Secure IoT Registry

IoT Ottawa Meetup

https://cira.ca/IoT

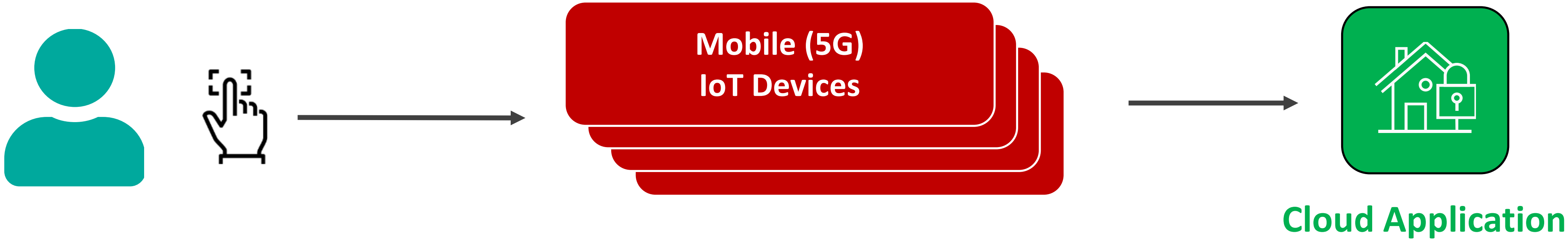
Presented by:

Jacques Latour | Andres Nunez| Jan 15, 2020

cira

IoT Turning Point: Hardcoded vs. Zero Touch

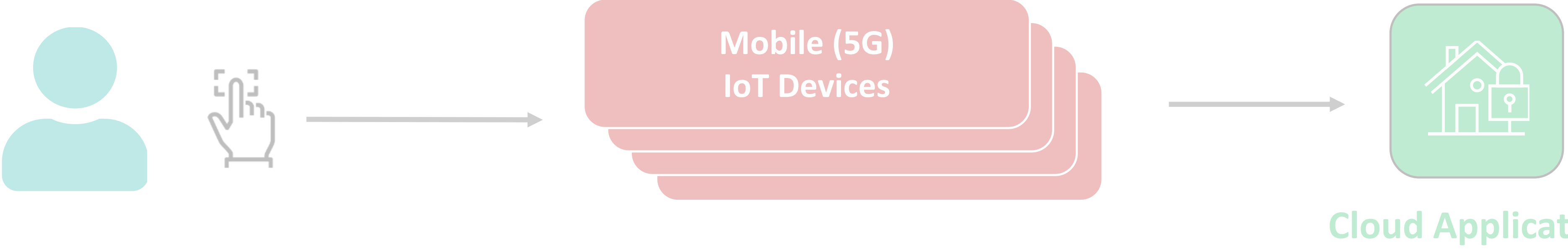
TODAY - HARDCODED



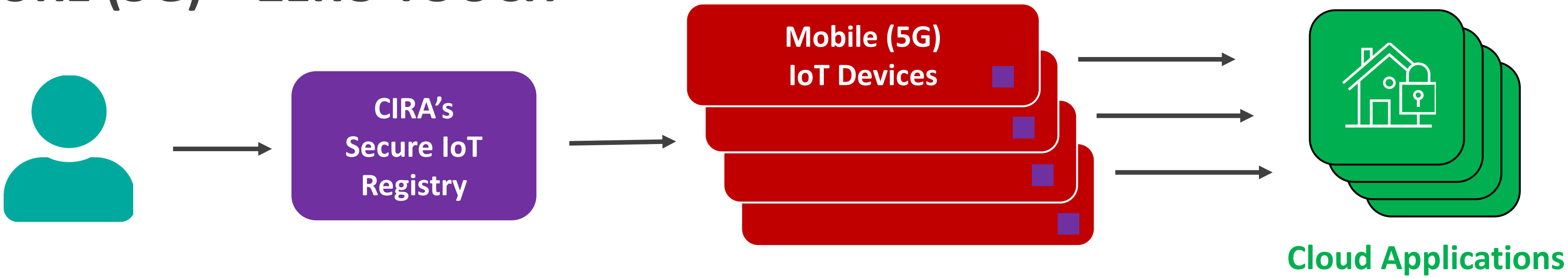
think 5G mobile IoT sensors on a pipeline or generic smart parking meters

IoT Turning Point: Hardcoded vs. Zero Touch

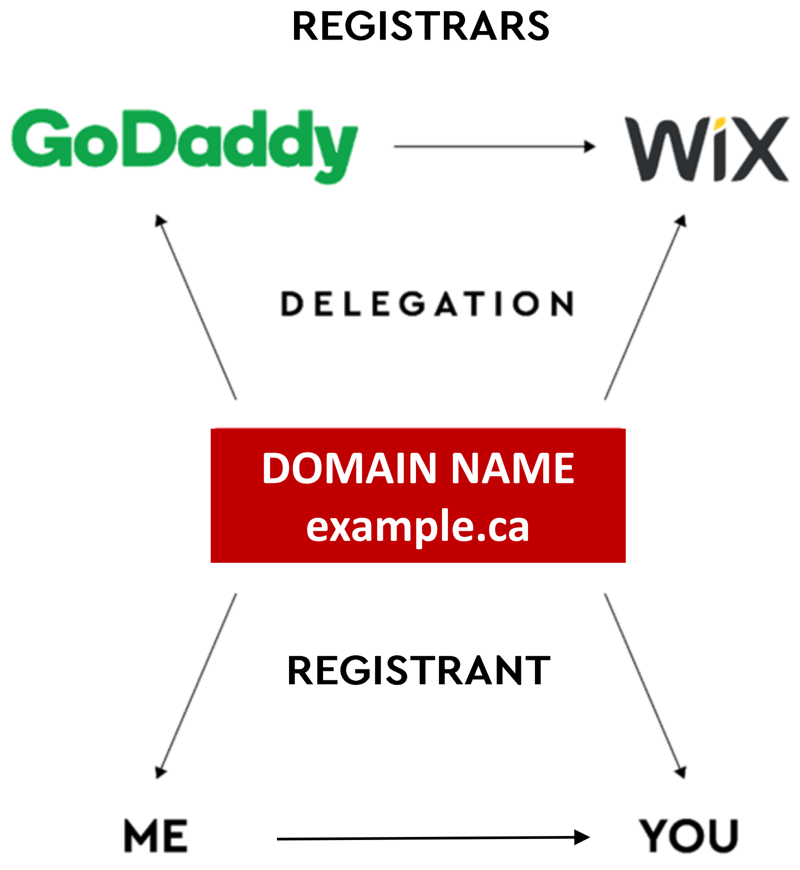
TODAY - HARDCODED



FUTURE (5G) – ZERO TOUCH



Similarity between Domain Names and Mobile IoT Devices



REGISTRARS

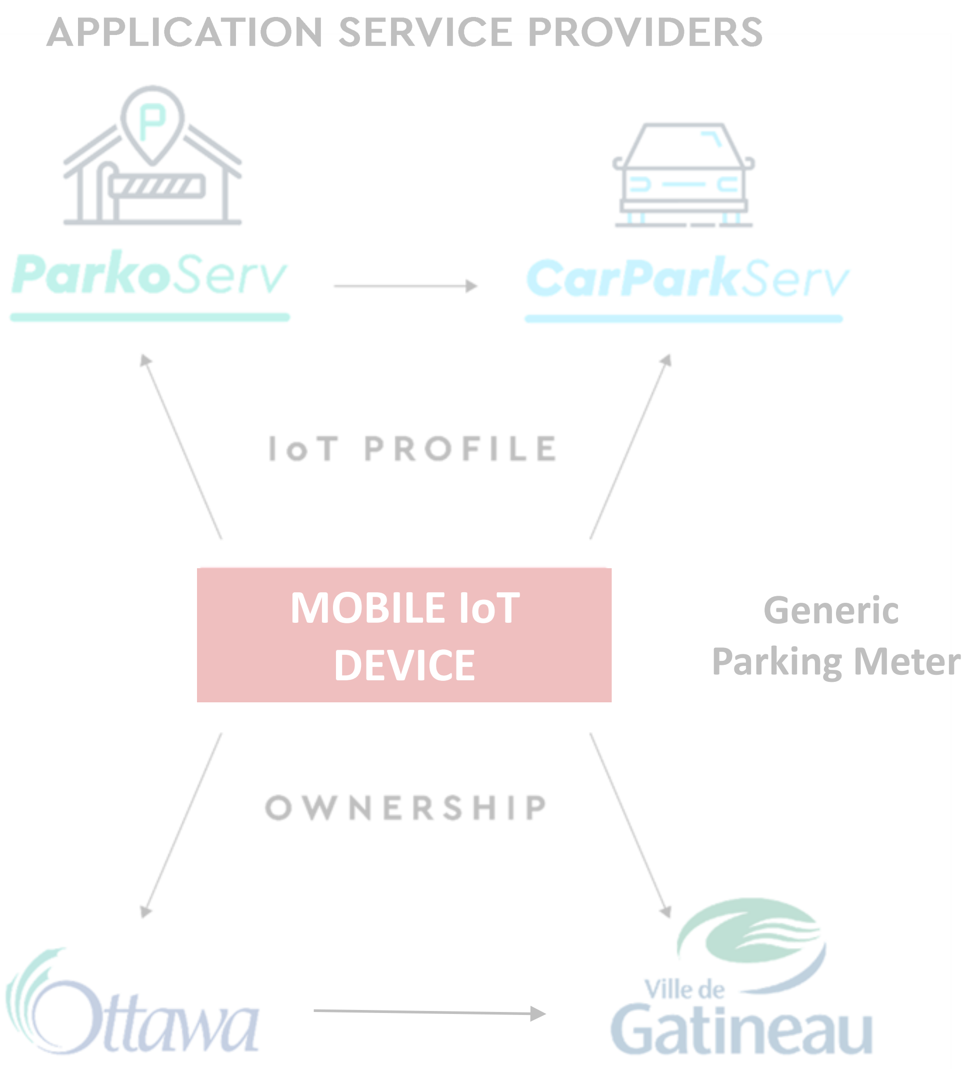
GoDaddy → WiX

DELEGATION

DOMAIN NAME
example.ca

REGISTRANT

ME → YOU



APPLICATION SERVICE PROVIDERS

ParkoServ → CarParkServ

IoT PROFILE

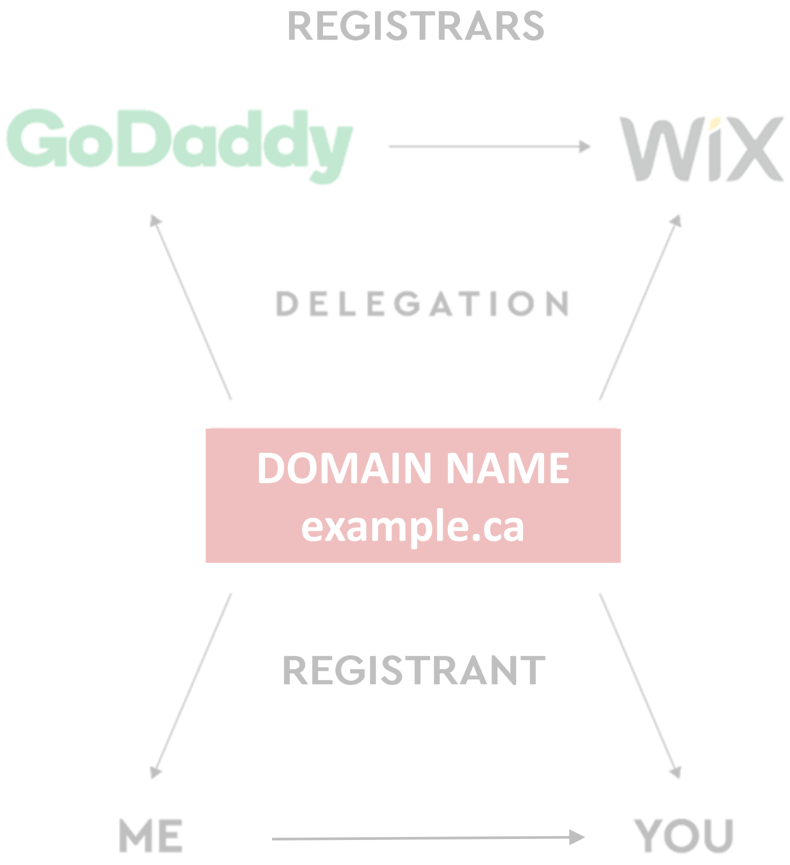
MOBILE IoT DEVICE

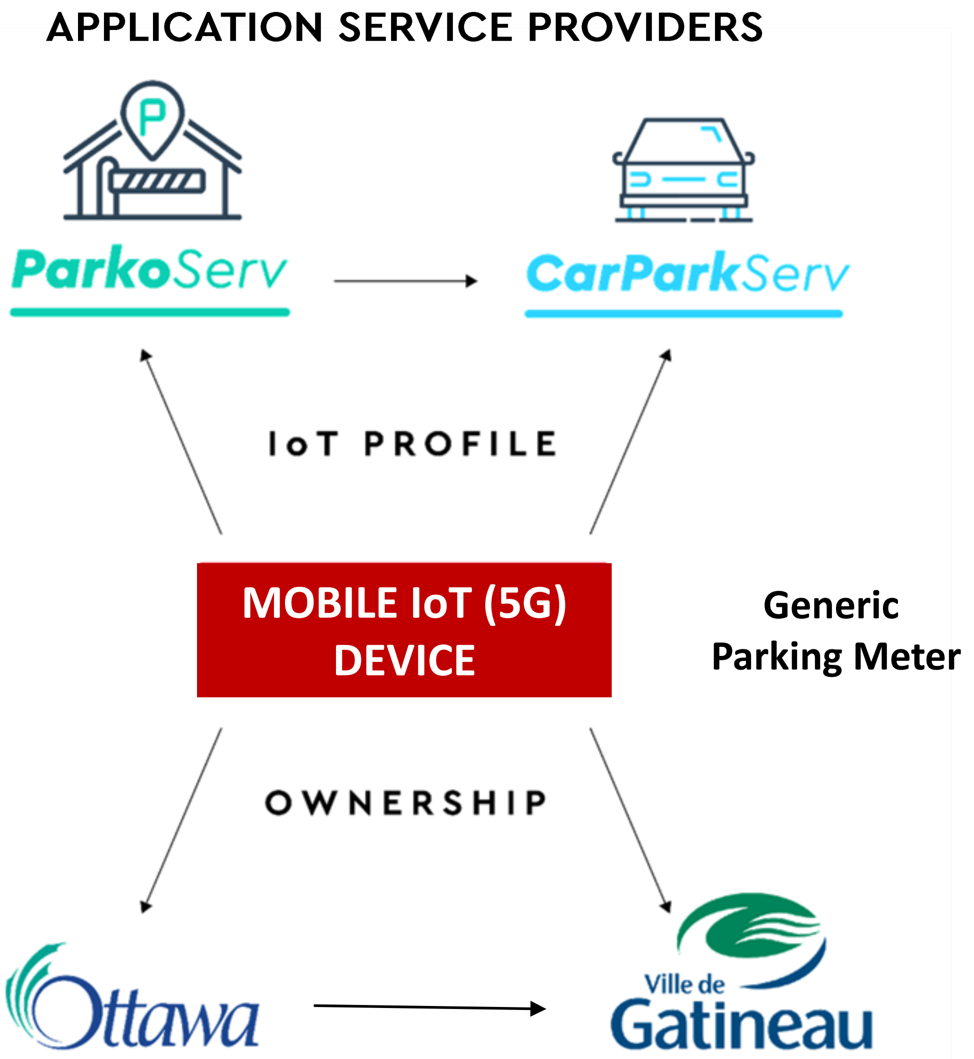
Generic Parking Meter

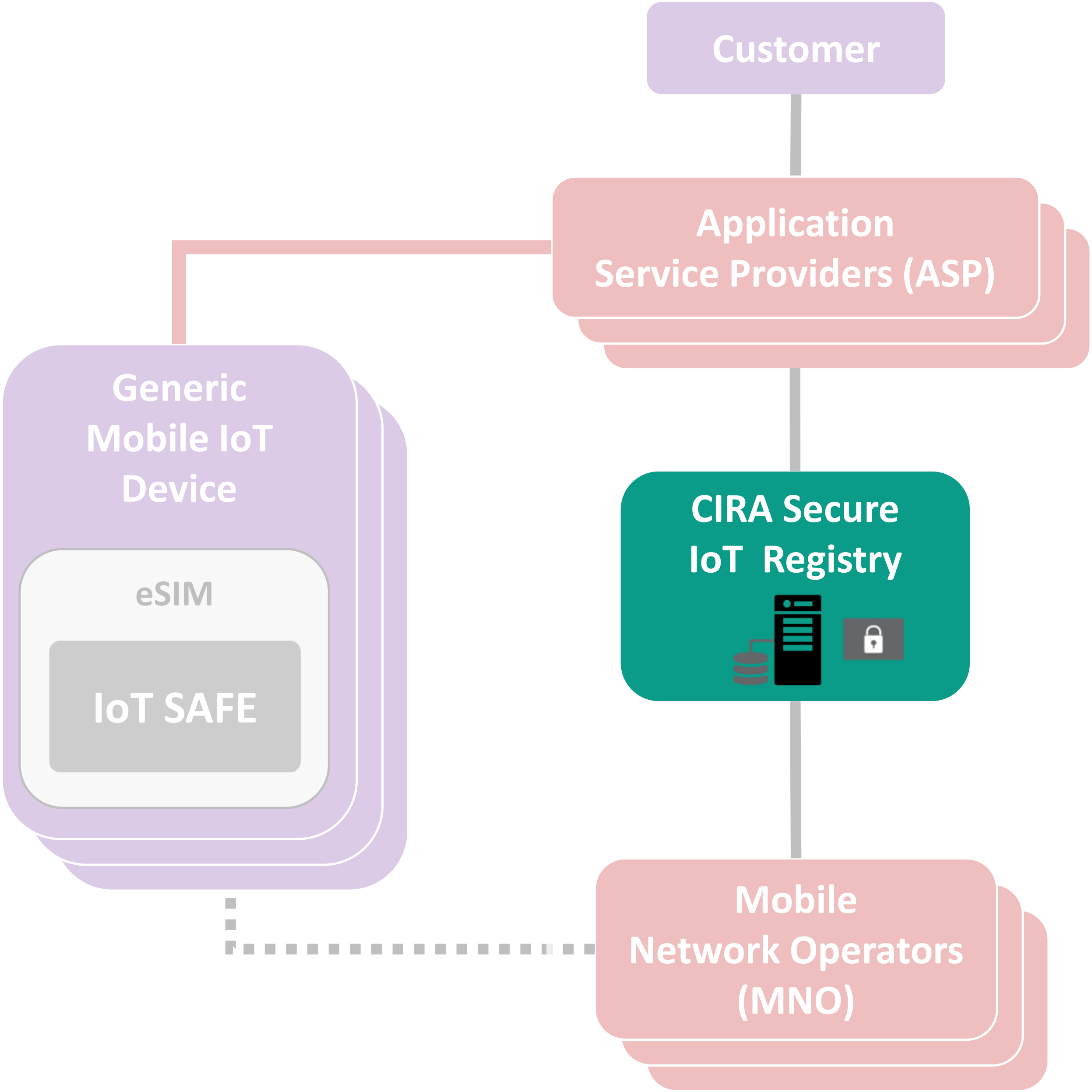
OWNERSHIP

Ottawa → Ville de Gatineau

Similarity between Domain Names and Mobile IoT Devices

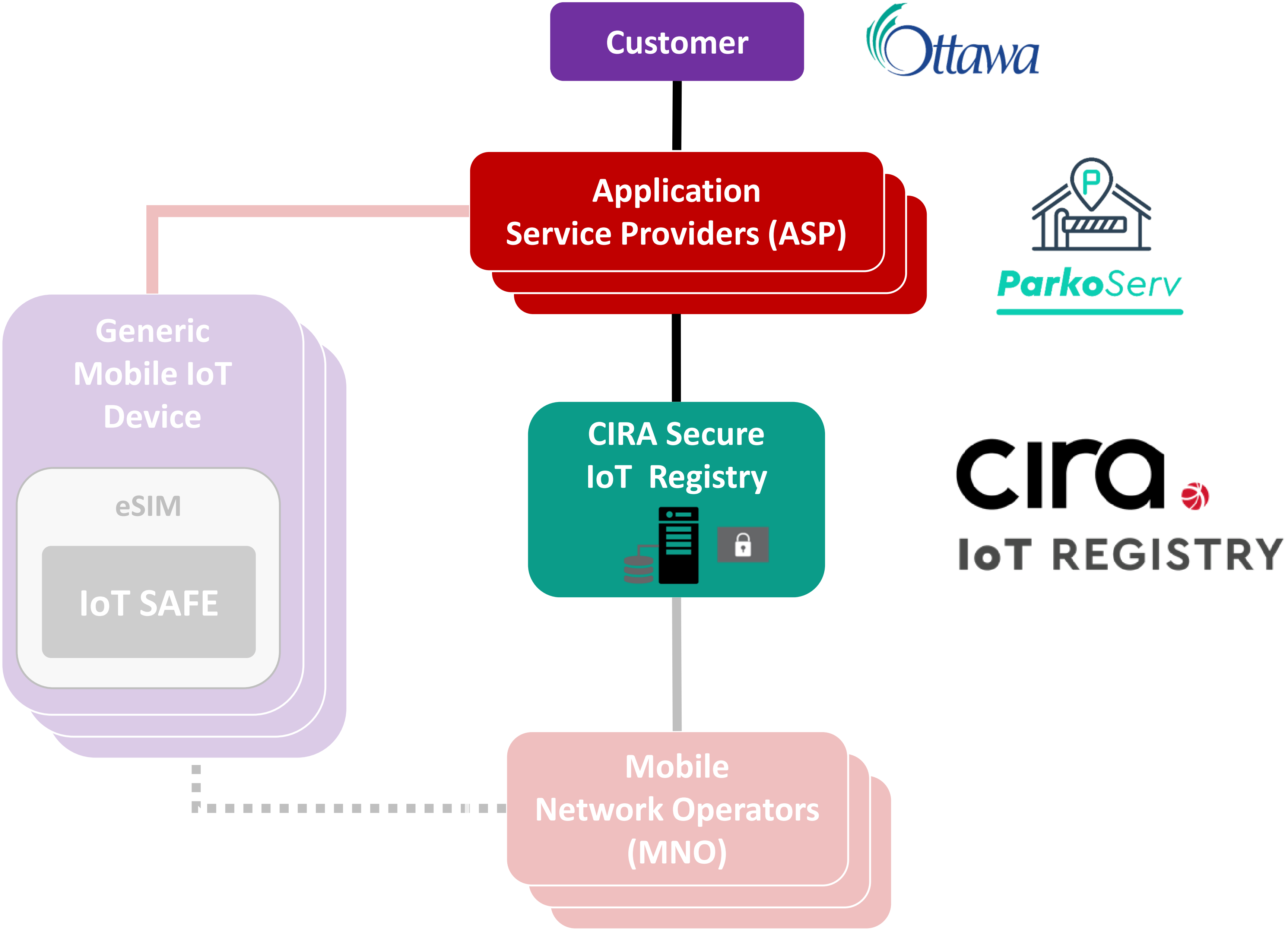


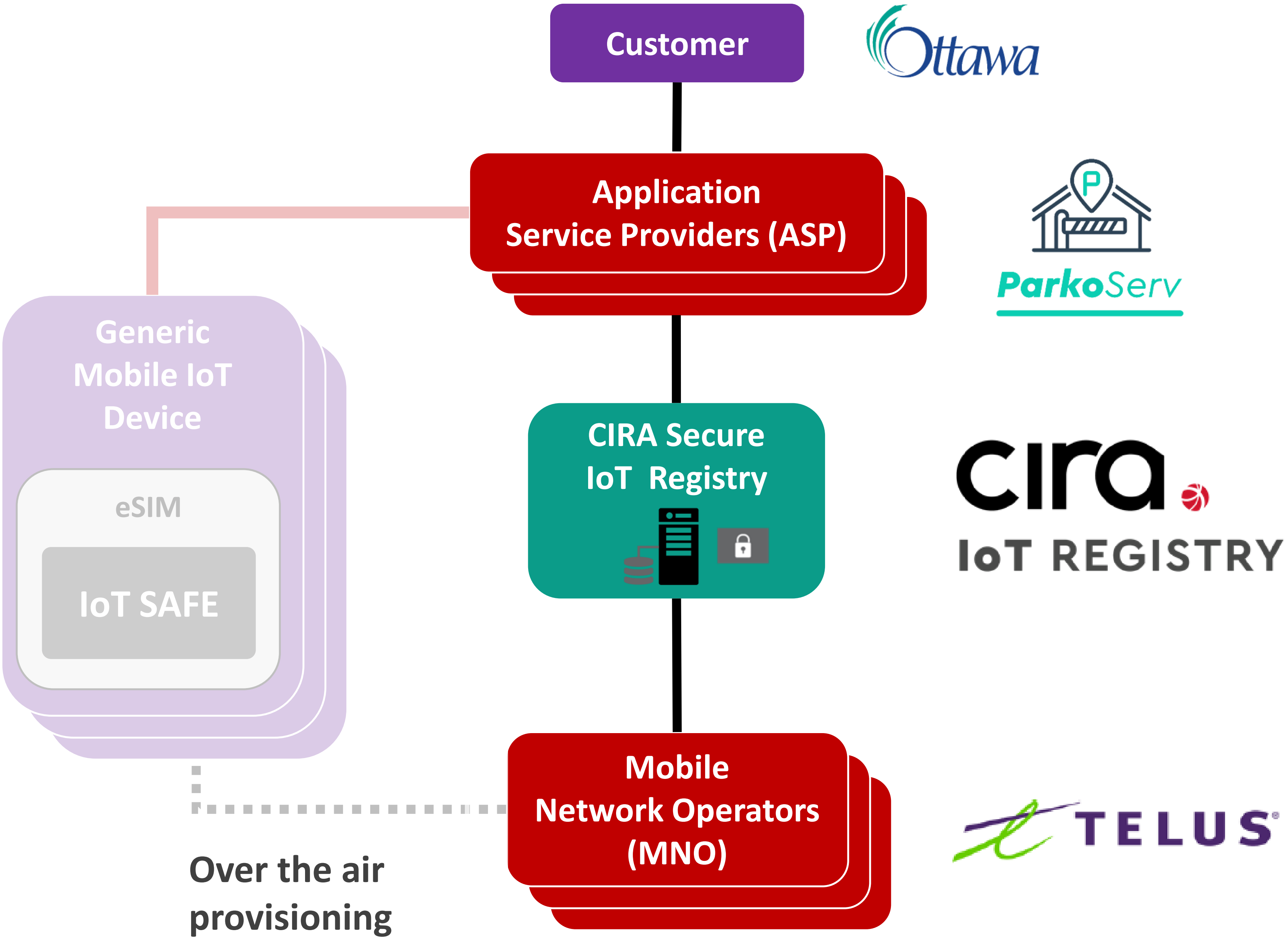



Customer
Application Service Providers (ASP)
Generic Mobile IoT Device
eSIM
IoT SAFE
CIRA Secure IoT Registry
Mobile Network Operators (MNO)

cira IoT REGISTRY

+Functional prototype
& proof of concept


Customer
Ottawa
Application Service Providers (ASP)
ParkoServ
Generic Mobile IoT Device
eSIM
IoT SAFE
CIRA Secure IoT Registry
cira
IoT REGISTRY
Mobile Network Operators (MNO)



Customer

Application Service Providers (ASP)

CIRA Secure IoT Registry

Mobile Network Operators (MNO)

Generic Mobile IoT Device

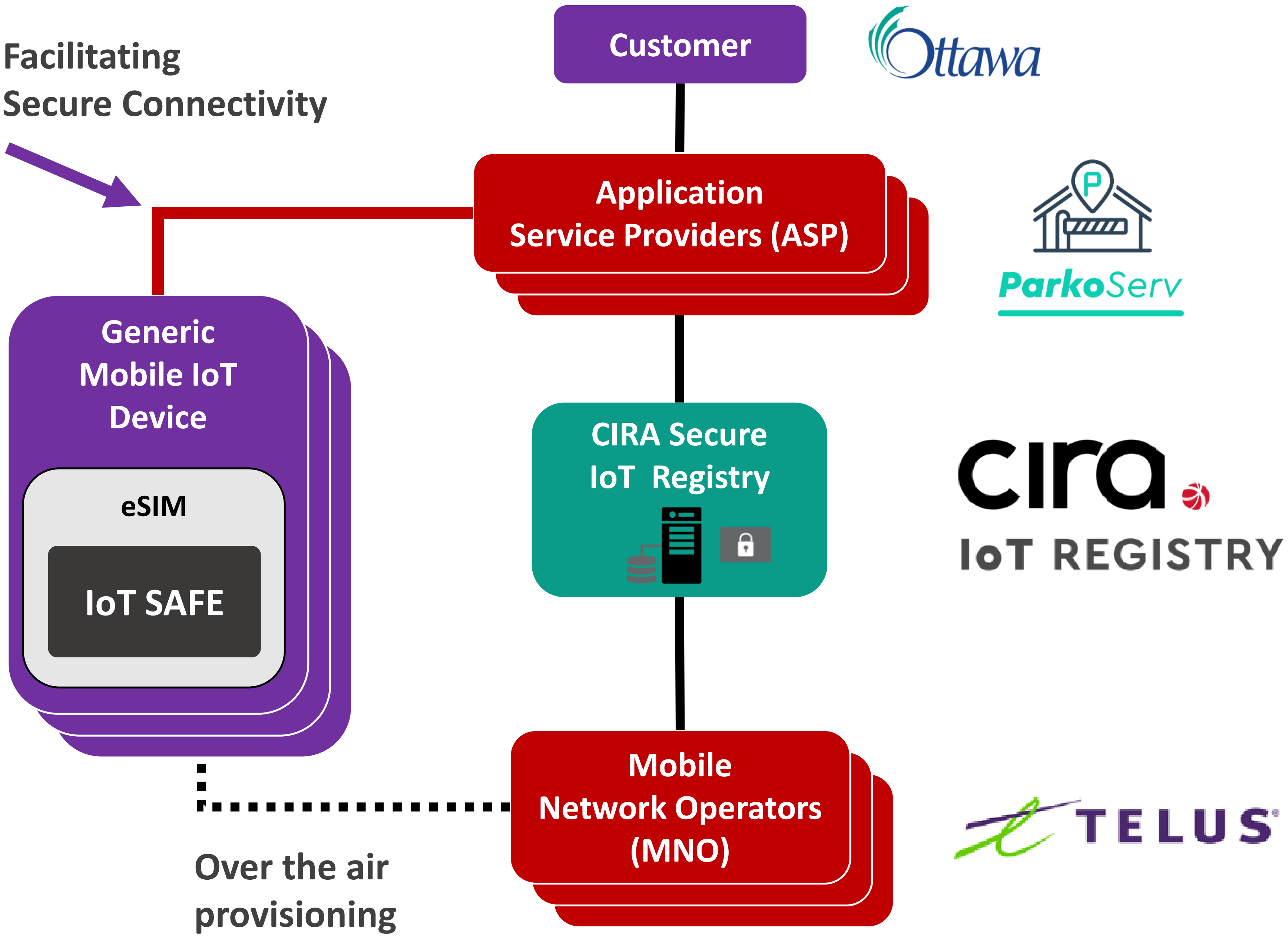
eSIM

IoT SAFE

Over the air provisioning

What's innovative?

Facilitating
Secure Connectivity



Customer

Ottawa

Application
Service Providers (ASP)

ParkoServ

Generic
Mobile IoT
Device

eSIM

IoT SAFE

CIRA Secure
IoT Registry

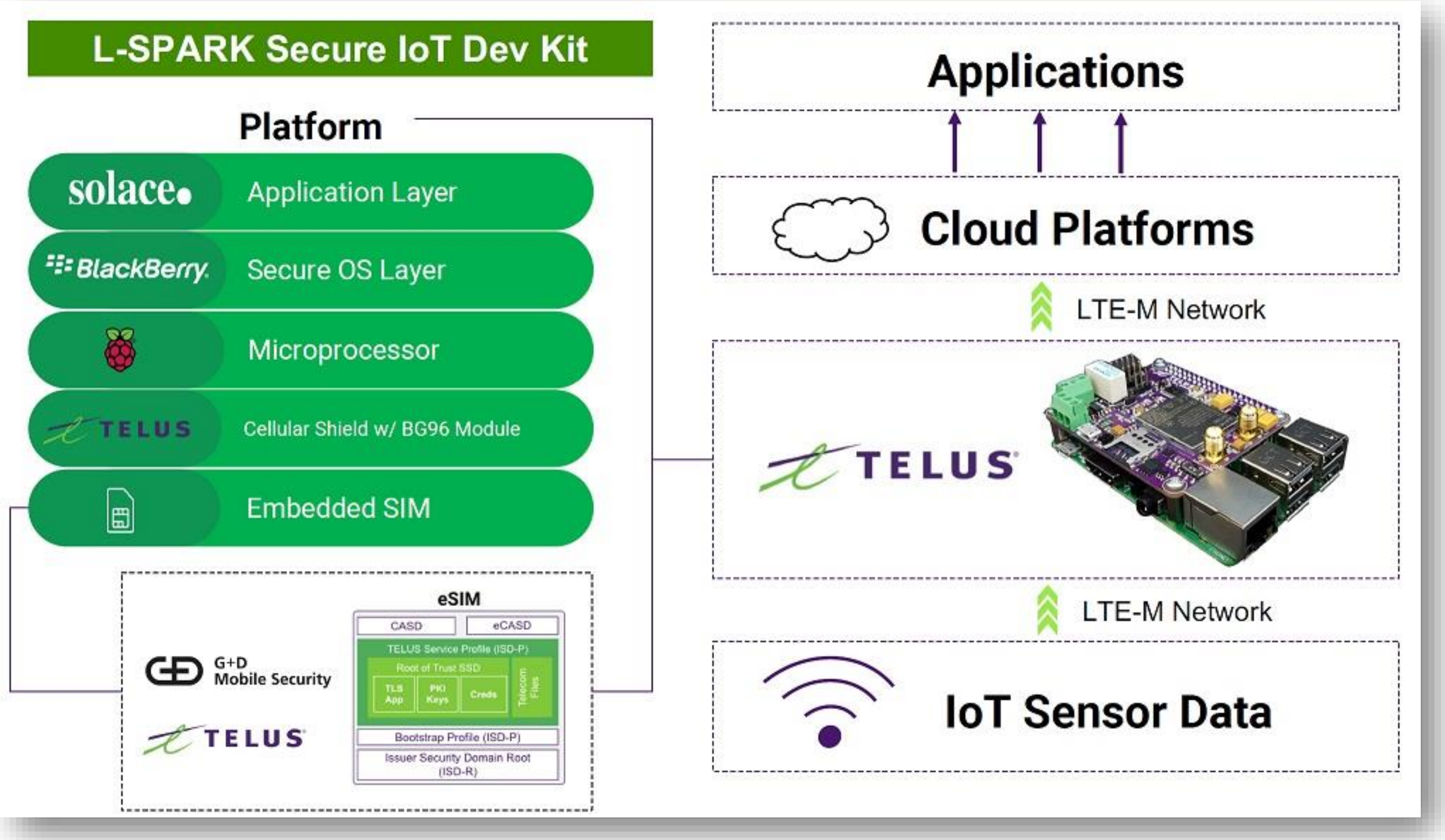
cira
IoT REGISTRY

Mobile
Network Operators
(MNO)

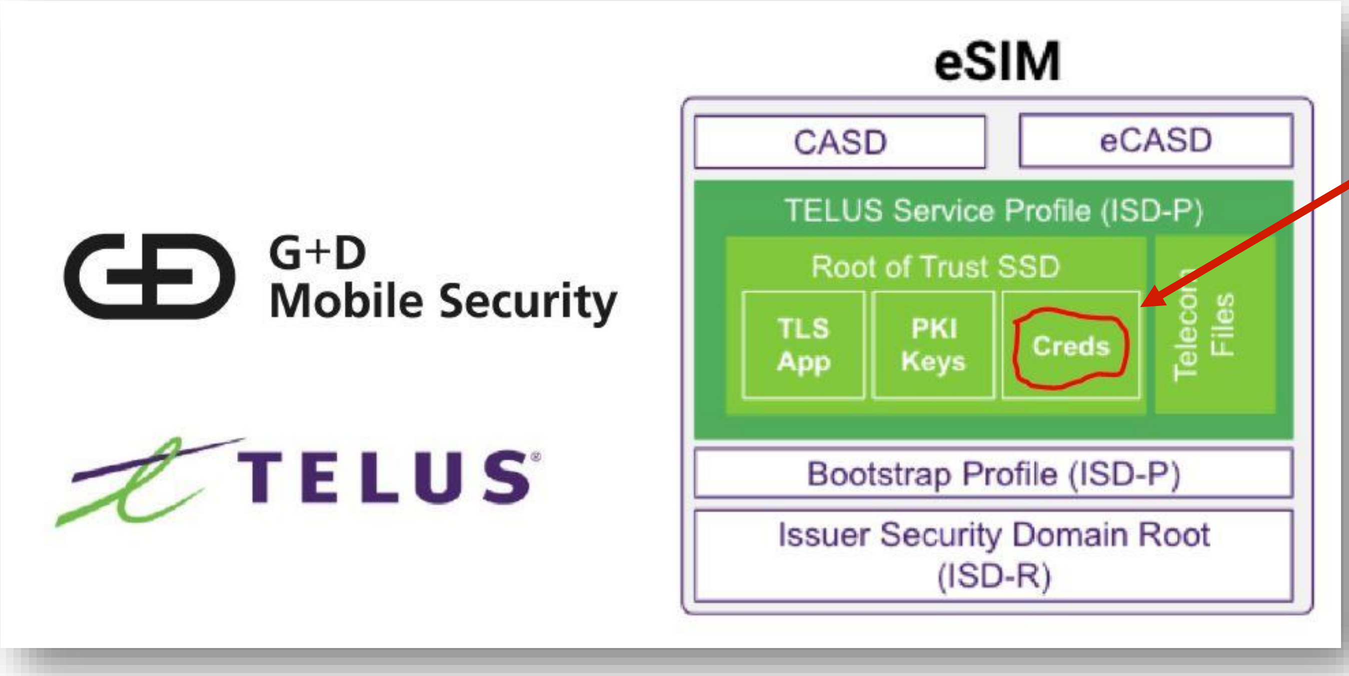
TELUS

Over the air
provisioning

The enablers are eSIMs & MNO Service Profiles



Let’s look at the eSIM & MNO Service Profile and how it can enable IoT Connectivity

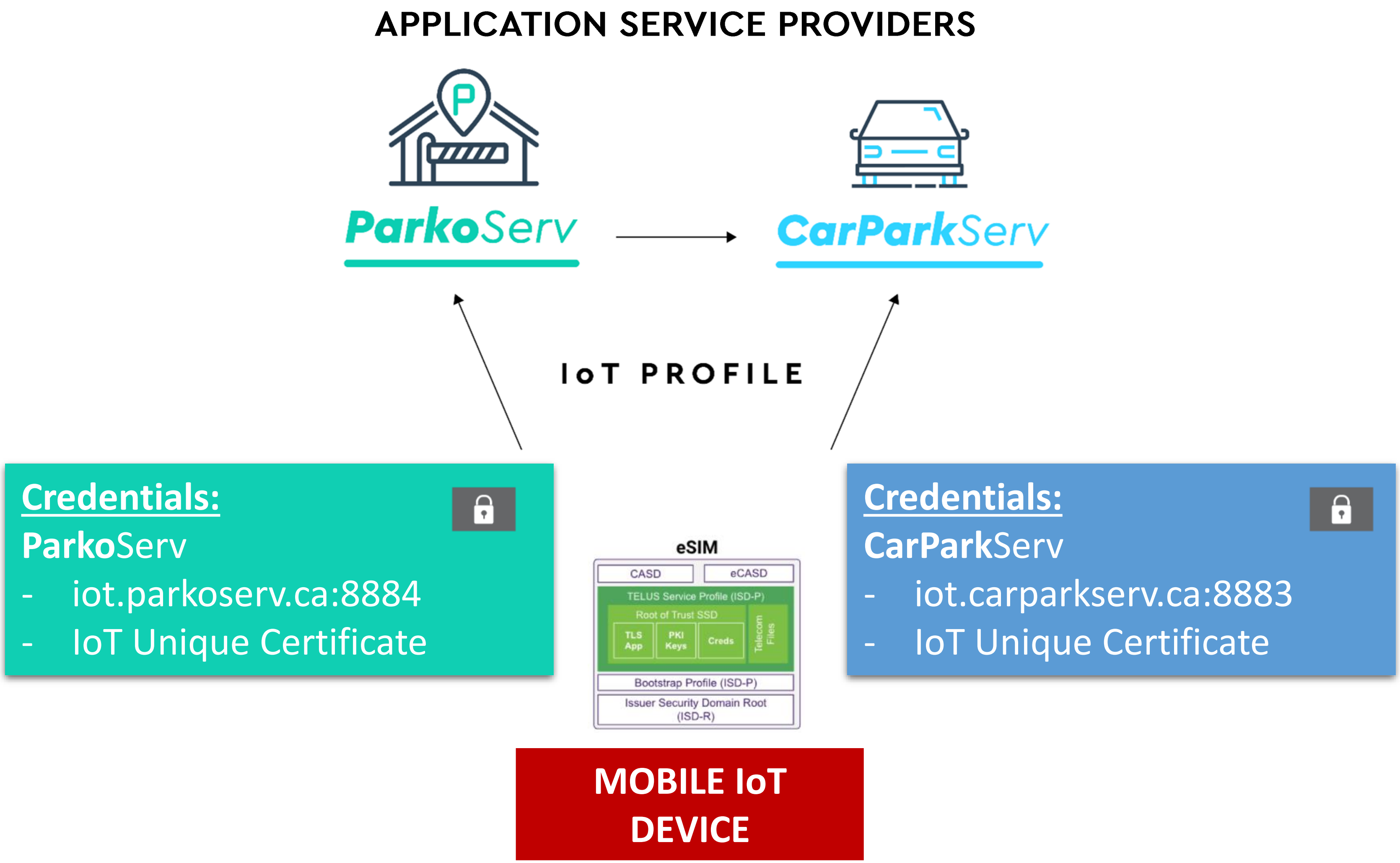

G+D Mobile Security
TELUS
eSIM
CASD
eCASD
TELUS Service Profile (ISD-P)
Root of Trust SSD
TLS App
PKI Keys
Creds
Telecom Files
Bootstrap Profile (ISD-P)
Issuer Security Domain Root (ISD-R)

Downloadable Encrypted IoT Application Credentials

Application/Cloud Service Provider

- Domain name / URL
- Port Number
- IoT Unique Certificate

No more hardcoding IoT devices to CSP or ASP



APPLICATION SERVICE PROVIDERS

ParkoServ → CarParkServ

IoT PROFILE

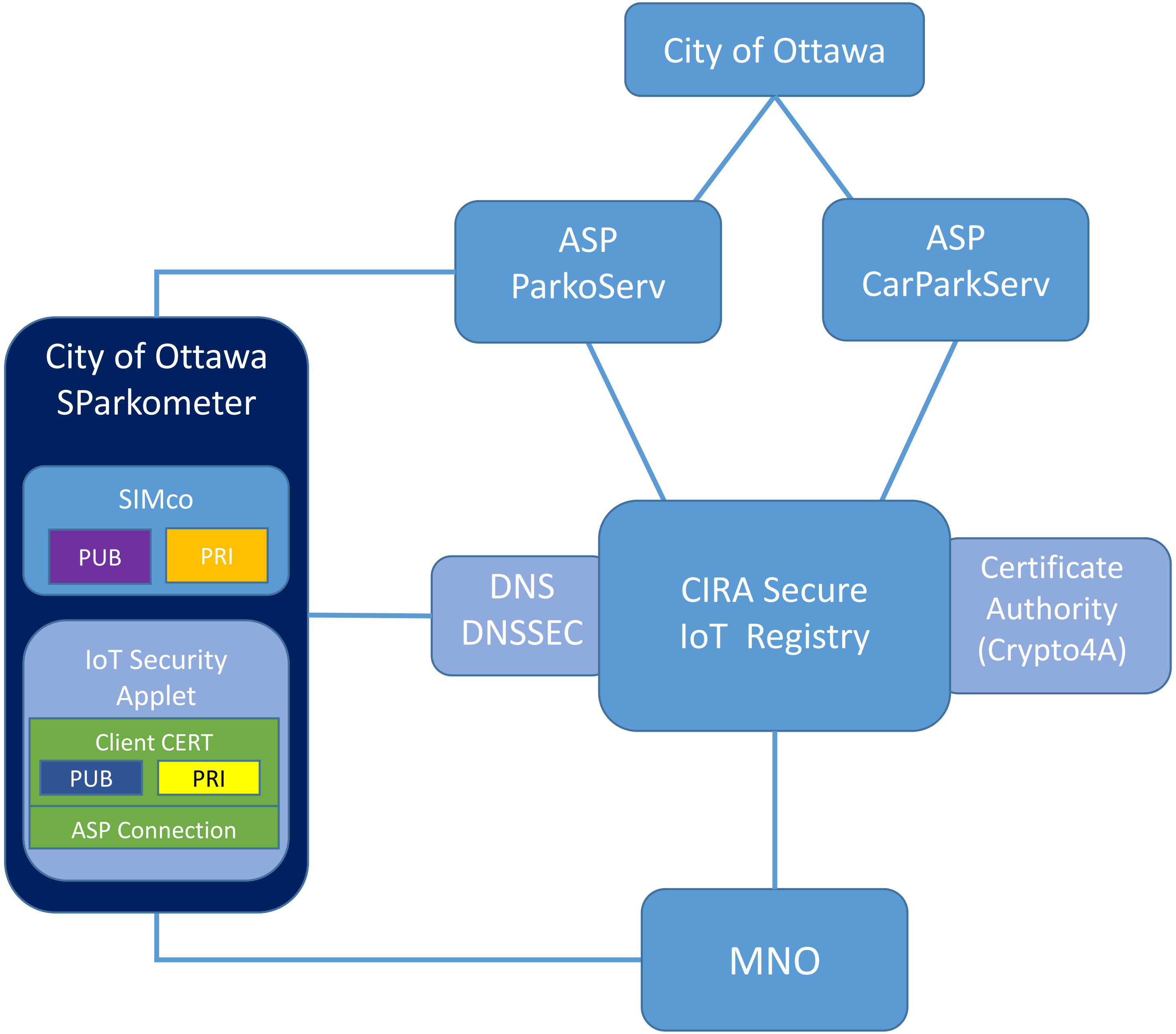
Credentials:
ParkoServ
- iot.parkoserv.ca:8884
- IoT Unique Certificate

Credentials:
CarParkServ
- iot.carparkserv.ca:8883
- IoT Unique Certificate

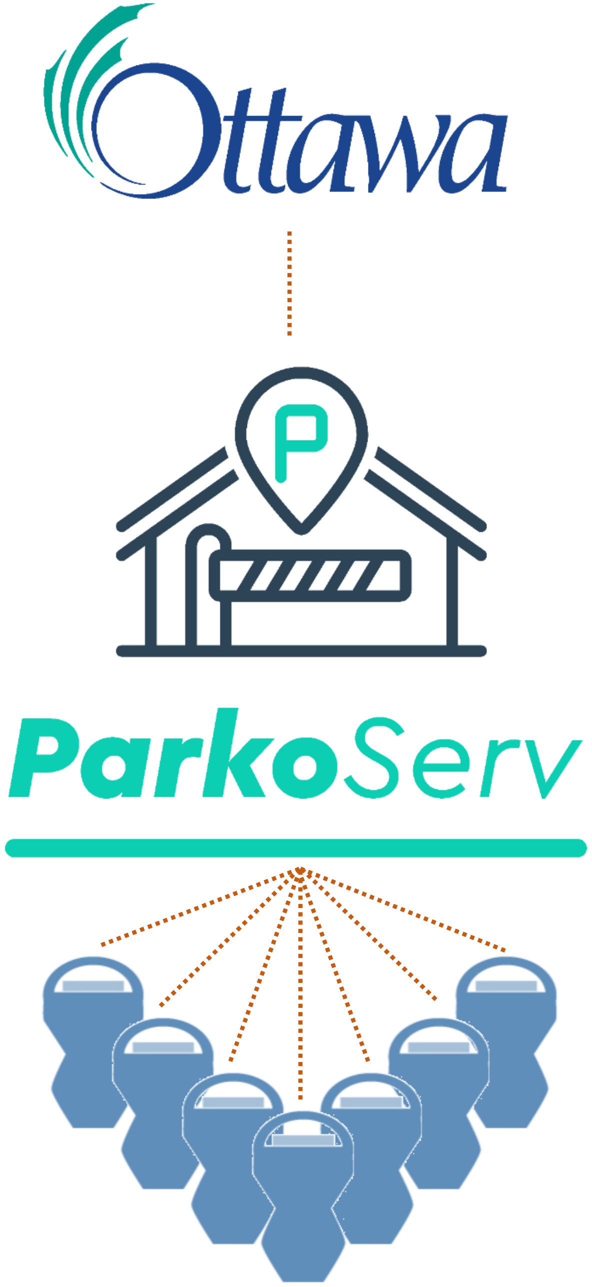
eSIM
CASD
eCASD
TELUS Service Profile (ISD-P)
Root of Trust SSD
TLS App
PKI Keys
Creds
Telecom Files
Bootstrap Profile (ISD-P)
Issuer Security Domain Root (ISD-R)

MOBILE IoT DEVICE

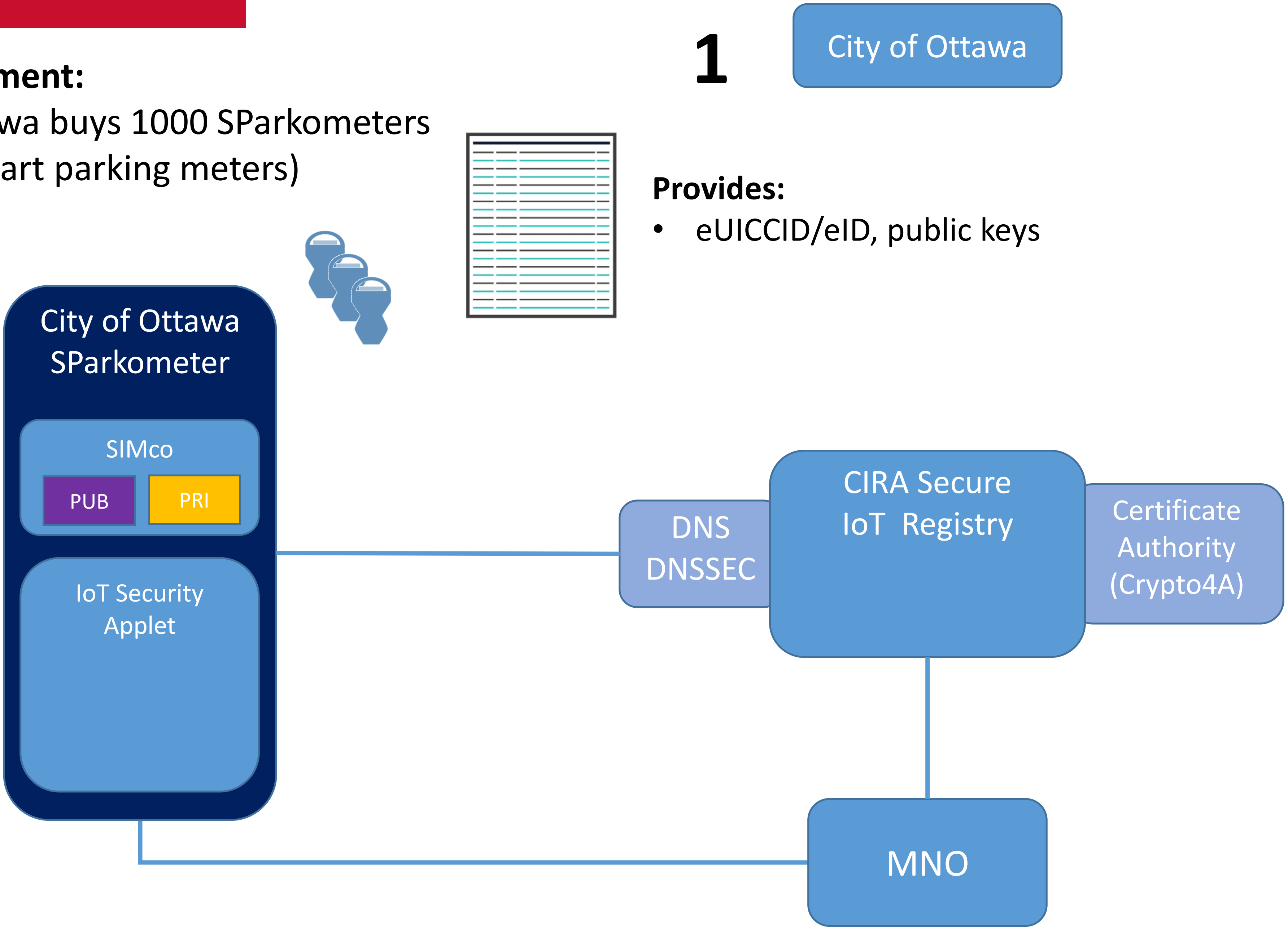
How does a Secure IoT Registry work?


City of Ottawa
ASP
ParkoServ
ASP
CarParkServ
City of Ottawa
SParkometer
SIMco
PUB
PRI
IoT Security
Applet
Client CERT
PUB
PRI
ASP Connection
DNS
DNSSEC
CIRA Secure
IoT Registry
Certificate
Authority
(Crypto4A)
MNO

THE CITY OF OTTAWA BUYS 1000 GENERIC SMART PARKING METERS AND SELECTS PARKOSERV AS CLOUD SERVICE PROVIDER



1 - Procurement:
City of Ottawa buys 1000 SParkometers (**generic** smart parking meters)

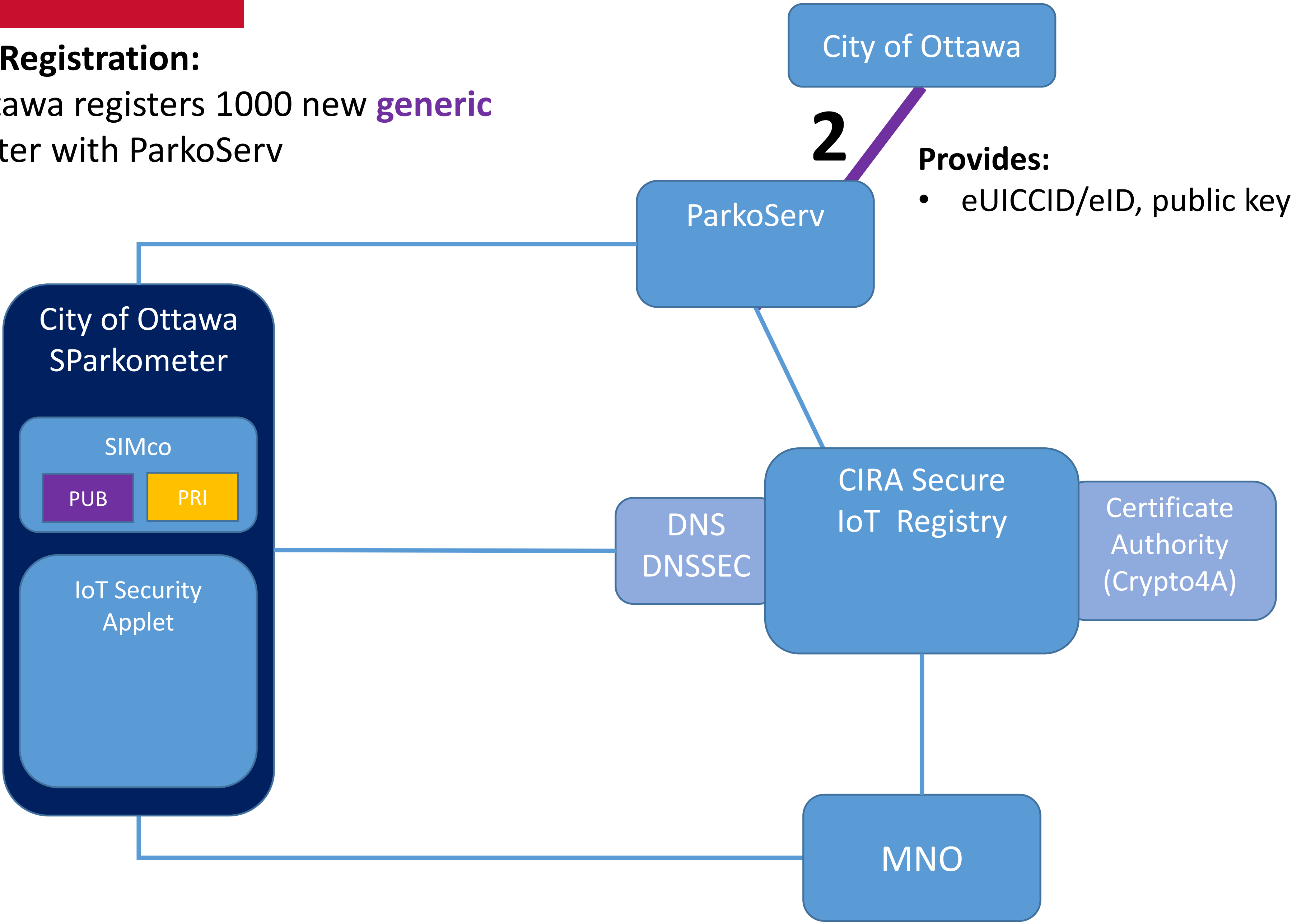


Provides:

- eUICCID/eID, public keys

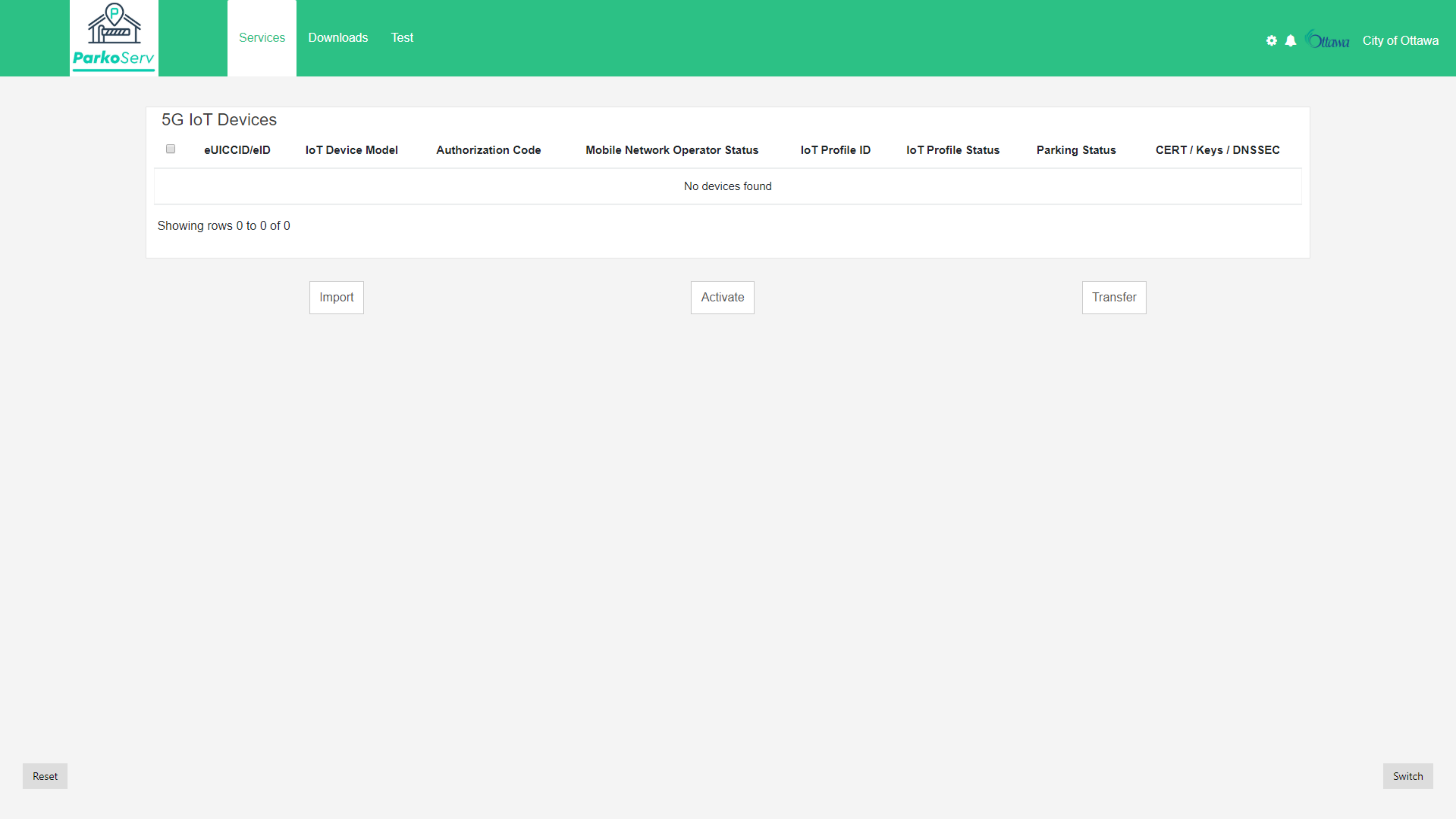
2 – Cloud Registration:

City of Ottawa registers 1000 new **generic** SParkometer with ParkoServ



Provides:

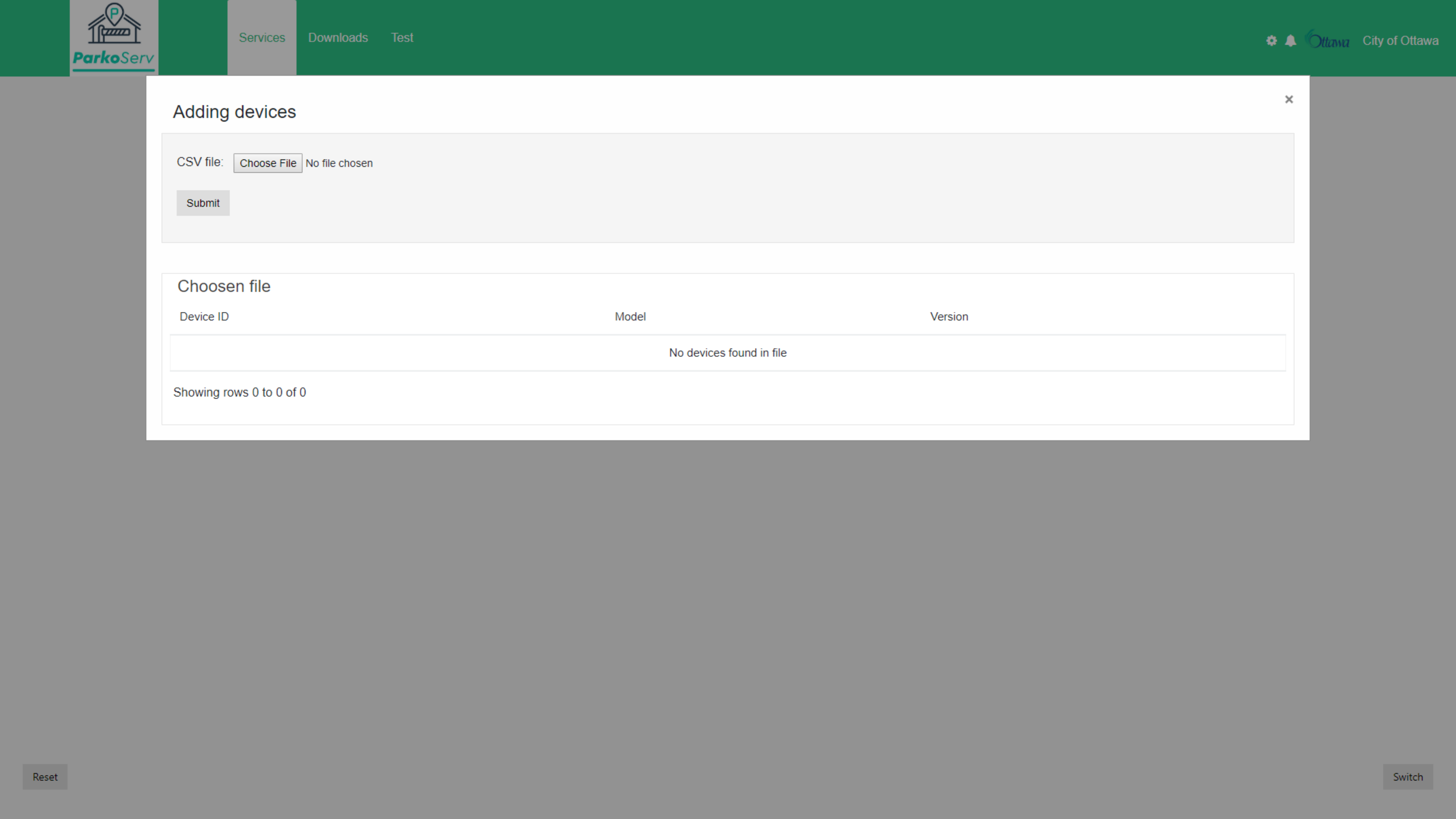
- eUICCID/eID, public keys



5G IoT Devices

□	eUICCID/eID	IoT Device Model	Authorization Code	Mobile Network Operator Status	IoT Profile ID	IoT Profile Status	Parking Status	CERT / Keys / DNSSEC
No devices found								

Showing rows 0 to 0 of 0



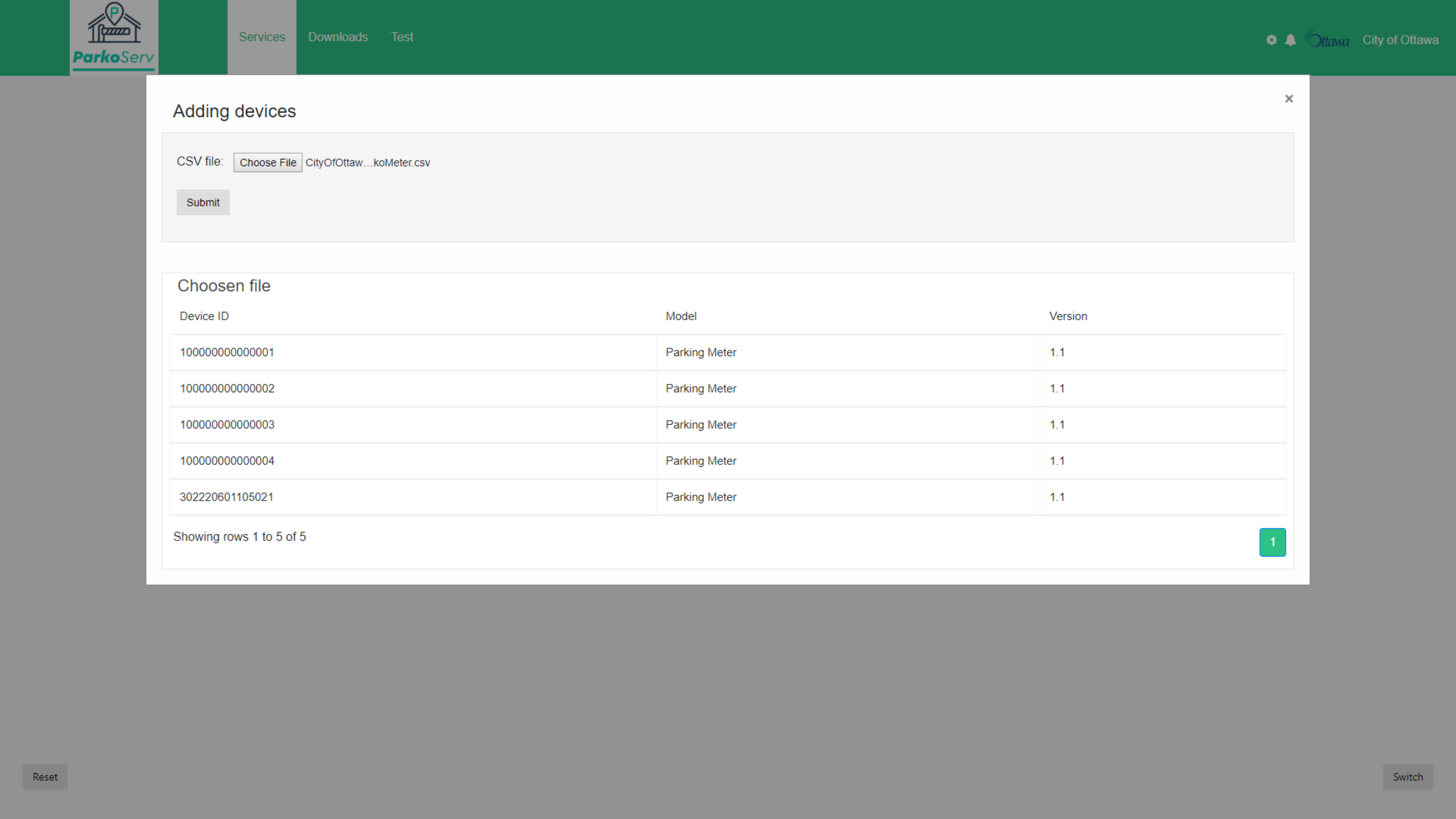
Adding devices

CSV file: Choose File No file chosen

Choosen file

Device ID	Model	Version
No devices found in file		

Showing rows 0 to 0 of 0



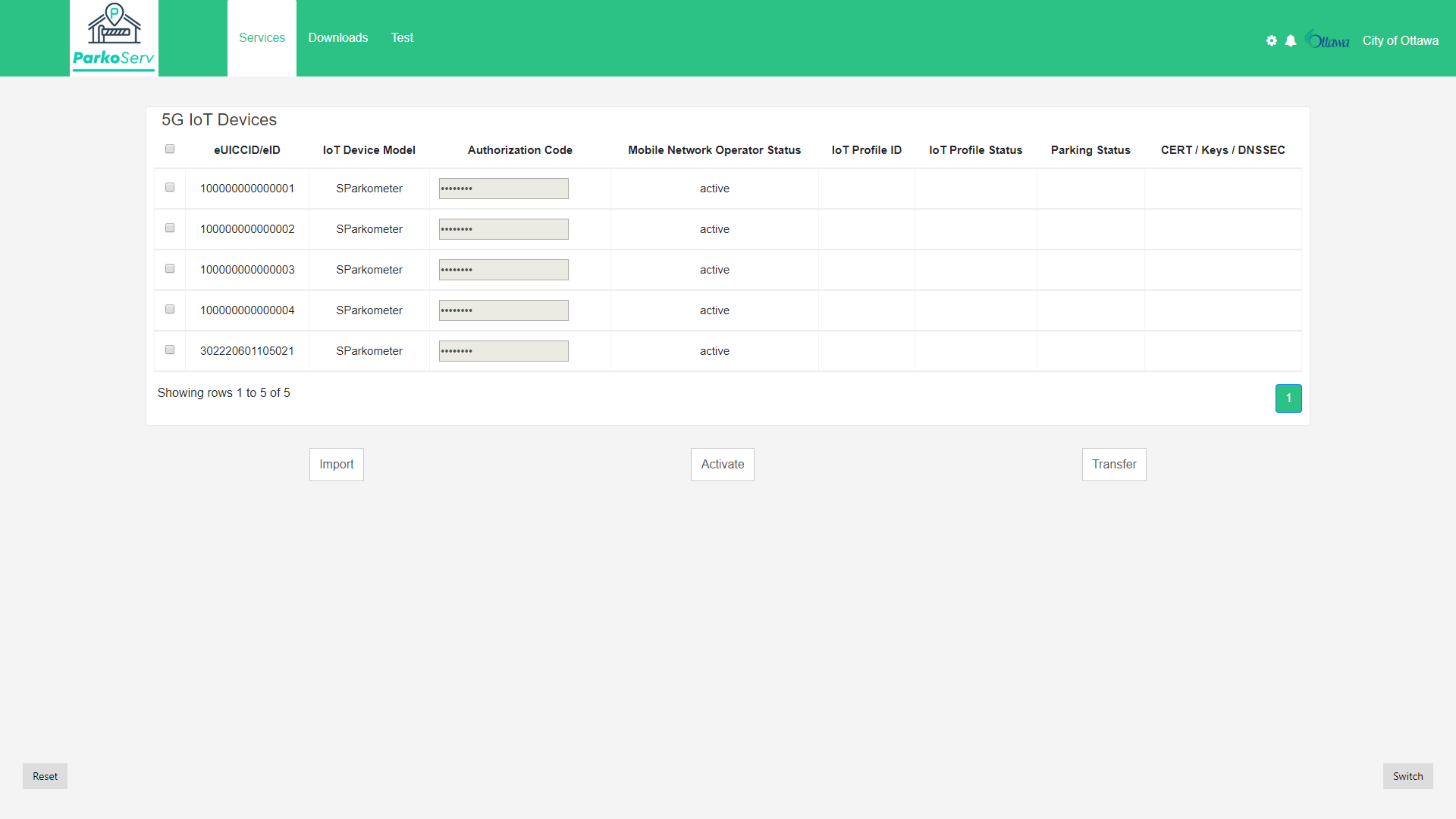
Adding devices

CSV file: CityOfOttaw...koMeter.csv

Choosen file

Device ID	Model	Version
100000000000001	Parking Meter	1.1
100000000000002	Parking Meter	1.1
100000000000003	Parking Meter	1.1
100000000000004	Parking Meter	1.1
302220601105021	Parking Meter	1.1

Showing rows 1 to 5 of 5



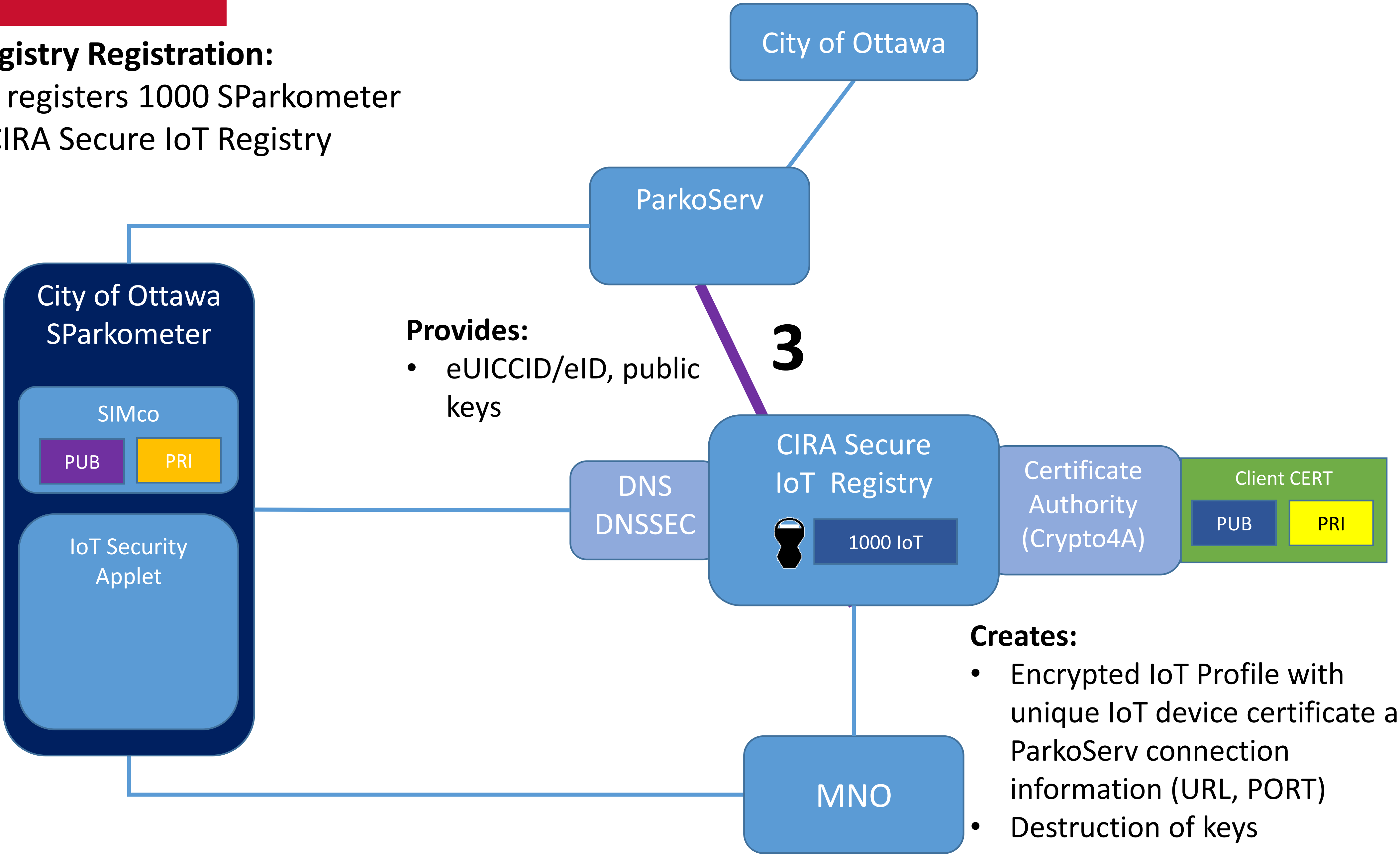
5G IoT Devices

□	eUICCID/eID	IoT Device Model	Authorization Code	Mobile Network Operator Status	IoT Profile ID	IoT Profile Status	Parking Status	CERT / Keys / DNSSEC
□	100000000000001	SParkometer	••••••••	active				
□	100000000000002	SParkometer	••••••••	active				
□	100000000000003	SParkometer	••••••••	active				
□	100000000000004	SParkometer	••••••••	active				
□	302220601105021	SParkometer	••••••••	active				

Showing rows 1 to 5 of 5

3 – IoT Registry Registration:

ParkoServ registers 1000 SParkometer with the CIRA Secure IoT Registry



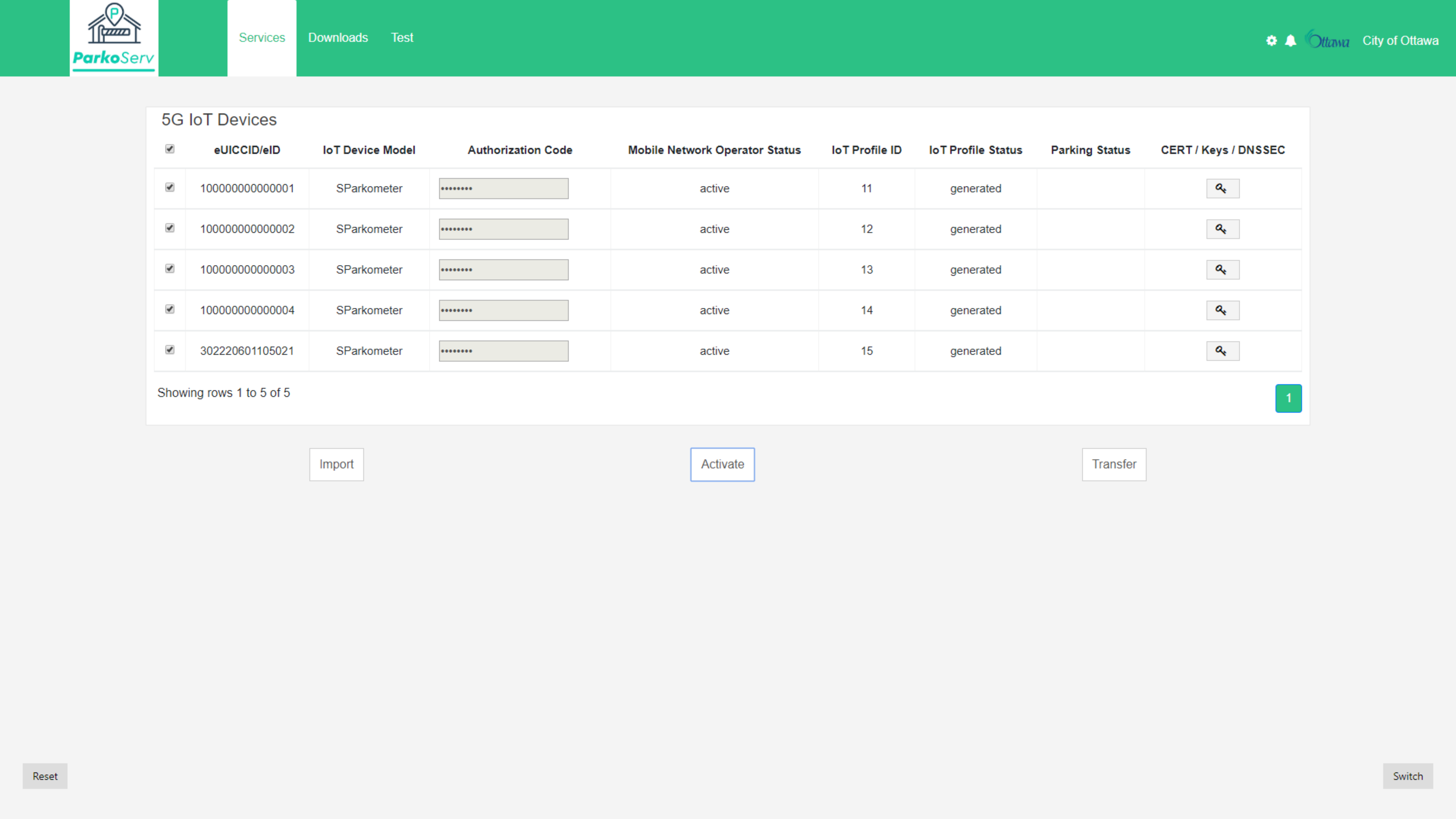
Provides:

- eUICCID/eID, public keys

Creates:

- Encrypted IoT Profile with unique IoT device certificate and ParkoServ connection information (URL, PORT)
- Destruction of keys

cira CIRA'S IOT REGISTRY



5G IoT Devices

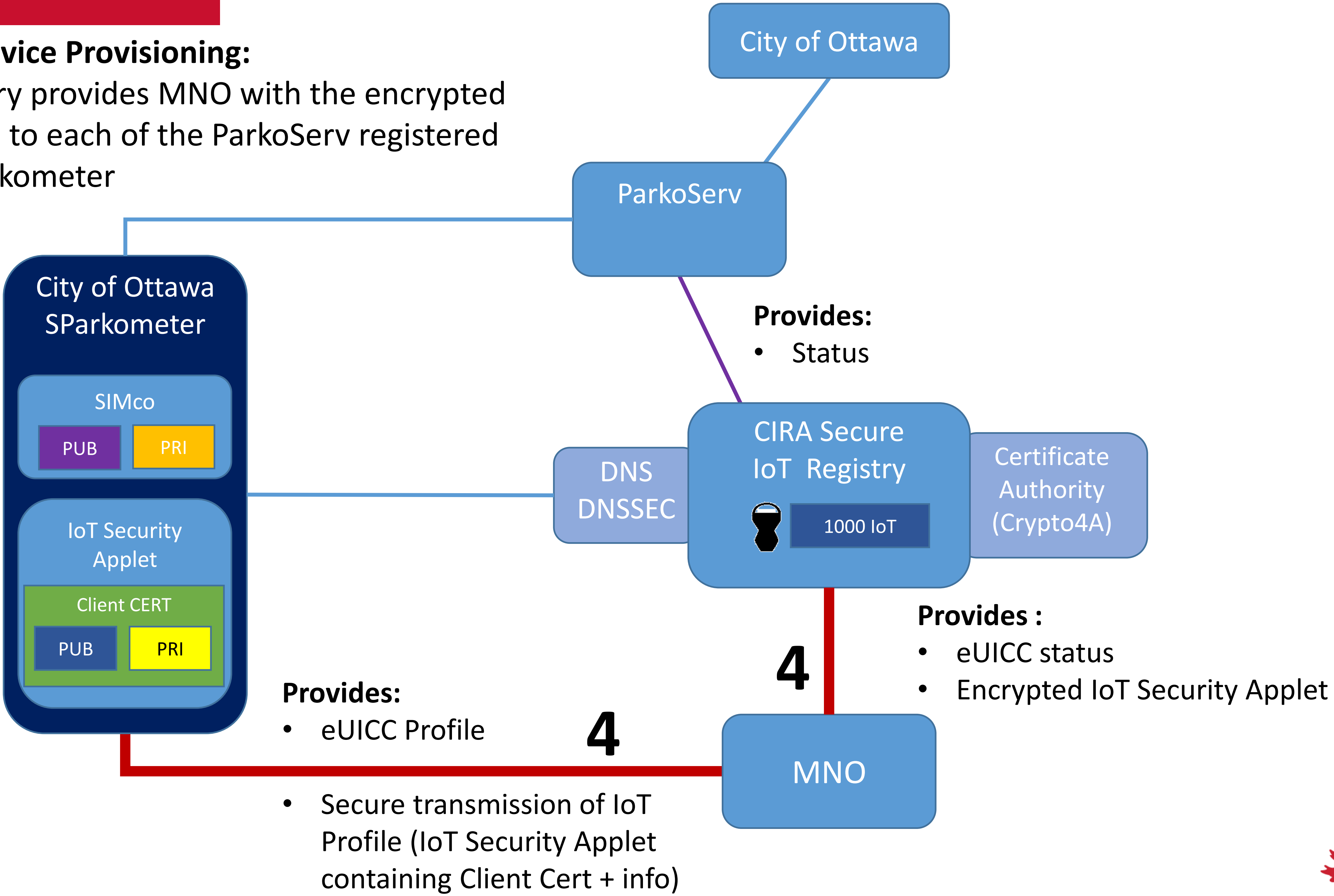
☑	eUICCID/eID	IoT Device Model	Authorization Code	Mobile Network Operator Status	IoT Profile ID	IoT Profile Status	Parking Status	CERT / Keys / DNSSEC
☑	100000000000001	SParkometer	••••••••	active	11	generated		🔑
☑	100000000000002	SParkometer	••••••••	active	12	generated		🔑
☑	100000000000003	SParkometer	••••••••	active	13	generated		🔑
☑	100000000000004	SParkometer	••••••••	active	14	generated		🔑
☑	302220601105021	SParkometer	••••••••	active	15	generated		🔑

Showing rows 1 to 5 of 5

1

4 – IoT Device Provisioning:

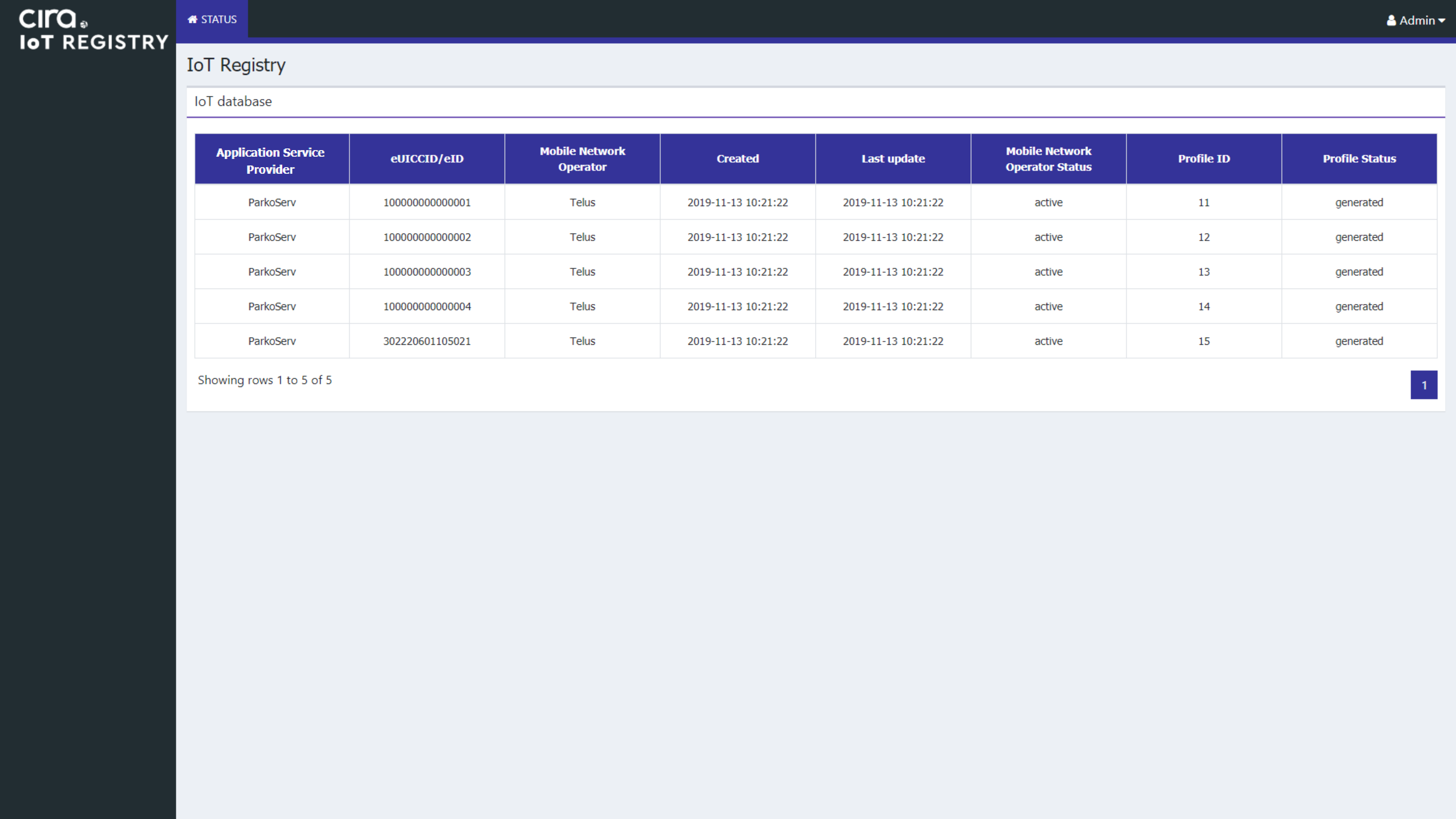
IoT Registry provides MNO with the encrypted IoT Profile to each of the ParkoServ registered 1000 SParkometer



Provides:
- Status

Provides :
- eUICC status
- Encrypted IoT Security Applet

Provides:
- eUICC Profile
- Secure transmission of IoT Profile (IoT Security Applet containing Client Cert + info)



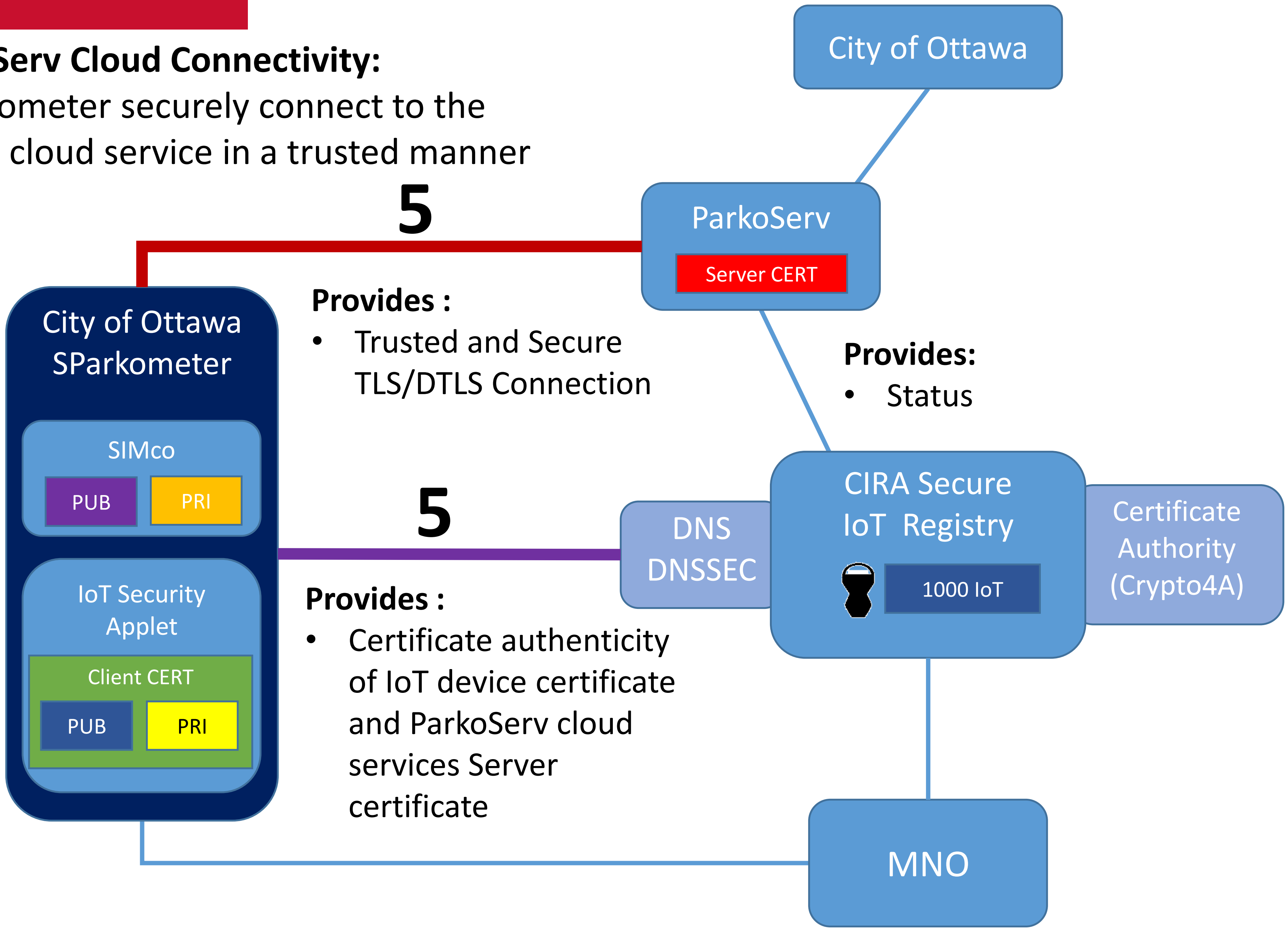
IoT Registry

IoT database

Application Service Provider	eUICCID/eID	Mobile Network Operator	Created	Last update	Mobile Network Operator Status	Profile ID	Profile Status
ParkoServ	100000000000001	Telus	2019-11-13 10:21:22	2019-11-13 10:21:22	active	11	generated
ParkoServ	100000000000002	Telus	2019-11-13 10:21:22	2019-11-13 10:21:22	active	12	generated
ParkoServ	100000000000003	Telus	2019-11-13 10:21:22	2019-11-13 10:21:22	active	13	generated
ParkoServ	100000000000004	Telus	2019-11-13 10:21:22	2019-11-13 10:21:22	active	14	generated
ParkoServ	302220601105021	Telus	2019-11-13 10:21:22	2019-11-13 10:21:22	active	15	generated

Showing rows 1 to 5 of 5

5 – ParkoServ Cloud Connectivity:
The SParkometer securely connect to the ParkoServ cloud service in a trusted manner



Provides :

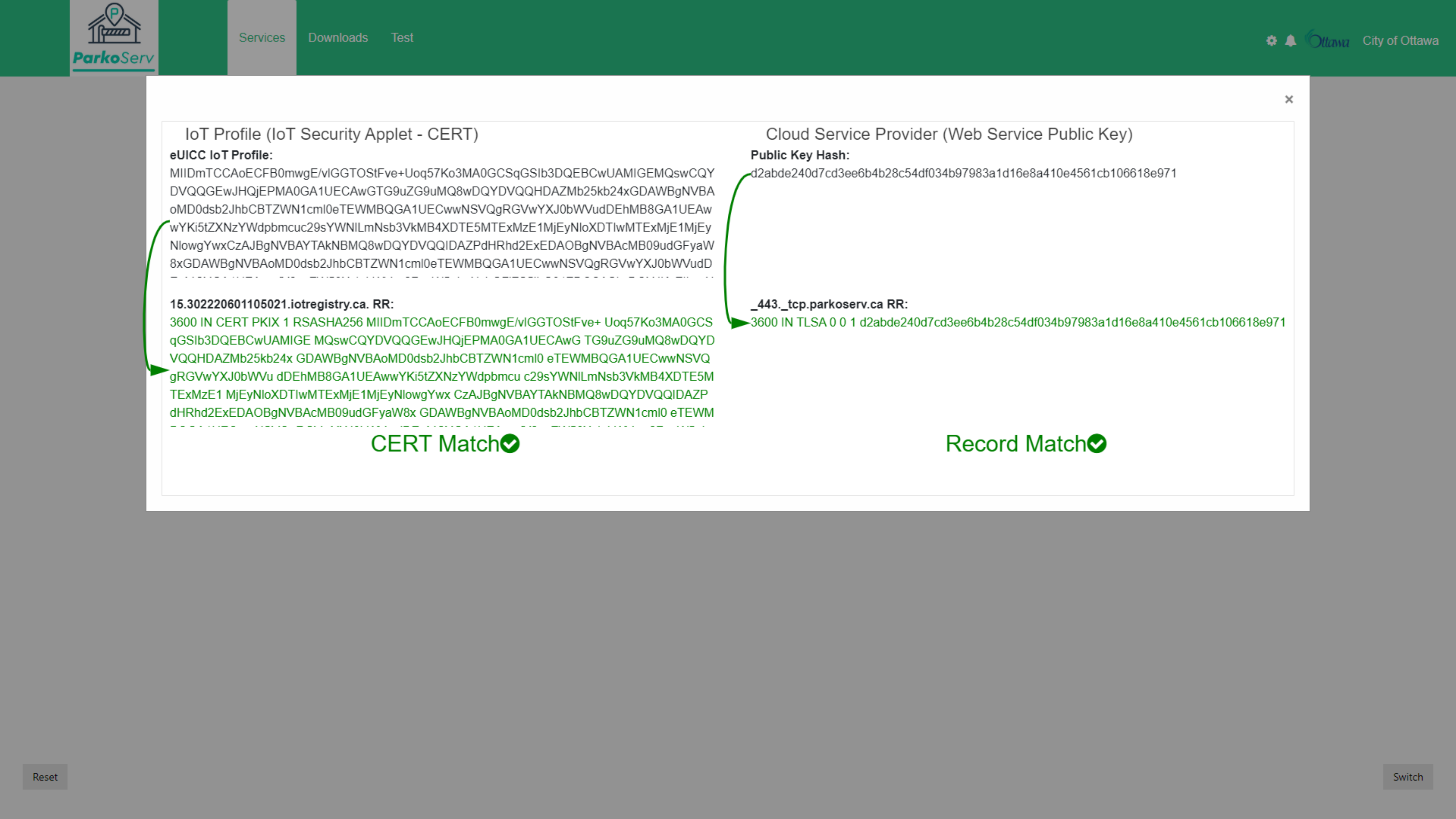
- Trusted and Secure TLS/DTLS Connection

Provides:

- Status

Provides :

- Certificate authenticity of IoT device certificate and ParkoServ cloud services Server certificate



IoT Profile (IoT Security Applet - CERT)

eUICC IoT Profile:

```
MIIDmTCCAoECFB0mwgE/vlGGTOStFve+Uoq57Ko3MA0GCSqGSIb3DQEBCwUAMIGEMQswCQY
DVQQGEwJHQjEPMA0GA1UECAwGTG9uZG9uMQ8wDQYDVQQHDAZMb25kb24xGDAWBgNVBA
oMD0dsb2JhbCBTZWN1cml0eTEWMBQGA1UECwwNSVQgRGVwYXJ0bWVudDEhMB8GA1UEAw
wYKi5tZXNzYWdpbmcuc29sYWNlLmNsb3VkMB4XDTE5MTExMzE1MjEyNloXDTIwMTExMjE1MjEy
NlowgYwxCzAJBgNVBAYTAkNBMQ8wDQYDVQQIDAZPdHRhd2ExEDAOBgNVBAcMB09udGFyaW
8xGDAWBgNVBAoMD0dsb2JhbCBTZWN1cml0eTEWMBQGA1UECwwNSVQgRGVwYXJ0bWVudD
```

15.302220601105021.iotregistry.ca. RR:

```
3600 IN CERT PKIX 1 RSASHA256 MIIDmTCCAoECFB0mwgE/vlGGTOStFve+ Uoq57Ko3MA0GCS
qGSIb3DQEBCwUAMIGE MQswCQYDVQQGEwJHQjEPMA0GA1UECAwG TG9uZG9uMQ8wDQYD
VQQHDAZMb25kb24x GDAWBgNVBAoMD0dsb2JhbCBTZWN1cml0 eTEWMBQGA1UECwwNSVQ
gRGVwYXJ0bWVu dDEhMB8GA1UEAwwYKi5tZXNzYWdpbmcu c29sYWNlLmNsb3VkMB4XDTE5M
TExMzE1 MjEyNloXDTIwMTExMjE1MjEyNlowgYwx CzAJBgNVBAYTAkNBMQ8wDQYDVQQIDAZP
dHRhd2ExEDAOBgNVBAcMB09udGFyaW8x GDAWBgNVBAoMD0dsb2JhbCBTZWN1cml0 eTEWM
```

CERT Match✓

Cloud Service Provider (Web Service Public Key)

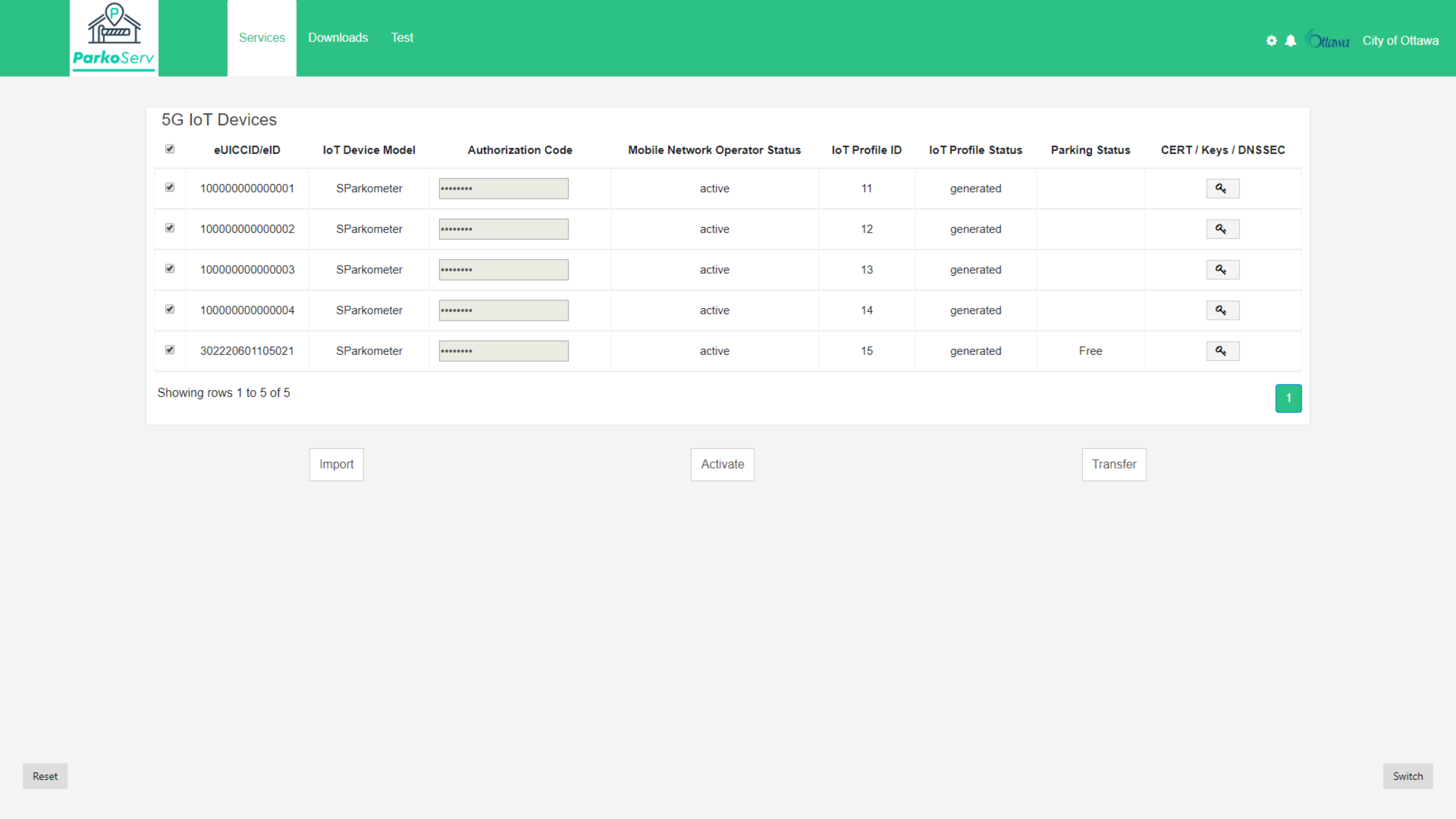
Public Key Hash:

```
d2abde240d7cd3ee6b4b28c54df034b97983a1d16e8a410e4561cb106618e971
```

_443._tcp.parkoserv.ca RR:

```
3600 IN TLSA 0 0 1 d2abde240d7cd3ee6b4b28c54df034b97983a1d16e8a410e4561cb106618e971
```

Record Match✓



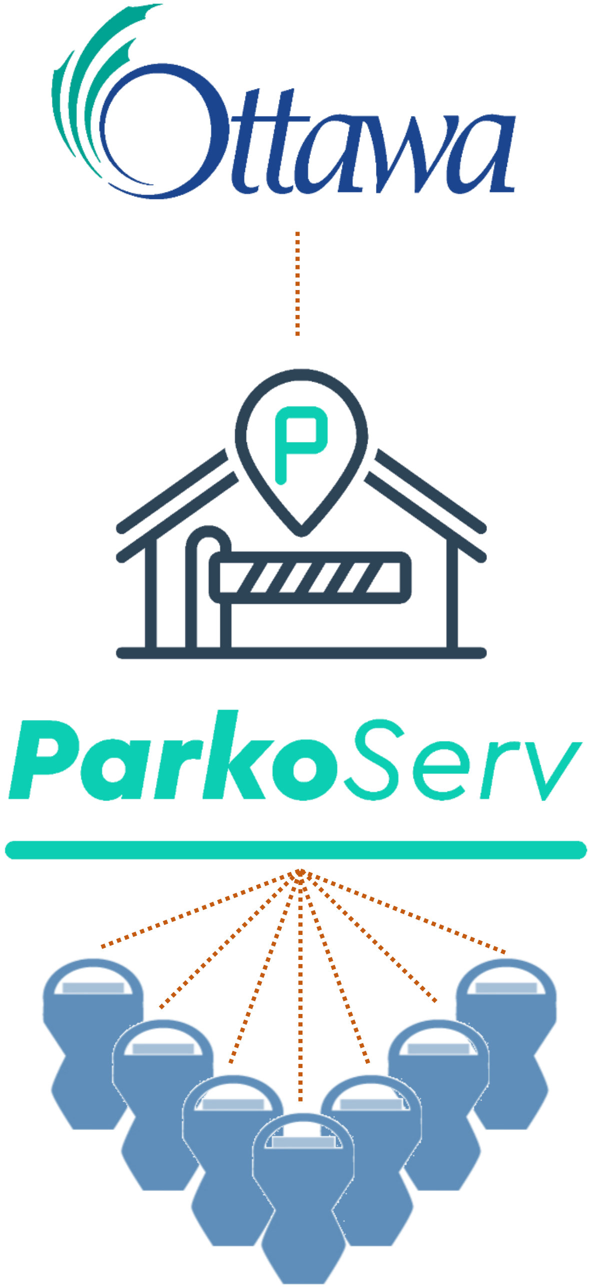
5G IoT Devices

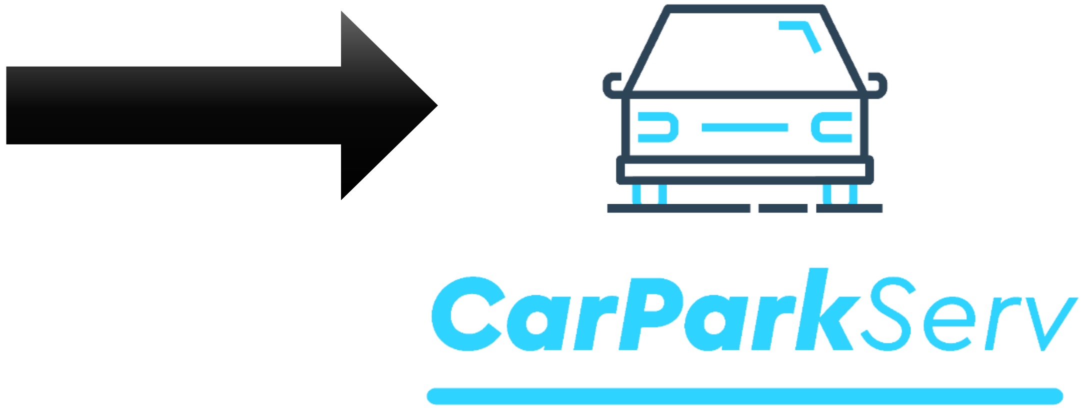
☑	eUICCID/eID	IoT Device Model	Authorization Code	Mobile Network Operator Status	IoT Profile ID	IoT Profile Status	Parking Status	CERT / Keys / DNSSEC
☑	100000000000001	SParkometer	••••••••	active	11	generated		🔑
☑	100000000000002	SParkometer	••••••••	active	12	generated		🔑
☑	100000000000003	SParkometer	••••••••	active	13	generated		🔑
☑	100000000000004	SParkometer	••••••••	active	14	generated		🔑
☑	302220601105021	SParkometer	••••••••	active	15	generated	Free	🔑

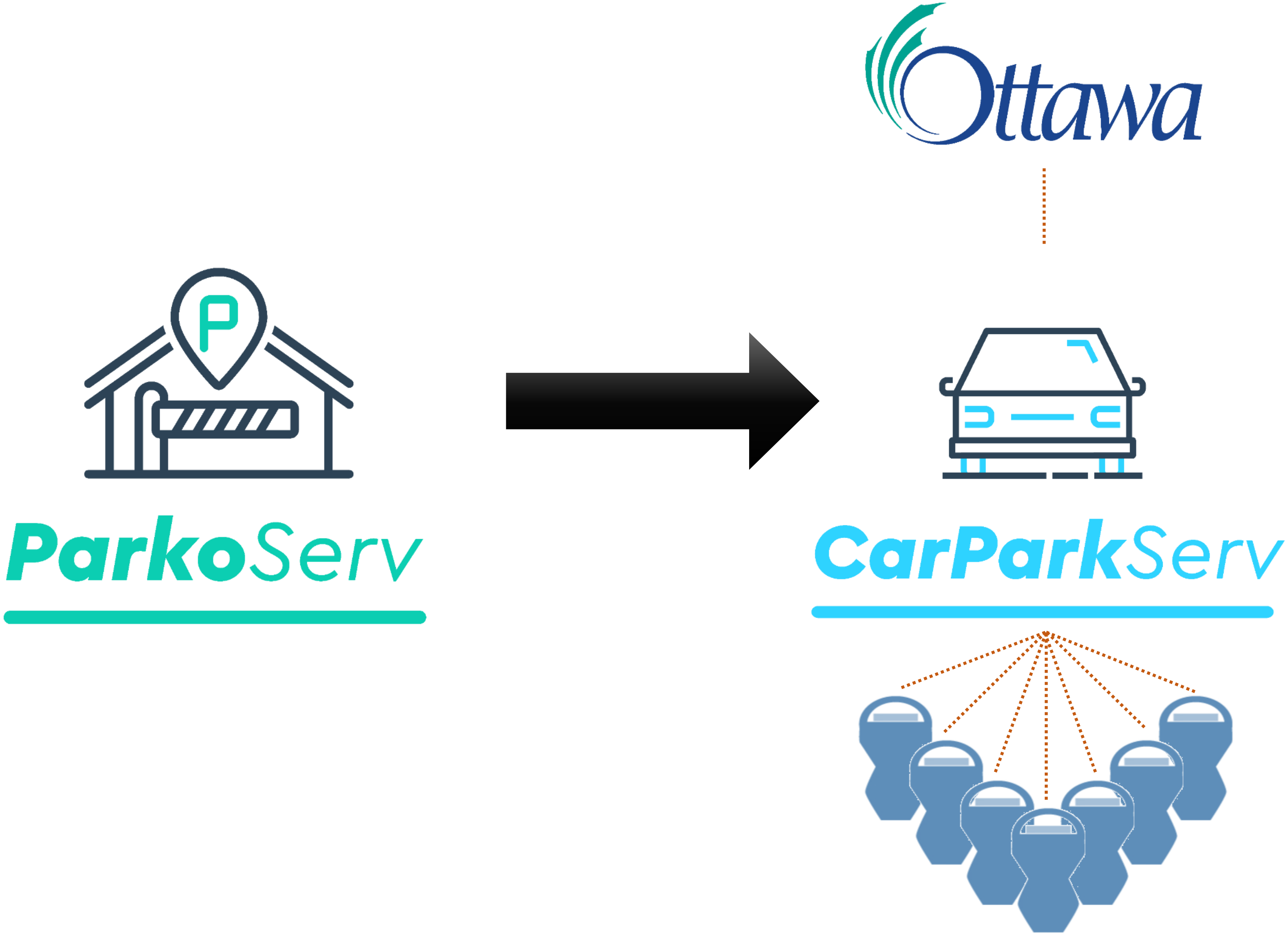
Showing rows 1 to 5 of 5

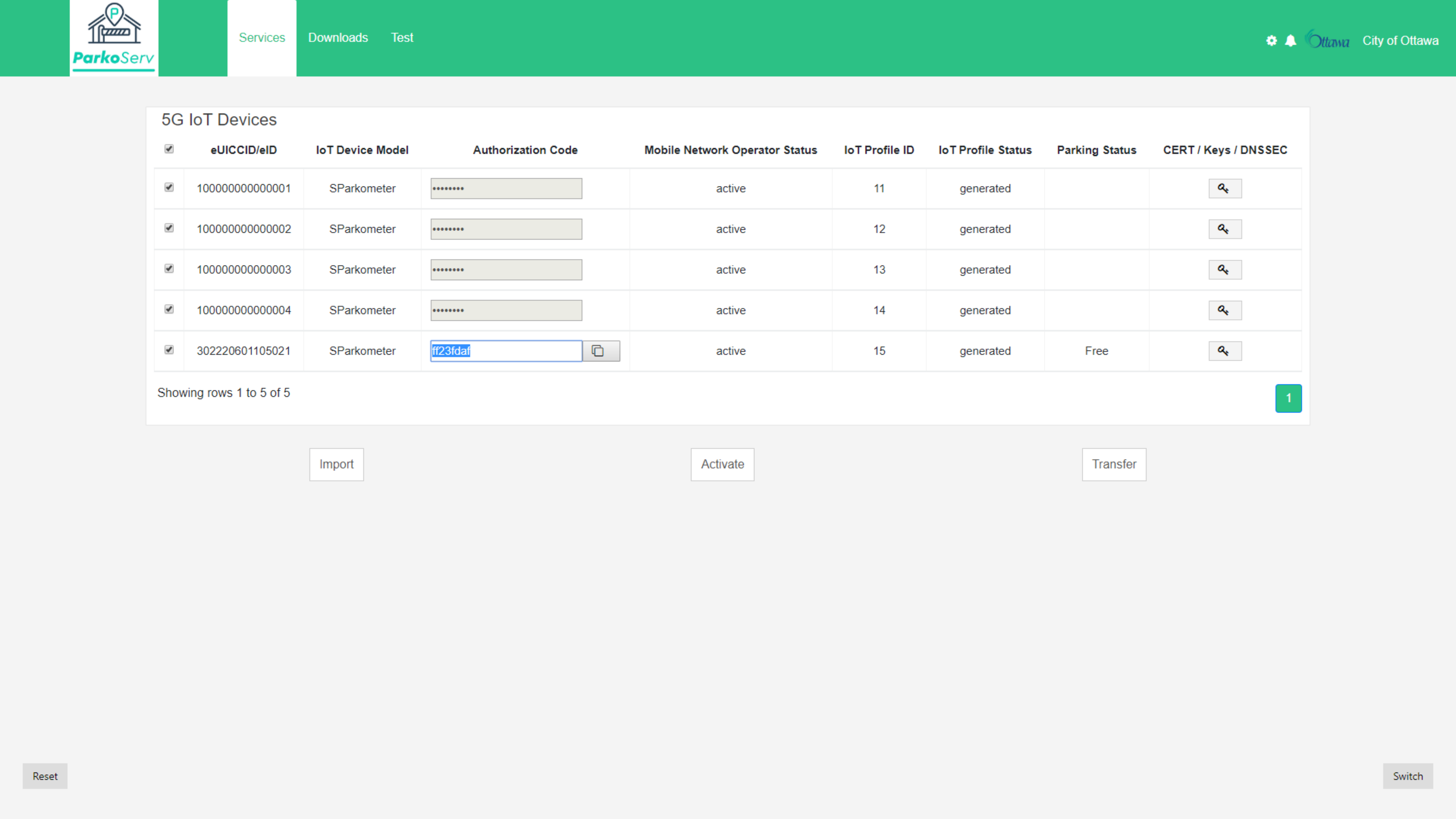
1

THE CITY OF OTTAWA CHANGES THEIR PARKING CLOUD PROVIDER






Ottawa
ParkoServ
CarParkServ



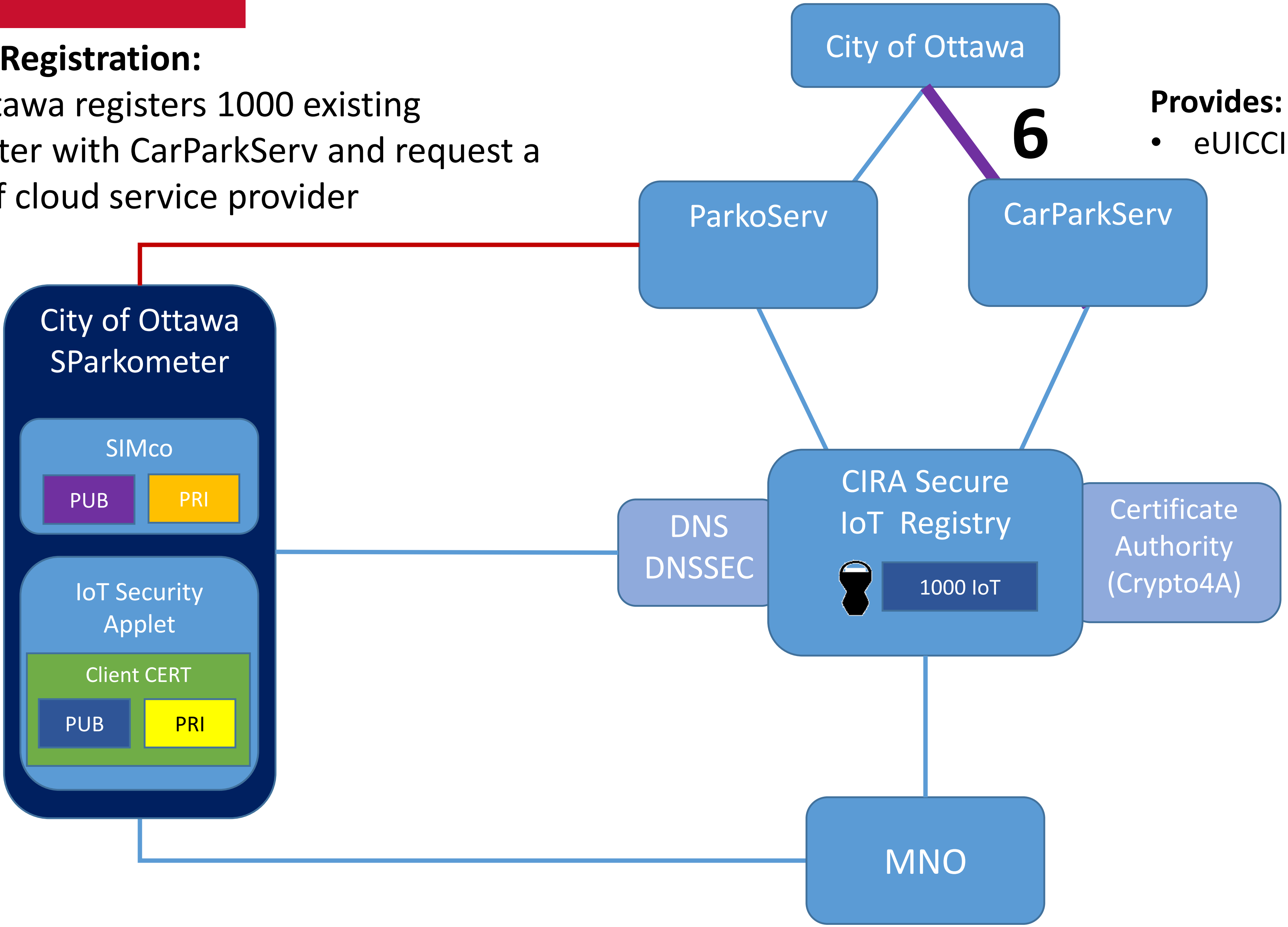
5G IoT Devices

☑	eUICCID/eID	IoT Device Model	Authorization Code	Mobile Network Operator Status	IoT Profile ID	IoT Profile Status	Parking Status	CERT / Keys / DNSSEC
☑	100000000000001	SParkometer	••••••••	active	11	generated		🔑
☑	100000000000002	SParkometer	••••••••	active	12	generated		🔑
☑	100000000000003	SParkometer	••••••••	active	13	generated		🔑
☑	100000000000004	SParkometer	••••••••	active	14	generated		🔑
☑	302220601105021	SParkometer	ff23fdaf	active	15	generated	Free	🔑

Showing rows 1 to 5 of 5

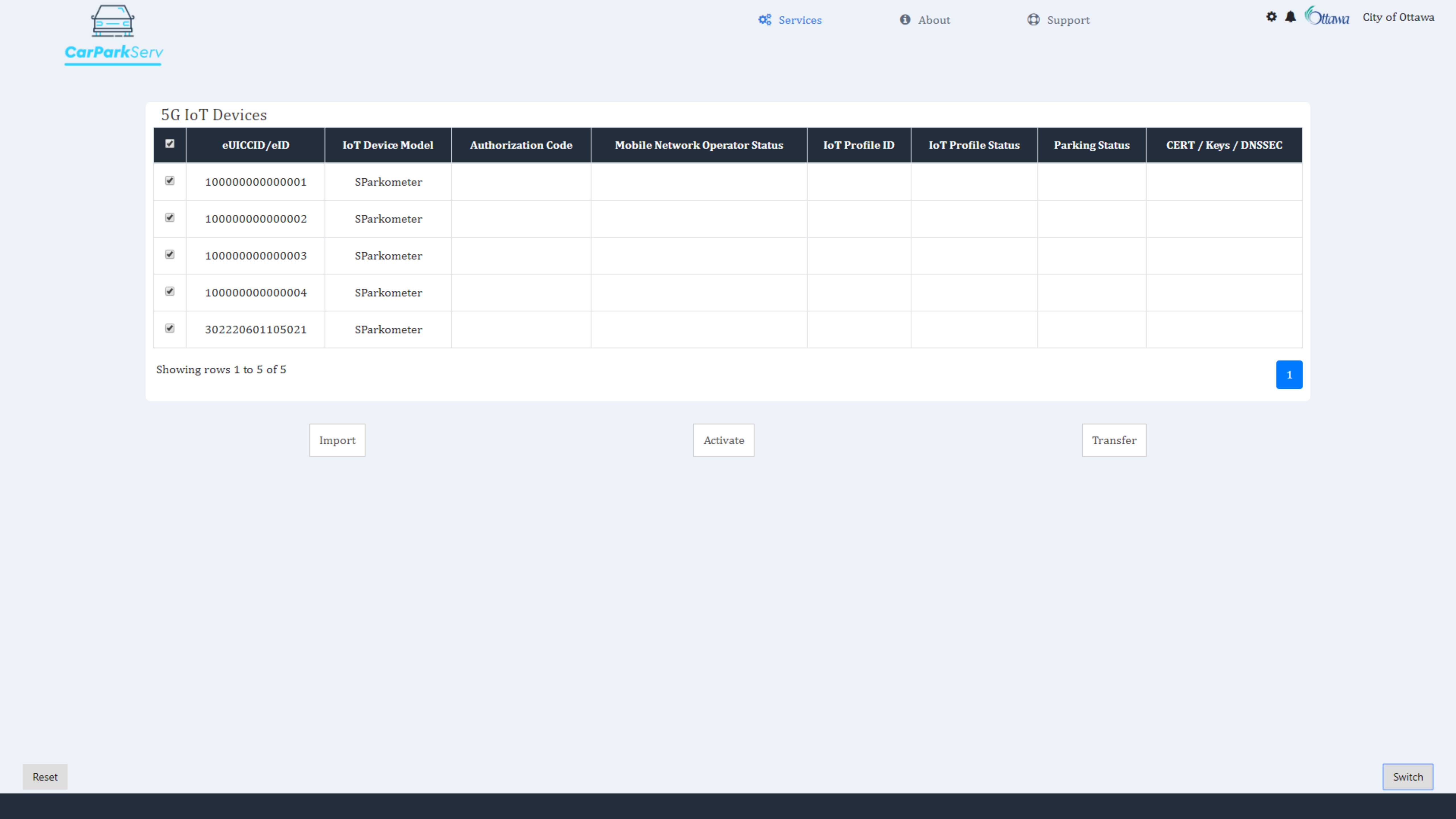
6 – Cloud Registration:

City of Ottawa registers 1000 existing SParkometer with CarParkServ and request a transfer of cloud service provider



Provides:

- eUICCID/eID, public keys

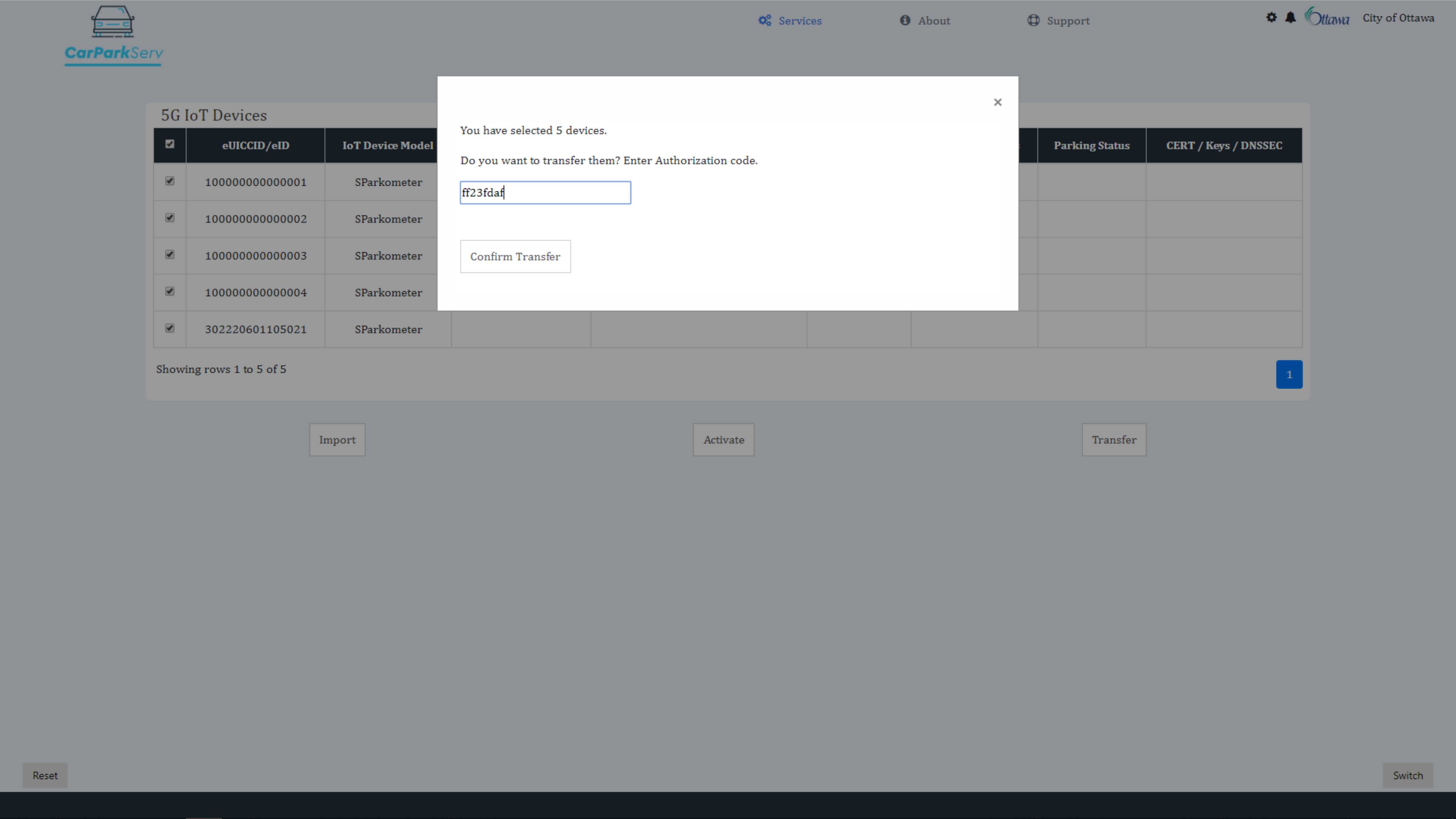


5G IoT Devices

☑	eUICCID/eID	IoT Device Model	Authorization Code	Mobile Network Operator Status	IoT Profile ID	IoT Profile Status	Parking Status	CERT / Keys / DNSSEC
☑	100000000000001	SParkometer						
☑	100000000000002	SParkometer						
☑	100000000000003	SParkometer						
☑	100000000000004	SParkometer						
☑	302220601105021	SParkometer						

Showing rows 1 to 5 of 5

1



5G IoT Devices

☑	eUICCID/eID	IoT Device Model	Parking Status	CERT / Keys / DNSSEC
☑	100000000000001	SParkometer		
☑	100000000000002	SParkometer		
☑	100000000000003	SParkometer		
☑	100000000000004	SParkometer		
☑	302220601105021	SParkometer		

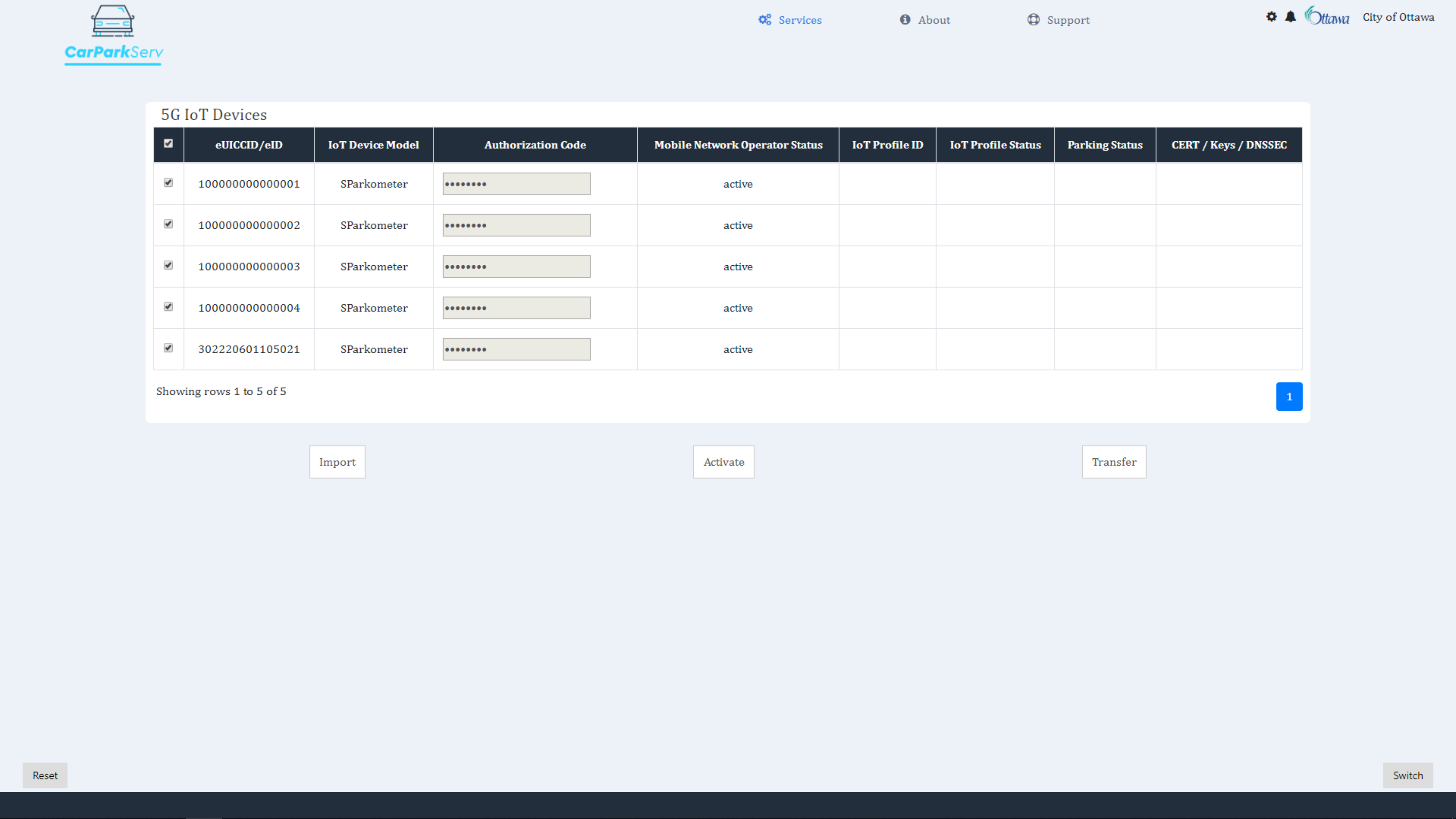
Showing rows 1 to 5 of 5

×

You have selected 5 devices.

Do you want to transfer them? Enter Authorization code.

ff23fdaf

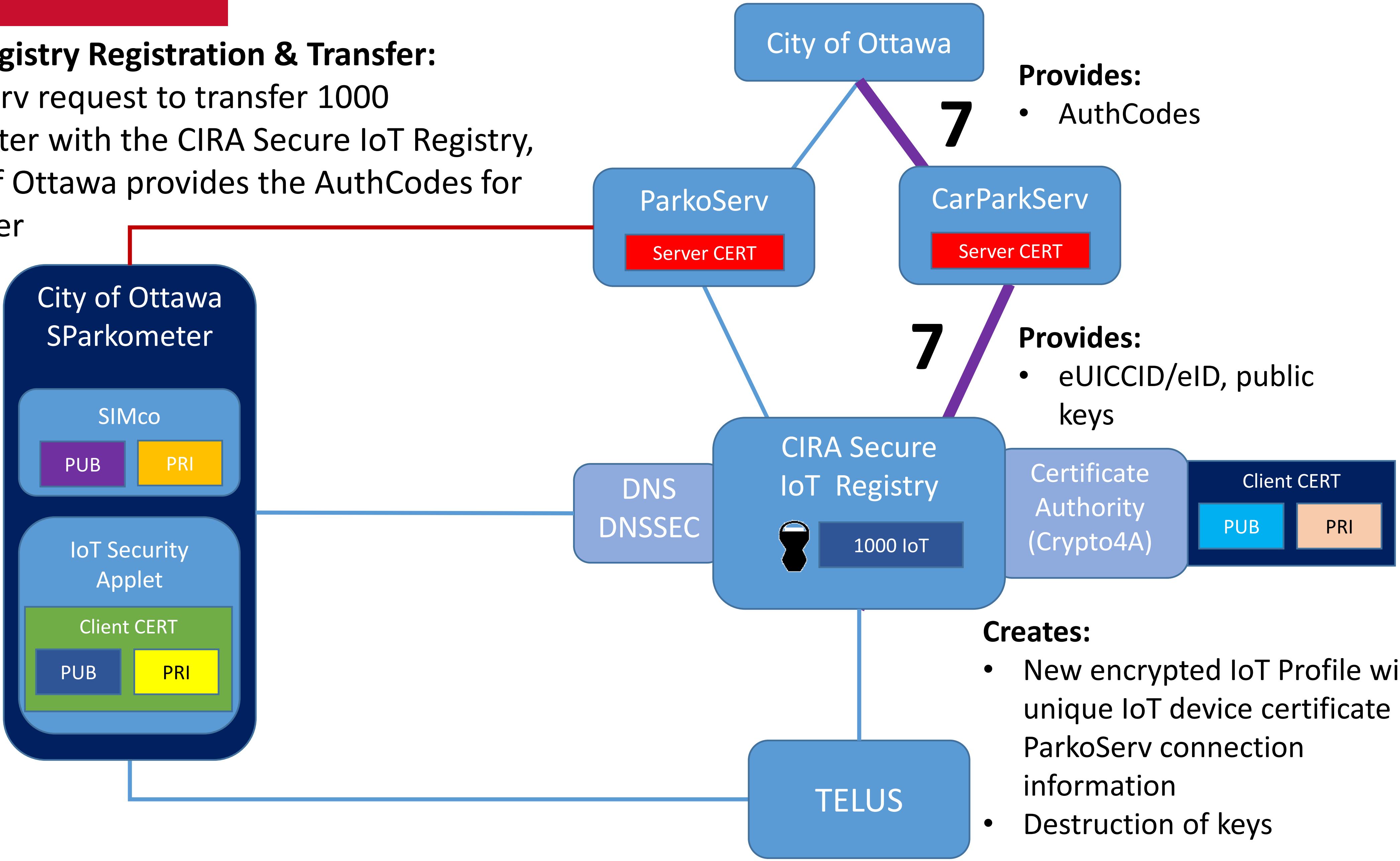


5G IoT Devices

☑	eUICCID/eID	IoT Device Model	Authorization Code	Mobile Network Operator Status	IoT Profile ID	IoT Profile Status	Parking Status	CERT / Keys / DNSSEC
☑	100000000000001	SParkometer	••••••••	active				
☑	100000000000002	SParkometer	••••••••	active				
☑	100000000000003	SParkometer	••••••••	active				
☑	100000000000004	SParkometer	••••••••	active				
☑	302220601105021	SParkometer	••••••••	active				

Showing rows 1 to 5 of 5

7 – IoT Registry Registration & Transfer:
CarParkServ request to transfer 1000 SParkometer with the CIRA Secure IoT Registry, the City of Ottawa provides the AuthCodes for the transfer



Provides:

- AuthCodes

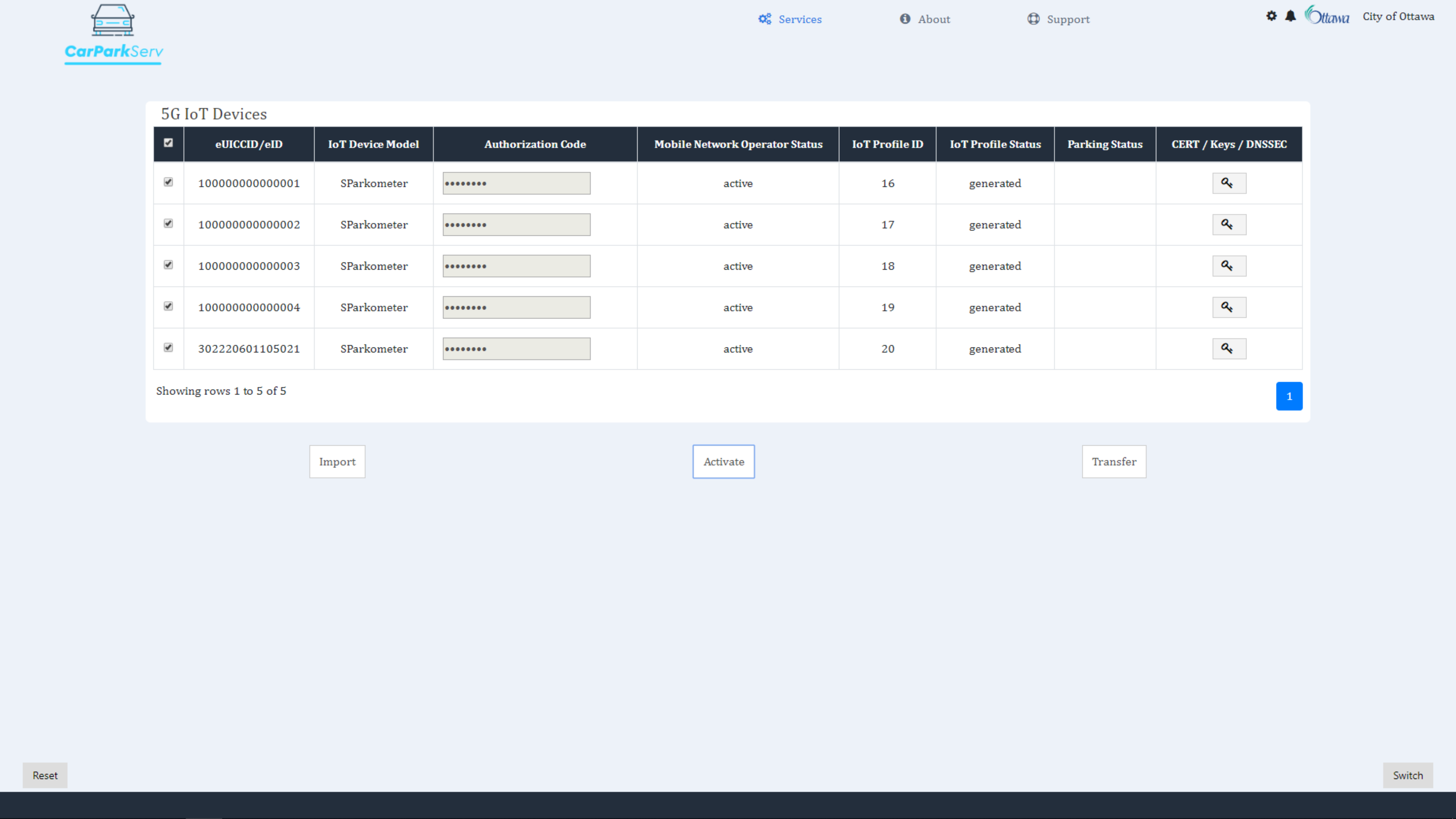
Provides:

- eUICCID/eID, public keys

Creates:

- New encrypted IoT Profile with unique IoT device certificate and ParkoServ connection information
- Destruction of keys

CIRA'S IOT REGISTRY



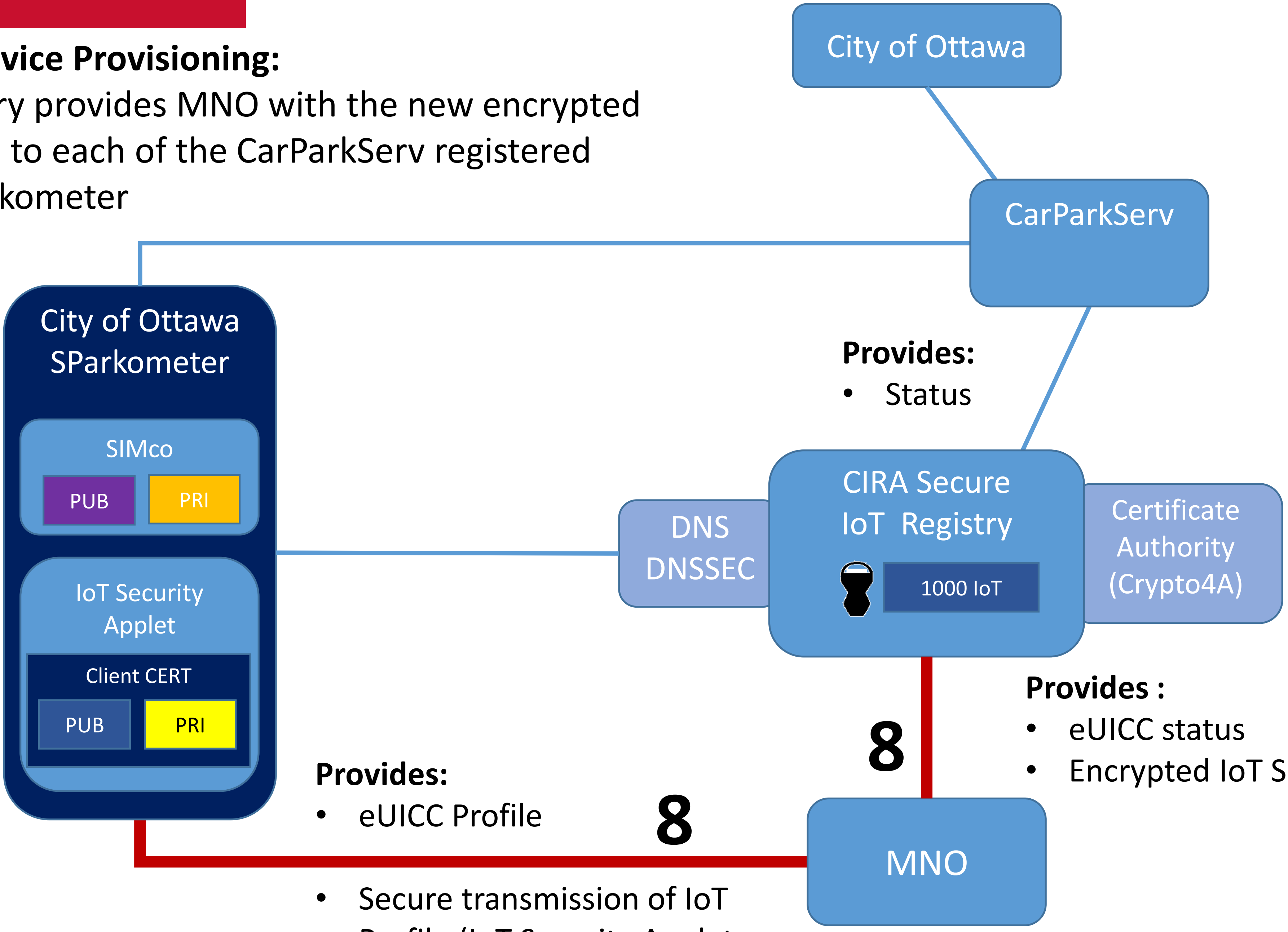
5G IoT Devices

☑	eUICCID/eID	IoT Device Model	Authorization Code	Mobile Network Operator Status	IoT Profile ID	IoT Profile Status	Parking Status	CERT / Keys / DNSSEC
☑	100000000000001	SParkometer	••••••••	active	16	generated		🔑
☑	100000000000002	SParkometer	••••••••	active	17	generated		🔑
☑	100000000000003	SParkometer	••••••••	active	18	generated		🔑
☑	100000000000004	SParkometer	••••••••	active	19	generated		🔑
☑	302220601105021	SParkometer	••••••••	active	20	generated		🔑

Showing rows 1 to 5 of 5

8 – IoT Device Provisioning:

IoT Registry provides MNO with the new encrypted IoT Profile to each of the CarParkServ registered 1000 SParkometer



Provides:

- Status

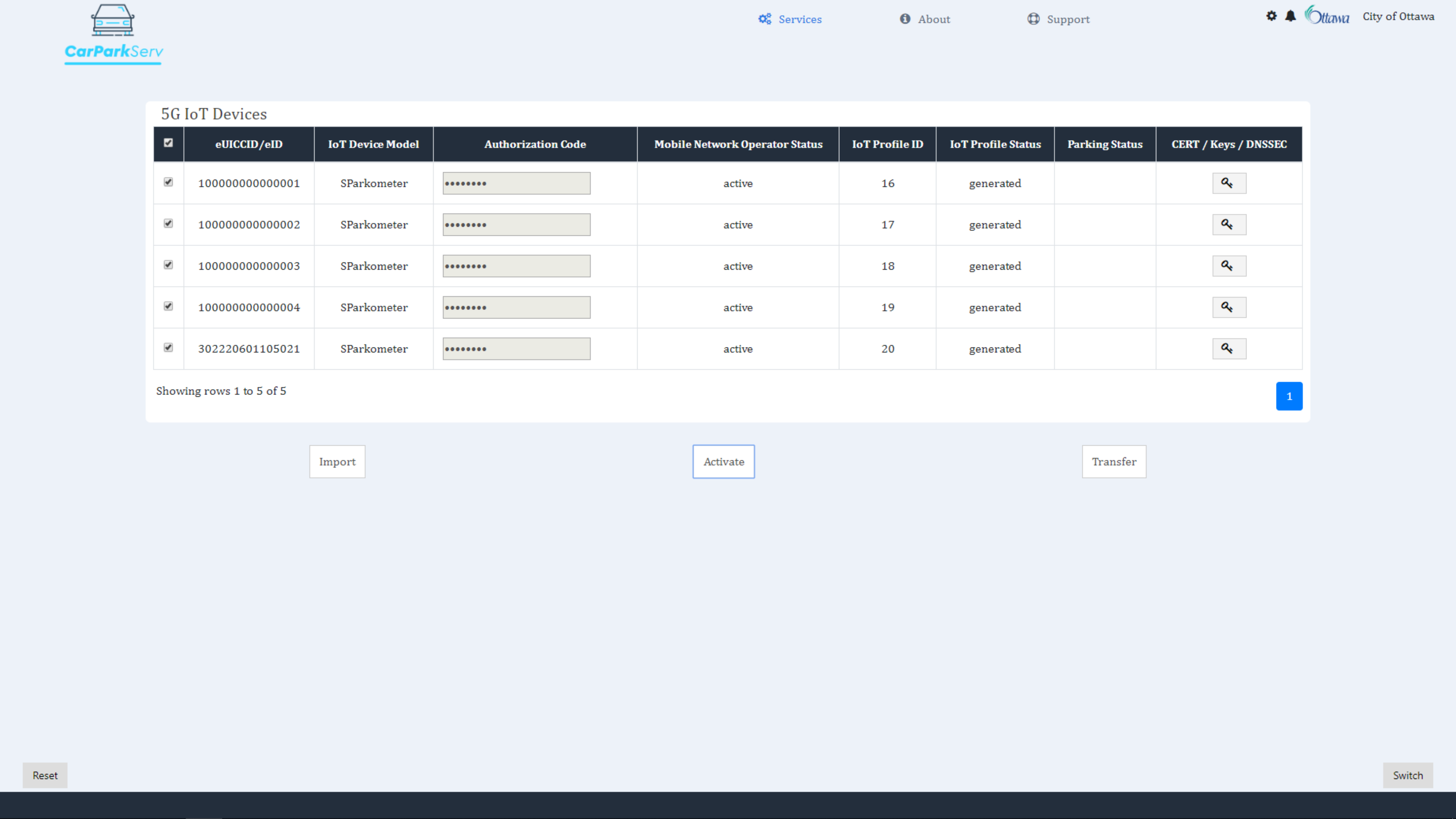
Provides :

- eUICC status
- Encrypted IoT Security Applet

Provides:

- eUICC Profile
- Secure transmission of IoT Profile (IoT Security Applet containing Client Cert + info)

CIRA'S IOT REGISTRY



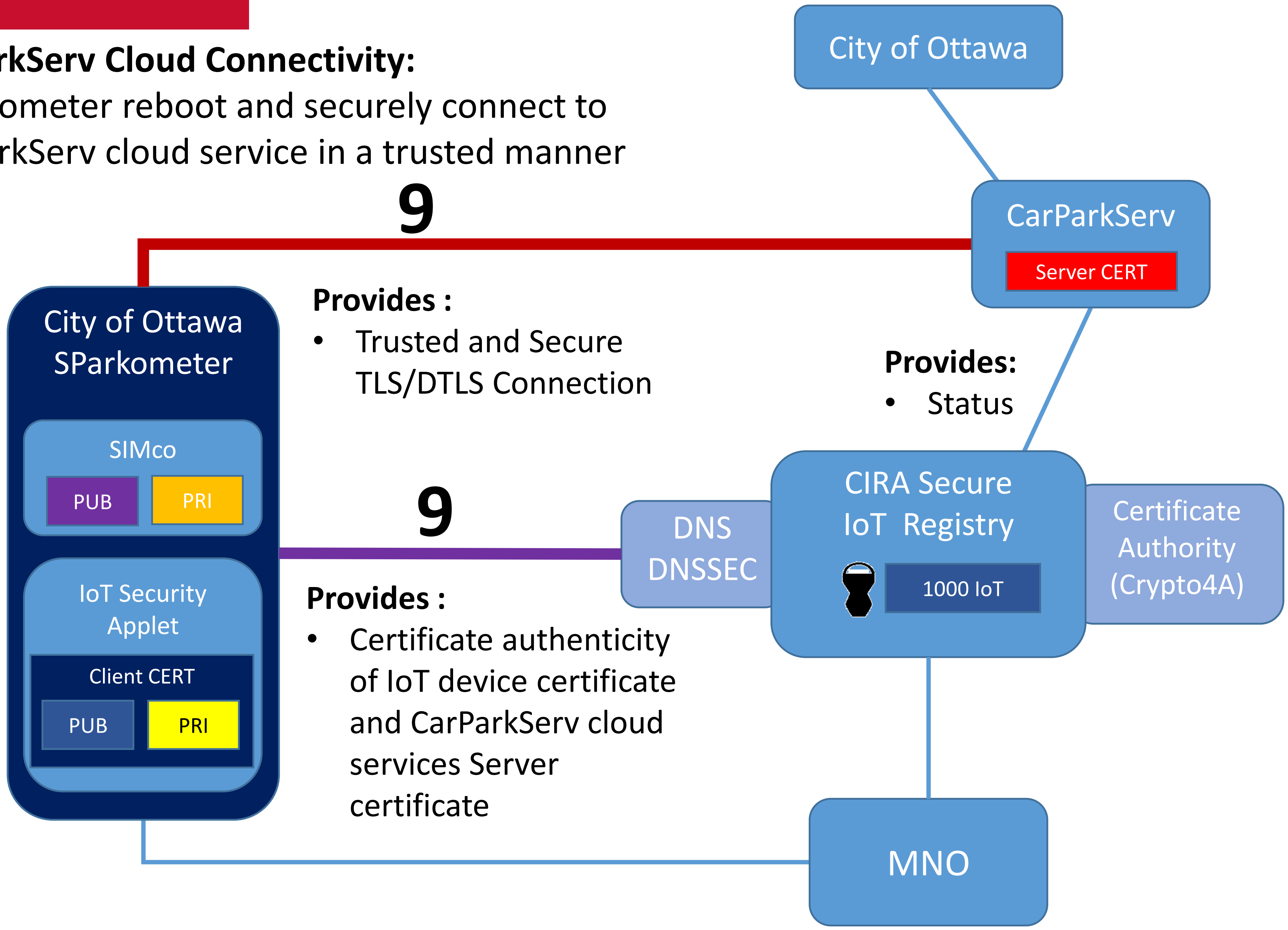
5G IoT Devices

☑	eUICCID/eID	IoT Device Model	Authorization Code	Mobile Network Operator Status	IoT Profile ID	IoT Profile Status	Parking Status	CERT / Keys / DNSSEC
☑	100000000000001	SParkometer	••••••••	active	16	generated		🔑
☑	100000000000002	SParkometer	••••••••	active	17	generated		🔑
☑	100000000000003	SParkometer	••••••••	active	18	generated		🔑
☑	100000000000004	SParkometer	••••••••	active	19	generated		🔑
☑	302220601105021	SParkometer	••••••••	active	20	generated		🔑

Showing rows 1 to 5 of 5

9 – CarParkServ Cloud Connectivity:

The SParkometer reboot and securely connect to the CarParkServ cloud service in a trusted manner



Provides :

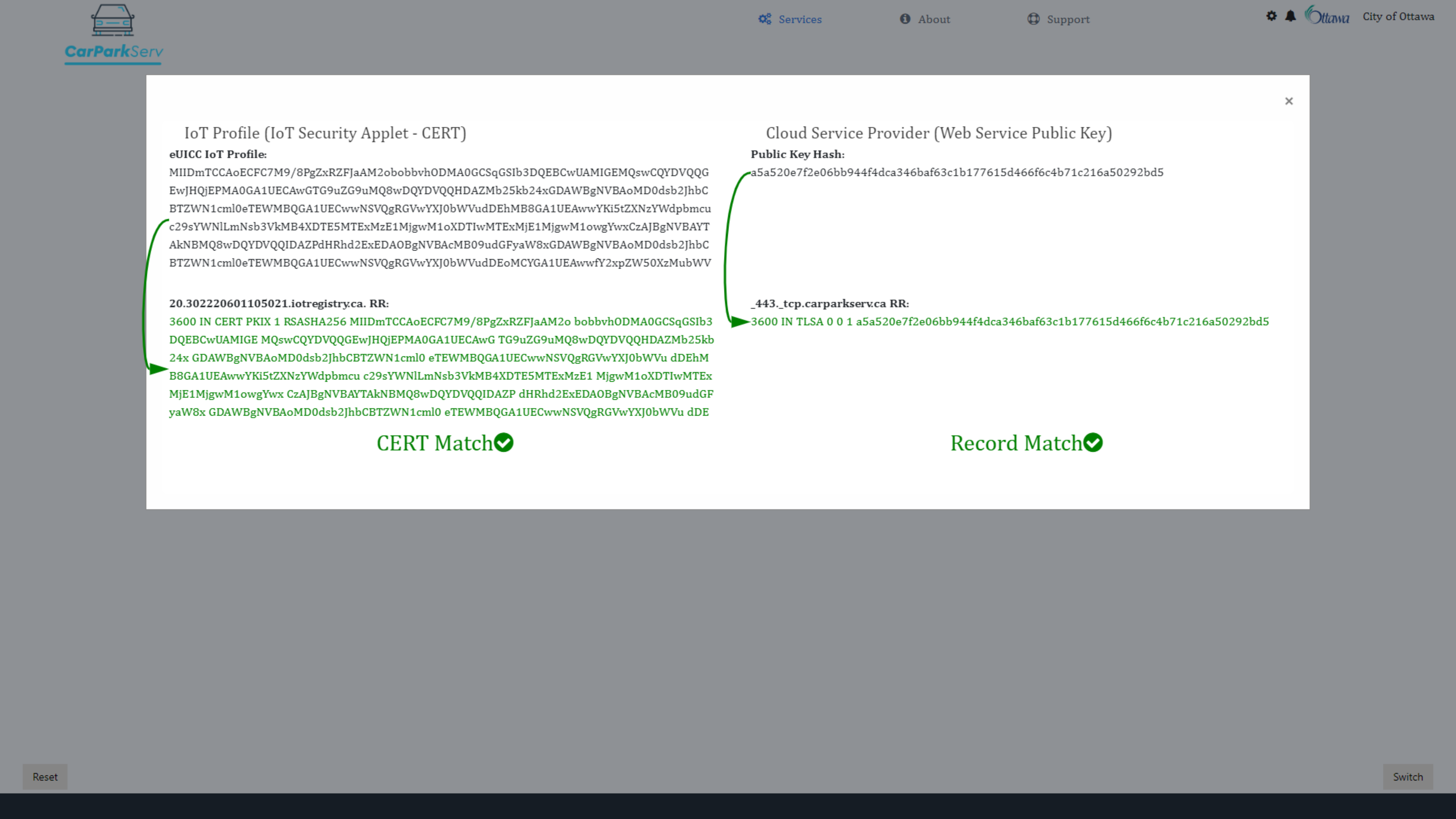
- Trusted and Secure TLS/DTLS Connection

Provides:

- Status

Provides :

- Certificate authenticity of IoT device certificate and CarParkServ cloud services Server certificate



IoT Profile (IoT Security Applet - CERT)

eUICC IoT Profile:

```
MIIDmTCCAoECFC7M9/8PgZxRZFJaAM2obobbvhODMA0GCSqGSIb3DQEBCwUAMIGEMQswCQYDVQQG
EwJHQjEPMA0GA1UECAwGTG9uZG9uMQ8wDQYDVQQHDAZMb25kb24xGDAWBgNVBAoMD0dsb2JhbC
BTZWN1cml0eTEWMBQGA1UECwwNSVQgRGVwYXJ0bWVudDEhMB8GA1UEAwwYKi5tZXNzYWdpbmcu
c29sYWNlLmNsb3VkMB4XDTE5MTExMzE1MjgwM1oXDTIwMTExMjE1MjgwM1owgYwxCzAJBgNVBAYT
AkNBMQ8wDQYDVQQIDAZPdHRhd2ExEDAOBgNVBAcMB09udGFyaW8xGDAWBgNVBAoMD0dsb2JhbC
BTZWN1cml0eTEWMBQGA1UECwwNSVQgRGVwYXJ0bWVudDEoMCYGA1UEAwwfY2xpZW50XzMubWV
```

20.302220601105021.iotregistry.ca. RR:

```
3600 IN CERT PKIX 1 RSASHA256 MIIDmTCCAoECFC7M9/8PgZxRZFJaAM2o bobbvhODMA0GCSqGSIb3
DQEBCwUAMIGE MQswCQYDVQQGEwJHQjEPMA0GA1UECAwG TG9uZG9uMQ8wDQYDVQQHDAZMb25kb
24x GDAWBgNVBAoMD0dsb2JhbCBTZWN1cml0 eTEWMBQGA1UECwwNSVQgRGVwYXJ0bWVu dDEhM
B8GA1UEAwwYKi5tZXNzYWdpbmcu c29sYWNlLmNsb3VkMB4XDTE5MTExMzE1 MjgwM1oXDTIwMTEx
MjE1MjgwM1owgYwx CzAJBgNVBAYTAkNBMQ8wDQYDVQQIDAZP dHRhd2ExEDAOBgNVBAcMB09udGF
yaW8x GDAWBgNVBAoMD0dsb2JhbCBTZWN1cml0 eTEWMBQGA1UECwwNSVQgRGVwYXJ0bWVu dDE
```

CERT Match✓

Cloud Service Provider (Web Service Public Key)

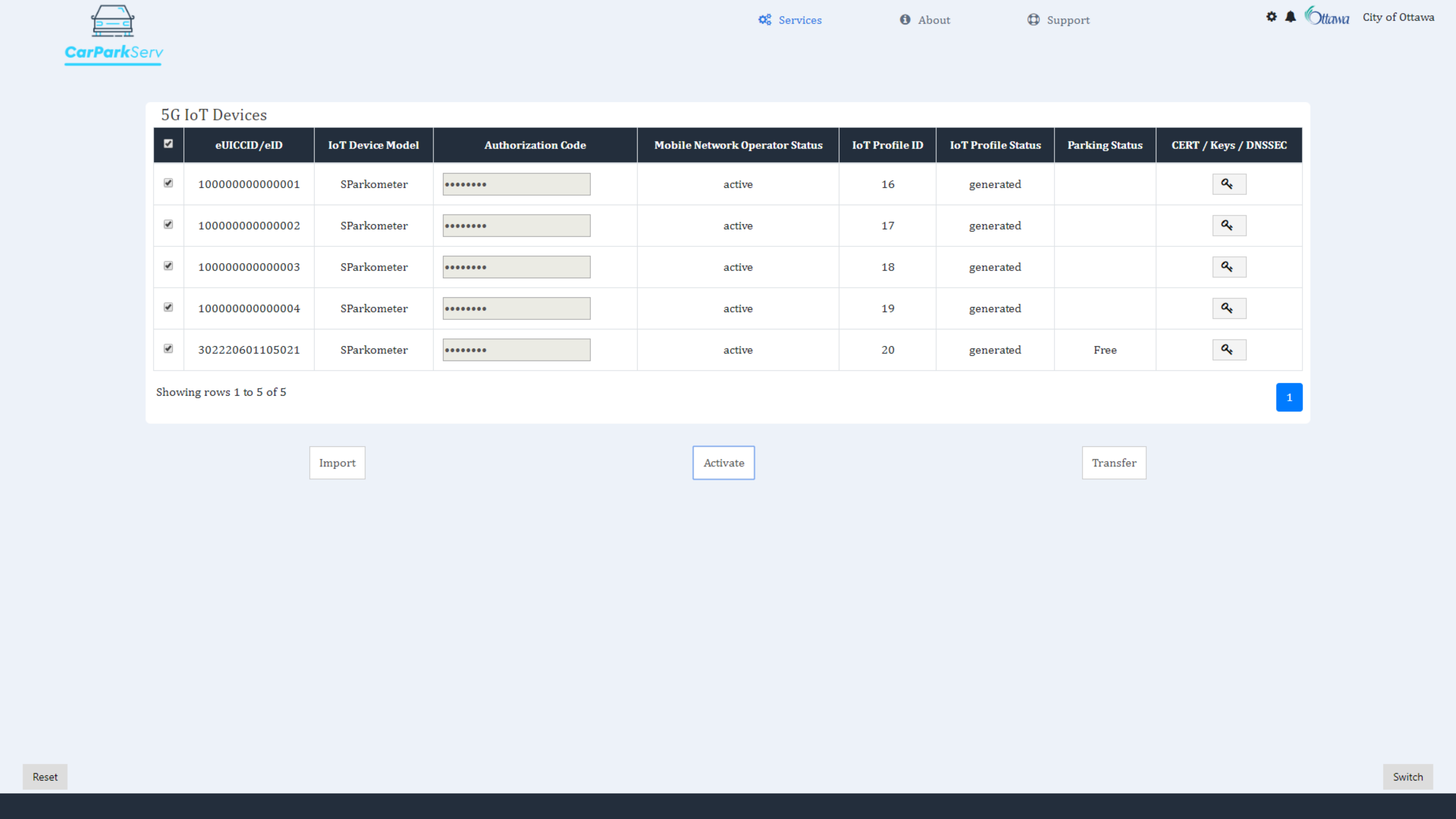
Public Key Hash:

a5a520e7f2e06bb944f4dca346baf63c1b177615d466f6c4b71c216a50292bd5

_443._tcp.carparkserv.ca RR:

3600 IN TLSA 0 0 1 a5a520e7f2e06bb944f4dca346baf63c1b177615d466f6c4b71c216a50292bd5

Record Match✓

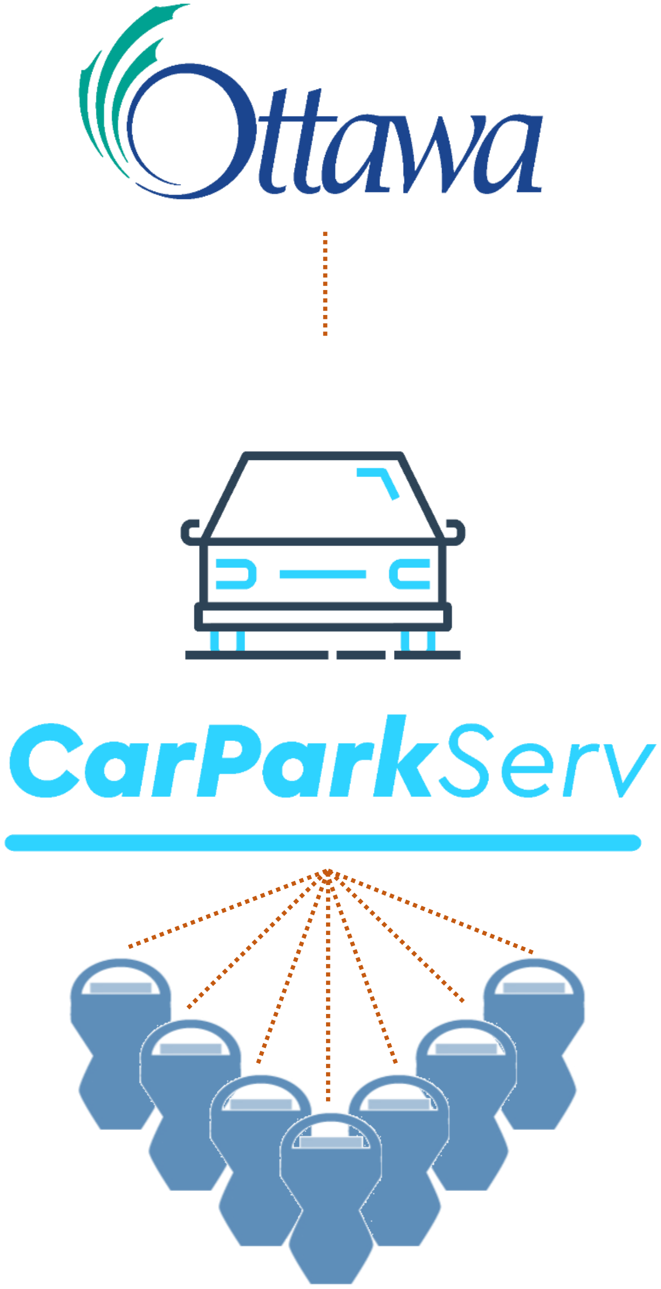


5G IoT Devices

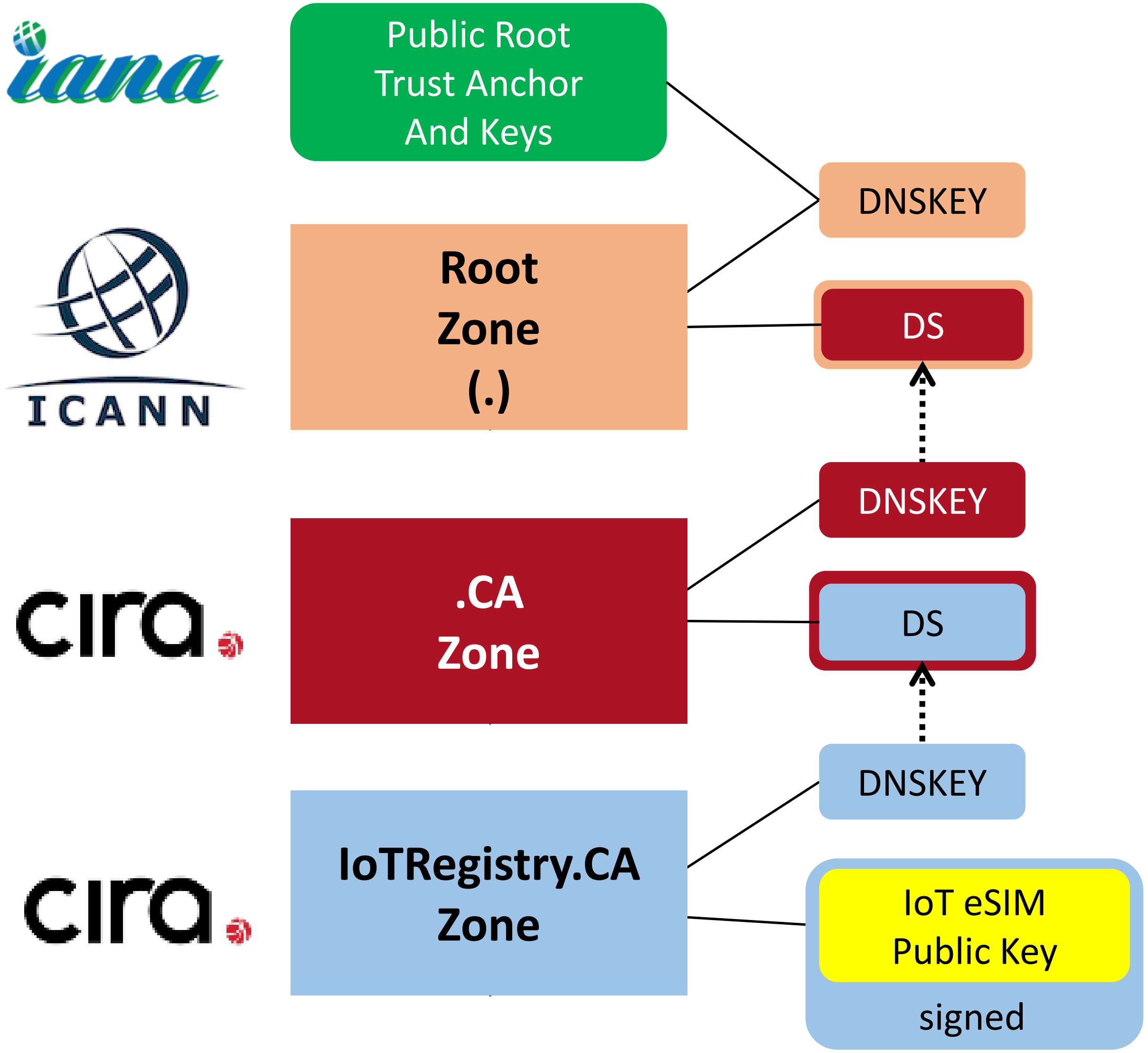
☑	eUICCID/eID	IoT Device Model	Authorization Code	Mobile Network Operator Status	IoT Profile ID	IoT Profile Status	Parking Status	CERT / Keys / DNSSEC
☑	100000000000001	SParkometer	••••••••	active	16	generated		🔑
☑	100000000000002	SParkometer	••••••••	active	17	generated		🔑
☑	100000000000003	SParkometer	••••••••	active	18	generated		🔑
☑	100000000000004	SParkometer	••••••••	active	19	generated		🔑
☑	302220601105021	SParkometer	••••••••	active	20	generated	Free	🔑

Showing rows 1 to 5 of 5

AND VOILA, WITH ZERO TOUCH, THE CITY OF OTTAWA HAS CHANGED CLOUD SERVICE PROVIDER SEAMLESSLY FOR A 1000 SMART PARKING METERS



A NEW ROOT OF TRUST - DNSSEC



Public Root Trust Anchor And Keys

Root Zone (.)

DNSKEY

DS

.CA Zone

DNSKEY

DS

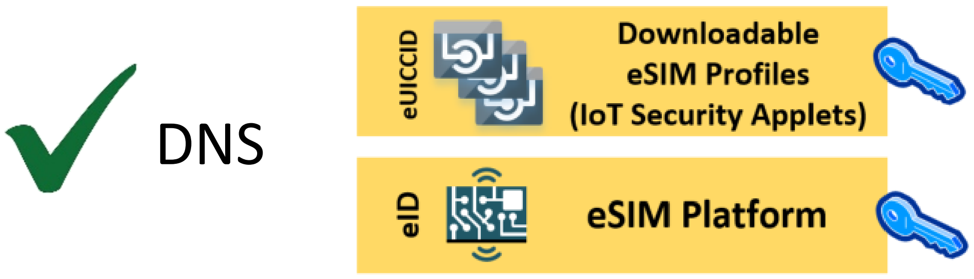
IoTRegistry.CA Zone

DNSKEY

IoT eSIM Public Key

signed

Leveraging the public DNS & DNSSEC to validate the authenticity of eSIM and IoT security applets and cloud service providers public keys



DNS

Downloadable eSIM Profiles (IoT Security Applets)

eSIM Platform

NEXT STEPS

- Standards development with GSMA and IETF
- Develop functional registry prototype
- Work with IoT Application Service Providers
- Work with IoT device builders

https://www.gsma.com/iot/iot-safe/

Thank you!

Questions?

cira
IoT REGISTRY