



**IT SECURITY
SPECIALISTS**

SSS - IT SECURITY SPECIALISTS
REGISTRATION AUTHORITY CHARTER

STANDARD POLICY

VERSION: 1.2

EFFECTIVE DATE: ON APPROVAL

SSS – IT Security Specialists Registration Authority Charter

Version 1.2 is applicable from Effective Date

 <p>SSS IT SECURITY SPECIALISTS</p>	SSS - IT SECURITY SPECIALISTS REGISTRATION AUTHORITY CHARTER
	STANDARD POLICY
	VERSION: 1.2
	EFFECTIVE DATE: ON APPROVAL

Table of Contents

Introduction	3
Definitions and Acronyms	4
Scope	5
Appointment	5
Document Name and Publication	5
Applicant and Subscriber	5
Domain of Use (Eligibility for Certification).....	6
Purpose of Certification	6
Ownership of Charter	6
Private Key Infrastructure Hierarchy	7
Certificate Content.....	7
Application for a User Account	7
Application for a Digital Certificate	8
Revocation of Certificates	8
Deletion of user accounts	9
Subscriber - RA Bi-annual Audit.....	9
References.....	9
Execution.....	10



**IT SECURITY
SPECIALISTS**

SSS - IT SECURITY SPECIALISTS
REGISTRATION AUTHORITY CHARTER


STANDARD POLICY

VERSION: 1.2

EFFECTIVE DATE: ON APPROVAL


Introduction

The terms contained in this Charter are subject to the terms and conditions contained in the SSS - IT Security Specialists Certificate Policy (CP) / Certification Practice Statement (CPS) document. This Charter supplements the SSS - IT Security Specialists CP / CPS in specifying the digital certification process and client's role as an issuing authority in terms of digital certificates provided by SSS - IT Security Specialists. All persons taking part in the client's digital certification process are required to adhere to the terms and conditions contained in the SSS - IT Security Specialists CP/ CPS, this Charter as well as the all the client's agreements with their employees that do not conflict with the SSS - IT Security Specialists CP / CPS.

 <p>IT SECURITY SPECIALISTS</p>	SSS - IT SECURITY SPECIALISTS REGISTRATION AUTHORITY CHARTER
	STANDARD POLICY
	VERSION: 1.2
	EFFECTIVE DATE: ON APPROVAL

Definitions and Acronyms

<i>Certificate Revocation List (CRL)</i>	the list of all SSS - IT Security Specialists CA certificates that have been revoked
<i>Client</i>	Organisation that registers and subscribes to use the SSS Managed PKI service
<i>CSR</i>	Certificate Signing Request or file submitted to the RA in order to apply for a certificate
<i>Client Registration Authority</i>	the entity appointed by SSS - IT Security Specialists to provide certificate lifecycle functions on behalf of the SSS - IT Security Specialists CA
<i>SSS - IT Security Specialists Registration Authority Charter</i>	the practices and processes that the Client will follow in performing the certificate lifecycle processes delegated by SSS - IT Security Specialists to the Client RA
<i>SSS - IT Security Specialists CA</i>	the SSS - IT Security Specialists legal entity that issues, signs, manages, revokes and renews digital certificates
<i>SSS - IT Security Specialists CP / CPS</i>	see SSS - IT Security Specialists Certificate Policy / Certification Practice Statement
<i>SSS - IT Security Specialists Certificate Policy / Certification Practice Statement</i>	the practices that the SSS - IT Security Specialists Certificate Authority needs to employ for certificate lifecycle management, and further includes the terms and conditions under which the SSS - IT Security Specialists CA makes such services available
<i>SSS - IT Security Specialists Policy Authority</i>	Responsible for drafting and setting the certificate policies and assuring that the activities of the PKI and end entities are conducted in a correct, sound and efficient manner.

	SSS - IT SECURITY SPECIALISTS REGISTRATION AUTHORITY CHARTER
	STANDARD POLICY
	VERSION: 1.2
	EFFECTIVE DATE: ON APPROVAL

Scope

This Charter is an addendum to the Client's Information Security Policy(ies) that is applicable to the Client.

Appointment

SSS - IT Security Specialists appoints the Client as a Registration Authority Client-RA) to:

1. Accept applications for user accounts to request digital certificates.
2. Request and use digital certificates from the SSS - IT Security Specialists CA
3. Perform authentication of identities and verification of information submitted by applicants when applying for the issuance of a digital certificate by the SSS - IT Security Specialists CA in terms of the provisions of this Charter, which has been approved by the SSS - IT Security Specialists Policy Authority.
4. Where such authentication and verification is successful, submit the request to the SSS - IT Security Specialists CA, in accordance with the provisions of this Charter and the SSS - IT Security Specialists CP / CPS.


The Client-RA is appointed for the purposes of authenticating the identity and verifying supporting and ancillary information of applicants using the PKI services provided by SSS – IT Security Specialists.

Document Name and Publication

This document is called the **SSS – IT Security Specialists Registration Authority Charter**. The latest version of the Charter may be accessed on <https://www.sss.co.nz/repo>

Applicant and Subscriber

In this Charter a natural person applying for a user account to access Client's RA to request a digital certificate on behalf of him/herself or for a digital certificate for a Client's machine shall be described as an "applicant" until the application for the client's user account has been granted. Once a Client user account has been enabled the natural person to whom it has been issued shall be referred to as a "subscriber".

 <p>IT SECURITY SPECIALISTS</p>	<p>SSS - IT SECURITY SPECIALISTS REGISTRATION AUTHORITY CHARTER</p>
	<p>STANDARD POLICY</p>
	<p>VERSION: 1.2</p>
	<p>EFFECTIVE DATE: ON APPROVAL</p>

Domain of Use (Eligibility for Certification)

Client employees can be certified under the following conditions:

1. The applicant is employed and in good standing with the Client company.
2. The applicant is fully aware of the responsibilities regarding the care and use of digital certificates (as contained in the subscriber agreement).

Purpose of Certification

Digital certification is to be used to provide the subscribers with trusted identity credentials to authenticate users and machines to the Client's systems and network

The issue of digital certificates in terms of the processes described in this Charter and the SSS - IT Security Specialists CP / CPS will ensure the authentication of the identity of the subscriber. The subscriber may only use the Client's Digital Certificate for legitimate business purposes.


Ownership of Charter

The Client Cybersecurity Manager / Information Security Manager / CISO is responsible for the upkeep of this Charter. Changes to this Charter are to be recommended by the Client Cybersecurity Manager / Information Security Manager / CISO and approved by the SSS - IT Security Specialists Policy Authority.

The Client Cybersecurity Manager / Information Security Manager / CISO limits its liability to the use of the certificate processes as described in the SSS - IT Security Specialists CP / CPS and this Charter.

The day-to-day business operations related to certificate lifecycle will be executed by the party appointed by the Client to act as the RA administrator.

The technical operations related to certificate lifecycle will be executed by the SSS – IT Security Specialists Technical Support team.

 <p>IT SECURITY SPECIALISTS</p>	<p>SSS - IT SECURITY SPECIALISTS REGISTRATION AUTHORITY CHARTER</p>
	<p>STANDARD POLICY</p>
	<p>VERSION: 1.2</p>
	<p>EFFECTIVE DATE: ON APPROVAL</p>

Private Key Infrastructure Hierarchy

The trust hierarchy is as follows:

- SSS - IT Security Specialists Root Certification Authority 4096 – Root Certification Authority (RCA)
- SSS - IT Security Specialists Policy Certification Authority 4096 – Policy Certification Authority (PCA)
- SSS - IT Security Specialists Certification Authority 4096 – Issuing Authority (IA)
- Client RA

The root key hierarchy is as follows:

- SSS - IT Security Specialists Root Certification Authority 4096 – ROOT CA
- SSS - IT Security Specialists Policy Certification Authority 4096 – Root Certification Authority (RCA)
- SSS - IT Security Specialists Certification Authority 4096 (Client Digital Certificates to be signed by this CA) Issuing CA

Certificate Content

- Common Name (Full First Names & Last Name for user certificate and server name/identification for machine identity)
- Subject Alternative Name
- Registration Authority: Client RA
- Issuing Authority: SSS - IT Security Specialists Certification Authority 4096


Application for a User Account

The Client RA shall be entitled to accept and process applications from natural persons for a user account to issue a Digital Certificate.

As a minimum the Client RA shall require from the natural person / applicant that applies for a user account to request a digital certificate user or machine:

- applicant's first names, last name, and contact detail;
- acceptance of the subscriber obligations in the subscriber agreement;
- application or server name

The application process to be followed includes:

 <p>IT SECURITY SPECIALISTS</p>	<p>SSS - IT SECURITY SPECIALISTS REGISTRATION AUTHORITY CHARTER</p>
	<p>STANDARD POLICY</p>
	<p>VERSION: 1.2</p>
	<p>EFFECTIVE DATE: ON APPROVAL</p>

1. The Client RA will receive the application information from the applicant, which will be verified for correctness
2. The applicant signs the subscriber agreement which will be sent to SSS – IT Security Specialists for record keeping
3. If the application is approved by the Client RA, SSS – IT Security Specialists will create the user account for the applicant and distribute the authentication credentials to access the Client RA portal for certificate request and issuance
4. SSS – IT Security Specialists will provide user training for the use of the RA portal for the issuance of digital certificates

Application for a Digital Certificate

The Client RA shall be entitled to accept and process applications from natural persons to request a Client Digital Certificate.

As a minimum the Client RA shall require from the natural person applicant that requests a digital certificate for a user or machine:

- applicant's first names, last name, and contact detail;
- application or server name where the digital certificate will be installed


Once authenticated to the Client RA, the subscriber will request the digital certificate for the user/machine as required on the RA portal. A properly formatted CSR will be sent to the SSS - IT Security Specialists Certification Authority 4096 and the digital certificate will be created. The certificate will be provided for download in accordance with the certificate template chosen by the client.

Issuing, revocation and querying or searching can be programmatically performed through the API that will be exposed via web services. Access to the web-based API services will require the application and/or user to authenticate to the RA portal using a digital certificate. The process for obtaining a certificate for authentication will follow the same process and agreements as when a Client RA admin request for a certificate connects to the RA web portal. The API will be maintained and supported by SSS – IT Security Specialists.

Revocation of Certificates

The subscriber shall promptly request that the digital certificate is revoked immediately on becoming aware of any inaccurate information contained in the digital certificate, or suspected loss, disclosure or compromise of the digital certificates associated private key.

On receipt of the revocation request, SSS – IT Security Specialists will revoke the digital certificate and cause the CRL to be updated

 <p>IT SECURITY SPECIALISTS</p>	SSS - IT SECURITY SPECIALISTS REGISTRATION AUTHORITY CHARTER
	STANDARD POLICY
	VERSION: 1.2
	EFFECTIVE DATE: ON APPROVAL

Deletion of user accounts

The Client shall inform SSS – IT Security Specialists when a subscriber is no longer employed at the Client so that the user account can be disabled and deleted.

Client RABi-annual Audit

The Client RA shall be audited twice per calendar year by the supplier for compliance with the practices and procedures set out in this Charter and the SSS - IT Security Specialists CP / CPS. If the results of an audit report recommend remedial action, the Client RA shall initiate corrective action within 30 (thirty) days of receipt of such audit report.

References

1. SSS - IT Security Specialists Certificate Policy / Certificate Practice Statement (<https://www.sss.co.nz/repo>)



**IT SECURITY
SPECIALISTS**

SSS - IT SECURITY SPECIALISTS
REGISTRATION AUTHORITY CHARTER

STANDARD POLICY

VERSION: 1.2

EFFECTIVE DATE: ON APPROVAL

Execution

The Client agrees to the terms of this Agreement and has directed their duly authorised Representative to execute this Agreement.

For Client by:

For SSS by:

(Signature of authorised person)

(Signature of authorised person)

(Date)

(Date)

(Name of authorised person)

(Name of authorised person)

(Role of authorised person)

(Role of authorised person)