



Final Project Demonstrations

CEN429 Secure Programming — Week 15

Asst. Prof. Dr. Uğur CORUH · 25.12.2026

This Week: Final Project Demonstrations (RAP2)

- No lecture; final report (**the complete guide**) + protected application + test results
- RAP2 = **70%** of the final · Quiz-2 = **30%** · Course grade = $0.4 \cdot \text{Grade_Midterm} + 0.6 \cdot \text{Grade_Final}$
- Detailed rubric: project guide · order and timing: in class
-  No late submissions · a **finding-action list** for the midterm feedback

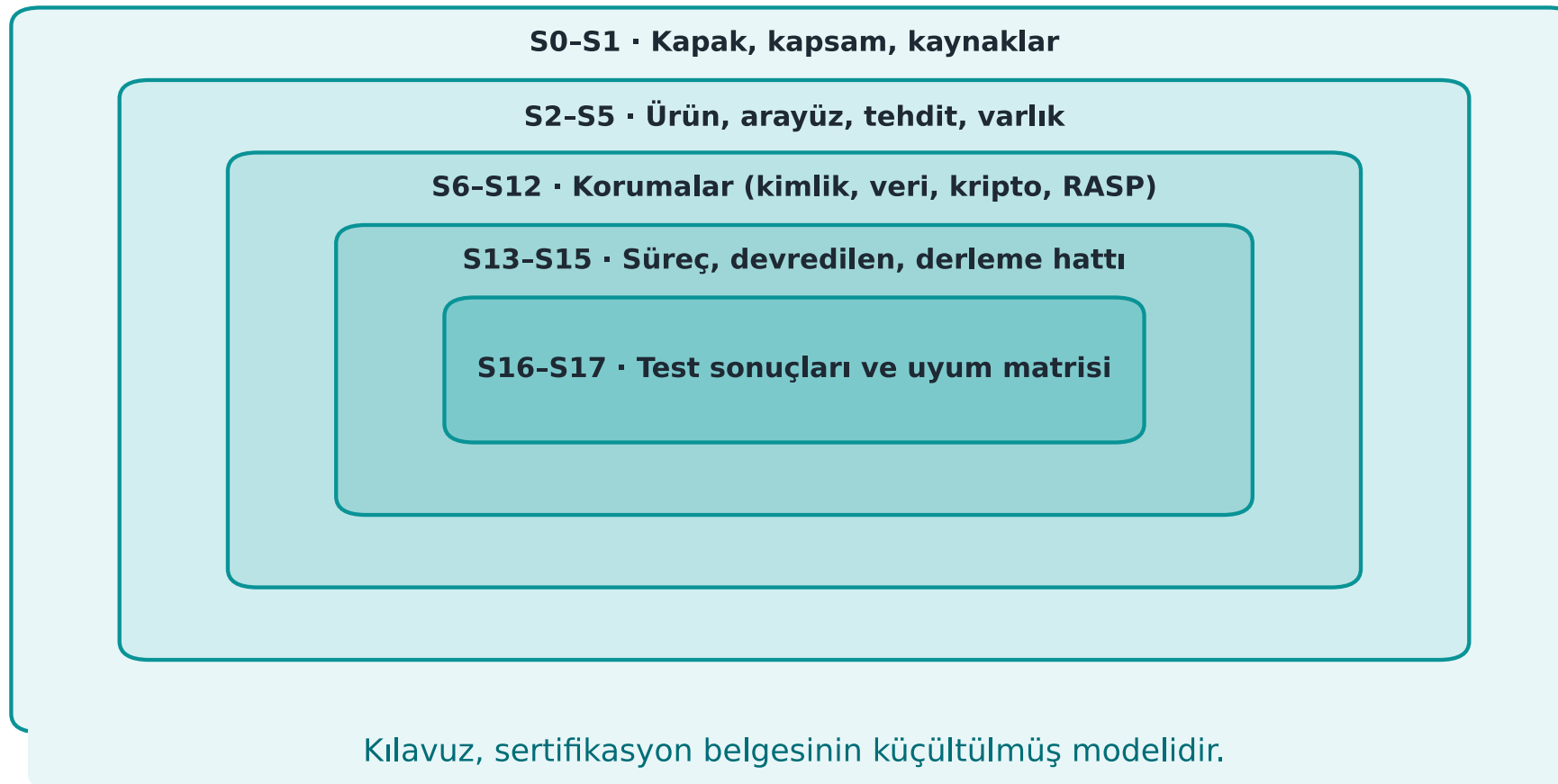
Final Rubric

Criterion	LO	Guide
Cryptography	2	S8
Secure communication	4	S6 · S11
Asset management	5	S5 (complete) · S8
Binary protections	3	S9 (advanced) · S15
Security testing and unit tests	6	S16 results
Standards	7	S1 · S14 · S17
Final report and presentation	7	All

Security Guide Map S0-S17 — Diagram

Güvenlik kılavuzu S0-S17

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



From Midterm to Final: New and Completed Sections

New	To be completed / updated
S6 identity and binding	S5 assets (complete)
S8 cryptography and keys	S9 hardening (advanced)
S11 secure communication	S12 reporting (complete)
S14 assumptions and deferred requirements	S13 updated SBOM
S15 build and deployment pipeline	S16 results · S17 complete matrix

RAP2 Submission — Diagram

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.

Preparation Checklist

Week	What you should be able to show
9, 14	Obfuscated functions and justification · cost table · obfuscation and signing in the build pipeline
10	Algorithm inventory · key lifecycle · TLS/pinning · signature verification
11	Protection method or justification for a sensitive asset
12	Test plan + results · unit tests · CI · finding–action list
13	Compliance matrix · assumptions and deferred requirements

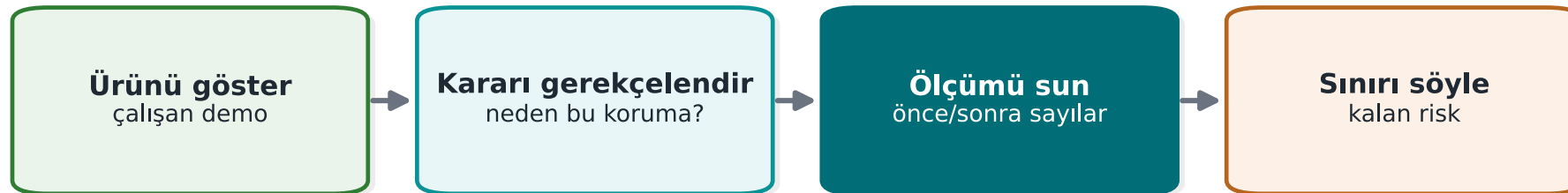
Suggested Demonstration Flow

1. **Summary:** product, architecture, the three most critical assets
2. **Since the midterm:** finding–action list
3. **Live demonstration:** cryptography, secure communication, a protection layer **working live**
4. **Evidence:** tests, protection table, SBOM, compliance matrix
5. **Remaining risk:** what was deliberately scoped out, and why

Final Demonstration — Diagram

Final gösteriminin dört adımı

değerlendirici bu dördünü arar



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

Sample Questions

- Which key is this key derived from, where does it live, when is it deleted?
- Where are chain and hostname verification performed?
- What happens if signature verification fails? Can an old but validly signed version still be installed?
- Did you measure the cost of obfuscation?
- Where is the evidence for this row marked "met"?
- Which requirement did you defer, and how will the other party meet it?

Common Mistakes

Mistake	Why is it a problem?
A test plan exists, but no results	At the final, results are expected
"Met" without evidence	Counted as unmet
Guide and code version differ	The assessed product becomes ambiguous
Empty remaining-risk section	Incomplete analysis
Midterm feedback was ignored	The finding–action loop is part of the process
Real secret / personal data in the repo	Values must be synthetic

S16: Results, Not a Plan — Diagram

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.

At the End of the Term

- Your guide = a small model of certification documents → **portfolio** (make sure it contains no confidential information)
- Every submitted line must be explainable; any team member may be asked a question

Final Exam Period

Week 16 — Quiz-2

- Scope: weeks 9–14
- Study guide: Week 16 page



Appendix · Final Rubric Item by Item

What Does the Final Measure?

The final demonstration measures the **entirety** of your project:

- cryptography, secure communication
- asset management (complete)
- advanced binary protections
- test **results**, standards

Item · Cryptography

- Algorithm inventory, key lifecycle.
- **Evidence:** S8 + tests.

Item · Secure Communication

- TLS, pinning, message level.
- **Evidence:** S6, S11 + tests.

Item · Advanced Binary Protections

- Obfuscation (S9 advanced), build pipeline (S15).
- **Evidence:** measurement table + signing.

Item · Testing and Verification

- Test **results** (not a plan).
- **Evidence:** S16.

Item · Standards and Compliance

- Compliance matrix (S17), deferred requirements (S14).
- **Evidence:** S14, S17.



Appendix · From Midterm to Final

New Sections

- S6 identity/binding
- S8 cryptography/keys
- S11 secure communication
- S14 assumptions/deferred requirements
- S15 build/deployment pipeline

To Be Completed

- S5 assets (complete)
- S9 hardening (advanced)
- S12 reporting (complete)
- S16 **results**
- S17 complete matrix

Finding–Action (from the Midterm)

- Midterm feedback into one table:
 - finding → action → closure.
- The assessor looks for this loop.



Appendix · Demonstration Flow

Flow · Summary + Since the Midterm

- Product, architecture, the three most critical assets.
- Finding–action list.

Flow · Live Demonstration

- Cryptography, secure communication and **a protection layer** working live.
- E.g., a tampered file being rejected.

Flow · Evidence + Remaining Risk

- Tests, protection table, SBOM, compliance matrix.
- Remaining risk: what was deliberately scoped out.



Appendix · Sample Questions

Question 1

Which key is this key derived from, where does it live, when is it deleted?

Question 2

Where is certificate chain and hostname verification performed?

Question 3

What happens if signature verification fails? Can an old but validly signed version still be installed?

Question 4

Did you measure the cost of obfuscation? Which function did you obfuscate, and why?

Question 5

Where is the evidence for this row marked "met" in the compliance matrix?



Appendix · Common Mistakes

Mistake List

- Test plan exists, no **results**.
- "Met" without evidence.
- Guide and code version differ.
- Remaining risk is empty.
- Midterm feedback was ignored.
- Real secret/personal data in the repo.

Final Word (RAP2)

At the final, **results** are expected: every protection is shown working, every requirement is tied to evidence.

Your guide is a small model of certification documents; it is a **portfolio** item.