

P A T E N T K R A V

1. Förfarande för att skapa en signal för tidstämpling av dokument, **k ä n n e t e c k n a t a v** att förfarandet inne-
5 fattar följande steg:

a) välja ett digitalt lagrat referensdokument, vilket referensdokument är en digitalt lagrad beskrivning eller sampling av det nuvarande tillståndet för en viss fysisk referensskälla och/eller informationsreferensskälla vid en
10 viss första tidpunkt, där äktheten för varje referensdokument kan verifieras genom att konsultera en eller flera publikt tillgängliga informationskällor avseende det historiska tillståndet för sagda referensskälla;

b) använda referensdokumentet som ett av åtminstone ett
15 ingångsvärde till en envägsfunktion, och beräkna motsvarande utgångsvärde från envägsfunktionen;

c) uppdatera signalen baserat på sagda utgångsvärde, så att sagda utgångsvärde utgör eller kan bestämmas baserat på värdet för signalen; och

d) upprepa från a) med hjälp av ett annat digitalt lagrat referensdokument som är en digital beskrivning eller sampling av det nuvarande fysiska tillståndet och/eller informationstillståndet för samma eller en annan referensskälla vid en senare tidpunkt.
20

2. Förfarande enligt krav 1, **k ä n n e t e c k n a t a v** att åtminstone en referensskälla är en uppsättning specificerad, offentligt publicerad information, vars tillstånd inte är känt i förväg, såsom en uppsättning börskurser eller en
25 uppsättning vinnande lottnummer.

3. Förfarande enligt krav 1 eller 2, **k ä n n e t e c k n a t a v** att åtminstone en referensskälla är en offentligt publicerad fysisk händelse, vars tillstånd inte är känt i förväg,

såsom en specifik idrottshändelse eller specificerad nyhetsrapportering.

4. Förfarande enligt något av föregående krav, **k ä n n e - t e c k n a t a v** att referenskällan är publikt tillgängligt videomaterial, i vilket bildrutorna hos videoströmmen och/eller en publikt tillgänglig ljudström används som referensdokument.

5. Förfarande enligt något av föregående krav, **k ä n n e - t e c k n a t a v** att referensdokumentet som väljs i steg a) associeras med utgångsvärdet som beräknas i steg b) eller signalvärdet som uppdateras i steg c), och av att referensdokumentet lagras för framtida referens.

6. Förfarande enligt något av föregående krav, **k ä n n e - t e c k n a t a v** att en uppsättning av olika referenskällor används, och av att referensdokument representerande olika referenskällor, eller olika kombinationer av sådana referensdokument, används som ingångsvärde i steg b) i olika iterationer av förfarandet.

7. Förfarande enligt något av föregående krav, **k ä n n e - t e c k n a t a v** att, för vissa eller alla iterationer av förfarandet, ett tidigare eller aktuellt värde för signalen, ett värde på vilket ett tidigare eller aktuellt värde för signalen baseras, eller ett värde som beräknas baserat på ett sådant tidigare eller aktuellt signalvärde, används som ingångsvärdet i steg b).

8. Förfarande enligt något av föregående krav, **k ä n n e - t e c k n a t a v** att ett visst dokument tidsstämplas med hjälp av det aktuella värdet för signalen, och av att åtminstone en del av en digitalt lagrad version av det vissa tidsstämplade dokumentet, eller ett utgångsvärde från en

envägsfunktion för vilken ett ingångsvärde är det vissa dokumentet, används som ingångsvärdet i steg b) i en iteration av förfarandet.

5 9. Förfarande enligt något av föregående krav, **k ä n n e - t e c k n a t a v** att det aktuella värdet för signalen kontinuerligt eller periodiskt publiceras eller sänds till en mottagare.

10 10. Förfarande enligt krav 10, **k ä n n e t e c k n a t a v** att värdet för signalen ändras, och av att den uppdaterade signalen publiceras eller sänds åtminstone en gång varje minut.

15 11. Förfarande för att skapa en digital signatur för ett dokument, varvid signaturen skapas så att den består av, innefattar eller beräknas baserat på utgångsvärdet från en viss signaturenvägsfunktion, där ett ingångsvärde till signaturenvägsfunktionen är åtminstone en del av en digitalt lagrad version av dokumentet ifråga, **k ä n n e t e c k n a d**
20 **a v** att en signal skapas i enlighet med något av de föregående kraven, och av att det aktuella värdet för signalen, eller ett värde som har beräknats baserat på det aktuella värdet för signalen, också används som ett ingångsvärde till
25 sagda signaturenvägsfunktion.

12. Förfarande enligt krav 11, **k ä n n e t e c k n a t a v** att signaturen, eller ett värde som har beräknats baserat på signaturen, publiceras offentligt över åtminstone en publiceringskanal, vilken kanal tillhandahåller möjligheten för
30 tredje parter att, vid en senare tidpunkt, verifiera publiceringstiden för signaturen.

13. Förfarande enligt krav 12, **k ä n n e t e c k n a t a v**
35 att publiceringskanalen kontrolleras av en tredje part.

14. Förfarande enligt krav 12 eller 13, **k ä n n e t e c k -
n a t a v** att signaturer beräknas för en mångfald dokument
vid olika tidpunkter, av att sagda beräknade signaturer lag-
5 ras logiskt som löv i en trädstruktur, av att ett respektive
utgångsvärde från en trädenvägsfunktion beräknas för varje
föräldranod i trädstrukturen, där signaturerna och/eller de
beräknade trädenvägsfunktionsutgångsvärden för varje respek-
tive barnnod till föräldranoden ifråga används som ingångs-
10 värden till trädenvägsfunktionen, och av att det är utgångs-
värdet från trädenvägsfunktionen för en trädrot, eller ett
värde som har beräknats baserat på detta utgångsvärde, som
publiceras offentligt.

15. Förfarande enligt krav 14, **k ä n n e t e c k n a t a v**
att utgångsvärdet från trädenvägsfunktionen för trädroten,
eller ett värde som har beräknats baserat på detta utgångs-
värde, publiceras även utan att vara en konsekvens av att en
signatur har skapats för ett dokument, och av att en sådan
20 publicering föregås av tillägget till trädstrukturen av ett
värde som inte är den nyligen beräknade signaturen för ett
dokument.

16. Förfarande enligt krav 15, **k ä n n e t e c k n a t a v**
25 att det värde som läggs till trädstrukturen är ett av de
tidigare beräknade utgångsvärdena från trädenvägsfunktionen.

17. Förfarande enligt något av kraven 11-16, **k ä n n e -
t e c k n a t a v** att den digitala versionen av dokumentet
30 som användes för beräkningen av signaturenvägsfunktionens
utgångsvärde associeras med signaturen och lagras för fram-
tida referens.

18. Förfarande enligt något av kraven 11-17, **k ä n n e -
35 t e c k n a t a v** att ett slumpstal också används som ett

ingångsvärde till sagda signaturenvägsfunktion, och av att slumptalet associeras med dokumentet och/eller signaturenvägsfunktionens utgångsvärde och lagras.

5 19. Förfarande för att tidsstämpla ett dokument, **k ä n n e -
t e c k n a t a v** att en signal skapas i enlighet med något av kraven 1-10, och av att det aktuella värdet, vid tidpunkten för tidsstämpling av dokumentet, bäddas in i dokumentet eller associeras med dokumentet och lagras tillsammans på en
10 central server tillsammans med dokumentet.

20. Förfarande enligt krav 19, **k ä n n e t e c k n a t a v** att signalen bäddas in i dokumentet i form av en information från vilken signalens värde kan härledas,

15 genom att införa ett grafiskt element, såsom en sträng av alfanumeriska tecken, en QR-kod eller en streckkod, in i en visuell representation av dokumentet, vilket grafiska element bär sagda information;

genom att lägga till sagda information till en digitalt
20 lagrad version av dokumentet som metadata; och/eller

genom att lägga till sagda information i form av en digitalt lagrad vattenstämpel till en digitalt lagrad version av dokumentet.

25 21. Förfarande enligt krav 19 eller 20, **k ä n n e t e c k -
n a t a v** att dokumentet innefattar information som fångats med hjälp av en samplingsutrustning för att sampla ett fysiskt fenomen, såsom en kamera eller en ljudinspelare, vilket samplade fysiska fenomen utgör dokumentet, av att samplings-
30 utrustningen ges tillgång till en kommunikationskanal över vilken det aktuella värdet för signalen kommuniceras till samplingsutrustningen, och av att samplingsutrustningen baddar in det aktuella signalvärdet i dokumentet i anslutning till utförandet av samplingen.

22. Förfarande enligt krav 20 eller 21, **k ä n n e t e c k -
n a t a v** att dokumentet innefattar åtminstone en still-
bild, eller en bildruta i en sekvens av rörliga bilder, vil-
5 ken fångats med användning av en bildfångande anordning såsom
en kamera, och av att det aktuella signalvärdet vid tidpunk-
ten för fångandet av bilden eller bildrutan bäddas in i bil-
den eller bildrutan genom att positionera en grafikpresente-
rande anordning, anordnad att visa ett grafiskt element som
10 bär sagda information, i bilden eller bildrutan så att det
grafiska elementet fångas som en del av den fångade bilden
eller bildrutan.

23. Förfarande enligt krav 22, **k ä n n e t e c k n a t a v**
15 att den grafikpresenterande anordningen är en del av samma
allmänna anordning som den bildfångande anordningen, och av
att den grafikpresenterande anordningen är anordnad att pre-
sentera sagda grafiska element vid samma tidpunkt som den
bildfångande anordningen fångar en bild som visar, via en
20 spegel, en bild som omfattar den grafikpresenterande anord-
ningen.

24. Förfarande enligt krav 20 eller 21, **k ä n n e t e c k -
n a t a v** att dokumentet innefattar åtminstone en still-
25 bild, eller en bildruta i en serie rörliga bilder, som fång-
ats med användning av en bildfångande anordning såsom en
kamera, och av att det aktuella signalvärdet vid tidpunkten
för infångandet av bilden eller bildrutan bäddas in i bilden
eller bildrutan genom att mata en signal till den bildfång-
ande anordningen och bringa den bildfångande anordningen att
30 bädda in sagda information digitalt i bilden eller bildrutan.

25. Förfarande enligt något av kraven 20-24, **k ä n n e -
t e c k n a t a v** att dokumentet är en bildruta i ett video-

material, och av att signalen bäddas in i videomaterialet genom att individuella bildrutor hos videomaterialet bringas att innehålla det respektive aktuella värdet för signalen vid tidpunkten för fångandet av bildrutan ifråga.

5

26. Förfarande enligt krav 25, **k ä n n e t e c k n a t a v** att ett antal på varandra följande bildrutor innehåller bildmaterial föreställande ett naturligt fenomen, vars utveckling är naturligt deterministisk.

10

27. Förfarande enligt krav 25 eller 26, **k ä n n e t e c k n a t a v** att videomaterialet fångas av ett videokonferenssystem.

15

28. Förfarande enligt krav 25 eller 26, **k ä n n e t e c k n a t a v** att videomaterialet fångas av ett videoövervakningssystem.

20

29. Förfarande enligt något av kraven 19-28, **k ä n n e t e c k n a t a v** att en digital signatur för det tidsstämplade dokumentet skapas i enlighet med något av kraven 11-18, associeras med dokumentet och lagras i den centrala servern.

25

30. Förfarande enligt krav 29, **k ä n n e t e c k n a t a v** att dokumentet fångas med användning av en samplingsutrustning för att sampla ett fysiskt fenomen, såsom en kamera eller en ljudinspelningsutrustning, vilken samplingsutrustning bringas att beräkna sagda digitala signatur i anslutning till att samplingen utförs, vilket samplade fysiska fenomen utgör dokumentet, och av att samplingsutrustningen förses med tillgång till en kommunikationskanal över vilken signaturen kommuniceras till den centrala servern.

30

35

31. Förfarande enligt krav 30, **k ä n n e t e c k n a t a v** att samplingsutrustningen bringas att sampla det fysiska

fenomenet upprepade gånger över en viss tidsperiod, så att flera referensdokument framställs, av att åtminstone en del av en digitalt lagrad version av åtminstone ett tidsstämplat dokument används, av den centrala servern, som ett ingångsvärde i steg b) i förfarandet enligt krav 1 för att skapa signalen, och av att signalvärdet efter att ha uppdaterats med hjälp av det tidsstämplade dokumentet bäddas in i ett referensdokument som framställs vid en senare tidpunkt än sagda åtminstone ett tidsstämplade dokument.

10

32. Förfarande enligt krav 29, **k ä n n e t e c k n a t a v** att dokumentet är en webbsida.

15

33. Förfarande enligt krav 32, **k ä n n e t e c k n a t a v** att webbsidan innefattar programkod anordnad att initiera en tidsstämpling i enlighet med krav 19 som en konsekvens av att webbsidan visas.

20

34. Förfarande för att tillhandahålla ett sätt att verifiera integriteten för ett dokument, **k ä n n e t e c k n a t a v** att förfarandet innefattar följande steg:

e) tidsstämpla dokumentet i enlighet med något av kraven 29-31;

25

f) publicera dokumentet med en visuellt inbäddad information i enlighet med krav 22;

g) tillhandahålla en kommunikationskanal över vilken en tredje part kan sända en avbildning av det publicerade dokumentet;

30

h) acceptera sagda avbildning av det publicerade dokumentet och härleda värdet för signalen från informationen som är synlig i avbildningen;

i) hitta, i den centrala servern och baserat på signalvärdet, det dokument som tidigare tidsstämplades med användning av sagda signalvärde, om något sådant dokument finns; och

35

j) ifall ett dokument hittas i den centrala servern, kommunicera till den tredje parten detta dokument självt och/eller information som är hänförligt till dokumentet.

5 35. Förfarande för att tillhandahålla ett sätt att verifiera integriteten för ett digitalt lagrat dokument som har publicerats på internet och som visas med hjälp av en webbläsare, **k ä n n e t e c k n a t a v** att förfarandet innefattar följande steg:

10 e) tidsstämpla dokumentet i enlighet med något av kraven 29-31;

f) publicera dokumentet på internet med associerad programkod anordnad att reagera på ett val av eller en klickning på dokumentet, eller en aktivering av en användarkontroll;

15 g) vid en detektering av ett val av eller klickning på dokumentet, eller en aktivering av sagda användarkontroll, av en tredje part som betraktar dokumentet, sända dokumentet till den centrala servern;

20 h) vid mottagandet av dokumentet däri, bringa den centrala servern att slå upp ifall dokumentet har tidsstämplats genom att beräkna motsvarande digitala signatur och kontrollera ifall ett dokument med samma digitala signatur tidigare har tidsstämplats; och

25 i) ifall ett sådant dokument hittas, kommunicera till den tredje parten information som är hänförlig till dokumentet.

36. Förfarande enligt krav 35, **k ä n n e t e c k n a t a v** att, i steg i), sagda hänförliga information kommuniceras i form av dokumentet självt med sagda hänförliga information visuellt inbäddad i dokumentet.

37. Förfarande enligt krav 35 eller 36, **k ä n n e t e c k -
n a t a v** att dokumentet är en stillbild eller en serie av
rörliga bilder, av att, vid ett första val av eller en första
klickning på dokumentet, eller en första aktivering av använ-
5 darkkontrollen, sagda hänförliga information publiceras i
anslutning till bilden utan att webläsaren lämnar den för
tillfället visade websidan.

38. Förfarande enligt krav 37, **k ä n n e t e c k n a t a v**
10 att, vid ett andra val av eller en andra klickning på doku-
mentet, eller en andra aktivering av användarkontrollen,
webläsaren omdirigeras till en annan sida, där dokumentet
tillsammans med hänförlig information presenteras.

15 39. Förfarande enligt något av kraven 34-38, **k ä n n e -
t e c k n a t a v** att sagda hänförliga information innefat-
tar tidpunkten för tidsstämplingen av dokumentet.

40. Förfarande för att verifiera integriteten för ett digi-
20 talt lagrat dokument, **k ä n n e t e c k n a t a v** att förfar-
andet innefattar att, vid en första tidpunkt, skapa en digi-
tal bevissignatur för dokumentet i enlighet med något av
kraven 11-18 och lagra den digitala bevissignaturen, och, vid
en senare andra tidpunkt, verifiera integriteten för dokumen-
25 tet ifråga genom att ta emot en digital kopia av dokumentet,
skapa en motsvarande digital verifieringssignatur av dokumen-
tet i enlighet med något av kraven 11-18 och med användning
av samma värde för signalen som användes för skapandet av den
digitala bevissignaturen, och bekräfta integriteten för doku-
30 mentet endast ifall den digitala bevissignaturen är identisk
med den digitala verifieringssignaturen.

41. Förfarande för att verifiera integriteten för en viss
metadatainformation hänförlig till ett digitalt lagrat doku-
35 ment, **k ä n n e t e c k n a t a v** att förfarandet innefattar

att, vid en första tidpunkt, skapa en digital bevissignatur av dokumentet i enlighet med något av kraven 11-18, varvid signaturenvägsfunktionen beräknas baserat på både åtminstone en del av den digitalt lagrade versionen av dokumentet självt
5 och på sagda metadatainformation, och lagra den digitala bevissignaturen och, vid en senare andra tidpunkt, verifiera integriteten för metadata ifråga genom att ta emot metadata-informationen, skapa en motsvarande digital verifieringssignatur av dokumentet i enlighet med något av kraven 11-18 och
10 med användning av samma värde för signalen som användes för skapandet av den digitala bevissignaturen, och bekräfta integriteten för metadatainformationen endast ifall den digitala bevissignaturen är identisk med den digitala verifieringssignaturen som är hänförlig till dokumentet.

15 42. Förfarande enligt krav 41, **k ä n n e t e c k n a t a v** att det finns flera metadata som är hänförliga till det digitalt lagrade dokumentet, av att, vid den sagda första tidpunkten, en separat digital metadatasignatur skapas i enlighet med något av kraven 11-18 för varje sådant metadata och
20 lagras, av att den digitala bevissignaturen skapas så att signaturenvägsfunktionen beräknas baserat också på varje digital metadatasignatur, av att, vid den sagda andra tidpunkten, en delmängd av sagda flera metadata tas emot, motsvarande digitala verifieringssignaturer skapas både för de
25 mottagna metadata och dokumentet i enlighet med något av kraven 11-18 och med användning av samma värde för signalen som användes för att skapa de digitala metadatasignaturerna och den digitala bevissignaturen, varvid de lagrade digitala
30 metadatasignaturerna används för sådana metadata som inte tagits emot vid den andra tidpunkten, och bekräfta integriteten för delmängden av metadata endast ifall den digitala bevissignaturen är identisk med den digitala verifieringssignaturen hänförlig till dokumentet.

43. Förfarande för att tillhandahålla ett sätt att verifiera att ett visst dokument publiceras i realtid eller nära realtid, **k ä n n e t e c k n a t a v** att förfarandet innefattar
5 följande steg:

e) kontinuerligt tidsstämpla dokumentet i enlighet med något av kraven 29-31; och

f) tillhandahålla åtkomst för en tredje part till ett organ för att jämföra en kontinuerligt uppdaterad information som bäddas in i dokumentet med ett motsvarande aktuellt signalvärde som lagrats i den centrala servern.

44. Förfarande enligt krav 43, **k ä n n e t e c k n a t a v** att dokumentet publiceras på internet, och av att sagda organ
15 för att jämföra den kontinuerligt uppdaterade informationen är i form av programkod som är associerad med dokumentet och anordnad att automatiskt utföra en sådan jämförelse och att signalera till den tredje parten huruvida ett signalvärde som härletts från informationen motsvarar det aktuella värdet för
20 signalen.

45. Förfarande för att verifiera integriteten för data i en databas, **k ä n n e t e c k n a t a v** att åtminstone en digital bevissignatur skapas för sagda data i enlighet med något
25 av kraven 11-18 och lagras, av att integriteten för sagda data vid upprepade tillfällen kontrolleras genom att jämföra den lagrade digitala bevissignaturen med en motsvarande men senare skapad digital verifieringssignatur som baseras på det aktuella värdet för de data som ska verifieras och på samma
30 signalvärde som användes för att skapa den digitala bevissignaturen, och av att en rapport sänds ifall någon skillnad mellan den digitala verifieringssignaturen och den digitala bevissignaturen föreligger.

46. Förfarande enligt krav 45, **k ä n n e t e c k n a t a v** att värdet för den lagrade digitala bevissignaturen uppdateras vid upprepade tillfällen, genom att skapa en ny digital bevissignatur i enlighet med något av kraven 11-18.

5

47. Förfarande enligt krav 46, **k ä n n e t e c k n a t a v** att uppdateringen av värdet för den lagrade digitala bevissignaturen utlöses av tillgångshändelser till databasen.