The bridge to possible

OpenRoaming under the hood

Bart Brinckman
Distinguished Engineer
bbrinckm@cisco.com

Jakub Sroga
Network Support Engineer
jsroga@cisco.com

BREKWN-2037

Cisco Webex App

https://ciscolive.ciscoevents.com/ciscolivebot/#BREKWN-2037

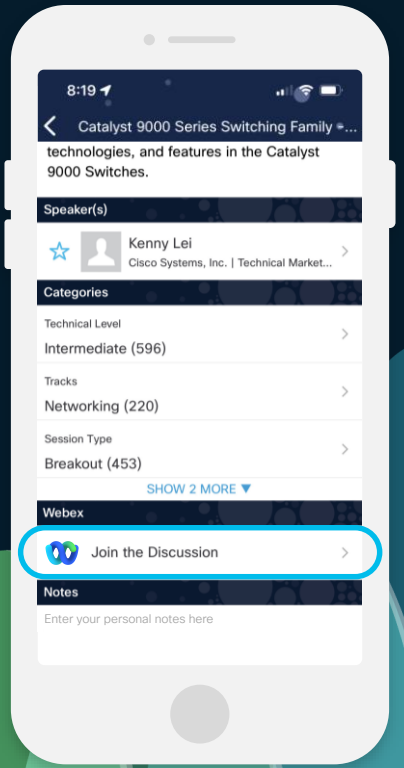
Questions?

Use Cisco Webex App to chat with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 7, 2024.

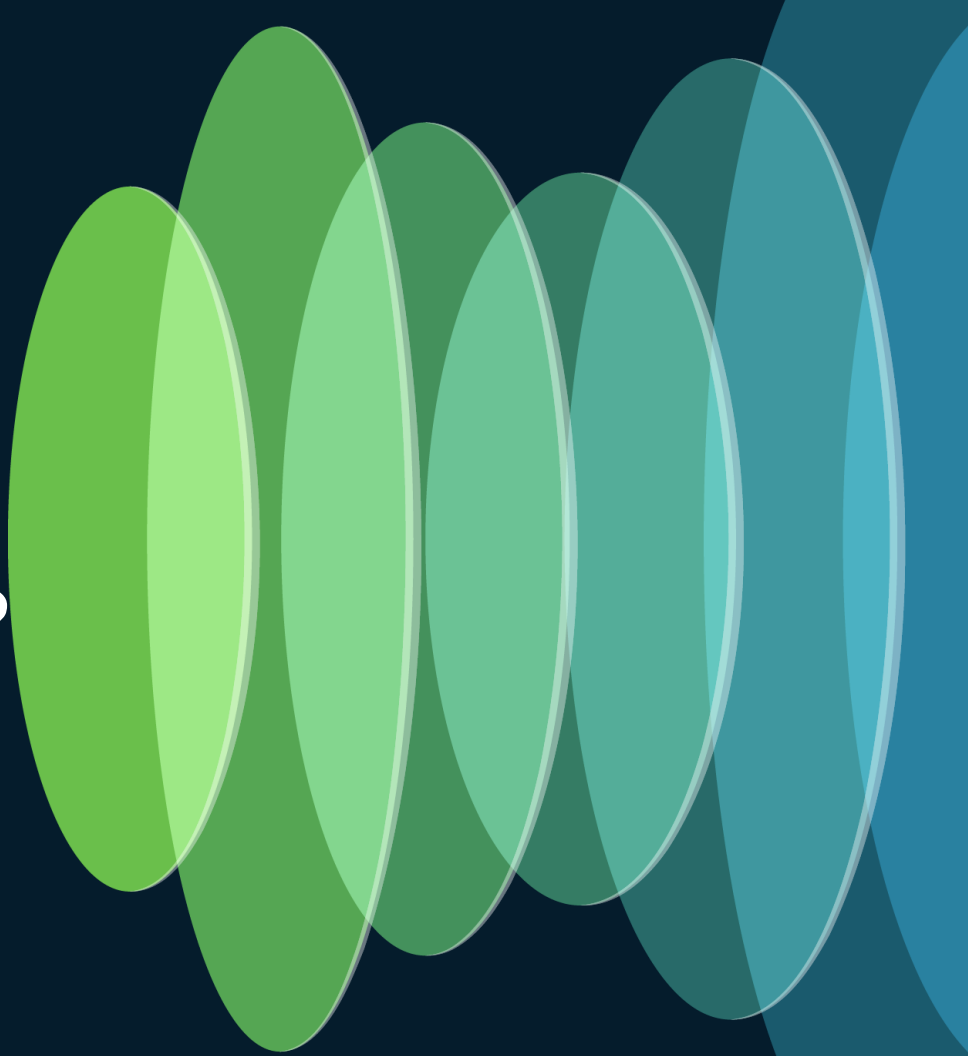


Agenda

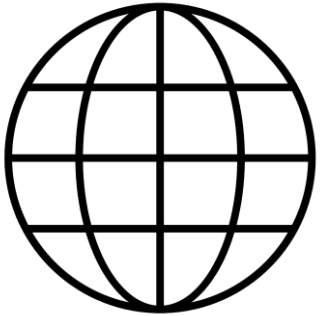
- What is it and why would I use it?
- How it works under the hood
- Your own Identity: SDK and Web-based provisioning
- Configuration and Live Demo with Meraki
- Conclusion

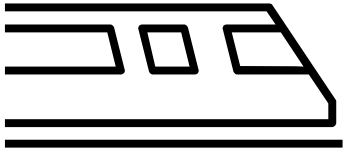
We start with...

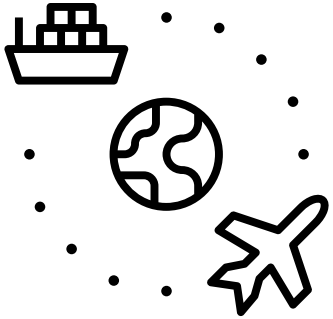
What is OpenRoaming? Why would I use it?

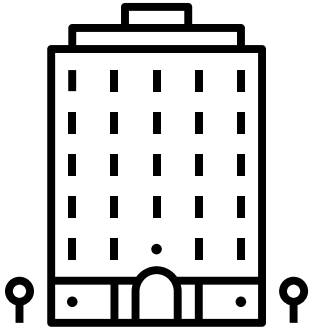


Reality today

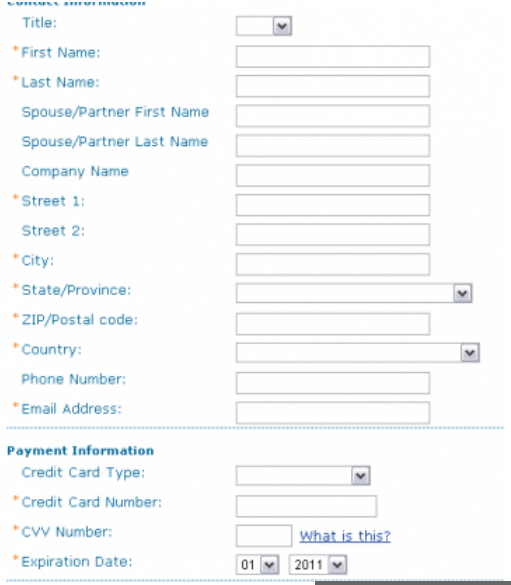


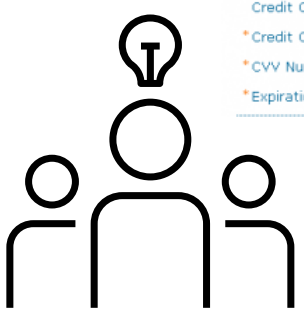


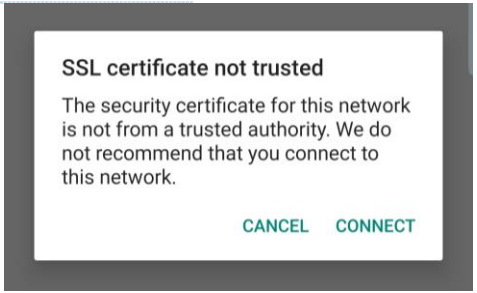


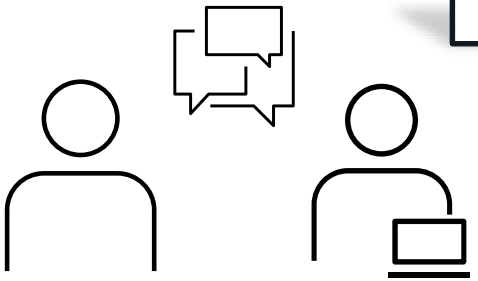


Reality today









password: $\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$

Username: g00dLuck
Password: zk1sowcaStF98LOZo2x

Our Goal: Intelligent Multi-Access

Access providers

Public
Ent. Guest

WiFi6 5G

Identity providers

Service-based

Converged Access for People and Things

To use all wireless stacks better, we need...

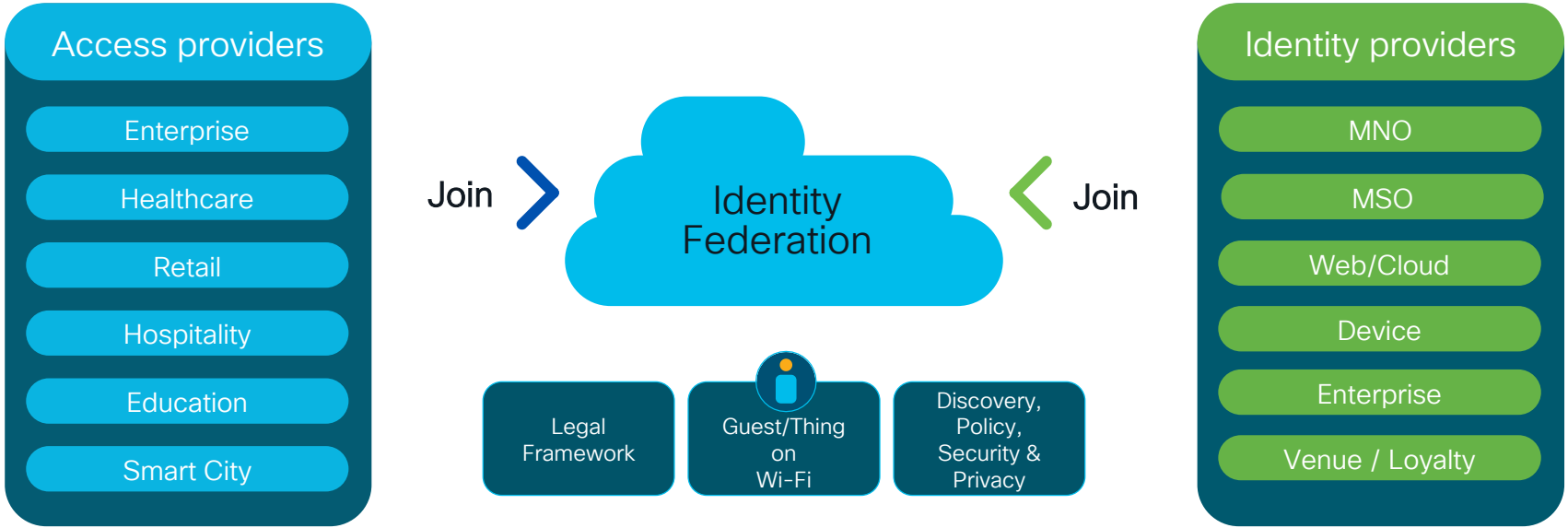
Frictionless Onboarding
OpenRoaming
(assure access to all available paths)

Seamless Handover
Roaming between Wi-Fi (private)
and cellular (public)

Seamless Interworking
Policy-based path selection for
Loosely coupled Access Networks

OpenRoaming: Opening the Wi-Fi Ecosystem to new experiences & business models

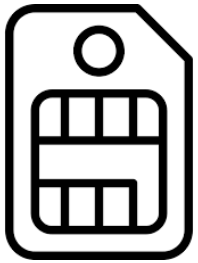
- Leverage Identity Federation to scale and facilitate relationships



OpenRoaming is a federation of identity & access providers to enable seamless roaming & onboarding

Which ID’s are available?

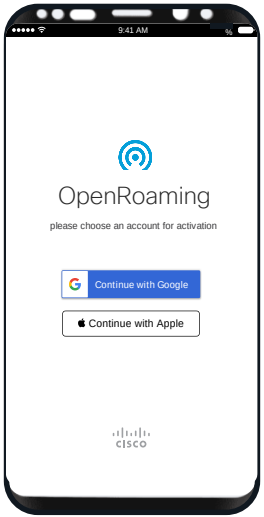
Service Provider



Enterprise

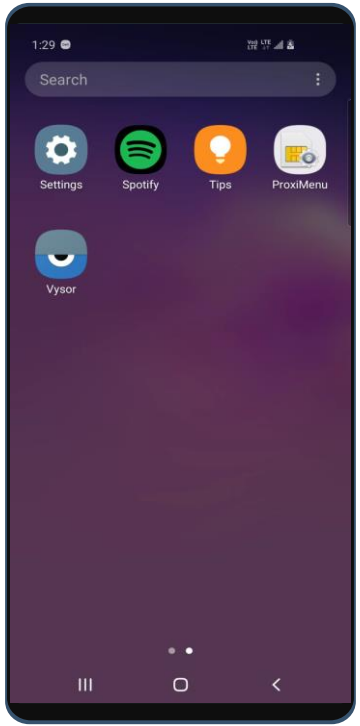
Device Embedded

Cloud ID

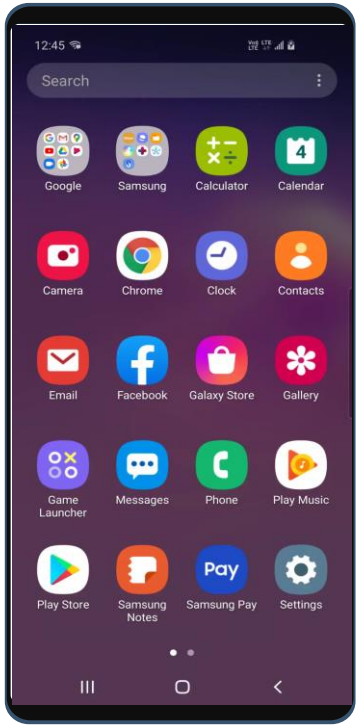


Loyalty

Use case: Seamless onboarding use case



Via Wi-Fi Picker



Via Notification Bar

Use Case:

Get users seamlessly and securely connected to a venue's Wi-Fi network

Value proposition:

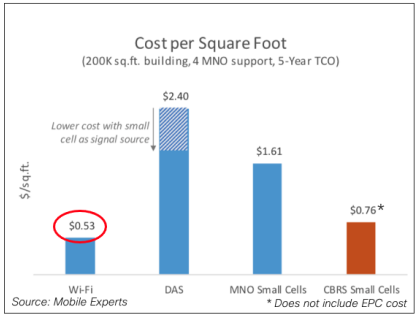
User	Better user experience, device is on the internet and ready to go Enhanced Security & Privacy vs portal-based solution
Venue	Improved customer experience & satisfaction Reduced IT and non-IT staff burden: Wi-Fi as easy as power Secure and private: lower exposure to malicious actors Analytics venue flow and density analytics

Who should run it?

- Public areas: Municipal Wi-Fi, libraries, public buildings
- Healthcare: Hospitals and care centers
- Transportation: Airports and train stations
- Retail: Shopping malls, big box stores
- Hospitality: Hotels and event venues

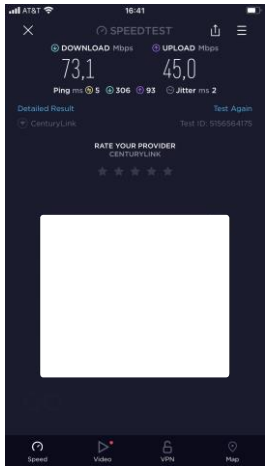
Use case: Service provider indoor coverage

Cost-comparison to DAS



SP1 on DAS*

SP2 on Wi-Fi*



Use Case:

Improve bad SP indoor coverage at a fraction of the cost of DAS (Digital Antenna Systems)

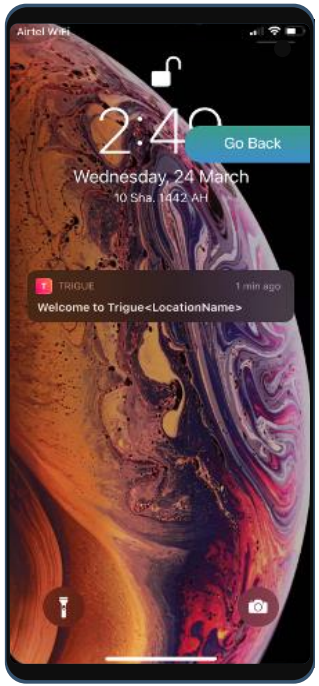
Value proposition:

User	Good indoor voice and data
Venue	Improved customer experience & satisfaction Reduced IT and non-IT staff burden: Wi-Fi as easy as power Lower cost alternative than DAS or in combination with DAS for lower-cost capacity Own the Analytics: venue flow and density analytics

Who should run it?

- Public indoor areas: libraries, public buildings
- Healthcare: Hospitals and care centers
- Transportation: Airports and train stations
- Retail: Shopping malls, big box stores, supermarkets
- Hospitality: Hotels and event venues

Use case: Smart contextual loyalty experiences



Use Case:

Connect loyalty users and visitors seamlessly, get person-based insights, and communicate with visitor in real-time

Value proposition:

User	Better user experience, device is on the internet and ready to go Able to communicate with the venue in real-time
Venue	Improved customer experience & satisfaction Reduced IT and non-IT staff burden: Wi-Fi as easy as power Better persona-based Analytics Real-time location-based notifications

Who should run it?

- Retail: Shopping malls, big box stores, grocery stores with loyalty programs
- Hospitality: Hotels with loyalty programs, events with event/fan apps, …
- Healthcare: Hospitals with patient apps

Use Case summary

Seamless, Secure Onboarding & User Insights

- OpenRoaming Mobile App
- Devices with Native Support
- Publicly available IDPs

DNA Spaces SEE

Smart, Contextual Loyalty Experiences

- iOS & Android: DNA Spaces SDK
- Web-based APIs for Web and Portal

DNA Spaces ACT

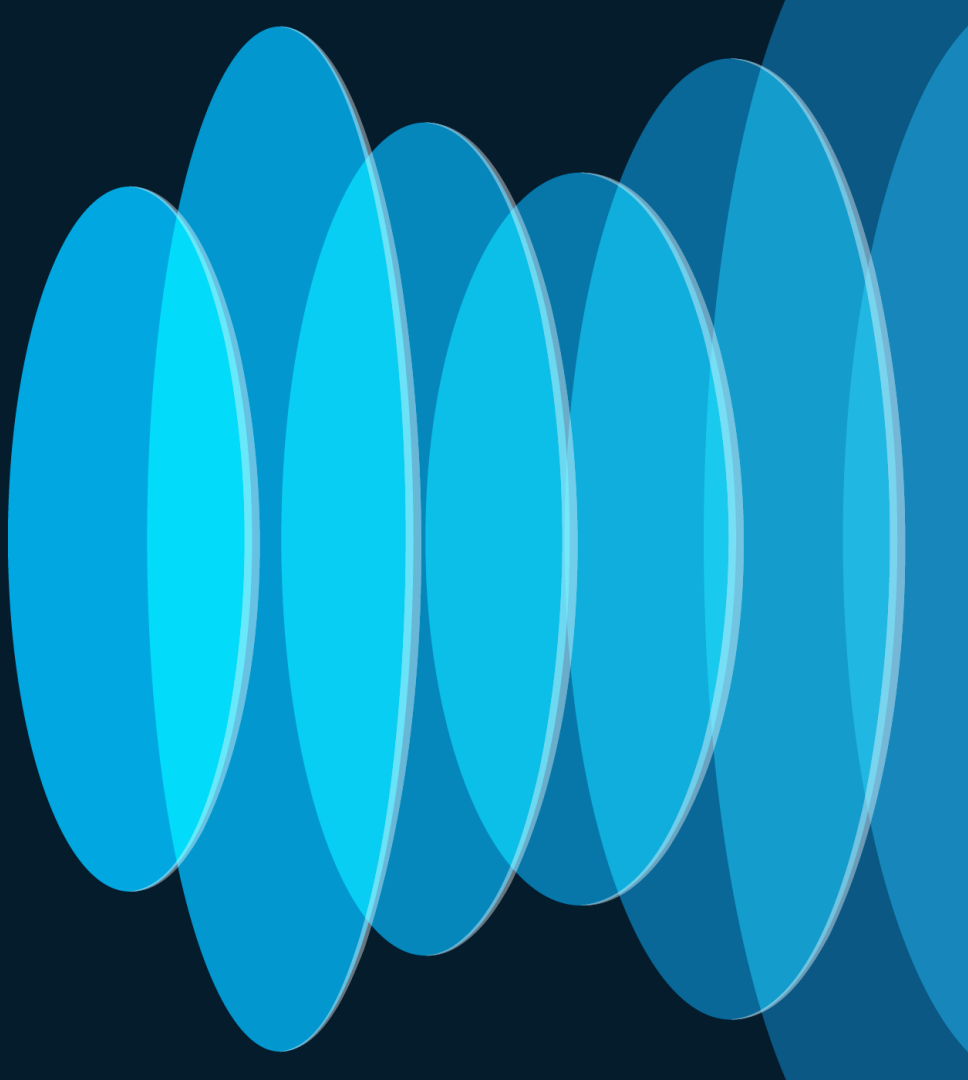
Enhance Indoor Coverage

- Service Provider (SP) Offload to Wi-Fi
- Devices with Native Support
- Publicly available IDPs

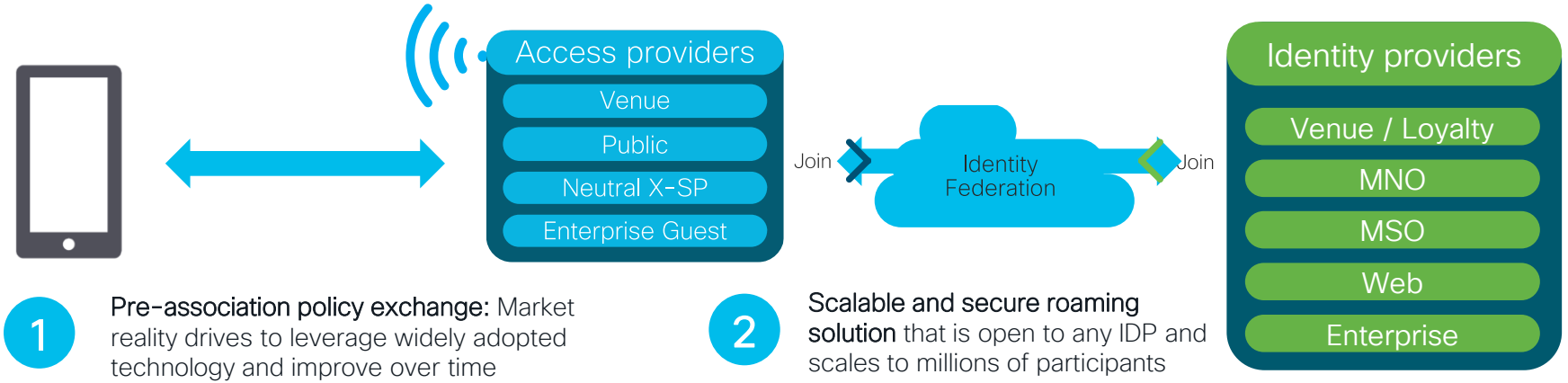
DNA Spaces EXTEND

What we are all here for...

How it works under the hood



The basic idea: Leverage and modernize roaming



1 **Pre-association policy exchange:** Market reality drives to leverage widely adopted technology and improve over time

2 **Scalable and secure roaming solution** that is open to any IDP and scales to millions of participants

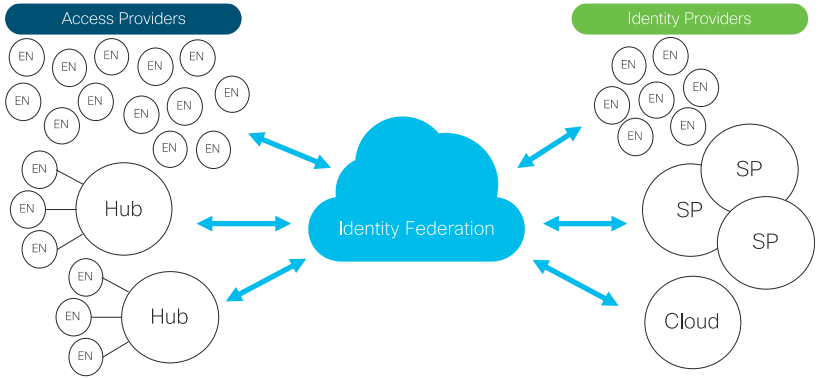
Wi Fi ALLIANCE

PassPoint

Phase 1: leverage what is supported
- Repurpose home/visited concept so signal IDP prioritization
- leverage 5 Byte RCOI field to signal policy

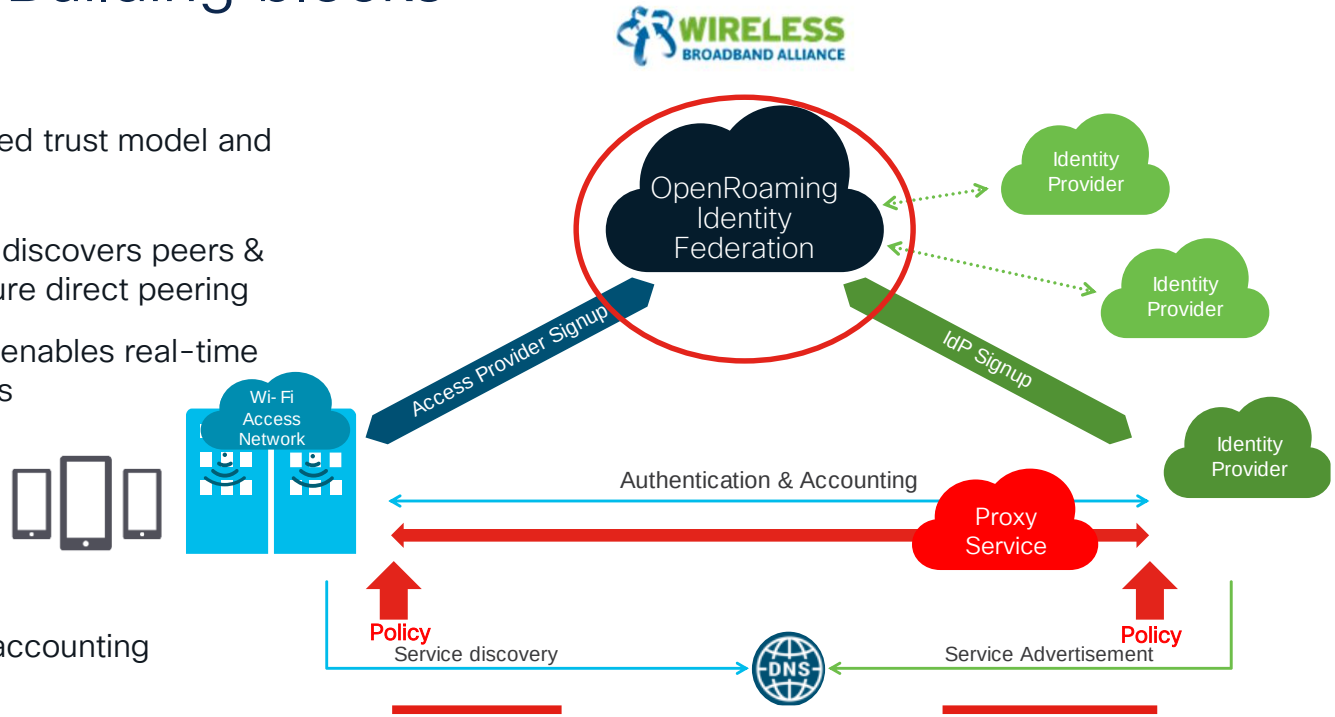
Phase 2: Improve the standard
- Update standard attributes to support policy exchange

Identity federation scales to millions of participants:



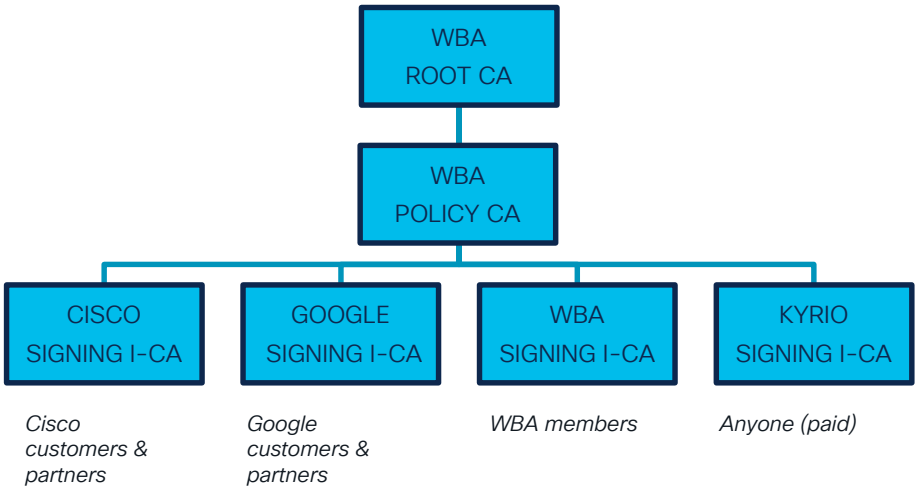
OpenRoaming: Building blocks

1. Identity Federation: PKI-based trust model and legal framework
2. Federation that dynamically discovers peers & services and allows for secure direct peering
3. Dynamic policy at the edge enables real-time ad-hoc roaming agreements
4. Secure Authentication and accounting over TLS
5. Proxy services can connect cloud-based identities or offer value-added services (e.g. settlement)

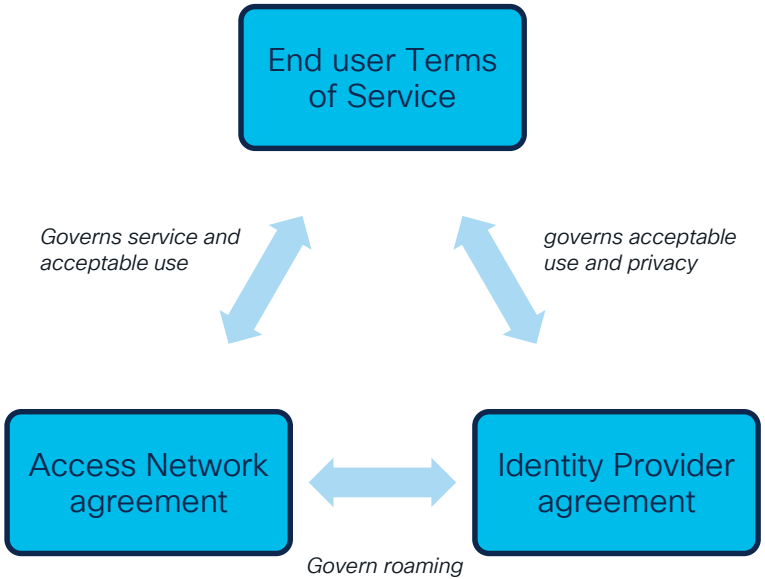


Federation Architecture

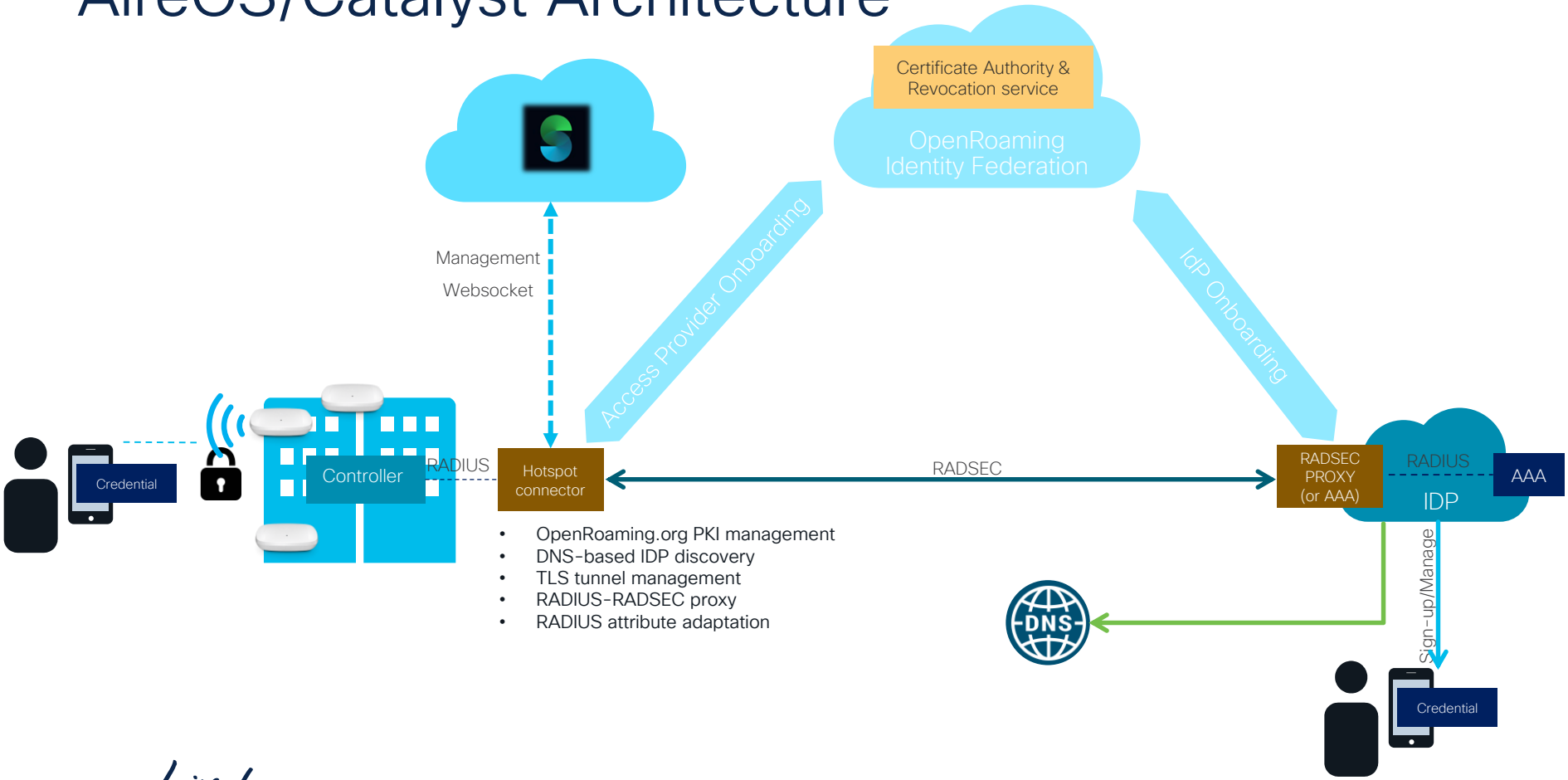
PKI Framework



Legal Framework

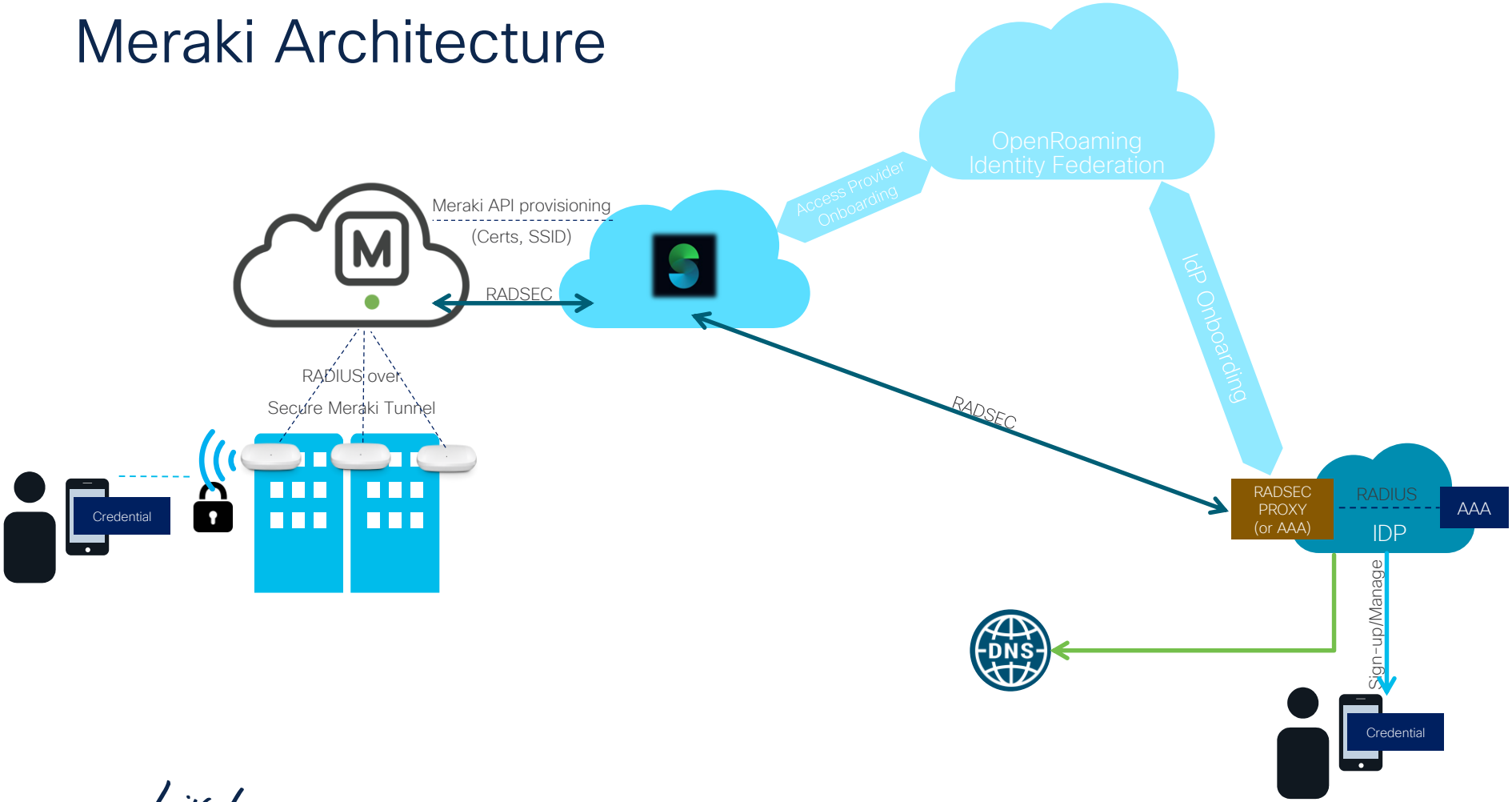


AireOS/Catalyst Architecture



- OpenRoaming.org PKI management
- DNS-based IDP discovery
- TLS tunnel management
- RADIUS-RADSEC proxy
- RADIUS attribute adaptation

Meraki Architecture

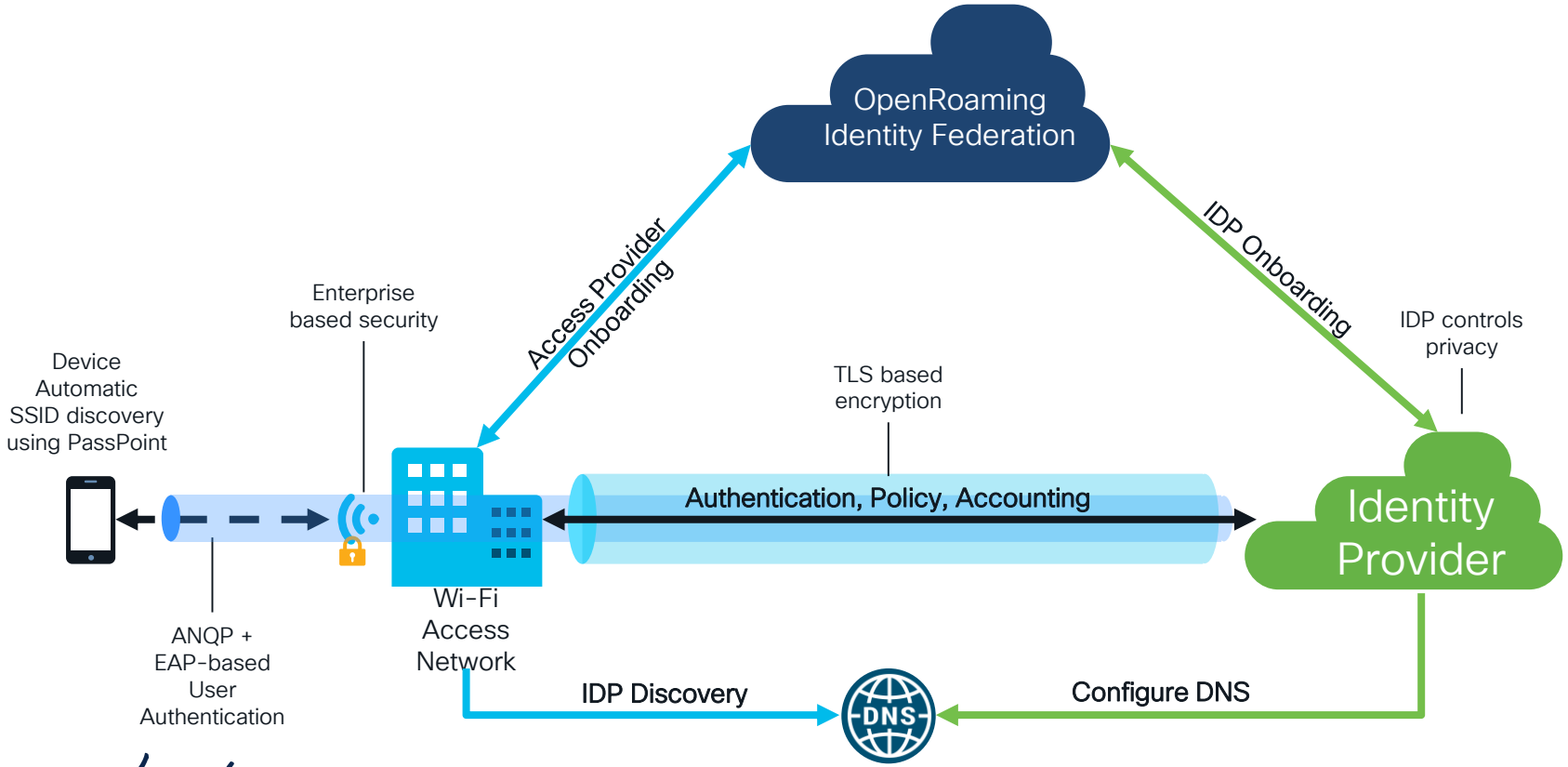


Join at

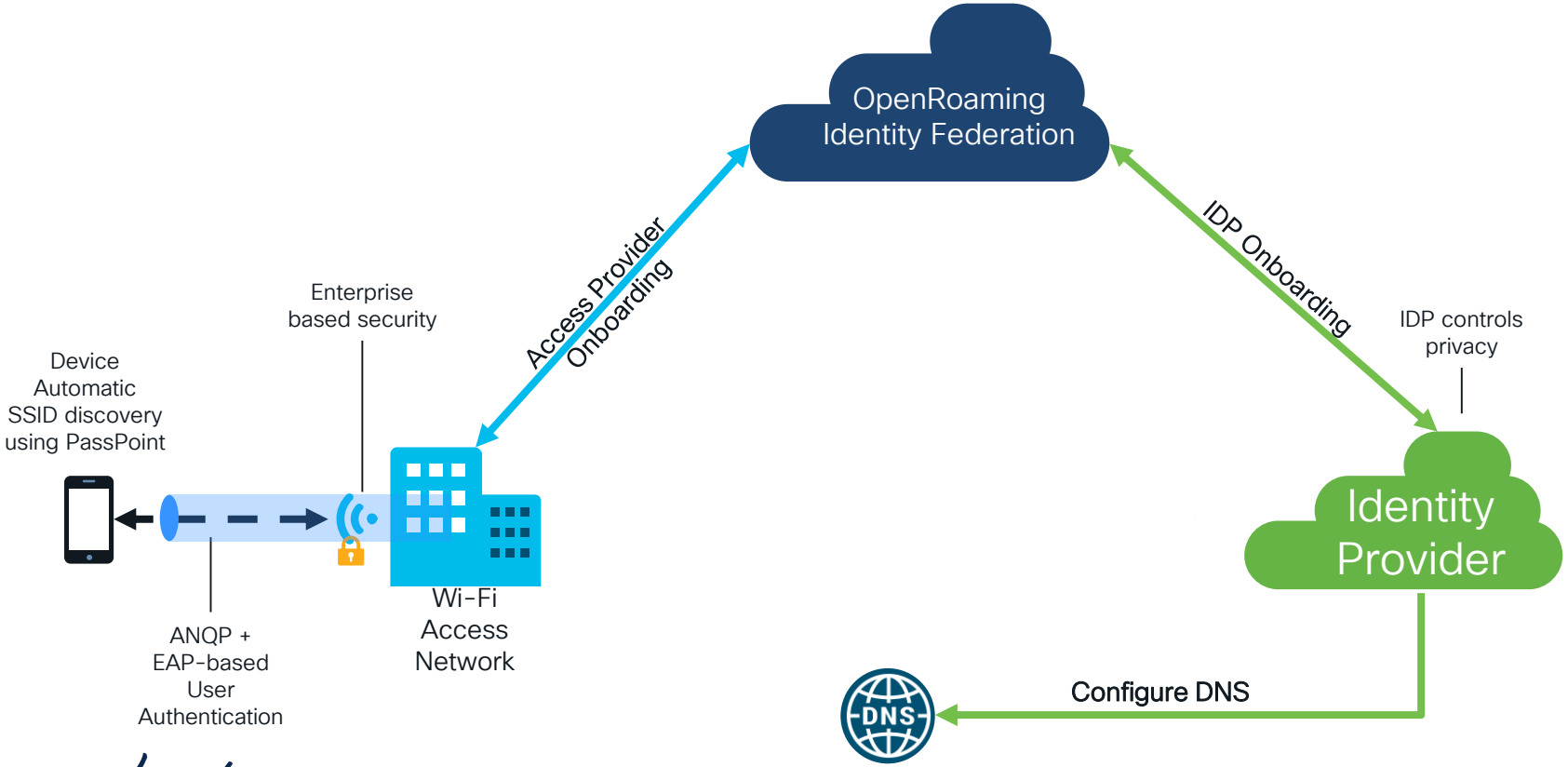
slido.com

#9708 804

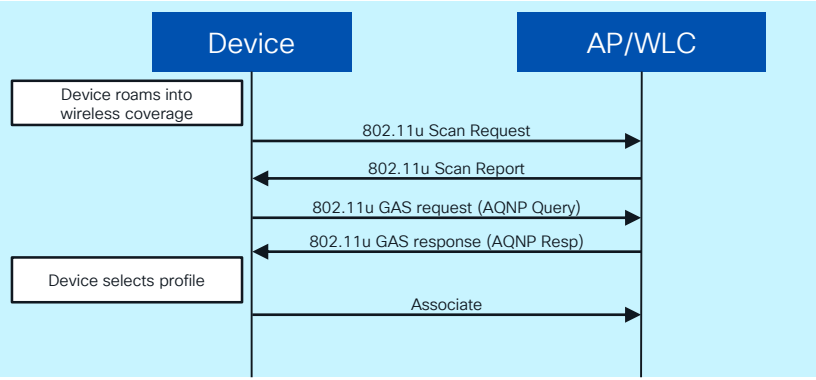
Complete onboarding flow



Onboarding flow – SSID discovery



SSID discovery and selection using 802.11u



1 AP Beacon or Probe response info

No.	Source	Protocol	Access Network Type	SSID
1	e2:cb:ac:8d:55:41	802.11	Free public network	"OR@Home"

```
Tag: Interworking
    Tag Number: Interworking (107)
    Tag length: 9
    .... 0011 = Access Network Type: Free public network (3)
    ...1 .... = Internet: 1
    ..0. .... = ASRA: 0
    .0.. .... = ESR: 0
    0... .... = UESA: 0
    Venue Group: Assembly (1)
    Venue Type: 0
    HESSID: 00:00:00_00:00:00 (00:00:00:00:00:00)
Tag: Advertisement Protocol
    Tag Number: Advertisement Protocol (108)
    Tag length: 2
    Advertisement Protocol element: ANQP
        Advertisement Protocol Tuple: Access Network Query Protocol
            .111 1111 = Query Response Length Limit: 127
            0... .... = PAME-BI: 0
            Advertisement Protocol ID: Access Network Query Protocol (0)
Tag: Roaming Consortium
    Tag Number: Roaming Consortium (111)
    Tag length: 10
    Number of ANQP OIs: 0
    .... 0011 = OI #1 Length: 3
    0101 .... = OI #2 Length: 5
    OI #1: 004096 - Cisco Systems, Inc
    OI #2: 5a03ba0000 - Wireless Broadband Alliance Ltd
```

RCOIs:
004096
5a03ba0000

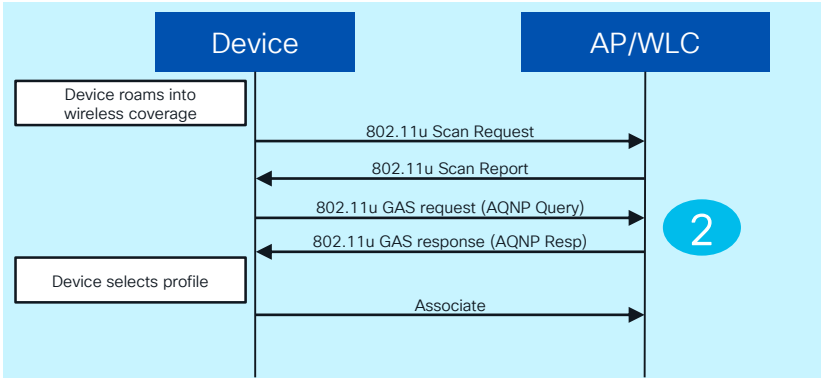
OpenRoaming RCOI

Roaming Consortium Organization Identifier (RCOI) :

- Allow all: Accepts users from any identity provider (IDP), with any privacy policy.
- Real ID: Accepts users from any IDP, but only with a privacy policy that shares real identity (anonymous not accepted).
- Custom: Accepts users of select identity types and privacy policies associated with the identity types.

Description	WBA Roaming OI	Cisco Roaming OI
All	5A03BA0000	004096
All with real-ID only	5A03BA1000	00500B
All paid	BAA2D00000	00500F
Device Manufacturer	5A03BA0A00	00502A
Device Manufacturer real-ID	5A03BA1A00	0050A7
Cloud ID	5A03BA0200	005014
Cloud ID real-ID	5A03BA1200	0050BD
Enterprise ID	5A03BA0300	00503E
Enterprise ID real ID	5A03BA1300	0050D1
Enterprise Customer program ID	Not defined	005050
Enterprise Customer program real ID	Not defined	0050E2
Loyalty Retail	5A03BA0B00	005053
Loyalty Retail real ID	5A03BA1B00	0050F0
Loyalty Hospitality	5A03BA0600	005054
Loyalty Hospitality real ID	5A03BA1600	00562B
SP free Bronze Qos	5A03BA0100	005073
New ID Types in OR-Std:	WBA Roaming OI	Cisco Roaming OI
Government ID free	5A03BA0400	Not defined
Automotive ID free	5A03BA0500	Not defined
Automotive Paid	BAA2D00500	Not defined
Education/Research ID free	5A03BA0800	Not defined
Cable ID free	5A03BA0900	Not defined
SP paid Gold QoS real ID	BAA2D05100	Not defined

802.11u GAS Initial Request (STA) and Response (AP)



STA request additional information .11u and ANQP

```
9717  5a:52:a1:14:c9:dc    802.11                    GAS Initial Request
  Fixed parameters
    Category code: Public Action (4)
    Public Action: GAS Initial Request (0x0a)
    Dialog token: 0x1b
    Tag Number: Advertisement Protocol (108)
    Tag length: 2
  > Advertisement Protocol element: ANQP
  v Query Request: ANQP Request - ANQP Query list
      Query Request Length: 27
    v Info ID: ANQP Query list (256)
        Length: 8
        ANQP Query ID: Domain Name list (268)
        ANQP Query ID: Roaming Consortium list (261)
        ANQP Query ID: 3GPP Cellular Network information (264
        ANQP Query ID: NAI Realm list (263)
    v Info ID: ANQP vendor-specific list (56797) - HS 2.0 HS Query list
        Length: 7
        OUI: 50:6f:9a (Wi-Fi Alliance)
        WFA Subtype: Hotspot 2.0 ANQP (17)
        Subtype: HS Query list (1)
        Reserved: 0
        Queried Subtype: Operator Friendly Name (3)
```

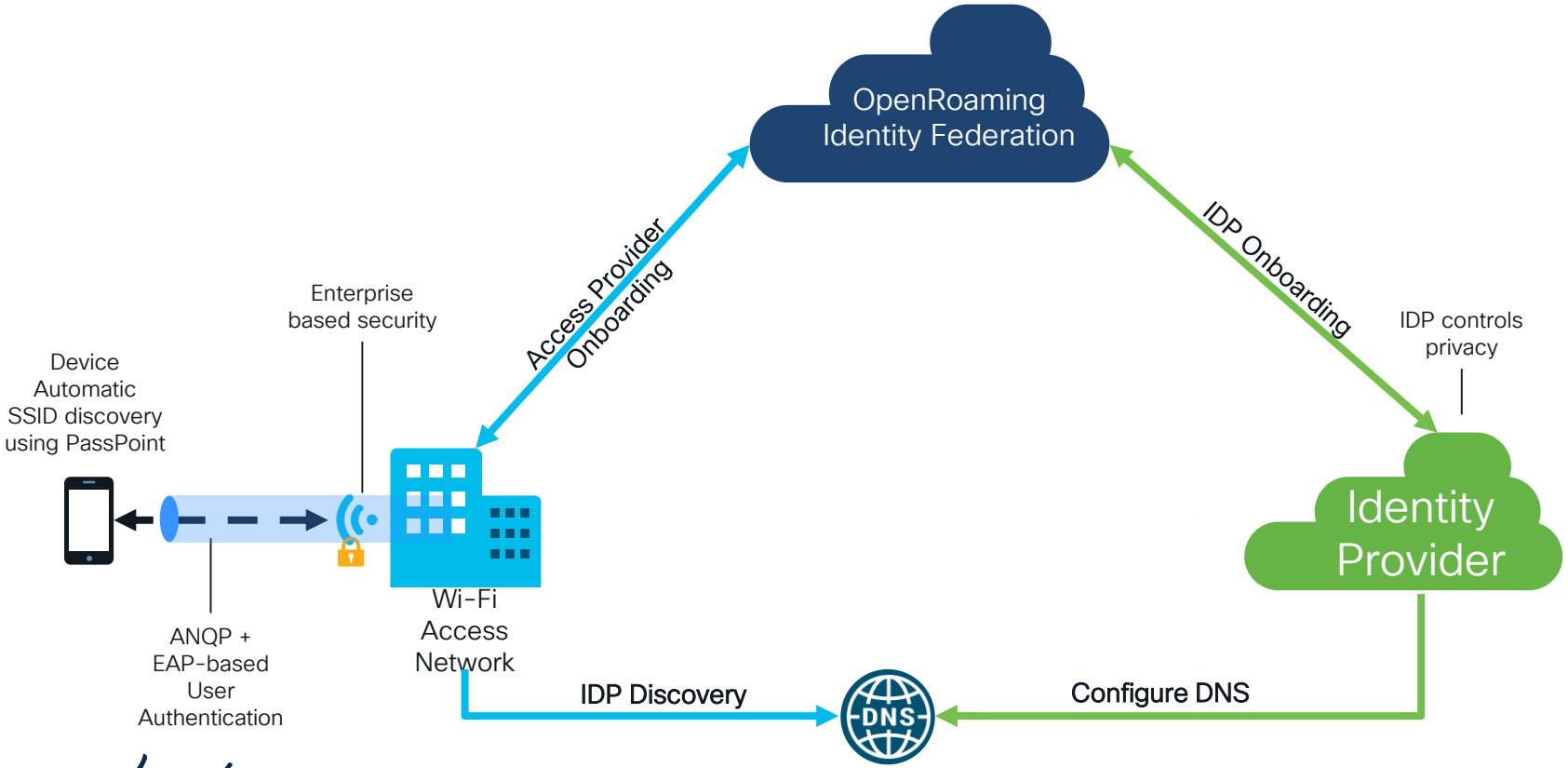
AP response .11u and ANQP

```
  > Advertisement Protocol element: ANQP
  v Query Response: ANQP Response - Roaming Consortium list, ..
      Query Response Length: 316
    > Info ID: Roaming Consortium list (261)
    v Info ID: NAI Realm list (263)
        Length: 228
        NAI Realm Count: 5
      > NAI Realm Data (open.openroaming.org)
      > NAI Realm Data (wlan.mnc150.mcc310.3gppnetwork.org)
      > NAI Realm Data (wlan.mnc280.mcc310.3gppnetwork.org)
      > NAI Realm Data (wlan.mnc100.mcc313.3gppnetwork.org)
      > NAI Realm Data (wlan.mnc410.mcc310.3gppnetwork.org)
    v Info ID: 3GPP Cellular Network information (264)
        Length: 17
        GUD: 0
        UDHL: 15
        IEI: 0 (PLMN List)
        PLMN Length: 13
        Number of PLMNs: 4
      > PLMN 0 (0x510013)
      > PLMN 1 (0x820013)
      > PLMN 2 (0x10313)
      > PLMN 3 (0x140013)
    v Info ID: Domain Name list (268)
        Length: 20
        Domain Name Length: 19
        Domain Name: preferreddomain.com
    v Info ID: ANQP vendor-specific list (56797) - HS 2.0 Operator Friendly Name
        Length: 21
        OUI: 50:6f:9a (Wi-Fi Alliance)
        WFA Subtype: Hotspot 2.0 ANQP (17)
        Subtype: Operator Friendly Name (3)
        Reserved: 0
      v Friendly Name [1]
          Length: 14
          Language Code: en
          Operator Friendly Name: OpenRoaming
```

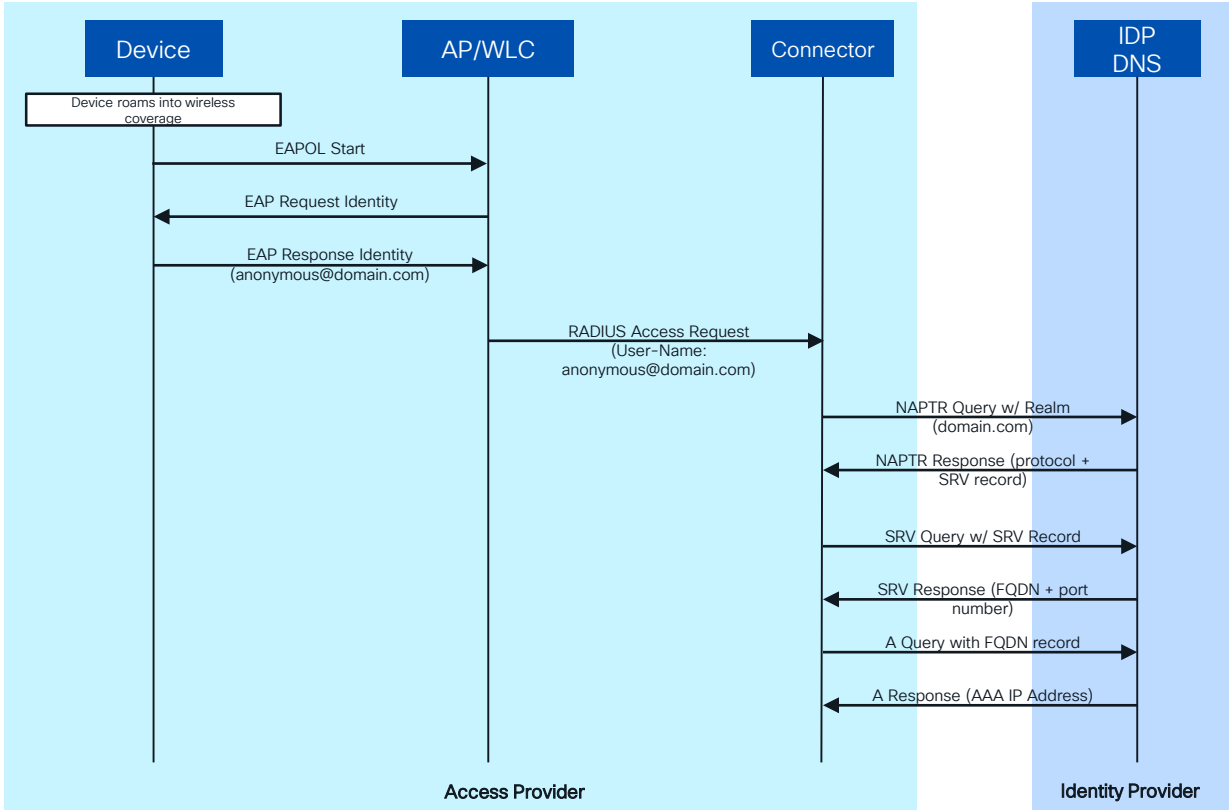
NAI Realm: openroaming.org

Domain: preferreddomain.com

Onboarding flow – IDP discovery



IDP Discovery Call Flow (RFC-7585)



sdk.openroaming.net

dig -t naptr sdk.openroaming.net
sdk.openroaming.net. 300 IN NAPTR 50 50 "s" "**aaa+auth:radius.tls.tcp**" "" **_radiustls._tcp.sdk.openroaming.net**.

dig -t srv _radiustls._tcp.sdk.openroaming.net
_radiustls._tcp.sdk.openroaming.net. 300 IN SRV 0 10 **2083 idp.openroaming.net.**

dig -t a idp.openroaming.net
idp.openroaming.net. 300 IN **A 3.208.239.144**

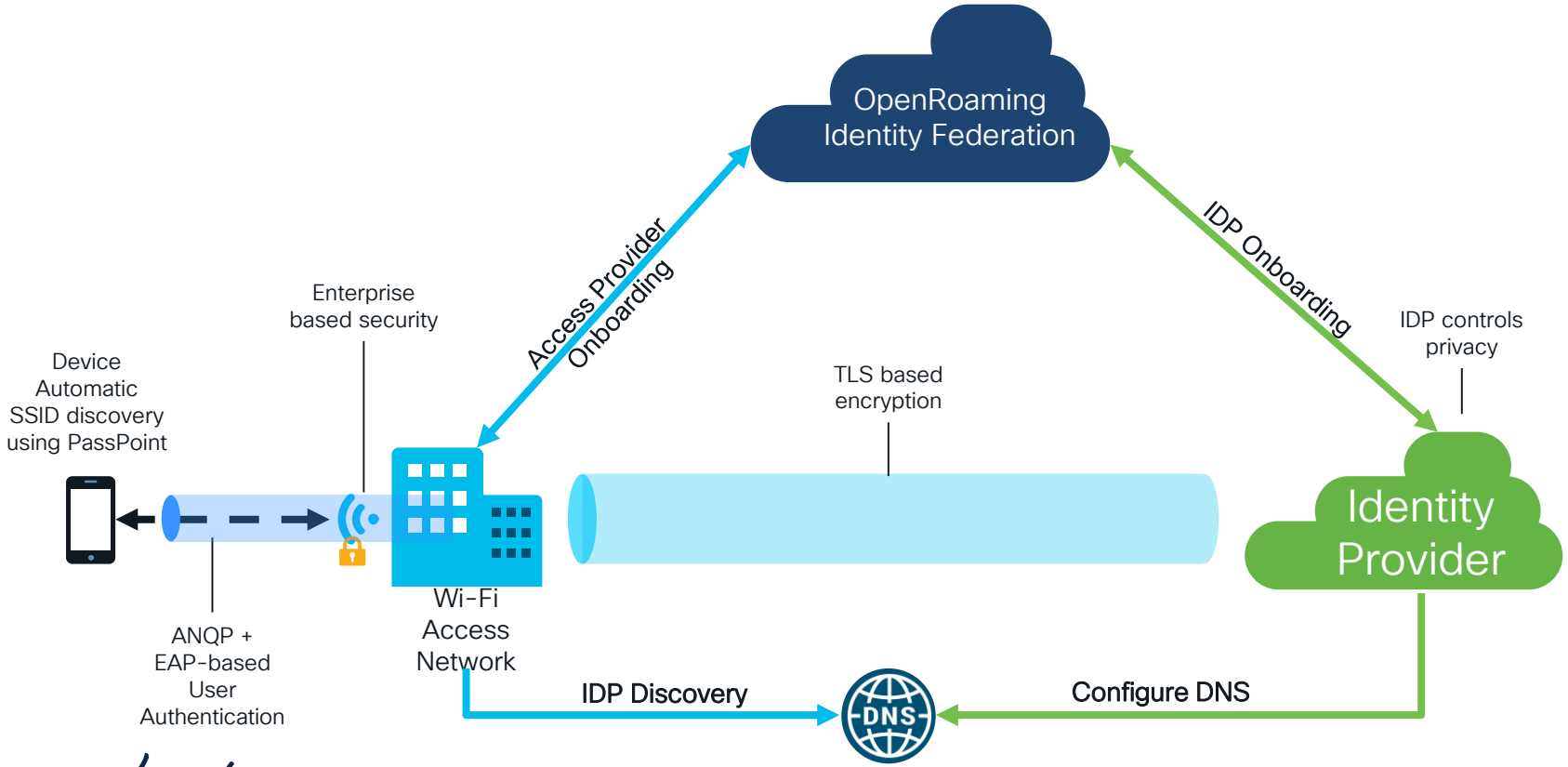
AT&T PLMN 410

dig -t naptr wlan.mnc410.mcc310.pub.3gppnetwork.org
wlan.mnc410.mcc310.pub.3gppnetwork.org. 3600 IN NAPTR 50 50 "s" "aaa+auth:radius.tls.tcp" "" _radiustls._tcp.3af521.net.

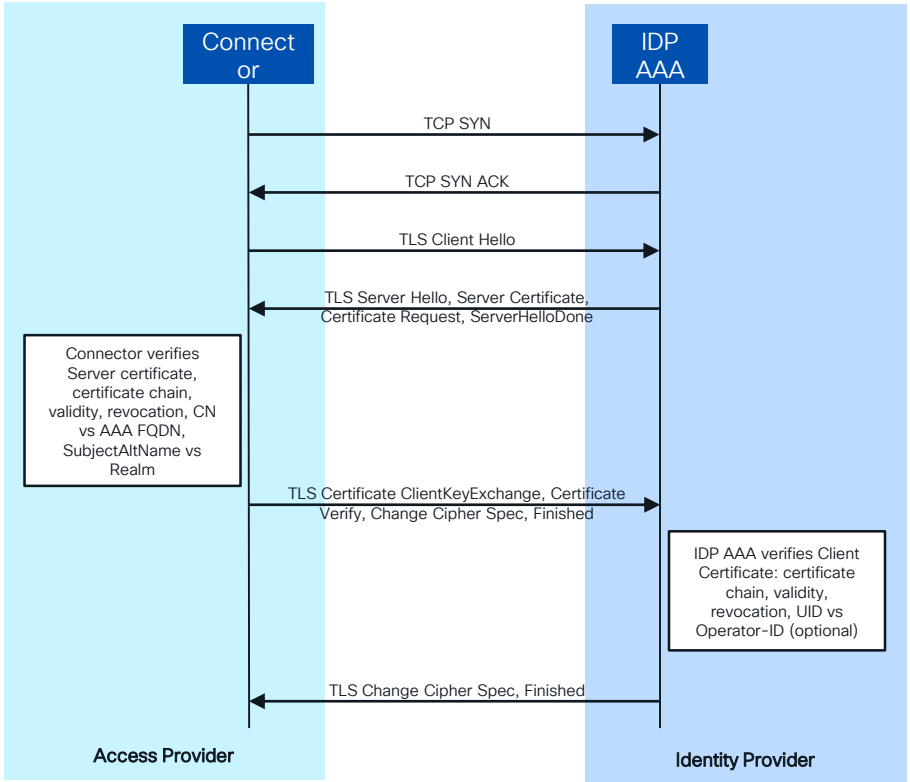
dig -t srv _radiustls._tcp.3af521.net.
_radiustls._tcp.3af521.net. 300 IN SRV 0 10 2083 idp.3af521.net.

dig -t a idp.3af521.net
idp.3af521.net. 300 IN CNAME public-radius-service.production.radius.one.singledigits.com.
public-radius-service.production.radius.one.singledigits.com. 60 IN CNAME a8f7a7d1bd6e54b4babbed926a990720-b4bc5d7f98840512.elb.us-east-1.amazonaws.com.
a8f7a7d1bd6e54b4babbed926a990720-b4bc5d7f98840512.elb.us-east-1.amazonaws.com. 60 IN A 54.146.180.226
a8f7a7d1bd6e54b4babbed926a990720-b4bc5d7f98840512.elb.us-east-1.amazonaws.com. 60 IN A 54.83.92.42

Onboarding flow – TLS Tunnel Setup



TLS Tunnel Setup Between Access Provider and IDP



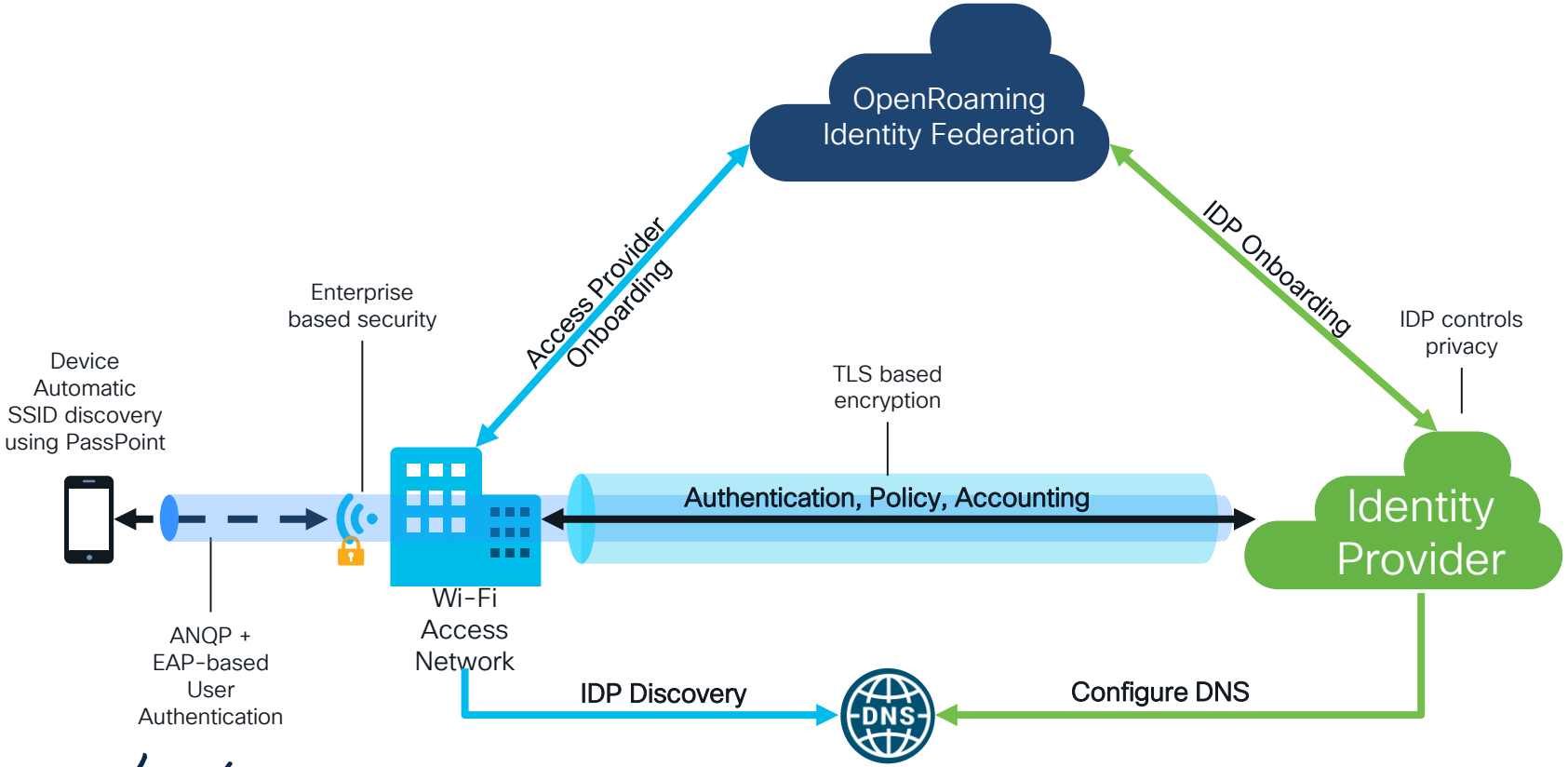
openssl s_client -connect idp.openroaming.net:2083 check SSL connection

```
CONNECTED(00000005)
depth=3 C = US, ST = California, L = San Jose, O = "Cisco Systems, Inc.", OU = Openroaming, CN = openroaming.org, emailAddress = enb-devops@cisco.com
verify error:num=19:self signed certificate in certificate chain
verify return:0
140704668922688:error:1401E412:SSL routines:CONNECT_CR_FINISHED:sslv3 alert bad certificate:/AppleInternal/Library/BuildRoots/97f6331a-ba75-11ed-a4bc-863efbbaf80d/Library/Caches/com.apple.xbs/Sources/libressl/libressl-3.3/ssl/ssl_pkt.c:1008:SSL alert number 42
---
Certificate chain
 0 s:/C=US/ST=CA/O=Cisco/CN=idp.openroaming.net
   i:/C=US/O=Cisco Systems Inc./OU=DNASpaces/ST=California/CN=cisco.openroaming.org/L=San Jose
 1 s:/C=US/O=Cisco Systems Inc./OU=DNASpaces/ST=California/CN=cisco.openroaming.org/L=San Jose
   i:/C=SG/ST=Singapore/L=Singapore/O=Wireless Broadband Alliance/OU=WBA/CN=openroaming.org/dnQualifier=WBA WRIX ECC Policy Intermediate CA-01
 2 s:/C=SG/ST=Singapore/L=Singapore/O=Wireless Broadband Alliance/OU=WBA/CN=openroaming.org/dnQualifier=WBA WRIX ECC Policy Intermediate CA-01
   i:/C=US/ST=California/L=San Jose/O=Cisco Systems, Inc./OU=Openroaming/CN=openroaming.org/emailAddress=enb-devops@cisco.com
 3 s:/C=US/ST=California/L=San Jose/O=Cisco Systems, Inc./OU=Openroaming/CN=openroaming.org/emailAddress=enb-devops@cisco.com
   i:/C=US/ST=California/L=San Jose/O=Cisco Systems, Inc./OU=Openroaming/CN=openroaming.org/emailAddress=enb-devops@cisco.com
---
Server certificate
subject=/C=US/ST=CA/O=Cisco/CN=idp.openroaming.net
issuer=/C=US/O=Cisco Systems Inc./OU=DNASpaces/ST=California/CN=cisco.openroaming.org/L=San Jose
---
Acceptable client certificate CA names
/C=US/ST=California/L=San Jose/O=Cisco Systems, Inc./OU=Openroaming/CN=openroaming.org/emailAddress=enb-devops@cisco.com
Server Temp Key: ECDH, P-256, 256 bits
---
SSL handshake has read 6164 bytes and written 138 bytes
---
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES256-GCM-SHA384
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : ECDHE-RSA-AES256-GCM-SHA384
    Session-ID: 9965F3B5DF5C740E7FEF85D01DB29FA2688237B007C46EDE537DF169031276B7
    Session-ID-ctx:
    Master-Key: 81A4848377685711A43018559E14CA4842A82FDC27017D1CCD6F32894DC32148219A91C5ED7F4E4865734CBF50417E6D
    Start Time: 1683543981
    Timeout   : 7200 (sec)
    Verify return code: 19 (self signed certificate in certificate chain)
---
```

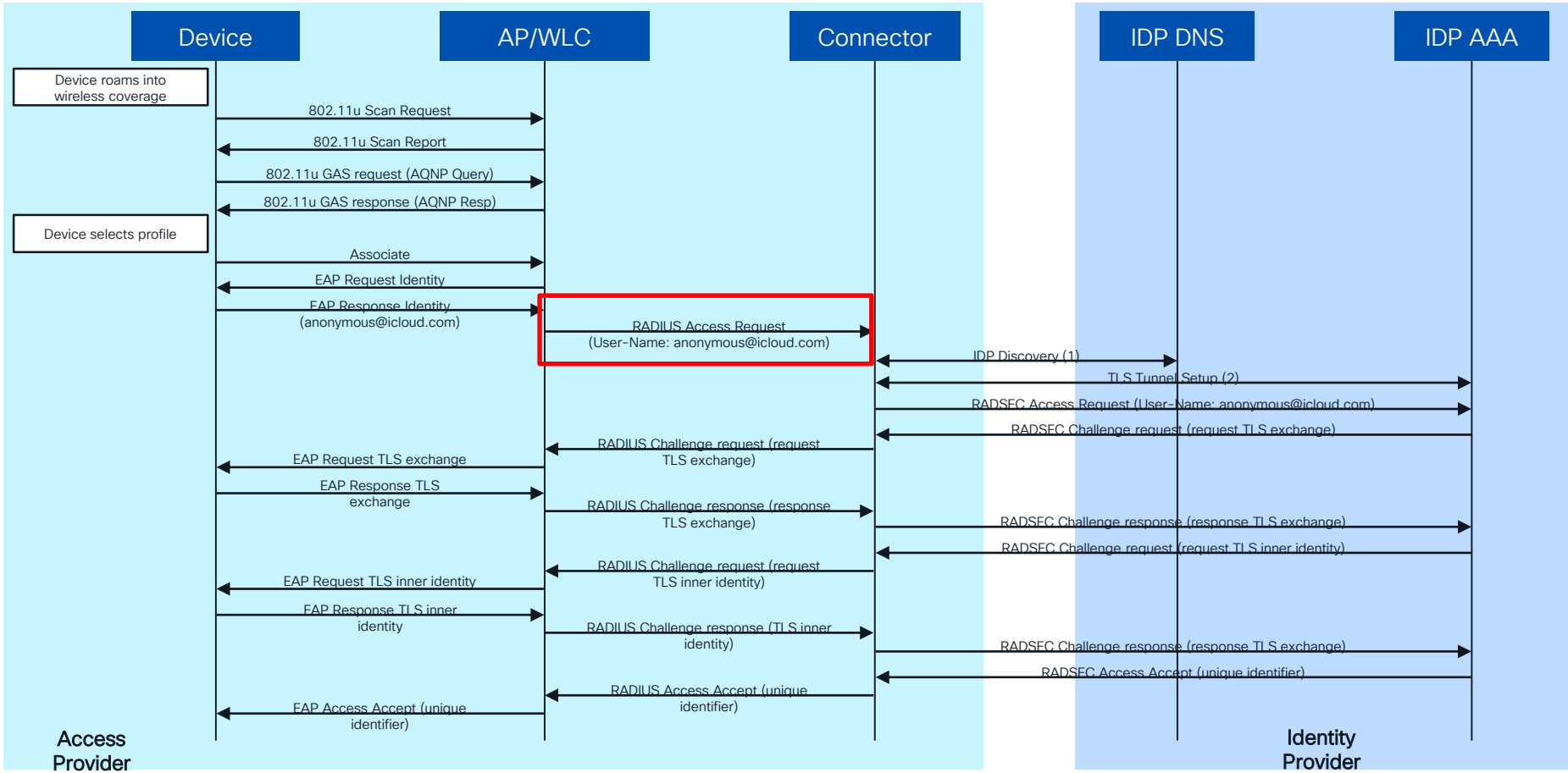
openssl s_client -connect idp.openroaming.net:2083 -showcerts show certificate chain(s)

openssl s_client -connect idp.openroaming.net:2083 -msg show all messages

Onboarding flow – packet flow inside TLS Tunnel



RADSEC EAP Authentication: EAP-TTLS



RADSEC EAP Authentication: EAP-TTLS (detailed)

AP/WLC Radius Access-Request to Spaces Connector:

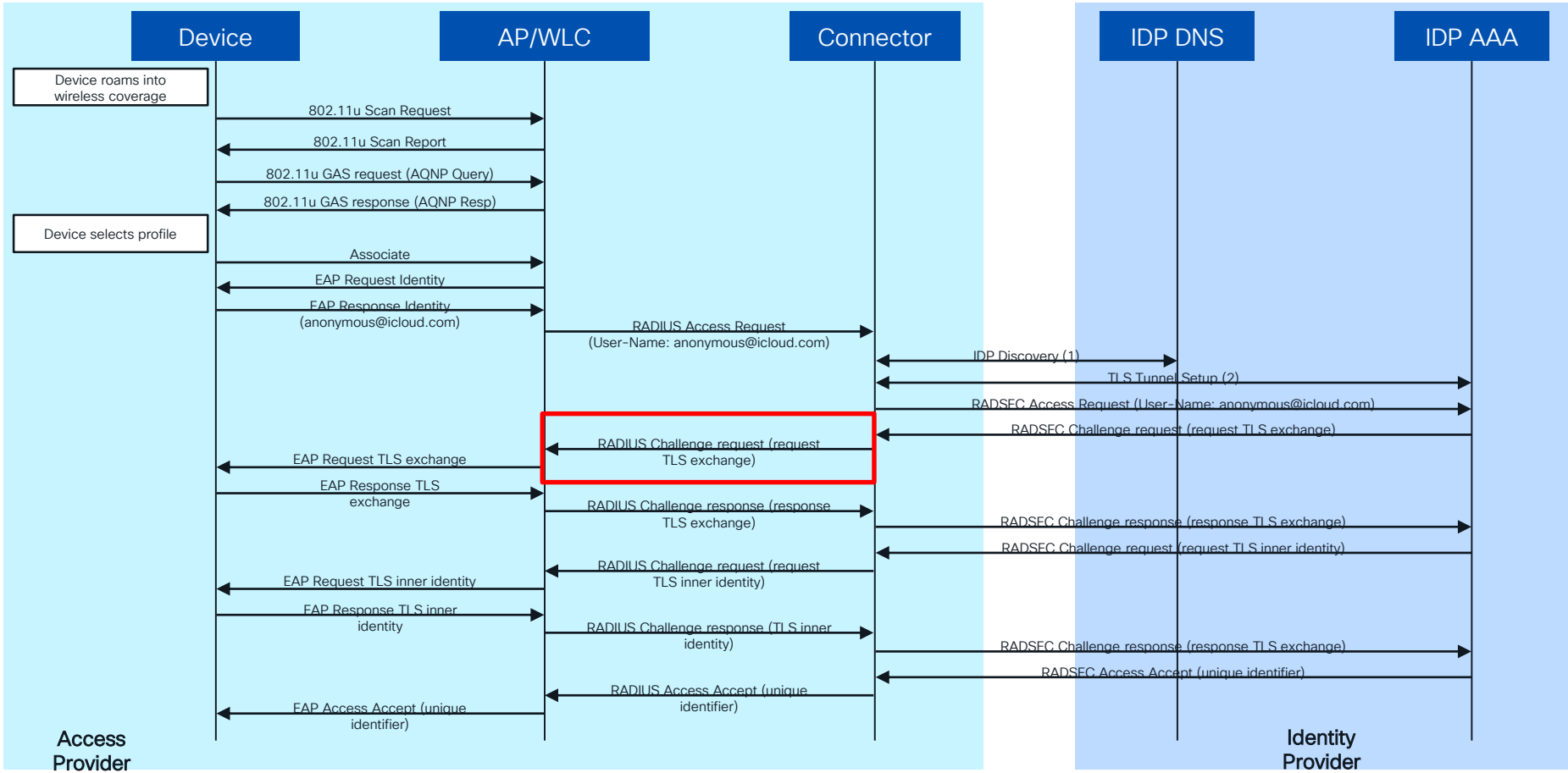
```
RADIUS Protocol
   Code: Access-Request (1)
   Packet identifier: 0x72 (114)
   Length: 528
   Authenticator: 029bc20178f543fc16df1aecc80ae721
   [The response to this request is in frame 38]
   Attribute Value Pairs
   > AVP: t=User-Name(1) l=38 val=anonymous@[redacted]openroaming.net
   > AVP: t=NAS-IP-Address(4) l=6 val=192.168.1.241
   > AVP: t=NAS-Identifier(32) l=19 val=openroaming_clair
   > AVP: t=NAS-Port-Type(61) l=6 val=Wireless-802.11(19)
   > AVP: t=Service-Type(6) l=6 val=Framed(2)
   > AVP: t=NAS-Port(5) l=6 val=2
   > AVP: t=Calling-Station-Id(31) l=19 val=BA-C3-F1-65-35-40
   > AVP: t=Connect-Info(77) l=56 val=CONNECT 54.00 Mbps / 802.11ac / RSSI: 51 / Channel: 52
   > AVP: t=Acct-Session-Id(44) l=18 val=94FD481E79523AE8
   > AVP: t=Acct-Multi-Session-Id(50) l=18 val=987D9F3891EA287E
   > AVP: t=Unknown-Attribute(186) l=6 val=000fac04
   > AVP: t=Unknown-Attribute(187) l=6 val=000fac04
   > AVP: t=Unknown-Attribute(188) l=6 val=000fac01
   > AVP: t=Vendor-Specific(26) l=16 vnd=Meraki Networks, Inc.(29671)
   > AVP: t=Vendor-Specific(26) l=8 vnd=Meraki Networks, Inc.(29671)
   > AVP: t=Vendor-Specific(26) l=8 vnd=Meraki Networks, Inc.(29671)
   > AVP: t=Called-Station-Id(30) l=27 val=E0-CB-BC-8D-55-41:OR@Home
   > AVP: t=Multi-Link-Flag(126) l=14 val=[unhandled integer length(12)]
   > AVP: t=Vendor-Specific(26) l=25 vnd=Meraki Networks, Inc.(29671)
   > AVP: t=Framed-MTU(12) l=6 val=1400
   > AVP: t=EAP-Message(79) l=138 Last Segment[1]
   > AVP: t=State(24) l=18 val=9cc9df109ad4caea21a996a61fe4d5e4
   > AVP: t=Vendor-Specific(26) l=9 vnd=Wi-Fi Alliance(40808)
   > AVP: t=Vendor-Specific(26) l=11 vnd=Wi-Fi Alliance(40808)
   > AVP: t=Message-Authenticator(80) l=18 val=91bf8fb835440d50a876c882d807d981
```

=> Anonymous User Name

=> NAS is the AP/WLC

=> AP Radio MAC : SSID

RADSEC EAP Authentication: EAP-TTLS



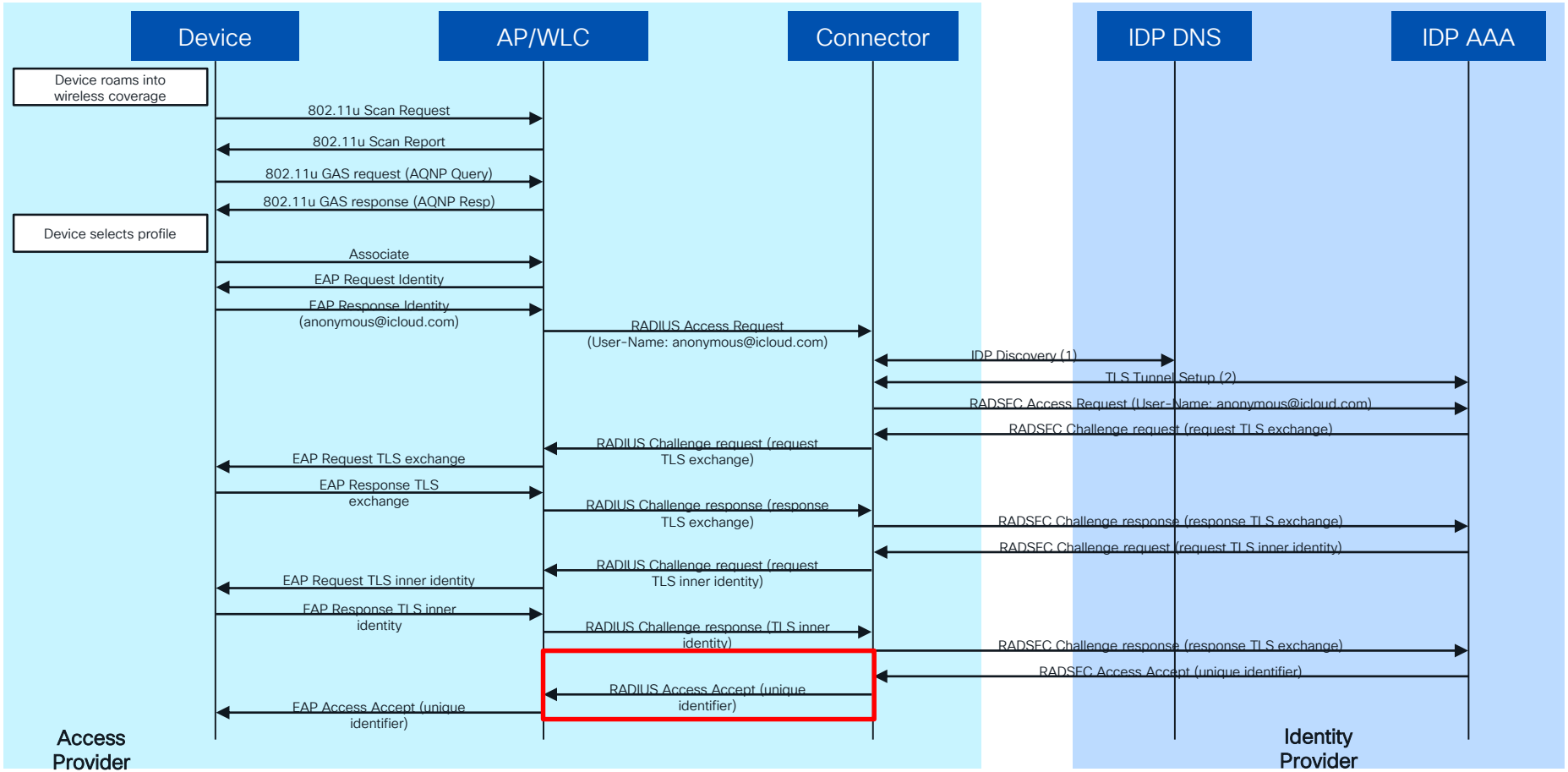
RADSEC EAP Authentication: EAP-TTLS (detailed)

Spaces Connector Radius Access-Challenge to AP/WLC

```
RADIUS Protocol
   Code: Access-Challenge (11)
   Packet identifier: 0x60 (96)
   Length: 64
   Authenticator: 64e7ddb7501b6016beffd763da5523f9
   [This is a response to a request in frame 1]
   [Time from request: 0.342074000 seconds]
 Attribute Value Pairs
   AVP: t=EAP-Message(79) l=8 Last Segment[1]
      Type: 79
      Length: 8
      EAP fragment: 01be00061520
    Extensible Authentication Protocol
       Code: Request (1)
       Id: 190
       Length: 6
       Type: Tunneled TLS EAP (EAP-TTLS) (21)
     EAP-TLS Flags: 0x20
        0... .... = Length Included: False
        .0.. .... = More Fragments: False
        ..1. .... = Start: True
        .... .000 = Version: 0
   AVP: t=Message-Authenticator(80) l=18 val=04d5b56f802938320d584d138b9c4512
   AVP: t=State(24) l=18 val=21d769f721697cee55884a6c8491f4a3
```

=> EAP Type TTLS

RADSEC EAP Authentication: EAP-TTLS



RADSEC EAP Authentication: EAP-TTLS (detailed)

Spaces Connector Radius Access-Accept to AP/WLC:

```
RADIUS Protocol
   Code: Access-Accept (2)
   Packet identifier: 0x73 (115)
   Length: 301
   Authenticator: cc15016c1c0cd84666938a2ce996c620
   [This is a response to a request in frame 39]
   [Time from request: 0.175524000 seconds]
 Attribute Value Pairs
   > AVP: t=Chargeable-User-Identity(89) l=24 val=ciscolive.or@gmail.com
   > AVP: t=User-Name(1) l=61 val=1b9d52d3b42817032a9b8eccbf677fa4@[redacted].openroaming.net
   > AVP: t=Vendor-Specific(26) l=56 vnd=ciscoSystems(9)
   > AVP: t=Vendor-Specific(26) l=58 vnd=Microsoft(311)
   > AVP: t=Vendor-Specific(26) l=58 vnd=Microsoft(311)
   > AVP: t=EAP-Message(79) l=6 Last Segment[1]
   > AVP: t=Message-Authenticator(80) l=18 val=d9339a5b6afe6409cf40feb6b677eda1
```

=> Inner Identity – user shared the email

=> Unique Identifier

OpenRoaming – Privacy Built-in

1

Authentication is private

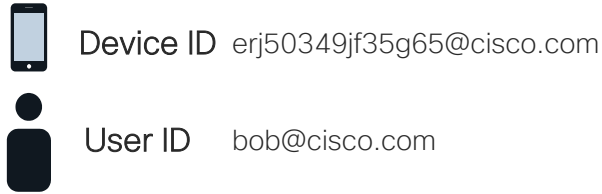
Secure and private authentication between user's device and IDP

2

User and device are identified in context

Identified with persistent Device ID and User ID with IDP context

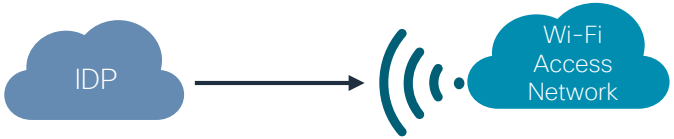
IDP shares (anonymized) data in the secured path



3

IDP shares identities on the user's behalf

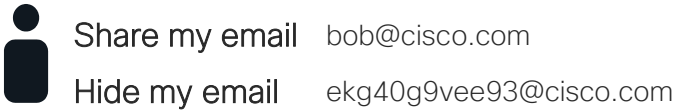
IDP manages identity and privacy for the user



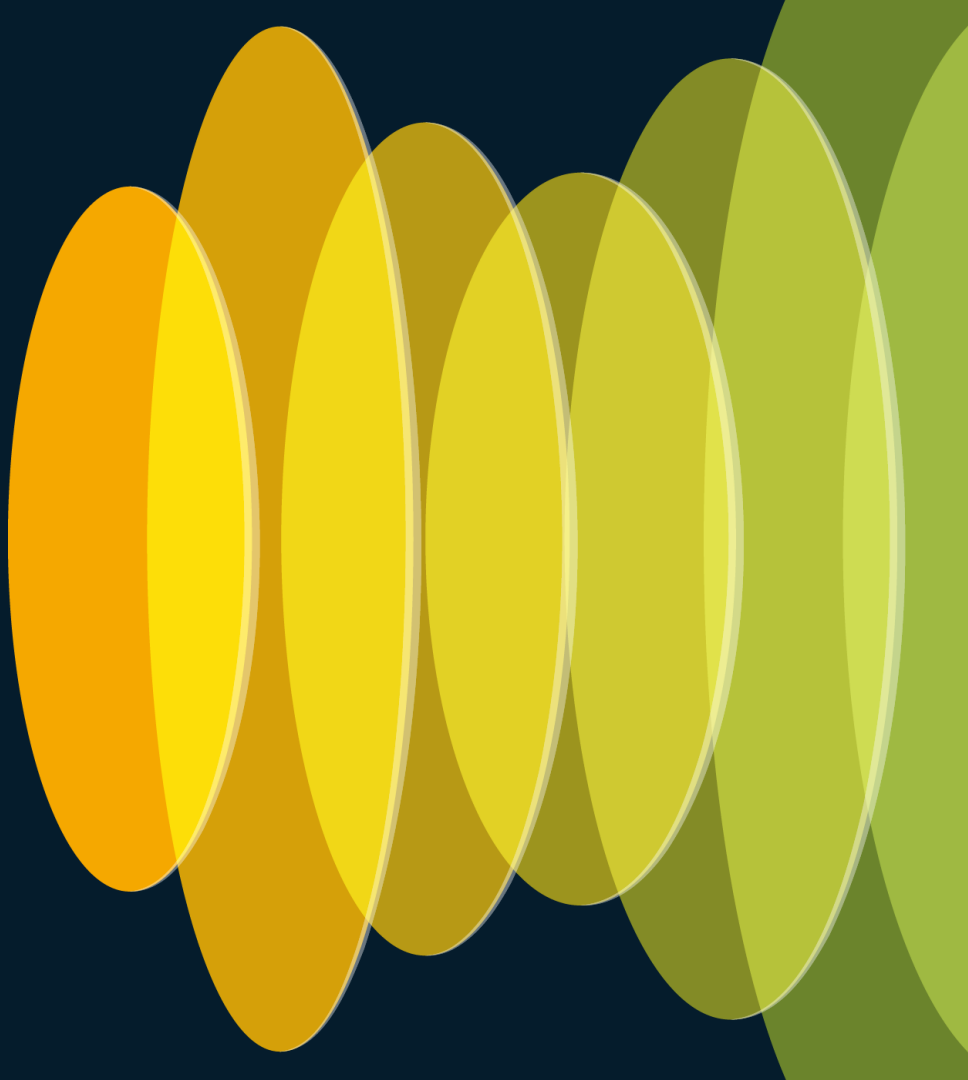
4

Privacy with user consent

User controls privacy, identifiers are always persistent



Your own Identity: SDK and Web-based provisioning



cisco Live!

Spaces SDK

Main SDK methods

Initialization

- The app registers with the Cisco DNA Spaces account using the account API key.

User Identity Association

- User logs onto the app using either:
  - IDP supported by DNA Spaces Backend
  - Enterprise or Loyalty ID
- User sets their privacy preference

Install OpenRoaming Profile

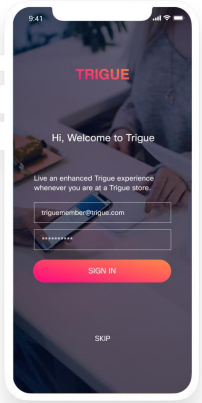
- The profile associated with the user identity is installed on their device
- Allows devices to automatically log into OpenRoaming networks

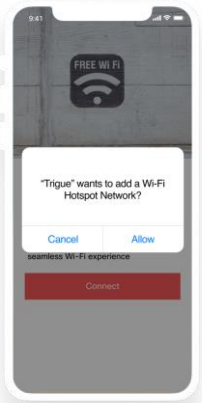
Enable Push Notifications

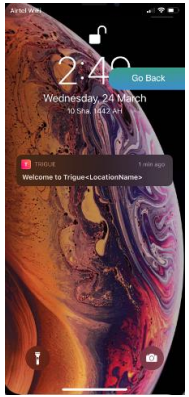
- Allows for DNA Spaces backend to send notifications to user devices

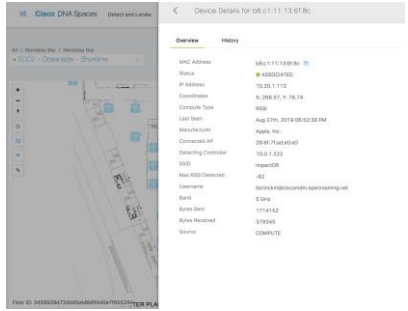
Location Information

- The app will report back the current location of the device back to DNA Spaces
- The location can be used for use cases like wayfinding or targeted engagements



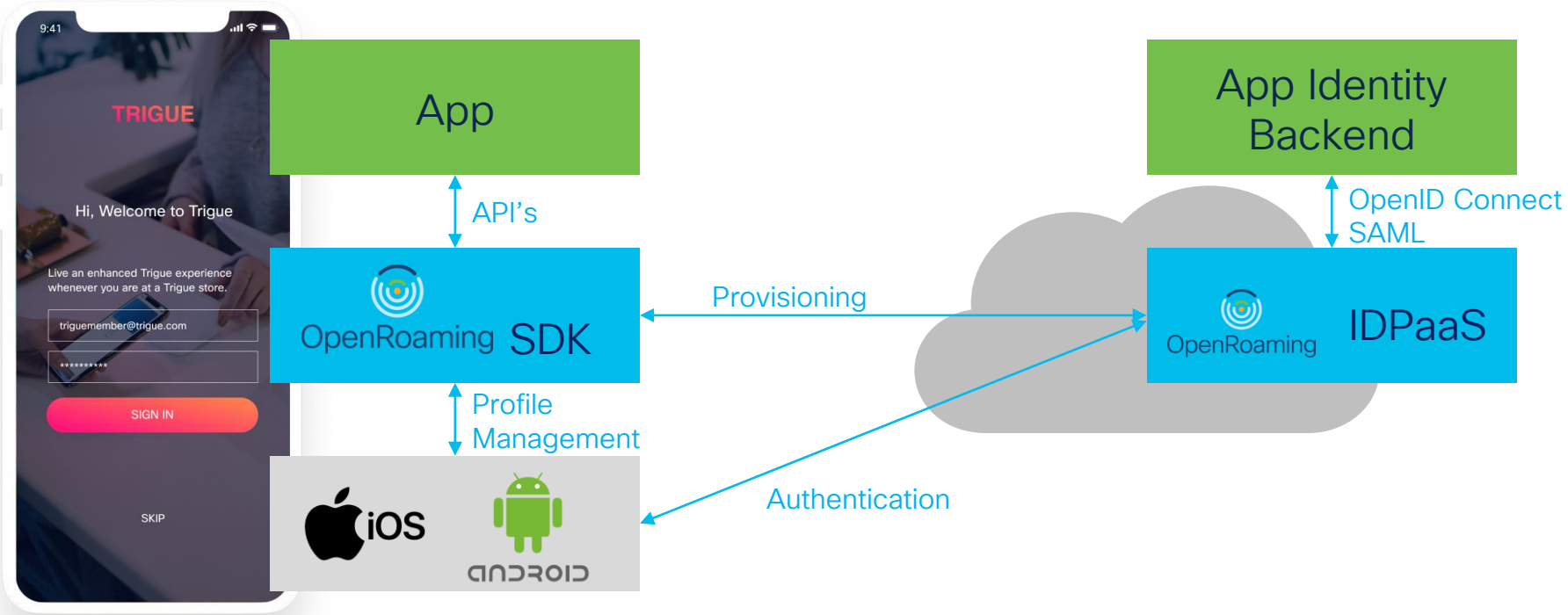




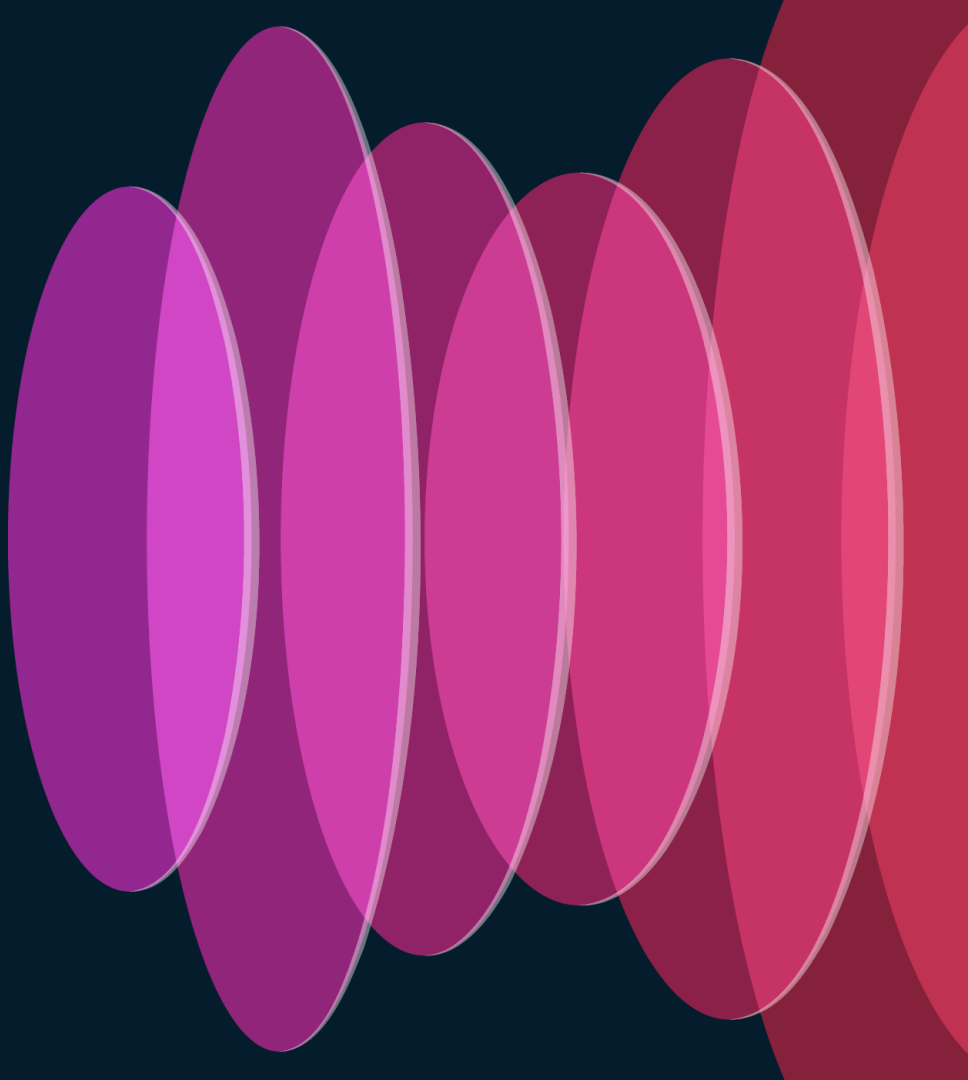


SDK for iOS & Android

https://developer.cisco.com/dna-spaces-sdk/



Configuration and Live Demo



Spaces OpenRoaming Configuration Steps

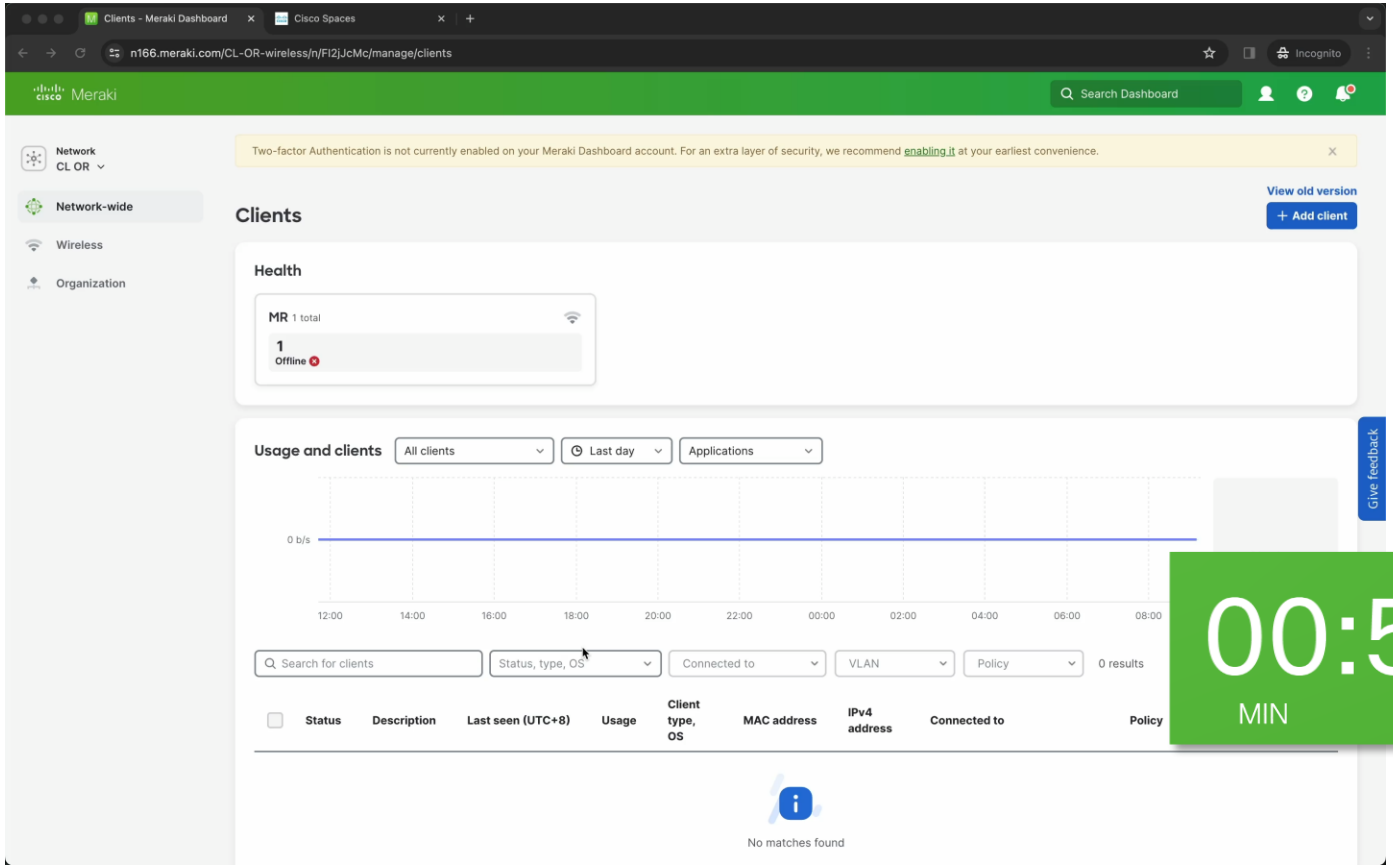
1. Create an OpenRoaming Profile
2. Enable Hotspot Connector
3. Select Catalyst controller
4. Configure the OpenRoaming SSID

cisco Meraki

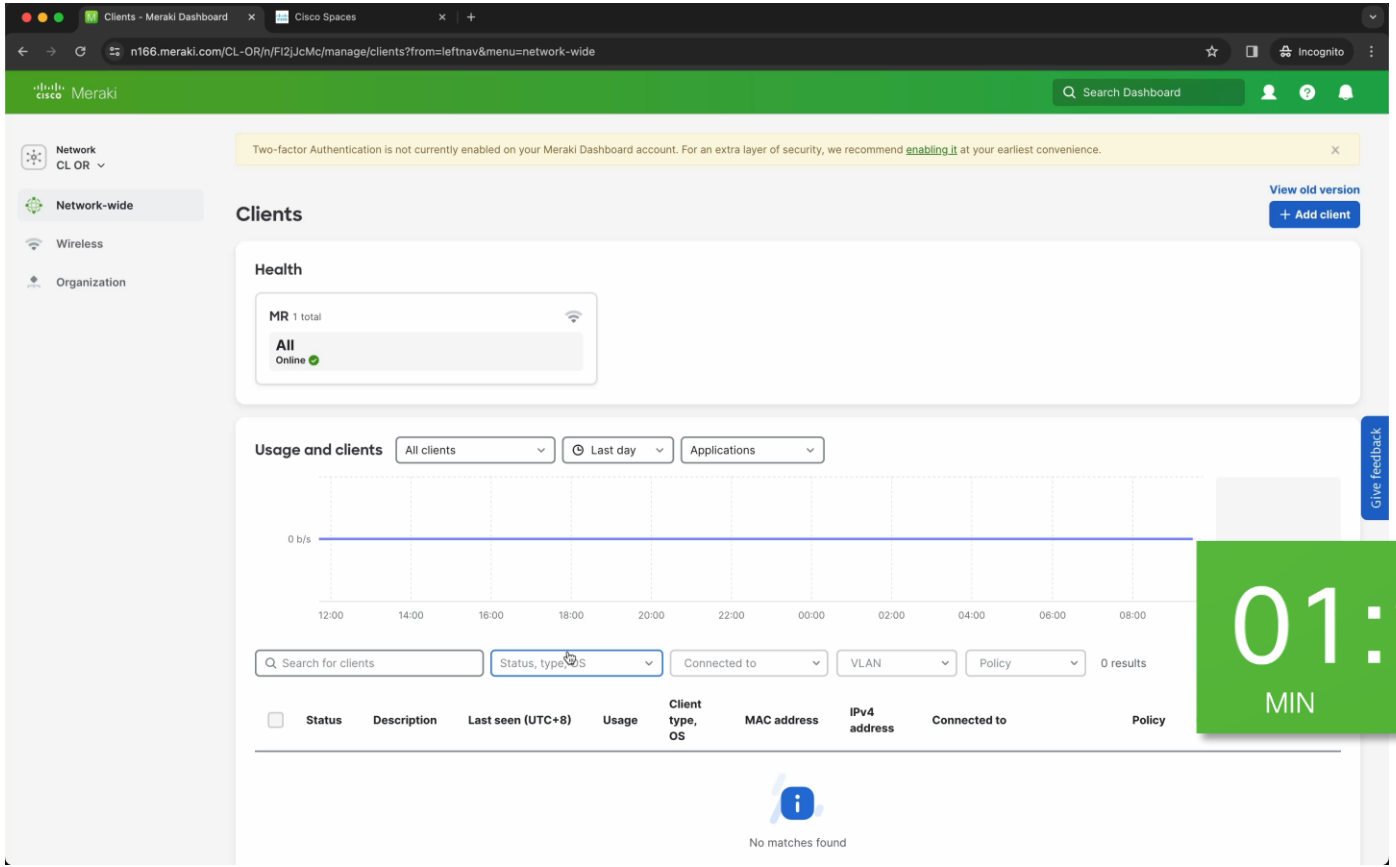
1. Create an OpenRoaming Profile
2. Enable Meraki API
3. Select Meraki network
4. Configure the OpenRoaming SSID

Demo Time!

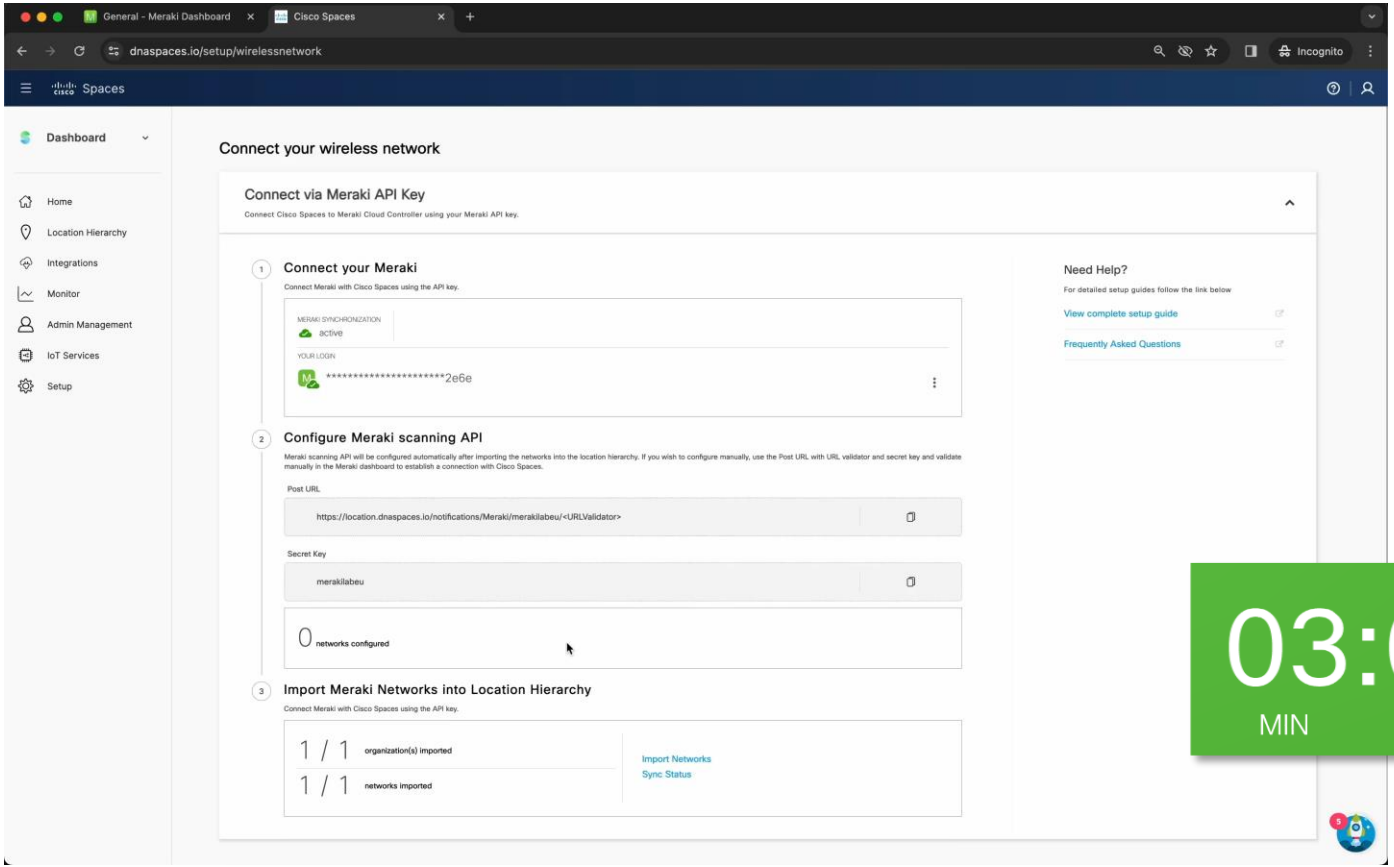
Prerequisites



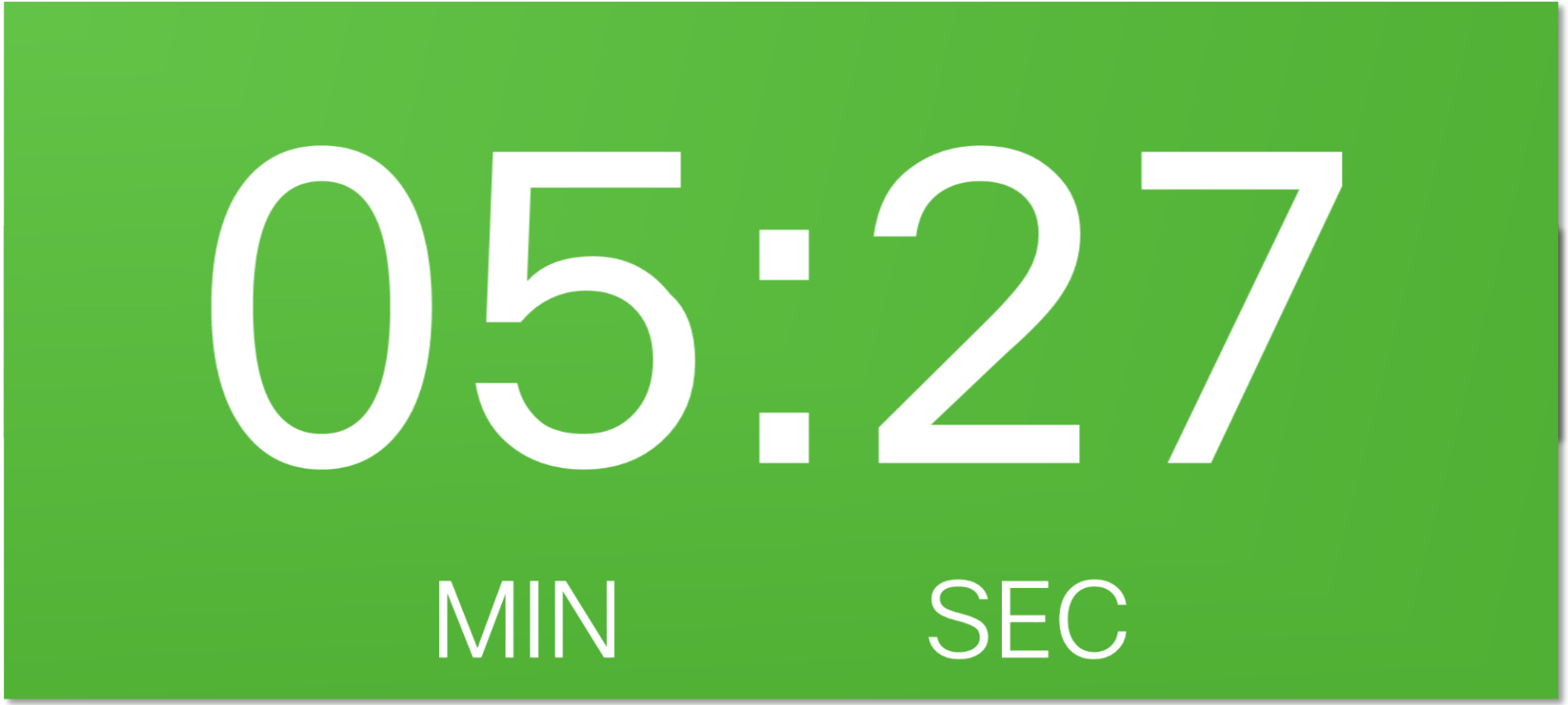
Connect Meraki Dashboard with Cisco Spaces



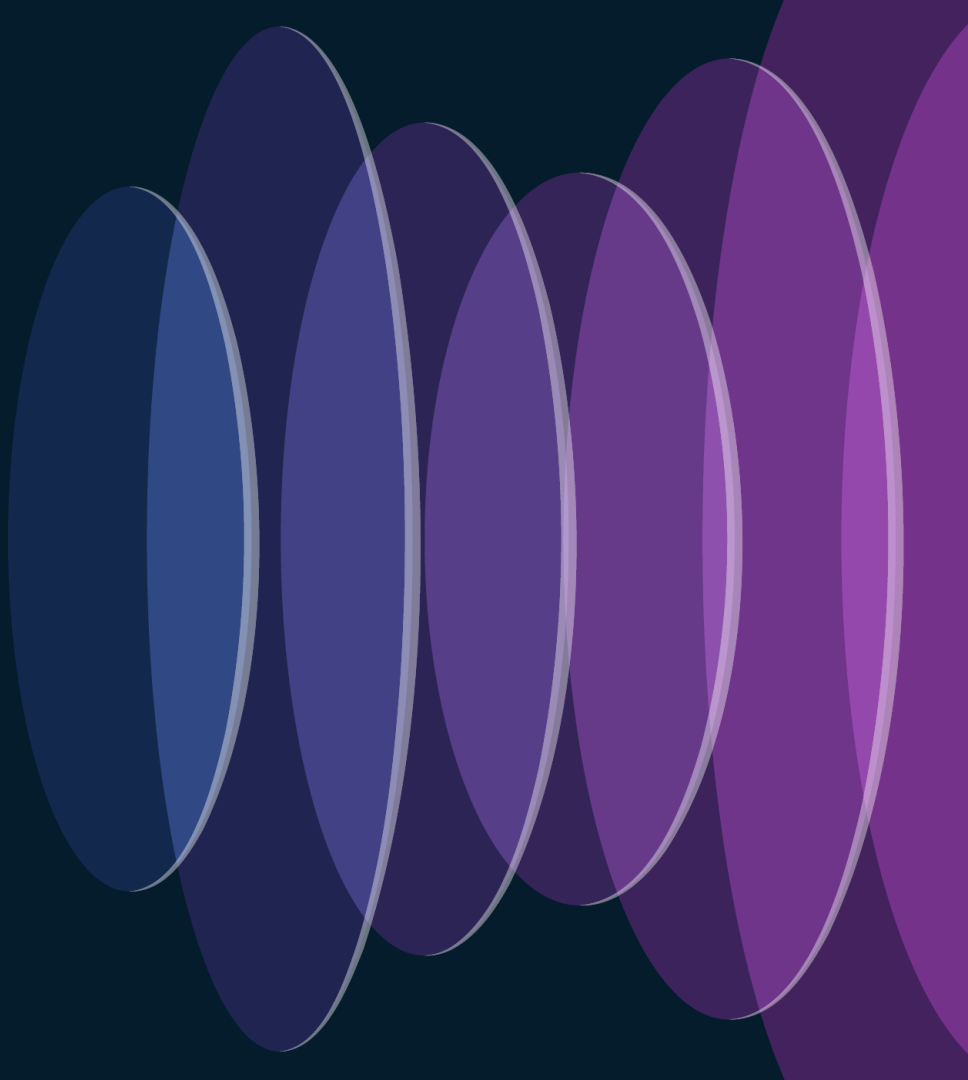
Configuration



Let’s summarize it

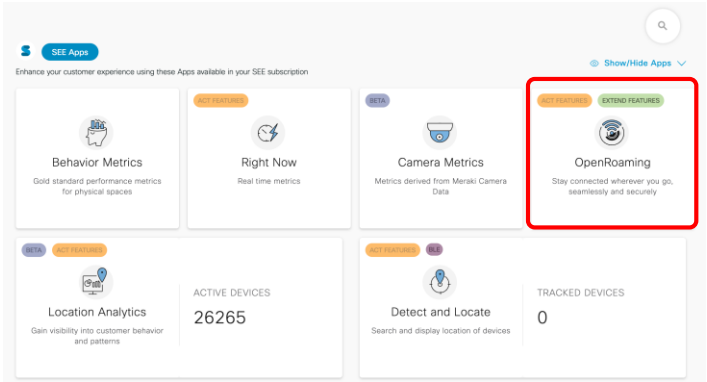


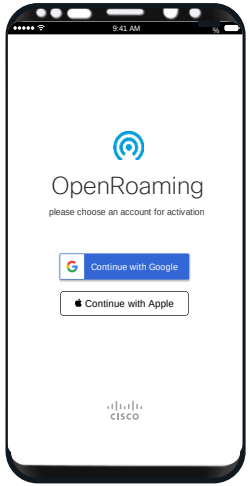
Conclusion



Conclusion: Try OpenRoaming!

- If you do not have a Spaces account, get a free trial: https://spaces.cisco.com/start-for-free/
- If you do not have a Meraki account, and device, get free trial: https://meraki.cisco.com/form/trial/
- If you have a spaces account, log in and activate OpenRoaming: https://ciscospaces.io/login



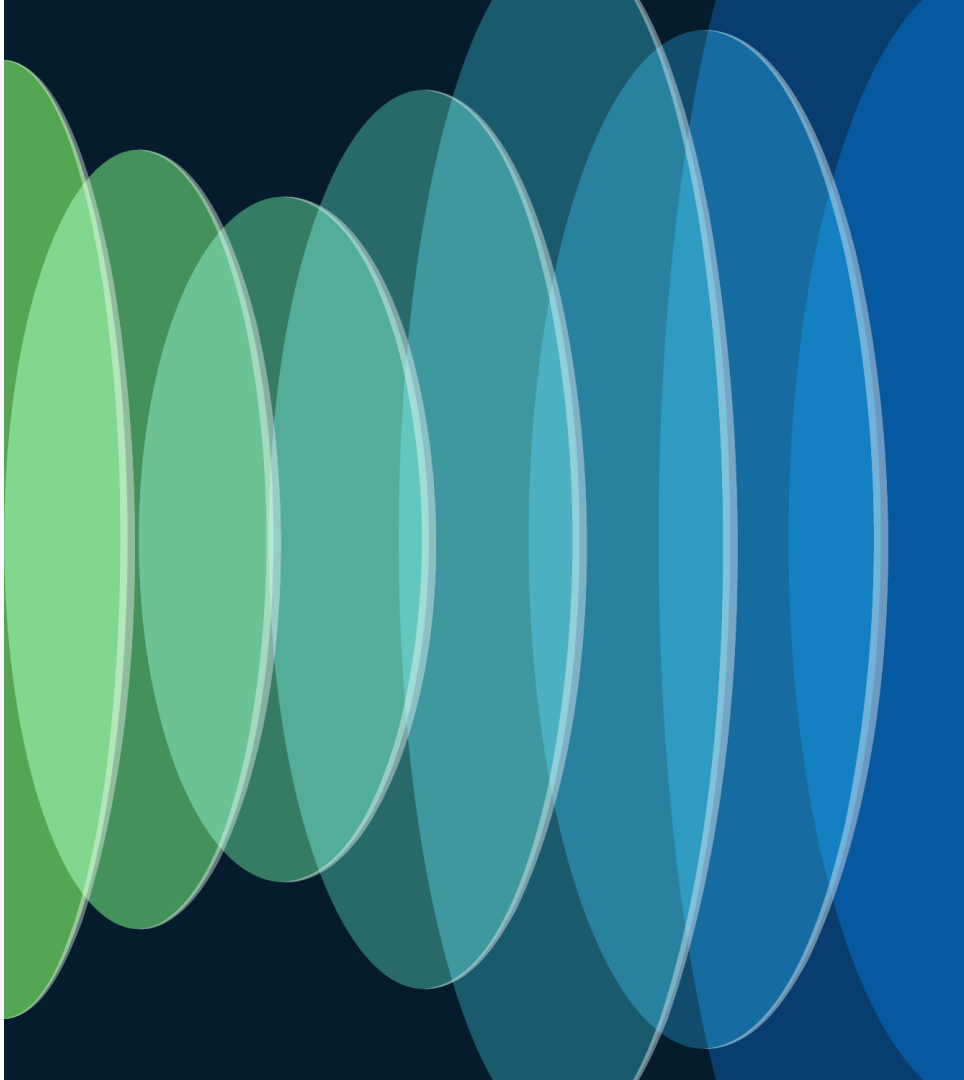


Try it out!

References to learn more about OpenRoaming

- Catalyst 9800 WLC Config Guide – OpenRoaming:
  - https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-11/config-guide/b_wl_17_eleven_cg/m_hotspot-2.html
- Meraki OpenRoaming integration with Cisco Spaces Documentation:
  - https://documentation.meraki.com/MR/Other_Topics/OpenRoaming_integration_with_Cisco_Spaces
- Cisco Spaces OpenRoaming Configuration Guide:
  - https://www.cisco.com/c/en/us/td/docs/wireless/spaces/openroaming/b-spaces-or-cg/m-config-or.html
- Cisco Spaces Connector 3.0 Config Guide:
  - https://www.cisco.com/c/en/us/td/docs/wireless/spaces/connector/config/b_connector_30.html
- How to configure OpenRoaming at C9800 Video: https://youtu.be/XsD6e6F6u4k
- Cisco Spaces SDK: https://developer.cisco.com/dna-spaces-sdk/
- WBA OpenRoaming: https://wballiance.com/openroaming/

Q&A



Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact us at:
bbrinckm@cisco.com
jsroga@cisco.com

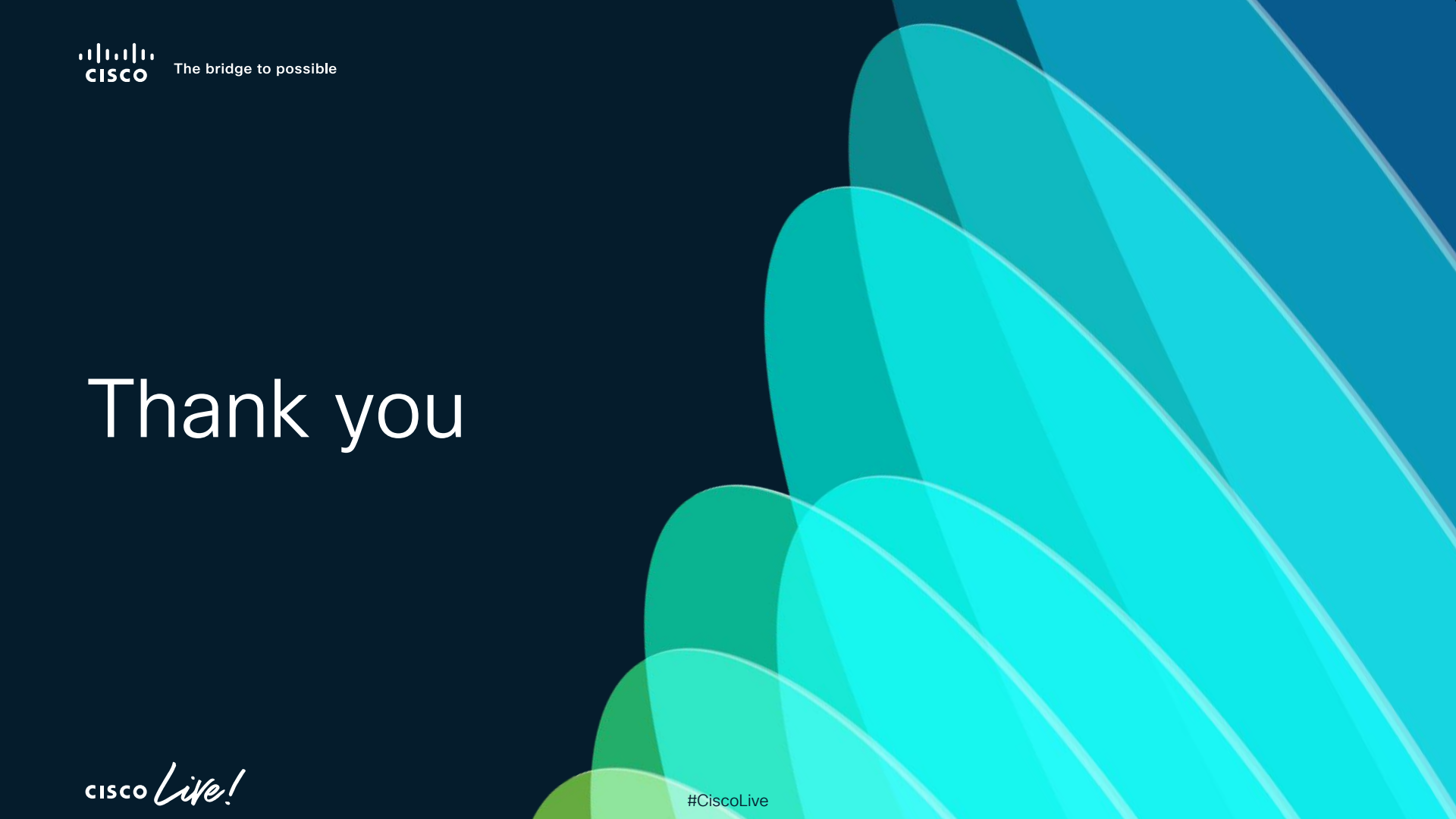
Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to **win 1 of 5 full conference passes** to Cisco Live 2025.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn **exclusive prizes!**

Complete your surveys in the **Cisco Live mobile app.**


The bridge to possible
Thank you
cisco Live!
#CiscoLive