

Programmeerimine II

HKI5003.HK

MARTTI RAAVEL

MRT@TLU.EE

3. loeng

- ▶ Tagasiside
- ▶ Kodused tööd
- ▶ Bcrypt, Middleware, JWT

Bcrypt

Funktsioon paroolide krüpteerimiseks

- Salt – juhuslikud andmed, mida lisatakse parooli krüpteerimise käigus
- Salt-rounds – aeglustab hashimise protsessi

Mis on middleware?

Middleware funktsioonid on funktsioonid, millel on juurdepääs päringuobjektile (req), vastuseobjektile (res) ja järgmisele funktsioonile rakenduse päringuvastuse tsüklis. Next funktsioon on Express-ruuteri funktsioon, mis käivitamisel käivitab middleware praeguse middleware'i järel.

Mida middleware teha saab?

- Käivitada koodi
- Teha muudatusi request ja response objektides
- Lõpetada request-response tsüklit
- Kutsuda välja järgjekorras järgmine middleware

Mida middleware teha saab?

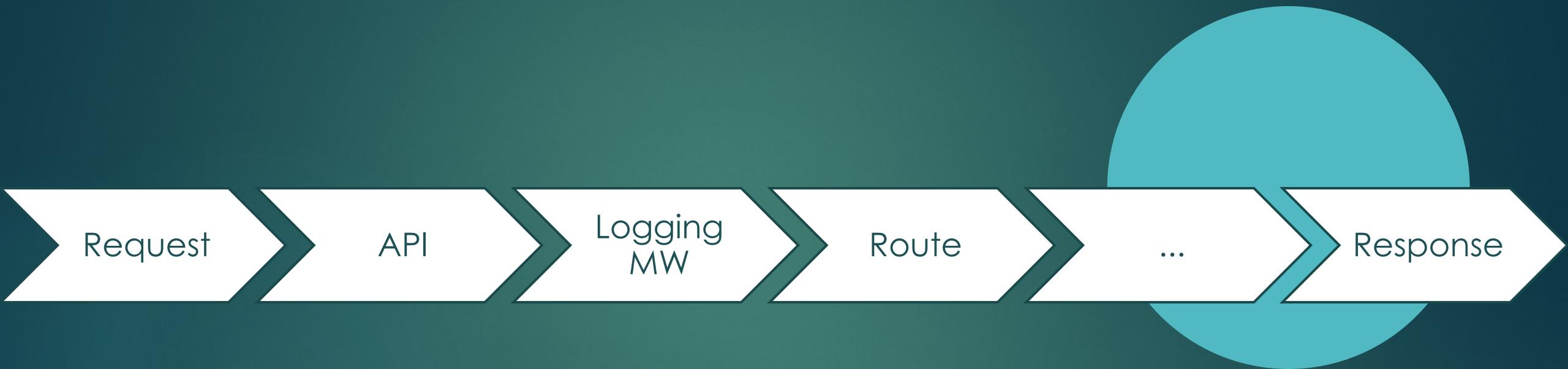
Kui middleware ei lõpetta päringu-vastuse tsüklit (näiteks `res.status(200).json(...)`), siis peab middleware kutsuma välja `next()` funktsiooni, muidu jäääb rakendus ‘rippuma’

Middleware kasutamine

```
// Logging middleware
const logger = (req, res, next) => {
  console.log(new Date(), req.url);
  next();
}
```

```
// Register middleware
app.use(logger);
```

Middleware kasutamine



JWT

JSON WEB TOKEN (JWT) on avatud standard, mis määratleb kompaktse ja iseseisva viisi teabe turvaliseks edastamiseks osapoolte vahel JSON-objektina. Seda teavet saab kontrollida ja usaldada, kuna see on digitaalselt allkirjastatud. JWT-sid saab allkirjastada parooliga või avaliku / privaatse võtmepaari abil RSA või ECDSA abil.

<https://jwt.io/introduction/>

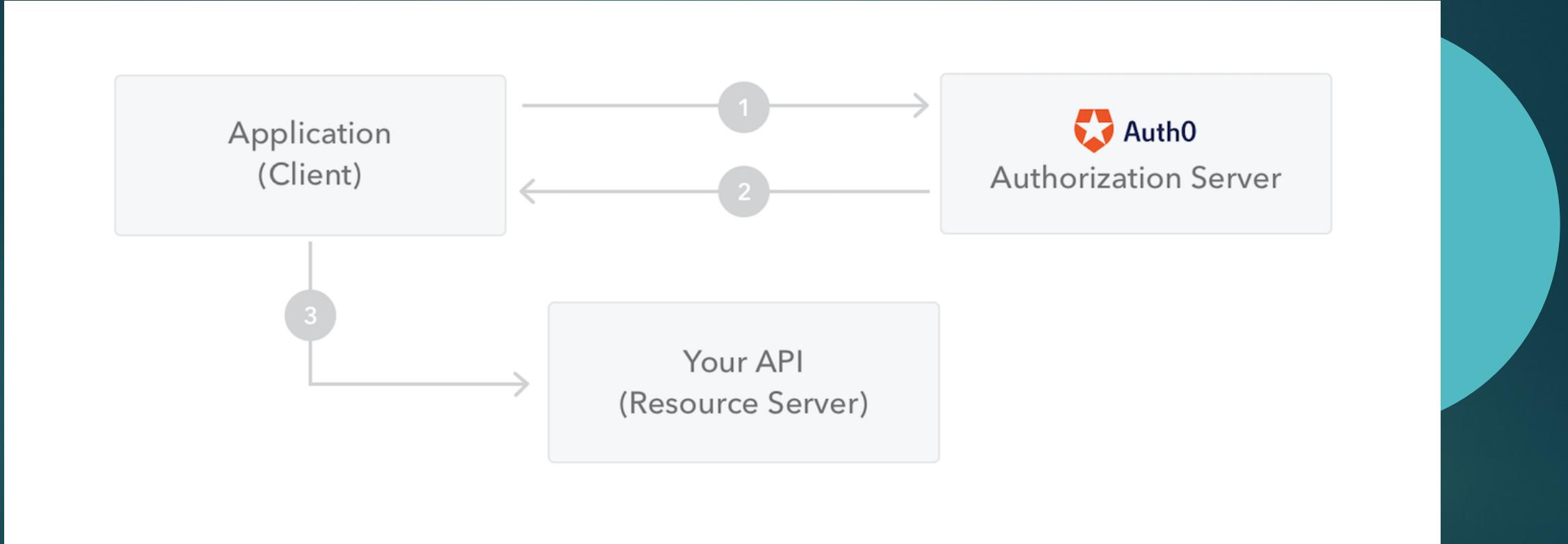
JWT struktuur

- Header
 - Päis koosneb tavaliselt kahest osast: loa tüübist, milleks on JWT, ja kasutatavast allkirjastamise algoritmist, näiteks HMAC SHA256 või RSA.
- Payload
 - Märgi teine osa on kasulik koormus, mis sisaldab nõudeid.
- Signature
 - Allkirjaosa loomiseks peate võtma kodeeritud päise, kodeeritud kasuliku koormuse, saladuse, päises määratud algoritmi ja sellele alla kirjutama.

Millal JWT-d kasutada

- **Autoriseerimine:** see on kõige tavalisem stsenaarium JWT kasutamiseks. Kui kasutaja on sisse logitud, sisaldab iga järgmine taotlus JWT-d, mis võimaldab kasutajal juurde pääseda selle märgiga lubatud marsruutidele, teenustele ja ressurssidele.
- **Teabevahetus:** JSON-i veebimärgid on hea viis turvaliselt osapoolte vahel teavet edastada. Kuna JWT-sid saab allkirjastada - näiteks kasutades avaliku / privaatse võtme paare -, võite olla kindel, et saatjad on need, kes nad end ütlevad. Lisaks, kuna allkiri arvutatakse päise ja kasuliku koormuse abil, saate ka kontrollida, kas sisu ei ole muudetud

JWT kasutamine



<https://cdn2.auth0.com/docs/media/articles/api-auth/client-credentials-grant.png>

Kodune töö

- ▶ Väljapääsupilet:
- ▶ <https://bit.ly/35pcOc3>
- ▶ Oma projektiarendamine –
paroolide hashimine, autentimine,
JWT