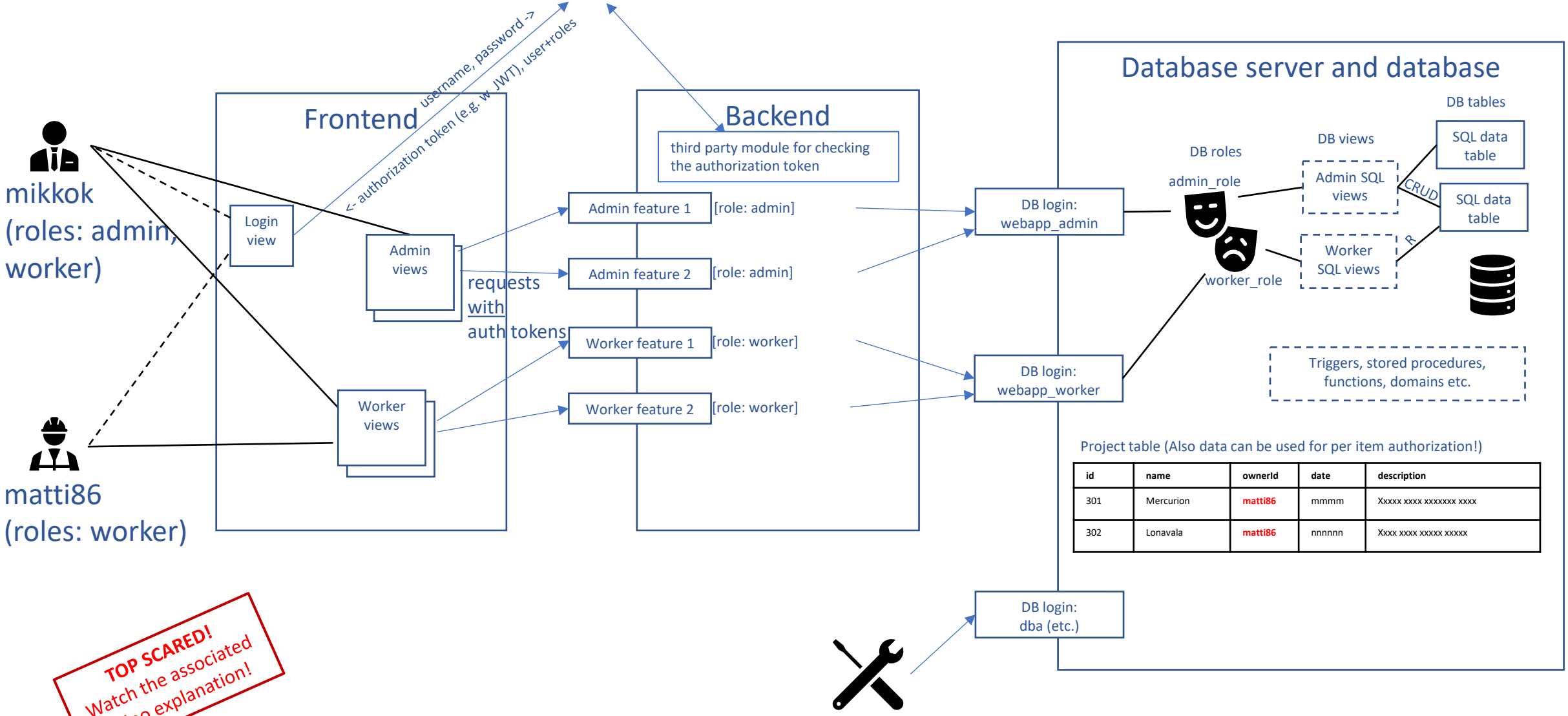
Explanation about Authentication and Authorization in a full-stack app

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

user	email	admin	worker	passwordHash (passwords never stored)
mikkok	mikko.käki@abb.fi	1	1	DSA2SDFIK3SFS4ADFLA93SDFL…
matti86	masa@jopo.fi	0	1	UAPOD1WJF02AWELADFJ2AW…

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



Project table (Also data can be used for per item authorization!)

id	name	ownerId	date	description
301	Mercurion	matti86	mmmm	Xxxxx xxxx xxxxxxx xxxx
302	Lonavala	matti86	nnnnnn	Xxxx xxxx xxxxx xxxxx

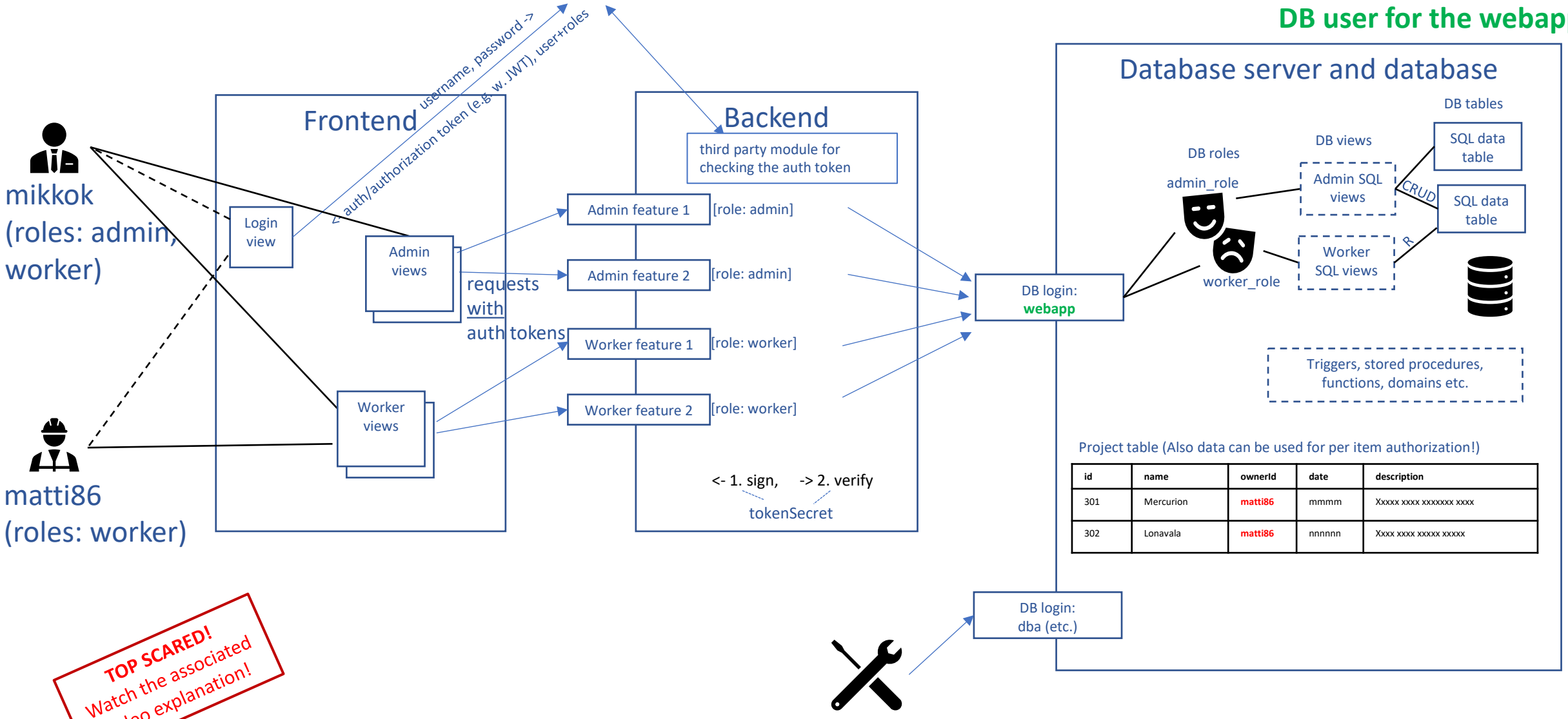
TOP SCARED!
Watch the associated video explanation!

Some developer building/maintaining DB and DB logins directly

user	email	admin	worker	passwordHash (passwords never stored)
mikkok	mikko.käki@abb.fi	1	1	DSA2SDFIK3SFS4ADFLA93SDFL…
matti86	masa@jopo.fi	0	1	UAPOD1WJF02AWELADFJ2AW…

Third party authentication system (often used)

Frequent option, just one DB user for the webapp



Project table (Also data can be used for per item authorization!)

id	name	ownerId	date	description
301	Mercurion	matti86	mmmm	Xxxxx xxxx xxxxxxx xxxx
302	Lonavala	matti86	nnnnnn	Xxxx xxxx xxxxx xxxxx

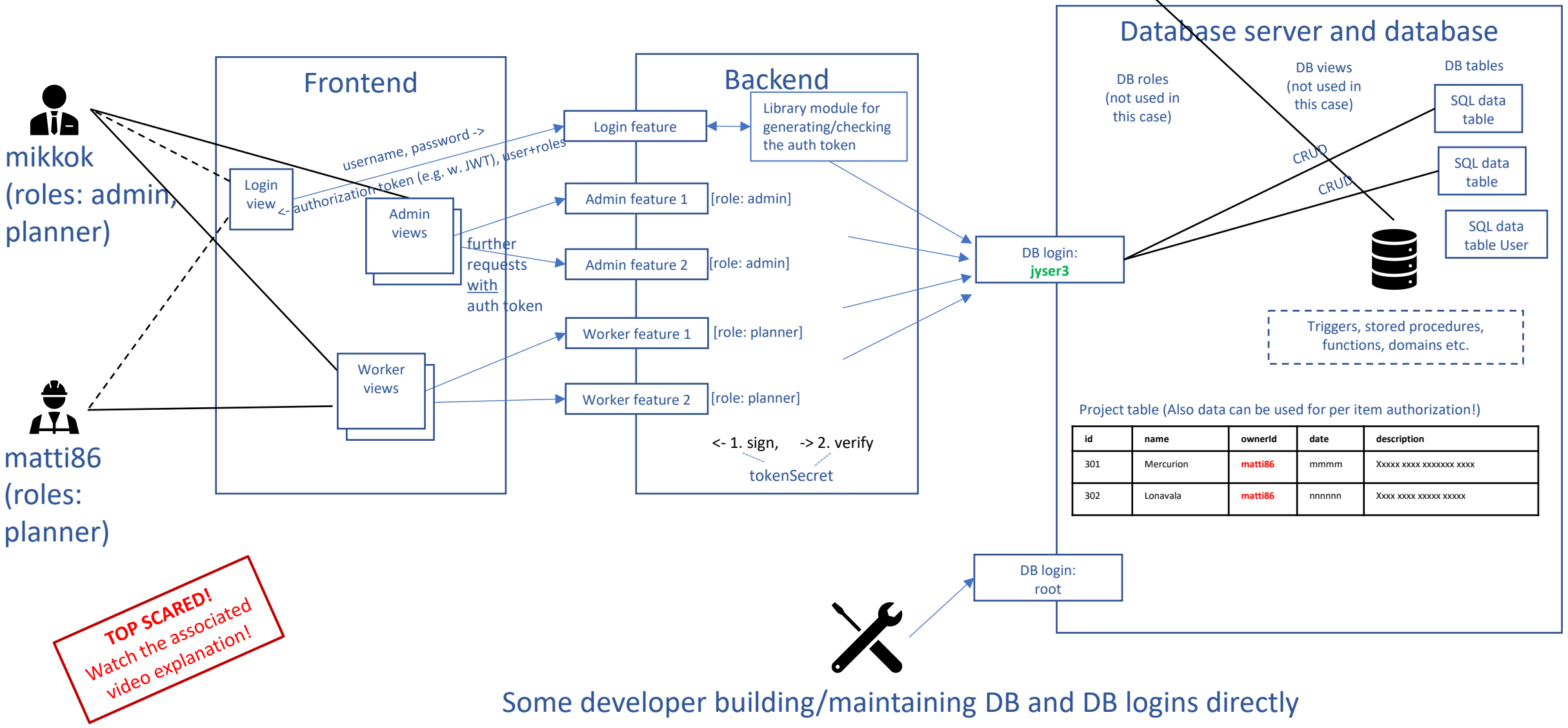
TOP SCARED!
Watch the associated video explanation!

Some developer building/maintaining DB and DB logins directly

One example project case

user	email	isAdmin	isPlanner	passwordHash (passwords never stored)
mikkok	mikko.käki@abb.fi	1	1	DSA2SDFIK3SFS4ADFLA93SDFL…
matti86	masa@jopo.fi	0	1	UAPOD1WJF02AWELADFJ2AW…

Frequent option, just one DB user for the webapp



id	name	ownerId	date	description
301	Mercurion	matti86	mmmm	Xxxxx xxxx xxxxxxx xxxx
302	Lonavala	matti86	nnnnnn	Xxxx xxxx xxxxx xxxxx

TOP SCARED!
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!**