Alder Grant Foundation – Reviewer Access to Application Documents

Author: Paweł Nowak

Review type: Application Security Design Review

Status: Working Draft. Fictional case study

1.Executive summary

Maya is an external reviewer assigned to a grant application. While reviewing the budget, she saves a link to the document. A coordinator later removes her assignment. Maya is still signed in when she opens the saved link.

The expected outcome is that the download is denied. Maya's account and reviewer role remain valid, but her permission to read this particular budget ended with the assignment. The download endpoint must check her current access before it returns any file content.

2. Context and scope

The review covers two operations: viewing a grant application and downloading one of its supporting documents. It considers both normal navigation through the dashboard and direct access through a saved link.

The fictional design uses three assumptions:

- A coordinator can assign a reviewer to an application and later revoke that assignment.
- Each document belongs to one application. An active assignment grants the reviewer read access to that application and its documents.
- Revoking one assignment leaves the reviewer signed in and preserves any other active assignments.

3. Security questions

1. What gives Maya permission to download a specific document?
2. If a request identifies both an application and a document, how does the server establish that the document belongs to that application?
3. What happens on the next request if Maya's assignment changes while the application page is still open?

4. Finding and potential impact

Finding: A saved document link could remain usable after assignment revocation.

In the design reviewed, the dashboard filters applications by assignment. The potential gap is at the download endpoint. If the endpoint checks only that Maya is signed in and has the REVIEWER role, both conditions still holds after her assignment ends. Removing the application from her dashboard would leave the saved link usable under those conditions.

The potential impact is disclosure of a confidential applicant document to a former reviewer. A related risk arises if the server checks Maya's access to the application named in the request without verifying that the requested document actually belongs to it.

Evidence status: These are findings from a design walkthrough. No application was tested and no disclosure was observed.

5. Recommendation

For every download, the server should identify the signed-in reviewer, look up the requested document and determine which application owns it. Before returning the file content, it should verify that the reviewer has an active assignment to that application. If the request also names an application, the server should verify that the two records belong together.

The application-details endpoint should enforce the same assignment rule when the page is opened directly or refreshed. A tab left open may still display information loaded earlier. Clicking **Download** from that tab starts a new request, so that the server can enforce the current permission at that point.

6. Proposed verification

All tests below are proposed. The table records expected outcomes.

Test	Precondition & action	Expected Result
Authorised download	Maya is signed in and assigned to application A. She downloads A's budget.	She receives the expected budget file.
Document from another application	Maya is assigned to A only. A download request names A, but identifies a document owned by B.	The server denies the download and returns no file content.
Saved link after revocation	Maya confirms that a link works while assigned to A. The coordinator revokes that assignment. Without signing out, Maya opens the same link again.	The second request is denied and returns no file content.
Download from an open tab	Maya leaves A open in her dashboard. After revocation, she clicks the existing **Download** button without refreshing the page.	The server denies the new request even if the button is still visible.
Direct access to application details	After revocation, Maya opens A's saved details URL in the same session.	The server denies access to A's detalis.
Another assignment remains active	Maya is assigned to A and B. The coordinator revokes A only. Maya requests B's budget.	She can still download B's budget.

7. Open question

What happens to a copy Maya downloaded while she was authorised?
The proposed control covers future requests to the application. A file already saved on Maya's device is a separete document-handling question for the foundation.