

CIVIL ACCESS TO THE PRECISE POSITIONING SERVICE OF THE NAVSTAR
GLOBAL POSITIONING SYSTEM

Michael J. Ellett

Navstar GPS Joint Program Office
Systems Engineering Directorate,
Los Angeles, AFS, CA

Abstract

US government policy is established and procedures are being formulated to direct the implementation of techniques providing limited civil access to full GPS accuracy. The results of these efforts balance the conflicting needs of civil GPS navigation and positioning against national security requirements. Granting this access will require sufficient and demonstrable user need, must clearly provide for both national and security interests, and may lead to the imposition of a user service charge. This access will only apply to Precise Positioning Service configured, code-tracking GPS receivers.

Introduction

The NAVSTAR Global Positioning System (GPS) is the second space-based navigation positioning system to be developed by the United States. The GPS will enter the operational phase within the next seven years. Like its predecessor, the Navy Navigation Satellite System, commonly called Transit, the GPS is principally intended for military applications. However, unlike Transit, it was recognized from inception that GPS would have a collateral mission in and greatly contribute to navigation, positioning, and time transfer in both the public and private civil sectors.

It was also recognized that allowing uncontrolled access to the GPS could provide an opportunity for hostile forces to use the GPS in ways which compromise US interests. The national security component of this concern led to the parallel developments of Selective Availability (SA) and Anti-Spoofing (A-S). SA is intended to deny use of the GPS in the real-time environment at the advertised full system performance of 16 meters spherical error probable (SEP). A-S was developed to increase the GPS resistance to intelligent jamming in the battlefield environment.

Code tracking receivers come in two basic types: Coarse/Acquisition (C/A) code and Precision (P) code receivers. The Standard Positioning Service (SPS) which will be broadcast in the clear, refers to the C/A code tracking receivers which are cur-

rently restricted to data on the L₁ carrier frequency. The SPS performance will be maintained at equal-to-or-better-than 100 meters 2 times distance root mean square ($2 d_{rms}$) during peace-time. The Precise Positioning Service (PPS) which will be encrypted, refers to the P-code capable receivers which track precision codes on both L₁ and L₂ carrier frequencies. To achieve the PPS performance of 16 meters SEP in real-time, the user will require the capability to recover the appropriate correction information for SA and A-S as implemented by the control and space segments of the GPS. Although differential GPS may approach the PPS performance in the immediate environment of a master station, the user will be dependent on a single frequency, C/A code-tracking receiver; in addition to a communications link between the master station and the mobile receiver; the overall reliability, integrity, and the coverage limitations of the differential GPS. Stand-alone GPS receivers that will provide the full system performance in real-time will require cryptographic technology, must be code-tracking, and will make use of the PPS.

The purpose of this paper is to present information related to civil access to the PPS. The author, except where referring to an official policy or document, is presenting his opinion and perspective on some of the relevant issues. These issues will impact the form and substance of the program being defined to provide for the civil access. This paper will compare differing concepts, examine existing policy and implementation options, present some qualification requirements for user access, and specify a user self-test to determine whether PPS is suitable for an individual user's needs.

Evolution of GPS Civil Access Policy:

Discussion and debate on how to provide for civil access to the GPS has been an issue within the DOD since the mid-1970's. The DOD has produced two different concepts on how this can be provided. The first concept was called "User Charge" (UC) and is no longer considered a viable approach. The second concept, which is still being formulated, can be called "PPS Civil Access".

UC was an attempt to define a comprehensive methodology to control civil use of the GPS. It evolved within the DOD in the 1979-1981 period and provided for a control mechanism effective on all code-tracking receivers, both civil and military. An access charge would have been imposed on all users except for those with "official US user" status. The core of the DOD UC concept was:

"To make the NAVSTAR GPS available on a user fee basis to both governmental and civilian users in a secure manner that will provide for the recouping of as much of the research and development (R&D), acquisition, and operating costs of the GPS as is deemed feasible".

Precedent existed for such a cost recovery approach in both the public and private sectors; was supported by requirements in US law and DOD regulations; and was reinforced by a Congressional requirement on the DOD to proceed with the UC approach. The DOD originally intended to apply the UC concept to the PPS only, but found that the estimate of the potential PPS user population was too small to satisfy the needs of cost recovery. Subsequently, the SPS user population was included into UC planning.

With both the SPS and the PPS populations drafted to provide for cost recovery, an encryption of the Navigation Message (NM) was chosen as the method to deny access to "unauthorized" users. The NM is digitally modulated on both the P and C/A codes on the L₁ carrier frequency and on the P code on the L₂ carrier frequency. This method works equally well on the SPS and the PPS. All code-tracking receivers require knowledge of the position and of the time of the transmissions from the satellites being tracked to solve for the user's position. Without access to the NM which contains part of this information, the code-tracking receiver must depend on externally generated position and time information to arrive at the local solution.

In 1984 resistance to the UC concept peaked and the following arguments were put forth as reasons to review the policy. The UC program:

- * would create a large bureaucracy and require significant logistic support,
- * would consume more financial resources than it could recover,
- * would inhibit civil acceptance of the GPS,
- * and was not consistent with contemporary White House and Congressional positions on civilian use and access to GPS.

In addition, the techniques proposed for UC were not capable of preventing circumvention of the UC process by differential and/or codeless receiver methods.

In May 1984, the DOD presented a report on "User Charges for the GPS" to the Senate and the House Committee on the Armed Services. The report recommended that Congress remove the requirement levied upon the DOD to implement the cost recovery program. Congress subsequently agreed but with the stipulation that the requirement could be reimposed upon the GPS in the future if Congress sees fit. Since the autumn of 1984, all UC efforts have ceased at NAVSTAR GPS Joint Program Office (JPO).

With the demise of the UC concept, the issue of civil access to the GPS was, once again, undefined. However, several events have occurred which indicate the direction the DOD is going in the evolution of the 'new' civil access program. Some of the more important features are as follows:

- * The DOD and the DOT agreed in July 1983, on minimum performance for the SPS during peacetime. This minimum

performance boundary would be set to support the non-precision approach requirements of the FAA for use of the GPS. The performance of the GPS will be equal-to-or-better than 100 meters 2 d_{rms}.

- * The Korean Airline (KAL) 007 disaster prompted the White House and Congress to increased efforts toward assuring GPS availability to civil users worldwide.
- * A Comprehensive GPS User Policy (revised) was approved by the Deputy Secretary of Defense on 22 May 1985. This document specifically states the policy which authorizes limited civil use of the PPS.
- * The DOD Position/Navigation (POS/NAV) Working Group has been developing the plan for the implementation of the announced policy of 22 May 1985.

The evolving new program for the civil access to the GPS will differ markedly from the previous UC in that:

- * No unique encryption of the NM will be required.
- * The program will be limited to the PPS.
- * There will be no cost recovery provision as defined under UC, however, there will be a charge to support the administration of the PPS access program.
- * Access to the PPS will be given only after significant justification has been provided.

The PPS Access Request Cycle:

Potential civil users of the PPS will be required to complete and submit an application of request for PPS access to the US government. The approval or denial of the application will be made by the Assistant Secretary of Defense (ASD) for Command, Control, Communications, and Intelligence (C³I). ASD/C³I will review the recommendation(s) presented to him by other members of an interagency/interdepartmental panel, presumably at the POS/NAV level, and then, make his determination. Although the specifics are ill-defined at this time, each application would be reviewed by the individual members of the evaluation panel. Clearly, membership on such a panel will have much wider ranging interests than just the DOD internal perspective. It is expected that each evaluation may require a few months to process.

The PPS civil access will be administered by a Central Control Office (CCO) which will be directly involved in the task of providing personnel, equipment, and/or information to the user to facilitate the PPS Access. All applicants would apply directly through the CCO for consideration of access approval. Once a decision has been rendered by ASD/C³I, the CCO would manage the notification process for all applicants. Applications which have been turned down should be returned or the applicant by the CCO in a timely fashion with the reason for denial and the recourse the applicant may have, if any.

The instructions accompanying each application form should

contain sufficient information for an applicant so as to insure high likelihood of success in the preparation process. Where possible some guidelines should be included to help the applicant frame his arguments and supporting evidence. In particular, guidelines could be made available which would both clearly define controlling criteria and the requisite user justification for the PPS access in the technical arena, possibly in the national interest category, and where obvious economic considerations prevail. Expect few guidelines, if any, in the area of military and security interests.

It is possible that a non-reimbursable application fee may be charged to cover the costs associated with the handling, evaluation, and notification processes attendant with each application. The application forms, instructions, and the notice of associated program fees will receive distribution through official channels; although the US government will not encourage the civil use of the PPS.

Principle Validation Criteria and User Self Assessment:

The approval of any application can be said to hinge on the following three DOD specified criteria:

- * The granting of the PPS access must be in the US national interest.
- * Equivalent accuracy cannot be achieved by other means.
- * The security of the GPS must be protected.

The author feels that the above criteria can be further decomposed into the following categories:

- * Military applications/implications
- * US national and security interests
- * Technical merit
- * Political and economic considerations

Such a decomposition would be inline with the expected interests of the members of the interagency panel which would review each application. US national interests are complex and appear to be contradictory at times. It is likely that unless the normal applicant can see a direct benefit to the US in granting him access to the PPS and articulate that benefit through cause and effect, his request for access will be denied. The applicant may have a large impact on the access evaluation by the way he states the justification for access on political, economic, and technical grounds. Concentrating in the technical arena, the applicant should:

- * Explain in depth his intended use of PPS access
- * Provide a detailed scenario of the application of the PPS capable equipment
- * Explain what other positioning/navigation techniques/-system might be considered as alternatives to the PPS,

and why, on a point-by-point basis, each alternative is inadequate or unsuitable, along with what critical limitation(s) of each alternative makes it unsuitable.

All supporting arguments or evidence that are of a political or economic nature should be separately examined and defended. In considering security criteria, there are two separate positions to be examined: The position of the US Government which will be addressed in a section called "US Government Concerns Related to PPS Civil Access" and the position of the civil user. Each applicant must be aware that he will be required to commit and guarantee by an as-yet-to-be-determined means and to an as-yet-to-be-determined extent of real risk, that his part in providing for the security of the GPS can be assured to the US Government. The stronger that the verifiable assurance can be made and the level of risk supported, the more confident the US Government control of PPS capable receiver operation by the user.

So, the potential user should attempt to assess whether or not he can put forth valid and justifiable arguments and document them before entering the application process. The applicant should turn the principal criteria into questions which he can positively answer in his particular case, support that answer with sound reasons and evidence, and be prepared to support whatever security restriction and use provisions that may be imposed in a PPS Access agreement.

US Government Concerns Related to Civil Access:

Since the beginning of planning for civil access to the PPS, the most difficult problem to solve has been providing for adequate system security. The GPS is first and foremost a navigation/positioning system intended to confer a military advantage to the United States and its allies where national security interests are at stake. With this perspective, guiding criteria can be articulated which will frame the bounds within which PPS civil access will be permitted. The criteria include the following:

- * The DOD will retain ultimate approval authority on each access request.
- * Any method which may be chosen to provide access will conform to existing and/or yet-to-be-defined DOD security policy, doctrine, and regulations.
- * Any potential civil compromise in the system security must not compromise the military utility of the GPS.
- * Any civil access program must include a plan to minimize the operating costs associated with its administration.
- * The PPS Civil Access program must not put the US Government in the position of competing with private industry.

The civil access program can be said to begin where the current military receiver development leaves off. The current generation and configuration of military receivers are, gener-

ally, PPS capable. These sets are required to provide the military user with full GPS system being implemented. Existing security regulations require that these sets, when in an authorized mode and when in operation, be classified. It appears that the DOD considers this classification penalty not unreasonable and can be tolerated in the military environment. There are no laws or regulations which currently exist that would permit use of classified equipment or information in the private civil environment. With this point in mind, it is clear that any PPS civil access program must surmount the classification/security issue to be viable.

There are at this time two competing philosophies on how to achieve this goal. For the purpose of simplicity, the first approach, which represents the existing SA and A-S implementation in the military user equipment, shall be called the "software solution" (SS); the second approach, which represents a change in how to achieve adequate SA and A-S related security in the user equipment, shall be called the "hardware solution" (HS). For practical purposes the objective of the HS is to overcome the classification requirement currently imposed on PPS receivers operating in an SA and A-S environment. A HS could provide for unclassified PPS receiver operations.

Each solution technique, whether SS or HS, can be used to construct a set of scenarios which would characterize the extremes of how the PPS might be made available to civil users. Each set of scenarios scales the varying levels of US government involvement in actual operations of PPS capable receivers. Rather than present scenarios, the characteristics common to a family of scenarios representing the SS and HS, can be compared. The characteristics related to the SS have the following in common:

- * Actual receiver operations will remain under the control of the US Government or its assigned agents.
- * Civil users would receive the product of the receiver operation through an authorized operator in near/real-time and through the PPS organization where post-processing is involved.
- * PPS receivers would be the property of the US government and/or its assigned representative organization.
- * Users would be provided the PPS service rather than having hands-on control of the receiver during operations.
- * Both the users need for the service and locations of the receiver operations would require security approval.
- * The SS requires in-depth involvement by the US government and its agents in the physical operation of providing the actual service. This could preclude making the PPS available to civil users within any reasonable cost to either the user or the US government.

The characteristics of the family of scenarios related to the HS

have the following in common:

- * Actual receiver operations may be under the control of the civil user.
- * The receiver would not require physical protection and a US government agent would not be required for physical control. Accountability and control may be the responsibility of the user and there would be legal penalties applied to a user who fails to abide by contractual requirements.
- * Only the user purpose and geographical location would need to be scrutinized for security purposes, not the site of the operation of the set.
- * The HS minimizes the involvement of the US government in actual PPS receiver operations in the civil environment. The HS reduces the cost of providing the PPS to the civilian community.

It is clear that, as government involvement increases in providing the service to the civil side, the cost to the civil user and to the US government also increases, and the utility of the PPS to the civil user is diminished. Where cost-effectiveness can be played against adequate security provisions, the HS technique appears to be the best choice. Where a comparison of the relative ease of use of the service is concerned, the HS technique also appears to be the winner. So, why is there any question as to what path to follow? Simply put, as yet there doesn't exist in US law or DOD security regulations a basis to authorize and permit the use of classified equipment and information for "private" purposes on the one hand; and, on the other hand, a HS has yet to be demonstrated to the satisfaction of the security interest of the US Government. Resolution of either of these will take time; but work is progressing in both areas.

Conclusion:

The DOD is in the process of formulating a program to provide the limited civil access to the Precise Positioning Service (PPS). Unlike the previous concept, User Charge, this program will not include the SPS, will not require a unique encryption technique, nor be based upon the idea that charges can provide for full cost recovery of the GPS. Previously released DOD policy clearly states that PPS access will be provided to the civil community only if applicants can provide a demonstrable need, if the granting of the access will be in the US national interest, and if the security of the GPS can be adequate. The PPS civil access will require a fee payment by the user to help offset the cost of administering the access program.

QUESTIONS AND ANSWERS

MR. ELLETT: I left a package of material outside as handouts. Within that handout is a letter requesting solicitation on your comments on GPS Civil Access. It is important that those of you who anticipate applying for that access respond to the survey. Send you responses to Colonel Baker at the Pentagon. If we don't get enough responses, the Civil Access Program will be put away. It will not be resurrected unless the civil community comes in with a very big stick.