i

National Electoral Institute

Directorate of Infrastructure and Applied Technology

Service

Data verification of the Credential for vote

Specifications Techniques

Manual version 3.8

Page 2

Change control

SVCV 2.0	Description: Technical Specification of the Service
DATE: October 2017	Data Verification 2.0

Document	Revised	Approved
First name:	First name:	First name:
Firm:	Firm:	Firm:

Page 3

Content

1 - Introduction

1.1 - Purpose

This document constitutes the technical description of the verification services of

data of the voting credential issued by the National Electoral Institute (INE). The documentation is oriented to provide the necessary technical elements to the consumption of the services defined here.

2 - Generic Services Overview

The National Electoral Institute (INE) provides interested institutions with a web service for consultation and / or verification of voter registration data.

Verifydata .- Allows verification of all data contained on the card to vote, as well as the minutiae of citizens.

Workflow of the Verification Credential Data Verification Service

Request Answer

Data Capture

-ocr -anioRegister

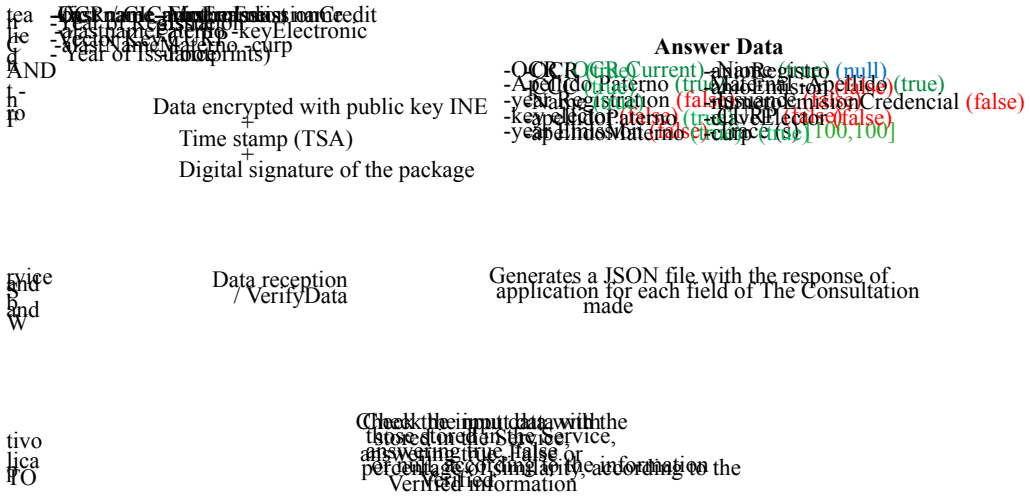

Figure 1 Description of the Data Verification Web Service

This service is available through HTTP requests using the POST method for the sending of the query parameters. These parameters can be sent as a XML document or a JSON document.

National Electoral Institute
Directorate of Infrastructure and Applied Technology
Technical specifications

3 - Definition of Service

3.1 - Data Verification Service

The Verification Credential Data Service for Voting Version 2.0 allows for a consult the data contained in the voter card and the details for verification, maximum two per request, from the citizen.

3.1.1 - Access

Access to the testing environment of the Credential Data Verification Service to Vote version 2.0 is available in the following route:

URL

http: // <IPAddress> / cxf / SVD / External entities / query

Table 1 URL for accessing the Web Service

3.1.2 - Parameters

The parameters accepted by the service are composed of two elements: headers and body. The headers are HTTP headers that describe the query type sent and the response desired:

- Content-Type:
  or application / json
- Accept:
  or application / json

Page 7

The body is a POST request with the structure of a json document, which includes the text and biometric data of the citizen that will be verified. The structure of the petition is the following:

data

VerifyData signature

timeStamp

Attribute	Description	Use	Kind
data	It contains the data of citizen and biometrics	Required	Elements dependents
signature	It contains the digestion of	Required	Elements

	signature, the digital signature of the data, the serial number of the certificate and parameters of calculation of the signature.		dependents
timeStamp	It contains the stamp of time spent by the Institution of data and digital signature.	Required	Elements dependents

Table 2 *Parameters for using the Web Service for data verification*

Before building the request to the Verification Service, it is important to have in Count the following:

to. The primary key search is performed by the **CIC;** however, if the voter card does not have CIC, the search key is composed of the following **OCR** data, **key voter** and **issue number credential**
b. Citizen data should be sent in capital letters and without accents, such as appear on the voter card.
c. Use the UTF-8 encoding.
d. Respect the JSON structure format (see page 36).

For encrypted data, you must comply with:

to. Encrypt the data with the RSA algorithm.
b. Use the public key of the INE whose length is 4096 bits.
c. The process can be performed within the HSM or the Information Encryption Module.
d. The result (cryptogram) must be encoded in base64.

For the digital signature, you must comply with:

to. Perform the digital signature within the HSM of the Information Encryption Module.
b. Use the private key of the Institution with a length of 2048 bits and the signature algorithm RSA-SHA256.
c. The result (signature) must be encoded in base64.

The institution will request the time stamp of the entire package that will be sent to the INE, the TSA will be one arranged by the institution or by filling in the required fields.

Here's how to build the request:

National Electoral Institute
Directorate of Infrastructure and Applied Technology
Technical specifications

I. Data Element

Description: Contains the encrypted data of the citizen and the location data of the institution.

Encrypted data

minutiae

Data

Location

feelingly

Attribute	Description	Use	Kind
Encrypted data	It contains the data of citizen encrypted with the key RSA 4096 of the INE.	Required	String Base64
minutiae	It contains the biometrics of citizen.	Optional	Elements dependents
Location	It contains the data of the location of the console that make the request	Required	Elements dependents
feelingly	Consent of the citizen to use your data in the check.	Required	Boolean

Table 3 Attributes of the data element

Page 10

Within the item **"datosCifrados"** it contains the data to verify the citizen, prior to encryption, the structure must be established:

Encrypted data

ocr

cic

first name

last name

mother's last name

anioRegistro

anioEmission

EmisionCredential number

KeyElector

curp

NOTE: The order of the data to be encrypted is immaterial, as long as the structure is respected (see page 33). Failure to verify any information required will have to declare as **null.**

Page 11

Technical specifications

Here is the description of each data:

Attribute	Use	Kind
ocr	Required* * *If the voter does not has CIC*	String Length: 13
cic	Required	String Length: 10
first name	Optional	String Length: 32
last name	Optional	String Length: 32
mother's last name	Optional	String Length: 32
anioRegistro	Optional	String Length: 4
anioEmission	Optional	String Length: 4
EmisionCredential number	Required* * *If the voter does not has CIC*	String Length: 2
KeyElector	Required* * *If the voter does not has CIC*	String Length: 18
curp	Optional	String Length: 18

Table 4 Attributes Data element Encrypted

Within the **"minutiae"** element it contains the elements that identify the type and value of Minutes to be verified, in case of not containing them, we define the node in the following way

"minutiae": null.

kind

width

minutiae high

minucia2

minucia7

Attribute	Use	Kind
kind	Required	Int (1 = ansi, 2 = wsq, 3 = raw)
width	Required	Int ANSI and WSQ = **null**
high	Required	Int ANSI and WSQ = **null**
minucia2	Required (at least one fingerprint)	String Base64 of the footprint of the right index
minucia7	Required (at least one fingerprint)	String Base64 of the footprint of the left index

Table 5 Attributes of the minutia element

Page 13

Within the element **"location"** data contains the location of the institution, satellite position or the locality. **At least one attribute of the "location" node is required.**

latitude

satellite position

length

Location

Postal Code

location city

state

NOTE: If you enable the attribute **"location"** are required elements:
"Address_zipCode", "city" and "state", otherwise we establish **"village": null.**

13

Page 14

National Electoral Institute
Directorate of Infrastructure and Applied Technology
Technical specifications

Attribute	Description	Use	Kind
satellite position	Position data satellite console who makes the request	Required	Elements dependents
location	Address data of the console that make the request	Optional	Elements dependents

Table 6 Attributes of the location element

Attribute	Use	Kind
latitude	Required	Float Length: 8
length	Required	Float Length: 8
Postal Code	Required	String Length: 5
city	Required	String Length: 20
state	Required	Int Length: 1 or 2 figures depending on the case (See catalog of federal entities, annexed at the end)

Table 7 Satellite Position Attributes and Location

Page 15

Within the **"consent"** element refers to the consent given by the citizen to use data in the verification, the value should be **"true".**

feelingly true

Attribute	Description	Use	Kind
feelingly	Consent of the citizen to use your data in the check.	Required	Boolean

Table 8 Satellite Position Attributes and Location

fifteen

National Electoral Institute
Directorate of Infrastructure and Applied Technology
Technical specifications

II. Signature element

Description: Contains the elements of the XML digital signature.

signedInfo

signature signatureValue

keyInfo

Attribute	Description	Use	Kind
signedInfo	It contains the calculation parameters of the signature	Required	Elements dependents
signatureValue	Digital signature of the information sent by the institution.	Required	String Base64
keyInfo	Certificate information with which the signature was made. (The serial number of the certificate is susceptible to uppercase and lowercase,	Required	Elements dependents

in case of containing letter).

Table 9 Attributes of the signature element

16

Page 17

National Electoral Institute
Directorate of Infrastructure and Applied Technology
Technical specifications

Within the item **"SignedInfo"** contains the calculation parameters of the firm.

canonicalizationMethod

signedInfo signatureMethod

digestMethod

reference

digestValue

Attribute	Use	Value
canonicalizationMethod	Required	Default: **"Http://www.w3.org/TR/2001/REC-xml-c14n-20010315 "**
signatureMethod	Required	Default: **"Http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 "**
reference	Required	Dependent elements

Table 10 Attributes signedInfo element

Page 18

National Electoral Institute
Directorate of Infrastructure and Applied Technology
Technical specifications

Within the **"reference"** element it contains the standards that must be met.

digestMethod

reference

digestValue

Attribute	Use	Kind	Value
digestMethod	Required	Settled down default	Default: **"Http://www.w3.org/2001/04/xmlenc#sha256"**
digestValue	Required Hash SHA-256 of the firm		Dependent element

Table 11 Attributes element reference

Page 19

Within the item **"keyInfo"**

Description: Information about the certificate with which the signature was made.

keyInfo x509Data x509SerialNumber

Attribute	Use	Kind
x509Data	Required	Dependent elements

Table 12 Attributes keyInfo element

Attribute	Use	Kind
x509SerialNumber	Required	String Serial number of the certificate issued by the CA of the INE.

Table 13 Attributes element x509Data

III. Element timeStamp

It contains the time stamp used by the "data" node institution.

moment

timeStamp index

Serial number

Attribute	Use	Kind
moment	Required	String **Ex.** "YYYYMMDDhhmmssZ" Time stamp in which the request was generated.
Index	Required	String Index of the time stamp generated by the institution.
Serial number	Optional	String Serial number of the TSA certificate with which the time stamp was signed

Table 14 Element attributes timeStamp

twenty

Page 21

National Electoral Institute
Directorate of Infrastructure and Applied Technology
Technical specifications

3.1.3 VerifyData response

When making the request to the web service (request) the response will have the following structure:

response

VerifyDataResponse

signature

timeStamp

Attribute	Description	Kind
response	It contains the verification of the data of the citizen, as well as response codes and folio of the transaction.	Dependent elements
signature	Contains the elements of the digital signature of the INE	Dependent elements
timeStamp	Time stamp of the response sent by the INE	Dependent elements

Table 15 VerifyDataResponse element attributes

I. Element response

It contains the verification of citizen data, as well as response codes and folio of the transaction.

dateOption Time

IndexApplication

dataResponse

response

minutiaeResponse

Time Processing

codeResponse

Page 23

Attribute	Description	Kind
dateOption Time	Date and time of arrival of the petition to Verification Service.	String (YYYY-MM-DD hh: mm: ss.ffffffff)
IndexApplication	Index sent by the institution within of the TimeStamp element.	String
dataResponse	Detail of the INE's response with regarding citizen data sent to verify.	Elements dependents
minutiaeResponse	Detail of the INE's response with regarding the minutiae sent to check.	Elements dependents

Time Processing	Time in milliseconds of processing of the application check.	Long
codeResponse	Code of the status of the response.	Int See table of codes

Table 16 Attributes element response

2. 3

National Electoral Institute
Directorate of Infrastructure and Applied Technology
Technical specifications

Within the **"dataResponse"** element it contains the detailed response regarding INE to the citizen's data sent to verify.

responseSituationRegistral

dataResponse

ReplyComparation

CodeDisponseData

Attribute	Description	Kind
respuestaSituacionRegistral	Displays the type of registration status citizen	Elements dependents
ReplyComparation	Element that contains the detail of the Items sent to verify	Elements dependents
CodeDisponseData	Request response code sent	Int See table of

codes

Table 17 Attributes dataResponse element

24

Page 25

National Electoral Institute
Directorate of Infrastructure and Applied Technology
Technical specifications

Within the **"respuestaSituacionRegistral"** element type of registration status shows of the citizen.

typeLocationRegistral

responseSituationRegistral

typeReportRoboExtravio

Attribute	**Kind**
typeLocationRegistral	String (Valid | NoVigente)
typeReportRoboExtravio	String

Table 18 Attributes element response SituationRegistral

Page 26

National Electoral Institute
Directorate of Infrastructure and Applied Technology
Technical specifications

Within the **"respuestaComparacion"** element it contains the detail of items sent to verify.

ReplyComparation	anioRegistro
	KeyElector
	last name
	anioEmission
	Emision credential number
	first name
	curp
	mother's last name
	ocr

Attribute	**Kind**
anioRegistro	Boolean
KeyElector	Boolean
last name	Boolean
EmisionCredential number	Boolean
First name	Boolean
Curp	Boolean
mother's last name	Boolean
OCR	Boolean

Table 19 Attributes element responseComparation

NOTE: See Annex comparison results.

National Electoral Institute
Directorate of Infrastructure and Applied Technology
Technical specifications

Within the **"minutiaeResponse"** element it contains detailed response INE regarding the minutiae sent to verify.

code AnswerMinucia

minutiaeResponse similarity2

similarity7

Attribute	Kind
code AnswerMinucia	Int See table of codes
similarity2	String Result of comparison of the footprint of the index law
similarity7	String Result of comparison of the footprint of the index left

Table 20 Attributes of the minutiaeResponse element

II. Signature element

It contains the elements of the digital signature of the INE.

signedInfo

signature signatureValue

keyInfo

Attribute	Description	Kind
signedInfo	It contains elements for the process of obtaining the firm	Dependent elements
signatureValue	Digital signature of the response issued by the INE	String Base64
keyInfo	It contains information of certificate used for digital signature	Dependent elements

Table 21 Signature element attributes

Page 29

Under **"SignedInfo"**

Description: Contains elements for the process of obtaining the signature.

canonicalizationMethod

signedInfo signatureMethod

digestMethod

reference

digestValue

Attribute	Use	Kind
canonicalizationMethod	Required	**http://www.w3.org/TR/2001/REC-xml-c14n-20010315**
signatureMethod	Required	**http://www.w3.org/2001/04/xmldsig-more#rsa-sha256**
Reference	Required	Dependent elements

Table 22 Attributes signedInfoInfo

Page 30

Within the item **"reference"**

Description: Standards that must be met.

digestMethod

reference

digestValue

Attribute	Use	Kind
digestMethod	Required	**http://www.w3.org/2001/04/xmlenc#sha256**
digestValue	Required	String Base64

Table 23 Attributes element reference

Page 31

Within the item **"keyInfo"**

Description: Information about the certificate with which the signature was made.

keyInfo x509Data x509SerialNumber

Attribute	Use	Kind
x509Data	Required	Dependent elements

Table 24 Attributes element keyInfo

Attribute	Use	Kind
x509SerialNumber	Required	String Serial number of the certificate issued by the CA of the INE.

Table 25 Attributes element x509Data

Page 32

III. Element timeStamp

Description: Time stamp of the response sent by the INE.

moment

timeStamp index

Serial number

Attribute	Use	Kind
Moment	Required	String Time stamp when the response was generated
Index	Required	String Index of the time stamp generated by the TSA of the institution.
Serial number	Required	String Serial number of the TSA certificate of the institution.

Table 26 Attributes element timeStamp

The time stamp is calculated with the "response" element. For the answer in format JSON, the item's hash is calculated by placing it on a single line.

National Electoral Institute
Directorate of Infrastructure and Applied Technology
Technical specifications

3.2 Data encryption

3.2.1 JSON format

In JSON format, the data that will be encrypted will have the following form:

```
{
 "ocr": "0720060838243",
 "cic": "80040529",
 "name": "VALERIA",
 "surnamePaterno": "LEPE",
 "surnameMaterno": "GARDENS",
 "anioRegistro": "2010",
 "anioEmission": "2014",
 "Crediting Issue Number": "04",
 "Elector key": "LPJRVL88110101H100",
 "curp": "LEJV881101HASJSN07"
}
```

A single line will be created with the data contained by "Encrypted data".

{"ocr": "0720060838243", "cic": "80040529", "name": "VALERIA", "surnamePaterno": "LEPE", "surnameMaterno": "GARDENS", " anioRegistro ":" 2010 "," anioEmision ":" 2014 "," numeroEmisionCredencial ":" 04 "," claveElector ":" LPJRVL88110101H100 "," curp ": "LEJV881101HASJSN07"}

The string will be encrypted with the **public key RSA 4096 INE,** using the type of **padding OAEP.**
The result will be placed as a value of the same tag:

"Encrypted data": "J / tJEzVeD1R6A1s8nCKsB8iRIa2gGWsssD9jxMpebUpzf9mqKHGQYrXx8j1c7Jk50iA4aV7VrxqRMLnzVrN
POzG / sooJP35Kc1B72K97P / MVzMwJx1pk2MPbAgcpOWrsF4Oj3WB / emOCGQgsEQ54UG + VC7Vacaq4XqBZI + 8eMs / tQSis
9RHtCVcRSickZj + n1l7vjNNeSNWJ + IkxMzhIEJxUiuiv16l6UcP0E6I4IwJZIDcT1UZPY0ObWagWF3h3K6rGPcuTLT7canfrkA
zNVCQktUvxRaNYgOICYutbVlG4Xtvmrvt8fff1ofAatCCEh57Soz9lA8BjLb / qPduVJke + cHbsROV4fqXJeSKFYBnizFOwFhM
pJ4Pwk6NcTwhwk2MRj / + L5VnkFlhaVvD8qokX99vzNbnXNT7ECU1VNV3hCO + etnWq8dsWzqifn4AdKdCJGQ4u4FrBvmqp
XwQxKNzycTvoCaRTezf7RusuVK8RR1mNHdw44xUUlSz / OLuy07pV3TWessG24LHFYnib3GxQQqaaaUWqJFkw17Z / UIKd
ocBafT3X / mhF944pGWM1MJurN0DS0JYSXt41CZTYg8ibWroQxMmMd0RHV1kXB6w4NhwGU7OKMjwpHurnB + JhBrMrh

wGbWAyP2UpNKwByyIqeRGqb1NHHlf7HwtCiVOvKD / qFdkVXS9 / 4 = ",

National Electoral Institute
Directorate of Infrastructure and Applied Technology
Technical specifications

3.3 Signed data

3.3.1 JSON format

In JSON format, the data that will be signed will have the following form:


```
{
 "Encrypted data":
"J / tJEzVeD1R6A1s8nCKsB8iRIa2gGWsssD9jxMpebUpzf9mqKHGQYrXx8j1c7Jk50iA4aV7VrxqRMLnzVrNPOzG / sooJP35K
c1B72K97P / MVzMwJx1pk2MPbAgcpOWrsF4Oj3WB / emOCGQgsEQ54UG + VC7Vacaq4XqBZI + 8eMs / tQSis9RHtCVcRSick
Zj + n1l7vjNNeSNWJ + IkxMzhIEJxUiuiv16l6UcP0E6I4IwJZIDcT1UZPY0ObWagWF3h3K6rGPcuTLT7canfrkAzNVCQktUvxR
aNYgOicYutbVlG4Xtvmrvt8fff1ofAatCCEh57Soz9lA8BjLb / qPduVJke + cHbsROV4fqXJeSKFYBnizFOwFhMpJ4Pwk6NcTw
hwk2MRj / + L5VnkFlhaVvD8qokX99vzNbnXNT7ECU1VNV3hCO + etnWq8dsWzqifn4AdKdCJGQ4u4FrBvmqpXwQxKNzycT
voCaRTezf7RusuVK8RR1mNHdw44xUUlSz / OLuy07pV3TWessG24LHFYnib3GxQQqaaaUWqJFkw17Z / UIKdocBafT3X / mh
F944pGWM1MJurN0DS0JYSXt41CZTYg8ibWroQxMmMd0RHV1kXB6w4NhwGU7OKMjwpHurnB + JhBrMrhwGbWAyP2
UpNKwByyIqeRGqb1NHHlf7HwtCiVOvKD / qFdkVXS9 / 4 = ",
 "minutiae": {
  "Type 1,
  "wide": null,
  "high": null,
  "minucia2":
"Rk1SACAyMAAAwgAAAAAAAAGgAaAAxQDFAQAAAFAbgKAAQG4AgNoAVWMAgOEAdHQAgOMAhpYAgKkArJ
MAgRAAuUgAgMQAzD0AgSFscA5FMAgIgBFUcAgI0BN08AQNYDAHF4AQMQAOWcAQJAAZXYAQJsAZhUAQM8A
Z3MAQJEAeXsAQN4A874f4gAQRMArz4AQSsAujkAQIYAyJYAQR4A2E8AQPsA3K0AQJcBC0QAQK4BC0QAQG4BDU
sAQPMBHlQAQK0BOU4AAAA = ",
  "minucia7":
"Rk1SACAyMAAA / gAAAAAAAAGgAaAxQDFAQAAAGQlgQsAXJ8AgM0AXqMAgRsAfJkAgKwAf6wAgP0AhJIAgKU
ApiEAgQoAtYsAgScAuZIAgG0AvI8AgKgAvD8AgPgAvIYAgIMAvZoAgRsA0YgAgPQA83YAgR8A9X8AgIMA9qYAgKY
BB08AgJMBF08AgScBJCIAgSYBNRIAftgRDDAMBRxAAgMABTwcAQNgAJ64AQPEAKFYAQLcAa6oAQRAAh5UAQG
QAi30AQLYAjngAQNsAmYoAQG0AnIgAQS0A4osAQOkA5XMAQT0A85YAQTYBAn8AQRcBFHUAQQEBOhoAQOkB
WwwAAAA = "
 },
 "Location": {
  "posicionSatelital": {
   "latitude": 19.12345,
   "length": -99.12345
  },
  "location": {
   "codePostal": "01710",
   "city": "CDMX",
   "state": 9
  }
 },
 "consent": true
} {
 "moment": "20170622130012Z",
 "index": "6545665423523153",
 "Serial number": "58.be.0e.58.16.82.6a.70.79.2b.b0.a1.f5.a8.84.8c"
}
```

Page 35

A single line will be created with the data contained by "data" and "timeStamp", of which
You will obtain the SHA256 ("digestValue") and signed with the private key RSA 2048 of the institution. He
result will be placed as value of the same tag:

{"Encrypted data": "J / tJEzVeD1R6A1s8nCKsB8iRIa2gGWsssD9jxMpebUpzf9mqKHGQYrXx8j1c7Jk50iA4aV7VrxqRMLnzVr
NPOzG / sooJP35Kc1B72K97P / MVzMwJx1pk2MPbAgcpOWrsF4Oj3WB / emOCGQgsEQ54UG + VC7Vacaq4XqBZI + 8eMs / tQS
is9RHtCVcRSickZj + n1l7vjNNeSNWJ + IkxMzhIEJxUiuiv16l6UcP0E6I4IwJZIDcT1UZPY0ObWagWF3h3K6rGPcuTLT7canfrk
AzNVCQktUvxRaNYgOICYutbVlG4Xtvmrvt8fff1ofAatCCEh57Soz9lA8BjLb / qPduVJke + cHbsROV4fqXJeSKFYBnizFOwFh
MpJ4Pwk6NcTwhwk2MRj / + L5VnkFlhaVvD8qokX99vzNbnXNT7ECU1VNV3hCO + etnWq8dsWzqifn4AdKdCJGQ4u4FrBvm
qpXwQxKNzycTvoCaRTezf7RusuVK8RR1mNHdw44xUUlSz / OLuy07pV3TWessG24LHFYnib3GxQQqaaaUWqJFkw17Z / UI
KdocBafT3X / mhF944pGWM1MJurN0DS0JYSXt41CZTYg8ibWroQxMmMd0RHV1kXB6w4NhwGU7OKMjwpHurnB + JhBr
MrhwGbWAyP2UpNKwByyIqeRGqb1NHHlf7HwtCiVOvKD / qFdkVXS9 / 4 = "," minutiae ": {" type ": 1," width ": null," high ": null," my
nucia2 ":" Rk1SACAyMAAAwgAAAAAAAAGgAaAAxQDFAQAAAFAbgKAAQG4AgNoAVWMAgOEAdHQAgOMAhpYA
gKkArJMAgRAAuUgAgMQAzD0AgSFscA5FMAgIgBFUcAgI0BN08AQNYDAHF4AQMQAOWcAQJAAZXYAQJsAZhUA
QM8AZ3MAQJEAeXsAQN4A874f4gAQRMArz4AQSsAujkAQIYAyJYAQR4A2E8AQPsA3K0AQJcBC0QAQK4BC0QAQG
4BDUsAQPMBHlQAQK0BOU4AAAA = "," minucia7 ":" Rk1SACAyMAAA / gAAAAAAAAGgAaAAxQDFAQAAAGQlgQsA
XJ8AgM0AXqMAgRsAfJkAgKwAf6wAgP0AhJIAgKUApiEAgQoAtYsAgScAuZIAgG0AvI8AgKgAvD8AgPgAvIYAgIMAv
ZoAgRsA0YgAgPQA83YAgR8A9X8AgIMA9qYAgKYBB08AgJMBF08AgScBJCIAgSYBNRIAftgRDDAMBRxAAgMABT
wcAQNgAJ64AQPEAKFYAQLcAa6oAQRAAh5UAQGQAi30AQLYAjngAQNsAmYoAQG0AnIgAQS0A4osAQOkA5XMA
QT0A85YAQTYBAn8AQRcBFHUAQQEBOhoAQOkBWwwAAAA = "}," location ": {" satellite position ": {" latitude ": 19.12345,"
length":-
99.12345}, "locality": {"codePostal": "01710", "city": "CDMX", "state": 9}}, "consent": true} {"moment": "20170622
130012Z "," index ":" 6545665423523153 "," serial number ":" 58.be.0e.58.16.82.6a.70.79.2b.b0.a1.f5.a8.84.8c "}

NOTE: Attention not have a line break at the end of the chain and / or some leftover character
that generates an alteration of the signature and results an error when consuming the web service.

Page 36

3.4 Example of consultation

3.4.1 JSON format


```
{
 "data": {
   "Encrypted data":
"J / tJEzVeD1R6A1s8nCKsB8iRIa2gGWsssD9jxMpebUpzf9mqKHGQYrXx8j1c7Jk50iA4aV7VrxqRMLnzVrNPOzG / sooJP35K
c1B72K97P / MVzMwJx1pk2MPbAgcpOWrsF4Oj3WB / emOCGQgsEQ54UG + VC7Vacaq4XqBZI + 8eMs / tQSis9RHtCVcRSick
Zj + n1l7vjNNeSNWJ + IkxMzhIEJxUiuiv16l6UcP0E6I4IwJZIDcT1UZPY0ObWagWF3h3K6rGPcuTLT7canfrkAzNVCQktUvxR
aNYgOicYutbVlG4Xtvmrvt8fff1ofAatCCEh57Soz9lA8BjLb / qPduVJke + cHbsROV4fqXJeSKFYBnizFOwFhMpJ4Pwk6NcTw
hwk2MRj / + L5VnkFlhaVvD8qokX99vzNbnXNT7ECU1VNV3hCO + etnWq8dsWzqifn4AdKdCJGQ4u4FrBvmqpXwQxKNzycT
voCaRTezf7RusuVK8RR1mNHdw44xUUlSz / OLuy07pV3TWessG24LHFYnib3GxQQqaaaUWqJFkw17Z / UIKdocBafT3X / mh
F944pGWM1MJurN0DS0JYSXt41CZTYg8ibWroQxMmMd0RHV1kXB6w4NhwGU7OKMjwpHurnB + JhBrMrhwGbWAyP2
UpNKwByyIqeRGqb1NHHlf7HwtCiVOvKD / qFdkVXS9 / 4 = ",
   "minutiae": {
    "Type 1,
    "wide": null,
    "high": null,
    "minucia2":
"Rk1SACAyMAAAwgAAAAAAAAGgAaAAxQDFAQAAAFAbgKAAQG4AgNoAVWMAgOEAdHQAgOMAhpYAgKkArJ
MAgRAAuUgAgMQAzD0AgSFscA5FMAgIgBFUcAgI0BN08AQNYDAHF4AQMQAOWcAQJAAZXYAQJsAZhUAQM8A
Z3MAQJEAeXsAQN4A874f4gAQRMArz4AQSsAujkAQIYAyJYAQR4A2E8AQPsA3K0AQJcBC0QAQK4BC0QAQG4BDU
sAQPMBHlQAQK0BOU4AAAA = ",
    "minucia7":
"Rk1SACAyMAAA / gAAAAAAAAGgAaAxQDFAQAAAGQlgQsAXJ8AgM0AXqMAgRsAfJkAgKwAf6wAgP0AhJIAgKU
ApiEAgQoAtYsAgScAuZIAgG0AvI8AgKgAvD8AgPgAvIYAgIMAvZoAgRsA0YgAgPQA83YAgR8A9X8AgIMA9qYAgKY
BB08AgJMBF08AgScBJCIAgSYBNRIAftgRDDAMBRxAAgMABTwcAQNgAJ64AQPEAKFYAQLcAa6oAQRAAh5UAQG
QAi30AQLYAjngAQNsAmYoAQG0AnIgAQS0A4osAQOkA5XMAQT0A85YAQTYBAn8AQRcBFHUAQQEBOhoAQOkB
WwAAAA = "
   },
  "Location": {
  "posicionSatelital": {
    "latitude": 19.12345,
    "length": -99.12345
   },
   "location": {
    "codePostal": "01710",
    "city": "CDMX",
    "state": 9
   }
  },
  "consent": true
 },
 "signature": {
  "signedInfo": {
   "canonicalizationMethod": {
    "algorithm": "http://www.w3.org/TR/2001/REC-xml-c14n-20010315"
   },
   "signatureMethod": {
    "algorithm": "http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"
   },
   "reference": {
    "digestMethod": {
     "algorithm": "http://www.w3.org/2001/04/xmlenc#sha256"
    },
```



```
    "digestValue": "DE1F6A8933C7A6955F2E518AA15A37E6E11605CC9765E2B062EA2D762BA65AB6",
    "uri": "#DATA"
   }
  },
  "signatureValue":
"ZJS + pjk3D2EvJ6iWE4LluLUJRQZSGJmL0SZ1zW1DtxCLAFJT54lmdJrirC0DTcH / vjYU9pkrGvWDOEdDTc8BqncwC / A68
wZu / VJdiOF / CWaEtDAIcgj0fF7KIaieezzKGHgkOlyLqxsSdbCbpUhUz12BF1VATdU7T2JZji8mTmGg0qJr + Ol7qdjPBLw / pe1
```

```
WgleZstczw2bQjhw+oFRWCmIQbQNbJSaoFN6ojvtXpyk4UmuLyeglozeAOAbOsKnymIPbsNx3toTHSSjA5RR3gyWwdsKB2v
CwC7F5wesYaBR/x9hqbIs6GqkI3bLPQvAQOjfzlMx1p8QtP++B3k5s5PXz7wNVEw==",
   "keyInfo": {
    "x509Data": {
     "x509SerialNumber": "4m"
    }
   }
  },
  "timeStamp": {
   "moment": "20170622130012Z",
   "index": "6545665423523153",
   "Serial number": "58.be.0e.58.16.82.6a.70.79.2b.b0.a1.f5.a8.84.8c"
  }
}
```


NOTE: The attributes "CanonicalizationMethod", "SignatureMethod", "reference" and "digestMethod" they are included in the JSON request to preserve XML support.

3.5 Response example

3.5.1 JSON format


```
{
 "response": {
   "FechaHoraPeticion": "07.12.2017 16: 47: 19,947"
   "IndiceSolicitud": "6545665423523153"
   "DataResponse": {
     "RespuestaSituacionRegistral" {
       "TipoSituacionRegistral": "VALID"
       "TipoReporteRoboExtravio": null
     },
     "RespuestaComparacion"  {
       "AnioRegistro": true,
       "ClaveElector": true,
       "LastName": true,
```

```
        "AnioEmision": true,
        "NumeroEmisionCredencial": true,
        "Name": true,
        "CURP": true,
        "ApellidoMaterno": true,
        "Ocr": true
      },
      "CodigoRespuestaDatos": 0
    },
    "MinutiaeResponse": {
      "CodigoRespuestaMinucia": 0,
      "Similitud2": "100.0%",
      "Similitud7": "100.0%"
    },
    "TiempoProcesamiento": 506,
    "CodigoRespuesta": 0
  },
  "Signature": {
    "SignedInfo": {
      "CanonicalizationMethod": { "algorithm": "http://www.w3.org/TR/2001/REC-xml-c14n-20010315"},
      "SignatureMethod": { "algorithm": "http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"},
      "Reference":    {
        "DigestMethod": { "algorithm": "http://www.w3.org/2001/04/xmlenc#sha256"},
        "DigestValue": "7xvDnM22K4jupFHUDNFEVW7dolq / Nu6IRDFhNm + u2KE ="
        "Uri": "#DATA"
      }
    },
    "SignatureValue"
"SFJkbhjhoASDQ / 9b22SKxLBC7ENRgVHIjjnph8GqFvKz3n2TMtebLThjQQ8hNqpcat73TT2e / B0x \ nMRPAsGLHmbCKJ6tAz
+ W7ipj / FkLLEoU4Wka3GHvtXRRTKbNVDpgNRbeeDIedupmKzGHyoF + EpkXwAyD \ npQt3pv3ntEqE4FQhB6nEU3QdfBOv
uBMZmG72LvqNXojGlLcd35iggggdiSpmij0QrKeTeo8onFZrFp1NG \ nrgTH6UcCiYPM61ehwNZh478pm6q75U8N7vIAVwcE
l + YSSwMg04i9NJ3ZSjojRS3mvDmLtiohpNHc \ n2jSMU1Um1ulH2YjEhPPZHwJ + rMpnamsIURIiOxeCasQIVwV9ljeFJq7Acq
6YOdkWAaPLF5W3V5vW \ n8tez0t22euiRTFtPW8KWrhbgqEi2rUZ4RFUvpLN4Y2Puzv6R2IbNbcSnZMVb3fmNh1Md6nbE7
N7D \ n7NAsgqXdAkWDCpiYUW3HGMXYeLikcwfmuu + ugObooz1wpn3X1JEAXv + LR2YiJBBC5Ne4QJwYSHf8 \ nQRtPKL
RexWTNdVsOaH51DUiDm5cQDh7Bp / o / txVqnw8nMs5Y38dhuyQKaj7ytax9mKDWAmodxmvW \ nVUCFP7biugxw4Q5ZyWt
ZLqpjBDVNdCrUnWvt / 8ke3n0eIDgEYiRFB09bJ1UVGeVKSiHCrt / ZK1A = "
    "KeyInfo": { "X509Data": { "x509SerialNumber" "SerialNumber"}}
```


Page 39


```
  },

  "Timestamp": {
    "Moment": "20170712214756.161Z"
    "Index": "2f000000002017051200000000000000000000000097739141481428"
    "NumeroSerie": "58.be.0e.58.16.82.6a.70.79.2b.b0.a1.f5.a8.84.8c"
  }
}
```


NOTE: The attributes "CanonicalizationMethod", "SignatureMethod", "reference" and "digestMethod" They are included in the JSON response to preserve compatibility with XML.

4 - Generation of certificates for HTTPS communication

The transfer of information between the institution and the INE is made using the HTTP protocol and TLS two-way. To carry it out, it is necessary that the institution generated by each of your servers (Used for this purpose) x509 certificate, which will be sent to INE for signature by the Certifying Authority (CA) established.

The generation process can vary, however it is considered mandatory:

- La llave privada debe ser RSA 2048
- Nombre de país (código 2 letras): MX
- Estado o provincia (nombre completo): Estado de la Institución
- Localidad (ciudad): Ciudad de la Institución
- Nombre de la organización: Nombre de la Institución
- Nombre común (FQDN): nombre-del-servidor.dominio-institucion
- Correo electrónico: correo del responsable del certificado

Estos datos se emplean para generar el Certificate Signing Request (.csr) que será enviado a la CA del INE; éste regresará el certificado firmado y, opcionalmente, una copia del certificado raíz de la CA (ambos en formato .cer), mismo que deberá ser usado para confirmar la identidad del servidor del INE. The signed certificate will be valid for 3 years.

The certificate signed by the CA INE also be used to authenticate the server.

The procedure is explained in detail in the document *Standard Certification Service DERFE* , included in the *technical certification package* .

NOTE: By the INE technical certification packet is sent. Application forms will be mail sent to **ssi.derfe@ine.mx**

40

Page 41

National Electoral Institute
Department of Infrastructure and Applied Technology
Technical specifications

5 Annexed

5.2 Response codes .

The description in the catalog of response codes for services is:

Code	Description	Service
0	okay	Central
100	License not in force.	Central
101	License not found.	Central
102	Unexpected error license validation.	Central
103	No privacy notice.	Central
104	Communication error with biometric service.	Central
105	Communication error with data query service.	Central
106	Error input parameters for biometrics.	Central
107	Unexpected service error outpatient.	Central
108	Error performing request biometric service.	Central
109	Error performing request data service.	Central
110	Invalid parameters.	Central
111	Failed to decrypt data	Central
112	Failed to verify the signature.	Central
113	Signature invalid.	Central
114	Error converting data encrypted.	Central
115	Failed to sign the response.	Central

116	Unexpected error saving the binnacle	Central
117	Unexpected error getting the timestamps	Central

Page 42

200	Error in search citizen.	Data
201	Unexpected error in the query citizen.	Data
202	Wrong parameters entry in the search citizen.	Data
205	Incomplete parameters search input citizen	Data
300	Unexpected service error biometric.	Biométricos
301	No files found footprints in the system.	Biométricos
302	No candidate fingerprint image valid.	Biométricos
303	Image format He sent as a sample is not supported.	Biométricos
304	Error comparing images.	Biométricos
305	The format of image It asks for file system is not supported.	Biométricos
306	The request is invalid for biometric.	Biométricos
307	The transaction id is invalid or null.	Biométricos
308	Citizen ID is invalid or null.	Biométricos
309	The type of image was not indicated.	Biométricos
310	And height parameters length are required.	Biométricos
311	The request contains more / less footprints possible.	Biométricos
312	The image type is incorrect.	Biométricos

Page 43

313	Too many open files.	Biométricos
314	The image has low quality or It is not a mark.	Biométricos
315	The image is low quality, very few trifles identifiable.	Biométricos
316	The image has a resolution incorrect.	Biométricos
317	Libraries are disabled.	Biométricos
318	The libraries are not loaded correctly.	Biométricos
320	Error converting image	Biométricos
321	Image format sent to convert it is not supported	Biométricos
322	No images in the petition Of conversation.	Biométricos
323	Invalid argument format	Biométricos

Table 27 Description of response codes obtained Verification Service

Page 44

Technical specifications

5.3 Catalog of Federal Entities.

standardized code	Federal entity
1	AGUASCALIENTES
2	BAJA CALIFORNIA
3	BAJA CALIFORNIA SUR
4	CAMPECHE
5	COAHUILA
6	COLIMA
7	CHIAPAS
8	CHIHUAHUA
9	MEXICO CITY
10	DURANGO
eleven	GUANAJUATO
12	WARRIOR
13	GENTLEMAN
14	JALISCO
fifteen	MEXICO
16	MICHOACAN
17	MORELOS
18	NAYARIT
19	NEW LION
twenty	OAXACA
twenty-one	PUEBLA
22	QUERETARO
2. 3	QUINTANA ROO
24	SAN LUIS POTOSI
25	SINALOA
26	SONORA
27	TABASCO
28	TAMAULIPAS
29	TLAXCALA
30	VERACRUZ
31	YUCATAN
32	ZACATECAS

Page 45

National Electoral Institute
Department of Infrastructure and Applied Technology
Technical specifications

5.4 Results comparison

Citizen data sent to the verification service can present

following cases.

1. If the data is sent to verify as null, the response will be null.

2. If the data is sent to verify vacuum, the response may be true or false depending on what is taken into database; example:

"ApellidoMaterno": "", or "lastName": "",

Only it occurs in data maiden name or mother's maiden name.

3. For the above, it is highly recommended, if the citizen does not have a name to send the data to null.

4. If any information to verify does not match what we have in the database response will be false.

5. The search keys are:

5.1. CIC.
5.2. OCR, key voter and issue number Credencial.

Four. Five