WiFi Network Usage Manual for temporary access of Visitors

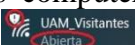|	Autor:	Nicolás Velázquez Campoy		
	Fecha de Creación:	08/10/2018	Versión:	1.1
	Revisado por:	Miguel Angel García Martínez		
	Fecha de Última Revisión:	08/10/2018		
	Destinatario:			

1. Service presentation.

The UAM offers temporary access to its wireless network for fifteen days[1] to anyone who, without having a relationship with this university or with other centres associated with the eduroam initiative, moves to the UAM campus.

The service only provides network access and will not provide any other additional service: e-mail account, VPN access, cable connection, telephone terminal equipment, etc..

Access will always be granted for a limited time of fifteen days. If you need access for a longer period of time, or more services, you can contact the University's Information Technology User Service Centre (cau@uam.es.es or 914974029).

2. Setup instructions:

1. In the Settings or Device Configuration, or in the selection of available wireless networks, look for the wireless network with the identifier UAM_Visitantes. Examples of how they can be displayed or .

2. In Android mobiles, in the selection of wireless networks, Eduroam and other networks appear with a padlock that indicates encryption. . The network **UAM_Visitantes** appears on Android without a padlock indicating that it is open . Windows computers display a warning shield and an explicit indication that it is open .

When selecting the **UAM_Visitantes** the computer may warn by a message[2] that it is a non-encrypted[3] network. We advise you not to exchange personal information during the connection and, if you are going to exchange user/password or sensitive personal information, make sure you always use encrypted protocols: vpn, ssh, https, sftp, etc...

---

[1] After that time, the credentials will be invalidated, and it will no longer be possible to use them to access this wireless network.

[2] Depending on the device, the operating system itself may display a warning for connecting to an open wireless network. And other times, the device's antivirus/antimalware or some other security application may display a warning message.

[3] Current technology does not allow a self-registration portal to be set up over an encrypted wireless network. This problem is suffered by all the wireless networks with self-registration that exist in many institutions: hospitals, administrations, shops, etc. It seems that the new WPA3 standard will solve the problem, but it is still in the development and implementation phase. Later on, we will have to wait until the user devices also have WPA3..

3. In the preferred browser that your device has, or the one you choose, a page will open where you can register for guest credentials.

   It could happen that the device does not propose you to open any browser. Start the browser of your choice and try to browse the Internet. Enter any address: www.elpais.com, www.rtve.es, etc. The registration page will appear.

   Be careful selecting the country code from your phone number. The country code is required to send your credentials.

   Once all the fields have been properly filled in, and the box for acceptance of the terms and conditions of use has been ticked, press the Send button.

4. You will receive an SMS to the phone you indicated in the registration. In this message you will see the username, password and duration of the credentials.

5. Go back to your browser and follow the instructions provided to enter your credentials.

   Remember that the username of the credentials is your telephone number with the country code.

   Once the credentials have been entered correctly, you can navigate with that device.

6. If you want to use more devices, follow steps one and two, but in step three, <u>don't fill out the registration page again</u>. <u>You already have valid credentials</u>. Go directly to the credentials entry page by clicking on the phrase:

   <u>If you already have a visitor account</u>,

   <u>login</u>.

   On the resulting page, enter the credentials you have already received by SMS.

   Remember that you can use the credentials on as many devices as you want, but you can only connect two of them <u>simultaneously</u>.

Universidad Autónoma de Madrid