WebTrust – mere end blot en elektronisk påtegning

Peter Havskov Christensen
Handelshøjskole Syd
Engstien 1
6000 Kolding
E-mail: phc@ko.hhs.dk

1. udgave – 14. august 1998

Resumé

Siden Elliot-rapportens offentliggørelse er interessen for Assurance Services øget væsentligt. WebTrust er et nyt initiativ indenfor Assurance Services. WebTrust principperne er bredt formulerede og har til hensigt at være forståelige for Internetbrugere i almindelighed. Den bagvedliggende teknik er mere kompleks. Den giver til gengæld revisorerne nogle muligheder, der rækker langt videre end selve WebTrust-konceptet. Denne artikel giver en gennemgang af den bagvedliggende teknik, sammenholder teknikken med WebTrust principperne samt skitserer nogle fremtidsmuligheder ved anderledes benyttelse af teknikken.

Baggrund

I 1994 oprettede American Institute of Certified Public Accountants (AICPA) en "Special Committee on Assurance Services" med Robert K. Elliot som formand. I 1996 udgav komiteen sin rapport, der i daglig tale kaldes "Elliot-rapporten".

På baggrund af faldende omsætning fra traditionel revision øges interessen for "Assurance Services". Der lægges oftere lægges anden information end reviderede regnskaber til grund ved beslutningstagning. Det er også en medvirkende faktor[1].

"Assurance Services" defineres som uafhængige professionelle serviceydelser som øger kvaliteten af information (eller dens kontekst) for beslutningstagere. Mange amerikanske revisorer anser "Assurance Services" som meget betydende for branchens fremtid. Denne amerikanske vision har allerede medført praktiske tiltag. WebTrust er et sådant tiltag.

WebTrust konceptet er udviklet af AICPA, Canadian Institute of Chartered Accountants (CICA) og Verisign (kommerciel udbyder af digitale certifikater). Det er meningen, at WebTrust konceptet skal signalere sikkerhed til potentielle kunder og dermed bevirke, at flere er villige til at handle på Internettet.

En undersøgelse foretaget i 1997 af Yankelovich Partners for AICPA viser, at 85% af brugerne på internet ikke vil oplyse deres kreditkortnummer on-line. Et stort flertal af

[1] Denne udvikling er nærmere beskrevet af Wivel, Hansen og Buhl (1997).

brugerne tøver også med at oplyse telefonnummer (74%) og adresse (67%). Andre undersøgelser har vist, at kun mellem 20 og 25% af brugerne er villige til at købe ind i Cyberspace (Johnson 1998).

En canadisk undersøgelse fra 1998 viser, at hele 89% af virksomhedslederne er enige i, at manglende sikkerhed ved og tillid til transaktioner på Internettet er en barriere for deres virksomheds handel via Internet (KPMG 1998).

Virkemåde

WebTrust konceptet er pakket pænt ind i en grafisk overflade i de moderne browsere. Brugerne ser ikke meget til den bagvedliggende virkemåde. Dette er sandsynligvis nødvendigt for, at konceptet kan få en bredere udbredelse, men det gør det vanskeligt at forstå konceptets virkemåde. Af den årsag opdeles beskrivelsen af virkemåden i "Virkemåde set fra brugeren", "Den bagvedliggende teknik" og en "Sammenholdelse".

Virkemåde set fra brugeren

WebTrust er AICPA og CICA's bud på en serviceydelse, der kan øge tilliden ved Internetbaseret handel og dermed øge handlen. Der er 3 overordnede WebTrust principper, der skal overholdes af virksomheder, der ønsker at opnå et WebTrust segl:

- **Business Practices Disclosure Principle.** The entity discloses its business practices for electronic commerce transactions and executes transactions in accordance with its disclosed business practices.
- **Transaction Integrity Principle.** The entity maintains effective controls to provide reasonable assurance that customers' orders placed using electronic commerce are completed and billed as agreed.
- **Information Protection Principle.** The entity maintains effective controls to provide reasonable assurance that private customer information obtained as a result of electronic commerce is protected from uses not related to the entity's business (AICPA og CICA 1997)[2].

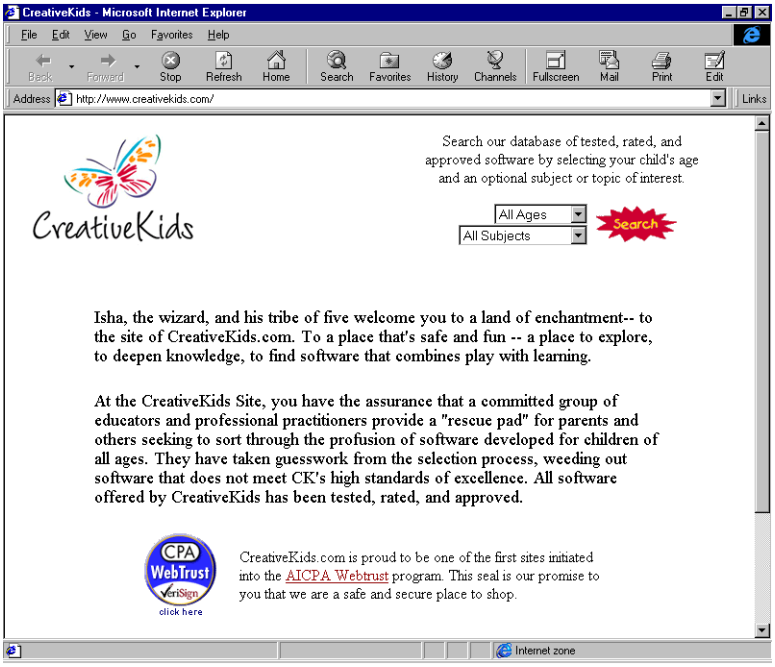
Medlemmer af AICPA og CICA, som har fået særlig træning i gennemgang af internetsider og elektronisk handel, kan udstede en erklæring til en virksomhed om, at virksomhedens internetsider og forretningsgange lever op til WebTrust principperne[3]. Virksomheder, der har fået en sådan erklæring, må benytte Webtrust seglet på deres hjemmeside. Seglet må

[2]Fra adressen http://www.cpawebtrust.org/shared/details/crit.pdf kan "WebTrust Principles and Criteria" downloades i Adobe Acrobat format. Det er pt tale om version 1.0 fra 23. december 1997. Ifølge Johnson (1998) arbejdes der for tiden på en version 1.1, der også indeholder specifikationer for on-line banking og handel med værdipapirer. Den nuværende version 1.0 er meget fokuseret på detailhandel. Det er også blevet påpeget af Journal of Accountancy (1998)

[3]Der er mange lighedspunkter mellem den anbefalede amerikanske og canadiske standarderklæring. En væsentlig forskel er dog, at den amerikanske standarderklæring benytter ordet "examined", mens den candiske benytter ordet "audited". Begge standarderklæringer er gengivet i WebTrust Principles and Criteria.

benyttes på alle sider. Det skal benyttes på den eller de sider, hvor den elektroniske transaktion afsluttes (typisk siden hvor kunden oplyser navn, adresse og kreditkortnummer). I figur 1 ses seglet benyttet af firmaet Creative Kids. WebTrust seglet er et symbol på, at en Webside har opnået en blank erklæring fra revisor.

Figur 1: Creative Kids Hjemmeside med WebTrust seglet



WebTrust seglet er, som alle andre billeder på Internet, blot en grafikfil. Det kan derfor meget let kopieres. Sikkerheden ligger således ikke i selve seglet, men i det bagvedliggende digitale certifikat. Certifikatet indeholder links til WebTrust principperne, ledelsens erklæring om overholdelse af WebTrust principperne, virksomhedens praksis vedrørende handel på internet, revisors erklæring om virksomhedens overholdelse af den offentliggjorte praksis og WebTrust principperne samt en vejledning fra Verisign. Vejledningen, der grafisk ligner et certifikat på papir, forklarer, hvordan det digitale certifikat efterprøves. Uden efterprøvelse af det digitale certifikat bør WebTrust seglet ikke betragtes som ægte.

Den bagvedliggende teknik

Når brugeren klikker på WebTrust seglet, sker der mere end blot visning af certifikatet. Kommunikationen mellem browser og server skifter fra usikker til sikker. Dette kan ses ved, at internetadressen starter med https:// i stedet for http:// som normalt. De nyere udgaver af Internet Explorer og Netscape viser desuden en hængelås (eller nøgle) i statuslinien, når der anvendes en sikker forbindelse.

Den sikre forbindelse etableres ved hjælp af en teknik kaldet Secure Socket Layer (SSL). SSL benytter kryptering til at sikre kommunikationen[4]. Der findes grundlæggende 2 typer af kryptering:

- **Symmetrisk kryptering** er den enkleste form for kryptering. Den samme nøgle (kode) benyttes til at enkryptere (oversætte fra klartekst til kodesprog) og dekryptere (oversætte fra kodesprog til klartekst). Symmetrisk kryptering kan sikre hemmeligholdelse. Den vigtigste forudsætning er, at de 2 parter i forvejen har aftalt nøglen på en måde, som uvedkommende ikke kan aflytte.

- **Asymmetrisk kryptering** kaldes også public key kryptering. Her anvendes et nøglepar bestående af en privat nøgle (private key) og en offentlig nøgle (public key). Ved denne krypteringsmetode kan der opnås sikkerhed uden forudgående udveksling af nøgler. En meddelelse, der enkrypteres med den ene nøgle (offentlig eller privat), skal dekrypteres med den anden nøgle fra det pågældende nøglepar[5]. Såfremt der enkrypteres med modtagers offentlige nøgle, vil dekryptering således kræve modtagers private nøgle og dermed sikre hemmeligholdelse. Autenticitet kan også dokumenteres, såfremt afsender enkrypterer med sin private nøgle. Modtager kan så prøve, at dekryptere med afsenders offentlige nøgle. Hvis det kan lade sig gøre, er det bevis for, at meddelelsen er enkrypteret med afsenders private nøgle. Asymmetrisk kryptering kan, når det anvendes korrekt, sikre hemmeligholdelse og dokumentere autenticitet (Christensen og Jensen 1997, 51–56).

Umiddelbart virker asymmetrisk kryptering som den oplagte løsning, men asymmetrisk kryptering er meget beregnings- og dermed tidskrævende. Dette skyldes, at der skal være en sammenhæng mellem den private og offentlige nøgle, men det må ikke være muligt at beregne den private nøgle ud fra den offentlige nøgle.

I praksis benyttes derfor ofte en kombination af de 2 metoder. Også SSL benytter en kombination. Når der etableres en sikker forbindelse via SSL sker der i hovedtræk følgende[6]:

1. Serveren og browseren udveksler offentlige nøgler (denne udveksling kan aflyttes, men det betyder ikke noget for sikkerheden).

2. Browseren genererer en tilfældig nøgle (kaldet session key) til brug for kryptering af meddelelserne.

3. Browseren enkrypterer den genererede nøgle med serverens public key og fremsender den til serveren.

[4]Kryptering er gennemgået med revisorer som målgruppe af Friedlob, Plewa, Schleifer og Schou (1997) og Sølberg og Juhl (1994).

[5]Princippet kendes fra programmet Pretty Good Privacy (PGP), som er beskrevet af Rasmussen og Thelin (1996) samt af Snedker (1997).

[6]En mere detaljeret beskrivelse findes hos Vanglo (1998). Af hensyn til overskueligheden er brug af hash-funktioner ikke beskrevet her. Hash-funktioner er en form for avanceret checksum, der benyttes til kontrol af, om de krypterede (og dermed uforståelige) data er ændret undervejs på nettet.

4. Serveren dekrypterer den fremsendte nøgle. Herefter er begge parter i besiddelse af een nøgle, som kan benyttes ved den senere udveksling af data (som krypteres symmetrisk af hensyn til hastigheden).

5. Browseren sender besked til serveren om hvilke algoritmer den understøtter og serveren vælger den stærkeste.

Som det fremgår af ovenstående, benyttes asymmetrisk kryptering til udveksling af nøgler. Derefter benyttes symmetrisk kryptering til selve dataoverførslen. Alt dette ser den almindelige bruger ikke. Når hængelåsen (eller nøglen) vises, er der udvekslet nøgler, og kommunikationen foregår sikkert.

Metoden giver en meget høj grad af sikkerhed for, at ingen uvedkommende kan lytte med på kommunikationen mellem browser og server. Der er derimod ikke i det ovenfor beskrevne sikkerhed for, at serveren virkelig tilhører det firma, som det ser ud til. Populært sagt er situationen den, at ingen kan lytte med på kommunikationen mellem browseren og serveren, men serverens identitet er ikke dokumenteret.

SSL indeholder også en løsning på dette. Serverens identitet sikres med et digitalt certifikat. Et sådant certifikat er et ID-kort, som er digitalt signeret af et firma, vi har fundet troværdigt. I den sammenhæng er det værd at bemærke, at når man installerer en af de nyere browsere, installerer man også en standardopsætning af, hvilke udstedere af digitale certifikat der er troværdige[7].

Sammenholdelse

Det er tilliden til krypteringen i SSL, der giver sikkerhed mod aflytning. Det er tilliden til udstederen af certifikatet, der er afgørende for tilliden til modpartens identitet. Overbevisning om sikkerhed mod aflytning og modpartens identitet kræver i princippet ikke, at der er en revisor inde i billedet.

Revisorerne kan gøre en forskel ved efterprøvelse af, om virksomheden følger den offentliggjorte forretningspraksis. Her kan de benytte den tillid, som der generelt er til revisorstanden[8]. Den tillid, som revisorerne nyder fra deres traditionelle revisionsopgaver, kan måske give dem en fordel frem for andre udbydere af tillid i forbindelse med Internethandel.

Om konkurrencen på området for Assurance Services er anført:

> Assurance services depart from the audit tradition in that a high proportion of them are outside the protected professional monopoly. Assurers are likely to be competing

[7] Du kan checke hvilke udstedere din browser accepterer på følgende måde:

- *Internet Explorer 4:* I menuen View vælges Internet Options. Klik på fanebladet Content og derefter knappen Authorities.
- *Netscape 4:* I menuen Window vælges Security Info. Klik på signers og der fremkommer en liste.

[8] Tilliden er tilsyneladende stadig eksisterende på trods af de mange eksempler på, at virksomheder med blank påtegning pludselig er gået ned. Som påpeget af Power (1994) har revision den bemærkelsesværdige egenskab ikke at være sårbar overfor egne fejl.

> with software firms, system houses, and consultancies, for example. This is not a case of outsiders poaching our traditional work. It arises because the greatest opportunities for new assurance services are in unregulated areas (Elliott 1998).

Elliott (1998) mener, at revisorerne har store muligheder i dette nye og konkurrenceprægede marked fordi, revisorer har ry for integritet, kompetence og erfaring indenfor kontroller, måling, efterprøvelse og IT.

Et væsentligt spørgsmål, som ikke er besvaret i de offentliggjorte undersøgelser, er, om det er sikkerheden mod aflytning, sikkerheden om modpartens identitet eller revisors erklæring der giver den øgede tillid. De 2 første punkter kan mindst lige så vel leveres af ikke revisorer.

Meget tyder på, at revisorerne, med WebTrust konceptet, kan levere den tillid, der er nødvendig for at øge handelen på Internet. Modsat er der ikke ingen tydelige tegn på, at revisorerne er de eneste, der kan levere den tillid.

Perspektiver

WebTrust konceptet er på mange måder en naturlig fortsættelse af udviklingen i revisionsbranchen. Der fokuseres i stadig højere grad på kontrol af kontrol og i mindre grad på efterprøvelse af substans. Det kan også virke umiddelbart logisk, når man ser på nogle af de videre perspektiver i Elliot-rapporten såsom åbne databaser, hvor eksterne interessenter kan trække de data, de ønsker. Såfremt revisor skal kunne tilføje nogen form for troværdighed til sådanne foranderlige data, kan det kun ske ved efterprøvelse af kontroller, da dataene ændres oftere end det er økonomisk muligt at verificere dem.

Revisorerne kunne dog også udnytte de teknologiske muligheder på en helt anden måde. Mange andre brancher har oplevet "back to basics" bølger, men denne trend har ikke påvirket revisionsbranchen. Den krypteringsteknologi som WebTrust konceptet udnytter til digitale certifikater, kan også bruges til digital signatur på EDI-bilag.

I så fald ville edb-baserede revisionsværktøjer ikke blot være særdeles egnede til sammentælling, statistik og analyse. Det ville være muligt hurtigt og effektivt at sammenholde bogholderi og elektronisk overførte digitalt signerede bilag. En tilbagevenden til substansrevision kunne blive at foretrække ud fra effektivitetshensyn.

Litteratur

AICPA og CICA (1997). Aicpa/cica webtrust principles and criteria for business-to-consumer electronic commerce. version 1.0. december 23, 1997. http://www.cpawebtrust.org/shared/details/crit.pdf (downloaded 14. august 1998).

Christensen, P. H. og M. J. Jensen (1997). *Edb-udviklingens betydning for revisionsmål, -beviser og -metoder*. København: Foreningen af Yngre Revisorer og Forlaget FSR.

Elliott, R. K. (1998). Assurance services and the audit heritage. *The CPA Journal* (7), 40–42, 44–47.

Friedlob, G. T., F. J. Plewa, L. L. F. Schleifer og C. D. Schou (1997). An auditor's primer on encryptation. *The CPA Journal* (11), 40–42, 44–45, 60–61.

Johnson, E. C. (1998). Testimony of Everett C. Johnson, chairman, aicpa task force on electronic commerce assurance services, partner deloitte & touche llp, wilton, connecticut, representing the american institute of certified public accountants (aicpa) before the house committee on commerce subcommittee on telecommunications, trade and consumer protection june 25, 1998. http://www.aicpa.org/belt/johnson.htm (6. august 1998).

Journal of Accountancy (1998). Webtrust isn't just for stores. *Journal of Accountancy* (4), 81.

KPMG (1998). 1998 electronic commerce survey. Downloaded fra Internet. URL: ftp://ftp.kpmg.ca/pub/ecomm/98ecs.pdf (14. august 1998).

Power, M. (1994). *The Audit Explotion*. London: Demos.

Rasmussen, K. og J. Thelin (1996). *Sikkerhed på internettet med PGP*. København: Borgen.

Snedker, S. (1997). Pgp for noble fritænkere (version 1.5 8-dec-97). *Alt om Data*. URL: http://www.aod.dk/aod/net-kurs/ss_pgp.htm (29-maj-1998).

Sølberg, H. og H. Juhl (1994). Månedens edb-begreb: Kryptering. *Revision og regnskabsvæsen* (9), 64–65.

Vanglo, R. (1998). Ssl og sikkerheden: Diskretion en æressag. *PC World* (11), 70–72, 74–75.

Wivel, T., J. V. Hansen og M. S. Buhl (1997). Visioner om fremtidens revisionsydelse. *Revision og regnskabsvæsen* (4), 9–25.