

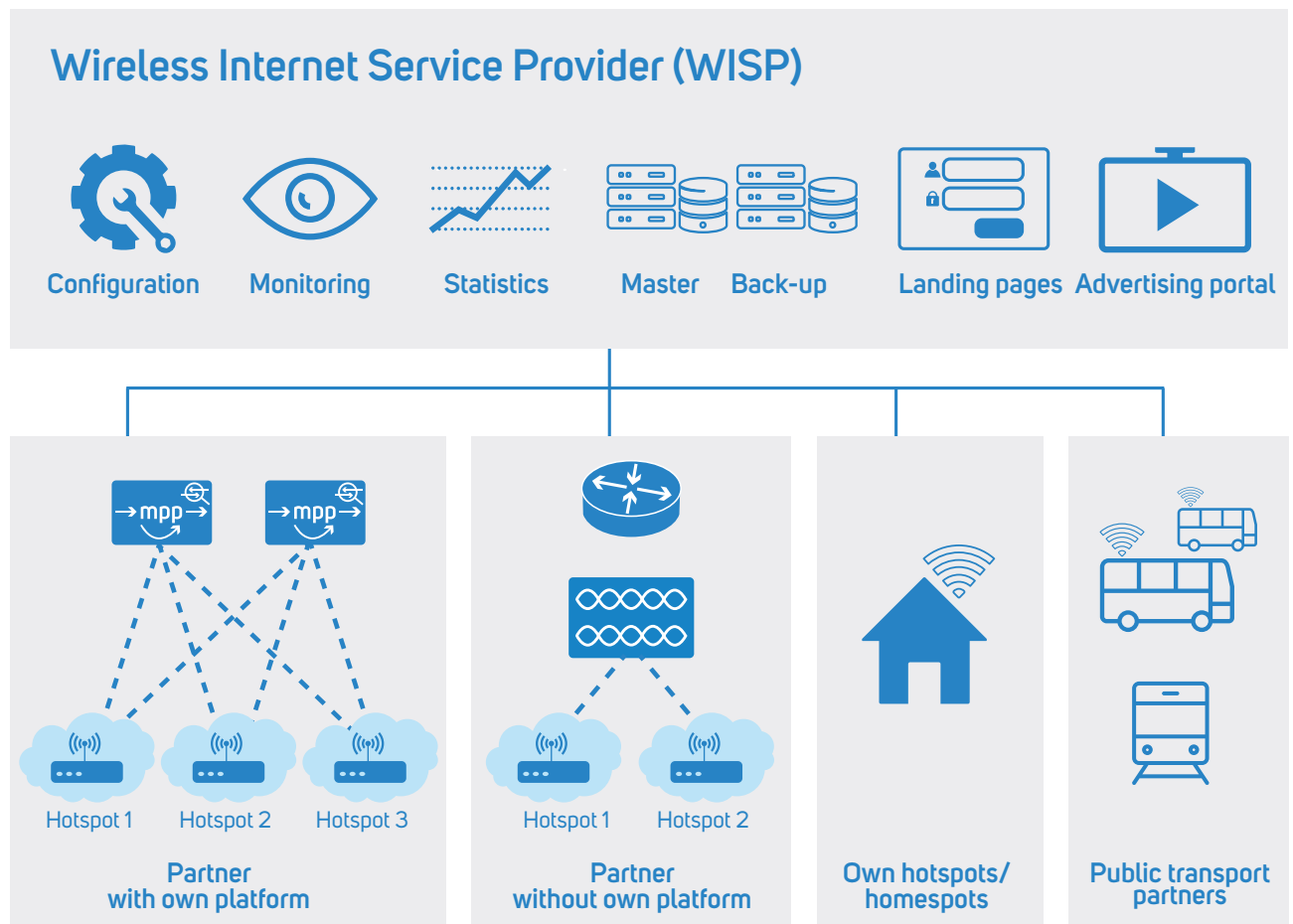


You are also a hotspot provider

Hotspot Providers or Wireless Internet Service Providers (WISP) not only include large telecommunications companies, but also cable network and mobile phone providers, IT service providers, energy suppliers, public transport companies, municipalities, hotel chains – in fact any organisation that operates several public hotspots. Usually, a central service platform is used, which regulates the authentication of users and devices or the allocation of services, for example. And herein lies the problem: different customers have different needs that are difficult to meet with a rigid «one-size-fits-all» solution. This fact makes it almost impossible for providers to respond to individual requirements flexibly and without great effort.

High demands from customers and partners alike

- Individual business models for different hotspots, i.e. free and paid internet access for customers and guests
- Unlimited or limited use (such as bandwidth, data volume, duration)
- Individual landing pages per hotspot for local information or advertising (Managed Internet Hotspot Service)
- Secure access for employees' personal devices
- Roaming option between other providers' hotspots (such as iPass, Boingo) or formation of a switching platform within partner alliances
- Connection to systems such as Active Directory, RADIUS, hospital information systems, hospitality software
- Use of private modems as hotspots (homespots)



Managed centrally yet designed individually: «WiFi as a service»

With **mpp** as both a centrally and decentrally applicable, multi-client-capable service platform, hotspot providers cannot only centrally manage their own services and hotspots. Rather, «WiFi as a Service» allows them to offer different customers/partners customised solutions and services on a cloud-based platform without much effort.

As a result, the corresponding landing pages can be automatically assigned to users during the registration process, designed as desired and, depending on the usage model and location, different payment systems can be set out.

Why is our mpp so special?

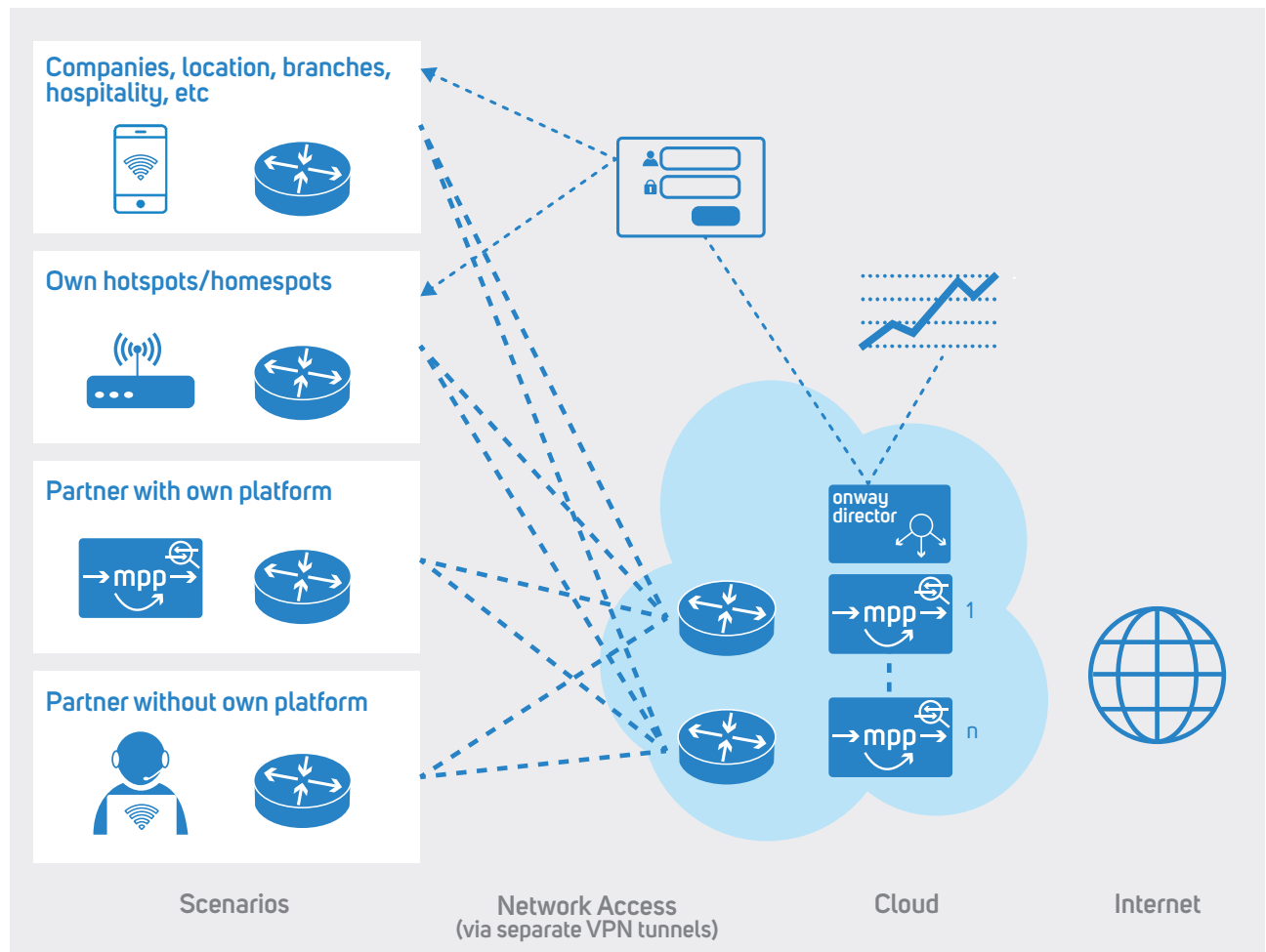
- Installation in the cloud or «on premises»
- Scalability up to several 100,000 simultaneous users
- Maximum availability
- Vendor independent (Cisco, Ruckus Aruba, Nokia, etc.)
- Technology independent (LAN, WLAN, mobile radio)
- Modern software architecture
- High flexibility when implementing individual customer requirements
- DNS/URL filtering
- Simple deployment of distributed platforms thanks to virtualisation
- Multi-client cloud management with multi-level authorisation concept
- Traceability thanks to historical data storage
- Compliance with legal requirements incl. real-time monitoring
- Automatic language recognition/multilingualism
- Monitoring/alerting
- Short development cycles for new product functions
- Our software is developed exclusively in Switzerland by our own specialists.



swiss made software

The optional **onway director** (sponsoring portal) complements mpp perfectly.

With this system, authorised persons can assign access rights for guests as well as for company and personal devices.

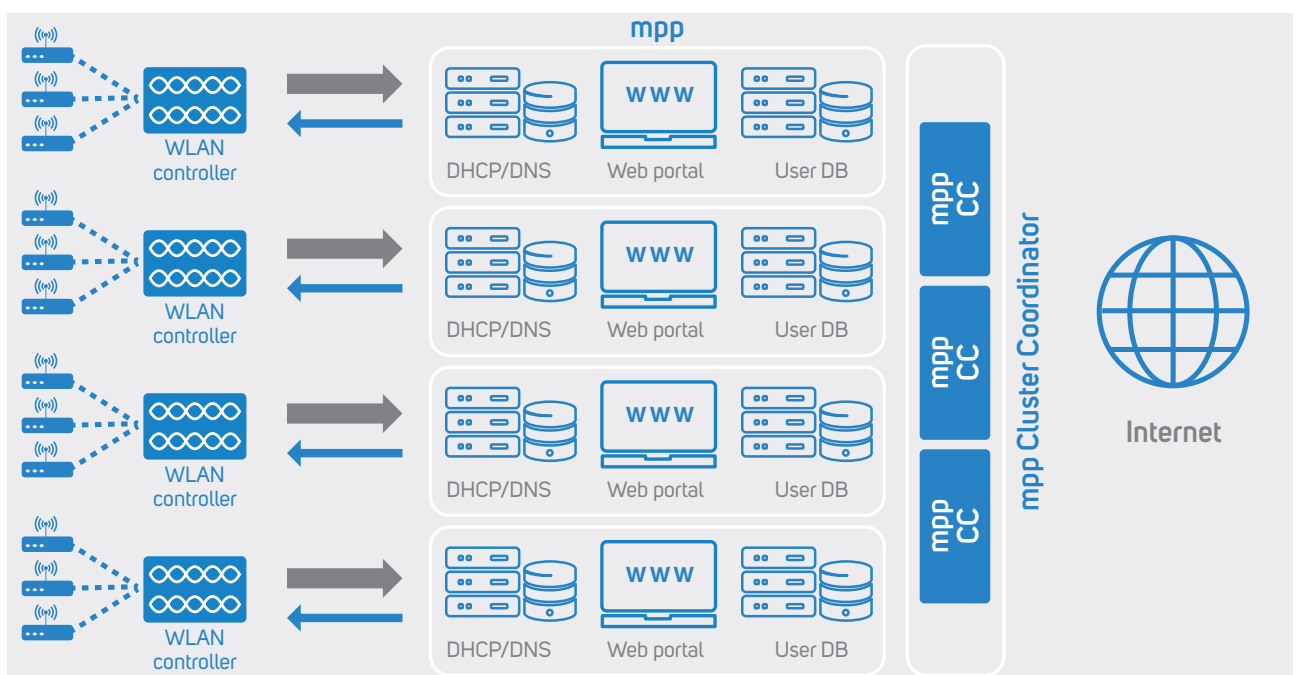


Four different example scenarios are shown in the graphic above:

- «WiFi as a Service» for business customers with multiple locations
- SMS authentication – used where many unknown persons (e.g. at railway stations, airports) access the internet via WLAN. Given that registration is a one-off, legal traceability requirements are guaranteed at any time yet the operator does not incur any additional administrative effort. Registered users receive their access code via SMS. As an option, the onway director (sponsoring portal) can be used to assign access rights.
- Business customers without their own platform benefit from both the functionalities offered and the evaluation options.
- In the homespot scenario, private customers' modems are transformed into WLAN hotspots for other customers as part of the cable network partner agreement. Authentication is via mpp.

Distributed architecture for maximum performance, scalability and reliability

The centralised architecture that was previously standard resulted in bottlenecks, especially in networks with thousands of users. Due to the increasing number of users and the associated growth in data traffic, previously centralised resources were unnecessarily overloaded and the overall service quality was compromised. With a modern, decentralised architecture, not only is scalability hugely increased and resilience improved, but location-based services are also easier to implement and manage. The distributed systems synchronise via the **mpp Cluster Coordinator** (mpp CC).



As almost every customer has individual requirements and needs, we have been able to garner a great deal of experience from all our projects since 2004. We incorporate this extensive expertise, as well as our clients' wishes, into the further development of our software solutions for Network Access Control (NAC), Bring Your Own Device (BYOD), Guest Access and communication access for public transport. This now means that over 100 companies across different industries and sectors are successfully using our software.

We would be delighted to support you with your plans. Why not get in touch and put us to the test?