Introducing Tiaki - DNS-SD implementations for C and Java

Regis Piccand

November 2015

Secure Service Discovery with DNS-SD

- DNS-SD is an IETF RFC

- It specifies how DNS can be used to store and retrieve connection and configuration information about services (IoT Platform, LWM2M bootstrap server, etc.)

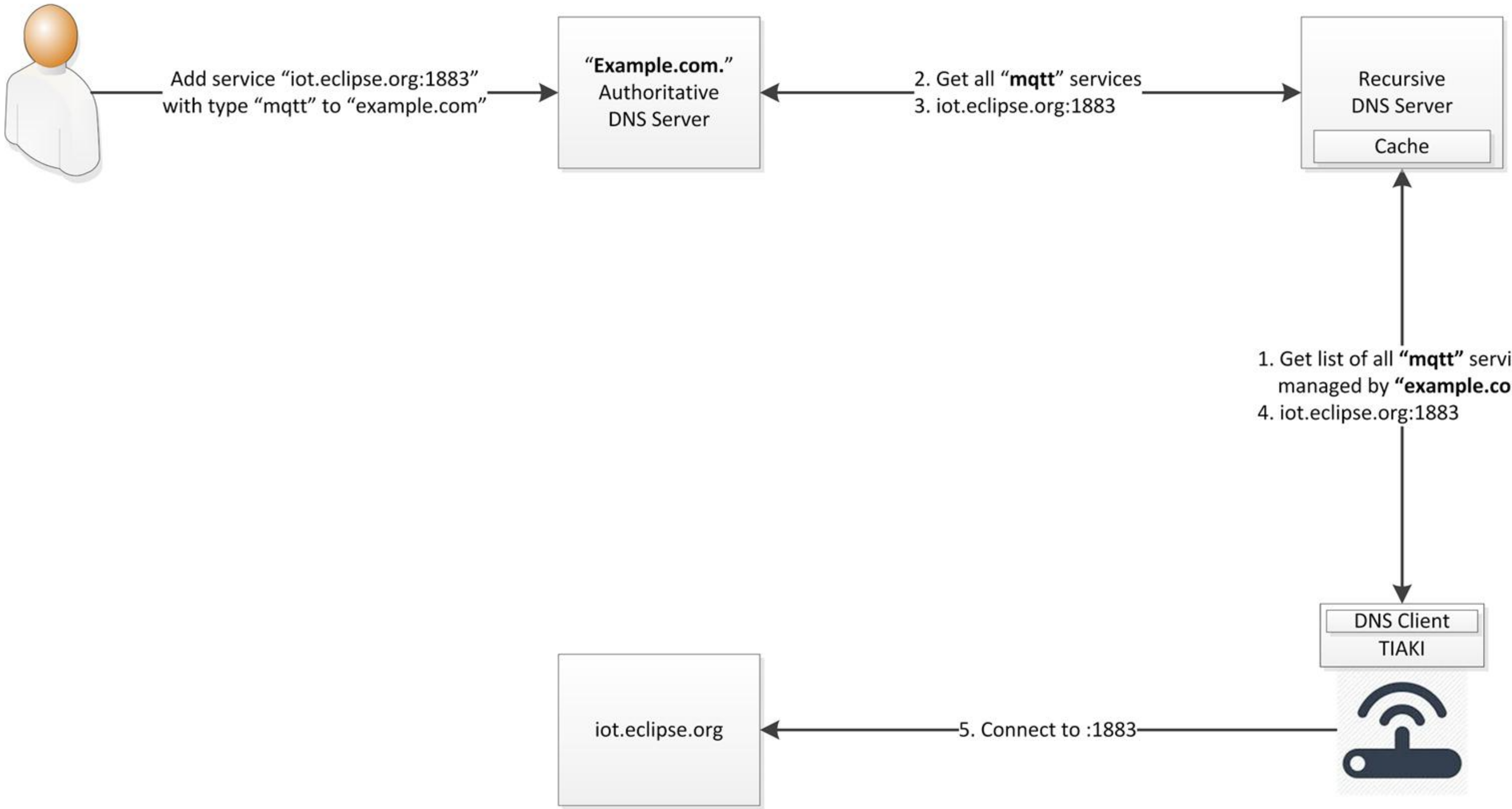
- Clients look up this information from DNS and can safely connect to the services

- The security aspect is provided by DNSSEC, another set of IETF RFCs, which specifies how to authenticate the origin of the data and its integrity

Tiaki, a DNS-SD client implementation

- Tiaki is a set of Java and C Libraries (and Command-Line wrapper) that allow clients to lookup connection and configuration information services from DNS
- Services are provisioned within a domain name (eg. example.com)
- For a given domain name, Tiaki can
  - List existing service types (MQTT, CoAP, etc.)
  - List existing services names, end points URL, ports and configuration
  - Authenticate the data and check its integrity using DNSSEC
  - Retrieve other DNS records (TLSA, TXT, etc.) for authentication or configuration purposes

DNS-based Service Discovery



Add service “iot.eclipse.org:1883” with type “mqtt” to “example.com”

“Example.com.” Authoritative DNS Server

2. Get all “**mqtt**” services
3. iot.eclipse.org:1883

Recursive DNS Server

Cache

1. Get list of all **“mqtt”** services managed by **“example.com”**
4. iot.eclipse.org:1883

DNS Client

TIAKI

iot.eclipse.org

5. Connect to :1883

Which records must be provisioned in DNS

Label	Type	RData
_services._dns-sd._udp.example.com	PTR	**_mqtt._tcp**.example.com
_mqtt._tcp.example.com	PTR	**Eclipse sandbox**._mqtt._tcp.example.com
Eclipse sandbox._mqtt._tcp.example.com	SRV	mqtt://iot.eclipse.org, 1883
Eclipse sandbox.*_mqtt._tcp.example.com*	*TXT*	*"server=Mosquitto””version=1.3.1"*

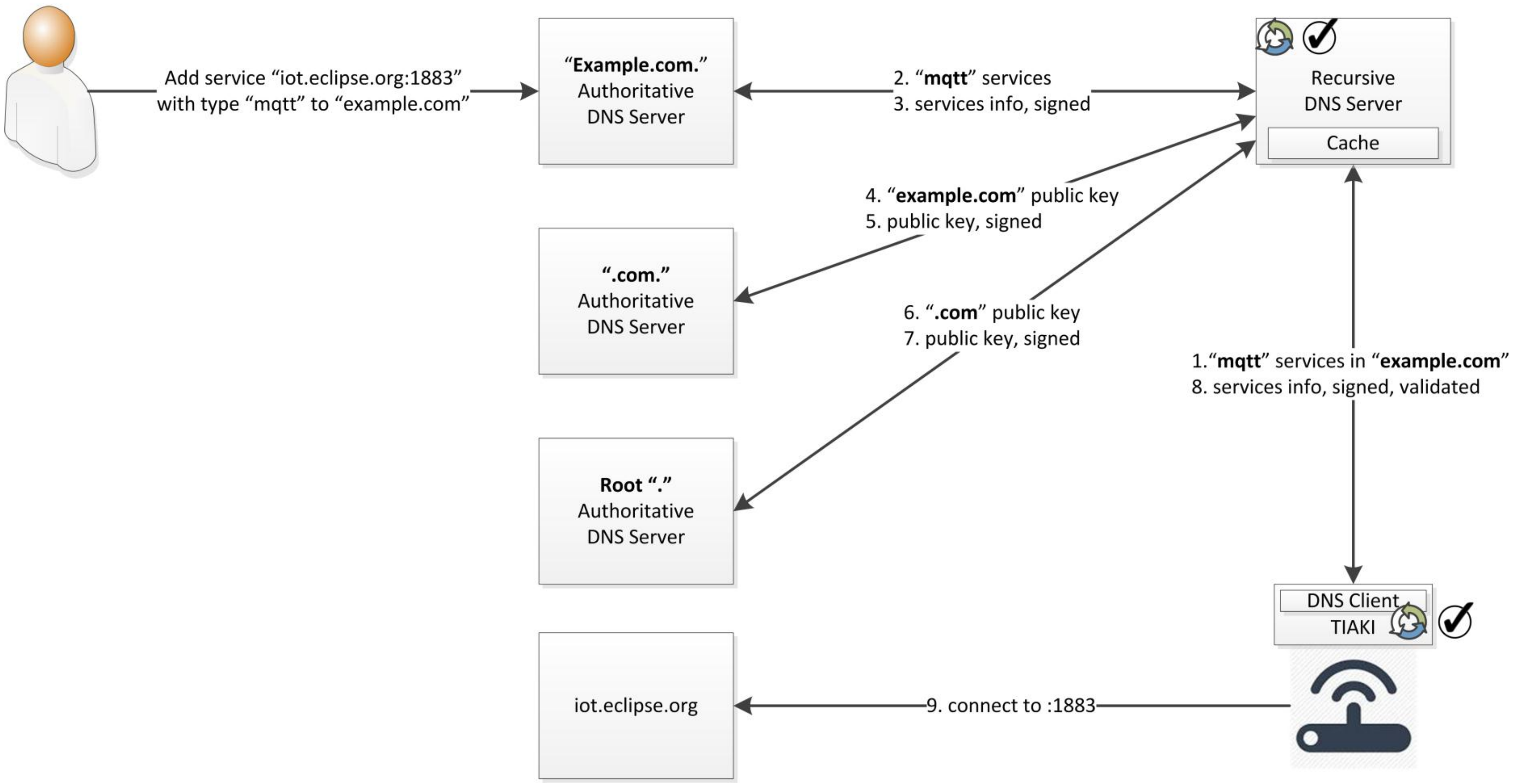
Code example

```
DnsServicesDiscovery discoverer = new DnsServicesDiscovery();
Fqdn fullyQualifiedDomainName = new Fqdn("example.com");
CompoundLabel serviceType = new CompoundLabel("mqtt");


Set<ServiceInstance> discoveryResult =
discoverer.listServiceInstances(fullyQualifiedDomainName, serviceType);
for (ServiceInstance instance : discoveryResult) {
        System.out.println(instance);
}
```

```
$> mqtt iot.eclipse.org:1883 "server=Mosquitto" "version=1.3.1"
```

Secure Service Discovery with DNSSEC


Add service "iot.eclipse.org:1883" with type "mqtt" to "example.com"
"Example.com." Authoritative DNS Server
2. "**mqtt**" services
3. services info, signed
Recursive DNS Server
Cache
4. "**example.com**" public key
5. public key, signed
".com." Authoritative DNS Server
6. "**.com**" public key
7. public key, signed
1."**mqtt**" services in "**example.com**"
8. services info, signed, validated
Root "." Authoritative DNS Server
DNS Client
TIAKI
iot.eclipse.org
9. connect to :1883

Benefits of using DNSSEC for Securing DNS

- DNSSEC guarantees the records' authenticity and integrity
  - Prevents man-in-the-middle and cache poisoning attacks

- DNSSEC uses unencrypted UDP/TCP
  - No need for certificates to ensure authenticity
  - No need for Crypto Libraries

- The Trust Anchor can be set at any particular level, thus allowing discovery to work within intranet
  - Not necessarily root – typically, could be at company.com level

- PKI Complexity handled by DNS service provider

Benefits of using DNS for Service Discovery

- Globally distributed Key-Value Pair Database “for free”
- Proven, always-on, Internet-scale infrastructure
- Updates to DNS records reflected almost immediately across the board
- Can be used for multiple kinds of data (DANE TLSA Certificates / Public Keys, etc.)

People!

- Committers:
  - Paolo Maresca, Verisign
  - Nicolas Brasey, IMTF

- Mentors:
  - Benjamin Cabe
  - Wayne Beaton

- Lead:
  - Regis Piccand rpiccand@verisign.com | @repicc

Project Status

- Initial contribution for Java : done!

- To come by year end:
  - Initial contribution for C
  - First release…

- Collaborations with Kura, Leshan, HawkBit, …

- Tiaki not (yet) targeted at constrained devices, your help is needed to make that happen!

- More info here: https://projects.eclipse.org/projects/iot.tiaki

Questions…

powered by

VERISIGN®