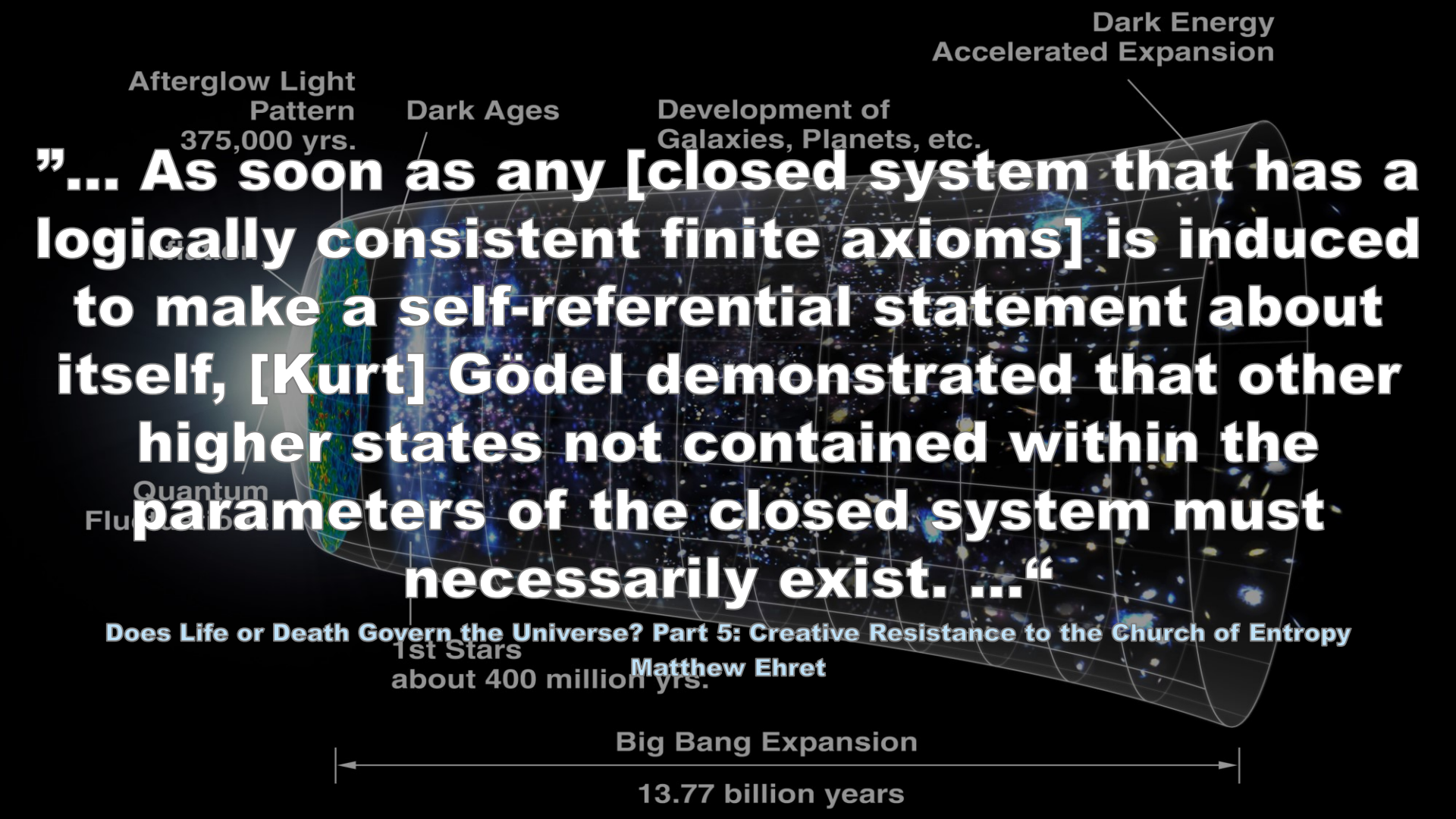


”... As soon as any [closed system that has a logically consistent finite axioms] is induced to make a self-referential statement about itself, [Kurt] Gödel demonstrated that other higher states not contained within the parameters of the closed system must necessarily exist. ...“

Does Life or Death Govern the Universe? Part 5: Creative Resistance to the Church of Entropy

Matthew Ehret

FormatE

Om kontrollfunktioner – när de behövs, vad som krävs för att bevara dem och när de kan gallras

eID och e-underskrifter i framtidens digitala förvaltning 16 november 2023

Riksarkivet

Vem är jag?

Juridisk och teknisk rådgivare och utredare på avdelningen för informationshantering (AFI)

- FormatE

Benjamin.Yousefi@Riksarkivet.SE

Har bland annat härjat:

- Utredningen för betrodda tjänster (expert)
- Samrådsgruppen (ledamot)
- ArkivE
- Elektroniska underskrifter
- Preforma
- PDF/A

Översikt

Riksarkivet

Vad jag ska prata om idag!

1. **Om FormatE och vägledningen**
2. **Om äkthet och äkthetsprövning**
3. **Om vad som krävs för att äkthetspröva en elektronisk handling**
   - Om induktiva och deduktiva metoder för äkthetsprövning
   - Materiel och metoder för att framställa elektroniska handlingar som kan äkthetsprövas
4. **Om vad som krävs för att bevara kontrollfunktioner**
   - Om bestyrkande

Riksarkivet

Om FormatE och vägledningen

Riksarkivet

Om FormatE och vägledningen

- Ett arbete som bedrivs inom FormatE
  - https://riksarkivet.se/FormatE
- Underlaget
  - *Förstudie om användning och hantering av underskrifter med elektroniska materiel och metoder* (2021-02-24) + remissvaren
  - Remissvaren av författningsförslagen (TeK och ArK)
- Dagens presentation ger en översikt av vägledningen
  - ~~Författningsförslag och författningskommentarer~~
  - Mer fokus på att *påvisa äkthet* än ”giltigheten” av underskrifter

Äkthet och äkthetsprövning

Riksarkivet

En äkta handling

En handling som kan bevisas ha omanipulerat härrört från den som är angiven som källan till handlingen

Riksarkivet

En äkta handling är per definition oavvislig

Det följer att, om en handling är äkta kan inte heller den som är angiven som källan till handlingen avvisa det faktumet, det vill säga att handlingen får en beskaffenhet av att vara *oavvislig*.

Äkthetsprövning

En metod för att bedöma äktheten hos en handling

– Är det bevisat att handlingen är äkta?

(Fundera över – Hur kan man bevisa ett påstående?)

Äkthetsprövning

Vad som krävs för att bevisa att en handling är äkta beror på *vilka materiel och metoder som används för att framställa handlingen*:

- **analoga [skriv- och tryck-] materiel och metoder**
- **digitaltekniska materiel och metoder**

Äkthetsprövning – analoga materiel och metoder

1. *En handling…*

- 12 kap. 3 § tryckfrihetsförordningen (1949:105)
  - Framställning i skrift eller bild [med **skriv- och tryck- materiel och metoder**]
    - ”Analog”
  - Upptagning som kan uppfattas endast med tekniska hjälpmedel
    - Analoga hjälpmedel
    - Elektroniska hjälpmedel
      - Analog elektronik
      - Digital elektronik

Äkthetsprövning – skriv- och tryck- materiel och metoder

2. … omanipulerat…

- Ursprungligt skick
- Ändringar på papper lämnar fysiska spår

Äkthetsprövning – skriv- och tryck- materiel och metoder

3. … härrört från den som är angiven som källan till handlingen.

- **En markering** som ger handlingen **särprägling**, till exempel med en egenhändig underskrift
  - men kan även vara
    - *initialer eller en pseudonym*
    - *en figur, ett kryss*
    - *bomärke, sigill eller stämplar*
  - *beroende av handlingens funktionella skick*

Äkthetsprövning – skriv- och tryck- materiel och metoder

Äkthetsprövning

- Visuella jämförelser
- Ytterst kriminaltekniska metoder

Äkthetsprövning – skriv- och tryck- materiel och metoder

Sammanfattning

- En **specifik person** har **unikt särpräglat** en handling som därefter förblir i **ursprungligt skick**
  - Äkthet mer än endast ”ursprungligt skick”
  - Måste alltså finnas en koppling till en specifik person
  - Jämför autenticitet
- Metod för äkthetsprövningen är en analys av ”särpräglingen”

Äkthetsprövning – digitaltekniska materiel och metoder

1. *En [elektronisk] handling…*

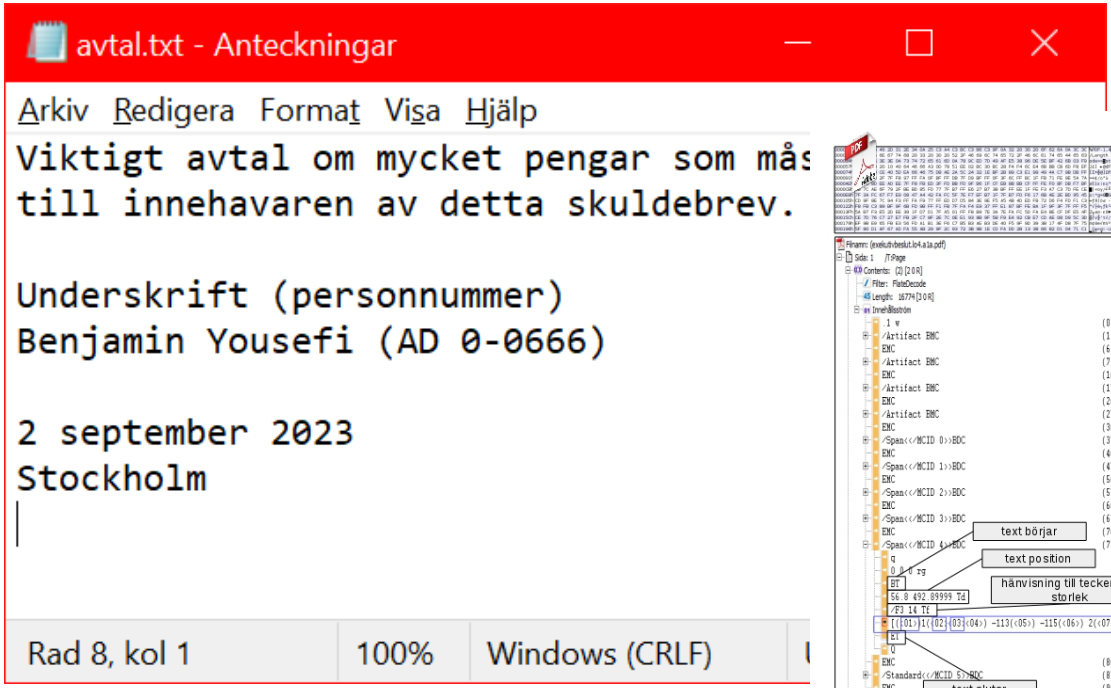
- 12 kap. 3 § tryckfrihetsförordningen (1949:105)
  - Framställt med [elektroniska] digitaltekniska materiel och metoder
- 14 kap. 1 § 2 brottsbalken (1962:700) om *urkunder*
  - Avgränsar begreppet handling till ett innehåll som endast kan läsas eller avlyssnas;
    - ett innehåll med form av text eller ljud som kommunicerar fakta som är av relevans i en rättslig angelägenhet
    - inte till exempel fotografier av föremål eller personer

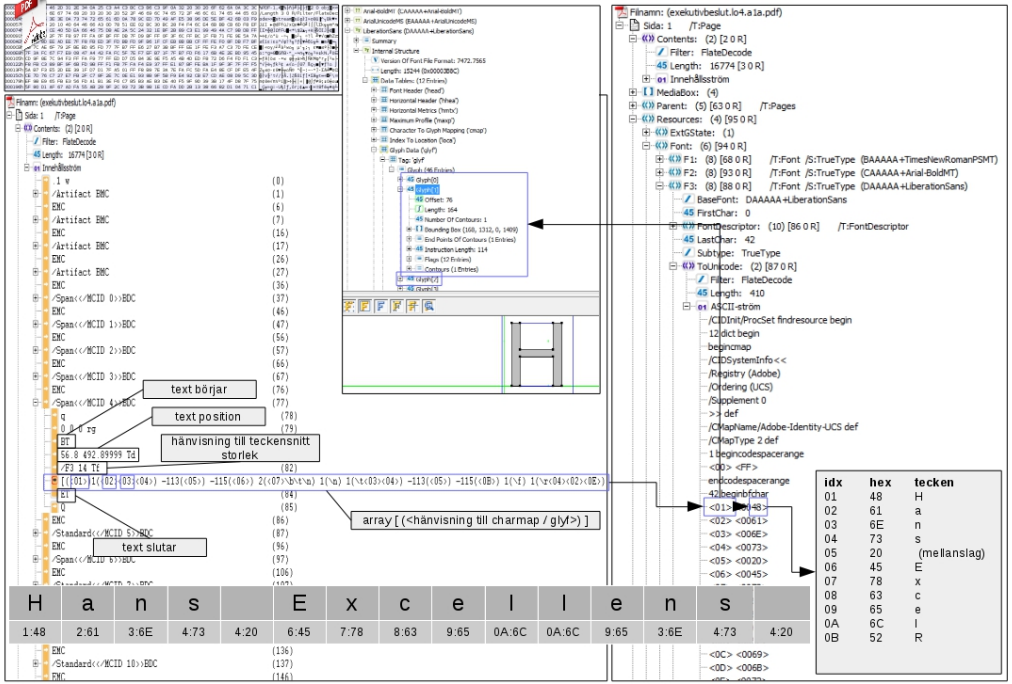
Äkthetsprövning – digitaltekniska materiel och metoder

2. … omanipulerat…

- Ändringar i elektroniska handlingar lämnar *nödvändigtvis inte* några fysiska eller digitala spår, i vart fall vanligtvis tillräckligt unika eller varaktiga spår (inte unikt särpräglat)
- **Super duper viktigt att förstå – *och kan inte betonas tillräckligt*,** att
  - *En och samma elektroniska handling kan framställas, användas och hanteras – kopieras och ändras – av ett obegränsat antal personer, ett obegränsat antal gånger utan att uppvisa något tecken på att det har skett*.
  - En person kan därför med **goda skäl avvisa** ett påstående om att de är källan till handlingen

Äkthetsprövning – digitaltekniska materiel och metoder





Riksarkivet

Äkthetsprövning – digitaltekniska materiel och metoder

2. … omanipulerat…

- ”Skalskydd”, till exempel program för granskning och loggning, behörighetskontroller, operativsystem, hårdvaruskydd – ”systemberoende åtgärder”
- Det kan finnas kopior av handlingarna, dokumentation, rutiner och regler för att använda och hantera elektroniska handlingar, till exempel i ett ”verksamhetssystem” eller ”e-arkiv”
  - Det kan vara lättare eller svårare att manipulera men det är fortfarande möjligt med rätt behörighet eller insatser, eller på grund av korruption
- Kräver ”yttre legitimitet” – Det går inte att validera sig själv.

Äkthetsprövning – digitaltekniska materiel och metoder

4. *… härrört från den som är angiven som källan till handlingen.*

- Angivna källor i elektroniska handlingar är påståenden och kan inte spåras tillbaka till en specifik fysisk och juridisk person endast till specifika *användare* (t.ex. ett användarkonto)
  - Anonyma
  - Pseudonymer

Äkthetsprövning – digitaltekniska materiel och metoder

Sammanfattning

- Det kan inte förutsättas att en elektronisk handling har ett innehåll som framställts av den som är angiven som källan

Slutsats

- En person kan med **mycket goda skäl avvisa** ett påstående om att de är källan till en elektronisk handling.

Vad som krävs för att äkthetspröva en elektronisk handling

Riksarkivet

Vad som krävs för att äkthetspröva en elektronisk handling

Teknikneutrala funktionella krav i svensk och unions- rätt

1. **koppla identitetsuppgifter** för en specifik fysisk eller juridisk person
   - personuppgifter eller organisationsnummer till en elektronisk handling som representerar personen (**elektronisk identitetshandling**), till exempel ett certifikat eller e-legitimation,
   - gällande rätt uppställer inget hinder mot att en *fysisk persons underskrift* kan representeras med ett falskt eller fingerat namn (pseudonym),
2. **koppla den elektroniska identiteten till ett innehåll**, och
3. **kontrollera att innehållet inte har förändrats** sedan personen framställt det (ursprungligt skick)

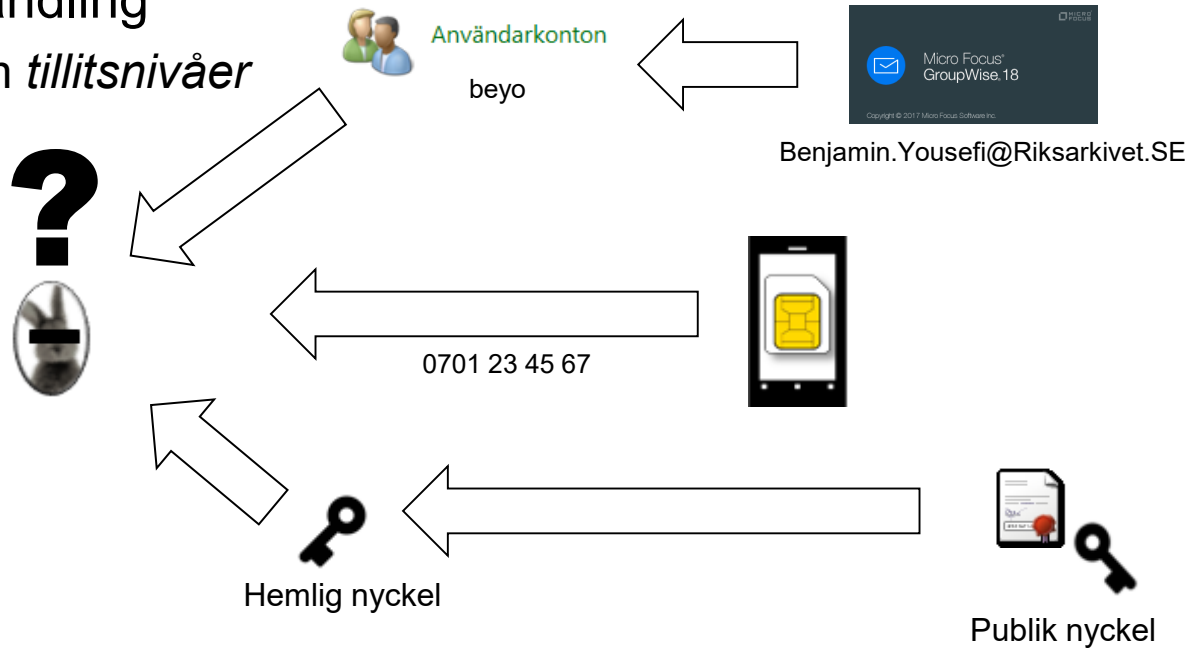
Rättsliga krav i svensk rättspraxis

4. Ingen **obehörig användning** av den elektroniska identitetshandlingen

Vad som krävs för att äkthetspröva en elektronisk handling – P1

Att koppla en identitet till en elektronisk identitet (identifiering)

- Vad som för olika krav krävs för att koppla en person till en elektronisk identitetshandling
  - Rättsligt reglerat som *tillitsnivåer*
  - I FormatE
    - en del av tillitsmodeller



Riksarkivet

Vad som krävs för att äkthetspröva en elektronisk handling – P1

Tillitsnivåerna för elektronisk identifiering			
Svensk rätt	Nivå Unionsrätt	*Exempel på krav på* identifiering	autentisering
1	Elektroniska underskrifter	• Ingen	• Användarnamn eller e-post och lösenord
2			• Tvåfaktorsautentisering
	Låg	• Kodkuvert till folkbokföringsadress.	• Engångslösenord från dosa eller mobiltelefon
3	Väsentlig	• Samma krav som för utfärdandet av nationell legitimationshandling • Kan ske på distans om utfärdaren tidigare har identifierat personen, till exempel vid anställning eller öppnande av ett bankkonto.	• Tvåfaktorsautentisering • Mjuka certifikat
4		• Personligt besök för förnyelse var femte år	• Tvåfaktorsautentisering • Hårda certifikat
	Hög	• Personligt besök vid utfärdande • Nationell legitimationshandling	

Vad som krävs för att äkthetspröva en elektronisk handling – P2-3

Att koppla den elektroniska identiteten till ett innehåll i ursprungligt skick

- En äkthetsprövning kan vara elektronisk och automatisk
  - och kan *som sådan* ha en **rättseffekt** och uppfyllas på olika sätt.
- En framställd elektronisk handling har **rättseffekt**
  - och kan *som sådan* användas [ligga till underlag] för en äkthetsprövning.

Vad som krävs för att äkthetspröva en elektronisk handling – P2-3

Elektroniska och automatiska äkthetsprövningar

- *Måste vara ett tekniskt förfarande*
- Matematiska beräkningar kan påvisa
  1. att ett innehåll är i ursprungligt skick,
  2. att innehållet har varit i ursprungligt skick sedan en viss specifik tidpunkt, och
  3. att en person ska ha haft kännedom om det.
- Det blir därför inte längre möjligt för en person **att utan goda skäl** avvisa att de är källan till handlingen

Vad som krävs för att äkthetspröva en elektronisk handling – P2-3

Elektroniska och automatiska äkthetsprövningar

- Enkla förfaranden
  - Olika tekniska metoder, till exempel
    - lösenordskyddat dokument
    - handlingar framställda från ett användarkonto
  - Inte nödvändigtvis samma matematiska tillförlitlighet som:
- Avancerade förfaranden
  - Vanligtvis digitala signaturer
- Kvalificerade förfaranden
  - Vanligtvis avancerade + striktare administrativa och säkerhets- krav

Vad som krävs för att äkthetspröva en elektronisk handling – P2-3

Alla elektroniska handlingar har alltid bevisverkan

- Både i svensk och unions- rätt

Inga elektroniska handlingar får förvägras rättsverkan

- *Enda giltiga grunden för att förvägra: formkrav*
- Äkthetsprövningen måste alltså inte vara
  - Kvalificerad
    - Äkthetsprövningen kan göras med enkla och avancerade förfaranden
    - Kvalificerade förfaranden aktualiserar dock presumtionsregler
  - Automatisk

Om induktiva och deduktiva metoder för äkthetsprövning

Riksarkivet

Om induktiva och deduktiva metoder för äkthetsprövning

Induktiva metoder (svensk rättstillämpning)

- Manuell [mänsklig] äkthetsprövning (sannolikhetsprövning)
- Vad som krävs för olika fall beror på omständigheterna i det enskilda fallet – en bedömningsfråga
  - Beviskrav, bevisbörda
  - Vad som yrkats, anförda rättsgrunder, åberopat bevis
  - Val av lämpliga materiel och metoder
    - Elektronisk identitetshandling, till exempel BankID, FrejaID
  - En god arkivvård
    - Dokumentation av rutiner för framställning av elektroniska handlingar, deras hantering och bevarande

Om induktiva och deduktiva metoder för äkthetsprövning

Induktiva metoder (svensk rättstillämpning)

- Risk för att lika fall döms olika

Om induktiva och deduktiva metoder för äkthetsprövning

Deduktiva metoder

- Automatisk äkthetsprövning (matematiskt prövning)
  - *Utför* äkthetsprövningen
- Syftet med deduktiva metoder är att det kan *förutsättas* att
  - källan till den elektronisk handling
    - är den som utges
    - är den som har framställt den elektroniska handlingen, och
    - att handlingen är i ursprungligt skick
- Det vill säga, ingen bedömning – möjligtvis med ett undantag
  - Pröva invändningar om att handlingen är framställd av obehörig person

Om induktiva och deduktiva metoder för äkthetsprövning

Gemensamt för båda metoderna: **spårbarhet i tre led:**

1. Påvisa att den elektroniska handlingen är i **ursprungligt skick**
2. Påvisa att angiven **specifik person** är källan till handlingen
3. Påvisa att **den personen har framställt** handlingen

- Vad som skiljer metoderna åt är den konkreta kopplingen mellan punkt 1 och 2, vilket alltså är antingen deduktiv eller induktiv.
  - P. 1-2 avser alltså de teknikneutrala funktionella kraven 1-3 i unionsrätt och svensk rätt
  - P. 3 avser svensk rättspraxis om [o]behörig användning

Om induktiva och deduktiva metoder för äkthetsprövning

Induktiva metoder (svensk rättstillämpning)

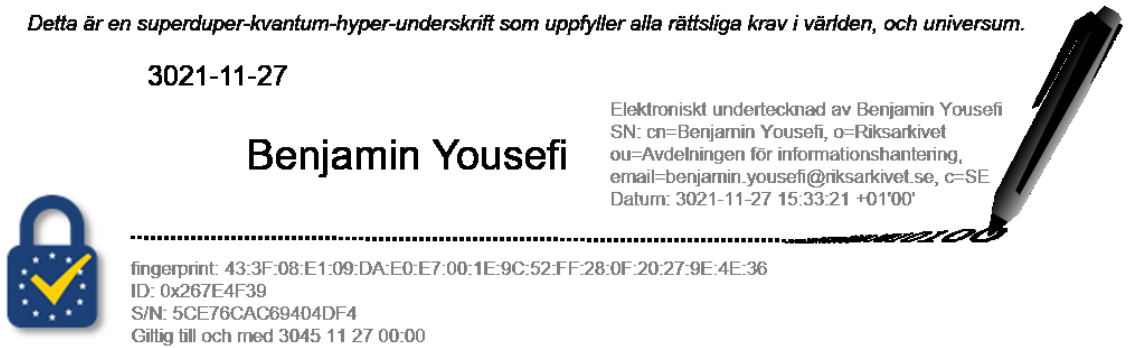
- Det är möjligt att äkthetspröva en elektronisk handling med ”tryckta uppgifter”
  - Till exempel, kopior av handlingarna, dokumentation, rutiner och regler…

Riksarkivet

Om induktiva och deduktiva metoder för äkthetsprövning

Deduktiva metoder (svensk och unions- rätt)

- Det är **inte** möjligt att äkthetspröva en elektronisk handling med ”tryckta uppgifter”
  - Uppmärksamma unionsrättens rättspraxis



Riksarkivet

Om induktiva och deduktiva metoder för äkthetsprövning

Induktiva metoder

- För *vissa typer* av elektroniska handlingar men inte för alla
  - **även om** de kan *tekniskt sätt* manipuleras eller inte direkt kopplas till en specifik person
  - Behöver generella digitaltekniska materiel och metoder

Deduktiva metoder

- För *alla typer* av elektroniska handlingar
  - men alltså inte nödvändigt för sådana som kan äkthetsprövas med induktiva materiel och metoder
  - Kräver speciella digitaltekniska materiel och metoder

Om induktiva och deduktiva metoder för äkthetsprövning – deduktiva metoder

För olika fall

- Rättsliga krav
  - Elektroniska urkunder och elektroniska dokument
- Rättsliga behov
  - Avtal, protokoll och liknande handlingstyper
  - Vidimering av innehåll, till exempel efter konverteringar
  - Handlingar som ska överlämnas till någon annan
    1. Internationellt eller nationellt
    2. Medborgare eller andra offentliga verksamheter
    3. Arkivmyndigheter eller annan med motsvarande ansvar

Om induktiva och deduktiva metoder för äkthetsprövning – deduktiva metoder

För olika fall

- Säkerhetsbehov
  - Hur vet jag vem det är jag kommunicerar med?
    - Till exempel, över e-post, nedladdningar av program
    - ”AI” presenterar nya former för bedrägerier – t.ex. för bilder och videon

Om induktiva och deduktiva metoder för äkthetsprövning – deduktiva metoder

För olika fall

1. Vilken rättslig betydelse har äktheten?
    1. Handlingens funktionella skick – autentisering eller äkthetsprövning
2. Vilken betydelse för arkivlagens ändamål har
    1. Handlingen
    2. Äktheten

Om induktiva och deduktiva metoder för äkthetsprövning

Mycket skillnad, så viktigt, mellan

- att en person ska kunna identifieras *med kontrollfunktionen*, och
- att en person *har identifierats* med en e-legitimation.
    - Elektronisk identifiering kan påvisa endast vem som har haft åtkomst till eller framställt en elektronisk handling men det finns inget som hindrar att handlingen därefter kan ändras utan att lämna några spår på att det har skett.

- Materiel och metoder för att framställa elektroniska handlingar som kan äkthetsprövas

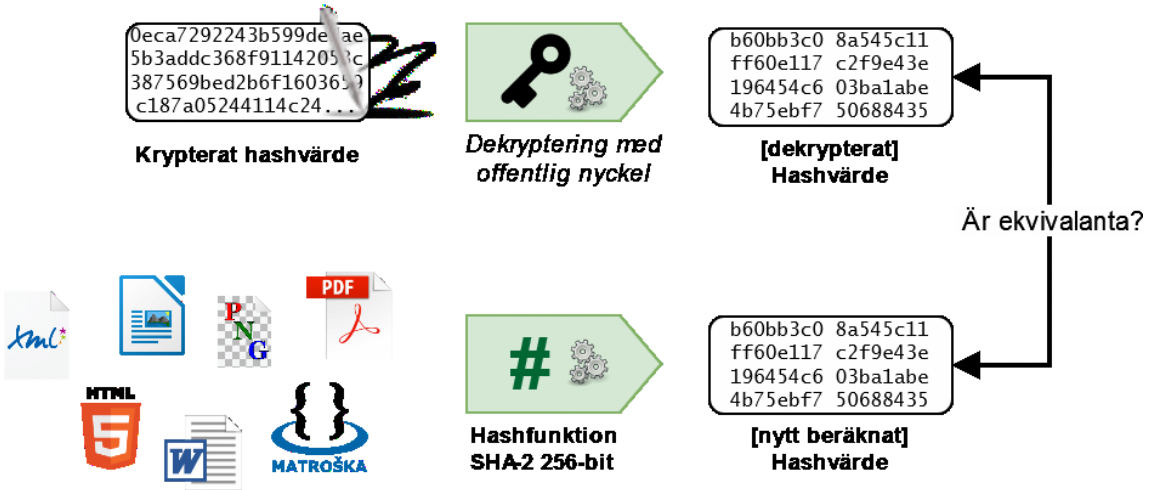
Materiel och metoder för att framställa elektroniska handlingar som kan äkthetsprövas

Kontrollfunktioner

- Fångar de gemensamma kraven i svensk och unions- rätt
  - Teknikspecifika metoder för att automatiskt äkthetspröva en elektronisk handling
- Samma grundläggande mekanism – *krypterade hashvärden*
  - Kryptografiska hashfunktioner
    - Påvisar att informationen är unik
    - Kontrollsummor är inte kryptografiska hashfunktioner
  - Asymmetriska krypteringsfunktioner
    - Påvisar att endast en *specifik användaren* kan ha krypterat hashvärdet

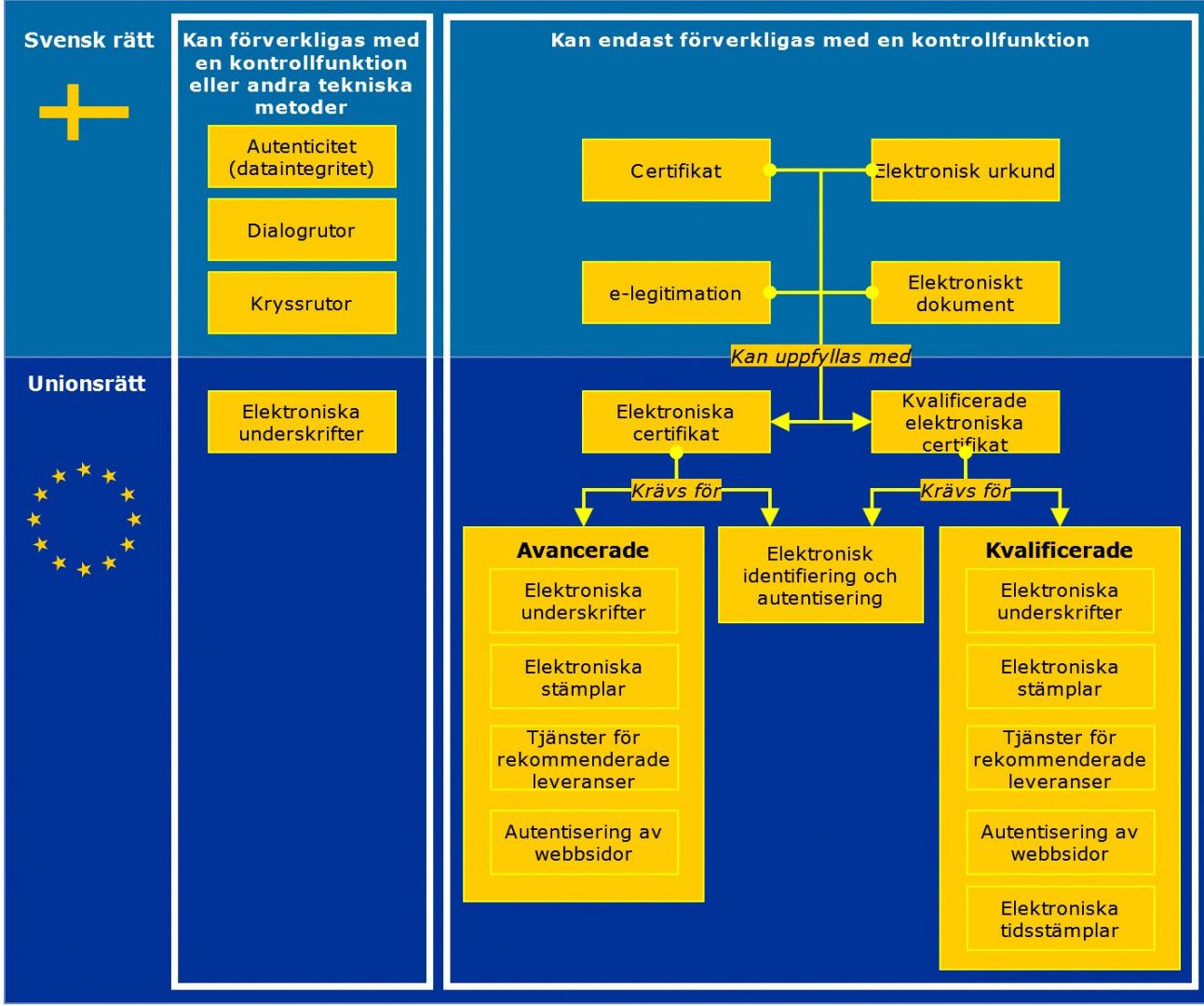
Materiel och metoder för att framställa elektroniska handlingar som kan äkthetsprövas

- Ett digitalt certifikat för hemlig nyckel
  - Används bl.a. för att implementera en digital signatur
- Ett digitalt certifikat för en publik nyckel
  - Används bl.a. för att kontrollera en digital signatur



Riksarkivet

Typer av kontroll-funktioner



Riksarkivet

Materiel och metoder för att framställa elektroniska handlingar som kan äkthetsprövas

- Digital signatur = krypterat hashvärde
- En kontrollfunktion förutsätter en digital signatur men är **inte** detsamma som en digital signatur
  - en kontrollfunktion är mer än att endast beräkna ett hashvärde, kryptera och dekryptera det.
- De rättsliga kraven förutsätter därutöver att
  1. det digitala certifikatet kan bevisas tillhöra en specifik fysisk eller juridisk person
     - (uppfylls med tillitsmodeller)
  2. att endast den personen har kunnat förfoga över certifikatet.
     - (uppfylls med anordningar)

Materiel och metoder för att framställa elektroniska handlingar som kan äkthetsprövas

Anordningar – tekniska skick och hjälpmedel för

- elektronisk identifiering
  - (t.ex. med digitala certifikat, vilka måste ha kontrollfunktioner)
- att framställa kontrollfunktioner

Tillitsmodeller

- Metod för att koppla en anordning till en specifik person (identifiering)
  - (t.ex. tillitsnivåer)

Materiel och metoder för att framställa elektroniska handlingar som kan äkthetsprövas

Anordningar

- En anordning är det tekniska hjälpmedlet tillsammans med ett eller flera program som ska garantera att endast den som har tilldelats anordningen ska kunna använda och hantera den (användaren).
  - Mobiltelefon (BankID)
  - ID-kort med ”chip”
  - Speciell ”dosa”
  - En molntjänst

Materiel och metoder för att framställa elektroniska handlingar som kan äkthetsprövas

Anordningar i centraliserade och decentraliserade system

System	Centraliserade	Decentraliserade
Slutna	Anordningen utfärdas av en aktör till specifika personer som endast kan använda anordningen mot bestämda parter, till exempel • en svensk myndighets egna lösningar för svenska medborgare för att utföra vissa rättshandlingar endast hos myndigheten eller andra myndigheter • ett banks användarkonto som vem som helst kan ansluta sig till men endast för att utföra rättshandlingar hos banken eller de som har avtal med banken.	Decentraliserade system kan per definition inte vara slutna.
Öppna	Anordningen utfärdas av en specifik aktör men det är öppet för allmänheten att ansluta sig till och använda eller förlita sig på den, till exempel BankID, FrejaID.	Vem som helst kan utfärda anordningen och vem som helst kan ansluta sig till och använda eller förlita sig på den, till exempel kryptotillgångar, OpenPGP PKI.

Materiel och metoder för att framställa elektroniska handlingar som kan äkthetsprövas

Tillitsmodeller

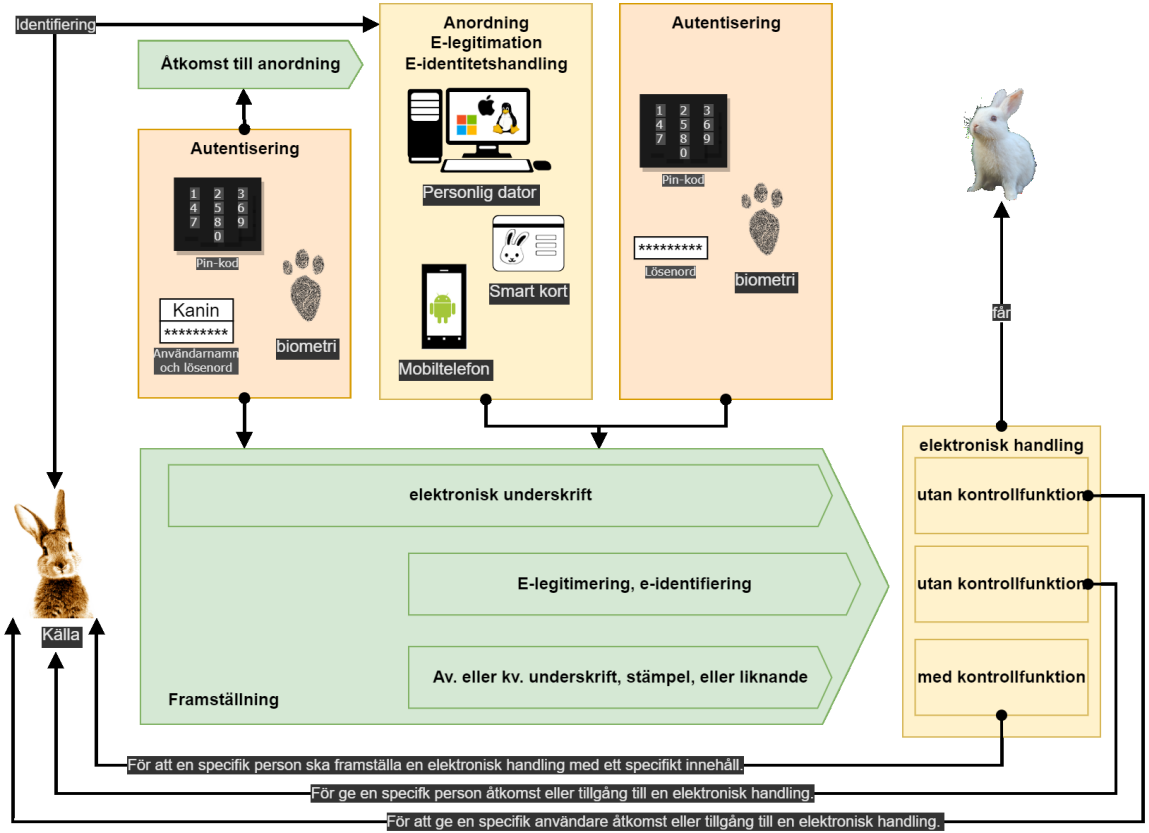
- Att fastställa att en fysisk eller juridisk person är den som den utger sig för att vara och koppla det till anordningen.
  - Tillitsnivåer
- Att den som ansvarar för bedömningen i första ledet är pålitlig.
  - T.ex. betrodd tjänstetillhandahållare
  - Hot – Vem har gett ut certifikatet?
- Att resultatet av bedömningen kan i sig visas vara äkta
  - Det vill säga, en äkthetsprövning av ”certifikatet”

Materiel och metoder för att framställa elektroniska handlingar som kan äkthetsprövas

Tillitsmodeller

Exempel	Ingen tillitsmodell	Centraliserad tillitsmodell	Decentraliserad tillitsmodell
Centraliserade system	En e-posttjänst som tillåter vem som helst att skapa ett användarkonto.	Ett verksamhetssystem med en egen X.509 PKI.	Verksamhetssystem eller e-posttjänst som använder OpenPGP PKI, eller e-posttjänst som inte tillhandahåller OpenPGP men vars användare kan själva använda OpenPGP för sin kommunikation.
Decentraliserade system	Kryptotillgång som tillåter vem som helst att skapa en digital plånbok.	Kryptotillgång som använder X.509 PKI för att koppla digitala plånböcker till personer.	Kryptotillgång som använder OpenPGP PKI för att koppla digitala plånböcker till personer.

Materiel och metoder för att framställa elektroniska handlingar som kan äkthetsprövas



Riksarkivet

Om vad som krävs för att bevara kontrollfunktioner

Riksarkivet

Om vad som krävs för att bevara kontrollfunktioner

- Tillräckligt att veta att en kontrollfunktion kan inte ändras utan att förlora sitt funktionella skick (kunna äkthetspröva)
  - Till exempel när innehållet ändras, eller certifikatet går ut
  - En ny kontrollfunktion måste framställas om det uppstår ett behov att ändra innehållet eller kontrollfunktionen
- Arbetsflöde, i vilket skede framställs kontrollfunktionen, till exempel
  - Av handlingen som XML
  - Av handlingen som PDF
  - Säg hej till Högsta domstolens dom (2023-06-02) i mål Ö 327-23

Om vad som krävs för att bevara kontrollfunktioner

Bestyrkande (i)

- Endast av innehåll, som avskrift eller kopia (vidimering)
- Innehåll och kontrollfunktion

Bestyrkande av innehåll och kontrollfunktion (ii)

- Oberoende av validering – AdES-familjen
  - Bestyrkande av allt; valideringen ska kunna återupprepas
- Efter validering – SVT (Digg)
  - Ett valideringsintyg av valideringen (vidimering?)
- Rekursivt bestyrkande av kontrollfunktioner (iii)
  - Bestyrka ett bestyrkande (se ii)

Om vad som krävs för att bevara kontrollfunktioner

- Innan kontrollfunktionen förfaller – bestyrka den
  - Repetera så länge äkthetsprövningen har betydelse
- Låta förfalla och tillämpa en induktiv metod
- Digg:s valideringstjänst
  - https://www.digg.se/digitala-tjanster/e-underskrift/valideringstjanst

Slut på kärlek

Riksarkivet