

# Route1<sup>®</sup> Security

Simplify Your Security and Information Assurance Infrastructure

## MOBINET

MobiNET is an identity management and service-delivery platform that universally manages the identities of users and entitlement to digital resources. MobiNET can authorize and facilitate secure connections between individuals and their digital resources from anywhere in the world. MobiNET technology is based on FIPS-140-2 cryptographic modules that have been evaluated by ICSA Labs, certified by the Canadian Security Establishment (CSE) and approved by various government and military organizations.

## ROUTE1 MOBIKEY

Route1 MobiKEY is a portable identity validation device that securely connects users to the myriad of MobiNET services from any Internet-enabled Windows-based computer. MobiKEY allows users to securely access data remotely without the need for expensive communications packages or cumbersome hardware.

Security is the cornerstone of Route1's solutions. Route1 MobiNET<sup>®</sup> takes care of the authentication, entitlement and offers the identity-based access to help any organization simplify their security and information assurance infrastructure. This document explains the five primary components of the Route1 security infrastructure.

## PUBLIC KEY INFRASTRUCTURE

Integrated within MobiNET is a complete certified root authority that is built on a Public Key Infrastructure (PKI) which manages the certificates and identities of all of the components of the MobiNET platform, including users, MobiKEY devices, Hosts, MobiNET appliances and any MobiNET servers. MobiNET is able to integrate with an organization's existing PKI, as well as be able to form the foundation for an organization's new PKI.

The MobiNET platform delivers secure interactions by uniquely and positively identifying each user, device and service connected to the MobiNET. MobiNET provides a means to instantly grant or revoke access to digital resources through the management of certificates. This is particularly useful in the event of a MobiKEY<sup>®</sup> being lost – ensuring that the MobiKEY can be instantly cut off from any services interacting with MobiNET.

Further, the PKI provides a level of trust between the MobiKEY and the Host computer, server or system. During the subscription process, a trusted public/private key relationship is established between the Host device and the MobiKEY device. During the connection procedure, this relationship is verified by the MobiNET Certifi-

cate Authority, thus ensuring the identity of the end points.

MobiNET ensures that the level of trust provided by a PKI cannot be circumvented, as exhibited when using local passwords, guest invitations and one-time-passwords (OTP) to authenticate users. Although innovative, these solutions present security risks associated with the delivery of the passwords and the management of their storage – often neither of these functions operates in an encrypted environment. A PKI is a superior alternative to these solutions because the Certificate Authority manages the certificates – their issuance and revocation – and allows the services and/or devices to authorize certificate access for specified amounts of time – once, multiple or time-based.

## INTEGRATED TWO-FACTOR AUTHENTICATION

Two-factor authentication – “something you have and something you know” – provides an easy-to-use security method to authorize users to MobiNET services. MobiKEY is the “something you have” and your MobiNET password is the “something you know.” Unlike other security solutions, this level of authentication is a basic MobiNET feature and does not require additional servers, services or devices. The seamless integration of PKI with MobiNET provides an additional level of confidence and security unattainable with systems involving multiple vendors cobbled together.

Two-factor authentication is one of the most important components of the MobiNET security infrastructure – providing a positive identification of the remote device and user. In the

## SECURITY

- Two-factor authentication
- Smart card, Common Criteria EAL4+ certified
- Private Key never leaves smart card
- 1024 to 4096-bit asymmetric keys
- FIPS 140-2
- TLS 1.0 (SSL 3.1)
- 128 bit AES encryption (256 bit AES available)
- RSA/SHA-1 signing algorithm (SHA-2 available)
- Evaluated by ICSA Labs

event that a MobiKEY is lost or rendered inoperative, Route1 provides a replacement service which can expedite a new MobiKEY to the user. The new MobiKEY and the Host computer can be remotely accessed through a simple-to-use administration system.

Unlike other tokens, a lost MobiKEY does not mean security or data have been compromised since no files exist on the device and the Public Key Infrastructure allows the administrator to instantly deactivate the certificate so the MobiKEY cannot connect to MobiNET and any of its services.

## SMART-CARD STORAGE

To ensure that all identifiable information is securely stored, the MobiKEY also uses smart-card technology to encrypt all certificates, passwords and connection information. Taking advantage of industry-leading technologies ensures that certificates and connection information – the only things stored on a MobiKEY – are secured in a trusted manner.

## HIGHLY SECURE COMMUNICATIONS

To ensure that a remote session remains secure, MobiNET provides a communications infrastructure called client-server SSL. This communications infrastructure creates a point-to-point two-way SSL conversation between the Host computer and MobiKEY.

The advantage of this conversation is that it ensures no devices in the middle are able to become a part of the conversation stream and decrypt the conversation.

MobiNET uses 128 AES for these conversations. In some cases, there might be a need for even higher confidence in the security of the connec-

tion and in that case a 256 bit AES SSL connection can be created.

## HOST COMPUTER FILES REMAIN WITHIN THE ORGANIZATIONAL NETWORK

To ensure compliance with privacy laws such as HIPAA, PIPEDA and Sarbanes-Oxley, organizations are mandating that corporate information remains within the firewalls and is properly and securely backed-up. Missing laptops, lost tapes and corporate data on home computers are growing concerns in today's privacy-conscience economy.

MobiNET addresses these concerns by ensuring that existing infrastructure put in place to adhere to these mandates are augmented – not circumvented or compromised. MobiKEY allows the user to directly access data on a secure computer – secured not only by the organization's existing infrastructure, but also by the secure communications infrastructure enabled by MobiNET.

Unlike other solutions that enable digital interactions – VPNs or certain remote access technologies – MobiNET keeps the data where it belongs, inside the corporate firewall. VPNs by their nature require that data is pulled out of the corporate 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 solutions provide facilities to allow users to easily move data from the Host computer to the Guest computer, fully circumventing the existing network security infrastructure.

For additional information please contact [sales@route1.com](mailto:sales@route1.com).



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