

JH kap 7
XBRL
Kryptering og signering
MRR 6274 V2010

Sporingsverktøy på internett

- På serveren
 - Logfiler
 - Tidspkt, IPadresse, tjeneste, osv
- Hos klienten
 - Logfiler
 - Sist besøkte sider, adresse og kopi
 - Informasjonskapsler (Cookies)
 - Spionvare

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

Revisjonsspor

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

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

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

SAMFUNNSØKONOMI

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

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

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

Data eller informasjon

- | | |
|--|--|
| <ul style="list-style-type: none">• Regnskapsdata<ul style="list-style-type: none">– Filformat– Tegnformat• I databaser?<ul style="list-style-type: none">– Standardisert/programmert bruk• Ved overføring?<ul style="list-style-type: none">– Flere sporadiske brukere | <ul style="list-style-type: none">• Tolkningsregler• Termdefinisjon v.hj.a.<ul style="list-style-type: none">– Maskinlesbare / menneskelesbare definisjoner– layout<ul style="list-style-type: none">• klassisk filoverføring• EDIFACT etc.– Tagging |
|--|--|

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)

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

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>`

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

Xbrl-element fra en
regnskapstaksonomi

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

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
 - Kjernetерmer
 - Juridiksjon ("over et namespace")
 - US-GAAP
 - IAS
 - UK-GAAP
 - N-GAAP (NRS)
 - » selskap
 - Bransjetermer
- Ligger på hjemmesider for termer

Hvem skal lage hva?

- Taksonomiene (termdefinisjonene)
 - logisk
 - “hjemmesider”
- Tagging av rådata
 - regnskapsavleggeren
 - RIS-produsenten
 - Produsenten av årsregnskapssystemer

Taksonomier

- Termdefinisjoner
- Årsregnskap
- Hovedbokstransaksjoner
- Applikasjonsavhengige
 - (XML, ikke nødvendigvis XBRL)
 - Banktransaksjoner
 - Tolltransaksjoner

Attestasjon / revisjon

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

Kryptering

Verktøy for konfidensialitet og integritet

Google, Wikipedia: PKI Kryptering

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

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 N_p som bare er kjent av eieren
 - offentlig nøkkel N_o som er kjent av alle
- $X=D(M,N_p)$ $M=D(X,N_o)$ integritet
- $X=D(M,N_o)$ $M=D(X,N_p)$ 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 offentlige nøkkel, summen kalles da digital signatur
- Send signaturen sammen med meldingen
- Mottageren gjentar MD5-beregningen og sammenligner med dekryptert signatur

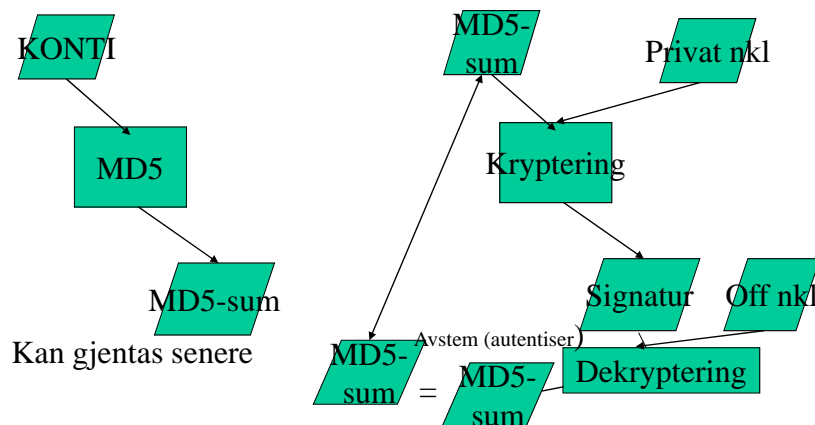
Lov om elektronisk signatur (§3)

- *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,
- **signaturfremstillingsdata:** 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

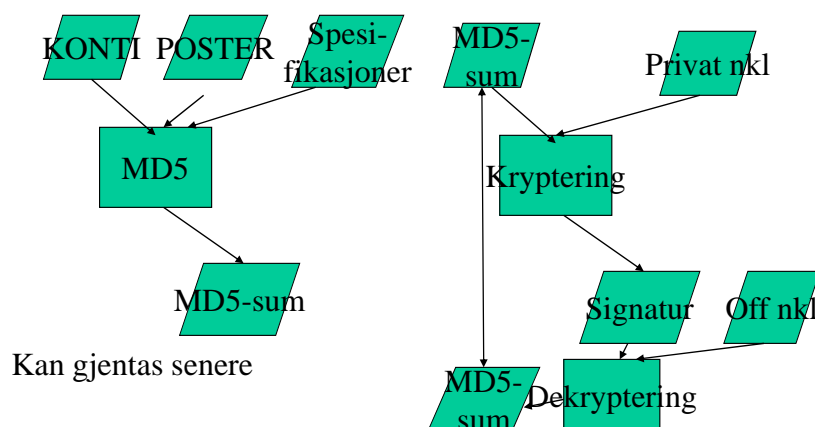
	<i>Std</i>	<i>Klasse</i>	<i>Resk-</i>	<i>SA-</i>	<i>RS-</i>	<i>Endret</i>	Elektronisk
<i>Ktonavn</i>	<i>Avdkode</i>	<i>A/E/G/I/K</i>	<i>kode</i>	<i>nr</i>	<i>nr</i>	<i>dato</i>	Signatur
Kunder		0 A	P			20060110	1A3201103F77C
Kasse		0 A	N			20060110	
Leverandører		0 G	J			20060110	
Mva Høy sats		0 G	N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

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

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)



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