Key Exchange is a mechanism for transferring secret keys securely across untrusted mediums. This is an extremely important part of the security policy as it can be the weakest part of the encryption system.

Two different types of key exchange are used by the Apollo solution. If blowfish had been selected as the symmetric cipher then AKEP2 (Authenticated Key Exchange Protocol v2) is used to securely exchange the session key. If the AES symmetric cipher has been selected for the Apollo service then Diffie Hellman key exchange is automatically used. Unlike AKEP2, Diffie Hellman uses public key cryptography which is considered a cryptographically safer approach for and a private key to decrypt. As the algorithms deal with large prime numbers they are computationally expensive, so are only used for key exchange. The much faster symmetric block ciphers are used for normal data encryption.

If a malicious person were to modify the data payload of packets transferred over the public network then this would be detected as corrupt packets. Firstly the payload is encapsulated by Frame Checksum Sequence bytes. Secondly the decryption and decompression would fail to produce a meaningful IP packet and would be discarded.

In the case where very similar packets are transmitted or common headers used, the cipher text byte sequence will show as common bytes. This information could be used by cryptanalysts or used for relay attacks. This form of attack is prevented by passing an initialisation vector into the CBC (Cipher Block Chaining) algorithm. The initialisation vector is randomly created for every packet sent and because the 128 bit blocks are chained, every block that makes up the packet is scrambled.

Despite the complexity behind encryption systems, Apollo makes it easy to configure. No pre-shared keys are required, just select the encryption type and go! Encryption keys are dynamically generated at runtime using Psendo Random Number Generator so no keys are stored on the device or need to be configured.

Multi-Factor Network Provision & Controlled Disk Encryption

Endpoint security needs to be controlled from a central internal position and not left to the remote employee to manage - ensuring no damaging data losses for the business. Often human error can result in data being left unencrypted and compromised. The Brand solution introduces multi-factor control so that the network infrastructure and security policies control the encryption on the device and not the user.

With Brand ‘Apollo’ endpoint security can control the following:

- Manage the access / usage of many different types of mobile device and removable storage
    - Laptops, Smartphones, Handhelds
    - Networks Connections, Wifi, Port Control
    - USB Drives and removable storage devices
- Permit and Block Access by using Granular Control, White Lists and Black Lists
    - Temporary Permissions
    - User Specific Control
- Reporting
    - Real Time Status Monitoring
    - Alarm / Alert Monitoring

‘Safe Drive’ Encryption

Apollo ‘ApSafe’ provides added security by setting up a secure encrypted virtual hard drive on the remote user’s mobile device to allow safe storage and access of critical data files and central control if a data breach occurs.

A virtual drive is a drive that appears to be a normal hard drive, but is actually stored on the local machine in a encrypted file. The drive looks and works like a normal drive so the mobile user can use it to store, edit and delete files. The difference is that it is encrypted so you have peace of mind that all the data is protected.

This automatic encryption ensures a high degree of security and operates transparently in the background so no in-depth user training is required or a change of work behaviour needed.

Apollo ‘ApSafe’ drive can also be remotely configured to be automatically created and made available when the user logs in. Apollo can create the format of the virtual disk and then alert the user that the drive is ready to use. Encryption keys for the ‘ApSafe’ drive are stored on the RADIUS server and only passed to the client when authentication is successful.

Lost / Stolen Devices

From time to time a situation may arise where a remote user accidently loses his/her laptop containing confidential company data. This situation could potentially cause the company financial loss, legal liability or brand damage and is one of the most underestimated risks facing organisations today.

With the amount of mobile devices increasing within organisations, with remote working becoming increasingly popular the need for strict and enforceable policies are absolutely necessary. Mobile devices can hold large amounts of sensitive information and with the use of mobile data the ability is there to access even more. It is vital you control access and enforce good working practices.

The first step is for network administrator to disable the use of the device on the mobile infrastructure as quickly and efficiently as possible. The user ID and password should also be disabled and the RADIUS account removed and the mobile operator should be contacted to disconnect the sim. If smartcards are used you are also able to revoke the certificate and lock out the machine to prevent any rogue login. Apollo also allows the administrator to run certain applications on the client machine as a function of the login process and before any client IP access is afforded. From the host end a self-destruct process can be sent to that particular device to destroy all data / applications. When using ApSafe, the encrypted drive cannot be decrypted unless a positive login/authentication is achieved and so accidential failure to turn on encryption by the user cannot happen. As such any compromised device lost in the field will always ‘fail safe’ leaving any secure data permanently encrypted.

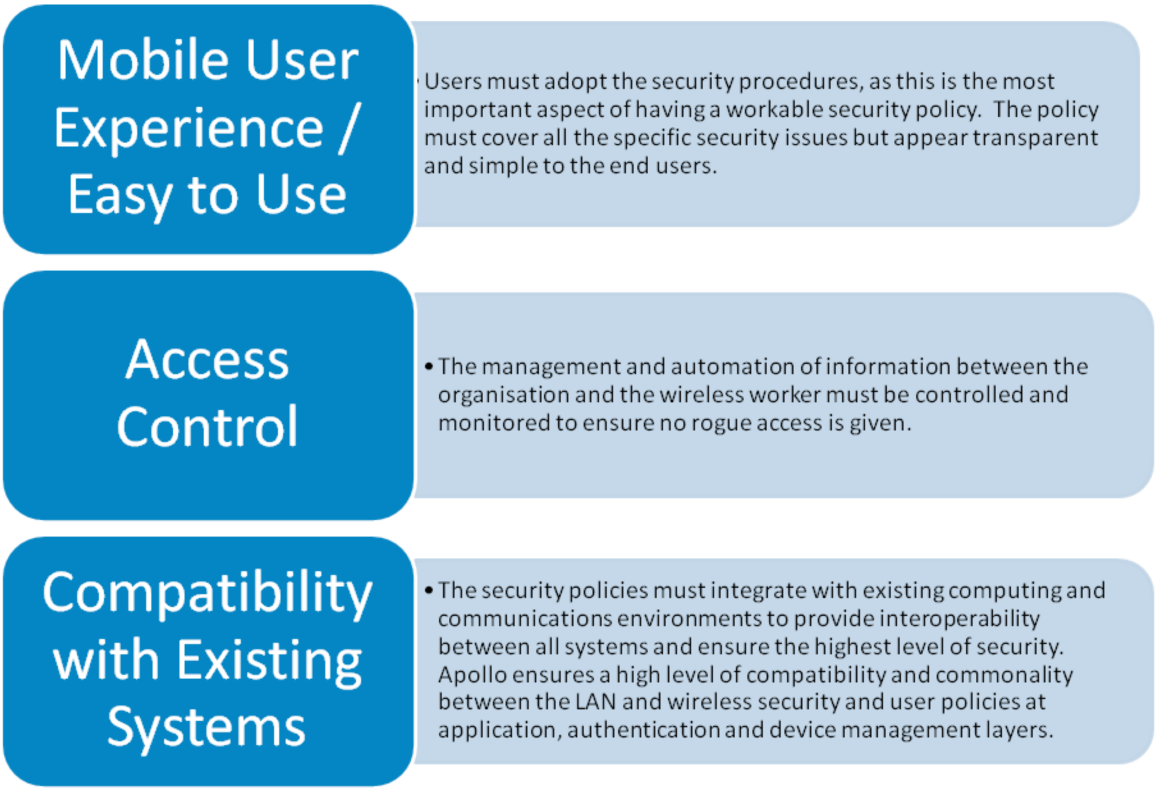
With effective policies in place the functionality to deny access to anyone or the ability to lock down individual machines in case of loss or theft of the device you are minimising any potential risks.

Remote Device Kill Function

A number of instances of compromised storage and media has resulted in the banning of devices containing secure/personal data unless stored in an encrypted form. Most encrypted systems can be easily compromised as the key to the encryption is often local to the device. Brand has a triple factor key for its file system security option which includes network and local keys. This provides an ability to immobilse data from a network end and also includes a kill option to destroy a device remotely.

Conclusion

The use of mobile data to access internal resources through the corporate VPN systems must be highly questionable. Adoption of security policies from the start will ensure the effective implementation of a mobile data strategy. It is important to consider the following aspects.



Mobile User Experience / Easy to Use

- Users must adopt the security procedures, as this is the most important aspect of having a workable security policy. The policy must cover all the specific security issues but appear transparent and simple to the end users.

Access Control

- The management and automation of information between the organisation and the wireless worker must be controlled and monitored to ensure no rogue access is given.

Compatibility with Existing Systems

- The security policies must integrate with existing computing and communications environments to provide interoperability between all systems and ensure the highest level of security. Apollo ensures a high level of compatibility and commonality between the LAN and wireless security and user policies at application, authentication and device management layers.

About Brand Communications

Brand Communications is a global leader in mobile data and remote access solutions. We develop, manufacture and market a range of leading mobile and remote office solutions for all environments including ISDN, PSTN, Fixed Lines, WLAN(802.11b), WIMAX(802.16), HSDPA, DVB, Satellite, GSM, HSCSD, GPRS and 3G.

Brands Apollo solution, matured over 14 years of successful deployment makes mobile data a reality for business-critical data applications using Seamless Roaming for users all over the world. It provides a military grade secure connection for the mobile user whilst travelling from location to location, and removes the uncertainty of using a wireless network to transfer vital information by transparently integrating GSM, GPRS and Wi-Fi networking with LAN environments.

Many Enterprises, Emergency Services, First Responders, Local Authorities, Governments and armed forces at home and overseas have enjoyed significant business benefits. Carriers have also benefited from increased market share and reduced churn as a result of the value added capabilities offered by Apollo.

Apollo has been described as 'Pure Innovation with a difference – it really works and delivers tangible benefits'. It is for these exact reasons that Apollo has simplified the way in which thousands of people work everyday and has led the world of mobile data communications into the future.

For more information about reliable, effective, highly secure mobile data solutions please contact Brand Communications on +44 (0)1480 442100 or e-mail contact@brandcomms.com