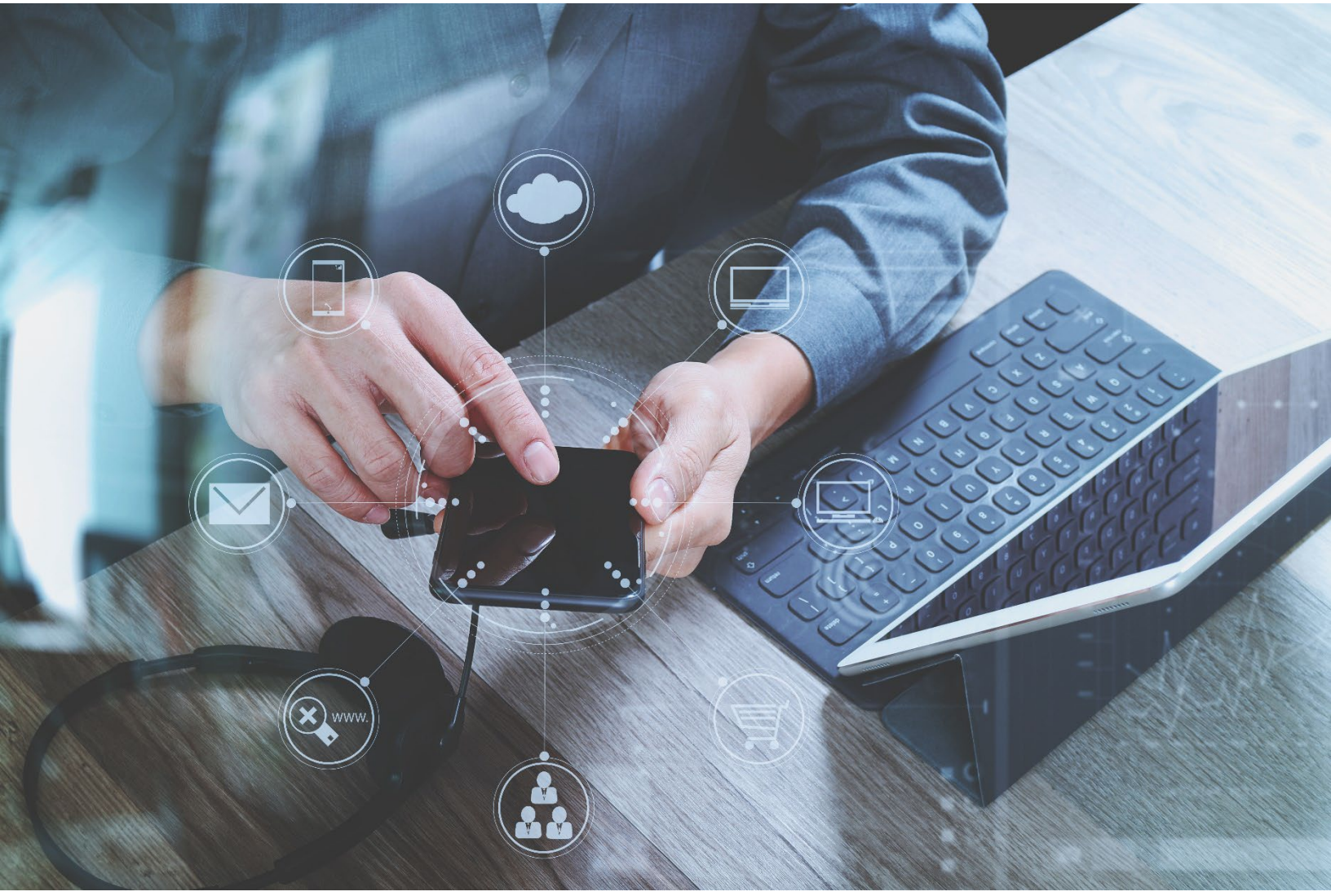
White Paper

RoamingiQ

MAC Randomization and Ubiquitous Wi-Fi Networks

This paper discusses technology for Wi-Fi network operators to reduce their reliance on MAC addresses in identifying customer devices, thereby improving the data privacy in business operations.

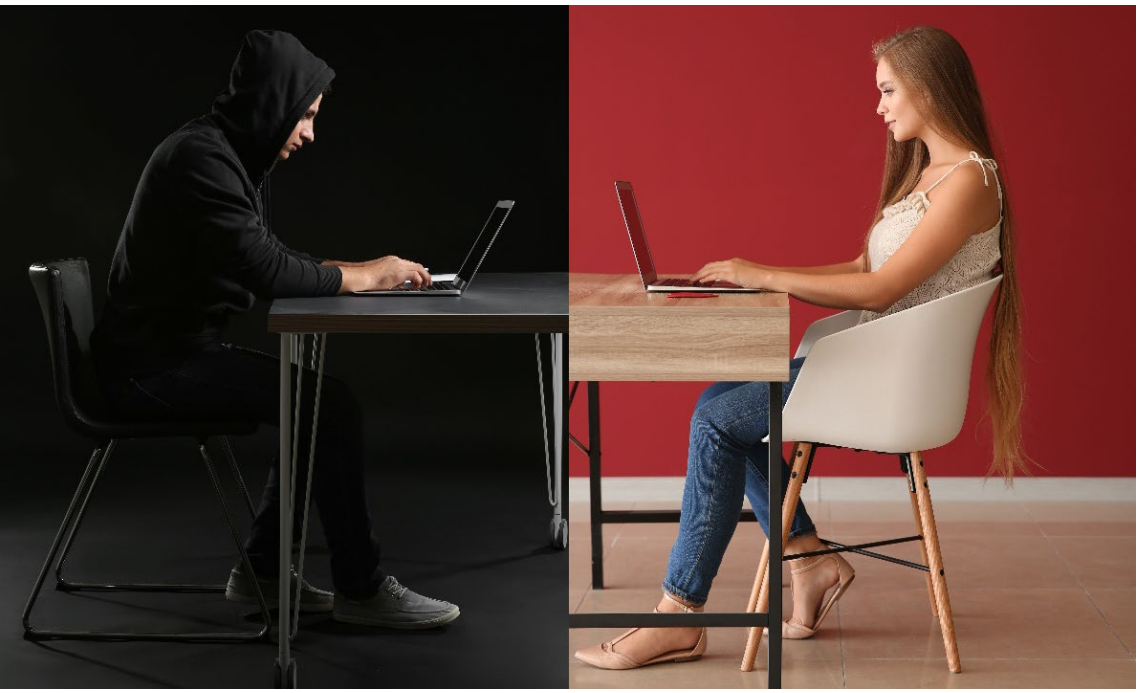


RoamingiQ.com

The Need for MAC Address Randomization

MAC addresses are designed to uniquely identify computing devices like smartphones within a physically connected network in a confined geographical area. MAC addresses can also be used to track the movements of devices, revealing the location and time of the individual possessing the device (without their knowledge or consent) to all Wi-Fi access points in the vicinity.

Location data is a goldmine for targeted advertising, and its implications have been of significant legal discussions worldwide. Various privacy regulations and laws like GDPR and CCPA are now in place to help protect consumers; thus, smartphone manufacturers are introducing risk mitigation strategies such as MAC randomization to increase the cost and complexity of identifying device users. As an unfortunate side effect, this also impacts the real-world operation of public access Wi-Fi networks such as in airports, hotels and apartment buildings.



Alarming Cyber Security Statistic

According to a Gallup® study, Americans are more worried about being a victim of cybercrime than being a victim of violent crime.

Seamless User Experience and Data Privacy

In public Wi-Fi networks such as hotels and airports, MAC addresses are used to identify unique users and to provide a seamless experience. This is especially useful in large areas with multiple access points where devices hop from one Wi-Fi access point to another or leave the premises and return later. If the MAC address of their device is changed during this service, the device does not reconnect to Wi-Fi automatically, and the user is redirected to a captive portal to enter their credentials again for Wi-Fi access.

In residential Wi-Fi networks, however, MAC address-based onboarding is not commonly used. Instead, WPA2/3 passphrases are used by devices to identify themselves to the Wi-Fi access points, and to establish a secure, encrypted connection to the Wi-Fi access points. While residential Wi-Fi systems are secure, they require that all devices on the network belong to a single user, making WPA2/3 infeasible for public Wi-Fi.

Change is in the Air

Recent advancements in Wi-Fi onboarding technologies from leading manufacturers like Ruckus (DPSK technology), Cisco (iPSK technology) and others now make it possible to deploy millions of WPA2/3 Wi-Fi keys (one for each user) on a single SSID.

With WPA2 keys for uniquely identifying the Wi-Fi users in large and public Wi-Fi networks, subscriber management platforms need not rely on MAC addresses to identify the service level for a user. Furthermore, technologies like RoamingiQ VAULT simplify the distribution of WPA2 keys for businesses with hundreds and thousands of locations globally. VAULT provides an encrypted key store to onboard Wi-Fi devices for billions of users securely and without user intervention. Each user can optionally be assigned personal policies such as a virtual network (VLAN) or personal area network (PAN) for added security and service quality management.

Network operators benefit from lower operating costs and simplified device onboarding experiences. An impactful gain compared to pre-installing certificates for Hotspot 2.0 MVNO deployments or the daunting task of self-installing certificates for BYOD and transient public Wi-Fi access. Technologies like VAULT are designed to be integrated with current Wi-Fi subscriber management platforms in use, thereby reducing the need for a complete overhaul of the Wi-Fi technology stack.

Using VAULT, network operators deliver a better subscriber satisfaction experience. Users manage their personal Wi-Fi keys for better-perceived security and control via smartphone apps and service management web portals (i.e. loyalty/membership apps common in the hospitality and travel industry).

Choices in Deploying Wi-Fi Networks

Reference the comparison chart below to see how VAULT improves your bottom line, customer satisfaction and legal compliance.

		FREE WIFI	Traditional Network Equipment Vendors	Wi Fi ALLIANCE Passpoint r3 (HS2)	SECURED BY VAULT™
Installation & Management	Self-installed and managed	Professionally managed	Professionally managed	Professionally managed	Professionally managed
Encrypted/Secure	Yes	No	Yes	Yes	Yes
Onboard IoT / Smart Home / Headless Devices	Yes	-	Yes	No	Yes
Wi-Fi Key Coverage	Single venue (< 1500 sq ft)	Single venue (> 1500 sq ft)	Single venue (> 1500 sq ft)	Global	Global
Specification Release	1998	2003	2018	2018	2020
Wi-Fi Keys	1-3	0	Hundreds	Certificate-based	Millions
Auto-Roaming at Business Locations of Partner Brands	-	Using device MAC address	-	Only carrier roaming, no B2B roaming	Both carrier roaming and B2B roaming
Specification Release	Secure Residential	Public Access	Secure public access Secure residential	LTE to Wi-Fi offload for smartphones	Secure public access Secure residential

RoamingiQ VAULT: A fully secure Wi-Fi network that reduces risks associated with data privacy, snooping and information manipulation issues.

VAULT Subscriber Management APIs

New Revenue Opportunities

- Offer encrypted Wi-Fi as a service at multiple business locations
- Supports both B2C and bulk Internet model (outsource subscriber management to B2B customers)
- Your B2C subscribers can auto-connect at any of your business locations
- Offer personal VLANs, bandwidth or any other network access policies at specific locations – such as home and office
- Limit number of concurrent/on-file devices a subscriber can connect
- Offer multiple Wi-Fi keys to your subscribers - to share with family/friends, SOHO separation, smarthome network
- Generate reciprocal revenue through Wi-Fi roaming/offloading agreements with other VAULT customers and expand your Wi-Fi footprint.

Privacy and Legal

- PII - Personal Identifiable Information
  - Subscriber pseudonym
  - MAC addresses of devices
- Compliance with
  - GDPR - General Data Protection Regulation
  - CCPA - California Consumer Privacy Act

Branding and Performance

- Subscriber management using your smartphone apps / web portals
- Authenticate known devices in less than 100 ms.
- Auto-onboard new devices in less than 2 seconds.

Infrastructure

- Private cloud in global SOC-2 compliant data centers
- Integration with leading Wi-Fi vendors (other vendor integrations on roadmap)
- Custom RADIUS attributes for your business needs, e.g. subscriber VLAN

Designed for Global Operations

- RADIUS farm available as additional module
- OpenAPI documentation and professional integration services
- Web portal for account and billing management
- 24x7 operational support (English only)

Ubiquitous Wi-Fi Authentication Built from Ground Up

The ubiquitous WPA2 Wi-Fi onboarding method supports both LTE-first smartphone devices and headless devices such as Apple TV, Google Chromecast, Samsung refrigerators, etc.

At RoamingQ, we engineer our products from the ground up with security and data privacy hygiene a top priority. We work ubiquitously with handheld devices and residential-grade smartphone devices.

www.RoamingiQ.com
sales@RoamingiQ.com

RoamingiQ™