- Multi-factor authentication
  - portal integration points
    - CE
      - ✓ login
        - login-web
        - struts LoginAction
      - ✓ API authentication — AuthVerifierFilter
      - ✓ SSO clients — AutoLoginFilter
    - EE
      - On Control Panel access
      - On Password change
      - On User details change (email) - my account portlet
      - Other portlets — system portlets for omni-admin
      - Layouts/Groups — control panel, organization pages
    - API: Registry of integrations
      - Name
      - Browser / Headless
    - SPI: to implement new integration
  - mfa providers
    - CE
      - ✓ TOTP
        - specification
        - time-based token, user types the number from smartphone app into portal
      - Location (IP)
        - can verify based on network mask/location
        - VPN access / admin acceess
      - Email OTP — user receives code over email
    - EE
      - SMS OTP — SMS by Twilio - can reuse push-notifications-* modules
      - U2F, FIDO2 Web Authentication spec — hardware tokens
      - Authy / Duo sec
        - 3rd party smartphone apps with own API
        - Partly implemented by the GS 2FA
      - Custom Liferay app
        - users woudl "tap" on smartphone to approve access
        - using push notifications modules + new app
    - API: Registry of providers
      - Name
      - Browser / headless
    - SPI: To integrate new provider
      - For Browser access
      - For Headlsess access
  - MFA verification (provider @ integration)
    - validation rule structure
      - ✓ Portal integration point — one of the deployed interations
      - ✓ MFA Provider — one of the deployed providers
      - ? Force revalidation — When to force revalidation
      - ? Which role to apply to
        - By default users - during authentication
        - Can be also admins for other places like control panel
    - Configurable by admin
    - example rule
      - Portal integration point
        - portal authentication
        - API authentication
      - What -MFA provider — TOTP
      - Force reauthentication? — only for new browser/client
      - Who - Role ? — User
    - example rule
      - Where - Portal integration point — control panel
      - What -MFA provider — FIDO
      - Force reauthentication? — session-based
      - Who - Role ? — Admin/Site Admin
    - ? Composite rules
      - mandatory — all configured providers must match
      - optional — just one provider is enough
  - Example scenarios
    - Optional 2FA using TOTP ✓
      - Portal admin enables TOTP for authentication
      - User instals TOTP enabled app on a smartphone — Google authenticator / FreeOTP/ Authy / ...
      - User setup TOTP in my-account or similar portlet — Scans QR code with the app
      - After then user must enter TOTP to sign into the account — Enters password and on the next screen enters 2FA token
    - Users can access Control Panel only from office/VPN
      - Portal admin enables IP provider and configures VPN netmask
      - Portal admin configures control panel integration with the IP check
      - After then only users with IP from the netmask range can access control panel
    - Admins (portal / site) must use a hardware token to sign in
      - Portal admin enables hardware token (U2F / Fido) provider
      - Portal admin configures authentication integration points
        - for admin role
        - for site-admin role
        - for organization-admin role
        - to use hardware token
      - After then users in portal admin role must authenticate using hardware token
  - Required features (CE?)
    - SPI
      - for portal integration points
      - for token providers
    - Integration
      - browser authentication
      - API access
    - Provider — TOTP (RFC standard)
    - UI
      - Setup & Verify
      - Portal admin config — can be settings portlet? ?
  - Other features
    - auditing
    - recovery / backup codes — only 2fa (something you have)
    - revalidation
      - client based (cookie?)
      - session-based
      - invalidation time
    - user email notifications
      - when new client / new platform signs in
      - when new provider is set up for the user account
    - policies like for password? — probably just each provider configuration
    - swap for existing solution — covered by SPI
  - Human interaction points
    - Setup screen
      - after sign-in — enforced
      - from user account — optional
    - Verification screen — enforced during verification (e.g. sign in)
    - Portal admin configuration
      - UI
        - Configurations only?
        - Or new portlet?
      - Configure each provider
      - Configure validation rule — provider x integration intersection
      - Configure rules composition
  - Headless interaction points
    - Token based request verification — probably using HTTP request header
    - IP based verification — remote IP