Route1®
Securing the Digital World™

MobiKEY

Secure Mobile Computing

Table of Contents

Executive Summary

Route1 is pleased to provide the enclosed information for consideration. Route1 believes MobiKEY is a good answer to secure remote access requirements for the following principal reasons: (a) data stays within your network's perimeter — NOT a browser-based solution and NOT a VPN, (b) deployment saves an enterprise money — in most cases saving more than the investment in the MobiKEY, (c) a hardware based, multi-factor authentication of the individual and not the device — can include the incorporation of government ID cards (CAC, PIV or FRAC) in the identification process, (d) built with security as the first priority, (e) integrates seamlessly into your existing IT infrastructure — no capital investment required, no network changes or reconfiguration required, and no additional servers needed, and (f) compliments an enterprise's VDI investment.

Route1's Technology — the MobiKEY

A highly secure and user-friendly, HSPD-12 compliant remote access solution. MobiKEY is enabled by the MobiKEY device, and Route1's patented identity and access management platform, the DEFIMNET.

Security	Features
• Hardware and smartcard based, multi-factor authentication • Smartcard Common Criteria EA4+ certified • 1024 to 4096-bit asymmetric keys • FIPS 140-2 cryptographic modules • TLS 1.1 • 256-bit AES encryption • RSA SHA-1 and SHA-2 signing algorithms • All files stay within the network • Leaves no footprint on the remote PC • Route1 has no ability to see into the user's data session • PKI-based solution	• Cross domain technology, Host assets can be on any domain or network • Requires no software installation or administrator privileges on the remote asset • Offers users exactly the same access remotely that they have at their office • Enterprise registration and deployment tools • Connection history details for auditing and reporting purposes • Full HSPD-12 compliance — MobiKEY Fusion device integrates with PIV, CAC or FRAC • Remote printing — optional • Remote password reset with MobiKEY Classic device — optional • Integration with Active Directory • Support Microsoft OS and Mac OS X • Bandwidth efficient — 20 kbps average bandwidth usage per connected user • Fully integrates with virtual desktop infrastructure

The Benefits of MobiKEY

1. Your data stays within your network's perimeter
   - NOT a browser based solution and NOT a VPN
2. Deployment saves an enterprise money — in most cases saving more than the investment in the MobiKEY Solution
   - To deploy the solution, the enterprise is not required to purchase laptops or tablets
   - If the enterprise chooses to purchase an asset, no application software required on the asset
3. Hardware based, multi-factor authentication of the individual and not the device
   - Can include the incorporation of government ID cards (CAC, PIV or FRAC) in the identification process
   - Smart card based security - not a one time password (OTP) token
4. Built with security as the first priority
5. Integrates seamlessly into your existing IT infrastructure
   - No capital investment required
   - No network changes or reconfiguration required
   - No additional servers needed
6. Compliment to an enterprise's VDI investment

Why Route1's Clients Use MobiKEY

"By using the MobiKEY the need for organizing, managing, provisioning and maintaining the equipment to make a secure connection to our internal network is eliminated."

"MobiKEY provides a true extension of our internal workstations to the authorized end users. A user can benefit from this access without the requirement to be physically present within our facility."

"The ability to isolate and control this solution using an enterprise PKI solution at the agency level with integrated granular control to the end machine creates an environment that is truly manageable. MobiKEY creates an environment that can be productive and secure without adding the complexity of laptop manageability."

"By using MobiKEY you know that your team can securely get to only the machines they are authorized to access. This connection is provided by a one-to-one associated digital certificate from Host machine to MobiKEY using a link that has an encrypted FIPS approved connection."

"Once a contractor has received their full BI you don't have to supply them with any office space or a PC anymore. MobiKEY is all virtualized on a standard platform completely controlled from within the enterprise."

"A standard desktop and access to all required resources can be built as soon as people have access to a windows based system with internet access. Dynamic allocation to our standard image is virtualized and ready to be used. How much time and money can be saved when comparing MobiKEY to getting a laptop ready for production."

"MobiKEY is another option in combination with other solutions. MobiKEY can provide an alternative method for secure access to a personal desktop that wasn't there before. This can eliminate some needs for flash drives and bringing work outside the secure boundary of their circle of trust."

"Imagine needing to get a critical report out and you pull out your laptop to VPN into the network to start working on that final report and the Laptop fails. How many things can go wrong with a secure laptop? If the Laptop needed to be replaced it could take weeks to re-provision, stage, build and test that laptop. With MobiKEY it can take as little as a few minutes to hand out a MobiKEY with an already pre-staged image built on a virtual Server."

"I can say that the MobiKEY is the most useful piece of equipment, next to my Blackberry, that I have been issued. Many of the emails I receive after hours, on weekends, and on leave have attachments I cannot view on the Blackberry. My laptop has been less that reliable, especially on leave where Wi-Fi is less than accessible (I have to drive 18 miles to the County Library or to the local Dunkin Donuts — the only two public Wi-Fi locations in the area — to get a signal, and then the network often drops me during my reviews. With the MobiKEY I can log-in at home almost instantaneously and access all of my files. Even in remote Upstate New York I can access via my in-laws' computer as while they are not configured for wireless (no need to as they only have one computer) but do have strong internet service (FIOS). I can log-in via the MobiKEY and get my work done in well less than half the time of the laptop and without all the log-in issues."

MobiKEY Compared to Other Approaches

For Authentication — One Time Password (OTP) Tokens

OTP tokens are not a remote access solution. They are part of an identity management solution that must be added on to a remote access solution in order to provide comparable benefits to MobiKEY. OTP tokens add a layer of security and authentication to a remote access solution and are often linked to VPN solutions. Organizations that combine OTP tokens with a remote access solution must piece multiple vendor technologies together, creating complex integration and implementation challenges as well as increased costs. Not only can the combined solution be challenging for organizations to implement and manage, it can also be inconvenient and cumbersome from a user perspective. This may be one of the reasons that many organizations use remote access solutions which offer convenience at the cost of security.

OTP tokens offer a two-step authentication process and have generally been considered to be relatively secure; however, that perception is now being widely questioned. In March 2011, RSA disclosed an attack on its systems which resulted in information related to its SecurID being compromised, and which could potentially allow the attackers to gain access as if they were in possession of the tokens. Further in June 2012, a research report was published which highlighted additional vulnerabilities with the RSA OTP and other OTP tokens and smartcard implementations, entitled "Efficient Padding Oracle Attacks on Cryptographic Hardware. MobiKEY does not use RSA SecurID technology and the architecture of the MobiKEY specifically protects against the kind of attack that affected RSA. Specific to the vulnerability noted in the padding oracle attack approach, MobiKEY does not use the C_ UnwrapKey command from the PKCS#11 API and as such is not vulnerable to this risk.

MobiKEY	OTP Token
• Real time access to the user's office desktop	• Contingent on the specific remote access solution being used in combination with the OTP token
• All data and files remain behind enterprise firewalls	• Depending on the remote access solution being used, data and files could be transferred to a remote PC and/or leave a footprint on that PC
• Absolutely no virus or malware get propagated into the client network	• Potential exists depending on the remote access solution being used
• No data footprint left on the remote PC	• Depending on the remote access solution being used, data or a footprint may be left on the remote PC. The OTP token does not protect against this
• Integrated identity management and remote access solution offering maximum ease of implementation and use	• Multiple vendors solutions pieced together to provide identity management and remote access with complexity of implementation and use and high cost
• HSPD-12 compliant by integrating with government issued PIV, CAC or FRAC	• Not HSPD-12-as compliant
• PKI architecture and Root Certificate Authority (RCA) protections are not vulnerable to this type of attacks. Route1's RCA which is the foundation for Route1's solution is offline and powered off. Strict and lengthy security protocols are required to access the RCA	• Information critical to RSA SecurID was hacked by cyber-criminals leading to attacks on an RSA customer. Due to the nature of the solution this information has to be readily available at the moment of authentication, making it hard to protect.
• MobiKEY does not use the C_UnwrapKey command from the PKCS#11 API and as such is not vulnerable to the risk highlighted in the June 2012 publication "Efficient Padding Oracle Attacks on Cryptographic Hardware"	• Impacted by the risks highlighted in the publication "Efficient Padding Oracle Attacks on Cryptographic Hardware"

For Remote Access — Virtual Private Network (VPN)

VPN solutions provide network access to a remote PC through software previously downloaded onto that PC. If unauthorized access is gained to the computer, or if the computer is lost or stolen, the network then becomes an easy target for cyber attacks. Because data and other network information are transmitted beyond enterprise firewalls through the Internet, man-in-the-middle and malware attacks are also possible. VPN solutions require hardware, software and IT resources to deploy and maintain. The cost and complexity can be significant. Because these solutions offer only single-factor authentication, many organizations add OTP tokens to create two-factor authentication, creating further cost and complexity for them and their users.

MobiKEY	VPN
• Driven by the identity of the individual user	• Driven by the software downloaded on the remote PC not the user
• Can read CAC/PIV cards for identity validation	• No capability to read CAC/PIV cards
• Multi-factor authentication of the user's identity as well as authentication of the user's computer and the enterprise server	• Single factor authentication. Two-factor authentication can be added on using security tokens. RSA disclosed a breach affecting up to 40 million tokens in June 2011
• Any internet enabled computer can be used safely and securely	• Requires a dedicated and pre-configured remote PC (laptop)
• All data/files remain behind enterprise firewalls	• Data/files leave enterprise firewalls
• No trace or data footprint on the remote PC	• Footprint left on the remote PC
• No opportunity for man-in-the-middle, virus or malware	• Susceptible to man-in-the-middle attack, virus or malware
• No data is stored on the MobiKEY device. If lost or stolen, can be instantly disabled with one phone call	• Serious security problem if remote PC is lost or stolen. Organization unable to recover data or know who is in possession
• Because no files are transmitted between the network and remote PC, there are minimal bandwidth requirements (kbps range)	• Megabytes of data travelling between the network and remote PC result in a significantly slower user experience
• Solution integrates seamlessly and easily into existing IT infrastructure	• Requires additional appliance(s) within the network with significant set-up costs. May also require considerable re-configuration of the network infrastructure
• Instant and safe disconnection. When MobiKEY is removed, the data session terminates immediately. There is no need to close down applications or saving of files	• Need to properly close down all applications in order not to lose data or files being worked on. Non-secure personnel may see screen as this is taking place
• Most cost-effective network security and protection solution available	• Higher cost solution in terms of hardware, software and IT resources to implement/ maintain

For Remote Access — USB Flash Drives

USB Flash Drive providers offer an encrypted data storage solution, not a real-time secure remote access solution. A USB Flash Drive provides static access to a user's files. When online again, files must then be re-synced with the office PC. Using a USB Flash Drive, sensitive network data/files can be transferred to a remote PC and possibly left on that PC. A footprint is also left on that PC. Access is limited to the information that has been downloaded to the USB Flash Drive. Secure, real-time remote access would require the integration of an additional solution.

MobiKEY	USB Flash Drive
• Real time access to the user's office desktop	• Static access to user's files if the USB Flash Drive has sufficient storage capacity
• No re-syncing of files/data with office PC required	• Files need to be re-synced with office PC upon return, rendering the computer out-of-date until this is completed
• User can begin work on their computer upon immediate return to the office	• May also require valuable Administrator time should a mishap occur during the re-sync
• All data and files remain behind enterprise firewalls	• Data and files can be transferred to the remote PC and could accidentally be left on the remote PC • If the remote PC crashes and the user is unable to fix the crash, this can also result in files/data being left on the remote PC
• No data footprint on the remote PC	• Footprint left on the remote PC
• Absolutely no virus or malware get propagated into the client network	• Potential for transfer of virus from remote PC through files being accessed by applications in the USB Flash Drive which make use of the local Operating System facilities
• User has full access to all of the network resources, information, data and drives for which they are authorized	• Access is limited to the files and data the user has downloaded onto the USB Flash Drive • An additional solution would be required to securely access network resources
• All email correspondence is sent/received through the user's office PC, behind network firewalls	• Additional secure email solution required
• Instant and safe disconnection	• Need to properly close down all applications in order not to lose data or files being worked on
• There is no need to close down applications or save files	• Non-secure personnel may see screen as this is taking place

Principal Use Cases and Scenarios

A. Teleworking
   - Full desk top computing experience. The user does not require the issuance of a government asset. The user can use a home computer, a computer at the public library, internet cafe, hotel business center, etc.

B. Continuity of operations (COOP)

C. Disaster recovery

Product Development Roadmap

October – December 2012

- Win 8 support for the host and remote asset — Classic and Fusion device form factors.
- Policy management.
  - Allow organizations to establish and implement MobiKEY policy management with real-time implementation of changes. Features ranging from security settings (encryption settings), default connection settings, password policy, operating systems and versions on remote computer and mobile devices permissible.
- Android OS support for the remote asset — soft application or MicroSD.
- Authentication as a service. Decoupling of the MobiKEY solution; authentication only offering.
- Remote access feature addition — audio support.

January – March 2013

- Remote access feature addition — video support.
- Win 8RT support for the host and remote asset — Classic and Fusion device form factors.
- iOS support for the remote asset — soft application or MicroSD.
- Android OS support for the remote asset — hardware based, two-factor of authentication with PIV, CAC and FRAC support.

April – June 2013

- iOS support for the remote asset — hardware based, two-factor of authentication with PIV, CAC and FRAC support.
- Linux support for the host and remote asset — Classic and Fusion device form factors.

ATTACHMENT A

Description of Route1's Solution

Route1 delivers industry-leading security and identity management solutions to government agencies and corporations who require universal, secure access to all digital resources and sensitive data. These customers depend on The Power of MobiNET—Route1's proprietary communications and service delivery platform. MobiNET provides identity assurance and individualized access to networks and data. Route1's patented solutions are based on FIPS 140-2 cryptographic modules, and simplify the process of meeting increasingly stringent regulatory requirements for privacy and security. MobiNET is at the core of Route1's DEFIMNET platform.

The Information Assurance Challenge

Identity management and information assurance have never been more critical. With the constant introduction of new devices, applications and users to enterprise networks, the risks increase for network resources, devices and sensitive data to be compromised or lost. Enterprises face the challenge of eliminating these threats while adding new tools and procedures that allow their people to maximize productivity and their partners to share information wherever they are.

Traditional security and identity management systems are often fall short of the required outcome because they piece together multiple vendor solutions to address a range of issues — network, hardware, information security, identity management, virtualization, auditing and remote access. With every solution, an access mechanism is required to present a user's credentials such as a username and password, access card, one-time password token or embedded key. These authentication methods are purpose-specific, and not universal. They require multiple designs and implementation of security models that are complex to administer and costly to manage.

It's not just about access; it's about secure access and the ever increasing need for it.

Route1 understands today's requirement for mobility and the need to stay in contact with your organization's network environment and personnel. Remote access is easy; the challenge is ensuring security that protects your organization's sensitive data and prevents network and employee information from being compromised — especially when data is accessed from outside of your organization's network.

Route1 offers enterprises and civilian and military government agencies a new-paradigm, an identity management and service delivery platform for information assurance. By leveraging Route1's public network platform or a private platform (hosted by client organizations), these organizations can extend their IT and security policies across and beyond their enterprise IT infrastructure with a high level of information assurance.

Security for Route1's Solution

1. Public Key Infrastructure (PKI)

Integrated with the MobiNET and the DEFIMNET platform is a PKI, which issues the certificates and identities for all MobiNET and DEFIMNET platform components including users, MobiKEY devices, Host computers and servers. The MobiNET and the DEFIMNET platforms can form the foundation for an organization's PKI, or can integrate with an organization's existing PKI.

The MobiNET and the DEFIMNET platforms deliver secure interactions by uniquely and positively identifying each user, device and service connected to the MobiNET or the DEFIMNET platform. Both platforms utilize the MobiKEY device which provides authentication but cannot copy or hold secure data like a USB "thumb drive." In addition, the MobiKEY device utilizes a smartcard, either by leveraging the user's existing Personal Identity Verification (PIV) card, common access Card (CAC) or First Responder Authentication Credential (FRAC) in the case of the MobiKEY Fusion device or with the smartcard embedded with the MobiKEY classic device. The MobiNET and the DEFIMNET platforms provide a means to instantly grant or revoke access to digital resources through the management of certificates. This is particularly important when a MobiKEY device or user's smartcard is compromised, lost or stolen — ensuring that the user can be instantly cut off from any services interacting with the MobiNET or the DEFIMNET platform.

The PKI also creates the trust between the MobiKEY device and the Host computer, server or system. During the subscription process, a trusted public/private key relationship is established between the Host computer and the MobiKEY device via a digital certificate issued by the PKI. This relationship is verified by all the communicating peers during the connection procedure, thus ensuring the identity of the end points as well as the authorization to establish that specific connection. The MobiNET and the DEFIMNET platforms ensure that the level of trust provided by a PKI cannot be circumvented; as can happen through the use of local passwords, guest invitations and one-time passwords to authenticate users. Although innovative, these alternative technologies present security risks associated with the delivery of the passwords and the management of their storage. A PKI is a superior alternative because the certificate authority manages the certificates — their issuance and revocation — and allows the services and devices to authorize different types of certificate access — once, multiple or time-based.

2. Multi-factor Authentication

Multi-factor authentication — requiring both "something you have and something you know" — provides an easy-to-use security methodology to authorize users to the MobiNET and the DEFIMNET platforms. The MobiKEY device is the "something you have" and the users existing PIV, CAC or FRAC smartcard in the case of the MobiKEY Fusion device or the smartcard embedded with the MobiKEY Classic device are also "something you have." The password, which is verified against both the smartcard and the platform, is the "something you know." In addition, once the secure computing session is established, additional login credentials are required which could be username and password or smartcard and PIN depending on network security policies. Unlike other technologies, this level of authentication is a basic feature of the MobiNET and DEFIMNET platforms and does not require additional servers or devices.

If a MobiKEY device is lost or rendered inoperative, Route1 provides a replacement service which can expedite a new MobiKEY device to the user. The new MobiKEY device and the Host computer can be remotely accessed through a simple-to-use administration system. Unlike other tokens or USB devices, a lost MobiKEY device does not mean security or data have been compromised: no corporate data exists on the device and the PKI allows the administrator to instantly deactivate the certificate so the MobiKEY device cannot connect to the MobiNET or the DEFIMNET platform and any of its services.

Multi-factor authentication is one of the most important components of the MobiNET and DEFIMNET platforms — providing a positive identification of the user.

3. Smartcard Technology

To ensure that all identifiable information is securely stored, the MobiKEY device utilizes smartcard technology to protect the user's authentication credentials. The smartcard is an embedded component in the MobiKEY classic device, while the MobiKEY Fusion device leverages the user's existing smartcard (PIV, CAC or FRAC) authentication credentials.

4. Integration with Active Directory

Once the user has authenticated locally and with the MobiNET or DEFIMNET platform, and the secure remote access data session has been established with the TruOFFICE application software, the login credentials required for the Host computer are validated against Active Directory entries, no different than when a user is physically in front of their Host computer. In addition, Active Directory integration can be implemented to utilize user information present in Active Directory so that large scale enterprise deployments and user registrations are seamless and efficient.

5. Host Computer Files Remain Within the Organization's Network

To ensure compliance with privacy laws, organizations are mandating that enterprise information remains within firewalls and is properly and securely backed-up. Missing laptops, lost tapes and enterprise data on home computers are growing concerns.

The MobiNET and DEFIMNET platforms address these concerns by ensuring that existing infrastructure put in place to adhere to these mandates is augmented — not circumvented or compromised. The MobiKEY device allows the user to access data directly on a secure computer; secured not only by the organization's existing infrastructure, but also by the secure communications infrastructure enabled by the MobiNET or the DEFIMNET platform, providing the identical user experience as if the user was physically sitting in front of their secure computer. Other technologies such as Virtual Private Networks (VPNs) or certain remote access technologies enable digital interactions. VPNs by their nature require that data be pulled out of the enterprise network to be accessed or worked on, thereby creating "islands" of information and potentially exposing these files and the network to new risks. Other remote access technologies allow users to easily move data from the Host computer to the Guest computer, circumventing the existing network security infrastructure. The MobiNET and DEFIMNET platforms keep the data where it belongs: inside the enterprise firewall.

6. Secure Communications

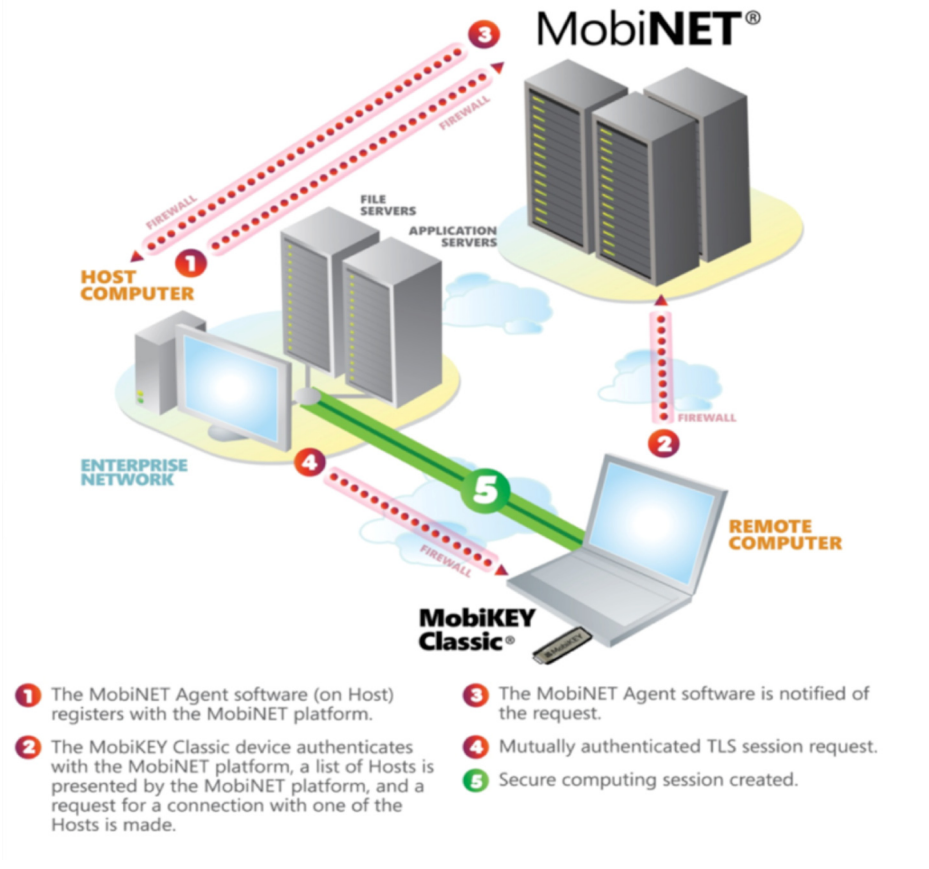
To ensure that a remote session remains secure, the MobiNET and DEFIMNET platforms use a Transport Layer Security (TLS) communications protocol, which is implemented in the most stringent mode requiring client-server authentication. This communications protocol creates a secure point-to-point, mutually authenticated tunnel between the Host computer and the MobiKEY device using 256-bit AES encryption. The advantage of this is that it ensures both sides are mutually authenticated and that no other devices are able to become a part of the data session and/or decrypt the data, rendering man-in-the-middle attacks impossible.

Description of Route1's Solution Components

A. Platforms — Delivering Information Assurance

MobiNET: Identity Management and Information Assurance

The MobiNET platform is a universal identity management and service delivery platform that confirms the identities of individual users and their entitlement to access specific data or resources. It is driven by the identity of the person, not the remote device they are using. Consistent and accurate identification of the individual or the entity — authentication using a MobiKEY device — significantly reduces the burden of securing access. Since authentication is inherently addressed by the MobiNET platform, IT managers can focus instead on what individuals are authorized to access — where they can go within the network and what they can do there. Organizations can ensure the integrity of their data, and authorize and facilitate secure connections between individuals and their digital resources from anywhere in the world.



Note: The image depicts the MobiKEY Classic device. The MobiNET platform supports both the MobiKEY Classic device and the MobiKEY Fusion device.

The MobiNET platform combines the strength of a PKI solution with the trust and flexibility of multi-factor authentication, meeting the stringent security mandates and policies established by governments, defense organizations and commercial enterprises.

EnterpriseLIVE Aggregation Gateway

An EnterpriseLIVE Aggregation Gateway (EL-AG) is a sophisticated appliance that provides enterprises with greater visibility and control over data traffic that flows across the network when the MobiNET platform, TruOFFICE application software, and MobiKEY device are deployed. The EL-AG provides IT staff with a highly effective way to monitor network resources, and ensure information security and regulatory requirements are being met when the MobiKEY device is in use. When installed within an enterprise network, the EL-AG appliance provides administrators with control over two essential functions that are today managed by the MobiNET platform: (1) signalling and control over the MobiKEY device connection status, and (2) facilitating data sessions that would otherwise be made through the MobiNET Switching Array (MSA).

With an EL-AG installed in the DMZ, all signalling data communications are sent directly to the EL-AG and then aggregated and synchronized with the MobiNET platform through an encrypted TLS tunnel. When a MobiKEY device is used to access digital resources, the data session is run directly through the EL-AG, providing network administrators with greater manageability and visibility of traffic flow across their network infrastructure. Initial authentication and authorization is facilitated through the MobiNET platform but all additional data communications happen through the EL-AG.

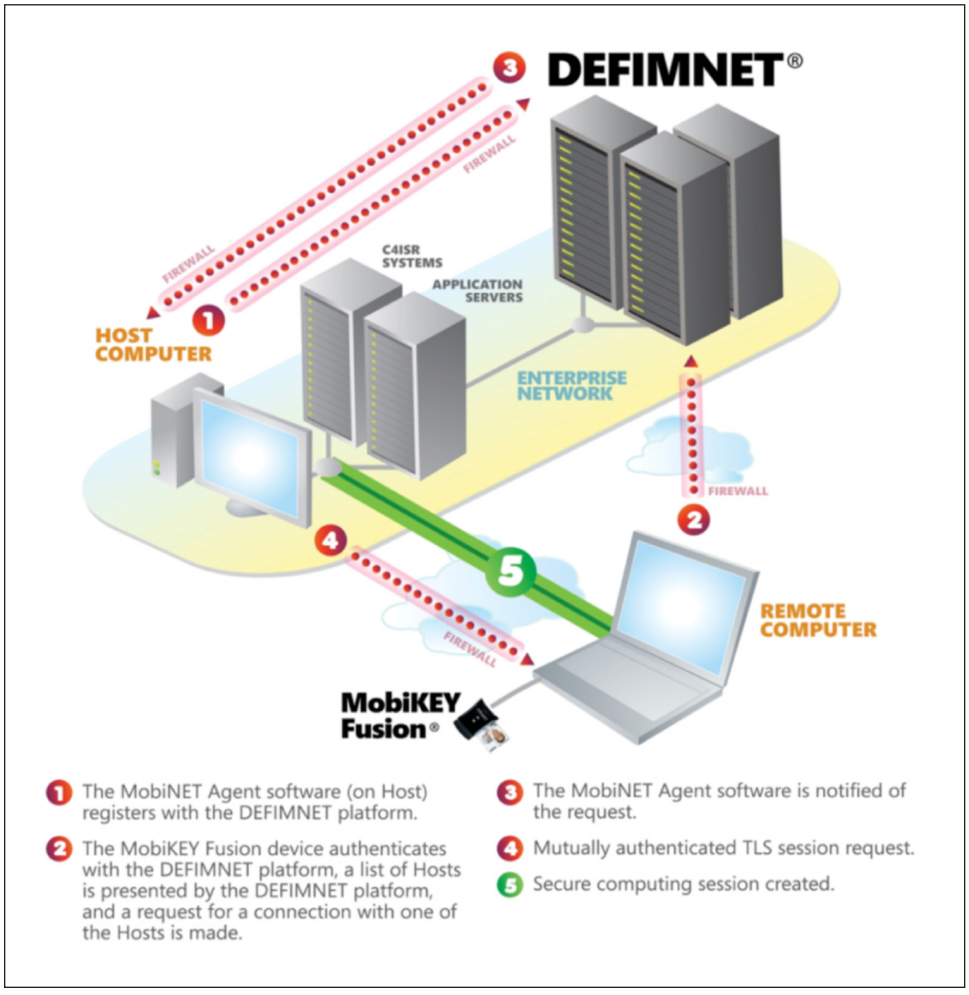
Making the Secure Connection

The MobiNET platform allows organizations to identify and authenticate users and provide them with specific access rights to digital resources. This model operates seamlessly alongside the organization's existing network architecture, making the service a simple and cost-effective remote access solution that requires minimal IT administrative support.

DEFIMNET: Identity and Entitlement Management for Government and Defense

In today's global operations and tactical landscape, identity and security must be absolutely guaranteed. As the battlefield moves into cyberspace, conventional weapons systems are ineffective at providing adequate defense through universal identity and entitlement manage¬ment.

DEFIMNET is an identity management and service delivery platform designed to reside within all levels of classified and unclassified networks. It works with other network systems to command and control confidentiality, integrity and availability of information. It enables consistent information assurance across commands, services, agencies, platforms and systems.



Note: The image depicts the MobiKEY Fusion device. The DEFIMNET platform supports both the MobiKEY Classic device and the MobiKEY Fusion device.

The DEFIMNET platform provides a framework for sharing and exchange of critical, time-sensitive information between government and defense organizations, international coalitions and civilian agencies. As the foundation of a defense-in-depth approach, DEFIMNET supports the requirements of military organizations, arming them with superior technology to gain power from information, access and speed. It is also a clear reflection of mandates such as that of the Defense Information Systems Agency (DISA) to move to an acquisition strategy focused on a Service Oriented Architecture and pay-per-use services.

Built on a foundation of information assurance through identity management and encryption, the DEFIMNET platform uses entitlement-based communication to enable access to resources, such as C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) systems, from anywhere and at any time. The DEFIMNET platform combines the strength of a PKI solution with the trust and flexibility of multi-factor authentication, creating an integrated system that unifies security across a variety of defense and government platforms to enable or revoke access to information and intelligence data in the field.

Making the Secure Connection

The DEFIMNET platform facilitates organization-wide deployments of an identity and access management security infrastructure that is dedicated to the organization. Organizations install Route1's DEFIMNET platform into their existing IT infrastructure. While developed from the MobiNET platform, it differs in that all authentications, access management, certificate distribution and connection facilitation takes place within the organization's network.

B. Applications & Services — Secure Access, Anywhere, Anytime

TruOFFICE: Secure Access Simplified

Route1's TruOFFICE application software is a secure remote access solution. It uses MobiNET or DEFIMNET based identity and entitlement management to reliably connect remote users to their workspace (office computer, desktop and digital applications) from any location in the world.

Note: Users simply insert their patented MobiKEY device into any personal computer's USB port for trusted access to their digital resources.

With the TruOFFICE application software, an organization's confidential information always remains within its own IT infrastructure and securely behind firewalls. This attack-resistant technology eases concerns about hacking, viruses and malware vulnerabilities often associated with remote access. It also eliminates the complexities of network configuration and minimizes the need to determine proxy settings, reconfigure firewalls or create special profiles to connect to the user's Host computer.

Establishing a secure remote access data session does not require applications or drivers to be installed on the Guest computer, thus minimum user privileges are sufficient, and once the remote data session is complete, the TruOFFICE application software ensures that no cache or temporary files are left behind on the Guest computer.

The TruOFFICE application software meets an organization's regulatory compliance needs and is ideal for day-to-day computing, security, teleworking, laptop reduction, disaster recovery and COOP.

Integrates with Virtual Desktop Infrastructure (VDI)

The Route1 TruOFFICE application software also is a secure remote access service that extends an organization's server consolidation strategy to the desktop. By organizing the operating system, user applications, and data into distinct component layers, virtualization enables IT administrators to change, update and deploy each component independently for greater business agility and improved response time. The result is a more flexible access model that improves security, lowers operating costs and simplifies desktop administration and management.

The Route1 EnterpriseLIVE Virtualization Orchestrator (EnterpriseLIVE VO or EL-VO) appliance is responsible for managing virtual machine pools and the allocation of available virtual machine resources for new session requests by TruOFFICE VDI application software users. The EL-VO appliance supports persistent desktop pools, non-persistent desktop pools and individual desktops.

TruOFFICE VDI also supports roaming user profiles. Roaming user profiles allow a user to log onto any computer on the same network and access their documents and have a consistent desktop experience, such as applications remembering toolbar positions and preferences or the desktop appearance staying the same.

C. Devices — Securing Your Digital World

MobiKEY Classic

The Route1 MobiKEY Classic device is an identity validation tool that simplifies the access component, while the MobiNET and DEFIMNET platforms universally manage the identities of users and entitlement to digital resources through software application software such as TruOFFICE and TruOFFICE VDI.

Users simply plug the MobiKEY device into any Internet-enabled, windows based computer to instantly and securely connect to, and access digital resources from anywhere at any time.

The MobiKEY device allows users to securely access data remotely without the need for expensive communications packages or cumbersome hardware. This patented solution is embedded on a smartcard enabled, cryptographic USB device, making it one of the most powerful and easy-to-use multi-factor authentication technologies available today.

Completely clientless and driverless, the MobiKEY device ensures that the user leaves no trace or evidence of their computing session on the Guest computer, while protecting the , simplifying security policy enforcement.

The MobiKEY device minimizes information security risks by eliminating the need for users to carry a laptop or other mobile devices loaded with enterprise data and applications. If the MobiKEY device is lost or stolen, enterprise networks cannot be compromised in any way — unlike other portable devices which can be used to store sensitive enterprise data and can easily put organizations at risk.

Just as a credit card or cell phone service can be suspended or cancelled when loss or theft occurs, digital certificates assigned by the MobiNET or DEFIMNET platforms can also be temporarily suspended or permanently revoked. The added advantage over the loss of a laptop or other mobile computing device is that no enterprise data is stored on the smartcard of the MobiKEY device.

MobiKEY Fusion

The MobiKEY Fusion device is a patented identity validation device that supports government issued identity cards such as CAC, PIV and FRAC. This multi-factor authentication solution combines physical possession of the MobiKEY and an identity card, with computer and network access, helping government and defense organizations meet the United States Homeland Security Presidential Directive 12.

It offers all the security features of the MobiKEY Classic device while leveraging smartcards already issued to government personnel, aided by the additional factors of authentication to secure the access component, while the MobiNET or the DEFIMNET platform universally manages the identities of users and entitlement to digital resources. Users can remotely access systems only with a combination of their MobiKEY Fusion device, an identity or access card and secret password or PIN.

The MobiKEY Fusion device provides government and defense employees and contractors with a combination of ease-of-use and strong cryptography for in-theatre operations. Coupled with strong multi-factor identification and sophisticated entitlement controls, the MobiKEY Fusion device ensures that personnel and combatants have secure access to C4ISR systems and information they need, when and where they need it.