Unlicensed Mobile Access

Clavister SSP™ Security Services Platform

firewall • VPN termination • intrusion prevention • anti-virus
content filtering • traffic shaping • authentication

clavister™

Protecting Values

- **Increased customer satisfaction through better in-home coverage**
- **Use the same platform for UMA security as for IWLAN, FemtoCell and other**
- **Proven and tested technology**
- **Investment friendly licensing model – Pay as you grow!**
- **Differentiated service levels and charging depending on performance provided**
- **Lowered costs when addressing new markets outside of your current geographical coverage**

UMA – Merging Internet and GSM networks for mobile communication

UMA (Unlicensed Mobile Access), also known as GAN (Generic Access Networks), makes it possible to use both GSM radio and WiFi - wireless broadband connections for mobile communication. Mobile communication in this case includes voice, SMS, MMS, internet browsing, or simply put: Any mobile service available today and in the future.

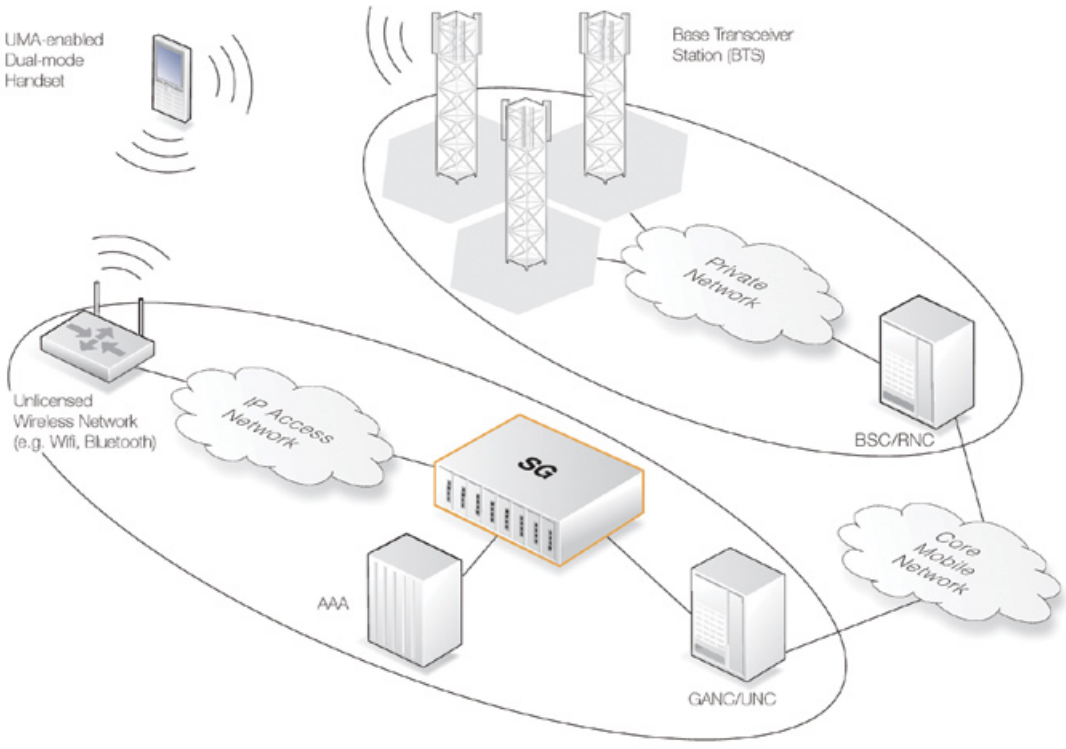
Customer experience

Today you have access to the Internet at home and/or at work, and more and more often access to broadband connections. When you use your mobile phone, you use a separate, GSM radio connection. But with UMA you can use both the internet and GSM networks to connect to the same services from a single device.

Since your broadband connection is reliable, fast, and always there, why not use it with your mobile phone too?

That's the idea behind UMA. It lets you connect your mobile device to your GSM services through WLAN.

When you're not in range of your WiFi connection the automatic switch from broadband to GSM is as seamless and simple as sitting in your car and passing by different GSM cells - you won't even notice it happening.



Clavister Security Gateway in a UMA network

UMA Security Challenges

Increasing the Average Revenue Per User (ARPU) and seizing the opportunities that a converged fixed / mobile networks presents also introduces risks which need to be addressed. As UMA is a fairly new technology there are still many security aspects which yet have not been explored, understood and most certainly, not defined by any standard.

We at Clavister believe that the key to success for any service provider who wants to offer Unlicensed Mobile Access is to look beyond the standards and investigate threats that yet haven't been defined. As UMA opens up operators core networks to the internet, it is necessary that you re-evaluate your security infrastructure to make sure that the entire network is kept safe even with the new environment.

Top Security Risks and Challenges

Intrusions and Denial of Services (DoS) attacks from UMA subscribers

Your customers, or at least the ones who you might think are your customers, impose a security threat as they can launch attacks either towards your core network or against other subscribers.

Clavister protects the UMA network against these threats through a variety of DoS attack mitigation techniques such as packet malformation checks, traffic and overload protection, network segmentation and policy enforcement.

Intrusion and DoS attacks from unknown sources on the Internet

As your network is exposed to the internet you are also exposed to the fact that practically anyone, no matter if they are one of your customers or not, can try to get into your network using fairly simple methods. It is not uncommon that these types of attacks are fueled by financial interests. Just as enterprises have been held hostage with the threat that a Denial Service Attack can be launched against them, this can also be true for a UMA network.

Clavister protects UMA networks against attacks from unknown sources on the internet by for instance facilitating strong authentication and access control mechanism, high performance and strong DoS protection. In short: Clavister ensures that only valid data sent from authenticated UMA subscribers reaches the core network, everything else is stopped at the perimeter of the network.

DoS attacks from GSM/GPRS access network to UMA network and subscribers

Attacks towards the UMA subscribers can also originate from users on the GSM network. This is a far more complicated attack to launch but needs to be considered just the same. Thanks to the design of the Clavister UMA Security Gateway, the same security checks can be performed independently of where the attacks are coming from and in what direction they are going. This means that with Clavister you have the same comprehensive protection mechanisms for these types of threats as for the attacks originating from the internet or from actual UMA subscribers.

Subscriber integrity

Your subscribers are used to sharing their information in a secure manner, thinking that no-one will intervene and snatch what they might be saying or sharing over the GSM network, with the exception of the ones who suspect that the government might be listening in. Having the information flow over the internet makes people cautious and they want to be assured that their conversations or data sharing is kept just as secret to the outside world as when being transported over the GSM network. As the Clavister UMA Security Gateway includes strong encryption standards like AES 256 bit encryption and EAP/SIM authentication these customer can rest easy. All communication between mobile devices and the operator's core network is encrypted and is not available even to the most skilled hacker.

Quick facts

For consumers:

- Use your mobile phones for all of your communications
- Excellent in-home coverage
- Seamless switch between WiFi and GSM radio network
- Reduced costs when using the the mobile phone at home
- No need to quarrel about the traditional phone being occupied

For operators:

- Better home coverage increases customer loyalty and satisfaction
- Decreases the pressure for expensive GSM cell build-ups
- Enables new traffic tariff charges
- Faster time to market and lowered costs when offering managed in-house GSM phone solutions to enterprises not covered by your normal GSM network

Clavister and the UMA network

The Clavister UMA Security Gateway (SGW)
The Clavister Security Gateway 5500 Series appliance is the device used as the UMA Security Gateway due to its resilliency, performance and scalability.

With room for eight (8) Secure Blade Modules, each with its own fast-path accelerator, the 5500 Series offers performance and scalability with support for 10,000 to 400,000 subscribers in one single chassis. Naturally the 5500 Series includes redundancy of every vital component and offers 99,999% service availability.

The main purpose of the Clavister UMA Security Gateway is to provide a safe and secure environment for subscribers as well as for operator's core networks.

The security features provided to the UMA network include DoS protection, NAT/Firewall traversal, Encryption (IPSec w/ IKEv2) and many other specific security features required by mobile service providers.

Integrity through strong encryption
By using strong IPsec encryption the Clavister Security Gateway ensures the integrity of all communication between mobile devices and the operator at the same time as it provides protection to the infrastructure. This means that any traffic between mobile devices will be as discrete and protected as when it is being transported over a GSM network.

Convenient Authentication
The secure and encrypted tunnel between the Clavister Security Gateway and the mobile devices are authenticated using public key-based certificates. Thanks to the support for the authentication protocol EAP-SIM and EAP-AKA in the Clavister Security Gateway the SIM card on the mobile device can conveniently be used as the certificate which identifies the subscriber.

Inside tunnel protection
In a security context, one can never trust traffic, not even if it comes from within one of the encrypted communication tunnels. Therefore the Clavister Security Gateway is also designed to inspect traffic within the VPN tunnels and to protect against attacks just as if it originated from normal internet traffic.

Key benefits with Clavister in UMA networks

Security
The Clavister Security Gateway is built to provide supreme security and includes all the necessary threat mitigation technologies in order to ensure a safe UMA network environment for the subscribers as well as the operator and service providers

Investment friendly
The xPansion Lines license model allows you to start with a single blade running 10,000 subscribers and upgrade the subscriber density by just changing the license file. If you need to scale beyond the capacity of a single blade, simply add a second or third one just as easily.

Performance
Each Security Blade Module provides VPN connectivity of up to 2 Gbit/s thus making it able to support a massive number of concurrent calls with high voice quality as well as data communication. At the same time as it is providing connectivity to tens of thousands of passive connections.

Reliability
- Redundant power supplies
- Redundant fan modules
- Redundant Secure Blade Modules
- Redundant Rear-Transition-Modules
- Redundant Out-of-Band management modules
- 99,999% reliability

Ability to support multiple service types in one platform
The Claivister SSP™, Security Services Platform, is able to support UMA, I-WLAN and other services within the same technology platform, thus making it possible to lower both your CapEx and OpEx.

Verified and Proven
Meets practically every telecom environment certification standard (e.g. ETSI standards). Interoperability tested with handsets from e.g. Nokia, Philips, Samsung and others.

Centralized Management
Included is Clavister FineTune™, a modern and graphically oriented management system that provides management capabilities for all aspects of your Clavister UMA security gateways.

Clavister SSP™ Security Services Platform
firewall • VPN termination • intrusion prevention • anti-virus
content filtering • traffic shaping • authentication

Protecting Values

Part number: CLA-UMA-DTS rev A04