“GO Remote” RAS/VPN Service

Upload Approved Forms

User Guide

Version 1.2
March 27, 2009
# Table of Contents

1 INTRODUCTION ................................................................................................................. 3  
2 PURPOSE AND OVERVIEW ............................................................................................. 4  
3 UPLOADING THE FORMS................................................................................................ 7  
  3.1 PREPARATION .................................................................................................................. 7  
  3.2 LOGGING TO THE “GO REMOTE” RAS/VPN ADMINISTRATION PORTAL ....................... 7  
  3.3 UPLOAD APPROVED FORMS PAGE PRESENTATION ...................................................... 9  
  3.4 FILE SELECTION AND UPLOAD ....................................................................................... 11  
4 MAILING THE FORMS.................................................................................................... 12
1 INTRODUCTION

“GO Remote” RAS/VPN is a Remote Access Service (RAS) / Virtual Private Network (VPN) that allows its users to authenticate via an internet facing gateway and to establish an encrypted tunnel in order to get secure and private access to the Government of Ontario internal network and applications.

The provisioning of the “GO Remote” RAS/VPN service requests for the users that don’t have a valid GO PKI (a.k.a. “Non-PKI Users”) requires the verification of the supporting documentation that is part of the request package for “GO Remote” RAS/VPN. The verification is completed by the Corporate Security Branch (CSB) which manages the RAS/VPN provisioning system.

The supporting documentation is the **GO-security Token Request form and the Authentication of Subscriber’s Identity form** which must be filled in by the user, the approving manager and the vendor representative. Once the forms are filled in they must be sent to CSB, either by uploading them on a dedicated site or mailing them (see the subsections below for details). The blank forms are available at:


**IMPORTANT NOTES:**

- **Full time OPS employees are considered by default “PKI Users” who are provisioned via the “PKI” workflow which does not require the verification of the supporting documentation. The uploading/mailing of the forms is not required for this category of users.**

- **External consultants are considered by default “Non-PKI Users” and therefore the uploading / mailing of the supporting documentation is required in order to complete the “GO Remote” RAS/VPN provisioning**

- **External consultants who have a valid GO PKI when requesting the RAS/VPN service will be provisioned via the “PKI” workflow in the same manner as the full time OPS employees. The uploading/mailing of the supporting documentation is not required for this category of consultants.**
2 PURPOSE AND OVERVIEW

This document is intended to be the user guide for the process of uploading or mailing the supporting documentation for the “GO Remote” RAS/VPN service requests. The supporting documentation is required only for the users that don’t have a valid GO PKI certificate (a.k.a. Non-PKI users).

The diagram below presents the overall “GO Remote” RAS/VPN provisioning workflow for the Non-PKI users.

Legend:

- user authentication is required

- on-line use interaction is required
RAS/VPN “GO Remote” Service – workflow for users without GO-PKI

1. Online Self Registration & Secret Questions and Answers (SQA) creation

2. Online Self Activation

3. Service use

4. Online Self-Administration

START

Approved RAS/VPN request from Service Desk

Supporting documentation upload

Request & supporting documentation pre-processing (validation and verification)

E-mail notification (invitation to register)

User

1. Online Self Registration & Secret Questions and Answers (SQA) creation

Shared Secrets

E-mail notification (invitation to activate + activation code)

User

Service Provisioning and Fulfilment

Token (sent via mail)

User

2. Online Self Activation

User

3. Service use

User

4. Online Self-Administration

SQA

User

STOP
The workflow starts with the submission and the approval of the request for “GO Remote” RAS/VPN service. This is a separate process, which is managed by the OPS IT Service Desk.

Once the request is approved, it is forwarded to the “Go Remote” RAS/VPN Provisioning System which is managed by the Corporate Security Branch (MGS).

The provisioning of the request continues only after the supporting documentation (the Go-Security Token Request form and the Authentication of Subscriber’s Identity form) are loaded in the “Go Remote” RAS/VPN Provisioning System and verified by CSB.

The request is released and the user will be notified via e-mail to self-register if the verification is successful.

If the verification is not successful, the request is not released, the uploaded form is deleted from the RAS/VPN Provisioning System and CSB notifies the approving manager to re-load/mail the corrected form.
3 UPLOADING THE FORMS

This is the preferred method for sending the supporting documentation (the “Go Remote” Token Request form and the Authentication of Subscriber’s Identity form) to Corporate Security Branch.

This method is secure, fast and it guarantees that the forms are loaded directly in the “Go Remote” RAS/VPN Provisioning System.

The “GO Remote” RAS/VPN Administration Portal has a dedicated page for uploading the supporting documentation. The portal / page can be accessed at:

https://www.goremoteadmin.gov.on.ca/vpn_admin/management/welcome.mag

3.1 Preparation

Prior to starting the upload process the forms must be verified that they are properly filled-in, dated and signed.

Once the forms are verified they must be scanned and stored in a PDF file.

3.2 Logging to the “GO Remote” RAS/VPN Administration portal

The portal can be accessed by coping and pasting the URL (see above) in the Internet Explorer browser. The URL can be bookmarked in the browser for future use.

This portal is protected and requires a valid GO PKI certificate in order to access it. The GO PKI credentials (user PKI profile name and password) must be entered on the login page (see sample below), as follows:

- select/enter the location of the GO PKI profile
- enter the GO PKI password (as per usual PKI authentication procedure)
- click the Continue button

A sample of the GO PKI login page is provided below.
Please login with your P90 profile and password.

Try using the "Auto Locate" button first, to locate your profile. If not found, select the "Manual Locate" button.

Note: Your P90 profile is stored in a file that ends with .epl. This file is typically kept either on the personal network drive or your local hard drive.

[Login form with buttons: Auto Locate, Manual Locate, Forget password, Continue]

You must have previously set up your secret questions and answers before using the "Forget your password?" button.
3.3 Upload Approved Forms page presentation

Once the GO PKI login is successful, the main page of the “GO Remote” RAS/VPN Administration portal will be presented, as below:

When the GO-Remote Token Request link is clicked the Upload Approved Forms page is opened, as presented below:
This is the page that is dedicated to the upload of the supporting documentation.

The Logout link available on the portal will close the portal and terminate the GO PKI session. The user will be redirected to the Government of Ontario site (http://www.ontario.ca) once the logout is completed.

The Help link available on the portal will open this document.

The Home link available on the portal returns the control to the main page of the portal during any stage of the upload process.

The Clear button available on the page will clear the entries in the E-mail Address and File Name fields.

The Upload button starts the upload process – please refer to the next section for details / instructions.
3.4 File selection and upload

The PDF file (containing the scanned forms) can be uploaded from the Upload Approved Forms page as follows:

1. Enter the user e-mail address in the corresponding field (as per the “Work e-mail address” line on the “GO-Remote” Token request form)

2. Enter the name of the PDF file to be uploaded (including the path - e.g. C:\Documentation\DocumentName.PDF) in the File Name field. Alternatively the file can be located and selected by clicking the Browse button.

3. Once both fields are filled in click the Upload button

If any of the two fields is empty or the values are not valid when the Upload button is clicked an error message (in red font) will be presented, as below:
If the upload is successful a confirmation message will be presented, as sampled below:

The file “filename.pdf” was uploaded on 20/Jan/2009 13:15:25 as the approved "GO-Remote Token Request" form for user John Smith with e-mail address John.Smith@ontario.ca.

The upload confirmation number is 1234567.

4. Click on the “Go Remote Token Request” link to upload another form or on the Logout link to exit the portal and terminate the GO PKI session.

4 MAILING THE FORMS

This method should be used only as a backup, when the upload can not be completed due to technical difficulties.

The forms can be sent via the Government of Ontario internal mail only to the RAS/VPN support group at the following address:

    RAS/VPN Support
    Corporate Security Branch (MGS)
    155 University Avenue, 5th Floor
    Toronto, Ontario
    M5H 3B7

Please make sure that the forms are completed properly filled-in, dated and signed.