PATENTKRAV

1. Ett datorläsbart medium innefattande ett datorprogram som är exekverbart med åtminstone en processor varvid datorprogrammet innefattar uppsättningar av instruktioner för:

mottagning av en speciell information, vilken innefattar en uppsättning sektioner; och

verifiering av autenticiteten för den speciella informationen genom användning av en digital signatur härledd från endast en kvasi-slumpartat vald delsektion från var och en av ett antal av sektionerna.

2. Datorläsbart medium enligt patentkrav 1, varvid uppsättningen instruktioner för verifiering av autenticiteten för den speciella informationen innefattar:

generering av den digitala signaturen genom hashning av endast de kvasi-slumpartat valda delsektionerna; och

jämförelse av den genererade digitala signaturen mot en digital signatur mottagen tillsammans med den speciella informationen.

3. Datorläsbart medium enligt patentkrav 2, varvid den mottagna digitala signaturen genereras av en uppsättning DRM servrar, vilka distribuerar den speciella informationen.

4. Datorläsbart medium enligt patentkrav 1, varvid den digitala signaturen är härledd från en kvasi-slumpartat vald delsektion av var och en av sektionerna.

5. Datorläsbart medium enligt patentkrav 1, varvid varje sektion innefattar en op-kod och en associerad uppsättning operander.

6. Ett datorläsbart medium lagrande ett datorprogram för exekvering med åtminstone en processor, varvid datorprogrammet innefattar uppsättningar av instruktioner för:

mottagning av en speciell information, vilken innefattar ett flertal uppsättningar av op-koder och operander tillsammans med en digital signatur härledd från endast en del av den speciella informationen, baserad på ett ordnat mönster av bits i den speciella informationen, varvid delen innefattar en del av var och en av ett flertal av uppsättningarna av op-koder och operander; och

verifiering av autenticiteten för den speciella informationen genom återberäkning av en digest använd vid härledningen av den digitala signaturen, varvid

den återberäknade digesten är härledd från endast samma del av den speciella informationen.

7. Datorläsbart medium enligt patentkrav 6, varvid uppsättningen av instruktioner för verifiering av autenticiteten för den speciella informationen innefattar en uppsättning instruktioner för verifiering av den återberäknade digesten med användning av en asymmetrisk integritetskontroll, som inte återberäknar den digitala signaturen.

8. Datorläsbart medium enligt patentkrav 6, varvid uppsättningen instruktioner för verifiering av autenticiteten för den speciella informationen innefattar uppsättningar av instruktioner för:

härledning av en ny digital signatur från den återberäknade digesten; och

jämförelse av den nya digitala signaturen med den mottagna digitala signaturen.

9. Datorläsbart medium enligt patentkrav 6, varvid den speciella informationen innefattar en uppdatering för firmware till en enhet.

10. Datorläsbart medium enligt patentkrav 6, varvid den speciella informationen innefattar mediainformation.

11. Metod för verifiering av en speciell information på en användarenhet, varvid metoden innefattar:

mottagning (i) av en speciell information, vilken innefattar ett flertal sektioner och (ii) en digital signatur genererad från en deluppsättning av nämnda flertal sektioner av den speciella informationen, varvid deluppsättningen är vald för att minska användningen av beräkningsresurser för verifiering av den digitala signaturen utan att öka sannolikheten för att digitala signaturer för två olika informationer blir desamma;

återberäkning av en digest från deluppsättningen av nämnda flertal sektioner av den speciella informationen; och

verifiering av autenticiteten för den speciella informationen med användning av den återberäknade digesten och den mottagna digitala signaturen.

12. Metod enligt patentkrav 11, varvid deluppsättningen också väljs för att förbättra detektering av manipulering av den speciella informationen.

13. Metod enligt patentkrav 11, varvid mottagningen, återberäkningen och verifiering av autenticiteten utförs av en första enhet, varvid metoden dessutom innefattar synkronisering med en andra enhet för överföring av den speciella informationen och mottagna digitala signaturen till den andra enheten.

14. Metod innefattande:

för en speciell information som innefattar ett flertal sektioner, val av en uppsättning sektioner av den speciella informationen;

generering av en digital signatur för den speciella informationen från endast den valda uppsättningen av sektioner från den speciella informationen, varvid uppsättningen sektioner väljs för att förbättra detektering av manipulering av den speciella informationen och minska användningen av beräkningsresurser för generering av den digitala signaturen; och

distribution av den digitala signaturen.

15. Metod enligt patentkrav 14, varvid uppsättningen sektioner väljes för att undvika en ökning av sannolikheten för att digitala signaturer för två olika informationer blir desamma.

16. Metod enligt patentkrav 14, dessutom innefattande distribution av den speciella informationen med den digitala signaturen.

17. Metod enligt patentkrav 14, varvid uppsättningen sektioner väljes kvasi-slumpartat.

18. Ett datorläsbart medium lagrande ett datorprogram som är exekverbart med åtminstone en processor varvid datorprogrammet innefattar uppsättningar av instruktioner för:

för en speciell information, vilken innefattar ett flertal uppsättningar av op-koder och associerade operander, val av en del av den speciella informationen som innefattar endast en op-kod från varje uppsättning;

generering av en digital signatur för den speciella informationen utifrån endast den valda delen av den speciella informationen; och

distribution av den digitala signaturen.

19. Datorläsbart medium enligt patentkrav 18, varvid den digitala signaturen distribueras med den speciella informationen till en användarenhet.

20. Datorläsbart medium enligt patentkrav 18, varvid användarenheten verifierar den digitala signaturen under användande av endast en op-kod från varje uppsättning av den speciella informationen.

21. Ett datorläsbart medium lagrande ett datorprogram som är exekverbart med åtminstone en processor varvid datorprogrammet innefattar uppsättningar av instruktioner för:

för en speciell information, vilken innefattar uppsättningar av op-koder och associerade operander, val av en del av den speciella informationen vilken innefattar en kvasi-slumpartat vald del av var och en av ett flertal av uppsättningarna av op-koder och associerade operander;

generering av en digital signatur för den speciella informationen utifrån endast den valda delen av den speciella informationen; och

distribution av den digitala signaturen.

22. Datorläsbart medium enligt patentkrav 21, varvid uppsättningen instruktioner för generering av den digitala signaturen innefattar en uppsättning instruktioner för generering av en hash digest av den valda delen av den speciella informationen.

23. Datorläsbart medium enligt patentkrav 21, varvid den speciella informationen innefattar en applikation för exekvering på en enhet.

24. Metod för generering av en digital signatur för en speciell information som innefattar en uppsättning sektioner, varvid metoden innefattar:

i en uppsättning av digitala rättsförvaltande (DRM) datorer, utvälja en delsektion från var och en av ett flertal sektioner i uppsättningen av sektioner baserat på ett ordnat mönster av bits i den speciella informationen, varvid var och en av nämnda flertal sektioner innefattar en första vald delsektion och en andra icke-vald delsektion;

generering av en enda digital signatur för den speciella informationen utifrån endast de valda delsektionerna av den speciella informationen; och

från uppsättningen av DRM datorer tillhandahålla den enda digitala signaturen för verifikation av hela den speciella informationen.

25. Metod enligt patentkrav 24, varvid var och en av sektionerna innefattar en fyra bytes microprocessor operationsenhet (MOU), och den valda delsektionen från var och en av nämnda flertal sektioner är en första byte från MOU.

26. Metod enligt patentkrav 24, varvid var och en av sektionerna innefattar en op-kod och associerade operander och den valda delsektionen från var och en av nämnda flertal sektioner innefattar op-koden.

27. Metod för verifiering av en information, som innefattar en uppsättning sektioner, varvid metoden innefattar:

mottagning av informationen och en enda digital signatur härledd från en del av informationen, varvid delen innefattar, för var och en av ett flertal sektioner, en första vald delsektion och en andra icke-vald delsektion;

verifiering av hela informationen med användning av den enda digitala signaturen.

28. Metod enligt patentkrav 27, varvid de valda delsektionerna väljes kvasi-slumpartat.

29. Metod enligt patentkrav 27, varvid de valda delsektionerna väljes utifrån ett ordnat mönster av bits.