CLASS-4

Sprint 3 Details

Olarn Rojanapornpun

Schedule

SEPT	5	2	3	4	5	6	7	8
	Exam 1	9	10	11	12	13	14	15
	6	16	17	18	19	20	21	22
	7	23	24	25	26	27	28	29
OCT	8	30	1	2	3	4	5	6
	9	7	8	9	10	11	12	13
	10	14	15	16	17	18	19	20
	Exam 2	21	22	23	24	25	26	27
	11	28	29	30	31	1	2	3

Sprint 2

Sprint 3

Sprint 4

Sprint 5

- Can UAT Sprint 2 with advisor by 17 September 2024
  - Still need to test with cypress and postman when they are available
- Must commit Sprint 3 by 17 September 2024
- Sprint 3 ends on 30 September 2024

Issues/questions in sprint 2

- Do not need to keep /v2/ endpoints
- If you do, tasks are stored on tasks_v2 table

SPRINT 2 UAT

PBI	NAME	BRIEF DESCRIPTION
18	SIMPLE-AUTHZ	User must authenticate before using the system
19	PERSONAL-BOARD	Each user can create his/her own personal task board

- Must pass both cypress and postman tests
- [PBI18] FE
  - use navigation guard to protect all endpoint (except /login)
  - send access_token in the header of every fetch request to BE (except /login)
  - Reset state and redirect to login page in case of 401
- [PBI18] BE – (on all but /login) if token is not valid or no token, returns 401
- [PBI19]
  - User can create one board.
  - Redirect to /board/:id when there is a board.
  - Owner can manage tasks and statuses, which are specific to each board.

SPRINT 3 PBIs

PBI	NAME	BRIEF DESCRIPTION
20	BOARD-VISIBILITY	Board owner can control visibility of the board
21	SECURE-CONNECTION	Connections between the client (browser) and the servers (proxy, frontend, backend) must be secure
22	INSTANT-ACCESS	Login state and tokens are stored to allow instant access of the board when the webpage is re-open
23	SIGN-OUT	Signed-in user can sign-out of the application

Technical Spikes

- Secure connection (nginx +optional spring boot)
- Authz personal board (including task/status) – private/public
- Refresh token
- Token storage

PBI20 BOARD-VISIBILITY

Board owner can control visibility of the board

Business/technical conditions:

1. Board visibility is specific to each board and has the value either 'private' or 'public' (but not both)
2. In 'private' mode, only board owner can access/control board. This is the default board visibility value (the user does not specify board visibility during creation of board.)
3. In 'public' mode, anyone (signed-in or not) can view the board (task list), task detail, and status list. (Owner can still manage the board.)
4. Only the board owner can change visibility of the board

visibility	user	change board visibility	view board info	view task list / task detail	manage task	view status list	manage status
private	owner	✓	✓	✓	✓	✓	✓
	other	✗	✗	✗	✗	✗	✗
public	owner	✓	✓	✓	✓	✓	✓
	other	✗	✓	✓	✗	✓	✗

PBI20 BOARD-VISIBILITY -- FE

Board owner can control visibility of the board

1. Add toggle button on /board/:id page
   When clicked, show modal "Do you want to change board visibility to <<new_mode>>?".
   "Confirm" and "Cancel" options are provided.
   When confirm, send request to PATCH: /boards/{id} with the new visibility mode {private, public}
   200: change display of visibility mode button to new_mode
   401: reset authentication state and redirect to login page
   403: show message "You do not have permission to change board visibility mode."
   other: show message "There is a problem. Please try again later."

2. Update /board/:id and /board/:id/status page

user	Visibility	FE behavior
owner	any	Display the task/status table. Can perform any operations as before.
other	private	Display a page with text "Access denied, you do not have permission to view this page.", stay on this page
	public	Display the task/status table. Disable 'Add', 'Edit', 'Delete', and 'visibility' buttons. Config the tooltips to show "You need to be board owner to perform this action."

PBI20 BOARD-VISIBILITY -- FE

Board owner can control visibility of the board

3. Update navigation guard (router)

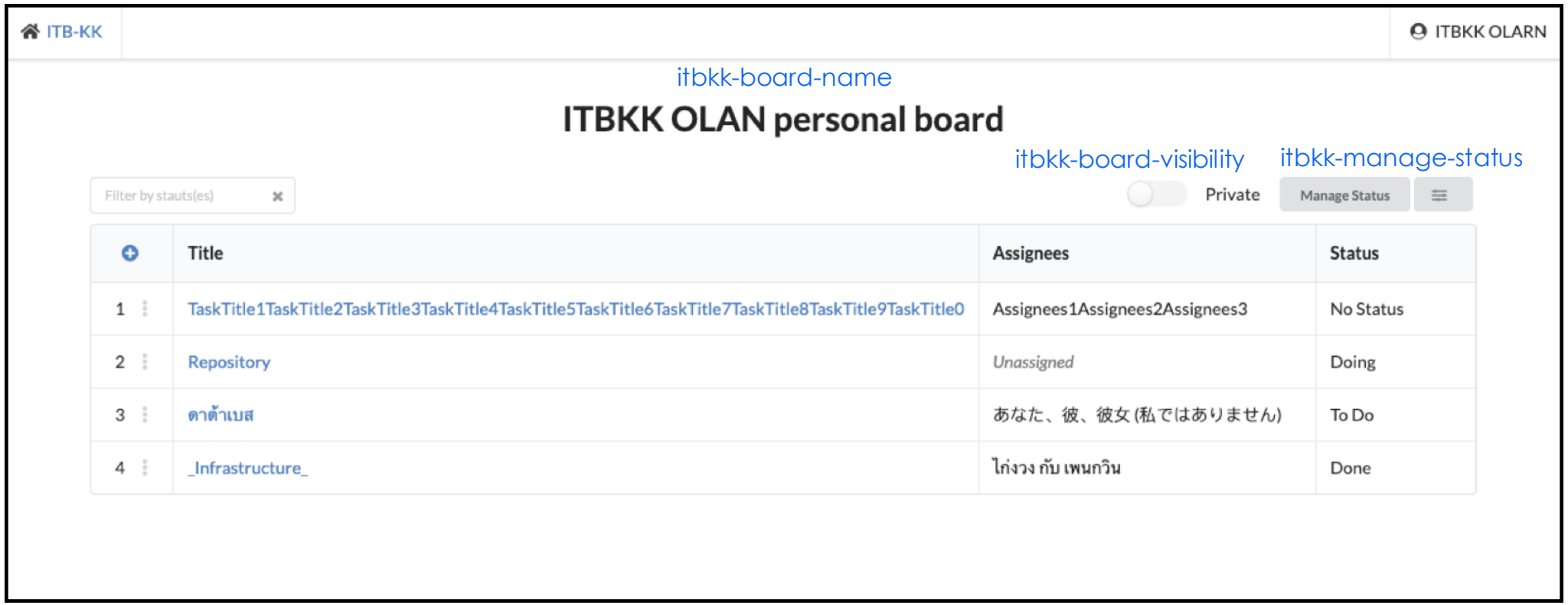
user	Visibility	/board/:id, /board/:id/task/:task-id, and /board/:id/status
owner	any	Redirect to corresponding page
other	public	Redirect to corresponding page
	private	Redirect a page with text "Access denied, you do not have permission to view this page.", stay on this page

user	Visibility	/board/:id/task/add, /board/:id/task/:task-id/edit
owner	any	Redirect to corresponding page
other	public	Redirect a page with text "Access denied, you do not have permission to view this page.", stay on this page
	private	

Sample UI: Board (/board/:id)

itbkk-home => /board

itbkk-fullname

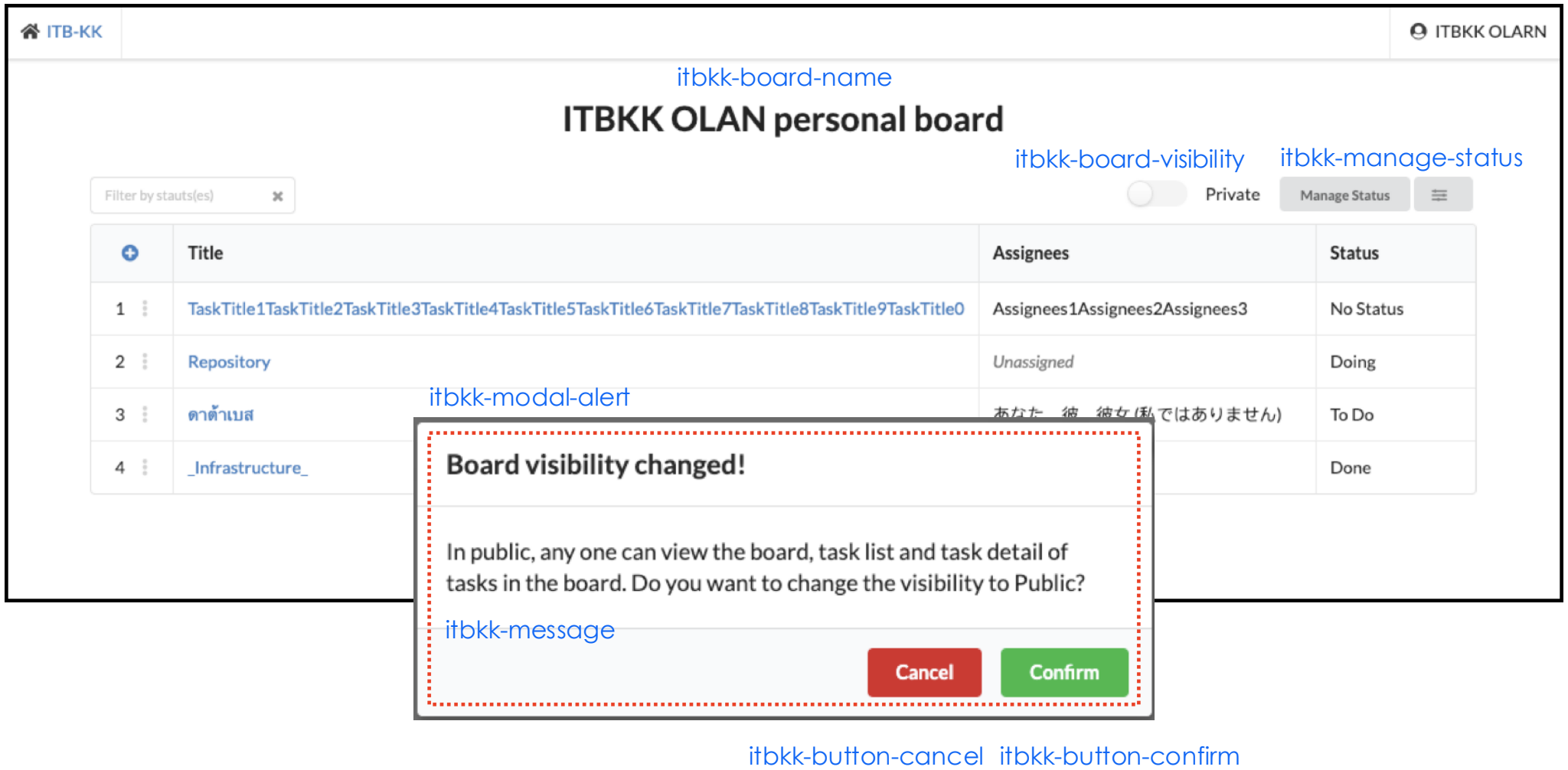


Sample UI: Board (/board/:id)

Confirmation alert

itbkk-home => /board

itbkk-fullname



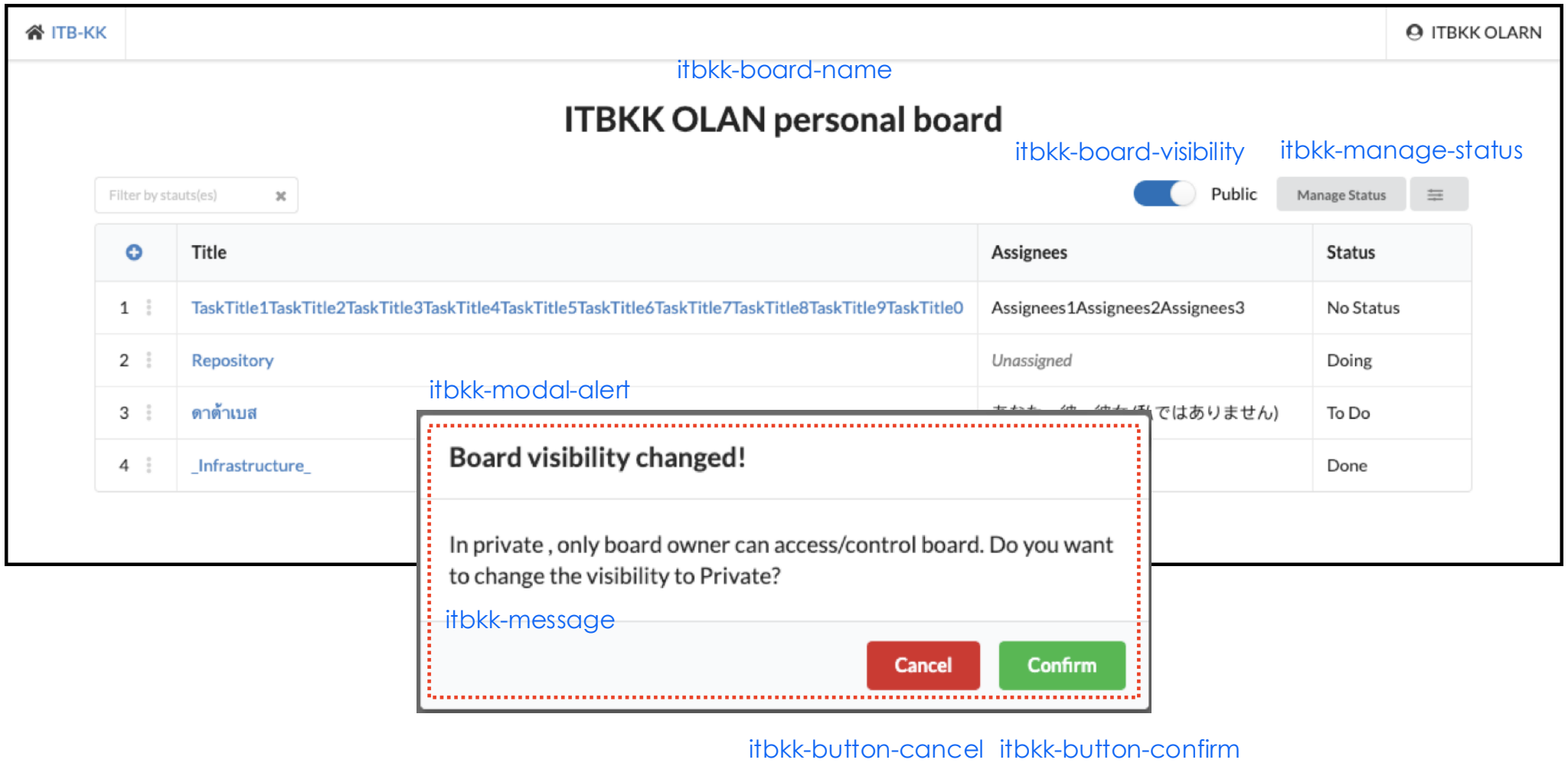
itbkk-button-cancel itbkk-button-confirm

Sample UI: Board (/board/:id)

Confirmation alert

itbkk-home => /board

itbkk-fullname



itbkk-button-cancel itbkk-button-confirm

PBI20 BOARD-VISIBILITY -- BE

Board owner can control visibility of the board

1. Add /boards/{id} endpoint

   [GET] returns board info with at least {id, name, owner, visibility}

Code	Scenario
200	boardIDExists AND (isOwner OR isPublic)
403	boardIDExists AND !(isOwner OR isPublic)
404	!boardIDExists

   [PATCH] update board.visibility to attribute visibility in request body

Code	Scenario
200	authenticated AND boardIDExists AND isOwner AND success
400	authenticated AND boardIDExists AND isOwner AND (board.visibility ∉ {private, public})
401	!authenticated
403	authenticated AND boardIDExists AND !isOwner
404	authenticated AND !boardIDExists

PBI20 BOARD-VISIBILITY -- BE

Board owner can control visibility of the board

2. Modify the existing endpoints with specified authorization behavior shown in the table.

Valid token	Board exists	is owner	is public	/boards/{id} /boards/{id}/tasks/** /boards/{id}/statuses/**	
				GET	POST/PUT /PATCH/DELETE
✓	✓	✓	–	200	200 / 201 / 400 / 404
✓	✓	X	✓	200	403
✓	✓	X	X	403	403
✓	X	–	–	404	404
X	✓	X	✓	200	401
X	✓	X	X	403	401
X	X	–	–	404	401

API Specifications for PBI20

GET `/v3/boards/{id}` Gets board by ID

Responses

Code	Description
200	Successful Operation

Media type: application/hal+json

Controls Accept header.

Example Value | Schema

```
{
  "id": "string",
  "name": "string",
  "visibility": "PRIVATE",
  "owner": {
    "oid": "string",
    "username": "string"
  }
}
```

PATCH `/v3/boards/{id}` Change board visibility to private/publi

Change board visibility to private/public

Parameters

No parameters

Request body required

Example Value | Schema

```
{
  "visibility": "PRIVATE"
}
```

Responses

Code	Description
200	Successful Operation

Media type: application/hal+json

Controls Accept header.

Example Value | Schema

```
{
  "visibility": "PRIVATE"
}
```

400 Bad Request

Media type: application/hal+json

Example Value | Schema

```
{
  "timestamp": "2024-04-23T08:29:03.133+00:00",
  "status": 404,
  "message": "Status id '99' NOT FOUND",
  "instance": "/v3/boards/X1/statuses/99",
  "errors": [
    {
      "field": "string",
      "message": "string"
    }
  ]
}
```

401 Authentication Failed

Media type: application/json

Example Value | Schema

403 User is not board owner

Media type: application/hal+json

Example Value | Schema

404 Not Found

Media type: application/hal+json

Example Value | Schema

```
{
  "timestamp": "2024-04-23T08:29:03.133+00:00",
```

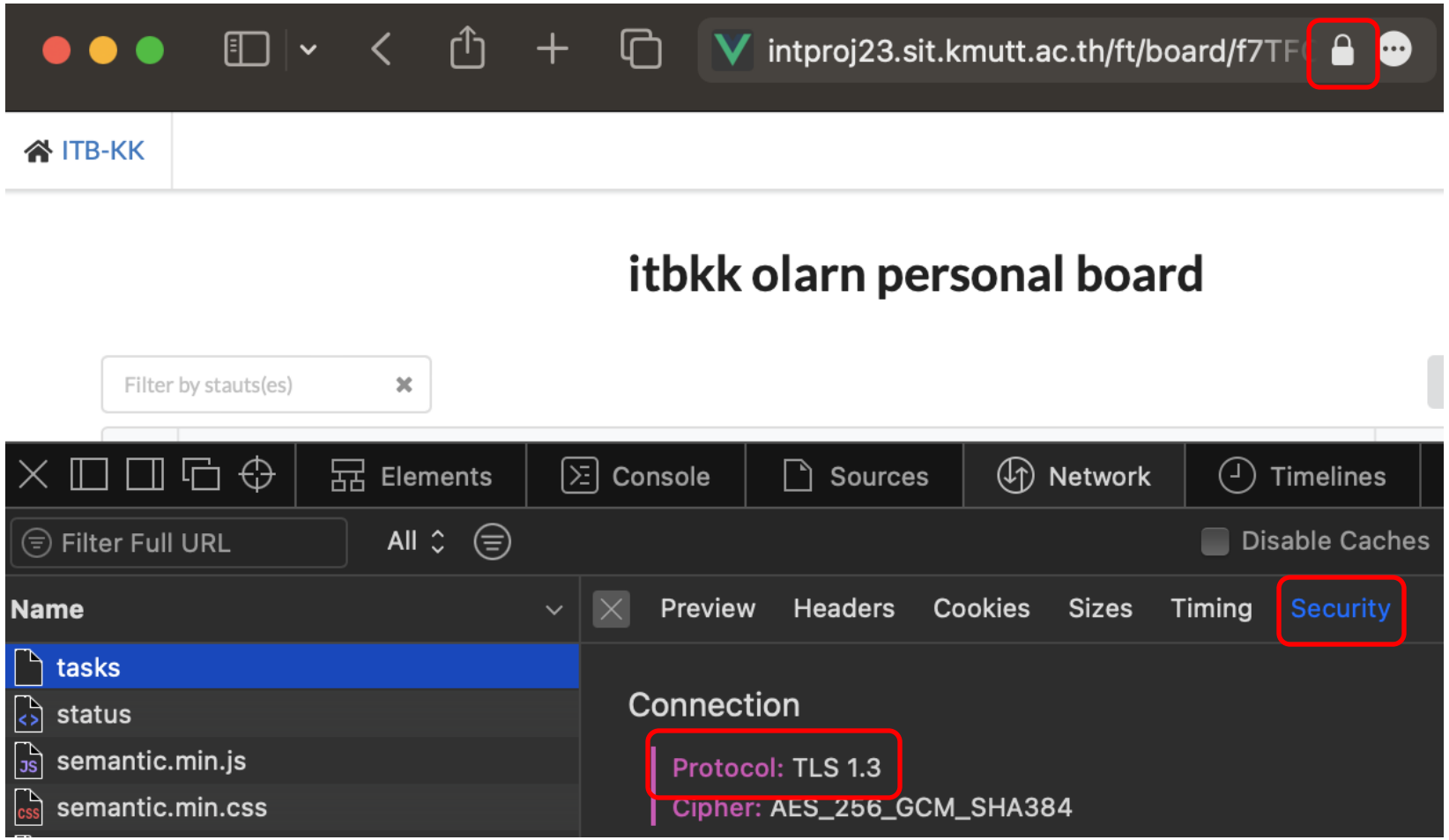
PBI21 SECURE-CONNECTION

Connections between the client (browser) and the servers (proxy, frontend, backend) must be secure.

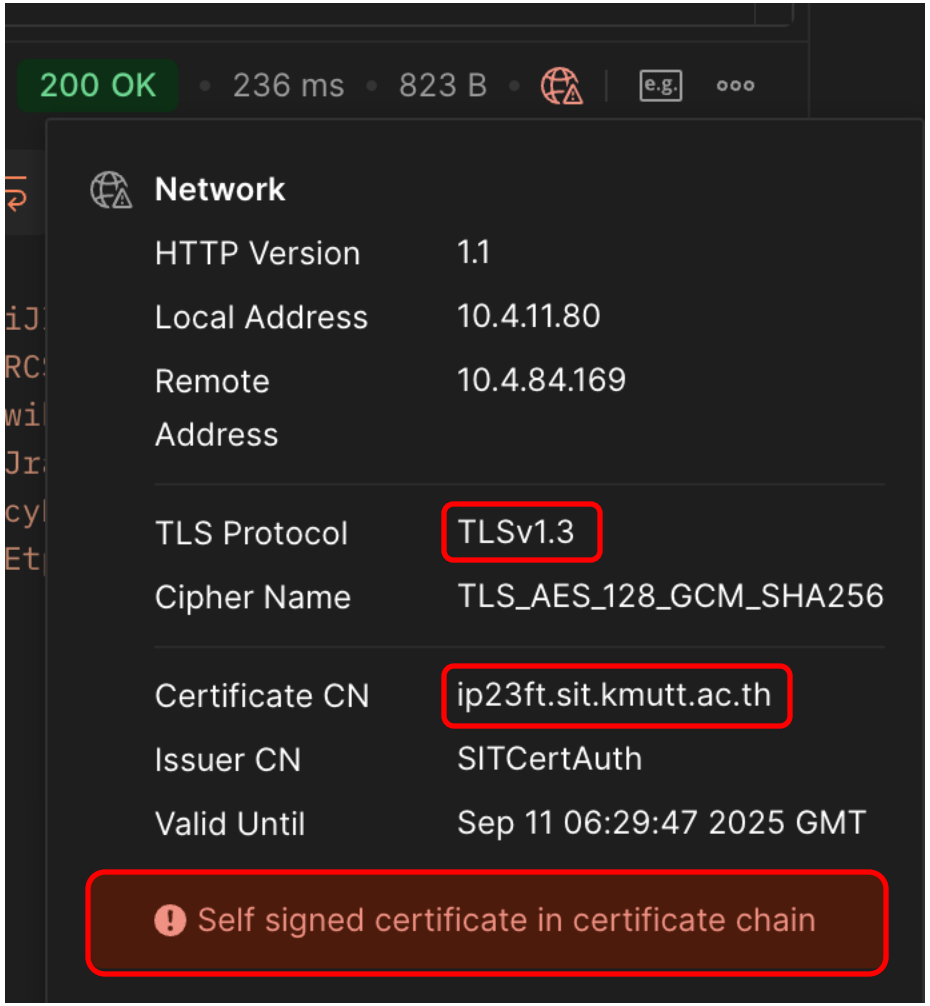
Infra conditions:

1. Use only TLSv1.3 protocol on port 443.
2. Un-secure connections must be redirected to the equivalent secure connection
3. (Optional) Config Tomcat (on backend) to accept only TLS v1.3 connections (port 8443)

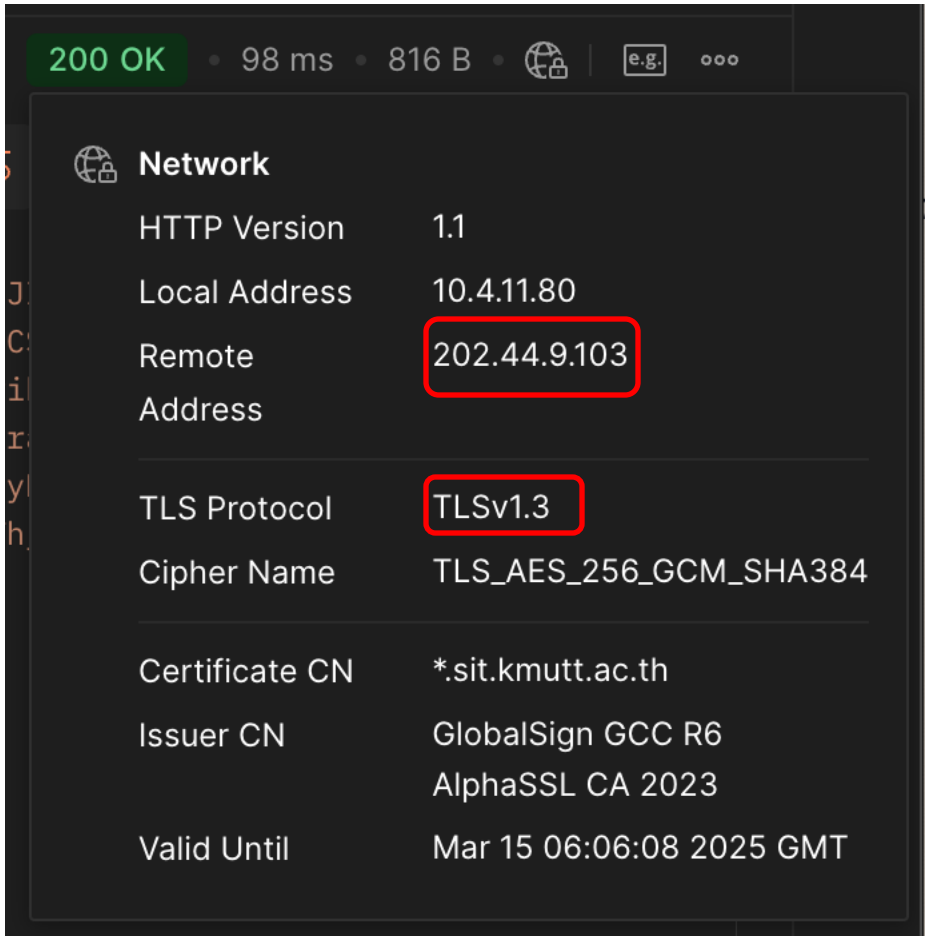
PBI21 SECURE-CONNECTION



PBI21 SECURE-CONNECTION



ip23ft.sit.kmutt.ac.th/



intproj23.sit.kmutt.ac.th/ft/

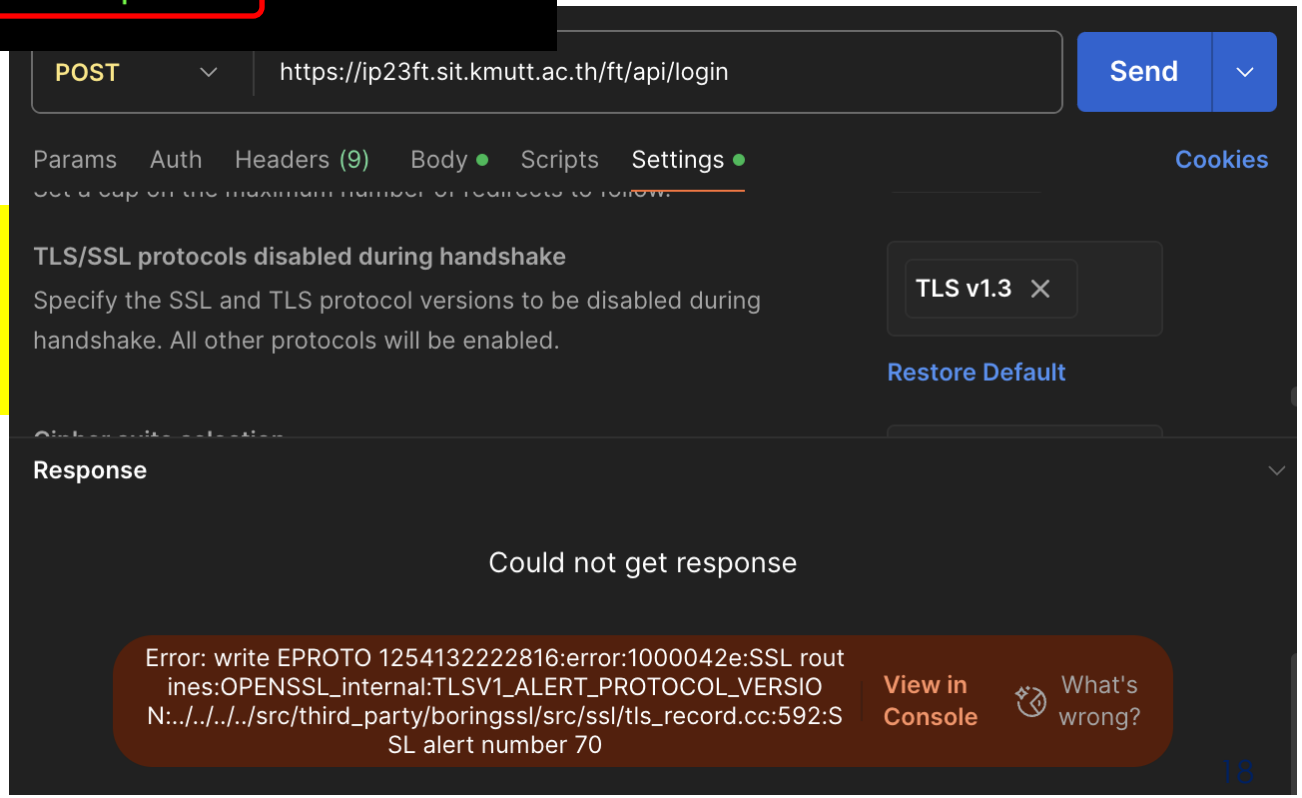
PBI21 SECURE-CONNECTION


```
olarnr@ORMBP-16 ~ % curl -v --tls-max 1.2 https://ip23ft.sit.kmutt.ac.th/ft/board
*   Trying 10.4.84.169:443...
* Connected to ip23ft.sit.kmutt.ac.th (10.4.84.169) port 443 (#0)
* ALPN: offers h2
* ALPN: offers http/1.1
*  CAfile: /etc/ssl/cert.pem
*  CApath: none
* (304) (OUT), TLS handshake, Client hello (1):
* error:1404B42E:SSL routines:ST_CONNECT:tlsv1 alert protocol version
* Closing connection 0
curl: (35) error:1404B42E:SSL routines:ST_CONNECT:tlsv1 alert protocol version
olarnr@ORMBP-16 ~ %
```

curl -v --tls-max 1.2 https://ip23ft.sit.kmutt.ac.th/ft/board

To test that your server is configured to use TLSv1.3 only, use Curl or postman as shown.

However, test this on private URL only.



PBI22 INSTANT-ACCESS

Login state and tokens are stored to allow instant access of the board when the webpage is re-open.

Business/technical conditions:

1. Authenticated user can use the system without having to sign-in again within 24 hours of the last valid sign-in.
2. 'Refresh' token which is valid for 24 hours is generated when the user is successfully signed-in.
3. The refresh token is used to request new access token (valid for 30 minutes) at /token.
4. If the refresh token has expired or is invalid, the user must sign-in again.

PBI22 INSTANT-ACCESS -- FE

Login state and tokens are stored to allow instant access of the board when the webpage is re-open.

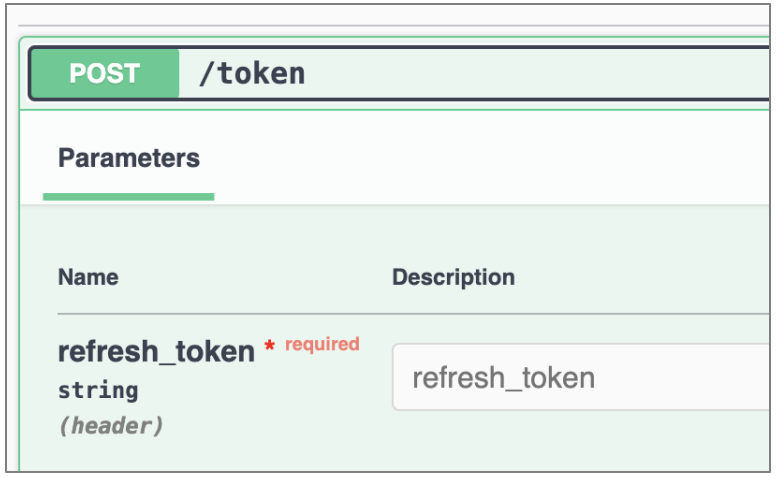
1. Store access token and refresh token on local storage (client machine) or more secure mechanism (such as http-only secure cookie)
2. When open a new webpage, the client looks for the stored tokens. If the token is not found, redirect to /login page.
3. If the token are found, the client attempts to access the BE with the stored token.
4. If the access token is valid, use the token to access the service until the access token has expired.
5. If the access token has expired or invalid, the client sends a request to /token using the stored refresh token (in the header of the request) to get a new access token:
   200: store new access token in-place of the old access token
   401: reset authentication state and redirect to login page
   no refresh token: reset authentication state and redirect to login page
   anything else: show message "There is a problem. Please try again later."

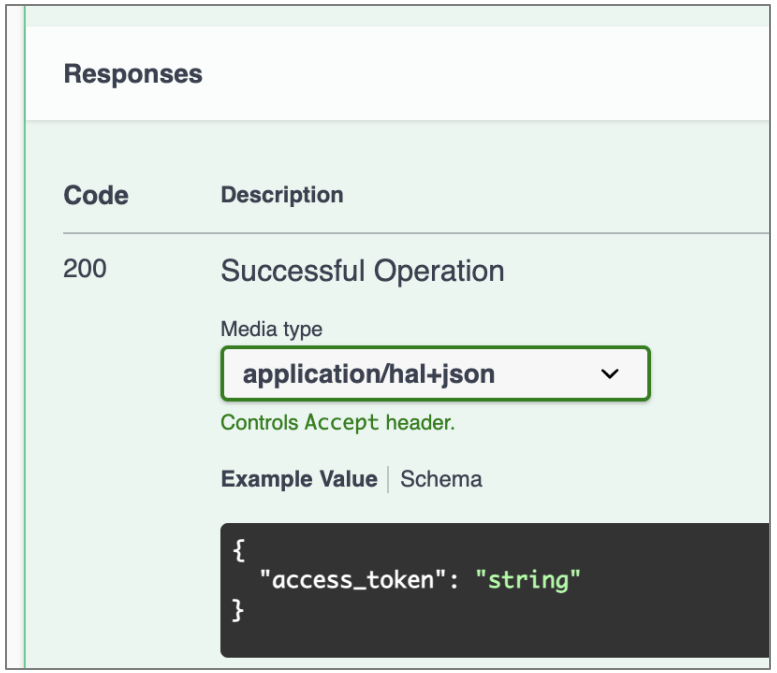
PBI22 INSTANT-ACCESS -- BE

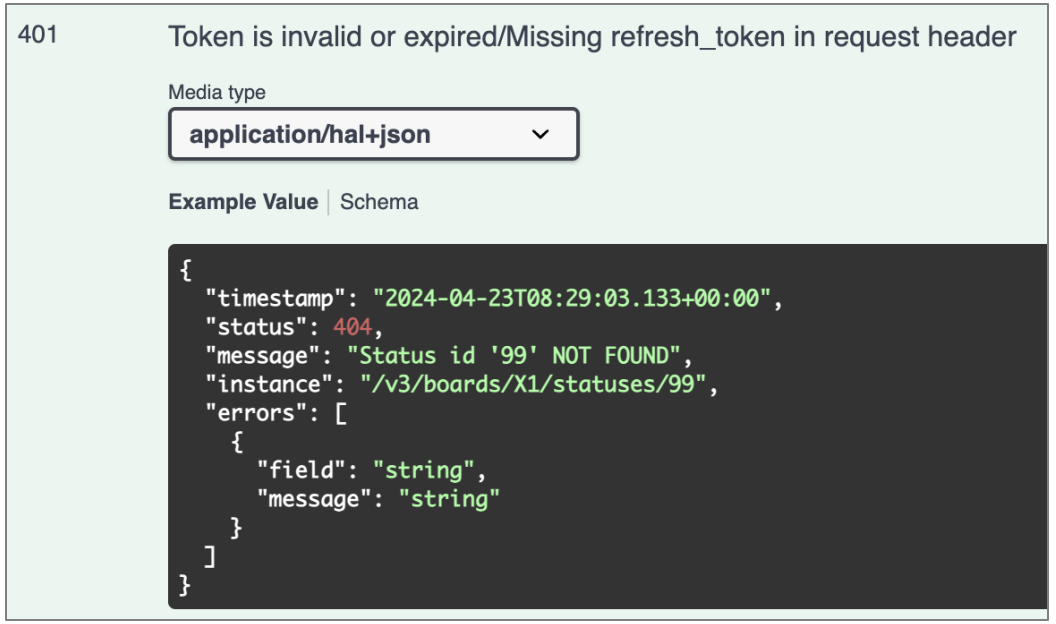
Login state and tokens are stored to allow instant access of the board when the webpage is re-open.

1. Update /login endpoint to also return refresh_token with {iss, iat, exp, oid} claims (valid for 24 hours)
2. Add new endpoint [POST] /token that expect refresh_token in the header (bearer) with empty request body. Returns:
   - 200: with new access_token (as in PBI17), if the refresh_token is valid (not expired, not tampered with)
   - 401: otherwise

API Specifications for PBI22







PBI23 SIGN-OUT

Signed-in user can sign-out of the application

FE

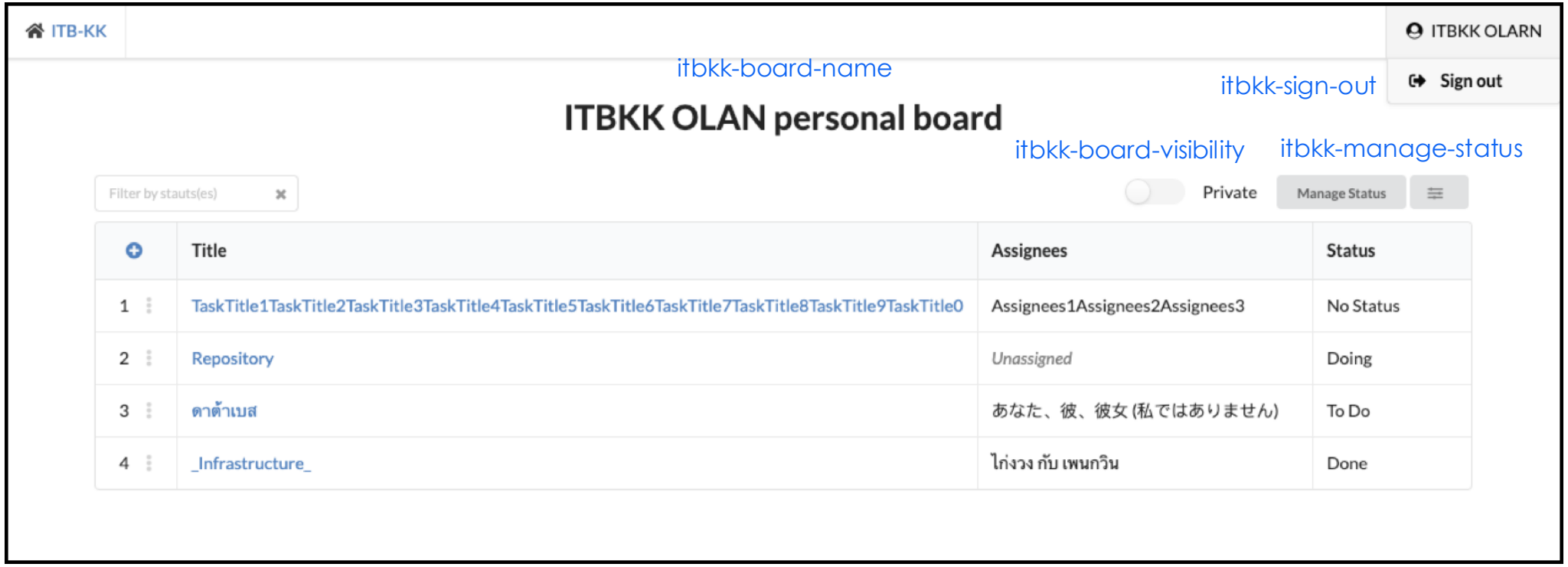
1. When the user is authenticated (PBI17, PBI22), add 'Sign-out' menu/button on every page (preferably with the username).
2. When the user click 'Sign-out', remove states and tokens from session/storage. Then, redirect to /login page.

Sample UI: Board (/board/:id)

Sign out

itbkk-home => /board

itbkk-fullname



Sprint 3 Test Cases

- Follows logically from the requirements
- Team should try to come up with test cases first
- Actual test cases will be released later

Sprint 4

- COLLAB-READ-ACCESS
  : owner can ADD, REMOVE collaborator to his/her board;
  collaborator with read access can view board/tasks/statuses
  collaborator can LEAVE

- COLLAB-WRITE-ACCESS
  : collaborator with write access can also manage tasks/statuses,
  but not board