Route1®
Securing the Digital World™

MobiKEY Technology Overview

Route1 delivers industry-leading security and identity management technologies to corporations and government agencies who require universal, secure access to digital resources and sensitive data. These customers depend on The Power of MobiNET - Route1's universal identity management and service delivery platform. MobiNET provides identity assurance and individualized access to applications, data and networks.

www.route1.com

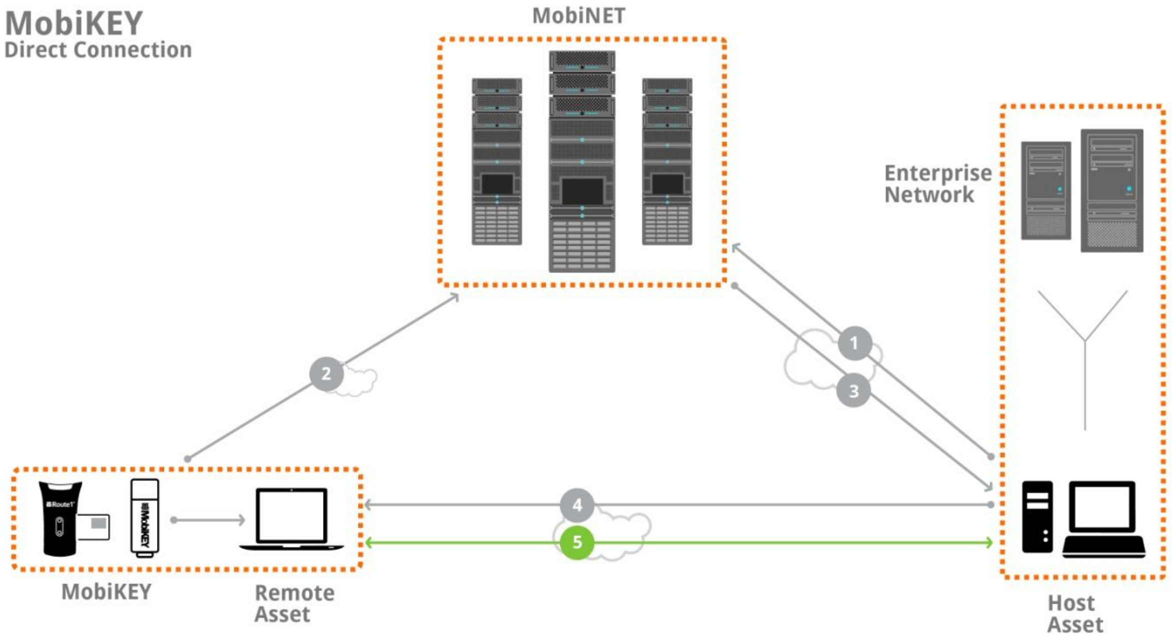
MobiKEY 4.2
February 2013

MobiKEY - Secure Remote Access Technology

MobiKEY is a complete desktop, secure remote access technology that integrates multi-factor authentication and identity management in a mobile computing environment.

Technology Differentiators

- Your data stays within your network's perimeter - not a browser based technology, not a VPN
- Deployment saves the enterprise money; saving more than the investment in MobiKEY for a net cost reduction
- Hardware and smartcard based, multi-factor authentication
- Built with security as the first priority
- Integrates seamlessly into your existing IT infrastructure – no (a) capital investment, (b) network changes or reconfiguration, or (c) additional servers, needed or required
- Compliment to an enterprise's virtual desktop infrastructure investment and a path to desktop consolidation



1 The MobiNET Agent software (on Host Asset) registers with the MobiNET platform.

2 MobiKEY authenticates with the MobiNET platform, a list of Hosts is presented by the MobiNET platform, and a request for a connection with one of the Hosts is made.

3 The MobiNET Agent software is notified of the request.

4 Mutually authenticated TLS session request.

5 Secure computing session established.

The MobiKEY technology includes the use of Route1's universal identity management and service delivery platform, an enabling device, and application software.

MobiKEY application software - A subscription based service that enables users to access digital resources securely from anywhere, at any time.

MobiKEY device - The MobiKEY technology's enabling device.

MobiNET - A universal identity management and service delivery platform that is multi tenant. DEFIMNET is a private, single tenant instance of MobiNET.

MobiNET Agent - Software that is deployed on the asset you want to access when you are remote, the Host Asset. Required in all cases.

MobiNET Aggregation Gateway (MAG) - An appliance that provides enterprises with greater visibility and control over data traffic that flows across the network when the MobiNET platform and MobiKEY are deployed. The use of this appliance is optional.

EnterpriseLIVE Virtualization Orchestrator (ELVO) – An appliance that is responsible for managing virtual machine pools and the allocation of available virtual machine resources for new session requests by MobiKEY users. The use of this appliance is optional.

Features

- Offers users exactly the same access remotely that they have at their office
- Compatible with Mac OS X and Windows
- Cross domain technology, Host Assets can be on any domain or network
- HSPD-12 compliant – integrates with PIV, CAC or FRAC

For the Administrator

- Requires no software installation or administrator privileges on the Remote asset
- No end-point security required
- Enterprise registration and deployment tools
- Integration with Active Directory
- Fully integrates with virtual desktop infrastructure
- Connection history details for auditing and reporting purposes
- Bandwidth efficient - 20 kbps average bandwidth usage per connected user

For the User – Policy Dependent

- Remote printing
- Password reset

With MobiKEY, 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 Asset. Establishing a secure remote access data session does not require applications or drivers to be installed on the Remote asset, thus minimum user privileges are sufficient, and once the remote data session is complete, zero foot print is left behind on the Remote asset.

Security Compliances

- Hardware and smartcard based, multi-factor authentication
- Smartcard chip, Common Criteria EAL 5+
- Smartcard operating system, FIPS 140-2 Level 3
- 1024 to 4096-bit asymmetric keys
- 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 asset
- Route1 has no ability to see into the user’s data session
- PKI based technology – access and authorization management
- Malware resistant – immune to zero day threats
- The Remote asset does not become a node on the enterprise network

MobiKEY meets an organization’s regulatory compliance needs and is ideal for day-to-day computing, security, teleworking, laptop or seat reduction, disaster recovery and COOP.

MobiNET

The MobiNET is a universal identity management and service delivery platform that confirms the identities of individual users and their entitlement to access specific applications, 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 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.

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

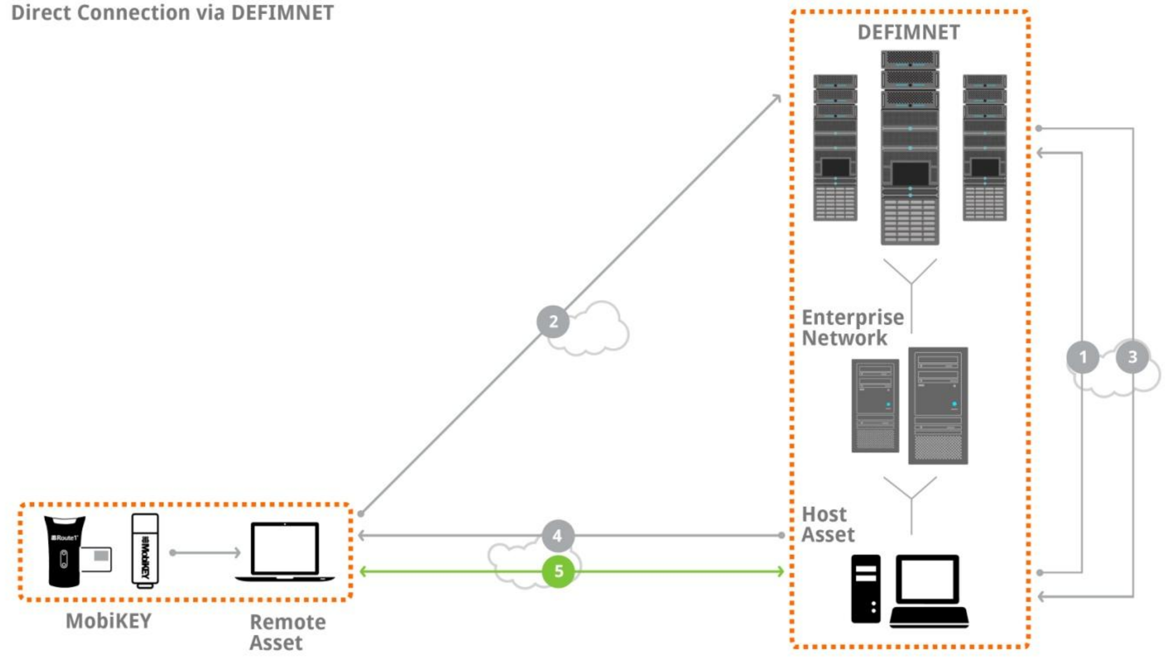
Patented Technology: *"System and Method for Accessing Host Computer via Remote Computer"* (U.S. Patent 7,814,216 – October 12, 2010) - In a peer-to-peer fashion, various host computers communicate with various remote computers using the internet so that user inputs from the remote computers are transferred to the host computers as if the user inputs occurred locally, and information generated by the host computers is displayed on the remote computers. Thus, a remote computer is able to access all of the information and application programs on the host computer.

DEFIMNET

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

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.

MobiKEY
Direct Connection via DEFIMNET



1 The MobiNET Agent software (on Host Asset) registers with the DEFIMNET platform.

2 MobiKEY authenticates with the DEFIMNET platform, a list of Hosts is presented by the DEFIMNET platform, and a request for a connection with one of the Hosts is made.

3 The MobiNET Agent software is notified of the request.

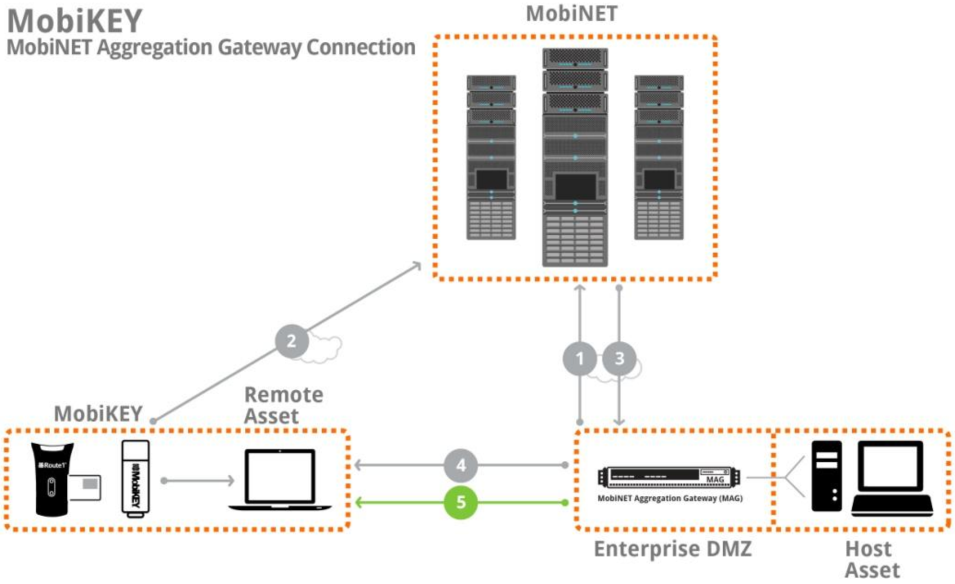
4 Mutually authenticated TLS session request.

5 Secure computing session established.

MobiNET Aggregation Gateway

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

With a MAG installed in the DMZ, all signalling data communications are sent directly to the MAG and then aggregated and synchronized with the MobiNET platform through an encrypted TLS tunnel. When MobiKEY is used to access digital resources, the data session is run directly through the MAG, 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 MAG.


MobiKEY
MobiNET Aggregation Gateway Connection
MobiNET
2
1
3
MobiKEY
Remote Asset
4
5
MAG
MobiNET Aggregation Gateway (MAG)
Enterprise DMZ
Host Asset

1 The MobiNET Agent software (on Host Asset) registers with the MobiNET platform via the MobiNET Aggregation Gateway (MAG).

2 MobiKEY authenticates with the MobiNET platform, a list of Hosts is presented by the MobiNET platform, and a request for a connection with one of the Hosts is made.

3 The MobiNET Agent software is notified of the request via the MAG.

4 Mutually authenticated TLS session request via the MAG

5 Secure computing session established.

MobiKEY - Leveraging Virtual Desktop Infrastructure

MobiKEY uses virtualization to break the bonds between the desktop and operating systems, applications and peripheral hardware. By encapsulating the operating system, user applications and data into isolated layers, MobiKEY 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. In short, MobiKEY is a secure remote access service that extends an organization's server consolidation strategy to the desktop and ensures "peace of mind".

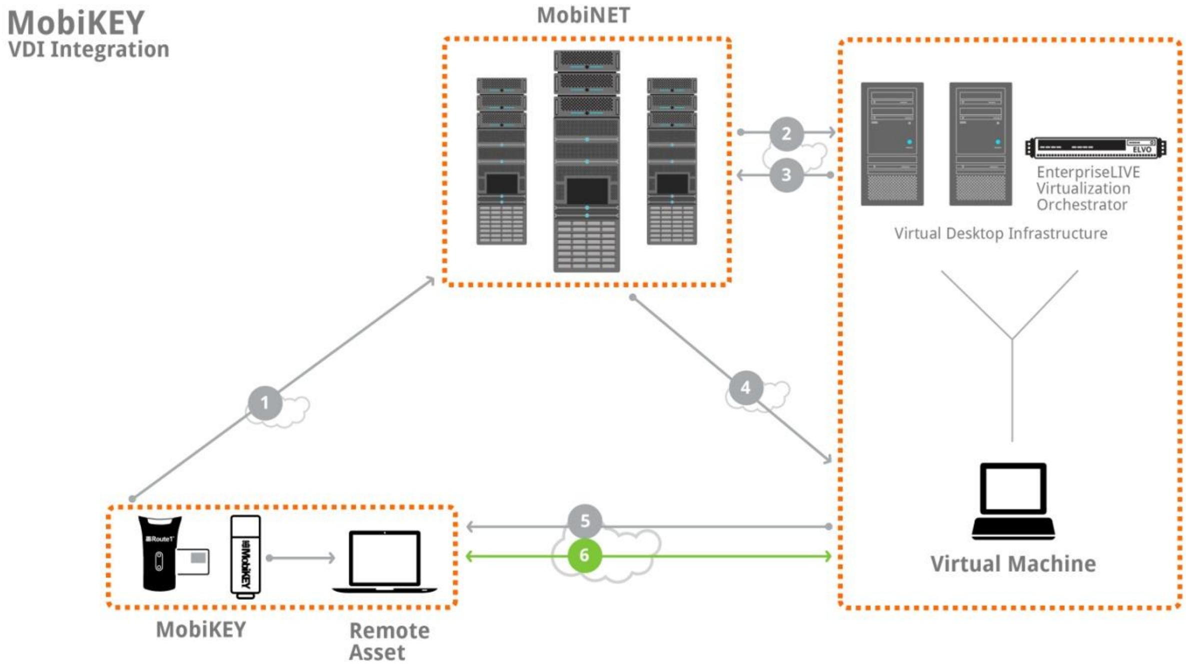
The virtual machine concept allows users to share the resources of a single computer across multiple users for maximum efficiency. MobiKEY has expanded this capability to enable a virtual infrastructure, which allows multiple users to virtually and securely share their resources (programs, applications, processes and data) across the entire network.

MobiKEY requires the deployment of the EnterpriseLIVE Virtualization Orchestrator (ELVO) appliance on the corporate network. The ELVO appliance is responsible for managing virtual machine pools and the allocation of available virtual machine resources for new session requests by MobiKEY users. The ELVO appliance interacts with your Virtual Desktop Infrastructure (VDI) servers to handle the creation and availability of virtual machines on demand. It also interacts with the Connection Arbitrator, which runs within the MobiNET platform environment.

The powerful ELVO appliance provides end-users with a familiar desktop experience, while enabling administrators to seamlessly integrate a unified secure desktop consolidation strategy within their corporate datacenters and maximize the utilization of system resources, to more effectively monitor and manage centralized virtualized desktops, all while providing a low total cost of ownership by minimizing e-waste and hardware overhead.

The ELVO hardware requires only basic network configuration. It does not require exposure to the Internet. It requires (a) an outgoing connection to the MobiNET platform, and (b) Incoming connection on port 443 accessible from where the VDI provider is located, commonly inside the corporate network.

MobiKEY includes integrated virtual desktop management capabilities that leverage the ELVO appliance, which provisions and manages allocation of available virtual desktop pools and resources. The ELVO appliance supports three types of virtual desktops: (a) persistent desktop pool, (b) non-persistent desktop pool, and (c) individual desktops.



1 MobiKEY authenticates with the MobiNET platform, a list of Hosts is presented by the MobiNET platform, and a request for a connection with one of the VDI pools is made.

2 The MobiNET platform forwards the connection request to the EnterpriseLIVE Virtualization Orchestrator (ELVO) appliance.

3 The ELVO appliance selects a virtual machine and returns the virtual machine ID to the MobiNET platform.

4 The MobiNET Agent software is notified of the connection request.

5 Mutually authenticated TLS session request.

6 Secure computing session established.

MobiKEY Classic 2 Device

The MobiKEY Classic 2 (MC2) is an identity validation tool that simplifies the access component, while the MobiNET platform universally manages the identities of users and entitlement to digital resources through the MobiKEY application software. This patented technology 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 Remote asset, while protecting the enterprise network from any viruses and malware. All enterprise files stay within the enterprise firewalls, simplifying security policy enforcement.

If the MC2 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 issued by the MobiNET platform 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 MC2 device.

> **Patented Technology:** *"Portable Device for Accessing Host Computer via Remote Computer" (*U.S. Patent 7,739,726 B2 - June 15, 2010) - A portable device enables access to a host computer via a guest computer. The portable device is connected to the guest computer, and a program stored in memory on the portable device is activated, the program including instructions for establishing communication with the host computer such that input to the guest computer serves as input to the host computer, and output displays from the host computer are displayed on the guest computer. The portable device includes a cryptographic processor for performing cryptographic processing for communicating with the host computer. The portable device also includes a protected memory for storing a private key accessible to the cryptographic processor, the private key being used during cryptographic processing. The protected memory can be internal or external to the cryptographic processor.

MobiKEY Fusion Device

The MobiKEY Fusion device is a patented identity validation device that integrates with government issued identity cards such as CAC, PIV and FRAC. This multi-factor authentication technology combines physical possession of the MobiKEY Fusion device 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 of the same security features of the MC2 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 only access systems remotely with a combination of their MobiKEY Fusion device, *an* identity or access card *and* secret PIN.

Deployment Summary

	MobiNET	DEFIMNET
MobiKEY application software	Required	Required
MobiKEY device	MC2 or Fusion	MC2 or Fusion
MAG	Optional	Optional
ELVO	Optional	Included