Elektroniske regnskskapsdata: Standardiserte formater, XBRL Kryptering og signering Altinn og Brønnøysundregistrene

REV3576

1

Lagring (egentlig gjenfinningsbehovet)

- Regnskapsmaterialet bl a som bevis/legitimasjon av posteringer
- I ustrukturerte filer (tekstfiler: dokumentasjon)
  - Hvordan gjenfinne/søke?
- Strukturerte filer (formatstyrt tolkning)
  - Strukturert lagring etter (viktigste) søkekriterier
  - I (relasjons-)databaser
  - I tabeller (formatstyrt tolkning)
    - Samling av tabeller
    - Med en definert sammenheng mellom tabellene

2

Pålitelig dokumentasjon og data

- Hvordan skape pålitelig lagring og bruk?
  - Styrt produksjon, lagring og bruk
    - Internkontrollopplegg
    - Autoriserte transaksjoner
- Hvordan kontrollere om data er pålitelige?
  - Erfaring, læring
  - Analyse av postens egenskaper
  - Kan vi se på bilaget om det er ekte?
  - Hva med lektroniske data

3

Risiko

- Uautorisert endring og tap av data
- Større usikkerhet rundt transport av data enn lagring av data
- Risiko håndteres med kontroller
- Redundans i data
  - Overflødig informasjon (mer data enn du trenger for å tolke data til informasjon)
  - Alle kontroller forutsetter redundant informasjon

4

Sikkerhet ved transport av data

- Sikkehetskomponentene
  - Tilgjengelighet
  - Konfidensialitet
  - Integritet
- Kan du se på skjermbildet om transporten er beskyttet når du anroper en hjemmeside på nettet?

5

Kryptering på nettet

- SSL (secure Socket Layer)
  - Konfidensialitet, ikke integritet
    - Kryptert med mottagerens off nkl
- Transaksjonsintegritet
  - Systemet behandler transaksjonen fullstendig, nøyaktig, i tide og autorisert
- Ikke-benektelse
  - Kryptert med avsenderens private nkl

6

Mer om revisjonsspor

- Elektroniske
  - Hvor oppstod trans
  - Hvem initierte trans
  - Når
  - Data som ble
    - Lagt til
    - Endret
    - Fjernet
- Krav om eksistens og bestandighet

7

EDU / EDI
Elektronisk datautveksling

- Tabell sendes fra avsender til mottager
  - Eks. betalingstrans til banken
- Formatene er forhåndsavtalt
  - Kolonner og layout
  - Kodealfabet
  - Krever mye standardiserings- og avtalearbeid
- EDIFACT

8

Alternative publiseringsformer

- WWW
  - HTML
  - PDF
  - Excel
  - XML
    - XBRL
- Interne applikasjoner
  - rapporter
  - spørrebilder
  - tabelltilgang
- Oppgavene
  - Manuell / automatisk behandling
  - Søking/navigasjon
    - Google
  - Import til egen applikasjon
    - Regnskapsanalyse
    - Konsolidering
  - Transformasjoner
    - NGAAP - USGAAP
    - IAS - USGAAP

9

SAMFUNNSØKONOMI

- Store kostnader ved
  - registrering
  - tolkning
  - tidsforsinkelse, nøyaktighet
- når regnskapsdata skal viderebehandles
  - jf Altinn-prosjektet
    - Applikasjon for SA, næringsskjema mm
    - Mottak av XML-filer fra bpkførimgssystemer/ÅR-systemer

10

Presentasjonsteknologier

- Bilde (.bmp, .jpg, .tif, osv)
- HTML-tekst (gir en viss tilpasning mellom layout og presentasjonsteknologi)
- HTML/CSS (standardisering av layout)
- XML (maskinell tolkning av form *og innhold*)
- XBRL e.l. - definisjoner i kontekst muliggjør tolkning

11

Hvorfor?

- Gjenbruk av data uten manuell behandling
  - Fullstendig ,Nøyaktig ,Pålitelig
  - Kostnadseffektiv
  - Tidsbesparende (gir økt infoverdi)
- Tolkningsrammen sammen med transene
- Automatisert tolkning (parser)
- SEC foreslo (mai 2008) obligatorisk rapportering v.hj.a. XBRL innen tre år
  - Implikasjoner for revisjonen

12

Data eller informasjon

- Regnskapsdata
  - Filformat
  - Tegnformat
- I databaser?
  - Standardisert/program-mert bruk
- Ved overføring?
  - Flere sporadiske brukere
- Tolkningsregler
- Termdefinisjon v.hj.a.
  - Maskinlesbare / menneskelesbare definisjoner
  - layout
    - klassisk filoverføring
    - EDIFACT etc.
  - Tagging

13

HTML

- (Rå-)dataene
  - dvs tabellinnholdet f.eks i POSTER
- Men hvordan skal disse vises på skjermen?
- Layoutopplysninger
  - <H1> . . . </H1> (Største heading)
  - . . . (fet skrift)
  -
 (betyr linjeskift)
- Standardiserte formatregler
  - CSS (Cascading style sheets)

14

XBRL er

- Royalty-fri lisensiert
- åpen spesifikasjon
- for programvare
- som bruker XML-tagger
- for å beskrive finansiell informasjon

15

Begreper

- Taksonomi
  - Et XML-skjema der nye elementer defineres i samsvar med et konsept som kan referes i et XBRL-dokument
- Forekomst(-dokument)
  - Et XML-dokument som inneholder XBRL-elementer
- Element
  - et XML-element *eller* et datum som uttrykker et faktum (dataverdi)

16

Forekomst

- <Item type="debitorer.kundeReskontro"> 1000000</item>

Xbrl-element fra en regnskapstaksonomi

Element med et faktum - dataverdi - som angis i tråd med reglene for XBRL-elementet

17

Dokumentet (forekomsten)

- Henviser til
  - -en taksonomi, dvs et XML-skjema
    - f.eks. http://www.iasc.org/xbrl/airline/2000-07-07-airline-xsd
    - evt. Foretaksspesifikke utbidelser av skjemaet
  - et CSS
    - et cascading style sheet som styrer layout ved ulike presentasjoner av dokumentet
- inneholder
  - dataverdier

18

Eksempel

- <element name="eiendeler.mestLikvideEiendeler" type="xbrl:beløp">
  - <annotation>
    - <appinfo>
      - <xbrl:rollup to="balansen.eiendeler" weight="1" order="1"/>
    - </appinfo>
  - </annotation>
- </element>

Sorteringsrekkefølge ved presentasjon

XBRL

- Rådata / forekomst
  - som i tabellen,
  - men merket med TAGGER
    - HTML/CSS
    - Semantiske termer
      - Ktonr
      - Transaksjonsdato
      - Regnskapsperiode
      - ("kolonnenavn")
- Ligger på regnskapets hjemmeside eller sendes
- Felles internasjonale definisjoner av regnskapstermer / skjema
  - Kjernetermer
  - Juridiksjon ("over et namespace")
    - US-GAAP
    - IAS
      - UK-GAAP
      - N-GAAP (NRS)
        - » selskap
  - Bransjetermer
- Ligger på hjemmesider

Hvem skal lage hva?

- Taksonomiene (termdefinisjonene)
  - logisk
  - "hjemmesider"
- Tagging av rådata
  - regnskapsavleggeren
  - Bokføringssystem-produsenten
  - Produsenten av årsregnskapssystemer

Taksonomier

- Termdefinisjoner
- Årsregnskap
- Hovedbokstransaksjoner

- Applikasjonsavhengige
  - (XML, ikke nødvendigvis XBRL)
  - Banktransaksjoner
  - Tolltransaksjoner

22

Attestasjon / revisjon

- Hva bør attesteres / revideres?
  - Rådata ?
  - Termbruk ?
  - Regnskapsproduksjonssystem?
- Hvordan vise attest ovenfor tredjepart?
  - Trust services

23

Bokføringen

- Rapportplikten styrer bokføringen
- Rapporten bygger på lagrede data
- Som igjen bygger på registreringer av
  - Transaksjoner
    - Ordre, lønn, faktura, bank, osv
  - Faste data i tabeller
    - Kontoplan, kunder, leverandører, osv
- Revisor må vite hvor data kommer fra for å kunne vurdere data- (regnskaps-) kvaliteten
  - Hele transaksjonen
  - Deler av transaksjonen

24

Årsavslutningssystem Næringsskjema og ligningspapirer

- Produseres i et årsavslutningssystem
  - F eks Maestro
- Funksjoner
  - Import av saldobalanse (saldoer på alle konti)
  - Saldoene styres til riktige felt i RF-skjemaet
    - Se skatteetaten for oer sikt over skjemaer
  - Beregninger og avstemminger
  - Signering og oversendelse
  - Lagring

25

Kryptering

Hvordan kan vi bekrefte at data er autentiske?

Hvorfor skal data være autentiske?

Sammenheng mellom autentiske og autoriserte data

Verktøy for konfidensialitet og integritet

Google, Wikipedia: PKI Kryptering

26

Nonsenstotaler

- MD5 Message digest nr 5
  - en avstemming
  - enkel å sammenligne for mennesker
  - dataverdier og posisjon påvirker summen
  - ikke teoretisk umulig men vanskelig å lage kompenserende endringer for å lure kontrollen
- Liten endring i tekst gir stor endring i totalen (summen)
- sal.bi.no/md5.htm

27

Symmetrisk kryptering

- En felles nøkkel avtales mellom sender og mottager
- X=D(M,N) og M=D(X,N)
  - eks. DES
- Fordeler
  - rask kryptering og dekryptering
- Ulemper
  - Mange nøkler nødvendig hvis flere parter

28

Assymmetrisk kryptering

- Hver deltager har to nøkler
  - privat nøkkel Np som bare er kjent av eieren
  - offentlig nøkkel No som er kjent av alle
- X=D(M,Nps) M=D(X,Nos) integritet
- X=D(M,Nom) M=D(X,Npm) konfidensialitet
- Fordeler
  - kun to nøkler hos hver deltager
- Ulemper
  - krypteringstid

29

Sertifikater

- Distribusjon av nøkler
  - Sertifikatutsteder krypterer din off nkl med sin private nkl
  - Du kan kopiere og videresende din off nkl, sertifikatet
  - mottager kan trygt dekryptere din off nkl ved hjelp av sertifikatutstederens off nkl

30

Eksempel på meldingssikring

- Ta MD5-sum av meldingen
- Krypter summen med din private eller mottagers off nkl, summen kalles da digital signatur
- Send signaturen sammen med meldingen
- Mottageren gjentar MD5-beregningen og sammenligner med dekryptert signatur

31

Lov om elektronisk signatur (§ 3)

- *elektronisk signatur*: data i elektronisk form knyttet til andre elektroniske data og som brukes som autentiseringsmetode,
- *avansert elektronisk signatur*: elektronisk signatur som
  - er entydig knyttet til undertegneren,
  - kan identifisere undertegneren,
  - er laget ved hjelp av midler som bare undertegneren har kontroll over
  - er knyttet til andre elektroniske data på en slik måte at det kan oppdages om disse har blitt endret etter signering,
- *kvalifisert elektronisk signatur*: avansert elektronisk signatur basert på et kvalifisert sertifikat og fremstilt av et godkjent sikkert signaturfremstillingssystem,

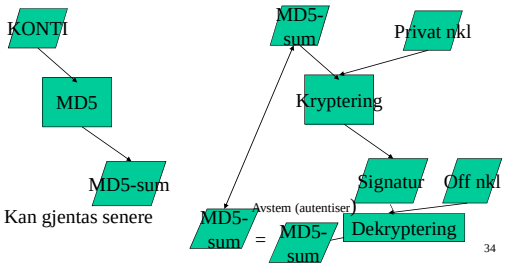
32

Lov om elektronisk signatur (§ 3)

- *undertegner*: den som disponerer et signaturfremstillingssystem og som handler på vegne av seg selv eller på vegne av en annen fysisk eller juridisk person,
- *signaturfremstillingssdata*: unike data, som for eksempel koder eller private nøkler, som undertegneren benytter for å fremstille en elektronisk signatur,
- *signaturfremstillingssystem*: programvare eller maskinvare som benyttes til å fremstille elektronisk signatur ved hjelp av signaturfremstillingsdata
- *signaturverifikasjonsdata*: unike data, som for eksempel koder eller offentlige nøkler, som benyttes til å verifisere en elektronisk signatur
- *signaturverifikasjonssystem*: programvare eller maskinvare som benyttes for å verifisere elektronisk signatur ved hjelp av signaturverifikasjonsdata
- *sertifikat*: kobling mellom signaturverifikasjonsdata og undertegner som bekrefter undertegners identitet og er signert av sertifikatutsteder
- *sertifikatutsteder*: fysisk eller juridisk person som utsteder sertifikater eller tilbyr andre tjenester relatert til elektronisk signatur

33

Signering av en hel tabell: KONTI



34

Signering av hver linje i KONTI

Ktonavn	Std Avdkode	Klasse A/E/G/I/K	Resk-kode	SA-nr	RS-nr	Endret dato	Elektronisk Signatur
Kunder	0	A	P			20060110	1A3201103F77C
Kasse	0	A	N			20060110	
Leverandører	0	G	J			20060110	
Mva Høy sats	0	G	N			20060110	
Salg avgpl høy sats	1	I	N			20060110	

1. MD5-sum av cellene som skal signeres
2. Kryptering med privat nøkkel

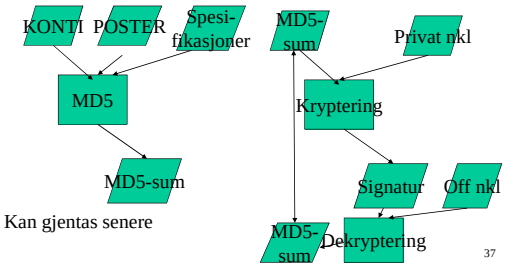
35

Signering i POSTER

- Brukerident for den som har registrert
- Regnskapsperiode
- Avansert signatur for den som har
  - registrert
  - foretatt regnskapsavslutning med posten
  - revidert posten

36

Signering av hele regnskapet (jf Altinn)



37

Revisjon av elektronisk publisert regnskap iflg Soltani (for eksempel XBRL-publisering)

- Momenter utover dagens revisjonshandlinger
  - Testing av tagger
    - Passende tag og fullstendige data
  - Kontroller
    - Dokumentasjon, vurdering, målrettethet
    - Testing av kontroller
      - Bruk av taksonomi
      - Tagging av data
      - Dataintegritet
  - Konkludere

38