

**BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI
KRİPTOGRAFİK GÜVENLİK FONKSİYONLARININ DOĞRULANMASI**

1. AMAÇ Bu doküman, Kriptografik Güvenlik fonksiyonu bulunan TOE'ler için gereken değerlendirici aktivitelerini içermektedir.	1. OBJECTIVE <i>This document describes the evaluator activities for the TOEs which have Cryptographic Support functionality.</i>
2. KAPSAM Bu doküman, OKBS yapısı içerisinde Ortak Kriterler değerlendirmeleri gerçekleştirecek tüm laboratuvarları kapsar.	2. SCOPE <i>This document includes all laboratories to make Common Criteria evaluations within The Common Criteria Certification Scheme.</i>
3. ONAYLI ALGORİTMALAR ST dokümanında sadece “SOGIS Crypto Evaluation Scheme – Agreed Cryptographic Mechanisms” dokümanında yayımlanan onaylı kriptografik algoritmalar kullanılmış olmalıdır. Bu doküman dışında kalan algoritmalar için OKDL ile birlikte duruma göre (case-by-case) karar verilir.	3. APPROVED ALGORITHMS <i>Only the approved cryptographic algorithms published in “SOGIS Crypto Evaluation Scheme – Agreed Cryptographic Mechanisms” document shall be used in the ST document. For algorithms not included in this document a case-by-case decision shall be made in collaboration with CCEL.</i>
4. ADV_IMP gereksinimleri ADV_IMP garanti ailesi içeren değerlendirmelerde ST dokümanında belirtilen kriptografik fonksiyonların implementasyonu doğrulanmalıdır. Örneğin ST dokümanında AES algoritmasının 256 bit anahtarlı CBC modu kullanıldığı belirtilmişse bunun doğrulanması gerekmektedir.	4. ADV_IMP activities <i>In evaluations that include ADV_IMP assurance family, implementation of cryptographic functions stated in ST document shall be verified. For instance, if it is stated in the ST document that CBC mode with 256 bits key of the AES algorithm is utilized, that should be verified.</i>

BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI KRİPTOGRAFİK GÜVENLİK FONKSİYONLARININ DOĞRULANMASI

5. ATE gereksinimleri ATE_COV garanti ailesini içeren değerlendirmelerde işletim çevresi (operational environment) tarafından sağlanan ve ST’de SFR’larda belirtilen kriptografik fonksiyonlarla ilgili olarak Değerlendiricinin geliştirici Testlerinde (developer tests) bu fonksiyonların implementasyonunun doğrulanması ile ilgili testlerin yer aldığını doğrulaması, geliştirici testlerinde yer almayan testleri ATE_IND garanti ailesi içinde bağımsız testlere eklemesi gerekmektedir. ST dokümanında belirtilen tüm imza, şifreleme ve özet algoritmalarının belirtilen anahtar uzunluklarında belirtilen tüm modlarına ait implementasyonlar doğrulanmalıdır.	5. ATE activities <i>In evaluations that include ATE_COV assurance family, for cryptographic functions stated in SFRs in the ST and provided by operational environment, the evaluator shall verify that tests regarding verification of implementation of these functions are present in the developer tests, shall add the tests that are not present in the developer tests to independent tests in ATE_IND assurance family. Implementation of all signature, encryption and hash algorithms stated in the ST document for defined key lengths and all defined modes shall be verified.</i>
6. AVA_VAN gereksinimleri AVA_VAN garanti aileleri ile ilgili olarak ST dokümanında belirtilen tüm algoritmalar ve ilgili modları ile ilgili olarak açıklık veritabanlarında tarama yapılması ve varsa zafiyet planında yer verilerek gerekirse atak yapılması gerekmektedir.	6. AVA_VAN activities <i>Regarding AVA_VAN assurance families, vulnerability databases shall be scanned for all algorithms and their related modes stated in ST document and if present it shall be included in vulnerability plan and if necessary shall be attacked.</i>
7. Genel gereksinimler TOE’de kullanılan kriptografik fonksiyonlarite dış bir arayüzden doğrulanamıyorsa değerlendirici aşağıdakilerden birini gerçekleştirmelidir. Güvenlik mekanizmaları mutlaka doğrulanmış olmalıdır. Geliştiriciden yardım alarak bu fonksiyonlara erişim için iç bir arayüze erişmek,	7. General requirements <i>If the cryptographic functionality utilized in the TOE cannot be verified on an external interface, evaluator shall conduct one of the options below. Security mechanisms shall definitely ve verified.</i> <i>Access an internal interface with support of the developer,</i>



BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI
KRİPTOGRAFİK GÜVENLİK FONKSİYONLARININ DOĞRULANMASI

- Doğrulama yapmak için bir test aracı yazmak,
- Kaynak kodu incelemek,
- TSE-OKBS'ye bunlardan farklı bir alternatif sunmak

- *Develop a testing tool to conduct verification,*
- *Analyze the source code,*
- *Present TSE-CCCS with a different alternative.*