Roam: Decentralized OpenRoaming WiFi Networks

Powered by MetaBlox Labs

Roam

LEGAL DISCLAIMER

PLEASE READ THE ENTIRETY OF THIS "LEGAL DISCLAIMER" SECTION CAREFULLY. NOTHING HEREIN CONSTITUTES LEGAL, FINANCIAL, BUSINESS OR TAX ADVICE AND YOU ARE STRONGLY ADVISED TO CONSULT YOUR OWN LEGAL, FINANCIAL, TAX OR OTHER PROFESSIONAL ADVISOR(S) BEFORE ENGAGING IN ANY ACTIVITY IN CONNECTION HEREWITH. NEITHER METABLOX TECHNOLOGIES INC. (THE **COMPANY**), ANY OF THE PROJECT CONTRIBUTORS (THE **ROAM TEAM**) WHO HAVE WORKED ON THE ROAM NETWORK (AS DEFINED HEREIN) OR PROJECT TO DEVELOP THE ROAM NETWORK IN ANY WAY WHATSOEVER, ANY DISTRIBUTOR AND/OR VENDOR OF $ROAM TOKENS (OR SUCH OTHER RE-NAMED OR SUCCESSOR TICKER CODE OR NAME OF SUCH TOKENS) (THE **DISTRIBUTOR**), NOR ANY SERVICE PROVIDER SHALL BE LIABLE FOR ANY KIND OF DIRECT OR INDIRECT DAMAGE OR LOSS WHATSOEVER WHICH YOU MAY SUFFER IN CONNECTION WITH ACCESSING THE PAPER, DECK OR MATERIAL RELATING TO $ROAM (THE **TOKEN DOCUMENTATION**) AVAILABLE ON THE ROAM PROJECT WEBSITE (THE **WEBSITE**, INCLUDING ANY SUB-DOMAINS THEREON) OR ANY OTHER WEBSITES OR MATERIALS PUBLISHED OR COMMUNICATED BY THE COMPANY OR ITS REPRESENTATIVES FROM TIME TO TIME.

Project purpose: You agree that you are acquiring $ROAM to participate in the Roam network and to obtain services on the ecosystem thereon. The Company, the Distributor and their respective affiliates would develop and contribute to the underlying source code for the Roam network. The Company is acting solely as an arms' length third party in relation to the $ROAM distribution, and not in the capacity as a financial advisor or fiduciary of any person with regard to the distribution of $ROAM.

Nature of the Token Documentation: The Token Documentation is a conceptual paper that articulates some of the main design principles and ideas for the creation of a digital token to be known as $ROAM. The Token Documentation and the Website are intended for general informational purposes only and do not constitute a prospectus, an offer document, an offer of securities, a solicitation for investment, any offer to sell any product, item, or asset (whether digital or otherwise), or any offer to engage in business with any external individual or entity provided in said documentation. The information herein may not be exhaustive and does not imply any element of, or solicit in any way, a legally-binding or contractual relationship. There is no assurance as to the accuracy or completeness of such information and no representation, warranty or undertaking is or purported to be provided as to the accuracy or completeness of such information. Where the Token Documentation or the Website includes information that has been obtained from third party sources, the Company, the Distributor, their respective affiliates and/or the Roam team have not independently verified the accuracy or completeness of such information. Further, you acknowledge that the project development roadmap, platform/network functionality are subject to change and that the Token Documentation or the Website may become outdated as a result; and neither the Company nor the Distributor is under any obligation to update or correct this document in connection therewith.

Validity of Token Documentation and Website: Nothing in the Token Documentation or the Website constitutes any offer by the Company, the Distributor, or the Roam team to sell any $ROAM (as defined herein) nor shall it or any part of it nor the fact of its presentation form the basis of, or be relied upon in connection with, any contract or investment decision. Nothing contained in the Token Documentation or the Website is or may be relied upon as a promise, representation or undertaking as to the future performance of the Roam network. The agreement between the Distributor (or any third party) and you, in relation to any distribution or transfer of $ROAM, is to be governed only by the separate terms and conditions of such agreement.

The information set out in the Token Documentation and the Website is for community discussion only and is not legally binding. No person is bound to enter into any contract or binding legal commitment in relation to the acquisition of $ROAM, and no digital asset or other form of payment is to be accepted on the basis of the Token Documentation or the Website. The agreement for distribution of $ROAM and/or continued holding of $ROAM shall be governed by a separate set of Terms and Conditions or Token Distribution Agreement (as the case may be) setting out the terms of such distribution and/or continued holding of $ROAM (the Terms and Conditions), which shall be separately provided to you or made available on the Website. The Terms and Conditions must be read together with the Token Documentation. In the event of any inconsistencies between the Terms and Conditions and the Token Documentation or the Website, the Terms and Conditions shall prevail.

Deemed Representations and Warranties: By accessing the Token Documentation or the Website (or any part thereof), you shall be deemed to represent and warrant to the Company, the Distributor, their respective affiliates, and the Roam team as follows:

(a) in any decision to acquire any $ROAM, you have not relied and shall not rely on any statement set out in the Token Documentation or the Website;

(b) you shall at your own expense ensure compliance with all laws, regulatory requirements and restrictions applicable to you (as the case may be);

(c) you acknowledge, understand and agree that $ROAM may have no value, there is no guarantee or representation of value or liquidity for $ROAM, and $ROAM is not an investment product nor is it intended for any speculative investment whatsoever;

(d) none of the Company, the Distributor, their respective affiliates, and/or the Roam team shall be responsible for or liable for the value of $ROAM, the transferability and/or liquidity of $ROAM and/or the availability of any market for $ROAM through third parties or otherwise; and

(e) you acknowledge, understand and agree that you are not eligible to participate in the distribution of $ROAM if you are a citizen, national, resident (tax or otherwise), domiciliary and/or green card or permanent visa holder of a geographic area or country (i) where it is likely that the distribution of $ROAM would be construed as the sale of a security (howsoever named), financial service or investment product and/or (ii) where participation in token distributions is prohibited by applicable law, decree, regulation, treaty, or administrative act (including without limitation the United States of America, Canada, and the People's Republic of China); and to this effect you agree to provide all such identity verification document when requested in order for the relevant checks to be carried out.

The Company, the Distributor and the Roam team do not and do not purport to make, and hereby disclaims, all representations, warranties or undertaking to any entity or person (including without limitation warranties as to the accuracy, completeness, timeliness, or reliability of the contents of the Token Documentation or the Website, or any other materials published by the Company or the Distributor). To the maximum extent permitted by law, the Company, the Distributor, their respective affiliates and service providers shall not be liable for any indirect, special, incidental, consequential or other losses of any kind, in tort, contract or otherwise (including, without limitation, any liability arising from default or negligence on the part of any of them, or any loss of revenue, income or profits, and loss of use or data) arising from the use of the Token Documentation or the Website, or any other materials published, or its contents (including without limitation any errors or omissions) or otherwise arising in connection with the same. Prospective acquirors of $ROAM should carefully consider and evaluate all risks and uncertainties (including financial and legal risks and uncertainties) associated with the distribution of $ROAM, the Company, the Distributor and the Roam team.

$ROAM Token: $ROAM are designed to be utilised, and that is the goal of the $ROAM distribution. In particular, it is highlighted that $ROAM:

(a) does not have any tangible or physical manifestation, and does not have any intrinsic value/pricing (nor does any person make any representation or give any commitment as to its value);

(b) is non-refundable, not redeemable for any assets of any entity or organisation, and cannot be exchanged for cash (or its equivalent value in any other digital asset) or any payment obligation by the Company, the Distributor or any of their respective affiliates;

(c) does not represent or confer on the token holder any right of any form with respect to the Company, the Distributor (or any of their respective affiliates), or their revenues or assets, including without limitation any right to receive future dividends, revenue, shares, ownership right or stake, share or security, any voting, distribution, redemption, liquidation, proprietary (including all forms of intellectual property or licence rights), right to receive accounts, financial statements or other financial data, the right to requisition or participate in shareholder meetings, the right to nominate a director, or other financial or legal rights or equivalent rights, or intellectual property rights or any other form of participation in or relating to the Roam network, the Company, the Distributor and/or their service providers;

(d) is not intended to represent any rights under a contract for differences or under any other contract the purpose or intended purpose of which is to secure a profit or avoid a loss;

(e) is not intended to be a representation of money (including electronic money), payment instrument, security, commodity, bond, debt instrument, unit in a collective investment or managed investment scheme or any other kind of financial instrument or investment;

(f) is not a loan to the Company, the Distributor or any of their respective affiliates, is not intended to represent a debt owed by the Company, the Distributor or any of their respective affiliates, and there is no expectation of profit nor interest payment; and

(g) does not provide the token holder with any ownership or other interest in the Company, the Distributor or any of their respective affiliates.

Notwithstanding the $ROAM distribution, users have no economic or legal right over or beneficial interest in the assets of the Company, the Distributor, or any of their affiliates after the token distribution.

For the avoidance of doubt, neither the Company nor the Distributor deals in, or is in the business of buying or selling any virtual asset or digital payment token (including $ROAM). Any sale or distribution of tokens would be performed during a restricted initial period solely for the purpose of obtaining project development funds, raising market/brand awareness, as well as community building and social engagement; this is not conducted with any element of repetitiveness or regularity which would constitute a business.

To the extent a secondary market or exchange for trading $ROAM does develop, it would be run and operated wholly independently of the Company, the Distributor, the distribution of $ROAM and the Roam network. Neither the Company nor the Distributor will create such secondary markets nor will either entity act as an exchange for $ROAM.

Informational purposes only: The information set out herein is only conceptual, and describes the future development goals for the Roam network to be developed. In particular, the project roadmap in the Token Documentation is being shared in order to outline some of the plans of the Roam team, and is provided solely for **INFORMATIONAL PURPOSES** and does not constitute any binding commitment. Please do not rely on this information in deciding whether to participate in the token distribution because ultimately, the development, release, and timing of any products, features or functionality remains at the sole discretion of the Company, the Distributor or their respective affiliates, and is subject to change. Further, the Token Documentation or the Website may be amended or replaced from time to time. There are no obligations to update the Token Documentation or the Website, or to provide recipients with access to any information beyond what is provided herein.

Regulatory approval: No regulatory authority has examined or approved, whether formally or informally, any of the information set out in the Token Documentation or the Website. No such action or assurance has been or will be taken under the laws, regulatory requirements or rules of any jurisdiction. The publication, distribution or dissemination of the Token Documentation or the Website does not imply that the applicable laws, regulatory requirements or rules have been complied with.

Cautionary Note on forward-looking statements: All statements contained herein, statements made in press releases or in any place accessible by the public and oral statements that may be made by the Company, the Distributor and/or the Roam team, may constitute forward-looking statements (including statements regarding the intent, belief or current expectations with respect to market conditions, business strategy and plans, financial condition, specific provisions and risk management practices). You are cautioned not to place undue reliance on these forward-looking statements given that these statements involve known and unknown risks, uncertainties and other factors that may cause the actual future results to be materially different from that described by such forward-looking statements, and no independent third party has reviewed the reasonableness of any such statements or assumptions. These forward-looking statements are applicable only as of the date indicated in the Token Documentation, and the Company, the Distributor as well as the Roam team expressly disclaim any responsibility (whether express or implied) to release any revisions to these forward-looking statements to reflect events after such date.

References to companies and platforms: The use of any company and/or platform names or trademarks herein (save for those which relate to the Company, the Distributor or their respective affiliates) does not imply any affiliation with, or endorsement by, any third party. References in the Token Documentation or the Website to specific companies and platforms are for illustrative purposes only.

English language: The Token Documentation and the Website may be translated into a language other than English for reference purpose only and in the event of conflict or ambiguity between the English language version and translated versions of the Token Documentation or the Website, the English language versions shall prevail. You acknowledge that you have read and understood the English language version of the Token Documentation and the Website.

No Distribution: No part of the Token Documentation or the Website is to be copied, reproduced, distributed or disseminated in any way without the prior written consent of the Company or the Distributor. By attending any presentation on this Token Documentation or by accepting any hard or soft copy of the Token Documentation, you agree to be bound by the foregoing limitations.

Abstract

Roam represents a pioneering protocol that empowers users to seamlessly traverse public WiFi networks using their decentralized identifiers (DIDs) and corresponding verifiable credentials (VCs). By doing so, it establishes a unified global WiFi OpenRoaming network, seamlessly interlinking distinct WiFi networks. This approach eliminates the tiresome cycle of repeated log-ins, reconnecting, password sharing, and redundant registrations that users currently contend with during local or international travels. The VC/DID-based Web3.0 WiFi credential is Roam's secret sauce. It allows token incentivization to kick off the flywheel whose logic governs the deployment and expansion of the worldwide decentralized wireless access network, yielding invaluable "3W" data - detailing Who is connecting, When, and Where.

The integration of Roam heralds the streamlined adoption of cutting-edge Passpoint^{TM} and OpenRoaming^{TM} technologies. Originally conceived by the global WiFi industry for enterprise use, these technologies are poised to assume a pivotal role in the 5G rollout and the alleviation of cellular traffic. Roam strategically enhances adoption across three key dimensions: optimizing the service provisioning process, reducing deployment obstacles, and broadening the user base. Crucially, the Roam network harmonizes with stringent privacy protocols and regulatory standards, cultivating an environment conducive to the proliferation of Web3.0 native applications and users.

Roam: Decentralized OpenRoaming WiFi Networks

1 One Global Wi-Fi Network and OpenRoaming

1.1 One Global Wi-Fi Network

With 70+% of all smartphone internet data [1] and 52% of overall internet data [2][3] being carried over Wi-Fi networks, it is clear that cellular deployments in the licensed spectrum have not been able to keep pace with consumer demands for wireless data. In particular, 5G cellular requires the very dense deployment of small cells, which further aggravates the investment and operational challenges telcos face. And in some cases, the energy demands of 5G small cells have raised sustainability concerns.

As a result, WiFi is being examined by telcos as an alternative solution for 5G deployment, particularly for indoor coverage. With the launch of WiFi 6 in 2019, WiFi 6E (6 GHz spectrum in addition to the regular 2.4GHz and 5GHz) in 2022, and with WiFi 7 forthcoming, WiFi is evolving to meet telcos' and users' growing demand for wireless data. Wi-Fi Halow is also being introduced to facilitate the adoption of WiFi in the IoT domain.

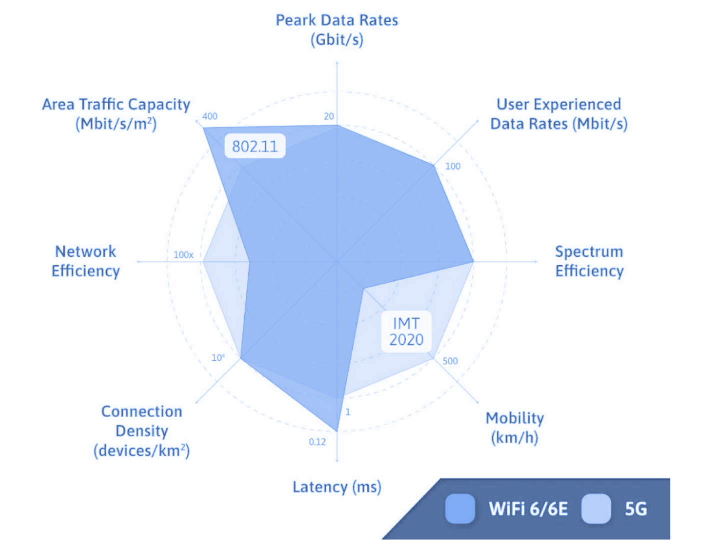


Fig 1,   Comparing Wi-Fi 6/6E (802.11) and 5GNR (IMT-2020) capabilities [4]

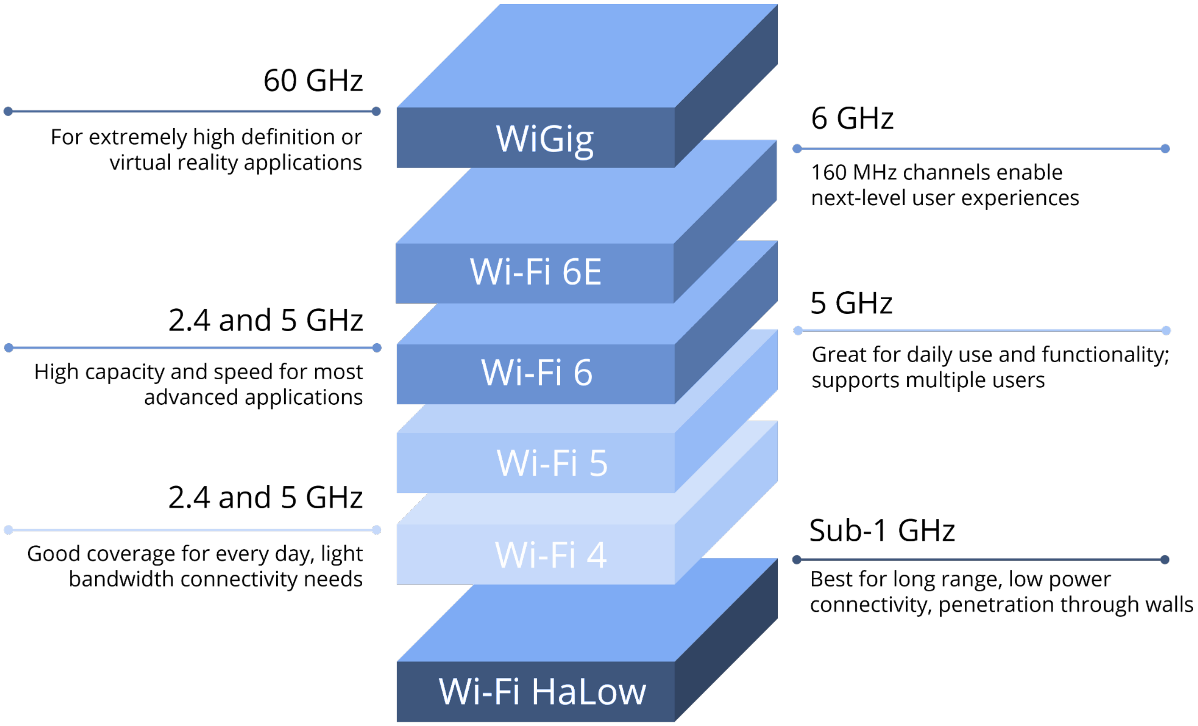

60 GHz
For extremely high definition or virtual reality applications
WiGig
6 GHz
160 MHz channels enable next-level user experiences
Wi-Fi 6E
2.4 and 5 GHz
High capacity and speed for most advanced applications
Wi-Fi 6
5 GHz
Great for daily use and functionality; supports multiple users
Wi-Fi 5
2.4 and 5 GHz
Good coverage for every day, light bandwidth connectivity needs
Wi-Fi 4
Sub-1 GHz
Best for long range, low power connectivity, penetration through walls
Wi-Fi HaLow

Fig 2, WiFi spectrum landscape [5]

However, the roaming experience offered by WiFi, as well as its security features, have to be improved. With cellular networks, when users travel across different cellular base stations, their devices connect automatically when they reach a new one, without interference or service interruptions. This happens no matter where the user goes, even when they cross between networks operated by different carriers. In addition, communication with the networks is secured using Extensible Authentication Protocol - Authentication and Key Agreement (EAP-AKA), or EAP Transport Layer Security (EAP-TLS). These security standards have been broadly accepted by the industry. In contrast, the typical onboarding experiences and network security levels offered by WiFi have been widely criticized. Generally, public WiFi is considered insecure and inconvenient to connect to. Users often become confused about which SSID to connect to, and are asked for access passwords, which is a nightmare. In some cases, users even need to receive an SMS or use their email or social media account to login. And once they move to another location, the same process repeats again!

Clearly, WiFi is overdue for a completely different user experience that's as seamless and secure as what's offered by cellular networks. If the onboarding and security issues mentioned above can be resolved, the world's 628 million guest WiFi networks [6] [7] could be integrated into one global WiFi roaming network in a secure way. Such a network would provide large-scale infrastructure for telcos, accelerate 5G deployment, and provide more affordable broadband wireless network services globally.

The vision of one global roaming WiFi network is shared by telcos, WiFi operators, equipment vendors, technology solution providers, governments, non-profit organizations, and, more importantly, 8 billion people globally - particularly the 4 billion who do not have internet access . One global WiFi network is also the mission of organizations like the WiFi Alliance, Wireless Broadband Alliance, Telecom Infra Projects, etc.

1.2 Enterprise WiFi

OpenRoaming is an open industry standard that automates device roaming between different WiFi networks. It is built upon enterprise WiFi technologies like Passpoint, which offers similar security as cellular networks.

1.2.1 Enterprise WiFi and Passpoint

Enterprise WiFi served the industry successfully for years before telcos tried looking into how WiFi can offer a 5G deployment alternative to small cells. Traditionally, enterprise WiFi has been referred to as “EPA-enterprise” and branded by the WiFi alliance as Passpoint, or sometimes “Hotspot 2.0.” Passpoint has been around since 2012 and is promoted by Telcos like AT&T, TMobile, etc for offloading cellular internet traffic to WiFi. Most mobile devices come pre-configured for Passpoint support. The technology itself contains three key components: IEEE802.1x and 802.11u standards, as well as the Extensible Authentication Protocol (EAP). Network side implementation is carried out by a Remote Authentication Dial-In User Service (RADIUS) system, which implements an AAA (authentication, authorization, and accounting) protocol for managing network access. RADIUS uses two types of data packets to manage the full AAA process: Access-Request, which manages authentication and authorization; and Accounting-Request, which manages accounting.

1.2.1.1 IEEE802.1x

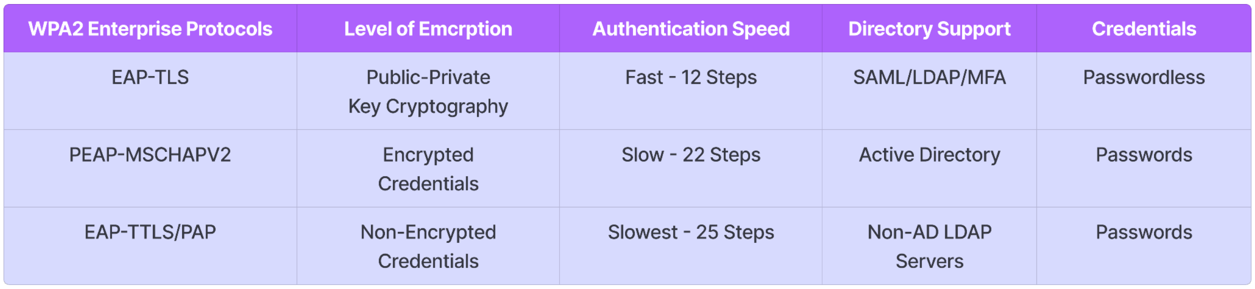
IEEE802.1x is An IEEE (Institute of Electrical and Electronics Engineers) standard for port-based network access control (PNAC) for wired and wireless access points. 802.1x defines authentication controls for any user or device trying to access a LAN or WLAN. The authentication involves three parties: a supplicant, an authenticator, and an authentication server. The supplicant is a client device (such as a laptop or cell phone) that wishes to attach to the LAN/WLAN. The authenticator is a network device that provides a data link between the client and the network, and that can allow or block network traffic between the two. This device could be an Ethernet switch or wireless access point, for example. The authentication server is typically a trusted server that can receive and respond to requests for network access, and can, based on different policies, tell the authenticator whether the connection is to be alloweds. Authentication servers typically run software supporting the RADIUS and EAP protocols. The authenticator acts like the security guard for a protected network. The supplicant is not allowed access through the authenticator to the protected side of the network until the supplicant's identity has been validated and authorized. With 802.1x port-based authentication, the supplicant must initially provide the required credentials to the authenticator - these will have been specified in advance by the network administrator and could include a username/password or a permitted digital certificate. The authenticator forwards these credentials to the authentication server to decide whether access is to be granted. If the authentication server determines the credentials are valid, it informs the authenticator, which in turn allows the supplicant (client device) to access resources located on the protected side of the network.

1.2.1.2 IEEE802.11u

IEEE802.11u defines the procedures related to hotspot connections and the authorization of clients by 3rd parties (for cellular network offloading). It includes airlink encryption, network discovery and selection (Access Network Query Protocol), Quality-of-Service (QoS) map distribution, etc. IEEE 802.11 is part of the IEEE 802 set of local area network (LAN) technical standards, and specifies the set of media access control (MAC) and physical layer (PHY) protocols for implementing wireless local area network (WLAN) communication.

1.2.1.3 EAP

EAP is used on encrypted networks to provide a secure method of sending identifying information for the purpose of network authentication. EAP was developed by the IETF (Internet Engineering Task Force), and has been widely adopted by wired and wireless access networks. In enterprise WiFi, commonly used authentication methods implement EAP-TLS (Transport Layer Security), EAP-TTLS (Tunneled Transport Layer Security) and EAP-PEAP (Protected Transport Level Security).



WPA2 Enterprise Protocols	Level of Emcrption	Authentication Speed	Directory Support	Credentials
EAP-TLS	Public-Private Key Cryptography	Fast - 12 Steps	SAML/LDAP/MFA	Passwordless
PEAP-MSCHAPV2	Encrypted Credentials	Slow - 22 Steps	Active Directory	Passwords
EAP-TTLS/PAP	Non-Encrypted Credentials	Slowest - 25 Steps	Non-AD LDAP Servers	Passwords

Table 1, WPA enterprise protocols comparison [8]

1.2.1.4 RADIUS

RADIUS is a client/server protocol that runs in the application layer, and can use either TCP or UDP transport layer protocols. Network access servers, which control access to a network, usually contain a RADIUS client component that communicates with the RADIUS server. RADIUS is often the back-end of choice for 802.1x authentication. A RADIUS server is usually a background process running on Linux or Microsoft Windows. A RADIUS server essentially acts as the "security guard" of an 802.1x network; as users connect to the network, the RADIUS authenticates their identity and authorizes them for network use. A user becomes authorized for network access after enrolling for a certificate from the PKI (Private Key Infrastructure) or confirming their credentials. Each time the user connects, the RADIUS confirms they have the correct certificate or credentials, and prevents any unapproved users from accessing the network.

RADIUS is commonly used to facilitate roaming between networks belonging to different ISPs. Thus, it allows for a single global set of credentials that are usable on many public networks. It also lets independent but collaborative institutions issue their own credentials to their own users, allowing visitors of new networks to be authenticated by their home institution, such as with eduroam. Eduroam has RADIUS servers working as proxies using RADSEC, or "RADIUS over TLS." The RADIUS server can authenticate the user's status at their home university via their home service provider (HSP), and grant them secure network access at a different university they are currently visiting, through the access network provider (ANP).

RADIUS facilitates this using realms, which identify where the RADIUS server should forward the AAA requests for processing. Realms can also be compounded using both prefix and postfix notation, to allow for complicated roaming scenarios; for example, somedomain.com\username@anotherdomain.com could be a valid username with two realms. Although realms often resemble domains, it is important to note that realms are in fact arbitrary text and need not contain real domain names. Realm formats are standardized in RFC4282 and RFC7542, which define a Network Access Identifier (NAI) in the form of 'user@realm'. In that specification, the 'realm' portion is required to be a domain name. However, this practice is not always followed.

RadSec is an 802.11x protocol for transporting RADIUS datagrams through TCP (Transmission Control Protocol) and TLS (Transport Layer Security), which themselves are protocols. RadSec is not to be confused with RADIUS using EAP-TLS, which refers to RADIUS authenticating for the certificate-based 802.1x protocol.

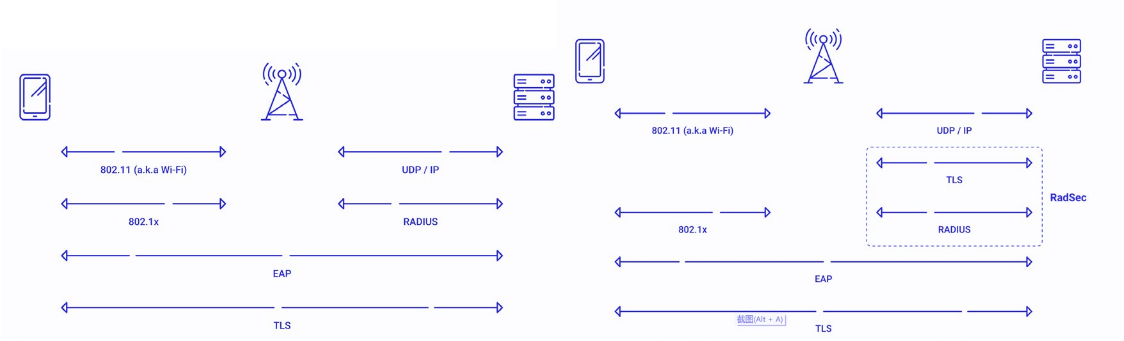


Fig 3, RADIUS and RADSEC [9]

A RADIUS system that allows users to login with a username and attributes instead of a password is critical for attracting them to use public infrastructure for authentication and authorization purposes. Otherwise, they would hire someone to manage their backend, or they would do it by themselves. EAP-TLS is passwordless, but it requires both client and server sides to have certificates, which is very cumbersome for the server side to manage. As a result, EAP-TTLS and EAP-PEAP are most used for public WiFi infrastructure, but both still require passwords.

1.2.2 OpenRoaming and Wireless Broadband Alliance

Essentially, OpenRoaming is a roaming federation service enabling an automatic and secure WiFi experience globally. The key is to allow users to access ANPs via their HSP and RADIUS proxy, and to establish a commercial term among these ANPs and HSPs. OpenRoaming was developed by Cisco for years until the Wireless Broadband Alliance (WBA) took over development in the beginning of 2020. From the start, the WBA and the WiFi Alliance (WFA) worked together to develop the standards OpenRoaming used (primarily WiFi CERTIFIED Passpoint^{TM} and Wireless Roaming Intermediary Exchange [WRIX]).

While Passpoint is able to provide local roaming and direct network partnerships, OpenRoaming targets a broader geographical area. Instead of using local networks as an intermediary to reach the HSP's RADIUS server, OpenRoaming utilizes federated directories to allow trusted networks to authenticate the user locally. Essentially, the goal of OpenRoaming is to develop one Global WiFi network. The roaming process can be divided into different functional components: firstly, configuring the network and the subscriber devices to allow roaming; secondly, creating the technical interconnections between the partnering companies/network providers, which allows for all real-time activities, such as authentication and accounting, to be performed; and finally, establishing the commercial framework for roaming, which includes billing and settlement agreements between the relevant companies.

1.2.2.1 Wireless Broadband Alliance (WBA)

The WBA is the global organization that connects people with the latest Wi-Fi initiatives. Founded in 2003, the vision of the Wireless Broadband Alliance (WBA) is to drive seamless, interoperable service experiences within the global wireless ecosystem via WiFi. The WBA's mission is to enable collaboration between service providers, technology companies, cities, regulators, and organizations to achieve that vision. The WBA's members include those major operators, identity providers, and leading technology companies across the WiFi ecosystem who share a common vision. Currently, it is supported by nearly all the largest players in the field.

The WBA undertakes programs and activities designed to address business and technical issues as well as opportunities for member companies. The alliance's work areas include standards development, industry guidelines, trials, and certification and advocacy. Its key programs include NextGen Wi-Fi, OpenRoaming, 5G, IoT, Testing & Interoperability, and Policy & Regulatory Affairs, with member-led Work Groups dedicated to resolving standards and technical issues in order to promote end-to-end services and grow business opportunities.

Currently, the WBA is managing OpenRoaming technical architecture, guidelines, standardization, and validation. It defines for service providers the best practices for roaming set-up, and outlines the reasons for providing roaming services while offering suitable strategies to foster adoption. Moreover, the WBA maintains a database of Operators' roaming-related data, including data on their Unique Organization Identifier(s) (WBAID), which are solely provided and maintained by the WBA.

1.2.2.2 Technical Architecture

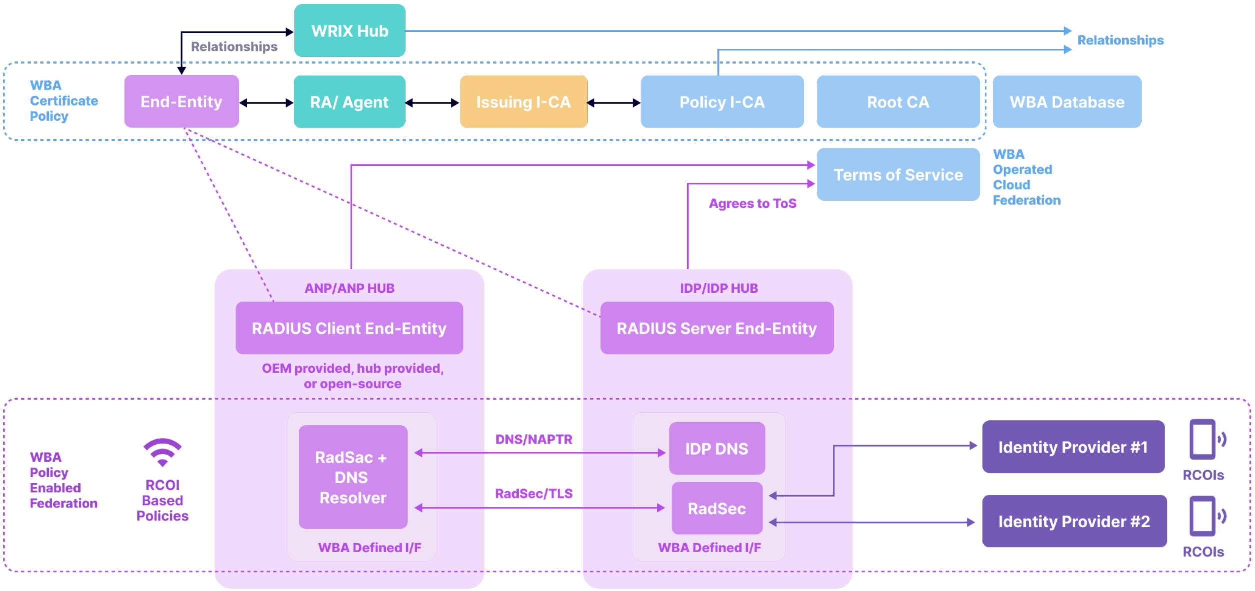


Fig 4, the WBA's OpenRoaming^{TM} federation technical architecture [10]

The diagram above describes the architectural framework for supporting the WBA's Policy-Enabled WiFi Federation. Together the WBA's Certificate Policy, Federation Terms of Service, and Database operations procedures define this federation's operations.

The key is how to onboard users to a federation of multiple identity providers (IdPs) and multiple venues. Initially designed for a venue to form an auto-onboarding agreement with a small set of carriers, OpenRoaming has rapidly grown, allowing consortiums of multiple carriers and other IdPs to form relationships for auto-onboarding with multiple venues. As adoption increased, this multi-to-multi relationship surfaced complexities and challenges that a smaller scale design was not made to address. The WBA OpenRoaming™ solution aims to bridge that need by recommending how these elements could be used in the context of an OpenRoaming network or regular Passpoint deployment (non-OpenRoaming network).

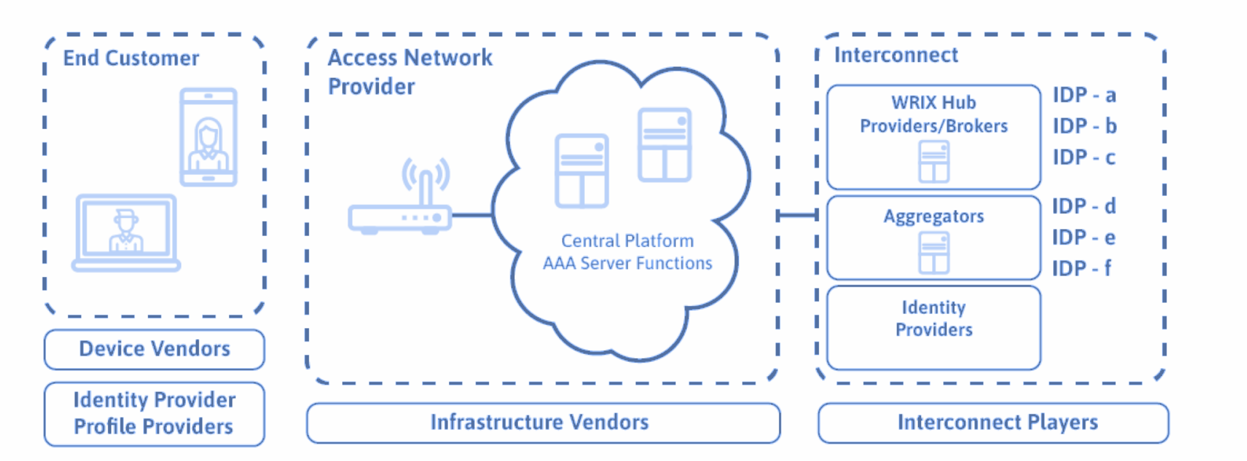


Fig 5, the WiFi OpenRoaming^{TM} ecosystem [11]

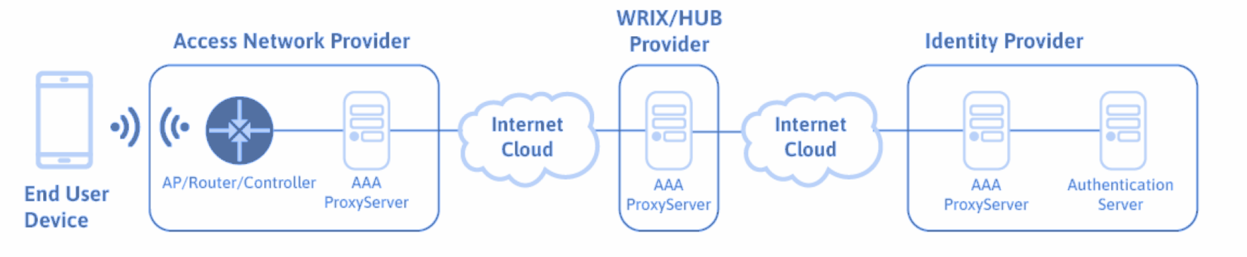
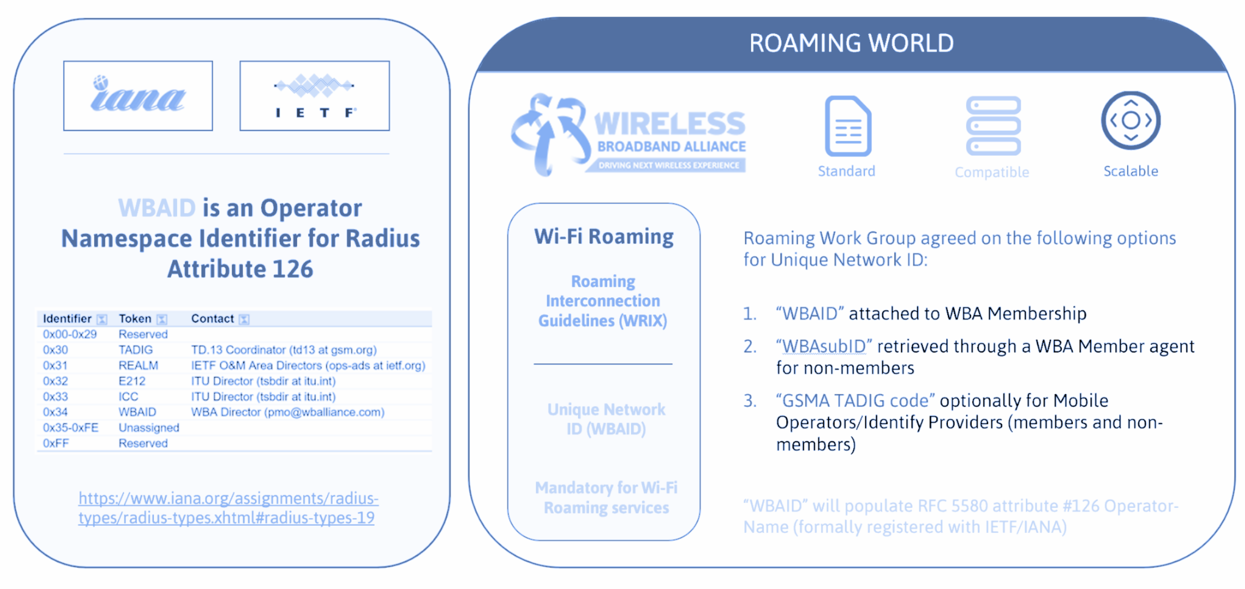


Fig 6, WLAN roaming bilateral interconnection using a WRIX hub [11]

To provide Wi-Fi roaming services, the ANP and IDP must have interoperability mechanisms in place which are defined by WRIX. OpenRoaming is built on a foundation of RadSec secured using the WBA's PKI (private key infrastructure), which requires all OpenRoaming participants to be identified using their WBAID. All ANPs shall support RADIUS Accounting for all OpenRoaming sessions, irrespective of which RCOIs (roaming identifiers) are supported, i.e., for both settled and settlement free service.

The WBAID consists of two parts, a mandatory "WBA Primary Member ID" which is assigned by the WBA when a company joins the WBA, and an optional prepended SubID that is allocated by a WBA Agent. WBAID is defined as follows: <Operator ID>:<country code>. It is included in the IDP and ANP identifiers in the usage exchange records as well as the financial information managed by the WRIX. Besides being used in the end to end communication and RADIUS attribute 'Operator Name', it is also used in the attribute 'Chargeable User Identity', combined with the user information and the WBAID Access-Accept in the Identity-Provider Vendor Specific Attribute. Other supporting processes, such as when requesting a PKI or during the exchange of configuration details, also require the WBAID.



WBAID is an Operator Namespace Identifier for Radius Attribute 126

Identifier	Token	Contact
0x00-0x29	Reserved	
0x30	TADIG	TD.13 Coordinator (td13 at gsm.org)
0x31	REALM	IETF O&M Area Directors (ops-ads at ietf.org)
0x32	E212	ITU Director (tsbdir at itu.int)
0x33	ICC	ITU Director (tsbdir at itu.int)
0x34	WBAID	WBA Director (pmo@wballiance.com)
0x35-0xFE	Unassigned	
0xFF	Reserved	

https://www.iana.org/assignments/radius-types/radius-types.xhtml#radius-types-19

ROAMING WORLD

Wi-Fi Roaming

Roaming Interconnection Guidelines (WRIX)

Unique Network ID (WBAID)

Mandatory for Wi-Fi Roaming services

Roaming Work Group agreed on the following options for Unique Network ID:

1. "WBAID" attached to WBA Membership
2. "WBAsubID" retrieved through a WBA Member agent for non-members
3. "GSMA TADIG code" optionally for Mobile Operators/Identify Providers (members and non-members)

"WBAID" will populate RFC 5580 attribute #126 Operator-Name (formally registered with IETF/IANA)

Fig 7, WBAID info [12]

3GPP 23.003 defines the sub-domain to be used with EAP-SIM, EAP-AKA and EAP-AKA' methods. The NAI realm is of the format:

wlan.mnc<MNC>.mcc<MCC>.3gppnetwork.org, where <MNC> and <MCC> are the MNC and MCC of the Mobile Network Operator (MNO).

The 3gppnetwork.org domain is operated by the GSMA. GSMA permanent reference document IR.67 describes the guidelines associated with the domain, including the operation of delegated zones by individual MNOs. In order to enable 3GPP defined NAI realms to continue to be used in Passpoint enabled devices, while avoiding impacting the security associated with the GSMA-defined DNS guidelines, those OpenRoaming systems that are not connected to the GSMA's inter-PLMN backbone and want to resolve any NAI realm of the form:

xxx.mnc<MNC>.mcc<MCC>.3gppnetwork.org

shall perform the DNS query using the modified realm:

xxx.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org

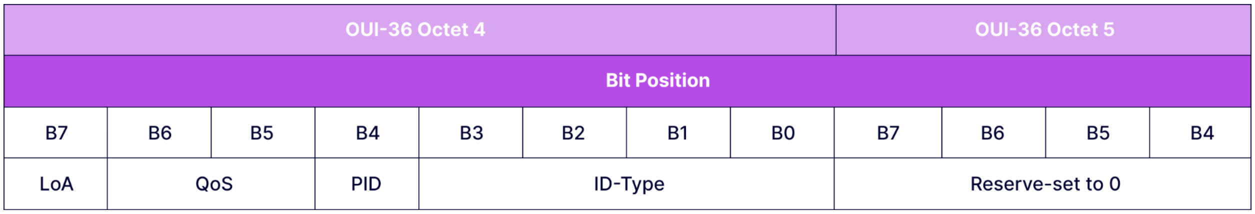
Similarly, those MNOs that have joined the OpenRoaming federation should provision the corresponding sub-domain in their DNS. This lets them identify the AAA peer used to authenticate their subscribers when using the OpenRoaming federation [9].

1.2.2.3 Onboarding Policy Control

The key to OpenRoaming is policy control once the exchange hub and proxy are established. The realization of policy controls for the OpenRoaming federation entails striking a balance between what’s required for fine grain policy enforcement, and what’s required to minimize the potential negative impacts of policy enforcement on user experience.

The Roaming Consortium Organization Identifier (RCOI) integrates with the Access Network Query Protocol (ANQP) to provide additional information to the ANP. This is the preferred approach for realizing ANP based authorization policy. If the ANP does not want to authorize all users associated with a particular RCOI, it will avoid broadcasting that RCOI and instead use an “allow list” of permitted NAI-realms to define the subset of authorized users associated with a particular RCOI. The normal rules for Passpoint access network selection thus ensure that OpenRoaming users will not attempt to authenticate to a network for which they are not authorized, and hence that they will not suffer any degraded connection experience associated with implementing authorization controls.

OpenRoaming defines the use of multiple RCOIs to facilitate the implementation of policies across the federation.



OUI-36 Octet 4								OUI-36 Octet 5			
Bit Position											
B7	B6	B5	B4	B3	B2	B1	B0	B7	B6	B5	B4
LoA	QoS		PID	ID-Type				Reserve-set to 0			

Table 2, extension of Octets 4 and 5 for OpenRoaming context dependent RCOI Field [10]

ID-Type Field				Description
B3	B2	B1	B0	
0	0	0	0	Any identity type is permitted
0	0	0	1	A service provider identity
0	0	1	0	A cloud provider identity
0	0	1	1	A generic enterprise identity
0	1	0	0	A government identity, e.g., including city
0	1	0	1	An automotive identity
0	1	1	0	A hospitality identity
0	1	1	1	An aviation industry identity
1	0	0	0	An education or research identity
1	0	0	1	A cable industry identity
1	0	1	0	A manufacture identity
1	0	1	1	A retail identity
Other values				Reserved (for future allocation by WBA)

Table 3, ROCI definition [10]

PID Field	Description
B4	
0	Baseline ID Policy applies, i.e., users can remain anonymous whilst using the service
1	A Permanent ID will be returned by the IDP

Table 4, OpenRoaming-Context PID field [10]

Where ‘xx-xx’ refers to the 12 bit extension, RCOI examples include:

OpenRoaming-Settled: BA-A2-D0-xx-xx

OpenRoaming-Settlement-Free: 5A-03-BA -xx-xx

1.2.2.4 Quality matrix

It is worth highlighting that the RCOI also identifies the Quality_of_Service (QoS) level of the given WiFi network, which is essential to ensuring a great user experience.

QoS Field		Description
B6	B5	
0	0	Baseline QoS
0	1	Silver
1	0	Gold
1	1	Reserved

Table 5, OpenRoaming-Context QoS field [10]

This OpenRoaming specification, referred to as Baseline QoS, defines the minimum WLAN and network requirements necessary for an access network to join the OpenRoaming federation. ANPs shall ensure that the following minimum requirements are provided when accessing on all its supported RCOIs, including, when configured, OpenRoaming-Settlement-Free:

- The ANP shall ensure that the availability of Service when used to access the Internet, measured during scheduled operations across the ANP's network, shall exceed 90% over any one month period.
- The ANP shall ensure that the aggregate bandwidth used to receive Internet service on the ANP's network shall be sufficient to enable each and every authenticated and authorized End User to receive a sustained 256 kilobits per second connection.

In addition to these minimum requirements, OpenRoaming defines two advanced service levels indicating an ANP's enhanced capabilities and configuration. Only those ANPs that support the necessary service level capabilities are permitted to broadcast OpenRoaming RCOIs with context identifiers signaling their corresponding QoS fields. The detailed definition of Silver and Gold tier is specified in ref [9]. In general, the definition sets the requirements for availability (percentage over any one month period), aggregate bandwidth for every authenticated and authorized end user, stream downlink speed (5 megabits per second measured over one-minute intervals for Silver tier) and end-to-end stream latency.

1.2.2.5 OpenRoaming Deployment

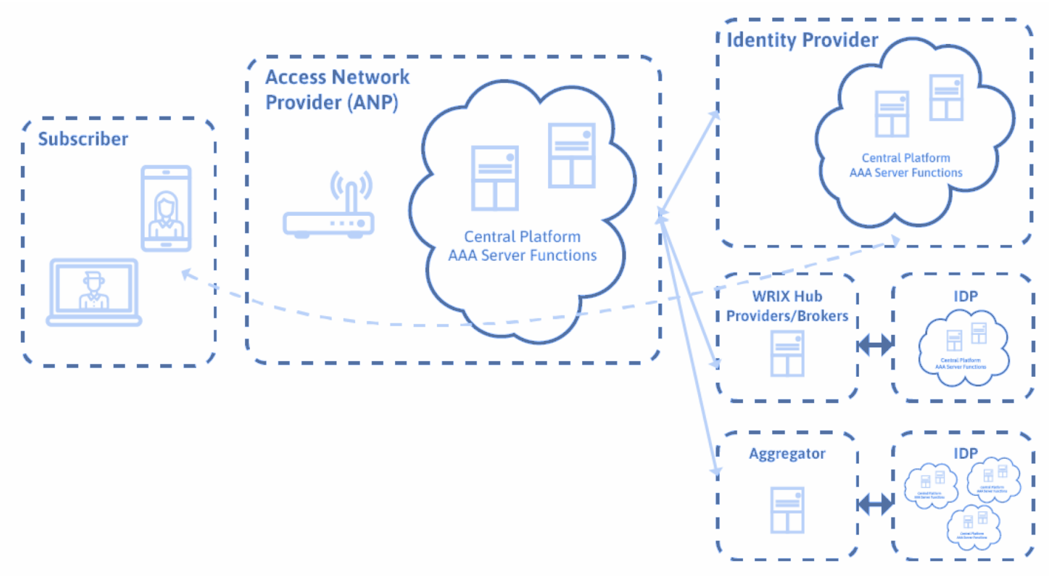


Fig 8, the WiFi roaming service ecosystem [11]

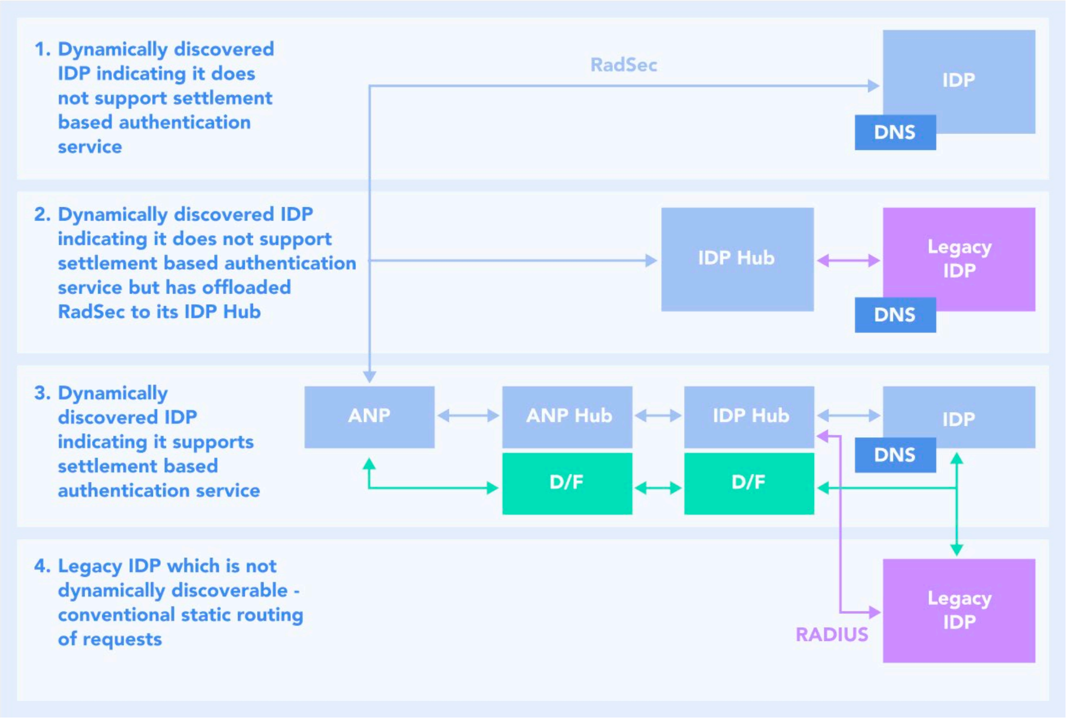

1. Dynamically discovered IDP indicating it does not support settlement based authentication service
RadSec
IDP
DNS
2. Dynamically discovered IDP indicating it does not support settlement based authentication service but has offloaded RadSec to its IDP Hub
IDP Hub
Legacy IDP
DNS
3. Dynamically discovered IDP indicating it supports settlement based authentication service
ANP
ANP Hub
IDP Hub
IDP
DNS
D/F
D/F
4. Legacy IDP which is not dynamically discoverable - conventional static routing of requests
RADIUS
Legacy IDP

Fig 9, roaming Scenarios with OpenRoaming enabled ANP [10]

If a legacy ANP has not deployed OpenRoaming, it can still be deployed by an ANP Hub provider to support the 4 different IDP use cases.

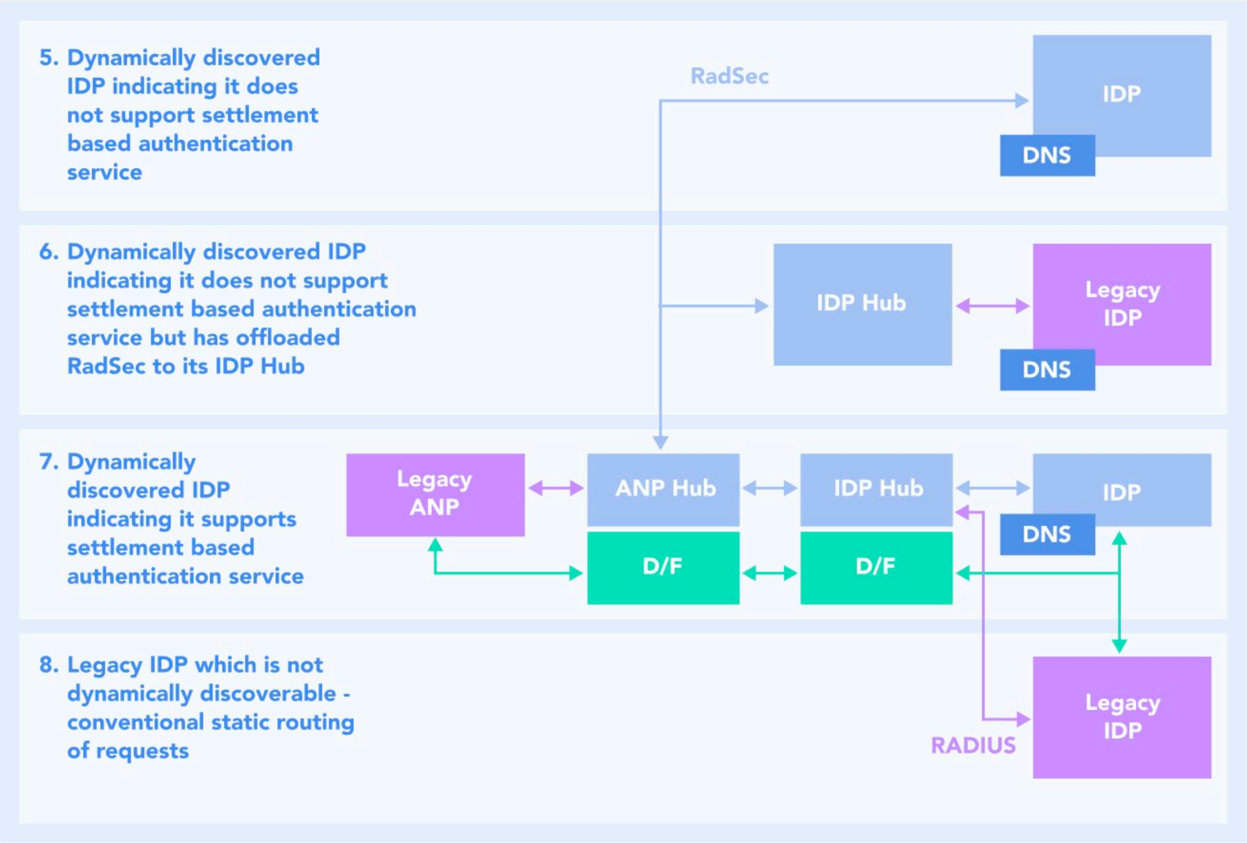

5. Dynamically discovered IDP indicating it does not support settlement based authentication service
RadSec
IDP
DNS
6. Dynamically discovered IDP indicating it does not support settlement based authentication service but has offloaded RadSec to its IDP Hub
IDP Hub
Legacy IDP
DNS
7. Dynamically discovered IDP indicating it supports settlement based authentication service
Legacy ANP
ANP Hub
IDP Hub
IDP
DNS
D/F
D/F
8. Legacy IDP which is not dynamically discoverable - conventional static routing of requests
RADIUS
Legacy IDP

Fig 10, roaming Scenarios with legacy ANP [10]

The current OpenRoaming federation maintains a security chain based on a minimum of 4 protection levels:

Level 1: OpenRoaming Root

Level 2: OpenRoaming Policy I-CA

Level 3: OpenRoaming Issuing I-CA

Level 3: Optional Registration Authority (RA) (e.g., WRIX Agent)

Level 4: End-Entity

The level 2 Policy I-CA is operated as a neutral federation service. The Level 3 issuing I-CA is intended to be operated by providers of OpenRoaming services, including those businesses that provide certificate services to WRIX agents, as well as other providers that have integrated OpenRoaming into their product/service offerings. The operator of the Level 1 and Level 2

Federation service will be determined by the WBA. Operators of Level 3 services will need to enter into an agreement with WBA for providing these services. Following such an agreement, the WBA shall ensure that the Level 2 operator signs the issuing I-CA certificate(s) for the Level 3 operator.

Other federations which want to interface with the OpenRoaming federation may use dynamic discovery with distinct NAPTR application service tags to facilitate integration. Specifically, eduroam plans to operate one central interchange point with OpenRoaming. By updating their DNS NAPTR records with the OpenRoaming defined service tags, an institution which is a member of the eduroam federation may permit its users to connect via an ANP supporting OpenRoaming.

Whereas the current eduroam service providers will use the eduroam defined "x-eduroam" application service tag to discover the home institution's RadSec peer for authentication, the OpenRoaming ANPs will use the WBA defined "aaa+auth" tag to discover a separate RadSec peer that can be defined for handling all inter-domain authentications.

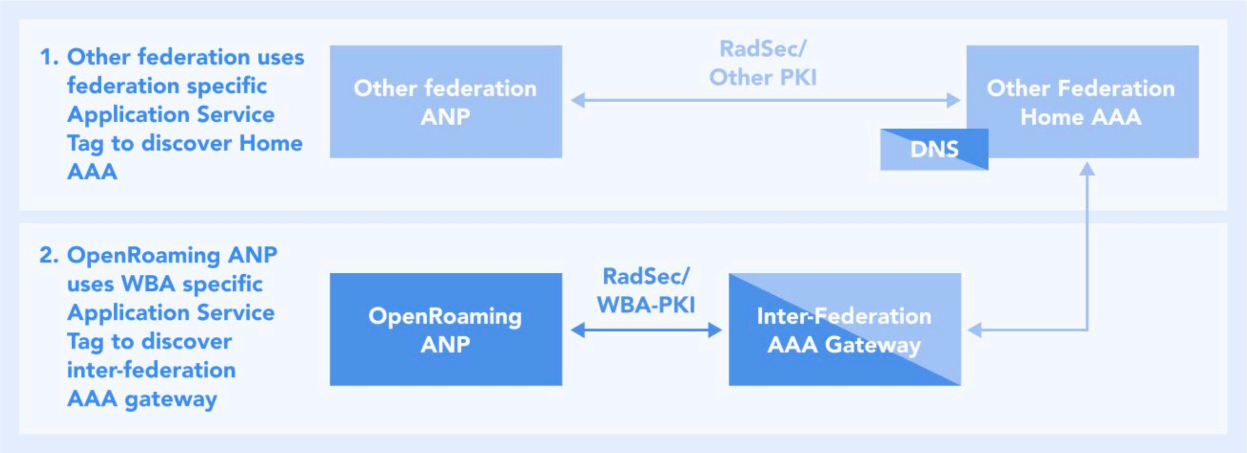

1. Other federation uses federation specific Application Service Tag to discover Home AAA
Other federation ANP
RadSec/ Other PKI
Other Federation Home AAA
DNS
2. OpenRoaming ANP uses WBA specific Application Service Tag to discover inter-federation AAA gateway
OpenRoaming ANP
RadSec/ WBA-PKI
Inter-Federation AAA Gateway

Fig 11, scheme using dynamic discovery to enable routing to an inter-federation AAA Gateway [10]

1.3 Achievements and Challenges of OpenRoaming

1.3.1 Fast Growing OpenRoaming Network

OpenRoaming has entered a fast track since the WBA picked up its development. In about 2 years, over 3 million access points have joined the global OpenRoaming network [13], and the momentum has been widely supported by telcos, ID providers, and main device vendors.

The WBA's OpenRoaming alliance creates an open connectivity framework that can be used by all organizations in the wireless ecosystem to power new opportunities in the 5G era.

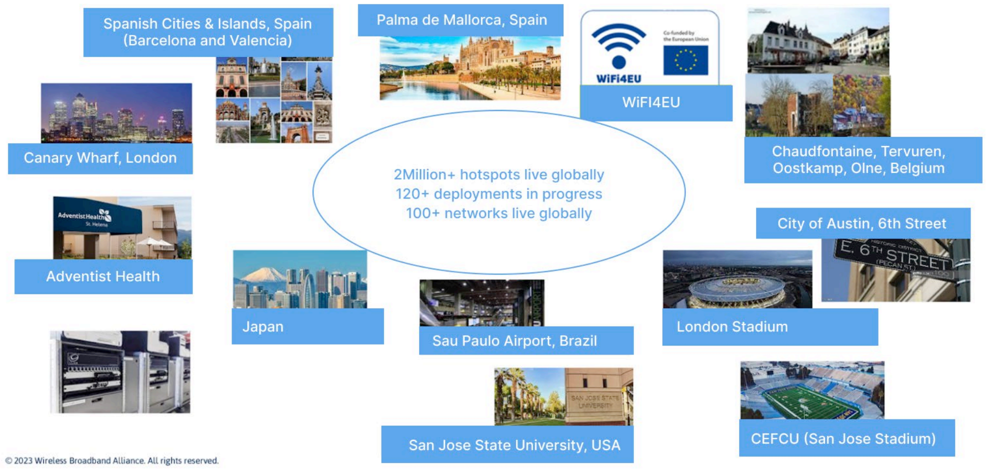

Spanish Cities & Islands, Spain
(Barcelona and Valencia)
Palma de Mallorca, Spain
WiFi4EU
Co-funded by the European Union
WiFI4EU
Chaudfontaine, Tervuren, Oostkamp, Olne, Belgium
Canary Wharf, London
2Million+ hotspots live globally
120+ deployments in progress
100+ networks live globally
City of Austin, 6th Street
E. 6TH STREET
Adventist Health
Japan
London Stadium
Sau Paulo Airport, Brazil
San Jose State University, USA
CEFCU (San Jose Stadium)
© 2023 Wireless Broadband Alliance. All rights reserved.

Fig 12, WBA OpenRoaming location examples in 2022 [14]

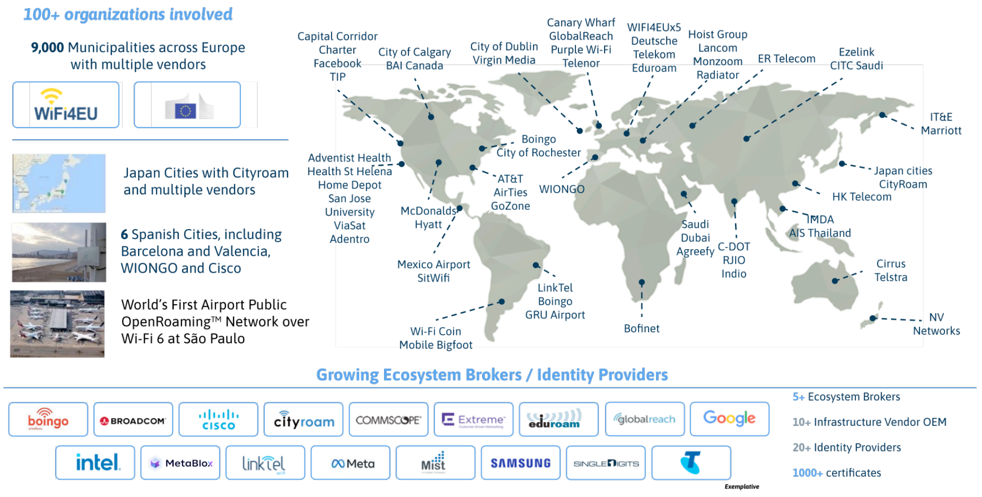


Fig 13, WBA OpenRoaming map [14]

By implementing the following technologies, the alliance has advanced WiFi services worldwide:

- Cyber security services: Cyber security enables simple, secure and scalable Wi-Fi connections amongst the different organizations that are part of WBA OpenRoaming™.

This allows for automatic and secure roaming between millions of networks, nationally and globally.

- Cloud federation: A cloud federation of networks and identity providers enables automatic roaming and user onboarding to Wi-Fi. Based on the WBA's WRIX standards, it allows for scaling and facilitates different business models under a harmonized framework.
- Network Automation: Network automation defines an automated roaming consortium codes framework (RCOI) to support policy provision on devices and networks. Organizations that manage a Wi-Fi certified Passpoint^{TM}-enabled network may become part of the WBA's OpenRoaming™ federation.

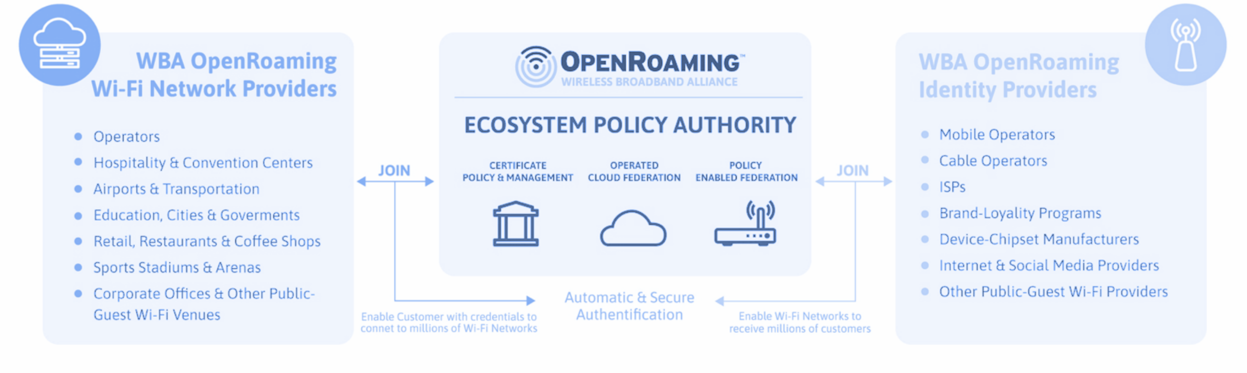

WBA OpenRoaming
Wi-Fi Network Providers
Operators
Hospitality & Convention Centers
Airports & Transportation
Education, Cities & Goverments
Retail, Restaurants & Coffee Shops
Sports Stadiums & Arenas
Corporate Offices & Other Public-Guest Wi-Fi Venues
JOIN
OPENROAMING
WIRELESS BROADBAND ALLIANCE
ECOSYSTEM POLICY AUTHORITY
CERTIFICATE POLICY & MANAGEMENT
OPERATED CLOUD FEDERATION
POLICY ENABLED FEDERATION
JOIN
WBA OpenRoaming
Identity Providers
Mobile Operators
Cable Operators
ISPs
Brand-Loyality Programs
Device-Chipset Manufacturers
Internet & Social Media Providers
Other Public-Guest Wi-Fi Providers
Enable Customer with credentials to connet to millions of Wi-Fi Networks
Automatic & Secure Authentification
Enable Wi-Fi Networks to receive millions of customers

Fig 14, the WBA ecosystem [14]

In terms of promotion of OpenRoaming, the WBA demonstrates that OpenRoaming could bring the industry the following four benefits:

- Seamless and secure onboarding: No more SSID-password guessing games, insecure login credentials or repetitive reconnections to public Wi-Fi. Instead, OpenRoaming creates a seamless WiFi connection experience, allowing billions of devices to connect automatically and securely to millions of Wi-Fi networks globally.
- Improved consumer satisfaction: No more billing surprises from overseas cellular roaming data.With OpenRoaming, Wi-Fi Roaming and cellular combines to create the best coverage and cost options, integrating guest/public Wi-Fi access with cellular networks worldwide, for a seamless user experience anytime, anywhere.
- Positive industry impact: OpenRoaming defines the industry policy & standards needed for all players in the Wi-Fi ecosystem to join and develop their services. It can grow new business opportunities with Wi-Fi roaming & the 5G offloading it enables, facilitating the convergence of Wi-Fi and 5G.
- A better connected world through unprecedented, global reach: billions of devices get automatic and secure connections to millions of Wi-Fi networks globally.

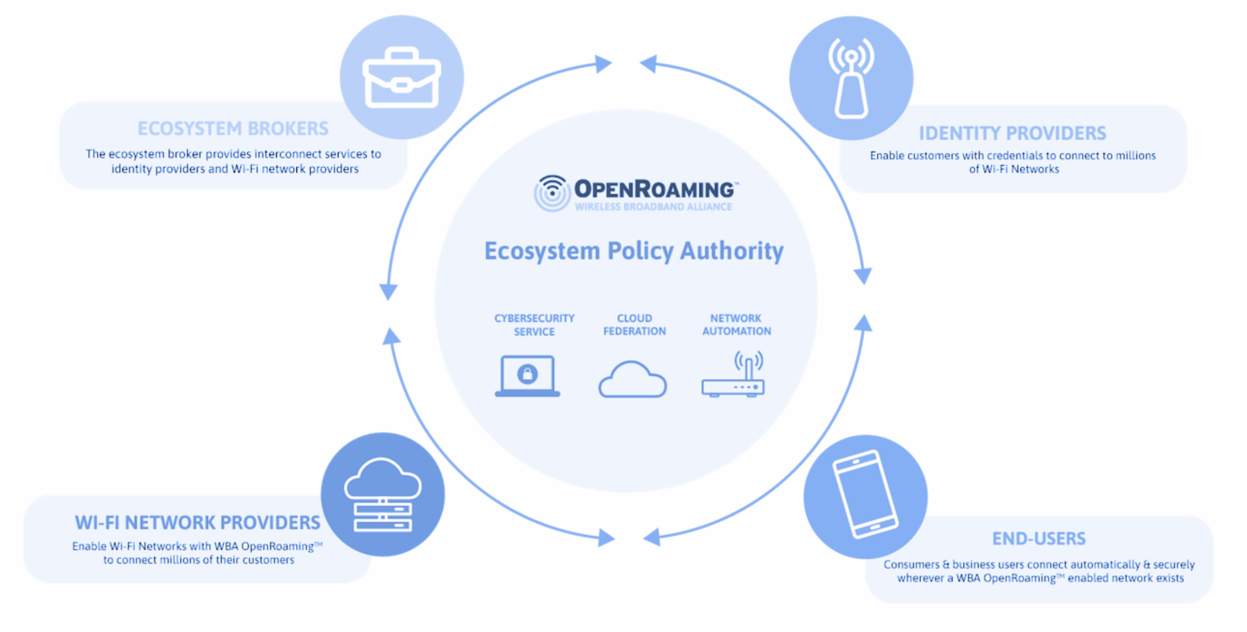

ECOSYSTEM BROKERS
The ecosystem broker provides interconnect services to identity providers and Wi-Fi network providers
IDENTITY PROVIDERS
Enable customers with credentials to connect to millions of Wi-Fi Networks
OPENROAMING
WIRELESS BROADBAND ALLIANCE
Ecosystem Policy Authority
CYBERSECURITY SERVICE
CLOUD FEDERATION
NETWORK AUTOMATION
WI-FI NETWORK PROVIDERS
Enable Wi-Fi Networks with WBA OpenRoaming™ to connect millions of their customers
END-USERS
Consumers & business users connect automatically & securely wherever a WBA OpenRoaming™ enabled network exists

Fig 15, the WBA's ecosystem cycle [14]

1.3.2 Challenges

New challenges have been exposed during the adoption process of global OpenRoaming. These drive the development of Roam.

1.3.2.1 Limits in Service Provision

What will happen if a user visits a venue for the first time and they do not have other means, like cellular data, to connect to WiFi besides connecting to that venue's network? Currently, there are two approaches. The first one is to use Online SignUp (OSU) services, and the second is to install a profile on their mobile device before they travel to the venue. Unfortunately, both methods have constraints and limit the growth of OpenRoaming.

The Wi-Fi Alliance expanded the Access Network Query Protocol (ANQP) to include Online Sign Up (OSU) concepts to leverage seamless onboarding and client security for Passpoint® networks. ANQP (mentioned in Section 1.2.1.2), which is the basis of IEEE802.11u, is a query-and-response protocol that defines the services offered by an access point (AP), typically at a Wi-Fi hotspot.When a subscriber queries an AP using the ANQP, that user receives a list of items that describe the services available, without having to commit to a network.

With OSU, the typical user experience is as follows: When a user comes into a venue where he or she has never been to, there will be 2 networks available:An unencrypted WiFi network called: Free_registration, and a secured one called: WiFi. The user will initially have as their only option going for the Free_registration ssid, and only it can be connected to the OSU. The user will follow and complete the registration process, subsequent to which they should expect a seamless experience logging into the secured network automatically. Unfortunately, this is not the case. iOS states that it's a security violation to start changing the phone setting with different Wi-Fi credentials when connecting to Free_registration. Thus to sign up to the network, the user must register with the Open network and then go back to the secured one to fill in the information which he or she just registered with. This process is non-user-friendly and basically prevents the mass adoption of OpenRoaming. With an Android based system, the process for connecting to WiFi at a new venue is easier but still not smooth.

The alternative solution is to get the users preloaded with an OpenRoaming profile before they travel or leave a network to which they're already connected. They can either download an iOS or Android app onto their cell phones or tablet, or scan a QR code via web browser and download the profile onto their cell phones. With this profile, their mobile devices will automatically connect to the OpenRoaming WiFi network whenever they encounter it. This approach works; however, it is difficult to ask people to pre-download a profile, particularly when they could not really test it immediately (before traveling to a new network). Unfortunately, this added step largely confuses the end users and restricts the adoption of OpenRoaming.

1.3.2.2 Constraints of IDPs

OpenRoaming profiles are managed by IDPs. Each IDP who wants to offer OpenRoaming services must set up a RADIUS based backend and work with site owners or agents like the WBA on adding the corresponding NAIs or Realm to the list of authorized identifiers. There are many IDPs - like credit card issuers, game producers, loyalty programs, etc - who want to offer OpenRoaming services, but they typically neither have locations to deploy WiFi nor know how to operate enterprise WiFi systems (or are willing to invest the necessary resources for that). So far, there are fewer than 10 IDPs providing OpenRoaming services. If easy integration of enterprise WiFi systems were available to IDPs, they could offer OpenRoaming to their customers without needing to operate an enterprise WiFi backend, releasing the potential of OpenRoaming to engage IDPs and grow its user base dramatically.

1.3.2.3 Challenges in Network Expansion

The ultimate goal of one global OpenRoaming WiFi network is to build a network as large as possible, with a focus on covering areas with high population density, as these need carrier off-loading the most. They include large venues or enterprise sites like sports complexes, libraries, stadiums, schools, and shopping centers; as well as small or medium sized locations like popular restaurants, fitness clubs, cafes, bars, playgrounds, campgrounds etc. Current OpenRoaming deployment is mainly performed in the former cases, as these sites have the budget and technicians needed to support enterprise grade WiFi. On the other hand, the owners of small or medium sized sites will typically not have strong motivation to deploy OpenRoaming until it has become a popular standard. They are hesitating to invest additional capital to upgrade their WiFi to enterprise grade, and even if they do so, they still lack the technical expertise needed to manage the backend.Oftentimes they must hire an agent to help them manage it, which means additional costs that could be an issue for these small to medium businesses.

Although OpenRoaming has grown dramatically since 2020, it is still considered to be in its early stages, and how to incentivize small or medium businesses to implement it remains a question to the industry.

1.3.3 Roam's Objective

Roam was developed to take a decentralized approach to building a global WiFi OpenRoaming network. It will help to accelerate the growth of the existing OpenRoaming networks and facilitate 5G roll out globally.

In this decentralized OpenRoaming network:

1. Any ID providers, government agencies or businesses like banks, online video streaming operators, game producers, etc., can become OpenRoaming ID providers and offer OpenRoaming services to their customers, either via the Roam mobile app or their own app.
2. Site operators could offer OpenRoaming without operating or hiring anyone to operate an AAA (Authentication, Authorization and Accounting) server, typically a RADIUS (Remote Authentication Dial-In User Service) based setup.
3. Users can use their Web3 DID (self-declared) and Verifiable Credentials (issued by IDPs) to roam on the global OpenRoaming Network. This network is decentrally built and managed but allows regulators and Verifiable Credentials issuers to work together to identify network users when needed. Within this network, users' data privacy will be protected per the Trust-Over-IP identity management concept. Subsequently, the privacy protected "3W" data (Who connects, When and Where) will be made available to the public via Roam protocol, helping developers build additional applications upon it.

2 Decentralized Wireless Access Network

2.1 The Decentralized Physical Infrastructure Network (DePIN) Concept

The decentralized physical infrastructure concept was brought to the attention of the academic world a few years ago. Broadly, it refers to the decentralization of any physical infrastructure network, from electricity grids and city-wide heating systems to wireless communication and storage networks, etc. DePINs are developed for a variety of purposes as well: better reliability compared to centralized networks, lower capital investment, shorter response latency, etc. It is worth noting that DePIN refers to two distinct cases. In the first case, it refers to a decentralized network structure that, for example, uses locally generated power (solar panels) instead of one big power plant, or uses wireless mesh networks instead of one network configured in a star structure. In the other case, DePIN refers to building an infrastructure network in a decentralized way by motivating community or multiple participants to build together, instead of building the network by its operator only.

DePIN has multiple sectors: cloud servers, wireless networks, sensor networks, automobile networks, energy networks, smart grid networks etc [15]. Like with other decentralized systems, this network model is subject to the blockchain trilemma: a trade-off has to be made among decentralization, scalability and security.

The cost model of the DePIN is important as a lot of them rely on the token incentive to bootstrap the network. The cost of the network has to be well modeled to function as the base of the tokenomics. The cost model is developed with a focus on designing (or modifying) an infrastructure system to provide a particular infrastructure product or services (water, natural gas, electricity, internet etc.) for a set of n locations or subnetworks (towns, buildings, etc.). Each location has some known demand for the product and also has the ability to produce this product locally with a production cost that varies with geography. In order to satisfy the demand at each location, one can either produce materials locally, or build an interconnection to some nearby locations that can produce them less expensively.

A formula has been proposed [16] which can be used for optimizing the cost-efficiency of a prospective DePIN . The formula has been simplified as follows:

$$O = (C + K) \cdot G + w\sqrt{N}\, F \cdot L - r \,/\, N\, \Delta D$$

where O stands for the optimal investment cost coefficient. It is a normalized item and independent of the number of locations. This allows us to study the optimal scheme of a centralized tree / star structure vs. a system of decentralized subnetworks or a mesh connection structure. The same formulation can be applied to networks of different spatial scales: a large country with many nodes (for instance), or a small city with fewer nodes, can be modeled by optimizing the value for this parameter. In most cases, the actual cost shall be close to linearly proportional to the number of locations. C is a vector representing the marginal cost of producing one unit of a good, and K is a vector representing the levelized cost of the production capacity needed for a node to produce at a rate of one unit per unit time. For example, if a particular power plant technology costs \$1000/kW to build, it would have a levelized capacity cost of k = \$79.2 per kW-year when amortized over a 20-year horizon at a 5% discount rate. If its production cost were \$10 per MWh, it would have an annual production cost of c = \$87.66/kW-year （8766 hours per year). G represents the quantity of goods produced, $w\sqrt{N}$ is an interconnection cost parameter (cost per unit length-capacity), N is the number of locations, w is the cost, L is the matrix of distance between each node, and F is the flow capacity. The smallest value of w refers to the situation wherein the mean component size is at or near the size of the network, while for the larger values of w, the component size is far smaller than the size of the network. For the case w = 1, it is hardly optimal to build any interconnection.

Reliability plays an enormous role in the design of infrastructure systems. P measures the cost of not serving demand in response to a set of node or link outages (perturbations). These costs are assumed to follow a linear function of the amount of unserved load over all perturbations. r is the reliability cost parameter, ranging from 0 to 1, and ΔD is the change (loss) of demand that results from perturbation, which is always a non-positive value. As a whole this formulation allows us to observe how network size and structure changes as we increase the relative importance of reliability. If r = 0, demand losses are effectively deemed irrelevant. On the other hand, as r increases, we hypothesize that networks are likely to become more meshed and more likely to include surplus production capacity. On the one hand, small, local networks will be more robust to failures and thus may be more optimal when reliability is very important. On the other hand, large interconnected systems provide a high level of redundancy, which also brings tremendous value. A tradeoff has to be made.

The model under discussion is designed to find fundamental properties of the DePIN system that do not depend on the size of the network. Thus, the cost function is designed so that both the production and the construction terms grow linearly with n. It has been observed, at least for the case of uniformly distributed node locations, that the distances between randomly selected node pairs decreases according to l ~ $1 / \sqrt{N}$, as a a result ensuring that linear growth of the interconnection cost term requires that we scale the relevant term by $\sqrt{N}$. The similar consideration given to the reliability item - the reliability term, is divided by *N* so that this term also roughly increases linearly with *N,* as ΔD is proportional to the number of perturbations, which is also proportional to the number of the nodes.

This formula explains the value created by production:

$$V = (R - O) \cdot N$$

where *R* is the revenue per node, *O* is the optimal cost per node, and *N* is the node matrix.

As for the decentralized telecommunication network, it is also important to note that Metcalfe's law applies. Metcalfe's law states that the value of a telecommunications network is proportional to the square of the number of connected users of the system (n^2). It works with both telecom networks as well as networks such as the Internet, social networks, and the World Wide Web.

However, the number *n* refers to the number of end devices, like cell phones, while in the Formula , N refers to the number of locations or subnetworks, like a gateway. In this situation

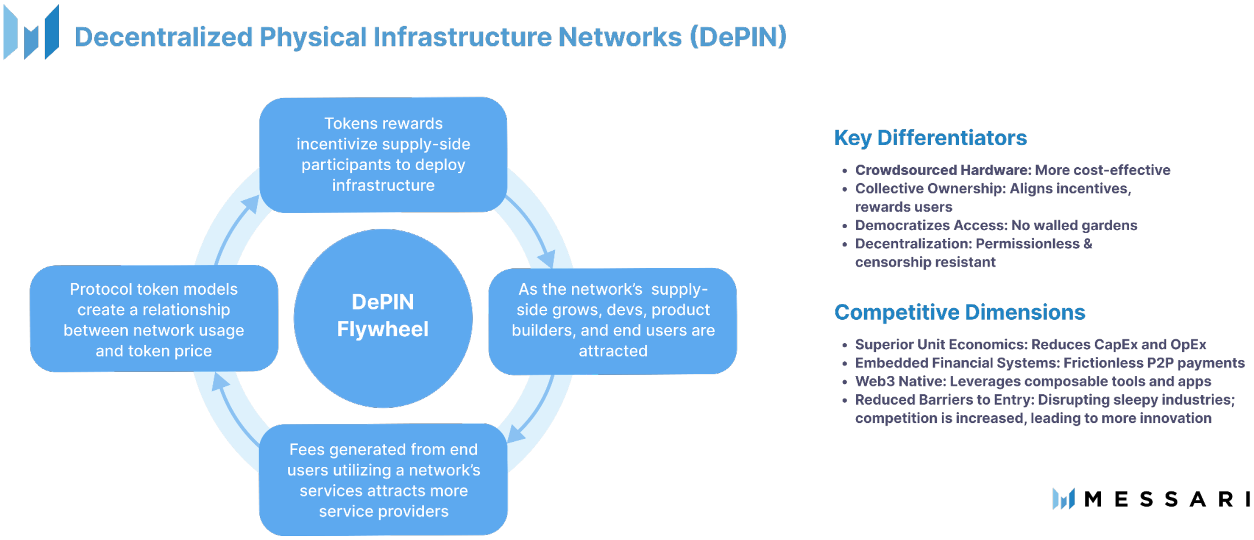
$$V = A \cdot n^2 + (R - O) \cdot N$$

where *A* is the network value coefficient for the telecommunication network. Often, it refers to the value generated by the information flow, while *R* is the direct value generated by the connectivity.

2.2 Token Incentivization

DePINs are also called Token Incentivized Physical Infrastructure Networks (TiPIN), as many of them require tokenomics to build. Traditional network operators manage the capital expenditures based on their fundraising and (operational) income generation capabilities. In the DePIN or TiPIN sector, such a process is instead managed by the tokenomics of the network. This model effectively solves the chicken-and-egg problem associated with traditional hardware networks. Using token rewards, a protocol can motivate individuals to bootstrap the supply-side of the network to the point where end users find its services attractive enough to use. The particular tokenomics model of a DePIN has to be resilient enough to work with all kinds of market conditions. The amount of rewards and the value of the token must be consistent with the value produced by the network. Whenever a valuation discrepancy happens, the tokenomics model must have a mechanism designed to realign the token valuation with the network valuation, without the risk of any catastrophic failures.

The flywheel below represents the business model of a typical DePIN or TiPIN project


Decentralized Physical Infrastructure Networks (DePIN)
Tokens rewards incentivize supply-side participants to deploy infrastructure
As the network's supply-side grows, devs, product builders, and end users are attracted
Fees generated from end users utilizing a network's services attracts more service providers
Protocol token models create a relationship between network usage and token price
DePIN Flywheel
MESSARI

Key Differentiators

- Crowdsourced Hardware: More cost-effective
- Collective Ownership: Aligns incentives, rewards users
- Democratizes Access: No walled gardens
- Decentralization: Permissionless & censorship resistant

Competitive Dimensions

- Superior Unit Economics: Reduces CapEx and OpEx
- Embedded Financial Systems: Frictionless P2P payments
- Web3 Native: Leverages composable tools and apps
- Reduced Barriers to Entry: Disrupting sleepy industries; competition is increased, leading to more innovation

Fig 16, DePIN features and flywheel [15]

The token incentivization process also needs to be designed and implemented to work with a complex economic model. If we refer to the cost model as described in Section 2.1, token incentivization brings the following impact:

a. It can reduce the cost of item *C* via utility token mining. Take decentralized wireless access networks as an example: with token incentivization, network operators do not have to pay things like electricity bills, air condition bills, etc. The miner will bear those costs with the expectation that the token will grow in value according to Metcalfe's law. Essentially, the token functions as a long-term "call" option. The miner paid the premium for that option (the cost to operate the miner) and expects to be profitable when the token value grows.
b. It can reduce the cost of item *K* via utility token mining. Using the same example, miners will pay for the mining rig which is typically a network gateway or similar device, and they also provide a free network location, while traditional telcos have to pay both the site acquisition and equipment costs. Again, this is equivalent to the miner paying the premium for that "call" option.
c. With the reduction in both cost items as specified above, the system could tolerate more interconnection costs and lean towards a more decentralized mesh solution. This will increase the robustness of the network and improve its availability, leading to more users and better return of the token value.

Overall, the token incentivization process does provide a more affordable way for operators to build their networks. The key to the success is to grow the number of users, as this will grow the network value dramatically.

The entire TiPIN economic model can be described as below:

$$V(t) = X(t) * p(t) = A \cdot n(N(t),t)^2 + (R - O + O') \cdot N(t) + Y(N(t),t) - Z(t)$$

where *X(t)* represents the total number of generated and unlocked tokens, *p(t)* is the price of the tokens, O' is the capitalized operator's investment, $Y(N(t),t)$ is the total premium received, as defined by the miners' / community builder's investment in terms of mining rigs, operational costs and site acquisition costs, etc. $Z(t)$ is the total amount withdrawn out of the ecosystem.

During a Token Generation Event (TGE), the above formula becomes

$$X(t) * p(t) = A \cdot n(N(t),t)^2 + (R - O + O') \cdot N(t)$$

The network ecosystem value ($A \cdot n(N(t),t)^2$) , the revenue, and the capitalized investment shall be equivalent to the investment amount by the TGE. These investments shall typically come from the operator itself and its institutional investors. After that, whether the token price can maintain really depends on the speed of on-boarding new users, as represented by the delta between $Y(N(t),t)$ and $Z(t)$; token generation and unlock speed; and the network growth speed.

2.3 DeWi

The broadband wireless access network is the most desirable development target for DePIN, as this type of network supports most people's daily telecommunication needs. With the challenges of 5G roll-out, it has become a hot sector in DePIN, and has been called Decentralized Wireless, or DeWi. This DePIN subsector often includes projects deploying narrow band wireless access networks as well.

The traditional capital-intensive, top-down model telcos use to build networks is unsuitable for building 5G networks, which requires significantly more base stations than older generation networks. This level of deployment has proven to be economically infeasible for telcos. Besides the large number of base stations, other issues like high site acquisition costs, complex and expensive wireless spectrum purchasing procedures, surprising electricity bills, challenges in mobilizing thousands of field technicians to install and maintain complex equipment, and the staggering affordability of the general public, all limit 5G deployment under centralized network deployment models.

In contrast, DeWi’s flywheel and open access-deployment business model can empower individuals and businesses to improve their connectivity and add wireless density where it is not financially feasible for traditional telcos or other network operators to do so. For example, the owner of a restaurant with historically bad connectivity could deploy their own DeWi equipment, solving their connectivity problem for themselves and their customers. While it’s highly unlikely that DeWi completely replaces traditional networks, the two can coexist with one another and develop a symbiotic relationship.

However, enabling a true decentralized infrastructure remains challenging, as this industry is conventionally dominated by Telcos and influential telecom equipment vendors. Complex telecommunication equipment is needed, and only well trained engineers and technicians can operate and maintain it. Interoperability and vendor dependency are big difficulties for telcos, and have set obstacles for decentralized telco concepts. The O-RAN, or Open Radio Access Network (O-RAN, OpenRAN), is a network design concept intended to improve the interoperability and standardization of RAN elements via a unified interconnection standard for white-box hardware and open source software elements from different vendors. OpenRAN ’s mission is to accelerate innovation and commercialization in the RAN domain with multi-vendor interoperable products and solutions that are easy to integrate within the operator’s network, and that are verifiable for different deployment scenarios. O-RAN architecture integrates a modular base station software stack with off-the-shelf hardware, which allows baseband and radio unit components from discrete suppliers to operate seamlessly together. In addition, 5G provides a cloud native architecture where the key network functions are managed via cloud and edge computing, which can be carried out by off-the-shelf computers

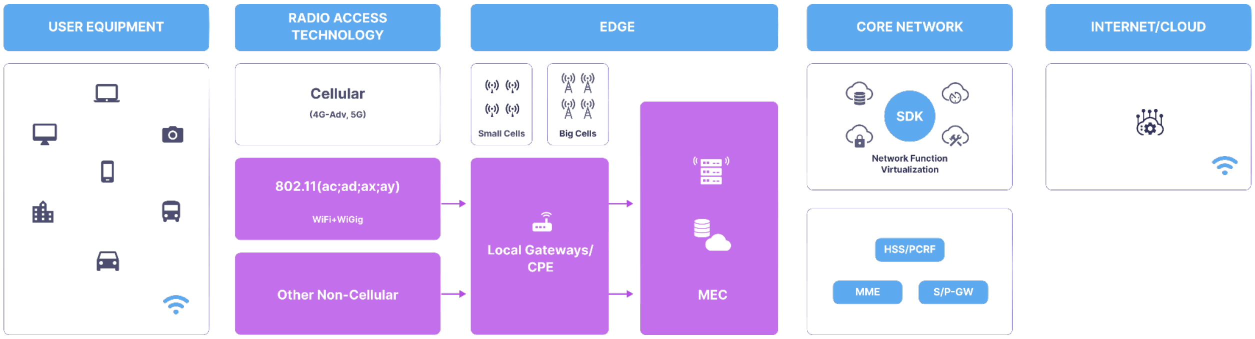
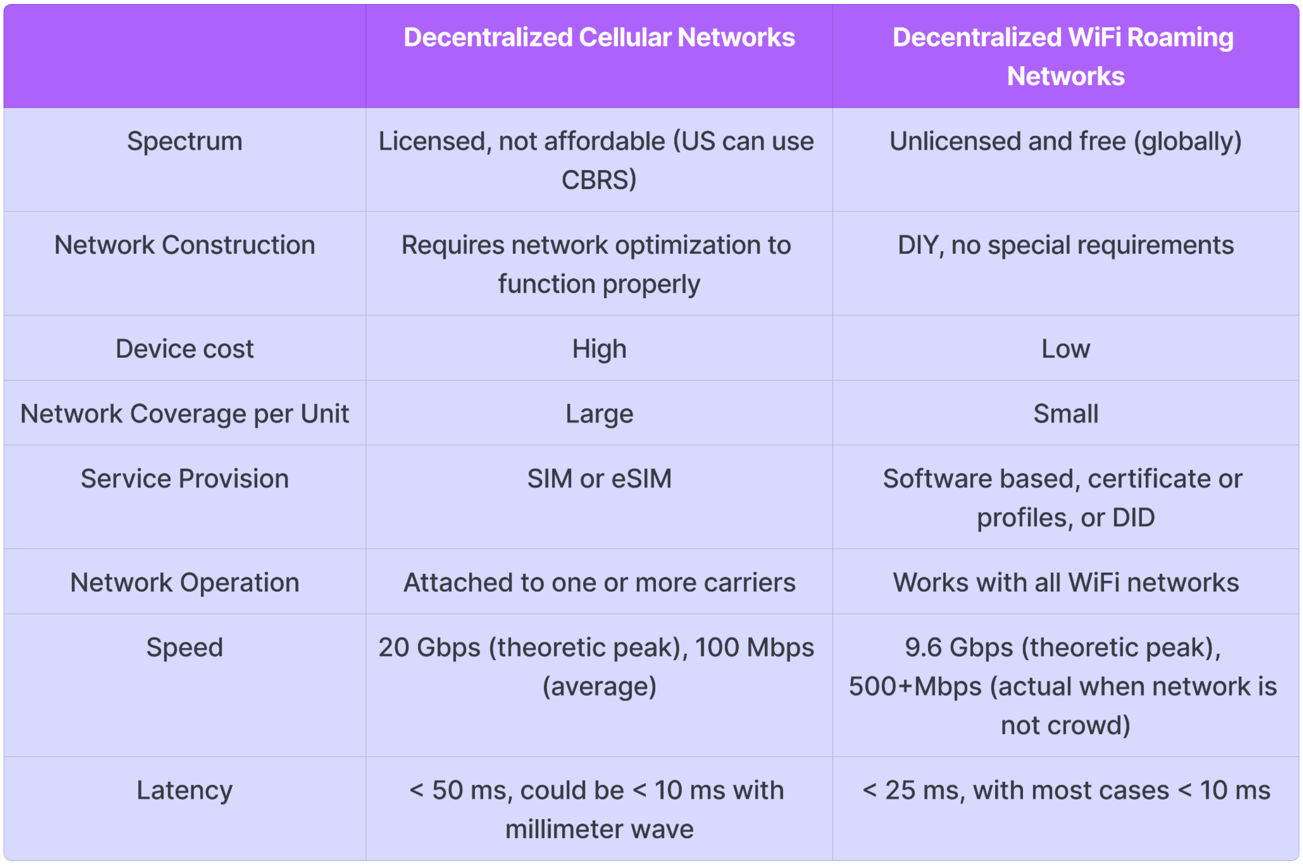


Fig 17, typical wireless access network architecture

rather than dedicated telco equipment. These initiatives and efforts have paved the way for a true decentralized network.

In the diagram above, WiFi and Cellular are represented by two parallel radio access networks, and the data traffic merges at the edge of the network. Since the release of iOS 7, most mobile phones have supported Hotspot 2.0 (formerly Passpoint), which is also supported by nearly all WiFi chips released since 2016. This allows for WiFi off-loading and in fact, (per Section 1.1) WiFi carries more data traffic than cellular networks.

The table below compares the decentralized cellular network with the decentralized WiFi roaming network. As it and the following figures indicate, the key network performance between 5G and WiFi are somewhat similar.



	Decentralized Cellular Networks	Decentralized WiFi Roaming Networks
Spectrum	Licensed, not affordable (US can use CBRS)	Unlicensed and free (globally)
Network Construction	Requires network optimization to function properly	DIY, no special requirements
Device cost	High	Low
Network Coverage per Unit	Large	Small
Service Provision	SIM or eSIM	Software based, certificate or profiles, or DID
Network Operation	Attached to one or more carriers	Works with all WiFi networks
Speed	20 Gbps (theoretic peak), 100 Mbps (average)	9.6 Gbps (theoretic peak), 500+Mbps (actual when network is not crowd)
Latency	< 50 ms, could be < 10 ms with millimeter wave	< 25 ms, with most cases < 10 ms

Table 5, comparison between decentralized cellular networks and decentralized WiFi roaming networks

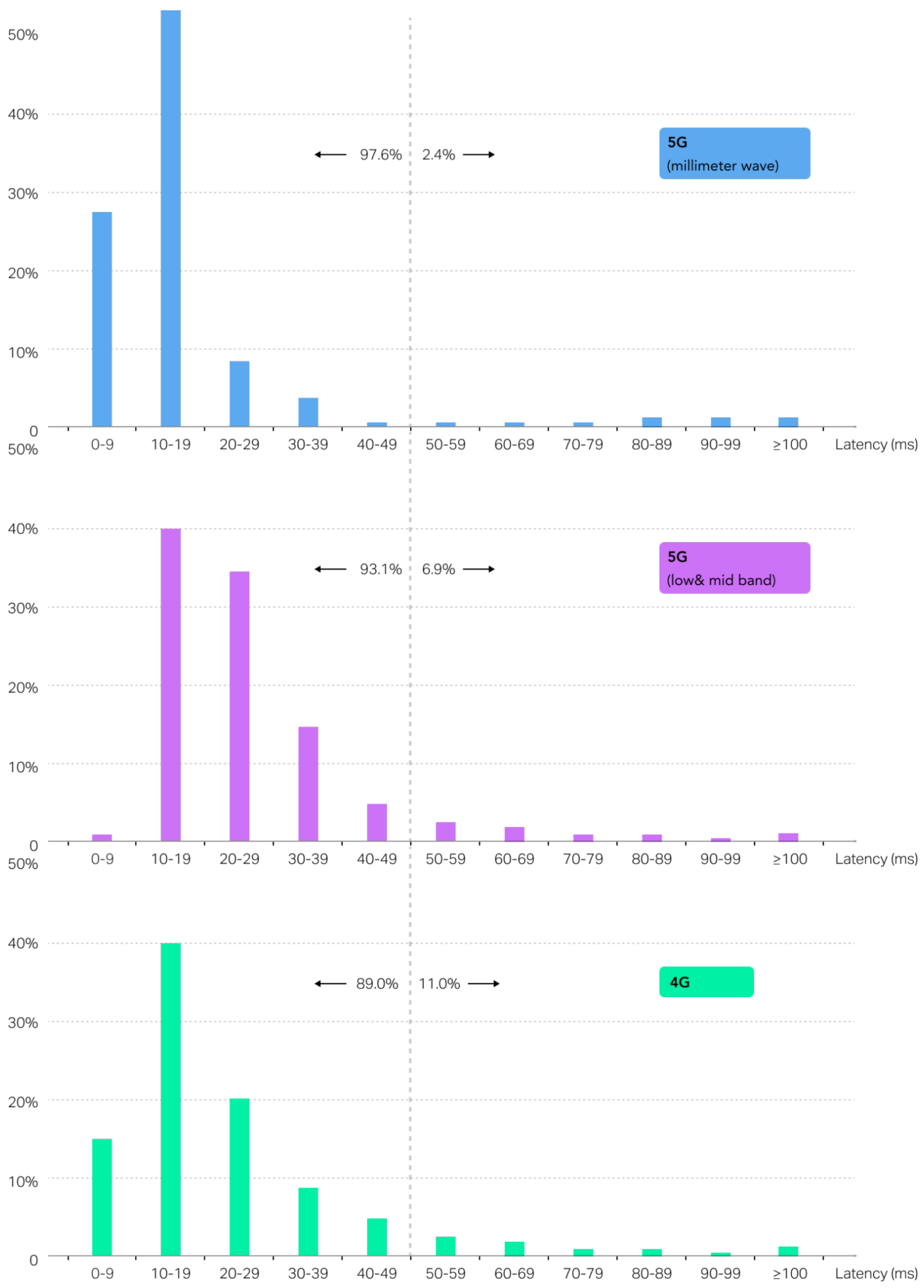


Fig 18, wireless access latency with cellular networks Source: Ericsson analysis of Ookla® Speedtest Intelligence® data U.S. Oct 2021-Mar.2022 [17]

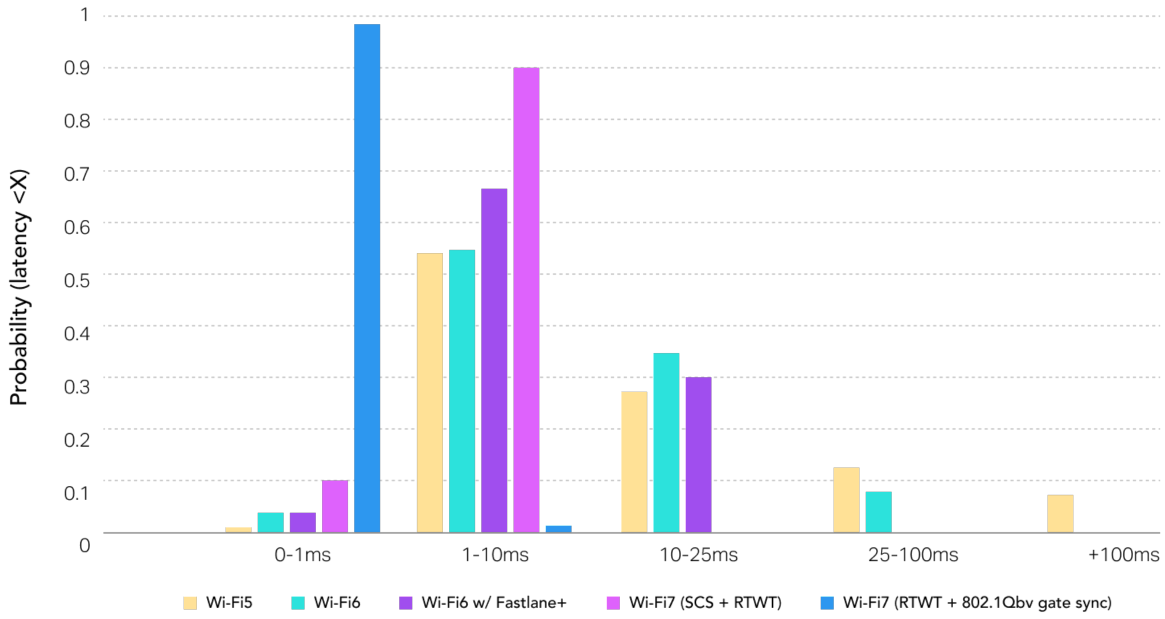


Fig 19, wireless access latency with WiFi networks latencies [18]

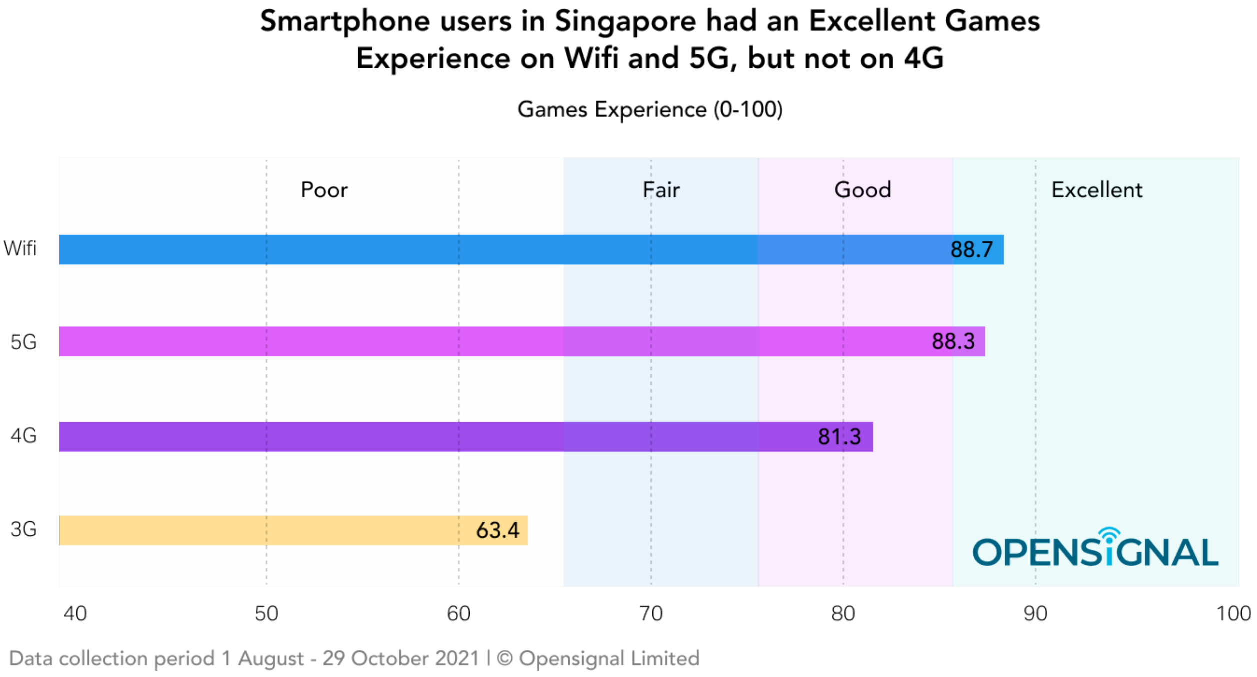
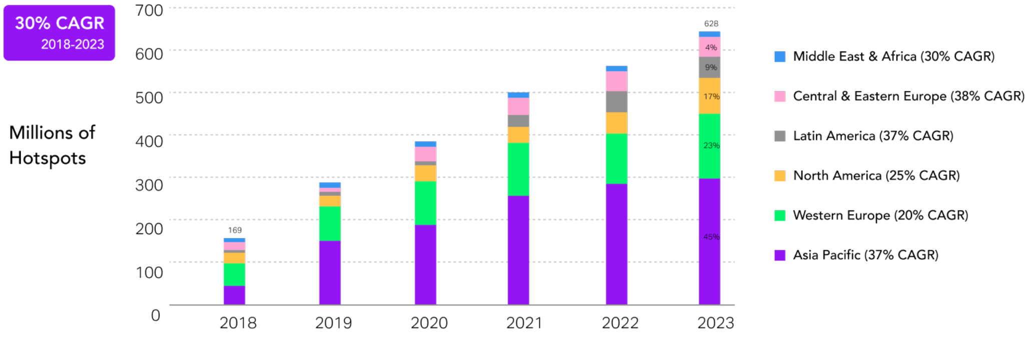


Fig 20, comparing cellular and WiFi connections experiences [19]

From the perspective of decentralized networks, the main challenge for cellular-based networks is the huge barrier set by the existing industrial players and even governments. Decentralized operators cannot acquire the necessary spectrum resources, and must piggyback on other carriers' networks except for the CBRS, which is a 150 MHz wide broadcast band of the 3.5 GHz band (3550 MHz to 3700 MHz) available in the United States only. While the precise spectrum allocations may be different than CBRS, countries like Germany, Brazil, UK and Japan will allow for the same privatization of public radio services. However, an auction must be expected. The number of relevant equipment vendors are also limited due to high entry barriers, and they typically work only with large enterprises, while SIM and eSIM are still highly regulated. The need for network optimization is another challenge unless the decentralized operators can come up with a way to reward people to conduct field services which are inherently off-chain.

On the other hand, WiFi roaming becomes attractive as a feasible path for DeWi. First of all, telcos and mobile devices all support WiFi off-loading now. Secondly, WiFi is the most popular wireless radio access technology available, and it also has the strongest supplier chain.There are 18+ billion WiFi-enabled devices in use, and 500+ million access points are produced every year [3][6][7]. WiFi will thus support decentralized network development, as a DeWi WiFi network's community could access the needed devices easily. Thirdly, WiFi operates in an unauthorized spectrum, and is available globally, making one global operator possible. Fourthly, WiFi does not require complex network optimization in most cases, which makes DIY and community-based deployment possible. And as explained in Section 1, after 10+ years of work by the WiFi alliance,WBA, and the entire industry, seamless global OpenRoaming is now possible, providing the foundation for decentralized global WiFi operators.



*Middle East & Africa represents 1% of global public Wi-Fi hotspots by 2023

Fig 21, global WiFi hotspot growth [6]

If we use the financial model described in Section 2.2 to examine decentralized cellular networks and decentralized WiFi networks, it is clear that WiFi based operators have a strong edge.

Let’s re-examine this formula again:

$$V(t) \ = \ X(t) * \ p(t) = A \ \cdot \ n(N(t), t)^2 \ + (R \ - \ O + O') \ \cdot \ N(t) \ + Y(N(t), t) \ - Z(t)$$

Item $A \cdot \ n(N(t), t)^2$ remains the same between both approaches, as the differences relate to R and O.

$$O = (C + K) \ \cdot \ G \ + \ w\sqrt{N} \ F \ \cdot \ L \ - \ r \ / \ N \ \Delta D$$

In cellular based DeWi networks, R refers to the data plan fees the decentralized carriers charge its customers. In the bootstrap phase, it could be considered minimum or negligible as consumers will not pay that. R could also come from the income generated from the apps or websites related to each location. However, even if a location, like a restaurant, installs a mining rig / small cell, there has not been any business model that proves the restaurant can get any additional value from network users. With WiFi based DeWi, though, locations could charge for WiFi-based services while in most cases, the basic usage of the network could be free. However, WiFi and location based add-on services have become very mature, and are already offered in airports, railway stations, sports venues, etc. Moreover, these revenues from WiFi usage and WiFi services do not require a network effect. Even just one hotspot can create revenue. In short, at the bootstrap phase, WiFi based DeWi enables much higher revenue than cellular based DeWi.

In terms of the cost item, it is known that WiFi gateways are much cheaper than small cells, and the deployment of such devices is much lower in cost and complexity. Their operational costs - for electricity and air conditioning, for example - are lower as well. WiFi networks also do not incur any spectrum usage fees or additional regulatory charges. Though the coverage of one WiFi gateway is still less than a 5G small cell, the overall deployment costs of WiFi networks is still lower, as the interconnection between different nodes largely relies on existing ISP infrastructures. The requirements of enterprise WiFi might adversely affect this conclusion; however, Roam will minimize such an impact by reducing the costs of maintaining a complicated backend.

2.4 Web3.0 and DePIN / DeWi

DePIN and DeWi are the bread and butter of Web3.0. Essentially, these are the main user acquisition channels for Web3.0. With physical network infrastructure becoming such a part of people's daily lives, hopefully a decentralized version could demonstrate the value of Web3.0 and bring people onboard. A decentralized infrastructure foundation is required to support the deployment of a Web3.0 native, user centric network, as the existing, centralized network infrastructure was developed to align with the best interests of telcos and other centralized platforms rather than with the interests of users themselves.

Decentralized infrastructure is infrastructure that is constructed in a self-organized, crowd-funded manner following a protocol; and that operates under autonomous governance. All the value created by such networks return to their founders and users. Profound social motivations and technological advancements drive the development of Web 3.0, which will inevitably arrive to the mainstream. In the 1990s, Web 1.0 emerged, where passively consumed content was presented by websites which became portals to pre-organized digital information. In the Web 2.0 era, companies provided platforms from which users could both consume and create web material. "User created content" became the buzzword of Web 2.0. However, this data was still owned by the platform operators, who also determined what kind of data to share and how. Individual users were identified by these platforms, and their online behaviors were tracked and documented. As a result, though individuals themselves contributed to the majority of Web2 .0 content, the profits it generated were taken by the platforms where they were published, undermining users' privacy. Gavin Wood, one of the early advocates of Web 3.0, pointed out that "the internet today is broken by design. We see wealth, power and influence placed in the hands of the greedy, the megalomaniacs, or the plain malicious. Traditional markets, institutions, and trust relationships have been transposed to this new platform, with the density, power and incumbents changed, but with the same old dynamics." Web 3.0 intends to give any participant in the web their own autonomous power and control. It will end online social unfairness permanently. In addition to that, a platform-centric internet won't be able to support future network needs in terms of scalability, data security and privacy. It also could not utilize tokenomics effectively to grow the internet ecosystem, as this requires a decentralized infrastructure. In short, Web 3.0 is the future of the wireless network, which calls for a new technology stack to support this transformation.

Key middleware is desperately needed in the process of building Web 3.0. First of all, it will enable a decentralized infrastructure layer and allow for the self-governance and self-operation of such infrastructure with the help of tokenomics and the contributions of individuals. Secondly, with the support of the new infrastructure, the middleware shall link the Web 2.0 world with Web 3.0 to allow all the data created in the past or under the conventional, centralized format to be utilized on the new internet. Lastly, it shall allow all users and the content they created to organize and interact on the new internet. Roam protocol was developed to provide this key component of Web 3.0's technology stack. It will return all the data generated by Roam's global OpenRoaming WiFi services back to the public with proper privacy protection measures. In addition, it will support decentralized data storage and edge computing. This is also consistent with ToIP's design principles mentioned above: "for maximum utility and adaptability, the best place to put intelligence and processing is at the endpoints of a network and not in the communications subsystems that connect those endpoints." [20] Under Roam protocol, users thus retain control of what and how to share their data as long as the access network is decentralized and secured.

3 Roam Decentralized OpenRoaming WiFi

3.1 Design Overview

Roam WiFi networks have three main components: Roam protocol, the Decentralized WiFi system, and supporting applications/add-on services. Roam, a provider of secure and seamless OpenRoaming services, is leveraging VCs to enable secure WPA2/3-EAP authentication for its OpenRoaming Network.

Roam protocol is a data exchange protocol designed per the Trust Over IP (ToIP) stack as specified by the Linux Foundation. The protocol serves as a ToIP layer 3, and is fully compatible with the W3C's DID standard and VC standard (to be officially released). It is built on permissionless blockchain systems and is agnostic against the underlying blockchain infrastructure.

The decentralized WiFi system includes three parts: RADIUS and Access Point Controller softwares which support DID/VC log-in; SDKs that allow mobile devices to login to OpenRoaming WiFi using DID/VC, and that gives mobile devices access to the on-chain data; and an OpenRoaming-supporting backend.

Supporting applications and add-on services include Gateway and AP softwares (based on OpenWRT), iOS and Android Apps, etc.

3.2 Roam Protocol

3.2.1 DID

The W3C's DID standard is one of the key components of Roam protocol. The decentralized identifier (DID) is a new, verifiable, and decentralized type of identifier. The DID architecture is shown in Fig. 22. A DID can point to any subject, such as person, transaction, organization, device, etc. It can also be parsed into a corresponding DID Document, which can express the encryption material, verification method, or service that points to the subject. Through these methods, a DID Controller can prove their control over a given DID. In order for the data to be parsed, the verifiable data registration center is responsible for storing DID and DID Document content. The registration center can take any form, such as a distributed ledger, decentralized file system, database, etc.

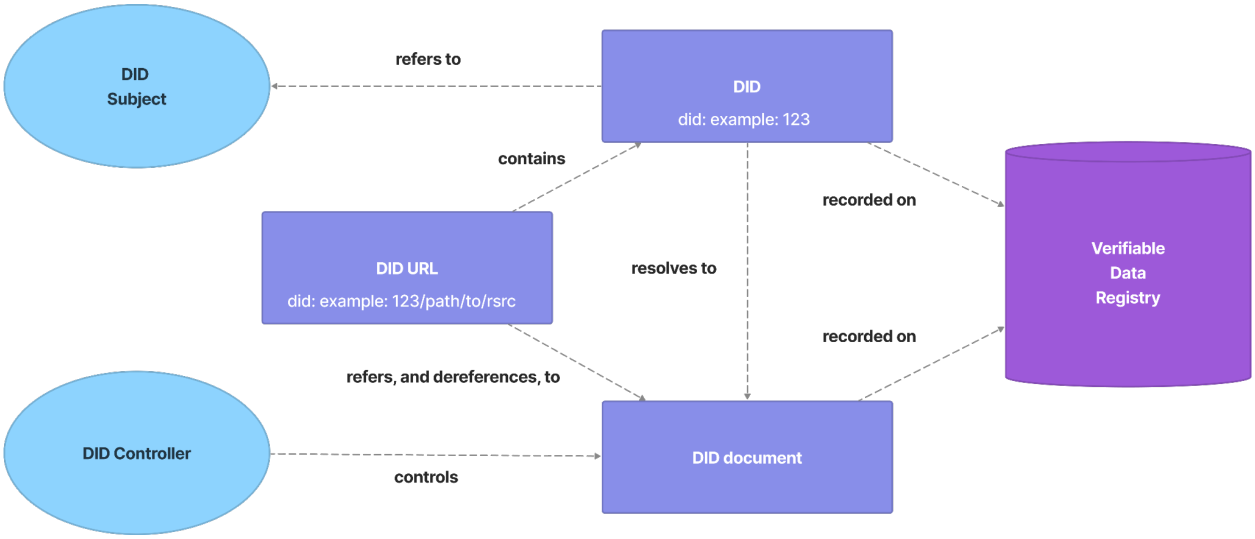


Fig 22, DID architecture, alternate representation [21]

The DID format is shown in Fig 23. A DID is composed of the fixed Scheme "did", DID Method, and identifier in the corresponding DID Method. The DID Method defines how this particular DID type is created, parsed, updated and destroyed.

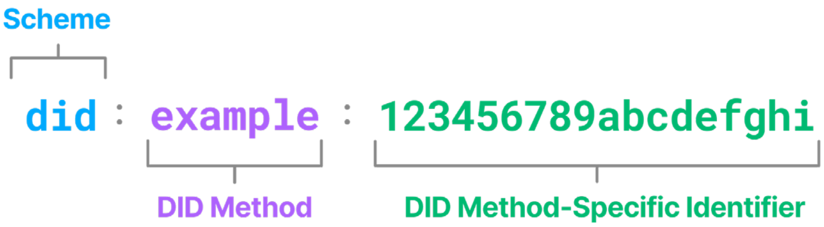

Scheme
did : example : 123456789abcdefghi
DID Method
DID Method-Specific Identifier

Fig 23, DID sample [21]

Roam protocol follows the W3C's DID standard [21], and focuses on its implementation via a permissionless blockchain.

The Elliptic Curve Cryptographic (ECC) algorithm is mainly used to generate the user's DID identity, and must be consistent with the blockchain which Roam protocol uses. Algorithms like SECP256k1, SECP256r1, and ED25519 will be employed in different SDKs. The corresponding private key is the user identity private key.

3.2.2 VC Data Model

The W3C also has a standard for the Verifiable Credential (VC). The VC is the user's digital credential, which has the same function as their physical credential. A verifiable credential is a tamper-evident credential whose authorship is cryptographically verifiable. Compared with a physical credential, the VC provides encryption security, respects privacy and allows for machine-verification, which is a more suitable method for use in Web 3.0 network scenarios.

The VC ecosystem is shown in Fig 24. The Issuer issues a VC to the Holder, who sends proof of it (the VC) to the Verifier. All participants verify its authenticity through the VC data registry. For example, the Issuer records the certificate format information and issuer information in the registration center, and Holder and Verifier check the authenticity of the certificate through the registration center and cryptographic algorithms.

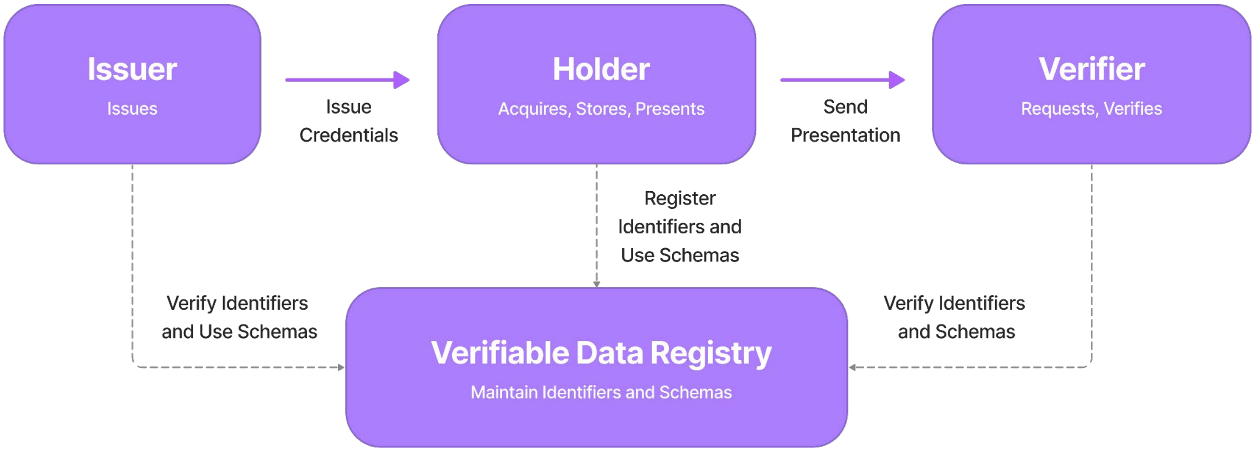

Issuer
Issues
Issue Credentials
Holder
Acquires, Stores, Presents
Send Presentation
Verifier
Requests, Verifies
Register Identifiers and Use Schemas
Verify Identifiers and Use Schemas
Verifiable Data Registry
Maintain Identifiers and Schemas
Verify Identifiers and Schemas

Fig 24, VC based data exchange model [22]

The basic components of the VC are shown in Fig 25. A VC includes metadata such as issuer information of the credential, expiration date, etc. The credential declaration includes the attribute information of the credential and the certification information of the issuer of the credential.

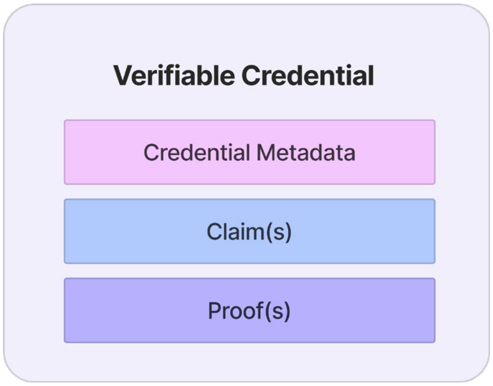


Fig 25, VC declaration scheme [22]

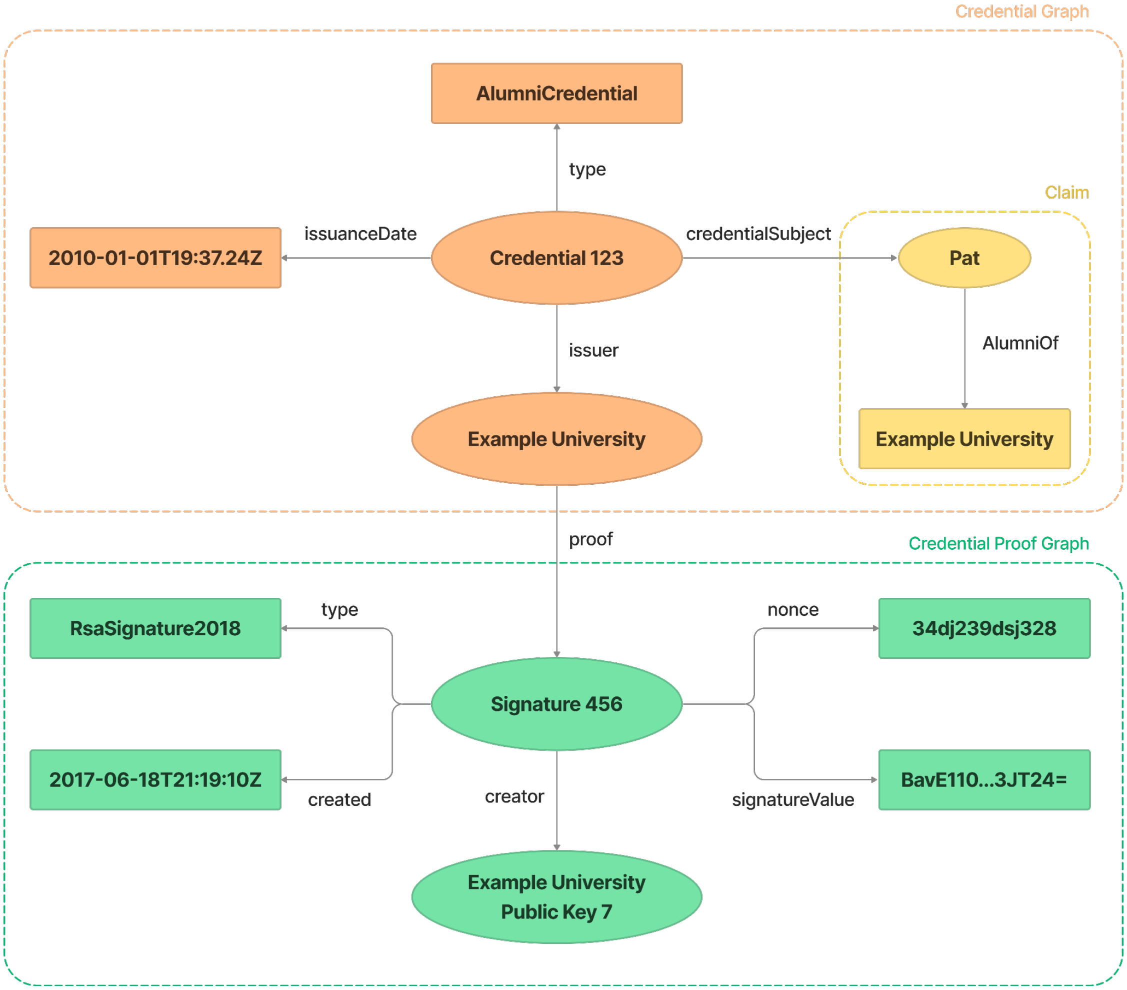


Fig 26, VC component graph [22]

The basic components of the Verifiable Presentation (VP) are shown in Fig 26 [22]. A VP is a display information which consists of metadata, the VC, and proof data. Enhanced privacy is a key feature of the design of this specification, so selecting and exposing only appropriate attribute information is very important for the implementation of this technology. It is common to use zero knowledge proof algorithms in a VP generation and validation process, which ensures that there won't be any privacy leakage concerns. The VC part can contain the attribute information of multiple VCs.

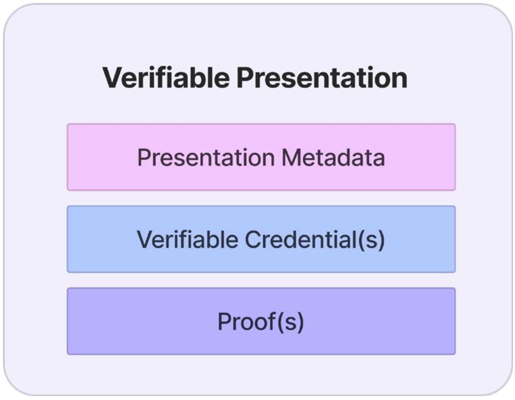


Fig 27, VP declaration scheme [22]

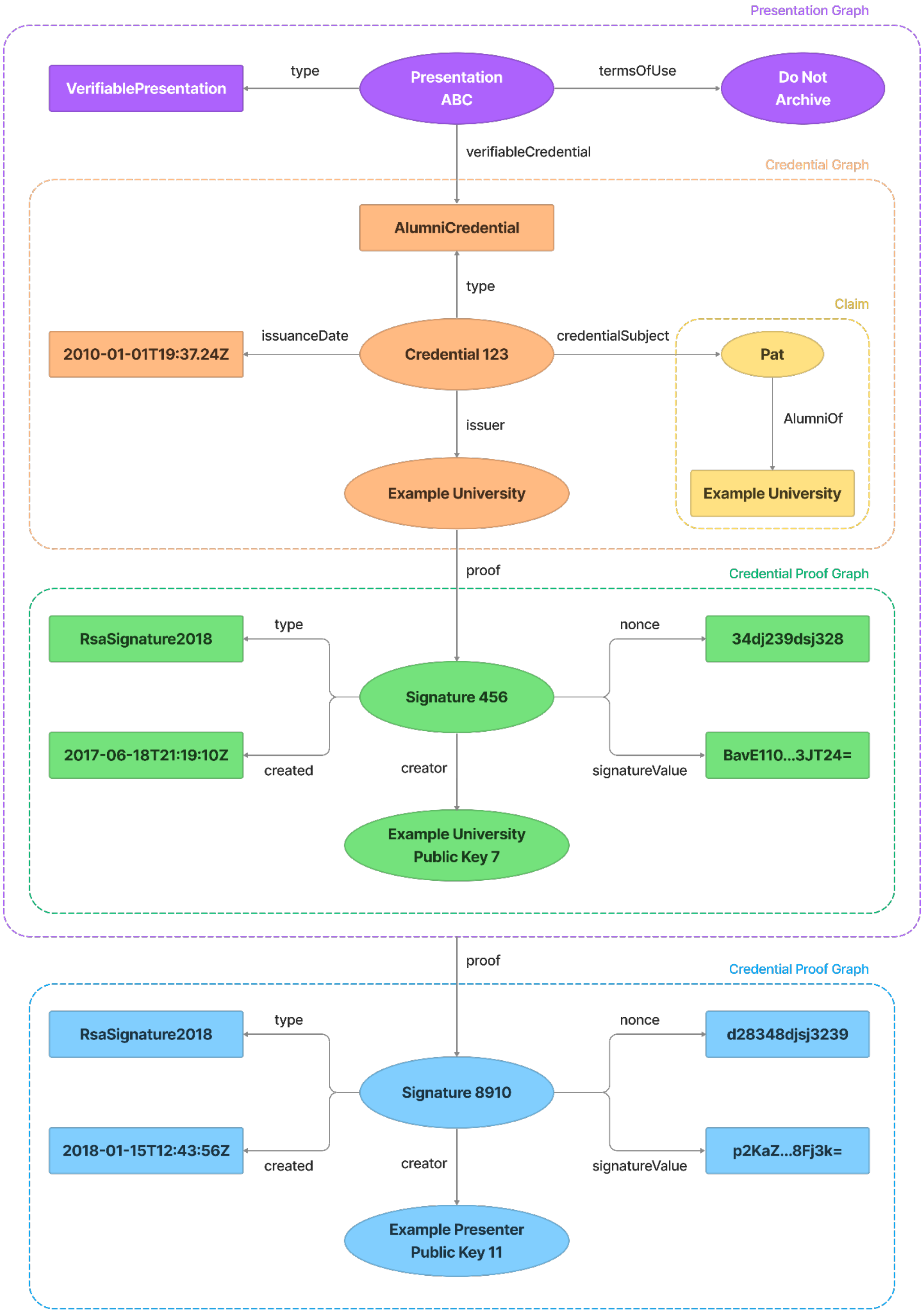


Fig 28, VP component graph [22]

Roam protocol follows the W3C's VC standard, and focuses on its implementation via a permissionless blockchain. Hash Algorithms SHA256, KECCAK-256, etc., are used to generate the hash value of the message to be signed with a private key.

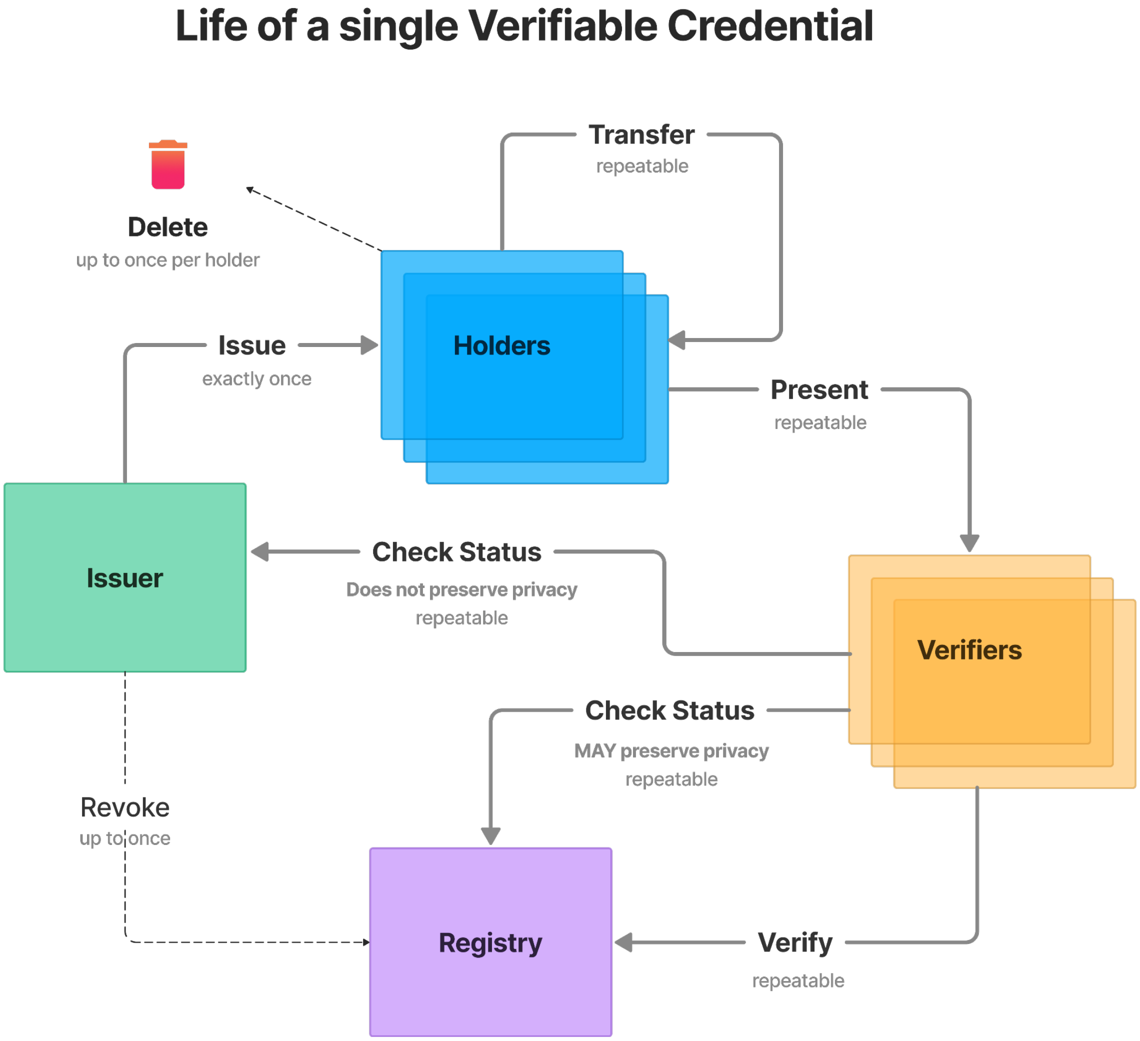


Fig 29, VC lifecycle [22]

Since Roam network utilizes DID/VC to achieve OpenRoaming network authentication, ID providers who want to let their users roam into this network need to download the SDK from Roam foundation to become a VC issuer. This SDK is fully compliant with the W3C's DID and Verifiable Credential standards.

3.2.3 Privacy Protection with DID-VC

Roam allows users to use DID and VC to login to the WiFi system, with all the interactions constituting this process being recorded on a blockchain. A zero-knowledge scheme could be implemented in the VP to add privacy protection to it. In this case, a derived VC (instead of the original one) which encrypts all of the holder's private information will be placed inside the VP.

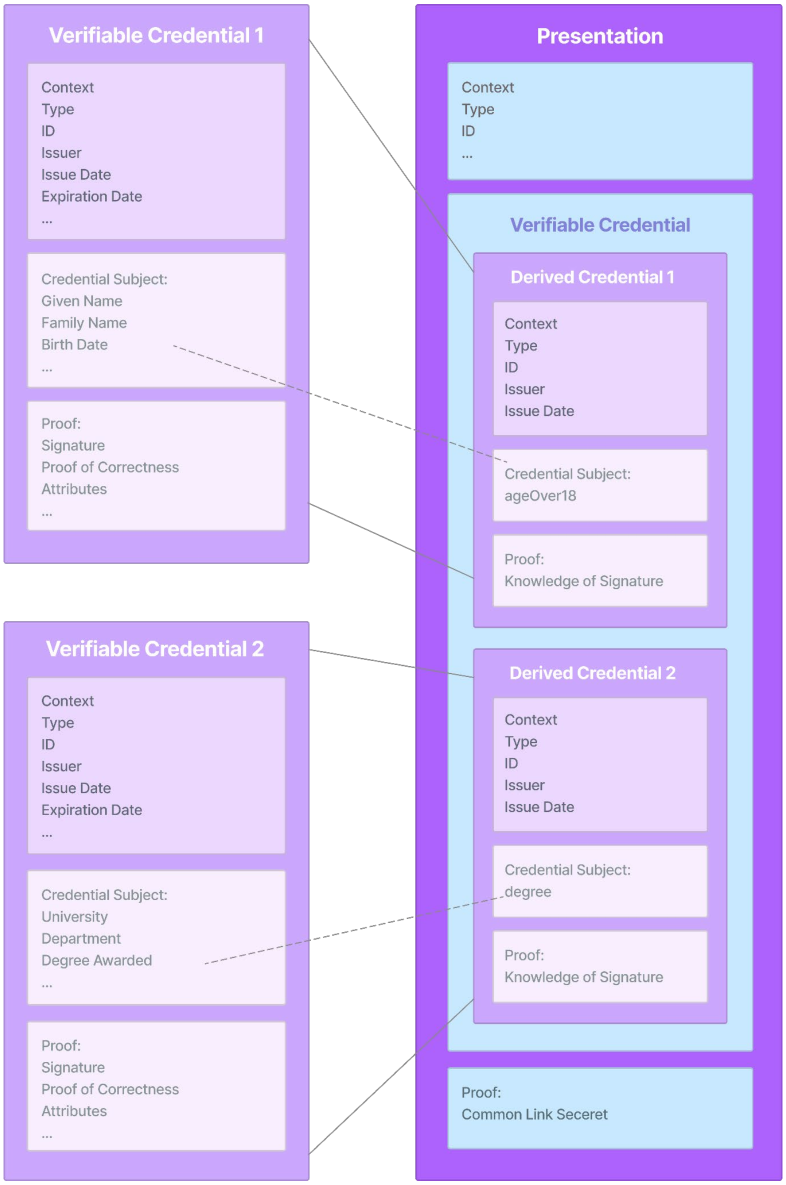


Fig 30, VC-to-VP derivation scheme [22]

ZKPs have two types: interactive and non-interactive. Non-interactive zero-knowledge proofs are cryptographic primitives where information between a prover and a verifier can be authenticated by the prover without revealing any of the specific information beyond the validity of the statement itself. The key advantage of non-interactive zero-knowledge proofs is that they can be used in situations where there is no possibility of interaction between the prover and verifier, such as in online transactions where the two parties are not able to communicate in real time. The ZK-SNARK (Succinct Non-Interactive Argument of Knowledge) is a common implementation of the non-interactive ZKP, and the proof size is limited, making it easy to use. Plonk (Permutations over Lagrange-bases for Oecumenical Non-Interactive arguments of Knowledge), Bulletproof, and SONIC are also common ZKP schemes.

Interactive ZKPs are more suitable for Roam applications, where a challenge is required during the log-in process, like authentication processes using the Challenge-Handshake Authentication Protocol (CHAP). A protocol implementing zero-knowledge proofs (of knowledge) necessarily requires interactive input from the verifier. This interactive input usually takes the form of one or more challenges such that the responses from the prover will convince the verifier if and only if the statement is true, i.e., if the prover does possess the claimed knowledge. If this were not the case, the verifier could record the execution of the protocol and replay it to convince someone else that *they* possess the secret information. In this case, the new party's acceptance would either be justified since the replayer does possess the information (which implies that the protocol leaked information, and thus, is not proved in zero-knowledge), or the acceptance would be spurious, i.e., it was accepted from someone who does not actually possess the information.

Roam protocol design refers to a design similar to the Hyperledger Indy blockchain. Hyperledger Indy provides tools, libraries, and reusable components for providing digital identities rooted on blockchains or other distributed ledgers so that they are interoperable across administrative domains, applications, and any other silo. Indy is interoperable with other blockchains, or can be used as standalone infrastructure powering the decentralization of identity [23]. The Camenisch-Lysyanskaya (CL) signature, Boneh-Lynn-Shacham signature, and other cryptographic signature schemes are employed by Roam protocol. These algorithms are used to either assist in selective disclosure of VC/VP data, or to prove that the attribute values satisfy a certain condition using zero-knowledge algorithms.

Taking the CL signature as an example of a selective disclosure algorithm, the details of its implementation are as follows:

There are three parties in the credential scenario: the issuer, the certificate holder, and the verifier. We assume that the certificate holder has L attributes (m1, m2, m3, ..., mL) that need to be issued by the issuer. The certification process is as follows:

1) Key Generation

The issuer randomly generates two prime numbers {p, q} as the private key, which multiply to create a number n from the private key p and q:

$$n = pq$$

Then, *L+2* random numbers are generated by calculating the quadratic remainder of modulo n:

$$a_1, a_2, a_3, \ldots a_L, \mathrm{b}, \mathrm{c}, \mathrm{n} \in QR_n$$

where, (*a1, a2, ..., aL, b, c, n*) constitute the public key of the message.

2) Signature Generation

The issuer generates a random prime number e, and a random number s. Assuming *L* input attributes in the format of *mi,* (*m1, m2, m3, ..., mL*), the issuing authority calculates a value *v* that satisfies the following formula:

$$v^e \equiv (a1^{m1} \ldots aL^{mL} b^s c) \, mod \, n$$

(*e,s,v*) forms the signature of the message (*m1,m2,...mL*)

3) Signature Verification

Given a signature (*e,s,v*), a message (*m1,m2,...mL*) uses the issuer's public key (*a1*, *a2,...,aL, b,c,n*) to check whether the following formula is satisfied:

$$v^e \equiv (a1^{m1} \ldots aL^{mL} b^s c) \, mod \, n$$

If true, the message invoked above proves that the certificate was issued by the issuing authority and has not been tampered with.

CL signatures support zero-knowledge proofs and selective disclosure of attributes. In the above steps, when the certificate holder sends a message to the verifier, one of two methods could be adopted:

1) Send *mi* directly to the signer/verifier, then the signer/verifier calculates (*ai^mi*) *mod n*
2) Calculate *(ai^mi) mod n*, call the commitment of *mi*, and send the commitment to the signer/verifier.

Since the discrete logarithms are mathematically difficult, it is challenging for the signer/verifier to infer the value of *mi* from the committed value, so the signer can generate the signature without knowing the original value. Similarly, a verifier can verify certificate attributes without knowing the original value.

For example, a certificate holder has attributes (*m1, m2, m3*) and wishes to disclose only (*m1, m2*) in the message, while *m3* uses a zero-knowledge proof. When the issuing authority signs the certificate, the certificate owner sends (*m1, m2, a3^m3 mod n*) to the issuing authority. When presenting the proof and the certificate owner only wants to disclose the attribute *m2*, they send (*a1^m1 mod n, m2, a3^m3 mod n*) to the verifier, who can prove that the certificate owner has not tampered with the attributes of the certificate, and who can see the value of *m2*.

3.2.4 Trust over IP Stack

The Trust over IP technology stack developed by the Linux foundation is referred to in Roam's architecture design. In the typical ToIP stack, Layer 1 is the utility layer, which supports the public DID utilities needed to look up and verify the current public keys of digital credential issuers. In public/private key infrastructure, these cryptographic "starting points" are called roots of trust, or trust anchors. ToIP Layer 2 is the communication layer, which supports the private digital wallets and agents needed in order to accept, store, and exchange digital credentials over a standard peer-to-peer protocol such as DIDComm. Layer 3 is the data exchange layer used to create the verifiable credential trust triangle that enables the establishment of transitive trust relationships between any three parties anywhere in the world using the data exchange formats and protocols for verifiable credentials. Layer 4 is the application layer, which enables the market applications needed to build healthy, vibrant digital trust ecosystems atop this new decentralized digital trust infrastructure.

Roam is one kind of implementation of Trust over IP in terms of real-world application. The W3C's DID and VC standards are relevant to ToIP Layer 1 and Layer 3 respectively, and they (DID and VC) are the foundation of Roam protocol. In addition, Roam protocol supports multiple DIDs for the same subject on one or multiple blockchains, and these subjects on different chains can use the Layer 2 DIDComm protocol per ToIP to communicate. Roam protocol provides a blockchain independent DID layer design which will greatly facilitate such communications. In the end, Roam protocol will support all the applications described in ToIP.

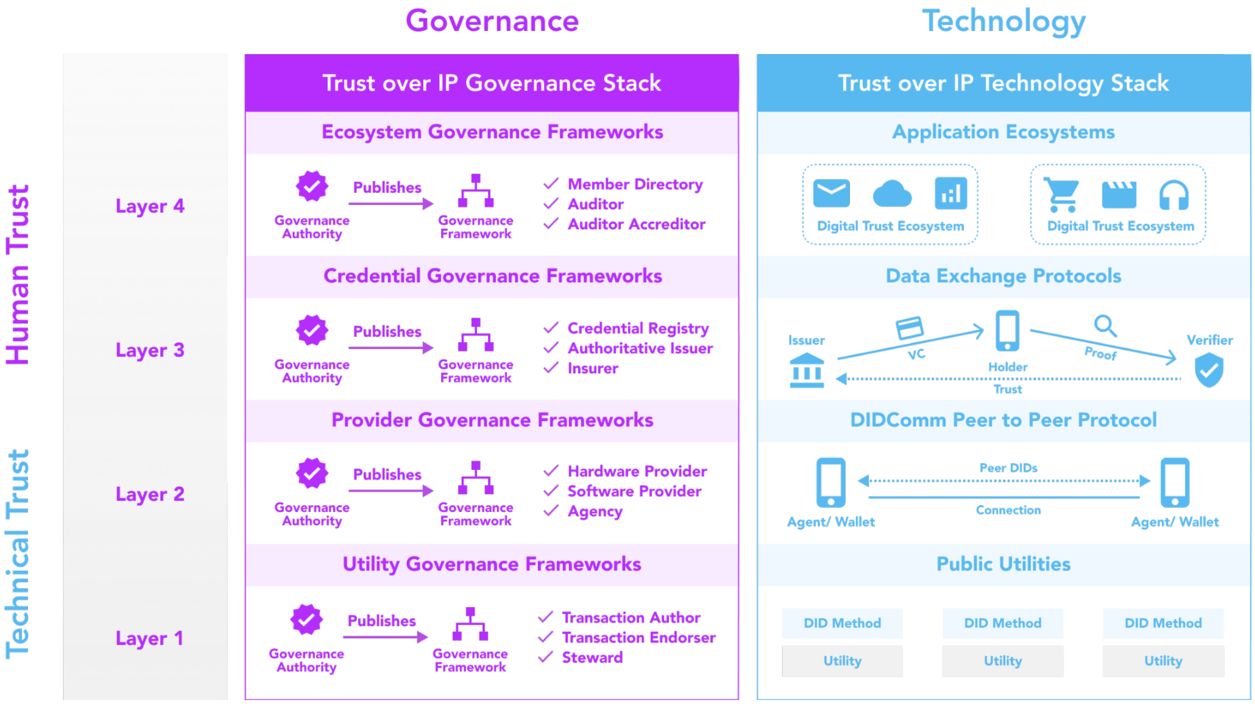


Fig 31, ToIP technology and management stack [23]

ToIP aims to provide a robust, common standard and complete architecture for internet-scale digital trust (as shown in Fig. 31), which is the basis of Web 3.0's user centric network. At the same time, the Linux foundation intentionally neglected to define how to implement ToIP. In fact, one of the key design principles of ToIP is that every protocol in the ToIP Technology Stack must be implementation-independent. Roam protocol is one such implementation, and provides a complete sdk to support applications built on ToIP.

The following design rules are followed by Roam protocol:

1) To maximize security, privacy, and confidentiality, cryptographic private keys should be stored at the edges of the network, not on intermediate nodes. Roam protocol allows users to control their own private key. The devices which are used to support Roam-enabled decentralized wireless network access, edge computing, storage, and caching will have their own private key stored in their own trustzone or similar hardware vault.

2) As part of digital trust, messages and data structures exchanged between parties should be verifiable as authentic using standard cryptographic algorithms and protocols. Parties communicating over ToIP protocols should expect communications to be secure, private, and confidential without any special thought or action required on their part. Roam protocol is developed based on proven cryptographic algorithms and is consistent with industry-

acknowledged standards. All communications that occur within the Roam-enabled network will remain secured and confidential by design.

3) To be trusted by all parties, a global network cannot favor any single centralized service or authority; it must allow functionality and authority to be distributed as widely as possible. Roam protocol follows this principle and will advocate a decentralized and self-operational wireless access network as well as an edge computing and storage / caching service network. These networks are expected to form the foundation of Web 3.0, for which no centralized service will be used.
4) For maximum utility and adaptability, the best place to put a network's intelligence and processing is at its endpoints rather than in the communications subsystems that connect those endpoints. This principle is consistent with the nature of decentralized communication infrastructure.
5) In a layered protocol architecture, the most successful design takes an hourglass shape where a single "spanning layer" in the middle connects a family of higher-level, application-facing protocols via a family of lower-level transport protocols. Roam was developed to support higher level data oracle protocols, authentication methods, and other user applications. On the other hand, it supports a lot of communication and network protocols like IEEE802.11u.

3.2.5 Blockchain Network Independence

In the traditional DID scheme, the private key of the DID user and their blockchain wallet address are the same. This design prevents the DID-based authentication process from being isolated from the details of the given blockchain platform where it is carried out. We believe that the core content of the DID consists of the different private keys that identify the user's identity; and that each private key should have a single purpose. Based on these ideas, we designed the Roam protocol.

First of all, we distinguish the wallet private key of the blockchain from the DID private key. For example, registering and updating a certain DID can be submitted by any blockchain address. At the same time, the blockchain will verify the legitimacy of the transaction itself, and a smart contract will check the submission for whether the data has a legal signature of the private key corresponding to the DID.

Secondly, in the basic library design of DID/VC, we separate the blockchain-related codes from the system access components. The overall architecture is shown in Figure 6. For the basic DID information, we use the same structure, and for the registry, we use different registration methods according to different blockchains.

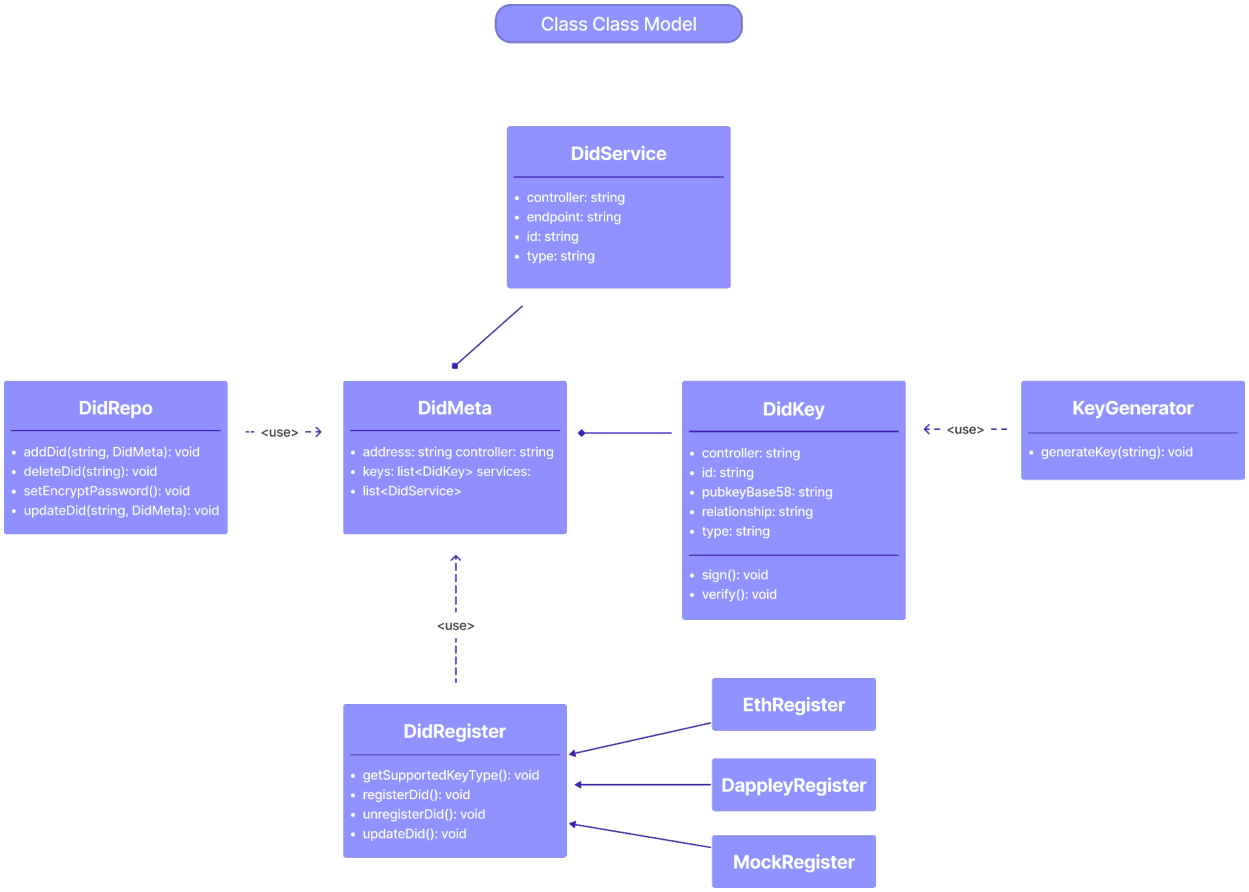


Fig 32, Roam DID/VC SDK architecture

3.2.6 Improvements over Hyperledger Indy/Aries

Roam protocol's design takes as a main reference the DID / VC implementation developed by Hyperledger Indy/Aries, which has been predominantly contributed to by Sorvin. Sorvin's Self-Sovereign Identity (SSI) concept and Hyperledger Indy/Aries inspire Roam protocol's design concepts. Roam protocol is necessary for the DID / VC implementation, however, as Hyperledger Indy is very difficult to port to other blockchains.

Roam DIDs and Indy DIDs share the following similarities:

(1) Both are designed based on the SSI concept.

(2) Both represent mature implementations of DID / VC, with the Roam zero-knowledge proof algorithm borrowing the mature implementation of Indy.

The main differences between these two DIDs are:

(1) Indy is based on its own blockchain design, development is tightly coupled with its own blockchain, and it is difficult to port to other platforms. One of the original design motivations of Roam protocol was the need to make adapting to other blockchains more friendly.

(2) The business goals are different. Indy/Aries is mainly positioned as a certificate issuing platform. Roam provides a user authentication infrastructure that protects user privacy based on the issuance of credentials.

3.2.7 On-chain Data Access

As a data exchange layer protocol, Roam protocol is designed for data interaction and supports on-chain data enquiry. Although the DID and VC are stored locally in the user's own wallet, the following information will be stored on a blockchain which the user can access via SDK.

The smart contracts on-chain include:

On-Chain registration

On-chain registration maintains the status of each VC (whether it is valid or not). When the verifier validates a VP, it relies on the on-chain registration to confirm the status of the VC, which is used to generate the VP.

On-Chain Mining Device Status and Location

Each Roam mining device will have a VC issued by the foundation. Each device will report to the on-chain smart contract their status, which includes their PCOI, location, QoS level, etc. Besides PCOI, most information publishing is optional for the access point (miner) hosts.

Validator Management

Any user who stakes a certain amount of tokens can become a network validator. To gain validation rights, they need to present a VP to the validator management smart contract.

Validation Management

Each time a validator validates the status of an access point, they interchange the VP between each other, and the VP of the other party will be embedded into the mining rewards request made to the smart contract. It will also validate the status and location information posted by the miner on-chain

Network Usage Check

Each time a user logs in to a Roam-powered OpenRoaming network, it is optional to post the relevant information to the blockchain for further data analytics purposes. Which data shall be posted will be determined by the community.

3.2.8 Roam Protocol System Architecture

The following system architecture is proposed for Roam protocol. It is designed to work with multiple L1 networks as an independent DID / VC middleware tool.

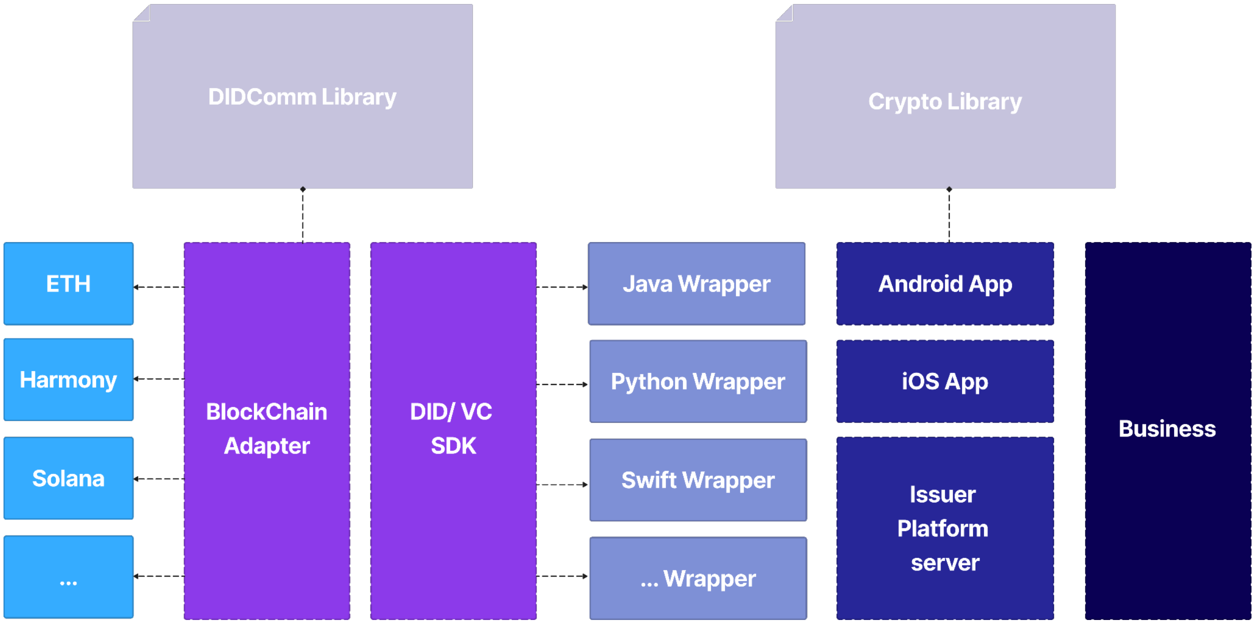


Fig 33, Roam protocol design

3.3 Roam WiFi

Roam WiFi is enabled by three components: a RADIUS and Access Point Controller which supports DID/VC-based log-ins; SDKs that allow for mobile devices to login to OpenRoaming WiFi with DID/VC, and that give these devices access to the on-chain data; and an OpenRoaming-supporting backend including SDKs for any ID providers becoming OpenRoaming ID providers via Roam.

3.3.1 DID/VC log-in

3.3.1.1 RADIUS Integration

In order to allow users to login to WiFi with DID/VC, the RADIUS system must support these standards, and the methods it uses must work with the user devices as well. The majority of the Roam innovation is related to the authentication process.

On the user device side and using iPhone as an example, developers can configure the various EAP protocols for Apple devices enrolled in a mobile device management (MDM) solution. MDM solutions can support the following 802.1x authentication methods for WPA Enterprise and WPA2 Enterprise networks: TLS, TTLS (MSCHAPv2), EAP-FAST, EAP-SIM, PEAP (EAP-MSCHAPv2, the most common form of PEAP), PEAP (EAP-GTC, less common and created by Cisco), EAP-AKA (requires no additional configuration). As mentioned in section 1.2.1.3, EAP-TLS, EAP-TTLS, and EAP-PEAP are three possible choices for enterprise WiFi, and all of them are supported by the existing RADIUS protocol.

Under EAP-TLS, both the client and the server must be assigned a digital certificate signed by a Certificate Authority (CA) that they both trust. With a client-side certificate, a compromised password is not enough to break into EAP-TLS-enabled systems because the intruder still needs to have the client-side certificate. Although EAP-TLS has a higher security standard, it is a nightmare to manage both sides of the certificate, which makes it impractical for a WiFi login system. As a result, EAP-TTLS and EAP-PEAP are more common for a WiFi RADIUS setup.

Both EAP-TTLS and EAP-PEAP make use of the Transport Layer Security (TLS) protocol to provide integrity and confidentiality protection. In EAP-TTLS/PEAP, the server mainly uses two phases, i.e., the TLS handshake and TLS tunnel phase, to establish a secure connection to the client. These protocols only require a server certificate, while the client authentication is optional per the RFC standard. During the TLS handshake phase, the TTLS server authenticates the client using standard TLS procedures. In the tunnel phase, the client authenticates the server using an arbitrary protocol within the encrypted tunnel. The protocol can be EAP, PAP, MS-CHAP, and so on. On EAP-TTLS, after the server is securely authenticated to the client via its CA certificate and optionally, the client to the server, the server can then use the established secure connection ("tunnel") to authenticate the client. EAP-PEAP is similar in design to EAP-TTLS, requiring only a server-side PKI certificate to create a secure TLS tunnel to protect user authentication. It uses server-side public key certificates to authenticate the server,then creates an encrypted TLS tunnel between the client and the authentication server. PEAP is an SSL wrapper around EAP,while TTLS is an SSL wrap.

EAP-PEAP is especially useful as a mechanism to augment the security of legacy EAP methods. The difference between it and EAP-TTLS is that instead of encapsulating EAP messages within TLS, the TLS payload of EAP-TTLS messages consists of a sequence of attributes. By including a RADIUS EAP-Message attribute in the payload, EAP-TTLS can be made to provide the same functionality as EAP-PEAP. If, however, a RADIUS Password or CHAP-Password attribute is encapsulated, EAP-TTLS can protect the legacy authentication mechanisms of RADIUS.

The advantage of this becomes apparent if the EAP-TTLS server is used as a proxy to mediate between an access point and a legacy home RADIUS server. When the EAP-TTLS server forwards RADIUS messages to the home RADIUS server, it encapsulates the attributes protected by EAP-TTLS and inserts them directly into the forwarded message. The EAP-TTLS messages are not themselves forwarded to the home RADIUS server. Thus the legacy authentication mechanisms supported by existing RADIUS servers in the infrastructure can be protected for transmission over wireless LANs. EAP-TTLS is also the most common approach to secure authentication and communication used for WiFi.

Let’s examine a typical RADIUS-based login process for Roam WiFi, where EAPoL Protocol = Extensible Authentication Protocol over LAN:

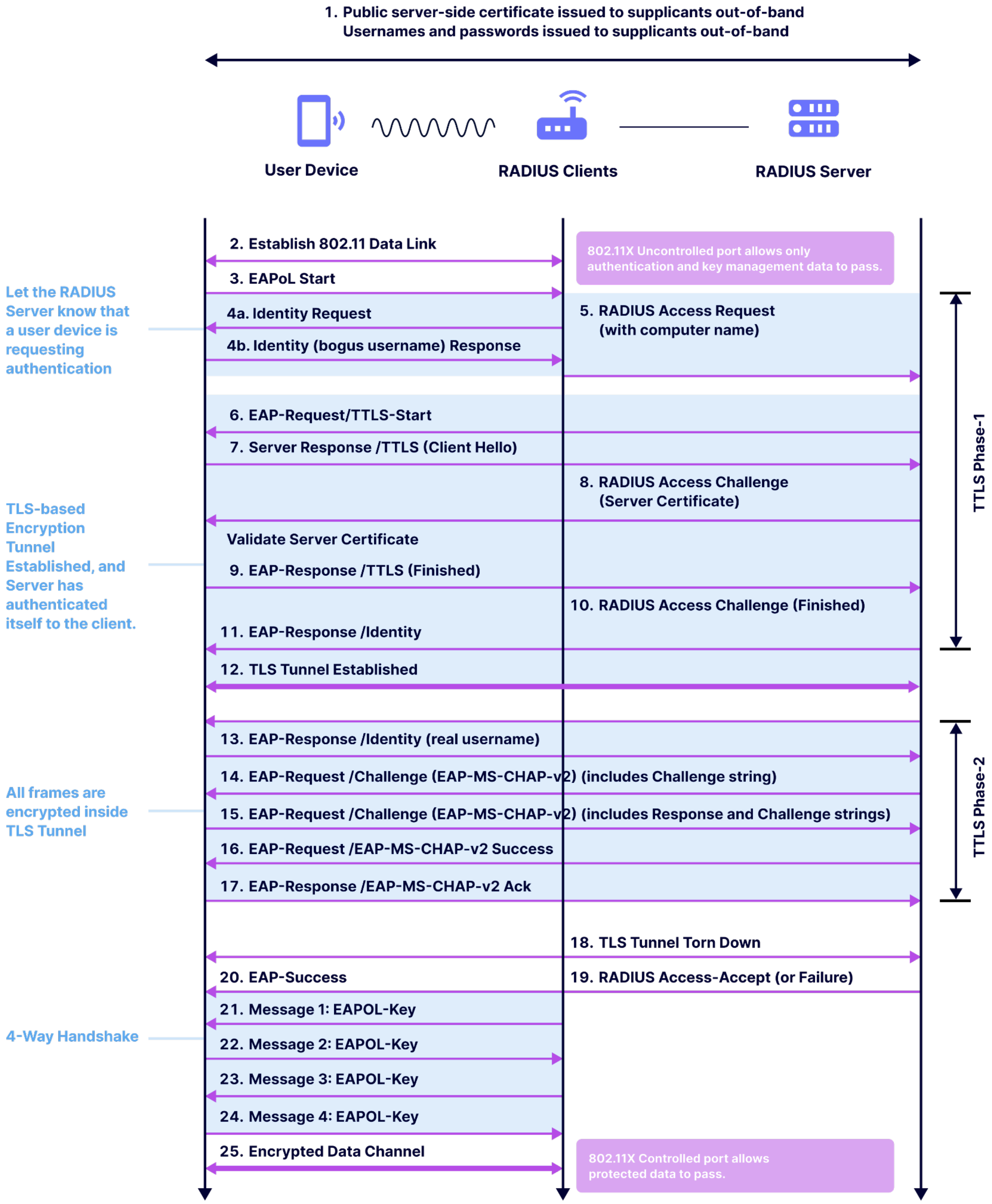

1. Public server-side certificate issued to supplicants out-of-band
Usernames and passwords issued to supplicants out-of-band
User Device
RADIUS Clients
RADIUS Server
2. Establish 802.11 Data Link
802.11X Uncontrolled port allows only authentication and key management data to pass.
3. EAPoL Start
Let the RADIUS Server know that a user device is requesting authentication
4a. Identity Request
4b. Identity (bogus username) Response
5. RADIUS Access Request (with computer name)
6. EAP-Request/TTLS-Start
7. Server Response /TTLS (Client Hello)
8. RADIUS Access Challenge (Server Certificate)
TLS-based Encryption Tunnel Established, and Server has authenticated itself to the client.
Validate Server Certificate
9. EAP-Response /TTLS (Finished)
10. RADIUS Access Challenge (Finished)
11. EAP-Response /Identity
12. TLS Tunnel Established
TTLS Phase-1
13. EAP-Response /Identity (real username)
14. EAP-Request /Challenge (EAP-MS-CHAP-v2) (includes Challenge string)
All frames are encrypted inside TLS Tunnel
15. EAP-Request /Challenge (EAP-MS-CHAP-v2) (includes Response and Challenge strings)
16. EAP-Request /EAP-MS-CHAP-v2 Success
17. EAP-Response /EAP-MS-CHAP-v2 Ack
TTLS Phase-2
18. TLS Tunnel Torn Down
20. EAP-Success
19. RADIUS Access-Accept (or Failure)
21. Message 1: EAPOL-Key
4-Way Handshake
22. Message 2: EAPOL-Key
23. Message 3: EAPOL-Key
24. Message 4: EAPOL-Key
25. Encrypted Data Channel
802.11X Controlled port allows protected data to pass.

Fig 34, a typical WiFi login process based on RADIUS-EAPoL [24]

If a login process does not rely on a username and password, the following changes shall be made:

In the handshake phase, the TLS tunnel will be established based on a certificate derived from the same private key as the DID owner. In this situation, the following steps are required:

a) First, the user, AP (RADIUS client), and RADIUS need to register their DIDs in the on-chain registry. The VC issuer will maintain VC status in on-chain registries as well. This will replace the step 1 in the standard WiFi login process.
b) To sign the certificate, the RADIUS will use the same private key as either the root CA, or the intermediate CA (if it is in the chain of trust within a large system).
c) Once a device encounters an access point (authenticator), communication will be established with the RADIUS via IEEE802.1x.
d) The AP will send an ID request, and the user provides a bogus username, which the AP adds with its DID, and sends to the RADIUS server.
e) The RADIUS server sends EAP requests with it DID, and the user provides their DID with a Hello message.
f) The RADIUS server responds to the user with its certificate, which the user will validate.
g) The user will respond and the RADIUS server will move to the next step and ask for a real username. After this, the tunnel is established.

In the tunneling phase, the main difference between Roam WiFi and regular WiFi is that the RADIUS does not use the username/password information as in the normal case. Instead, the RADIUS server will try to validate the VP of the user to check whether the VC holder who issued the VP has the right to log-in. The tunneling phase of the Roam WiFi login process is as follows:

a)The user sends their DID including a Roam realm to the RADIUS server.
b)The RADIUS server sends a request with a MS-CHAP-V2 challenge. The challenge is a random number per MS-CHAP-V2 protocol.
c)The user responds to the challenge by sending a VP back to the RADIUS server, in which the nonce is set by the challenged number defined in the last step. Due to the fact that MS-CHAP-V2 has a fixed attribute specification, the VP could not be incorporated unless it has been put into the vendor-specific field per RFC 2865 section 5.26.
d）Once the RADIUS server receives the VP, it will from the blockchain validate its content (checking that it is ok to login) and the status of the VC behind it.
e) The RADIUS server will acknowledge the user.
f) Encrypted data communication will start.
g) The RADIUS server will return the VP of the RADIUS back to the user, who will acknowledge the VP's reception.

The key process is to attach the VP to the CHAP challenge. Note that the above process implemented with EAP-TTLS has a weakness: in the RADIUS protocol associated with EAP-TTLS, the vendor-specific information is not originally designed as a judgment factor but rather as an optional factor. Though Roam can manage this weakness with an update to RADIUS, it is still better to use EAP-TEAP instead. Tunnel Extensible Authentication Protocol (TEAP) is a tunnel-based EAP method that enables secure communication between a peer and a server by using the Transport Layer Security (TLS) protocol to establish a mutually authenticated tunnel. Within the tunnel, data in the form of type, length, and value (TLV) objects are used to send further authentication-related data between the EAP client and the EAP authentication server. The main benefit of engaging TEAP rather than TTLS is that with TEAP, the VP which is associated with the vendor specific information could be included as a mandatory attribute of the challenge. Due to this situation, any devices which support EAP-TEAP - like Windows 10 and Windows 11 devices - will natively support Roam protocol, and a mobile app will not be needed purely for the WiFi log-in process.

The EAP-TEAP implementation process for WiFi logins is as follows:

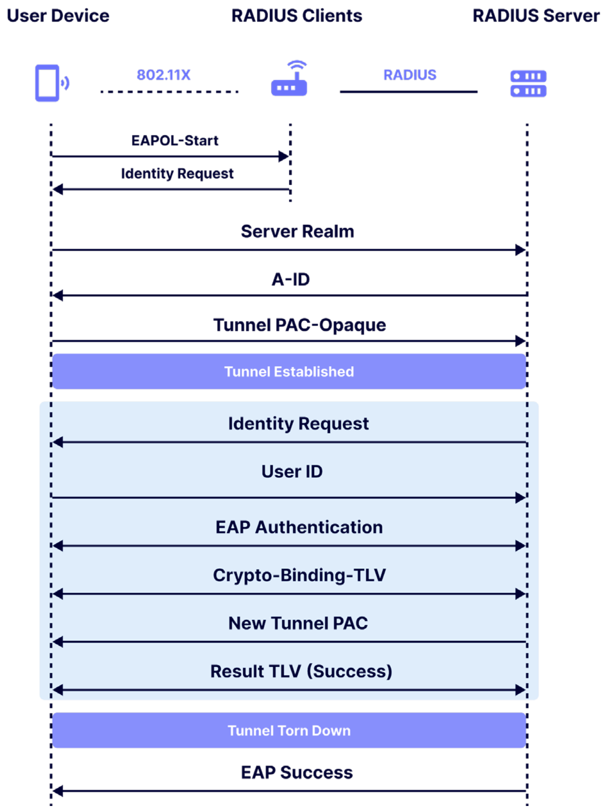
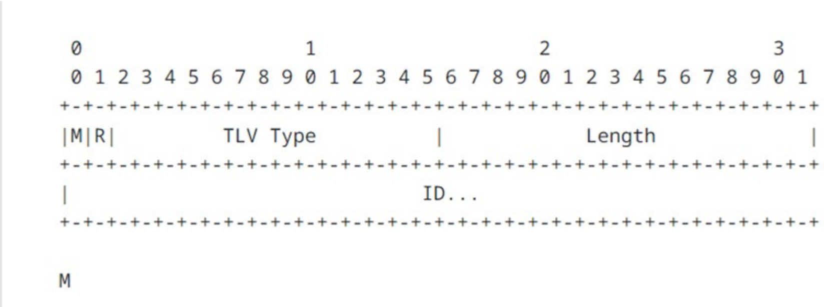


Fig 35, the RADIUS-based WiFi login process implementing EAP-TEAP

In comparison to the standard process as shown above, the following changes have been made to EAP-TEAP by Roam protocol to provide a more native implementation of DID / VC for the WiFi authentication process:

a) In the (Authority-ID TLV) sent by the RADIUS server to the supplicant (user), the RADIUS DID is included in the ID session following the format below:

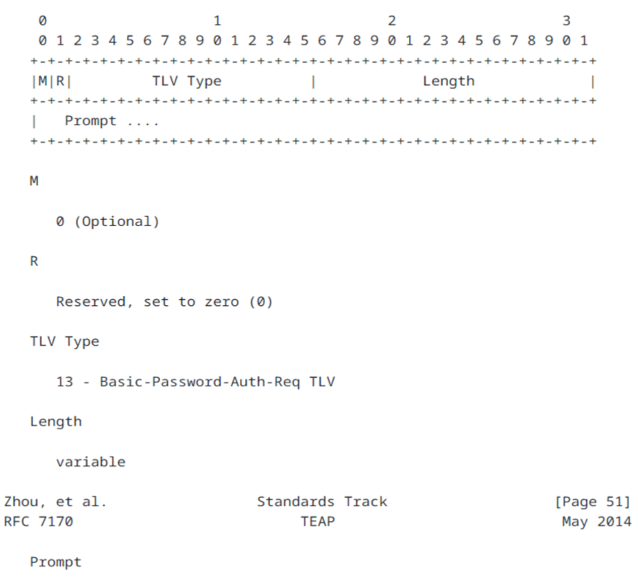


```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|M|R|         TLV Type          |            Length             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                              ID...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+


M
```

Fig 36, the ID session of EAP-TEAP [25]

b) The user authentication process is based on Basic-Password-Auth-Req. Similar to the login implementation of EAP-TTLS, the username is the user's DID and the Prompt is the user's VP. The RADIUS server verifies the user's identity via their VP. The Basic Password-Auth-Req TLV is as follows:



```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |M|R|         TLV Type          |            Length             |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |   Prompt ....
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

   M

      0 (Optional)

   R

      Reserved, set to zero (0)

   TLV Type

      13 - Basic-Password-Auth-Req TLV

   Length

      variable

Zhou, et al.                 Standards Track                   [Page 51]
RFC 7170                          TEAP                          May 2014

   Prompt
```

Fig 37, the Basic Password-Auth-Req TLV of EAP-TEAP [25]

The above discussion explains the difference in the authentication processes between Roam and regular Passpoint / OpenRoaming WiFi. In terms of authorization and accounting, the process will be similar between Roam and other Passpoint / OpenRoaming WiFi networks as described in Section 1.2.2.3 (Onboarding Policy Control).

3.3.1.2 Distributed RADIUS Service

To support Roam WiFi, a distributed RADIUS will be operated by the Roam foundation initially. Access points could search the RADIUS and connect to a usable RADIUS server automatically. The status of the credentials of these distributed RADIUS servers will be maintained by the blockchain. Load balancing will be implemented by allowing miners to randomly select different RADIUS /AAA servers. Later-on, elected community representatives will participate in these services by staking a certain number of tokens. In return, they will be awarded with further tokens since they must defend the network against malicious attacks and ensure its smooth operation. The distributed RADIUS could be further developed based on FreeRADIUS, using one of its modules for the updated EAP-TTLS implementation as well as the EAP-TEAP implementation. Please note that the RADIUS client will reside in each miner.

The proposed log-in process requires users to hold a valid VP. As a result, trustworthy VC issuers are required, and the Roam foundation maintains a list of their public keys. When a device interacts with the access points, both parties will verify each other's DID status on-chain. If both are valid, the exchange of VPs will happen as well. During this process, the VC information included in either party's VP will be examined, including who the issuer is, whether the issuer is trustworthy per the on-chain list, and whether the VC has been altered illegally. This will be carried out by validating the signature and the consistency between the signature and the public key information inside the VC. If the VC is ok, future validation will be performed with the VP, including validation of whether its associated DID is consistent with the DID used for the authentication process.

One more step will be performed when a user logs into the Roam network. Their device will submit connection information like QoS status to the on-chain smart contract, and a copy of this info will be sent to the Roam backend as well. At the same time, Roam access points will submit the information on the connected DIDsto Roam's backend and on-chain smart contracts. This DID info will be the source of the network's "3W" data.

3.3.1.3 DID and VC Integration on Mobile Devices

DID, VC and Wallet

As introduced in Chapter 3.2.2, the DID has emerged as a promising solution for providing secure and privacy-preserving digital identity, while VCs are digital credentials that enable individuals to prove their identity, qualifications, or other attributes without revealing unnecessary personal information. Roam is leveraging VCs to enable secure WPA2/3-EAP authentication for its OpenRoaming Network. To enable access to these services, a public key Infrastructure (PKI) is required to distribute and manage VCs. In the initial development phase, Roam will deploy a PKI and combine it with Decentralized Identifiers (DIDs).

Roam's DID will be derived as follows: an Elliptic Curve Digital Signature Algorithm generates a private key, then Keccak-256 is used to hash and produce an Etherem compatible Account Address which joins with the DID scheme and method prefixes. Other organizations could deploy their own PKIs, and the VCs which they generate could be recognized by Roam protocol as long as they support the WBA OpenRoaming framework.

DIDs provide a unique and decentralized way of identifying users, enabling them to control their identity and associated data. When users want to access Roam services for the first time without any VC, they could choose to accept a VC signed by the Roam Foundation. If they accept, a VC with the users DID will be issued to them instead of a standard x509 user certificate. The VC will contain their identity information, which can be verified using a decentralized ledger. The VC can be saved in a specialized credential saving area of the users' Wallet, along with identity documents issued by other organizations. Once their VC has been issued, users can produce a one-time Verifiable Presentation (VP) by adding their holder information to the VC whenever they need to identify themselves. It is also possible for users to choose what information they want to present using their VP, preserving privacy. This VP could be used for the WiFi login process as described in Chapter 3.3.1.1.

VCs for Roam network access could be issued by any organizations which incorporate the W3C's DID and Verifiable Credential protocols. Such organizations could become VC issuers and maintain the status of the VCs which they issue on the blockchain. If a given WiFi node is an RCOI-free node, the VC holders from any of these organizations could log-in at this node. If a specific user-login management scheme is defined in the relevant nodes, only users whose VC includes the credentials satisfying the scheme's requirements can log in at these nodes. This approach enables users to control their identity and associated data, providing increased privacy and security. VCs are designed to be interoperable and can be used across different services and organizations, making them a promising solution for a range of identity use cases.

Mobile Phones

The implementation of Roam using mobile phones will happen in different phases, as it takes time for mobile phone manufacturers to catch up. In the meantime, the Roam app or any app which integrates Roam SDKs is required to interact with the OpenRoaming access points.

The Roam mobile app provides users with a Crypto Wallet, DID, Roam Foundation-signed VC, and other OpenRoaming credentials. Users connecting to Roam network for the first time via the app can either use their emails or social media accounts; or they can choose to create a new Wallet or import their existing one using their private Key. The App generates a DID by using the user's public key as input, which key remains secure and undisclosed due to the use of a hashing algorithm. The DID is then added to the Decentralized Ledger and used to request a VC from the Roam Foundation. Using the VC, the App automatically provisions an OpenRoaming Profile for users with a compatible device. The VC is securely stored in the Wallet and can be used to verify users' identities when interacting with the Roam access points.

When a mobile device interacts with the access points, the mobile app will handle the further interactions with Roam’s distributed RADIUS as defined in Section 3.3.1.2. Such interactions will be recorded and submitted to the Roam backend and on-chain smart contract by both the mobile app and the access point. This will result in the generation of DID-based Who, When and Where (“3W”) data.

Windows / Linux

It is fairly straightforward to integrate DID / VC with Windows platforms via Windows Native APIs, which support the proposed implementations of both EAP-TTLS and EAP-TEAP.

With Linux, the integration development uses an open-source WPA_Supplicant module. As for EAP-TEAP, it is developed based on the existing EAP-Flexible Authentication via Secure Tunneling (FAST) module, for which a client side authentication process will be released. VP authentication will be added to the Basic-Password-Auth process per EAP-TEAP as well. As for EAP-TTLS, it will update the existing FAST module.

The Roam access point also offers an effortless way for users to access the Roam OpenRoaming Network from their desktops or laptops. By default, the access point broadcasts an Onboarding WiFi signal in addition to the OpenRoaming WiFi signal. Users can easily connect to the Onboarding WiFi and access a Portal where a dynamically generated QR code can be scanned using the Roam Phone App. Once it scans this code, the computer will download and provision an OpenRoaming Profile that is compatible with the user's desktop or laptop system if the App holds a valid VC. This enables users to enjoy seamless access to the OpenRoaming Network without any manual configuration.

3.3.2 WiFi Hardware

3.3.2.1 Enterprise WiFi Devices

The typical setup of an enterprise WiFi network includes a wireless access controller (AC) which manages multiple wireless access points. An access point is the device that allows multiple wireless devices to connect with each other via a single or multiple wireless networks. An access point can also be used to extend a wired network to wireless devices. In enterprise WiFi, the network intelligence stays with the AC, which could be a dedicated server or a server in the cloud. All APs are configured by the AC. In comparison to regular WiFi, this approach provides services that can lower the price of deployment, ease the management process, and provide several layers of security.

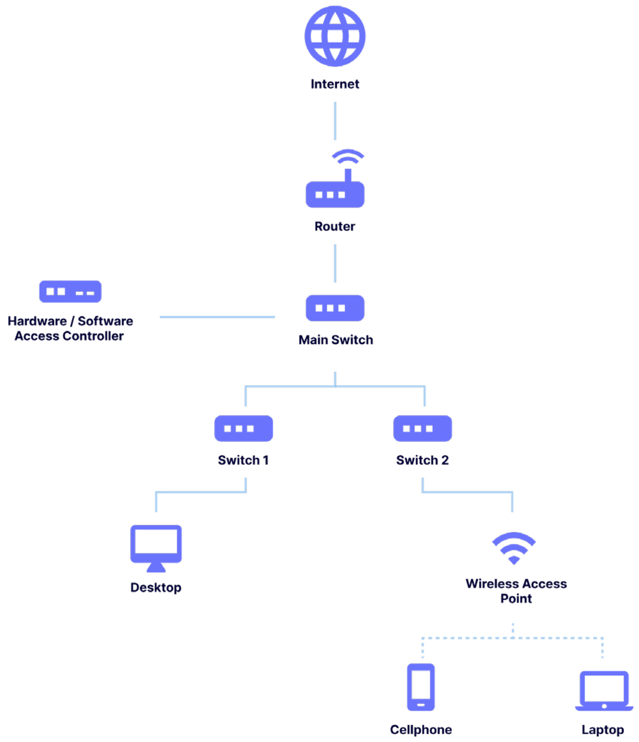


Fig 38, enterprise WiFi setup

The Roam network Gateway contains a software-based access controller (AC) that can push configurations using the Control and Provisioning of Wireless Access Points (CAPWAP) protocol.

As a result, any standard market-available access points (AP) that support OpenRoaming and CAPWAP protocol can be adopted and managed by the Roam AC, enabling users to easily extend their network.

Additionally, users have the option to add Roam APs to the network, providing a more consistent experience. Compatible APs can be connected to the Roam Gateway via its LAN port or through a switch, allowing them to join the Gateway's network and broadcast the OpenRoaming and/or Free WiFi signal.

Oftentimes, these APs are powered by Power-Over-Ethernet cables, and a POE switch will be included in the hardware list. A wired gateway or modem / router is commonly used to connect the WiFi network to the internet.

3.3.2.2 Roam Mining Device

The Roam mining device is the device which hosts the RADIUS client. It could be a wired gateway or modem / router, and can be configured with a DID and VC issued from the Roam Foundation. The controlling private key will be stored in the device locally inside the trustzone or a TPM chip. This key is not accessible by anyone else, including the Roam Foundation, ensuring that the device owners have total control over their miners.

Since the Roam mining device is an essential part of the Roam ecosystem, a series of checks will be performed before issuing a VC to the device, protecting the network's integrity. The Roam mining device could then present the issued VC to prove its own authenticity when users try to validate the Roam OpenRoaming Network.

Roam mining devices could also function as edge computing units capable of providing wireless access, storage, and computing functions. For mining device provisioning, Roam foundation will certify qualified third party units and grant the relevant manufacturing licenses to their certified vendors.

3.3.2.3 On-Chain Registry

On-chain registries will be used to record both DID and VC status information.

<u>DID registry</u>

As for the DID registry, the metadata including the DID itself, DID public key information, and DID attributes will be registered. The DID document will not be registered, and the holder will generate it when needed. The DID format will be:

did:Roam:public key of the controller#self-defined name no more than 256 bytes

The attributes of the DID will be saved in the event structure:

```
event DIDAttributeChanged(
   string indexed did,
   bytes32 name,
   bytes value
 );
```

VC registry

In terms of the VC registry, the issuer is defined as:

mapping(string => string) public vcIssuers;

'Key' is the name of the VC in a url format, which could be associated with certificate numbers like: "https://Roam.io/test_certificates/100". The value attribute will be the issuer's DID information.

VC information includes expiry time, credential image, revoke mechanism, claims, etc. Similar to the DID, Roam uses the following event structure to store its VC operations:

```
 event VCSchemaChanged(
    string indexed vcName,      bytes32  name,
    bytes    value
  );
```

The storage format of Claims is:

name "claims"

value json dataset for holders attributes, i.e.["id", "name", "graduate_time"]

The Implementation of Nonce

Everytime a smart contract is called, the requester / DID holder shall sign the request with their DID's private key. The smart contract then requests the usage of nonce to prevent a relay attack. The requestor / DID holder will check the nonce value of the smart contract prior to the call request. Then, he / she will sign it with the predefined method per smart contract. When the signature has been successfully validated once, the nonce value will increase automatically.

3.3.2.4 Overall Discovery, Authentication and Authorization process

The above two sections explained the overall log-in process for a Roam user roaming into a Roam-built network. But what happens if a Roam user roams into another WBA roaming partner's network (which is built in the traditional way), or vice versa: if a user with a centralized ID but an OpenRoaming profile roams into the Roam network?

In cases where the Roam OpenRoaming service is not available, users can still connect to another WBA member's OpenRoaming Network (access network) to enjoy WiFi network services. The overall login process is like accessing a Roam-built network. Once an identity request is made by the access point, the user device will respond with a bogus ID like xxx@Roam.network. The access network will be able to recognize this Roam realm and confirm that a RADIUS server is available by checking the Name Authority Pointer (NAPTR) records. If it has been configured per WBA framework, the IP address of the RADIUS server could be obtained via DNS Service Record (SRV), and the RADIUS request could be forwarded via a proxy RADIUS. The proxy server could then redirect the incoming request, preferably including the accounting information and the user device's VC/VP, to a Roam RADIUS server. Using the accounting information, the Roam RADIUS server will allow users to access WiFi networks which are not RCOI-Free. Roam RADIUS will then look up the VC/VP record in the decentralized ledger and validate this information before sending a response to the access network RADIUS server based on the result (of the validation). Authorized users can then roam in the available WiFi network. The communication between the access network RADIUS and Roam RADIUS will use EAP-TLS, with the tunnel being encrypted by a WBA-issued certificate. Both the access network RADIUS and the Roam RADIUS shall have these certificates as required by EAP-TLS. This seamless process ensures that users can enjoy a secure and hassle-free browsing experience, regardless of the network they are connected to.

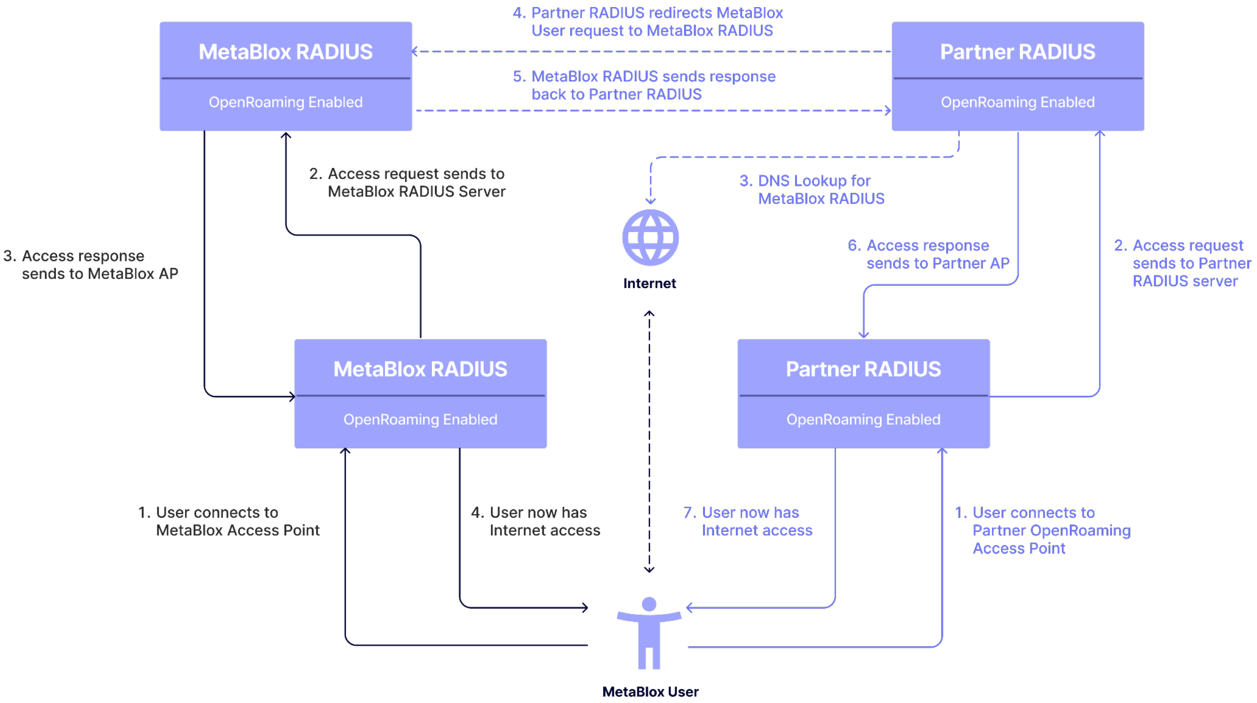

4. Partner RADIUS redirects MetaBlox User request to MetaBlox RADIUS
5. MetaBlox RADIUS sends response back to Partner RADIUS
MetaBlox RADIUS
OpenRoaming Enabled
Partner RADIUS
OpenRoaming Enabled
2. Access request sends to MetaBlox RADIUS Server
3. DNS Lookup for MetaBlox RADIUS
3. Access response sends to MetaBlox AP
Internet
6. Access response sends to Partner AP
2. Access request sends to Partner RADIUS server
MetaBlox RADIUS
OpenRoaming Enabled
Partner RADIUS
OpenRoaming Enabled
1. User connects to MetaBlox Access Point
4. User now has Internet access
7. User now has Internet access
1. User connects to Partner OpenRoaming Access Point
MetaBlox User

Fig 39, the RADIUS-based authentication process

When a user from another network roams into the Roam network, a similar process will happen. The only difference is that the Roam RADIUS will serve as the access network RADIUS, and will handle the legacy username/password-based login process. Roam ensures that the accounting information will be forwarded to the roaming partners' RADIUS as well.

Roam compatible WiFi APs and gateways typically offer WiFi services under their own SSIDs. The above process won't be affected.

3.3.3 Network Privacy Protection and Regulatory Requirements

The core value of the Roam network is the global OpenRoaming capability and the 3W data generated by these networks. As it creates a global public network, OpenRoaming has to balance the privacy and regulatory requirements in different countries.

The DID is an essentially anonymous identifier as it is an ID that's self-declared by its user/holder. Roam "3W" data represents users via their DIDs, so it won't infringe on people's privacy. However, 3W does provide great value to businesses which want to utilize such information, as most of them do not care about the real identity of their WiFi users.

During the WiFi login process, verifiable credentials are the key elements which are typically issued by verifiable credential issuers. Based on the regulatory requirements of the given jurisdiction, a Know Your Customer (KYC) process could be performed before on-boarding businesses as VC issuers for Roam protocol. In the jurisdictions where a real (non-anonymous) identity is required for internet browsing, the VC issuer will be required to maintain the relationship between the user's real-world identity and the verifiable credentials issued to them. It is still the users themselves who link their DIDs with their own VCs. In the Roam network, these authentication services allow users to roam based on the VP generated by the VC, while the users are identified by the associated DIDs to maintain anonymity. When a regulatory body needs to investigate the network's activities, it will be able to reach the relevant VC issuer(s) and obtain the necessary information. The Roam network won't maintain such records.

3.3.4 Roam Applications

A series of applications are needed to facilitate the adoption of Roam. These include:

A network host backend which supports WiFi management and data analytics at Roam network locations.

An application marketplace. Common apps in the marketplace include crypto payment gateways, check-in-to earn apps, etc.

A point-redemption rewards system which allows Roam points to interface with other token reward systems.

A staking system which allows users who hold Roam tokens to generate more yield.

An NFT-based cloud mining system which allows users who do not own a hosting site to deploy a miner in such a site via the Roam foundation, and receive all of that miner's rewards.

4 Roam Tokenomics

4.1 Tokenomics Enabled Flywheel

As discussed in Chapter 2, the key to the success of a DePIN project is to kick-off the network building flywheel properly. What does this for Roam is the community. Riding the wave of WiFi 6 / 6E upgrades and supporting 5G deployment are two motivations for building the network. However, the mining incentives are also very important, particularly in the bootstrap phase. Thanks to this decentralized model for OpenRoaming deployment, network coverage can be improved and devices can be upgraded at a low cost. This DePIN model also turns customers into Web3 users when they visit OpenRoaming sites hosted by businesses.

It is clear that properly designed tokenomics is necessary to the network's bootstrap and growth phases. Strong tokenomics is also valuable for promoting the development of applications based on the decentralized OpenRoaming networks.

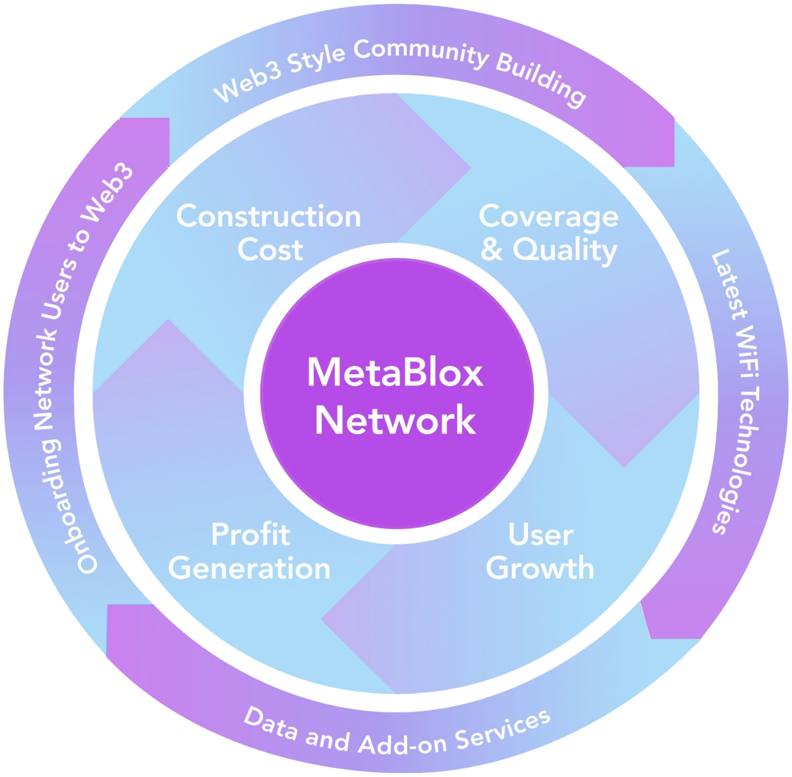


Fig 40, the Roam DePIN flywheel

4.2 Category and Quantity

Introduction of Roam token ($ROAM) and Roam Points (Roam Points)

$ROAM is a typical utility token designed to accrue network value. Its circulation represents the beneficiary change of the network. The $ROAM token has a hard cap at 1 billion units. Among these 1 billion tokens:

400 million units will be generated at the Token Generation Event. The remaining 600 million will be identified as growth tokens, and will be produced by the mining or staking processes. Among the 400 million tokens generated at the TGE, 280 million will be reserved for sales, and 120 million will be reserved for the team. The release of these tokens will be managed by different vesting programs under the supervision of the community.

The Roam Points are interim tokens without a hard cap. They serve three purposes:

- To decouple daily operations from value accruement. In the real world, using either currency or points for user rewards is totally irrelevant to the company shares; and in other early-stage DePIN projects, using the same token as both a reward and for value accruement is fairly common. This move by DePINs, however, will create a situation in which the token is owned by a product / service user instead of the investor who believes the value of the project. This will cause unnecessary volatility in token value and could be toxic to the ecosystem in some unfavorable market conditions.
- To provide an interim step to generating $ROAM. Different kinds of network participants will receive Roam Points as the rewards for their contributions. They can stake these points for $ROAM.
- To provide a mechanism for receiving cash inflow into the ecosystem without selling $ROAM.

Like many rewards programs do to facilitate the transfer of value inside the ecosystem without the impact of volatility, Roam Points are designed to be pinned to a regular currency, for example, the US dollar.

4.3 Proof-of-Service and Proof-of-Validation Mining

4.3.1 Roles

Mining rigs, Roam access points, and Roam gateways implementing Roam protocol need to prove to the network that they are continuously providing high quality Wi-Fi services. In return, they will receive mining rewards. Due to the close coverage density of Wi-Fi networks, it is impossible for mining rigs to communicate to check each other's statuses, so independent validators have to be introduced for this purpose. Roam encourages the sharing of Wi-Fi in public areas such as cafes, shopping plazas, public transportation stations, commercial buildings, etc. As a result, the mining rewards shall be designed to reward service providers in these areas. Based on this, we propose a Proof-of-Service mining algorithm which proves that honest miners continue to provide network services as required, while allowing the network to quickly discover malicious miners. At the same time, validators are required to validate the status of the WiFi services, for which they will be rewarded with tokens as well.

There are multiple roles in the WiFi mining process, namely:

（1） Wi-Fi Miner

WiFi miners are responsible for providing good quality network services in public areas, reporting the validator's validation activities and the user's check-in activities. Minersobtain corresponding rewards after the validator submits the network service proof to the network and receives the confirmation from the smart contract that the information submitted by the miner and the validator is consistent.

（2） Validator

Validators are responsible for verifying that the miners are providing good quality WiFi services. When the (good) quality of a miner's service is confirmed, the validator sends the confirmation credential information to the miner. The validator then gets paid for proving that the miner is providing adequate services. To carry out these duties, the validator has to obtain a Validator VC from the Roam foundation, and must stake a certain amount of $ROAM as a security deposit.

（3） Other roles

Additional roles will be gradually introduced to the network, including:

Discoverers who find other OpenRoaming locations not deployed by Roam, and successfully mark them on Roam's WiFi map.

RADIUS providers: the community members who run AAA servers for the network. Each provider first needs to stake a certain amount of $ROAM, and subsequently their rewards will be issued via the staking process.

Witnesses who voluntarily find cheating activities between Miners and Validators, if there is any. The proposed rewards system will be resilient against potential cheating events, and this role might not be necessary. However, it could be incorporated as needed.

4.3.2 Mining Process

4.3.2.1 Main Mining Process

The main mining process is as follows:

（1） Wi-Fi mining device initialization

When a Wi-Fi device is initialized, the miner needs to configure the device's location, MAC address, public key address, and certificate information.

（2） Validator validation of Roam mining devices

Roam encourages Wi-Fi miners to continuously provide network services to the public in open areas. After the Wi-Fi devices are online, nearby Validators can obtain Roam Points by verifying that the mining devices are online and reporting the network matrix. The miner will also receive rewards when its status is reported by the Validator. At a fine level of detail, this process includes two steps:

The first step is the regular DID/VC login check as specified in Section 3.3.1.2.

In the second step, the mining device will in real-time post the Validator's VP to the on-chain smart contract, while the Validator will collect the mining device's VP. When the validator submits the mining device's proof (VP) to the blockchain, the mining rewards smart contract will compare the submission time stamps to those of both proofs. And for both proofs, the time gap between proof creation and submission has to be within limit *T*. Otherwise, the mining will be considered invalid. If any VP submitted by the validator is invalid, none of the other proofs in the same submission will receive the mining rewards. Note that the validator has to accumulate a minimum of *n* proofs before being eligible to submit.

During the above mining process, additional information will be collected and submitted to the Roam backend as well as the blockchain smart contract. The Validator will collect certain information about the behaviors of the mining device in the past 24 hours, e.g. the mining rewards, the total network traffic carried, extensive QoS data, the number of users served, the number of validators interacted with, the status of Roam Points staking by the device, the location of connected RADIUS servers, etc. The mining device will collect additional information on the Validators as well, including the status of Roam Points staking by the Validator, mining devices it has interacted with, the total network traffic volume created by these interactions over the last 24 hours, received Roam Points, etc.

Please note that the mining device constantly sends a "heartbeat" packet which includes its operation status to both the Roam backend and the blockchain. The reported heartbeat information will also be checked against the information reported by Validators.

（3） Rewards distribution

Roam Points will be distributed to the miner and validator once the validation is confirmed by the blockchain. The amount of rewards will be adjusted to encourage the mining device to serve as many people as possible.

For each mining device/validator pair, only one reward opportunity will be presented within each given predefined time frame, and the reward amount will be reduced if the same pair has occurred repetitively. Other measures designed to optimize the network's services will be introduced to the rewards distribution scheme as well.

4.3.2.2 Other Mining Processes

As mentioned in Section 4.3.1, additional mining processes are available to facilitate the growth of the network. These methods will be introduced or removed via votes by the community.

-

RCOI-Free discovery process: whenever a Discoverer identifies an RCOI-Free OpenRoaming node not deployed by Roam, it can mark it in the app so Roam users can access it with their Roam OpenRoaming profiles. Subsequent to adding an OpenRoaming location to the

app, a mining reward could be distributed to the Discoverer. The amount would be proportional to the total rewards allocated to this process during the particular time slot.

4.3.3 Device Certification and Licensing

Device Certification

In order to prevent manufacturers and equipment from cheating, mining device manufacturers need to go through an audit and certification process before they can formally produce the Roam mining device. This process examines the quality of service which the device would likely provide, how it utilizes the trust platform modules, its regulatory compliance including both EMI and safety, and its compliance to Roam protocol. Roam Foundation will form a technical committee to handle this certification process.

Each Roam mining device shall require a pre-deposit of Roam Points as an activation fee. These Roam Points will be removed from the user's wallet once it is activated. If the mining device changes owner, the new owner shall activate the device using their own wallet.

Each Roam mining device producer shall stake a certain amount of $ROAM tokens as collateral to ensure that it will support the community's growth and not abuse its manufacturing rights. The exact amount will be determined by the community management committee.

4.4 Staking Process

The staking process is an essential part of community building to motivate and incentivize users to participate. In the Roam ecosystem, $ROAM tokens could be generated by staking either Roam Points or $ROAM in different pools to contribute to network operations. More importantly, some $ROAM tokens will be rewarded to the community service providers via staking.

For example, the RADIUS service operators will receive the staking rewards if they meet the following conditions:

i) They demonstrate to the foundation that they are capable of providing an AAA service to the network

ii) They have staked the required $ROAM (fixed amount)

iii) They passed the quarterly performance review based on the operational results

If more than the required number of RADIUS service operators have applied for the role, a community vote will be conducted.

4.5 Tokenomics Models

4.5.1 Definitions of Key Parameters and Formulas

$ROAM's basic token generation formula is defined as follows:

$n(t) = a(t)e^{-\lambda t} \quad \beta(t) = v(t) + m(t) + w(t)$, the number of tokens generated at any given moment, where a(t) represents the time 0 rate, λ is the decay constant, $\beta(t) = \frac{D(t)}{\widehat{D}(t)}$, the adjustment factor where $D(t)$ is mining difficulty and $\widehat{D}(t)$ is the high water mark mining difficulty. $v(t)$ is the number of tokens awarded to the validators, $m(t)$ is the number of tokens awarded to the miners and $w(t)$ is the number of tokens awarded to other roles and generated by staking processes.

The total amount of tokens in circulation is defined as

$L(t) = L(t-1) + n(t) + s(t) + r(t)$, where $L(t)$ is the total number of tokens in circulation, $s(t)$ is the net number of staked tokens, and $r(t)$ is the number of recycled tokens.

$N(t)$is the total number of miners in service, counted via the heartbeat of the mining devices.

$p(t)$ is the price of the token, $p(t) = \frac{V(t)}{\sum \quad n(t) + n_0} = \frac{A\,[\gamma(t)X(t)]^2 \quad +[R(t)-O(t)]N(t)}{\sum \quad n(t) + n_0}$, where V(t) is the value of the network as defined in Chapter 2.

$X(t) = \sum \quad [q(t)d(t)v(t)]$, the weighted number of VPs collected in 1000 seconds at time slot t, where $q(t)$ is the quality factor, $d(t)$ is the density factor, and $v(t)$ is the number of VPs collected at time slot t.

$\underline{X}(t)$, the average $X(t)$ in 1000^2 seconds, or 1 million seconds in total length.

$C(t) = \frac{n(t)\,p(t)}{N(t)}$, the average mining rewards received per miner.

$\gamma(t)$, the ratio between the number of users and the number of validators.

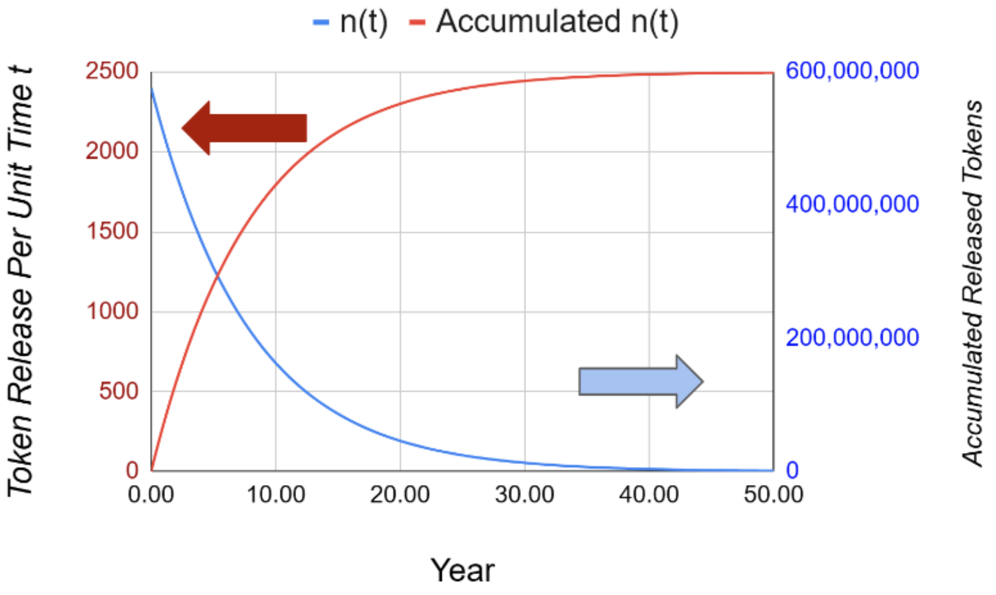


Fig 41, the Roam growth token release schedule

4.5.2 Difficulty Adjustment

The token incentive is the key economical factor motivating a DePIN system. With the growth or shrinkage of the network, the incentive amount and targets shall be adjusted accordingly to ensure the efficiency of the incentivization. Bitcoin has demonstrated this theory in the past decades, as its token generation difficulty level has been dynamic to the network's computing power to ensure roughly the same block production time. Inspired by this mechanism, Roam also implements a difficulty adjustment feature. Its goals are as follows:

i) When the network scale shrinks, the token release schedule has to be adjusted to reduce the selling pressure in the market and protect the token price if possible. However, such reduction in the token releasing amount shall not hurt the income of valuable miners, particularly when the price is also dropping;

ii) When the token price goes down over time, find a mechanism to allow average mining income for miners to bounce back to support the continuous prosperity of the community;

iii) Strengthen the incentive for miners who offer network services to high traffic areas, and gradually eliminate the weak miners who provide a network without much usage. However, when the traffic bounces back, their rewards bounce back as well.

The implementation of the difficulty adjustment is as follows:

After every 1 million seconds, $\underline{D}(t)$ will be compared with the previous historical high of $\widehat{D}(t)$. If $\underline{D}(t)$is equal to or larger than $\widehat{D}(t)$, $\beta(t)$ will be 1, otherwise, $n'(t) = a(t)\, e^{-\lambda t} \ [1-\beta(t)]$ will be added to $a(t)$ in the next 1 million seconds. Basically, it will increase $C(t)$ for the miners who still deliver effective network services.

When the token price is increasing, $N(t)$ goes up typically and $n(t)$ goes down, and as a result $C(t)$ will drop and eventually, some miners will be taken out of the market as their rewards will be barely minimum if they do not contribute valuable network coverage and handle large traffic. Then, $N(t)$ is expected to drop or increase slowly, and $C(t)$ will become attractive again.

When the token price is decreasing, $N(t)$ is expected to drop or increase slowly, and through difficulty adjustment, $n(t)$ will eventually increase and $C(t)$ will become attractive again.

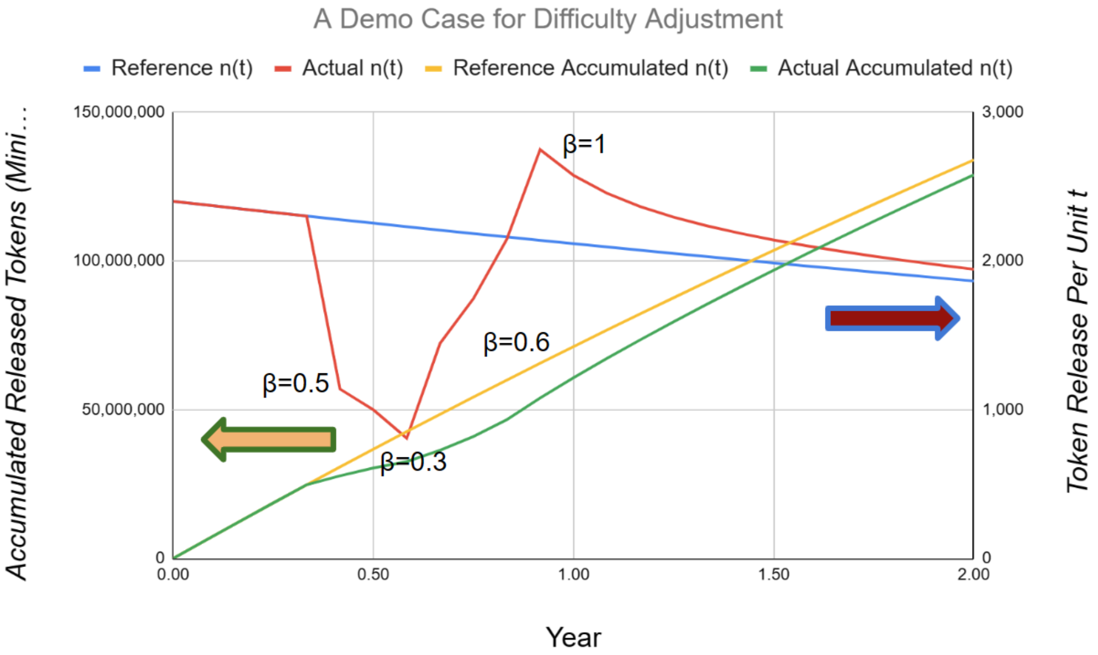


Fig 42, The impact of a difficulty adjustment event.

In the above simulation event, when $\beta(t)$ drops to 0.3 (lowest point), assuming the network scales down and $N(t)$ drops proportionally, *n(t）* will drop to ~ 36% of the reference case (no difficulty adjustment) and *n(t)/N(t)* will be ~20% higher than the reference case (no difficulty adjustment). This proves that the miners providing more valuable network coverage will receive more financial incentives to offset the drop in token price when the network shrinks. At the same time, the overall amount of tokens released is reduced in this scenario to alleviate the selling pressure in the market. In terms of accumulated released tokens, the actual releasing curve is lower than the reference curve, which means that the token release will be delayed, though the gap between these two curves will be reduced over time due to a higher token release rate once the network scaling speed resumes.

Besides the scale of the network, the scale of Roam Points staking pool shall also be considered as a parameter to track. If the size of the staking pool shrinks, less ecosystem value will be accrued to $ROAM tokens, in this case, the difficulty adjustment shall include this factor to reduce the corresponding $ROAM release. However, it shall reward the participants who continue to accrue the network value to $ROAM and their average income shall be increased. The same process as defined for the impact of network size will be introduced.

4.5.3 Introduction of Non-Fungible Tokens (NFTs)

Section 4.5.1 explained that the mining rewards from Roam network will be prioritized for the mining devices deployed where there's a lot of foot traffic. What if a miner host does not own this kind of site but still wants to deploy their device in a premium, high-traffic location? In this situation, he or she could purchase a Roam NFT, which is bonded to a particular mining device and receives all of the mining rewards generated by this device. This situation happens when a business deploys Roam WiFi products solely for better WiFi services or for OpenRoaming/the associated applications. Sales and deployment agents will conduct the work of setting up a Roam miner/WiFi network at businesses. NFT holders will essentially support such deployment and in return, receive the mining rewards made by the business-site miners. The Roam Foundation will manage the bonding relationship and present it on the blockchain.

The other purpose of Roam NFTs is to represent holders' "OG" community status. NFT holders will receive airdrops, enjoy the free passes to community events, and own the right to vote in the community. They can also stake their NFTs to receive $ROAM as a reward for their early support for MetBlox.

4.6 The Generation, Circulation and Usage of $ROAM Tokens

4.6.1 Roam Points

<u>Generation</u>

Section 4.3 explained the mining mechanism and how miners, validators and other role players receive Roam Points as rewards for their contributions to the network. The other way to generate Roam Points is to purchase them directly from the Roam foundation or to redeem loyalty points from businesses whose reward programs align with the Roam foundation. Please note that the generation of Roam Points could be boosted during different marketing campaigns.

Roam Points could also be generated by selling $ROAM tokens. Such sales activities will only be allowed to take place within applications registered with the Roam foundation.

<u>Circulation</u>

The circulation of Roam Points, which function as a quasi-stable token, takes place largely within the ecosystem. Its circulation mainly relates to business activities. For instance, built inside each

Roam Gateway will be an application market where the user can spend Roam Points to purchase third party applications; and where businesses can spend Roam Points to access the "3W" data generated by the network, or to post advertisements within the Roam network's landing page environments. Essentially, Roam Points functions as the "dollar" within the Roam ecosystem. Note that a 5% value-added "tax" will be charged on the above transactions and payable to the Roam foundation treasury.

The other key function of the Roam Point is to generate $ROAM via the staking process. Such a process ensures that network contributors can receive their rewards in a transparent manner while the network scales.

Consumption of Roam Points

Roam Points will be consumed during the following scenarios:

a) After they have been staked in a pool to generate $ROAM
b) When Roam Points are redeemed for other digital assets not issued within the Roam ecosystem. This type of redemption can only happen in applications approved by the Roam foundation
c) When Roam Points are used to purchase $ROAM by the Roam Foundation Treasury. This will be performed mandatorily once in a quarter based on the balance of the Treasury department, and the funds shall come from the value added "tax"generated by the ecosystem. Only the Roam Foundation Treasury has the rights to purchase $ROAM directly with Roam Points.
d) When activating a mining device or changing its location.

4.6.2 $ROAM

The native cryptographically-secure fungible protocol token of the Roam network (ticker symbol **$ROAM**) is a transferable representation of attributed utility functions specified in the protocol/code of the Roam network, and which is designed to be used solely as an interoperable utility token thereon.

$ROAM is a functional multi-utility token which will be used as the native utility token and economic incentives which will be distributed to encourage users to exert efforts towards contribution and participation in the ecosystem on the Roam network, thereby creating a mutually beneficial system where every participant is fairly compensated for its efforts. $ROAM is an integral and indispensable part of the Roam network, because without $ROAM, there would be no incentive for users to expend resources to participate in activities or provide services for the benefit of the ecosystem. Given that additional $ROAM will be awarded to a user based only on its actual usage, activity and efforts made on the Roam network and/or proportionate to the frequency and volume of transactions, users of the Roam network and/or holders of $ROAM which did not actively participate will not receive any $ROAM incentives.

$ROAM does not in any way represent any shareholding, ownership, participation, right, title, or interest in the Company, the Distributor, their respective affiliates, or any other company, enterprise or undertaking, nor will $ROAM entitle token holders to any promise of fees, dividends, revenue, profits or investment returns, and are not intended to constitute securities in Panama, Singapore or any relevant jurisdiction. $ROAM may only be utilised on the Roam network, and ownership of the same carries no rights, express or implied, other than the right to use $ROAM as a means to enable usage of and interaction within the Roam network. The secondary market pricing of $ROAM is not dependent on the effort of the Roam team, and there is no token functionality or scheme designed to control or manipulate such secondary pricing.

For the avoidance of doubt, neither the Company nor the Distributor deals in, or is in the business of buying or selling any virtual asset or digital payment token (including $ROAM). Any sale or distribution of tokens would be performed during a restricted initial period solely for the purpose of obtaining project development funds, raising market/brand awareness, as well as community building and social engagement; this is not conducted with any element of repetitiveness or regularity which would constitute a business.

<u>Generation</u>

The generation rate of $ROAM tokens is straightforwardly determined by the formulas defined in Section 4.5. Multiple staking pools will be developed to generate $ROAM. Roam Point holders, $ROAM holders, and Roam NFT holders will all have the opportunity to receive $ROAM via these pools. The yields of the staking pools follow the formula $n(t) = a(t)e^{-\lambda t} \quad \beta(t),$ with the adjustment for difficulty.

<u>Circulation</u>

The primary usage of $ROAM tokens is for staking:

a) Validators and witnesses must stake $ROAM tokens as an indicator of commitment for the right to validate the services provided by the miners, and also to ensure service standards. As rewards for their work, participants would be able to earn $ROAM token rewards.
b) Additional roles will be gradually introduced to the network, and all active contributors to the safety and security of network operations will be able to earn $ROAM token rewards. The staking process is an essential part of community building to motivate and incentivize users to participate.
c) Users can stake $ROAM tokens while voting in a community election, and the number of voting tickets granted to them will be proportional to the amount of $ROAM they stake
d) Given the fact that multiple blockchain projects work with Roam network to bring value to their customers or ecosystem partners, users can stake $ROAM tokens to gain priority

access to campaigns/airdrops from these other projects (by actively engaging, users will be able to earn various token rewards).

e) RADIUS operators and mining device manufacturers must stake a predefined amount of $ROAM for the rights of operation. This would ensure service standards.

f) $ROAM functions as an access token, so community members can stake $ROAM for other community privileges.

$ROAM represents the utility value available on the Roam network.

4.6.3 NFTs

Roam NFTs are the essential part of the community and tokenomics model as defined in Section 4.5.3.

Generation

All NFTs will be issued by the Roam foundation directly, and, when they become available, bonded to particular mining devices by the Roam foundation.

Circulation

$ROAM NFTs could be transferred within any NFT marketplace or via peer-to-peer transfers. If the holder stakes the NFT, he or she can receive $ROAM rewards.

Lifetime

Similar to other electronic devices, Roam mining devices have a limited lifetime too. Roam ensures that the mining device bonded to the NFT can work for at least two years. The actual lifetime for each unit will be unit specific.

Once a mining device reaches the end of life, the NFT holders can still enjoy their "OG" community status and potential airdrops. The NFT can also be continuously staked for $ROAM.

5 Roadmap

Future work with Roam will focus on three aspects: continuous improvement of the DID/VC based WiFi OpenRoaming network, the addition of secondary decentralized infrastructure built on top of the decentralized wireless access network, and the further development of Roam protocol.

5.1 Decentralized OpenRoaming

The industry still has a long way to go before fully adopting OpenRoaming. To accelerate this process, Roam will work with the WBA, WiFi Alliance, and industrial partners on the following action items:

i) Greater EAP-TEAP adoption by WiFi devices, access points, and access controllers. This will help Roam provide better user experiences to its customers;

ii) A standardized SDK for ID providers to incorporate in their backend. The SDK shall follow the W3C's DID and Verifiable Credential guidances, and, for industrial adoption, it will be developed under the WBA's Decentralized OpenRoaming Group;

iii) Research work with the IEEE 802.11 working group on IEEE802.11bi activities for privacy protection and regulatory compliance with blockchain technologies;

iv) A proposal for EAP-DID created alongside the Internet Engineering Task Force (IETF). This will open the door for the large-scale adoption of DID/VC based authentication in multiple industries.

5.2 Decentralized Edge Computing Networks

Riding the wave of WiFi 6 and WiFi 6E upgrades, Roam provides a global-scale decentralized wireless access network. The ultimate goal of the DePIN model is to provide a complete set of computing, storage, network, energy, and sensing infrastructure in a decentralized way. On top of the network services, Roam has the potential to provide a decentralized edge computing network.

Moreover, the WiFi Gateway always constitutes the core IT equipment of any local network. It can be attached to storage devices, computing units, and IoT gateways to facilitate the built out of edge computing units as shown in Figure. Such units are consistent with the 5G deployment scheme and can support AI applications running within the decentralized infrastructure. The core technologies needed to achieve this include DID implementation, blockchain integration with communication models, confidential computing, and data encryption. Roam intends to incubate other DePIN projects which can be built upon its global OpenRoaming networks.

5.3 Future Development of Roam Protocol

Roam protocol is essentially a verifiable credential-based data exchange protocol as defined by the Trust-Over-IP stack. It can support other applications in addition to global WiFi OpenRoaming. For example, it can support an on-chain KYC system to allow the users of regular ID providers to participate in DeFi activities, as they can use the VP generated from their VC (provided by the ID providers) to prove who they are.

Roam protocol could also be used in crypto payment gateways to allow for a liquidity pool based decentralized payment protocol to replace the traditional enterprise crypto wallet used by existing centralized crypto payment gateways. The other application of Roam protocol is to support the DID-based credit rating system, as the Roam network provides a large amount of user activity information.

A series of tools and gadgets are required to facilitate new applications beyond global WiFi roaming as explained above. Roam plans to build these alongside its community members as well as with fellow projects in this domain.

6 Conclusion

This paper comprehensively delineates the Roam network's technological foundation and its seamless integration with OpenRoaming WiFi. Furthermore, it expounds upon the tokenomics underpinning Roam and outlines the trajectory of its future development.

The aspiration of a global OpenRoaming WiFi network has long captivated the WiFi industry and garnered substantial dedication from the technology community over the past decades. This commitment has yielded pivotal technologies like Passpoint^{TM} and OpenRoaming^{TM}, ensuring WiFi's enduring prominence as the preeminent wireless access technology in the 5G epoch. Roam emerges as a catalyst for the adoption of these innovations across three pivotal domains. Primarily, it streamlines the implementation of Passpoint^{TM} and OpenRoaming^{TM}, democratizing the creation of WiFi networks at par with conventional setups. Secondly, it supersedes the conventional process of procuring a roaming certificate from WiFi roaming ID providers, introducing an intuitive and user-friendly airdrop procedure. This pioneering approach empowers individuals to possess a WiFi roaming pass upon establishing a DID within a mobile app or crypto-wallet. Lastly, it presents an avenue for merchants sans physical premises yet desiring to furnish wireless network access services, ushering in the era of OpenRoaming-as-a-Service. This innovative model augments network awareness and expansion.

Embracing a decentralized architecture propelled by token incentivization, Roam empowers users to traverse distinct WiFi networks using their Web3 credentials. This paradigm safeguards the privacy of "3W" data, which only serves the users themselves. The Roam protocol seamlessly aligns with the Trust-Over-IP technology stack, leveraging a DID-centered utility layer and a verifiable credential-driven data exchange stratum. This architecture invites the community to forge applications rooted in this user-centric wireless access framework.

Tokenomics stands as the bedrock of every DePIN endeavor and fuels the ecosystem flywheel's momentum. Roam introduces a dual token framework alongside adaptive adjustments within the mining process. These innovative facets are poised to fortify the network's resilience against challenging market conditions and to streamline the path to enduring prosperity. While the overarching tokenomics framework presented herein provides a foundational structure, it remains a fertile ground for further refinement and evolution, a journey that this whitepaper initiates.

RISKS

The Roam network is currently in the initial development stages and there are a variety of unforeseeable risks. You acknowledge and agree that there are numerous risks associated with acquiring $ROAM, holding $ROAM, and using $ROAM for participation in the Roam network. In the worst scenario, this could lead to the loss of all or part of $ROAM held. **IF YOU DECIDE TO ACQUIRE $ROAM OR PARTICIPATE IN THE ROAM NETWORK, YOU EXPRESSLY ACKNOWLEDGE, ACCEPT AND ASSUME THE FOLLOWING RISKS:**

■ Uncertain Regulations and Enforcement Actions: The regulatory status of the Roam network, $ROAM and distributed ledger technology is unclear or unsettled in many jurisdictions. The regulation of digital assets has become a primary target of regulation in all major countries in the world. It is impossible to predict how, when or whether regulatory agencies may apply existing regulations or create new regulations with respect to such technology and its applications, including $ROAM and/or the Roam network. Regulatory actions could negatively impact $ROAM and/or the Roam network in various ways. The Company, the Distributor (or their respective affiliates) may cease operations in a jurisdiction in the event that regulatory actions, or changes to law or regulation, make it illegal to operate in such jurisdiction, or commercially undesirable to obtain the necessary regulatory approval(s) to operate in such jurisdiction. After consulting with a wide range of legal advisors to mitigate the legal risks as much as possible, the Company and Distributor have worked with the specialist blockchain department at GS Legal LLC and obtained a legal opinion on the token distribution, and will be conducting business in accordance with the prevailing market practice.

■ Inadequate disclosure of information: As at the date hereof, the Roam network is still under development and its design concepts, consensus mechanisms, algorithms, codes, and other technical details and parameters may be constantly and frequently updated and changed. Although this material contains the most current information relating to the Roam network, it is not absolutely complete and may still be adjusted and updated by the Roam team from time to time. The Roam team has neither the ability nor obligation to keep holders of $ROAM informed of every detail (including development progress and expected milestones) regarding the project to develop the Roam network, hence insufficient information disclosure is inevitable and reasonable.

■ Failure to develop: There is the risk that the development of the Roam network will not be executed or implemented as planned, for a variety of reasons, including without limitation the event of a decline in the prices of any digital asset, virtual currency or $ROAM, unforeseen technical difficulties, and shortage of development funds for activities.

■ Security weaknesses: Hackers or other malicious groups or organisations may attempt to interfere with $ROAM and/or the Roam network in a variety of ways, including, but not limited to, malware attacks, denial of service attacks, consensus-based attacks, Sybil attacks, smurfing and spoofing. Furthermore, there is a risk that a third party or a member of the Company, the Distributor or their respective affiliates may intentionally or unintentionally introduce weaknesses into the core infrastructure of $ROAM and/or the Roam network, which could negatively affect $ROAM and/or the Roam network. Further, the future of cryptography and security innovations are highly unpredictable and advances in cryptography, or technical advances (including without limitation development of quantum computing), could present unknown risks to $ROAM and/or the Roam network by rendering ineffective the cryptographic consensus mechanism that underpins that blockchain protocol.

■ Risk of Dissolution: Start-up companies such as the Company, the Distributor or their affiliates involve a high degree of risk. Financial and operating risks confronting start-up companies are significant, and the aforementioned entities are not immune to these. Start-up companies often experience unexpected problems in the areas of product development, marketing, financing, and general management, among others, which frequently cannot be solved. It is possible that, due to any number of reasons, including, but not limited to, an unfavourable fluctuation in the value of cryptographic and fiat currencies, decrease in the utility of $ROAM due to negative adoption of the Roam network, the failure of commercial relationships, or intellectual property ownership related challenges, the Roam network may no longer be viable to operate and the Company, the Distributor or their affiliates may be dissolved.

■ Other risks: In addition, the potential risks briefly mentioned above are not exhaustive and there are other risks (as more particularly set out in the Terms and Conditions) associated with your participation in the Roam network, as well as acquisition of, holding and use of $ROAM, including those that the Company or the Distributor cannot anticipate. Such risks may further materialise as unanticipated variations or combinations of the aforementioned risks. You should conduct full due diligence on the Company, the Distributor, their respective affiliates, and the Roam team, as well as understand the overall framework, mission and vision for the Roam network prior to participating in the same and/or acquiring $ROAM.

References

[1] Hetting, Claus. 2018. “Wi-Fi percentage of US smartphone traffic at 74%, says Netradar.” Wi-Fi NOW. https://wifinowglobal.com/news-and-blog/wi-fi-percentage-of-us-smartphone-traffic-at-74-says-netradar/.
[2] CISCO. n.d. “Global - 2021 Forecast Highlights - VNI Complete Forecast Highlights.” Cisco. Accessed July 16, 2023. https://www.cisco.com/c/dam/m/en_us/solutions/service-provider/vni-forecast-highlights/pdf/Global_2021_Forecast_Highlights.pdf.
[3] WiFi Alliance. n.d. “COVID-19 and the Economic Value of Wi-Fi.” Wi-Fi Alliance. Accessed July 16, 2023. https://www.wi-fi.org/download.php?file=/sites/default/files/private/COVID-19_Economic_Value_Wi-Fi_202012.pdf.
[4] WBA 5G Working Group. 2022. “Private 5G and Wi-Fi Convergence: Key use cases and Requirements.” (August).
[5] WiFi Alliance. n.d. “Wi-Fi CERTIFIED HaLow.” Wi-Fi Alliance. Accessed July 17, 2023. https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-halow.
[6] CISCO. n.d. “Cisco Annual Internet Report - Cisco Annual Internet Report (2018–2023) White Paper.” Cisco. Accessed July 15, 2023. https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html.
[7] WiFi Alliance. n.d. “Value of Wi-Fi.” Wi-Fi Alliance. Accessed July 16, 2023. https://www.wi-fi.org/discover-wi-fi/value-of-wi-fi.
[8] Grubbs, Patrick. 2021. “What is EAP-TLS?” SecureW2. https://www.securew2.com/blog/what-is-eap-tls.
[9] SecureW2. n.d. “RadSec vs RADIUS: What's the difference?” Cloud RADIUS. Accessed July 17, 2023. https://www.cloudradius.com/radsec-vs-radius/.
[10] Wireless Broadband Alliance. 2022. “WBA OpenRoaming: The Framework to Support WBA's Wi-Fi Federation.” June, 2022.
[11] Wireless Broadband Alliance Roaming Work Group. 2022. “WBA WRIX Umbrella: Introduction and Overview to the Wireless Roaming Intermediary eXchange (WRIX) Framework.” Sept, 2022.
[12] Wireless Broadband Alliance. 2022. “One Global Wi-Fi Network.” January, 2022.
[13] Hetting, Claus. 2023. “Guest blog: WBA's OpenRoaming federation rolls out to 3 million access points globally with secure and automatic Wi-Fi.” Wi-Fi NOW. https://wifinowglobal.com/news-and-blog/guest-blog-wbas-openroaming-federation-rolls-out-to-3-million-access-points-globally-with-secure-and-automatic-wi-fi/.
[14] Wireless Broadband Alliance. 2023. “WBA OpenRoaming Overview 2023Q1.” Jan, 2023.
[15] Kassab, Sami. 2023. “The DePIN Sector Map.” Messari. https://messari.io/report/the-depin-sector-map.

[16] Hines, Paul D., Seth Blumsack, and Markus Schlapfer. 2017. "When are decentralized infrastructure networks preferable to centralized ones?" *Proceedings of the 50th Hawaii International Conference on System Sciences* 392:3241.
[17] Valerie. 2022. "How Important is Latency to 5G Users? - Welcome To The 5Gstore Blog Welcome To The 5Gstore Blog - Latest News, Product Info & More." 5Gstore.com. https://5gstore.com/blog/2022/08/18/how-important-is-latency-to-5g-users/.
[18] Grayson, Mark. 2023. "Wireless First: Delivering deterministic experiences." January, 2023.
[19] Fenwick, Sam. 2021. "Singaporean mobile users see nearly 50% faster speeds on 5G than on Wifi." Opensignal. https://www.opensignal.com/2021/12/14/singapore-faster-speeds-on-5g-than-on-wifi.
[20] Trust Over IP Foundation. 2021. "Introduction to Trust Over IP." Trust Over IP. https://trustoverip.org/wp-content/uploads/Introduction-to-ToIP-V2.0-2021-11-17.pdf.
[21] W3C DID Working Group. 2022. "Decentralized Identifiers (DIDs) v1.0." W3C. https://www.w3.org/TR/did-core/.
[22] W3C Verifiable Credentials Working Group. 2023. "Verifiable Credentials Data Model v2.0." W3C. https://www.w3.org/TR/vc-data-model-2.0/.
[23] Hyperledger Foundation. n.d. "Hyperledger Indy – Hyperledger Foundation." Hyperledger. Accessed July 19, 2023. https://www.hyperledger.org/use/hyperledger-indy.
[24] Vivek, Raj. 2022. "EAP-TLS vs. EAP-TTLS/PAP." SecureW2. https://www.securew2.com/blog/eap-tls-vs-eap-ttls-pap.
[25] Internet Engineering Task Force (IETF). 2014. "RFC 7170 - Tunnel Extensible Authentication Protocol (TEAP) Version 1." IETF Datatracker. https://datatracker.ietf.org/doc/html/rfc7170.