

Unlicensed Mobile Access Solution Data Sheet

- Increased customer satisfaction through better in-home coverage
- Use the same platform for UMA/GAN security as for IWLAN, FemtoCell, PicoCell, MacroCell and other Fixed Mobile Convergence (FMC) networks
- Proven and tested technology
- Differentiated service levels and charging depending on performance provided
- Lowered costs when addressing new markets outside of your current geographical coverage

UMA/GAN – Merging Internet and GSM Networks for Mobile Communication

Unlicensed Mobile Access (UMA), also known as Generic Access Networks (GAN), makes it possible to use both GSM radio and Wi-Fi – wireless broadband connections for mobile communication. This includes voice, SMS/Text Messages, MMS, Internet browsing, or any mobile service available today and in the future.

Customer Experience

Today customers have access to the Internet either at home and/or at work, and more and more often access to a broadband connection. When customers use their mobile phones, they use a separate, GSM radio connection. But with UMA/GAN customers can use both the Internet and GSM network to connect to the same services from a single device. Since the broadband connection is reliable, fast, and always there, it makes perfect sense to use it with a mobile phone.

That is the idea behind UMA/GAN. It lets customers connect their mobile device to GSM services through WLAN. When customers are outside the Wi-Fi connection range they are automatically switched from broadband to GSM. This switch is automatic and seamless, and no different from when driving past different GSM cells – the customer will not even notice the switch.

UMA/GAN Security Challenges

Increasing the Average Revenue per User (ARPU) and seizing the opportunities that a converged fixed/mobile network presents also introduces risks which need to be addressed. As UMA/GAN 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.

Clavister believe that the key to success for any service provider who wants to offer UMA/GAN is to look beyond the standards and investigate threats that have yet to be defined. As UMA/GAN opens up operator's core networks to the Internet, it is necessary that service providers re-evaluate their security infrastructure making sure that the entire network is kept safe even with the new environment.

Management Options

Clavister offers you a wide range of management options to manage your Clavister Security Gateway. Regardless if you choose a centralized management solution or use the built-in web-based management solution, all Clavister Security Gateways Series products and services are managed in the same way.

Clavister InControl

Clavister InControl offers a comprehensive centralized management solution that will assist and help you perform daily tasks faster, easier and more streamlined. Its intuitive user interface and support for task-driven workflow management will guide you through complex and repetitive tasks, thus alleviating the burden of managing large installations.

Clavister Web Management

Clavister Web Management is an easy to use Web-based administration interface, which greatly simplifies product deployment.

Command-Line Interface

All Clavister Security Gateway Series products also support a comprehensive command-line interface. It is a powerful tool for anyone who wants to build custom administration interfaces.

Top Security Risks and Challenges

Intrusion and DoS Attacks from UMA/GAN Subscribers

Subscribers can impose a security threat since they can launch attacks either towards your core network or against other subscribers. The Clavister Security Gateway protects the UMA/GAN network against these threats through a variety of Denial of Services (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

With the core network exposed to the Internet, a potential attack can originate from any unknown source; it does not have to be a subscriber. It should be noted that breaching the core network can be done with a number of 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 DoS attack can be launched against them, this can also be true for a UMA/GAN network.

Clavister Security Gateway protects UMA/GAN networks against attacks from unknown sources on the Internet by facilitating strong authentication and access control mechanism, high performance and strong DoS protection. This means that Clavister Security Gateway ensures that only valid data sent from authenticated UMA/GAN subscribers reaches the core network, everything else is stopped at the network perimeter.

DoS Attacks from GSM/GPRS Access Network to UMA/GAN Network and Subscribers

Attacks towards the UMA/GAN 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 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 Security Gateway, service providers have the same comprehensive protection mechanisms for these types of threats as for the attacks originating from the Internet or from actual UMA/GAN subscribers.

Solution Highlights

For consumers:

- Use your mobile phones for all of your communications
- Excellent in-home coverage
- Seamless switch between Wi-Fi and GSM radio network
- Reduced costs when using 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

Performance and Subscriber Density

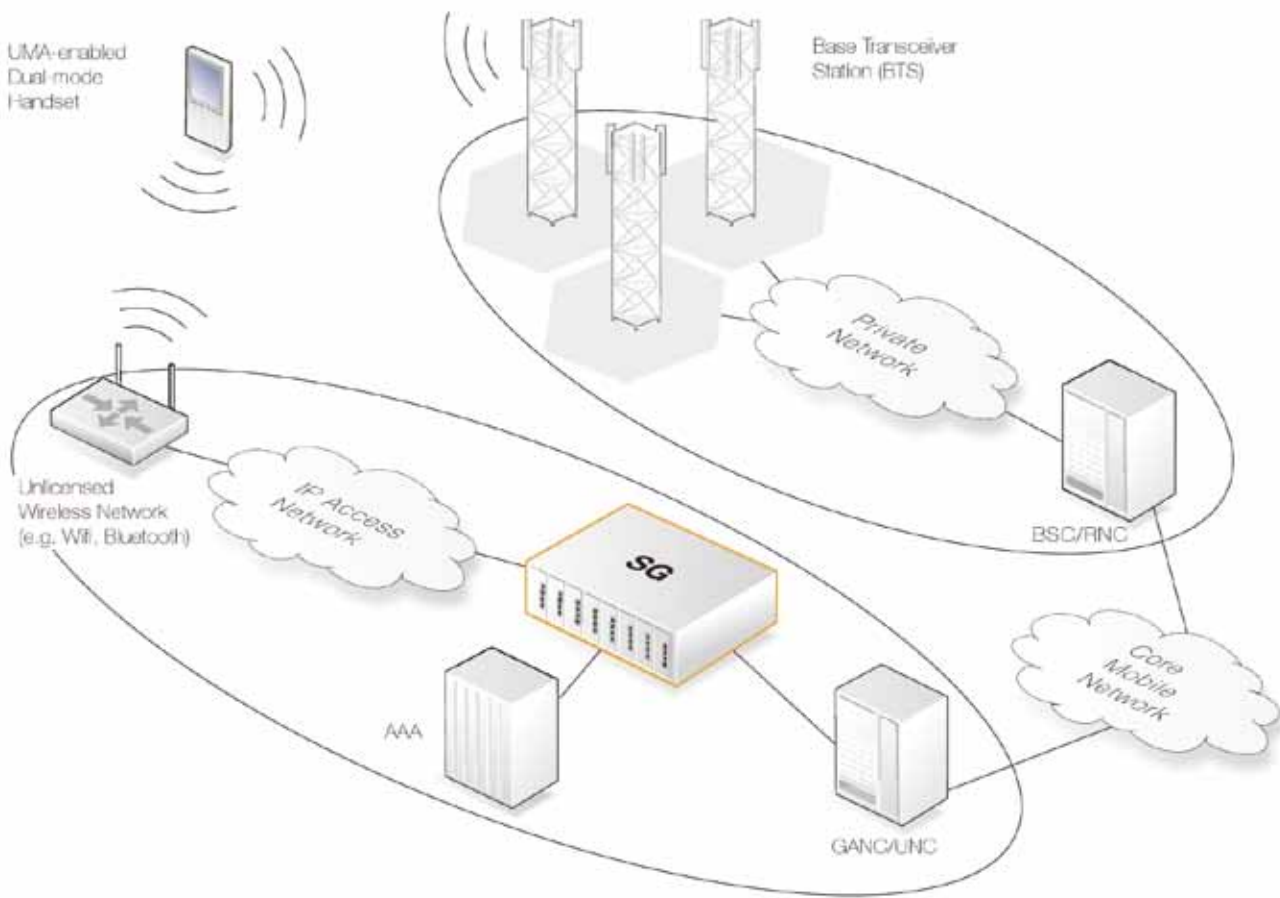
One of the most important aspects of the Clavister Security Gateway 4370 FMC is its extreme performance. With a capacity of up to 7.5 Gbps in firewall performance, 5 million concurrent connections and an astonishing 1.4 million Packets per Second (PPS), the Clavister Security Gateway 4370 FMC delivers an extremely high density of Unlicensed Mobile Access (UMA/GAN) subscribers in a single box.

Equally impressive is the 2.5 Gbps in VPN performance, and 550 000 PPS and 70 000 concurrent VPN tunnels, which further solidify the Clavister Security Gateway 4370 FMC as the market leader for Fixed Mobile Convergence applications.

Thanks to a 1U slim form factor, the density per rack space units is among the world's highest and will not only simplify dimensioning but also saves costs in terms of cost per square feet of allocated space in any Data Center.

Big on Performance - Low on Maintenance

Clavister Service Provisioning Network (CSPN) is a trait that Clavister Security Gateway 4370 FMC share with all other Clavister products. This high-speed network ensures that system administrators are kept informed about new Clavister CorePlus updates and gives them freedom to concentrate on running their network without having to worry about finding the latest Clavister CorePlus updated to install.



Subscriber Integrity

Subscribers are used to share their information in a secure manner, thinking that no-one will intercept and steal what they say or share over the GSM network. Having the information flow over the Internet makes subscribers 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. Clavister Security Gateway includes strong encryption standards like AES 256 bit encryption and EAP/SIM authentication, offering subscriber's full encryption for their data traffic. All communication between mobile devices and the service provider's core network is encrypted and inaccessible even to the most skilled hacker.

Clavister and the UMA/GAN Network

The Clavister 4370 FMC

The ability to cope with high performance in aggressive traffic scenarios, a security gateway solution must cater for strong performance, high scalability and enduring resilience. The Clavister 4370 FMC security gateway is a turnkey appliance designed to function as a UMA/GAN security gateway, an IWLAN Tunnel Terminating gateway or as a security gateway in Telecom Access Networks (Femtocell/Picocell/Macrocell). This makes the Clavister Security Gateway 4370 FMC one of the world's most adapted security systems for Fixed Mobile Convergence networks.

Based on the same award-winning technology found in all Clavister products, the Clavister Security Gateway 4370 FMC has been designed using a modern hardware architecture with cutting edge ASIC acceleration chipsets to ensure high performance of firewall and VPN traffic.

The product comes equipped with six 10BASE-T/100BASE-TX/1000BASE-T interfaces and four SFP (Mini-GBIC) connectors and it is based on a purpose-built and highly optimized hardware platform, which means extreme security, high performance and versatile connectivity.

In addition to cutting-edge performance, the Clavister SG4370 FMC is built for demanding environments with up to two hot-swappable power supplies and three hot-swappable fan modules.

With a Mean Time Between Failure (MTBF) exceeding 324 000 hours*, redundant power supplies and cooling fans, and world-class high availability clustering capabilities, the Clavister SG4370 FMC is the premium choice in even the most demanding UMA/GAN networks with requirements on 99,999% availability and in-service performance.

The main purpose of the Clavister SG4370 FMC 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/GAN 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 SG4370 FMC 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 SG4370 FMC security gateway and the mobile devices are authenticated using public key-based certificates. Thanks to the built-in support for the authentication protocol EAP-SIM and EAP-AKA in the Clavister SG4370 FMC 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 SG4370 FMC 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.

* MTBF value reflects usage with two (2) redundant PSU

Key Benefits with Clavister in UMA/GAN Networks

Security

The Clavister SG4370 FMC security gateway is built to provide supreme security and includes all the necessary threat mitigation technologies in order to ensure a safe UMA/GAN network environment for the subscribers as well as the operator and service providers.

Ability to Support Multiple Service Types in One Platform

The Clavister SG4370 FMC security gateway is able to support UMA/GAN, IWLAN and other services within the same technology platform, thus making it possible to lower both your CAPEX and OPEX.

Verified and Proven

The Clavister SG4370 FMC security gateway meets practically every telecom environment certification standard, such as the ETSI standards and it has been interoperability tested with handsets from Nokia, Philips, Samsung and other vendors.

About Clavister

Since 1997, Clavister has been delivering leading network security solutions, providing commercial advantage to tens of thousands of businesses worldwide. The Clavister family of unified threat management (UTM) appliances and remote access solutions provide innovative and flexible network security with world-class management and control.

Clavister has pioneered virtual network security, and this along with its portfolio of hardware and software appliances gives customers the ultimate choice. Clavister products are backed by Clavister's award-winning support, maintenance and education program.

Headquartered in Sweden, Clavister's solutions are sold through International sales offices, distributors, and resellers throughout EMEA and Asia.

To learn more, visit www.clavister.com.

Clavister Contact Information

General Information
info@clavister.com

Technical Support
support@clavister.com

Partner Information
partner@clavister.com

Sales Information
sales@clavister.com

Ordering Information
order@clavister.com

CLAVISTER®
WE ARE NETWORK SECURITY

Clavister AB, Sjögatan 6 J, SE-891 60 Örnsköldsvik, Sweden
Phone: +46 (0)660 29 92 00 | Fax: +46 (0)660 122 50 | Web: www.clavister.com | Email: info@clavister.com