

Swedish Certification Body for IT Security  
Scheme Note 31 - New procedures for site visit oversight and testing oversight

**Scheme Note**

Decision Date 2020-10-15	Matter ID CR-2945	
Decision by (Name/Title) Dag Ströman, Head of CSEC	Scheme Note Number 31	Dnr 20FMV6057-2:1
Presentation by Mats Engquist	Present at the Meeting CCB 2020-10-15	

**Schematolkningens innebörd/Scheme Note Statement**

Description and References

**Background**

The Common Criteria requires the evaluator to perform a site visit as part of the ALC-assessment at EAL3 and above.

According to the regulations of the Swedish Common Criteria Evaluation and Certification Scheme the Certification Body would perform a site visit oversight at EAL3 and above meaning that a certifier is witnessing the evaluator's site visit at the developer site. The site visit oversight is often combined with a testing oversight where a certifier makes a visit at the ITSEF or developer site during independent and penetration testing.

This policy has led to extensive traveling for the certifiers and is, for many reasons, not defensible to uphold.

There is no requirement for the certifier to attend the site visits performed by the evaluator neither in the Common Criteria nor in the arrangements on mutual recognition at the assurance levels for which the Swedish Certification Body for IT Security is approved.

During the Corona-pandemic new procedures for site visits and site visit oversight have been developed and have been found to work very well.

Based on this the Certification Body has decided to update the policy for site visit oversight end testing oversight as stated below.

**New procedure**

The evaluator shall perform a site visit according to the Common Criteria and the requirements for mutual recognition considering relevant additional and/or temporary instructions such as:

- IAF (International Accreditation Forum, Inc.): IAF MD 4:2018 IAF Mandatory Document for the Use of Information and Communication Technology (ICT) for Auditing/Assessment Purposes
- SOGIS: JIL Temporary Covid19 pandemic operational SOGIS evaluation and certification policy and rules

The certifier may attend site visits performed by the evaluator. Site visit oversight is performed at EAL 3 and above, unless otherwise decided. The purpose is for the certifier to observe the evaluator actions.

If possible the site visit oversight should be made remotely using Information and Communication Technology (ICT), suitable for the purpose of the site visit oversight.

The evaluator is responsible to provide the certifier with the possibility to attend remotely and to acquire the developers consent on the remote participation of the certifier.

The Certification Body may decide to accompany the evaluator at site visit performed on site. Such decisions will be motivated and documented.