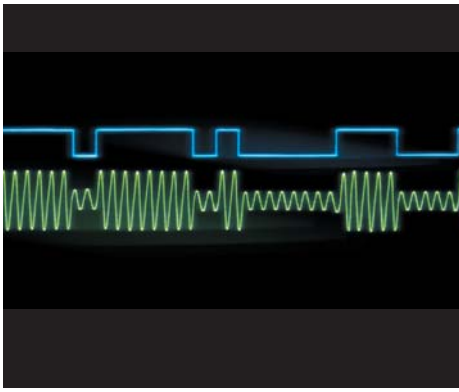
Symmetricom

Why Convert to a SAASM based Global Positioning System (GPS)?



WHITE PAPER

Why Convert to a SAASM based Global Positioning System (GPS)?

The views expressed in this brochure are those of Symmetricom and do not necessarily reflect the official policy or position of the Navstar GPS Joint Program Office, the Air Force, the Department of Defense, or the U.S. Government.

In 1998 The Joint Chiefs of Staff selected SAASM (Selective Availability Anti-Spoofing Module) as the security architecture to bring the Global Positioning System (GPS) to the next level and issued the following mandate: As of 1 October 2006, all newly-fielded Department of Defense GPS systems will use SAASM-compliant Precise Positioning System (PPS) devices. Procurement of non-SAASM GPS user-equipment will be disallowed unless wavered.

Despite a government mandate requiring all newly-fielded Department of Defense GPS systems to use SAASM-compliant Precise Positioning System (PPS) devices by October of 2006, many military groups and other federal agencies continue to purchase receivers without SAASM compliance. Military users purchasing a GPS receiver without SAASM, or anyone who waits until the October 2006 deadline is taking a security risk. Standard GPS service could be denied at any time via warfare tactics such as jamming or spoofing, and if this occurs, GPS receivers without SAASM will find it difficult to correct the situation quickly -- the process to acquire SAASM-compliant receivers requires significant time for authorization and processing. We are going to attempt to explain what SAASM is all about, why it's important to GPS receiver end-users, and why those who deploy non-SAASM receivers are putting their organization at risk right now – even though the deadline is less than a year away.

The need for improving GPS security came to the forefront even more so in December 2004 in an announcement by President George W. Bush in which he issued the Space-Based Positioning, Navigation and Timing (PNT) policy. The PNT policy authorizes the improvement of the United States' capabilities to deny hostile use of any space-based positioning, navigation, and timing services without unduly disrupting civil and commercial access. In the policy, the President specifically directed the Secretary of Defense to develop and maintain navigation warfare capabilities required to effectively utilize the Global Positioning System services in the event of jamming or other interference by adversaries.

This announcement underscores the fact that the federal government is increasing the level of urgency to safeguard GPS. The pressure for government agencies and military units to convert to SAASM-compliant GPS receivers is bound to also increase dramatically. Along with the selection of SAASM by the Joint Chiefs, the writing on the wall is clear: All defense agencies should begin converting to SAASM GPS receivers.

SAASM Explained

To understand the risks and why it's important to deploy SAASM-compliant GPS receivers as soon as possible, a brief recap of GPS and SAASM will help. GPS has come to play a significant role in our everyday tasks during the past decade. GPS makes it possible to pinpoint the precise location of any person or place, anywhere in the world. It helps with everyday things such as how to drive our vehicles from Point A to Point B via on-board navigation systems.

GPS has also become critically important to the military to identify the whereabouts of friends and foes, and it plays a crucial role in the success of military operations by providing precise time and frequency to communication systems. This allows military units to synchronize movements and ensure they communicate over secure frequency bandwidths that change on an irregular basis to avoid detection by the enemy.

Since GPS relies on low-powered frequency waves traveling from satellites to GPS receivers on the ground, the technology also lends itself to intentional jamming by enemies as well as unintentional or intentional jamming by allies. For example, the civil, course acquisition (C/A) code signal may be intentionally jammed by the U.S. and other allies to allow only SAASM and legacy P(Y) receivers to access GPS. GPS is also susceptible to enemy spoofing — the deliberate attempt to mimic a legitimate signal and introduce erroneous position and time information.

To combat this situation, the U.S. government launched a program in the 1990s referred to as SAASM. SAASM deploys anti-spoofing measures using cryptography to protect authorized users from false satellite signals generated by an enemy. To understand the reasons for SAASM, it helps to have an understanding of the components of the GPS system used by people, organizations and governments throughout the world.

GPS Mini-History

Through a satellite navigation system, GPS provides positioning and clock time to GPS receivers on the earth. Conceptualized in 1973, the first GPS satellite was launched in 1978, and in 1995 the system became fully operational. Today (May 2006) the system consists of 29 satellites orbiting 12,500 miles above the Earth.

GPS was originally intended as a military force enhancement system but now serves dual purposes: GPS has evolved to improve not only military security but also the accuracy of the position, velocity and time of any object on earth — securely to military users and freely to civil users. GPS does this by offering two positioning services: PPS (Precise Positioning Service) for authorized military users only, and SPS (Standard Positioning Service) for everyone includ-

ing the military. SPS utilizes a simpler, unprotected coarse acquisition (C/A) code which is openly available to commercial, civil and military users.

The GPS signals are transmitted on two L-band frequencies: L1 (1575.42 MHz) and L2 (1227.60 MHz). The SPS service is provided on L1 and the PPS service on both L1 and L2.

The Department of Defense (DoD) relies upon GPS as the primary source for position, navigation, time, and time-synchronization. Therefore the GPS network was also built to allow for the deployment of security measures. Selective Availability (SA) is a security technique that involves the introduction of intentional errors into the GPS signal which denies full system accuracy to SPS users. On 2 May 2000, however, the effects of SA were set to zero and it appears unlikely SA will ever be set higher. But the potential still exists, and this would degrade the accuracy of GPS for SPS users. Anti-spoofing (A-S) utilizes cryptography to protect a GPS PPS receiver from receiving false satellite signals generated by an adversary.

The SAASM Manufacturing and Integration Process

The detailed regulations that the U.S. government has applied to the SAASM manufacturing process clearly demonstrate how serious GPS security has become and the need for immediate conversion to SAASM-compliant receivers.

Manufacturers of SAASM GPS receiver modules and the products that they are integrated into, referred to as PPS Host Application Equipment (HAE), must work closely with the Key Data Processor (KDP) Loading and Installation Facility (KLIF) under strict guidelines. After manufacturing the SAASM unit, the GPS receiver manufacturer ships the SAASM hardware to the KLIF for the loading of the KDP (crypto) software. After return of the SAASM device to the manufacturer, production test is completed and the unit is ready for sale to JPO approved customers.

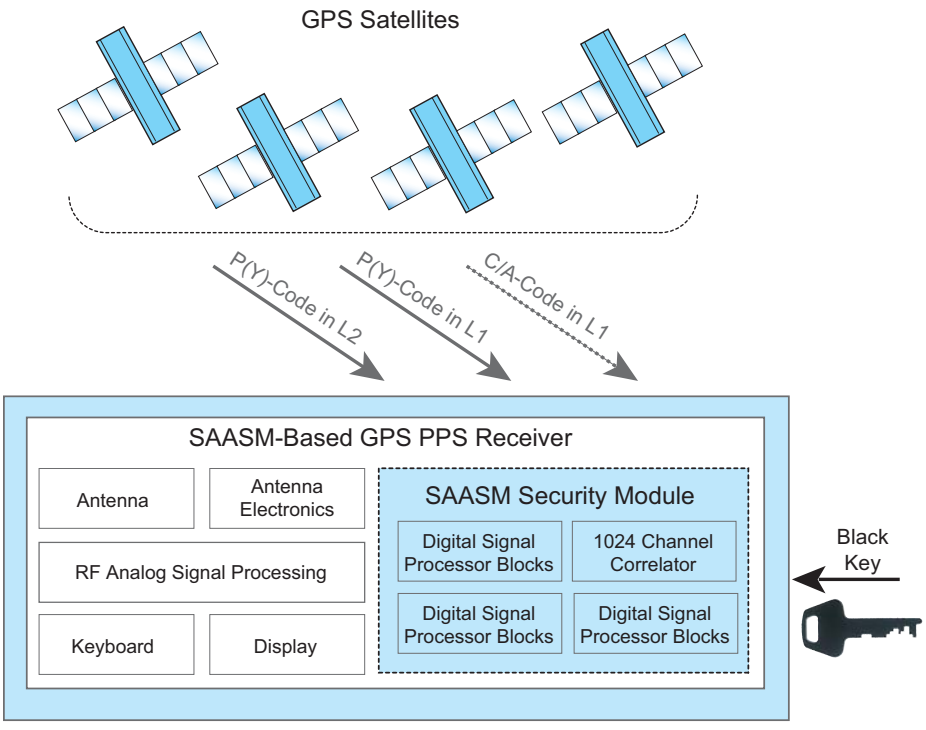
XLi SAASM

SAASM GPS Receiver Manufacturing Process and Integration into PPS HAE

SAASM receivers support two key types to decrypt anti-spoofing and remove selective availability: Physical-form red keys are classified, and distribution is closely protected. Newer, black keys, on the other hand, are unclassified. They can be distributed and loaded electronically although paper tape distribution is still common. The decryption of the key only takes place within the secure SAASM module. Black keys may be renewable in the future via over-the-air-rekeying (OTAR). Black keys make sense because they solve key distribution problems and are useless to the enemy since they are encrypted. The DoD recognizes the security, delivery, and cost savings associated with black keys and wants users to transition from red to black key usage as soon as possible.

To ensure security of the classified technology within a SAASM receiver and to preclude unauthorized procurement, the Navstar GPS Joint Program Office (JPO) at the Space and Missile Systems Center at Los Angeles AFB ensures compliance to DoD security requirements. All developers, integrators and users of SAASM GPS must be JPO authorized.

SAASM developers and manufacturers must also meet several strict requirements. This includes securing a COMSEC (Communications Security) account, a KLIF account and undergoing a complete JPO design-review process. Developers and manufacturers also have to prove they are free of foreign ownership, control and influence, and that they have a



facility security clearance issued by the Defense Security Service (DSS).

Military end-users must receive authorization from the JPO to procure SAASM-based devices. When proper authorization occurs, the JPO issues a formal letter so that authorized manufacturers of SAASM GPS receivers will know authorization has formally been granted.

Benefits of SAASM GPS Receivers

By purchasing a SAASM receiver now, authorized users comply with the DoD GPS security architecture and possess the most secure GPS technology to enhance their ability to use precise positioning, velocity, and time in all environments. SAASM-based GPS receivers have the capability to directly acquire the encrypted, military GPS-code and no longer have to depend on the often-jammed civil GPS code.

The need for deploying a SAASM receiver could become critical at any moment since access to the standard GPS service (SPS) could be denied via warfare tactics focused on local and regional denial (jamming) of the civil code within an area of conflict. In addition to losing access to the signal, upgrading GPS SPS based systems to SAASM is non-trivial since the process to acquire product and distribute the keys that can decrypt coded signals requires significant time for authorization and processing.

Without a doubt, those military and agencies that wait until the SAASM deadline approaches in October 2006 are taking a security risk. If an enemy source attempts to jam or spoof the GPS signal, users of non-SAASM receivers could lose all of their GPS capabilities.

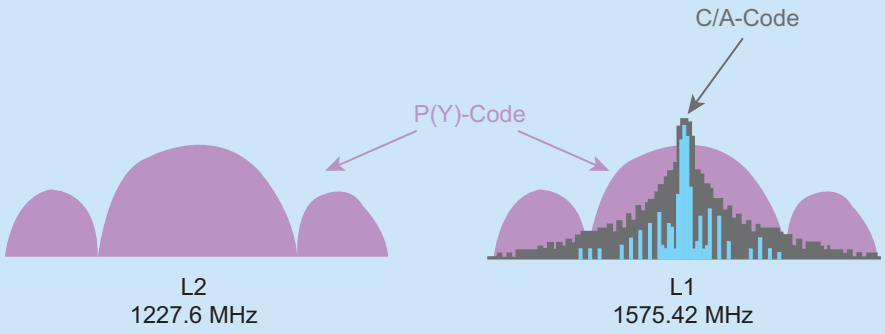
For more information please contact Ron Holm at rholm@symmetricom.com or if you would like information on our SAASM receivers please visit: http://www.symmttm.com/products_gps_time_code_instrumentation.asp

Spoofing and Encrypted Coding

GPS spoofing involves the intentional sending of a fake GPS signal by a simulated satellite mimicking a legitimate GPS satellite. Spoofing produces a false reading in GPS Standard Positioning System (SPS) devices and if properly executed can introduce position and timing errors disrupting navigation and communication systems.

The low power GPS satellite transmitters deliver extremely low strength signals (equivalent to 0.0000000000000001 watt) to earth-based GPS receivers which are vulnerable to jamming and spoofing. Jammers are inexpensive, unintelligent, electronic devices that merely produce a higher power "blocking" signal at the GPS frequency. Jamming is disruptive but usually detected by the GPS receiver as it stops tracking satellites. Spoofing requires more sophisticated, expensive equipment. Spoofing poses a particular security risk as it is often undetected by a GPS SPS device.

The key to preventing spoofing is to deploy a GPS receiver that can acquire encrypted GPS signals referred to as P(Y) coded signals, which are more robust and jam resistant. GPS satellites broadcast two signals: a civilian, unencrypted signal (referred to as C/A) that all GPS receivers can access; and the military encrypted coded signal P(Y). GPS devices in compliance with SAASM can receive and decrypt the P(Y) code (when keyed) which authenticates the signal originated from the GPS satellites.



Symmetricom

SYMMETRICOM, INC.
2300 Orchard Parkway
San Jose, California
95131-1017
tel: 408.433.0910
fax: 408.428.7896
info@symmetricom.com
www.symmetricom.com