<K+ LAB>

Fundación Karisma

ANEXOS TÉCNICOS

Análisis de la aplicación

CÉDULA DIGITAL

Este informe se basa en investigaciones realizadas por el Laboratorio de seguridad digital y privacidad de la Fundación Karisma durante el segundo semestre del 2024 y en el mes de enero 2025. En el presente documento se quitaron algunas partes para no generar riesgos de seguridad digital. La versión completa se mandó a las entidades del Estado a cargo de la aplicación, la Registraduría Nacional del Estado Civil (RNEC) y al MINTIC.

ÍNDICE

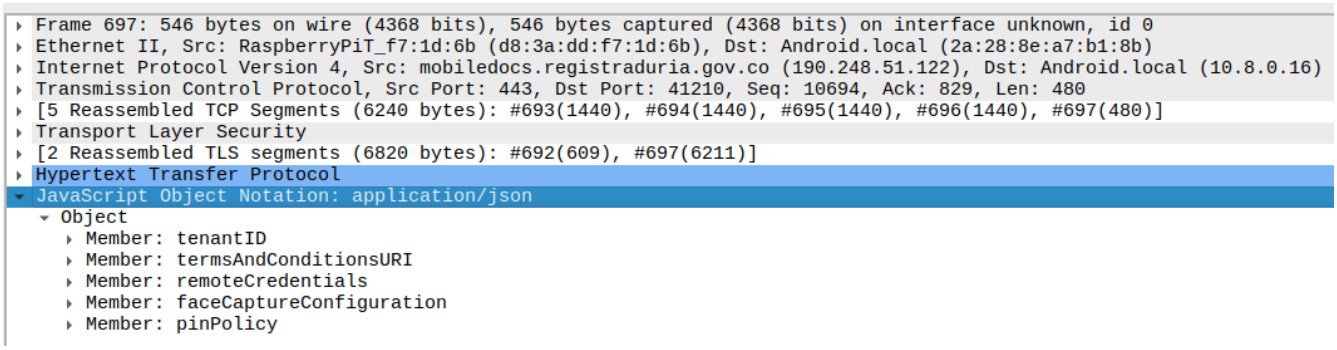
ANEXO I: EL ARCHIVO DE CONFIGURACIÓN DE LA APLICACIÓN

Al iniciar la aplicación de *Cédula digital*, una de las primeras cosas que hace es buscar un archivo de configuración ubicado en el subdominio de la RNEC (“mobiledocs.registraduria.gov.co”).

Esto se puede observar en la solicitud HTTPS generada por la aplicación y capturada y descifrada con *Pirogue Tool Suite* (el 19 de noviembre 2024):

[Se quitó esta parte para no generar riesgos de seguridad]

En respuesta a esta solicitud, el servidor manda al teléfono el siguiente archivo de configuración JSON:



Contenido del archivo de configuración JSON:

El archivo JSON está disponible sin autenticación en esta URL:

[Se quitó esta parte para no generar riesgos de seguridad]

Y se puede visualizar así:

[Se quitó esta parte para no generar riesgos de seguridad]

[Se quitó esta parte para no generar riesgos de seguridad]

Algunos extractos interesantes – conteniendo en particular las URL con los términos y condiciones y la política de privacidad de la aplicación *Mobile ID* de IDEMIA - se muestran aquí:


```
"termsAndConditionsURI": [
    {
        "locale": "en_US",
        "value": "https://www.idemia-mobile-id.com/enduserterms"
    }
],
"remoteCredentials": [
    {
        "friendlyName": [
            {
                "locale": "en_US",
                "value": "Cédula de ciudadania"
            }
        ],
        "documentType": "IC",
        "jurisdictionId": "COL",
        "businessProcess": "COLOMBIA_RNEC",
        "credentialScopes": [
            "id_basic",
            "id_basic_clb",
            "id_csj",
            "user_inum"
        ],
        "credentialAcrValues": [
            "mid",
            "mid_pin",
            "mid_face_pin",
            "mid_face",
            "mid_light_oembio"
        [...]

        "URIs": {
            "faq": [
                {
                    "locale": "en_US",
                    "value": "https://www.idemia-mobile-id.com/FAQs"
                }
            ],
            "help": [
```

```
                    {
                        "locale": "en_US",
                        "value": "https://www.idemia-mobile-id.com/help"
                    }
                ],
                "about": [
                    {
                        "locale": "en_US",
                        "value": "https://www.idemia-mobile-id.com/about"
                    }
                ],
                "privacyPolicy": [
                    {
                        "locale": "en_US",
                                                                    "value":
"https://www.idemia-mobile-id.com/enduserprivacy"
                    }
                ],
                "termsAndConditions": [
                    {
                        "locale": "en_US",
                                                                    "value":
"https://www.idemia-mobile-id.com/enduserterms"
                    }
                                                            "issuingAuthority":
"https://mobiledocs.registraduria.gov.co/fabric"
```


[Se quitó esta parte para no generar riesgos de seguridad]

El archivo JSON que se puede acceder en esta última URL es el siguiente:

[Se quitó esta parte para no generar riesgos de seguridad]

Muestra que han configurado niveles bajos (“LOW”) en estos cuatro procesos: faceCaptureConfiguration, ONLINE_AUTHENTICATION, UNLOCK y MIGRATION.

ANEXO 2: EL FORMULARIO "TRAMITA LA CÉDULA DIGITAL SIN AGENDAR CITA" Y SUS ERRORES

El formulario su ubica en la URL: https://ceduladigital.registraduria.gov.co/index y se presenta de la forma siguiente:

Lo llenamos (varias veces) y analizamos el tráfico HTTP(S) generado por la página web. En la solicitud HTTPS/POST de envío de los datos, el servidor responde con el código 302 ("HTTP 302 found") que indica que la página se trasladó a otra dirección y no hay otra respuesta después. La ubicación de la página respondida por el servidor ("Location") es la misma que la de esta página, generando así un

“bucle”. La persona usuaria se encuentra entonces de nuevo en la misma página sin ninguna información sobre su registro. Tampoco recibe correo y no se puede conectar usando el link “Si ya tiene cuenta Ingresa aquí”.

Aquí van los extractos del tráfico HTTPS que muestran esto (los datos personales reales se reemplazaron aquí por XXX):

> https://ceduladigital.registraduria.gov.co/index **[SOLICITUD, datos mandados]**
> Host: ceduladigital.registraduria.gov.co
> […]
> fullname=XXXX&document=XXX&issuedate=XXX&email=XXX&email_confirmation=XXX&password=XXX&password_confirmation=XXX
> **POST**
>
> **HTTP/1.1 302 Found** **[RESPUESTA SERVIDOR, datos recibidos]**
> Date: Mon, 23 Sep 2024 16:26:12 GMT
> […]
> **Location: https://ceduladigital.registraduria.gov.co**

Además en otra solicitud, el servidor web responde con un error: “**NS_ERROR_CORRUPTED_CONTENT**” que también debería ser analizado.

ANEXO 3: CARACTERÍSTICAS MÍNIMAS ANDROID E IPHONE (RESPUESTA A LA PREGUNTA 8 AL DERECHO DE PETICIÓN)

En su respuesta al Derecho de petición sobre los motivos por los cuales la aplicación requiere teléfonos recientes (pregunta 8), la RNEC dio esta respuesta:

> *8. Indique las razones por las cuales se limita el uso de la aplicación Cédula Digital a versiones tan recientes de teléfonos inteligentes (Android 9 o superior, iOS 12 o superior, con una resolución mínima de 1280 x 720 Megapíxeles HD o superior).*
> ***Rta**.: Las versiones Android 9 y IOS 12 actualmente no son soportadas por los fabricantes, se adjunta información de las versiones soportadas actualmente por los fabricantes, las cuales son las versiones recomendadas para el óptimo funcionamiento de la Aplicación de Cédula Digital.*

Android 12	Snow Cone	12	31	October 4, 2021
Android 12L	Snow Cone v2	12.1[a]	32	March 7, 2022
Android 13	Tiramisu	13	33	August 15, 2022
Android 14	Upside Down Cake[26]	14	34	October 4, 2023
Android 15	Vanilla Ice Cream[27]	**15**	35	October 15, 2024

Versión aun en mantenimiento Ultima Versión

iOS 17	September 18, 2023	17.7.2	November 19, 2024
iOS 18	September 16, 2024	18.2	December 11, 2024

Versión aun en mantenimiento Ultima Versión

ANEXO 4: ANÁLISIS ESTÁTICO (PERMISOS Y RASTREADORES)

El análisis de la versión Android 4.0.0 (publicada en noviembre 2024) con *Exodus Privacy* muestra que **la aplicación tiene en este momento 43 permisos** que se listan aquí:

! ACCESS_COARSE_LOCATION *access approximate location only in the foreground*	INTERNET *have full network access*	RECEIVE
! ACCESS_FINE_LOCATION *access precise location only in the foreground*	NFC *control Near Field Communication*	BIND_GET_INSTALL_REFERRER_SERVICE
ACCESS_NETWORK_STATE *view network connections*	POST_NOTIFICATIONS	READ_SETTINGS
ACCESS_WIFI_STATE *view Wi-Fi connections*	READ_APP_BADGE	UPDATE_SHORTCUT
BLUETOOTH *pair with Bluetooth devices*	! READ_EXTERNAL_STORAGE *read the contents of your shared storage*	CHANGE_BADGE
BLUETOOTH_ADMIN *access Bluetooth settings*	! READ_PHONE_STATE *read phone status and identity*	READ_SETTINGS
! BLUETOOTH_ADVERTISE *advertise to nearby Bluetooth devices*	RECEIVE_BOOT_COMPLETED *run at startup*	! WRITE_SETTINGS
! BLUETOOTH_CONNECT *connect to paired Bluetooth devices*	USE_BIOMETRIC *use biometric hardware*	UPDATE_BADGE
! BLUETOOTH_SCAN *discover and pair nearby Bluetooth devices*	USE_FINGERPRINT *use fingerprint hardware*	READ_SETTINGS
! CAMERA *take pictures and videos*	WAKE_LOCK *prevent phone from sleeping*	! WRITE_SETTINGS
CHANGE_NETWORK_STATE *change network connectivity*	! WRITE_EXTERNAL_STORAGE *modify or delete the contents of your shared storage*	READ
CLIPBOARD_WRITE	DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	WRITE
FLASHLIGHT	UPDATE_COUNT	BROADCAST_BADGE
FOREGROUND_SERVICE *run foreground service*	RECEIVE	PROVIDER_INSERT_BADGE
		BADGE_COUNT_READ
		BADGE_COUNT_WRITE

El reporte se puede encontrar aquí:

https://reports.exodus-privacy.eu.org/es/reports/532946/

En cuanto a los rastreadores, *Exodus Privacy* encuentra los tres siguientes:

Los dos primeros rastreadores tienen que ver con la Analítica de datos de Google (***Firebase Analytics***) y una solución de analítica de datos y Marketing de la empresa *Upland Software* llamada ***Localytics***. El análisis de tráfico (ver Anexos siguientes) muestran que se genera tráfico hacia los servidores de estas dos empresas y que se genera efectivamente rastreo de la persona usuaria mediante el envío de varios identificadores.

Según el sitio web de ***Open Telemetry***, es "*a collection of APIs, SDKs, and tools. Use it to instrument, generate, collect, and export telemetry data (metrics, logs, and traces) to help you analyze your software's performance and behavior*."[1] Aunque el SDK es considerado cómo un rastreador que puede generar envío de datos a terceros, puede que hasta ahora no se haya usado de esta forma y en todo caso, no lo hemos detectado en nuestros análisis.

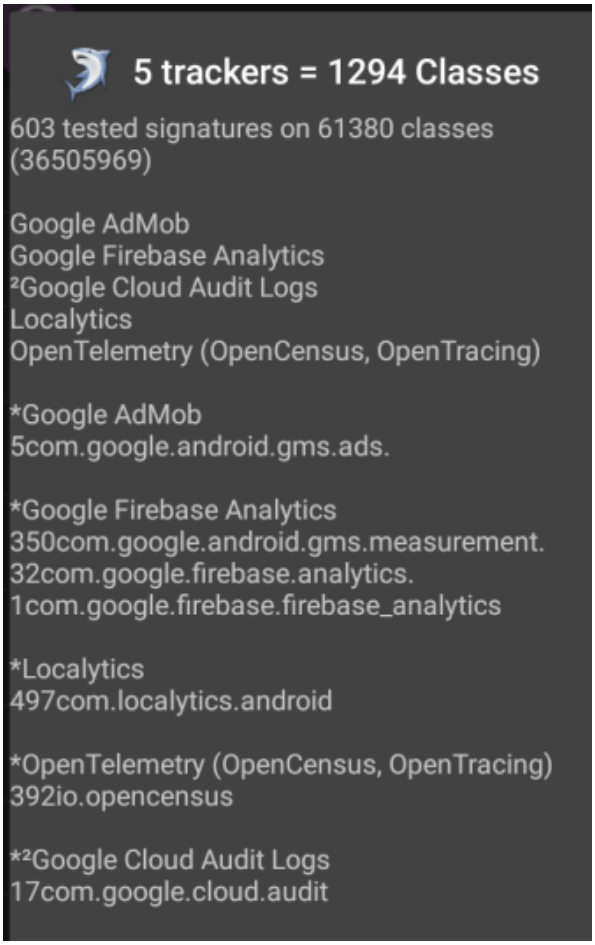
Además de estos tres rastreadores, el análisis de la misma versión de la Cédula Digital con otra herramienta libre (*ClassyShark3xodus*[2]) - realizada el 2 de diciembre del 2024 - mostró dos rastreadores adicionales. Aunque estos rastreadores no parecen activarse ni generar envíos de datos en las pruebas realizadas, de funcionar **se activarían 5 rastreadores presentes en la aplicación**.

Además ambos generan preguntas de privacidad:

- ***Google Ad Mob***: Es el servicio de publicidad para móviles de Google.
- ***Google Cloud Audit Logs***: Es el servicio de auditoría de logs de Google Cloud. Surge entonces la pregunta de si la aplicación usa directamente Google Cloud o si es sólo para la funcionalidad de analítica de datos Google Firebase (ya que ambas se pueden interconectar).

1 https://opentelemetry.io/

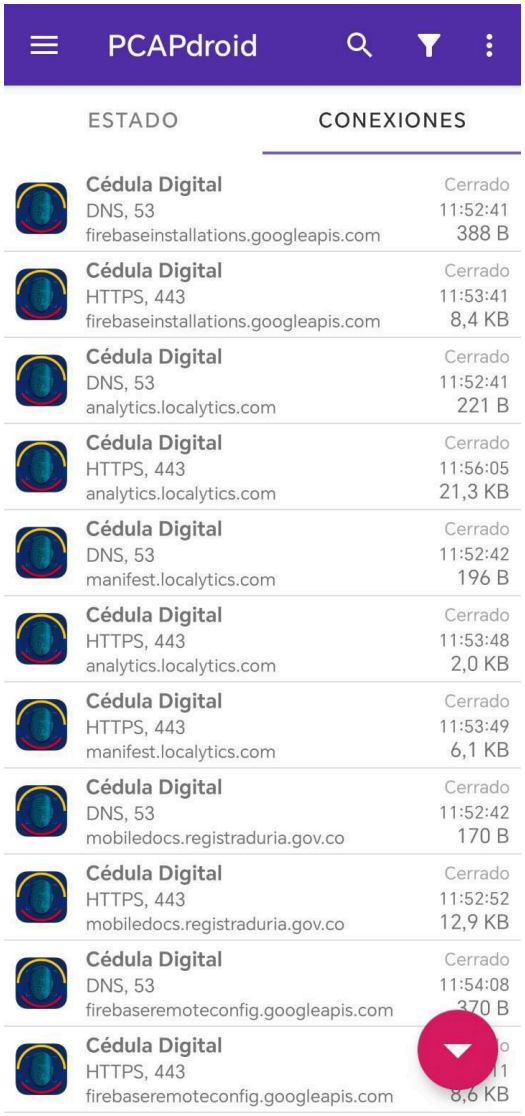
2 https://fossdd.gitlab.io/fdroid-website/en/packages/com.oF2pks.classyshark3xodus/


5 trackers = 1294 Classes
603 tested signatures on 61380 classes (36505969)
Google AdMob
Google Firebase Analytics
²Google Cloud Audit Logs
Localytics
OpenTelemetry (OpenCensus, OpenTracing)
*Google AdMob
5com.google.android.gms.ads.
*Google Firebase Analytics
350com.google.android.gms.measurement.
32com.google.firebase.analytics.
1com.google.firebase.firebase_analytics
*Localytics
497com.localytics.android
*OpenTelemetry (OpenCensus, OpenTracing)
392io.opencensus
*²Google Cloud Audit Logs
17com.google.cloud.audit


file:///data/app/~~-xdQ3pSt5gypCCw6iH7sGA%3D%3D/co.gov.registraduria.ceduladigital-1InoGKpbx7jQh06RSY4-bg%3D%3D/base.apk
MD5sum: a43c9a4de4ed2822c74131cf74c5dfa3
SHA1sum: 21869a53bcf472968191ff9ab1b3f002a9a8336a
SHA256sum: 9841ebeb9710a566ba681d051681afeda7e4405cadefd5db89709502d93f8112
CN=Android,OU=Android,O=Google Inc.,L=Mountain View,ST=California,C=US
SHA256withRSA
CERTIFICATE fingerprints:
md5: b2a1dd834b6d43fbc9b1511b6183ee4b
sha1: ec8ed5855ca7ff7472b9600ca5831d82b8e77fe9
sha256: c75e39773a50a6a41ba5177a3a9fb915bf949aa624b5460fb90dc9cb93b6cd2b

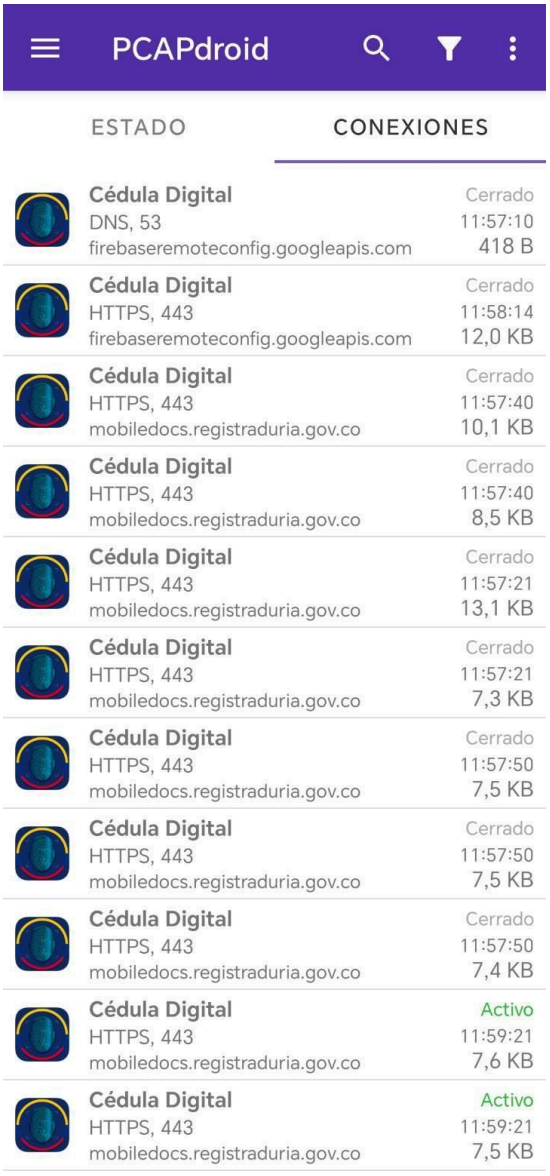
ANEXO 5: DOMINIOS CONTACTADOS POR LA APLICACIÓN

En un proceso completo de inicio, activación y navegación en la “Cédula digital” (el 27 de enero 2025 con la versión 4.0.0 de Android), hicimos una captura del tráfico generado por la aplicación, sin descifrarlo, por medio de la aplicación de código abierto PCAPdroid[3]. Aquí aparecen cronológicamente, los dominios contactados y los protocolos (DNS y HTTPS) junto con el volumen de datos transferidos:



[3] https://play.google.com/store/apps/details?id=com.emanuelef.remote_capture&hl=es


PCAPdroid
ESTADO
CONEXIONES
Cédula Digital
HTTPS, 443
mobiledocs.registraduria.gov.co
Cerrado
11:56:21
10,7 KB
Cédula Digital
HTTPS, 443
mobiledocs.registraduria.gov.co
Cerrado
11:56:21
7,4 KB
Cédula Digital
HTTPS, 443
mobiledocs.registraduria.gov.co
Cerrado
11:56:23
7,6 KB
Cédula Digital
HTTPS, 443
mobiledocs.registraduria.gov.co
Cerrado
11:57:20
6,7 KB
Cédula Digital
DNS, 53
firebaseremoteconfig.googleapis.com
Cerrado
11:57:10
418 B
Cédula Digital
HTTPS, 443
firebaseremoteconfig.googleapis.com
Cerrado
11:58:14
12,0 KB
Cédula Digital
HTTPS, 443
mobiledocs.registraduria.gov.co
Cerrado
11:57:40
10,1 KB
Cédula Digital
HTTPS, 443
mobiledocs.registraduria.gov.co
Cerrado
11:57:40
8,5 KB
Cédula Digital
HTTPS, 443
mobiledocs.registraduria.gov.co
Cerrado
11:57:21
13,1 KB
Cédula Digital
HTTPS, 443
mobiledocs.registraduria.gov.co
Cerrado
11:57:21
Cédula Digital
HTTPS, 443
mobiledocs.registraduria.gov.co
7,5 KB


PCAPdroid
ESTADO
CONEXIONES
Cédula Digital
DNS, 53
firebaseremoteconfig.googleapis.com
Cerrado
11:57:10
418 B
Cédula Digital
HTTPS, 443
firebaseremoteconfig.googleapis.com
Cerrado
11:58:14
12,0 KB
Cédula Digital
HTTPS, 443
mobiledocs.registraduria.gov.co
Cerrado
11:57:40
10,1 KB
Cédula Digital
HTTPS, 443
mobiledocs.registraduria.gov.co
Cerrado
11:57:40
8,5 KB
Cédula Digital
HTTPS, 443
mobiledocs.registraduria.gov.co
Cerrado
11:57:21
13,1 KB
Cédula Digital
HTTPS, 443
mobiledocs.registraduria.gov.co
Cerrado
11:57:21
7,3 KB
Cédula Digital
HTTPS, 443
mobiledocs.registraduria.gov.co
Cerrado
11:57:50
7,5 KB
Cédula Digital
HTTPS, 443
mobiledocs.registraduria.gov.co
Cerrado
11:57:50
7,5 KB
Cédula Digital
HTTPS, 443
mobiledocs.registraduria.gov.co
Cerrado
11:57:50
7,4 KB
Cédula Digital
HTTPS, 443
mobiledocs.registraduria.gov.co
Activo
11:59:21
7,6 KB
Cédula Digital
HTTPS, 443
mobiledocs.registraduria.gov.co
Activo
11:59:21
7,5 KB

Se pueden observar conexiones HTTPS y resoluciones de dominio (DNS) hacia:

- "**mobiledocs.registraduria.gov.co**", el dominio de la RNEC usado para la aplicación,
- "**idemia.com**" (subdominio "api.eu.labs") dominio de la empresa IDEMIA,
- "**xantav.com**" (subdominio "prd.lkms"), dominio que pertenece a IDEMIA,
- "**localytics.com**" (subdominios "manifest" y "analytics"), servicio de analítica de datos y marketing de la empresa Upland Software Inc,
- "**googleapis.com**" (subdominios "firebaseremoteconfig" y también "content-autofill" que aparece en otra captura), Firebase es la plataforma de hosting y desarrollo de aplicaciones de Google que incluye muchas funcionalidades: análisis de errores, analítica de datos e incluso envío de notificaciones y publicidad.

ANEXO 6: DOMINIOS, IP Y SERVIDORES

Aquí identificamos algunos dominios, direcciones IP y ubicación de los servidores correspondientes, usando los comandos Linux *host* y *whois.* Estos comandos consultan respectivamente registros DNS (servidores de dominio) y bases públicas de asignación de dominios y direcciones IP (de LACNIC y del ICANN).

Dominio principal "mobiledocs.registraduria.gov.co"

```
host mobiledocs.registraduria.gov.co
mobiledocs.registraduria.gov.co has address 190.248.51.122
[Esta IP también se puede observar directamente en el tráfico de red capturado]

whois 190.248.51.122
% IP Client: 89.187.173.173

% Joint Whois - whois.lacnic.net
%  This server accepts single ASN, IPv4 or IPv6 queries

% LACNIC resource: whois.lacnic.net


% Copyright LACNIC lacnic.net
%  The data below is provided for information purposes
%  and to assist persons in obtaining information about or
%  related to AS and IP numbers registrations
%  By submitting a whois query, you agree to use this data
%  only for lawful purposes.
%  2025-01-26 12:04:46 (-03 -03:00)

inetnum:     190.248.51.96/27
status:      reallocated
aut-num:     N/A
owner:       REGISTRADURIA NACIONAL DEL ESTADO CIVIL
ownerid:     CO-RNEC-LACNIC
responsible: Luis Soto
address:     Avenida 2BN No. 26N - 54, ,
address:      - CALI - VA
country:     CO
phone:       +57 2 6079966
owner-c:     DBT
tech-c:      DBT
```

```
abuse-c:     DBT
created:     20231116
changed:     20231116
inetnum-up:  190.248.0.0/15

nic-hdl:     DBT
person:      EMCALI E.I.C.E. E.S.P.
e-mail:      lacnic.emcali@emcali.net.co
address:      Carrera 25 No. 5 - 70, Telefonica San Fernando (Emcali), 70,
Telefonica San Fernando (Emcali)
address:     076001 - Cali - Other (Non U.S.)
country:     CO
phone:       +57  28998317 [0000]
created:     20040305
changed:     20220309

% whois.lacnic.net accepts only direct match queries.
% Types of queries are: POCs, ownerid, CIDR blocks, IP
% and AS numbers.
```

Dominios de IDEMIA

El dominio "xantav.com"

No era evidente *a priori* que el dominio "xantav.com" con el cual se comunica la aplicación (se conecta hasta el subdominio "**prd.lkms.xantav.com**") fuese de IDEMIA pero los datos de este dominio están públicos y el resultado de *whois* muestra que pertenece a ***IDEMIA Identity & Security France***:

```
whois xantav.com
   Domain Name: XANTAV.COM
   Registry Domain ID: 2227131726_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.corporatedomains.com
   Registrar URL: http://cscdbs.com
   Updated Date: 2024-02-12T14:46:18Z
   Creation Date: 2018-02-14T16:34:49Z
   Registry Expiry Date: 2025-02-14T16:34:49Z
   Registrar: CSC Corporate Domains, Inc.
   Registrar IANA ID: 299
   Registrar Abuse Contact Email: domainabuse@cscglobal.com
   Registrar Abuse Contact Phone: 8887802723
                    Domain      Status:      clientTransferProhibited
https://icann.org/epp#clientTransferProhibited
   Name Server: NS-1499.AWSDNS-59.ORG
   Name Server: NS-16.AWSDNS-02.COM
   Name Server: NS-1814.AWSDNS-34.CO.UK
```

Name Server: NS-852.AWSDNS-42.NET
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-01-26T20:27:20Z
[…]

Registrant Organization: IDEMIA Identity & Security France
Registrant Street: 11 boulevard Gallieni
Registrant City: Issy-les-Moulineaux
Registrant State/Province:
Registrant Postal Code: 92130
Registrant Country: FR
Registrant Phone: +33.158112500
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: hostmaster@morpho.com
Registry Admin ID:
Admin Name: Digital Communications
Admin Organization: IDEMIA Identity & Security France
Admin Street: 11 boulevard Gallieni
Admin City: Issy-les-Moulineaux
Admin State/Province:
Admin Postal Code: 92130
Admin Country: FR
Admin Phone: +33.158112500
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: **hostmaster@morpho.com**
Registry Tech ID:
Tech Name: Digital Communications
Tech Organization: Safran Identity & Security
Tech Street: 11 boulevard Gallieni
Tech City: Issy-les-Moulineaux
Tech State/Province:
Tech Postal Code: 92130
Tech Country: FR
Tech Phone: +33.158112500
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: **hostmaster@morpho.com**
Name Server: ns-16.awsdns-02.com

```
Name Server: ns-1814.awsdns-34.co.uk
Name Server: ns-852.awsdns-42.net
Name Server: ns-1499.awsdns-59.org
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System:
http://wdprs.internic.net/
>>> Last update of WHOIS database: 2024-02-12T09:46:18Z
```

Hay dos otras cosas interesantes en el resultado de este *whois*:

1. El contacto administrativo y técnico están en la misma dirección en Francia, la del grupo internacional de defensa SAFRAN (IDEMIA proviene de la fusión de Safran Identity & Security y Oberthur Card System).
2. Los servidores de dominios se ubican en **Amazon Web Services**, lo que se confirma con el hosting de las IP correspondientes en Amazon.

En la captura de tráfico se puede observar que el tráfico hacia el dominio “prd.lkms.xantav.com” se resolvió y se hizo hacia **la dirección IP 143.204.23.30.** Como se ve aquí, **pertenece a Amazon Technologies Inc. (Seattle).**

```
whois 143.204.23.30

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#

# start

NetRange:       143.204.0.0 - 143.204.255.255
CIDR:           143.204.0.0/16
NetName:        AT-88-Z
NetHandle:      NET-143-204-0-0-1
Parent:         NET143 (NET-143-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   Amazon Technologies Inc. (AT-88-Z)
RegDate:        2018-01-05
Updated:        2018-01-05
Ref:            https://rdap.arin.net/registry/ip/143.204.0.0
```

```
OrgName:        Amazon Technologies Inc.
OrgId:          AT-88-Z
Address:        410 Terry Ave N.
City:           Seattle
StateProv:      WA
PostalCode:     98109
Country:        US
RegDate:        2011-12-08
Updated:        2024-01-24
Comment:        All abuse reports MUST include:
Comment:        * src IP
Comment:        * dest IP (your IP)
Comment:        * dest port
Comment:        * Accurate date/timestamp and timezone of activity
Comment:        * Intensity/frequency (short log extracts)
Comment:         * Your contact details (phone and email) Without these
we will be unable to identify the correct owner of the IP address at
that point in time.
Ref:            https://rdap.arin.net/registry/entity/AT-88-Z
```

El dominio "api.eu.labs.idemia.com"

"api.eu.labs.idemia.com" es un subdominio del dominio principal de IDEMIA y por lo tanto pertenece a IDEMIA.

```
host api.eu.labs.idemia.com
api.eu.labs.idemia.com is an alias for
d-n2cmsvngtg.execute-api.eu-north-1.amazonaws.com.
d-n2cmsvngtg.execute-api.eu-north-1.amazonaws.com has address
13.49.174.153
d-n2cmsvngtg.execute-api.eu-north-1.amazonaws.com has address
13.50.214.183
d-n2cmsvngtg.execute-api.eu-north-1.amazonaws.com has address
13.48.80.20
```

El resultado del comando *host* muestra que el dominio es un alias (CNAME) para subdominios de Amazon Web Services (AWS). **Las direcciones IP correspondientes pertenecen a Amazon y están ubicadas en Europa (Suecia y Alemania).**

ANEXO 7: CONEXIONES HACIA EL DOMINIO DE LA RNEC

En el Anexo 4 se muestran las conexiones en un proceso completo de inicio, envío del código QR de validación, activación mediante el reconocimiento facial y navegación en la aplicación.

Aquí se muestran paquetes HTTPS que se mandan al dominio de la RNEC (“mobiledocs.registraduria.gov.co”) y que se pudieron descifrar gracias a la herramienta Pirogue. Corresponden a las dos primeras partes del proceso (inicio y envío del código QR de validación). El proceso de reconocimiento facial generó un error en nuestro teléfono con Pirogue (posiblemente por la versión de Android) y no fue posible descifrar los datos del final del proceso. Aquí van extractos de los logs de Pirogue que muestran que se agarra con procesos que corresponden a la Cédula Digital ("co.gov.registraduria.ceduladigital") :

```
16:03:17 INFO     Connecting to the USB device...
         INFO     Connected...
16:03:18 INFO     Saving device properties

16:03:20 INFO     Starting Frida server...
         INFO     Starting network interception...
16:03:21 INFO     Starting screen recording...
16:03:47 INFO     Enabled spawn gating
         INFO     Waiting for data
16:13:47    INFO                    New    process    caught    Spawn(pid=487,
identifier="co.gov.registraduria.ceduladigital")
                            INFO              Instrumenting   Spawn(pid=487,
identifier="co.gov.registraduria.ceduladigital")
         INFO     i Running Script on Android
         INFO     i libssl.so found & will be hooked on Android!
[*] Android dynamic loader hooked.
         INFO     Waiting for data
16:13:51    INFO                    New    process    caught    Spawn(pid=745,
identifier="co.gov.registraduria.ceduladigital")
                            INFO              Instrumenting   Spawn(pid=745,
identifier="co.gov.registraduria.ceduladigital")
         INFO     i Running Script on Android
         INFO     i libssl.so found & will be hooked on Android!
[*] Android dynamic loader hooked.
```

Acá se muestran unos extractos de los datos capturados y comentados, visualizados con Wireshark. Son datos mandados y recibidos al domino “mobiledocs.registraduria.gov.co”:

[Se quitó esta parte para no generar riesgos de seguridad]

Los paquetes aparecen con el protocolo HTTP porque han sido descifrados pero eran originalmente HTTPS (HTTP + TLS).

En la primera etapa, la aplicación solicita un archivo de configuración que se muestra en el Anexo 2 y que permite adaptar la aplicación de IDEMIA al contexto de la Cédula digital colombiana, hacerle su "branding" local.

El archivo de configuración completo se puede encontrar en esta URL:

[Se quitó esta parte para no generar riesgos de seguridad]

(**que se puede acceder sin autenticación**).

Después, la aplicación hace varios intercambios de datos vía solicitudes con una URL conteniendo un código hexadecimal que se encontraba en el código QR de activación recibido:

https://mobiledocs.registraduria.gov.co/**[....]**/fa9507bc-83fe-405a-8c82-ea76f0858039/status

El servidor responde con datos técnicos contenidos en un archivo JSON y vinculados con el proceso. Por ejemplo en este, se puede ver que el código QR fue aceptado y que esto genera una primera autenticación ("generic OTP: accepted"), pero que después el reconocimiento facial fue rechazado :

```
JavaScript Object Notation: application/json
    Object
        Member: id
            [Path with value: /id:fa9507bc-83fe-405a-8c82-ea76f0858039]
            [Member with value: id:fa9507bc-83fe-405a-8c82-ea76f0858039]
            String value: fa9507bc-83fe-405a-8c82-ea76f0858039
            Key: id
            [Path: /id]
        Member: status
            Object
                Member: global
                    [Path with value: /status/global:EXPECTING_INPUT]
                    [Member with value: global:EXPECTING_INPUT]
                    String value: EXPECTING_INPUT
                    Key: global
                    [Path: /status/global]
                Member: expectedData
                    Array
                                                        [Path with value:
/status/expectedData/[]:FACE_MATCHING]
                        [Member with value: []:FACE_MATCHING]
```

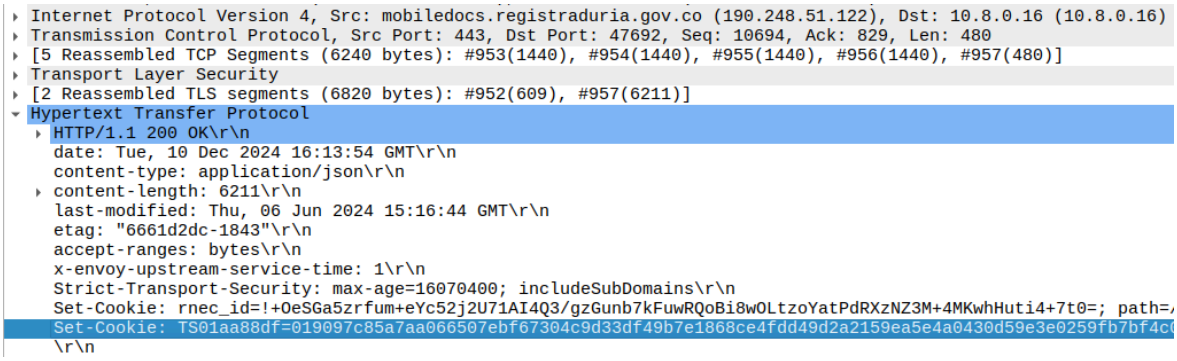
```
                        String value: FACE_MATCHING
                    Key: expectedData
                    [Path: /status/expectedData]
                Member: states
                    Object
                        Member: IDENTITY_ATTRIBUTES
                                                                [Path  with  value:
/status/states/IDENTITY_ATTRIBUTES:ACCEPTED]
                            [Member with value: IDENTITY_ATTRIBUTES:ACCEPTED]
                            String value: ACCEPTED
                            Key: IDENTITY_ATTRIBUTES
                            [Path: /status/states/IDENTITY_ATTRIBUTES]
                          Member: GENERIC_OTP
                                                                [Path  with  value:
/status/states/GENERIC_OTP:ACCEPTED]
                            [Member with value: GENERIC_OTP:ACCEPTED]
                            String value: ACCEPTED
                            Key: GENERIC_OTP
                            [Path: /status/states/GENERIC_OTP]
                        Member: FACE_MATCHING
                                                                [Path  with  value:
/status/states/FACE_MATCHING:REJECTED]
                            [Member with value: FACE_MATCHING:REJECTED]
                              String value: REJECTED
                            Key: FACE_MATCHING
                              [Path: /status/states/FACE_MATCHING]
                    Key: states
                    [Path: /status/states]
                Member: errors
                    Object
                        Member: FACE_MATCHING
                            Array
                                Object
                                      Member: code
                                                                 [Path with value:
/status/errors/FACE_MATCHING/[]/code:1600]
                                          [Member with value: code:1600]
                                          String value: 1600
                                          Key: code
                                                                              [Path:
/status/errors/FACE_MATCHING/[]/code]
                            Key: FACE_MATCHING
                            [Path: /status/errors/FACE_MATCHING]
                    Key: errors
                    [Path: /status/errors]
```

```
    Key: status
    [Path: /status]
Member: businessProcessName
    [Path with value: /businessProcessName:COLOMBIA_RNEC]
    [Member with value: businessProcessName:COLOMBIA_RNEC]
    String value: COLOMBIA_RNEC
    Key: businessProcessName
    [Path: /businessProcessName]
Member: qrCode
    [Path with value [truncated]: /qrCode:/9j/4AAQSkZ        [...]
```

ANEXO 8: TECNOLOGÍAS DETRÁS DE "MOBILEDOCS.REGISTRADURIA.GOV.CO"

La cookie de load balancing

Analizando los paquetes que se muestran en el Anexo 5, la primera cosa que nos llamó la atención fue la instalación de dos cookies HTTP vía dos "Set-Cookie" por el servidor correspondiente:



Estas dos cookies son ambas cookies técnicas:

- "**rnec_id**" que contiene un número de identificación codificado en base64, y que posiblemente sirva para identificar la persona usuaria en la aplicación,
- "**TS01aa88df**" que es una cookie de sesión que contiene caracteres hexadecimales. Este tipo de cookie es usada por los repartidores de cargas ("load balancer") de tipo BigIP de la empresa F5[4].

El uso de esta última cookie muestra por lo tanto la presencia de un repartidor de carga ("load balancer") de tipo BigIP de la empresa F5 en la infraestructura de la Cédula Digital.

Identificación con WappAlyzer y uso de un Reverse Proxy Envoy

Usando la herramienta WappAlyzer[5], se pudieron identificar las tecnologías siguientes en el dominio "mobiledocs.registraduria.gov.co" (a la fecha del 25 de enero del 2025):

[Se quitó esta parte para no generar riesgos de seguridad]

[4] Ver detalles en estos artículos en el sitio web de la empresa F5: https://my.f5.com/manage/s/article/K6850 y https://my.f5.com/manage/s/article/K54501322

[5] https://www.wappalyzer.com/

ANEXO 9: SERVICIOS ABIERTOS EN "MOBILEDOCS.REGISTRADURIA.GOV.CO"

Usando la herramienta NMAP, analizamos los puertos/servicios abiertos en el dominio en dos fechas distintas. Es interesante ver que se añadió un nuevo puerto (no estándar) el "1000". Podría vincularse con el uso de firewall *Fortigate* de la empresa Fortinet[6].

```
host mobiledocs.registraduria.gov.co
mobiledocs.registraduria.gov.co has address 190.248.51.122
```

```
nmap 190.248.51.122
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-07 16:28 -05
Nmap scan report for 190.248.51.122
Host is up (0.16s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE  SERVICE
53/tcp  open   domain
113/tcp closed ident
179/tcp open   bgp
443/tcp open   https
```

```
nmap 190.248.51.122
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-26 11:27 -05
Nmap scan report for 190.248.51.122
Host is up (0.17s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE  SERVICE
53/tcp   open   domain
113/tcp  closed ident
179/tcp  open   bgp
443/tcp  open   https
1000/tcp open   cadlock
```

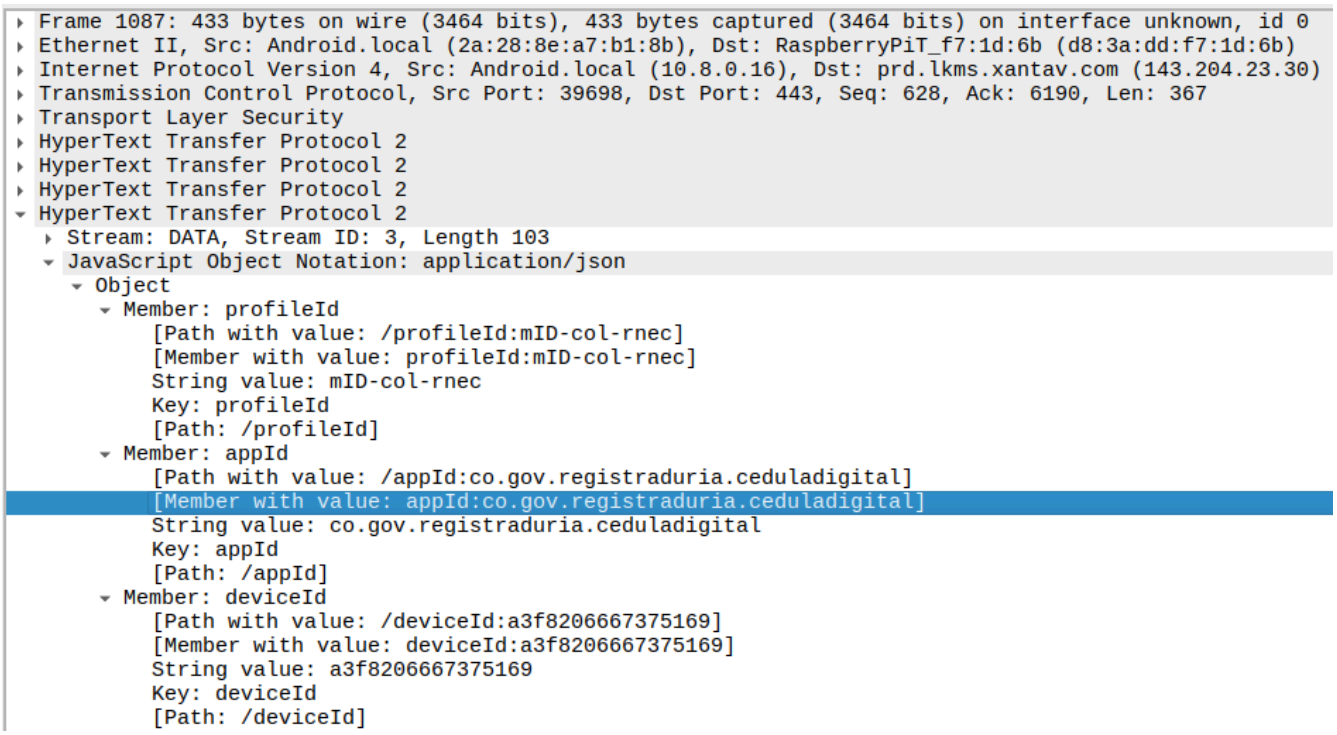
En cuanto al puerto 179 (BGP), interroga sobre su uso en este contexto ya que se suele usar normalmente para el intercambio de información de encaminamiento entre sistemas autónomos. Es posible que haya sido dejado abierto por negligencia/olvido o error. En este caso tocaría cerrarlo, en el caso contrario sería interesante saber a qué sirve y cómo se usa en la infraestructura de la Cédula Digital.

[6] https://community.fortinet.com/t5/FortiGate/Technical-Tip-Why-is-TCP-port-1000-open/ta-p/197269

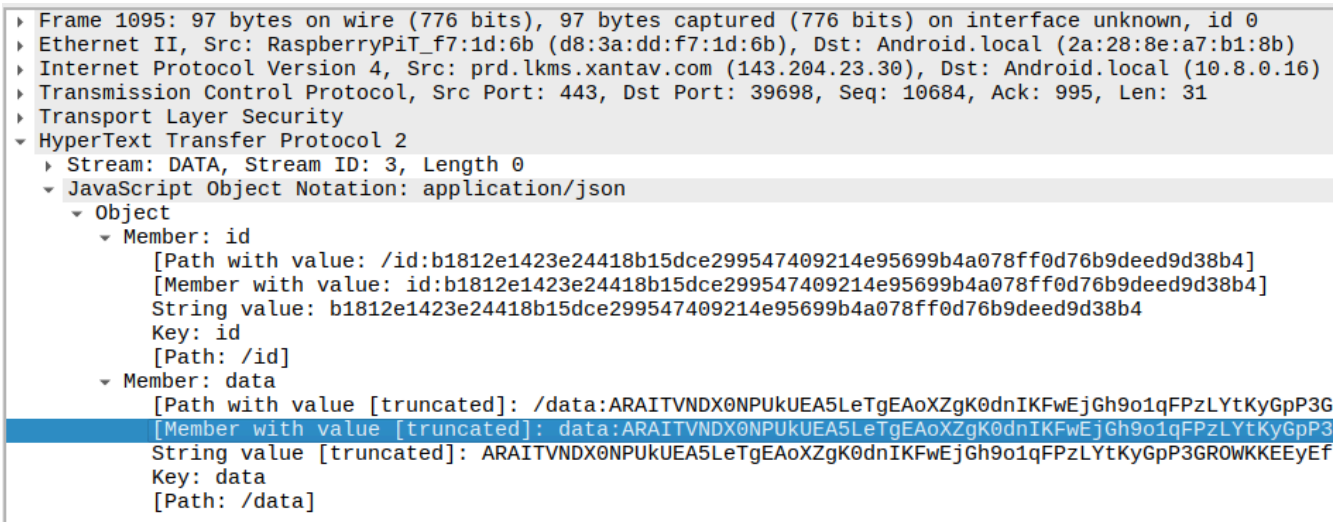
ANEXO IO: COMUNICACIONES CON DOMINIOS DE IDEMIA

En los Anexos 4 y 5 se identificaron dos dominios de IDEMIA. Se trata de los dominios "**api.eu.labs.idemia.com**" y "**prd.lkms.xantav.com**" que aparecieron en los análisis de tráfico. Usando Pirogue, se pudo descifrar el tráfico (datos mandados y recibidos) hacia el dominio "prd.lkms.xantav.com" pero no hacia el dominio "api.eu.labs.idemia.com" por motivos ya explicados. En un primer envío, se mandan datos en un formato no entendible pero en el segundo se mandan datos:

- que identifican el perfil del cliente de IDEMIA (profileID: mID-col-rnec),
- que identifican la app (appID: co.gov.registraduria.ceduladigital),
- que identifican el teléfono de la persona usuaria (en este caso deviceID: a3f8206667375169).



En respuesta el servidor manda datos codificados en base64:



Una decodificación del contenido del paquete permite entender que estos datos tienen que ver con autorizar la aplicación a usar el *Mobile ID* de IDEMIA mediante la entrega de varias licencias específicas a cada componente y de certificados criptográficos al nombre de IDEMIA:

- la primera parte tiene que ver con licencias, en este caso con nombres: MSC_CORE, MORPHOFACS, MSC_LIVENESS, MSC_DUMP y MSC_REPLAY[7].
- la segunda parte tiene que ver con **certificados criptográficos X509 al nombre de IDEMIA IDENTITY & SECURITY FRANCE** (LKMS Root CA y LKMS license cert for profile mID-col-rnec).

Un detalle interesante es que en los datos, aparecen también nombres (de paquete) alternos para la aplicación, dos de ellos siendo probablemente para versiones de desarrollo (“dev”) y después el nombre común que se usa hoy:

- com.idemia.mobileid.colombia.rnec
- com.idemia.mobileid.colombia.rnec.dev
- com.idemia.mobileid.colombia.rnec.dev.pl
- co.gov.registraduria.ceduladigital

Estos nombres alternos contienen “mobileid” que es el nombre de la aplicación genérica de IDEMIA, ya mencionada.

[7] Estas licencias se pueden ver en la documentación técnica de IDEMIA, en esta página: https://experience.idemia.com/identity-proofing/develop/capture-sdk/ios/4_x/document-integration-guide/

ANEXO II: LICENCIAS Y MOBILE ID EN LOS LOGS

El hecho de que la aplicación vaya a **buscar licencias en el dominio de IDEMIA** "xantav.com" (Ver Anexo 10) se encuentra también en los logs Android generados por la aplicación. Aquí va un extracto relacionado:

> **co.gov.registraduria.ceduladigital-86-yX9_j-O0Rv1FUXNhbJg**==/split_config.arm64_v8a.apk!/lib/arm64-v8a/libdeviceenvironment.so using ns clns-6 from class loader (caller=base.apk!classes4.dex): ok' b' [35m **CreateLicenseV3Module** [0m [30;104m D [0m **NETWORK_RELATED CREATE_LICENSE_V3 request: {"profileId":"mID-col-rnec","appId":"co.gov.registraduria.ceduladigital","deviceId":"0bb2fe3ef6a6b95a"}**' b' [30;104m D [0m **NETWORK_RELATED url**
>
> **[Se quitó esta parte para no generar riesgos de seguridad]**

En los mismos logs de Android aparecen constantemente componentes de IDEMIA que contienen "mobileID" o "MID". Acá van algunos ejemplos:

```
UnlockAppEventonSuccess:com.idemia.mid.unlock.UnlockSuccess@2e38ec3'
      Handling launch of ActivityRecord{d2b206e token=andr
oid.os.BinderProxy@8be6be9  {co.gov.registraduria.ced\n
uladigital/com.idemia.mobileid.pinmanagement.pinsuccess.PinFlowSuccessActivity}}'
```

Este log de iOS muestra que la aplicación, que tiene como identificador "co.gov.registraduria.ceduladigital", se ubica en la carpeta de aplicación ("Bundle") "mID_CO.app" y tiene como nombre "mID_CO":

> **tccd[45] <Notice>**: requestor: TCCDProcess: identifier=com.apple.lsd, pid=122, auid=501, euid=501, binary_path=/usr/libexec/lsd is checking access for accessor TCCDProcess: identifier=co.gov.registraduria.ceduladigital, pid=943, auid=501, euid=501, binary_path=/private/var/containers/Bundle/Application/3E44DBFD-B61B-410D-B2FE-61290282244D/mID_CO.app/mID_CO

Los logs de iOS que corresponden a eventos de la Cédula Digital aparecen con el prefijo “mID_CO” (probablemente abreviación de “Mobile ID Colombia”) como aquí:

```
mID_CO(UIKitCore)[943] <Notice>: sceneOfRecord: sceneID:
sceneID:co.gov.registraduria.ceduladigital-default  persistentID:
D47A5D49-E0AB-4670-B5CF-EF2A1229C455
mID_CO(UIKitCore)[943] <Error>: BUG IN CLIENT OF UIKIT: Setting
UIDevice.orientation is not supported. Please use
UIWindowScene.requestGeometryUpdate(_:)
mID_CO(CFNetwork)[943] <Notice>: Task
<73CFB8D6-8061-41C6-A0CE-6E604BFB6903>.<12> received response, status 404
content K
```

ANEXO I2:
TRÁFICO HACIA EMPRESAS DE ANALÍTICAS Y MARKETING

Envíos de datos al dominio "localytics.com"

La aplicación envía con regularidad, e incluso antes de conectarse al dominio principal, datos a un subdominio de la empresa de analítica de datos y marketing *Localytics* (que hoy pertenece a Upland Software). Aquí mostramos unos paquetes y datos capturados con Pirogue en procesos de arranque y envío del código QR de la aplicación (hechos en noviembre y diciembre 2024):

Estos datos siempre incluyen: características del teléfono, de la aplicación, la zona geográfica y varios identificadores (en formato hexadecimal) que permiten reconocer la persona usuaria, en particular el "customer_id"[8]. Así se presenta:

"{"dt":"h","u":"fd5f2e96-96cb-484d-a33a-b9a4d9eb87bc","pa":1733846613,"seq":17,"attrs":{"dt":"a","**au":"a1fb2128835f1e441bc8368-30d3618a-29cb-11eb-40d3-007c928ca240**","lv":"androida_6.3.4:6.3.4","av":"4.0.0","dp":"Android","dll":"en","dlc":"US","nc":"co","dc":"","dma":"**Google**","dmo":"**Pixel 3a**","dov":"12","nca":"","dac":"wifi","**iu":"7beb62f1-f47d-442b-8677-9cc2a6516aec**","push":"","ne":false,"we":true,"nas":2,"nbs":1,"nls":1,"nasy":1,"ncs":0,"nss":1,"**aid":"a3f8206667375169**","caid":"a3f8206667375169","pkg":"co.gov.registraduria.ceduladigital","lad":false,"dsdk":32,"lpg":0,"**tzid":"America\/Bogota**

[8] Se puede encontrar más detalles en la documentación técnica de Localytics al respecto: https://help.uplandsoftware.com/localytics/dev/android.html#collected-data-android

"},"ids":{**"customer_id":"95315a34-b376-3159-ae1f-fe7e7a2a864c"**}}\x0a{"dt":"e"
,"ctd":1733847244132,"u":"5bf5c6a1-3629-4f7b-a223-0fa33cba6c40",**"su":"c66c3f0
3-ca05-4748-9515-54a7f166bbdf"**,"n":"Application
started","cid":"95315a34-b376-3159-ae1f-fe7e7a2a864c","utp":"known","ids":{"c
ustomer_id":"95315a34-b376-3159-ae1f-fe7e7a2a864c"},"c0":"DE","c1":"cIl5mrl3S
Ei9xRpmN58_PH:APA91bFgLDyppUbGcLyiaIBnti5fFRZAhrcKv_-RnOOuHThJsbpALnZtj2ZQDTl
wBrg5kaxeSyShimeRnQqu8xOo0RMhswKwRmLoksfPit3NTgEN7wh1yOg","attrs":{}}\x0a{"dt
":"h","u":"0e1edf18-2561-4ca1-a781-21d58808e030","pa":1733846613,"seq":18,"at
trs":{"dt":"a","au":"a1fb2128835f1e441bc8368-30d3618a-29cb-11eb-40d3-007c928c
a240","lv":"androida_6.3.4:6.3.4","av":"4.0.0","dp":"Android","dll":"en","dlc
":"US","nc":"co","dc":"","dma":"Google","dmo":"Pixel
3a","dov":"12","nca":"","dac":"wifi","iu":"7beb62f1-f47d-442b-8677-9cc2a6516a
ec","push":"","ne":false,"we":true,"nas":2,"nbs":1,"nls":1,"nasy":1,"ncs":0,"
nss":1,"aid":"a3f8206667375169","caid":"a3f8206667375169",**"pkg":"co.gov.regis
traduria.ceduladigital"**,"lad":false,"dsdk":32,"lpg":0,"tzid":"America\/Bogota
"},"ids":{"customer_id":"95315a34-b376-3159-ae1f-fe7e7a2a864c"}}\x0a{"dt":"e"
,"ctd":1733847244568,"u":"b358b0d5-3c29-4171-b2e2-58ed38eddc4d","su":"c66c3f0
3-ca05-4748-9515-54a7f166bbdf","n":"Registration
Start","cid":"95315a34-b376-3159-ae1f-fe7e7a2a864c","utp":"known","ids":{"cus
tomer_id":"95315a34-b376-3159-ae1f-fe7e7a2a864c"},"c0":"DE","c1":"cIl5mrl3SEi
9xRpmN58_PH:APA91bFgLDyppUbGcLyiaIBnti5fFRZAhrcKv_-RnOOuHThJsbpALnZtj2ZQDTlwB
rg5kaxeSyShimeRnQqu8xOo0RMhswKwRmLoksfPit3NTgEN7wh1yOg","attrs":{"transaction
ID":"fa9507bc-83fe-405a-8c82-ea76f0858039"}}\x0a"

Además en ciertos envíos se mandan datos relacionados con el contenido de la aplicación y las etapas en las cuáles se encuentra la persona usuaria. Aquí van dos ejemplos que provienen también de datos capturados con Pirogue y que se mandan a Localytics:

> *"On Boarding Tutorial Screen","Tutorial Step Fragment Estás a salvo con tu Cédula Digital. Tu información personal, siempre en tu dispositivo móvil","OnBoarding Tutorial step: Es el futuro.","Tutorial Step Fragment Es el futuro. Tu identidad personal en línea, en cualquier lugar y momento.","OnBoarding Tutorial step: Eres tú y solo tú.","Tutorial Step Fragment Eres tú y solo tú. Olvídate de las contraseñas, preguntas y otros medios de identificación. Creamos confianza real y seguridad.","Permissions Screen","Register with QR Code Tutorial Screen","Tutorial Step Fragment A continuación, escanea el código QR que recibiste por correo. Escanea el código QR o presiona el botón Activar enviado a tu correo electrónico."*

> *"Registration Start"*
> *"El código QR ya fue utilizado o su tiempo de vida ya expiró"*

Cómo no hemos podido capturar y descifrar el tráfico con Pirogue en la parte en la cual la aplicación muestra los datos personales, no sabemos qué datos se mandan en esta parte. La documentación técnica de Localytics muestra que puede mandar muchos datos y depende de la forma en la cual se configura así que el riesgo de transferencia de datos personales hacia Localytics existe en caso de mala configuración.

Envíos de datos al dominio googleapis.com"

Por otra parte la aplicación manda y recibe datos del dominio "googleapis.com", en los subdominios "firebaseremoteconfig" y "content-autofill".

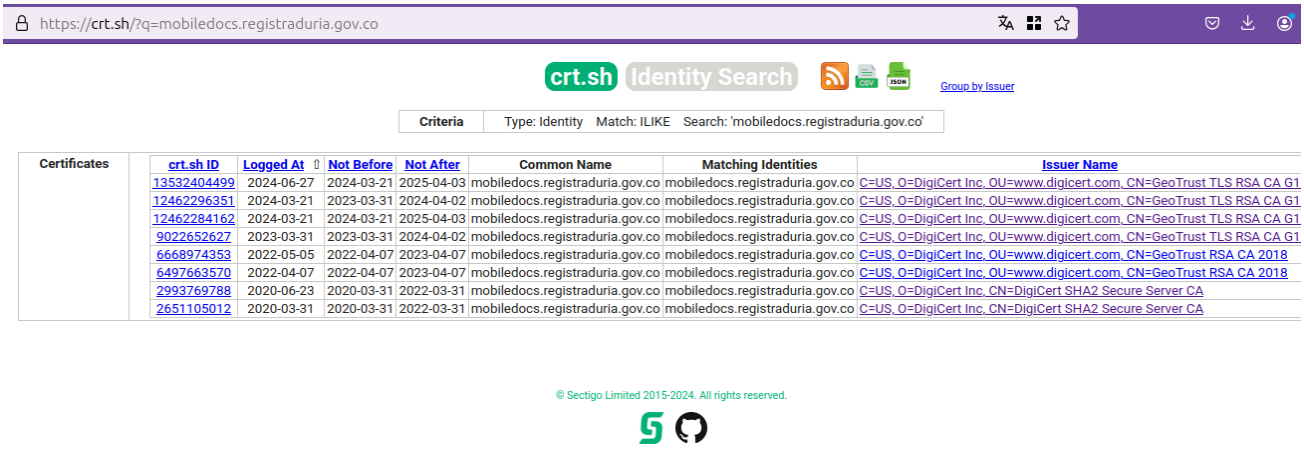
Firebase es la plataforma de hosting y desarrollo de aplicaciones de Google que incluye muchas funcionalidades: análisis de errores, analítica de datos e incluso envío de notificaciones y publicidades. El tráfico hasta este dominio no hace parte del tráfico que se pudo descifrar y por lo tanto no se pueden conocer cuáles datos se mandaron.

En cuanto al subdominio "content-autofill.googleapis.com", estas son las categorías de datos que se mandan:

ANEXO I3: SEGURIDAD DIGITAL EN DOMINIOS DE LA RNEC

Implementación del protocolo cifrado HTTPS/TLS[9]

El dominio "mobiledocs.registraduria.gov.co", subdominio de la RNEC que usa la aplicación *Cédula Digital*, tiene un historial de certificados criptográficas emitidos por la empresa Digicert/GeoTrust desde el 2020:



En una prueba automática realizada en enero 2025 en SSL Labs[10], la implementación obtiene una nota de B:

[Se quitó esta parte para no generar riesgos de seguridad]

Aunque la nota de implementación es globalmente buena, se recomienda corregir estos problemas (menores).

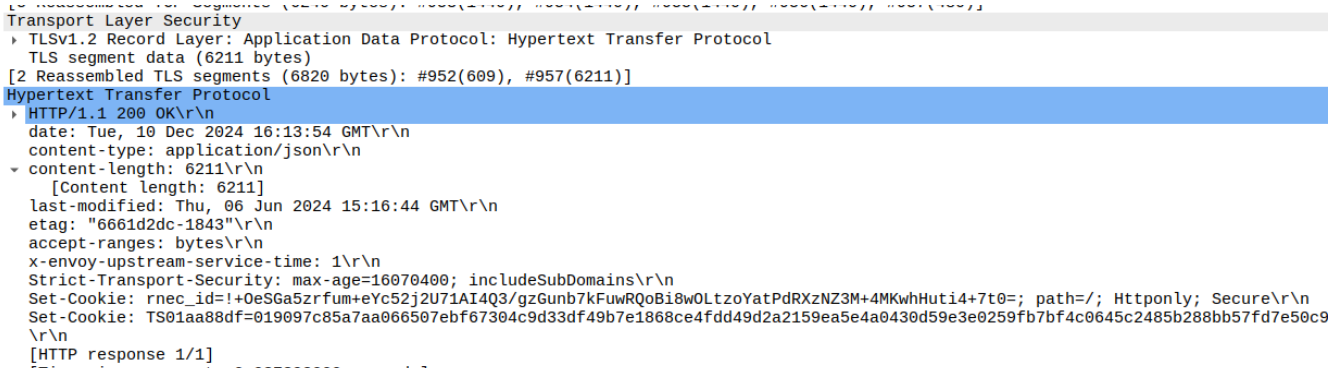
Un punto positivo - que también aparece en las respuestas del servidor - es el uso de HSTS (*HTTP Strict Transport Security*) que garantiza que todos los datos y recursos se mandan usando el protocolo cifrado HTTPS.

Respuestas del servidor de la aplicación y características de seguridad

[9] El protocolo HTTPS (*Hypertext Transfer Protocol Secure*) consiste en la encapsulación del protocolo HTTP en el protocolo cifrado SSL (*Secure Socket Layer*) o su sucesor TLS (Transport Layer Security,).

[10] https://www.ssllabs.com/ssltest/

Aquí se muestra una respuesta del servidor, con las capas de red TLS y HTTP:



[Se recortó la captura para no generar riesgos de seguridad]

Se pueden observar varias cosas:

- la implementación del protocolo TLS v 1.2,
- el uso de la tecnología de Reverse Proxy Envoy,
- la implementación de la política de seguridad HSTS, incluyendo los eventuales subdominios,
- la instalación de dos cookies técnicas asociadas al dominio (rnec_id y TS01aa88df) con los atributos de seguridad *Secure* y *HTTP Only* para la primera y *HTTPOnly* para la segunda[11]. Como se explica en el Anexo 8, la cookie "TS01aa88df" tiene que ver con el uso de un repartidor de carga (load balancer) de tipo F5 / BigIP.

Respuestas del servidor web (formularios)

Aquí se muestra la respuesta del servidor web del subdominio "ceduladigital" de la RNEC, donde se ubican los formularios mencionados en el informe:

https://ceduladigital.registraduria.gov.co/

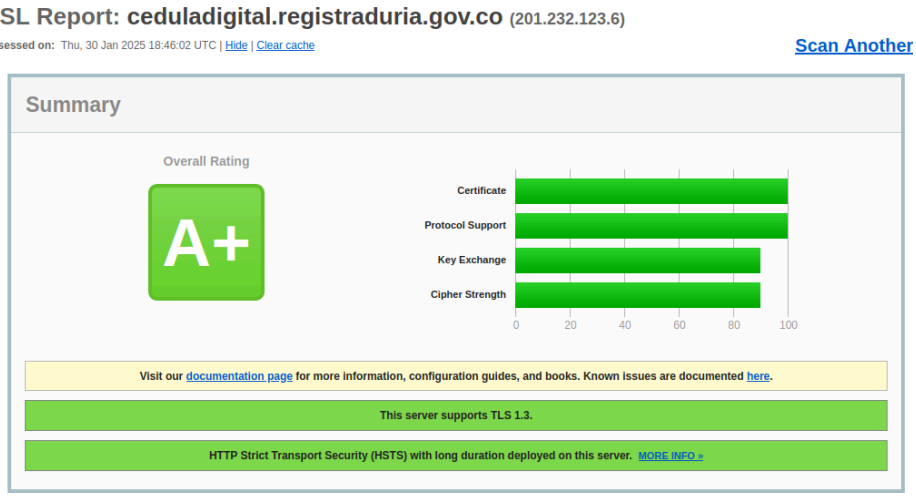
```
GET: HTTP/1.1 200 OK
Date: Mon, 23 Sep 2024 16:12:22 GMT
Server: XXXXXXX
X-Powered-By: XXXXXXXXXXX
Cache-Control: max-age=0, must-revalidate, no-cache, no-store, private
Pragma: no-cache
Expires: Sun, 02 Jan 1990 00:00:00 GMT
Set-Cookie: XSRF-TOKEN=[….] D; path=/; httponly;
```

[11] No se ve el atributo *Secure* de la cookie *TS01aa88df* por el recorte, pero está. *HTTPOnly* permite asegurar que las cookies sólo se puedan acceder vía el protocolo HTTP, y no desde una función javascript de un tercero por ejemplo. *Secure*, que sólo se transmite la cookie con el protocolo HTTPS. En este caso la implementación de *HSTS* y de *HttpOnly* no hace necesaria el Secure, aunque permite "defensa en profundidad".

```
samesite=laxf5_cspm=1234;;
X-Frame-Options: ALLOW-FROM https://www.nomasfilas.gov.co
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
X-XSS-Protection: 1
content-length: 43359
```

Se puede observar la implementación de la política HSTS, de características de seguridad sobre las cookies y de cabeceras de seguridad (X-Content-Type-Options, X-Frame-Options, X-XSS-Protection). Estas características son partes de las *Condiciones mínimas técnicas y de seguridad digital* (para sitios webs) anexados a la Resolución MinTIC 1519 del 2020[12].

Además se puede notar que las tecnologías y versiones del servidor web se remplazo por “XXX” con el fin de dificultar la fase de reconocimiento en un ataque, lo que es algo positivo. Finalmente se puede notar la cookie “f5_cspm” también característica de un balanceador de carga de la empresa F5.
Para este dominio una evaluación en SSL Lab da la nota máxima A+:



12 https://gobiernodigital.mintic.gov.co/portal/Noticias/160997:MinTIC-publica-la-Resolucion-1519-del-2020-sobre-transparencia-en-el-acceso-a-la-informacion-accesibilidad-web-seguridad-digital-web-y-datos-abiertos

ANEXO I4: SOLICITUDES HTTP EN LOS LOGS ANDROID

Este extracto proviene de los eventos (logs) Android de la Cédula Digital (capturados con la herramienta *Pidcatdroid*) en un proceso de activación de la Cédula Digital analizado el 27 de enero del 2025:

```
Http.LimitedHttpLogger\x1b[0m \x1b[30;104m D \x1b[0m -->
GET https://mobiledocs.registraduria.gov.co/[...]

[Se quitó esta parte para no generar riesgos de seguridad]
```

Muestra un extracto de una solicitud HTTP(S) y de la respuesta del servidor, incluyendo el inicio del payload (un archivo JSON en este caso, que esta completo en los logs). Es una solicitud y una respuesta similar a la que se muestra en al Anexo 1 y que había sido capturada y descifrada con Pirogue.