Week 15 — Final Project Demonstrations

Date	25.12.2026
Learning outcomes	LO.1–7
Duration	3 hours

What happens this week?

There is no lecture this week. The **second checkpoint of the term project (RAP2)** takes place: each team submits its final report (the complete security guide) and demonstrates its protected application and its test results. RAP2 is **70% of the final grade**; the remaining 30% is Quiz-2 in the final exam period (`Grade_Final = 0.7·RAP2 + 0.3·QUIZ2`). The course passing grade is calculated as `0.4·Grade_Midterm + 0.6·Grade_Final`. The detailed rubric is in the project guide.

Submission and timing rules

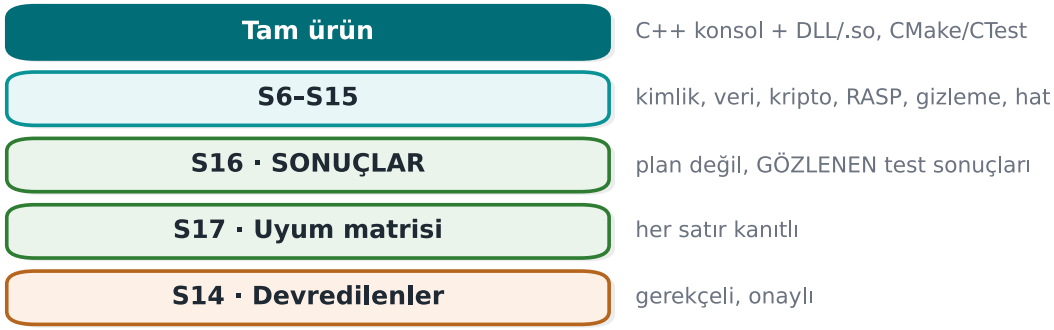
Late submissions are not accepted (syllabus, section G). The demonstration order, time per team and submission time are announced in class. Prepare a finding–action list showing how you closed out the feedback you received at the midterm checkpoint.

1. What does the final checkpoint measure?

The criteria of the final checkpoint rubric in the syllabus, and the corresponding sections in your security guide:

RAP2 (final) teslimi: ne bekleniyor?

vizedeki yapının üzerine ölçüm ve kanıt eklenir



RAP2 = 0,7 · final notu. En sık kayıp: S16'da sonuç yerine plan yazmak.

Criterion	Learning outcome	Where in the guide	Which weeks?
Cryptography implementation	LO.2	S8 algorithm inventory, key lifecycle and hierarchy, random numbers	3, 10
Secure communication	LO.4	S6 authentication and binding · S11 TLS, pinning, message-level protection	3, 10
Asset management	LO.5	S5 asset list (complete) · S8 keys	1, 3, 13
Binary application protections	LO.3	S9 code hardening (advanced) · S15 build, signing and deployment pipeline	4, 5, 6, 9, 14
Security testing and unit tests	LO.6	S16 test and verification results	4, 12
Security standards	LO.7	S1 references · S14 assumptions and deferrals · S17 compliance matrix	12, 13
Final report and presentation	LO.7	All sections; document structure, consistency, presentation	All

Sections that must be present in the final report

At the final checkpoint, every section is expected to be **complete**:

No	Section	Difference from the midterm
S0	Cover, document control, version history	Version history up to date; changes marked
S1	Scope, target audience, abbreviations, references	Complete
S2–S4	Product, architecture, threat model	Updated with midterm feedback
S5	Asset list and protection scheme	**Complete**: lifecycle and C/I/I+ for every asset
S6	Authentication, identification, device/version binding	New
S7	Data security + security shell matrix	Updated
S8	Cryptographic methods, key lifecycle and hierarchy	New
S9	Code hardening	**Advanced** (including obfuscation)
S10	RASP + response policy	Updated
S11	Secure communication	New
S12	Reporting and logging policy	Complete
S13	Development process, SBOM, change management	Updated SBOM
S14	Assumptions and deferred requirements	New
S15	Build, signing and deployment pipeline	New
S16	Security testing and verification	**Results** (not a plan)
S17	Requirement compliance matrix	Complete

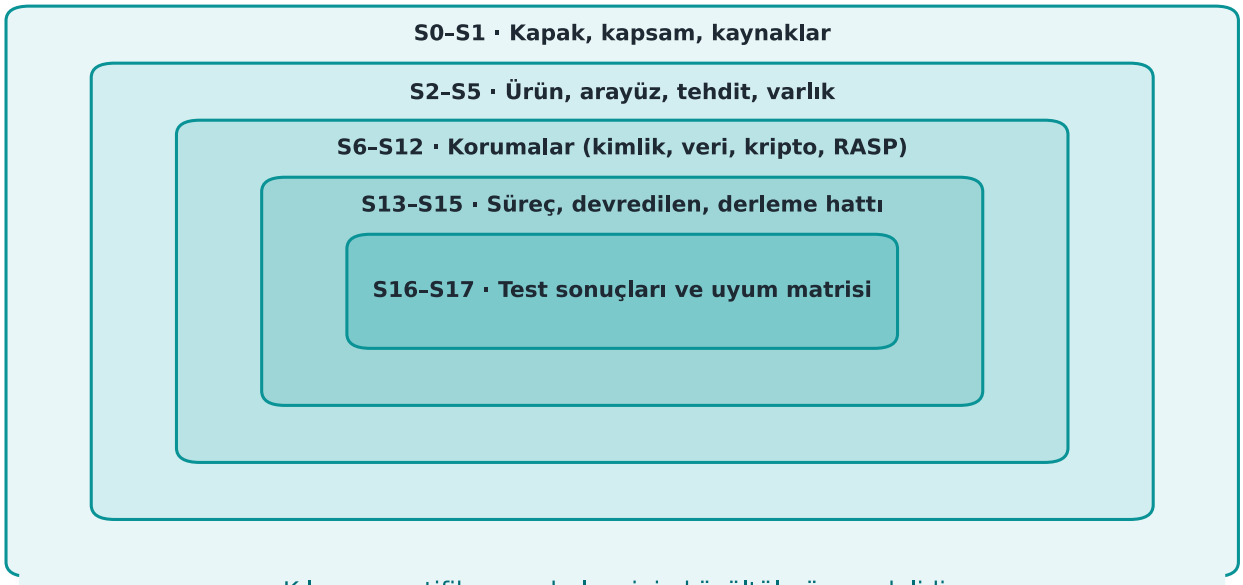
2. Preparation checklist (weeks 9–14)

Weeks 9 and 14 — Advanced code hardening (S9, S15)

- [ ] Which functions obfuscation was applied to and why; a before/after cost table (time, size).
- [ ] Obfuscation and signing steps in the build pipeline; version identity and digest values.
- [ ] Metrics for before and after obfuscation (ratio of meaningful names, count of plaintext sensitive strings).

Güvenlik kılavuzu S0–S17

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



Kılavuz, sertifikasyon belgesinin küçültülmüş modelidir.

Week 10 — Cryptography and PKI (S8, S11)

- Algorithm inventory: purpose, key length, mode, standard, library.
- Key lifecycle table: generation, storage, crypto-period, renewal, destruction.
- TLS validation; SPKI pinning and a backup pin if used; signature verification on the update file.

Week 11 — Key protection (S8)

- Protection method and justification for at least one sensitive asset (e.g., device binding, layered protection); if not used, the justification for why not.

Week 12 — Testing and assessment (S16)

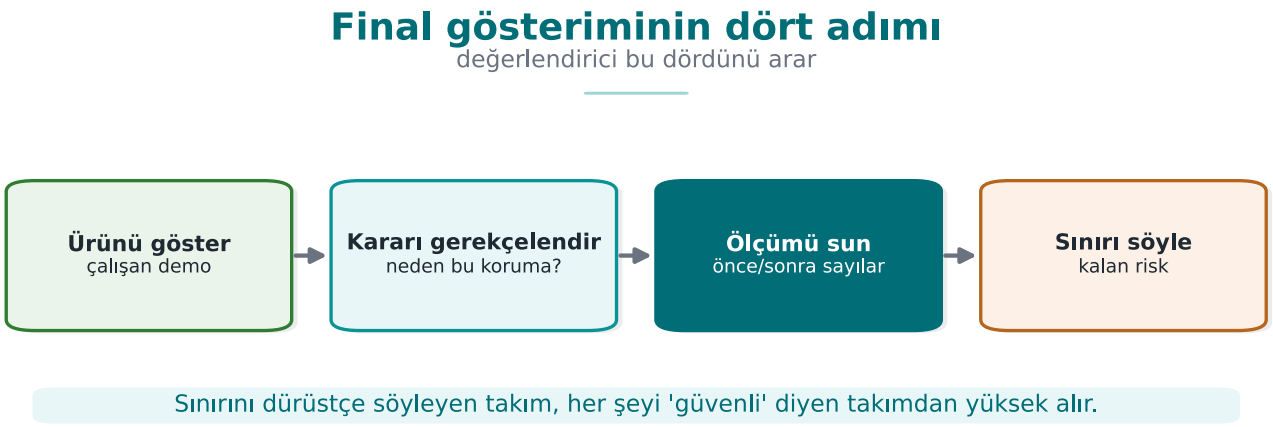
- Test plan and **results**: for each test, the purpose, method, expected and observed result.
- Unit tests (for cryptography and protection functions) and a continuous integration record.
- A finding–action list for the midterm feedback.

Week 13 — Requirements (S14, S17)

- Compliance matrix: for every implemented requirement, its status, section, verification and evidence.
- Assumptions and deferred requirements: to whom, why, how.

3. Demonstration: suggested flow

1. **Summary:** Product, architecture, and the three most critical assets (a single diagram).
2. **Since the midterm:** The feedback received and how it was addressed (finding–action list).
3. **Live demonstration:** Run the protected build; show cryptography, secure communication and at least one protection layer **working live** (e.g., a tampered file or an update with a broken signature being rejected).
4. **Evidence:** The tests, the protection table, the SBOM and the compliance matrix themselves; "we ran this command and got this output."
5. **Remaining risk:** What did you deliberately scope out, what could you not meet, and why?



Sample questions you may be asked during the demonstration

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

Common mistakes

Mistake	Why is it a problem?
There is a test plan but no results	At the final checkpoint, S16's **results** are expected
"Met" with no evidence in the compliance matrix	Counted as unmet in the assessor's eyes
A version mismatch between the guide and the code	The product being assessed becomes ambiguous; version identity and digest values must be consistent
An empty remaining-risk section	No product has zero remaining risk; an empty section means an incomplete analysis
Ignoring the midterm feedback	The finding–action loop is part of the process
Real secrets or personal data in the repository	A serious security mistake; all values must be synthetic

4. Academic integrity

The "Academic Integrity" section of the syllabus applies to the project as well. You must be able to explain every line you submit; any member of the team may be asked a question during the demonstration. If you used someone else's code or text, cite the source.

5. At the end of the term

- Your security guide is a scaled-down model of the documentation that certified products carry; you can use it as a **portfolio** item in job applications (make sure it contains no confidential information).
- Quiz-2 is held in the final exam period; its scope is weeks 9–14 (see the Week 16 page).