

# Solution Overview

## Identity and Entitlement Management

### WE'VE CHARACTERIZED SIX DIFFERENT TYPES OF MOBILE WORKERS:

**Teleworker:** regularly works from home but needs to stay connected to coworkers and computer systems at the corporate office and other locations.

**Road Warrior:** often travels for business. Although he may be out of the office, he needs access to information stored at his regular workplace.

**Corridor Worker:** works away from her desk throughout the day, although she stays within the building. She may attend meetings in conference rooms, or visit with clients and patients outside of her office.

### INDIVIDUALS AT WORK

To many of us, the office is a place where we do most of our work, which may be our homes, hotel rooms, airports, branch locations, or client sites. The concept of work is not only a place but an activity, and with today's technology, work can be done virtually anywhere, and at any time.

### ORGANIZATIONS AT WORK

This hyper-connected environment constantly introduces new devices, applications, and users to an organization's network, creating more opportunities for network resources or individuals to be compromised. Organizations struggle to keep pace with mitigating these threats while empowering personnel and customers with new tools to maximize productivity wherever they are.

### INDIVIDUALS' NEEDS

Wherever and whenever people choose to do their work or interact with their digital resources, they all have one thing in common: they need secure reliable access. For mobile workers, they need the same corporate applications and data that their office-bound colleagues use, such as email, software applications, company intranet, and enterprise databases.

### ORGANIZATIONAL NEEDS

Over the years, Information Technology (IT) departments have come up with various approaches to meeting the needs of these mobile and remote workers. Some of the solutions so far have been limited in scope, such as using a specialty device to deliver services like access email only. Other approaches, such as virtual private networks (VPNs) have given users access to corporate information – which is stored on network servers – but these roaming users lose the ability to access information or applications on their office desk-

top PCs. Even worse, many mobile workers have multiple devices: a desktop PC, as well as a notebook computer, and perhaps even a personal digital assistant (PDA) – that create problems such as out-of-synch data and security risks, not to mention higher costs.

### IT'S NOT JUST ABOUT ACCESS; IT'S ABOUT SECURITY

At Route1, we understand today's requirement for mobility and the need to stay in contact with your organization's network environment. The biggest challenge is ensuring a level of security that protects your organization's sensitive data, network, and employees' information from being compromised, especially once data is accessed from outside of your organization's network.

### INFORMATION ASSURANCE CHALLENGE

Traditional security and identity management systems require multiple vendors pieced together to address network, hardware and information security, identity management, virtualization, auditing and remote access. With any solution that combines access, an access mechanism is required to present a user's credentials, such as a user name and password, access card, OTP (one-time password) device or an embedded device key.

These authentication methods are purpose-specific, meaning that one individual is associated with multiple forms and instances of credentials. Sometimes these credentials are assigned by location or device and therefore have limited portability and distribution options. Credentials are also not universal, requiring multiple designs and implementation of security models which are costly to administer and manage. The result is often a "weak" security solution.

**Day Extender:** the person who just can't leave his work behind when he leaves the office for the day. He finds himself accessing the office information systems after hours.

**Client:** requires secure online access to account information for banking, investing, insurance, and other services. She may access this sensitive information from multiple computers including an unsecured connection from home that can leave your online presence and her digital identity vulnerable.

**Partner/Contractor:** requires isolated connections to an organization's digital resources both within and outside of the organization's facilities.

## ROUTE1 APPROACH

Route1 has built the MobiNET® platform to address all of these challenges for organizations of any size. MobiNET universally manages the identities of users and their entitlement, and secures transactions to deliver any number of services. MobiNET takes care of the authentication, entitlement, and offers the identity-based access to help you simplify your information assurance infrastructure.

MobiNET delivers universal identity management that is individual-centric as opposed to service-centric. By being able to authenticate – consistently and accurately identify the individual or the entity – the burden of securing access is significantly reduced. This approach allows IT managers to focus on managing what the individual is authorized to “do” or “access” – the authentication component is inherently addressed by MobiNET. 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.

## COMPONENTS OF THE ROUTE1 SOLUTION

MobiNET combines the strength of a Public Key Infrastructure (PKI) solution with the trust and flexibility of two-factor authentication, creating a platform that meets the stringent security mandates and policies established by governments, militaries, financial institutions, enterprises, and health services.

Route1 simplifies the access component with MobiKEY®, the identity validation device, while MobiNET universally manages the identities of users and entitlement to digital resources through services such as TruOFFICE and PurLINK.

## TruOFFICE™

TruOFFICE is an identity-based remote access service that empowers an organization's personnel to simply and securely access their digital resources (desktop, files, data bases) from anywhere, at any time, as if they never left their computer.

Since users are working directly off their workspace, (desktop, laptop, server, virtual machine, terminal server) TruOFFICE mitigates the threat of data leakages from end-point devices while preserving the security, mobility, and simplicity of an IT framework that seamlessly supports remote users. TruOFFICE offers more than remote access; it enables increased productivity, business continuity, data protection, and seamless communication and collaboration.

## PurLINK®

PurLINK is an identity-based service that enables organizations to deliver to their workforce or customers a trusted and secure way of connecting and accessing online systems, portals, and applications.

## EnterpriseLIVE® AG

EnterpriseLIVE AG is a hardware network appliance that allows IT administrators to monitor, manage, and audit the network users within their organization. With EnterpriseLIVE AG, all data traffic generated by the organization is routed, managed and maintained within the organization's network. When installed on an enterprise network, EnterpriseLIVE AG allows IT administrators to employ organization-specific IT security policies, perform audits, and generate reports to comply with regulatory and security mandates: SOX (Sarbanes-Oxley), HIPAA (Health Insurance Portability and Accountability Act), and PIPEDA (Personal Information Protection and Electronic Documents Act).



### **EnterpriseLIVE® SR**

EnterpriseLIVE SR is a flexible and scalable hardware network appliance that enables businesses to build a robust, web-based solution that is secured by Route1's MobiNET identity management and service-delivery platform.

### **MobiNET Administration and Provisioning Portal (MAP)**

MAP is a web-based portal that provides IT administrators with centralized, organization-wide management of usage policies for subscribers of Route1's services such as TruOFFICE and PurLINK, and products such as MobiKEY. This simple-to-access provisioning tool also enables organizations to cost-effectively manage large-scale deployments of Route1's single-vendor products and services.

## **MAKING THE SECURE CONNECTION FOR TRUOFFICE**

### **Infrastructure as a Service**

When subscribing to the TruOFFICE service, organizations utilize the global Route1 MobiNET platform to identify and provide access rights to digital resource for its personnel.

This Infrastructure as a Service model seamlessly operates alongside an organization's existing firewall structure, making the service a simple and cost-effective remote access solution that requires minimal IT administrative support. See Figure 1 for a step-by-step view of the infrastructure as a service architecture.

### **Integrated Infrastructure**

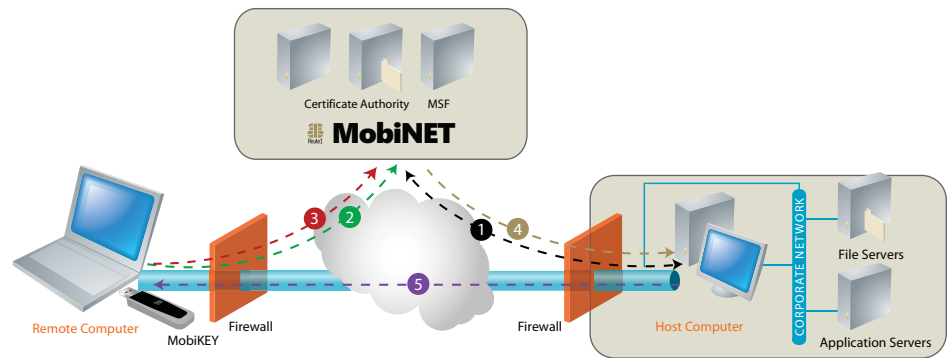
When organizations employ the Integrated Infrastructure model to access their digital resources, organizations use both the global MobiNET platform – as described above – and a network appliance called EnterpriseLIVE AG that is installed in the organization's network. With the integrated

infrastructure, organizations still benefit from the MobiNET security infrastructure, which performs identity and access management, but the data traffic generated by the organization is routed, managed, and maintained by the EnterpriseLIVE AG.

The integrated infrastructure seamlessly integrates into an organization's existing IT infrastructure, ensuring all data traffic is monitored, managed, and audited by the organization's IT administrators. See Figure 2 for a step-by-step view of the integrated infrastructure architecture.

Organizations deploying PurLINK would interact with MobiNET in the same fashion as the Integrated Infrastructure example.

FIGURE 1: TRUOFFICE - INFRASTRUCTURE AS A SERVICE DEPLOYMENT



**1. Host Computer is Registered with MobiNET:** The MobiNET Agent can be installed and activated on multiple Host computers. MobiNET manages a user's identity and the services they are authorized to access by issuing to Route1 subscribers, digital X.509 certificates.

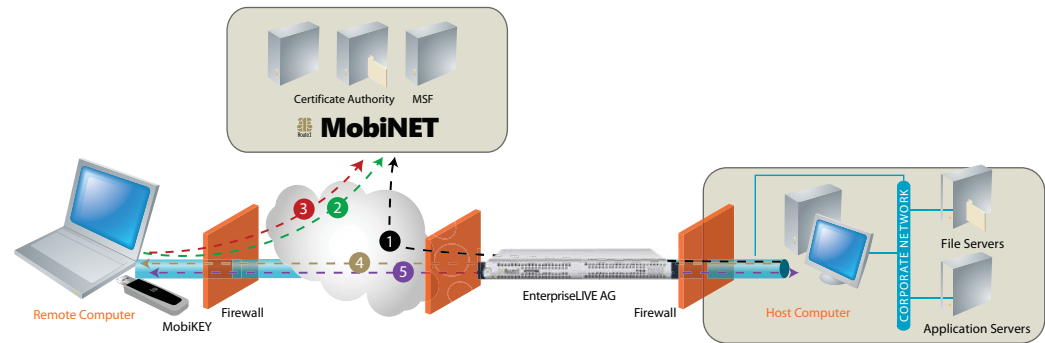
**2. MobiNET Authentication:** Plug your MobiKEY, with TruOFFICE, into the USB port of any Internet-enabled PC. Enter your MobiNET password, which is validated by the smart card embedded on MobiKEY. Once authenticated, MobiNET presents your list of Hosts and their availability.

**3. Connection Request and Notification:** Selecting the desired Host computer initiates a connection request to MobiNET which, in turn, provides the connection information back to the MobiNET Agent.

**4. Session Request and Mutually Authenticated TLS (SSL):** MobiNET Agent establishes a secured TLS(SSL) connection with the MobiKEY. This mutually authenticated end-to-end session eliminates any man-in-the-middle vulnerabilities.

**5. Secure Computing Session Established**

FIGURE 2: TRUOFFICE - INTEGRATED INFRASTRUCTURE DEPLOYMENT



**1. Host Computer is Registered via EnterpriseLIVE AG to MobiNET:** The MobiNET Agent can be installed and activated on multiple Host computers. MobiNET manages a user's identity and the services they are authorized to access by issuing to Route1 subscribers digital X.509 certificates.

**2. MobiNET Authentication:** Plug your MobiKEY, with TruOFFICE, into the USB port of any -enabled PC. Enter your MobiNET password, which is validated by the smart card embedded on MobiKEY. Once authenticated, MobiNET presents your list of Hosts and their availability.

**3. Connection Request and Notification:** Selecting the desired Host computer initiates a connection request to the Route1 EnterpriseLIVE AG which, in turn, provides the connection information back to the MobiNET Agent.

**4. Session Request and Mutually Authenticated TLS (SSL):** MobiNET Agent establishes a secured TLS(SSL) connection with the MobiKEY. This mutually authenticated end-to-end session eliminates any man-in-the-middle vulnerabilities.

### 5. Secure Computing Session Established

## BENEFITS OF THE ROUTE1 SOLUTION

Route1 offers a myriad of benefits for organizations of any size, across multiple industries, and its workforce and customers.

**Increase Security:** Security is the cornerstone of Route1's solution. MobiNET uses a multilayer approach, combining the strength of a Public Key Infrastructure (PKI) solution with the trust and flexibility of two-factor authentication. Encrypted keystrokes and screen images are transferred between the Host, MobiKEY and Guest machines using an end-to-end SSL connection. All data and applications continue to reside on the Host computer, behind the organization's firewall.

**Reduce Operating Costs:** The Route1 solution allows organizations to maintain a lean IT infrastructure while expanding their user base with an all-in-one, end-to-end solution that provides security, service delivery, and identity-based access. Blade PCs or servers located in the data center can reduce equipment like laptops and centralize IT support to one location for all personnel. IT can easily maintain a common desktop image, reduce viruses and worms, and simply upgrade new applications. Any changes to the virtual desktop environment are automatically reflected wherever the user accesses his digital resources.

**Increase Productivity:** Being away from the office does not have to mean a day of lost productivity. Whether employees are out of the office due to inclement weather, transit disruptions, or staying home with sick children, they could still put in a productive day of work.

**Ease of Use:** Establishing a connection requires plugging in a MobiKEY device. There's no additional software to learn and no complicated set up. Once connected, users are working on their own desktop system. Everything is accessible as if they were in front of your own PC. And there is no ramp up time.

**Increase Data Integrity:** Enterprise data never leaves the safety of the office environment. Real-time data is stored on the desktop hard drive or the corporate network, and is never duplicated or out-of-synch. No trace of information is left behind. Organizations maintain control of their corporate and client information and intelligence.

**Ensure Business Continuity:** Organizations can continue essential and non-essential operations in the event of a disaster, pandemic or any other disruption. IT can administer their networks remotely and personnel can access corporate digital resources as if they never left their desks.

**Adhere to Regulatory Requirements:** Organizations can protect their customer's privacy, adhere to corporate security policies and regulatory mandates, since there is no copying or storing of files outside of the corporate network.

**Ease of Implementation:** Route1 has kept the complexity in securing connections and invested in simplifying usability for users and IT administrators; in fact, it's a self-serve solution that does not require any special maintenance, extra hardware, training, or intervention from IT.

**Go Green:** Enabling secure telecommuting not only saves time and increases productivity; it reduces your organization's carbon footprint by eliminating the physical commute to and from the office.

## SECURE YOUR DIGITAL WORLD WITH ROUTE1

Route1 delivers innovative and secure services, enabling customers with trusted and convenient digital services anywhere, any time. Route1's easy-to-use identity and entitlement management solution satisfies organizational requirements for security, service delivery, and remote access. Route1's technology is transforming the way people work, live and play by securing and simplifying all digital interactions.



155 University Avenue, Suite 1920  
Toronto, Ontario Canada  
M5H 3B7  
Phone +1-416-848-8391  
Fax +1-416-848-8394