**Dokumentation Metodbok som används för Metodbeskrivningar och lathundar på Strålbehandlingen NUS.**Utvecklat av Robin Vingsle med start 2023

**Licenser och programvara**

Programvaror och licenser som använts för att bygga programmet:

* *Exeoutput for PHP* - Kompilator för programmet
* *SSL.com* - Kodsigneringscertifikat
* *Envato Elements* - Bootstrap 5-design licens
* *PHP 8.2* - Programmeringsspråk (Metodbok.exe)
* *Javascript* - Programmeringsspråk (Metodbok.exe)
* *Python* - Programmeringsspråk (Metodbok installer.exe)
* *SQLite v. 3.39* - Databas
* *TinyMCE* - WYSIWYG-texteditor GPL licens  
    
  *Eftersom TinyMCE går under en GPL-licens har alla som använder Metodboken även rätt till all källkod. Källkoden får du genom att maila mig så skickar jag en uppdaterad länk för nerladdning.* ***OBS!*** *Detta gäller endast källkod för den del av programmet som använder TinyMCE. All känslig källkod som involverar kryptering och lösenordsskydd kommer avlägsnas innan*

**Rekommendationer på utrustning**

* **Operativsystem:** *Windows är ett krav. (Testad och fungerar på Windows 10 och 11.) MAC fungerar ej, tror inte heller rimligt att göra en sådan version…någonsin…!*
* **Programvara:** *Word och excel om man vill använda word/exel-filer att skapa metoder av.*
* **Regionsdatorer:** *Programmet fungerar även på äldre datorer men kan ibland stängas ner oväntat på de sämsta datorerna. Vid liten datorkraft och stor skärm kan lagg upplevas.*

**Teknisk beskrivning av säkerhetsfunktioner i Metodboken**

**Metodboken** implementerar ett flertal säkerhetsfunktioner för att skydda data och förhindra obehörig åtkomst eller manipulation. Nedan beskrivs de viktigaste teknikerna och hur de fungerar:

**1. Kryptering av data med XSalsa20-Poly1305 (Libsodium SecretBox)**

För att skydda känslig information, såsom dokument, PDF-filer och binära data, används symmetrisk kryptering via Libsodiums funktion **SecretBox**.  
SecretBox bygger på algoritmen **XSalsa20-Poly1305**, som är erkänd för sin höga säkerhet och prestanda.

**Så fungerar det:**

* **XSalsa20** är en strömkryptoalgoritm som genererar en pseudorandom ström av bytes utifrån en hemlig nyckel och ett unikt "nonce" (number used once).
* **Poly1305** är en MAC-algoritm ("Message Authentication Code") som används för att verifiera att datan inte har manipulerats under transport eller lagring.
* Vid kryptering skapas först ett slumpmässigt nonce för varje krypteringsoperation, vilket förhindrar angrepp där samma data skulle kunna identifieras.
* Datan krypteras och förses med en MAC, vilket innebär att mottagaren kan verifiera att datan är äkta och inte har ändrats.
* Den krypterade datan lagras som en base64-kodad sträng, tillsammans med nonce och MAC.

**Resultat:**  
Endast den som har tillgång till den hemliga nyckeln kan dekryptera och läsa datan. Om någon försöker ändra på datan, kommer valideringen att misslyckas och datan anses vara komprometterad. En nyckel ser ut ungefär såhär:

**2. Dataintegritet med digitala signaturer (Libsodium crypto\_auth)**

För att skydda mot manipulation av kritisk data, såsom användarroller, status, kommentarer, och verifieringar, används digitala signaturer.

**Så fungerar det:**

* När data sparas, skapas en digital signatur med hjälp av **crypto\_auth** och den hemliga nyckeln.  
  Signaturen genereras genom att skapa ett MAC-värde av datan (exempelvis användarnamn, lösenordshash och roller).
* Signaturen lagras tillsammans med datan.
* Vid validering kontrolleras att signaturen stämmer överens med den aktuella datan.
* Om någon ändrar datan i databasen utan att ha tillgång till nyckeln, kan signaturen inte återskapas, och manipulationen upptäcks direkt.

**Resultat:**  
Metodboken kan omedelbart identifiera och blockera försök till datamanipulation, vilket skyddar mot såväl yttre attacker som interna misstag.

**3. Hashning av lösenord**

Lösenord lagras **aldrig i klartext**.  
Istället används en stark hashfunktion för att omvandla lösenordet till ett hashvärde innan det sparas i databasen.

**Så fungerar det:**

* När användaren anger sitt lösenord, beräknas ett hashvärde (envägskryptering).
* Vid inloggning jämförs det hashade värdet, inte själva lösenordet.
* Om någon får tillgång till databasen, kan de inte återställa det ursprungliga lösenordet från hashvärdet.

**4. Säker hantering av kryptonycklar**

Den hemliga nyckeln som används för kryptering och signering lagras **inte direkt i koden eller databasen**, utan hämtas via en miljövariabel.  
Detta gör det svårare för angripare att komma över nyckeln även om de får tillgång till applikationens filer. Filen där nyckeln återfinns är även den krypterad.

**5. Felhantering och kontroll**

Metodboken hanterar fel på ett säkert och tydligt sätt, till exempel när dekryptering misslyckas eller när signaturer inte stämmer.  
Det innebär att potentiella säkerhetsproblem fångas upp och blockeras innan de kan påverka systemet.

**6. Versionkontroll**

Metodboken sparar upp till 20 versioner på publicerade dokument / metodbeskrivningar gjorda i Metodboken. Alla sparade versioner och dokument sparas krypterade och kan endast läsas med krypteringsnyckel => Kan endast öppnas i metodboken. Versionkontrollen sparas endast om en metod är ”publicerad” vilket är valbart vid skapande av metodbeskrivning samt vid uppdatering av metodbeskrivning. Ett ej publicerat dokument blir även det, endast synlig för behörig personal.

**7. Backup**

Var 6te dag gör metodboken automatiskt en backup på databasen som sparas lokalt, samtidigt skickas ett mail till huvudansvarig admin som går att ställa in under inställningar, i mailet återfinns även där kopian på backup-filen. Alla metodbeskrivningar är såklart även här, krypterade. 10 backupfiler sparas sedan rensas den äldsta. 10x6 = 60 dagar sparas backup lokalt. Alla återfinns dock på admins mail som ställs in under inställningar. Mail skickas via tredjeparts SMTP server, ingen känslig information bör därför skickas. Metoder är krypterade, word dokument sparas endast som filvägar, inga dokument finns i databasen som skickas.

**8. Databashantering**

I dom bästa av världar hade jag haft tillgång till en databas som legat på en server. Då hade allt varit snäppet säkrare och mycket tid har lagts på att klura ut hur man ska dela på EN sqlite databas över nätverket. Dessa databaser är inte tillverkade för nätverksdelning/hantering men det fungerar utan problem med lite extra försiktighet.  
Databasen kopieras när en användare loggar in, alla användare läser då en direkt uppdaterad fil. Efter det uppdateras databasen automatiskt var 30nde minut samt varje gång man skriver. Så för admins som skriver / ändrar data håller den sig alltid uppdaterad. Det finns även en ”uppdatera” knapp om man vill manuellt ha en helt uppdaterad kopia. För att minimera risken att flera användare skriver samtidigt vilket kan göra databasen korrupt finns en funktion som låser databasen så fort någon skriver, en vingsle.lock fil skapas med en tidsstämpel, och raderas efter användaren är färdig. Har det gått 10sekunder och filen fortfarande är kvar, raderas filen ändå. Användare nummer 2 kan som max få vänta 10 sekunder innan deras ”skrivning” går igenom, men detta hör till ovanligheten då det tar under en sekund att skriva till databasen. Varje gång en användare loggar in kollas databasen igenom för att se om den är korrupt innan inloggning sker, även alla backupfiler kontrolleras och verifieras att de inte är korrupterade via SQLites inbyggda funktioner för integritetskontroll.

**Sammanfattning**

* **XSalsa20-Poly1305** säkerställer att känslig data är krypterad och autentiserad.
* **Digitala signaturer** skyddar mot datamanipulation.
* **Hashning** av lösenord förhindrar att lösenord avslöjas vid dataläckor.
* **Miljövariabler** används för nyckelhantering, vilket ger ett extra säkerhetslager.
* **Säker felhantering** upptäcker och blockerar försök till manipulation.
* **Versionhantering** sparar äldre versioner av publicerade dokument krypterade med upp till 20 versioner.
* **Backup** sparar data i 60 dagar

**Brister och förbättringsmöjligheter för säkerhet:** Databasen ligger lokalt, den går att öppna och läsa i men med verifikationshash går det ej ändra på information utan att det flaggas. Det går fortfarande radera rader, t.ex radera sparade lathundar i HTML. De finns dock sparade i backups som skapas var 6te dag samt backup mail till admin.

**Funktioner och användning  
  
*Metodboken*** innehålleren rad olika funktioner. Jag kommer inte gå inte så djupt på var och en då det är funktionerna kring metodbeskrivningar och lathundar som är huvudanvändningsområdet.

**1. Metodbeskrivningar och Lathundar - Dokumenthantering**

**A.** Skapa metodbeskrivningar eller lathundar utifrån redan färdiga word, pdf eller excel dokument. Metodboken kopierar dokumenten som existerar för att inte låsa eller misslyckas öppna låsta dokument. Word-filer bearbetas med office COM funktion för att konvertera den till PDF, excel-filer konverteras till HTML och PDF filer kopieras endast. Länkar extraheras ur dokumenten och läggs i en .txt fil som sedan avläses vid sidan om dokumenten. Alla dokument visas sedan i en inbyggd PDF-visare. Dokumenten är som tidigare beskrivet krypterade och kan ej öppnas utanför Metodboken. Denna typ av dokumenthantering fungerar för både lokala filer och filer som ligger på internet. De filer som ligger på webbadresser laddas ner med PHP CURL funktion och använder ”Native CACERT” som autentisering. Det fungerar i nuläget INTE att ladda hem filer från Sharepoint då tillträde till detta kräver mer än jag kan. DOCK eftersom användare kan lägga till sharepoint mappar i sin onedrive, går det att länka och använda dokument från onedrive, funktion kring detta mer beskrivet under stödfunktioner. Alla filer håller sig uppdaterade genom att via lokala filer kolla när filen är sparad via PHP funktionen ”filemtime” som skickar tillbaka UNIX timestamp, om den tiden är ändrad, laddas den nya versionen till Metodboken.  
Om en lokal fil ändrar namn söker Metodboken efter liknande filer i samma mapp och ger admin-användare möjlighet att uppdatera till nytt filnamn.  
Exempel Prostat med körtlar 77gy.docx byter namn till Prostat med körtlar 77gy och lite annat.docx = > Admin användare får frågan om vi vill använda Prostat med körtlar 77gy och lite annat.docx istället, ja eller nej.  
Filer hämtade från webbsidor har ett ETAG nummer samt en header när dokumentet senast ändrades på servern, ändras ETAG betyder det att dokumentet ändrats eller servern uppdaterat något kring dokumentet, då laddas nytt dokument ner.  
Varje gång ett dokument laddas ner och vi antar blivit uppdaterat, skapas en ny version till versiondatabasen som spara krypterat. Alla versioner ökar då i versionnummer från 1 till 1.001 1.002 osv.

**B,** Metodbokens inbyggda text-editor TinyMCE går att använda där versionkontroll fungerar på samma sätt. All text sparas som HTML (krypterat) och körs igenom ett antal funktioner innan texten visas. Länkar till lokala filer fungerar, alla ord är kopplade till en ordlista i metodboken som öppnas som en ”tooltip” där bilder och text kan beskriva. T.ex mamupplägg skapar en tooltip på vad ett standard mamupplägg innehåller.  
Bilder kan laddas upp och infogas och dessa sparas lokalt på datorn. Det finns möjlighet att spara dessa direkt i databasen men då skulle databasen växa sig enorm snabbt.  
  
**2. Signering av metodbeskrivningar**

Signering av metodbeskrivningar läggs till av admin eller EA användare. Metodbeskrivningen blir ”blurrad” och grå så vanliga användare INTE kan se vad som står, samt en text om varför den är grå. T.ex inväntar publicering, inväntar signering osv. När en metod uppdateras eller ett dokument (word excel pdf) uppdaterats nollställd signeringarna så de är ”Ej giltig”, detta gäller även om ett word dokument uppdaterats, det behöver inte varit uppdaterat i metodboken. Admin-användare får endast en ”grå” hinna över ej signerade dokument, även användare om ej har admin-funktion OM de ligger som signerare, så de kan läsa metoden innan signering. Vid signering bekräftas med crypt\_auth att användaren ej är manipulerad och att lösenordet stämmer. En signering behöver inte vara rollspecifik utifrån admin eller EA rättigheter. Den person som är ombedd att signera får upp en notis ”x antal metoder att signera”, det finns även en lista över de signerade metoderna. Skulle en metod uppdateras så signeringen blir ogiltig dyker detta upp på signerarens notis-lista igen.

**3. Stödfunktioner för metodbeskrivningar**

**A. Uppladdning av bilder och filer**Bilder och filer kan laddas upp och visas antingen i löpande text via ”admin uppladdning till bildbank” samt en sidomeny för bilder, filer länkas genom att lägga till länk i löpande text eller ladda upp en länk vid sidan av. Bilderna sparas på nätverket där Metodbokens root finns, när en användare loggar in kopieras alla bilder som inte existerar i dess bildmapp och detta sker även löpande i bakgrunden så bildmappen är uppdaterad.

**B. Relaterade metoder**Relaterade metoder visas i en sidomeny där man kan länka till andra metodbeskrivningar, öppnar man en relaterad metod öppnas dem upp i ett eget fönster så man inte behöver frångå den metod man redan läser.

**C. Ordlista och ersättning av ord**Det finns en ordlista för att förklara förkortningar och upplägg, dessa, som beskrivet innan är kopplade direkt till metodbeskrivningar gjorda i TinyMCE text editor och visar då ett tooltip vad förkortningen eller ordet betyder.  
Ersättning av ord är kopplad direkt till metodbeskrivningar och annan text i metodboken, du kan använda den för att massersätta ett ord. T.ex skriva ”bäckenförklaring” och ersätta med en hel berättelse eller beskrivning av upplägg, för att sedan skriva bäckenförklaring i löpande text och den då ersätts med din långa beskrivning. Detta kan vara särskilt bra om en metodbeskrivning har samma upplägg eller förklaring, därför behöver man inte uppdatera alla beskrivningar utan bara beskrivningen i detta ord…… Man kan då också ersätta t.ex mamupplägg med mammmmaupplägg om vi någon gång skulle ändra på hur vi beskriver något, för att slippa leta upp detta i alla dokument.  
  
**D. Utskrifter**Alla metodbeskrivningar går att skriva ut, med följer version och signeringslistor. Word / pdf skrivs ut genom PDF-visaren

**E. Behörigheter**En admin eller EA kan lägga till behörigheter för endast aktuellt dokument, en behörighet ger vilken användare som helst rättigheter att uppdatera lägga till och skapa i en metodbeskrivning. Man kan lägga till hur många behöriga man vill för vilka dokument man vill. Aktuell person står då som uppdaterare t.ex

**F. Sharepoint Onedrive**För att kringå problematik att ladda filer från Sharepoint då jag antar att detta kräver lite handpåläggning går det att spara mappar i Onedrive, dessa länkar och dokument får då en filväg t.ex: C:\user\rovi07\OneDrive - Region Vösterbotten\mappstruktur\dokument.docx. Den inloggade användaren (i exemplet rovi07) har tillgång till dokumenten men om t.ex aboo01 är inloggad i windows fungerar inte länken. Aboo01 måste också lägga till den aktuella mappen i sin OneDrive (beskrivning för detta finns) genom Sharepoint och en funktion i metodboken byter alltid länkar innehållande windows användare till den inloggade användarens namn. En länk med C:\user\rovi07\ blir då i aboo01’s fall C:\user\aboo01\ automatiskt och länken fungerar. Detta är det närmaste jag kommer en fungerande Sharepoint lösning i dagsläget.

**G. Kopiera metodbeskrivningar**Den enda funktionen som fungerar för alla admin användare på alla rum är att kopiera metodbeskrivningar. Tillhör du Rum CT med behörighet admin och/eller EA och inte har behörighet till Rum Hej, har du fortfarande möjlighet att kopiera en metod. Det kan vara designen på metoden alternativt hur den är skriven. Du väljer en egen titel och den kommer hamna under ditt rums metoder. Tillagda filer och bilder som inte är delade direkt i metoden kopieras inte.

**Andra funktioner som ej tillhör lathundar och metodbeskrivningar  
  
Nyheter/anslagstavla** – Där man kan skriva nyheter till specifika rum, koppla filer och även välja att skicka detta som mail till de användare som godkänt mail via metodboken  
  
**Gröna korset -** Fullt fungerande digital gröna korset som tillverkades av tristhet, kommer säkert aldrig användas men den finns där.  
  
**Beställning –** Beställningslistor för apotek, förråd, fixationsmaterial där de användare med ansvar för detta kan skapa listor och användare lägg till, ta bort och skriva nya beställningar. List-ägaren kan sedan stänga beställningen och skriva ut listan i ett excel dokument.

**Telefonbok –** Lägg till / ta bort telfonnummer, sök bland telefonnummer etc

**Filhanterare** – Skapa ”mappar” och lägg in filer som används ofta så placeras dom 2-3 klick bort i en ”dropdown” meny. Filer delas in per rum. Filerna kollas även om dom existerar innan de visas, existerar dom inte visas dom med ett streck över. Samt för admin användare kommer en notis att ”x antal filvägar fungerar inte längre”.  
Finns även ”dropdown” meny för 2 andra gemensamma grupper av länkar där jag testat lägga in en som ”diagnosgrupper” och en som ”studier” som då länkar filer till de pågående studierna som pågår samt diagnosgruppfiler.  
  
**Påminnelser och utlåning av utrustning** - Påminnelser där man ställer in när påminnelsen ska ge en notis, finns även kommentarfunktion där man kan beskriva eller länka till filer. Utlåning av utrustning tillvekades för att få statistik på hur ofta vi lånar ut fix-utrustning vi bara har en av varje, om det är rimligt att köpa in fler..

**Kalender** – alla rum har en kalender och varje användare har en kalender. Man kan lägga till andras kalendrar. Kalendern är även kopplat till påminnelser så påminnelser även syns i respektive kalender. Man kan även lägga ner en ”nedräkning” som kommer upp som en notis på skärmen när man loggar in. ”x antal dagar och timmar till xxx händer…”

**Inställningar** – Här har EA användare (Högre behörighet än admin) möjlighet att göra inställningar för Metodboken. Lägga till Rum, Utrustning för funktionen ”låna ut utrustning”, göra mailinställningar om man vill att Metodboken ska kunna skicka mail och vilken admin-mail som ska användas. Metod-grupper kopplade till de Rum som skapas, dvs de sub-grupper som kan användas för att skapa metodbeskrivningar i per Rum. Länka ihop Rum för adminanvändare, om jag vill skapa ett ”Hej” rum men mitt admin-rum är CT och jag vill ha koll på Hej-rummets länkar och metoder, ha behörighet till dessa för administrering kan jag länka CT med Hej, då kommer adminanvändare på CT ha tillgång till allt som görs på rum Hej, men Hej har inte tillgång till t.ex CT. Inställning för Nätverksvägar görs endast om en ny partition börjar användas. Te.x som när vi flyttade till V:. Metodboken behöver båda nätverksvägar samt mappad filväg tex V: har en nätverksväg [\\vll.se\Ytor](file:///\\vll.se\Ytor). Scriptet körs och alla mappade och nätverksvägar läggs till i databasen för att kunna hantera länkar skapade av Word dokument. Word dokument använder ofta nätverksvägen för att öppna filer, Metodboken behöver den mappade filvägen, därför jämförs nätverksvägar mot länkar och ersätts med dess mappade filväg. I vissa fall när länken är ”nära” word-filen används endast ..\..\document.docs eller bara mapp\dokument.docx, i dessa fall extraheras filvägen till originaldokumentet och antingen tar bort mappar eller lägger till mappstruktur för att hitta dokumentet.

**Framtida uppdateringar om Metodboken får leva vidare:**  
1. Valbart hur många metoder som sparas i versionskontrollen

2. Beskriva hur användare kan använda AI för att skapa snygga metoder och lathundar.

3. Beskriva i text i Metodboken hur och när man kan använda en webblänk för att ladda ner och visa metoder/dokument.

4. Istället för att alla metodbeskrivningar får en påminnelse efter 1 år, ska denna intervall kunna väljas vid skapande av en metod.

5. För tillfället endast metodbeskrivningar som är krypterade. Kan eventuellt läggas till på fler saker.

6. Endast användare, signeringar och behörigheter som har en verifikations-hash. Dvs ändras dessa på något vis blir de ogiltiga. Användare som ändras loggas ut och kan ej loggas in igen utan handpåläggning av admin/ea. Ändra en signering eller behörighet till metod renderar i en ogiltig signering eller ogiltig behörighet. Förslagsvis är dessa de enda ”viktiga” delar att skydda extra för manipulering men kan läggas till på t.ex filer / bilder som tillhör metoder för mer skydd.

7. Versionhanteringen bör splittas upp i månader och eventuellt år för att slippa stor databas.

8. Uppdaterad PHP version till över 8.5 fungerar ej på regionsdatorer, eventuellt vid uppdatering till win 11 görs nytt test för detta.

9. Just nu används chromium (chrome) för att rendera html, det finns en möjlighet att använda webbview2 vilket skulle göra programmet mindre och snabbare, just nu är det dock en hel del jobb att ändra funktioner att fungera med webview och problemet med chromium och att programmet tar plats är inte ett så stort problem.

**Övrigt**

Programmet används av CT och MR på strålbehandlingen NUS och hjälper oss att hålla koll på, och uppdatera metoder och lathundar på ett enklare och säkrare sätt än en mappstruktur i windows. Sarah Arvidsson Kelverot har fungerat som ”beta-testare” och får ofta testa funktioner och återkomma med kritik, i övrigt är det vi personal som använder den och fel hanteras så fort de uppstår. Nya funktioner skapas efter önskemål och behov. Förhoppningsvis är vi snart inne i en helt färdig produkt…….. men uppdateringar är roliga och kommer ofta allt eftersom jag lär mig mer om dokumenthantering och säkerhet.