OST
Eastern Switzerland
University of Applied Sciences

# Distributed Systems & Blockchain (DS1)

## Admin

Thomas Bocek

12 August 2021

# Beratungswoche

- Exam: 16.08.2021 – 15:50 – 16:50 (4.101)
  - Check Terminplan for changes
  - Be there earlier (5-10min)
    - Zeit: 60 min.
    - Zuerst diese Hinweise, dann die Prüfungsteile ganz durchlesen.
    - Diese Prüfung ist "Closed Book".
    - Taschenrechner ist nicht erlaubt.
    - Sonst sind keine Hilfsmittel zugelassen; auch kein Handy oder Smart Watch.
    - Alle Antworten und Lösungen in diese Aufgabenblätter schreiben.
    - Keinen Bleistift und keine rote Farbe verwenden.
    - Die Antworten und Lösungen müssen nachvollziehbar sein. Bitte alles in leserlicher Schrift!
    - Keine Fragen während der Prüfung. Bei Unklarheiten sind sinnvolle Annahmen zu treffen und
    - diese klar zu dokumentieren.
    - Die Bewertungspunkte der Aufgaben können nach der Korrektur noch etwas variieren.

# Beratungswoche

- Allgemein / Kommen konkrete Fragen zu den News?
  - Nein, die Themen ändern sich rasant, deshalb sind die News Themen jeweils in dieser Woche relevant, danach nicht mehr. Diese News sollen ihnen aber zeigen, dass im Themengebiet «Verteilte Systeme und Blockchain» viel passiert. Zudem können sie Wissen aus der Vorlesung (z.B. HW will fail eventually) anknüpfen.
- Allgemein / Verstehe ich das richtig, dass sie keine Fragen zu den Interviews mit Moflix, AxLabs und den Challenge Task Präsentationen stellen werden?
  - Korrekt
- Allgemein / Dort wo man verschiedenen Sachen zur Auswahl hatte, z.B. Kubernetics oder DockerSwarm. Kommen nur theoretische, allgemein Fragen oder spezifische zu zum jeweiligen Syntax? Bez. Allgemein Syntax/Code gefragt oder eher theoretische Fragen?
  - Syntax ändert sich ebenfalls, und wichtiger ist die Theorie. Den Syntax bitte nicht auswendig lernen. Zum Nachschlagen gibt es immer noch das Internet.

# Beratungswoche

- Allgemein / Sehe ich das richtig, dass wir an der Prüfung von DS1 keinen Code (z.B.: GoLang, Yaml, Solidity,... ) schreiben müssen?
  - Ja, korrekt. Es wird keine Aufgabe geben, wo ihr Code schreiben müsst.
- Allgemein / Ich fand es schwierig, wie ausführlich die Antworten bei den jeweiligen Aufgaben ausfallen sollten. Könntest du dazu in der Vorbereitungswoche noch was sagen?
  - Ich werde in dieser Prüfung jeweils angeben in welchem Umfang ich die Fragen erwarte: z.B. Beantworten Sie die Frage in max. 2 Sätzen.

# Beratungswoche

| | | | |
|---|---|---|---|
| | [illegible] | | |
| 5 | Traefik ist ein Beispiel eines L4 und L7 Load Balancers | | |

- Bei der Aufgabe 3a5 setzt du voraus, dass wir von der Vorlesung noch alle Beispiele von Software kennen, welche du uns gezeigt hast. Ist dies der Fall, müssten wir bei jeder Software auswendig lernen, für was man diese brauchen kann und was sie genau macht?
  - Bei den Loadblancern habe ich Traefik, Caddy (neu im FS21), Nginx, und HAproxy genauer vorgestellt. Damit habt ihr euch im Challenge Task auch auseinandersetzen müssen, welchen ihr davon verwendet. Deshalb sollte diese Frage beantwortbar sein.

# Beratungswoche

- Folie: 04/16 / CORS: Allow-Origin:* ist ja nicht gut, aber was ist mit Allow-Origin: und die versch. Services (Domains/URL's) angeben? Ist doch auch eine sichere Möglichkeit? (Auch wenn Reverse Proxy flexibler ist)
  - Absolut! Allow-Origin:* erlaubt alles, fürs entwickeln ist das ok, aber wenn man Cross-Origin Resource Sharing im produktivem System braucht, dann unbedingt die Domains angeben.
- Folie: 04/11: LB und Docker "load balance between services and not between servers": Wie werden die duplizierten Services genau unterschieden? LB mit verschiedenen Server funktioniert ja mit versch. IP's, aber wie im Docker-Umfeld auf gleicher Maschine möglich, dort doch alles localhost?
  - Man kann die Unterscheidung per Port machen (Folie 4/9)
- Folie: 04/4: L4 LB mit QUIC: Wenn ich ein klassischen L4 Load Balancer habe, der UDP Pakete (stateless) an verschiedene Server senden, funktioniert dann ein Protokoll wie QUIC noch? (Da dieses ja statefull ist, jedoch erst auf L7)
  - Sehr gute Frage! Jein, L4 LB mit QUIC funktioniert wenn die Pakete an den gleichen Connection ID an den gleichen Rechner geschickt werden. Dazu muss der LB aber wissen dass es QUIC ist (was er im Prinzip nicht weiss). Als Fallback könnte man jeweils src IP und port verwenden um zu sehen wohin es geschickt werden soll. Dann funktioniert aber eine IP Wechsel des Senders nicht mehr. Die andere Frage ist, ob es LB für UDP überhaupt braucht. Hier eine Diskussion

# Beratungswoche

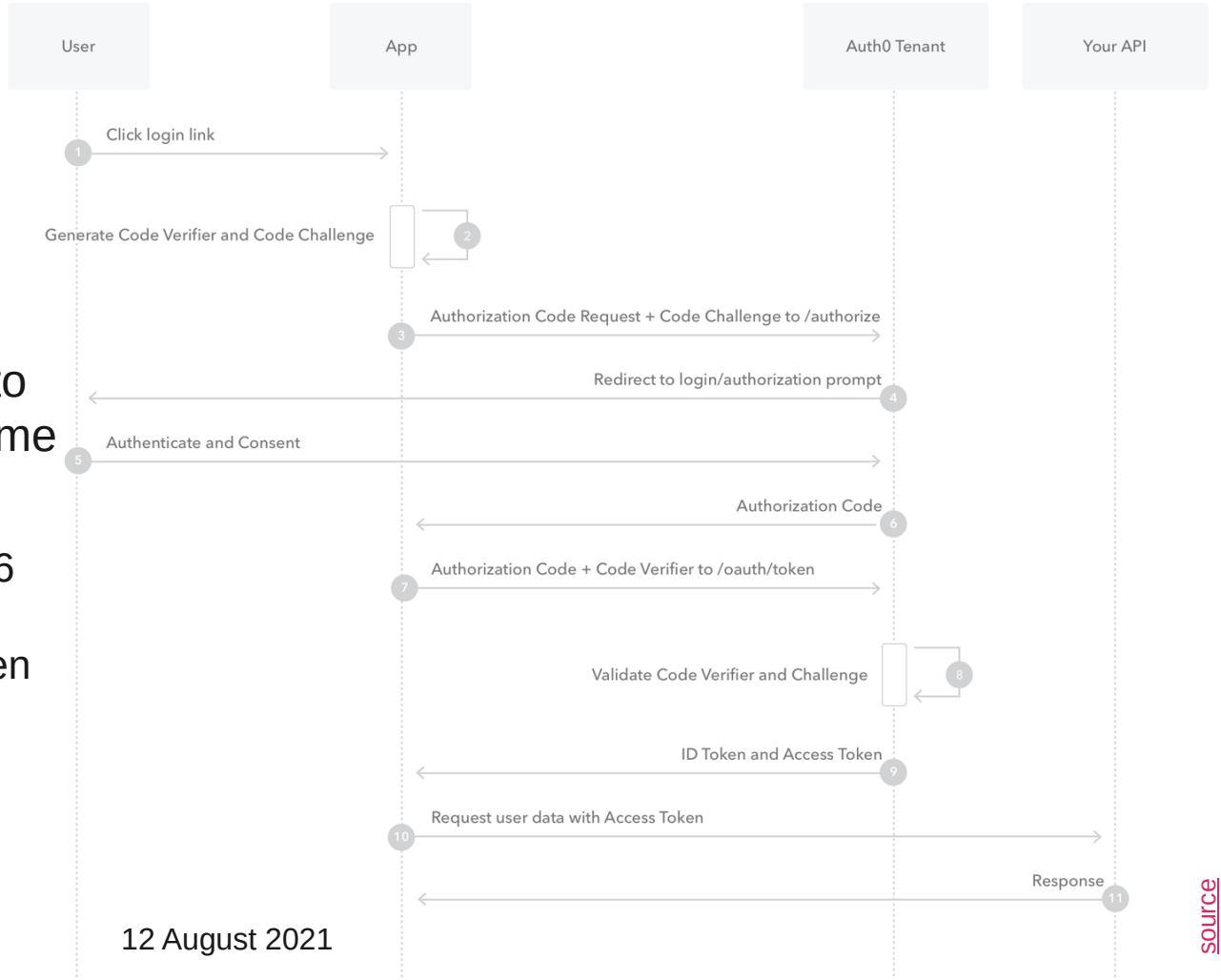
- Folie: 04/4: LB L4&L7 mit HTTPS: Wo wird genau terminiert? Warum mit L4 kein HTTPS möglich wenn TLS auf L4 läuft (HTTPS = HTTP+TLS)?
  - Ein L7 load balancer terminiert die TLS Session, und erstellt eine neue Anfrage. TLS ist Layer 7. Layer 4 kennt nur IP/Port, kein TLS, und kann deswegen auch TLS nicht terminieren.
- Folie: 05/6: Ist DigestAuth überhaupt zu empfehlen wenn nur SHA (MD5) genützt werden kann? Gemäss CySec-Module sollte SHA nie für PW's benützt werden (auch nicht SHA-256..512)!Falls Ja: DigestAuth somit auch ohne HTTPS sicher?
  - Ich empfehle DigestAuth nicht, wenn HTTPS verwendet wird, kann man auch BasicAuth verwenden. Die Komplexität ist geringer, und die nonce und das gehashte Passwort bringen wenig Mehrwert wenn HTTPS verwendet wird. Auch DigestAuth würde ich nicht ohne HTTPS verwenden.
- Folie: 05/7: Wie ist das Diagramm genau zu verstehen? Auth auch zwischen LB und Services? Der Load Balancer muss ja fast zwingend HTTPS derminieren und kann nicht nur durchreichen (aktive Sockerts)?
  - Ja, zwischen LB und Services sollte man die Connection ebenfalls verschlüsseln (wenn es nicht auf dem gleichen Rechner läuft). Da bietet es sich an langlebige Zertifikate zu erstellen.

# Beratungswoche

- Bitcoin difficulty
  - Miner Antminer S19: 95 TH/s – can check 95 x 1000 x 1000 x 1000 x 1000 SHA256 hashes in 1 second
  - Block 695381 Hash: 00000000000000000ff94f4614e9aeefef1a9d97da8e57e7cd12014e927660
    - In order to have 4 zeros, you need on average 16^4 hashes to calculate (example) – 16, as its hexadecimal and hashes are uniformly distributed, so 4 zeros are as likely as any other value, thus 16^4.
    - For, 19 zeros, you need 16^19 to calculate (we are guestimating)
      - I mentioned 2^64 in the lecture (which is wrong)
  - How much Antminer do I need to check 16^19 hashes in 10min? (10min = 600s)
    - 16^19 / 95TH/s x 600 = 1’325’576
    - Cross-check with ~100m TH/s in the whole bitcoin network: with 1m S19 miners, you would end up with 95m TH/s, which is in that range (guestimation!)

# Beratungswoche

- PKCE – the figure in the slides 05/13 is not precise enough to explain why code-verifier and code-challenge are important
  - Here we have User and App separated, App is accessing API on behalf on user
  - code_challenge = hash(random string)
    code_verifier = random string
  - With code_challenge/ code_verifier we want to ensure, that the request 3 comes from the same App as the request 7
    - Attack scenario: Auth0 Tenant sends in request 6 the code to the wrong App (due to attack), with code_challenge/code_verifier, the id/access token is not created



# Q&A