AHO Approach to Shared UPN for S100 Security Scheme Project Team

Background

1. The AHO has operated an ENC service in one form or another for National and Government users since approximately 2001. The current iteration, AusENC, was released to the market in 2011 to satisfy national carriage requirements of Domestic Commercial Vessels and is in wide use by local Ports/Pilots/Government a range of other users.
2. AusENC is provided to users in S63 format only; there is no S57 service available for navigation.
3. The AHO also produces a desktop chart viewer, AusChartViewer, which is capable of reading S63, HCRF, GeoTiff and other spatial formats. This software has the capability to use a network dongle and share a single UPN within a specified number of installations within an organisation (programmed into the dongle).
4. The AHO was approached by Qastor to permit the use of a shared UPN by users of their PPU software that is in wide use by Australian Ports and Pilots.

Shared UPN Approach

5. AHO wishes to permit users of AusENC to use shared/duplicated UPN's and this permission is limited to AusENC only.
6. AusChartViewer Network Dongle:
    a. As a matter of policy, network dongles are only supplied to other Government agencies and are programmed up to an agreed user limit.
    b. The AHO has arrangements with each agency using a network dongle that sets the T&C. Of specific relevance to the PT, network dongle users are not permitted to use ENC data from any other source other than AusENC.
7. Qastor QPS:
    a. In broad terms, the Qastor QPS system uses a shore based administration tool (Qastor ENC Manager) to convert S.63 into an internal format (QNC) suitable for use in QPS. QPS and its ENC Manager Tool has the capability to use a single shared UPN across a corporate installation of the software.
    b. This approach is said to simplify chart loading for organisations with a significant number of users and is said to reduce errors when relying upon individual pilots to keep their charts up to date.
    c. The AHO is content to permit this use of AusENC in a controlled manner.
8. In most cases, the AHO will have a direct agreement with Ports and Pilot services regarding exchange of products and data. These are binding agreements that set a clear framework for cooperation and exchange of material.
9. When agreeing to the installation of a shared UPN the AHO asserts the following additional conditions:
    a. Using the shared UPN <organisation> commits to only sourcing charts from the AHO using this shared UPN unless <organisation> discloses the shared UPN arrangement to the other data providers and obtain their written consent. For complete clarity, AHO is only giving permission for the shared UPN to be used for viewing AusENC and not any other ENC service from any other supplier.
    b. <organisation> will subscribe to, and where relevant pay for, the correct number of systems. To enable the AHO to do so, <organisation> must provide the names of the

pilots/vessels using the service or a specific identifier per software installation and the location of the system.

c. The single UPN is specific to <organisation> and use of that UPN is limited to <organisation>. In the case that a user / pilot moves organisation and takes their equipment, the AHO must be notified (and steps should be taken to revert the system to the standard UPN).

10. This approach is in use in a significant percentage of Australian Ports. There are no known reports of Pilots using out of date charts when using this approach. Anecdotally, through our technical support team, there are reports of out of data ENC data causing confusion in users of other systems/approaches.

Conclusion

11. The AHO manages shared UPNs amongst users of its service with a set of binding terms and conditions and reporting down to the user level.
12. Duplicate or shared UPN's assist users by providing a simpler path to chart installation by providing a single set of permits across an organisation, systems or vessel. This should be supported, in a controlled manner.
13. S100 Part 15 does not currently permit duplication of HW_ID and therefore generation of shared UPN.
14. The examples provided are all non-ECDIS. It seems quite conceivable, given the current wording of S63, that there are duplicated UPNs in use in ECDIS and supported by other data servers, OEM's or their resellers. Visibility and application of this is uncertain.
15. There is a need to look at the operation of networked dongles and to agree an approach. Networked dongles (physical or soft-lock) maybe used in shore based viewing systems, GIS systems and on-board vessels.

Recommendations

16. Agree that there are legitimate use cases for shared/duplicate UPN and that these need to be closely managed to ensure that a safe approach is implemented that is in conformance with data providers IP and revenue considerations.
17. Recommend an approach that entails a mixture of legally binding and enforceable commitments and reporting from OEM's and other participants in the security scheme seeking to provide shared UPNs.
18. This approach could look like:
    a. An annex to the IHO agreement setting out the obligations of the OEM when providing systems with shared UPNs.
    b. Disclosure obligations (to disclose shared UPN to Data Server). There maybe a technical solution to this. Consider if it would be possible for manufacturers to be provided additional system type (network dongle or other shared UPN) specific M_KEY for that OEM that is linked to the agreement above and can be used only for shared/duplicated UPNs provided to end users.
    c. If this type of approach is taken, it will then be up to each Data Server if they wish to have this M_KEY in their system and therefore support, with controls, the use of networked dongles or other variations of shared/duplicated UPNs.

   d. Reporting obligations (to both the IHO and Data Servers / Providers). There maybe a technical solution to reporting obligations that builds upon the suggestion above. S-100 15-4.4 states: "The manufacturer must provide a secure mechanism within their software systems for uniquely identifying each end user installation ". This mechanism if implemented could provide logs for reporting.

19. Note this paper.