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 innefattar 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 referenskälla och/eller informationsreferenskälla vid en 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 referenskälla;

b) använda referensdokumentet som ett av åtminstone ett 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 referenskälla vid en senare tidpunkt.

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

9. Förfarande enligt något av föregående krav, **kännetecknat av** att det aktuella värdet för signalen kontinuerligt eller periodiskt publiceras eller sänds till en mottagare.

10. Förfarande enligt krav 10, **kännetecknat av** att värdet för signalen ändras, och av att den uppdaterade signalen publiceras eller sänds åtminstone en gång varje minut.

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, **kännetecknad av** 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 sagda signaturenvägsfunktion.

12. Förfarande enligt krav 11, **kännetecknat av** att signaturen, eller ett värde som har beräknats baserat på signaturen, publiceras offentligt över åtminstone en publiceringskanal, vilken kanal tillhandahåller möjligheten för tredje parter att, vid en senare tidpunkt, verifiera publiceringstiden för signaturen.

13. Förfarande enligt krav 12, **kännetecknat av** att publiceringskanalen kontrolleras av en tredje part.

14. Förfarande enligt krav 12 eller 13, **kännetecknat av** att signaturer beräknas för en mångfald dokument vid olika tidpunkter, av att sagda beräknade signaturer lagras 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 respektive barnnod till föräldranoden ifråga används som ingångsvärden till trädenvägsfunktionen, och av att det är utgångsvärdet från trädenvägsfunktionen för en trädrot, eller ett värde som har beräknats baserat på detta utgångsvärde, som publiceras offentligt.

15. Förfarande enligt krav 14, **kännetecknat av** att utgångsvärdet från trädenvägsfunktionen för trädroten, eller ett värde som har beräknats baserat på detta utgångsvärde, publiceras även utan att vara en konsekvens av att en signatur har skapats för ett dokument, och av att en sådan publicering föregås av tillägget till trädstrukturen av ett värde som inte är den nyligen beräknade signaturen för ett dokument.

16. Förfarande enligt krav 15, **kännetecknat av** att det värde som läggs till trädstrukturen är ett av de tidigare beräknade utgångsvärdena från trädenvägsfunktionen.

17. Förfarande enligt något av kraven 11-16, **kännetecknat av** att den digitala versionen av dokumentet som användes för beräkningen av signaturenvägsfunktionens utgångsvärde associeras med signaturen och lagras för framtida referens.

18. Förfarande enligt något av kraven 11-17, **kännetecknat av** att ett slumptal också används som ett

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

19. Förfarande för att tidsstämpla ett dokument, **kännetecknat av** 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 central server tillsammans med dokumentet.

20. Förfarande enligt krav 19, **kännetecknat av** att signalen bäddas in i dokumentet i form av en information från vilken signalens värde kan härledas,

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 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.

21. Förfarande enligt krav 19 eller 20, **kännetecknat av** 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 samplingsutrustningen ges tillgång till en kommunikationskanal över vilken det aktuella värdet för signalen kommuniceras till samplingsutrustningen, och av att samplingsutrustningen bäddar in det aktuella signalvärdet i dokumentet i anslutning till utförandet av samplingen.

22. Förfarande enligt krav 20 eller 21, **kännetecknat av** att dokumentet innefattar åtminstone en stillbild, eller en bildruta i en sekvens av rörliga bilder, vilken fångats med användning av en bildfångande anordning såsom en kamera, och av att det aktuella signalvärdet vid tidpunkten för fångandet av bilden eller bildrutan bäddas in i bilden eller bildrutan genom att positionera en grafikpresenterande anordning, anordnad att visa ett grafiskt element som 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, **kännetecknat av** att den grafikpresenterande anordningen är en del av samma allmänna anordning som den bildfångande anordningen, och av att den grafikpresenterande anordningen är anordnad att presentera sagda grafiska element vid samma tidpunkt som den bildfångande anordningen fångar en bild som visar, via en spegel, en bild som omfattar den grafikpresenterande anordningen.

24. Förfarande enligt krav 20 eller 21, **kännetecknat av** att dokumentet innefattar åtminstone en stillbild, eller en bildruta i en serie rörliga bilder, som fångats 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 bildfångande anordningen och bringa den bildfångande anordningen att bädda in sagda information digitalt i bilden eller bildrutan.

25. Förfarande enligt något av kraven 20-24, **kännetecknat av** 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.

26. Förfarande enligt krav 25, **kännetecknat av** att ett antal på varandra följande bildrutor innehåller bildmaterial föreställande ett naturligt fenomen, vars utveckling är naturligt deterministisk.

27. Förfarande enligt krav 25 eller 26, **kännetecknat av** att videomaterialet fångas av ett videokonferenssystem.

28. Förfarande enligt krav 25 eller 26, **kännetecknat av** att videomaterialet fångas av ett videoövervakningssystem.

29. Förfarande enligt något av kraven 19-28, **kännetecknat av** 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.

30. Förfarande enligt krav 29, **kännetecknat av** 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.

31. Förfarande enligt krav 30, **kännetecknat av** 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.

32. Förfarande enligt krav 29, **kännetecknat av** att dokumentet är en webbsida.

33. Förfarande enligt krav 32, **kännetecknat av** att webbsidan innefattar programkod anordnad att initiera en tidsstämpling i enlighet med krav 19 som en konsekvens av att webbsidan visas.

34. Förfarande för att tillhandahålla ett sätt att verifiera integriteten för ett dokument, **kännetecknat av** att förfarandet innefattar följande steg:

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

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;

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

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.

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 webläsare, **kännetecknat av** att förfarandet innefattar följande steg:

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;

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;

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

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

36. Förfarande enligt krav 35, **kännetecknat av** 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, **kännetecknat av** 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 användarkontrollen, sagda hänförliga information publiceras i anslutning till bilden utan att webläsaren lämnar den för tillfället visade websidan.

38. Förfarande enligt krav 37, **kännetecknat av** att, vid ett andra val av eller en andra klickning på dokumentet, eller en andra aktivering av användarkontrollen, webläsaren omdirigeras till en annan sida, där dokumentet tillsammans med hänförlig information presenteras.

39. Förfarande enligt något av kraven 34-38, **kännetecknat av** att sagda hänförliga information innefattar tidpunkten för tidsstämplingen av dokumentet.

40. Förfarande för att verifiera integriteten för ett digitalt lagrat dokument, **kännetecknat av** att förfarandet innefattar att, vid en första tidpunkt, skapa en digital 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 dokumentet ifråga genom att ta emot en digital kopia av dokumentet, skapa en motsvarande digital verifieringssignatur av dokumentet 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 dokumentet 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 dokument, **kännetecknat av** 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 och på sagda metadatainformation, och lagra den digitala bevissignaturen och, vid en senare andra tidpunkt, verifiera integriteten för metadata ifråga genom att ta emot metadatainformationen, skapa en motsvarande digital verifieringssignatur av dokumentet 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 metadatainformationen endast ifall den digitala bevissignaturen är identisk med den digitala verifieringssignaturen som är hänförlig till dokumentet.

42. Förfarande enligt krav 41, **kännetecknat av** 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 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 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 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, **kännetecknat av** att förfarandet innefattar 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, **kännetecknat av** att dokumentet publiceras på internet, och av att sagda organ 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 signalen.

45. Förfarande för att verifiera integriteten för data i en databas, **kännetecknat av** att åtminstone en digital bevissignatur skapas för sagda data i enlighet med något 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 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.

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.