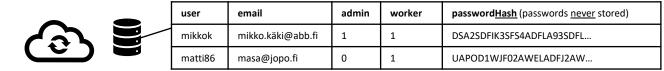
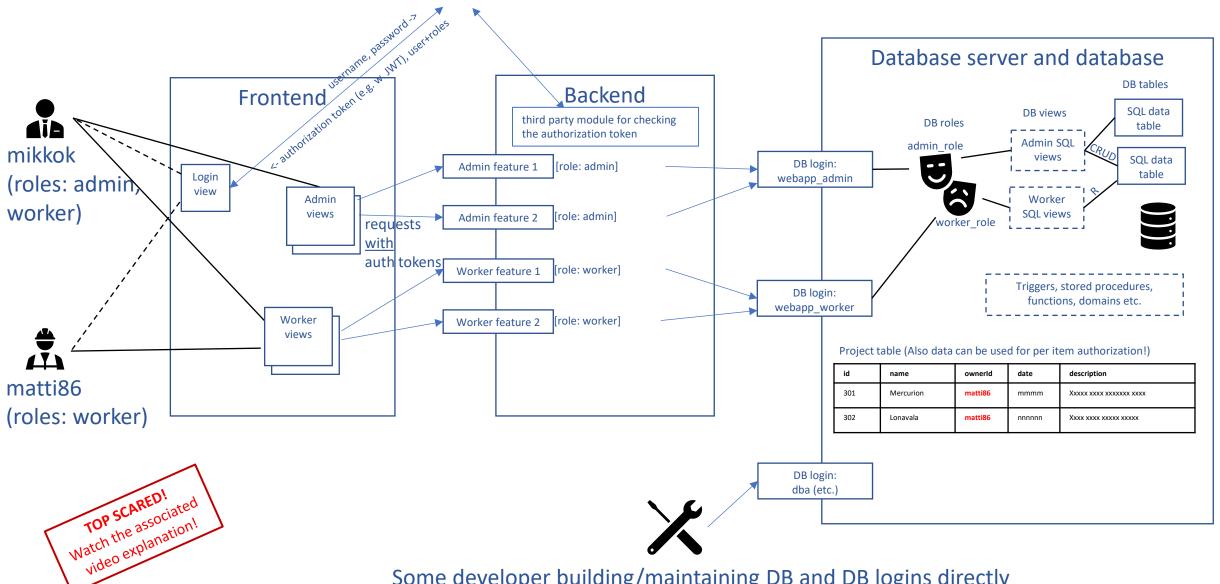
Explanation about Authentication and Authorization in a full-stack app

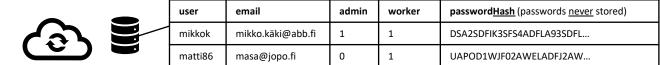
- Frontend
- Possible third party authentication/authorization service
- Backend
- Database server

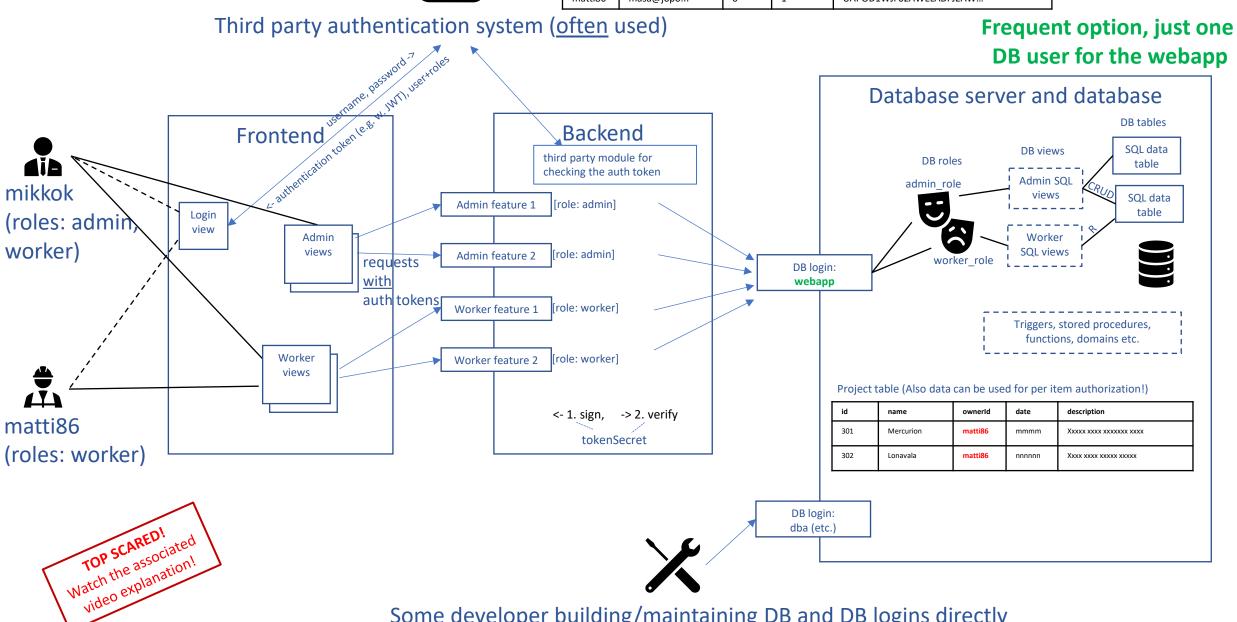


Third party auth system (often used). E.g. w. OAuth tokens



Some developer building/maintaining DB and DB logins directly





Some developer building/maintaining DB and DB logins directly

email isAdmin isPlanner passwordHash (passwords never stored) user mikkok mikko.käki@abb.fi DSA2SDFIK3SFS4ADFLA93SDFL.. One example project case 0 matti86 masa@jopo.fi UAPOD1WJF02AWELADFJ2AW... Frequent option, just one DB user for the webapp Database server and database **DB** views **DB** tables **Backend** Frontend DB roles (not used in (not used in SQL data this case) Library module for this case) table username, password -> Login feature generating/checking view_authentication token (e.g. w. JWT), user+roles the auth token mikkok SQL data CRU table (roles: admin), Admin feature 1 [role: admin] planner) SQL data views further table User DB login: Admin feature 2 [role: admin] requests jyser3 with auth token Triggers, stored procedures [role: planner] Worker feature 1 functions, domains etc Worker views Worker feature 2 [role: planner] Project table (Also data can be used for per item authorization!) name ownerId date description <- 1. sign, -> 2. verify matti86 301 matti86 Mercurion Xxxxx xxxx xxxxxx xxxx mmmm tokenSecret (roles: 302 matti86 Lonavala nnnnnn Xxxx xxxx xxxxx xxxxx planner) DB login: root Watch the associated video explanation!

Some developer building/maintaining DB and DB logins directly

SECURITY NOTES

Especially when database server usually is on another server, behind the internet and firewall, consider these:

- Call you DB user something else than 'app', 'webapp', or 'webapp_user', or 'backend' like 50-90% of the developers call it
 - e.g. call it 'bunker_rat' or 'sochi', those would not be any criminals guesses. Or, maybe they are now, so maybe something else random.
- Whitelist/allow in only those IP addresses from where database connections are allowed.
 - Backend server
 - DBA (database admins computer)
- In all security related aspects, write/collect them to one document and harden them before publishing any systems!