Digital signatur. En eksemplarisk analyse af en teknologis indre mekanismer og processer.

Niels Jørgensen (nielsj@ruc.dk)
d. 17. december, 2018

Indhold

1 Indledning

Denne artikel er et case-studium af digital signatur. Formålet er at redegøre for begrebet "en teknologis indre mekanismer og processer". Meget kort sagt henviser begrebet til hvordan en given teknologi virker. Artiklen søger at være eksemplarisk i den forstand som kendes fra Martin Wagenschein ([27]) og andre med tilknytning til den tyske reformpædagogiske tradition. Her betyder eksemplarisk at en case kan afspejle det generelle. Artiklen har således både til formål at analysere casen om digital signatur og at belyse det generelle begreb om indre mekanismer og processer.

Begrebet "indre mekanismer og processer" er det første af seks trin i TRIN-modellen, som er vist i tabel 1.

1. Teknologiers indre mekanismer og processer.
2. Teknologiers artefakter.
3. Teknologiers utilsigtede effekter.
4. Teknologiske systemer.
5. Modeller af teknologier.
6. Teknologier som innovation.

Tabel 1: De seks trin i TRIN-modellen til teknologibeskrivelse.

Formålet med TRIN-modellen er at inspirere analyser og beskrivelser af teknologier, med hovedvægt på teknisk-videnskabelige aspekter af teknologierne. Modellen foreslår at man søger at besvare seks spørgsmål, herunder "Hvad er teknologiens indre mekanismer og processer?"

Dette indledningsafsnit giver først en motivation for TRIN-modellen, som især er baseret på en sammenligning med to andre modeller af teknologi, og derefter en oversigt over de seks trin i modellen.

Motivation for TRIN-modellen

Vi underviser i TRIN-modellen på den humanistisk-teknologiske bacheloruddannelse (humtek) på RUC fordi det er vores håb, at de studerende kan bruge

modellen når de analyserer en teknologi. Det gør de studerende blandt andet i projektarbejdet på uddannelsens 2. semester, hvor projektet er knyttet til uddannelsens teknisk-videnskabelige kernefaglighed. Akronymet TRIN står for **T**eknologi og **R**adikalt og **I**nkrementelt design i **N**etværk.

Baggrunden for at vi har foreslået en ny model er, at vi ikke har kunnet finde en eksisterende model, som vi skønnede levede op til formålet.

En meget anerkendt teknologi-definition er den, som Carl Mitcham foreslog i bogen *Thinking ThrougDrivkræfter og barrierer for udbredelse af teknologienh Technology* [15] (s. 154-160). Mitcham definerer teknologi som bestående af fire elementer, som vist i tabel 2.

teknologi = objekt + viden + aktivitet + vilje

Tabel 2: Mitchams definition af teknologi.

De fire elementer i Mitchams definition kan eksemplificeres således med flyteknologien: Objekter (Mitcham bruger det engelske begreb objects) er eksempelvis flyvemaskiner. Der er tale om menneskeskabte objekter, og så vidt jeg kan se, kunne Mitcham have brugt begrebet artefakter i stedet for objekter. Viden (knowledge) kan være videnskabelig teori om aerodynamik, som ligger til grund for konstruktionen af flyvingerne, men det kan også være pilotens færdighed i at styre flyet, og således omfatte kunnen som i nogen grad er ubevidst, til forskel fra bevidst, videnskabelig viden. Aktivitet (activity) kan eksempelvis være arbejde med at designe, bygge, vedligeholde, styre eller bare bruge flyet som passager. Vilje (volition) kan være passagerens ønske om hurtig transport og pilotens fascination af at flyve, og punktet hænger sammen med at teknologi har et formål. Det engelske udtryk volition kan i nogle sammenhænge også oversættes til hensigt eller intension, som vi også kunne have brugt i tabel 2.

Mitchams definition fokuserer for det første på objekter. Dette fremgår også flere andre steder i hans bog, hvor han eksempelvis giver en mere kortfattet definition af teknologi som "*the making and using of artifacts*"([15], s. 1). Og for det andet fokuserer definitionen på tre aspekter af menneskers relation til objekterne, nemlig menneskelig viden, aktivitet og vilje - om og i

relation til objekterne. På den måde har definitionen et enkelt udgangspunkt og en vis indre konsistens.

Definitionen virker overbevisende og er som sagt meget anerkendt. Den anvendes blandt andet i De Vries' bog *Teaching about Technology* [25]. De Vries skriver s. 132 om Mitchams bog som inspirationskilde.

Imidlertid er Mitchams definition forholdsvis generel, og indeholder ingen nærmere spørgsmål til teknologien, hverken til dens tekniske eller andre egenskaber. Mitcham har ikke suppleret definitionen med underspørgsmål eller lignende. Derfor synes vi ikke den understøtter en teknisk analyse, eller overhovedet en analyse af en teknologi. I Mitchams bog bruger han faktisk heller ikke definitionen som inpiration til at udarbejde en konkret teknologianalyse.

Derimod bruger bruger Mitcham definitionen som disposition for bogen *Thinking Through Technology*. Således er bogen disponeret med et kapitel om teknologi-teoretikere, der især har skrevet om teknologi som objekter, et kapitel om teorier om teknologi som viden, etc. Både Mitchams bog fra 1994 og De Vries' fra 2016 er oversigter over teknologifilosofi og teknologiteori. Ingen af bøgerne indeholder konkrete analyser af bestemte teknologier. Derfor er det måske naturligt, at teknologi-definitionen er abstrakt. Formålet med Mitchams definition er at inddele de foreliggende teorier om teknologi i nogle grupper eller kategorier, snarere end at analysere en bestemt teknologi.

En mere konkret og analyse-orienteret teknologi-definition af foreslået af Müller og medforfattere i [16]. Definitionen indeholder også fire elementer og er vist i tabel 3. I det følgende kalder vi den for nemheds skyld Müllers definition.

teknologi = teknik + viden + organisation + produkt

Tabel 3: Müllers definition af teknologi.

Müllers definition har fælles træk med Mitchams definition. For det første går elementet viden igen i begge definitioner. For det andet er Müllers element, organisation, beslægtet med Mitchams element, vilje. Dette fremgår af, at Müller forklarer organisations-elementet bl.a. med at "*Den tekniske viden skal mobiliseres og organiseres. Maskinerne skal stilles op på en særlig*

måde [..]". Denne argumentation henviser til bevidst, målstyret menneskelig indgriben, og er på den måde beslægtet med Mitchams begreb om vilje.

Det fremtræder umiddelbart som en forskel mellem Mitcham og Müllers definitioner, at elementet aktivitet ikke indgår i Müllers definition. Men faktisk indgår et aktivitetsbegeb flere steder i Müllers definition, nemlig i de uddybninger, forfatterne giver af de fire elementer. Hvert element er således uddybet med en definition. På den måde er Müllers teknologi-definition mere konkret end det fremgår af tabel 3. Müller fremhæver bl.a. begrebet arbejdsproces i definitionen af teknik-elementet som "*sammenføjningen af arbejdsmidler, arbejdsgenstande og arbejdskraft i arbejdsprocessen*". Ligeledes indgår arbejdsproces i definitionen af viden-elementet som "*sammenføjningen af kunnen, videnskabelig indsigt, og intuition i arbejdsprocessen*"(s. 16-18). I definitionerne af elementerne organisation og produkt indgår også aktivitetsrelaterede begreber som arbejde, arbejdsdeling og produktionsproces (s. 21-24).

Müllers definition søger med de mere konkrete definitioner af de fire elementer at lægge op til mere konkrete teknologi-analyser, og den har et fokus på tekniske aspekter. Dette svarer til formålet med TRIN-modellen. Müllers definition har imidlertid overvejende fokus på arbejds- og produktionsprocesser. Eksempelvis med vindmølle-teknologien vil det sige et fokus på produktionen af bl.a. de store vindmøllevinger. I forhold hertil vil vi gerne med TRIN-modellen fokusere både på teknologiers produktion/design *og* deres brug. Med trin 3 om utilsigtede virkninger sigter vi eksempelvis i høj grad på uhensigtmæssige virkninger i relation til anvendelsen af teknologien, fx at store vindmøller kan støje og skæmme udsigten. Ligeledes er nogle af de store udfordringer med teknologien digital signatur knyttet til brugen af den, snarere end til produktionen eller udviklingen af den. Det gælder eksempelvis brugervenligheden (som kan være dårlig) og forskellige risici for brugeren (herunder risikoen for tyveri af brugerens private nøgle til digital signatur). Mange teknologier har utilsigtede virkninger i form af miljøpåvirkninger, og her er det netop vigtigt at have øje for både udviklings-aspektet (hvor der kan være miljøpåvirkninger af de som medvirker til produktionen) og anvendelses-aspektet (hvor der kan være påvirkninger af store naturområder m.m.).

Sammenfattende kan man sige, at TRIN-modellen på den ene side er mere konkret end Mitchams model, idet TRIN-modellen eksempelvis foreslår at man undersøger teknologiens indre mekanismer og processer, og at man ser på dens utilsigtede virkninger. TRIN-modellen er på den anden side min-

dre konkret end Müllers definition, idet TRIN-modellen særligt er mindre fokuseret på arbejds- og produktionsprocessen end Müllers definition.

Oversigt over de seks trin i TRIN-modellen

Nu kommer en oversigt over modellens seks trin. Gennemgangen af hvert trin indledes med en definition. Eksemplerne i oversigten er hovedsageligt hentet fra artiklens case, digital signatur.

Hvis man analyserer en teknologi med udgangspunkt i et eller flere af trinnene i TRIN-modellen, er det anbefalelsesværdigt at gå tilbage til litteraturkilderne til trinnene. Formålet med TRIN-modellen er ikke at give en ny definition af teknologiske artefakter, modeller, m.v., men snarere at samle bud fra eksisterende litteratur i en model med seks centrale trin.

Trin 1: Teknologiers indre mekanismer og processer.

De centrale mekanismer og processer i en teknologi, som bidrager til at opfylde teknologiens formål. For eksempel i en vindmølle, hvis formål er at transformere vindens bevægelsesenergi til elektricitet, er de centrale mekanismer at vingerne drejes rundt af vinden, og at vingerne driver en generator, som skaber elektricitet.

Trin 1 anvendes i afsnit 2 i en analyse af digital signatur. Hovedformålet med en digital signatur er at vise autenciteten af underskriveren og originaliteten af det dokument, underskriveren har signeret. Det svarer til formålet med en traditionel, håndskrevet signatur på papir. De centrale indre mekanismer for digital signatur er asymmetrisk kryptering og kryptografisk hashing. Begge bliver brugt både når signaturen skabes af underskriveren og når den bekræftes af en modtager. Autenciteten af underskriveren understøttes især af den asymmetriske kryptering, hvor man underskriver med en privat nøgle, som underskriveren er den eneste med kendskab til. Asymmetrisk kryptering og kryptografish hashing er altså en slags støtte-teknologier i digital signatur. Afsnit fokuserer på støtte-teknologiernes formål og rolle i forhold til digital signatur, og uden at gå ind på hvordan asymmetrisk kryptering og krypto-

grafisk hashing selv fungerer. (Det sidste ville svare til også at redegøre for de indre mekanismer og processer af støtte-teknologierne).

Trin 1 analyseres mere teoretisk i afsnit 3 med udgangspunkt i Walter Vincentis begreb om en teknologis operationelle princip. Dette begreb er inspirationskilden til TRIN-modellens begreb om indre mekanismer og processer. Afsnittet skitserer også nogle forskelle på TRIN-modellen og Vincentis brug af begrebet. Det drejer sig bl.a. om, at TRIN-modellen lægger op til, at det er en vurderingssag, hvilke mekanismer og processer, der er de centrale, mens der er en tendens til at Vincenci opfatter det operationelle princip som noget givet eller fastlagt ved en teknologi. Afsnittet gennemgår eksempler på operationelle principper (indre mekanismer og processer) for bl.a. flyvemaskiner og kraftvarmeværker. Til sidst giver afsnittet en liste af tommelfingerregler for brugen af begrebet indre mekanismer og processer.

TRIN-modellens trin 2 til 6 anvendes i en samlet teknisk analyse af digital signatur i afsnit 4:

Trin 2: Teknologiers artefakter.

Artefakter er menneskeskabte genstande og adskiller sig som sådan fra genstande frembragt gennem processer i naturen. Et teknologisk artefakt er et artefakt, som har en teknologisk funktion. Teknologi er omformning af natur (stof og energi) under anvendelse af naturlige og sociale ressourcer samt information, viden og praktisk erfaring med henblik på at opfylde menneskelige behov.

Trin 2 handler altså om menneskeskabte objekter med en teknologisk funktion. Dette trin lægger op til en konkret gennemgang af de artefakter, der hører med til en teknologi. Digital signatur omfatter offentlige og private nøgler og programmer til at signere, generere nøgler m.m. Digital signatur indeholder også eksempler på artefakter, som har samme funktion, men forskellig form. Det gælder de medier, brugeren kan anvende til at opbevare den private nøgle. Den private kan opbevares i en fil på brugerens PC, hvilken man kan betegne som en software-løsning. Problemet med denne løsning er, at nøglen kan stjæles hvis PCen er tilkoblet internettet. Alternativt kan den private nøgle opbevares på et separat usb-stik, hvor det også kan beskyttes

med en ekstra kode. Denne hardware-baserede løsning giver en ekstra sikkerhed, men løsningen er dyrere.

Trin 3: Teknologiers utilsigtede effekter.

De utilsigtede effekter er effekter, som vurderes at være negative. For eksempel at en vindmølle støjer og ødelægger udsigten. Man kan skelne mellem utilsigtede effekter, som har karakter af risici, nogle som skyldes designfejl og endelig nogle som skyldes økonomiske hensyn.

Mens trin 1 handler om de indre mekanismer, som bidrager til teknologiens formål, altså dens tilsigtede effekter, så fokuserer trin 3 på de utilsigtede effekter. Man kan skelne mellem om en utilsigtet effekt er en risiko eller en normal effekt af en teknologi. Underafsnittet drøfter især den utilsigtede virkning af digital signatur, at at brugerens private nøgle kan blive stjålet fra brugerens computer. Denne utilsigtede effekt er selvfølgelig en risiko. Utilsigtede effekter kan skyldes designfejl eller økonomomiske hensyn.

Trin 4: Teknologiske systemer.

Teknologiske systemer er sammenhængende systemer af teknologiske artefakter, som samlet besidder en bestemt funktionalitet, der muliggør omformning af natur med henblik på opfyldelse af menneskelige behov.

Mens trin 2 om artefakter er et "mikro-punkt", som fokuserer på teknologiens elementer og detaljer, så er trin 4 et "makro-punkt", som fokuserer på de store sammenhænge. Digital signatur som samlet, teknologisk system omfatter også brugerne, udviklerne og fx de organisationer, der udarbejder standarder for digital signatur. Digital signatur er også knyttet til andre teknologiske systemer, og hvilke af disse, man særligt vil fremhæve, afhænger af synsvinklen på digital signatur. Hvis man er interesseret i hvorfor behovet for

digital signatur kommer, er en af faktorerne internettet, hvor der handles og indgås aftaler digitalt. En anden teknologisammenhæng, som er relevant for digital signatur, er det såkaldte PKI, som står for Public Key Infrastructure (offentlig nøle-infrastruktur). PKI er en vision om en teknologisk løsning på udfordringen med at fastslå, om en offentlig nøgle taktisk hører til en bestemt person. Det har desværre vist sig, at visionen med PKI har været vanskelig at realisere.

Trin 5: Modeller af teknologier.

Modeller af teknologier kan være numeriske (abstrakte), visuelle eller fysiske. De er repræsentationer, hvor særlige udvalgte egenskaber ved en teknologi søges gengivet og/eller undersøgt. En model kan samtidig være et værktøj til at skabe eller udvikle konkrete artefakter.

Inddelingen af modeller i tre typer af baseret på [17]). I delafsnittet om brugen af trin 5 til analyse af digital signatur beskrives en numerisk model. Modellen handler om hvor store krypteringsnøgler, det er tilrådeligt at vælge. Krypteringsnøgler skal over tid vælges større og større, fordi det over tid bliver muligt at knække større og større nøgler, med metoder til såkaldt primtalsfaktorering. Modellen er baseret på data over hvor store nøgler, det er lykkedes at primtalsfaktorere i tidligere år. Modellen siger at nøgler skal vælges 32 bit større for hver år. I dag anbefales krypteringsnøgler på mindst to tusind bits, hvilket formentlig også er sikkert i en længere periode, så man er sikret mod at skulle vælge en ny nøgle hvert eneste år.

Visuelle modeller kan have til formål at forklare et design eller en teknologi på en overskuelig måde. Eksempelvis kan man sige, at figur 2 i denne artikel er en enkel, visuel model af digital signatur, som fremhæver at der bruges private og offentlige nøgler. Fysiske modeller anvendes bl.a. i bilindustrien, hvor man bygger fuld-skala modeller af biler i materialer som træ og ler, for at få et realistisk indtryk af hvordan bilens ydre design fremtræder.

Trin 6 om innovation er på den ene side en uddybning af teknologiens formål, som indgår i trin 1. Teknologiens formål må jo typisk være at tilvejebringe en fordel, og realiseringen af denne fordel vil være en af drivkræfterne

Trin 6: Teknologier som innovation.

Innovation er implementering af nye eller væsentligt forbedrede produkter, produktionsprocesser eller organisationsformer. Innovationsteorier handler ofte om hvilke forhold, der driver en ny teknologi frem, og om barriererne for at teknologien bliver udbredt.

for udbredelsen af teknologien. Der kan også være barrierer for udbredelsen, som kan være knyttet til utilsigtede effekter (trin 3) eller andre forhold. Det skal siges, at det som nogle betragter som en fordel ved teknologien, og som betyder at de gerne vil udbrede teknologien, kan for andre være en ulempe, som gør at de ønsker at bremse teknologien. Det som nogle ser som en utilsigtet effekt, synes andre måske er en fordel. Hvad angår digital signatur, har staten i Danmark aktivt fremmet teknologien, blandt andet på grund af et håb om besparelser i den offentlige administration. På den måde kan indførelsen af digital signatur ses som en del af effektiviseringen og DJØFfiseringen af den offentlige sektor, som i øjeblikket får meget kritik.

Drivkræfter og barrierer for udbredelsen af en teknologi studeres samlet inden for innovationsteorien, som er et felt inden for samfundsvidenskaberne, eller i bredere forstand humanvidenskaberne. Hvis man eksempelvis analyserer staten som drivkræft for udbredelsen af digital signatur, og lægger vægt på analyse af statens og finansministeriets økonomiske motiver, vil der overvejende være tale om humanvidenskab. Hvis man analyserer de konkrete udfordringer med at få PKI (infrastruktur for offentlige nøgler, som nævnt ovenfor) for til at fungere, vil der dog overvejende være tale om teknisk videnskab.

En af grundene til at vi har medtaget trin 6 om innovationsteori i TRIN-modellen er at vi gerne vil have et punkt, hvor man kan sige noget sammenfattende om teknologien. Og et sammenfattende spørgsmål er jo netop om teknologien faktisk er blevet udbredt? og hvilke drivkræfter eller barrierer der har forårsaget dette? Denne synsvinkel er en slags kontekst for flere af trinnene, fx trin 3 om utilsigtede virkninger. For når man støder på en væsentlig utilsigtet virkning, er det oplagt at stoppe op, og spørge: Hallo, betyder det her, at teknologien slet ikke bør tages i brug? eller at denne ulempe må fixes hvis teknologien skal udbredes? De spørgsmål, vi stiller i TRIN-modellen,

skal kunne stilles på en meningsfyldt måde til teknologier inden for forskellige teknologifelter, herunder digital teknologi, miljø- og energiteknologi og sundhedsteknologi. Her er innovationsteoriens spørgsmål om drivkræfter og udbredelse passende generelle.

Samlet set kan en analyse af drivkræfter og barrierer for digital signatur bidrage til at forklare, at vi i Danmark har fået NemID-systemet. NemID-systemet har på den ene side træk til fælles med andre systemer til digital signatur; men på den anden side er NemID et meget specielt eller usædvanligt system fordi det er en statsstyret digital signatur, hvor staten opbevarer brugerens private nøgle. Et "Big Brother"-system som kan virke skræmmende.

Thomas Budde Christensen, Erling Jelsøe og undertegnede har udviklet TRIN-modellen, og underviste første gang i modellen i efteråret 2017. Modellen har endnu ikke fundet en færdig form, og vi modtager gerne alle former for kritik og anden feedback.

2 Digital signaturs indre mekanismer og processer

Et eksempel på digital signatur er PGP, der står for Pretty Good Privacy og især bruges til signering af elektronisk post. Figur 1 nedenfor viser en email med en PGP-signatur.

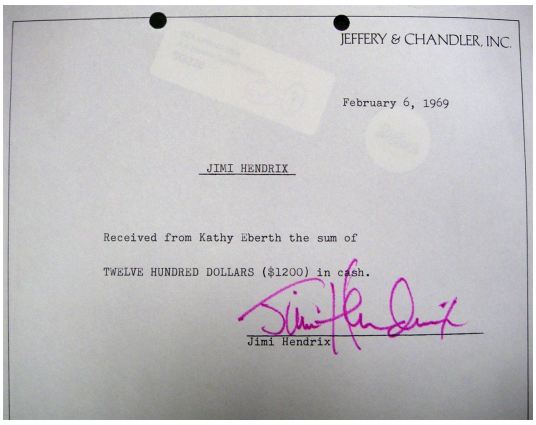
Et andet eksempel er Nem ID-systemet i Danmark. Selv om man kan lave digital signatur med Nem-ID, bruges systemet primært til at logge på netbanker og offentlige digitale tjenester. I parentes bemærket er det endvidere omdiskuteret, om NemID med rette kan betegnes som digital signatur. Digital signatur bruger en privat nøgle, som kun brugeren kender. Men i NemID opbevares nøglen på en central, landsdækkende server, snarere end af brugeren selv. Dette omdiskuterede aspekt ved NemID drøftes nærmere i afsnit 4. Digital signatur anvendes også inden for finanssektoren og er en grundpille i de nye kryptovalutaer, fx i Bitcoin [18].

Indre mekanismer og processer henviser som nævnt til de principper ved digital signatur, som bidrager til at teknologien opfylder sit formål. Derfor er det til at starte med en god ide at få klarhed over formålet.

Formålet med digital signatur

Hovedformålene med en digital signatur er det samme som med en fysik underskrift, nemlig at vise originaliten af dokumentet og autenciteten af underskriveren. Derfor handler dette underafsnit både om digital og fysisk signatur. Digital signatur er altså en digitalisering af en eksisterende fremgangsmåde. Vi gør noget med digital teknologi, som vi før i tiden gjorde uden teknologi, eller rettere, med meget primitiv teknologi (papir og pen).

Originaliteten af dokumentet
Det ene hovedformål med en signatur, at vise originaliten at dokumentet, betyder at bekræfte at dokumentet ikke er ændret. Figur 1 viser en fysisk og en digital signatur. I det fysiske brev til venstre i figuren om en betaling til Jimi Hendrix kunne en ændring eksempelvis være at skrive et større beløb, fx 2000$, efter at Hendrix havde skrevet under. Når det drejer sig om et fysisk dokument, vil ændringer ofte være tydelige, eksempelvis overstregninger på dokumentet, eller om nogle tegn er skrevet med en anden type maksinskrift end de øvrige tegn. Kvitteringen i eksemplet er udformet så beløbet



JEFFERY & CHANDLER, INC.

February 6, 1969

JIMI HENDRIX

Received from Kathy Eberth the sum of

TWELVE HUNDRED DOLLARS ($1200) in cash.

Jimi Hendrix

——BEGIN PGP SIGNED MESSAGE——
Hash: SHA512

FreeBSD-SA-17:07.wpa
Security Advisory The FreeBSD Project

I. Background
Wi-Fi Protected Access II (WPA2) is a security protocol developed by the Wi-Fi Alliance to secure wireless computer networks.
....
The latest revision of this advisory is available at ¡URL:https://security.FreeBSD.org/advisories/FreeBSD-SA-17:07.wpa.asc¿
——BEGIN PGP SIGNATURE——

iQKTBAEBCgB9FiEEHPf/b631yp+G4yy7Wfs1l3Pa
....
ZhMb/V4WmWV+4WnLKPwCQZ9fimKA==aNWn

——END PGP SIGNATURE——
————————————————————————-
freebsd-announce@freebsd.org mailing list
https://lists.freebsd.org/mailman/listinfo/freebsd-announce
To unsubscribe, send any mail to "freebsd-announce-unsubscribe@freebsd.org"

Figur 1: En fysisk og en digital signatur. Den fysiske signatur til venstre er skrevet af Jimi Hendrix. Den digitale signatur til højre er udført af sikkerhedsteamet bag operativsystemet FreeBSD. Eller rettere: signaturerne er angiveligt *skrevet af Jimi Hendrix og FreeBSDs sikkerhedsteam, og det er op til modtagerne at tjekke om det faktisk er tilfældet. I mailen har jeg fremhævet signaturen med rødt farve, og mailen er forkortet på de to steder hvor der er indsat "....".*

er skrevet både med bogstaver og tal, og dermed er ekstra svært at ændre uden det bliver opdaget. Formålet med at ændre beløbet kunne være (det er selvfølgelig et tænkt eksempel) at Kathy Eberth ville stikke forskellen på 800$ i egen lomme, uden pengene manglede i regnskabet, hvor Kathy Eberth kunne vise en kvittering på det større beløb.

Det digitale dokument til højre i figuren er fra en mail fra sikkerhedsteamet bag operativsystemet FreeBSD. Mailen handler om en fejl i WPA2, der er en sikkerhedsprotokol for mobile netværk, og forklarer hvordan fejlen rettes hvis man bruger WPA2 i forbindelse med Freebsd. For FreeBSDs sikkerhedsteam, er det afgørende at brevet ikke ændres, fx af hackere eller efterretningstjenester, for så vil der kunne være brugere, der får forkerte instruktioner i hvordan fejlen rettes. I et digitalt dokument er det svært at se om der er lavet ændringer, hvilket har øget behovet for metoder til at bekræfte at et dokument er uændret.

Autenciteten af underskriveren
Det andet hovedformål med en signatur, at vise autenciteten af underskriveren, betyder at bekræfte underskriverens identitet. Med denne begrebsanvendelse betyder identitet altså en slags påstand om at være en bestemt person, mens autentificering er en bekræftelse af identiteten. I det fysiske brev i figur 1 er identiteten udtrykt med det maskinskrevne navn Jimi Hendrix, og autentificeringen muliggøres af den håndskrevne underskrift. Hvis det kommer til uenighed om hvorvidt Jimi Hendrix faktisk har underskrevet dokumentet, så vil man kunne sammenligne med andre fysiske underskrifter foretaget af Jimi Hendrix.

Den digitale signatur til højre i figur 1 er indrammet af "BEGIN PGP SIGNATURE"og "END PGP SIGNATURE", og yderligere markeret med nogle tankestreger. Formålet med indramningen er at det program, der skal bekræfte at signaturen er korrekt, har brug for at vide, hvor signaturen står, altså at få signaturen adskilt fra den øvrige tekst i mailen.

Selve signaturen består af en sekvens af bogtaver "iQKT..". Figuren viser blot et udsnit af den originale email, hvor bogstavsekvensen består af ca. 900 tegn, altså en meget lang signatur. Bogstaverne er blot en måde at skrive signaturen på; i virkeligheden er signaturen et meget stort tal, og hvis man skrev tallet med binære (0-1) eller decimale (0-9) cifre, ville det fylde endnu mere på tryk.

Underskriver knyttes sammen med dokumentet
Udover de to hovedformål er der også et tredje formål på spil: Ved at sætte sin signatur på dokumentet, udtrykker underskriveren, at han eller hun godkender eller står inde for dokumentets indhold. Det kan være som forfatter til en tekst, eller at man godkender en tekst, som andre har skrevet. Denne relation mellem dokument og underskriver kan være eksplicit eller implicit. I dokumentet med Jimi Hendrix' underskrift kunne relationen gøres mere eksplicit hvis brevet var skrevet i jeg-form, som for eksempel "Jeg har modtaget.."eller "Med min underskrift bekræfter jeg..". Underskriften vil som udgangspunkt være bindende også selv om denne sammenhæng ikke er gjort eksplicit, fordi underskriveren forventes at være klar over, at sådan bliver underskriften forstået.

Lovgivning og domstolsbehandling
En af grundene til at der er tradition for signerede aftaler inden for forskellige handelsområder, fx kontrakter om arbejde, ejendomshandler eller bilhander,

er muligheden for at trække en part for en domstol, hvis parten ikke lever op til aftalen. Det gælder fx den fysisk signerede aftale til venstre i figur 1, men ikke den digitalt signerede tekst til højre, som er en vejledning, snarere end en aftale.

Man kunne tro at det blev fastslået i den første lov om digital signatur, som blev vedtaget i 2000 [14], at digital signatur var lige så bindende som en fysisk signatur. Men dette er ikke indeholdt i loven.

Domstolene tager i stedet udgangspunkt i, at både almindelige skriftlige og digtale aftaler principielt er gældende, ja selv mundtlige aftaler betragtes som gældende. Hvis en mundtlig aftale skrives ned og signeres, har man nemmere ved at bevise aftalen, men det er altså ikke nødvendigt for at den principielt betragtes som gældende. Som alternativ til signering kan man bevise en aftale med en video, en lydoptagelse eller vidner. Og faktisk er heller ikke sådanne beviser altid nødvendige. Når man som forbruger køber et produkt i en forretning, er kvitteringen ofte et gyldigt bevis på købet, og dermed garanti for visse forbrugerrettigheder. Som forbruger vil man kunne gå til klagenævn og i sidste instans til en domstol, også selv om kvitteringen er uden underskrift.

Hvis en domstol skal vurdere om en fysisk underskrift er ægte, kan den lægge vægt på flere forhold end selve underskriftens lighed med andre underskrifter fra den (angiveligt) samme person. I Danmark blev Rasmus Trads, der var en højtstående medarbejder i pensionsselskabet PFA, i år 2000 idømt fem års fængsel for bedrageri. Omdrejningspunktet i sagen var at han havde forfalsket underskriften fra sin chef, Andre Luplin, der var administrerende direktør i selskabet. Da PFA-sagen kom frem, fik politiet undersøgt nogle af de falske underskrifter, hvilket tydede på at de var forfalskede. Den tekniske undersøgelse var dog ikke afgørende i sagen. Andre Luplin sagde selv, at han ikke havde skrevet under, og Rasmus Trads indrømmede falskneriet. Der var ialt 13 falske underskrifter på forskellige dokumenter. Dokumenterne gav typisk en økonomisk garanti fra PFA til projekter med byggeentreprenøren Jens Thorsen, der nogle år forinden var gået konkurs, og som med garantierne fik mulighed for banklån og anden hjælp til projekterne. At udstede sådanne garantier lå ikke umiddelbart inden for PFAs forretningsområde [3], så det var usandsynligt, at Andre Lupin ville have skrevet under. Det betyder formentlig, at selv om Rasmus Trads havde lavet en perfekt efterligning af Andre Luplins underskrift, ville det alligevel være blevet fastslået, at dokumenterne var forfalskede.

Nøglecentre

Lovgivningen indeholder således ikke en udtrykkelig ligestilling af digital med fysisk signatur. I stedet fastsætter den nogle krav til at digitale signaturer kan være betryggende, især ved at stille krav til nøglecentre (på engelsk Certificate Authorities). Et nøglecenter kan give en bruger adgang til at signere digitalt. Det kan ske ved at udlevere et program, som kan generere en offentlig og privat nøgle, og ved at skabe et såkaldt digitalt certifikat, som knytter borgerens identitet sammen med den offentlige nøgle. I loven hed det eksempelvis:

> "Nøglecentre skal fastsætte og anvende betryggende procedurer til at kontrollere identiteten og andre forhold vedrørende underskriveren forud for udstedelsen af certifikatet."(§6 i Lov om elektroniske signaturer [14]).

I skrivende stund (i 2018) er et nyt lovforslag på vej om digital signatur, og lige som den oprindelige lov fra 2000 handler forslaget især om nøglecentrene. I den nye lov er der fokus på borgernes klageadgang. Loven fastslår, at forvaltningsloven gælder for nøglecentre, også selv om et privat firma varetager opgaven. Forvaltningsloven giver borgerne adgang til at klage, fx hvis nøglecenteret ikke vil give dem adgang til at bruge digital signatur.

"Kollektive" signaturer

En principiel forskel mellem fysisk og digital signatur er at den digitale kan repræsentere en virksomhed eller på anden måde et kollektiv. Således er mailen fra FreeBSD ikke underskrevet af en bestemt, identificerbar person. Som nævnt i underteksten til figur 1 er mailen underskrevet af et medlem af FreeBSDs sikkerhedsteam. Alle i teamet har mulighed for at lave denne form for underskrift. Bekræftelsen af en fysisk signatur udnytter, at den enkeltes skrift er unik, så det findes ikke "kollektive" fysiske signaturer.

Og dog. Denne principielle forskel mellem fysisk og digital signatur er i hvert fald ikke helt skarp. I PFA-sagen kom det frem, at Andre Luplin i nogle tilfælde faktisk lod nogle medarbejdere skriver under for sig, altså forfalske underskriften [10]. Udlånet af underskriften galdt dog tilsyneladende kun i de årlige julekort og lignende.

En praksis, hvor en medarbejder skriver under i en andens navn, og endda i "rigtige" sager, snarere end alene på julekort, er faktisk ikke ukendt i dansk erhvervsliv. I A.P. Møller - Mærsk drev man i perioden 1965-2003

denne praksis meget vidt. Efter A.P. Møllers død i 1965 og fremefter i den nævnte periode underskrev lederne i firmaet sig med underskriften "A. P. Møller"[2]. Denne fremgangsmåde var kendt i erhvervslivet, og underskriften var forpligtende for firmaet. Den blev ikke betragtet som en forfalskning. Virksomheden var Danmarks største i denne periode.

Sammenfatning af formålet med digital signatur
Samlet set kan man altså sige, at hovedformålet med en digital signatur er det samme som med en fysisk underskrift, nemlig at vise autenciteten af underskriveren og originaliteten af dokumentet. En domstols behandling af en signeret aftale kan gøre selv den mest perfekte efterligning af en fysisk underskrift utilstrækkelig til at gennemføre et bedrageri; for ofte vil domstolen også kunne lægge vægt på andre forhold, fx vidneudsagn fra den person, hvis underskrift (måske) er blevet kopieret. Det er et meget interessant spørgsmål, i hvilken udstrækning det samme gælder for digitale signaturer; men jeg vil mene, at hvis man kan sandsynliggøre, at ens private nøgle er blevet stjålet fra computeren, så har man et godt argument for at ens digitale signatur kan være forfalsket.

Brugerens interaktion med digital signatur

Interaktionen mellem brugeren og software med digital signatur gennemgås i det følgende, blandt andet fordi interaktionen kan fungere som en første introduktion til teknikken i digital signatur, især til brugen af en privat og en offentlig nøgle.

Når man som bruger skaber en digital signatur, arbejder man med to inputs, en tekst og en privat nøgle, som vist i figur 2. Man vil ofte kende den præcise tekst, hvis der fx er tale om en aftale eller mail man skriver under. I andre tilfælde kender man kun hovedindholdet af eller meningen med teksten, men ikke dens udformning eller opsætning, hvis det fx er en bankoverførsel, man underskriver. Teksten i figur 2 repræsenterer netop en bankoverførsel fra Kathy Eberth til Jimi Hendrix. Vi kan forestille os at bankoverførslen er gået forud for at Hendrix satte sin fysiske signatur på dokumentet i figur 1.

Ligeledes vil man som bruger ofte være opmærksom på at man signerer med en privat nøgle, men i andre tilfælde er brugeren blot klar over at han eller hun bruger en eller anden form for nøgle eller password. Typisk vil valget af hvilken privat nøgle, man skal bruge, foregå automatisk, altså så brugeren ikke selv vælger nøgle.

Output er den signerede tekst, som består af den originale tekst og en signatur. Brugeren vil i nogle tilfælde selv kunne se den signerede tekst, eksempelvis i udboksen i Enigma, og i andre tilfælde ikke umiddelbart kunne se den, fx i forbindelse med en bankoverførsel.

I figur 2 er signaturen tallet $27ba8a9f015d25g2$. Det er en signatur jeg har frit opfundet (og jeg har jo ikke Kathy Eberths private nøgle). En realistisk signatur vil være et noget større tal, men figuren viser princippet: at signaturen er et tal. Tallet i figuren er vist i hexadecimal form, som jeg også bruger i nogle eksempler senere i dette afsnit. Der er seksten hexadecimale cifre:

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f$$

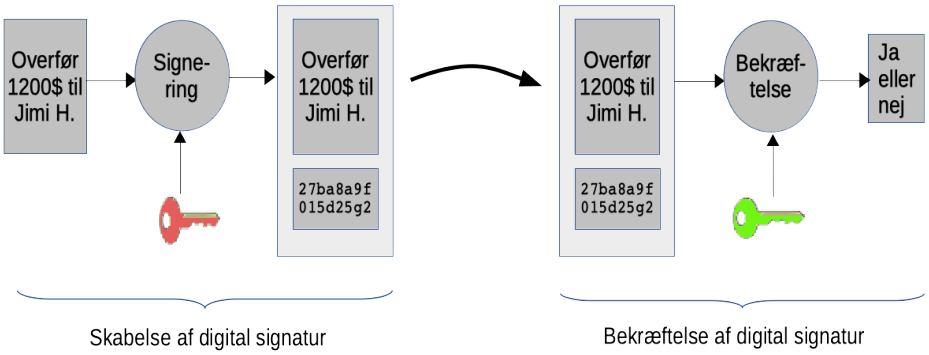
Der er altså seks flere cifre end i titalssystemet, hvor der som bekendt er ti. Den hexadecimale form kan være mere velegnet end titalsformen til at vise et tal til en menneskelig læser (fx i en tekst som denne). Tallet kan skrives lidt kortere, samtidig med at cifrene $0 \ldots 9$ og $a \ldots f$ er genkendelige. Det hexadecimale tal $9b$ kan omskrives til 155 i titalssystemet:

$$9b = 9 * 16 + 11 * 1 = 144 + 11 = 155$$

Så tallet 155 kan altså skrives lidt kortere (kun med to cifre), når man bruger den hexadecimale notation.

Inden brugeren signerer første gang, skal brugeren generere den private nøgle. Nøglegenereringen er ikke vist på figuren. Den private nøgle skabes af et program. Brugeren vil eventuelt blive instrueret i at gemme den private nøgle i en nøglefil, og ofte kunne se filnavnet og vælge hvilket katalog, filen placeres i. I princippet vil brugeren også kunne se den private nøgle, men det er jo blot et langt til, og alt for langt til, at brugeren kan huske det. Sammen med den private nøgle genereres også en offentlig nøgle, som brugeren ofte vil blive instrueret i at offentliggøre. Nøgleparret hører til en bestemt person - eller i nogle tilfælde til en gruppe eller organisation, hvilket som nævnt er tilfældet med nøgleparret for FreeBSDs sikkerhedsteam.

Modtageren af et underskrivet dokument, som han eller hun ønsker at bekræfte, skal bruge den offentlige nøgle. Igen vil modtageren ofte, men ikke altid, være klar over, at bekræftelsesprocessen indeholder de elementer, der er vist i figur 2, altså det underskrevne dokument og den offentlige nøgle. Modtageren skal sørge for at vælge den offentlige nøgle, som hører til den person, der har underskrevet dokumentet. Resultatet af bekræftelses-processen



Figur 2: Sådan fremtræder digital signatur for underskriveren og modtageren: Underskriveren signerer teksten med en privat nøgle, hvilket skaber det underskrevne dokument. Når modtageren bekræfter autencitet og originalitet af det modtagne, underskrevne dokument, sker det med en offentlig nøgle.

er enten en godkendelse eller afvisning. En afvisning betyder at der er noget galt med enten underskriver-autentiteten eller dokument-originaliteten, eller begge dele. Hvis det program, som udfører bekræftelses-processen, når frem til en afvisning, svarer det bare "Nej" og vil typisk sige uddybende, at der er et eller andet galt, men at det ikke ved hvad der er galt. I nogle tilfælde foregår bekræftelsen automatisk, fx i en bank, og mennesker bliver kun alarmeret, hvis der er noget galt.

Beskrivelse af de centrale mekanismer og processer i digital signatur

Mens Figur 2 som blev gennemgået ovenfor beskrev digital signatur i grove træk, så beskriver jeg i dette afsnit teknologien mere konkret, blandt andet med de to figurer 3 og 4. De to figurer viser henholdsvis tre delprocesser i skabelsen og fire delprocesser i bekræftelsen af en digital signatur.

Måske er det mest centrale i figur 3 og 4 at signaturen afhænger både af den private nøgle og af teksten. Der er altså ikke tale om, at skaberen af signaturen en gang for alle skaber en signatur, som han eller hun så hæfter sammen med teksten, og bagefter også kan hæfte sammen med andre tekster. Det duer ikke! For genbrug af den samme signatur til forskellige tekster ville jo gøre det nemt at forfalske signerede dokumenter. En angriber ville blot kunne kopiere signaturen, når den optræder sammen med en tekst, og sætte den

sammen med en anden tekst. I digitaliseringens tidsalder er det naturligvis afgørende, at falske signaturer ikke kan produceres bare med cut-and-paste. Derfor er signaturen forskellig alt efter hvilket dokument, der signeres af den samme bruger og med den samme private nøgle.

Notationen i diagrammerne er at bruge en kasse til at vise data og en cirkel til at vise en funktion. I diagrammerne har alle funktionerne et eller to input-data og et eller to output-data. Data er eksempelvis i figur 3 det dokument, der er input til hashing-funktionen. Dette input har i figuren navnet "Tekst", men det dokument, der signeres, må faktisk gerne være billeder eller andre former for data.

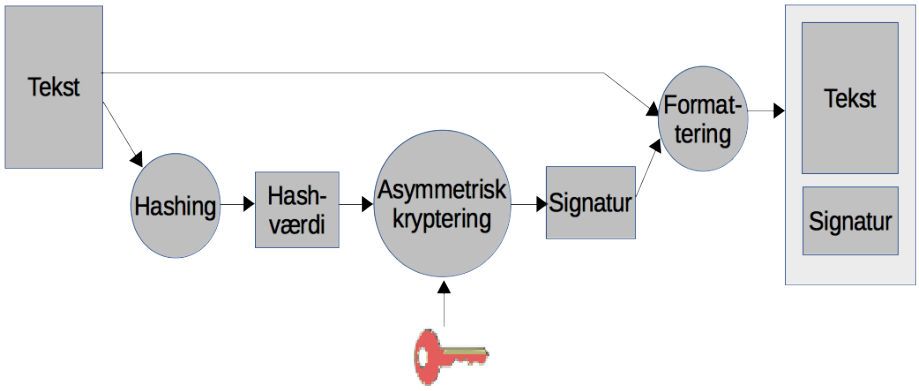
En funktion er i samme figur eksempelvis hashing-funktionen. Med en funktion mener jeg en fastlagt bearbejdning af inputdata til outputdata. Vendingen "fastlagt" betyder at funktionen giver det samme resultat, hver gang den får det samme input. Dette kan også udtrykkes med at funktionen er deterministisk; det modsatte ville være at funktionen indeholdt et randomiseret (tilfældigt) aspekt. En fastlagt bearbejdning af inputdata til outputdata betegnes i datalogien som en algoritme. Dette svarer også til funktionsbegrebet i matematikken. Et simpelt eksempel på en funktion i matematikken er $x \rightarrow x^2$. Her er x et tal, som er input-data til funktionen, og output-data er x^2, det vil sige x ganget med sig selv.

I både skabelsen og bekræftelsen er asymmetrisk kryptering og kryptografisk hashing de to centrale mekanismer. I skabelsen indgår der derudover også en formattering. I bekræftelsen indgår også en syntaksanalyse og en sammenligning. Så alt i alt fremhæver jeg tre processer i skabelsen og fire processer i bekræftelsen.

Den asymmetriske kryptering kunne være med RSA-metoden og en nøglelængde på 2048 bits, og hashfunktionen kunne være SHA 512, hvor hashværdien har en størrelse på 512 bits. Der findes flere forskellige algoritmer til asymmetrisk kryptering, som alle har de egenskaber, der lægges vægt på i dette afsnit. RSA er dog den mest kendte og udbredte metode betegnes. Betegnelsen RSA er et akronym, som henviser til Rivest, Shamir og Adelman, som beskrev metoden i 1978. RSA bruges i både PGP og NemID. På samme måde er SHA 512 kun en af flere mulige, kryptografiske hashfunktioner, men igen en udbredte og anerkendt metode.

De tre processer i skabelsen af digital signatur (se figur 3):
Figur 3 viser disse tre skridt i skabelsen af en digital signatur:

For det første udfører underskriveren en kryptografisk hashing af teksten,



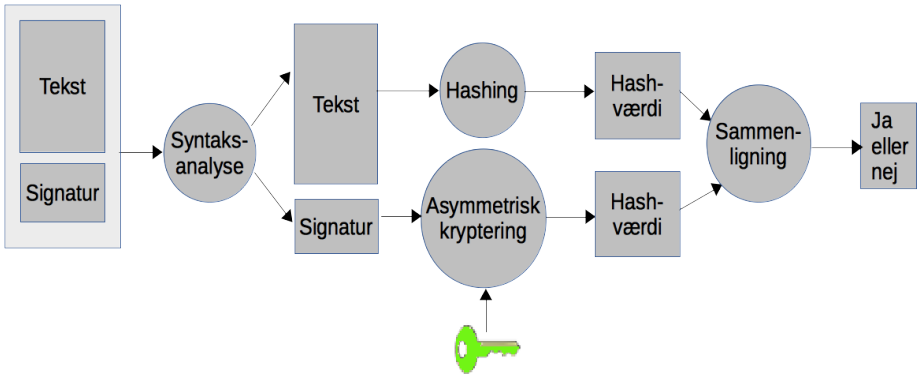
Figur 3: Skabelse af et digitalt signeret dokument. Den røde nøgle er den private nøgle.

hvis output er en hashværdi. Hashværdien har en fastsat lille størrelse, eksempelvis 512 bits, uanset hvor lang teksten er. En hashværdi af en tekst kan betragtes som et "fingeraftryk" af teksten, hvilket kan forstås sådan, at alle tekster har et forskelligt fingeraftryk, på samme måde som alle menneskers fingeraftryk er forskellige.

For det andet foretager underskriveren en asymmetrisk kryptering af hashværdien. Krypteringen tager som et input en rød nøgle. Rød nøgle symboliserer en privat nøgle i en asymmetrisk krypteringsalgoritme. Resultatet af krypteringen er signaturen. Signaturen er altså et krypteret fingeraftryk af teksten.

I den sidste og tredje proces i skabelsen af en digital signatur sammensættes dokumentet og signaturen til et samlet format. Et signeret dokument er således et dokument, hvor der er tilføjet et krypteret fingeraftryk, og som foreligger i et bestemt format. Et eksempel på et format ses i figur 1, hvor signaturen bl.a. er fremhævet med "BEGIN PGP SIGNATURE". Sammensætningen til et samlet format er en slags formalitet og er meget simpel. Formatteringen muliggør at det program, som laver bekræftelsen, kan identificere hvad der er signatur og hvad der er dokument.

Det er vigtigt at fremhæve at formålet med krypteringen (i den anden delproces) er at understøtte autentificeringen af den person der underskriver. Autentificeringen bygger på at underskriveren er den eneste der kender underskriverens private nøgle. Formålet med krypteringen er derimod ikke at hemmeligholde noget. Det der krypteres er kun hashværdien af teksten.



Figur 4: Bekræftelse af en digital signatur. Den grønne nøgle er den offentlige nøgle.

Teksten indgår i krypteret form i det signerede dokument. Og da det signerede dokument som udgangspunkt er offentligt, kan alle læse dokumentet. Alle kan også genskabe hashværdien, nemlig simpelthen ved selv at udføre hashfunktionen med teksten som input. Hashfunktionen og de andre delprocesser i signeringen er offentligt kendte. I mange andre sammenhænge anvendes kryptering for at sikre fortrolighed (hemmeligholdelse) af en tekst, men det er altså ikke tilfældet i digital signatur. Hvis man vil sende et signeret dokument og bevare det som fortroligt, er det muligt at bruge kryptering til dette formål, men det kræver ekstra tiltag, og omtales ikke nærmere i denne artikel.

De fire processer i bekræftelsen af signaturen (se figur 4):
For det første gennemføres en syntaksanalyse, hvorved signatur og dokument identificeres. I datalogien betegner syntaks-analyse i store træk det samme som i lingvistikken, altså eksempelvis at opdele en sætning i bestanddele som grundled og verbum. Syntaksanalysen bruger de markører, der blev indsat i formatteringsdelen af signatur-skabelsen (eksempelvis "BEGIN PGP SIGNATURE"). Syntaksanalysen er ukompliceret, så det er en mindre del af bekræftelsen, men alligevel en nødvendig del.

For det andet sker der en asymmetrisk kryptering af signaturen med den offentlige nøgle. Den asymmetriske kryptering er som funktion identisk med den asymmetriske kryptering i signeringen; forskellen ligger kun i inputtet: nu er input den offentlige nøgle (i signeringen var det den private nøgle) og

signaturen (i signeringen var det hashværdien). Effekten af disse ændringer er at krypteringen fungerer som en dekryptering, der genskaber hashværdien fra signeringen.

For det tredje sker der en kryptografisk hashing af dokumentet. Denne delproces er helt mage til processen i skabelsen af signaturen.

For det fjerde og sidste sammenlignes hashværdien og den dekrypterede signatur. Hvis de er ens, er autenticitet og originalitet bekræftet. Hvis de er forskellige, kan dette ikke bekræftes; men som nævnt i afsnittet om brugergrænsefladen, kan metoden kun fortælle at noget er galt, ikke hvad.

Analyse af de centrale mekanismer og processer i digital signatur

Begrebet analyse i overskriften sigter til, at artiklen nu skifter fokus og skitserer en begrundelse for, at de centrale mekanismer og processer i digital signatur faktisk virker. Indtil nu har artiklen beskrevet hvilke delprocesser der indgår i digital signatur, men ikke begrundet at delprocesserne giver det ønskede resultat. Det nye fokus gælder i resten af afsnit 2. Her kommer tre centrale kriterier for at en teknologi med digital signatur virker.

1. *Hurtig:* Digital signatur skal være rimelig hurtig. Især skal signeringen og bekræftelsen foregår hurtigt, fx maksimalt nogle tiendedele af et sekund til at signere en mail.

2. *Korrekt:* Bekræftelsen af digital signatur skal altid sige "ja" til de signerede dokumenter, hvor teksten er original og underskriveren er autentisk.

3. *Sikker:* Omvendt skal bekræftelsen sige "nej" til alle andre signerede dokumenter.

Bemærk at kriterie 2 og 3 hænger godt sammen med formålet med digital signatur, som blev drøftet tidligere i dette afsnit. Kriterierne er specifikke for digital signatur, og kan ikke overføres fx til vindmøller. Det er muligt at formulere kriterier for digital signatur på andre måder, fx mere matematisk præcist, eller med mere vægt på brugervenlighed af teknologien.

Hurtigheds-kriteriet

Kriterium 1 med hurtighed kan man undersøge ved at prøve at signere og bekræfte. Det går hurtigt. En vigtig grund til at signeringen foregår hurtigt er det grundlæggende design, som fremgår af figur 3, nemlig at man først hasher hele teksten, og derefter bruger asymmetrisk kryptering på hashværdien.

Dette design hænger sammen med, at kryptografish hashing er hurtig, mens asymmetrisk kryptering er langsom. Eksempelvis fylder filen med pdf-udgaven af denne artikel cirka 1 Megabyte (MB). På min computer tager det under en tiendedel af et sekund af skabe en hashværdi af filen med hashfunktionen SHA 512. Til sammenligning er asymmetrisk kryptering forholdsvis langsom. Som bruger ville man komme til at sidde og vente på at signeringen blev færdig, hvis man skulle asymmetrisk kryptere en fil på 1 MB. En hashværdi på 512 bits udgør et relativt lille data, og derfor er det ikke noget problem at foretage asymmetrisk kryptering af hashværdien. Det samlede dokument på ca. 1 MB er omkring 15.000 gange større end hashværdien på 512 bits.

Korrektheds-kriteriet

Kriterium 2 om korrekthed hænger sammen med egenskaber ved asymmetrisk kryptering. Afsnittet viser hvordan korrektheden følger af disse egenskaber, dog uden at forklare hvordan de enkelte metoder til asymmetrisk kryptering, fx RSA, opnår disse egenskaber. Afsnittet forklarer således ikke de indre egenskaber og processer ved fx RSA.

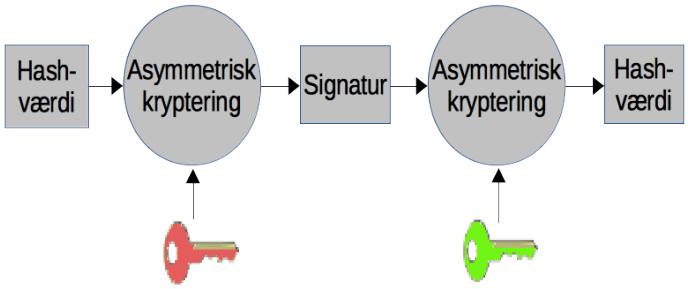
Så hvordan sikrer vi korrekthed, altså at et dokument, der er ægte og signeret med underskrives private nøgle, bliver godkendt af modtageren, når modtageren bruger underskriverens offentlige nøgle?

Et system til asymmetrisk kryptering opfylder følgende:

$$D_{PK}(E_{SK}(X)) \quad = \quad X \tag{1}$$

Her er X en hvilken som helst tekst. Ligningen siger, at hvis man først krypterer X og bagefter dekrypterer, så kommer man tilbage til X. Dette svarer naturligvis til hvad man ville forvente når man dekrypterer det krypterede. Egenskaben er vist i figur 5.

I ligningen 1 har jeg brugt forkortelser af forskellige engelske udtryk. Det vil sige at E_{SK} står for kryptering med den private nøgle SK. Forkortelsen E



Figur 5: Digital signatur som asymmetrisk kryptering (med den private nøgle, markeret med rød) plus dekryptering (med den offentlige nøgle, markeret med grøn). Figuren er en sammentrækning af elementer fra figur 3 og 4. Obs obs. Hash -¿ tekst. Populariser: Dekryptering ophæver kryptering. Og tænk over kryptering/dekryptering.

står for det engelske udtryk *encryption* og SK for *secret key*. Videre står D_{PK} for dekryptering med den offentlige nøgle PK. Her kommer D fra *decryption* og PK fra public key.

Egenskaben i ligning 1 gælder per definition for en asymmetrisk krypteringsmetode, fx RSA. Egenskaber forudsætter naturligvis at PK er den offentlige nøgle, som hører til den private nøgle SK. Krypteringsformen betegnes asymmetrisk fordi den bruger to forskellige nøgler, i stedet for kun at bruge en enkelt nøgle (hvilket betegnes symmetrisk kryptering).

Det følgende argument viser korrektheden: Det signerede dokument består af to dele: $\langle tekst, signatur \rangle$. Ifølge figur 3 frembringes *signatur* på følgende måde:

$$signatur = E_{SK}(H(tekst)) \tag{2}$$

Her H for en kryptografisk hashfunktion. Ifølge figur 4 skal modtageren sammenligne disse to værdier:

$$\begin{array}{ll} (a) & H(tekst) \\ (b) & D_{PK}(signatur) \end{array}$$

Hvis vi indsætter 2 i (b) får vi

$$\begin{array}{ll} (a) & H(tekst) \\ (b) & D_{PK}(signatur) \quad = D_{PK}(E_{SK}(H(tekst))) \end{array}$$

Hvis vi nu bruger ligning 1 til at omskrive (b) får vi

$$\begin{array}{ll} (a) & H(tekst) \\ (b) & D_{PK}(signatur) \quad = D_{PK}(E_{SK}(H(tekst))) = H(tekst) \end{array}$$

De to værdier (a) og (b) er altså ens, så signaturen godkendes. Dette viser at kriterium 2 om korrekthed er opfyldt. De centrale forudsætninger for ræsonnementet er, at den offentlige og private nøgle hører sammen, og at *tekst* er den samme tekst hos afsender og modtager.

Sikkerheds-kriteriet (asymmetrisk kryptering)

Kriterium 3 om sikkerhed handler om at afvise forfalskede signaturer. Når vi skal analysere digital signatur ud fra, om kriteriet er opfyldt, skal vi derfor tage spionbrillerne på og prøve at tænke konspiratorisk: hvordan kunne man prøve at forfalske en digital signatur? Vi skal altså forestille os noget i den digitale verden, som svarer til at lave forfalskede, håndskrevne underskrifter eller at bruge viskelæder eller andet til at rette i et dokument efter det er underskrevet.

Vi vil se på to forskellige forsøg på forfalskninger. Fremover kalder jeg dem for "angreb". Det første er *angreb på den private nøgle i den asymmetriske kryptering*, og det andet er *angreb på hashfunktionen ved at finde en kollision.* I drøftelsen af begge angreb forestiller vi os angrebsscenariet i figur 6.

Lad os først se på beskyttelsen mod *angreb på den private nøgle i den asymmetriske kryptering.* Det vil sige om en hacker kan finde frem til den private nøgle, hvis hackeren har kendskab til den tilsvarende offentlige nøgle og de andre oplysninger i angrebsscenariet. Det er faktisk et krav til asymmetrisk kryptering, at den skal beskytte mod sådanne angreb, men hvori består denne beskyttelse?

For det første kunne H. Acker prøve at gætte den private nøgle. Den private nøgle er jo et tal. H. Acker kunne prøve alle de mulige værdier, altså

Angrebs-scenarie

H. Acker vil have banken til at tro at følgende falske dokument kommer fra Kathy Eberth, så pengene bliver overført fra Eberths konto:

"Overfør 2000$ til H. Acker"

Den præcise beløbsstørrelse er underordnet, så teksten må gerne nævne et beløb som 2001$, 2002$ eller lignende, så længe beløbet er stort, uden at være mistænkeligt stort.

Udfordringen for H. Acker er altså at skabe en signatur på det falske dokument, så banken tror dokumentet er underskrevet med Kathy Eberths private nøgle.

Vilkårene er:

ss 1) H. Acker kender *ikke* Kathy Eberths private nøgle.

2) Men H. Acker *kender* følgende:

- Kathy Eberths offentlige nøgle.
- Den asymmetriske krypteringsmetode og den kryptografiske hashfunktion
- Dokumentet "Overfør 1200$ til Jimi H." fra figur 2 og dets hashværdi $ed2b6d5f41f43344$ og signatur $27ba8a9f015d25g2$.

Figur 6: Scenariet for de angreb, som drøftes i relation til kriterium 3 om sikkerhed. Hashværdi og signatur er vist med de første 16 hexadecimale cifre. I virkeligheden er de længere. (Hashværdien er den faktiske hashværdi af dokumentet, mens signaturen som nævnt er en, jeg har fundet på). Alle de oplysninger, H. Acker råder over, er principielt offentligt tilgængelige. Eksempelvis kan H. Acker beregne hashværdien ved at dekryptere signaturen (jf. figur 4).

$SK = 0, 1, 2, \ldots$. For hvert gæt, lad os kalde det SK', af den private nøgle kunne han beregne

$$E_{SK'}(H(\text{Overfør 1200\$ til Jimi H.})$$

og så sammenligne med signaturen $27ba8a9f015d25g2$. Hvis han gætter en privat nøgle, som giver den rigtige signatur, er hans gæt SK' lig med Kathy Eberths private nøgle SK. Så kan han signere sit forfalskede dokument. Signaturen ville overbevise banken, fordi signaturen var lavet med den rigtige private nøgle. Så H. Acker ville få overført et stort beløb til sin konto fra Kathy Eberths konto - uha!

Denne metode duer imidlertid ikke for H. Acker, for der er alt for mange mulige nøgler, som han skal prøve. Hvis nøglelængden eksempelvis er 2048 bits, er der astronomisk mange nøgler. Selv om H. Acker havde adgang til alle jordens computere i 100vis af år, ville han ikke kunne nå at afprøve bare en rimelig stor del af de mulige nøgler. Man kan kalde denne angrebsmetode for et "rå kraft-angreb"(*brute force*). Og der er altså ikke computere nok i verden til et "rå kraft-angreb". I praksis ville H. Acker bruge en form for rå kraft-angreb, hvor en stor del af tallene $0, 1, 2, ..$ på forhånd kunne udelukkes, hvilket gør metoden hurtigere, men alligevel er metoden ikke praktisk fremkommelig.

Alternativt kan H. Acker prøve at gætte den private nøgle på en mere intelligent måde. H. Acker kunne tro, at når han kender funktionen D_{PK}, må han kunne finde den omvendte funktion E_{SK}. Til sammenligning, hvis H. Acker kender funktionen x^2, kan han nemt se hvad den omvendte funktion er, nemlig $\sqrt{x}$. Man kan sige at funktionen x^2 er nem at invertere (omvende). Imidlertid er metoder til asymmetrisk kryptering netop kendetegnet ved, at de er meget vanskelige at invertere. Af denne grund betegnes de også som "envejs-funktioner"(*one-way functions*).

Det at asymmetrisk kryptering bruger envejs-funktioner kan illustreres med RSA. Det hænger sammen med at RSA er en slags matematisk metode, som bruger visse egenskaber ved primtal. Et primtal er fx 7, og er defineret ved at det kun kan divideres med tallet selv og med 1. Modsat er fx 6 ikke er primtal, for det kan divideres med 2 og 3. Den offentlige nøgle i RSA indeholder et tal, som er et produkt af to primtal. Hvis man kan finde disse to primtal, kan man nemt beregne den private nøgle. Eksempelvis er tallet 39 et produkt af de to primtal 3 og 13. At finde 3 og 13 ud fra 39 betegnes som at primtalsfaktorere 39. Der findes imidlertid ikke nogen god metode til

at primtalsfaktorere. En mulighed er at gætte primtallene: man kan gætte et primtal, og prøve at dividere det op i tallet, og hvis resultatet også er et primtal, har man fundet begge primtal, og så kan man nemt finde den private nøgle. Der er imidlertid alt for mange primtal. Derfor er gætte-metoden ikke praktisk brugbar, da den ville kræve for meget computerkraft og tid.

Der findes mere avancerede metoder til at primtalsfaktorere, end blot at gætte primtallene, men heller ikke disse er praktisk brugbare når produktet (det tal der skal primtalsfaktoreres) er stort, eksempelvis med en RSA-nøglestørrelse på 2048 bits.

En bit er enten 0 eller 1. Skrevet i titalssystemet, altså med cifre fra 0 til 9, svarer et tal med 2048 bits til et tal med ca. 600 cifre i titalssystemet. Det er et ekstremt stort tal. Man vælger altså et stort antal bits til nøglestørrelsen for at gøre det vanskeligt at finde den private nøgle. Man kan sige at at kriterium 3 om sikkerhed er opfyldt sålænge angriberen kun har computerkraft til rådighed som er realistisk.

Sikkerheds-kriteriet, fortsat (kryptografisk hashing)

Kryptografisk hashing understøtter den digitale signering ved at skabe et "fingeraftryk" (en hashværdi) af dokumentet. Herefter er det kun nødvendigt at foretage asymmetrisk kryptering af fingeraftrykket, ikke hele dokumentet. Dette er vigtigt af tidsmæssige grunde, da asymmetrisk kryptering tager lang tid, selv med moderne, kraftige computere. På den måde bidrager hashingen til kriterium 1 om hurtighed.

Kryptografisk hashing giver i princippet mulighed for et angreb, som dette afsnit forklarer: *angreb på hashfunktionen ved at finde en kollision.*

Angrebet går ud på, at H. Acker forsøger at finde et falsk dokument, som får banken til at overføre et større beløb til H. Acker, og hvor dokumentet har samme hashværdi som Kathy Eberths dokument. Herefter vil H. Acker tilføje Kathy Eberths signatur på den oprindelige tekst til bankoverførslen. Spørgsmålet er, om det er muligt for H. Acker at skabe et sådant falsk dokument med den samme hashværdi?

Tabel 4 viser nogle hashværdier, vi kan forestille os H. Acker har beregnet.

Tabellen viser, at der ikke er nogen af hashværdierne, der er ens. Det vil sige, at det ikke i første omgang er lykkedes for H. Acker at finde et forfalsket dokument, som kan overføre penge til H. Acker, og som har samme hashværdi som det ægte dokument.

Den originale tekst	*Hashværdi*
Overfør 1200$ til Jimi H.	`ed2b6d5f41f43344` ...

Forfalskede tekster	*Hashværdier*
Overfør 2000$ til H. Acker	`8268c3b6ed8ef489` ...
Overfør 2001$ til H. Acker	`a9cb6c924693805c` ...
Overfør 2002$ til H. Acker	`11cbe7fb6b7d03da` ...
...	...
Overfør 2006$ til H. Acker	`e1e183b2aaa9ac46` ...
Overfør 2006$ til Hr Acker	`9db843086c69efe3` ...

Tabel 4: Hashværdier af den originale og de forfalskede tekster. Hashværdierne er beregnet med den kryptografiske hashmetode SHA-512, og kun de første 16 hexadecimale cifre er vist. Rød farve fremhæver et match på det første ciffer. Der er (selvfølgelig) ingen af hashværdierne af de forfalskede tekster der matcher alle cifrene i hashværdien af den originale tekst.

Tabellen viser også, at H. Ackers angreb går ud på at lave små ændringer i teksten - som alle bevarer det grundlæggende indhold i teksten, nemlig at overføre penge til H. Acker.

Grunden til at det er svært eller umuligt for H. Acker at skrive et forfalsket dokument, som hasher til den samme hashværdi som det ægte dokument, er at det simpelthen er et krav til kryptografiske hashfunktioner, at de ikke må have *kollisioner*. Ved en kollision forstås at to forskellige tekster har samme hashværdi.

Der findes ikke nogen kendte kollisioner i hashfunktionen SHA 512. I teorien findes der faktisk kollisioner, men det er bare praktisk umuligt at finde dem. Grunden til at der i teorien findes kollisioner, er at der er mange flere mulige tekster end der er hashværdier, og derfor må nogle af teksterne have samme hashværdi. Igen er det vigtigt at tænke på "realistisk computerkraft". Hvis man hypotetisk set havde adgang til ubegrænsede mængder af computerkraft, ville man godt kunne finde to forskellige tekster med samme hashværdi; og det ville måske også være muligt at finde en variant af teksten, som overfører penge til H. Acker, som kolliderede med hashværdien for det ægte dokument. Med med en sikker hashfunktion, som fx SHA 512, er det ikke muligt med den computerkraft, som findes for øjeblikket.

Den næstsidste række i tabellen viser, at når H. Acker forsøger med teksten *Overfør 2006$ til H. Acker*, bliver det første ciffer i hashværdien til e,

altså det samme som i hashværdien af det ægte dokument. Vi kan forestille os, at det fik H. Acker til at tænke, at nu var han på rette vej! I næste skridt fastholdt han beløbet 2006$, for at fastholde e som starten på hashværdien, og prøvede så at ændre et andet sted i teksten, nemlig ved at skrive Hr foran $Hacker$. Men som tabellens sidste række viser, så giver dette en helt anderledes hashværdi, som ikke begynder med e. Dette hænger sammen med "lavineeffekten" ved kryptografiske hashfunktioner. Lavineeffekten betyder at små ændringer i teksten giver store ændringer i hashværdien (lige som et sneboldskast kan udløse en lavine). Så når H. Acker ændrede $H.$ til Hr, så "ødelagde" dette, at H. Acker havde fundet en tekst, som i det mindste hashede til $e \ldots$.

Sammenfattende peger analysen af digital signaturs indre mekanismer og processer for det første på, at teknologien er hurtig (kriterium 1), fordi designet sikrer, at man først hasher dokumentet, og derefter krypterer hashværdien. Asymmetrisk kryptering er langsom, så det er vigtigt at man kun skal kryptere et lille input (hashværdien). For det andet er teknologien korrekt (kriterium 2) på grund af den naturlige egenskab ved asymmetrisk kryptering, at dekryptering så at sige ophæver kryptering.

Men for det tredje har analysen af sikkerheden (kriterium 3) kun givet nogle argumenter, men ikke nogen garanti, for at forfalskede signaturer opdages.

Vi kunne naturligvis have mere tiltro til sikkerheden ved teknologien til digital signatur, hvis der fandtes et decideret bevis for, at det ikke var muligt at gennemføre de to angreb, jeg har diskuteret ovenfor, eller andre angreb. Det gør der ikke. Det ene angreb (på asymmetrisk kryptering) handler om at "invertere" krypteringen uden at kende den offentlige nøgle. Det andet angreb (på hashingen) handler om at finde kollisioner, altså to tekster, som hasher til den samme værdi, hvilket jo bryder ideen med hashing: at hashværdien er et unikt "fingeraftryk". Som nævnt er angrebene faktisk mulige i princippet. Der findes ikke engang noget kendt *bevis* for, at angrebene er umulige med realistisk computerkraft, kun *argumenter* - og nogle af disse er skitseret ovenfor. Der findes også andre angrebstyper, som ikke er nævnt her, og der gør sig det samme gældende med, at der findes argumenter for, at angrebene ikke er realistiske, men der findes ikke beviser for dette.

Med hensyn til sikkerheden findes der dog et slags empirisk eller praktisk argument: Der er ikke nogen, som i praksis har forfalsket en digital signatur, og som har offentliggjort det. Vel at mærke digital signatur med passende store nøglestørrelser m.v. (eksempelvis en RSA-nøglestørrelse på 2048 bits

og hashfunktionenen SHA med 512 bits). Hvis en sikkerhedsekspert kunne dokumentere, at nu havde eksperten forfalsket en digital signatur, ville vedkommende få megen hæder. Det er principielt muligt, at de hemmelige efterretningstjenester, fx den amerikanske NSA (National Security Agency) kender metoder til at angribe digital signatur. Men det er antagelsen blandt uafhængige sikkerhedseksperter, at det gør de ikke, for så skulle efterretningstjenesterne være afgørende foran de uafhængige eksperter.

3 Walter Vincentis analyse af indre mekanismer og processer

Begrebet "indre mekanismer og processer" er inspireret af Walter Vincentis begreb om en teknologis operationelle princip. Vincenti introducerer begrebet i "What Engineers Know and How They Know it" [24]. Bogen indeholder primært fem case-studier fra flyindustriens historie, bl.a. om design og brug af vingeprofiler, propeller og nitter. Men derudover indeholder bogen også nogle kapitler, hvor Vincenti reflekterer over casestudierne. I disse reflektioner indløser han det ambitiøse løfte fra bogens titel, og svarer altså på hvad ingeniører ved og hvordan de ved det. Begrebet operationelt princip er en central del af ingeniørers viden, ifølge Vincenti.

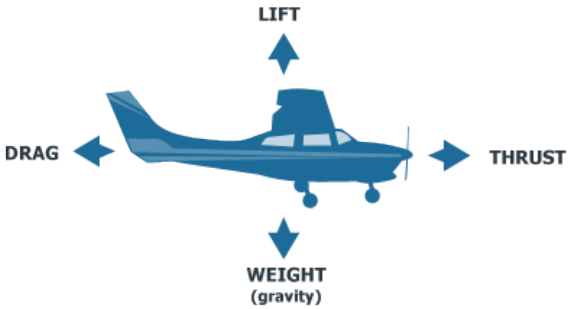
Afsnittet er organiseret således: Først gennemgår afsnit 3 Vincentis definition af begrebet operationelt princip. Dernæst omtaler afsnit 3 to andre centrale begreber hos Vincenti, som han knytter til det operationelle princip, nemlig normal konfiguration og normalt design. Afsnit 3 diskuterer andre teknologiteoretikere, giver to kritikpunkter af Vincentis begreb og begrunder hvorfor TRIN-modellen bruger betegnelsen indre mekanismer og processer, i stedet for operationelt princip. Afslutningsvis giver afsnit 3 nogle tommelfingerregler om indre mekanismer og processer.

Vincenti om det operationelle princip

Vincentis uformelle sammenfatning af begrebet det operationelle princip lyder således: "in brief, how the device works"([24], s. 208), altså hvordan teknologien virker. Jeg forstår dette sådan, at hvis man skal forklare hvordan en teknologi virker, fx hvordan en flyvemaskine kan flyve, så svarer det til at forklare det operationelle princip. I nogle tilfælde kan man få en god ide om det operationelle princip for en teknologi ved at læse populære fremstillinger af hvordan de virker. Eksempelvis giver websitet science.howstuffworks.com en forklaring på det operationelle princip i en vindmølle. Forklaringen kan kort sammenfattes således: vindmøllens vinger omdanner bevægelsesenergien i vinden til en roterende bevægelse, der driver en elgenerator [9].

Vincentis primære eksempel på et operationelt princip er for flymaskiner, som er emnet for hans bog. Han sammenfatter princippet for flyvemaskiner således (se illustrationen i figur 7):

> ".. to make a surface support a given weight by the application



Figur 7: Illustration af Vincentis operationelle princip for flyvemaskiner. Et fly er overordnet set i balance, forstået som at det kan holde sig på vingerne i en konstant højde og med konstant hastighed, hvis weight *(flyets samlede vægt) er lige så stor som* lift *(opdriften skabt af luftstrømmen forbi vingerne), og hvis* thrust *(den fremadrettede kraft som skabes af motoren) er lige så stor som* drag *(luftmodstanden af hele flyet). Det kritiske er balancen mellem weight og lift, og for at opnå balancen er det nødvendigt at flyet har en høj hastighed (høj thrust).*

of power to the resistance of air" (s. 208).

I citatet henviser *surface* til vingen, *a given weight* til vægten af hele flyet, og *application of power* til motoren. I citatet er princippet nok formuleret lige lovlig kortfattet. Det er underforstået at motorkraften driver flyet fremad, eksempelvis via en propel, hvilket skaber en opadrettet kraft på vingen, som opvejer flyets tyngdekraft. Citatet i Vincentis bog er faktisk fra 1809, altså knapt et hundrede år før de første flyvemaskiner. Citatet stammer fra Sir George Cayley, som Vincenti citerer fra s. 48 i [22]. Betydningen af indsigten i dette operationelle princip for flyvemaskiner var ifølge Vincenti, at det fik de første flyopfindere til at se bort fra tidligere tiders ideer om bevægelige vinger, inspireret af fugle, og i stedet koncentrere sig om fastmonterede vinger. Det operationelle princip kunne dog først realiseres i årene lige efter 1900 med en forbrændingsmotor. I det meste af 1800-tallet havde dampmaskiner og senere elmotorer været de eneste kendte motorer, og de var alt for tunge i forhold til ydeevnen til at konceptet kunne realiseres.

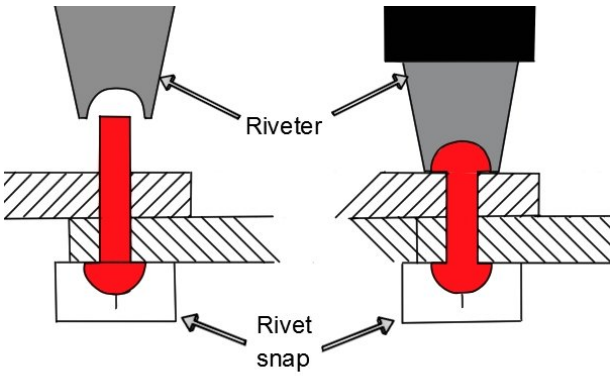
Ifølge Vincenti har alle teknologier et operationelt princip. Dette antager vi også i TRIN-modellen. Den forklaring af indre mekanismer og processer i digital signatur, som blev givet i afsnit 2 svarer i Vincentis begrebsapparat

til at definere det operationelle princip i digital signatur. Digital signaturs to hovedkomponenter er asymmetrisk kryptering og kryptografisk hashing, som igen har hver deres operationelle principper.

Man kan godt redegøre for en *teknologis* operationelle princip uden at redegøre for *komponenternes* operationelle principper. Eksempelvis redegjorde jeg i ovennævnte afsnit for det operationelle princip i digital signatur netop uden at redegøre for det operationelle princip i kryptografisk hashing. Om kryptografisk hashing beskrev afsnittet således kun hvilke egenskaber, hashingen skal leve op til, og hvordan disse egenskaber bruges i digital signatur, men ikke det operationelle princip for hashing, altså hvordan hashingen selv fungerer. Begrebet om en teknologis operationelle princip har således indbygget en mulighed for at man afgrænser sig fra et gå i yderligere detaljer.

I mange sammenhænge kan det være relevant at arbejde med det operationelle princip for en teknologis komponenter, eksempelvis en flyvinge. En flyvinge har ikke et selvstændigt praktisk formål, forstået som at den ikke i sig selv løser et problem for mennesker, men den har et formål som en del af en flyvemaskine. Formålet er at skabe opdrift til flyvemaskinen, jf. figur 7. En flyvinges operationelle princip drejer sig altså om hvorledes dette formål realiseres. Det sker kort sagt ved at vingen står lidt på skrå i forhold til flyveretningen og har en særlig profil, der medfører et overtryk på undersiden og (især) undertryk på oversiden når vinden passerer hurtigt forbi.

Man kan tale om operationelle principper for selv de mindste komponenter. Lad os igen se på flyvingen. En flyvinge, som jo er en komponent i flyvemaskinen, kan selv ses som sammensat af forskellige komponenter. Eksempelvis er bagsiden af vingen, med dens bevægelige flaps, en meget vigtig komponent. Og de bevægelige flaps består selv af komponenter. Og så fremdeles. Man kan fortsætte til de mindste komponenter såsom nitter, som Vincenti også studerede. En nitte har en meget lille størrelse og minder om et søm. Formålet med en nitte er at holde to stykker materialer sammen (fx to plader, der danner oversiden af en vinge eller flap). Materialerne skal holdes sammen selv om der er kræfter, der bevæger materialerne fra hinanden, og nitten skal endvidere tætne det hul i pladerne, nitten går igennem. En nittes operationelle princip skal formuleres, så det forklarer hvordan man opnår denne effekt med nitten. Et element i denne forklaring er at man slår på den ene side af nitten, som trykkes sammen over hullet i pladerne (se figur 8).



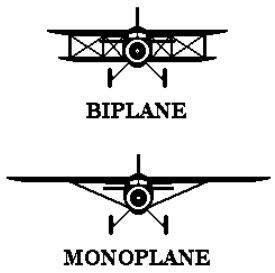
Figur 8: En nitte bearbejdes, så den kan holde to materialer sammen. Billedet til venstre viser den oprindelige nitte. Billedet til højre viser nitten efter bearbejdning, hvor et værktøj foroven ("rivetter") har deformeret den ene ende af nitten, mens et værktøj forneden ("rivet snap") har fastholdt den anden ende af nitten.

Vincenti om normal konfiguration og normalt design

Vincenti definerer to begreber, "normal configuration" og "normal design" (her stavet på engelsk) i tilknytning til begrebet operationelt princip.

Den normale konfiguration er "the general shape and arrangement that are commonly agreed to best embody the operational principle" (s. 209). For flymaskiner vil den normale konfiguration eksempelvis være at flyet er et monoplan (med en vinge), modsat et dobbeltdækkerfly (med to vinger over hinanden). De to vingekonfigurationer er vist i figur 9. De designvalg, som er omfattet af begrebet den normale konfiguration, er altså på den ene side vigtige, eksempelvis ved at de fastlægger antallet af centrale komponenter (fx antallet af vinger), og på den anden side er de ikke så vigtige, at de ændrer det operationelle princip. Dobbeltdækkeren er en mere stiv konstruktion, hvilket kort sagt skyldes at vingerne kan forbindes. Dette modvirker at vingerne knækker. Dobbeltdækkeren med bjælker eller wirer mellem vingerne har til gengæld større luftmodstand. Monoplanet med den mindre luftmodstand skal så sikre en rimelig stiv vingekonstruktionen på anden vis, hvilket giver en designudfordring, hvor man bl.a. skal afveje balancen mellem vingens styrke og dens vægt.

Med hensyn til digital signatur kan man spørge om den normale konfi-



Figur 9: Et moderne flys normale konfiguration er som monoplan (en enkelt vinge), mens ældre fly ofte var dobbeltdækkere.

guration omfatter at bruge RSA-algoritmen til asymmetrisk kryptering? På den ene side er RSA-algoritmen den mest udbredte til dette formål i digital signatur. Endvidere er de basale mekanismer i digital signatur uafhængige af om man benytter RSA eller en anden metode til asymmetrisk kryptering. Tilsammen taler dette for at brugen af RSA er en del af den normale konfiguration. På den anden side er der ikke almindelig enighed om, at RSA er mere velegnet end alle andre metoder, og nogle digitale signaturer bruger faktisk andre metoder. Da der ikke er almindelig enighed om at bruge RSA, hører RSA ikke med til den normale konfiguration, ifølge Vincentis definition af begrebet. I stedet kan man måske betegne valget af krypteringsmetode som en central designbeslutning i udviklingen af et system til digital signatur.

Begrebet normalt design kommer ind i billedet i situationer, hvor et teknologi har et fastlagt operationelt princip og en normal konfiguration. Det betegner den type designopgaver, der arbejdes med i denne situation: at forbedre teknologien inden for disse rammer. Dette betegnes i nogle sammenhænge også som inkrementel innovation, og skal forstås som udviklingen af en række små forbedringer til et eksistende designprincip. Det modsatte begreb, radikalt design, kommer ind i billedet når et nyt operationelt princip er under udvikling, eller i hvert fald når en ny konfiguration er det.

Vincenti understreger at ofte tager ingeniører en teknologis operationelle princip og normale konfiguration for givne, og de er ikke til diskussion i en praktisk designsammenhæng. I en artikel om udviklingen af passagerflyet Boeing 777 har jeg beskrevet nogle af de centrale udfordringer i det praktiske designarbejde med flyet [12]. Udfordringerne var blandt andre øget brug af letvægtsmaterialer, et designprincip om øget genbrug af de samme dele (eksempelvis opnået ved at flyets døre havde ens dimensioner) og et haleror

som kunne tåle en meget stærk belastning. Det operationelle princip er ikke ændret ved nogen af disse designbeslutninger, og heller ikke af de tusindvis af andre designbeslutninger i udviklingen af Boeing 777. I skrivende stund i 2018 overvejer Boeing-fabrikkerne at udvikle fabrikkens næste passagerfly. Det skal formentlig hedde Boeing 797, efter Boeing 787, som blev leveret til flyselskaberne første gang i 2009, altså 14 år efter 777. Designarbejdet med det nye fly, som i givet fald vil være klar til levering omkring 2025, vil handle om letvægts-materialer til flykroppen og mere brændstoføkonomiske motorer [4], som er typiske udfordringer inden for normalt design af fly. Og det nye fly vil fortsat - selvfølgelig - være baseret på det operationelle princip og den normale konfiguration for fly.

Vincentis bog [24] handler som nævnt om hvad ingeniører ved og hvordan de ved det. Vincenti understreger at den største del af ingeniørers viden er om normalt design, og at normalt design er langt den mest almindelige fase, designarbejdet befinder sig i. Det normale designarbejdes vægt kommer bl.a. til udtryk i en model, Vincenti opstiller over ingeniør-viden. Modellen omfatter ialt seks kategorier, og kun den første kategori, som han betegner "Fundamental design concepts", omfatter det operationelle princip og den normale konfiguration. Alle fem øvrige kategorier vedrører normalt design! Det gælder fx kategorien "Theoretical tools", der bl.a. omfatter tekniske modeller, som indgår i TRIN-modellens punkt tre.

Selv om normalt og radikalt design er modsatte begreber, er den præcise grænse mellem dem flydende. Eksempelvis kan man sammenligne et fjernvarmeværk med et traditionelt kraftværk, og spørge om et fjernvarmeværk betegner et radikalt nyt design i forhold til det traditionelle? eller om et fjernvarmeværk snarere er et resultat af en inkrementel forbedring af det traditionelle kraftværk, opnået gennem mange års arbejde med normalt design af kraftværker? Et kraftvarmeværk producerer både elektricitet ("kraft") og fjernvarme ("varme"). Et kraftvarmeværk ligner derfor et traditionelt kraftværk (som kun producerer el), men er på den anden side radikalt forbedret ved også at producere fjernvarme. Man kan beskrive det operationelle princip for et kraftvarmeværk således: Den første del af processen, elproduktionen, foregår ved at en forbrænding opvarmer vand til damp, der har et højt tryk og driver en turbine, som driver en elgenerator. Den anden del af processen, fjernevarmeproduktionen, udnytter at dampen, efter den har drevet turbinen, stadig har en relativt høj temperatur, uanset om dampen er fortættet til vand, eller fortsat har dampform. Temperaturen er så høj at dampen/vandet kan opvarme fjernvarmevandet ved at udveksler varme med

det i en varmeveksler. Det operationelle princip for et traditionelt kraftværk indeholder kun den første del af processen; i et traditionelt kraftværk ledes en stor mængde overskudsvarme bort, eksempelvis ved at varmt ved ledes ud i en flod. I forhold hertil er det en stor energibesparelse at udnytte overskudsvarmen til fjernvarme, der kan opvarme boliger og institutioner, i stedet for at disse eksempelvis opvarmes med el. Måske kan man sige, at et fjernvarmeværk rent faktisk er et radikalt nyt design, i forhold til et kraftværk, fordi fjernvarmeværket har et andet (udvidet) operationelt princip.

Andre teknologiteoretikere om det operationelle princip

Vincentis teori om ingeniørers viden, herunder hans begreb om teknologiers operationelle princip, er meget kendt og anerkendt. Eksempelvis har Vincentis teori en fremtrædende placering i Mitchams oversigtsværk om teknologifilosofi [15] (se især s. 200-201). Teorien har ligeledes en centrale plads i Marc de Vries' introduktion til samme emne [25] (se især s. 28-29). Vincentis begreb om det operationelle princip var et centralt referencepunkt i et forskningsprojekt på Delft University i Holland, ledet af Peter Kroes, om det filosofiske grundlag for moderne teknologi (se eksempelvis [13]).

Vincentis analyse af det operationelle princip har også interessante teorihistoriske rødder. Definitionen er baseret på den ungarsk-britiske filosof Mihail Polanyis arbejde i 1960erne. En af de definitioner af operationelt princip, Vincenti bruger, har han hentet direkte fra Polanyis arbejde, nemlig denne: "how its characteristic parts [...] fulfil their special function in combining to an overall operation which achieves the purpose" (for teknologien). Definitionen stammer fra s. 328 i Polanyis bog [20], og gengives s. 208 i Vincentis bog [24].

I betragtning af den brede anerkendelse af begrebet operationelt princip kan det virke paradoksalt, at der er relativt få beskrivelser af operationelle principper i den videnskabelige litteratur. Måske kan dette tildels forklares med, som Vincenti allerede er refereret for at hævde, at ingeniører og designere ofte tager en teknologis operationelle princip for givent. I hvert fald er der relativt få sadanne beskrivelser, og derfor beskriver afsnit 3 nedenfor nogle tommelfingerregler til brug for arbejdet med princippet.

Der har i den videnskabelige litteratur mig bekendt ikke været rejst nogen kritik af Vincentis arbejde om det operationelle princip. Derfor vil jeg selv skitsere to kritikpunkter.

For det første er Vincentis begreb, det operationelle princip, jo i ental. Til

forskel herfra bruger vi flertalsform i TRIN-modellens begreb "indre mekanismer og processer", og vi har opdelt i både mekanismer og processer. Generelt taler Vincenti om operationelt princip som noget givet, som entydigt karakteriserer en teknologi. Til forskel herfra lægger begreberne "indre mekanismer og processer"op til at det kan diskuteres hvad der er de centrale mekanismer og processer ved en teknologi. I eksemplet med digital signatur har jeg peget på to centrale elementer, asymmetrisk kryptering og kryptografisk hashing. Alternativt kunne man måske hævde, at asymmetrisk kryptering var det centrale, i hvert fald hvis man vælger en kort beskrivelseform, hvor man gerne vil fremhæve en enkelt mekanisme. Man kan således sige, at det i nogen grad er en vurderingssag, hvad der helt præcist udgør en teknologis indre mekanismer og processer, og at det derfor er ekstra vigtigt at argumentere for den beskrivelse man vælger.

Opdelingen i to underbegreber, mekanismer og processer, lægger endvidere op til at man kan pege på forskellige typer af virkemåder for en teknologi. Måske er begrebet mekanisme mest relevant når der er tale om noget helt automatisk, eksempelvis noget der udføres af software. Omvendt er begrebet proces måske mest relevant når der er tale om en kontrolleret naturlig proces, som fx forbrændingen i en ovn i et fjernvarmeværk.

En anden forskel mellem Vincentis begrebsapparat og TRIN-modellen er at Vincenti typisk bruger begrebet device, hvor vi i TRIN-modellen bruger begrebet teknologi. Vincenti bruger eksempelvis device-begrebet i den definition af operationelt princip, jeg citerede ovenfor i afsnit 3, og han kalder også en flyvemaskine for et "device". Device kan oversættes til apparat eller tingest, og kan forstås som en slags "anvendelsesorienteret ting". Brugen af begrebet teknologi, i stedet for apparat, om fx et fly eller en digital signatur understreger i højere grad at der indgår menneskelig viden og processer. Det er således nødvendigt med piloter for at et flymaskine kan flyve, som skitseret i figur 7, og med maskinarbejdere for at lukke en nitte om en pladesamling, som skitseret i figur 8. Selv om man anerkender at der i stigende grad sker en automatisering af anvendelserne af teknologierne, eksempelvis med fly uden piloter, så indgår der fortsat menneskelige viden og aktivitet i design og produktion af teknologierne, og anvendelsen sker stadig under en eller anden form for menneskelig overvågning og kontrol.

Tommelfingerregler

Som sammenfatning på diskussionen om TRIN-modellens første trin om indre mekanismer og processer viser tabel 5 nedenfor et sæt af tommelfingerregler. Det er forslag til hvordan man kan bruge trinnet i praksis - det vil sige når man laver en teknologi-beskrivelse med hovedvægt på dens teknisk-videnskabelige aspekter.

- Indre mekanismer og processer handler om hvordan en teknologi virker.
- Nærmere bestemt handler indre mekanismer og processer om det eller de principper ved teknologien, som bidrager til at opfylde teknologiens formål.
- Da definitionen har fokus på teknologiens formål, kan en redegørelse for formålet være en vigtig del af beskrivelsen af indre mekanismer og processer.
- Man kan give forskellige beskrivelser af indre mekanismer og processer for den samme teknologi, da det i nogen grad er en vurderingssag, hvad der faktisk er væsentligt at fremhæve, og hvilket detaljeringsniveau man ønsker.
- Omfanget af en beskrivelse af indre mekanismer og processer kan gå fra ultrakort, som fx de få linjer i definitionen for flyvemaskiner i citatet fra Vincenti i afsnit 3, til at strække sig over flere sider, som fx definitionen i denne artikels afsnit 2 af digital signaturs indre mekanismer og processer.
- Man kan beskrive indre mekanismer og processer både for et helt produkt med en brugbarhed for mennesker (eksempelvis en flyvemaskine), for en stor og central komponent (eksempelvis en flyvinge) og for en lille bitte komponent (eksempelvis en nitte).
- En beskrivelse af indre mekanismer og processer (fx for et fly) vil ofte henvise til egenskaber ved en komponent (fx flyvinger), uden at komponetens egne indre mekanismer og processer forklares.
- En beskrivelse af indre mekanismer og processer kan både indeholde beskrivelser af artefakter (fx flyvinger), naturprocesser (fx forbrænding i en ovn) og menneskelig aktivitet (fx at slå en nitte fast).

Tabel 5: Tommelfingerregler om en teknologis indre mekanismer og processer.

4 Digital signatur analyseret med hele TRIN-modellen

Dette afsnit giver en samlet beskrivelse af digital signatur med brug af hele begrebsapparatet i TRIN-modellen (se tabel 1). Formålet med afsnittet er således at vise brugen af TRIN-modellen i praksis, og samtidig give en uddybet redegørelse for digital signatur. Trin 1 om indre mekanismer og processer er behandlet i de foregående afsnit, så jeg begynder med trin 2.

Trin 2: Teknologiers artefakter

Dette trin handler om at indkredse hvilke artefakter, der indgår i en teknologi, og om at beskrive dem. Et artefakt er en menneskeskabt genstand. Når vi i TRIN-modellen taler om artefakter, mener vi tekniske artefakter, hvilket skal forstås som artefakter med en praktisk funktion eller formål i relation til teknologien. Denne formålsbestemthed er til forskel fra artefakter i kunst, fx et maleri.

Dette afsnit begynder med en kort analyse af de allerede omtalte artefakter i relation til digital signatur, nemlig nøgleparret med en privat og en offentlig nøgle, og softwareprogrammer til skabelse og bekræftelse af signatur. Herefter beskrives et smartcard til digital signatur, som er en slags specialbygget hardware, hvilket giver anledning til en diskussion af forskellen på software-artefakter og hardware-artefakter. Til sidst omtaler afsnittet nogle standarder, som spiller en meget vigtig rolle inden for digital signatur, og disse standarder er også artefakter.

Nøgleparret. De private og offentlige nøgle, der benyttes i digital signatur, er i sig selv interessante og vigtige artefakter.

I RSA-udgaven af assymmetrisk kryptering er den private og den offentlige nøgle hver især et ordnet par. Den private nøgle er det ordnede par $\langle p, n\rangle$, hvor p står for privat, og den offentlige nøgle er det ordnede par $\langle o, n\rangle$, hvor o står for offentlig. Tallet n går igen i både den private og offentlige nøgle. n betegner en såkaldt modulus, eksempelvis tallet 143 i RSA-eksemplet i afsnit 2. Man angiver styrken af et nøglepar ved den omtrentlige størrelse af n. En størrelse på 4096 bits, som er benyttet i signaturen i figur 1, regnes aktuelt for en stor, sikker værdi.

Software til skabelse og bekræftelse af digital signatur. Den mest udbredte udgave af digital signatur til elektronisk post er mig bekendt Enigmail.

Enigmail er en tilføjelse til open-source mailprogrammet Thunderbird, som er knyttet til open-source browseren Mozilla. Bekræftelsen af den digitale signatur i figur 1 har jeg foretaget i Thunderbird udvidet med Enigmail. Enigmail er en softwarepakke, som kan køre på alle computere, som i forvejen kan køre Thunderbird, og kræver således ikke at man tilkøber ekstra hardware eller andet. Både den asymmetriske kryptering og den kryptografiske hashing kan køre på en tidssvarende computer uden generende forsinkelser: når man modtager en signeret mail i Thunderbird/Enigmail, foregår bekræftelsen af signaturen inden for en brøkdel af et sekund.

Program til nøglegenerering. Forud for at en bruger kan bruge digital signatur, skal brugeren køre et program, som genererer nøgleparret. Det vigtigste skridt i nøglegenereringen er at finde to store primtal, p og q, hvis produkt p*q er af den størrelsesorden, der er fastsat af nøglestørrelsen. Når nøgleparret er genereret, skal den private nøgle lagres på en beskyttet måde af brugeren, så andre forhindres i at se nøglen, mens den offentlige nøgle skal distribueres til de som brugeren kommunikerer med.

Kryptering med private og offentlige RSA-nøgler udnytter nøglernes særlige matematiske egenskaber. De centrale egenskaber har været kendt i matematikken i århundreder; nogle af de vigtigste blev beskrevet af den schweitziske matematiker Leonard Euler, der virkede i 1700-tallet.

Specialbygget hardware. Mens nøgler, nøglegenereringsprogrammer m.m. er software-artefakter, benytter man i nogle tilfælde også specialbygget hardware til digital sigantur. Figur 10 viser et hardware-modul (et smartcard) til brug med NemID. Når brugeren vil skabe en digital signatur, forbindes hardwaremodulet til computeren, via en kortlæser, og når signaturen er skabt, kobles modulet fra igen. Hardwaremodulet opbevarer brugerens private nøgle, og det giver sikkerhed mod tyveri af den private nøgle. Tyveri af en software-baseret privat nøgle kan ske hvis en anden person hacker sig ind på computeren, og kopierer den fil, som indeholder den private nøgle. Dette er man beskyttet imod hvis den private nøgle er gemt på et eksternt hardwaremodul. En anden fordel ved at særligt hardware-modul, som brugeren kan medbringe, er at brugeren kan være interesseret i at foretage signering på sin mobiltelefon eller på computere på biblioteker, universiteter og andre offentlige steder. Dette giver et særligt hardware-modul mulighed for, da modulerne er små og nemt kan medbringes i en lomme eller taske.

Forskellen på software-artefakter (fx RSA-nøgler) og hardware-artefakter (fx krypteringsmodulet i 10) er umiddelbart ret stor. Hardware har en fysisk eksistens, og kan ikke uden videre kopieres, mens software er flygtigt, og let

Figur 10: Hardware til den bruger, som selv ønsker at opbevare den private nøgle til digital signatur. Den viste hardware er et smartcard, der blev lanceret til NemID i 2012.

kan kopieres. Specielt er det let at komme til at kopiere en offentlig nøgle, mens man selvfølgelig håber at ens private nøgle ikke bliver kopieret.

Specialbygget hardware til at skabe en digital signatur har samme overordnede formål eller funktion som et program til digital signatur (som Enigmail), men forskellig form. Det er således et eksempel på at artefakters funktion og form ikke følges ad. Motivationen for den specialbyggede hardware er i dette tilfælde at give en øget sikkerhed og fleksibilitet, som nævnt ovenfor. Da dette også kan betegnes som en supplerende funktion, er funktionerne dog forskellige på det mere detaljerede plan. Det har i øvrigt vist sig vanskeligt at få den specialbyggede hardware til at fungere, altså at indhøste fordelen ved den øgede sikkerhed og fleksibilitet. Den specialbyggede hardware kræver at den enhed, hardwaren tilsluttes, bruger noget bestemt software, og har også været ramt af en række andre problemer. I februar 2018 kunne Gemalto-smartcard'et ikke bestilles.

Softwareprogrammet Enigmail skal naturligvis også bruge hardware for at køre. Der er blot tale om den computer, brugeren formodes at være i besiddelse af i forvejen. Typisk vil computeren have en kraftigere processer end den specialbyggede hardware (figur 10), men til gengæld er computerens processor designet så den kan bruges til mange forskellige opgaver, så samlet set er det ikke sikkert, at skabelsen af en digital signatur går hurtigere på computeren end på den specialbyggede hardware.

Generelt er den digitale teknologi særdeles afhængig af hardware. På den

måde giver det god mening at betegne digital teknologi - som fx digital signatur - som en materiel teknologi. Digital signatur forudsætter at brugerens hardware er tilstrækkelig avanceret til at krypteringsoperationerne m.v. i skabelsen af digital signatur kan foregå tilstrækkelig hurtigt.

Standarder spiller en meget stor rolle for digital signatur. Der anvendes standarder bl.a. fra det amerikanske standardiseringsinstitut NIST (National Institute of Standards and Technology) og fra det private sikkerhedsfirma RSA, der sælger sikkerhedsprodukter baseret på RSA-algoritmen. Standarderne er dokumenter, som beskriver eksempelvis formater for en digital signatur (herunder det allerede nævnte spørgsmål om adskillelse af signatur og tekst) og nøglestørrelse (eksempelvis en RSA-nøgle på 4096 bit). En standard for digital signatur bør også fastlægge en måde hvorpå underskriverens program kommunikerer hvilken krypteringsmetode og hashmetode, der er anvendt, så modtagerens program kan bruge de samme metoder. Disse informationer er indeholdt i det signerede dokument. Se for eksempel linjen med "Hash: SHA512" i figur 1. Et eksempel på en standard er Digital Signature Standard [21], som kræver at amerikanske offentlige myndigheder skal bruge digital signatur i en af tre forskellige hovedvarianter, hvoraf den ene er med RSA, hvor standarden kræver nøglestørrelser fra 1024 bits og opad.

Trin 3: Teknologiers utilsigtede effekter

Dette afsnit handler om punktet "Identifikation af en teknologis tilsigtede og utilsigtede effekter"i TRIN-modellen. Hovedsigtet med punktet er identifikation og analyse af en teknologis utilsigtede effekter, og især de uønskede blandt disse.

Måske den største uønskede effekt er digital signatur er, at der er en betydelig risiko for at brugeren får stjålet sin private nøgle. Den private nøgle med en nøglelængde på eksempelvis to tusind bits er umulig at huske for mennesker uden helt ekceptionelle talmæssige evner. For at forestille sig hvor svært det er, kan man sammenligne med at skulle huske et password på cirka 200 tegn. Vel at mærke et password hvor hvert tegn kan være både stort og lille bogstav, et ciffer eller et kommaterings-tegn. For antallet af kombinationsmuligheder i et sådant password svarer nogenlunde til antallet af forskellige nøgler på to tusind bits. Da det er helt umuligt at huske et sådant password, er det nødvendigt at lagre den private nøgle. Som nævnt under afsnittet om artefakter, findes der sikre løsninger hvor den private nøgle er lagret på et separat stykke hardware, der kan forbindes til computeren når

nøglen skal bruges, men den almindelige bruger har ikke umiddelbart adgang til denne form for hardware. Derfor er den basale løsning at lagre den private nøgle på computeren. Denne løsning bruges som standardløsning i Enigmail. Løsningen blev også anvendt i de danske bankers signatur-baserede løsninger til netbank, som var i anvendelse indtil ca. 2008.

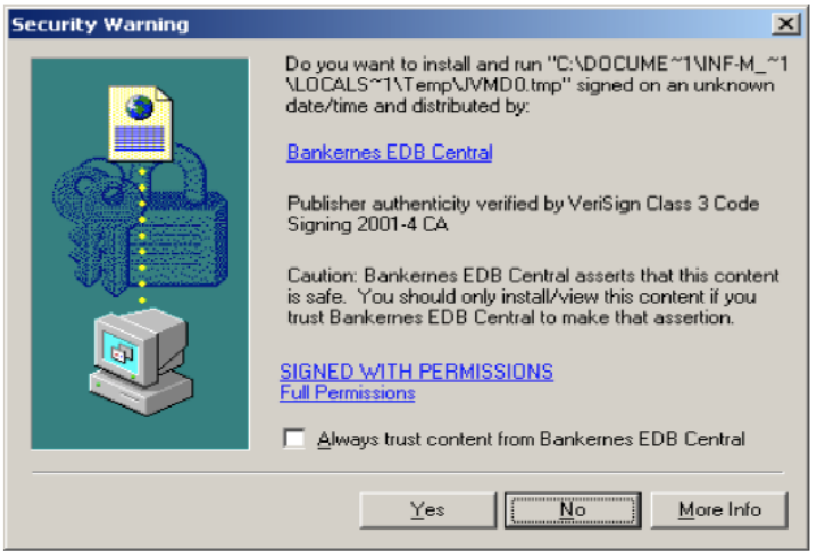
Når den private nøgle er lagret på computeren, er nøglen sårbar over for at hackere får adgang til computeren og kopierer nøglen. Man kan delvist beskytte sig mod dette med en metode, hvor man password-beskytter filen med den private nøgle, men dels er dette ikke fuldt ud effektivt, og dels komplicerer det også brugen af nøglen, da brugeren nu skal huske et password for at kunne signere.

Til den private nøgle er der også knyttet en anden udfordring, nemlig at den private (og den offentlige) nøgle skal genereres. Da den private nøgle er hemmelig, bør nøglerne genereres af brugeren, hvilket sker ved at brugeren downloader og anvender software til opgaven. Opgaven med at få nøglegenereringsprogrammet til at generere nøgleparret kan imidlertid være vanskelig og i hvert fald svær for brugeren at følge med i.

Brugernes vanskeligheder med bl.a. nøglegeneringen er beskrevet bl.a. af Whitten og Tygar [26], der handler om signerings-software baseret på PGP. Forfatterne bad nogle testpersoner om at bruge PGP-programmet til at sende forskellige krypterede og signerede beskeder. Det var gennemgående meget vanskeligt for testpersonerne at udføre opgaverne. Det var også vanskeligt for testpersonerne at forstå betydningen af de forskellige skridt, fx signering med en nøgle og kryptering med en anden nøgle.

Whitten og Tygar definerede begrebet "usable security"så det bl.a. omfattede, at brugeren skulle have forståelse for de sikkerhedsmæssige opgaver, de skulle udføre. Definitionen omfattede fem punkter, blandt andet dette: "Definition: Security software is usable if the people who are expected to use it: 1. are reliably made aware of the security tasks they need to perform; [..]"[26].

I en analyse af de danske netbanker, jeg var med til at skrive i 2004 [8], studerede vi de danske netbankers signaturløsninger, med udgangspunkt i Whitten og Tygars begreb om "usable security", som vi oversatte til brugervenlig sikkerhed. Vi studerende bl.a. nøglegenereringsprocessen for fem forskellige netbanksløsninger baseret på digital signatur. Vores konklusion var at nøglegenereringsprocessen var meget svær for brugeren at gennemføre. Processen lod sig i store træk kun gennemføre, hvis brugeren mere eller mindre bevidstløst trykkede "ja" til forskellige spørgsmål. Eksempelvis skulle



Figur 11: Browserbesked, som brugeren skulle sige "Yes"til for at gennemføre nøglegenerering i en dansk netbanksløsning med digital signatur i 2004.

brugeren typisk svare "Yes" , når brugeren fik browserbeskeden i figur 11.

Brugeren kunne undgå denne og andre nærmest uforståelige browserbeskeder ved at indstille browserens sikkerhedsniveau til at være lavt. Men hermed udsatte brugeren sig jo netop for større risiko for at blive hacket m.v., herunder for at få stjålet den private nøgle.

Nøglegenereringsprogrammerne forsøgte at guide brugeren ved at forklare de forskellige grundtermer. Dette svarede til Whitten og Tygars intension (jf. citatet ovenfor) om på en pålidelig måde at gøre brugeren opmærksom på de sikkerhedsmæssige opgaver. Men dette forsøg kunne i sig selv være med til at skabe forvirring. De fem systemer præsenterede brugeren for mellem 8 og 14 forskellige sikkerhedsrelaterede begreber, herunder fx autentificering, verifikation, signering, certifikat, sikker forbindelse, privat nøgle and signaturfil. Generelt kan man sige, at sikkerhed med kryptering og nøgler er et vanskeligt emne, som mange brugere ikke har kendskab til, og som det derfor er vanskeligt for mange at bruge på en korrekt og sikker måde. Man kan således sige, at digital signatur har den meget væsentlige utilsigtede effekt, at den er svært at forstå for almindelige brugere. Og dette kan være medvirkende til at brugerne ikke beskytter sig tilstrækkeligt mod tyveri af deres private

nøgler.

Trin 4: Teknologiske systemer

Dette trin handler om de større teknologi-sammenhænge, en teknologi indgår i. Man kan dels tale om, at digital signatur i sig selv er et teknologisk system, og dels om at digital signatur hænger sammen med andre teknologiske systemer, især internettet og PKI, som står for Public Key Infrastructure (offentlig nøgle-infrastruktur).

Digital signatur er i sig selv et teknologisk system
Teknologien digital signatur kan betragtes som et teknologisk system med software, hardware, andre artefakter og menneskelige aktører. Underafsnittet om trin 2 ovenfor omtalte software til bl.a. nøglegenerering, hardware til at gemme private nøgler på samt artefakter i form af standarder. De menneskelige aktører er brugerne, som enten skaber eller bekræfter signaturer. De organisationer, som udvikler software, hardware og standarder, kan også betegnes menneskelige aktører.

En af årsagerne til at det er vigtigt at betragte det samlede teknologiske system, er at væsentlige ulemper ved teknologien kan hænge sammen med elementer i det teknologiske system, som man måske ikke i første omfang har tænkt på som centrale. Eksempelvis kan det - som skitseret i afsnit 3 lige ovenfor - være vanskeligt for en bruger at skabe et nøglepar og forstå at det er vigtigt at opbevare den private nøgle på en meget sikker måde. Derfor skal man være opmærksom på, at nøglegenerering hører med til teknologien digital signatur.

Digital signatur hænger sammen med internettet
Internettet bruges meget ofte i forbindelse med digital signering. Meget ofte sendes et signeret dokument til modtageren med internettet, fx hvis man sender en signeret kontrakt som vedhæftet fil til en mail.

Endvidere bruges internettet af mange til at downloade programmel til digital signering, fx udvidelsen Enigmail til mailprogrammet Thunderbird.

På den måde fungerer internettet som distributionskanal både for signerede dokumenter og for programmerne til at bruge digital signatur.

Risikoen for tyveri af brugerens private nøgle hænger også sammen med internettet. Mange brugere er ofte eller konstant logget på internettet, og

besøger eksempelvis websteder, hvorfra brugeren risikerer at downloade forskellige virus, orme og anden "malware", som kan give hackere adgang til brugerens computer.

Digital signatur hænger sammen med PKI
Det andet system, digital signatur indgår i, er PKI. PKI er i nogen grad en vision, snarere end en realiseret teknologi, så det er måske mere rigtigt at sige, at PKI er et teknologisk system, som digital signatur kan indgå i, i den udstrækning PKI realiseres.

Hensigten med den offentlige nøgle-infrastruktur er at give den person, der skal bekræfte en digital signatur, en sikkerhed for at den offentlige nøgle faktisk hører til den person, der hævdes at have udført signaturen. I eksemplet fra afsnittet om asymmetrisk kryptering, går banken, når den bekræfter signaturen på teksten om overførsel af penge fra Kathy Eberth til Jimi Hendrix' konto ud fra, at den offentlige nøgle faktisk tilhører Kathy Eberth. Men hvordan kan banken faktisk vide dette? Hvad hvis H. Acker giver sig ud for at være Kathy Eberth, og overbeviser banken om, at hans offentlige nøgle er Kathy Eberths offentlige nøgle? Der kan altså være to personer, der henvendte sig digitalt til banken, og begge hævdede at være Kathy Eberth, og sendte banken deres offentlige nøgle.

En PKI kan give sikkerhed for tilhørsforholdet af en offentlig nøgle med to elementer, certifikater og certifikatudstedere. På engelsk betegnes certifikatudsteder som Certificate Authority (CA). En certifikatudsteder skal kontrollere identiteten af en person. Herefter udsteder CAen et certifikat, hvor de to vigtigste oplysninger er om personens identitet og personens offentlige nøgle. Personen skal selv generere nøgleparret, og herefter præsentere sig for CAen sammen med den offentlige nøgle. I Danmark bruger Nets, der står bag NemId-systemet, det centrale personnummerregister (CPR) til at kontrollere en persons identitet, i stedet for at kræve at personen møder frem personligt. Det sker i praksis ved at sende en kode til den adresse, personen står opført med i CPR-registeret, og når personen senere demonstrerer, at han kender koden (ved at indtaste denne i en webapplikation), tages dette som udtryk for, at det er den rigtige person. Ræsonnementet er at vedkommende må bo på adressen, når han eller hun har modtaget koden.

Selve certifikatet er selv en digital signatur. I denne digitale signatur er teksten oplysningerne om personens identitet og offentlige nøgle, og signaturen er udført med certifikatudstederens private nøgle. Hvis Kathy Eberth har et certifikat fra en CA, som banken stoler på, vil banken på denne måde

kunne overbevise sig om rigtigheden af den offentlige nøgle, hun sender banken. Fordelen ved en PKI er at den overfører tillidsspørgsmålet til et mindre antal certifikatudstedere. Man kan argumentere for, at det er nemmere for banken at holde rede i et mindre antal certifikatudstedere, den har tillid til, end i selv at skulle tage stilling til hver enkelt bruger. I Danmark er Nets, der driver NemID-systemet, en af certifikatudstederne. Det er principielt muligt at reducere antallet af certifikatudstedere, som den enkelte borger eller institution skal have tillid til, ved at certifikatudstederne kan udstede certifikater til hinanden. Det kan eventuelt være i en kæde, så certifikatudsteder A garanterer identiteten på certifikatudsteder B, som garanterer identiteten på certifikatudsteder C, osv.

Man kan betegne teknologisystemet PKI som et forsøg på en teknologisk løsning på en risiko ved teknologisystemet digital signatur.

I en vurdering af PKI må man konstatere, at det ikke er lykkedes at skabe et teknologisk system med et lille antal certifikatudstedere, som alle kan have tillid til. Der eksisterer faktisk et uoverskueligt kaos med mange certifikatudstedere. Eksempelvis kommer en moderne browser med en liste af certifikatudstedere, browseren stoler på. Disse kan ses ved at gå ind i browserens sikkerhedsindstillinger. I Firefox-browseren kan certifikatudstederne ses ved at vælge Preferences, Privacy & Security, View certificates og til sidst Authorities. Det betyder at Firefox - på brugerens vegne - stoler på certifikater udstedet af disse CA-er. Listen i min Firefox omfatter hundredevis af certifikatudstedere.

Afsluttende bemærkninger om teknologisk system
Jeg må nok erkende, at i denne artikel bruger jeg begrebet "digital signatur" i flere betydninger. Afsnit 2 om indre mekanismer i digital signatur bruger begrebet til at betegne softwarebaseret signering og bekræftelse (fx i figur 2), mens dette afsnit bruger begrebet til at betegne det samlede teknologiske system - altså med nøglegenerering, brugere, standardisering m.v. Måske kunne jeg skelne mellem "den softwarebaserede, teknologiske kerne af digital signatur" og "digital signatur som teknologisk system", men jeg foretrækker en "ærlig flertydighed" - og så håber jeg, at vi i det videre arbejde med TRIN-modellen kan opnå en større begrebsafklaring.

Spørgsmålet om hvilke andre teknologi-systemer, en teknologi indgår i, afhænger af blandt andre historiske forhold og af hvilket fokus man har som betragter. Historisk set opstod digital signatur før internettet. Digital signatur blev første gang beskrevet i en artikel fra 1976 af Whitfield Diffie og

Martin Helman [5]. På dette tidspunkt fandtes en række mindre computernetværk, inklusive det såkaldte ARPANAT, hvoraf mange senere blev koblet sammen i internettet, men selve internettet eksisterede ikke. Diffie og Helman motiverede digital signatur med, at den kunne bruges i pengeautomater ("cash dispensers") og computer-terminaler (en skærm og et tastatur sluttet til en central computer), og de nævnte af gode grunde ikke internettet, som jeg ellers nævnte ovenfor som centralt anvendelsesområde i dag.

Valget af PKI som et centralt teknologi-system, som digital signatur hænger sammen med, skyldes også at jeg i denne artikel har lagt vægt på at beskrive risici ved digital signatur i relation til opbevaring af private nøgler og troværdighed af offentlige nøgler. På den måde afhænger valget af teknologisk system eller systemer også af det fokus, man har som betragter. Hvis man bruger trin 4 i en teknologi-analyse, kan det ofte anbefales, at man giver en begrundelse for hvilke elementer, man prioriterer i det teknologiske system, og at begrundelsen henviser til det fokus, man har i sin analyse.

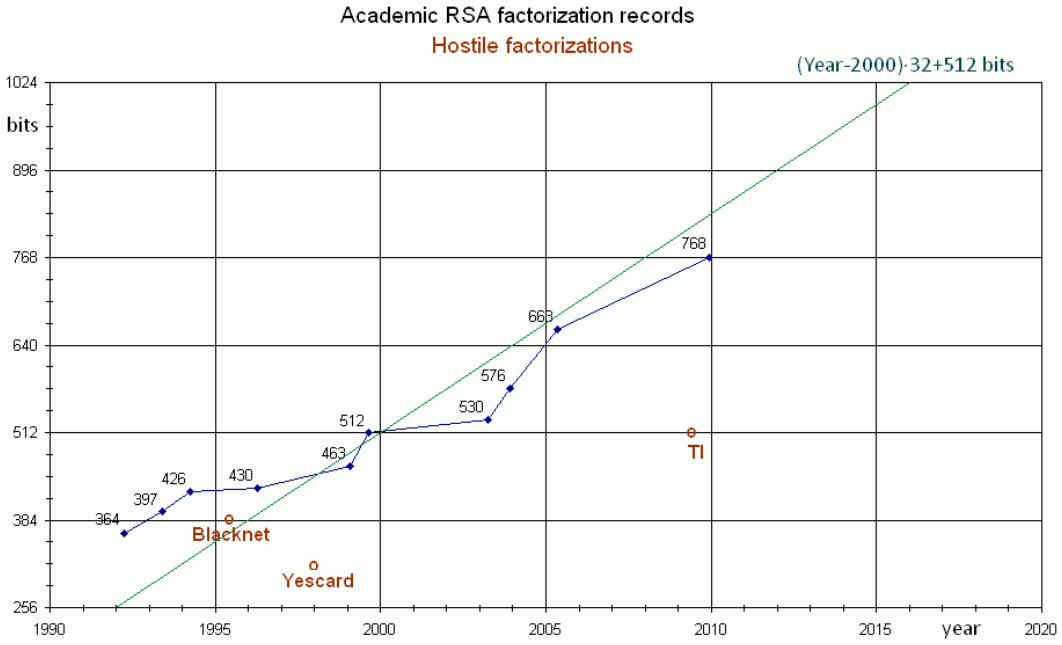
Trin 5: Modeller af teknologier

Dette afsnit handler særligt om numeriske modeller af teknologi, også betegnet som abstrakte modeller.

Francois Grieu har foreslået en model [6], der forudsiger hvor store nøgler, der er tilrådelige i asymmetrisk kryptering med RSA - og dermed i digital signatur, hvis man bruger RSA hertil. Modellen siger, at man som bruger på lang sigt skal forøge nøglestørrelsen med 32 bits om året Det skal forstås således, at hvis en nøglestørrelse på cirka tusind bits er lige akkurat tilstrækkeligt det ene år, så vil en størrelse på 32 plus tusind bits være lige akkurat tilstrækkelig det næste år. I praksis skal man ikke skifte nøglestørrelse hele tiden, men sørge for at man i en årrække af rimeligt over det akkurat tilstrækkelige.

Modellen er relevant fordi man ikke bare kan vælge en ekstrem stor nøglestørrelse, da dette vil være for tidskrævende for krypteringsprogrammerne. Modellen kan derfor bruges til at finde en god balance mellem sikkerhed (hvilket taler for stor nøglelængde) og tidsforbrug (hvilket taler for lille nøglelængde).

Modellens input drejer sig om primtalsfaktorering. Primtalsfaktorering er en metode til at knække RSA-nøgler, det vil sige til at gætte den private nøgle ud fra kendskab til den offentlige nøgle. Primtalsfaktorering af store tal er vanskelig, men med stigende computerkraft - og computerens hastighed



Figur 12: Francois Grieus model som forsøger at forudsige hvor stor tal det vil være muligt at primtalsfaktorisere i et givet år.

stiger jo hele tiden - er det muligt at primtalsfaktorere større og større tal. Endvidere sker der en forbedring af metoderne til primtalsfaktorering.

Modellen er vist grafisk i 12. Modellens input om primtalsfaktorering er empiri-baseret. Den er baseret på i hvilket år, det første gang lykkedes at primtalsfaktorisere et tal af en bestemt størrelse. Disse tal ses som blå og røde prikker på figur 8. Den generelle model er baseret på de blå tal, som viser det som Francois Grieu betegner som akademiske rekorder, hvormed han sigter på resultater publiceret af universitetsfolk. De røde tal viser primtalsfaktoreringer udført af hackere. Dem skal man jo også beskytte sig mod, og så vidt jeg forstår, er grunden til at Grieu ikke har baseret modellen på dem at der er så få af dem.

Den generelle model siger at man i år "Year" vil kunne primtalsfaktorisere tal, der er repræsenteret med n bits, hvor n = (Year-2000)*32+512. Formlen står i figur 8 øverst til højre. Modellen, der blev offentliggjort første gang i 2012, siger eksempelvis, at i år 2017 vil man kunne primtalsfaktorisere tal i størrelsen 1056 bits. Dette tal fremkommer som

$$(2018 - 2000) * 32 + 512 = 1088$$

Modellens svagheder er blandt andre, at man naturligvis ikke kan vide, om der kommer nye metoder til primtalsfaktorering i fremtiden. Eksempelvis er det muligt at en fremtidig udvikling af kvantecomputere vil gøre primtalsfaktorering meget mere overkommelig.

Udover primtalsfaktoriseringer fra universitetsverdenen og hackermiljøer bør man også overveje hvor store tal, der kan primtalsfaktoreres af efterretningstjenesterne, herunder den amerikanske teknologiske efterretningstjeneste NSA. De har formentlig endnu større maskiner til rådighed end universitets- og hackermiljøerne.

Det anbefales i dag at bruge nøgler med en størrelse på mindst to tusind bits. Som allerede nævnt bruger sikkerhedsteamet i FreeBSD en nøglestørrelse på 4096 bits, så teamet har valgt at prioritere sikkerhed forholdsvis højt, og muligvis på bekostning af udførelsestiden på lidt ældre computere. I mange sammenhænge regnes en RSA-nøglestørrelse på 2048 bits for at være tilstrækkelig.

Francois Greius model er en abstrakt model i henhold til opdelingen mellem visuelle, fysiske og abstrakte (numeriske) modeller i Müllers artikel om modeller [17].

Trin 6: Teknologier som innovation

Det sjette og sidste trin i TRIN-modellen shandler om drivkræfter og barrierer for udbredelse af digital signatur. Trinnet giver mulighed for at arbejde mere samlet med en teknologi og spørge hvorfor vi overhovedet har fået den? Hvorfor har vi for eksempel fået en variant af digital signatur, hvor nøglen er opbevaret centralt? Eller hvorfor går det ikke hurtigere i Danmark med at overgå til vedvarende energiformer - hvilke barrierer er der?

Drivkræften for udbredelsen af digital signatur er knyttet til formålet, at være et digitalt alternativ til den fysiske signatur. Digitale signaturer kan være fordelagtige når en meget stor del af kommunikationen foregår digitalt over internettet, fx kommunikation mellem borger og erhvervsliv (fx netbank) og mellem borger og stat (fx skat og uddannelsessystem).

I Danmark har finansministeriet presset på for en øget digitalisering af den offentlige administration, herunder med brug af digitale signaturer, blandt

andet med den hensigt at digitalisering kunne give mulighed for besparelser på de offentlige udgifter. Håbet har blandt andet været at staten kunne spare personale på samme måde som bankerne har gjort, i takt med overgangen til netbanker og nedlæggelse af en række fysiske bankfilialer. På den måde har en del af drivkraften i høj grad handlet om økonomi. Generelt handler innovationsteori i nogen grad om økonomi og andre humanvidenskabelige emner, og altså ikke om teknisk videnskab. På den måde adskiller trin 6 sig fra de første frem trin.

Danmark er så vidt jeg ved det land i verden, hvor den største andel af den voksne befolkning, nemlig 92% af alle over 15 år, bruger digital signatur [1]. Det er i form af NemID-systemet. NemID udbydes af firmaet Nets, der oprindeligt hovedsageligt var ejet af danske banker, men i 2014 blev solgt til udenlandske kapitalfonde.

Lov om elektroniske signaturer, som er omtalt i afsnit 2, er fra år 2000. Loven er en implementering af et EU-direktiv om digital signatur fra 1999, og fastsatte retningslinjer for blandt andre certifikatudstedere og certifikater. De første certifikater baseret på lovens retningslinjer hed OCES-certifikater (Offentlige Certifikater til Elektronisk Service) og kom i brug i 2003. I 2007 var der ca. en million brugere af signaturer baseret på OCES-certifikaterne [19], hvilket var lige under 25% af befolkningen over 15 år.

Den særlige danske model for statsstøttede digitale signaturer, baseret på OCES-certifikater, overgik i 2008 til NemID-systemet. NemID bruger digital signatur, men adskiller sig fra den sædvanlige model for digital signatur ved at alle brugeres private nøgle opbevares på en central server, og ikke af den enkelte bruger. Lad os prøve at sammenligne den centrale server-løsning med et samrtcard, der opbevarer den private nøgle, som diskuteret under trin 2 i nærværende afsnit. Smartcardet forbindes kun til computeren når nøglen skal bruges til at signere med. Begge metoder sikrer at den private nøgle ikke ligger på brugerens PC. I begge systemer befinder den private nøgle sig kun på den særlige hardware; når brugeren skal signere noget, det vil sige have krypteret en hashværdi, sendes hashværdien til hardwaren (usb-forbundet hardware eller den centrale server), og signaturen sendes derefter tilbage fra hardwaremodulet. Men der er stor forskel på om nøglen opbevares af hardware, som brugeren selv har, eller opbevares af staten.

Kritikken af NemID-systemet med central opbevaring af den private nøgle har blandt andet været, at skaden ved et hackerangreb på den centrale server vil kunne blive meget stor. Endvidere kan man som bruger principielt ikke udelukke, at ens nøgle er misbrugt, enten ved et hackerangreb på den centrale

server, eller ved at en myndighed, fx en efterretningstjeneste, har fået adgang til ens private nøgle. Man kan sige at den centrale nøgleopbevaring betyder, at staten autentificerer borgeren og derefter skriver under på vegne af borgeren.

Javier Lopez og andre diskuterer i [11] hvad årsagerne kunne være til, at PKI, som forfatterne siger, har fejlet internationalt set. Denne diskussion er vigtig, fordi digital signatur forudsætter en eller anden form for PKI-struktur. Hermed mener jeg, at digital signatur forudsætter en eller anden måde, hvor man kan få garanti for at en offentlig nøgle hører til en bestemt person. En af de mulige forklaringer, som forfatterne nævner, er fraværet af en business case for certifikatudstedere. Det er altså svært for en CA at tjene penge. Og i særlig grad har certifikatudstedere ikke noget økonomisk incitament til at krydscertificere, altså til at garantere identiteten for hinanden, da dette kan være medvirkende til at give kunder til konkurrerende udstedere, og altså undergrave eget eksistensgrundlag. Man kan sige, at digital signatur ville have gavn af - om ikke et monopol - så i hvert fald et oligopol, med et lille antal dominerende certifikatudstedere, og at vi i stedet har fået en markedsmodel med mange konkurrerende CAer.

I lyset af vanskelighederne med at udbrede PKI, som er en nødvendig forudsætning for at udbrede digital signatur, kan det være relevant at se på hvordan NemID med den centrale nøgleopbevaring overvinder nogle af barriererne for PKI og digital sigantur. Den centrale nøgleopbevaring udgør et bud på en løsning på de to mest centrale barrierer for udbredelsen af digital signatur. For det første fjerner NemID-systemet risikoen for tyveri af nøglen fra den enkelte bruger (godt nok erstattes den af risikoen for et angreb på den centrale server). For det andet medfører den centrale opbygning, med ikke alene en central nøgleserver men også et fælles system for digital signatur til alle netbanker og til alle offentlige tjenester, at man undgår det kaos, der kan opstå med mange forskellige certifikatudstedere i en mere løseligt organiseret PKI-struktur.

NemID-systemets næste generation er i øjeblikket i udbud, og specifikationen på det nye system indeholder en mulighed for at brugerne selv opbevarer den private nøgle [1].

Litteratur

[1] Agency for Digitisation (Digitaliseringsstyrelsen). *Next Generation of National Digital Identity and Signing.* July 27th, 2016. URL: kan downloades fra http://www.digst.dk. Tilgået 5.11.2017.

[2] Berlingske Business. *Møller har sat sin sidste signatur.* 14.8.2012. URL: https://www.business.dk/oekonomi/moeller-har-sat-sin-sidste-signatur. Tilgået 5.11.2017.

[3] Berlingske Business. *PFA afviser ansvar efter dokumentfalsk.* 21.1.1999. URL: https://www.business.dk/evb-archive/pfa-afviser-ansvar-efter-dokumentfalsk. Tilgået 5.11.2017.

[4] Jay Bennett. *Boeing 797? Aviation Giant Teases New Airliner at Paris Air Show.* 23. juni 2017. URL: http://www.popularmechanics.com/flight/airlines/news/a27055/797-boeing-nma-new-airliner/ Tilgået 11.12.2017.

[5] Whitfield Diffie and Martin Helman. New Directions in Cryptography. *IEEE Transactions on Information Theory*, Vol. IT-22, No. 6, November 1976.

[6] Francois Grieu. *How big an RSA key is considered secure today?* Skriftligt svar på stackexchange.com. Det oprindelige svar er fra 2012, og den seneste gang opdatering er fra 21.1.2015.
URL: https://crypto.stackexchange.com/questions/1978/how-big-an-rsa-key-is-considered-secure-today. Tilgået 5.11.2017.

[7] The FreeBSD Documentation Project *FreeBSD Handbook. Appendix D. OpenPGP Keys.*
URL: https://www.freebsd.org/doc/handbook/book.html#pgpkeys Tilgået d. 22.2.2018.

[8] Morten Hertzum, Niels Jørgensen, and Mie Nørgaard. Usable Security and E-Banking: Ease of Use Vis-á-Vis Security. *Australasian Journal of Information Systems, Special Issue, December 2004, pp 52-65.* URL: ruc.dk/ñielsj/research/publications/eBanking-ajis.pdf

[9] How Wind Power Works. URL: https://science.howstuffworks.com/environmental/green-science/wind-power.htm.

[10] Information. *PFA holdt bestyrelsen i uvidenhed.* 2.2.1999. URL: https://www.information.dk/1999/02/pfa-holdt-bestyrelsen-uvidenhed Tilgået 5.11.2017.

[11] Javier Lopez, Rolf Oppliger and Gunther Penul. Why have public key infrastructures failed so far? *Internet Research, Vol. 15 No. 5, 2005, pp. 544-556*

[12] Niels Jørgensen. The Boeing 777: No chainsaw massacres, please! *Journal of Integrated Design and Process Science,* Vol. 10, No. 2, 2006, pp. 79-91.

[13] Peter Kroes. Technological explanations: the relation between structure and function of technological objects. *Techne, 3 (3),* 1998. URL: http://scholar.lib.vt.edu/ejournals/SPT/v3n3/KROES.html. Tilgået 12.12.2017.

[14] *Lov om elektroniske signaturer.* 31. maj 2000. URL: https://www.retsinformation.dk/Forms/R0710.aspx?id=6193. Tilgået 8.3.2018.

[15] Carl Mitcham. *Thinking through Technology. The Path between Engineering and Philosophy.* The University of Chicago Press, 1994, Chicago.

[16] J. Müller, A. Remmen og P. Christensen. Hvad er teknologi? Kapitel 2 (s. 15-28) i *Samfundets teknologi, teknologiens samfund.* Systime, Herning, 1984.

[17] Roland Müller. The Notion of a Model: A historic overview. *Handbook of the Philosophy of Science. Volume 9: Philosophy of Technology and Engineering Sciences.*

[18] Satoshi Nakomoto. *Bitcoin: A Peer-to-Peer Electronic Cash System.* http://www.ildgroup.si/uploads/product/20/bitcoin.pdf

[19] Morten Storm Petersen. *Første MOCESbog - en beretning om digital signatur i Danmark.* 30. november 2016. Blog på version2.dk. URL: https://www.version2.dk/artikel/kronik-foerste-mocesbog-beretning-digital-signatur-danmark-944607. Tilgået 5.11.2017.

[20] Michael Polanyi. *Personal Knowledge: Towards a Post-Critical Philosophy.* University of Chicago Press, Chicago, 1962.

[21] National Institute of Standards and Technology. *Digital Signature Standard (DSS). PUB 186-4.* Juli 2013. URL: kan downloades fra https://csrc.nist.gov/publications.

[22] C. H. Gibbs-Smith. *Sir George Cayley's Aeronautics, 1796-1855.* London 1962.

[23] Marc Stevens et al. *The First collision for full SHA-1.* Crypto 2017. En pædagogiske forklaring af artiklens indhold kan læses på http://shattered.io (tilgået 5.11.2017).

[24] Walter G. Vincenti. *What Engineers Know and How They Know it. Analytical Studies from Aeronautical History.* The John Hopkins University Press, Baltimore and London, 1990.

[25] Marc J. de Vries. *Teaching about Technology. An Introduction to the Philosophy of Technology for Non-philosophers.* 2/E, Springer, 2016, Schweiz.

[26] A. Whitten, and J.D. Tygar. (1999). *Why Johnny can't encrypt: a usability evaluation of PGP 5.0.* Proceedings of the 8th USENIX Security Symposium, USENIX, Berkeley, CA.

[27] M. Wagenschein. Teaching to understand: On the Concept of the Exemplary in Teaching, in: Westbury et. al (Eds), *Teaching as a Reflective Practice. The German Didaktik Tradition*, Lawrence Erlbaum, 2000.