

Final Proje Gösterimleri

CEN429 Güvenli Programlama — Hafta 15

Dr. Öğr. Üyesi Uğur CORUH · 25.12.2026

Bu hafta: final proje gösterimleri (RAP2)

- Ders anlatılmaz; final raporu (**kılavuzun tamamı**) + korumalı uygulama + test sonuçları
- RAP2 = finalin **%70**'i · Quiz-2 = **%30** · Başarı = $0,4 \cdot \text{Vize} + 0,6 \cdot \text{Final}$
- Ayrıntılı rubrik: proje rehberi · sıra ve süre: ders sınıfı
-  Geç teslim yok · vize geri bildirimleri için **bulgu–aksiyon listesi**

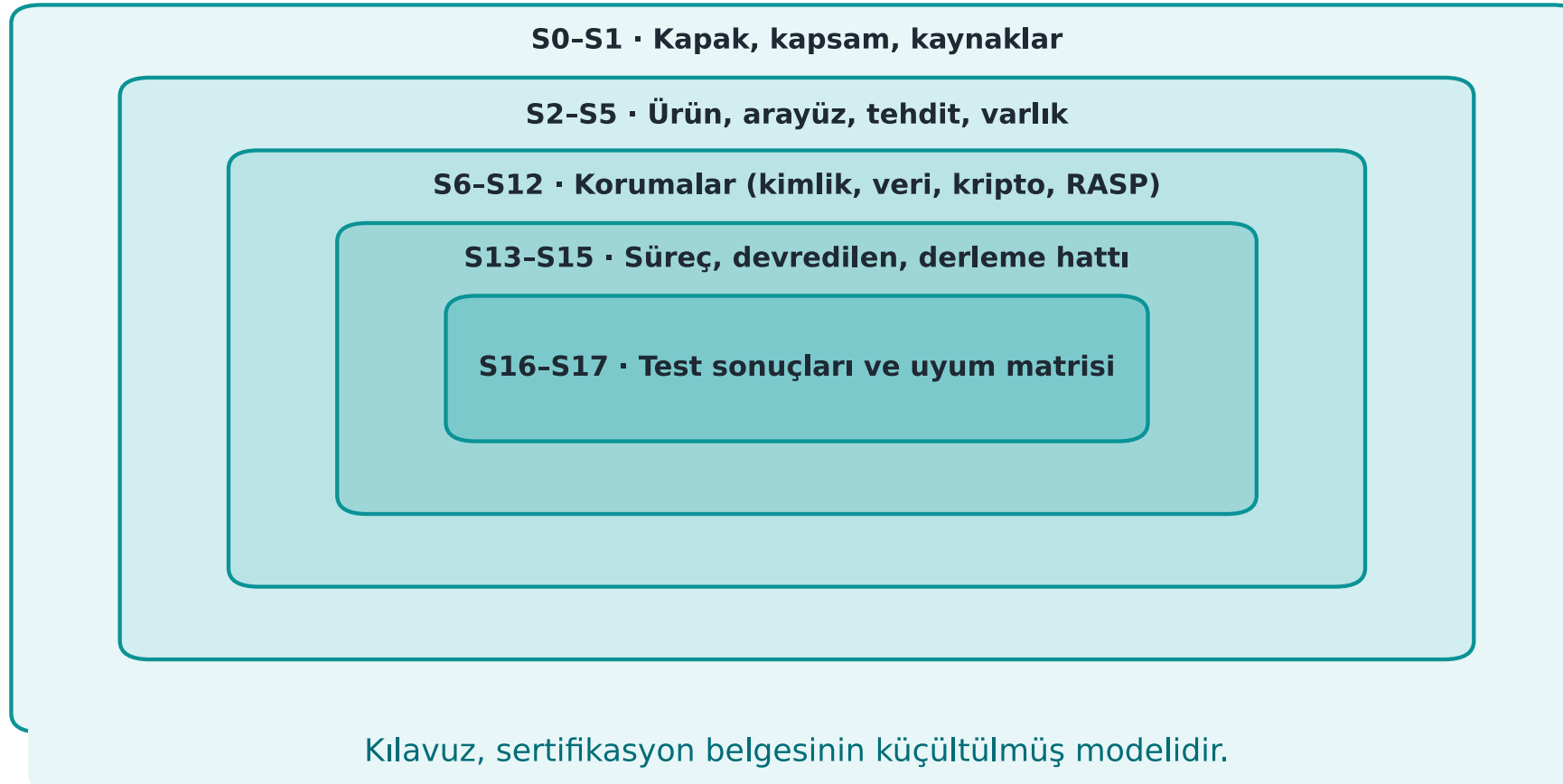
Final rubriği

Kriter	ÖÇ	Kılavuzda
Kriptografi	2	S8
Güvenli iletişim	4	S6 · S11
Varlık yönetimi	5	S5 (tam) · S8
İkili korumalar	3	S9 (ileri) · S15
Güvenlik testi ve birim testleri	6	S16 sonuçlar
Standartlar	7	S1 · S14 · S17
Final rapor ve sunum	7	Tümü

Kılavuz haritası S0-S17 — şema

Güvenlik kılavuzu S0-S17

dıştan içe değil, alttan üste: her bölüm bir öncekine dayanır



Vizeden finale: yeni ve tamamlanacak bölümler

Yeni	Tamamlanacak / güncellenecek
S6 kimlik ve bağlama	S5 varlıklar (tam)
S8 kriptoloji ve anahtarlar	S9 sağlamlaştırma (ileri)
S11 güvenli iletişim	S12 raporlama (tam)
S14 varsayımlar ve devredilenler	S13 güncel SBOM
S15 derleme ve dağıtım hattı	S16 sonuçlar · S17 tam matris

RAP2 teslimi — şema

RAP2 (final) teslimi: ne bekleniyor?

vizedeki yapının üzerine ölçüm ve kanıt eklenir

Tam ürün

C++ konsol + DLL/.so, CMake/CTest

S6-S15

kimlik, veri, kriptu, RASP, gizleme, hat

S16 · SONUÇLAR

plan değil, GÖZLENEN test sonuçları

S17 · Uyum matrisi

her satır kanıtlı

S14 · Devredilenler

gerekçeli, onaylı

$RAP2 = 0,7 \cdot \text{final notu}$. En sık kayıp: S16'da sonuç yerine plan yazmak.

Hazırlık kontrol listesi

Hafta	Gösterebilmeniz gereken
9, 14	Gizlenen fonksiyonlar ve gerekçe · maliyet tablosu · derleme hattında gizleme ve imzalama
10	Algoritma envanteri · anahtar yaşam döngüsü · TLS/sabitleme · imza doğrulaması
11	Hassas varlık için koruma yöntemi ya da gerekçesi
12	Test planı + sonuçlar · birim testleri · CI · bulgu–aksiyon listesi
13	Uyum matrisi · varsayımlar ve devredilenler

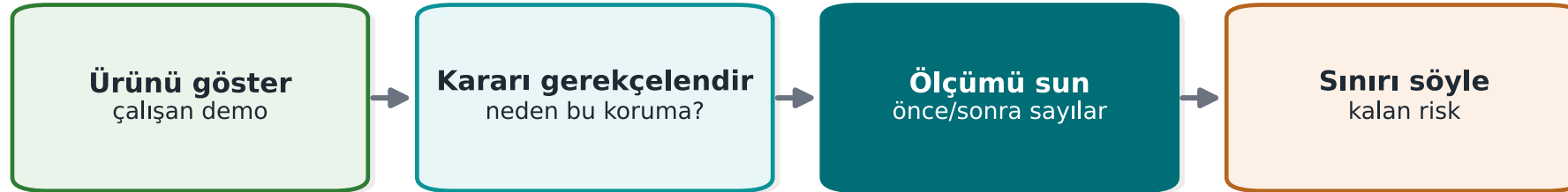
Önerilen gösterim akışı

1. **Özet:** ürün, mimari, en kritik üç varlık
2. **Vizeden bu yana:** bulgu–aksiyon listesi
3. **Canlı gösterim:** kriptu, güvenli iletişim, bir koruma katmanı **çalışırken**
4. **Kanıt:** testler, koruma tablosu, SBOM, uyum matrisi
5. **Kalan risk:** bilerek kapsam dışı olanlar ve nedenleri

Final gösterimi — şema

Final gösteriminin dört adımı

değerlendirici bu dördünü arar



Sınırını dürüstçe söyleyen takım, her şeyi 'güvenli' diyen takımdan yüksek alır.

Örnek sorular

- Bu anahtar nereden türetiliyor, nerede duruyor, ne zaman siliniyor?
- Zincir ve ad doğrulaması nerede?
- İmza doğrulaması başarısızsa ne oluyor? Eski imzalı sürüm yüklenebilir mi?
- Gizlemenin maliyetini ölçtünüz mü?
- Şu "karşılandı" satırının kanıtı nerede?
- Hangi gereksinimi devrettiniz, karşı taraf nasıl karşılayacak?

Sık yapılan hatalar

Hata	Neden sorun?
Test planı var, sonuç yok	Finalde sonuç beklenir
Kanıtsız "karşılandı"	Karşılanmamış sayılır
Kılavuz ile kod sürümü farklı	Değerlendirilen ürün belirsiz
Boş kalan risk bölümü	Eksik analiz
Vize geri bildirimi yok sayılmış	Bulgu–aksiyon döngüsü sürecin parçası
Depoda gerçek sır / kişisel veri	Değerler sentetik olmalı

S16: plan değil sonuç — şema

S16: plan mı, sonuç mu?

finalde S16'dan GÖZLENEN sonuç beklenir

PLAN (yetersiz)

'Şu testleri yapacağız'
'Şu araçları kullanacağız'

→ hiçbir şey kanıtlanmadı

SONUÇ (beklenen)

'Şu test çalıştırıldı'
'Gözlenen çıktı şu'
'Karar: geçti / kaldı'

→ kanıt var

Test kartı: amaç · ön koşul · adımlar · beklenen · GÖZLENEN · karar · kanıt.

Dönem sonunda

- Kılavuzunuz = sertifikasyon belgelerinin küçük bir modeli → **portfolyo** (gizli bilgi içermediğinden emin olun)
- Teslim edilen her satır açıklanabilmeli; her takım üyesine soru sorulabilir

Final dönemi

Hafta 16 — Quiz-2

- Kapsam: 9–14. haftalar
- Çalışma rehberi: 16. hafta sayfası

Ek · Final rubriği madde madde

Final neyi ölçer?

Final gösterimi projenizin **tamamını** ölçer:

- kriptto, güvenli iletişim
- varlık yönetimi (tam)
- ileri ikili korumalar
- test **sonuçları**, standartlar

Madde · kriptografi

- Algoritma envanteri, anahtar yaşam döngüsü.
- **Kanıt:** S8 + testler.

Madde · güvenli iletişim

- TLS, sabitleme, mesaj düzeyi.
- **Kanıt:** S6, S11 + test.

Madde · ileri ikili korumalar

- Gizleme (S9 ileri), derleme hattı (S15).
- **Kanıt:** ölçüm tablosu + imzalama.

Madde · test ve doğrulama

- Test **sonuçları** (plan değil).
- **Kanıt:** S16.

Madde · standartlar ve uyum

- Uyum matrisi (S17), devredilenler (S14).
- **Kanıt:** S14, S17.

Ek · Vizeden finale

Yeni bölümler

- S6 kimlik/bağlama
- S8 kript/anahtarlar
- S11 güvenli iletişim
- S14 varsayımlar/devredilenler
- S15 derleme/dağıtım hattı

Tamamlanacaklar

- S5 varlıklar (tam)
- S9 sağlamlaştırma (ileri)
- S12 raporlama (tam)
- S16 **sonuçlar**
- S17 tam matris

Bulgu–aksiyon (vizeden)

- Vize geri bildirimleri bir tabloya:
 - bulgu → aksiyon → kapanış.
- Değerlendirici bu döngüyü arar.

Ek · Gösterim akışı

Akış · özet + vizeden bu yana

- Ürün, mimari, en kritik üç varlık.
- Bulgu–aksiyon listesi.

Akış · canlı gösterim

- Kripto, güvenli iletişim ve **bir koruma katmanı** çalışırken.
- Ör. kurcalanmış dosyanın reddi.

Akış · kanıt + kalan risk

- Testler, koruma tablosu, SBOM, uyum matrisi.
- Kalan risk: bilerek kapsam dışı olanlar.

Ek · Örnek sorular

Soru 1

Bu anahtar hangi anahtardan türetiliyor, nerede duruyor, ne zaman siliniyor?

Soru 2

Sertifika zinciri ve ad denetimi nerede yapılıyor?

Soru 3

İmza doğrulaması başarısızsa ne oluyor? Eski imzalı sürüm yüklenebilir mi?

Soru 4

Gizlemenin maliyetini ölçtünüz mü? Hangi fonksiyonu neden gizlediniz?

Soru 5

Uyum matrisinde şu "karşılandı" satırının kanıtı nerede?

Ek · Sık yapılan hatalar

Hata listesi

- Test planı var, **sonuç** yok.
- Kanıtsız "karşılandı".
- Kılavuz ile kod sürümü farklı.
- Kalan risk boş.
- Vize geri bildirimi yok sayılmış.
- Depoda gerçek sır/kişisel veri.

Son söz (RAP2)

Finalde **sonuç** beklenir: her koruma çalışırken gösterilir, her gereksinim kanıtla bağlanır.

Kılavuzunuz sertifikasyon belgelerinin küçük bir modelidir; bir **portfolyo** öğesidir.