Spring Professional Exam Tutorial v5.0

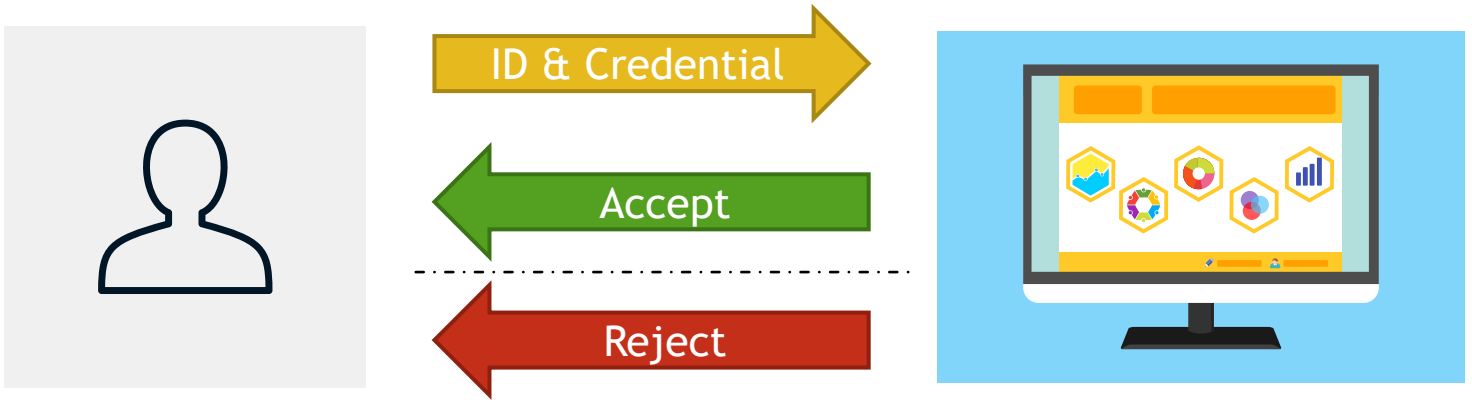
Question 01

Question 01 - What are authentication and authorization? Which must come first?

Authentication is a process of verifying that user, device or external system is who he/she/it claims to be. It involves validation that submitted proof of identity is true.

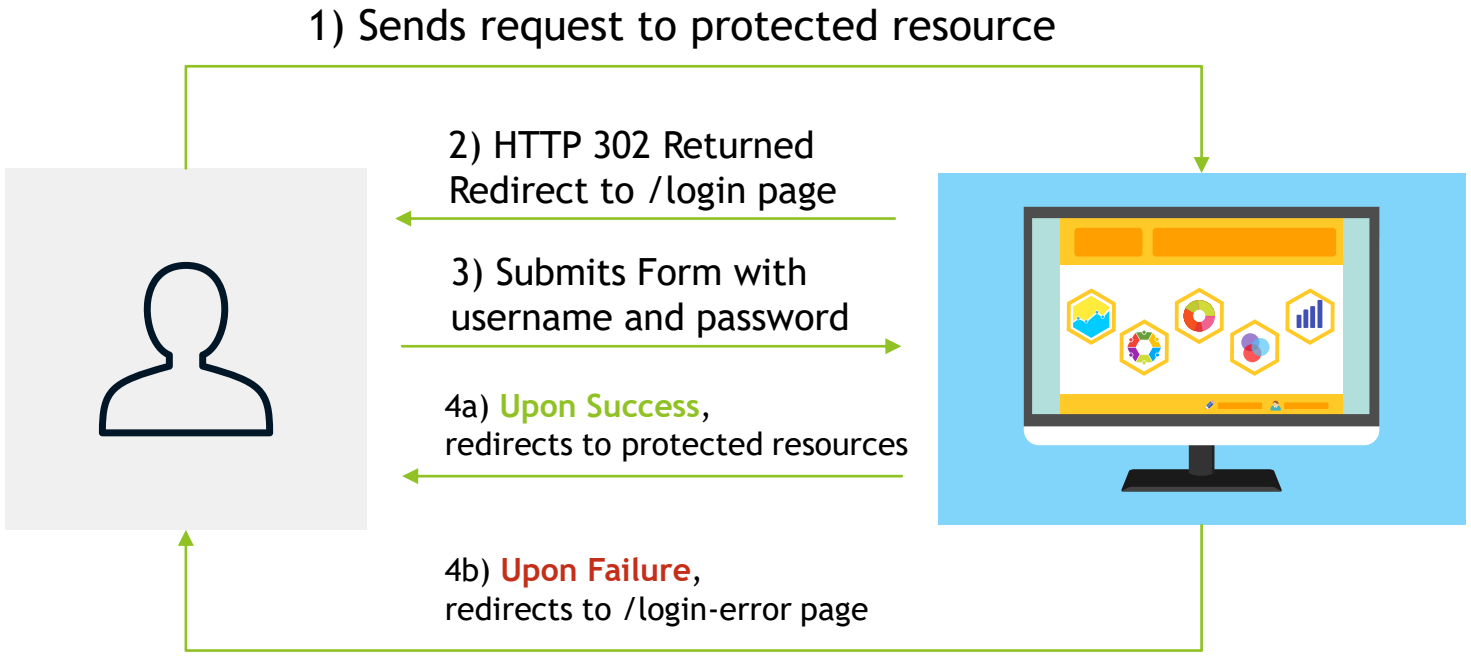
In other words, authentication answers question “Who are you?”, and checks if provided answer is valid.

Process usually involves one side sending Identity and Credential that is used to validate that Identity statement is true, and other side that checks Credential and accepts or rejects claimed Identity based on Credential.



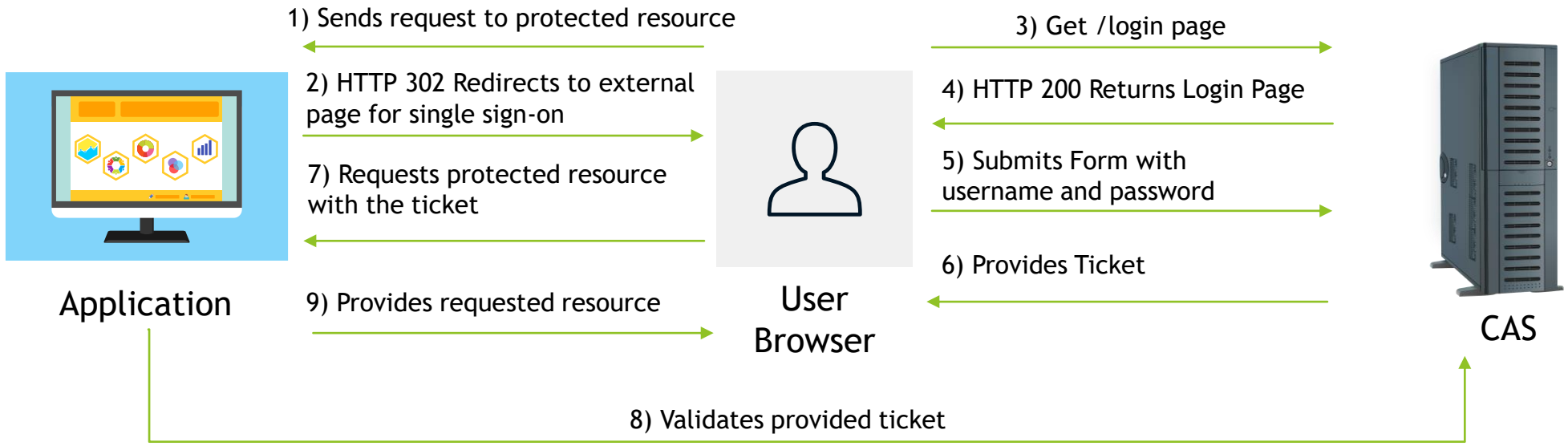
Question 01 - What are authentication and authorization? Which must come first?

Authentication may take different forms, simplest one uses username as Identity and password as credential – proof of identity.



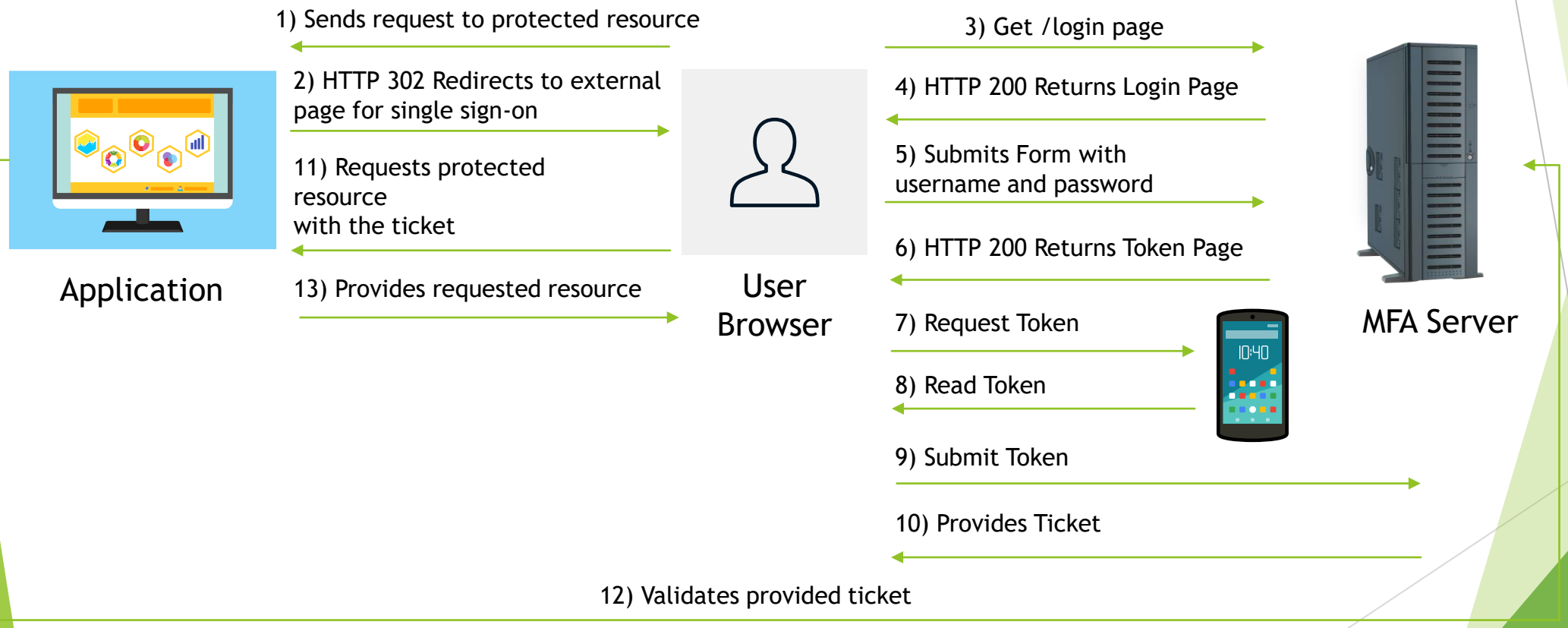
Question 01 - What are authentication and authorization? Which must come first?

More sophisticated forms of authentication, may involve three parties for implementation of Central Authentication Service (CAS) to allow single sign-on.



Question 01 - What are authentication and authorization? Which must come first?

Recently, Multi Factory Authentication is becoming more popular to provide greater degree of security.



Question 01 - What are authentication and authorization? Which must come first?

Spring Security provides following support for Authentication:

- Username/Password Authentication
  - Form Login
  - Basic Authentication
  - Digest Authentication
- Remember-Me Authentication
- OpenID Support
- CAS Authentication (single sign-on)
- X.509 Certificate Authentication
- OAuth 2.0 Login
- SAML2

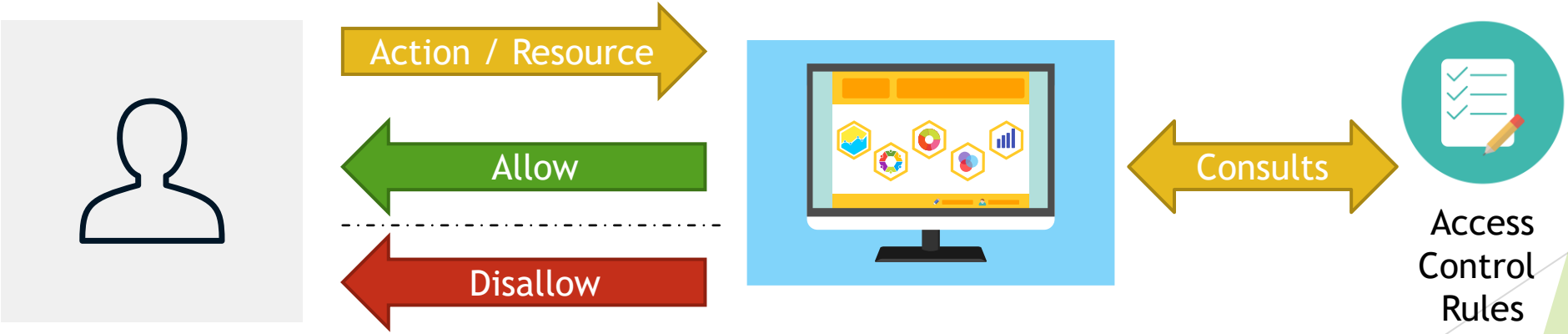
- Storage Mechanism
  - Simple Storage with In-Memory Authentication
  - Relational Databases with JDBC Authentication
  - Custom data stores with UserDetailsService
  - LDAP storage with LDAP Authentication
- Password Encoders:
  - bcrypt
  - PBKDF2
  - scrypt
  - argon2
  - sha256
  - …

Question 01 - What are authentication and authorization? Which must come first?

Authorization is a process of determining whether an authenticated user is allowed to access certain resources within the system or allowed to perform a certain action within the application.

In other words, authorization answers question “What are you allowed to do?”.

Authorization usually uses formalized policy specified as access control rules, to determine allowed and disallowed parts of the system that authenticated user can visit and act upon.



Question 01 - What are authentication and authorization? Which must come first?

Spring Security allows you to implement **authorization** within your application on two levels:

- Web Security Level with usage of Expression
  - `mvcMatchers("/admin/**").hasRole("ADMIN")`
- Method Security Level with usage of:
  - `@Secured` annotation
  - `@PreAuthorize` annotation
  - `JSR 250` annotations
    - `@RolesAllowed`
    - `@PermitAll`
    - `@DenyAll`
    - `...`

Question 01 - What are authentication and authorization? Which must come first?

Access Control Rules can be expressed via:

- Roles
  - Represents a high-level set of privileges, for example `ROLE_ADMIN`, `ROLE_STAFF`, `ROLE_CUSOMERS` etc.
  - Used with expressions like `hasRole`
- Authorities
  - Represents a low-level, granular privilege/authority in the system for example `READ_CUSTOMERS`, `DELETE_EMPLOYEE`, `ACCESS_API` etc.
  - Used with expressions like `hasAuthority`
- Hierarchical Roles
  - Allows you to specify relationships between roles and express that one role includes all permissions granted to other role
  - Example:
    - `ROLE_ADMIN > ROLE_STAFF` - `ROLE_ADMIN` includes `ROLE_STAFF`

Question 01 - What are authentication and authorization? Which must come first?

Authentication needs to be executed first, before **authorization**, because for authorization process to know which roles/authorities can be granted for particular user, system needs to be sure that user is who he/she claims to be.