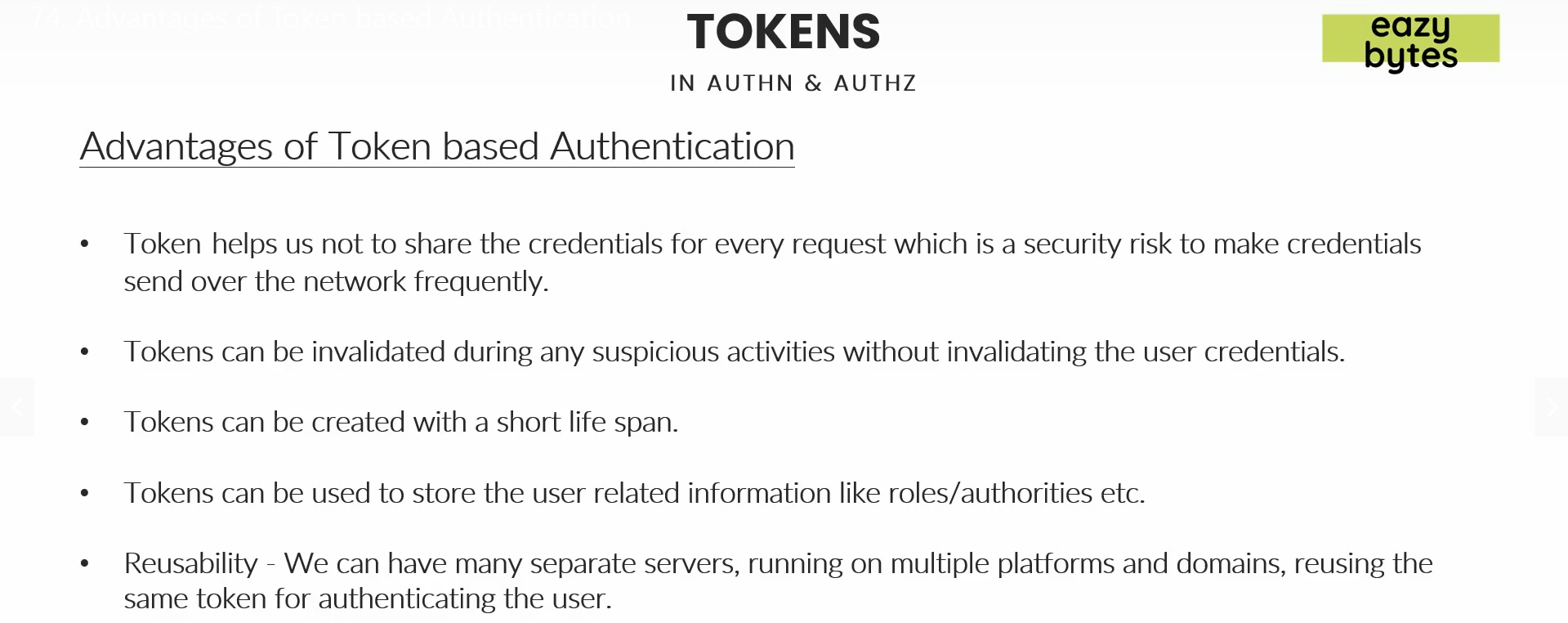
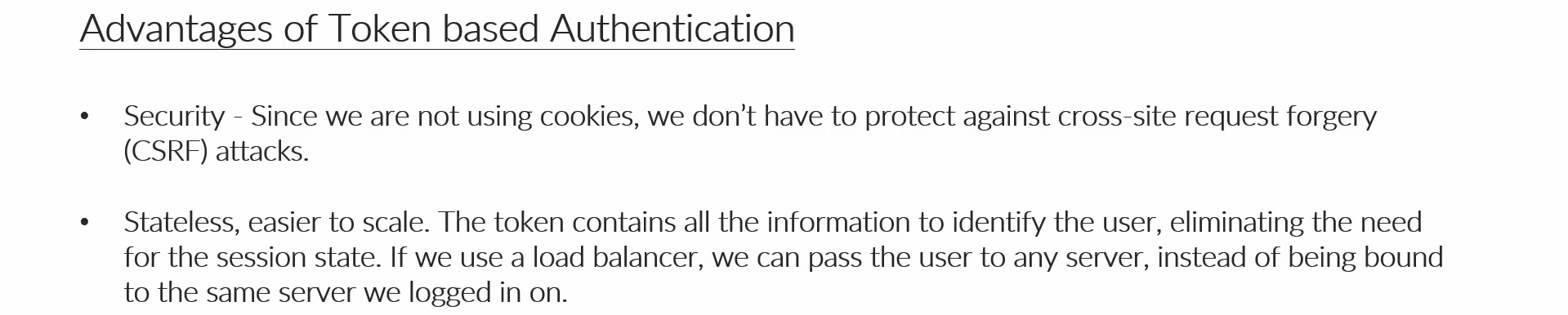
1.  
2. **Sharing credentials only once**:
   1. Compare with hotel scenario where you prove your authentication only once with receptionist and the receptionist gives you access card that access card is the token you use every time you access your room, restaurant
3. **Invalidate Token**:
   1. If credentials are invalidated, the user has to call the call centre or reset the password which is cumbersome process.
4. **User related info inside token**:
   1. Email, Mobile numbers etc. in encrypted or encoded format so that such info can be consumed on the client slide.
5. **Reusability**:
   1. In microservice app.
6. **Security**:
   1. We don’t maintain JWT token as cookie so it saves us from CSRF (Cross Site Request Forgery) attack.  
      As we know JSESSIONID is maintained as cookie on browser side.
7. 