XBRL
hva og hvorfor

Svein A. Løken

EDU - EDI

- Effektivt og pålitelig
- Alternativer å sende
  - Regneark (formater?)
  - Tradisjonelle filer (kolonner)
  - Data og tolkningsinformasjon sammen
    - EDI, dvs EDIFACT og lignende
    - XML
      - XBRL

XBRL er

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

XBRL kommer fra

- xbrl.org
- AICPA / CICA
- Revisororganisasjonene forøvrig
- US-GAAP og IAS forankring

Hvorfor?

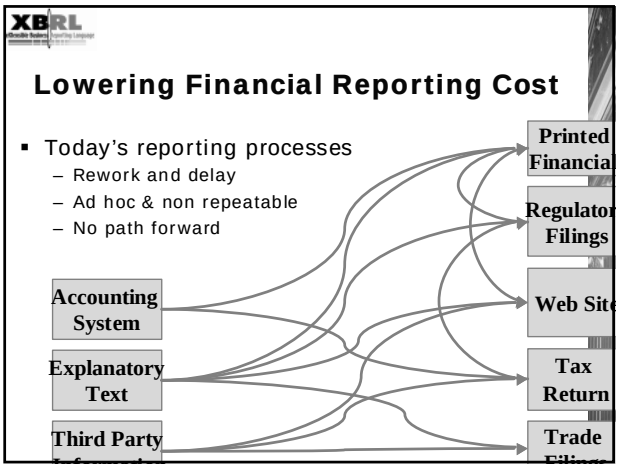
- Gjenbruk av data uten manuell behandling
  - Fullstendig ,Nøyaktig ,Pålitelig
  - Kostnadseffektiv
  - Tidsbesparende (gir økt infoverdi)
- Tolkningsrammen sammen med transene
- Automatisert tolkning (parser)

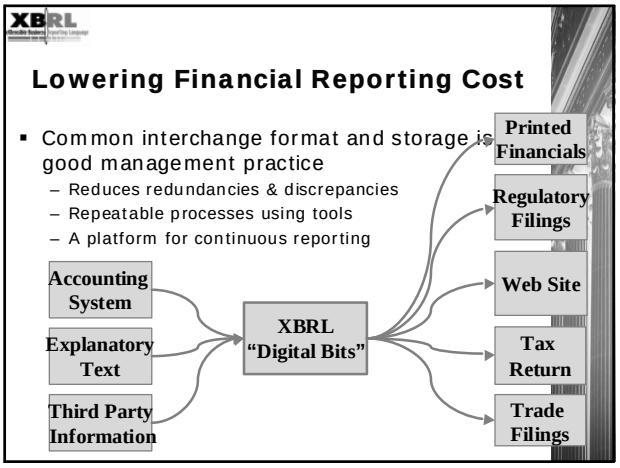
Presentasjonsteknologier

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

Wikipedia-adresser

- http://en.wikipedia.org/wiki/HTML
- http://en.wikipedia.org/wiki/XML
  - Se på DTD og XML-schema
- http://en.wikipedia.org/wiki/XBRL
- http://en.wikipedia.org/wiki/MD5
- http://en.wikipedia.org/wiki/Public_key_infrastructure





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)

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

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

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

Kryptering

REV2403 - 2008

Hvordan kan vi bekrefte at data er autentiske?

Hvorfor skal data være autentiske?

Hva er sammenhengen mellom autentiske data og autoriserte data?

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

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

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

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

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

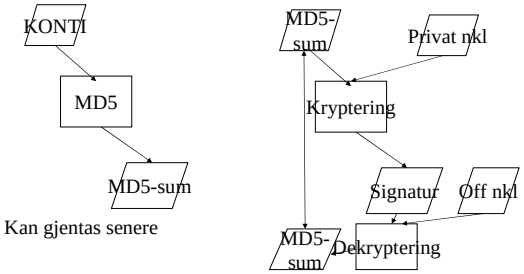
Lov om elektronisk signatur (§3)

- *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,

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

Signering av en hel tabell: KONTI



Signering av hver linje i KONTI

	Std	Klasse	Resk-	SA-	RS-	Endret	Elektronisk Signatur
Ktonavn	*Avdkode*	*A/E/G/I/K*	*kode*	*nr*	*nr*	*dato*	
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

Signering i POSTER

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

Signering av hele regnskapet (jf Altinn)