|  |  |
| --- | --- |
| Authentication | * Là 1 hành động nhằm thiết lập hoặc chứng thực một thông điệp hoặc 1 đối tượng nào đó đáng tin cậy. Sau khi xác thực thành công thì có thể tin tưởng vào thông điệp hoặc thông báo mà đối tượng đưa ra. |
| Authorization | * Là quá trình xác định xem một người dùng có quyền truy cập một tài nguyên cụ thể để thực hiện một số hành động hay không * Việc cấp quyền không thể được tiến hành mà không có sự xác thực đi kèm |
| Các cơ chế xác thực Authentication | • HTTP Basic: là phương thức dể client cung cấp username và password khi thực hiện yêu cầu.  • Cookies  • Tockens: Json Web Token là 1 tiêu chuẩn mở định nghĩa cách thức truyền tin an toàn giữa các thành viên bằng một đối tượng json. Thông tin này có thể xác thực và đánh dấu tin cậy nhờ vào “chữ ký” của nó. Phần chữ ký của JWT sẽ đc mã hóa bằng HMAC  - Gồm 3 thành phần:  + Tiêu đề, chứa loại mã thông báo và thuật toán Hash  + Size, chứa xác nhận quyền sở hữu  + Chữ ký  • Signature: chữ ký số khóa công khai là 1 mô hình sử dụng các kỹ thuật mật mã để gán vs mỗi người sử dụng 1 cặp khóa công khai – bí mật và qua đó có thể ký các văn bản điện tử cũng như trao đổi các thông tin mật. Khóa công khai sẽ thường đc phân phối thông qua chứng thực khóa công khai  • One-time password: cơ chế xác thực 1 lần trong 1 khoảng thời gian nhất định  • Certificate  • OAuth2: xác thực thông qua các udung khác (gg, facebook,…) |
| Spring sercurity | * Là 1 dự án trong hsthai của spring, cung cấp các dịch vụ bảo mật toàn diện cho các ứng dụng doanh nghiệp có nền tảng java EE * Là 1 framework tập trung vào việc authentication (xác thực) và authorization (phân quyền) trong 1 udung   + Authentication: là tiến trình thiết lập 1 principal (1 ng, 1 thiết bị, 1 hệ thống có thể thực hiện 1 hành động nào đó  + Authorication: là tiến trình quyết định 1 principal có đc phép hành động trong ứng dụng hay k |
|  |  |