Bkav®

Bkav Single Sign On

Phần mềm quản lý xác thực tập trung

SSO

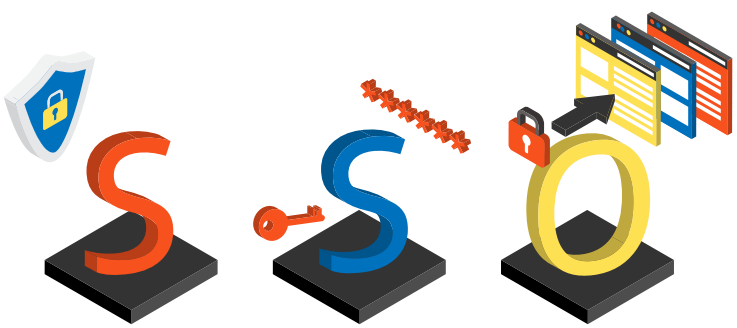
1. Giới thiệu

Phần mềm quản lý xác thực tập trung - Bkav Single Sign On (Bkav SSO) được xây dựng để đơn giản hóa việc truy cập an toàn vào các website và ứng dụng (Ứng dụng Web, hoặc Mobile) của mỗi cá nhân trong một cơ quan, đơn vị, tổ chức. Sử dụng phần mềm Bkav SSO, người dùng chỉ cần đăng nhập một lần và ghi nhớ một tài khoản

Bkav SSO tập trung vào việc đơn giản hóa việc truy cập an toàn vào ứng dụng web và thiết bị cho nhân viên và đối tác của tổ chức và đơn giản hóa quản lý khách hàng. Giải pháp cho phép tổ chức cung cấp cho nhân viên, khách hàng và đối tác truy cập an toàn vào các ứng dụng của tổ chức từ bất kỳ loại thiết bị nào.

2. Đặc điểm nổi bật của giải pháp

- **Hỗ trợ xác thực một lần qua giao thức SAML2, OpenId Connect, và WS-Federation Passive**
- **Hỗ trợ xác thực đa nhân tố**
- **Hỗ trợ nhiều kho người dùng**
- **Quản lý đăng nhập một lần và ủy quyền xác thực**
- **Cung cấp các cơ chế xác thực bảo mật**
- **Quản trị và quản lý định danh**
- **Cung cấp SSO cho nhân viên để loại bỏ nhu cầu quản lý nhiều mật khẩu.**
- **Kích hoạt khả năng liên doanh (federation) để chia sẻ thông tin một cách an toàn với các bên đối tác.**
- **Bảo vệ tài nguyên bằng cách cung cấp truy cập chỉ cho người dùng được ủy quyền.**
- **Đảm bảo rằng người dùng được ủy quyền có thể truy cập tài nguyên bất kể địa điểm hoặc loại thiết bị mà họ sử dụng.**
- **Đảm bảo rằng người dùng chỉ có thể truy cập vào các tài nguyên cần thiết cho công việc của họ.**
- **Cung cấp kiểm soát truy cập được kích hoạt bởi danh tính để bảo vệ quyền riêng tư và thông tin nhạy cảm của người dùng.**
- **Cung cấp cơ hội truy cập vào các tài nguyên được bảo vệ bằng cách sử dụng các giao thức dựa trên mã thông báo.**
- **Cung cấp cơ hội cho người dùng sử dụng thông tin đăng nhập hiện có của họ để truy cập các dịch vụ từ các nhà cung cấp dịch vụ khác nhau, chẳng hạn như Office 365 và Salesforce.**
- **Quản lý nhiều tài khoản SaaS trong môi trường doanh nghiệp của bạn.**
- **Xác định và cung cấp truy cập tùy thuộc vào bài toán: ai, điều gì, khi nào, ở đâu, lịch sử.**



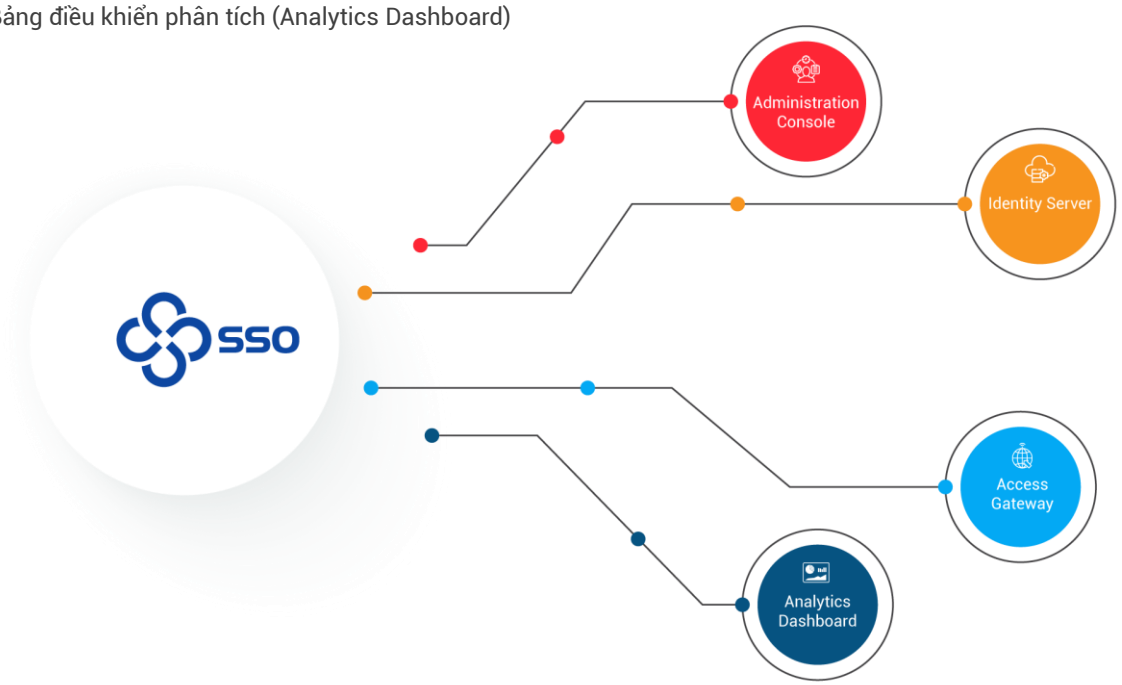
3. Các trường hợp sử dụng thông thường của Bkav SSO

- **Quản lý Truy cập Web An toàn** Cung cấp SSO an toàn và liền mạch cho nhân viên đến các ứng dụng trên nội bộ, đám mây và SaaS. Nó cho phép tổ chức cung cấp truy cập an toàn vào dữ liệu nhạy cảm bằng cách sử dụng xác thực đa yếu tố nhận biết bối cảnh và kiểm soát truy cập cụ thể.
- **Đối tác Hợp tác Hiệu quả** Cung cấp khả năng quản trị được ủy quyền để quản lý truy cập an toàn cho đối tác. Cho phép truy cập hạn chế vào các ứng dụng chỉ cần thiết thay vì toàn bộ mạng cho đối tác. Điều này giúp loại bỏ nguy cơ vi phạm bảo mật bởi bất kỳ đối tác bên thứ ba nào.
- **Quản lý Truy cập Khách hàng (Consumer Access Management)** Đơn giản và An toàn Cung cấp quản lý truy cập mạnh mẽ bao gồm tự phục vụ trên-boarding và SSO cho khách hàng của bạn. Nó cho phép khách hàng của bạn đăng ký và thiết lập tài khoản của riêng họ bằng các danh tính xã hội như Facebook, Google, Twitter và LinkedIn. Phần mềm xác thực tài khoản cho phép tự phục vụ quản lý dữ liệu danh tính và hồ sơ của khách hàng của bạn và kiểm soát truy cập của họ vào các ứng dụng và dịch vụ. Phần mềm xác thực tài khoản đảm bảo rằng danh tính, thông tin cá nhân và quyền riêng tư của người tiêu dùng được bảo vệ.

Phần mềm quản lý xác thực tập trung - Bkav Single Sign On cho phép tổ chức cung cấp truy cập an toàn đến các ứng dụng của tổ chức cho nhân viên, khách hàng và đối tác của họ từ bất kỳ loại thiết bị nào. Các tính năng truy cập linh hoạt, nhận biết bối cảnh và an toàn cho phép người dùng được ủy quyền truy cập các ứng dụng Intranet và đám mây từ bất cứ đâu và bất cứ thiết bị nào. Phần mềm xác thực tài khoản sử dụng các chuẩn ngành như SAML, OAuth, OpenID Connect và WS-Federation để cung cấp đăng nhập một lần liên doanh và hỗ trợ xác thực đa yếu tố, kiểm soát truy cập dựa trên vai trò và mã hóa dữ liệu

4. Các thành phần Bkav SSO bao gồm

- Bảng điều khiển quản trị (Administration Console)
- Identity Server
- Access Gateway
- Bảng điều khiển phân tích (Analytics Dashboard)



4. Các thành phần Bkav SSO bao gồm (tiếp)

4.1 Bảng điều khiển Quản trị

Bảng điều khiển Quản trị cung cấp một bảng điều khiển thống nhất cho việc cấu hình và quản lý tất cả các thành phần của Access Manager.

Các tính năng chính:

- Quản lý tài nguyên, chẳng hạn như chính sách và chứng chỉ
- Giám sát sức khỏe và thống kê của các thành phần riêng lẻ
- Quản trị chính sách
- Quản lý chứng chỉ
- Quản trị ủy quyền
- Lưu trữ cấu hình liên tục
- Kiểm tra dò sử dụng chi tiết bằng cách sử dụng máy chủ syslog

4.2 Identity Server

Identity Server có thể hoạt động như một nhà cung cấp danh tính (Indentity Provider). Tuy nhiên, bạn có thể cấu hình nó như một người tiêu dùng hoặc nhà cung cấp dịch vụ danh tính bằng cách sử dụng các giao thức Liberty, SAML hoặc OAuth.

Các tính năng chính:

- Xác thực bằng cách sử dụng x509, RADIUS, Mật khẩu một lần dựa trên thời gian, xác thực xã hội bằng cách sử dụng các nhà cung cấp OAuth bên ngoài, xác thực dựa trên rủi ro và nhiều hơn nữa.
- Xác thực liên kết sử dụng Liberty, SAML, WS Federation, WS Trust hoặc OAuth.
- Xác thực các danh tính người dùng được lưu trữ trong nhiều kho danh tính, chẳng hạn như eDirectory, Microsoft Active Directory hoặc Sun ONE Directory Server.
- Cung cấp tài khoản nhà cung cấp dịch vụ bằng cách tạo tài khoản người dùng tự động trong quá trình yêu cầu liên kết.
- Đăng nhập một lần và đăng xuất.
- Cung cấp dịch vụ xác thực và danh tính cho các Cổng truy cập được cấu hình để bảo vệ các máy chủ web.
- Quản lý RBAC (kiểm soát truy cập dựa trên vai trò) để liên kết vai trò và thuộc tính với người dùng được xác thực.

4.3 Access Gateway

Access Gateway cung cấp truy cập an toàn đến các máy chủ web dựa trên HTTP hiện có. Nó cung cấp các dịch vụ bảo mật (ủy quyền, đăng nhập một lần và mã hóa dữ liệu) được tích hợp với các dịch vụ định danh và chính sách của Access Manager.

4. Các thành phần Bkav SSO bao gồm (tiếp)

4.3 Access Gateway (tiếp)

Các tính năng chính:

- Đăng nhập một lần cho các dịch vụ web được bảo vệ (với Identity Server).
- Ủy quyền cho người dùng đã xác thực.
- Đăng nhập một lần cho các máy chủ web cũ thông qua form-fill và identity injection. Identity injection là việc lấy thông tin từ thư mục LDAP và chèn thông tin vào tiêu đề HTML, chuỗi truy vấn hoặc tiêu đề xác thực cơ bản để gửi thông tin này đến các máy chủ web phía sau. Các máy chủ web sử dụng thông tin này để cá nhân hóa nội dung hoặc để đưa ra các quyết định ủy quyền bổ sung.
- Multi-homing cho phép sử dụng một địa chỉ IP công cộng duy nhất để bảo vệ nhiều loại tài nguyên web.
- Bộ nhớ cache để tăng hiệu suất phân phối nội dung. Khi người dùng đáp ứng yêu cầu xác thực và ủy quyền, người dùng sẽ nhận được trang từ bộ nhớ cache thay vì yêu cầu từ máy chủ web.
- Chuẩn hóa hoặc viết lại URL để đảm bảo các điều kiện sau được đáp ứng:
    - Tham chiếu URL chứa lược đồ đúng (HTTP hoặc HTTPS).
    - Tham chiếu URL chứa địa chỉ IP riêng hoặc tên DNS riêng được thay đổi thành tên DNS đã xuất bản của Access Gateway hoặc các máy chủ.
- Gateway truy cập có sẵn trong hai mô hình triển khai:
    - Thiết bị Gateway truy cập: Nó được cài đặt dưới dạng thiết bị mềm, bao gồm hệ điều hành.
    - Dịch vụ Gateway truy cập: Yêu cầu bạn cung cấp hệ điều hành.

4.4 Bảng điều khiển phân tích

Bảng điều khiển phân tích phân tích việc sử dụng, hiệu suất và sự kiện của Access Manager. Nó bắt, lọc và phân tích các sự kiện được tạo ra bởi Access Gateway và Identity Server. Các sự kiện cần thiết được hiển thị trên Bảng điều khiển.

Hỗ trợ xem thông tin đã phân tích theo các cách sau:

Đồ thị động trên Bảng điều khiển Access Manager

Báo cáo được tạo ra dưới định dạng khác nhau

Các bản ghi kiểm toán gốc

5. Chức năng chính

Phần mềm quản lý xác thực tập trung - Bkav Single Sign On cung cấp đúng mức truy cập cho tất cả người dùng của bạn trên mạng nội bộ và các dịch vụ trên đám mây

Phần mềm Bkav SSO cung cấp truy cập đơn giản và bảo mật cho cả nhân viên và người tiêu dùng, bất kể là máy tính xách tay hay di động

5.1 Đăng nhập một lần

- Phần mềm Bkav SSO thiết lập xác thực cho các ứng dụng và cung cấp phân quyền cho các ứng dụng đó. Với Phần mềm Bkav SSO phục vụ cho xác thực phía trước, bạn có thể triển khai đăng nhập một lần (SSO) dựa trên tiêu chuẩn.
- Với SSO, nhân viên, đối tác và khách hàng của tổ chức chỉ cần nhớ một mật khẩu hoặc quy trình đăng nhập duy nhất để truy cập tất cả các ứng dụng doanh nghiệp và trên web mà họ được phép sử dụng. Bằng cách đơn giản hóa quản lý mật khẩu.
- Phần mềm Bkav SSO giúp nâng cao trải nghiệm người dùng, tăng cường bảo mật, tối ưu hóa quy trình kinh doanh và giảm chi phí quản trị hệ thống và hỗ trợ.

5.2 Quản lý Danh tính Liên minh (Identity Federation)

Bảo mật trong môi trường kinh doanh hiện nay, các tổ chức cần chia sẻ tài nguyên với các đối tác kinh doanh đáng tin cậy một cách bảo mật. Phần mềm Bkav SSO cung cấp quản lý danh tính liên minh để cho phép người dùng xác thực một cách liền mạch và bảo mật trên các miền danh tính tự động.

- Phần mềm Bkav SSO cũng hỗ trợ cung cấp liên minh. Tài khoản người dùng mới có thể được tạo tự động trong hệ thống của đối tác (hoặc nhà cung cấp) được tin tưởng của bạn. Ví dụ, một nhân viên mới trong tổ chức của bạn có thể khởi tạo việc tạo tài khoản trong hệ thống đối tác kinh doanh của bạn thông qua Phần mềm Bkav SSO thay vì phải dựa vào đối tác kinh doanh cung cấp tài khoản. Khách hàng hoặc đối tác kinh doanh tin cậy có thể tự động tạo tài khoản trong hệ thống của bạn.
- Phần mềm Bkav SSO cho phép bạn xác định thông tin doanh nghiệp và cá nhân nào từ thư mục doanh nghiệp của bạn để chia sẻ với người khác. Quản trị viên có thể chọn chia sẻ chỉ thông tin cần thiết để thiết lập tài khoản tại nhà cung cấp dịch vụ hoặc đối tác đáng tin cậy. Phần mềm Bkav SSO hỗ trợ tích hợp và SSO với Microsoft SharePoint và Office 365.

5.3 Xác thực đa yếu tố

- Khi được sử dụng kết hợp với Advanced Authentication, Phần mềm Bkav SSO hỗ trợ xác thực đa yếu tố để cung cấp truy cập bảo mật từ bất kỳ thiết bị nào với chi phí quản trị tối thiểu. Advanced Authentication cung cấp các cơ chế xác thực khác nhau cho phép xác thực danh tính và xác nhận ngoài xác thực dựa trên tên người dùng và mật khẩu truyền thống.
- Cho phép xác thực trên các nền tảng đa dạng bằng cách sử dụng các công cụ xác thực khác nhau như: Vân tay, OTP và Smartphone.

5.4 Xác thực và Kiểm soát Truy cập Dựa trên Ngữ cảnh

- Cho phép các tổ chức chọn các phương pháp xác thực phù hợp với ngữ cảnh truy cập.
- Giải pháp cung cấp kiểm soát truy cập, xác thực và phân quyền dựa trên ngữ cảnh, mô hình, vị trí và các thuộc tính khác.
- Sử dụng loại xác thực đúng cách cung cấp bảo mật cao cho thông tin nhạy cảm trong khi đơn giản hóa truy cập cho người dùng được phép.

5. Chức năng chính (tiếp)

5.5 Xác thực không cần mật khẩu

Xác thực không cần mật khẩu khác với hệ thống đăng nhập dựa trên tên người dùng và mật khẩu truyền thống. Thay vì yêu cầu người dùng nhớ và nhập mật khẩu, nó sử dụng sinh trắc học, mã một lần được gửi qua SMS hoặc email hoặc một chìa khóa bảo mật vật lý. Phần mềm xác thực tài khoản hỗ trợ nó thông qua các tính năng sau:

- Xác thực Kerberos
- Xác thực dựa trên chứng chỉ
- Tích hợp với Advanced Authentication
- Khi tích hợp với Advanced Authentication, Phần mềm Bkav SSO hỗ trợ xác thực không cần mật khẩu thông qua các phương pháp Advanced Authentication.

5.6 Nhận dạng thiết bị

- Người dùng có thể đăng nhập vào các ứng dụng bằng bất kỳ thiết bị nào. Thiết bị có thể là máy tính để bàn, máy tính xách tay hoặc thiết bị di động. Mỗi thiết bị có nhiều đặc điểm, chẳng hạn như hệ điều hành, phần cứng và các đặc điểm trình duyệt.
- Phần mềm Bkav SSO sử dụng các đặc điểm thiết bị và danh tính người dùng để tạo ra một vân tay duy nhất của thiết bị. Bạn có thể sử dụng vân tay này để xác định một cách duy nhất và kết hợp một hồ sơ rủi ro cho thiết bị.

5.7 Hỗ trợ xác thực với các mạng xã hội (Social Indentities)

- Phần mềm xác thực tài khoản hỗ trợ xác thực qua các nhà cung cấp OAuth bên ngoài, chẳng hạn như: Facebook, Google+, Twitter và LinkedIn. Xác thực với các mạng xã hội đơn giản hóa đăng nhập cho người dùng và không yêu cầu duy trì các kho lưu trữ người dùng lớn.
- Đăng nhập bằng danh tính xã hội cung cấp một cách tiện lợi cho người dùng, cải thiện sự hài lòng của khách hàng và tăng tỷ lệ đăng ký.

5.8 Xác thực và Phân quyền Liên tục

Phần mềm Bkav SSO cung cấp khả năng tái đánh giá rủi ro liên quan đến một phiên hoạt động định kỳ. Khi các tham số ngữ cảnh của người dùng, chẳng hạn như địa chỉ IP hoặc vị trí, thay đổi, Phần mềm Bkav SSO có thể thực hiện bất kỳ một trong các hành động sau:

- Yêu cầu người dùng xác thực lại
- Yêu cầu người dùng thực hiện xác thực yếu tố thứ hai
- Đăng xuất người dùng

5.9 Hỗ trợ OAuth và OpenID

- Phần mềm Bkav SSO hỗ trợ OAuth và OpenID Connect cho phân quyền dựa trên thông tin mã thông báo an toàn (token-based). Nhờ đó người dùng có thể cho phép các khách hàng bên thứ ba truy cập vào các tài nguyên riêng.
- Người dùng không cần phải chia sẻ thông tin đăng nhập của họ. Các khách hàng bên thứ ba có thể là các ứng dụng web, điện thoại di động, thiết bị cầm tay và các ứng dụng trên máy tính để bàn. Phần mềm Bkav SSO sử dụng OpenID Connect cùng với OAuth để thực hiện giao thức đăng nhập một lần trên quy trình phân quyền OAuth.

5.10 Truy xuất và Chuyển đổi Thuộc tính

- Cho phép hệ thống truy xuất các thuộc tính từ nguồn dữ liệu bên ngoài (bất kỳ cơ sở dữ liệu nào, dịch vụ web REST hoặc các kho LDAP) và chuyển đổi trước khi sử dụng (assertion). Người quản trị cũng có thể chuyển đổi các thuộc tính cục bộ của người dùng (thuộc tính LDAP, Mật khẩu chia sẻ và các hồ sơ khác như: Hồ sơ Cá nhân và Hồ sơ Nhân viên).

5. Chức năng chính (tiếp)

5.11 Hỗ trợ cho Môi trường cũ (Legacy)

Trong các môi trường cũ không thể tích hợp thông qua các giải pháp mới, Phần mềm Bkav SSO có thể phục vụ như một reverse proxy để bảo vệ các nguồn tài nguyên web.

6. Chức năng liên quan đến người dùng cuối

6.1 Mobile Access

Phần mềm Bkav SSO bao gồm một SDK cho iOS, OpenID Connect hoặc OAuth cho các tổ chức cung cấp dịch vụ thông qua các ứng dụng di động.

6.2 Quản lý Truy cập B2C

Phần mềm Bkav SSO cung cấp một giải pháp giải quyết một tập hợp rộng các trường hợp sử dụng Doanh nghiệp đến Khách hàng (B2C). Giải pháp B2C cho phép bạn xác định và tương tác an toàn với khách hàng của bạn trong khi cung cấp trải nghiệm liền mạch trên bất kỳ thiết bị, ứng dụng hoặc dịch vụ nào mà họ đang sử dụng.

- Access Manager, kết hợp với Self Service Password Reset và Advanced Authentication, cung cấp hỗ trợ cho các trường hợp sử dụng B2C, chẳng hạn như việc đăng ký người dùng mới, xác minh tài khoản, đăng nhập web tùy chỉnh, tích hợp cổng thông tin, đăng ký và quản lý thiết bị, quản lý tùy chọn, hồ sơ và quản lý quyền riêng tư.
- Cho phép khách hàng thiết lập các ứng dụng và cổng thông tin phía người tiêu dùng cuối, tạo điều kiện tương tác tốt hơn với người tiêu dùng cuối. Nó cũng cung cấp các công cụ để hỗ trợ các yêu cầu về quyền riêng tư và bảo mật được đề ra trong các quy định như GDPR và PSD2.

6.3 Quản lý Sự đồng ý (Consent Management)

- Cho phép người dùng cuối lựa chọn thông tin cá nhân nào họ muốn chia sẻ với doanh nghiệp thông qua một số phương pháp như: OAuth Consent Scopes…

6.4 Chức năng ký số

- Trường hợp người ký số trên thông điệp dữ liệu là cá nhân, cho phép người ký số sử dụng khóa bí mật cá nhân để thực hiện việc ký số vào thông điệp dữ liệu; Trường hợp người ký số trên thông điệp dữ liệu là tổ chức, cho phép người ký số sử dụng khóa bí mật tổ chức để thực hiện việc ký số vào thông điệp dữ liệu.

6.5 Chức năng kiểm tra hiệu lực của chứng thư số

- Cho phép việc kiểm tra chứng thư số của người ký số trên thông điệp dữ liệu phải kiểm tra theo đường dẫn tin tưởng trên chứng thư số và phải thực hiện đến tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia.
- Nội dung kiểm tra hiệu lực của chứng thư số tại thời điểm ký số:
    - Thời gian có hiệu lực của chứng thư số; Trạng thái chứng thư số qua danh sách chứng thư số thu hồi (CRL) được công bố tại thời điểm ký số hoặc bằng phương pháp kiểm tra trạng thái chứng thư số trực tuyến (OCSP) ở chế độ trực tuyến trong trường hợp tổ chức cung cấp dịch vụ chứng thực chữ ký số có cung cấp dịch vụ OCSP.
    - Thuật toán mật mã trên chứng thư số; Mục đích, phạm vi sử dụng của chứng thư số.

6. Chức năng liên quan đến người dùng cuối (tiếp)

6.6 Lưu trữ và hủy bỏ các thông tin sau kèm theo thông điệp dữ liệu ký số

- Chứng thư số tương ứng với khóa bí mật mà người ký số sử dụng để ký thông điệp dữ liệu tại thời điểm ký số; Danh sách chứng thư số thu hồi tại thời điểm ký của tổ chức cung cấp dịch vụ chứng thực chữ ký số đã cấp chứng thư số để ký số tương ứng với chữ ký số trên thông điệp dữ liệu đi;
- Quy chế chứng thực của tổ chức cung cấp dịch vụ chứng thực chữ ký số đã cấp chứng thư số tương ứng với chữ ký số trên thông điệp dữ liệu đi; Kết quả kiểm tra trạng thái chứng thư số tương ứng với chữ ký số trên thông điệp dữ liệu được gửi đến.

7. Chức năng liên quan đến quản trị

Giao diện quản trị dạng web cung cấp một vị trí trung tâm cho các tổ chức của bạn để xem, cấu hình và quản lý tất cả các thành phần và chính sách đã cài đặt. Ngoài ra, các quản lý CNTT có thể giám sát sức khỏe thời gian thực của toàn bộ mạng và tự động hóa việc phân phối chứng chỉ bằng cách sử dụng bảng điều khiển này.

7.1 Phân quyền quản trị

- Quản trị viên cấp cao có thể ủy quyền một số nhiệm vụ quản trị cho một người dùng có quyền quản trị giới hạn. Ví dụ, đặt lại mật khẩu người dùng. Điều này giúp giảm gánh nặng của các quản trị viên. Khả năng này cũng loại bỏ bất kỳ rủi ro về việc xâm nhập bảo mật khi hợp tác với các đối tác. Bạn có thể cung cấp cho đối tác của mình quyền truy cập hạn chế vào chỉ các ứng dụng cần thiết.

7.2 Application Connectors

- Phần mềm Bkav SSO sử dụng các Connectors để thiết lập kết nối giữa Phần mềm Bkav SSO và các ứng dụng. Khi cấu hình một kết nối cho một ứng dụng, hệ thống tự động tạo một appmark cho ứng dụng này và thêm nó vào trang User Portal.
- Phần mềm Bkav SSO cung cấp một Danh mục Application Connector Catalog chứa danh sách các kết nối ứng dụng có sẵn mà Phần mềm hỗ trợ cho SSO. Danh mục Kết nối Ứng dụng hiển thị tất cả các kết nối có sẵn và các trình duyệt tương thích với các kết nối. Danh mục có thể hiển thị các kết nối theo tên hoặc theo loại kết nối. Các loại kết nối có sẵn là Trợ lý SSO, SAML, Quản lý Tài khoản SAML và WSFED.

7.3 Tùy chỉnh User Portal

- Phần mềm Bkav SSO cung cấp một cổng người dùng có thể tùy chỉnh. Người sử dụng có thể tùy chỉnh các giao diện người dùng, chẳng hạn như: Trang đăng nhập và cổng tùy chọn. Với sự cố gắng tối thiểu, bạn có thể đặt thương hiệu cho trang đăng nhập với logo và màu sắc doanh nghiệp của riêng bạn.
- Người dùng cũng có tính linh hoạt để lựa chọn mục yêu thích và loại chế độ xem mà họ muốn trải nghiệm.

7.4 Hỗ trợ API

- Phần mềm Bkav SSO có sẵn các API quản trị và các API OAuth và OpenID Connect. Các API quản trị giúp tự động hóa các nhiệm vụ quản trị thông thường. Các API OAuth và OpenID Connect dành cho tất cả các chức năng OAuth, chẳng hạn như các điểm cuối để đăng ký khách hàng và lấy mã truy cập.

7. Chức năng liên quan đến quản trị (tiếp)

6.6 Lưu trữ và hủy bỏ các thông tin sau kèm theo thông điệp dữ liệu ký số

- Chứng thư số tương ứng với khóa bí mật mà người ký số sử dụng để ký thông điệp dữ liệu tại thời điểm ký số; Danh sách chứng thư số thu hồi tại thời điểm ký của tổ chức cung cấp dịch vụ chứng thực chữ ký số đã cấp chứng thư số để ký số tương ứng với chữ ký số trên thông điệp dữ liệu đi;
- Quy chế chứng thực của tổ chức cung cấp dịch vụ chứng thực chữ ký số đã cấp chứng thư số tương ứng với chữ ký số trên thông điệp dữ liệu đi; Kết quả kiểm tra trạng thái chứng thư số tương ứng với chữ ký số trên thông điệp dữ liệu được gửi đến.

6.7 Bảo mật API

- Secure API Manager mở rộng khả năng của Phần mềm Bkav SSO để bảo mật các micro-services, dịch vụ web REST-based và các hệ thống API cổ điển. Secure API Manager cung cấp việc tạo ra API, quản lý vòng đời API, quản lý lưu lượng API và phân tích.
- Secure API Manager yêu cầu Phần mềm Bkav SSO làm Nhà cung cấp Định danh. Phần mềm Bkav SSO cung cấp xác thực của khách hàng API và ủy quyền của các API được bảo vệ bởi Secure API Manager.

6.8 Dashboard quản trị

- Phần mềm Bkav SSO bao gồm Bảng điều khiển để cung cấp phân tích trực quan về dữ liệu liên quan đến truy cập dựa trên việc sử dụng, hiệu suất và sự kiện của Access Manager.
- Các sự kiện được ghi lại và được lọc thông qua thành phần Máy chủ Phân tích. Bảng điều khiển này giúp trong việc hiển thị mô hình truy cập, điều chỉnh chính sách và nhận được thông tin về việc sử dụng Phần mềm Bkav SSO trong môi trường của bạn. Bạn cũng có thể giám sát các mô hình truy cập dữ liệu thời gian thực để quyết định các hành động tiếp theo.

6.9 Quản lý vòng đời cấu hình

- Cho phép quản trị viên khởi chạy một máy chủ mới, sao lưu hoặc di chuyển các chính sách từ một môi trường Phần mềm Bkav SSO sang một môi trường Phần mềm xác thực tài khoản khác trong vài phút. Bạn có thể sử dụng công cụ này để sao chép cấu hình giữa hai hệ thống Phần mềm xác thực tài khoản nằm trong các mạng khác nhau, có số lượng thiết bị khác nhau và có lưu trữ người dùng khác nhau.

6.10 Self Service Password

- Sử dụng cùng với Self Service Password Reset, Phần mềm Bkav SSO cho phép người dùng đặt lại mật khẩu hoặc mở khóa tài khoản của họ mà không cần gọi đến bộ phận trợ giúp.
- Phần mềm Bkav SSO phân phối cập nhật mật khẩu trong thời gian thực trên tất cả các nguồn lực vật lý và ảo của bạn. Điều đó làm cho môi trường của bạn không cần bảo trì mật khẩu.

6.11 Mô phỏng (Impersonation)

- Cho phép đội ngũ hỗ trợ (help-desk) thực hiện một số hành động thay mặt người dùng mà không biết thông tin xác thực của họ. Nhờ đó tăng tốc độ phát hiện và xử lý lỗi.

6.12 Logging

- Các thành phần Phần mềm Bkav SSO đã được lập trình để gửi cảnh báo đến các loại hệ thống khác nhau như máy chủ SIEM hoặc máy chủ syslog.

8. Khả năng triển khai linh hoạt

Phần mềm Bkav SSO cung cấp khả năng triển khai linh hoạt như một thiết bị All-In-One chuyên biệt hoặc cài đặt trên các máy chủ thông dụng. Giải pháp cũng có thể cài đặt như một máy chủ ảo trong trung tâm dữ liệu riêng của tổ chức, điện toán đám mây công cộng (Amazon Web Services (AWS) EC2 và Microsoft Azure).

Phần mềm Bkav SSO đi kèm với các tùy chọn triển khai sau:

Triển khai các thành phần riêng lẻ (Identity Server, Access Gateway, Analytics Server và Administration Console). Mỗi thành phần có thể được cài đặt và quản lý trên các máy chủ riêng biệt. Chúng cũng có thể được triển khai dưới dạng dịch vụ trên Amazon Web Services EC2 và Microsoft Azure.

Triển khai các thành phần Phần mềm xác thực tài khoản thông qua một cơ chế containerized. Phần mềm Bkav SSO sử dụng Kubernetes để quản lý các container Docker. Các thành phần Phần mềm xác thực tài khoản được cung cấp dưới dạng hình ảnh Docker.

Triển khai tất cả các thành phần như một thiết bị. Phần mềm Bkav SSO Appliance là một thiết bị mềm dựa trên SUSE Linux Enterprise Server. Nó gói các Identity Server, Access Gateway và Administration Console được cấu hình trước trên một máy chủ. Analytics Server được cài đặt và quản lý trên một máy chủ riêng biệt.

Giải pháp & Thông số kỹ thuật
Ngôn ngữ lập trình: Java, JS, C, CSS, HTML, Python
Cơ sở dữ liệu: MSSQL, SQL Server, PostgreSQL, H2
Công nghệ sử dụng: Mã nguồn mở WSO2
Cấu hình tối thiểu: 2 Cores CPU; 8 GB RAM; 200 GB HDD

Giấy phép sử dụng
License Enterprise: 02 Core Identity Server
Hỗ trợ kỹ thuật: Tối thiểu 2 năm (Tùy thuộc vào từng trường hợp cụ thể)