COUNCIL OF THE EUROPEAN UNION

Brussels, 20 June 2013

10681/13

CSC 55
CSCI 33

"I" ITEM NOTE

From:	Council Security Committee
To:	COREPER
Subject:	Review of implementation of the provisions of the security rules regarding cryptographic products

When it adopted the security rules for protecting EU classified information on 31 March 2011, the Council approved five Declarations and entered them in its minutes (doc. 8054/11 ADD 1).

The Council Security Committee was tasked by the Declaration in annex IV to document 8054/11 ADD 1 to review the situation concerning second-party evaluations of cryptographic products and the relevant provisions of the security rules and to report to COREPER. This report can be found in the annex.

COREPER is invited to take note of the report, which was endorsed by the Council Security Committee at its meeting on 6 June 2013 and has been taken into account in the technical update of the Council security rules which has just been completed (doc. 10086/13).

Annex

Report on the implementation of the provisions of the security rules regarding cryptographic products

Background

1. When the Council approved the "Security rules for protecting EU classified information (Council Security Rules/ CSR)" on 31 March 2011, it also entered five declarations in the minutes of the session. The declaration in annex IV to document 8054/11 ADD1, which is also supported by the European Commission, reads as follows:

   "Given the need for the European Union to deploy communication and information systems (CIS) handling EUCI swiftly and securely, the Council and the Commission underline the urgency for the European Union to have at its disposal a sufficiently wide choice of cryptographic products for protecting EUCI approved in accordance with Article 10(6) of the Council's security rules. To that end, the Council and the Commission note that:

   - Member States will step up their efforts to offer as many nationally approved cryptographic products as possible for second party evaluation, and

   - Member States with appropriately qualified authorities commit themselves to undertaking as a matter of priority such second party evaluations.

   The Council and the Commission also underline the long-term objective of achieving as consistent a level of assurance as possible throughout the EU with regard to protecting the confidentiality of EUCI."

2. The Council invited the Council Security Committee to review the situation and the relevant provisions of the security rules and to report to COREPER.

Legal Basis

3. Cryptographic products for protecting the transmission of EUCI are approved by the Council or the Secretary-General following the successful completion of a second party evaluation of the product conducted by a recognised and accredited crypto approval authority (CAA) in another Member State. The second party evaluation as defined in paragraph 26 of annex IV of the CSR is carried out by Appropriately Qualified Authorities (AQUAs). In addition to the initially established AQUAs (in France, Germany, Italy, the Netherlands and the United Kingdom), a Swedish authority was accredited as an AQUA in November 2011.

Current Situation

4. Since 2004, the AQUAs have performed thirty five second party evaluations, which were the basis for the subsequent recommendations by the Information Assurance sub-area of the Council Security Committee for approval to the Council or the Secretary-General respectively:

   – Thirteen cryptographic products received Council approval for the protection of information classified up to and including SECRET UE/EU SECRET;

   – Five cryptographic products received Secretary-General approval for the protection of information classified up to and including CONFIDENTIEL UE/EU CONFIDENTIAL; and

   – Seventeen cryptographic products received Secretary-General approval for the protection of information classified RESTREINT UE/EU RESTRICTED.

5. Eighteen of the cryptographic products listed above have received EU approval since the revised CSR entered into force in 2011.

6. The list of approved cryptographic products (LACP) is regularly updated and published as a Council document (see document 6629/2/13). A Council document is also published per individually approved cryptographic product. Additionally, details of the approved cryptographic products are available on the Council's website, in the section "Policies", sub-section "Information Assurance".

Workshop to promote Second Party Evaluations

7. Currently, the number of cryptographic products submitted to second party evaluations by the Member States without an accredited AQUA is very limited. One of the reasons for the low take-up is that specialised expertise in this field in the Member States is limited. In order to increase knowledge in this area and to encourage Member States to provide more cryptographic products for second party evaluation, a workshop will be held on 2 and 3 July 2013. The workshop will be open to all Member States and will serve as a forum to discuss all relevant aspects of the EU procedures for approving Member States' cryptographic products. The Member States with AQUAs will play a central role in the success of this workshop and details have already been discussed with their representatives.

8. At the workshop experts of the AQUAs will present all aspects of the second party evaluation process. Representatives of other Member States producing cryptographic products will be invited to give an overview of their cryptographic products which could undergo a second party evaluation. The workshop will offer several discussion sessions with the aim to clarify as many of the possible issues that currently prevent the submission of more cryptographic products for second party evaluation.

9. Another reason for reluctance to submit cryptographic products to second party evaluation is the fact that very sensitive national information must be shared with another country. The workshop will also inform the participants on an initiative taken by a group of Member States to reduce this reluctance by offering standardised varieties of cryptographic algorithms that meet the requirements of the Information Assurance Policy on Cryptography. These are offered free of charge to all other EU Member States on the basis of a Memorandum of Agreement. The use of these standardised algorithms avoids the need to give a national algorithm to another country performing the second party evaluation.

10. There are few accredited AQUAs, although in principle all Member States can propose that a CAA of their country is accredited as an AQUA by the Information Assurance sub-area of the Council Security Committee on the basis of a monitoring process performed by an existing AQUA. The workshop will also cover all relevant aspects of the work of AQUAs with a view to encouraging more Member States to create such authorities and consequently to increase the capacity for second party evaluations.

11. In this context it should be borne in mind that the policy basis for second party evaluations has recently been approved by the Council Security Committee (Information Assurance Security Guidelines on Second Party Evaluation, document 13910/12, R-UE/EU-R). These guidelines support the general principles of the Information Assurance Policy on Cryptography (cf. document 10745/11, R-UE/EU-R).

Survey on the use of cryptographic products used by Member States

12. Following questions related to the cryptographic protection of EU classified information in national systems the Council Security Committee sub-area for Information Assurance conducted a survey on the protecting of EU classified information handled in Member States' communication and information systems.

13. As a result it was determined that, in principle, all Member States respect the requirements of article 10(6) of the Council Security Rules. However, some delegations have informed the GSC that they are not able to provide a complete overview on the cryptographic products used for protecting EU classified information in their country.

14. The GSC is continuing to monitor the situation in the Member States. Regular EU inspection visits covering all aspects of the protection of EU classified information in the Member States are a useful instrument for such an assessment.

Mutual acceptance of cryptographic products

15. When the Council enters into security agreements for the exchange of classified information with third states and international organisations, it is normally agreed that, when such information is exchanged electronically, it its encrypted in accordance with the originator's requirements as outlined in its security rules and regulations. The originator's requirements must be met when transmitting, storing and processing classified information in internal networks of the Parties.

16. This requirement makes it necessary in principle that cryptographic products approved by the providing partner have to be installed if their classified information is transmitted in communication and information systems of the receiving partner.

17. Given that the approval procedures for cryptographic products in partner countries are often comparable to those in the EU, it is proposed that the Council approve decisions to accept cryptographic products approved by a third state or international organisation for the protection of EUCI released to that partner.

18. This decision would be based on the evaluation of a questionnaire completed by the partner. The CSC(IA) has endorsed a generic questionnaire for this purpose.

19. The acceptance of approval procedures for cryptographic is mutual, i.e. partners would also accept that their classified information is protected by EU approved cryptographic products.

20. In December 2012 the Council approved such a decision concerning the acceptance of NATO cryptographic products for the protection of EU classified information released to NATO. This decision will enter into force once the NATO Military Committee has approved a similar decision concerning the acceptance of EU approved cryptographic products for the protection of NATO classified information released to the EU.

21. Member States that receive NATO classified information as NATO Partnership for Peace countries have made it clear that mutual acceptance is a good basis for bilateral agreements with NATO so that they could use EU approved cryptographic products to protect this kind of classified information. NATO services have indicated that they are willing to openly examine such an option.

Survey on operational requirements for cryptographic products

22. A process has begun involving discussion with other EU institutions, bodies and agencies as well as with the Member States, to assess future needs for certain types of cryptographic products. The topic will be discussed at the CSC(IA) Workshop on Second Party Evaluation. The results will be communicated to the CSC in order to ensure that such product types are developed and that they subsequently undergo a second party evaluation process.

23. The Coordination Committee for Communication and Information systems plays an essential role in defining such requirements. A feasibility study for highly classified information exchange requirements for the European Council and the Council will be examined in this committee in the near future in order to determine options for putting in place such a system linking the GSC and Member States. In this context, consideration will need to be given to the cryptographic functionality that should be implemented and the availability of such products with the required EU approval.

Conclusion

24. The Council Security Rules state that as a general rule, EU classified information must be transmitted by electronic means protected by cryptographic products approved by the Council or the Secretary-General. A considerable number of cryptographic products now fulfil this requirement.

25. The second party evaluation process entails the exchange of highly classified proprietary information about sophisticated national scientific products in order to evaluate cryptographic products. This can be seen as an impediment to Member States who wish to contribute to this process. However, both parties involved in the process play an equal role, with neither party assuming control over the other.

26. Second party evaluation of cryptographic products has generated a sufficient level of trust required for cryptographic products that are essential for the protection of classified information.

27. Second party evaluations are currently only performed by a small number of Member States. To realise the full potential of second party evaluations more Member States should be encouraged to participate. A situation where only Council or Secretary-General approved cryptographic products are used in national networks of the Member States, might further increase the confidence that sufficient measures are taken to protect EU classified information when it is transmitted outside protected areas.

28. Member States contributing to the AQUA system are encouraged to continue supporting this process as defined in the Council Security Rules. Member States that have not yet provided cryptographic products for second party evaluation should consider doing so. Moreover, they should also consider acting as an AQUA.