LANCOM™ White Paper
Hotspot 2.0 - WLAN as easy as cellular

Introduction

These days, users with multimedia devices increasingly expect to find wireless LAN access wherever they go. This is why there is now stiff competition to offer end customers the best in hotspot technology. In order to remain competitive, businesses, hotels, department stores, and other establishments are faced with the necessity of offering their customers WLAN. Apart from providing the widest possible coverage, other important aspects that can make a hotspot attractive to customers are its security and usability. Hotspot 2.0 combines all of the advantages of public guest-access technologies, be they for end customers, venue owners, or providers.

Current situation

Everyday life has changed. Thanks to mobile end devices such as smartphones and tablets, we are online everywhere and all the time. Having an Internet access has become a matter of course - thanks to cellular networking. However, people instinctively look for open WLAN hotspots, since the available cellular connections can sometimes be slow and users want to save their monthly data volume.

When looking for a public WLAN hotspot, users are usually faced with a problem: Looking at the list of available WLANs (SSIDs) the user usually doesn't know which network to choose. In most cases, the hotspot provider also requires login data (username and password). And even if the user has these, they have to be entered manually on the web portal every time they access it. The usual result is that users choose a slower but less complicated cellular network connection. As soon as the device is inside a cellular network cell, it automatically authenticates itself using the SIM card and goes online.

Why can't WLAN work that easily?

Hotspot 2.0

The general goal of Hotspot 2.0 is to make guest access to WLAN secure and automatic. The selection of the correct SSID and login at the hotspot occur in the background and go unnoticed by the user. The underlying WLAN standard IEEE 802.11u facilitates communications in advance between the end device and the access point. At the same time, the access point with Hotspot 2.0 functionality informs the client about the supported authentication method so that the client can compare it with its own methods. When there is a match with one of the available methods, an automatic, encrypted authentication of the client is performed for the WLAN access, and the connection is made - without the user having to do anything.

Tech facts

From the technical perspective, there are two steps in the authentication process for encrypted access to the WLAN: "Network Discovery and Selection" and "Authentication". These are based on the certification program "WPA2-Enterprise" from the Wi-Fi Alliance, which specifies the standards and protocols for IEEE 802.1X, EAP, and IEEE 802.11i, as supported by all popular mobile end devices.

Network Discovery and Selection (1)

The initial communication between the access point and the client usually relies on beacons. The client receives basic information about the (B)SSID, the signal strength, and the generally supported features of the IEEE 802.11u standards, among others. New with Hotspot 2.0: Using a Layer-2 connection that is provided by the GAS protocol (Generic Advertisement Service), ANQP packets (Access Network Query Protocol) are transmitted to the client with further information. The exchanged information contains, for example, the properties of the supported roaming partners and authentication methods: By means of a SIM card from the hotspot provider, digital X.509 certificates, or a combination of username and password. The client compares this with its own available authentication methods and can then request further information from the access point.

Authentication (2 - 5)

If the client supports one of the available methods it can authenticate using IEEE 802.1X, whereby one specific EAP variant is used each time.

- SIM card → EAP-SIM
- Digital X.509 client certificate → EAP-TLS
- Username and password → EAP-TTLS and MS-CHAPv2

Using the EAP variant, the client sends an authentication request to the access point, which is then forwarded over the Internet to the corresponding authentication server for a validity check. If the validity is confirmed, the access point registers the client in the local user table and grants access to the hotspot.

Business model

Apart from the advantages it offers for operations and security, Hotspot 2.0 also opens up new business models: To reduce the load on the cellular network, providers are interested in setting up hotspots at strongly frequented locations with large numbers of clients. The provider or, alternatively, an intermediate roaming broker concludes a roaming

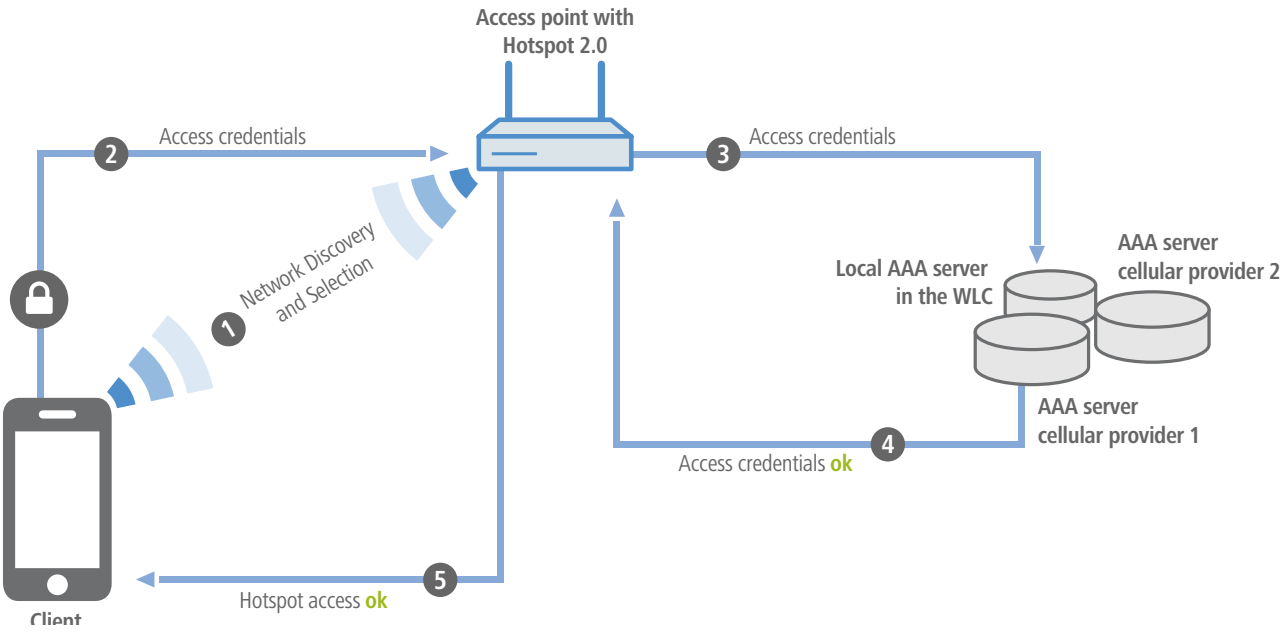

Diagram: Network search and authentication using Hotspot 2.0

agreement with a venue such as a café, department store, airport, or even an enterprise. To provide a public hotspot, the venue owner receives the necessary hardware as well as a subscription fee from the provider. End customers then pay a user fee to their own (cellular network) provider for using the available hotspot.

Advantages of Hotspot 2.0

Hotspot 2.0 provides many advantages for everybody involved; the end customers, venue owners, and providers.

Advantages for end customers

- Using WLAN becomes as easy as using a cellular
- No manual selection of SSIDs or input of access credentials
- Secure authentication on WLAN hotspots thanks to WPA2/EAP encryption
- Faster Internet experience compared to cellular networks
- Savings on mobile data volumes, depending on the cellular service contract
- Access to WLAN hotspots at different locations

Advantages for venue owners

- WLAN access as a competitive advantage leads to higher customer satisfaction among multimedia users
- Increased turnover as customers stay longer thanks to WLAN access
- Customers gladly return to the hotspot locations even at other branch locations (e.g., for WLAN access abroad)
- Simple provision of the necessary technology through cooperation with providers or roaming brokers
- Provision of hotspot login data is no longer necessary

Advantages for providers

- Load reduction of the cellular network due to WLAN offloading
- Simple integration in the venue's existing network infrastructure
- Higher market visibility at subsidized hotspot locations
- Customer loyalty thanks to Hotspot 2.0 roaming agreements reduces the churn rate

Deployment scenarios

Example: Authentication using digital certificates or with username and password (without a cellular network provider)

The authentication using digital certificates or with username and password is especially interesting for mobile clients without SIM cards. In this case, the authentication method has to be set up one time by the user or administrator. This involves the hotspot provider supplying either a username and password or a digital X.509 certificate for

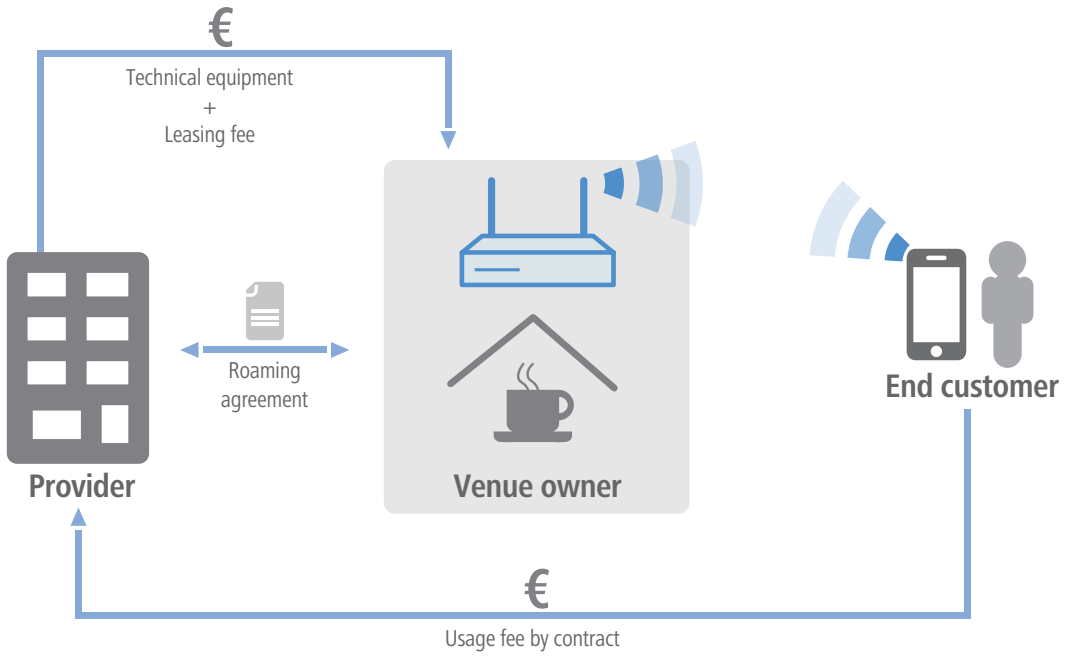

Diagram: Potential business model with Hotspot 2.0

storage on the client. After this one-time setup, login to all supported access points with Hotspot 2.0 functionality is fully automated and occurs in the background, just like the method with SIM cards. This method is particularly attractive for venue owners or enterprises who only grant access to certain clients, or who do not want to have a roaming contract with a large cellular network provider.

Example: Authentication using a SIM card (with cellular network provider)

The most convenient method to authenticate against Hotspot 2.0 is to use the SIM card in an end device. The prerequisite for this is a roaming agreement between the venue owner and one or more cellular network providers. As soon as a smartphone with a suitable SIM card is within range of a Hotspot 2.0 access point, it is automatically authenticated for hotspot access - without any action by the user.

Hotspot 2.0 Release 2

The Wi-Fi Alliance has initiated a marketing program for Hotspot 2.0 named "Passpoint". The purpose of this program is to certify WLAN devices for interoperability with Hotspot 2.0 functionality based on the IEEE 802.11u standard. The Passpoint program is being implemented in a number of steps. Passpoint Release 1 was published in June 2012 and will be expanded with Release 2. Passpoint Release 2 makes it possible for end customers to directly request login data (username and password, or a certificate) at the hotspot. For example, the user can choose a suitable offer based on his needs, whether it is volume-based, time-limited, or even free. The client receives the necessary

login data automatically. The venue owner or provider no longer has to provide the login data manually. Instead, the end customer can login independently with a minimum of effort for everyone involved.

Summary and forecast

Hotspot 2.0 is a future-oriented technology, and its potential is gaining recognition. The tangible benefits depend largely on two developments:

On the one hand, there is the increased prevalence of IEEE 802.11u-compatible WLAN devices, both end devices as well as access points. There are already hundreds of millions of 11u-compatible end devices in use. The certification "Wi-Fi Alliance CERTIFIED Passpoint™" is a seal of quality that contributes to the expansion of the 11u standard.

On the other hand, there is market penetration. The win-win-win situation for end customers, venue owners, and providers must be recognized as such, so that the technologies can be deployed on a wide scale and the business models can be implemented effectively.