



Connectivity and Mobility Services: Virtual Private Network (VPN) Remote Access

Service Description Version 1.01

Effective Date: 07/01/2012

Purpose

This Enterprise Service Description is applicable to **Virtual Private Network (VPN) Remote Access** that is part of **the Connectivity and Mobility Services** product set offered by MN.IT Services and available in the MN.IT Service Catalog. This description provides **State of Minnesota** customers with specific expectations regarding features, benefits, delivery parameters and support of the IT services included in this Connectivity and Mobility service.

Overview

Virtual Private Network (VPN) Remote Access offers MN.IT customers remote connectivity across the public Internet to secure State network services and resources. VPN Remote Access provides end users who are working away from their offices with secure access to their organization's internal network. This can include access to files shared on LAN drives, printers and secure applications.

VPN Remote Access is tailored to meet the requirements of a mobile worker who has the need to routinely connect to their workplace network across an unsecured Internet connection. Internet connections can be any unsecured connection such as a "Wi-Fi" connection at a commercial business or hotel, guest wireless services at another government site, a home network, or a cellular data connection. VPN Remote Access services are connected to MN.IT network infrastructure and direct traffic to specific customer networks and resources.

This service is ordered in two parts. First, an organization works with MN.IT Services to establish a VPN connection capability into the customer's secure network. Contact the MN.IT Service Desk or your MN.IT account manager to initiate this capability. Afterwards, authorized customers may request individual VPN accounts through

the MN.IT Service Catalog. **Wireless access:** Allows laptops, tablets and other wireless capable devices to access MN.IT managed wireless networks operating within State locations. This service can provide connections that are temporary (“guest” access for visitors while on-site) or can be subscribed for regular wireless network access. Guest wireless is configured for public internet access. Subscribed regular wireless access can be public internet access or connected to an internal (non-public) secure network.

Benefits

- **Productivity** – end users are able to access customer networks and resources when not in the office.
- **Security** – VPN connections protects and encrypts all traffic between an end user’s computer and the business network; to access government data and print servers. Additionally, VPN connections extend customer security and content filter policies to remote workers so that customer specific firewall and other security policies are enforced during VPN connections.
- **Cost- savings** – Customer organizations benefit from the shared service model for support and maintenance of VPN infrastructure.
- **Business efficiencies** - MN.IT Services meets customer business needs and protects the State’s data integrity by reducing risk.

Standard Features

Support Hours and Service Availability

To use VPN Remote access service an end-user will need software client on their computing device. End users are given login credentials and will have secure password that is a combination of two sets of numbers (also known as “two-factor authentication”.) The first set of numbers, referred to as the “PIN” is known only by the end user. The second set of numbers is randomly generated at the time of login, on a “key fob” assigned to the end user. Key fobs are provided as part of the service and are distributed at the time the VPN account is setup. Since key fobs typically have expiration dates, the service will replace them on a periodic, as needed basis.

Limits

- When using VPN remote access, any local network devices available to the computer prior to the VPN connection (e.g., networked home printers and other computer resources) may not be available when the VPN client is connected. If this occurs, to use or access local network home printers and other local computer resources, the VPN session must be disconnected.

Customer Responsibilities

- Request the establishment of a VPN capability into the customer’s internal network.
- Request and manage accounts for individual end user VPN access.
- Contact MN.IT Services if a key fob is about to expire and the end user has not been notified of a replacement.
- Contact MN.IT Services to de-activate individual VPN accounts

MN.IT Responsibilities

- Manage and maintain the Virtual Private Network infrastructure.
- Install and configure the VPN client software on end user devices.
 - Deploy key fobs to end users.
 - Replace key fobs before they expire (typically 3 years or less).

Related Information

- Minnesota Statutes 207 Chapter 16E (Office of Enterprise Technology)
- Enterprise Technology Fund 970 Rate Schedule

- Operational documents and information on MN.IT's website
- Connectivity and Mobility Service Level Agreement (SLA) Document

History & Ownership

Note:

This section is for internal use only and should be removed before creating a PDF file for distribution to customers

Revision History – record additions as Major releases, edits/corrections as Minor

Date	Author	Description	Major #	Minor #

Revision History – periodic reviews to ensure alignment with business requirements

Date	Reviewer	Description	Compliance

Approval History – record of approval phases

Phase	Description	Date