

NATIONAL IDENTIFICATION AUTHORITY (NIDA)



Tanzania NID
CIG Technical Interface
For External Stakeholders
Interface Guide

NIDA_CIG_API_DOCUMENT_20190610

PREPARED BY NATIONAL IDENTIFICATION AUTHORITY

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

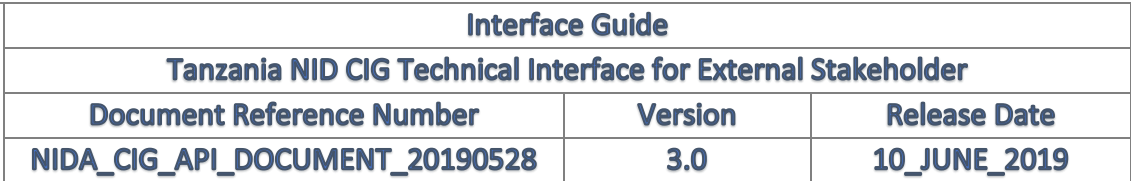
DOCUMENT RELEASE DETAIL

Project	Tanzania NID CIG Technical Interface
Document	Interface Guide for External Stakeholders
Document Reference Number	NIDA_CIG_API_DOCUMENT_20190528
Version Number	3.0
Release Date	10/June/2019
Prepared By	NIDA-Department of Management Information System (NIDA-MIS)
Technical Reviewers	NIDA-MIS
Classification	Confidential – Distribution restricted to intended audience only

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

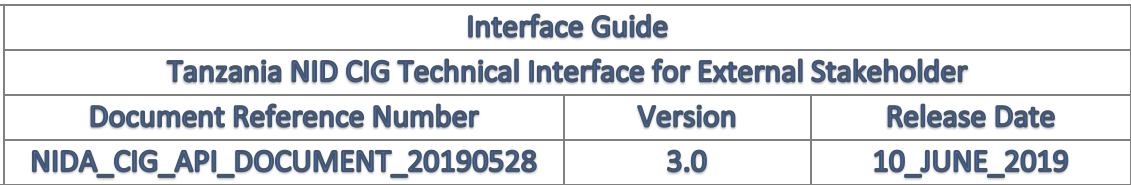
DOCUMENT APPROVAL

APPROVER NAME	TITTLE	SIGNATURE	DATE



DOCUMENT CHANGES TRACK

[illegible]



DOCUMENT DISTRIBUTION LIST

[illegible]

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

TABLE OF CONTENTS

1. INTRODUCTION.....	10
1.1. Scope	10
1.2. Terms and Acronyms.....	11
1.3. Intended Audience	12
2. CIG Interface Architecture	13
3. System Requirements & Pre-Requisitions.....	14
3.1. Development Environment.....	14
3.2. Network Connection.....	15
3.3. Credential & CIG Web Services Security	15
3.4. Types of Certificate Required	15
3.4.1. CIG Certificate Installation (Windows Environment)	17
3.4.1.1. Cert Store Management Console Configuration.....	17
3.4.1.2. Certificate Installation	21
3.4.1.3. Certificate Access Permission to Network Service.....	22
4. CIG Web Services	28
4.1. Query Personal Information by OTP Authentication Method.....	30
4.1.1. Method.....	30
4.1.1.1. Request Parameters.....	30
4.1.1.2. Request Payload.....	31
4.1.1.3. Response	32
4.1.1.4. Response Payload.....	33
4.1.1.5. Sample Response Payload	39
4.2. Query Personal Information by Biometric Fingerprint Authentication Method...	42
4.2.1. Method	42
4.2.1.1. Request Parameters.....	42
4.2.1.2. Request Payload.....	43
4.2.1.3. Response	44
4.2.1.4. Response Payload.....	45

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

4.2.1.5.	Sample Response Payload	45
4.3.	Alternative to Biometric Verification Method	46
4.3.1.	Method	46
4.3.1.1.	Request Parameters.....	46
4.3.1.2.	Request Payload.....	47
4.3.1.3.	Response	48
4.3.1.4.	Response Payload.....	49
4.4.	Query Personal Information by Demographic Questions Authentication Method 50	
4.4.1.	Method	50
4.4.1.1.	Request Parameters.....	50
4.4.1.2.	Request Payload.....	51
4.4.1.3.	Response	52
4.4.1.4.	Response Payload.....	53
4.4.1.5.	Sample Response Payload	53
4.4.1.6.	Error or Status Codes and Descriptions.....	54
4.5.	Query Personal Information Without Authentication Method	56
4.5.1.	Method	56
4.5.1.1.	Request Parameters.....	56
4.5.1.2.	Request Payload.....	57
4.5.1.3.	Response	58
4.5.1.4.	Response Payload.....	59
4.5.1.5.	Sample Response Payload	59
4.6.	Transaction Verification Method.....	60
4.6.1.	Method	60
4.6.1.1.	Request Parameters.....	60
4.6.1.2.	Request Payload.....	61
4.6.1.3.	Response	62
4.6.1.4.	Response Payload.....	63

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

4.6.1.5.	Sample Response Payload	63
4.7.	Identification Method	64
4.7.1.	Method	64
4.7.1.1.	Request Parameters.....	64
4.7.1.2.	Request Payload.....	65
4.7.1.3.	Response	67
4.7.1.4.	Response Payload.....	69
4.7.1.5.	Sample Response Payload	69
5.	Getting Started	70
5.1.	Configuring Certificates in the SSL Client and Server.....	70
5.2.	Certificates on SSL Client and Server.....	70
5.3.	Construct Web Service Request.....	71
5.5.	Mapping the IP Address to Hostname	73

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

LIST OF FIGURES

Figure 2- 1 CIG Integration Architecture.....	13
Figure 3 - 1 Run prompt with mmc key	17
Figure 3 - 2 Cert Store Management Console	17
Figure 3 - 3 Add/ Remove Snap-in	18
Figure 3 - 4 Add or Remove Snap-ins	19
Figure 3 - 5 Certificates snap-in	19
Figure 3 - 6 Select Computer	20
Figure 3 - 7 Add or Remove Snap-ins	20
Figure 3 - 8 Import Certificates	21
Figure 3 - 9 Browse to Insert Certificate	22
Figure 3 - 10 Locate FindPrivateKey.exe	23
Figure 3 - 11 Launch Command Prompt	23
Figure 3 - 12 Client Certificate with Private key	24
Figure 3 - 13 Client Certificate's Thumbprint	25
Figure 3 - 14 Copy Thumbprint to Command Prompt	25
Figure 3 - 15 Location of Private Key file	26
Figure 3 - 16 Properties of Private Key	26
Figure 3 - 17 Set Access Permission of Private Key	27
Figure 5 - 1 Certificates on SSL Client and Server	71
Figure 5 - 2 Web Service Request	71
Figure 5 - 3 Web Service Response.....	72
Figure 5 - 4 Hosts file.....	73

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

LIST OF TABLES

Table 3 - 1 Hardware Specifications for External Stakeholder	14
Table 3 - 2 Types of Certificate Required	16
Table 4 - 1 CIG Web Services for External Stakeholder	30
Table 4 - 2 OTP Authentication Method	30
Table 4 - 3 OTP Authentication Request Parameters.....	31
Table 4 - 4 OTP Authentication Request Payload	31
Table 4 - 5 OTP Authentication Response	33
Table 4 - 6 OTP Authentication Response Payload.....	39
Table 4 - 7 BiometricVerification Authentication Request Parameters.....	43
Table 4 - 8 BiometricVerification Authentication Request Payload.....	43
Table 4 - 9 BiometricVerification Authentication Response	45
Table 4 - 10: Alternative Biometric Verification Method.....	46
Table 4 - 11 AltBiometricVerification Request Parameters	47
Table 4 - 12 AltBiometricVerification Request Parameters	47
Table 4 - 13 AltBiometricVerification Request Response.....	49
Table 4 - 14 RQVerification Authentication Method	50
Table 4 - 15 RQVerification Authentication Request Parameters.....	51
Table 4 - 16 RQVerification Authentication Request Parameters.....	51
Table 4 - 17 RQVerification Authentication Request Response.....	53
Table 4 - 18 Error Code and Descriptions	55
Table 4 - 19 QueryFullDemographic Method	56
Table 4 - 20 QueryFullDemographic Request Parameters	57
Table 4 - 21 QueryFullDemographic Request Parameters	57
Table 4 - 22 QueryFullDemographic Request Response	59
Table 4 - 23: Transaction Verification Method	60
Table 4 - 24 TransactionVerification Request Parameters	61
Table 4 - 25 TransactionVerification Request Parameters	61
Table 4 - 26 TransactionVerification Request Response	63
Table 4 - 27 TransactionVerification Response Payload\	63
Table 4 - 28 Identification Method	64
Table 4 - 29 Identification Request Parameters.....	65
Table 4 - 30 Identification Request Parameters.....	66
Table 4 - 31 Identification Request Response	69

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

1. INTRODUCTION

To enable external stakeholders to gain benefit from CIG services provided by NIDA, external stakeholders can integrate their system with CIG services either to update/ gather or verify identity of the citizen/ permanent residence/ refugees. As NIDA is the trusted entity in issuing the National ID to verified citizen/ permanent residence/ refugees, thus information retrieve from CIG services provided by NIDA are verified and trusted in identifying a person identity.

Details technical requirements in establishing the integration with NIDA CIG services are illustrated in this document. External stakeholders should be able to proceed with their CIG integration development based on this document.

1.1. Scope

The scope of this document is to illustrate the integration required in term of technical expect to the external stakeholder on CIG services provided by NIDA. Functions available for external stakeholders are as below:

- ✓ OTP Authentication Method
- ✓ Demographic Questions Authentication Method
- ✓ Biometric Finger Print Authentication Method.
- ✓ Query without Authentication Method
- ✓ Transactions Verification Method

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

1.2. Terms and Acronyms

Please refer to the table below for a list of the acronyms and definitions used in this document.

Terms & Acronyms	Description
OTP	One Time Password
CIG	Common Interface Gateway
NIDA	National Identification Authority
DMZ	Demilitarized Zone
NIN	National Identification Number
VPN	Virtual Private Network
XML	Extensible Markup Language
SSL	Secure Socket Layer
UDDI	Universal Description, Discovery and Integration
WSDL	Web Service Description Language
GUI	Graphical User Interface
ID	Identification
RSA	Public-Key Cryptosystem introduced by Ron Rivest, Adi Shamir and Leonard Adleman
AES	Advanced Encryption Standard
OS	Operating System
DB	Database
SHA1	Secure Hash Algorithm
PKCS	Private Key Certificate Signature
RAM	Random Access Memory
PKI	Private Key Infrastructure
ERN	Enrolment Reference Number
CA	Certificate Authority

Table 1-1 Terms & Acronyms

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

1.3. Intended Audience

- Technical Manager
- Software Engineer/ Developer

CONFIDENTIAL

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

2. CIG Interface Architecture

CIG integration architecture is as shown in diagram below. A dedicated server (Common Interface Gateway Server) will be hosted in DMZ zone of NIDA data center which is separated from the private zone. This common interface gateway server will receive request from external stakeholder and response accordingly through dedicated web services.

Access to CIG services is through internet via a secure communication VPN network. Access permission to VPN is granted by NIDA. External stakeholder needs to obtain the VPN access from NIDA before starts the integration to CIG services.

There will be total of 3 CIG Authentication services available for external stakeholder to retrieve personal information. Each of the authentication service serve purposes to either gather applicant personal information or to verify applicant identity. Details of the services is described in Section 4: CGI Web Services.

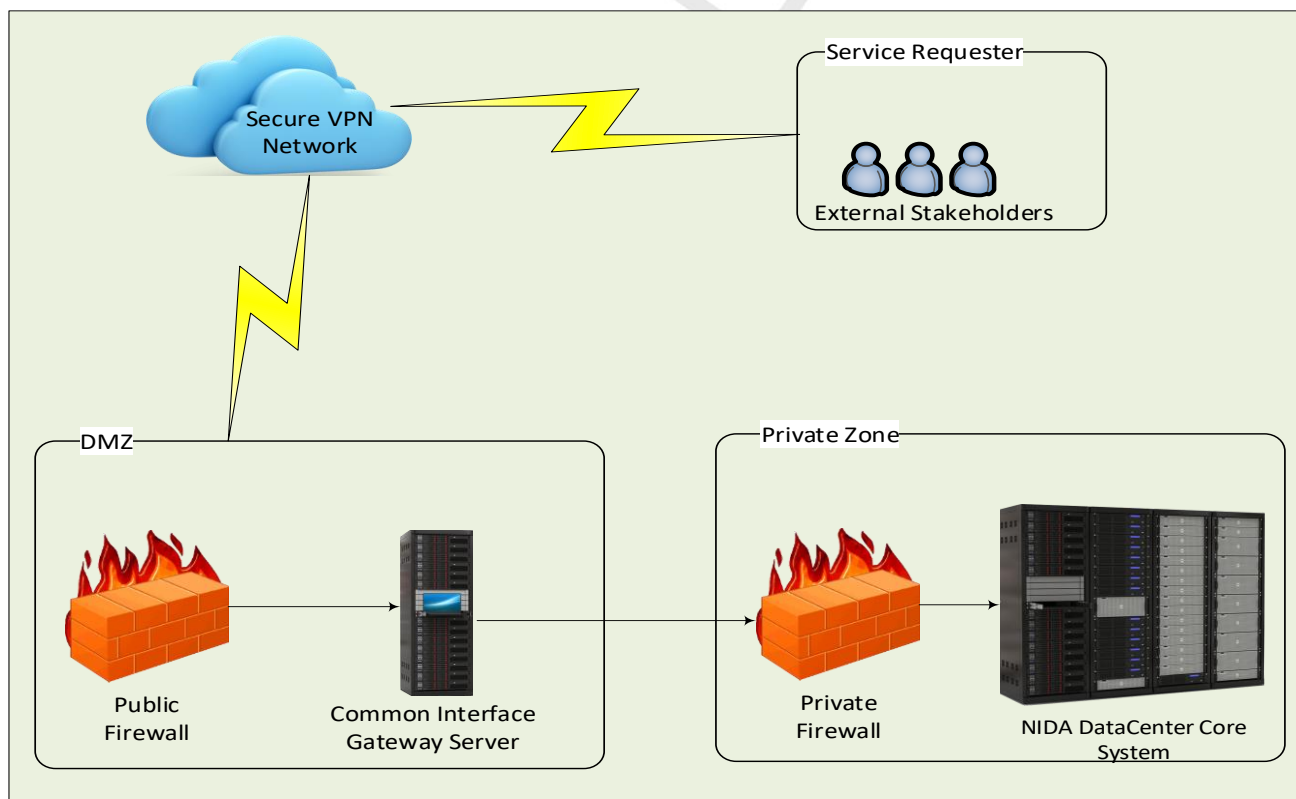


Figure 2- 1 CIG Integration Architecture

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

3. System Requirements & Pre-Requisitions

3.1. Development Environment

CIG services are standardized web services using the XML, SOAP, WSDL and UDDI open standards over an Internet protocol backbone. XML is used to tag the data, SOAP is used to transfer the data, WSDL is used for describing the services available and UDDI is used for listing what services are available. These CIG services allow external stakeholders to obtain certified identity information through a programmatic interface across a network. External stakeholder can then add the services to a GUI (such as web page or an executable program) to offer specific functionality based on stakeholders needs. Due to all CIG services are communicated in XML, therefore the development of CIG integration does not tie to any one of the operating system or programming language. For example, external stakeholder can develop their application in Java or Perl in Windows or UNIX operating system. In this document, the sample code given is in .NET Framework 4.0 on Windows operating system.

Below are the minimum hardware specifications for external stakeholder to integrate with CIG services:

No	Hardware	Specifications
1.	Entry Level Server	<u>Server Specification:</u> 2 Cores, Minimum 2.33/ 2.66 GHz (speed) 2GB RAM per Core Standard hard drive, 100 GB free Network Connectivity <u>Operating System:</u> Windows Server 2008 SP2 or greater, 64-bit or Unix or Linux or any OS which is compatible

Table 3 - 1 Hardware Specifications for External Stakeholder

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

3.2. Network Connection

Access to NIDA CIG services is through internet via a secure communication VPN network. Access permission to VPN is granted by NIDA. External stakeholder has to request from NIDA to obtain the VPN access.

3.3. Credential & CIG Web Services Security

Trusted certificates are typically used to make secure connections to a server over the Internet. Thus, in this CIG interface, trusted certificates are issued out to authorized stakeholders by NIDA to verify the stakeholders before establishing the secure connection. It is the key to identify the stakeholders who they claimed they are.

3.4. Types of Certificate Required

In order to facilitate the CIG Web Service implementation, authorized stakeholder shall request the following certificates from NIDA:

No	Certificate	Format	Description
1.	Root CA Certificate (NIDACA)	Certificate File with “.cer” file extension	CIG Server CA root certificate for CIG Web Server. Install to cert store: Console Root\Certificates (Local Computer) \ Trusted Root Certification Authorities
2.	Sub CA Certificate (NIDASubCA)	Certificate File with “.cer” file Extension	CIG Sub CA root certificate for Stakeholder Certificate Install to cert store: Console Root\Certificates (Local Computer) \ Intermediate Root Certification Authorities

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

3.	Stakeholder Certificate	Stakeholder has to submit Certificate Signing Request (CSR) to NIDA where it will be signed to produce .cer certificate.	Web Service request/response and generation of stakeholder digital signature. Install to cert store: Console Root\Certificates (Local Computer) \ Personal
4.	Message Security Certificate	Certificate file with “.cer” file Extension	Used for computation of CIG Web Service request/response and verification of CIG Web Service digital signature. Install to cert store: Console Root\Certificates (Local Computer) \ Personal

Installation Summary (Windows)

SN	Certificate Type	Certificate Name	Installation Path
1	Client Certificate	StakeholderName	LocalComputer/Personal i.e. use Personal Information Exchange .p12
2	Root Certificate	NIDACA	LocalComputer/Trusted Root Certification Authorities
3	Sub CA Certificate	NIDASubCA	LocalComputer/Intermediate Root Certification Authority
4	Message Security	NIDACIGSecurity	LocalComputer/Personal

Table 3 - 2 Types of Certificate Required

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

3.4.1. CIG Certificate Installation (Windows Environment)

To have the certificates installed on stakeholder machine which later on the certificates are used to sign the service request/ response during the CIG integration by external stakeholder, following are the installation guideline based on Windows Operating System.

3.4.1.1. Cert Store Management Console Configuration

Perform following steps to configure the Cert Store Management Console:

1. Click **Start+R** button, type **mmc** Click on mmc.exe to launch the Console Management software.

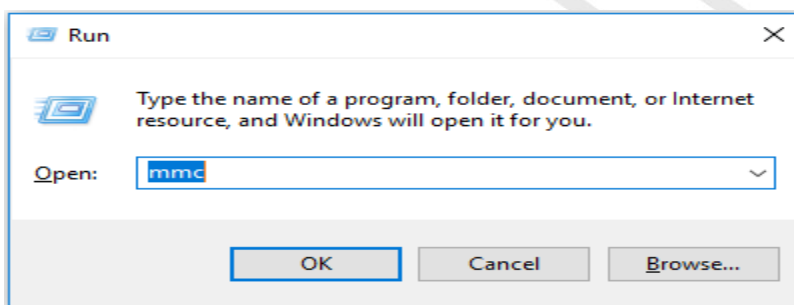


Figure 3 - 1 Run prompt with mmc key

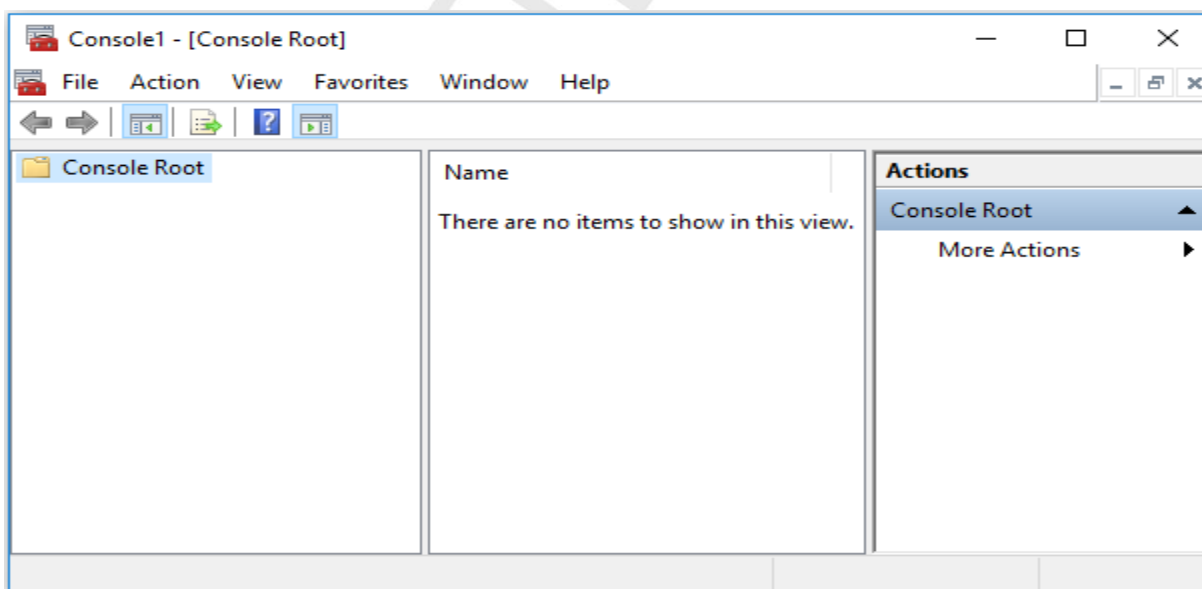


Figure 3 - 2 Cert Store Management Console

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

2. At menu bar, click **File** and select **Add/Remove Snap-in**.

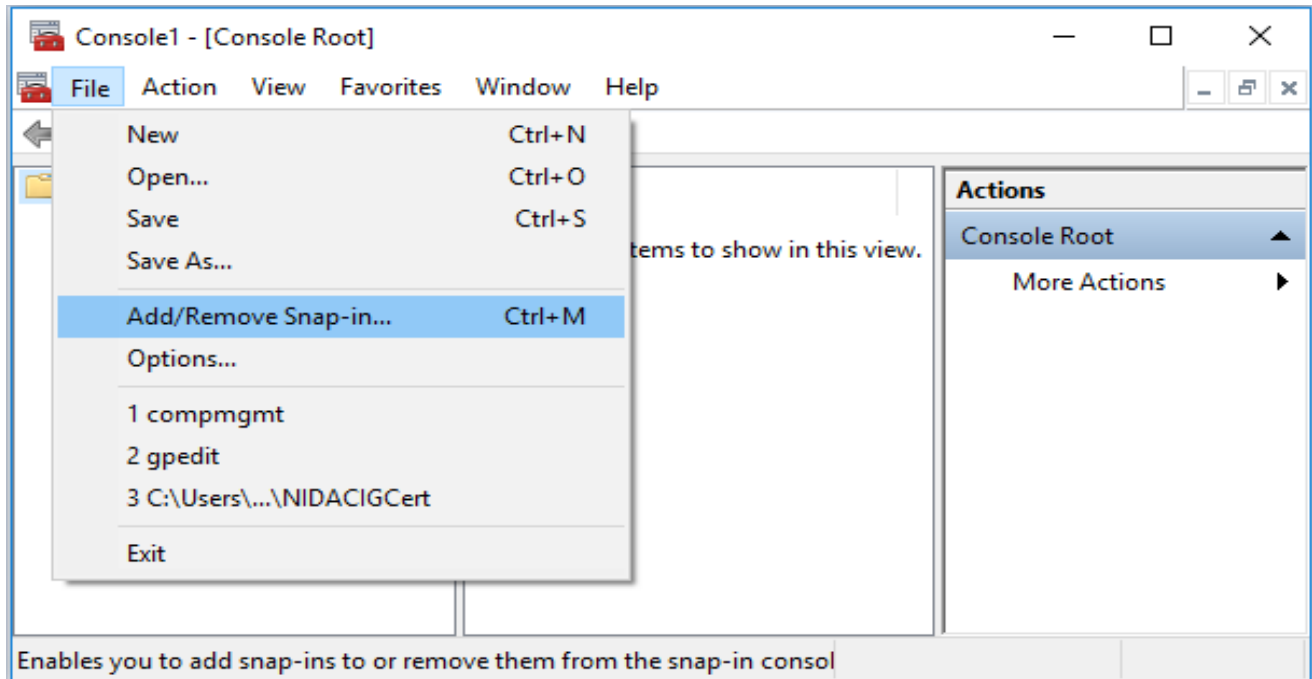


Figure 3 - 3 Add/ Remove Snap-in

3. The **Add or Remove Snap-ins** window appears as follow:

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

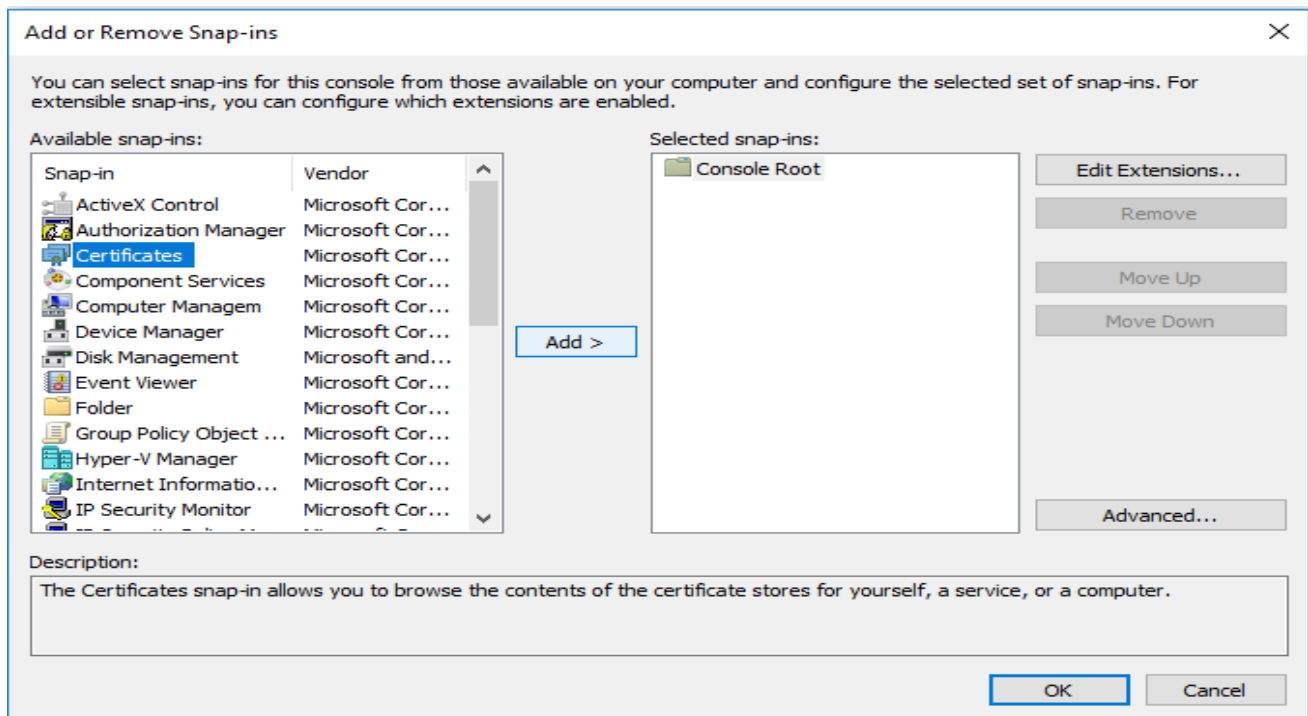


Figure 3 - 4 Add or Remove Snap-ins

4. At **Available snap-ins** table, under **Snap-in** column, select **Certificates**. Click **Add** button. Certificates snap-in window appears as follow. Select **Computer account**, click **Next** button.

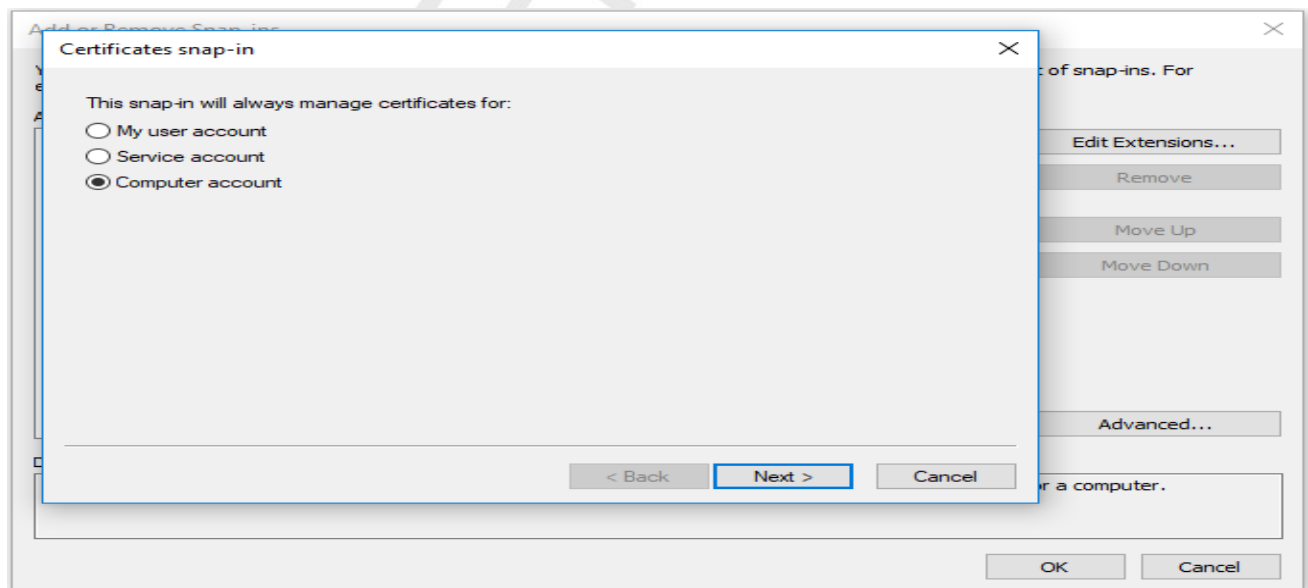


Figure 3 - 5 Certificates snap-in

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

5. Select **Local computer**, click **Finish** button.

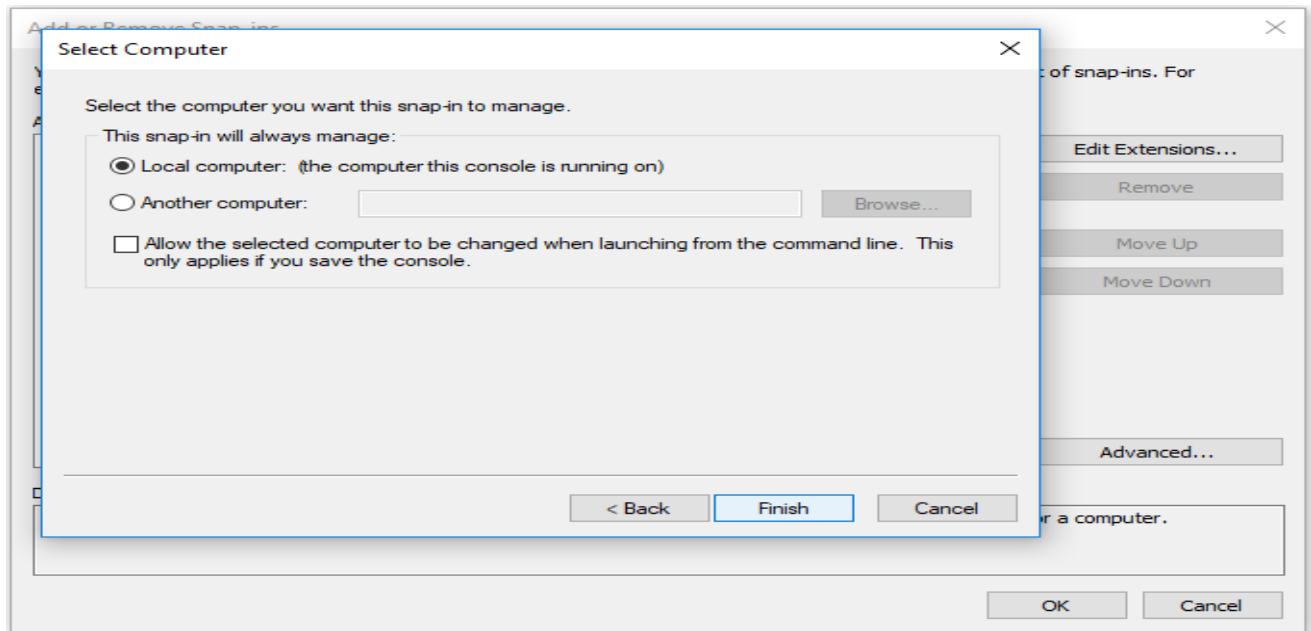


Figure 3 - 6 Select Computer

6. Upon completion, the screen shall appear as follow. Click **OK** button to commit the setting.

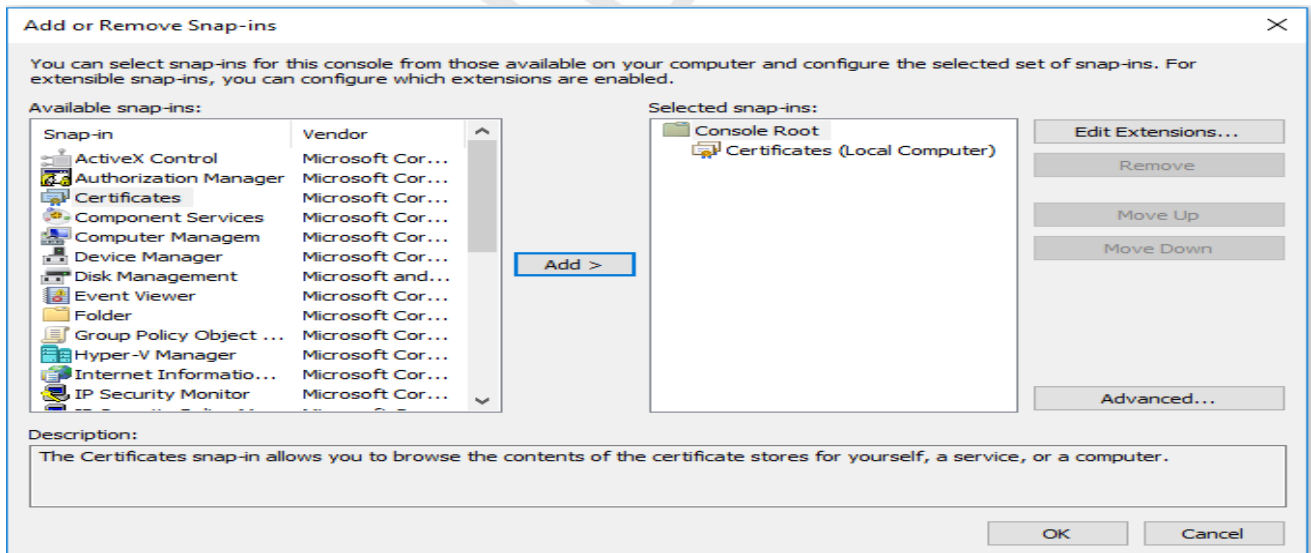


Figure 3 - 7 Add or Remove Snap-ins

7. To save the view configuration, at menu bar, click **File** and select **Save**.

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

8. In future, at the **Window Start Search** textbox, enter “Certs” to open this view.

3.4.1.2. Certificate Installation

1. At the Console Management software, select destination store:

Server CA Certificate and Client CA Certificate

- Select path “**Console Root\Certificates (Local Computer) \ Trusted Root Certification Authorities**

Stakeholder Certificate and Message Security Certificate

- Select path “**Console Root\ Certificates (Local Computer) \ Personal**”

2. Right click on the selected folder, select **All Tasks -> Import**

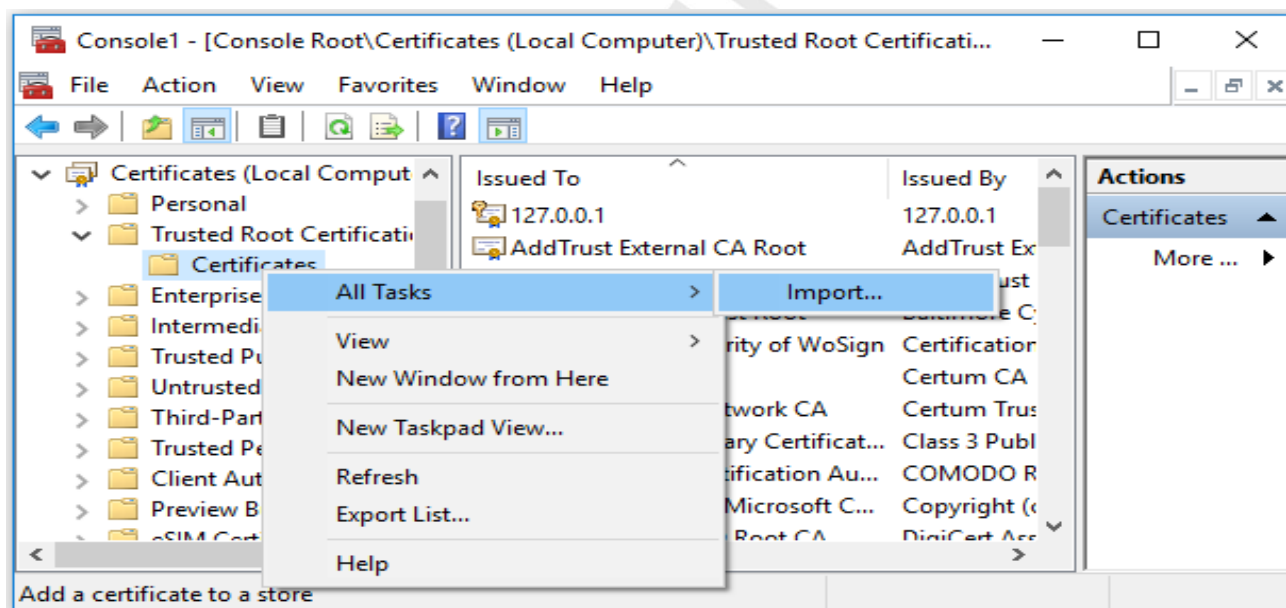


Figure 3 - 8 Import Certificates

3. **Certificate Import Wizard** appears. Click **Next** button. To select the intended certificate, click **Browse** button.

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

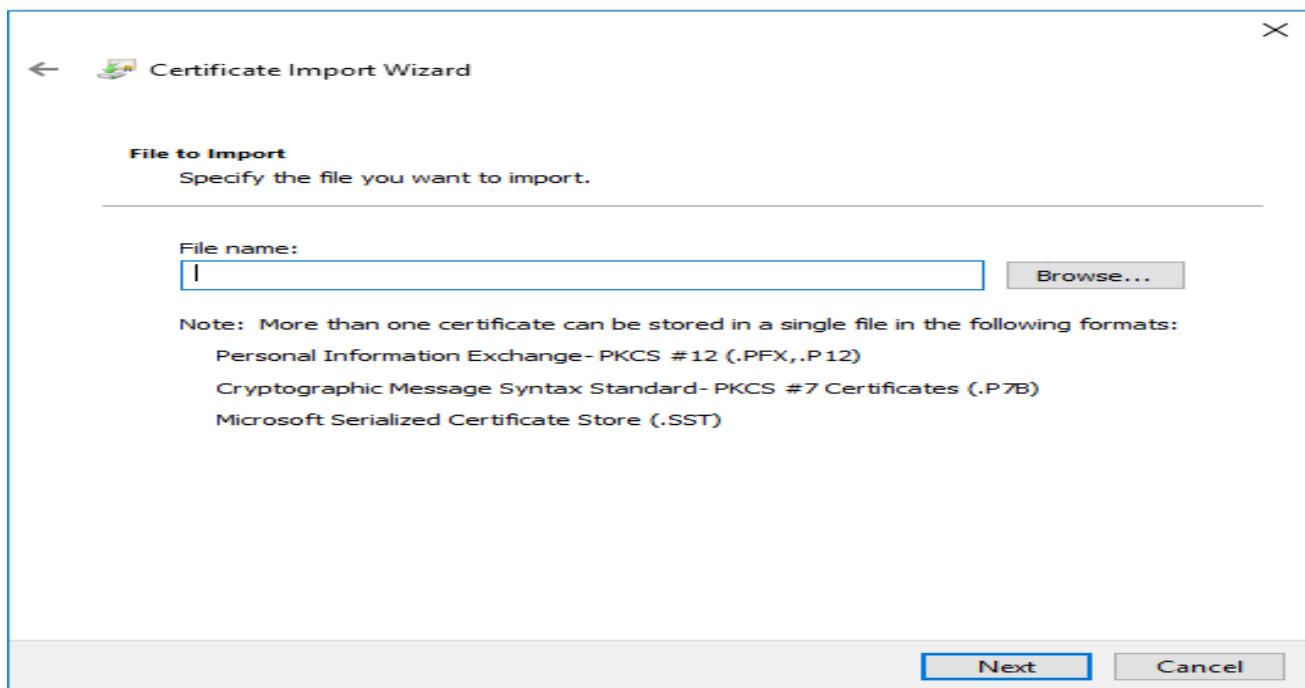


Figure 3 - 9 Browse to Insert Certificate

Note:

- A. To import certificate with private key, set the filter to “**Personal Information Exchange**” at the file open dialog:
- B. Enter the **password** in the Password textbox

3.4.1.3. Certificate Access Permission to Network Service

Perform the following steps to grant permission on the Message Security Private Key file to Network Service:

1. Launch **Command Prompt** with **Administrator** permission.
2. Identify the location of the **FindPrivateKey.exe**. (At least .NET Framework 2.0 is required to run the FindPrivateKey tool).

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

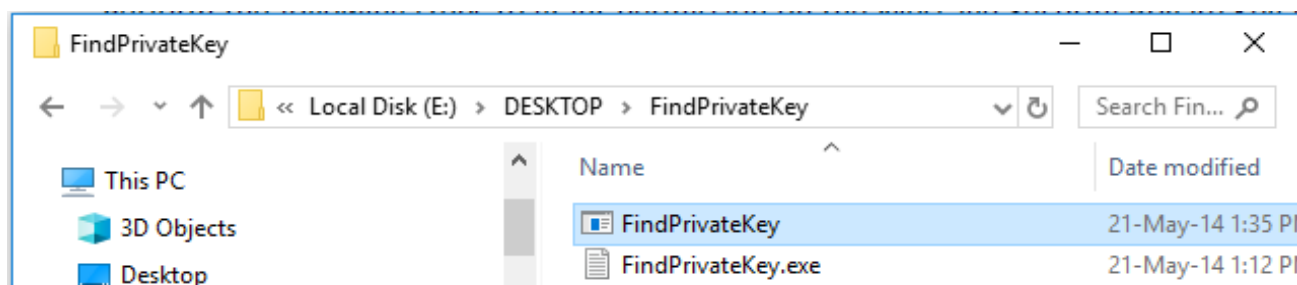


Figure 3 - 10 Locate FindPrivateKey.exe

3. Direct the command prompt to path where the FindPrivateKey.exe is located.

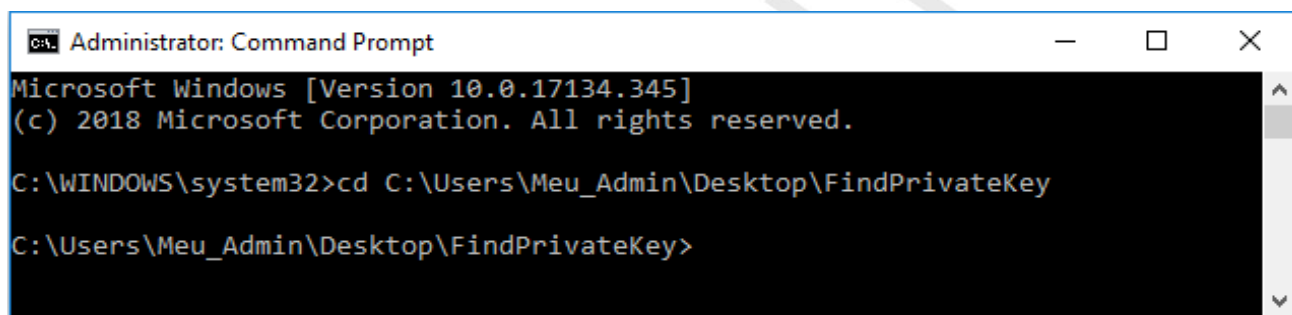


Figure 3 - 11 Launch Command Prompt

4. Click Windows Start button, type **mmc.exe**. Click mmc.exe to launch the **Console Management** software.

5. Navigate to path where the **Message Security Certificate** is located, i.e. "**Console Root\ Certificates (Local Computer) \ Personal**".

6. Double click on the Client Certificate (Certificate with stakeholder name). The Certificate window appears as below:

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

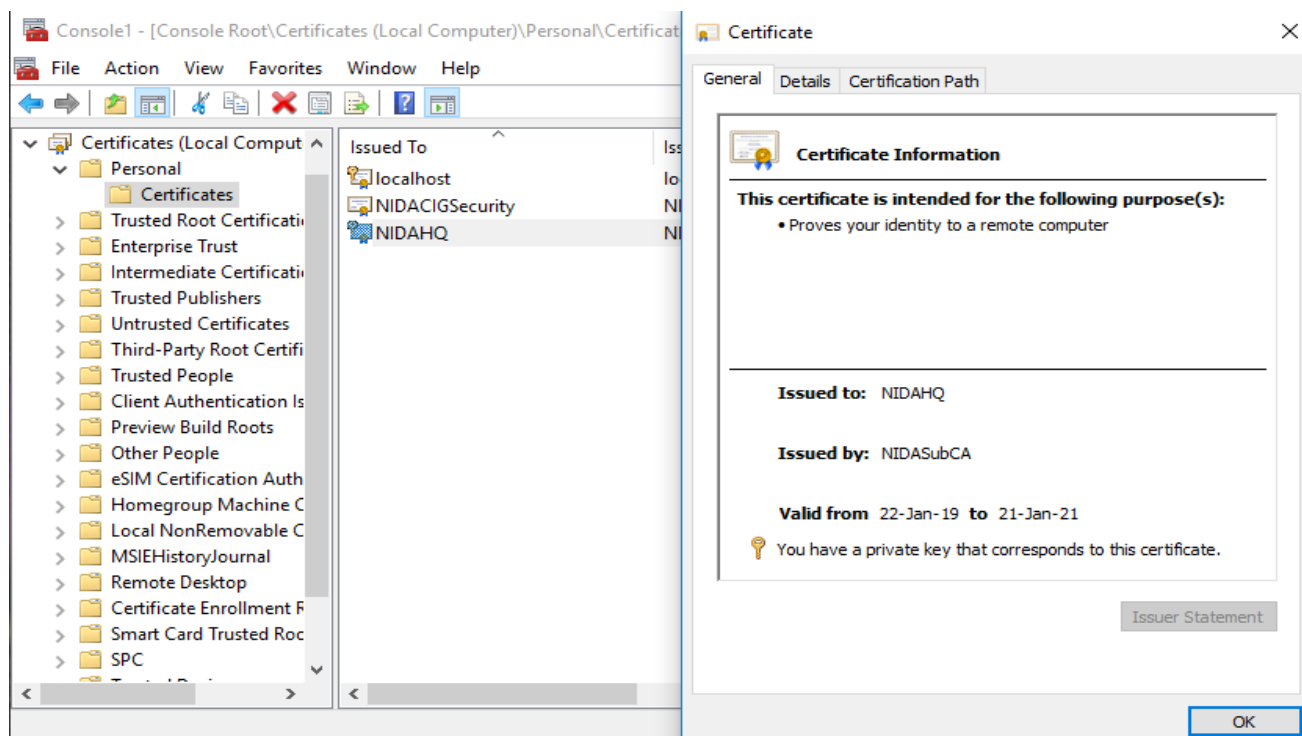


Figure 3 - 12 Client Certificate with Private key

7. At the Certificate windows, click **Details** tab. Search for certificate's **Thumbprint** and copy the value.

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

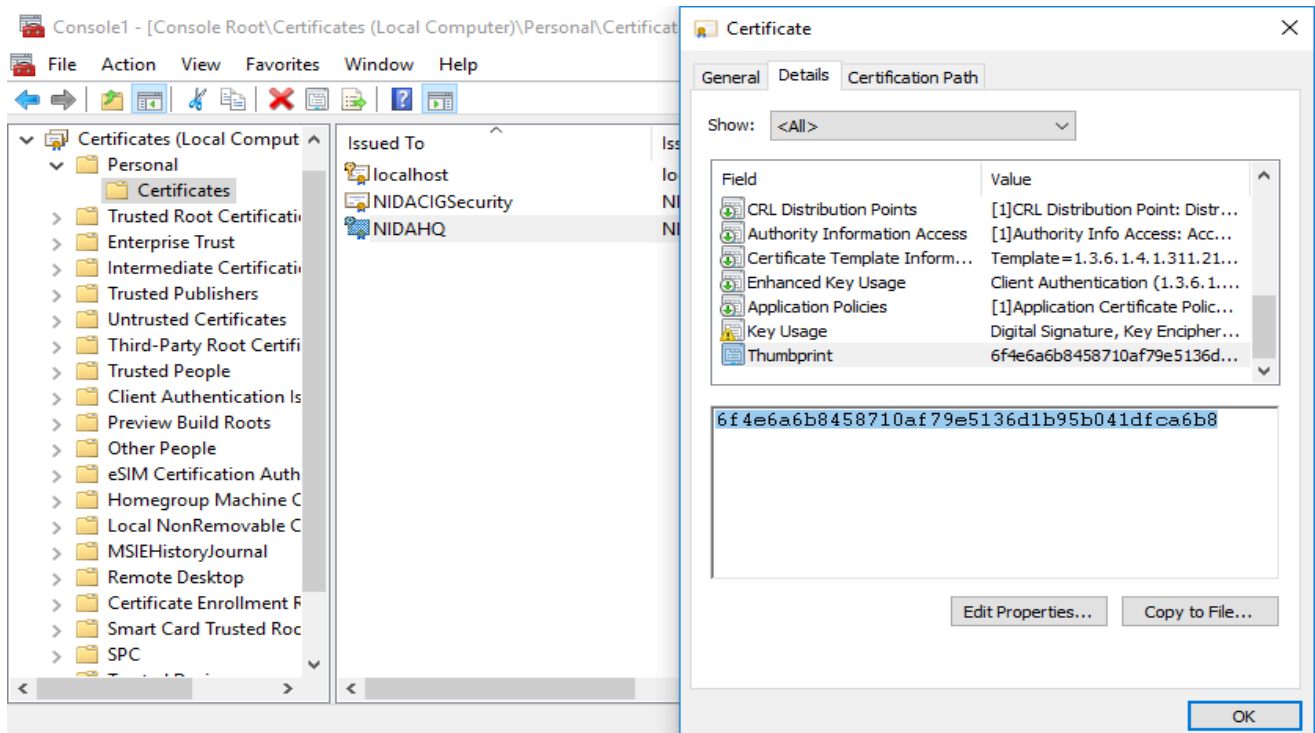


Figure 3 - 13 Client Certificate's Thumbprint

8. Enter command as shown in below with the copied **Thumbprint** value. Press **Enter** key to proceed.

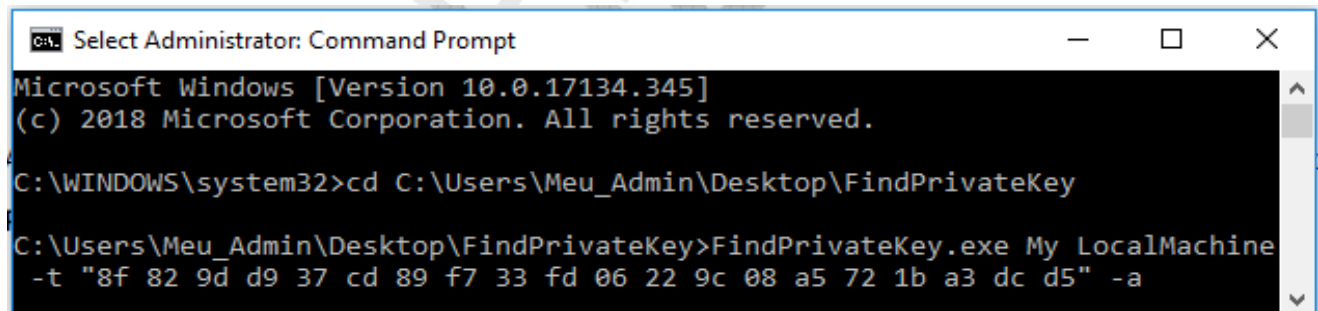
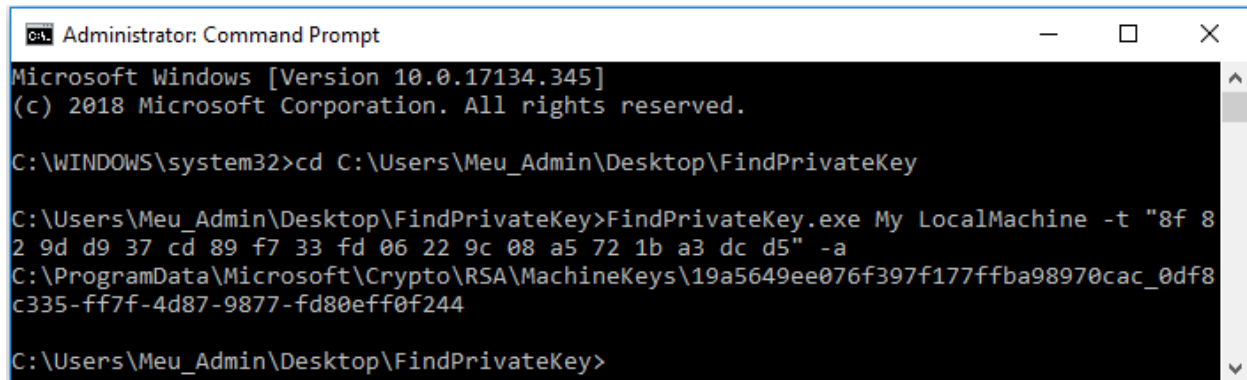


Figure 3 - 14 Copy Thumbprint to Command Prompt

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

9. Upon successful, the location of Private Key file will be retrieved.



```

Administrator: Command Prompt
Microsoft Windows [Version 10.0.17134.345]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>cd C:\Users\Meu_Admin\Desktop\FindPrivateKey

C:\Users\Meu_Admin\Desktop\FindPrivateKey>FindPrivateKey.exe My LocalMachine -t "8f 8
2 9d d9 37 cd 89 f7 33 fd 06 22 9c 08 a5 72 1b a3 dc d5" -a
C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\19a5649ee076f397f177ffb98970cac_0df8
c335-ff7f-4d87-9877-fd80eff0f244

C:\Users\Meu_Admin\Desktop\FindPrivateKey>

```

Figure 3 - 15 Location of Private Key file

10. Access to the Private Key storage path, and right click on the **Private Key** file and select **Properties**.

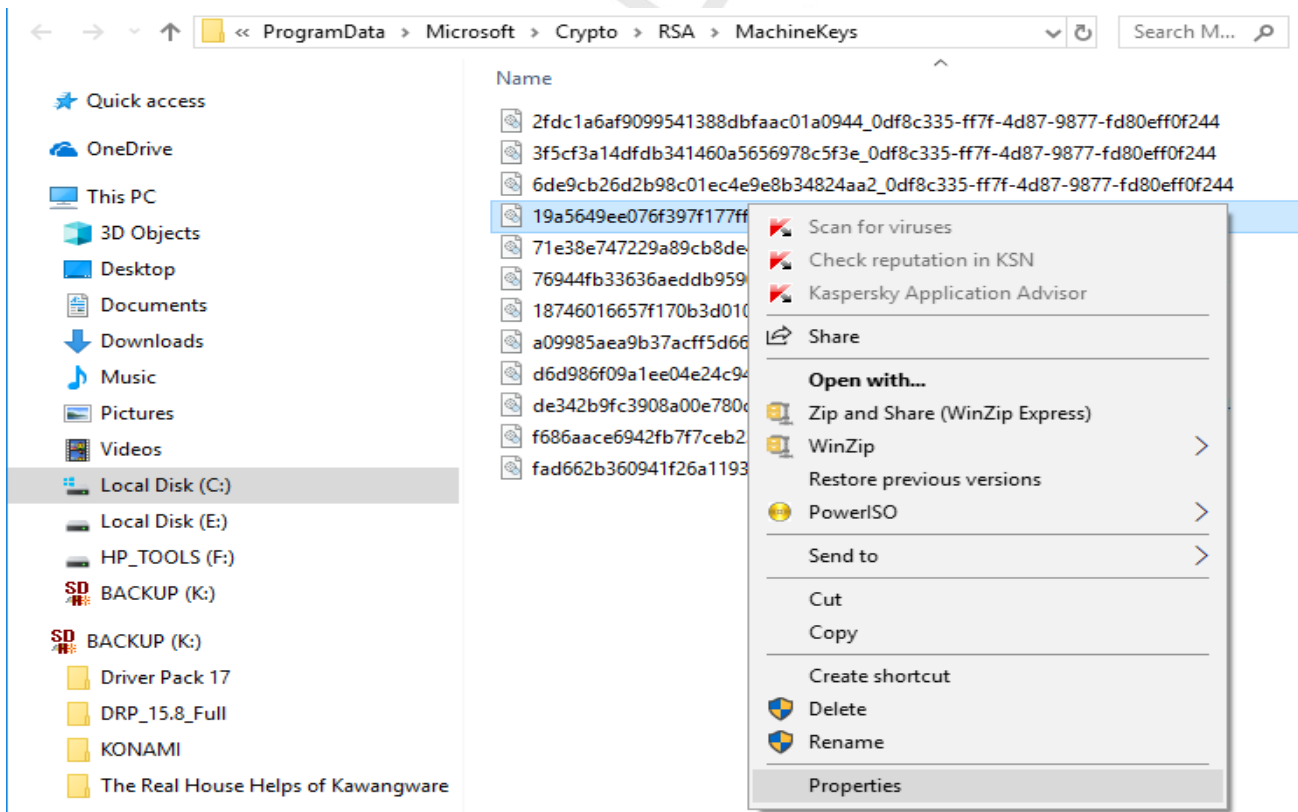


Figure 3 - 16 Properties of Private Key

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

11. File properties window appears. Select **Security** tab and click **Edit** button.
12. To add permission, click Add button and search for **Network Service** group.
13. Select the following two permissions, i.e. **Read & Execute** and **Read** for Network Service. Click **OK** button to commit.
14. To add permission again, click Add button and search for **IIS_IUSRS** group.
15. Select the following two permissions, i.e. **Read & Execute** and **Read** for Network Service. Click **OK** button to commit.

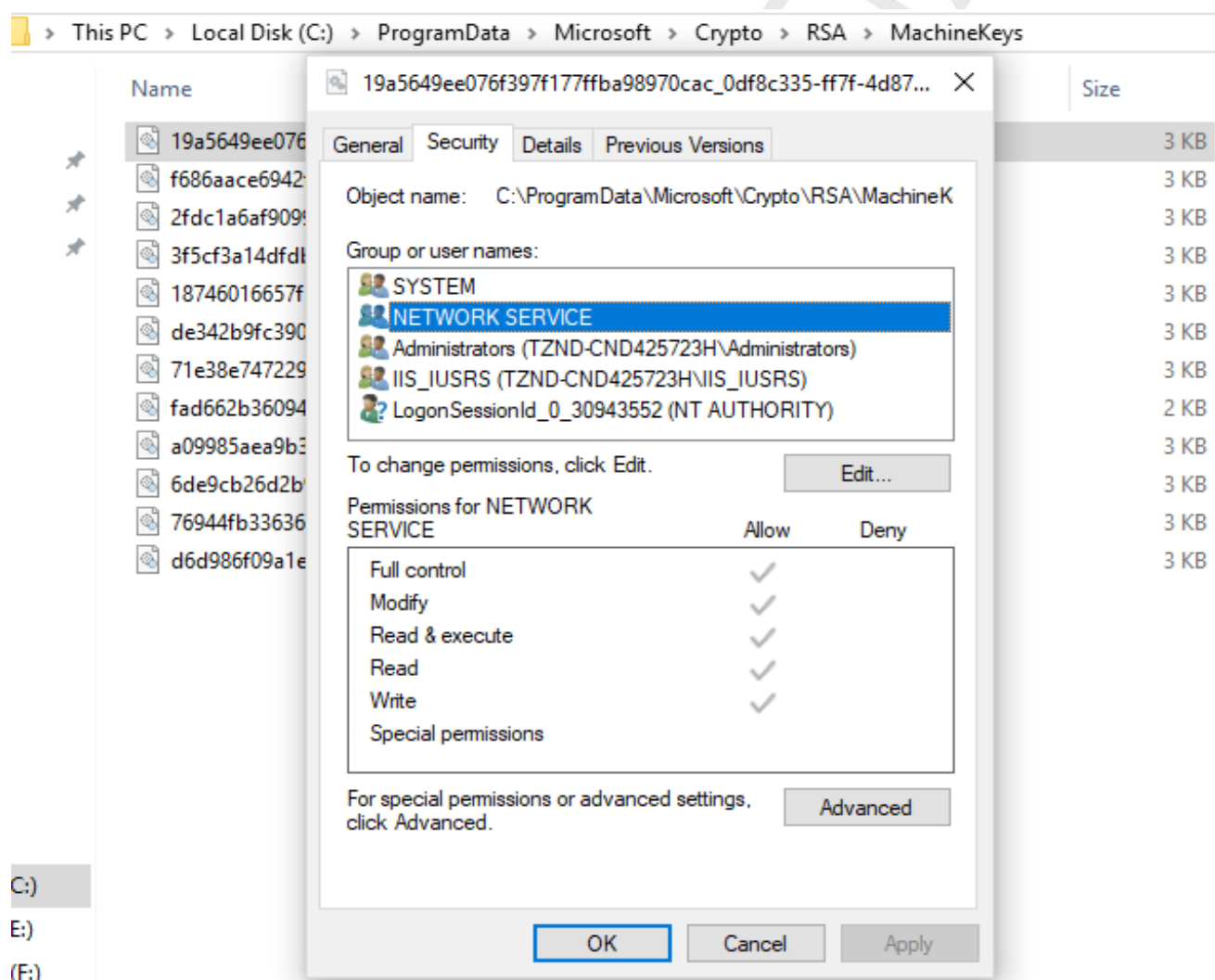


Figure 3 - 17 Set Access Permission of Private Key

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

4. CIG Web Services

Common Interface Gateway (CIG) is implemented as a standard interface which allows NIDA's authorized stakeholder to obtain data from NIDA Data Center database over a closed network. The CIG framework uses web service as the communication protocol to facilitate the information exchange between NIDA and the authorized stakeholder.

The Following are the summary of CIG web service methods available for external stakeholder:

No.	Web Service Method	Description
1.	Query Personal Information by OTP Authentication Method	To retrieve Tanzania Cardholder Personal Information by using One Time Password as a way to protect information retrieval without Cardholder's consent. A one-time password (OTP) is an automatically generated numeric that authenticates the user for a single transaction or session, it is a secure way to provide access to NIDA CIG or perform a transaction only one time. The password becomes invalid after it has been used and cannot be reused. Pre-Condition: The Phone number used here is that declared during National ID Registration. In OTP authentication Level of assurance is MEDIUM.
2.	Query Personal Information by Demographic Questions Authentication	To retrieve Tanzania Cardholder Personal Information by using Demographic questions generated randomly from information registered to NIDA as a way to protect information retrieval without Cardholder's consent.

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

		In Demographic authentication Level of assurance is LOW.
3.	Query Personal Information by Fingerprint Authentication	To retrieve Tanzania Cardholder Personal Information by using Biometric verification i.e. fingerprints as a way to protect information retrieval without Cardholder's consent. This is a user identity verification process that involves biological input, is widely known as the most effective type of authentication because it is extremely difficult to transfer biological material or features from one user to another. For NIDA CIG, fingerprint is used as a biological input in biometric authentication method. In Biometric authentication Level of assurance is HIGH.
4.	Query Personal Information Without Authentications (Special Case)	To retrieve Tanzania Cardholder Personal Information by just sending NIN, this is treated as a special case and this method is granted to special government institutions like Law Enforcers. It allows retrieving personal information even with cardholder absentees.
5.	Identification Method	This method is used to perform one to many identification searches.
6.	Transaction Verification Method	This is the method for comparing and then verifying all transactions which were sent by Stakeholder and were successfully verified by NIDA via National ID Common Interface Gateway (CIG)

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

Table 4 - 1 CIG Web Services for External Stakeholder

4.1. Query Personal Information by OTP Authentication Method

4.1.1. Method

Name:	OTPVerification
Description:	Tanzania cardholder basic demographic data will be retrieved with the specified NIN and One Time Password (OTP)

Table 4 - 2 OTP Authentication Method

4.1.1.1. Request Parameters

Name:	IRequest		
Direction:	Input		
Type:	OTPVerification		
	Content Model:		
	Component	Type	
	Header	RequestHeader	
		Contains elements as defined in the following table:	
		Component	Type
		Description	
		Id	String
		TimeStamp	Datetime
		ClientNameorIP	String
		UserId	String
	Body	RequestBody	
		Contains elements as defined in the following table:	
		Component	Type
		Description	

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

		CryptoInfo	RequestCryptoInfo	Contains elements as follows:	
				Component	Type
				*EncryptedCryptoKey	string
				*EncryptedCryptoIV	string
		Payload	String	Payload contains the following data which shall be encrypted with CryptoKey and CryptoIV as per the CryptoInfo. Refer to 4.1.1.2 for input data.	
		Signature	String	Digital signature generated with stakeholder Private Key.	

Table 4 - 3 OTP Authentication Request Parameters

4.1.1.2. Request Payload

Request payload shall be constructed in XML format which started with “Payload” as the first level element and follow by the following sub-elements:

No.	Element	Type	Description
1.	NIN.	String	NIN with 20 characters in length
2.	PhoneNumber	String	Phone number with 10 characters in length

Table 4 - 4 OTP Authentication Request Payload

Step 1: Send OTP

```
<Payload>
<NIN>XXXXXXXXXXXXxxx</NIN>
<PhoneNumber>XXXXXXXXXX</PhoneNumber>
</Payload>
```

Step 2: Verify OTP

```
<Payload>
<NIN>XXXXXXXXXXXXxxx</NIN>
```

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

<OTPVerificationCode>XXXXX</OTPVerificationCode>
</Payload>

Once OTP is verified data will be sent after sending the request that containing the OTPVerificationCode (Step 2)

4.1.1.3. Response

Name:	OTPVerificationResult			
Direction:	Output			
Type:	OTPVerificationResponse			
	Content Model:			
	Component	Type		
	Header	ResponseHeader		
		Contains elements as defined in the following table:		
		Component	Type	Description
		Id	String	System Generated ID
		TimeStamp	Datetime	System Generated timestamp
	Body	ResponseBody		
		Contains elements as defined in the following table:		
		Component	Type	Description
		CryptoInfo	ResponseCryptoInfo	Contains elements as follows:
Component				Type
*EncryptedCryptoKey				string
*EncryptedCryptoIV				String
Payload	String	Payload will be encrypted with the CryptoKey and CryptoIV as per CryptoInfo.		

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

				Decrypted payload contains string of character which begin with start tag (e.g. <section>) and end with end tag (e.g. </section>). Refer to 4.1.1.4 for detailed return value.
		Signature	String	Digital signature generated with GIC Server Private Key.
	Status	StatusSectionBase		
		Component	Type	Description
		Code	String	See Error or Status Codes and Descriptions

Table 4 - 5 OTP Authentication Response

4.1.1.4. Response Payload

The response payload is constructed in a root element (i.e. with tag named NidaResponse) which contain a group of child elements as defined in the following table.

Note: For child element which access is not granted to the stakeholder, the corresponding tags will be omitted from the response payload.

No.	Tag	Remarks
1	NATIONALIDNUMBER	Cardholder National ID Number
2	FIRSTNAME	Cardholder first name
3	MIDDLENAME	Cardholder middle name
4	LASTNAME	Cardholder last name
5	OTHERNAME	Cardholder other names
6	SEX	Cardholder gender
7	NATIONALITY	Cardholder Nationality
8	DATEOFBIRTH	Cardholder date of birth

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

		Date is formatted to YYYY-MM-DD
9	PLACEOFBIRTH	Cardholder place of birth
10	PLACEOFBIRTHCOUNTRY	Cardholder birth country
11	PLACEOFBIRTHREGION	Cardholder birth Region
12	PLACEOFBIRTHDISTRICT	Cardholder birth District
13	PLACEOFBIRTHWARD	Cardholder birth ward
14	BIRTHCERTIFICATENUMBER	Cardholder birth certificate Number
15	PHONENUMBER	Cardholder phone number
16	MARITALSTATUS	Cardholder marital status
17	OCCUPATION	Cardholder occupation
18	EMPLOYERNAME	Cardholder employer name
19	PRIMARYSCHOOLEDUCATION	Cardholder primary school education data
20	PRIMARYSCHOOLDISTRICT	Cardholder primary school district
21	PRIMARYSCHOOLYEAR	Cardholder primary education completion year
22	PERMANENTADDRESSCOUNTRY	Cardholder permanent address (country).
23	PERMANENTADDRESSREGION	Cardholder permanent address (Region). This tag is only applicable for Citizen
24	PERMANENTADDRESSDISTRICT	Cardholder permanent address (District). This tag is only applicable for Citizen
25	PERMANENTADDRESSWARD	Cardholder permanent address (Ward). This tag is only applicable for Citizen

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

26	PERMANENTADDRESSVILLAGE	Cardholder permanent address (Village). This tag is only applicable for Citizen
27	PERMANENTADDRESSSTREET	Cardholder permanent address (street). This tag is only applicable for Citizen
28	PERMANENTADDRESSPOSTCODE	Cardholder permanent address (postcode). This tag is only applicable for Citizen
29	ADDRESS1	Cardholder permanent address line 1. This tag is only applicable for noncitizen
30	ADDRESS2	Cardholder permanent address line 2. This tag is only applicable for noncitizen
31	ADDRESS3	Cardholder permanent address line 3. This tag is only applicable for noncitizen
32	ADDRESS4	Cardholder permanent address line 4. This tag is only applicable for noncitizen
33	ADDRESS5	Cardholder permanent address line 5. This tag is only applicable for noncitizen
34	RESIDENTIALADDRESSHOUSENUMBER	Cardholder residential address (house number)
35	RESIDENTIALADDRESSSTREET	Cardholder residential address (street)
36	RESIDENTIALADDRESSVILLAGE	Cardholder residential address (village)

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

37	RESIDENTIALADDRESSWARD	Cardholder residential address (ward)
38	RESIDENTIALADDRESSDISTRICT	Cardholder residential address (district)
39	RESIDENTIALADDRESSREGION	Cardholder residential address (region)
40	POSTCODE	Cardholder residential address (postcode)
41	POSTALADDRESS	Cardholder residential address (Postal Address)
42	CITIZENCERTIFICATEREGISTRATIONNUMBER	Cardholder Citizen Certificate Registration Number
43	DOSSIERNUMBER	Cardholder Dossier Number
44	FATHEROFAPPLICANTFULLNAME	Cardholder father full name which contains first, middle and last name
45	FATHEROFAPPLICANTCOUNTRYOFBIRTH	Cardholder father's country of Birth
46	FATHEROFAPPLICANTDATEOFBIRTH	Cardholder father's date of birth Date is formatted to YYYY-MM-DD
47	MOTHEROFAPPLICANTFULLNAME	Cardholder mother full name which contains first, middle and last name
48	MOTHEROFAPPLICANTCOUNTRYOFBIRTH	Cardholder mother's country of Birth
49	MOTHEROFAPPLICANTDATEOFBIRTH	Cardholder mother's date of birth Date is formatted to YYYY-MM-DD
50	PASSPORTNUMBER	Cardholder passport number
51	FATHERSIDENTIFICATIONNUMBER	Cardholder father's identification Number
52	MOTHERSIDENTIFICATIONNUMBER	Cardholder mother's identification Number
53	DRIVINGLICENSENUMBER	Cardholder driving license number
54	VOTERREGISTRATIONNUMBER	Cardholder voter registration Number

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

55	HEALTHINSURANCENUMBER	Cardholder health insurance Number
57	TAXIDENTIFICATIONNUMBER	Cardholder tax identification Number
58	IDNUMBEROFZANZIBARRESIDENT	Cardholder Zanzibar Resident ID Number
59	PENSIONORSOCIALSECURITYFUND	Cardholder pension or social security fund information
60	PENSIONORSOCIALSECURITYFUNDNUMBER	Cardholder pension or social security number
61	CERTIFICATIONNUMBEROFSECONDARYEDUCATION	Cardholder secondary education certification number
62	CERTIFICATIONNUMBEROFSECONDARYEDUCATIONOFGOG	Cardholder government secondary education certification number
63	RESIDENTPERMITNUMBER	Cardholder Resident Permit Number
64	RESIDENTPERMITEXPIRYDATE	Cardholder Resident Permit expiry date Date is formatted to YYYY-MM-DD
65	WORKPERMITNUMBER	Cardholder Working Permit Number
66	WORKPERMITEXPIRYDATE	Cardholder Working Permit expiry date Date is formatted to YYYY-MM-DD
67	REFUGEEIDCARDNUMBER	Cardholder Refugee ID card Number
68	REFUGEEIDCARDEXPIRYDATE	Cardholder Refugee ID card expiry date Date is formatted to YYYY-MM-DD
69	CONVENTIONTRAVELDOCUMENTNUMBER	Cardholder Convention Travel Document number
70	CONVENTIONTRAVELDOCUMENTEXPIRYDATE	Cardholder Convention Travel Document Expiry date Date is formatted to YYYY-MM-DD
71	PHOTO	Cardholder portrait image

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

		Portrait image is in JPEG format and returned in Base64 string
72	CENTERNUMBER	Enrolment Center Number
73	CENTERREGION	Enrolment Center Region
74	CENTERDISTRICT	Enrolment Center District
75	CENTERWARD	Enrolment Center Ward
76	CENTERNAME	Enrolment Center Name
77	APPLICATIONDATE	Enrolment Application Date Date is formatted to YYYY-MM-DD
78	LEFTFINGERINDICATOR	Enrolled left fingerprint indicator 2 bytes fingerprint indicator as follow: o L1 – Left Thumb o L2 – Left Index o L3 – Left Middle o L4 – Left Ring o L5 – Left Little
79	LEFTFINGERIMAGE	Enrolled left fingerprint image associated with LeftFingerIndicator Fingerprint image is in JPEG format and returned in Base64 string
80	LEFTFINGERTEMPLATE	Enrolled left fingerprint template associated with LeftFingerIndicator Fingerprint template is in ISO format and returned in Base64 string
81	RIGHTFINGERINDICATOR	Enrolled right fingerprint indicator 2 bytes fingerprint indicator as follow: o R1 – Right Thumb o R2 – Right Index o R3 – Right Middle

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

		- o R4 – Right Ring - o R5 – Right Little
82	RIGHTFINGERIMAGE	Enrolled right fingerprint image associated with RightFingerIndicator Fingerprint image is in JPEG format and returned in Base64 string
83	RIGHTFINGERPRINTTEMPLATE	Enrolled right fingerprint template associated with RightFingerIndicator Fingerprint template is in ISO format and returned in Base64 string
84	BIOMETRICRESULT	See Error Description & Status Codes
85	SIGNATURE	Cardholder Signature image Signature image is in JPEG format and returned in Base64 string

Table 4 - 6 OTP Authentication Response Payload

4.1.1.5. Sample Response Payload

<NidaResponse>

<NIN>19760507111010000122</NIN>

<FIRSTNAME>VINCENT</FIRSTNAME>

<OTHERNAMES />

<SEX>MALE</SEX>

<DATEOFBIRTH>1976-05-07</DATEOFBIRTH>

<PLACEOFBIRTH />

<PA1 />

<SURNAME>WATT</SURNAME>

<PERMANENTCOUNTRY />

<RESIDENTREGION>DAR ES SALAAM (ILALA CBD)</RESIDENTREGION>

<RESIDENTDISTRICT>ILALA CBD</RESIDENTDISTRICT>

<RESIDENTWARD>KIVUKONI</RESIDENTWARD>

<RESIDENTVILLAGE>KIVUKONI</RESIDENTVILLAGE>

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

<RESIDENTSTREET>TRET</RESIDENTSTREET>
 <RESIDENTHOUSENO />
 <RESIDENTPOSTALADDRESS />
 <RESIDENTPOSTCODE>4473</RESIDENTPOSTCODE>
 <CITIZENPERMANENTCOUNTRY>TANZANIA, THE UNITED
 REPUBLIC</CITIZENPERMANENTCOUNTRY>
 <PERMANENTREGION>GEITA</PERMANENTREGION>
 <PERMANENTDISTRICT />
 <PERMANENTWARD>USHIROMBO</PERMANENTWARD>
 <PERMANENTVILLAGE>NANSANSA</PERMANENTVILLAGE>
 <PERMANENTSTREET>RET</PERMANENTSTREET>
 <BIRTHCOUNTRY>TANZANIA, THE UNITED REPUBLIC</BIRTHCOUNTRY>
 <BIRTHREGION>KASKAZINI PEMBA</BIRTHREGION>
 <BIRTHDISTRICT>MICHEWENI</BIRTHDISTRICT>
 <BIRTHWARD>WINGWI NJUGUNI</BIRTHWARD>
 <BIRTHCERTIFICATENO />
 <NATIONALITY>TANZANIAN</NATIONALITY>
 <PHONENUMBER>0714466330</PHONENUMBER>
 <MARITALSTATUS>SINGLE</MARITALSTATUS>
 <OCCUPATION>EMPLOYED</OCCUPATION>
 <EMPLOYERNAME>COMPANY</EMPLOYERNAME>
 <PRIMARYSCHOOLEDUCATION />
 <PRIMARYSCHOOLDISTRICT />
 <PRIMARYSCHOOLYEAR />
 <DOSSIERNUMBER />
 <CITIZENCERTREGNO>RERE324234</CITIZENCERTREGNO>
 <FATHERSFIRSTNAME>DFR</FATHERSFIRSTNAME>
 <FATHERSMIDDLENAME>DF</FATHERSMIDDLENAME>
 <FATHERSLASTNAME>DF</FATHERSLASTNAME>
 <FATHERSCOUNTRYOFBIRTH>TANZANIA, THE UNITED
 REPUBLIC</FATHERSCOUNTRYOFBIRTH>
 <FATHERSDATEOFBIRTH>1950-03-04</FATHERSDATEOFBIRTH>

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

<MOTHERSFIRSTNAME>T</MOTHERSFIRSTNAME>
 <MOTHERSMIDDLENAME>RT</MOTHERSMIDDLENAME>
 <MOTHERSLASTNAME>RT</MOTHERSLASTNAME>
 <MOTHERSCOUNTRYOFBIRTH>TANZANIA, THE UNITED
 REPUBLIC</MOTHERSCOUNTRYOFBIRTH>
 <MOTHERSDATEOFBIRTH>1954-07-08</MOTHERSDATEOFBIRTH>
 <PASSPORTNO />
 <FATHERSNIN />
 <MOTHERSNIN />
 <DRIVINGLICENCENO />
 <VOTERREGISTRATIONNO />
 <HEALTHINSURANCENO />
 <TAXIDNO />
 <ZANZIBARIDNO />
 <PENSIONSOCIALSECURITYFUND />
 <PENSIONSOCIALSECURITYNO />
 <CERTNOSECEducation />
 <CERTNOADVSECEducation />
 <RESIDENTPERMITNO />
 <PERMITRESIDENTEXPIRYDATE />
 <WORKPERMITNO />
 <WORKPERMITEXPIRYDATE />
 <REFUGEEIDNO />
 <REFUGEEIDEXPIRYDATE />
 <CONVENTIONTRAVELDOCUMENTNO />
 <CONVENTIONTRAVELEXPIRYDATE />
 <SIGNATURE>**Signature (64-base strings)**<SIGNATURE>
 <PHOTO>**Photo (64-base strings)**<PHOTO>
 </NidaResponse>

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

4.2. Query Personal Information by Biometric Fingerprint Authentication Method

4.2.1. Method

Name:	BiometricVerification
Description:	Tanzania cardholder basic demographic data will be retrieved with the specified NIN and Fingerprint verification.

4.2.1.1. Request Parameters

Name:	IRequest		
Direction:	Input		
Type:	BiometricVerification		
	Content Model:		
	Component	Type	
	Header	RequestHeader	
		Contains elements as defined in the following table:	
		Component	Type
		Description	
		Id	String
		TimeStamp	Datetime
		ClientNameorIP	String
		UserID	String
	Body	RequestBody	
		Contains elements as defined in the following table:	
		Component	Type
		Description	

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

		CryptoInfo	RequestCryptoInfo	Contains elements as follows:	
				Component	Type
				*EncryptedCryptoKey	string
				*EncryptedCryptoIV	string
		Payload	String	Payload contains the following data which shall be encrypted with CryptoKey and CryptoIV as per the CryptoInfo. Refer to 4.1.1.2 for input data.	
		Signature	String	Digital signature generated with stakeholder Private Key.	

Table 4 - 7 BiometricVerification Authentication Request Parameters

4.2.1.2. Request Payload

Request payload shall be constructed in XML format which started with “Payload” as the first level element and follow by the following sub-elements:

No.	Element	Type	Description
1.	NIN.	String	NIN with 20 characters in length
2.	FINGERIMAGE	String	Fingerprint Image base64
3.	FINGERCODE	String	Finger Code (R1, R2, R3, R4, R5, L1, L2, L3, L4, L5)

Table 4 - 8 BiometricVerification Authentication Request Payload

Example:

```

<Payload>
<NIN>12345678901234567890</NIN>
<FINGERIMAGE></FINGERIMAGE>
<FINGERCODE>R1</FINGERCODE>
</Payload>

```

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

4.2.1.3. Response

Name:	BiometricVerificationResult		
Direction:	Output		
Type:	BiometricVerificationResponse		
	Content Model:		
	Component	Type	
	Header	ResponseHeader	
		Contains elements as defined in the following table:	
		Component	Type
		Id	String
		TimeStamp	Datetime
		System Generated timestamp	
	Body	ResponseBody	
		Contains elements as defined in the following table:	
		Component	Type
		CryptoInfo	ResponseCryptoInfo
		Contains elements as follows:	
		*EncryptedCryptoKey	string
		*EncryptedCryptoIV	string
	Payload	String	Payload will be encrypted with the CryptoKey and CryptoIV as per CryptoInfo. Decrypted payload contains string of character which begin with start tag (e.g.

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

				<section>) and end with end tag (e.g. </section>). Refer to 4.1.1.4 for detailed return value.
		Signature	String	Digital signature generated with GIC Server Private Key.
	Status	StatusSectionBase		
		Component	Type	Description
		Code	Int	See Error or Status Codes and Descriptions

Table 4 - 9 BiometricVerification Authentication Response

4.2.1.4. Response Payload

The response payload is constructed in a root element (i.e. with tag named NidaResponse) which contain a group of child elements as defined in the following table.

Note: For child element which access is not granted to the stakeholder, the corresponding tags will be omitted from the response payload.

See **4.1.1.4** for response payload table.

4.2.1.5. Sample Response Payload

See **4.1.1.5** for sample response payload

If the Response code is 141, the simple response payload will suggest on fingers to be used for verification which have been found in National ID system.

<NidaReponse>

<Fingerprints>R1 | R2 | R3 | R4 | R5 | L1 | L2 | L3 | L4 | L5</Fingerprints>

</ NidaReponse>

If the response code is 172 means the applicant has no fingerprint registered and Alternative to Biometric method can be switched for alternative verification.

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

4.3. Alternative to Biometric Verification Method

4.3.1. Method

Name:	AltBiometricVerification
Description:	This method used when stakeholder failed to verify a customer by Biometric Verification provided that customer has not registered fingerprints.

Table 4 - 10: AltBiometric Verification Method

4.3.1.1. Request Parameters

Name:	IRequest			
Direction:	Input			
Type:	AltBiometricVerification			
	Content Model:			
	Component	Type		
	Header	RequestHeader		
		Contains elements as defined in the following table:		
		Component	Type	Description
		Id	String	System Generated ID
		TimeStamp	Datetime	System Generated timestamp
		ClientNameorIP	String	Caller Machine IP (Auto-detected by system)
	UserID	String	Stakeholder User ID	
Body	RequestBody			
	Contains elements as defined in the following table:			
	Component	Type	Description	
	CryptoInfo	RequestCryptoInfo	Contains elements as follows:	

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

				Component	Type
				*EncryptedCryptoKey	string
				*EncryptedCryptoIV	string
				Payload	String
				Payload contains the following data which shall be encrypted with CryptoKey and CryptoIV as per the CryptoInfo. Refer to 4.5.1.2 for input data.	
				Signature	String
				Digital signature generated with stakeholder Private Key.	

Table 4 - 11 AltBiometricVerification Request Parameters

4.3.1.2. Request Payload

Request payload shall be constructed in XML format which started with “Payload” as the first level element and follow by the following sub-elements:

No.	Element	Type	Description
1.	NIN.	String	NIN with 20 characters in length
2.	Question Code	String	Every Question has code number
3.	Answer	String	Answer of questions asked

Table 4 - 12 AltBiometricVerification Request Parameters

Step 1: Request First Question by sending the following Payload

```
<Payload>
<NIN>XXXXXXXXXXXXxxx</NIN>
</Payload>
```

Step 2: Submit the answer with the following Payload

```
<Payload>
<NIN>XXXXXXXXXXXXxxx</NIN>
<RQCode>XXXXXXX</RQCode>
```

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

<QNANSW>XXXXXX</QNANSW>
</Payload>

After receiving Response Payload, you can check if the Previous answer was correct by checking if the 'PREV_ANSW_CODE' tag has a value of 123 if this tag has a value of 124 means the Previous answer was **incorrect**.

Once the number of Correct answers is equal to the suggested (2), then data will be sent in the Response Payload.

4.3.1.3. Response

Name:	AltBiometricVerificationResult		
Direction:	Output		
Type:	GetAltBiometricVerificationResponse		
	Content Model:		
	Component	Type	
	Header	ResponseHeader	
		Contains elements as defined in the following table:	
		Component	Type
		Id	String
		TimeStamp	Datetime
		System Generated timestamp	
	Body	ResponseBody	
		Contains elements as defined in the following table:	
		Component	Type
		CryptoInfo	ResponseCryptoInfo
		Contains elements as follows:	
		Component	Type
		*EncryptedCryptoKey	string
		*EncryptedCryptoIV	string

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

		Payload	String	Payload will be encrypted with the CryptoKey and CryptoIV as per CryptoInfo. Decrypted payload contains string of character which begin with start tag (e.g. <section>) and end with end tag (e.g. </section>). Refer to 4.1.1.4 for detailed return value.
		Signature	String	Digital signature generated with GIC Server Private Key.
	Status	StatusSectionBase		
		Component	Type	Description
		Code	Int	See Error or Status Codes and Descriptions

Table 4 - 13 AltBiometricVerification Request Response

4.3.1.4. Response Payload

The response payload is constructed in a root element (i.e. with tag named NidaResponse) which contain a group of child elements as defined in the following table.

Note: For child element which access is not granted to the stakeholder, the corresponding tags will be omitted from the response payload.

See **4.1.1.5** for response payload table.

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

4.4. Query Personal Information by Demographic Questions Authentication Method

4.4.1. Method

Name:	RQVerification
Description:	Tanzania cardholder basic demographic data will be retrieved with the specified NIN and Answers of Demographic Questions.

Table 4 - 14 RQVerification Authentication Method

4.4.1.1. Request Parameters

Name:	IRequest		
Direction:	Input		
Type:	RQVerification		
	Content Model:		
	Component	Type	
	Header	RequestHeader	
		Contains elements as defined in the following table:	
		Component	Type Description
		Id	String System Generated ID
		TimeStamp	Datetime System Generated timestamp
		ClientNameorIP	String Caller Machine IP (Auto-detected by system)
		UserID	String Stakeholder User ID
	Body	RequestBody	
		Contains elements as defined in the following table:	
		Component	Type Description

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

		CryptoInfo	RequestCryptoInfo	Contains elements as follows:	
				Component	Type
				*EncryptedCryptoKey	string
				*EncryptedCryptoIV	string
		Payload	String	Payload contains the following data which shall be encrypted with CryptoKey and CryptoIV as per the CryptoInfo. Refer to 4.1.1.2 for input data.	
		Signature	String	Digital signature generated with stakeholder Private Key.	

Table 4 - 15 RQVerification Authentication Request Parameters

4.4.1.2. Request Payload

Request payload shall be constructed in XML format which started with “Payload” as the first level element and follow by the following sub-elements:

No.	Element	Type	Description
1.	NIN.	String	NIN with 20 characters in length
2.	Question Code	String	Every Question has code number
3.	Answer	String	Answer of questions asked

Table 4 - 16 RQVerification Authentication Request Parameters

Step 1: Request First Question by sending the following Payload

```
<Payload>
<NIN>XXXXXXXXXXXXxxx</NIN>
</Payload>
```

Step 2: Submit the answer with the following Payload

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

```

<Payload>
<NIN>XXXXXXXXXXXXxxx</NIN>
<RQCode>XXXXXXXX</RQCode>
<QNANSW>XXXXXX</QNANSW>
</Payload>

```

After receiving Response Payload, you can check if the Previous answer was correct by checking if the 'PREV_ANSW_CODE' tag has a value of 123 if this tag has a value of 124 means the Previous answer was **incorrect**.

Once the number of Correct answers is equal to the suggested (2), then data will be sent in the Response Payload.

4.4.1.3. Response

Name:	RQVerificationResult		
Direction:	Output		
Type:	GetRQVerificationResponse		
	Content Model:		
	Component	Type	
	Header	ResponseHeader	
		Contains elements as defined in the following table:	
		Component	Type
		Id	String
		TimeStamp	Datetime
		System Generated timestamp	
	Body	ResponseBody	
		Contains elements as defined in the following table:	
		Component	Type
		CryptoInfo	ResponseCryptoInfo
		Contains elements as follows:	
		Component	Type

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

				*EncryptedCryptoKey	string
				*EncryptedCryptoIV	string
		Payload	String	Payload will be encrypted with the CryptoKey and CryptoIV as per CryptoInfo. Decrypted payload contains string of character which begin with start tag (e.g. <section>) and end with end tag (e.g. </section>). Refer to 4.1.1.4 for detailed return value.	
		Signature	String	Digital signature generated with GIC Server Private Key.	
	Status	StatusSectionBase			
		Component	Type	Description	
		Code	Int	See Error or Status Codes and Descriptions	

Table 4 - 17 RQVerification Authentication Request Response

4.4.1.4. Response Payload

The response payload is constructed in a root element (i.e. with tag named NidaResponse) which contain a group of child elements as defined in the following table.

Note: For child element which access is not granted to the stakeholder, the corresponding tags will be omitted from the response payload.

See **4.1.1.4** for response payload table.

4.4.1.5. Sample Response Payload

See **4.1.1.5** for sample response payload

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

4.4.1.6. Error or Status Codes and Descriptions

SN	Error Code	Error Description
1	000	Stakeholder Account is ok.
2	001	Stakeholder Account does not exist
3	002	Stakeholder Account is Suspended
4	003	Stakeholder Account has expired
5	010	Certificate is ok.
6	011	Stakeholder Certificates are not ok.
7	012	CIG Certificate is not ok.
8	020	Signature Verification Success
9	021	Signature Verification fail
10	030	Decryption of Key and IV is Success
11	031	Decryption of Key not Success
12	032	Decryption of IV not Success
13	040	Decryption of Payload Success
14	041	Decryption of Payload not Success
15	042	Payload is not in XML format
16	050	This CIG Method is Allowed for you institution
17	051	This CIG Method is not allowed for your institution
18	060	Phone Number entered is similar to number registered by NIDA
19	061	Phone Number entered is different from Number registered by NIDA
20	060	OTP has been successfully sent
21	063	Failed to send OTP
22	060	OTP Verified successfully
23	064	Failed to verify OTP
24	070	Payload Encrypted Successfully
25	071	Failed to Encrypt Payload
26	080	Signature Successfully generated
27	081	Failed to generate signature
28	090	Key and IV Encrypted Successfully
29	091	Failed to Encrypt Key
30	092	Failed to Encrypt IV
31	100	Response XML processed successfully
32	101	Failed to process XML Response
33	102	No data assigned for this Stakeholder Account
34	111	Unable to process XML Payload Request
35	120	Success Loaded Question Codes.
36	121	Failed to load Question Codes.
37	122	Limited number of attempts on answering security questions has been reached.
38	123	Previous answer was correct
39	124	Previous answer was incorrect

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

40	130	NIN is valid
41	131	NIN is invalid
42	132	NIN not Found
43	140	Biometric Fingerprint Verification Success
44	141	Biometric Fingerprint Verification Failed
45	142	Invalid Fingerprint data
46	143	Invalid Finger codes
47	150	Transaction has successfully verified
48	151	Transaction has not successfully verified
49	152	Transaction not found
50	153	Invalid web method
51	154	Invalid Transaction ID
52	155	Invalid Stakeholder ID
53	156	Missing Input Parameters
54	160	Identification Match Found
55	161	Identification Match not Found
56	162	Unspecified Response from Matching Engine
57	163	Wait for Matching Engine to process your request
58	164	Request ID not Registered
59	165	Payload is missing fingerprint
60	170	Alternative to biometric verification allowed for this ID holder
61	171	Alternative to biometric verification not allowed for this ID holder
62	172	Switch to alternative to biometric verification
63	00	General Success
64	01	General Failure.

Table 4 - 18 Error Code and Descriptions

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

4.5. Query Personal Information Without Authentication Method

4.5.1. Method

Name:	QueryFullDemographic
Description:	Tanzania cardholder basic demographic data will be retrieved with the specified NIN only.

Table 4 - 19 QueryFullDemographic Method

4.5.1.1. Request Parameters

Name:	IRequest		
Direction:	Input		
Type:	RQVerification		
	Content Model:		
	Component	Type	
	Header	RequestHeader	
		Contains elements as defined in the following table:	
		Component	Type
		Description	
		Id	String
		TimeStamp	Datetime
		ClientNameorIP	String
		UserID	String
	Body	RequestBody	
		Contains elements as defined in the following table:	
		Component	Type
		Description	
		CryptoInfo	RequestCryptoInfo
		Contains elements as follows:	

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

				Component	Type
				*EncryptedCryptoKey	string
				*EncryptedCryptoIV	string
		Payload	String	Payload contains the following data which shall be encrypted with CryptoKey and CryptoIV as per the CryptoInfo. Refer to 4.1.1.2 for input data.	
		Signature	String	Digital signature generated with stakeholder Private Key.	

Table 4 - 20 QueryFullDemographic Request Parameters

4.5.1.2. Request Payload

Request payload shall be constructed in XML format which started with “Payload” as the first level element and follow by the following sub-elements:

No.	Element	Type	Description
1.	NIN.	String	NIN with 20 characters in length
2.	Question Code	String	Every Question has code number
3.	Answer	String	Answer of questions asked

Table 4 - 21 QueryFullDemographic Request Parameters

Step 1: Request by Sending NIN

```
<Payload>
<NIN>XXXXXXXXXXXXxxx</NIN>
</Payload>
```

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

4.5.1.3. Response

Name:	QueryFullDemographicResult		
Direction:	Output		
Type:	GetQueryFullDemographicResponse		
	Content Model:		
	Component	Type	
	Header	ResponseHeader	
		Contains elements as defined in the following table:	
		Component	Type
		Id	String
		TimeStamp	Datetime
		System Generated timestamp	
	Body	ResponseBody	
		Contains elements as defined in the following table:	
		Component	Type
		CryptoInfo	ResponseCryptoInfo
		Contains elements as follows:	
		Component	Type
		*EncryptedCryptoKey	string
		*EncryptedCryptoIV	string
	Payload	String	Payload will be encrypted with the CryptoKey and CryptoIV as per CryptoInfo. Decrypted payload contains string of character which begin with start tag (e.g.

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

				<section>) and end with end tag (e.g. </section>). Refer to 4.1.1.4 for detailed return value.
		Signature	String	Digital signature generated with GIC Server Private Key.
	Status	StatusSectionBase		
		Component	Type	Description
		Code	Int	See Error or Status Codes and Descriptions

Table 4 - 22 QueryFullDemographic Request Response

4.5.1.4. Response Payload

The response payload is constructed in a root element (i.e. with tag named NidaResponse) which contain a group of child elements as defined in the following table.
Note: For child element which access is not granted to the stakeholder, the corresponding tags will be omitted from the response payload.

See **4.1.1.4** for response payload table.

4.5.1.5. Sample Response Payload

See **4.1.1.5** for sample response payload

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

4.6. Transaction Verification Method

4.6.1. Method

Name:	TransactionVerification
Description:	This is the method for comparing and then verifying all success transactions which were sent by Stakeholder.

Table 4 - 23: Transaction Verification Method

4.6.1.1. Request Parameters

Name:	IRequest			
Direction:	Input			
Type:	TransactionVerification			
	Content Model:			
	Component	Type		
	Header	RequestHeader		
		Contains elements as defined in the following table:		
		Component	Type	Description
		Id	String	System Generated ID
		TimeStamp	Datetime	System Generated timestamp
		ClientNameorIP	String	Caller Machine IP (Auto-detected by system)
		UserID	String	Stakeholder User ID
Body	RequestBody			
	Contains elements as defined in the following table:			
	Component	Type	Description	
	CryptoInfo	RequestCryptoInfo	Contains elements as follows:	

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

				Component	Type
				*EncryptedCryptoKey	string
				*EncryptedCryptoIV	string
				Payload	String
				Payload contains the following data which shall be encrypted with CryptoKey and CryptoIV as per the CryptoInfo. Refer to 4.5.1.2 for input data.	
				Signature	String
				Digital signature generated with stakeholder Private Key.	

Table 4 - 24 TransactionVerification Request Parameters

4.6.1.2. Request Payload

Request payload shall be constructed in XML format which started with “Payload” as the first level element and follow by the following sub-elements:

No.	Element	Type	Description
1.	NIN.	String	NIN with 20 characters in length
2.	TransactionId	String	ID with 21 character in length provided to stakeholder in response payload.
3.	ClientId	String	Stakeholder Client Name eg. AIRTEL, VODACOM, HALOTEL, TIGO, SMILE, TTCL, ZANTEL

Table 4 - 25 TransactionVerification Request Parameters

Step 1: Request by Sending NIN

<Payload>

<NIN>XXXXXXXXXXXXXXXXXXXXXX</NIN>

<TransactionId>XXXXXXXXXXXXXXXXXXXXXX</ TransactionId >

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

<ClientId>STAKEHOLDERNAME</ClientId>
</Payload>

4.6.1.3. Response

Name:	TransactionVerificationResult		
Direction:	Output		
Type:	GetTransactionVerificationResponse		
	Content Model:		
	Component	Type	
	Header	ResponseHeader	
		Contains elements as defined in the following table:	
		Component	Type
		Id	String
		TimeStamp	Datetime
		System Generated timestamp	
	Body	ResponseBody	
		Contains elements as defined in the following table:	
		Component	Type
		CryptoInfo	ResponseCryptoInfo
		Contains elements as follows:	
		Component	Type
		*EncryptedCryptoKey	string
		*EncryptedCryptoIV	string
	Payload	String	Payload will be encrypted with the CryptoKey and CryptoIV as per CryptoInfo.

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

				Decrypted payload contains string of character which begin with start tag (e.g. <section>) and end with end tag (e.g. </section>). Refer to 4.5.1.4 for detailed return value.
		Signature	String	Digital signature generated with GIC Server Private Key.
	Status	StatusSectionBase		
		Component	Type	Description
		Code	Int	1- Success 0- Failed.

Table 4 - 26 TransactionVerification Request Response

4.6.1.4. Response Payload

The response payload is constructed in a root element (i.e. with tag named NidaResponse) which contain a group of child elements as defined in the following table.

Note: For child element which access is not granted to the stakeholder, the corresponding tags will be omitted from the response payload.

No.	Tag	Remarks
1	NIN	Cardholder National ID Number
2	TransactionId	Cardholder first name
3	ClientId	Cardholder middle name

Table 4 - 27 TransactionVerification Response Payload

4.6.1.5. Sample Response Payload

A. Sample response for Success Transaction

<NidaResponse>

<NIN>19760507111010000122</NIN>

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

```

<TransactionDate>2019-05-0917:30:08</TransactionDate>
<TransactionStatus>1</TransactionStatus>
<VerificationType>QUERYFULLDATA</VerificationType>
</NidaResponse>

```

B. Sample response for Failed Transaction

```

<NidaResponse>
<NIN>19760507111010000122</NIN>
<TransactionStatus>0</TransactionStatus>
</NidaResponse>

```

4.7. Identification Method

4.7.1. Method

Name:	Identification
Description:	This method is used to perform one to many identification searches.

Table 4 - 28 Identification Method

4.7.1.1. Request Parameters

Name:	IRequest		
Direction:	Input		
Type:	Identification		
	Content Model:		
	Component	Type	
	Header	RequestHeader	
	Contains elements as defined in the following table:		
	Component	Type	Description
	Id	String	System Generated ID
	TimeStamp	Datetime	System Generated timestamp

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

		ClientNameorIP	String	Caller Machine IP (Auto-detected by system)		
		UserID	String	Stakeholder User ID		
	Body	RequestBody				
		Contains elements as defined in the following table:				
		Component	Type	Description		
		CryptoInfo	RequestCryptoInfo	Contains elements as follows:		
				Component	Type	
				*EncryptedCryptoKey	string	
				*EncryptedCryptoIV	string	
	Payload	String	Payload contains the following data which shall be encrypted with CryptoKey and CryptoIV as per the CryptoInfo. Refer to 4.1.1.2 for input data.			
Signature	String	Digital signature generated with stakeholder Private Key.				

Table 4 - 29 Identification Request Parameters

4.7.1.2. Request Payload

Request payload shall be constructed in XML format which started with “Payload” as the first level element and follow by the following sub-elements:

No.	Element	Type	Description
1.	NIN.	String	NIN with 20 characters in length
2.	Firstname	String	Cardholder first name

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

3.	Middlename	String	Cardholder middle name
4.	Surname	String	Cardholder surname
5.	Gender	String	Cardholder Gender
6.	Nationality	String	Cardholder Nationality
7.	DateOfBirth	String	Cardholder date of birth
8.	Photo	String	Base64 jpeg image string
9.	R1	String	Base64 wsq string
10.	R2	String	Base64 wsq string
11.	R3	String	Base64 wsq string
12.	R4	String	Base64 wsq string
13.	R5	String	Base64 wsq string
14.	L1	String	Base64 wsq string
15.	L2	String	Base64 wsq string
16.	L3	String	Base64 wsq string
17.	L4	String	Base64 wsq string
18.	L5	String	Base64 wsq string
19.	RequestId	String	Request ID

Table 4 - 30 Identification Request Parameters

Step 1: Request Template

```

<Payload>
<NIN></NIN>
<Firstname></Firstname>
<Middlename></Middlename>
<Surname></Surname>
<Gender></Gender>
<Nationality></Nationality>
<DateOfBirth></DateOfBirth>
<Photo></Photo>
<R1></R1>
<R2></R2>
<R3></R3>
<R4></R4>
<R5></R5>

```

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

<L1></L1>

<L2></L2>

<L3></L3>

<L4></L4>

<L5></L5>

</Payload>

Response 1

if the match results found instantly, then see for **4.1.1.5 Sample Response Payload**

Response 2

If Match Results to not found (**Code 161**)

Response 3

If the Matching Engine failed to process the transaction instantly, the API returns **code 163** with the Request Id as shown in the below payload

```
<NidaResponse>
<RequestId>XXXXXXXXX</RequestId>
</NidaResponse>
```

Request Id can be used later to search if the Matching Engine has completed to process the request.

```
<Payload>
<RequestId>XXXXXXXXX</RequestId>
</Payload>
```

if the match results found, then see for **4.1.1.5 Sample Response Payload**

If the Matching Engine has not completed to process the request, the API returns **code 163** with the Request Id as shown in the below payload

```
<NidaResponse>
<RequestId>XXXXXXXXX</RequestId>
</NidaResponse>
```

4.7.1.3. Response

Name:	IdentificationResult
Direction:	Output

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

Type:	GetIdentificationResponse		
	Content Model:		
	Component	Type	
	Header	ResponseHeader	
		Contains elements as defined in the following table:	
		Component	Type
		Id	String
		TimeStamp	Datetime
	Body	ResponseBody	
		Contains elements as defined in the following table:	
		Component	Type
		CryptoInfo	ResponseCryptoInfo
		Contains elements as follows:	
		Component	Type
		*EncryptedCryptoKey	string
		*EncryptedCryptoIV	string
	Payload	String	Payload will be encrypted with the CryptoKey and CryptoIV as per CryptoInfo. Decrypted payload contains string of character which begin with start tag (e.g. <section>) and end with end tag (e.g. </section>). Refer to 4.1.1.4 for detailed return value.

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

		Signature	String	Digital signature generated with GIC Server Private Key.
	Status	StatusSectionBase		
		Component	Type	Description
		Code	Int	See Error or Status Codes and Descriptions

Table 4 - 31 Identification Request Response

4.7.1.4. Response Payload

The response payload is constructed in a root element (i.e. with tag named NidaResponse) which contain a group of child elements as defined in the following table.

Note: For child element which access is not granted to the stakeholder, the corresponding tags will be omitted from the response payload.

See **4.1.1.4** for response payload table.

4.7.1.5. Sample Response Payload

See **4.1.1.5** for sample response payload

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

5. Getting Started

In order to interface to NIDA services, few steps below need to be established:

1. Establish an SSL connection
2. Construct Web Service Request
3. Interpret Web Service Response

5.1. Configuring Certificates in the SSL Client and Server

SSL client and server application require four certificates:

- i. Root CA
- ii. NIDA Sub CA
- iii. Client certificate (Stakeholder Certificate)
- iv. Message Security Certificate

Details of the certificates, please refer to section 3.3.1 Types of Certificate Required.

5.2. Certificates on SSL Client and Server

Certificates on SSL Client and Server is used when establishing SSL connections between web browsers and a web server. As part of the initialization, the SSL server loads a certificate (Nida Sub CA certificate) signed by a Root CA. This Root CA is trusted by the SSL clients. When a client verifies the server, the server certificate is sent to the client and then is verified against the CA certificate. The fact that the server has a certificate signed by a trustworthy CA means that the server can be trusted by the client, because the client trusts the CA. This certificate setup prevents the SSL client from establishing an SSL connection an untrustworthy SSL server.

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

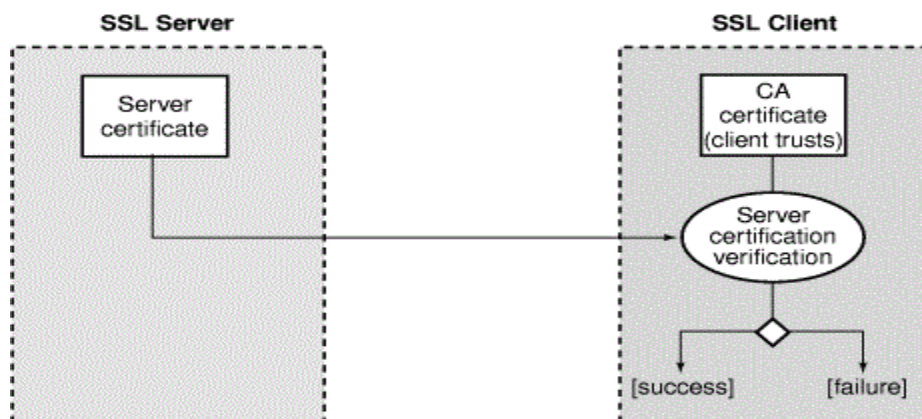


Figure 5 - 1 Certificates on SSL Client and Server

5.3. Construct Web Service Request

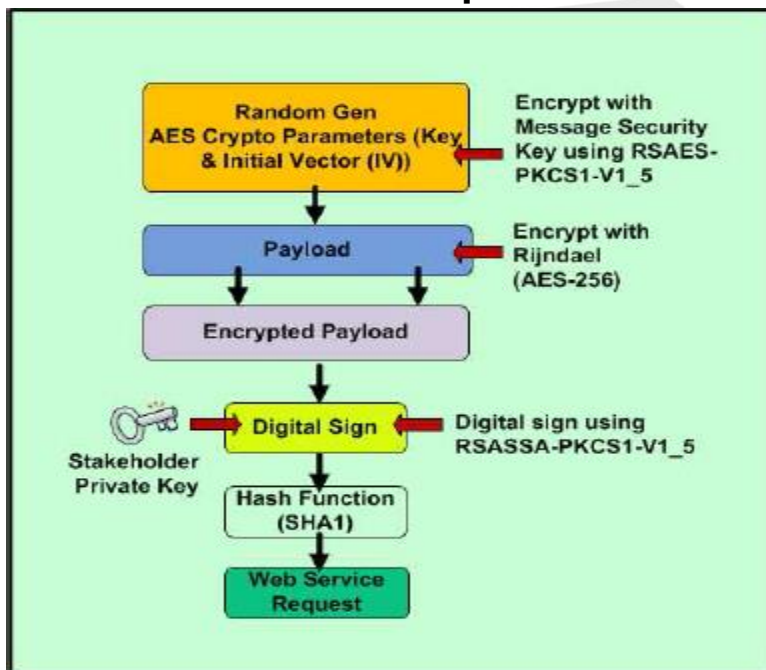


Figure 5 - 2 Web Service Request

For stakeholder to construct the web service request, below are the steps to follow:

1. Construct CIG Web Service request payload as per the respective web service method.
2. Encrypt the request payload using **Rijndael (AES-256)** algorithm.

Note: AES crypto parameter (i.e. Key and Initial Vector (IV)) shall be randomly generated on each encryption operation.

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

3. Encrypt **AES crypto parameter** with **Message Security Public Key** using **RSAES-PKCS1-V1_5** encryption scheme.
 4. Digitally sign the **encrypted payload** with **Stakeholder Private Key** using **RSASSA-PKCS1-V1_5** signature scheme and **SHA1** cryptographic hash function.
- Note:** Refer to PKCS #1 v2.1: RSA Cryptography Standard specification for PKCS1-v1.5 Signature and Encryption scheme.

5.4. Interpret Web Service Response

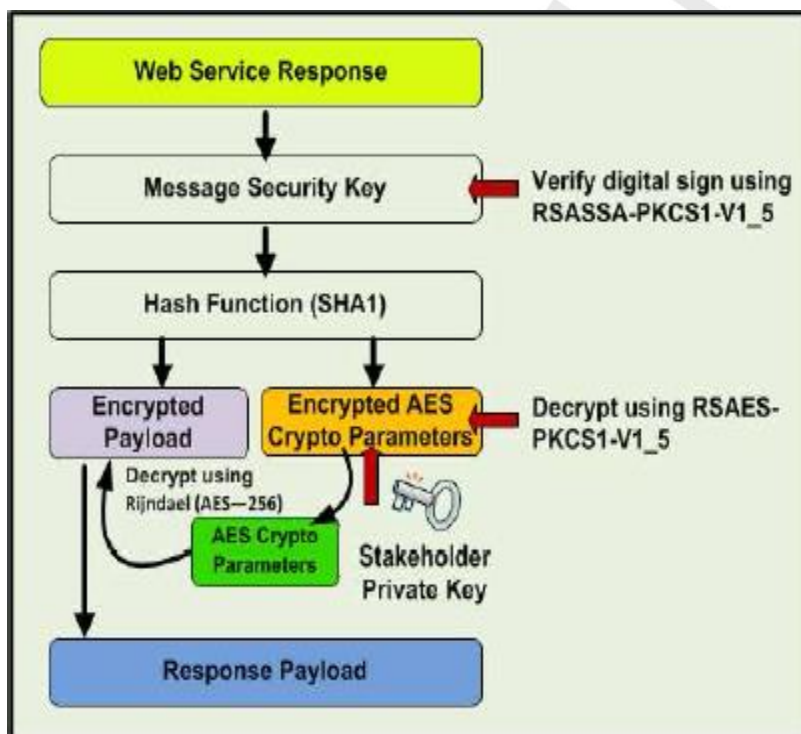


Figure 5 - 3 Web Service Response

For stakeholder to interpret the web service response, below are the steps to follow:

1. Verify the Digital Signature in the response with **Message Security Public Key** using **RSASSA-PKCS1-V1_5** signature scheme and **SHA1** cryptographic hash function.
2. Upon successful verification, decrypt **encrypted AES crypto parameter** with **Stakeholder Private Key** using **RSAES-PKCS1-V1_5** encryption scheme.

	Interface Guide		
	Tanzania NID CIG Technical Interface for External Stakeholder		
	Document Reference Number	Version	Release Date
	NIDA_CIG_API_DOCUMENT_20190528	3.0	10_JUNE_2019

3. Decrypt the response payload with AES crypto parameter using **Rijndael (AES—256)** algorithm.

Note: For Update Method, skip Step 2 and Step 3.

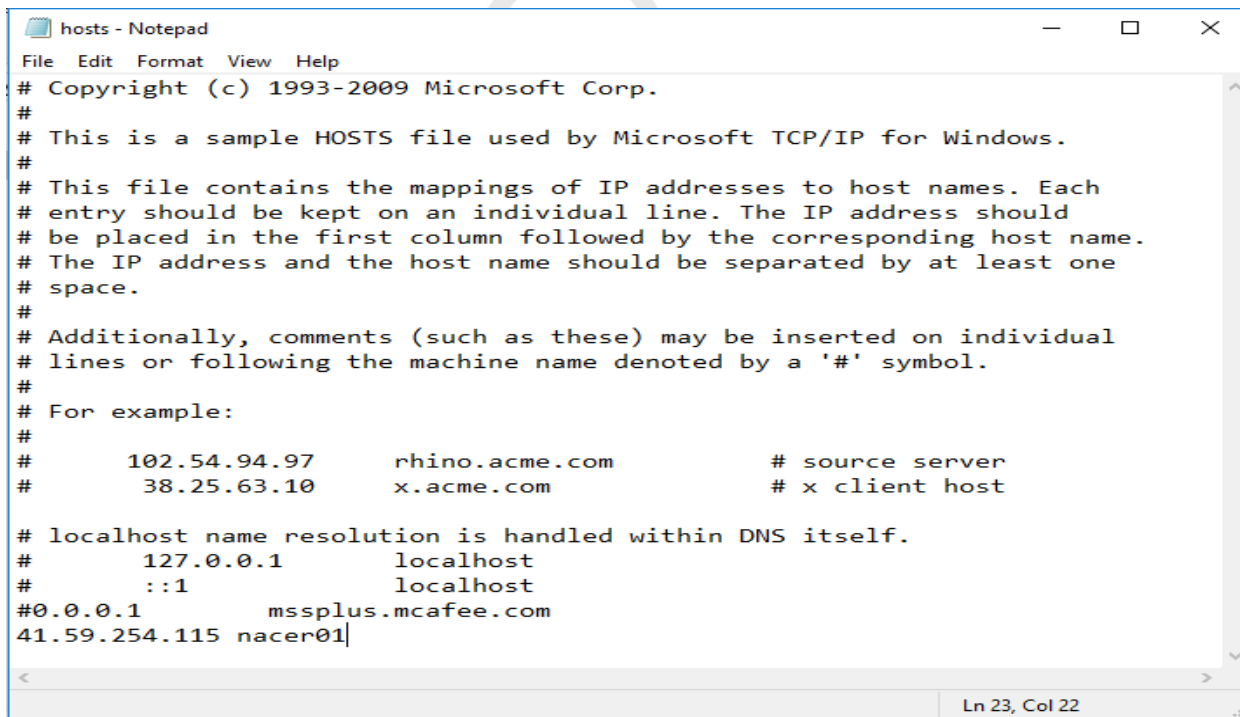
Note: Refer to PKCS #1 v2.1: RSA Cryptography Standard specification for PKCS1-v1.5 Signature and Encryption scheme.

5.5. Mapping the IP Address to Hostname

The location of the **hosts** file, depending on the operating system that you are using:

- **Windows** - *SystemRoot > system32 > drivers > etc > hosts*
- By default, the system root is *C:\Windows*, so if you are using Windows, your **hosts** file is most probably: *C:\Windows\System32\drivers\etc\hosts*
- **Linux** - */etc/hosts*

Define the hostname with the respective IP address
Example. Add **41.59.254.115 nacer01** and then Save the file.



```

hosts - Notepad
File Edit Format View Help
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com           # source server
#       38.25.63.10       x.acme.com               # x client host
#
# localhost name resolution is handled within DNS itself.
#       127.0.0.1         localhost
#       ::1               localhost
#0.0.0.1                 mssplus.mcafee.com
41.59.254.115 nacer01

```

Figure 5 - 4 Hosts file

WSDL Address: https://nacer01/TZ_CIG/GatewayService.svc?wsdl