(12) **PATENT**

(19) NO (11) **325464** (13) **B1**

NORGE

(51) Int Cl.
G07B 17/00 (2006.01)
G07D 7/00 (2006.01)
G07D 7/20 (2006.01)

Patentstyret

(21)	Søknadsnr	20035858	(86)	Int.inng.dag og søknadsnr	2002.06.28 PCT/DE02/02348
(22)	Inng.dag	2003.12.30	(85)	Videreføringsdag	2003.12.30
(24)	Løpedag	2002.06.28	(30)	Prioritet	2001.07.01, DE, 10131254
(41)	Alm.tilgj	2004.01.20			
(45)	Meddelt	2008.05.05			

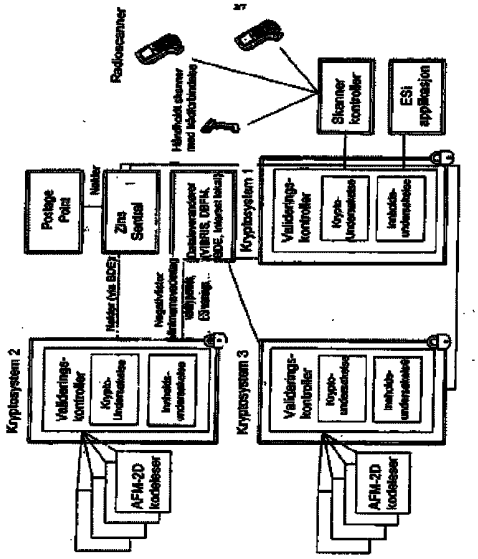
(73) Innehaver Deutsche Post AG, Charles de Gaulle Strasse 20, 53113 BONN, DE
(72) Oppfinner Alexander Delitz, Im Etzental 19, 53177 BONN, DE
Peter Fery, Passwiese 24, 64673 ZWINGENBERG, DE
Jürgen Helmus, Birlinghovener Strasse 6 A, 53229 BONN, DE
Aloysius Höhl, Freidrich-Harth-Strasse 10, D-36041 Fulda, DE
Gunther Meier, Am Wembach 41, 64354 REINHEIM, DE
Elke Robel, Johannesstrasse 76, 53225 BONN, DE
(74) Fullmektig Protector Intellectual Property Consultants AS, Postboks 5074 Majorstua, 0301 OSLO

(54) Benevnelse **Fremgangsmåte for verifisering av gyldigheten til digitale frankeringsmerker**

(56) Anførte publikasjoner EP 732 673 A2, US 6041704, EP 901107 A2, WO 00/31993 A1

(57) Sammendrag

Oppfinnelsen vedrører en fremgangsmåte for verifisering av gyldigheten til et frankeringsmerke plassert på en forsendelse. I henhold til oppfinnelsen blir kryptografisk informasjon i frankeringsmerket dekodet og blir brukt for verifisering av frankeringsmerkets gyldighet. Fremgangsmåte i henhold til oppfinnelsen er kjennetegnet ved at avlesningsenheten grafisk registrerer frankeringsmerket og sender det til en verifiseringsenhet og at verifiseringsenheten kontrollerer en sekvens med deltester.



Foreliggende oppfinnelse vedrører en fremgangsmåte for å verifisere gyldigheten av digitale frankeringsmerker.

Det er kjent praksis å tilveiebringe postforsendelser med digitale frankeringsmerker. Fra EP 732 673 A2 er det kjent metoder for å verifisere frankeringsmerker på postenheter.

For å gjøre det lettere for avsendere av postforsendelser å tilveiebringe frankeringsmerker, tillater for eksempel frankeringssystemet som anvendes av Deutsche Post AG, fremstilling av frankeringsmerker i et kundesystem og sende disse til en printer ved bruk av enhver form for interface.

For å forhindre at denne fremgangsmåten misbrukes, inneholder de digitale frankeringsmerkene kryptografisk informasjon, for eksempel vedrørende identiteten til brukersystemet som kontrollerer fremstillingen av frankeringsmerket.

Oppfinnelsen er basert på den hensikt å tilveiebringe en fremgangsmåte som kan brukes til å verifisere gyldigheten av frankeringsmerker på en rask og pålitelig måte. Spesielt er fremgangsmåten ment å passe for verifisering i stor skala, spesielt i brev- eller fraktsentra.

Oppfinnelsen oppnår denne hensikten ved hjelp av avlesningsenheten som grafisk registrerer frankeringsmerket og overfører dette til en verifiseringsenhet, og ved hjelp av verifiseringsenheten kontrollere en sekvens med undersøkelseskomponenter.

Det er spesielt fordelaktig at en av undersøkelseskomponentene innbefatter dekryptering av den kryptografiske informasjonen som frankeringsmerket inneholder.

Integrering av dekrypteringen av den kryptografiske informasjonen inn i undersøkelsesprosessen gjør det mulig å registrere gyldigheten av

frankeringsmerkene direkte, noe som betyr at verifiseringen kan utføres online – spesielt mens be behandles i en prosesseringsmaskin.

En annen fordel er at en av undersøkelseskomponentene inneholder en sammenligning mellom produksjonsdatoen for frankeringsmerket og nåværende dato. Integrering av produksjonsdatoen til frankeringsmerket, spesielt i kryptert form – øker databeskyttelsen, siden sammenligningen mellom produksjonsdatoen for frankeringsmerket og nåværende data forhindrer flergangs bruk av et frankeringsmerke for utlevering av postforsendelser.

Disse og andre hensikter oppnås ved en fremgangsmåte ved verifisering av gyldigheten av et frankeringsmerke som har blitt satt på et brevstykke, hvor kryptografisk informasjon i frankeringsmerket blir dekryptert og anvendt for verifisering av frankeringsmerkets gyldighet, hvilken fremgangsmåte er kjennetegnet ved at verifiseringen skjer i et system innbefattende en verifiseringsenhet og flere avlesningsenheter,
hvorved en av avlesningsenhetene grafisk registrerer et frankeringsmerke og matrikskoden i frankeringsmerket blir overført til verifiseringsenheten,
hvorved verifiseringsenheten kontrollerer en sekvens av partielle undersøkelser for den mottatte matrikskoden,
hvorved verifiseringsenheten samtidig utfører partielle undersøkelser av den mottatte matrikskoden, og
hvorved verifiseringsenheten sender undersøkelsesresultatene fra den mottatte matrikskoden til den korrekte avlesningsenheten.

For å øke verifiseringshastigheten ytterligere, er det fordelaktig at avlesningsenheten og verifiseringsenheten utveksler informasjon ved bruk av en synkron protokoll.

Det er i denne forbindelse spesielt fordelaktig dersom avlesningsenheten sender et databudskap til verifiseringsenheten.

Fortrinnsvis inneholder databudskapet innholdet i frankeringsmerket.

Ytterligere fordeler, spesielle trekk og foretrukne utviklinger av oppfinnelsen vil fremgå av underkravene og i den etterfølgende beskrivelse av utførelseseksempler med henvisning til tegningene.

I tegningene:

Figur 1 viser en grunnleggende illustrasjon av systemkomponenter i et vederlagsbeskyttelsessystem;

Figur 2 viser en spesielt foretrukket utførelsesform av vederlagsbeskyttelsessystemet, håndholdt skanner og vederlagsbeskyttelse PC);

Figur 3 viser en grunnleggende illustrasjon av fremstilling og verifisering av frankeringsmerker;

Figur 4 viser en oversikt av komponenter i kryptosystemet;

Figur 5 viser en foretrukket implementering av verifiseringsmetoden;

Figur 6 viser en annen foretrukket utførelsesform av verifiseringsmetoden med en spesielt foretrukket sekvens av undersøkelseskomponenter;

Figur 7 viser en foretrukket sekvens for fordeling av nøkler mellom en sentral lastestasjon (postpunkt) og individuelle kryptografiske verifiseringsenheter (kryptoserver).

Oppfinnelsen vil bli illustrert under ved å bruke et eksempel med et PC frankeringssystem. I dette tilfellet er fremgangsmåtetrinnene som anvendes for vederlagsbeskyttelse uavhengig av systemet som brukes for fremstilling av frankeringsmerkene.

Den lokale verifiseringen ved individuelle inspeksjonsstasjoner, spesielt i brevsentra, som er vist er spesielt foretrukket, selv om sentralisert verifisering likedan er mulig.

I henhold til en første utførelsesform av oppfinnelsen, blir gyldigheten av frankeringsmerkene fortrinnsvis verifisert på en tilfeldig prøvebasis med individuelle skannere.

Et verifiseringssystem som er hensiktsmessig i denne forbindelse innbefatter komponentene vist i figur 1.

Figur 1 viser hvilke subsystemer kryptosystemet vedrører. Disse blir kort beskrevet under.

Skanner

Skannerne brukes for avlesning av frankeringsmerket fra PC frankeringsmaskinen. Frankeringsmerkene er 2D koder i data matriksformat. Hvor det brukes ECC200 feilkorreksjon. Avhengig av skannertype, blir dataene overført via radio eller kabel, hvor radioskannerne har en flerlinjes skjerm og derved en utgangsmulighet og en berøringsskjerm, eller et tastatur for rudimentær innlegging. Grenseflaten mellom skannerne og de resterende systemene til det foretrukne vederlagsbeskyttelses PC frankeringssystemet utgjøres av skannerkontrolleren og valideringskontrolleren som komponenter. Skannerkontrolleren håndterer en kø med matrikskoder som stammer fra den håndholdte skanneren, er tilgjengelig for undersøkelse og i det vesentligste opprettholder kontakt med skannerne, er den i kontakt med det videre systemet kun via valideringsskanneren.

Skannerkontroller/valideringskontroller

Skannerkontrollere, eller valideringskontrollere, virker som en interface mellom skannerne og det videre systemet for verifisering av 2D strekkoder. De blir sendt det feilkorrigerte 2D strekkodeinnholdet omdannet fra optisk avlesning, og de foranlediger deretter verifiseringen og, i tilfellet med radioskannere, sikrer de

utmating av avlesningen og undersøkelsesresultatet og virker som en interface mellom enhver nødvendig manuell etterbearbeiding og undersøkelse av en gransker og de øvrige systemene.

Kryptosystem

Kryptosystemet sørger for den innholdsmessige og kryptografiske verifiseringen av 2D strekkode innholdet og også for den beskyttede lagringen av sikkerhetsrelaterte data og algoritmer. De individuelle komponentene vil bli diskutert ved et senere tidspunkt.

Gebyrsumladestasjon (Porto Point)

Gebyrsumladestasjonen (Porto Point) er det sentrale systemet i PC frankeringsanlegget. Det virker som en interface til kundesystemene. Fra dette kan kunden laste ut forinnstilte summer for etterfølgende frankering. Gebyrsumladestasjonen (Porto Point) blir brukt til å generere nøklene for beskyttelse av metoden. I tillegg brukes den som en interface tilavregningssystemet. Interfacene under er tilveiebragt for det foretrukne vederlagsbeskyttelsessystemet for PC frankering:

- sendingsinformasjon med 2D strekkoden
- symmetriske nøkler
- grunnlagsdata, så som forutinnstilte mengder, kontobalanser

Foretrukket vederlagsbeskyttelsessentral

I det foretrukne vederlagsbeskyttelsessentralsystemet, blir sendingsrelatert informasjon innsamlet og gjort tilgjengelig for andre systemer. Dette er hvor produksjonsrapportene blir dannet, som i sin tur resulterer i dannelse av de negative filene. I tillegg mottar vederlagsbeskyttelsessentralsystemet fra gebyrsumladestasjonen (Porto Point) de gjeldende nøkkeldata og sender disse til de individuelle kryptoserverne.

Dataleverandører

For å verifisere innholdet til 2D strekkodene, er det nødvendig med en serie grunnlagsdata, så som negative filer, minimum vederlag, gyldighetsperioder i forhold til produktet og vederlagbeskyttelsesvarsels- og oppfølgingsbehandlingskoder. Disse dataene blir tilveiebragt fra forskjellige systemer (BDE, VIBRIS, lokalt vederlagsbeskyttelsessystem).

Vederlagsbeskyttelsesanvendelse

Vederlagsbeskyttelsesanvendelsen gir AGB-granskeren, som må gjøre ferdig de utmatede PC frankeringssendingene, med mulighet for å utføre en mer detaljert verifisering av frankeringen, med presentasjonen av undersøkelsesresultatene som ikke er begrenset av de begrensede utmatingsmulighetene fra skanneren. I tillegg kan granskeren i dette tilfellet også inspisere andre data, så som gyldighetstidsrommet for portobeløpet, til hvilken nåværende postforsendelse tilhører og også mengden og frankeringen som er brukt.

Automatisk registrering av 2D strekkodene

2D strekkodene blir automatisk registrert innen SSA. For dette blir billedinformasjon sendt til AFM-2D kodeleseren. Her blir bildet omdannet til innholdet til datamatrikskoden. Deretter blir 2D strekkodeinnholdet overført til kryptosystemet for granskning, det returnerte granskningsresultatet blir evaluert og blir overført til det optiske registreringssystemet (IMM) i den hensikt å kode. Foretrukne deler av en verifiseringsmetode utvidet på denne måten er vist i figur 2.

AFM-2D kodeleser

For hver avlesningsmaskin (ALM/ILVM) er det en AFM-2D kodeleser som mottar billeddata fra via et optisk registreringssystem (IMM) og behandler dem videre av vederlagsbeskyttelseshensikter. Innen rammen for den foretrukne vederlagsbeskyttelses PC frankeringen, dette betyr, når en 2D kode har blitt identifisert, at 2D matrikskoden blir ekstrahert fra billeddataene og blir omdannet, ved

bruk av ECC200 korreksjonsmetoden, til en bytestreng som representerer innholdet til 2D strekkoden.

Denne bytestrengen blir overført til valideringskontrolleren i den hensikt å verifiseres. Granskningsresultatet blir deretter ledet via interfacen i det optiske registreringssystemet, hvor det brukes for koding.

Kryptosystem for AFM 2D kodeavleser

Avhengig av egenskapene til kryptokortene, kan det som eksempel forventes 27 undersøkelser per sekund. Siden hastigheten til avlesningsmaskinene blir tilnærmet 10 postforsendelser avlest per sekund, synes det meningsløst å kombinere hver av AFM-2D kodeavleserne med et kryptosystem. I tillegg til dette faktum kan det tillegges at det heller ikke kan antas at PC F forsendelsen blir fremstilt på alle maskiner samtidig til 100 prosent. Det synes derfor passende å separere kryptosystemene og å operere et mangfold PC-F avlesere med et kryptosystem. I dette tilfellet, bør det velges en løsning slik at det kan skaleres, det vil si at det er mulig med et mangfold kryptosystemer per brevsenter. Dette er eksempelvis relevant for brevsentra som har et høyt forsendelsesvolum og et stort antall avlesningsmaskiner, som innledningsvis kan være forsynt med et andre kryptosystem. I tillegg er det senere mulig å øke antallet servere i drift ettersom behovene øker.

Innen denne rammen, for å redusere kompleksiteten, kan arkitekturen fortrinnsvis være valgt slik at de individuelle avlesningsmaskinene er fast forbundet med et kryptosystem og kan også utvides med en ytterligere fallbackkonfigurasjon, som i tilfellet av en feil forsøker å svitsje over til et annet kryptosystem.

Separasjonen av kryptosystem og AFM-2D kodeavleser kan også gi den fordelen at både maskinavlesning og undersøkelser med håndholdt skanner kan utføres ved bruk av samme kryptosystem, og samme funksjoner behøver derfor ikke å implementeres to ganger, noe som i tillegg også gir betydelige fordeler ved implementering av oppfinnelsen.

Foretrukne fremgangsmåtetrinn for å tilveiebringe en postforsendelse med et digitalt frankeringsmerke etter at en vederlagssum har blitt tilført fra en sentral ladestasjon (Porto Point) og frankeringsmerket har blitt fremstilt av en lokal PC og også at deretter har blitt levert og frankeringsmerket påsatt på har blitt verifisert som vist i figur 3.

Uansett nøkkelfordelingen, utføres sekvensen på en slik måte at kunden først legger inn en portomengde på sin PC. For å identifisere forespørselen, blir det i dette tilfellet generert et tilfeldig tall. Vederlagssumlastestasjonen (Porto Point) tilveiebringer et nytt portobeløp for den respektive kunden, og det tilfeldige tallet som overføres, brukes til å danne med ytterligere informasjon vedrørende kundesystemets identitet (kundesystem identifikasjonsangivelse, heretter betegnet Porto ID), og til portobeløpet blir "kryptostrengen" dannet, som er kryptert ved bruk av en eksisterende hemmelig symmetrisk nøkkel som er tilstede i vederlagssumlastestasjonen (Porto Point).

Denne kryptostrengen og den korresponderende portoen blir deretter overføre til kunde-PC'en og blir lagret, sammen med det tilfeldige tallet, i brukerens PC's "safe box", sikret mot uønsket tilgang

Dersom kunden frankerer en postforsendelse med portoen som er mottatt ved hjelp av denne prosedyren, vil data relevant for 2D strekkoden, blant annet kryptostrengen, frankeringsdato og frankeringssummen, utvidet med det tilfeldige tallet, og porto ID'en innsamlet i en ikke-kryptert form og det dannes en hash-verdi som klart identifiserer innholdet.

Siden det tilfeldige tallet er i kryptert form i kryptostrengen og også er i ikke-kryptert form i hash-verdien, sikres det at forsendelsesdataene ikke kan endres, eller genereres vilkårlig, og det er mulig å trekke slutninger vedrørende skaperen.

De relevante dataene for postforsendelsen blir deretter omdannet til en 2D strekkode og blir trykket på postforsendelsen som et korresponderende frankeringskjennetegn av kundens printer. Den ferdige postforsendelsen kan deretter settes inn i postkretsløpet..

I en spesielt foretrukket utførelsesform av vederlagsbeskyttelsen, blir 2D strekkoden avlest og deretter verifisert i brevsenteret med en AFM-2D kodeavleser, eller med en håndholdt skanner. De tilhørende prosesstrinnene fremgår klart av illustrasjonen under henvisningstallene 5-8. For å verifisere riktigheten av 2D strekkoden, overfører AFM-2D kodeavleseren alle forsendelsesdataene til kryptosystemet. Her blir den kryptografiske informasjonen i forsendelsesdataene, spesielt informasjon forbundet med kryptostrengen, dekryptert for å undersøke det tilfeldige tallet som brukes ved generering av hash-verdien

Deretter blir funnet en hash-verdi (også betegnet Message Digest) for forsendelsesdataene innbefattende det dekrypterte tilfeldige tallet, og det utføres en verifisering for å fastslå hvorvidt resultatet er identisk med hash-verdien i 2D strekkoden.

I tillegg til den kryptografiske valideringen, utføres det også videre undersøkelser av innholdet (operasjon nummer 7b) som, for eksempel, forhindrer gjentatt bruk av en 2D strekkode eller undersøker hvorvidt kunden har vært påfallende på grunn av forsøk på bedrageri og derfor er svartelistet.

Det korresponderende undersøkelsesresultatet blir deretter sendt til PC-F avleseren, som sender resultatet til det optiske registreringssystemet (IMM) for koding av strekkoden. Strekkoden blir deretter trykket på brevet og forsendelsene blir utelukket i tilfellet av et negativt undersøkelsesresultat.

Kryptosystemarkitektur:

Komponent oversikt

Figur 4 gir en oversikt av subkomponentene til kryptosystemet, hvor de merkede pilene representere inngående og utgående datastrømmer for eksterne systemer. Siden det foretrukne vederlagsbeskyttelsessentralsystemet blir brukt som

dreieskive ved fordeling av nøklene fra vederlagssumladestasjonen (Porto Point) til kryptosystemet i de lokale vederlagsbeskyttelsessystemene, og disse dataene må være bufferlagret, må det her likeens være tilveiebragt en kryptosystemkomponent, men involverer generelt ikke bruk av valideringskontrolleren

Subkomponentene til kryptosystemet blir beskrevet mer detaljert under.

Valideringskontroller

Valideringskontrollerer er grensesnittet for verifisering av hele 2D strekkodeinnholdet. Verifiseringen av 2D strekkoden innbefatter en innholdsverifisering og en kryptografisk verifisering. For å oppnå dette, må 2D strekkodeinnholdet lest inn skannerne bli sendt videre til valideringskontroller av skannerkontrolleren.

Siden den ansvarlige skannerkontrolleren for den ledningsforbundede skanneren og valideringskontrolleren er på forskjellige datamaskinsystemer, er det nødvendig å tilveiebringe TCP/IP basert kommunikasjons mellom dem, ved bruk av en protokoll basert på dette, i stedet for en ren socket-programmering som medfører fordeler. Innen rammen av kryptosystemet, er det i dette tilfellet hensiktsmessig med meldingshåndtereren som brukes i driftsdataregistrering (BDE) eller protokollen som brukes innen omfanget av det optiske registreringssystemet, så som Corba/IIOP.

Valideringskontrolleren initierer de individuelle undersøkelsesrutinene, som i sin tur senter undersøkelsesresultatene til bake til denne.

Siden et mangfold av AGB granskere med forskjellige skannere blir aktive samtidig, må valideringskontrolleren være utformet med en "multisession evne". Det vil si at den må være i stand til å be om samtidige undersøkelsesforespørsler og rette det korresponderende resultatet til den korrekte skanneren. I tillegg bør den være utformet slik at den samtidig kan håndtere et mangfold undersøkelsesforespørsler og også noen av undersøkelsestrinnene, for eksempel hash-verdi undersøkelse og minimumsvederlagsundersøkelse parallelt med dette.

Ved begynnelsen av sesjonen, blir kontrolleren gjort oppmerksom på typen skannere som den kommuniserer med, og den blir tilordnet en mulighet, ved callback-metoden, å aktuere rutiner for utmating og for manuelle gjentatte undersøkelser Avhengig av driftsmodus og skannertype, blir resultatene deretter utmatet enten til radioskanneren eller til vedrelagsbeskyttelsessystemet, og det blir også registrert manuelle undersøkelsesresultater.

Kryptokort

Et spesielt problemområde er å oppbevare nøkkelen som brukes for kryptering av kryptostrengen I en 2D strekkode og for dekryptering av denne igjen av undersøkelsesårsaker. Denne nøkkelen sikrer at 2d strekkodene er beskyttet mot forfalskning og dette må derfor ikke være mulig å oppnå uten spionasje. Det er derfor nødvendig å anvende spesielle sikkerhetsforanstaltninger for å sikre at denne nøkkelen aldri er synlig å klart språk på harddisken, i minnet eller ved overføring og er i tillegg beskyttet av kraftige kryptografiske metoder.

Rene software-baserte løsninger gir ikke tilstrekkelig sikkerhet I dette tilfellet, siden det på enkelt punkter i systemet fremtrer en nøkkel I klar tekst, eller nøkkelen kan avleses I ren tekst fra minnet ved bruk av en debugger. Dette er en risiko som også er tilstede spesielt på grunn av det faktum at systemene kan fjernadministreres, eller kan forlate firmaet på grunn av reparasjoner..

I tillegg medfører de kryptografiske fremgangsmåtene en høy belastning på systemets prosessor, som ikke er optimalisert for de operasjonene som skal utføres.

Anvendelse av et kryptoprosessorkort med følgende egenskaper kan derfor anbefales:

- spesiell kryptoprosessor for akselerering av de kryptografiske metodene
- et forseglet svart bokssystem for å forhindre tilgang til sikkerhetskritiske data og metoder.

Kortene som tilfredsstiller disse egenskapene er autarkiske systemer som, avhengig av formen, er forbundet med datamaskinen via PC-bussen eller ISA-bussen og kommuniserer med software-systemene til datamaskin via en driver.

I tillegg til et batteri-bufret hovedminne, har kortene og et flash ROM mine I hvilket det er mulig å lagre en individuell applikasjonskode. Direkte tilgang til hovedminnet er ikke mulig fra eksterne systemer, noe som betyr at det sikres et meget høyt sikkerhetsnivå, siden verken nøkkeldataene eller de kryptografiske metodene for å tilveiebringe sikkerhet kan brukes bortsett fra via den beskyttede driveren.

I tillegg anvendes det dedikerte sensorer for å overvåke hvorvidt det har blitt gjort forsøk på manipulering (avhengig av kortutforming, for eksempel temperaturspisser, bestråling, åpning av beskyttelsesdeksel, spenningstopper).

Dersom det blir gjort slike manipuleringsforsøk, blir det innholdet i det batteribufrede hovedminnet slettet umiddelbart og kort blir avstengt.

For kryptoserveren, bør funksjonen for dekryptering av porto-ID, funksjonen for å undersøke hash-verdien og også funksjonen med å importere nøkkeldata være lagt direkte på kortet, siden disse rutinene er meget sikkerhetsrelevante.

Videre bør alle kryptografiske nøkler og også konfigurasjonene til sertifikatene som er nødvendig for å utføre autentiseringen på same mate være lagret I kortets batteribufrede minne. Dersom kortet ikke har tilstrekkelig minne, inneholder kortet vanligvis en masternøkkel som kan brukes til å kryptere dataene angitt over, og deretter lagre dem på systemets harddisk. Dette krever imidlertid at anvendelse av denne informasjonen først skjer etter dekryptering av dataene igjen

Tabellen under gir en oversikt over passende kortmodeller fra forskjellige produsenter og angir samtidig deres sertifiseringer.

Kryptokort for bruk i det foretrukne vederlagsbeskyttelsessystemet for PC-frankering.

Produsent	Type descriptor	Sertifisering
IBM	4758-023	FIPS PUB 140-1 Level 3 og ZKA-eCash
IBM	4758-002	FIPS PUB 140-1 Level 4 og ZKA-eCash (prob. 07/2000) CCEAL 5 (forsøkt, fremdeles I sertifiseringsfasen)
Utimaco	Krypto Server	ITSEC-E2 og ZKA-eCash
Utimaco	Krypto Server 2000 (tilgjengelig ca. 1Q/01)	FIPSPUB 140-1 Level 3, ITSEC-E3 og ZKA-eCash (forsøkt)
Racal/Zaxus	WebSentry PCI	FIPS PUB 140-1 Level 4

tillegg til å tilfredsstille kravene til kortet, betyr den ønskede BSI sertifiseringen også at det er meget viktig hvilke sertifiseringer de individuelle modellene har nå og hvilke sertifiseringer som nå er i evalueringsprosessen.

I dette tilfellet er sertifikatene som er utstedt for produktene oppdelt I tre klassifiseringer gjort av forskjellige sertifiseringsstasjon.

ITSEC er en kriteriemekanisme publisert av the European Commission I den hensikt å sertifisere IT produkter og IT systemer med hensyn til deres sikkerhetsegenskaper. Vurderingen av pålitelig er basert på nivåer E0 til E6, hvor E0

angir utilstrekkelig sikkerhet og E6 angir den høyeste sikkerheten. Videre utvikling og harmonisering med lignende internasjonale standarder er CC (Common Criteria) som for tiden er i en standardiseringsprosess ved ISO (ISO standard 15408). Denne kontrollmekanismen brukes for å vurdere systemets sikkerhet.

Det er fremdeles ikke noe produkt I tabellen over som har et sertifikat på linje med CC. IBM modellen 4758-002 er nå i en slik sertifiseringsfase.

Standarden FIPS PUB 140-1 er et kriterieverk som er utgitt av den amerikanske regjeringen for å vurdere sikkerheten til kommersielt kryptografisk utstyr. Dette kriterieverket er I meget stor grad orientert mot hardware-egenskaper. Vurderingen gjøres på fire nivåer, hvor nivå 1 angir den laveste sikkerheten, mens nivå 4 angir den høyeste sikkerheten.

I tillegg til de tidligere nevnte vurderingsstandardene, er det et ytterligere kriterieverk som er utgitt av the Central Credit Committee (ZKA) og kontrollerer lisenser for drift av IT systemer og produkter i området med elektroniske kontanter.

I tillegg til de tidligere nevnte egenskapene til kortene og de allokerte sertifiseringene, er det imidlertid også en rekke ytterligere fordeler som er kort angitt under

- mulig frembringelse av egen (signert) software og opplasting til kortet
- integrert tilfeldig tallgenerator (FIPS PUB 140-1 sertifisert)
- DES, Triple DES og SHA-1 implementert på hardware-siden
- RSA nøkkelfremstilling og privat/offentlig nøkkel- prosessering for nøkler med lengde opp til 2048 bits
- nøkkelforvaltningsfunksjoner
- sertifikatforvaltningsfunksjoner
- I en viss grad mulig med drift av et mangfold kryptokort parallelt I ett system.

Kryptogrensesnitt.

Funksjonene vedrørende sikkerhet innen rammen av kryptokortapplikasjonen er lagret direkte på kortet og er derfor kun eksternt tilgjengelig ved å bruke kortdriveren. Grensesnittet som brukes mellom driveren og valideringskontrolleren er kryptogrensesnittkonponenten, som sender forespørslene om undersøkelsesrutinene ved bruk av driveren til kortet.

Siden det er mulig å anvende et mangfold kort i en datamaskin, er oppgaven til kryptogrensesnittet også å utføre belastningsfordeling for de individuelle undersøkelsesforespørslene. Denne funksjonen er spesielt raskt, når undersøkelsesrutinene til kryptosystemet anvendes av en annen eller, avhengig av brevsenteret, et mangfold AFM-2D kodeavlesere.

En annen oppgave er håndteringen av kommunikasjonen I den hensikt å distribuere nøkkeldataene. Ved nivå 2, kan det være tilstede kun en rudimentær mekanisme som overfører de krypterte nøklene av sikkerhetshensyn i en signert fil. En forespørsel til kryptogrensesnittet vil da medføre tilveiebringelse av en utility som tillater an det kan importeres en slik fil.

Funksjoner til kryptosystemet

Undersøkelsessekvensen i valideringskontrolleren

For å underøkse 2D strekkoden, tilveiebringer valideringskontrolleren en sentral undersøkelsesfunksjon som et grensesnitt til skanneren eller avlesningssystemene. Denne undersøkelsesfunksjonen koordinerer sekvensen til de individuelle undersøkelseskomponentene.

Kodene som er sendt fra de individuelle undersøkelsesrutinekomponentene for vederlagsbeskyttelseshendelsen blir

omdannet til den passende vederlagsbeskytelseskoden ved bruk av en tidligere definert tabell som fortrinnsvis vedlikeholdes sentralt og blir overført til kryptosystemet. I denne tabellen er det i tillegg stipulert prioriteter som regulerer hvilken vederlagsbeskyttelseskode som er allokert når et mangfold vederlagsbeskyttelseshendelser har blitt oppfattet.

Denne vederlagsbeskyttelseskoden blir deretter returnert som et undersøkelsesresultat sammen med en beskrivende tekst. Avhengig av om systemet utfører ytterligere prosessering utenfor kryptosystemet, blir dette resultatet deretter utmatet på radioskanneren eller inn i vederlagsbeskyttelsesapplikasjonen, eller blir omformet til en TIT2 kode under den automatiske undersøkelsen og blir trykket på postforsendelsen.

Siden sekvensene mellom de håndholdte skannersystemene og de automatiske avlesningssystemene er forskjellige, blir det implementert en forskjellig funksjon for de to applikasjonstilfellene.

Anrop og retur av resultater er forskjellig i henhold til hvilken kommunikasjonsmekanisme som brukes mellom avlesningssystemet og valideringskontrolleren. Dersom det brukes en synkron RPC basert protokoll så som Corba/IIOP, anropes undersøkelsesmetoden direkte og undersøkelsesresultatene blir overført når undersøkelsen er ferdig. Klienten, det vil si skannerkontrolleren, og avlesningssystemet vil da vente på implementering og retur av undersøkelsesresultatene. For sistnevnte er det derfor nødvendig å tilveiebringe klienten med en threadpool, som kan utføre parallellundersøkelse av et mangfold forespørsler.

I tilfellet med den asynkrone mekanismen som anvender TGM, vil ikke skannerkontrolleren, eller avlesningssystemet, anrope undersøkelsesmetoden direkte, men i stedet blir det sendt en melding til kryptosystemet som inneholder undersøkelsesforespørselen, innholdet av 2d strekkoden og ytterligere informasjon, så som det aktuelle sorteringsprogrammet. Ved mottak av denne meldingen i kryptosystemet, anropes undersøkelsesfunksjonen, utføres og avlesnings- og undersøkelsesresultatene blir i sin tur returnert som en ny melding. Fordelen med

denne metoden er at prosessen ikke blokkeres på forespørselssystemet inntil resultatet er tilgjengelig.

Undersøkelse med håndholdte skannersystemer:

Undersøkelsesrutinen for de håndholdte skannersystemene venter på sesjons-IDen og også innholdet i 2D strekkoden som innmatingsverdier. Som en ytterligere parameter, ventes det også på IDen til sorteringsprogrammet. Sistnevnte parameter brukes til å bestemme minimumsvederlaget.

Figur 5 viser en oversikt over sekvensen av undersøkelsen I valideringskontrolleren I det tilfellet hvor undersøkelsen har blitt trigget av et handhold skannersystem. I dette tilfellet forutsettes det en undersøkelse hvor det brukes en radioskanner med etterfølgende manuell sammenligning av adressen med 2D strekkodeinnholdet. I tilfellet med en ledningsforbundet skanner, vil presentasjonen bli gjort på en tilsvarende måte på vederlagsbeskyttelsessystemet, eller på vederlagsbeskyttelsesapplikasjonen.

En foretrukket verifiseringssekvens som anvender en radioskanner, en skannerkontroller og en verifiseringsenhet (valideringskontroller) er vist i figur 5.

I det spesielt foretrukne utførelseseksempelet kontrollerer verifiseringsenheten en sekvens av undersøkelseskomponenter, hvor den første undersøkelseskomponenten innbefatter innlesing av en matrikskode som inneholdes i det digitale frankeringsmerket. Matrikskoden som har blitt avlest blir først overført fra en radioskanner til en skannerkontroller. Deretter undersøker skannerkontrollerens domene matrikskoden og sender den til verifiseringsenheten. Verifiseringsenheten splitter deretter kodeinnholdet. Det avleste resultatet blir deretter sendt til registreringsenheten – i det viste tilfellet en radioskanner. Som et resultat, finner en bruker av avlesningsenheten ut, som eksempel, at det har vært mulig å avlese frankeringsmerket og ved å gjøre dette gjenkjenne informasjonen som inneholdes i matriksen. Deretter krypterer verifiseringsenheten en kryptostreng som inneholdes i matrikskoden. For å gjøre dette, blir fortrinnsvis versjonen av nøkkelen som

sannsynligvis brukes for å danne frankeringsmerket, verifisert først. Hash-verdien i kryptostrengen blir deretter testet.

I tillegg undersøkes det minimale tilveiebragte vederlaget.

Videre verifiseres et identifikasjonsnummer (Porto ID) for kundesystemet som kontrollerer fremstillingen av frankeringsmerket.

Deretter sammenlignes identifikasjonsnummeret med en negativliste.

Disse verifiseringstrinnene gjør det mulig, på denne spesielt enkle og raske formen, å sikre frankeringsmerker produseres enkelt i henhold til autentiseringen.

Resultatet av overføringen blir sendt som en digital melding, hvilken digitale melding er i stand til å kunne sendes for eksempel til den opprinnelige radioskanneren. Som et resultat kan brukeren av radioskanneren for eksempel fjerne postforsendelsen fra forsendelsessyklusen. I tilfellet med automatisk implementering av denne metodevarianten, er det imidlertid like naturlig mulig å fjerne postforsendelsen fra den normale prosesseringssyklusen til postforsendelsene.

Fortrinnsvis blir resultatet av undersøkelsen logget i verifiseringsenhetens domene.

Som en returverdi, bør koden tilhørende vederlagsbeskyttelsestilfellet og den tilhørende tekstmeldingen og også 2D strekkoden returneres.

Undersøkelsessekvens med AFM-2D kodeavleser

Innmatingsparametrene som undersøkelsesrutinen venter op for AFM-2D avleseren er likeens sesjons-IDen, og også innholdet av 2D strekkoden og den unike identifikasjonen til sorteringsprogrammet som nå er aktivt.

Figur 6 viser en oversikt over sekvensen til undersøkelsen i valideringskontrolleren når undersøkelsen har blitt trigget av et avlesningssystem.

For å illustrere sekvensen, viser figuren også I tillegg det optiske registreringssystemet (IMM system) og også AFM-2D kodeavleseren, for å illustrere den totale rammen til undersøkelsen. Delen av kryptosystemet er imidlertid begrenset til å undersøke funksjonene mellom 2D strekkoden og returen og også logging av resultatet.

I tilfelle med meldingshåndteringsgrensesnittet, vil valideringskontrolleren starte et mangfold serviceoppgaver som ville vente på undersøkelsesforespørselsmeldingene og vill bruke meldingsinnholdet til å anrope undersøkelsesrutinen. Resultatet av undersøkelsesrutinen avventes og pakkes inn i en melding og returneres til den spørrende klienten.

Figur 6 viser en ytterligere foretrukket utførelsesform for kontroll av en sekvens av undersøkelseskomponenter av verifiseringsenheten (valideringskontroller). I dette tilfellet av den foretrukne utførelsesformen, blir frankeringsmerkene registrert av et optisk gjenkjennelsessystem (Prima/IMM). Dataene er fra den optiske verifiseringsenheten til en avlesnings- og registreringsenhet (AFM-2D kodeavleser)

I tilfellet med utførelsesformen vist I figur 6 for metoden for verifisering av gyldigheten til digitale frankeringsmerker, blir de digitale frankeringsmerkene avlest på fortrinnsvis en enda mer høyt automatisert måte, for eksempel ved hjelp av optisk registrering av en stasjon for en postforsendelse på hvilken frankeringsmerket fortrinnsvis er plassert. De ytterligere verifiseringstrinnene utføres i det vesentligste på linje med undersøkelsessekvensen vist i figur 5.

Returverdien for undersøkelsesrutinen innbefatter først vederlagsbeskyttelseskoden og en tilhørende melding og også de omdannede innholdet tillagt porto-ld'en. Disse returverdiene blir brukt til å frembringe en melding og sende denne til det forespørrende avlesningssystemet.

Innholdsundersøkelser

Oppdele og omforme 2D strekkodeinnholdet

Innmating: skannet 2D strekkode
Beskrivelse:
I denne funksjonen må 80-byte innholdet til 2D strekkoden deles opp og omdannes til et strukturert objekt, heretter betegnet som 2D strekkode-objekt, for å oppnå bedre fremvisningsmuligheter og også mer effektiv ferdiggjøring. De individuelle feltene og omdannelsene er beskrevet i tabellen under:

Ved omdannelse av de binære tallene til desimaltall, bør det huskes på at den venstre byte'n i en bytre-rekke er den mest signifikante byte'n. Dersom det ikke er mulig å omdanne, muligens på grunn av en type konflikt eller manglende data, vil det være nødvendig å generere en vederlagsbeskyttelsestilfelle-melding "PC-F strekkode uleselig" eller returnere den til valideringskontrolleren. Det er ikke hensiktsmessig med en ytterligere kryptografisk eller innholdsmessig verifisering.

Felt	Type	Skal omdannes til:	Beskrivelse
Postforetak	ASCII (3 bytes)		Omdannelse ikke nødvendig
Frankeringstype	Binær (1 byte)	Lite heltall	
Versjons-karakteristikk	Binær (1 byte)	Lite heltall	Versjonsnummer til metoden
Nøkkel nr.	Binær (1 byte)	Lite heltall	Nøkkeltype
Kryptostreng	Binær (32 bytes)		Byte-sekvens som skal overføres uendret, etter dekryptering blir porto ID delt fra.
Porto ID		Tekst (16 karakterer)	Vil bli fylt etter dekryptering av kryptostrengen.
Løpende sendingsnummer	Binær (3 bytes)	Heltall	Kun positive tall
Produktnøkkel	Binær (2 bytes)	Heltall	Positive tall, referanse til tilhørende

			referansetabell
Vederlag	Binær (2 bytes)	Float	Omdannelse til positivt desimaltall som kan deles med 100, angitt i Euro
Frankeringsdato	Binær (3 bytes)	Dato	Etter omdannelse til positivt desimaltall, kan datoen omdannes i henhold til formatet ÅÅÅÅMMDD
Postnummer mottaker	Binær (3 bytes)	2 verdier, en for land, en for postnummer	Etter omdannelse til positivt desimaltall, gir de to første tallene landekoden og de fem resterende tallene postnummeret.
Gate/postboks	ASCII (6 bytes)	Gateforkortelse eller postboks	Dersom de første karakterene er tall, har et postnummer blitt kodet, ellers er det første og de tre siste karakterene veien med husnummer
Restportosum	Binær (3 bytes)	Float + valutafelt (tekst 32 karakterer)	Etter omdannelse til et positivt desimaltall, gir et første tallet valutaen (1 = euro), de neste fire tallene anger tallene før desimalpunktet og de gjenværende to tallene anger tallene etter desimalpunktet
Hash-verdi	Binær (20 bytes)		Byte-sekvens som må overføre uendret, brukes for kryptografiske validering av frankeringen

Returverdi: 2D strekkodeobjekt

Varselkode 00 dersom omdannelse er OK

Dersom ikke, varsel for vederlagsbeskyttelsetilfelle "PC-F strekkode uleselig"

Undersøkelse av versjonsnummer

Innmating: nåværende 2D strekkodeobjekt

Beskrivelse:

De tre første feltene angir versjonen til 2D strekkoden. Av dette kan det også sees hvorvidt frankeringsmerket egentlig er en 2D strekkode forbundet med Deutsche Post og ikke en 2D strekkode forbundet med et annet postforetak. Feltinnholdet må sammenlignes med en liste over gyldige verdier som har blitt prekonfigurert i applikasjonen. Dersom det ikke finnes noe samsvar, blir det returnert et vederlagsbeskyttelsesvarsel "PC-F versjon" Verifisering av ytterligere innhold og kryptografiske aspekter blir deretter meningsløst og bør ikke utføres.

Returverdi: Varselskode 00 dersom versjonsundersøkelse OK, ellers varselkode for vederlagsbeskytelsestilfelle "PC-F versjon"

Verifiser Porto ID

Innmating: 2D strekkodeobjekt med dekryptert Porto ID

Beskrivelse:

Porto ID'en i 2D strekkoden er beskyttet av en undersøkelsessiffermetode (CRC 16) som må verifiseres ved dette punktet. Dersom verifiseringen mislykkes, vil resultatet måtte returneres som et vederlagsbeskyttelsesvarsel "PC-F antatt forfalskning (Porto ID)". Verifisering av porto ID'en krever den foregående dekrypteringen av kryptostrengen.

Returverdi: kode "00" dersom undersøkelse OK, ellers varselskode for vederlagsbeskyttelsestilfelle "PC-F antatt forfalskning (Porto ID)"

Undersøkelse av tidsoverkjøring (time overrun):

Innmating: 2D strekkodeobjekt

Beskrivelse

Denne funksjonen brukes for automatisk verifisering av tidsintervallet mellom frankering av en PC-frankert forsendelse og prosessering derav ved postsenteret. Kun et bestemt antall dager er tillatt å ligge mellom de to datoene. I dette tilfellet er antall dager basert på produktet og dets overføringstid pluss en dags venting.

Konfigurasjonen av perioden er fortrinnsvis lagret i et produktvaliditetsperiodeforhold og opprettholdes sentralt innen rammen av en vedlikeholdsmaske. For hver mulig produktnøkkel for PC frankering (2D strekkodefeltet), lagrer forholdet det tilhørende antall dager som er tillatt å ligge mellom frankering og prosessering ved postsenteret. I en forenklet metode, er kun en periodesetning prekonfigurert, som er relatert til standard forsendelser og er lagret som en konstant i systemet.

I verifiseringshensikter, er antall dager mellom nåværende testdato under prosesseringen og datoen I 2D strekkoden for eksempel 08.02. til 08.01. = 1 dag. Dersom det fastslåtte antallet dager er større enn verdien foreskrevet for produktet, vil vederlagsbeskyttelseskoden forbundet med varseltilfellet (PC-F dato (frankering)" bli returnert til valideringskontrolleren, hvis ikke blir en kode som dokumenterer vellykket undersøkelse bli returnert. Dersom en forenklet undersøkelse alltid innebærer en sammenligning med verdien for standardforsendelser, vil det etter utmating av undersøkelsesresultatet være mulig å korrigere dette undersøkelsesresultatet, for eksempel manuelt ved å bruke en knapp på skanneren, dersom foreliggende produkt tillater en lengre overføringstid.

En ytterligere undersøkelse av tidsoverkjøringen vedrører innholdet av porto ID'en. En portosum nedlastet innen rammen av en forhåndsinnstilt, og derved også porto ID'en, har en bestemt validitetsperiode innen hvilken forsendelsene må være frankert. Porto ID'en inneholder tidspunktet inntil hvilket portosummen er gyldig. Dersom frankeringsdatoen er et spesielt antall dager store enn denne gyldighetsdatoen, returneres vederlagsbeskyttelsesvarselkoden forbundet med vederlagsbeskyttelsesvarselet "PC-F dato (portosum)".

Returverdi: Kode "00" dersom undersøkelse OK,
ellers varselkode for vederlagsbeskyttelsestilfelle
"PC-F dato (portosum)" eller
"PC-F dato (franking)"

Vederlagsundersøkelse

Innmating: 2D strekkodeobjekt; nåværende sortingsprogram ID

Beskrivelse:
I denne funksjonen, blir vederlaget I 2D strekkoden undersøkt for et minimumsvederlag som er definert for forsendelser til det tilhørende sorteringsprogrammet. Summen er eurosummer.

Forbindelsene blir tilført mellom sorteringsprogrammet in minimumsvederlag via et automatisk grensesnitt.

En forenklet metode kan anvendes på en tilsvarende måte ved undersøkelse av tidsoverkjøringen. I dette tilfellet definerer konfigurasjonsfilen for applikasjonen et konstant minimumsvederlag som gjelder alle forsendelsene. Det er derfor ikke nødvendig å overføre sorteringsprogrammet.

Den etterfølgende undersøkelsen medfører sammenligning av hvorvidt minimumsvederlaget i 2D strekkoden er lavere enn dette merket. Dersom dette er tilfellet, blir koden forbundet med vederlagsbeskyttelsestilfellet "PC-F underfrankering" returnert, hvis ikke blir vellykketkoden returnert.

Returverdi: Kode "00" dersom undersøkelse OK
Ellers varselskode for vederlagsbeskyttelsestilfelle
"PC-F underfrankering"

Justering med negativfile

Innmating: 2D strekkodeobjekt med dekryptert Porto ID

Beskrivelse:
I denne funksjonen kommer undersøkelsen med å bestemme hvorvidt porto ID'en forbundet med 2D strekkoden fines I en negativfil. De negative filene blir brukt til å fjerne fra forsendelsessyklusen enhver postforsendelse fra kunder som har kommet frem i lyset på grunn av forsøk på misbruk, eller hvis PC har blitt stjålet.

I dette tilfellet håndteres negativfilene sentralt som en del av prosjektet Databasefrankering. Innen rammen til grensesnittet for dette prosjektet, må metoden for utveksling av dataene bestemmes for de lokale postsentersystemene.

Dersom vedlikeholdsapplikasjonen, eller datautvekslingen, eventuelt fremdeles ikke eksisterer, må det i dette tilfellet dannes en overgangsmekanisme. Disse dataene kan vedlikeholdes som en del av en overgang i et Excel regneark, fra hvilket det dannes en csy-fil. Denne filen kan sendes med e-mail til AGB-kontrollørene og kan leses inn i systemene av sistnevnte ved bruk av en importmekanisme som må være tilveiebragt. Senere blir overføringen gjort via en bane definert i det foretrukne vederlagsbeskyttelses-IT-finkonseptet.

En porto ID karakteriserer en innstilling som en kunde mottar fra systemet (Porto Pont). Disse innstillingene er lagret i en "safeboks" på kundens system. Dette er en maskinvarekomponent I form av et smartkort innbefattende avlesningssystem, eller en dongle. Safeboksen oppbevarer de innstilte summene på en siker måte og kunden kan hente opp individuelle frankeringssummer fra denne uten å være tilkoblet gebyrsumladestasjonen (Porto Point) online.

Hver safeboks er karakterisert av en unik ID. Denne safeboks-ID'en er lagt inn i den negative filen dersom de tilhørende forsendelsene må fjernes på grunn av mistanke om misbruk. Safeboks-ID'en utgjøres av et mangfold felter. I tillegg til den unike nøkkelen, inneholder safeboks-ID'en også ytterligere felter, så som gyldighetsdato og undersøkelsessiffer. I den hensikt å identifisere safeboksen på en entydig måte, er

det tre første feltene til safeboks-ID'en avgjørende. Disse finnes også i de tre første feltene til porto-ID'en, noe som betyr at det kan gjøres en tilordning mellom safeboksen og innstillingen. Feltene er beskrevet i tabellen under.

Byte nr.	Lengde	Betydning	Datainnhold	Kommentar
b1	1	Leverandør identifikasjon	00	Brukes ikke
			01	Testleverandør: postforsendelsesfirma
			FF	Porto point boks forbundet med postforsendelsesfirmaet
b2	1	Lisensiert modell Nr.	xx	Skal brukes for hver produsent, øker fra 01 (første leverte modell), for hver ny lisensiert modell.
b3, b4, b5	3	Modellens serienummer	xx xx xx	Skal brukes for hver lisensiert model fra hver produsent, stigende fra 00 00 01 til FF FF FF.

Dersom de tre første feltene til porto-ID'en til den aktuelle undersøkte frankeringen er identisk med de tre første feltene til en safeboks-ID som er i den negative filen, vil vederlagsbeskyttelsestilfellet forbundet med kunden i den negative filen bli returnert, ellers vil vellykketkoden bli returnert..

Returverdi: Kode "00" dersom undersøkelse OK,
ellers varselkode forbundet med kunden eller med safeboksen i negativfilen.

Sammenligning av 2D strekkodeinnhold med forsendelsesklartekst.

Innmating: 2D strekkodeobjekt

Beskrivelse:
For å forhindre at det er mulig å kopiere 2D strekkodene, blir det gjort en sammenligning av forsendelsesdata kodet I 2D strekkoden og dataene indikert i klartekst på forsendelsen. Denne sammenligning er direkte mulig med radioskannere, siden disse har tilstrekkelige visnings- og innmatingsmuligheter. I tilfellet med håndholdte skannere med en ledningsforbindelse, må undersøkelsen utføres på Pc-en (vederlagsbeskyttelsessystem).

Forløpet til sekvensen er slik at valideringskontrolleren sender ut dataene I 2D strekkoden på radioskanneren, eller på vederlagsbeskyttelses-PC'en, etter at den automatiske undersøkelsen er utført. For dette står det til disposisjon en callback-metode som er tilordnet starten av en sesjon.

Valideringskontrolleren kaller opp denne callback-metoden med det nåværende 2D-strekkodeobjektet. Skannerkontrolleren og vederlagsbeskyttelses-PC'en er da ansvarlige for å vise 2D strekkodeinnholdet og returnere en "00" eller en tilhørende feilkode, som returverdi (etter å ha blitt undersøkt av kontrolløren) for callback-metoden.

Dersom evalueringen er vellykket, blir vellykketkoden returnert, hvis ikke blir koden til vederlagsbeskyttelsesvarselet "PC-F klartekst" returnert.

I tilfellet med en automatisk undersøkelse, er denne undersøkelsen ikke nødvendig. I dette tilfellet kan undersøkelsen fortrinnsvis utføres innen rammen av de sentrale vurderingene offline, enten ved bruk av omsetningssammenligning eller ved bruk av en sammenligning av målpostnummeret og postnummeret i 2D strekkoden.

Returverdi: Kode "00" dersom undersøkelse OK,

Ellers varselkode for vederlagsbeskyttelsestilfelle "PC-F klartekst"

Kryptografiske undersøkelser

Den kryptografiske undersøkelsen omfatter to deler:

a) en dekryptering av kryptostrengen og
b) sammenligning av hash-verdien.

Begge metodene må utføres i det beskyttede området til kryptokortet, siden en kunde kan fremstille en gyldige frankerings-hash-verdier ved å spionere på informasjonen som dannes under prosesseringen.

Dekryptering av kryptostrengen

Innmating: 2D strekkodeobjekt

Beskrivelse:
Som innmatingsparameter mottar denne funksjonen det splittede 2D strekkodeobjektet fra skannerresultatet. Frankeringsdatoen og nøkkelnummeret brukes til å søke etter den symmetriske nøkkelen som er gyldig på dette tidspunktet, og det overførte objektets kryptostreng blir dekryptert ved bruk av denne nøkkelen i henhold til Triple DES CBC metoden. Hvilken verdi som må mates inn i initialiseringsvektoren, og hvorvidt innerbound eller outerbound CBC og hvilken blokklengde som brukes, blir bestemt innen rammen av grensesnittet til vederlagsbeskyttelsessystemet.

Dersom nøkkel i 2D strekkoden ikke er tilgjengelig i kryptosystemet, blir vederlagsbeskyttelsesvarselet "PC-F mistenkt svindel (nøkkel)" blir returnert med feilmeldingen om at nøkkelen ikke ble funnet ved bruk av nøkkelnummeret.

Resultatet av operasjonen innbefatter den dekrypterte porto-ID'en, og også det dekrypterte tilfeldige tallet. Den dekrypterte porto-ID'en blir lagt inn i et passende felt i 2D strekkodeobjektet. Det tilfeldige tallet bør av sikkerhetshensyn ikke bli vist, siden kunden kunne fremstille gyldige hash-verdier og derved forfalske 2D strekkodene dersom han hadde denne informasjonen

Etter dekrypteringen, blir hash-verdiberegningen hentet fra metoden og dens returverdi blir returnert.

Hash-verdi beregning.

Innmating: 2D strekkodeobjekt
Dekryptert tilfeldig tall fra kryptostrengen (det dekrypterte tilfeldige tallet må ikke være kjent utenfor kortet)

Beskrivelse:
Hash-verdiberegningsfunksjonen fastsetter de første 60 bytene fra det opprinnelige skanneresultatet i 2D strekkodeobjektet. Dette har den dekrypterte porto-ID'en og også det overførte dekrypterte tilfeldige tallet forbundet med denne. SHA 1 metoden brukes for å beregne en hash-verdi fra dette og nevnte hash-verdi blir sammenlignet med 2D strekkodens hash-verdi i 2D strekkodeobjektet. Dersom alle 20 bytene matcher, er den kryptografiske verifiseringen vellykket, og en tilhørende returverdi bli returnert.

Dersom det ikke er noen match, blir det returnert et vederlagsbeskyttelsesvarsel "PC-F antatt forfalskning (hash-verdi)" til valideringskontrolleren.

Som returverdi blir I tillett den beregnede hash-verdien sendt slik at den også kan utmates for undersøkelsesresultatet.

Returverdi: Beregnet hash-verdi
kode "00" dersom undersøkelse OK

ellers vederlagsbeskyttelsestilfelle "PC-F antatt forfalskning (hash-verdi)" eller "PC-F antatt forfalskning "nøkkel)"

Utmating av resultat

Presentere undersøkelse og avlesningsresultat

Beskrivelse:

En callback-metode gir valideringskontrolleren mulighet for å kontrollere et utmatet resultat på utmatingsenheten forbundet med foreliggende undersøkelse. For å oppnå dette overfører valideringskontrolleren 2D strekkodeobjektet og den fastslåtte vederlagsbeskyttelsesvarselkoden til denne callback-metoden. Den tilførte returverdien kan være koden til etterbearbeidingsmetoden valgt av AGB-kontrolløren.

Callback-metoden for utmatingen blir på same måte som ved starten av sesjonen tilordnet ved registrering på valideringskontrolleren.

Resultatlogging
Innmating: 2D strekkodeobjekt kode for undersøkelsesresultat

Beskrivelse:
I en forenklet metode skjer resultatloggingen i en fil på systemet på hvilket valideringskontrolleren kjører. Vanligvis blir resultatene eller direktivsettene sendt direkte til BDE og blir skrevet til databasen i det foretrukne lokale vederlagsbeskyttelsessystemet via det foretrukne vederlagsbeskyttelses-BDE-grensesnittet.

Fortrinnsvis blir porto-ID, serienummer, frankeringsdato, portoen, produktnøkkelen, postnummeret, vederlagsbeskyttelseskoden, meldingsteksten, lengde av undersøkelsen, undersøkelsestidspunktet, skannernes ID'er, skannerens driftsmodus, registreringsmodus og også typen av etterbehandling lagret. Alle verdier blir matet ut, separert fra hverandre med et semikolon, i et respektivt sett pr postforsendelse og kan evalueres ytterligere i denne form, for eksempel i Excel.

Dersom systemet er i det "innledende registrering" moduset, vil en "e" bli lagt inn i registreringsmoduskolonnen i stedet for en "n" for etterfølgende registrering.

Fremleggelse av stamdata.

Beskrivelse:
En serie stamdata er nødvendig for innholdsverifisering. Disse er:

- PC-F negativ fil
- sorteringsprogrammer og minimumsvederlag
- generelt minimumsvederlag
- produktnøkkel PC-F
- maksimal leveringstid per produktnøkkel PC-F
- generell maksimal leveringstid
- vederlagsbeskyttelsestilfeller, prioriteter og tilordning med viderebehandlingsinstruksjoner
- viderebehandlingsinstruksjoner

Stamdata kan være fast forkonfigurert i en overgangstid med unntak av den PC-F negative filen og også de kryptografiske nøklene for gebyrsumladestasjonen (Porto Point).

Om nødvendig kan det for enkelte av dataene implementeres enkle prosesserings- og fordelingsapplikasjoner. I dette tilfellet bær vedlikeholdet utføres i et Excelark, fra hvilket det genereres en csy-fil. Denne filen skal sendes til AGB-kontrolløren med e-mail og skal leses inn i systemene av ABG-kontrolløren ved bruk av en mekanisme som må være tilveiebragt.

Vanligvis er dataene fordelt på linje med metoden beskrevet I det foretrukne vederlagsbeskyttelses-IT-finkonseptet, eller det gis tilgang til disse dataene.

De tilhørende datastrukturene er beskrevet i datamodellen for det foretrukne vederlagsbeskyttelses-IT-finkonseptet.

Distribusjon av nøkkeldataene.

De symmetriske nøklene, som brukes I gebyrsumladestasjonen (Porto Point) I den hensikt å beskytte 2D strekkodeinnholdet og som er nødvendig for validering I kryptosystemet, blir av sikkerhetsmessige årsaker utvekslet med jevne mellomrom. Når de anvendes i alle postsentrene, vil nøklene måtte overføres automatisk og sikkert fra (Porto Point) til kryptosystemene.

I dette tilfellet, bør utvekslingen skje via den foretrukne vederlagsbeskyttelsesserveren, siden gebyrsumladestasjonen (Porto Point) ikke bør ha noen konfigurasjon med hensyn til hvilke foretrukne lokale vederlagsbeskyttelsessystemer og hvilke kryptosystemer eksisterer for disse.

Spesielt foretrukne metodetrinn er utveksling av nøkler er vist i figur 7. Den foretrukne utvekslingen av nøkler skjer mellom en sentral ladestasjon (Porto Point), en sentral kryptoserver og et mangfold lokale kryptoservere.

Siden de symmetriske nøklene er av stor betydning for 2D strekkodenes forfalskningssikkerhet, må utvekslingen være beskyttet av et høyt nivå av kryptografi og ved entydig autentisering av kommunikasjonspartnerne.

Konfigurasjon

Grunnleggende konfigurasjon/nøkkelhåndtering til kryptomaskinvaren.

For kryptokortets grunnleggende konfigurasjon, er det nødvendig med visse foranstaltninger. Disse kan være utført av en sikkerhetsadministrator. De medfører grovt følgende aktiviteter:

- installasjon av programvare-API på kortet

- generering og installasjon av private nøkler for beskyttelse av administrasjonsapplikasjoner og nedlastbar programvare.

Avhengig av den valgte korttypen og kortprodusenten, krever dette forskjellige foranstaltninger.

Kryptokortets applikasjonsrelaterte grunnleggende konfigurasjon tilveiebragt for det foretrukne vederlagsbeskyttelsessystemet innbefatter følgende trinn:

- Sikker kryptering og overføring av de symmetriske nøklene til kortet – for eksempel RSA krypteringspar – med simultan sertifikatgenerering for den offentlige nøkkelen og utmating av nøkkelen
- fast prekonfigurere et sertifikat for gebyrsumladestasjonen (Porto Point) for å sikre at nøkkelen som skal importeres har blitt utstedt av gebyrsumladestasjonen (Porto Point).

Grunnleggende konfigurasjon av kryptosystemapplikasjonen.

Hver skanner, hver bruker og hvert Kryptokort I kryptosystemet må være kjennetegnet av en unik ID. Endelig er det også nødvendig å identifisere hver AFM-2D kodeavleser ved hjelp av en unik ID.

Login/logoff

Ved starten av en sesjon med valideringskontrolleren, må det være en login. Som parametre, inneholder dette login skanner-ID'en, bruker-ID'en og også callback-metodene for den manuelle undersøkelsen, eller utmating av avlesningen og undersøkelsesresultatene.

Den returnerte returverdien er en sesjons-ID som også må overføres ved etterfølgende undersøkelsesanrop i sesjonen. For sesjons-ID'en, blir en

sesjonskontekst lagret på valideringskontrolleren, hvilken sesjonskontekst lagrer overføringsparametrene.

Dersom brukere under denne sesjonen gjør endringer av driftsmodusen til de predefinerte produktet, eller andre sesjonsinnstillinger som kan konfigureres under driftstiden, blir disse endringene rekonstruert i variabler allokert av denne hensikt i sesjonskonteksten.

For en logoff, blir om passende sesjonskonteksten ødelagt. Etterfølgende undersøkelsesanrop med denne sesjons-ID'en blir forkastet.

Denne håndteringen av brukere og passord må være definert i et generelt brukerhåndteringskonsept for foretrukken vederlagsbeskyttelse, som er en del av det foretrukne vederlagsbeskyttelses-IT-finkonseptet.

Avlesningssystemene må være registrert med valideringskontrolleren før undersøkelsesforespørselen blir utført. Parametrene som skal overføres er avlesningssystemets ID og også et passord. Returverdien som returneres ved en vellykket registrering er på samme måte en sesjons-ID, som må sendes ved etterfølgende verifiseringsforespørsler.

Når avlesningssystemet er avslått. Må det være en korresponderende logoff med denne sesjons-ID.

Diverse

Spesielle brukerroller.

Innen rammen til sikkerhetskonseptet, må det være tilveiebragt to spesielle brukerroller, som må utføres av forskjellige mennesker.

Sikkerhetsadministrator

Rollen til sikkerhetsadministrator består av følgende oppgaver:
:

- danne kommandofiler for administrasjon av kryptokortet
- signere disse kommandofilene
- initialisere og håndtere kryptokortene
- overvåke ned nedlastbare programvaren og tilhørende konfigurasjon

Sikkerhetsadministratoren autentiserer seg selv ved bruk av den private nøkkelen for kortadministrasjon. Denne er lagret på en diskett eller smartkort og må alltid være strengt nedlåst av sikkerhetsadministratoren.

Kun administrasjonskommandoer signert ved bruk av denne nøkkelen kan utføres på kryptokortet. Siden denne mekanismen beskyter kommandosekvensen og de tilhørende parametre, kan utførelsen av disse kommandoene også være delegert til systemadministratorer in situ. For å oppnå dette må sikkerhetsadministratoren gjøre kommandoene tilgjengelige og skrive passende metodeinstruksjoner.

En annen oppgave er håndtering av kryptokortene, med serienummer, konfigurasjon og systemnummer til system i hvilket disse kortene er installert, og også lokaliseringen til hvert kort i systemet blir registrert. For reserve kryptokortene, er det også et register over hvem som har kortene.

Sammen med sikkerhetssjefen QA, overvåker han programvarekildene og den tilhørende programvarekonfigurasjonen og gjør dem mulige for installasjon.

I tillegg blir programvare som må installeres, eller er installer, på kortet og på kryptoserveren undersøkt og kortprogrammet blir også gjort klart og signert.

Kortprogramvaren må spesielt undersøkes for å bestemme hvorvidt de hemmelige nøklene på noe punkt kan komme ut via drivergrensesnittet, eller hvorvidt det her har

blitt gjort manipuleringsforsøk, så som lagring av konstants predefinerte nøkler eller bruk av usikre krypteringsmetoder. I tillegg til kortets programvare, er det også nødvendig å undersøke kryptoserverens applikasjonsprogramvare som er forbundet med nevnte kortprogramvare.

Autentisering blir utført på nøyaktig samme måte som i tilfelles med sikkerhetsadministratoren som bruker en privat nøkkel. I dette tilfellet er det imidlertid involvert en privat nøkkel for programvaresignering.

En ytterligere sikkerhet I dette tilfellet, medfører installasjon av programvaren krever ikke bare at programvaren er signert, men også de tilhørende installasjonskommandoene. Siden to forskjellige mennesker (QA sjef og sikkerhetsadministrator) er ansvarlige for dette, og siden de tilhørende nøklene blir holdt på to forskjellige steder, blir det på samme måte oppnådd en høy grad av sikkerhet også i dette tilfellet.

Programvaren blir distribuert av sikkerhets-QA sjefen i overensstemmelse med sikkerhetsadministratoren.

Denne spesielt foretrukne utførelsesformen av oppfinnelsen gir derved to forskjellige autentiseringsnøkler, noe som betyr at datasikkerheten er økt betydelig grad.

P a t e n t k r a v

1.

Fremgangsmåte ved verifisering av gyldigheten av et frankeringsmerke som har blitt satt på et brevstykke, hvor kryptografisk informasjon i frankeringsmerket blir dekryptert og anvendt for verifisering av frankeringsmerkets gyldighet,
k a r a k t e r i s e r t v e d at verifiseringen skjer i et system innbefattende en verifiseringsenhet og flere avlesningsenheter,
hvorved en av avlesningsenhetene grafisk registrerer et frankeringsmerke og matrikskoden i frankeringsmerket blir overført til verifiseringsenheten,
hvorved verifiseringsenheten kontrollerer en sekvens av partielle undersøkelser for den mottatte matrikskoden,
hvorved verifiseringsenheten samtidig utfører partielle undersøkelser av den mottatte matrikskoden, og
hvorved verifiseringsenheten sender undersøkelsesresultatene fra den mottatte matrikskoden til den korrekte avlesningsenheten.

2.

Fremgangsmåte i henhold til krav 1,
k a r a k t e r i s e r t v e d at en av undersøkelseskomponentene innbefatter dekryptering av den kryptografiske informasjonen i frankeringsmerket.

3.

Fremgangsmåte i henhold til et eller flere av kravene 1 til 2,
k a r a k t e r i s e r t v e d at en av undersøkelseskomponentene innbefatter en sammenligning mellom produksjonsdatoen til frankeringsmerket og nåværende dato.

4.

Fremgangsmåte i henhold til et eller flere av de foregående krav,

k a r a k t e r i s e r t v e d at den ene avlesningsenheten og verifiseringsenheten utveksler informasjon ved bruk av en synkron protokoll.

5.

Fremgangsmåte i henhold til krav 4,
k a r a k t e r i s e r t v e d at protokollen er RPC-basert.

6.

Fremgangsmåte i henhold til et eller flere av kravene 1 til 5,
k a r a k t e r i s e r t v e d at den ene avlesningsenheten og verifiseringsenheten kommuniserer med hverandre ved bruk av en asynkron protokoll.

7.

Fremgangsmåte i henhold til krav 6,
k a r a k t e r i s e r t v e d at den ene avlesningsenheten sender en datamelding til verifiseringsenheten.

8.

Fremgangsmåte i henhold til krav 7,
k a r a k t e r i s e r t v e d at datameldingen inneholder innholdet av frankeringsmerket.

9.

Fremgangsmåte i henhold til et eller flere av kravene 1 til 8,
k a r a k t e r i s e r t v e d at datameldingen inneholder en forespørsel om å starte en kryptografisk verifiseringsrutine.

10.

Fremgangsmåte i henhold til et eller flere av kravene 1 til 9,
k a r a k t e r i s e r t v e d at et kryptogrensesnitt utfører en lastfordeling mellom et mangfold verifiseringsanordninger.

11.

Fremgangsmåte i henhold til et eller flere av kravene 1 til 10, k a r a k t e r i s e r t v e d at innholdet I frankeringsmerket blir oppdelt i individuelle felter.

12.

Fremgangsmåte i henhold til et eller flere av de foregående krav, k a r a k t e r i s e r t v e d at et identifikasjonsnummer (porto-ID) for kundesystemet som kontrollerer produksjonen av frankeringsmerket blir fastslått fra frankeringsmerket.

13.

Fremgangsmåte i henhold til et eller flere av de foregående krav, k a r a k t e r i s e r t v e d at individuelle kundesystem-identifikasjonsspesifikasjoner (porto-ID) blir registrert i en negativ fil, og brevstykkene forbundet med denne porto-ID'en blir fjernet fra en normal prosesseringsprogresjon for brevstykker.

14.

Fremgangsmåte i henhold til et eller flere av de foregående krav, k a r a k t e r i s e r t v e d at en kryptert mottageradressesetning i frankeringsmerket blir sammenlignet med en mottageradresse indikert for levering av brevstykket.

15.

Fremgangsmåte i henhold til et eller flere av kravene 1 til 14, k a r a k t e r i s e r t v e d at verifiseringsparametre for fremgangsmåten kan endres.

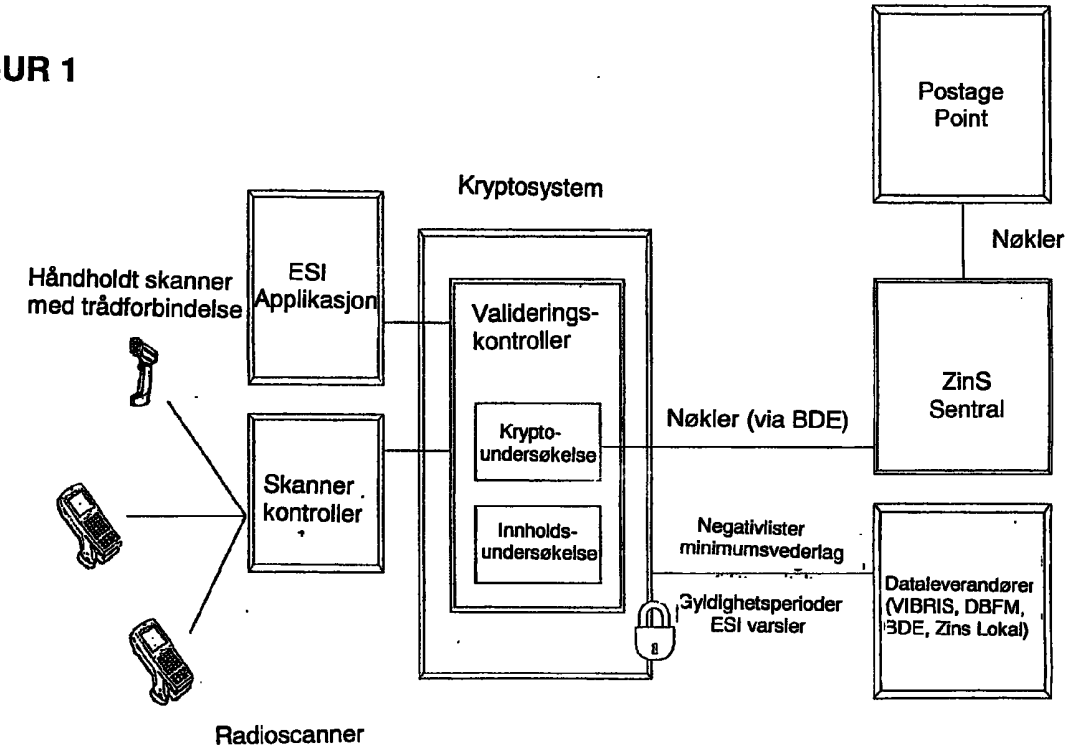
16.

Fremgangsmåte i henhold til krav 15,

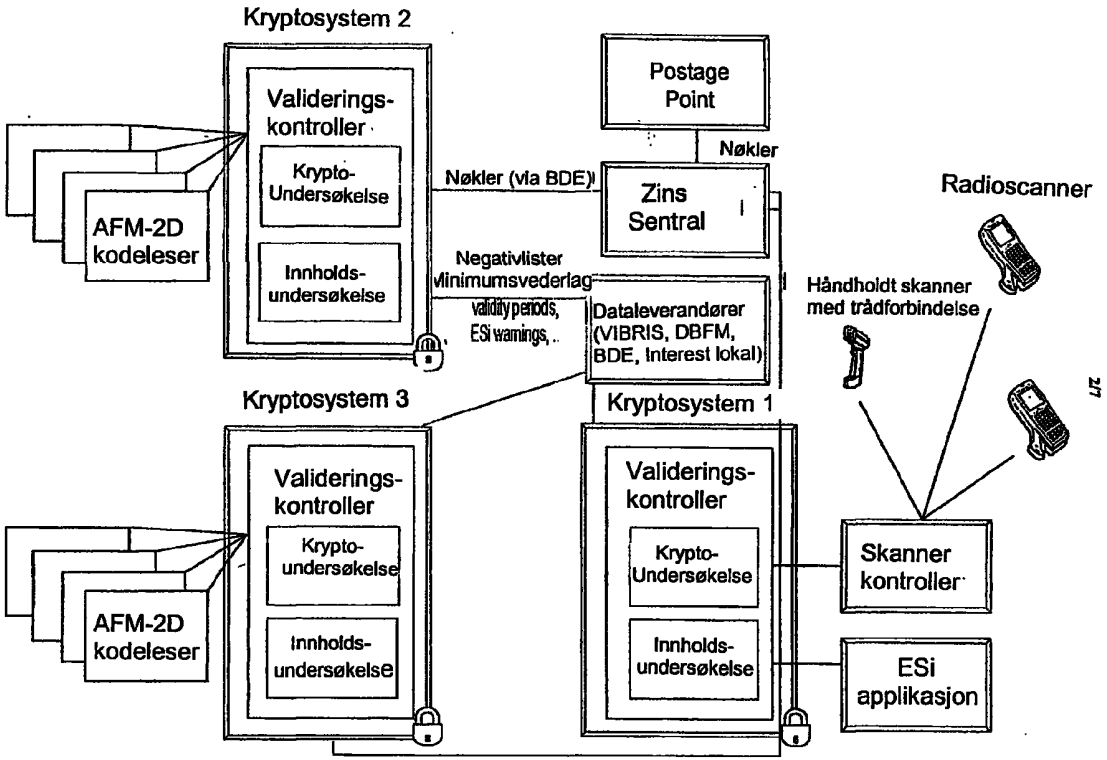
k a r a k t e r i s e r t v e d at fremgangsmåteparametrene kun blir endret etter innmating av en personlig digital nøkkel (privat nøkkel) forbundet med en systemadministrator.

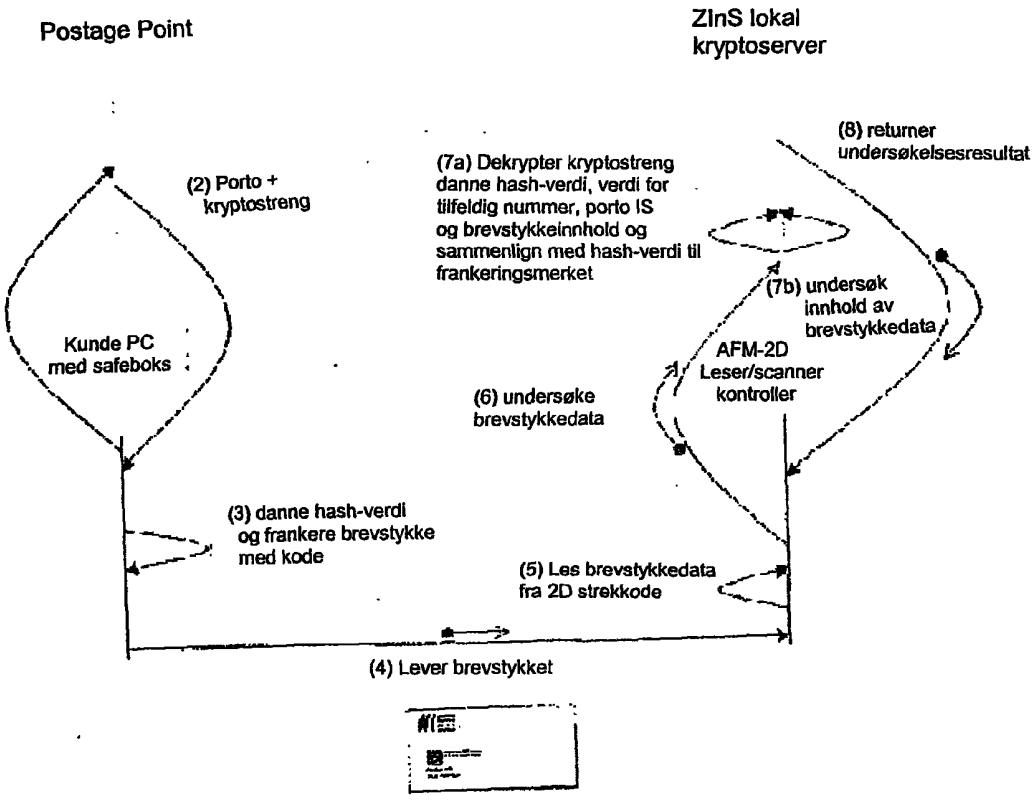
5

FIGUR 1


Postage Point
Nøkler
Kryptosystem
Håndholdt skanner med trådforbindelse
ESI Applikasjon
Valideringskontroller
Krypto-undersøkelse
Innholds-undersøkelse
Skanner kontroller
Nøkler (via BDE)
ZinS Sentral
Negativlister minimumsvederlag
Gyldighetsperioder ESI varsler
Dataleverandører (VIBRIS, DBFM, BDE, Zins Lokal)
Radioscanner

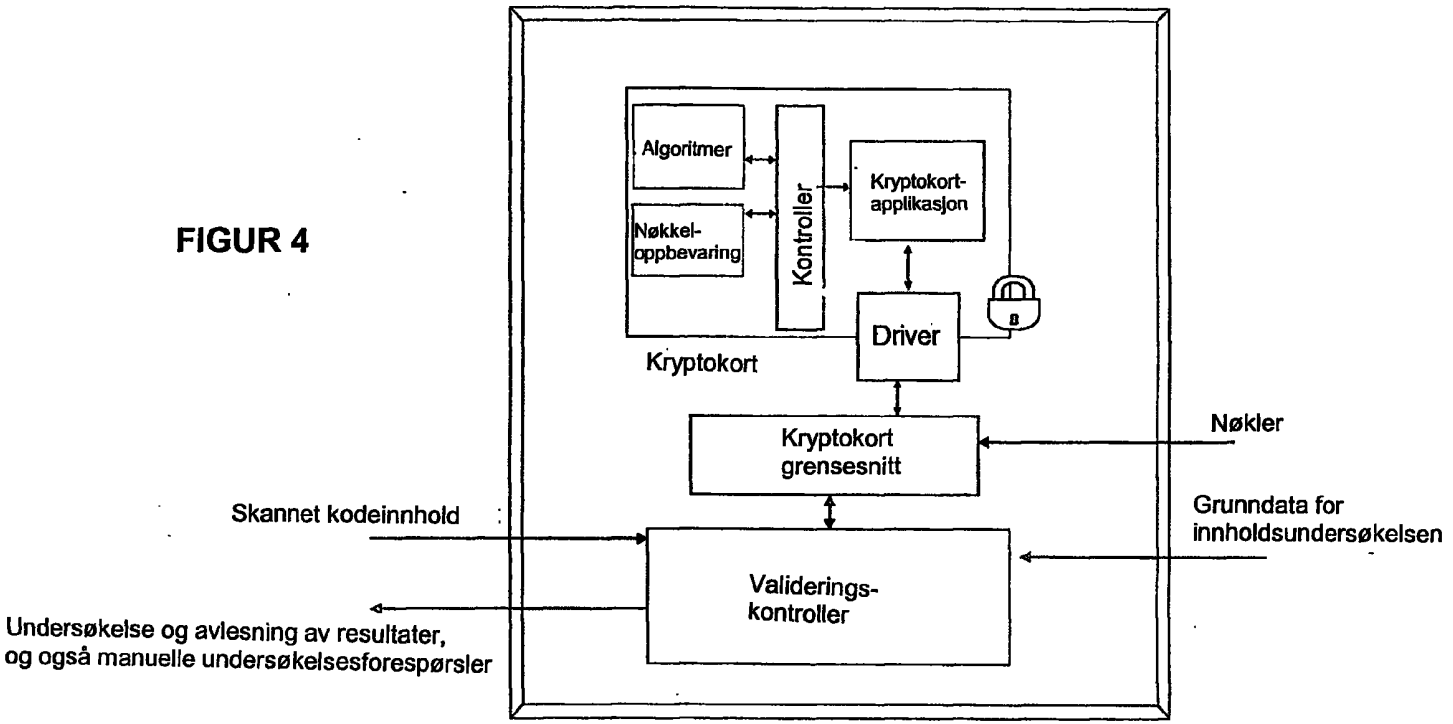
FIGUR 2

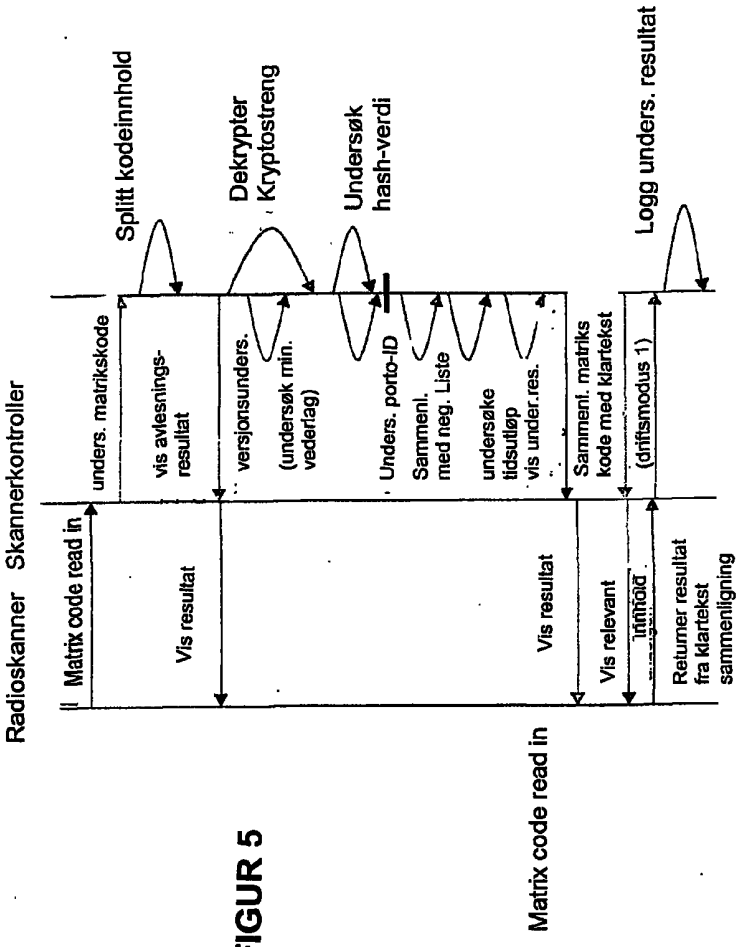

Kryptosystem 2
Valideringskontroller
Krypto-Undersøkelse
Innholds-undersøkelse
AFM-2D kodeleser
Postage Point
Nøkler
Nøkler (via BDE)
Zins Sentral
Radioscanner
Negativlister
Minimumsvederlag
validity periods,
ESi warnings, ..
Dataleverandører (VIBRIS, DBFM, BDE, Interest lokal)
Håndholdt skanner med trådforbindelse
Kryptosystem 3
Kryptosystem 1
Valideringskontroller
Krypto-undersøkelse
Innholds-undersøkelse
AFM-2D kodeleser
Valideringskontroller
Krypto-Undersøkelse
Innholds-undersøkelse
Skanner kontroller
ESi applikasjon


Postage Point
ZInS lokal kryptoserver
(8) returner undersøkelsesresultat
(7a) Dekrypter kryptostreng danne hash-verdi, verdi for tilfeldig nummer, porto IS og brevstykkeinnhold og sammenlign med hash-verdi til frankeringsmerket
(2) Porto + kryptostreng
(7b) undersøk innhold av brevstykkedata
Kunde PC med safeboks
AFM-2D Leser/scanner kontroller
(6) undersøke brevstykkedata
(3) danne hash-verdi og frankere brevstykke med kode
(5) Les brevstykkedata fra 2D strekkode
(4) Lever brevstykket

FIGUR 3

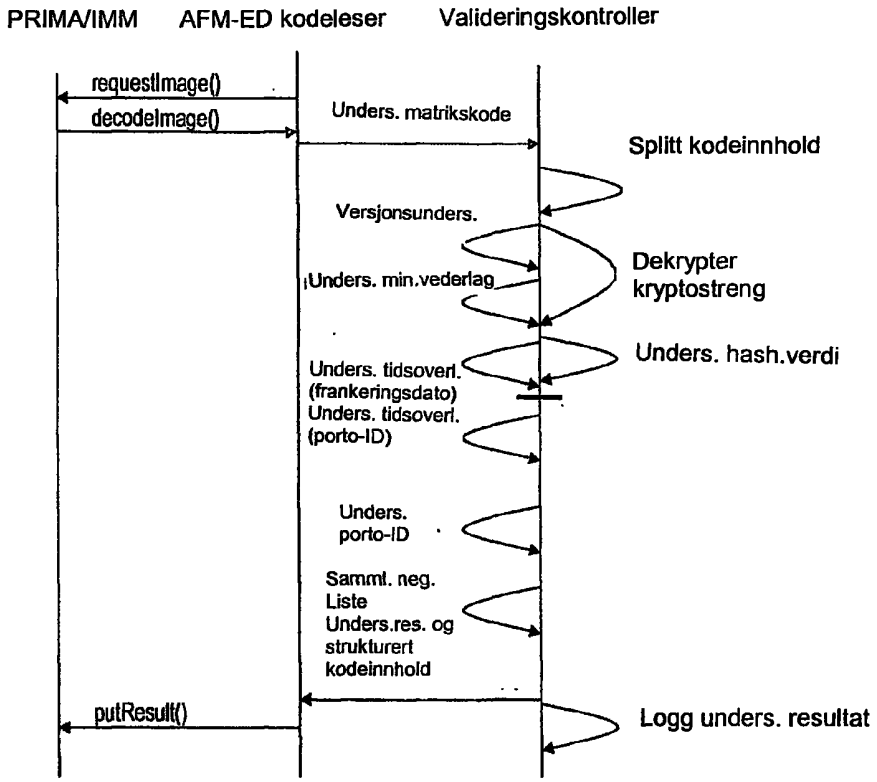
FIGUR 4

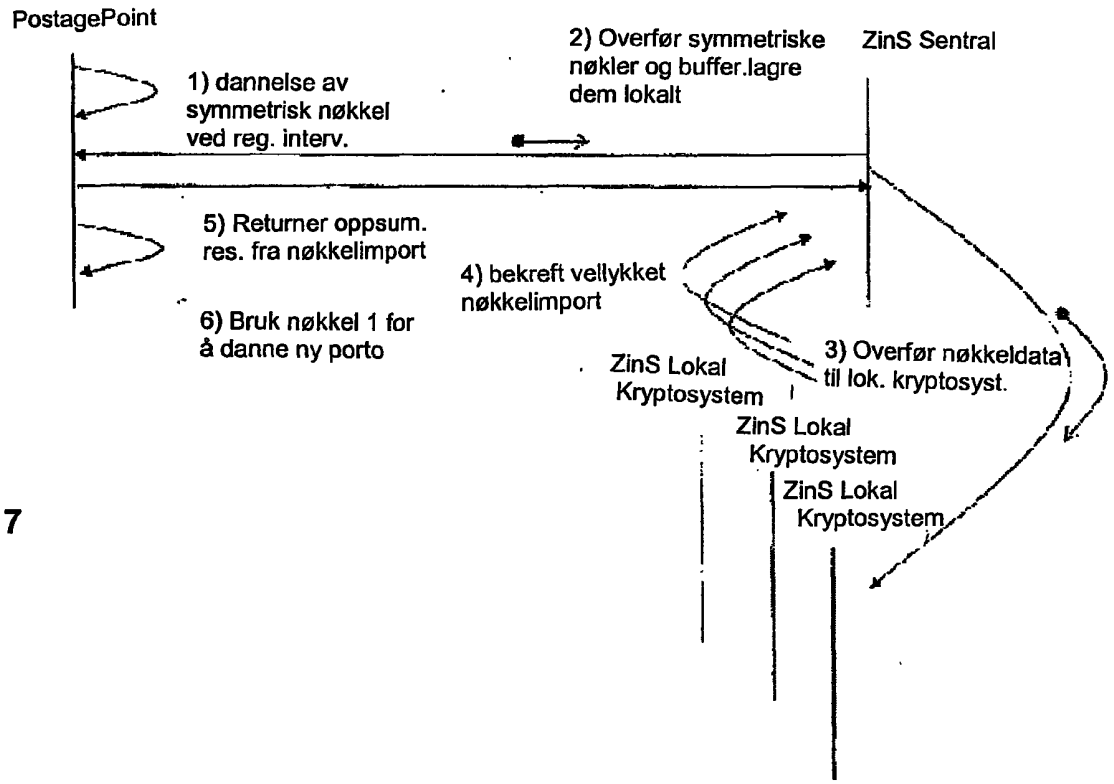

Algoritmer
Nøkkel-oppbevaring
Kontroller
Kryptokort-applikasjon
Driver
Kryptokort
Kryptokort grensesnitt
Nøkler
Skannet kodeinnhold
Grunndata for innholdsundersøkelsen
Valideringskontroller
Undersøkelse og avlesning av resultater, og også manuelle undersøkelsesforespørsler


Radioskanner
Skannerkontroller
Matrix code read in
unders. matrikskode
vis avlesnings-resultat
Vis resultat
versjonsunders.
(undersøk min. vederlag)
Splitt kodeinnhold
Dekrypter Kryptostreng
Undersøk hash-verdi
Unders. porto-ID
Sammenl. med neg. Liste
undersøke tidsutløp
vis under.res.
Vis resultat
Sammenl. matriks kode med klartekst
Vis relevant
(driftsmodus 1)
innhold
Returner resultat fra klartekst sammenligning
Logg unders. resultat
Matrix code read in

FIGUR 5

FIGUR 6


PRIMA/IMM
AFM-ED kodeleser
Valideringskontroller
requestImage()
decodeImage()
Unders. matrikskode
Splitt kodeinnhold
Versjonsunders.
Unders. min.vederlag
Dekrypter kryptostreng
Unders. hash.verdi
Unders. tidsoverl. (frankeringsdato)
Unders. tidsoverl. (porto-ID)
Unders. porto-ID
Samml. neg. Liste Unders.res. og strukturert kodeinnhold
putResult()
Logg unders. resultat


PostagePoint
1) dannelse av symmetrisk nøkkel ved reg. interv.
2) Overfør symmetriske nøkler og buffer.lagre dem lokalt
ZinS Sentral
5) Returner oppsum. res. fra nøkkelimport
4) bekreft vellykket nøkkelimport
6) Bruk nøkkel 1 for å danne ny porto
3) Overfør nøkkeldata til lok. kryptosyst.
ZinS Lokal Kryptosystem
ZinS Lokal Kryptosystem
ZinS Lokal Kryptosystem

FIGUR 7