INTERNATIONAL MARITIME ORGANIZATION

IMO

E

SUB-COMMITTEE ON STANDARDS OF TRAINING AND WATCHKEEPING
34th session
Agenda item 5

STW 34/5/2
20 December 2002
Original: ENGLISH

UNLAWFUL PRACTICES ASSOCIATED WITH CERTIFICATES OF COMPETENCY

The considerations of central databases and smart cards

Submitted by the ICFTU

SUMMARY

Executive summary:	This paper addresses the problems of smart cards and central databases
Action to be taken:	Paragraph 11
Related documents:	STW 33/6, STW 33/6/1, STCW 95/Circ.1/Rev.3, MSC 74/6/2

Background

1 The resolution of the problem of fraudulently issued and counterfeit certificates has made little progress since the presentation at STW 33 of the report on "Unlawful Practices Associated with Certificates of Competency" undertaken by the Seafarers' International Research Centre (SIRC). Whilst many countries spoke at length of taking strong action to eliminate these practices, others played down the conclusions and undermined the credibility of the report. A circular, STCW 95/Circ.1/Rev.3, was issued in March 2002 by the IMO to all member States with respect to the verification of validity and authenticity of certificates and requested notification by States of any fraudulently issued certificates identified. The IMO has, it would appear, received little response. Although the Paris Memorandum of Understanding on Port State Control has identified initially over one third of certificates that do not comply with STCW 95 requirements, little information on counterfeit and fraudulently issued certificates has been identified. This circular also dealt with the invitation of the Sub-Committee to develop a website as a focal point for administrations.

Considerations

2 Positive action has been taken by a number of member States including Cyprus, which has been reported to have discovered a considerable number of forged certificates. The media report states, '*Cyprus is refusing to recognise certificates presented from Georgia and Ukraine held by seafarers who are not nationals of those countries*'. At the same time the Cyprus administration is demanding full background assessments before accepting certificates issued by other administrations to foreign nationals and has identified other nations responsible for 'inappropriate certificates'.

3 It is understood from the media reports that this position was taken by the Cypriot administration after it was unable to verify certificates largely issued by Panama, Liberia and the Marshall Islands. At the same time the Marshall Islands stated that 53,000 certificates will be issued by the end of this year and, with modern technology, it can be sure to detect those that are fraudulent or counterfeit. In fact it is extremely difficult to detect fraudulently issued certificates and once these have been entered into a database without full auditing they are, to a large extent, validated.

Central Databases

4 Cyprus has again called for a global database, as was proposed by the SIRC report, which would include an effective international audit of administrations and training institutions. There is no doubt that the endorsement process under I/10 has put a large workload on flag States, which an effective central database would reduce. However, we may wish to question the credibility of any certificate issued by flag States that have neither the capacity nor the ability to carry out background checks on the underlying certificates before they issue any endorsement. Malta stated it has a similar policy to Cyprus and Bermuda has stated that so far it has identified only 20-30 cases of forged certificates or certificates that did not appear to be correct. Currently these details do not appear to be registered with the IMO as per STCW 95/Circ.1 Rev 3. The fact remains that, unless a full audit can be made of every certificate prior to entry on a database, we are only perpetuating the fraud and for any central database to be credible it must be independent of financial and political considerations, protect the individual's rights and be corruption free.

5 The UK has called for a pro-active approach to developing and adopting international quality standards for counter-forgery measures and an agreed standard for Administrations' databases. There has been reference to past discussions on the maintenance of a register of certificates and to the possibility of making the storage of data electronically a Convention requirement.

6 Whilst this may be initially expensive, based on a voluntary involvement, it could ultimately save costs for Administrations and provide an internationally accepted, IMO numbered, reliably audited and easily transportable document, simply verified and respected by owners, flags and seafarers. If STCW relevant information including personal medical details required for the certificate are to be stored in any central database, the issues of data protection and auditing standards may be best covered by a suitable Convention.

Smart Cards

7 Any person who possesses a bankcard is aware of some of a smart card's abilities. In fact the technology is available and the potential for smart cards is extensive. Integrated circuit chips (ICC) on smart cards are more durable than magnetic strips, can retain far greater memory and consolidate information across multiple systems. The cost of smart cards is relatively small — approximately US$10 per card — however the technology required to facilitate them is neither cheap nor universally available. Organisations need a secure method to identify and authenticate a seafarer's information while ensuring confidentiality of each individual's personal information. Smart cards can provide this data and can be continuously updated. However, whilst they may be far more difficult to illegally access, counterfeit or alter, their fraudulent use is still a concern that the banking industry has been plagued with. Indeed, as more organisations have access to read or enter data, the security of the card and the quality of the information becomes suspect. Should the card only be used for the retention of training and STCW certificate information entered by only one flag State with selected read only options by other parties, the standing of the card can be maintained. It should be noted, however, that the current STCW 95 regulations I/14

Responsibilities of companies requires the original certificates to be available at all times for the administrations to inspect. In this case endorsements from any other flag State would be issued in hard copy and the original issuing authority must carry out any update to the smart card.

8 In some countries there are a larger number of organizations that believe they should have access to the database on these cards, not only to read but also to enter a wide range of information including:

.1 Medical fitness records;
.2 Sea time service records;
.3 Disciplinary records;
.4 Biometric details;
.5 Digital, transmittable photo;
.6 Employment and contract details;
.7 Personal details and background checks; and
.8 Security clearance.

9 This list can be extensive, as can those who could find a use for this card. On a national basis, with the use of personal identification numbers (PIN), limited access can be set up or alternatively encoded data can be entered for more sensitive matters. The fact remains that once information has been entered in any database it is unrealistic to believe that those with the appropriate technology will not unlawfully access it or, as may be the case, the authority use the data for a purpose not intended. It is difficult to see that a card with access from a number of organizations will be of any benefit to the seafarer or can ensure their right to data protection and confidentiality.

Conclusion

10 Before any further consideration of international databases or a move towards the use of smart cards, there is a need to evaluate national databases and records established pursuant to STCW Regulation I/9. It may therefore be appropriate to task the Secretariat with undertaking such a review, having due regard to the Council's discussion on seafarers' human rights, and with submitting an overview of the current state of affairs which would guide the Sub-Committee at STW 35.

Action requested of the Sub-Committee

11 The Sub-Committee is invited to review the current measures being implemented by flag State administrations to restrict the proliferation of counterfeit and fraudulently issued STCW 95 certificates and to:

.1 Undertake a review of current national databases' standards, record systems and anti-fraud measures on certificates;

.2 Consider if these measures should be covered in more detail under the STCW Convention;

.3 Consider whether the IMO can offer a central database service that would enhance the various national systems and give a reliable, credible option for the international seafarer;

.4 Consider what further measures can be taken to improve the status of the STCW95 'White List' certificates; and

.5 Take measures to ensure data received for the verification of STCW 95 certificates is protected and that only selected information is released for the correct purposes and only within strict criteria.

_____