

Afterglow Light  
Pattern  
375,000 yrs.

Dark Ages

Development of  
Galaxies, Planets, etc.

Dark Energy  
Accelerated Expansion

**”... 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. ...“**

Quantum  
Fluctuations

**Does Life or Death Govern the Universe? Part 5: Creative Resistance to the Church of Entropy**  
1st Stars  
Matthew Ehret  
about 400 million yrs.

Big Bang Expansion

13.77 billion years

- 
- 
- 
- 
- 
- 
- 

# FormatE

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

*Registratordagarna 4 oktober 2023*



Riksarkivet

# Vem är jag?

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



[Benjamin.Yousefi@Riksarkivet.SE](mailto:Benjamin.Yousefi@Riksarkivet.SE)

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

- 
- 
- 
- 
- 
- 
- 

# Översikt

# 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 FormatE och vägledningen**
- 
- 
- 
- 
- 
-

# 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~~

- 
- Äkthet och äkthetsprövning
- 
- 
- 
- 
- 
-



# En äkta handling

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

# 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 skulle få 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 **särpräglning**, 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, eller i vart fall vanligtvis tillräckligt unika 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

avtal.txt - Anteckningar

Arkiv Redigera Format Visa Hjälp

Viktigt avtal om mycket pengar som mås till innehavaren av detta skuldebrev.

Underskrift (personnummer)  
Benjamin Yousefi (AD 0-0666)

2 september 2023  
Stockholm

Rad 8, kol 1

100%

Windows (CRLF)



Riksarkivet

The screenshot displays three overlapping windows from a PDF analysis tool. The left window shows the document's internal structure with a tree view of objects. The middle window shows a detailed view of a glyph, specifically the letter 'H', with its bounding box and various metrics. The right window shows the font's internal structure, including the font dictionary and the glyph set. A table at the bottom right lists the glyph names and their corresponding hex codes and character codes.

idx	hex	tecken
01	48	H
02	61	a
03	6E	n
04	73	s
05	20	(melanslag)
06	45	E
07	78	x
08	63	c
09	65	e
0A	6C	l
0B	52	l

# Äkthetsprövning – digitaltekniska materiel och metoder

## 2. ... omanipulerat...

- 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

# 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*
  - 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
- 
- 
-



# 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 person* 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)

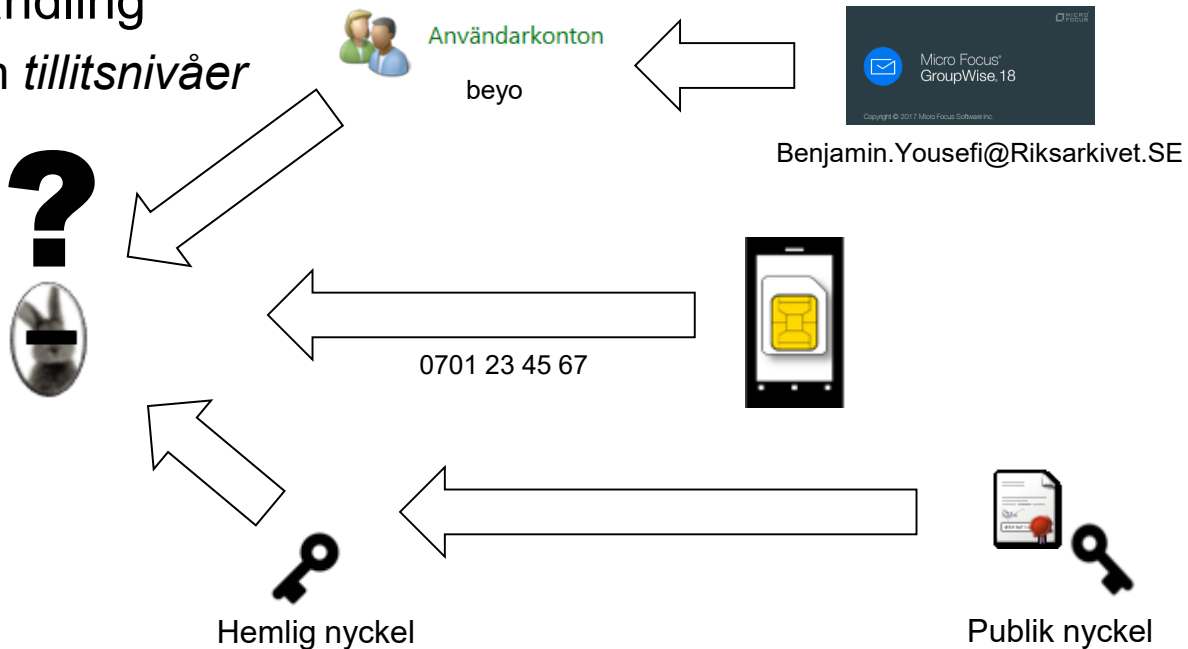
## Rättsliga krav i svensk rättspraxis

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*
  - Tillitsmodeller



# 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

## 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

## Elektroniska och automatiska äkthetsprövningar

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

# Vad som krävs för att äkthetspröva en elektronisk handling

## **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*
- Äkthetsprövning kan göras med enkla och avancerade förfaranden
- Äkthetsprövning med kvalificerade förfaranden aktualiserar presumtionsregler

- 
- Om induktiva och deduktiva metoder för
- äkthetsprövning
- 
- 
- 
-

# 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
  - En god arkivvård
    - Dokumentation av rutiner för framställning av elektroniska handlingar, deras hantering och bevarande



# 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
    - Kan invända med 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 unionsrätten och svensk rätt)
  - (p. 3 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...

*Detta är en superduper-quantum-hyper-underskrift som uppfyller alla rättsliga krav i världen, och universum.*

3021-11-27

Benjamin Yousefi

Elektroniskt undertecknad av Benjamin Yousefi  
SN: cn=Benjamin Yousefi, o=Riksarkivet  
ou=Avdelningen för informationshantering,  
email=benjamin.yousefi@riksarkivet.se, c=SE  
Datum: 3021-11-27 15:33:21 +01'00'



fingerprint: 43:3F:08:E1:09:DA:E0:E7:00:1E:9C:52:FF:28:0F:20:27:9E:4E:36  
ID: 0x267E4F39  
S/N: 5CE76CAC69404DF4  
Giltig till och med 3045 11 27 00:00

# 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

*Detta är en superduper-kvantum-hyper-underskrift som uppfyller alla rättsliga krav i världen, och universum.*

3021-11-27

Benjamin Yousefi

Elektroniskt undertecknad av Benjamin Yousefi  
SN: cn=Benjamin Yousefi, o=Riksarkivet  
ou=Avdeleningen för informationshantering,  
email=benjamin.yousefi@riksarkivet.se, c=SE  
Datum: 3021-11-27 15:33:21 +01'00'



-----  
fingerprint: 43:3F:08:E1:09:DA:E0:E7:00:1E:9C:52:FF:28:0F:20:27:9E:4E:36  
ID: 0x267E4F39  
S/N: 5CE76CAC69404DF4  
Giltig till och med 3045 11 27 00:00

# 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

## Deduktiva metoder

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

# Om induktiva och deduktiva metoder för äkthetsprövning

## För olika fall (när välja)

- Rättsliga krav på deduktiva metoder
  - Elektroniska urkunder
- Rättsliga behov
  - Avtal och liknande handlingstyper
- 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

## För olika fall (när bevara, gallra)

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

Rättsligt krav	Teknisk metod	Tillitsnivå	Resultat	Funktionellt skick
Elektronisk underskrift	Användarnamn och lösenord	1 eller högre	Elektronisk handling	Autentisering
E-legitimation	Digitala certifikat	3 eller högre	Elektronisk handling	Autentisering
Avancerad elektronisk underskrift, stämplar	Digitala certifikat	3 eller högre	Elektronisk handling med kontrollfunktion	Autentisering? Äkthetsprövning?
Kvalificerad elektronisk underskrift, stämplar	Digitala certifikat	4	Elektronisk handling med kontrollfunktion	Autentisering? Äkthetsprövning?



- 
- 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

# Typer av kontrollfunktioner

Svensk rätt



Kan förverkligas med en kontrollfunktion eller andra tekniska metoder

Autenticitet (dataintegritet)

Dialogrutor

Kryssrutor

Unionsrätt



Elektroniska underskrifter

Kan endast förverkligas med en kontrollfunktion

Certifikat

Elektronisk urkund

e-legitimation

Elektroniskt dokument

Kan uppfyllas med

Elektroniska certifikat

Kvalificerade elektroniska certifikat

Krävs för

Krävs för

**Avancerade**

Elektroniska underskrifter

Elektroniska stämplrar

Tjänster för rekommenderade leveranser

Autentisering av webbsidor

Elektronisk identifiering och autentisering

**Kvalificerade**

Elektroniska underskrifter

Elektroniska stämplrar

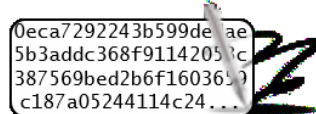
Tjänster för rekommenderade leveranser

Autentisering av webbsidor

Elektroniska tidsstämplrar

# 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

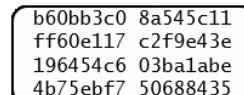


```
0eca7292243b599de1ae  
5b3addc368f91142050c  
387569bed2b6f1603650  
c187a05244114c24...
```

Krypterat hashvärde



Dekryptering med  
offentlig nyckel



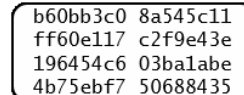
```
b60bb3c0 8a545c11  
ff60e117 c2f9e43e  
196454c6 03ba1abe  
4b75ebf7 50688435
```

[dekrypterat]  
Hashvärde

Är ekvivalanta?



Hashfunktion  
SHA-2 256-bit



```
b60bb3c0 8a545c11  
ff60e117 c2f9e43e  
196454c6 03ba1abe  
4b75ebf7 50688435
```

[nytt beräknat]  
Hashvärde

# 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

## Viktigt! Observera! Viktigt!

- Innehållet i en elektronisk handling *är formatet*
  - Samma innehåll kan ibland representeras med olika format
  - **Det går inte att bevara ett innehåll om inte formatet bevaras**
- Kryptografiska hashvärden beräknas utifrån formaten (binär data)

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

- Den fluffiga kaninen skuttade över en annan kanin...

<b>Teckenkodning</b>	<b>SHA-2 256</b>
<b>UTF-8</b>	c2620c1cf58d0764a398f74faf0c665e1a948c9543dfc6c0a7f38531b49bbf60
<b>ISO 8859-1 (Latin-1)</b>	2de40d3e179bacc6437a7af59556d17ff5708d365a7c592394a85d64ed056373

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

**Anordningar** – tekniska skick och hjälpmedel för att framställa

- Elektroniska identitetshandlingar
  - (t.ex. med digitala certifikat, vilka måste ha kontrollfunktioner)
- Kontrollfunktioner

## **Tillitsmodeller**

- Metod för att koppla en anordning till en specifik person (identifiering)
  - bl.a. 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

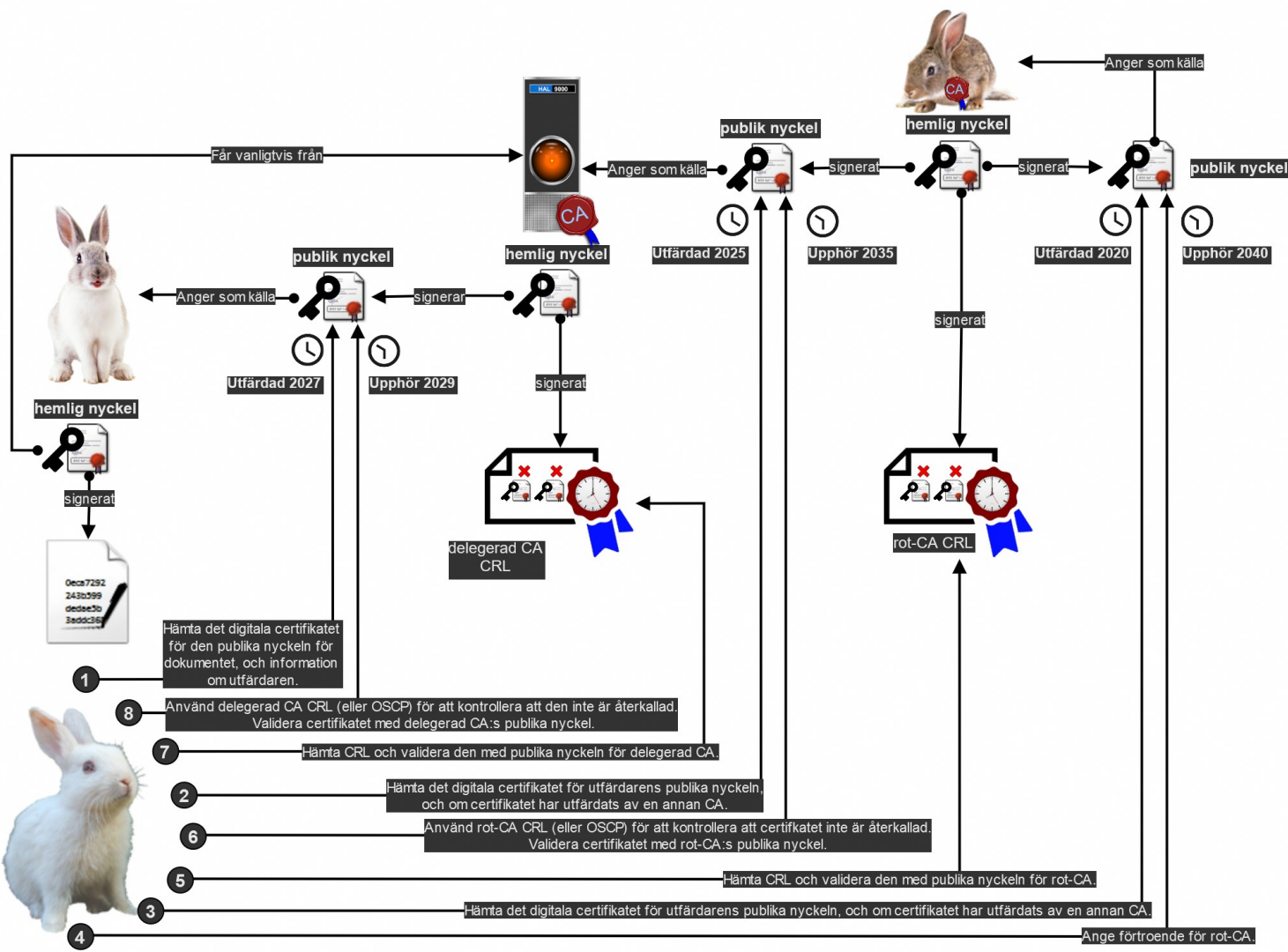
System	Centraliserade	Decentraliserade
Slutna	<p>Anordningen utfärdas av en aktör till specifika personer som endast kan använda anordningen mot bestämda parter, till exempel</p> <ul style="list-style-type: none"><li>• en svensk myndighets egna lösningar för svenska medborgare för att utföra vissa rättshandlingar endast hos myndigheten eller andra myndigheter</li><li>• 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.</li></ul>	<p>Decentraliserade system kan per definition inte vara slutna.</p>
Öppna	<p>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.</p>	<p>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.</p>

# 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
  - = digitala certifikat för hemliga och publika nycklar
- Att den som ansvarar för bedömningen i första ledet är pålitlig.
  - Hotbild – Vem har gett ut certifikatet?
- Att bedömningen kan i sig visas vara äkta
  - Digitala certifikat för publika nycklar behöver kontrollfunktioner
    - Certifikatutfärdare och introduktörer

# Exempel



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

## Tillitsmodeller

Exempel	Ingen tillitsmodell	Centraliserad tillitsmodell	Decentraliserad tillitsmodell
<b>Centraliserade system</b>	En e-posttjänst som tillåter vem som helst att skapa ett användarkonto.	Ett verksamhetssystem med en egen X.509 PKI.	Verksamhetssystem som använder OpenPGP PKI.
<b>Decentraliserade system</b>	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

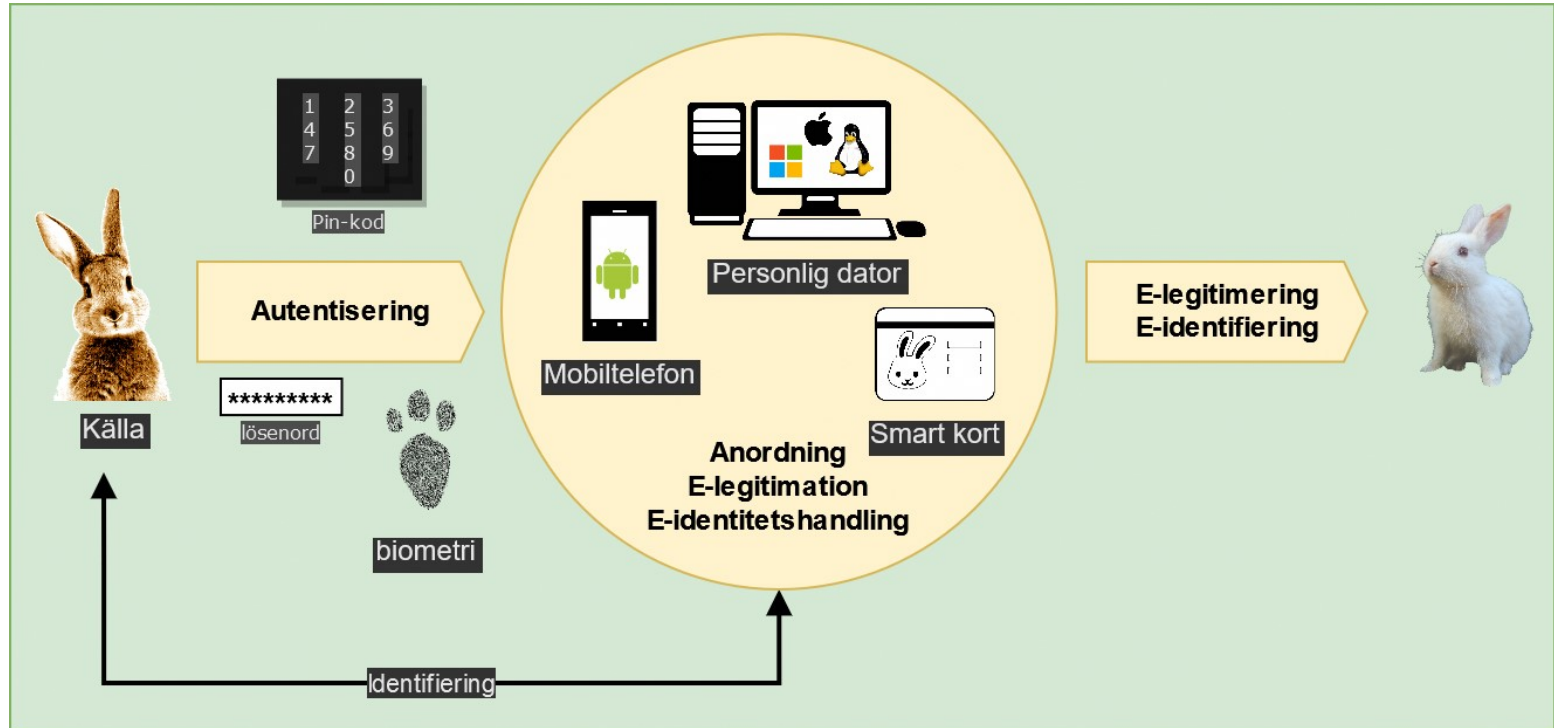
Tillitsnivåerna för elektronisk identifiering			
Nivå		Exempel på krav på	
Svensk rätt	Unionsrätt	identifiering	autentisering
1	Elektroniska underskrifter	<ul style="list-style-type: none"> <li>Ingen</li> </ul>	<ul style="list-style-type: none"> <li>Användarnamn eller e-post och lösenord</li> </ul>
2	Låg	<ul style="list-style-type: none"> <li>Kodkuvert till folkbokföringsadress.</li> </ul>	<ul style="list-style-type: none"> <li>Tvåfaktorsautentisering</li> <li>Engångslösenord från dosa eller mobiltelefon</li> </ul>
3	Väsentlig	<ul style="list-style-type: none"> <li>Samma krav som för utfärdandet av nationell legitimationshandling</li> <li>Kan ske på distans om utfärdaren tidigare har identifierat personen, till exempel vid anställning eller öppnande av ett bankkonto.</li> </ul>	<ul style="list-style-type: none"> <li>Tvåfaktorsautentisering</li> <li>Mjuka certifikat</li> </ul>
4	Hög	<ul style="list-style-type: none"> <li>Personligt besök för förnyelse var femte år</li> <li>Personligt besök vid utfärdande</li> <li>Nationell legitimationshandling</li> </ul>	<ul style="list-style-type: none"> <li>Tvåfaktorsautentisering</li> <li>Hårda certifikat</li> </ul>

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

Hur förhåller sig autentisering, identifiering, och e-legitimation till kontrollfunktioner?

Term	Begrepp
<i>Anordning</i> <i>Elektronisk legitimation</i> <i>Elektronisk identitetshandling</i>	<ul style="list-style-type: none"><li>• Format, program (tekniska skicket) och, eller det tekniska hjälpmedlet</li></ul>
<i>Autentisering</i> <i>Elektronisk legitimering</i> <i>Elektronisk identifiering</i>	<ul style="list-style-type: none"><li>• Åtkomst till en anordning eller tjänst</li><li>• Framställa en elektronisk handling med eller utan kontrollfunktion</li></ul>
<i>Identifiering</i>	<ul style="list-style-type: none"><li>• Att koppla en person till en anordningen</li><li>• Tillitsnivåer</li></ul>
<i>Auktorisering</i>	<ul style="list-style-type: none"><li>• Vad får man göra eller inte göra med anordningen, t.ex. framställa kontrollfunktioner</li></ul>

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





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

## **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 kan ändras utan att lämna några spår på att det har skett.

- 
- Om vad som krävs för att bevara
- kontrollfunktioner
- 
- 
- 
-

# 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

# Om vad som krävs för att bevara kontrollfunktioner

- Låta förfalla och tillämpa en induktiv metod
- Innan kontrollfunktionen förfaller – bestyrka den
  - Bestyrkande och rekursivt bestyrkande
  - Digg:s valideringstjänst
    - <https://www.digg.se/digitala-tjanster/e-underskrift/valideringstjanst>

*Slut på kärlek*