Whitepaper

OpenRoaming™ – secure and seamless Wi-Fi connections

Current Situation at Wi-Fi Hotspots

We all know the challenges when using public Wi-Fi:

- Different network names (SSIDs) that need to be found first.
- Different login procedures: from accepting terms to passwords to SMS registration. If someone leaves the hotspot briefly, the process starts again.
- Captive portals do not always work – making connection impossible.
- Missing security: no encryption and frequent certificate issues.

For people using the service, this means reduced convenience, and for operators, higher support effort and costs. At the same time, the demand for reliable, secure, and user-friendly connectivity is increasing.

What is OpenRoaming™?

OpenRoaming™ enables a stable, secure internet connection worldwide – without repeated logins. Similar to mobile roaming, the device automatically connects to trusted networks (here: Wi-Fi). Authentication happens seamlessly, based on established standards. OpenRoaming™ was developed by the Wireless Broadband Alliance (WBA).

Benefits

Seamless Connection

Automatic connection without captive portals or login steps: As soon as a device is within range of a certified OpenRoaming™ hotspot, it connects automatically. Travellers can save mobile data and reduce roaming costs abroad.

Security

OpenRoaming™ uses modern standards such as WPA3 and strong encryption to reliably protect data.

Comfort

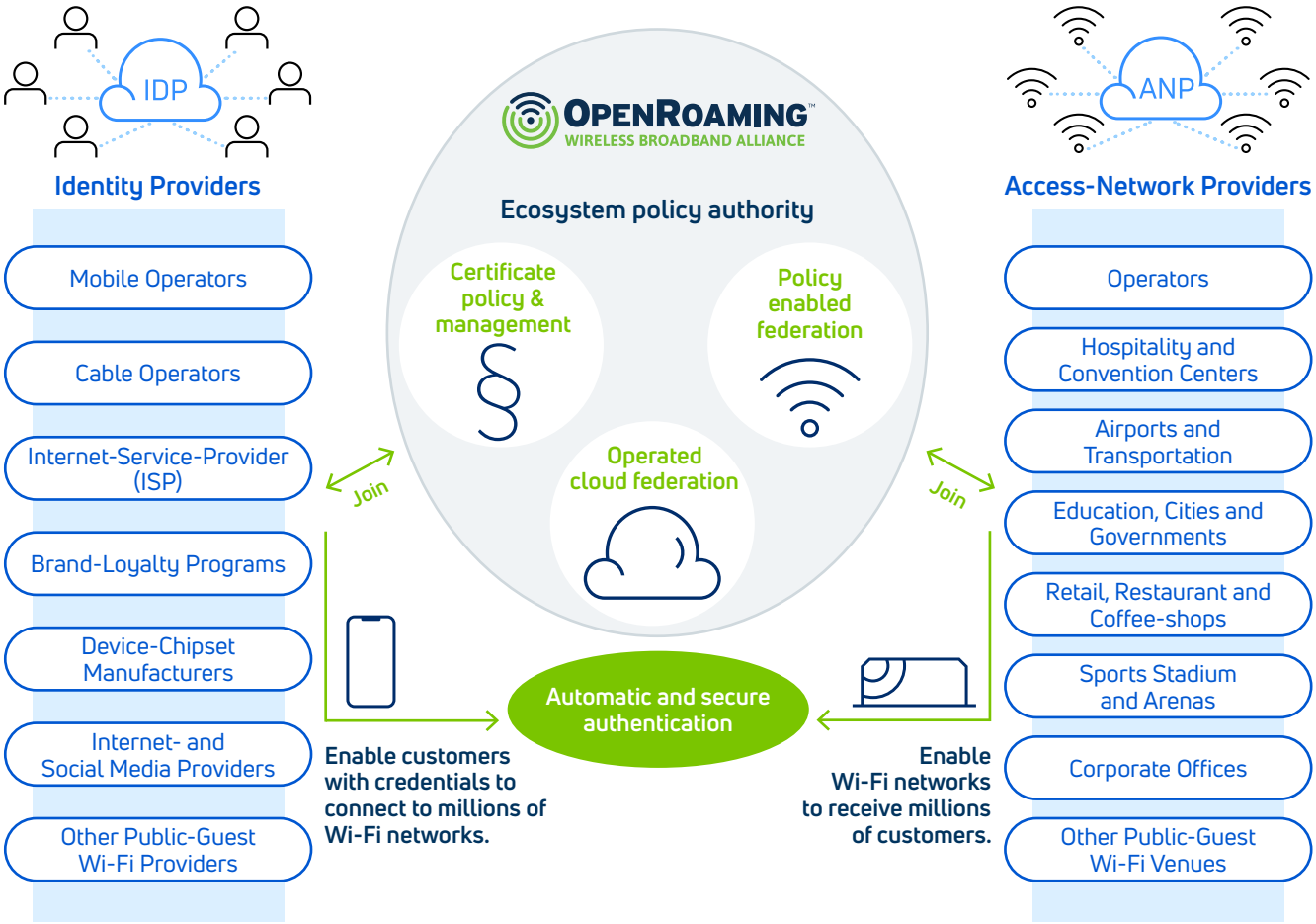
Companies and network operators provide their guests with easy access, without constantly issuing new login credentials. At the same time, the effort for support and SMS-based authentication is reduced.

Potential Applications and Markets

- **Tourism and hospitality:** Guests benefit from seamless Wi-Fi without manual login.
- **Smart cities:** Area-wide coverage for navigation, traffic management, or electronic payments, e.g. when buying public transport tickets.
- **Airports and train stations:** By roaming automatically between Wi-Fi networks, travellers stay online without interruption.
- **Retail:** Automatic connection for personalised services, loyalty programs, or apps (e.g. Twint).
- **Healthcare:** Secure connectivity for patients, visitors, and medical devices.
- **Industry and logistics:** Stable network coverage in warehouses, production facilities, or ports.
- **Education:** Universities and schools use OpenRoaming™ as an evolution of eduroam.

Architecture

OpenRoaming™ is based on a clear role model:



- Identity Providers (IDP): Manage user identities and authenticate end devices. IDPs are typically organisations with large user bases: examples include telecom providers, transport companies, tourism organisations, large enterprises such as banks, insurance companies, retailers, health insurers, etc.
- Federation Policies: Define trust, security and interoperability between all parties.
- Access-Network Providers (ANP): Provide the Wi-Fi infrastructure. ANPs are Wi-Fi operators offering secure hotspots to their guests.

How to Join OpenRoaming™

As in mobile networks, users need a contractual relationship. In mobile networks, this is a mobile operator. With OpenRoaming™, this can be any Identity Provider (IDP), for example: a public transport company such as SBB, a retail provider such as Migros or Coop, or a tourism organisation (digital guest card) – simply an organisation with which the person already has a customer relationship.

- This IDP creates a profile that is installed on the device.
- Thanks to this profile, the device connects automatically and securely to any Access Network Provider (ANP) that supports OpenRoaming™.
- The connection uses standardised protocols such as EAP and RADIUS.

Requirements for Users

- **Compatible devices:** Modern smartphones and laptops already support OpenRoaming™.
- **Registration with an IDP:** The user activates their OpenRoaming™ profile through the chosen identity provider.

Benefits and Requirements for Identity Providers (IDP)

Customer loyalty is strengthened, as the customer relationship generates value even outside the organisation's own environment. For example, integrating OpenRoaming™ into an existing customer app significantly increases its usefulness: people experience seamless, secure, and encrypted Wi-Fi access not only within the organisation's facilities, but also at thousands of other OpenRoaming™ hotspots worldwide.

Requirements:

IDPs provide their customers with an OpenRoaming™ profile via their website or app.
For this, they require an OpenRoaming™ Registrar service, for example from onway.

Benefits and Requirements for Access Network Providers (ANP)

For hotspot providers, OpenRoaming™ offers many **advantages:**

- Automatic access for customers → seamless user experience.
- Reduced administrative effort thanks to standardized authentication.
- Lower support costs through easier handling.
- Increased security for company and customer data.

Requirements:

The Wi-Fi infrastructure must support OpenRoaming™ and include::

- Hotspot 2.0 support
- AAA infrastructure with a RADIUS server for authentication

Example: SBB

SBB acts as an **IDP**: Customers authenticate once via SMS token or SwissPass login.
They then receive an OpenRoaming™ profile that can be used worldwide – comparable to a digital SIM card. With over 4 million SwissPass accounts, this results in significant potential.

SBB also acts as an **ANP** and provides an OpenRoaming™-capable network that guests can use automatically. International visitors can therefore use their existing profile (e.g. from their mobile operator) while in Switzerland.

onway Solution Architecture

onway extends OpenRoaming™ with practical features:

- **Secure Guest Wireless:** secure guest access, without manual registration, compliant with Swiss data protection law.
- **Self-Registration Portal:** legally compliant user registration and provisioning of OpenRoaming™ profiles.
- **Integration into apps and loyalty programs:** e.g. ticketing, payment, or voucher systems.
- **Connection to Open-ID-Connect:** easy management of user profiles and devices.
- **Compliance:** storage of all connection data according to Swiss legal requirements; only verified roaming partners are allowed via whitelists.

Conclusion

OpenRoaming™ enables global, secure, and seamless Wi-Fi connections. Through the clear distribution of roles between ANP and IDP and the federation policies, a scalable and interoperable model is created. With onway's software solutions, implementation can be realized easily, quickly, and in compliance with legal requirements.

Who we are – onway ag

onway is a leading provider of tailored communication solutions for all areas of modern network infrastructures. We support more than 150 customers from various industries in the design, implementation, operation, and support of secure ICT infrastructures. Our own products include a multi-tenant smart access solution, public hotspots, and mobile solutions for public transport vehicles. We also integrate communication solutions from established manufacturers, creating seamless, future-proof networks.

The onway Group is fully certified according to ISO 9001:2015, ISO 14001:2015 and ISO/IEC 27001:2022.

onway ag | Stauffacherstrasse 16 | 8004 Zurich | Switzerland | Phone +41 55 214 18 30 | sales@onway.ch | www.onway.ch