ID Card Toolkit

الهيئة الاتحادية للهـوية والجنسيـة

FEDERAL AUTHORITY FOR IDENTITY & CITIZENSHIP

ID Card Toolkit – Programmer's Reference - v1.8

Revision History

Version	Date	Description of changes
1.0	23rd Feb, 2018	Release Version 1.0.0
1.1	27th May, 2018	Release Version 1.0.5
1.2	17th Jul, 2018	Release Version 1.0.7
1.3	4th Sept, 2018	Release Version 1.0.8
1.4	10th Jan, 2019	Release Version 1.0.10
1.5	16th Feb, 2019	Release Version 1.0.13
1.6	09h Apr, 2019	Release Version 1.2.0
1.7	13h May, 2019	Release Version 1.3.0
1.8	22nd Feb, 2022	Release Version 2.0.3

Table of Contents

Abbreviations

API	Application Programming Interface
ICA	Identity & Citizenship Authority
JWS	Java Web Start
NFC	Near Field Communication
NPAPI	Netscape Plugin Application Programming Interface (NPAPI)
OTG	USB On-The-Go
PCSC	Personal Computer Smart Card
PKI	Public Key Infrastructure
REST	Representational State Transfer
SDK	Software Development Kit
SP	Service Provider
USB	Universal Serial Bus
VG	Validation Gateway, provided by ICA
VPN	Virtual Private Network
SAM	Secure Messaging Module
JRE	Java Runtime Environment
DSS	Digital Signature Service

1 Introduction

The Identity Citizenship Authority (ICA) has developed the ID Card Toolkit to address the requirements of service providers (SP) to integrate, into their business applications: Identification, Authentication, Digital Signature and Non-repudiation services, around the capabilities of the Emirates ID Card. The Toolkit is comprised of a number of Software Development Kits (SDK) supporting different programming languages and platforms. The supported programming languages include: C/C++, Java, Objective C, Swift and C#.

Programming language specific developer guides and samples are provided as part of each SDK to support developers with Toolkit integration.

The Toolkit also provides a migration path for SPs that have existing web applications using ICA's Validation Gateway (VG) Applet and ActiveX components. With minimal changes an existing web application can be upgraded to the new Toolkit.

1.1 Purpose

This document provides reference information required by the Toolkit programmers irrespective of the programming languages and environments used.

2 Emirates ID card Data Elements

This section of the document list the various data elements present on the Emirates ID Card.

2.1 Non Modifiable Data

#	Attribute Name	Description	Remarks
1	IdNumber	Unique Identification Number for the card holder	Format: 784YYYYnnnnnnnC • YYYY – Year of Birth of the Card Holder • nnnnnnn- unique number • C – Check Digit for the previous 14 digits
2	CardNumber	Unique Card Number of the card holder	Unique Card Number
3	IDType	ID Type	String with following values. • "ID" Identity Cards for Citizens • "IR" Identity Cars for Residents • "IL" Identity Cards for GCC
4	IssueDate	ID Card Issue Date	Format : DD/MM/YYYY DD-Date, MM-Month, YYYY-Year
5	ExpiryDate	ID Card Expiry Date	Format : DD/MM/YYYY DD-Date, MM-Month, YYYY-Year
6	TitleArabic	Title in Arabic	Refer to Toolkit References document for Title
7	FullNameArabic	Full Name in Arabic	**For Citizens :** Full name is a combination of First Name, Father Name, Grandfather Name, Grand Grandfather Name, Family Name, Tribe and Clan **For Residents:** Full name is a combination of First Name, Second Name, Third Name, Last Name, Family Name, Tribe and Clan
8	TitleEnglish	Title in English	Refer to Toolkit References document for Title
9	FullNameEnglish	Full Name in English	**For Citizens :** Full name is a combination of First Name, Father Name, Grandfather

			Name, Grand Grandfather Name, Family Name, Tribe and Clan **For Residents:** Full name is a combination of First Name, Second Name, Third Name, Last Name, Family Name, Tribe and Clan
10	Gender	Gender	For Male : M For Female : F Others :
11	NationalityArabic	Nationality in Arabic	Refer to Toolkit References document for the list of Nationalities
12	NationalityEnglish	Nationality in English	Refer to Toolkit References document for the list of Nationalities
13	NationalityCode	Nationality Code	Refer to Toolkit References document for the list of Nationalities
14	DateOfBirth	Date Of Birth	Format : DD/MM/YYYY DD-Date, MM-Month, YYYY-Year
15	PlaceOfBirthArabic	Place Of Birth in Arabic	
16	PlaceOfBirthEnglish	Place Of Birth in English	

2.2 Modifiable Data

#	Attribute Name	Description	Remarks
Occupation Details			
1	OccupationCode	Occupation Code	Refer to Toolkit References document for the Occupation Codes
2	OccupationArabic	Occupation in Arabic	Refer to Toolkit References document for the Occupation
3	OccupationEnglish	Occupation in English	Refer to Toolkit References document for the Occupation
4	FamilyID	Family ID	
5	OccupationTypeArabic	Occupation Type in Arabic	Refer to Toolkit References document for the Occupation Type
6	OccupationTypeEnglish	Occupation Type in English	Refer to Toolkit References document for the Occupation Type

7	OccupationFieldCode	Occupation Field Code	Refer to Toolkit References document for the Occupation Field Code
Company Details			
8	CompanyNameArabic	Company Name in Arabic	
9	CompanyNameEnglish	Company Name in English	
Marital Status and Husband ID Number			
10	MaritalStatusCode	Marital Status Code	Refer to Toolkit References document for the Marital Status codes
11	HusbandIdNumber	Husband Emirates Identity Number	
Sponsor Details			
12	SponsorTypeCode	Sponsor Type Code	Refer to Toolkit References document for the Sponsor Type Codes
13	SponsorUnifiedNumber	Sponsor Unified Number	
14	SponsorName	Sponsor Name	
Residency Details			
15	ResidencyTypeCode	Residency Type Code	
16	ResidencyNumber	Residency Number	
17	ResidencyExpiryDate	Residency Expiry Date	Format : DD/MM/YYYY DD-Date, MM-Month, YYYY-Year
Passport Details			
18	PassportNumber	Passport Number	
19	PassportTypeCode	Passport Type Code	Refer to Toolkit References document for the Passport Type Code
20	PassportCountryCode	Passport Country Code	Refer to Toolkit References document for the Passport Country Code
21	PassportCountryArabic	Passport Country Description in Arabic	Refer to Toolkit References document for the Passport Country Description
22	PassportCountryEnglish	Passport Country Description in English	Refer to Toolkit References document for the Passport Country Description
23	PassportIssueDate	Passport Issue Date	Format : DD/MM/YYYY DD-Date, MM-Month, YYYY-Year
24	PassportExpiryDate	Passport Expiry Date	Format : DD/MM/YYYY DD-Date, MM-Month, YYYY-Year
Education Qualification			

25	QualificationLevelCode	Qualification Level Code	
26	QualificationLevelArabic	Qualification Level Description in Arabic	
27	QualificationLevelEnglish	Qualification Level Description in English	
28	DegreeDescriptionArabic	Degree Description in Arabic	
29	DegreeDescriptionEnglish	Degree Description in English	
30	FieldOfStudyCode	Field Of Study Code	Refer to Toolkit References document for the Field of Study Code
31	FieldOfStudyArabic	Field Of Study in Arabic	Refer to Toolkit References document for the Field of Study
32	FieldOfStudyEnglish	Field Of Study in English	Refer to Toolkit References document for the Field of Study
33	PlaceOfStudyArabic	Place Of Study in Arabic	
34	PlaceOfStudyEnglish	Place Of Study in English	
35	DateOfGraduation	Date Of Graduation	Format : DD/MM/YYYY DD-Date, MM-Month, YYYY-Year
Mother Full Name			
36	MotherFullNameArabic	Mother Full Name in Arabic	**For Citizens :** Full name is a combination of First Name, Father Name, Grandfather Name, Grand Grandfather Name, Family Name, Tribe and Clan **For Residents:** Full name is a combination of First Name, Second Name, Third Name, Last Name, Family Name, Tribe and Clan
37	MotherFullNameEnglish	Mother Full Name in English	**For Citizens :** Full name is a combination of First Name, Father Name, Grandfather Name, Grand Grandfather Name, Family Name, Tribe and Clan **For Residents:** Full name is a combination of First Name, Second Name, Third Name, Last Name, Family Name, Tribe and Clan

2.3 Address Data

#	Attribute Name	Description	Remarks
Home Address			
1	AddressTypeCode	Address Type Code	
2	LocationCode	Location code	
3	EmiratesCode	Emirates code	Refer to Toolkit References document for the Emirates Code
4	EmiratesDescArabic	Emirate Description in Arabic	Refer to Toolkit References document for the Emirates Description
5	EmiratesDescEnglish	Emirate Description in English	Refer to Toolkit References document for the Emirates Description
6	CityCode	City code	Refer to Toolkit References document for City codes
7	CityDescArabic	City Description in Arabic	Refer to Toolkit References document for City Description
8	CityDescEnglish	City Description in English	Refer to Toolkit References document for City Description
9	StreetArabic	Street Name in Arabic	
10	StreetEnglish	Street Name in English	
11	POBOX	Post Office box Number	
12	AreaCode	Area code	Refer to Toolkit References document for Area Codes
13	AreaDescArabic	Area Description in Arabic	Refer to Toolkit References document for Area Description
14	AreaDescEnglish	Area Description in English	Refer to Toolkit References document for Area Description
15	BuildingNameArabic	Building Name in Arabic	
16	BuildingNameEnglish	Building Name in English	
17	FlatNo	Flat number	
18	ResidentPhoneNumber	Resident Phone Number	
19	MobilePhoneNumber	Mobile Number	
20	Email	Email Identifier	
Work Address			
1	AddressTypeCode	Address Type Code	
2	LocationCode	Location code	
3	CompanyNameArabic	Company Name Description in Arabic	

4	CompanyNameEnglish	Company Name Description in English	
5	EmiratesCode	Emirates code	Refer to Toolkit References document for Emirates Codes
6	EmiratesDescArabic	Emirate Description in Arabic	Refer to Toolkit References document for Emirates Description
7	EmiratesDescEnglish	Emirate Description in English	Refer to Toolkit References document for Emirates Description
8	CityCode	City code	Refer to Toolkit References document for City Codes
9	CityDescArabic	City Description in Arabic	Refer to Toolkit References document for City Description
10	CityDescEnglish	City Description in English	Refer to Toolkit References document for City Description
11	POBOX	Post Office box Number	
12	StreetArabic	Street Name in Arabic	
13	StreetEnglish	Street Name in English	
14	AreaCode	Area code	Refer to Toolkit References document for Area Codes
15	AreaDescArabic	Area Description in Arabic	Refer to Toolkit References document for Area Description
16	AreaDescEnglish	Area Description in English	Refer to Toolkit References document for Area Description
17	BuildingNameArabic	Building Name in Arabic	
18	BuildingNameEnglish	Building Name in English	
19	LandPhoneNumber	Office Landline Phone Number	
20	MobilePhoneNumber	Mobile Phone Number	
21	Email	Email Identifier	

2.4 Photo

#	Attribute Name	Description	Remarks
1	CardHolderPhoto	Photo of the Card holder	Photo in JFIF format (JPEG File Interchange Format)

2.5 Signature Image

#	Attribute Name	Description	Remarks

1	HolderSignatureImage	Card Holder Hand Signature Image	Signature Image in TIFF format (Tagged Image File Format)

2.6 Family Book

Family Book contains information regarding Family head, four wives and twenty children details.

#	Attribute Name	Description	Remarks
HeadOfFamily			
1	HolderIdNumber	Family Head Emirates ID Number	
2	FamilyID	Family Identifier	
3	EmirateNameArabic	Emirate Name in Arabic	
4	EmirateNameEnglish	Emirate Name in English	
5	FirstNameArabic	First Name in Arabic	
6	FirstNameEnglish	First Name in English	
7	FatherNameArabic	Father Name in Arabic	
8	FatherNameEnglish	Father Name in English	
9	GrandFatherNameArabic	Grand Father Name in Arabic	
10	GrandFatherNameEnglish	Grand Father Name in English	
11	TribeArabic	Tribe in Arabic	Refer to Toolkit References document for Title
12	TribeEnglish	Tribe in English	
13	ClanArabic	Clan in Arabic	
14	ClanEnglish	Clan in English	
15	NationalityCode	Nationality Code	Refer to Toolkit References document for Nationality Codes
16	NationalityArabic	Nationality in Arabic	Refer to Toolkit References document for Nationality Description
17	NationalityEnglish	Nationality in English	Refer to Toolkit References document for Nationality Description
18	Gender	Gender	For Male : M For Female : F Others :
19	DateOfBirth	Date of Birth	Format : DD/MM/YYYY DD-Date, MM-Month, YYYY-Year
20	PlaceOfBirthArabic	Place of Birth in Arabic	
21	PlaceOfBirthEnglish	Place of Birth in English	
22	MotherFullNameArabic	Mother Full Name in Arabic	

23	MotherFullNameEnglish	Mother Full Name in English	
Wife			
1	WifeIdNumber	Wife Emirates Identity Number	
2	FullNameArabic	Full Name in Arabic	**For Citizens :** Full name is a combination of First Name, Father Name, Grandfather Name, Grand Grandfather Name, Family Name, Tribe and Clan **For Residents:** Full name is a combination of First Name, Second Name, Third Name, Last Name, Family Name, Tribe and Clan
3	FullNameEnglish	Full Name in English	**For Citizens :** Full name is a combination of First Name, Father Name, Grandfather Name, Grand Grandfather Name, Family Name, Tribe and Clan **For Residents:** Full name is a combination of First Name, Second Name, Third Name, Last Name, Family Name, Tribe and Clan
4	NationalityCode	Nationality Code	Refer to Toolkit References document for Nationality Codes
5	NationalityArabic	Nationality in Arabic	Refer to Toolkit References document for Nationality Description
6	NationalityEnglish	Nationality in English	Refer to Toolkit References document for Nationality Description
Child			
1	ChildIdNumber	Child Emirates Identity Number	
2	FirstNameArabic	First Name in Arabic	
3	FirstNameEnglish	First Name in English	
4	Gender	Gender	For Male : M For Female : F Others :

5	DateOfBirth	Date of Birth	Format : DD/MM/YYYY DD-Date, MM-Month, YYYY-Year
6	PlaceOfBirthArabic	Place of Birth in Arabic	
7	PlaceOfBirthEnglish	Place of Birth in English	
8	MotherIdNumber	Mother Emirates Identity Number	
9	MotherFullNameArabic	Mother Full Name in Arabic	
10	MotherFullNameEnglish	Moher Full Name in English	

3 Procedure for Certificate preparation

This section describes the preparation procedure for the X.509 certificates used by the TLS protocol.

A certificate chain is a combination of all related certificates together in a single file commonly called certificate bundle or chain.

Certificate verification happens against the certificate chain or bundles. For preparing Certificate chain the related certificates need to be in base 64 encoded X.509 formats.

3.1 Preparing Base 64 X.509 certificate

Base 64 encoded X.509 format the certificate data exists between **"-----BEGIN CERTIFICATE-----"**
And "**-----END CERTIFICATE-----" t**ags as shown below:

```
-----BEGIN CERTIFICATE-----
MIIDQzCCAiugAwIBAgIQAR1804ZGefEEnWEODLh48jANBgkqhkiG9w0BAQUFADB0
MSowKAYDVQQDDCFUZWNobmljYWwgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkxDjAM
aIhAEg2oes/UEygvEF+7/+O67ANcErKKG2sJ1v2KS3gqPgnjdtNbKOBpVVmWAtAu
OA2+PWzIe54N3z8QUHz8gRwBz5b5nmI=
-----END CERTIFICATE-----
```

If the certificates are not in Base64 encoded X.509 format. Please use the following openssl commands to convert to base64 encoded format for different format certificates

Convert DER to base64 encoded format:
openssl x509 -inform der –in <CertFileName> -out <Base64enocdedCertFileName>

Convert x509 to base64 encoded format:
openssl x509 –in <CertFileName> -outform PEM -out <Base64enocdedCertFileName>

Convert pfx to base64 encoded format:
openssl pkcs12 –in <CertFileName> -out <Base64enocdedCertFileName>

<CertFilename>: final name of the: DER, X.509 or PFX file to be converted.
<Base64enocdedCertFileName>: file name where the converted base64 encoded certificate will be stored.

3.2 Preparing certificate chain

Find below the commands to prepare certificate chain or bundle with group of related base 64 X.509 certificates

For Windows:
copy <Certficate>+<Certficate>+<Certficate> <CertChain>

For Linux / Mac:
cat <Certficate> <Certficate> <Certficate> > <CertChain>

<Certficate>: Base 64 encoded X.509 certificate
<CertChain>: Certificate chain file to be created

4 Configuration Parameters

There are two approaches to configure the Toolkit SDK:

1. Programmatic Configuration – this approach supports specifying configuration parameters directly through the toolkit SDK API. The name of the parameter through which the configuration is provided is `config_params`.

2. Declarative Configuration – this approach supports specifying configuration parameters in a configuration file that is loaded by the toolkit during initialization. The name of the configuration file is `config_ap` for Toolkit operated in In-Process mode and `config_ag_ap` for Toolkit operated in agent mode.

A combination of both approaches can also be adopted. In the scenario where configuration parameters are specified both programmatically and declaratively the parameters specified programmatically take precedence. This facility can be used to override the configuration in `config_ap` at runtime if required.

These configuration parameters control various aspects of the Toolkit such as:

a. Enabling or disabling features
b. The location from which other required configuration files are loaded
c. The location to where log files are written

The following table describes the behavior of the toolkit when various combinations of `config_params` and `config_ap` are provided.

config_params	config_ap	Remarks
Provided	Not provided	All configuration parameters will be defined through `config_params`. ***Note:*** In the case of the Transitional Applet config_ap must be provided.
Not provided	Provided	The toolkit will search for `config_ap` in the directory where the toolkit binaries are located. All configuration parameters will be defined through `config_ap`.

Provided	Provided	The configuration parameters from config_params and config_ap are consolidated, where a parameter is provided by both sources the value from config_params will take precedence.
Not provided	Not provided	The toolkit will search for all required configuration files in the directory where the toolkit binaries are located (***Note:*** config_ap is not required). If all of the required configuration files are found the toolkit will complete initialization. Once initialized only the offline version of the read public data service will be available, if permitted by the license. Accessing any other service will return error.

Note: The minimum requirement for accessing other services is the vg_url configuration parameter.

The structure, content and format of config_params and config_ap / config_ag_ap are the same except for four additional parameters supported in config_params. These additional parameters are: config_url, config_directory, config_tls_cert and config_tls_cert_chain. In Agent mode, these additional configuration parameters need to be provided through config_ag_ap file placed in the agent binary location.

The config_url will take precedence over config_directory if both are specified. If neither of these parameters are specified the toolkit will load all configuration files from the directory where the toolkit binaries are located. Any parameter specified in config_params will take precedence over the same parameter specified in config_ap.

The following table describes the common configuration parameters that can be specified in config_params and config_ap / config_ag_ap:

Parameters	
vg_url	URL to access the Validation Gateway (VG). The URL can address either VG directly or a reverse proxy. ***Note:*** in the production VG environment, this URL must be HTTPS. In the pre-production environment, either HTTP or HTTPS may be used. ***Note:*** For toolkit operating in agent mode, if the vg_url is provided through the agent configuration config_ag_ap file and if application doesn't provide vg_url via config_ap / config_params, the vg_url provided through config_ag_ap is used.
vg_connection_timeout	Validation Gateway (VG) connection time out value in seconds. If VG does not respond within the timeout value, the toolkit will return network error.***Note:*** For toolkit operating in agent mode, if the vg_connection_timeout is provided through the agent configuration config_ag_ap file and if application doesn't provide vg_connection_timeout via config_ap / config_params, the

	vg_connection_timeout provided through config_ag_ap is used.
config_url	URL path from where configuration files are downloaded.
config_directory	Directory path from where configuration files are loaded. If config_url is specified along with this parameter then this parameter will be ignored.
environment	Used to indicate a sub-path under config_url and config_directory where all required configuration files, except config_ap, are loaded from. config_ap will always be loaded from the base url or directory specified by config_url and config_directory respectively. This option allows support for multiple environments by changing one configuration parameter.
log_directory	Path to the directory where the Toolkit log file is written. If this parameter is not specified, by default the toolkit binary path will be considered as the log_directory. If this parameter is not specified on the iOS and Android platforms, log file will not be created.
log_level	This optional parameter has the following values. The default value is INFO. **Value** — **Meaning** **ERROR** — Log all types of error events. **WARN** — Log warning and error events. A warning is any potentially harmful or undesirable state or behavior in the Toolkit. **INFO** — Log all informational, warning and error events An informational event is any significant life cycle event or major state transition.
log_performance_time	Boolean flag indicating whether performance counters should be logged. The default value is **false**.
enable_digital_signature_service	Boolean flag indicating whether the digital signature services (DSS) are enabled. The default value is **false**. ***Note:*** For toolkit operating in Agent mode, this parameter will not be considered if provided through application configuration as well.

jre32_directory jre64_directory	One of these parameters is required when the enable_digital_signature_service parameter is set to **true**. The value of the parameter is the path to the 32/64 bit java runtime environment (jre). The Toolkit will select the correct JRE according to the toolkit binary architecture. ***Note:*** For toolkit operating in Agent mode, this parameter will not be considered if provided through application configuration as well.
agent_tls_enabled	This parameter is used to enable TLS mode for communicating with agent. To enable SSL mode this parameter is set to **true**. The default value is **false.** ***Note:*** This value need to be same in both config_ag_ap file as well as config_ap file, for successful agent communication.
config_tls_cert	Base64 encoded string of Configuration URL TLS certificate. This parameter need to be provided through config_params parameter of the Initialize function when config_url is used. Refer to Section 3.1 for TLS certificate preparation. This certificate prepared need to be base64 encoded and provided as a string to this parameter
config_tls_cert_chain	Base64 encoded string of Configuration URL TLS certificate Issuer chain. This parameter need to be provided through config_params parameter of the Initialize function when config_url is used. Refer to Section 3.2 for issuer certificate chain preparation. This certificate chain prepared need to be base64 encoded and provided as a string.

The following table describes the configuration parameters that can be specified in config_params / config_ap:

Parameters	
read_publicdata_offline	Boolean flag indicating if public data should be read in offline mode. The reading of public data offline must also be enabled in the license. This parameter is required to distinguish the mode in which public data should be read when both the online and offline modes are permitted by the license.
agent_host_name	Common name of the certificate issued for Toolkit agent. This is an optional parameter which needs to be mentioned whenever there is a change in the agent certificate.
plugin_directory_path	This parameter is used only for Android; it specifies the path to the directory where the native plugin files are located. ***Note:*** This parameter is specific to Android.

The following table describes the configuration parameters that can be specified in `config_ag_ap`:

Parameters	
`agent_init_retry_interval`	This parameter is used only for Toolkit Agent Service; it specifies the periodic wait time period in seconds for Toolkit Initialization to happen successfully in case of Network error. ***Note:*** This parameter is specific to Toolkit Service.
`application_session_timeout`	This parameter is used only for Toolkit Agent Service; it specifies the timeout period in minutes a Toolkit application can remain idle holding a valid session with Toolkit Agent Service after application Initialization. ***Note:*** This parameter is specific to Toolkit Service.

Note: As the validity interval of Validate Gateway (VG) response is calculated based on the local time and time zone, the system / mobile on which the toolkit application is running need to correctly set the local time and time zone.

A sample of configuration parameter values is presented below:

```
# VG/VG Proxy access configuration
vg_url = http://vg-pre-prod.ica.gov.ae/ValidationGatewayService
vg_connection_timeout = 60

# Configuration Settings
environment = dev
config_url = http://application.organisation.com/config
config_directory = D:/toolkit_cfg

# Read Public Data Settings
read_publicdata_offline = false

# Log Settings
log_directory = D:/toolkit_logs
log_level = INFO
log_performance_time = true

# Agent Settings
agent_tls_enabled = false
config_connection_timeout = 10

# Digital Signature Settings
enable_digital_signature_service = false
jre32_directory = C:/Java/jre1.8.0_121
jre64_directory = C:/Java/jre1.8.0_121

# Android specific plugin configuration
plugin_directory_path =
/data/user/0/ae.emiratesid.idcard.toolkit.sample/lib/
```

5 Request ID

The purpose of the Request ID is to bind a Toolkit response to its corresponding request. This is an effective security measure to prevent the replay of old responses.

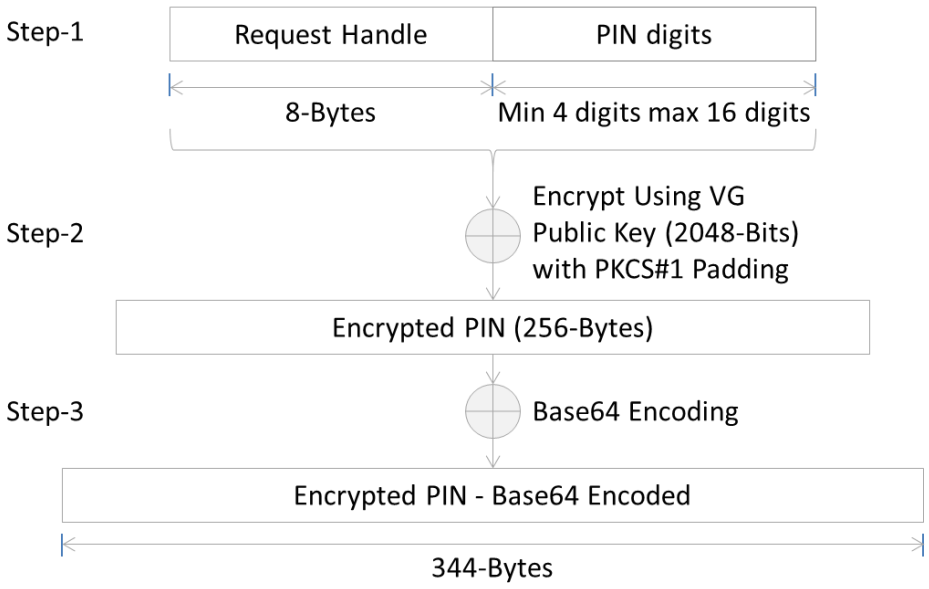
The Request ID is a randomly generated sequence of 40 bytes. An application that integrates with the ID Card Toolkit is responsible for generating the Request ID. A new request ID must be generated for each request. It must be ensured that a reliable secure random number generator is used in the generation process. The Request ID must be passed to the Toolkit in base64 encoded format. The base64 encoded Request ID will be 56-Bytes in length.

An application that integrates the ID Card Toolkit can verify that a response is current by checking that the Request ID sent in the request matches the one received in the response.

To ensure that this security measure is effective verification of the Request ID must be coupled with verification of the digital signature applied to XML response. The digital signature ensures that the response has not been changed in any way and the Request ID ensures that the response is current and not replayed.

6 PIN Encoding Procedure

Emirates ID card PIN is confidential and need to be protected. In order to protect PIN from unauthorized disclosure, ICA Toolkit employs a security scheme. The procedure to securely pass PIN to the ICA Toolkit is illustrated in the following diagram. Please refer to sample code provided along with the Toolkit for details PIN encoding.



Following steps need to be followed by the developers to encrypt PIN. Toolkit also provides language specific sample codes as reference implementation.

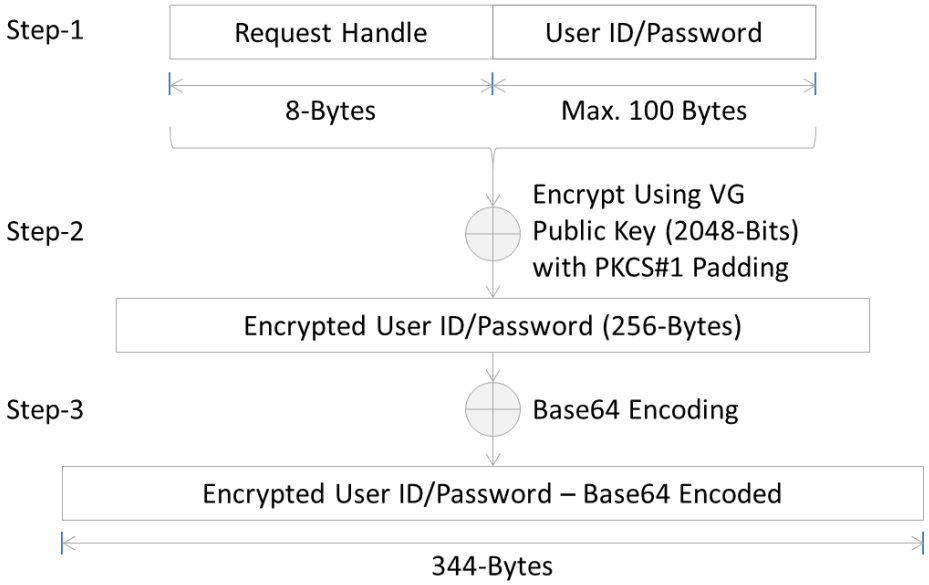
1. Prepare input data
    a. Input data is an array of N-Bytes where N = Length of Request Handle (8-Bytes) + length of the PIN.

b. First 8 bytes consist of Request Handle received by the application through the successful call to PrepareRequest method. The Request Handle returned by the Toolkit will be of base64 encoded format. Developers need to base64 decode the Request Handle returned by the Toolkit to extract the 8-Byte request handle.
c. PIN digits (0..9) are appended to the string after the Request Handle. That is from the 8th Byte onward.
d. Total number of digits in a PIN cannot exceed 16 and a valid PIN should have a minimum of 4 digits

2. Encrypt PIN using RSA encryption using VG public key (2048-bits) with PKCS#1 padding. The VG Public key is received through the successful call to GetDataProtectionKey method. This will give an encrypted output of 256-Bytes.
3. Convert the encrypted PIN which is of 256-Bytes into base64 format. The output base64 string would be of 344-Bytes. The application developer needs to pass this encrypted PIN in base64 format only to Toolkit services that take PIN as a parameter.

7 User ID & Password Encoding Procedure

Register Device service of the Toolkit requires User ID and Password of the authorized Service Provider (SP) user for authentication. For security purpose, the User ID and Password need to be sent in encrypted format. Following diagram illustrates the procedure to encode User ID and Password;



Please note that the User ID and Password need to be encoded separately using the procedure illustrated in the diagram. Following steps provides the details of the procedure. Toolkit also provides language specific sample codes as reference implementation.

1. Prepare input data
    a. Input data is an array of N-Bytes where N = Length of Request Handle (8-Bytes) + length of the User ID/Password. Length of the User ID/Password cannot exceed 100 bytes.
    b. First 8 bytes consist of Request Handle received by the application through the successful call to PrepareRequest method. The Request Handle returned by the Toolkit

will be of base64 encoded format. Developers need to base64 decode the Request Handle returned by the Toolkit to extract the 8-Byte request handle.

c. User ID/Password is appended to the string after the Request Handle. That is from the 8th Byte onward.

2. Encrypt User ID/Password using RSA encryption using VG public key (2048-bits) with PKCS#1 padding. The VG Public key is received through the successful call to GetDataProtectionKey method. This will give an encrypted output of 256-Bytes.
3. Convert the encrypted User ID/Password which is of 256-Bytes into base64 format. The output base64 string would be of 344-Bytes. The application developer needs to pass this encrypted User ID/Password in base64 format only to the RegisterDevice service of the Toolkit.

8 Fingerprint reference Identifiers

Following are the list of finger reference identifiers with corresponding names

Reference Identifier	Finger Name
0	Finger validation against both the reference identifiers stored in the card
3	NO_MEANING
5	RIGHT_THUMB
9	RIGHT_INDEX
13	RIGHT_MIDDLE
17	RIGHT_RING
21	RIGHT_LITTLE
6	LEFT_THUMB
10	LEFT_INDEX
14	LEFT_MIDDLE
18	LEFT_RING
22	LEFT_LITTLE

9 Digital Signature Context attributes

Following are the list of attributes corresponding to the signature creation

Attribute	Description
SIGNATURE_LEVEL **(Supported Signatures levels)** Refer to ETSI EN 319 162 document for details regarding packaging modes. Refer to the following documents for details regarding signature profiles 1. ETSI EN 319 132 2. ETSI EN 319 122 3. ETSI EN 319 142	**BASELINE_B** (Baseline) Basic Electronic Signature, basic form just satisfying Directive legal requirements for advanced signature.
	BASELINE_T (timestamp) Adding timestamp field to protect against repudiation.
	BASELINE_LT (Long Term) Adding Revocation values for long term validation
	BASELINE_LTA (Long Term Archived) Adding archived timestamp values at multiple levels for long term signature validation
PACKAGING_MODE **(Supported packaging modes)** Refer to ETSI EN 319 162 document for details regarding packaging modes	**ENVELOPED** When the Signature applies to data that surround the rest of the document
	ENVELOPING When the signed data form a sub element of the signature itself.
	DEATACHED When the signature relates to the external resources separated from it.
DIGEST_ALGORITHM **(Supported Digest algorithms)**	**DS_ALG_SHA256** SHA256 digest algorithm

user_pin	Emirates ID Card PKI PIN
pkcs11_module_path	EIDA Toolkit SDK binary path
tsa_url	Time Stamping URL
ocsp_url	OCSP URL
cert_path	Folder path of issuer and root certificates
SIGNER_LOCATION	Location the signer 1. country_code 2. state_or_province 3. postal_code[4. locality 5. street

10 PAdES Signature parameters

Following are the list of Parameters corresponding to the PAdES signature creation

Parameter	Description
sign_reason	Purpose of signing the PDF document
signer_location	Location of the Person who is signing the PDF document
signer_contact_info	Contact information of the signer
signature_xaxis	X coordinate location for placing the visible signature box
signature_yaxis	Y coordinate location for placing the visible signature box
signature_image	Signature image to be placed on the signature box
background_color	Signature box background color to be used
font_color	Text color in the signature box
font_name	Font to be used for the signature box (Please make sure that the specified font should be available in the system)
font_size	Size of the signature text font
signature_text	Visible signature text
sign_visible	Flag to enable or disable visible signature in pdf
name_position	Position of the signature text relative to the signature (LEFT, RIGHT, TOP, BOTTOM)
page_number	Page number of the pdf to attach visible signature

11 Digital Signature Verification Context attributes

Following are the list of parameters corresponding to the signature verification

Parameter	Description
ocsp_url	OCSP URL
cert_path	Folder Path of issuer and root certificates
is_deattached	TRUE, if the verified document is of detached type or else FALSE

12 Digital Signature Verification Report Types

The result of the validation process consists of three elements:

- Simple report
- Detailed report and
- Diagnostic data

All these reports are encoded using XML, which allows the implementer to easily manipulate and extract information for further analysis. You will find below a detailed description of each of these elements.

12.1 Simple Report

This is a sample of the simple validation report.

```
<SimpleReport xmlns="http://dss.esig.europa.eu/validation/simple-report">
    <Policy>
        <PolicyName>QES AdESQC TL based</PolicyName>
        <PolicyDescription>Validate electronic signatures...</PolicyDescription>
    </Policy>
    <ValidationTime>2016-05-09T10:55:02</ValidationTime>
    <DocumentName>PAdES_B_PVDB.pdf</DocumentName>
    <ValidSignaturesCount>1</ValidSignaturesCount>
    <SignaturesCount>1</SignaturesCount>
    <Signature Id="id-30b3acd8c4fe0ced13b26ed2e6574d91e2e77b19e06a42b6c513a0b046b4561b"
SignatureFormat="PAdES_BASELINE_B">
        <SigningTime>2015-07-30T13:49:14</SigningTime>
        <SignedBy>Pierrick Vandenbroucke (Signature)</SignedBy>
        <Indication>TOTAL_PASSED</Indication>
        <SignatureLevel>AdESqc</SignatureLevel>
        <Warnings>The certificate is not supported by SSCD!</Warnings>
        <Infos>The certificate is not issued to a legal person.</Infos>
        <SignatureScope name="Full PDF" scope="FullSignatureScope">Full
document</SignatureScope>
    </Signature>
</SimpleReport>
```

The result of the validation process is based on very complex rules. The purpose of this report is to make as simple as possible the information while keeping the most important elements. Thus the end user can, at a glance, have a synthetic view of the validation. To build this report the framework uses some simple rules and the detailed report as input.

12.2 Detailed Report

This is a sample of the detailed validation report. Its structure is based on the ETSI standard [R08] and is built around Basic Building Blocks, Basic Validation Data, Timestamp Validation Data, AdES-T Validation Data and Long Term Validation Data. Some segments were deleted to make reading easier. They are marked by three dots:

```
<DetailedReport xmlns="http://dss.esig.europa.eu/validation/detailed-report">
    <Signatures Id="id-30b3acd8c4fe0ced13b26ed2e6574d91e2e77b19e06a42b6c513a0b046b4561b">
        <ValidationProcessBasicSignatures>
```

```
            <Constraint Id="id-
30b3acd8c4fe0ced13b26ed2e6574d91e2e77b19e06a42b6c513a0b046b4561b">
                <Name NameId="ADEST_ROBVPIIC">Is the result of the Basic Validation Process
conclusive?</Name>
                <Status>OK</Status>
            </Constraint>
            <Conclusion>
                <Indication>PASSED</Indication>
            </Conclusion>
        </ValidationProcessBasicSignatures>
        <ValidationProcessLongTermData>
            <Constraint>
                <Name NameId="LTV_ABSV">Is the result of the Basic Validation Process
acceptable?</Name>
                <Status>OK</Status>
            </Constraint>
                   ...
            <Conclusion>
                <Indication>PASSED</Indication>
            </Conclusion>
        </ValidationProcessLongTermData>
        <ValidationProcessArchivalData>
            <Constraint>
                <Name NameId="ARCH_LTVV">Is the result of the LTV validation process
acceptable?</Name>
                <Status>OK</Status>
            </Constraint>
            <Conclusion>
                <Indication>PASSED</Indication>
            </Conclusion>
        </ValidationProcessArchivalData>
    </Signatures>
    <BasicBuildingBlocks Id="B033DE5A4F6980014D4A51D7C4248C410AAEA11A95B2E731FD277DBC69516D62"
Type="REVOCATION">
        <ISC>
            <Constraint>
                <Name NameId="BBB_ICS_ISCI">Is there an identified candidate for the signing
certificate?</Name>
                <Status>OK</Status>
            </Constraint>
            <Conclusion>
                <Indication>PASSED</Indication>
            </Conclusion>
        </ISC>
        <CV>
            ...
            <Conclusion>
                <Indication>PASSED</Indication>
            </Conclusion>
        </CV>
        <SAV>
            <Constraint>
                <Name NameId="ASCCM">Are signature cryptographic constraints met?</Name>
                <Status>OK</Status>
            </Constraint>
            <Conclusion>
                <Indication>PASSED</Indication>
            </Conclusion>
```

```
        </SAV>
        <XCV>
            ...
            <Conclusion>
                <Indication>PASSED</Indication>
            </Conclusion>
        </XCV>
        <Conclusion>
            <Indication>PASSED</Indication>
        </Conclusion>
    </BasicBuildingBlocks>
    <BasicBuildingBlocks Id="id-
30b3acd8c4fe0ced13b26ed2e6574d91e2e77b19e06a42b6c513a0b046b4561b" Type="SIGNATURE">
        <FC>
            ...
            <Conclusion>
                <Indication>PASSED</Indication>
            </Conclusion>
        </FC>
        <ISC>
            ...
            <Conclusion>
                <Indication>PASSED</Indication>
            </Conclusion>
        </ISC>
        <VCI>
            ...
            <Conclusion>
                <Indication>PASSED</Indication>
            </Conclusion>
        </VCI>
        <CV>
            ...
            <Conclusion>
                <Indication>PASSED</Indication>
            </Conclusion>
        </CV>
        <SAV>
            ...
            <Conclusion>
                <Indication>PASSED</Indication>
            </Conclusion>
        </SAV>
        <XCV>
            ...
            <Conclusion>
                <Indication>PASSED</Indication>
            </Conclusion>
        </XCV>
        <Conclusion>
            <Indication>PASSED</Indication>
        </Conclusion>
    </BasicBuildingBlocks>
    <BasicBuildingBlocks Id="DEBA6AAEB488203F71BF3EFC5BCD9F120A9BA500C011010A94911D1224C8FC15"
Type="REVOCATION">
        <ISC>
            ...
            <Conclusion>
```

```
                <Indication>PASSED</Indication>
            </Conclusion>
        </ISC>
        <CV>
            ...
            <Conclusion>
                <Indication>PASSED</Indication>
            </Conclusion>
        </CV>
        <SAV>
            ...
            <Conclusion>
                <Indication>PASSED</Indication>
            </Conclusion>
        </SAV>
        <XCV>
            ...
            <Conclusion>
                <Indication>PASSED</Indication>
            </Conclusion>
        </XCV>
        <Conclusion>
            <Indication>PASSED</Indication>
        </Conclusion>
    </BasicBuildingBlocks>
</DetailedReport>
```

The building blocks are divided into seven elements:
FC - Format Checking
ISC - Identification of the Signing Certificate
VCI - Validation Context Initialization
RFC - Revocation Freshness Checker
XCV - X.509 certificate validation
CV - Cryptographic Verification
SAV - Signature Acceptance Validation
The following additional elements also can be expected in case of validation in the past:
PCV - Past Certificate Validation
VTS - Validation Time Sliding process
POE extraction - Proof Of Existence extraction
PSV - Past Signature Validation
Each block contains a number of rules that are executed sequentially. The rules are driven by the constraints defined in the validation policy. The result of each rule is OK or NOT OK. The process is stopped when the first rule fails. Each block also contains a conclusion. If all rules are met then the conclusion node indicates PASSED. Otherwise FAILED or INDETERMINATE indication is returned depending on the ETSI standard definition.

12.3 Diagnostic Data

This is a data set constructed from the information contained in the signature itself, but also from information retrieved dynamically as revocation data and information extrapolated as the mathematical validity of a signature. All this information is independent of the applied validation policy. Two different validation policies applied to the same diagnostic data can lead to different results.

This is an example of the diagnostic data for a XAdES signature. Certain fields and certain values were trimmed or deleted to make reading easier:

```
<DiagnosticData xmlns="http://dss.esig.europa.eu/validation/diagnostic">
    <DocumentName>PAdES_B_PVDB.pdf</DocumentName>
    <Signature Id="id-30b3acd8c4fe0ced13b26ed2e6574d91e2e77b19e06a42b6c513a0b046b4561b">
        <DateTime>2015-07-30T13:49:14</DateTime>
        <SignatureFormat>PAdES_BASELINE_B</SignatureFormat>
        <BasicSignature>
            <EncryptionAlgoUsedToSignThisToken>RSA</EncryptionAlgoUsedToSignThisToken>
            <KeyLengthUsedToSignThisToken>1024</KeyLengthUsedToSignThisToken>
            <DigestAlgoUsedToSignThisToken>SHA256</DigestAlgoUsedToSignThisToken>
            <ReferenceDataFound>true</ReferenceDataFound>
            <ReferenceDataIntact>true</ReferenceDataIntact>
            <SignatureIntact>true</SignatureIntact>
            <SignatureValid>true</SignatureValid>
        </BasicSignature>
        <SigningCertificate
Id="4199E98D0E5B02935EB72DC8B7F9188E27DDF8A1DCB7BC8C3C3F3C7C1C099D5B">
            <AttributePresent>true</AttributePresent>
            <DigestValuePresent>true</DigestValuePresent>
            <DigestValueMatch>true</DigestValueMatch>
            <IssuerSerialMatch>true</IssuerSerialMatch>
        </SigningCertificate>
        <CertificateChain>
            <ChainCertificate
Id="4199E98D0E5B02935EB72DC8B7F9188E27DDF8A1DCB7BC8C3C3F3C7C1C099D5B">
                <Source>SIGNATURE</Source>
            </ChainCertificate>
            <ChainCertificate
Id="5A304EA217132A215EF6769CC2933E867377EBDD62815B8FB930F6151ECC6DD3">
                <Source>SIGNATURE</Source>
            </ChainCertificate>
            <ChainCertificate
Id="9F9744463BE13714754E1A3BECF98C08CC205E4AB32028F4E2830C4A1B2775B8">
                <Source>TRUSTED_LIST</Source>
            </ChainCertificate>
        </CertificateChain>
        <ContentType>application/pdf</ContentType>
        <SignatureScopes>
            <SignatureScope name="Full PDF" scope="FullSignatureScope">Full
document</SignatureScope>
        </SignatureScopes>
    </Signature>
    <UsedCertificates>
        <Certificate Id="5A304EA217132A215EF6769CC2933E867377EBDD62815B8FB930F6151ECC6DD3">
            <SubjectDistinguishedName Format="CANONICAL">2.5.4.5=#1306323031313036,cn=citizen
ca,c=be</SubjectDistinguishedName>
            <SubjectDistinguishedName Format="RFC2253">2.5.4.5=#1306323031313036,CN=Citizen
CA,C=BE</SubjectDistinguishedName>
            <IssuerDistinguishedName Format="CANONICAL">cn=belgium root
ca2,c=be</IssuerDistinguishedName>
            <IssuerDistinguishedName Format="RFC2253">CN=Belgium Root
CA2,C=BE</IssuerDistinguishedName>
            <SerialNumber>626284432178890619388938501552115081 30</SerialNumber>
            <CommonName>Citizen CA</CommonName>
            <CountryName>BE</CountryName>
```

```
            <DigestAlgAndValue>
                <DigestMethod>SHA1</DigestMethod>
                <DigestValue>dMxuVVn/18LdBSbAwhWTxWyThPM=</DigestValue>
            </DigestAlgAndValue>
            <NotAfter>2017-07-16T13:00:00</NotAfter>
            <NotBefore>2010-11-16T12:00:00</NotBefore>
            <PublicKeySize>2048</PublicKeySize>
            <PublicKeyEncryptionAlgo>RSA</PublicKeyEncryptionAlgo>
            <KeyUsageBits>
                <KeyUsage>keyCertSign</KeyUsage>
                <KeyUsage>crlSign</KeyUsage>
            </KeyUsageBits>
            <BasicSignature>
                <EncryptionAlgoUsedToSignThisToken>RSA</EncryptionAlgoUsedToSignThisToken>
                <KeyLengthUsedToSignThisToken>2048</KeyLengthUsedToSignThisToken>
                <DigestAlgoUsedToSignThisToken>SHA1</DigestAlgoUsedToSignThisToken>
                <ReferenceDataFound>true</ReferenceDataFound>
                <ReferenceDataIntact>true</ReferenceDataIntact>
                <SignatureIntact>true</SignatureIntact>
                <SignatureValid>true</SignatureValid>
            </BasicSignature>
            ...
        </Certificate>
        <Certificate Id="7C37121A7E63DCE1F808523CC3A70AF9428A5C973FFAF773E615A526C9E363A7">
            <SubjectDistinguishedName Format="CANONICAL">c=be,cn=belgium ocsp
responder</SubjectDistinguishedName>
            <SubjectDistinguishedName Format="RFC2253">C=BE,CN=Belgium OCSP
Responder</SubjectDistinguishedName>
            <IssuerDistinguishedName Format="CANONICAL">2.5.4.5=#1306323031313036,cn=citizen
ca,c=be</IssuerDistinguishedName>
            <IssuerDistinguishedName Format="RFC2253">2.5.4.5=#1306323031313036,CN=Citizen
CA,C=BE</IssuerDistinguishedName>
            <SerialNumber>48357032784599652094806 78</SerialNumber>
            <CommonName>Belgium OCSP Responder</CommonName>
            <CountryName>BE</CountryName>
            <DigestAlgAndValue>
                <DigestMethod>SHA1</DigestMethod>
                <DigestValue>ywdlEr+sSR+BKDStlAOj2bdcwcE=</DigestValue>
            </DigestAlgAndValue>
            <NotAfter>2017-01-29T12:00:00</NotAfter>
            <NotBefore>2015-12-08T12:00:00</NotBefore>
            <PublicKeySize>2048</PublicKeySize>
            <PublicKeyEncryptionAlgo>RSA</PublicKeyEncryptionAlgo>
            <KeyUsageBits>
                <KeyUsage>digitalSignature</KeyUsage>
            </KeyUsageBits>
            <IdKpOCSPSigning>true</IdKpOCSPSigning>
            <IdPkixOcspNoCheck>true</IdPkixOcspNoCheck>
            <BasicSignature>
                <EncryptionAlgoUsedToSignThisToken>RSA</EncryptionAlgoUsedToSignThisToken>
                <KeyLengthUsedToSignThisToken>2048</KeyLengthUsedToSignThisToken>
                <DigestAlgoUsedToSignThisToken>SHA1</DigestAlgoUsedToSignThisToken>
                <ReferenceDataFound>true</ReferenceDataFound>
                <ReferenceDataIntact>true</ReferenceDataIntact>
                <SignatureIntact>true</SignatureIntact>
                <SignatureValid>true</SignatureValid>
            </BasicSignature>
            ...
```

```
        </Certificate>
        <Certificate Id="9F9744463BE13714754E1A3BECF98C08CC205E4AB32028F4E2830C4A1B2775B8">
            <SubjectDistinguishedName Format="CANONICAL">cn=belgium root
ca2,c=be</SubjectDistinguishedName>
            <SubjectDistinguishedName Format="RFC2253">CN=Belgium Root
CA2,C=BE</SubjectDistinguishedName>
            <IssuerDistinguishedName Format="CANONICAL">cn=belgium root
ca2,c=be</IssuerDistinguishedName>
            <IssuerDistinguishedName Format="RFC2253">CN=Belgium Root
CA2,C=BE</IssuerDistinguishedName>
            <SerialNumber>3098404661496965511</SerialNumber>
            <CommonName>Belgium Root CA2</CommonName>
            <CountryName>BE</CountryName>
            <DigestAlgAndValue>
                <DigestMethod>SHA1</DigestMethod>
                <DigestValue>UcygcQr3cz00rNwZRQmfQ1x/xZ8=</DigestValue>
            </DigestAlgAndValue>
            <NotAfter>2021-12-15T09:00:00</NotAfter>
            <NotBefore>2007-10-04T12:00:00</NotBefore>
            <PublicKeySize>2048</PublicKeySize>
            <PublicKeyEncryptionAlgo>RSA</PublicKeyEncryptionAlgo>
            <KeyUsageBits>
                <KeyUsage>keyCertSign</KeyUsage>
                <KeyUsage>crlSign</KeyUsage>
            </KeyUsageBits>
            <BasicSignature>
                <EncryptionAlgoUsedToSignThisToken>RSA</EncryptionAlgoUsedToSignThisToken>
                <KeyLengthUsedToSignThisToken>2048</KeyLengthUsedToSignThisToken>
                <DigestAlgoUsedToSignThisToken>SHA1</DigestAlgoUsedToSignThisToken>
                <ReferenceDataFound>true</ReferenceDataFound>
                <ReferenceDataIntact>true</ReferenceDataIntact>
                <SignatureIntact>true</SignatureIntact>
                <SignatureValid>true</SignatureValid>
            </BasicSignature>
            ...
        </Certificate>
        <Certificate Id="4199E98D0E5B02935EB72DC8B7F9188E27DDF8A1DCB7BC8C3C3F3C7C1C099D5B">
            <SubjectDistinguishedName
Format="CANONICAL">2.5.4.5=#130b383730313237333037333338,2.5.4.42=#130d506965727269636b205061636
f,2.5.4.4=#130d56616e64656e62726f75636b65,cn=pierrick vandenbroucke
(signature),c=be</SubjectDistinguishedName>
            <SubjectDistinguishedName
Format="RFC2253">2.5.4.5=#130b383730313237333037333338,2.5.4.42=#130d506965727269636b205061636f,
2.5.4.4=#130d56616e64656e62726f75636b65,CN=Pierrick Vandenbroucke
(Signature),C=BE</SubjectDistinguishedName>
            <IssuerDistinguishedName Format="CANONICAL">2.5.4.5=#1306323031313036,cn=citizen
ca,c=be</IssuerDistinguishedName>
            <IssuerDistinguishedName Format="RFC2253">2.5.4.5=#1306323031313036,CN=Citizen
CA,C=BE</IssuerDistinguishedName>
            <SerialNumber>212676479325590367318037476768858558 37</SerialNumber>
            <CommonName>Pierrick Vandenbroucke (Signature)</CommonName>
            <CountryName>BE</CountryName>
            <GivenName>Pierrick Paco</GivenName>
            <Surname>Vandenbroucke</Surname>
            <DigestAlgAndValue>
                <DigestMethod>SHA1</DigestMethod>
                <DigestValue>42by2G4VKm3tcQ6c6F5XvOMsSLk=</DigestValue>
            </DigestAlgAndValue>
```

```
            <NotAfter>2017-02-18T00:59:59</NotAfter>
            <NotBefore>2012-02-23T09:24:09</NotBefore>
            <PublicKeySize>1024</PublicKeySize>
            <PublicKeyEncryptionAlgo>RSA</PublicKeyEncryptionAlgo>
            <KeyUsageBits>
                <KeyUsage>nonRepudiation</KeyUsage>
            </KeyUsageBits>
            <BasicSignature>
                <EncryptionAlgoUsedToSignThisToken>RSA</EncryptionAlgoUsedToSignThisToken>
                <KeyLengthUsedToSignThisToken>2048</KeyLengthUsedToSignThisToken>
                <DigestAlgoUsedToSignThisToken>SHA1</DigestAlgoUsedToSignThisToken>
                <ReferenceDataFound>true</ReferenceDataFound>
                <ReferenceDataIntact>true</ReferenceDataIntact>
                <SignatureIntact>true</SignatureIntact>
                <SignatureValid>true</SignatureValid>
            </BasicSignature>
           ...
        </Certificate>
    </UsedCertificates>
</DiagnosticData>
```