(12) **Translation of European patent specification**

(11) **NO/EP 3935536 B1**

NORWAY

(19) NO

(51) Int Cl.

G06F 21/53 (2013.01)

G06F 9/455 (2018.01)

Norwegian Industrial Property Office

(45)	Translation Published	2023.10.02
(80)	Date of The European Patent Office Publication of the Granted Patent	2023.08.16
(86)	European Application Nr.	20707417.0
(86)	European Filing Date	2020.02.27
(87)	The European Application's Publication Date	2022.01.12
(30)	Priority	2019.03.08, US, 201916296478
(84)	Designated Contracting States:	AL ; AT ; BE ; BG ; CH ; CY ; CZ ; DE ; DK ; EE ; ES ; FI ; FR ; GB ; GR ; HR ; HU ; IE ; IS ; IT ; LI ; LT ; LU ; LV ; MC ; MK ; MT ; NL ; NO ; PL ; PT ; RO ; RS ; SE ; SI ; SK ; SM ; TR
(73)	Proprietor	International Business Machines Corporation, New Orchard Road, Armonk, New York 10504, USA
(72)	Inventor	BUENDGEN, Reinhard, c/o IBM Deutschland Research & Development GmbH Schoenaicher Strasse 220, 71032 Boeblingen, Tyskland BRADBURY, Jonathan, c/o IBM Corp. 2455 South Road, Poughkeepsie, New York 12601, USA
(74)	Agent or Attorney	BRYN AARFLOT AS, Stortingsgata 8, 0161 OSLO, Norge

(54) Title **SECURE EXECUTION GUEST OWNER CONTROLS FOR SECURE INTERFACE CONTROL**

(56) References Cited:

EP-A1- 3 140 770

US-A1- 2018 239 892

US-A1- 2016 148 001

US-A1- 2015 178 504

Enclosed is a translation of the patent claims in Norwegian. Please note that as per the Norwegian Patents Acts, section 66i the patent will receive protection in Norway only as far as there is agreement between the translation and the language of the application/patent granted at the EPO. In matters concerning the validity of the patent, language of the application/patent granted at the EPO will be used as the basis for the decision. The patent documents published by the EPO are available through Espacenet (http://worldwide.espacenet.com) or via the search engine on our website here: https://search.patentstyret.no/

Patentkrav

1. En datamaskin-implementert fremgangsmåte, omfattende:

å oppnå, ved hjelp av en sikker grensesnittkontroll (230, 250) i et datasystem, krypterte metadata (240) som omfatter én eller flere kontroller (260), metadataene (240) er kryptografisk koblet til en datafil med oppstartprogram av en sikker gjest (210) for å startes av en eier og administreres av en hypervisor (230), hvori metadataene (240) er utilgjengelige for den sikre gjesten (210) og for hypervisoren (230), hvori hver kontroll av den ene eller flere kontroller som inngår i metadataene (240) er en granulær kontroll av funksjonalitet som indikerer til den sikre grensesnittkontrollen (250) om den sikre gjesten (210) generert fra datafilen med oppstartprogram har tillatelse til å få et svar på en bestemt forespørsel, hvori den sikre grensesnittkontrollen (250) er kommunikativt koblet til hypervisoren (230), hvor hypervisoren (230) administrerer én eller flere gjester inkludert sikre gjester (210);
oppfangning, ved hjelp av den sikre grensesnittkontrollen (250), via hypervisoren (230), fra den sikre gjesten (210) generert fra datafilen med oppstartprogram, under kjøretiden til den sikre gjesten (210), en forespørsel;
å gi tilgang, ved hjelp av den sikre grensesnittkontrollen (250), den ene eller flere kontroller (260) i metadataene (240) ved å bruke en privat vertsnøkkel;
å bestemme, ved hjelp av den sikre grensesnittkontrollen (250), basert på den ene eller flere kontroller (260), om den sikre gjesten (210) har tillatelse til å motta et svar på forespørselen;
basert på å bestemme at den sikre gjesten (210) har tillatelse til å oppnå svaret, ved å starte, ved den sikre grensesnittkontrollen (250), oppfyllelse av forespørselen, innenfor databehandlingssystemet; og
basert på å bestemme at den sikre gjesten (210) ikke har tillatelse til å oppnå svaret, og ignorerer, av den sikre grensesnittkontrollen (250), forespørselen.

2. Den datamaskin-implementerte fremgangsmåten ifølge krav 1, hvori innledningen omfatter:

å oppnå, ved hjelp av den sikre grensesnittkontrollen (250), svaret på forespørselen; og
å overføre, ved hjelp av den sikre grensesnittkontrollen (250), svaret til den sikre gjesten (210).

3. Den datamaskin-implementerte fremgangsmåten ifølge krav 1 eller 2, hvori tilgangen til én eller flere kontroller (260) i metadataene (240) videre omfatter:
dekryptere, ved hjelp av den sikre grensesnittkontrollen (250), en del av metadataene (240) koblet til datafilen med oppstartprogram til den sikre gjesten (210), hvori metadataene (240) er integritetsbeskyttet og delen ble kryptert med en nøkkel utledet ved bruk av den private vertsnøkkelen som omfatter et kryptografisk mål på datafilen med oppstartprogram til den sikre gjesten (210).

4. Den datamaskin-implementerte fremgangsmåten ifølge krav 3, hvori den krypterte delen av metadataene (240) omfatter den ene eller flere kontroller (260).

5. Den datamaskin-implementerte fremgangsmåten ifølge krav 3 eller 4, hvori forespørselen er valgt fra gruppen bestående av: en forespørsel til den sikre grensesnittkontrollen (250) om å sende ut en innkapslet nøkkel brukt til å eksportere en side, en forespørsel til den sikre grensesnittkontrollen (250) for å generere metadata (240) for en oppdatert versjon av datafilen med oppstartprogram til den sikre gjesten (210), en forespørsel om å tillate den sikre grensesnittkontrollen (250) å kryptere data

ved å bruke nøkler gitt i metadataene (240) og returnere de krypterte dataene til den sikre gjesten (210).

6. Den datamaskin-implementerte fremgangsmåten ifølge ett av kravene 3 til 5, hvori svaret på forespørselen er valgt fra gruppen som består av: den innkapslede nøkkelen som brukes til å eksportere siden, metadataene (240) for den oppdaterte versjonen av datafilen med oppstartprogram til den sikre gjesten (210), og krypterte data, hvori de krypterte dataene ble kryptert av den sikre grensesnittkontrollen (250) ved bruk av nøklene tilveiebrakt i metadataene (240).

7. Den datamaskin-implementert fremgangsmåten ifølge ett av kravene 3 til 6, hvori den private vertsnøkkelen eies av den sikre grensesnittkontrollen (250) og brukes utelukkende av den sikre grensesnittkontrollen (250).

8. Den datamaskin-implementerte fremgangsmåten ifølge krav 7, hvori nøkkelen utledet ved bruk av den private vertsnøkkelen deles mellom den sikre grensesnittkontrollen (250) og eieren.

9. Den datamaskin-implementerte fremgangsmåten ifølge ett av kravene 1 til 8, hvori metadataene (240) omfatter verdier utledet fra et oppstartsbilde av den sikre gjesten (210) beregnet ved bruk av en kollisjonsbestandig enveisfunksjon.

10. Den Datamaskin-implementerte fremgangsmåten ifølge ett av kravene 1 til 9, hvori den ene eller flere kontroller (260) hver omfatter en positiv betegnelse eller en negativ betegnelse for forskjellige funksjoner, hvori den positive betegnelsen indikerer at den sikre gjesten (210) har tillatelse til å innhente svaret på den bestemte forespørselen, og den negative betegnelsen indikerer at gjesten ikke har tillatelse til å motta svaret på den bestemte forespørselen.

11. Den datamaskin-implementerte fremgangsmåten ifølge ett av kravene 1 til 10, hvori å bestemme om den sikre gjesten (210) har tillatelse til å få svaret på forespørselen, videre omfatter:

> å identifisere, ved hjelp av den sikre grensesnittkontrollen (250), i den ene eller flere kontroller (260), en kontroll som er relevant for forespørselen; og
> å bestemme, ved hjelp av den sikre grensesnittkontrollen (250), om kontrollen muliggjør eller begrenser mottak av svaret på forespørselen fra den sikre gjesten (210).

12. Et dataprogramprodukt som omfatter:
et datamaskinlesbart lagringsmedium som kan leses av én eller flere prosessorer (16) og lagre instruksjoner for utførelse av én eller flere prosessorer (16) for å utføre en fremgangsmåte som omfatter:

> å oppnå, ved hjelp av en sikker grensesnittkontroll (250) i et datasystem utført av den ene eller flere prosessorene (16) i datasystemet, krypterte metadata (240) som omfatter én eller flere kontroller (260), metadataene (240) er kryptografisk koblet til et oppstartsbilde av en sikker gjest (210) som skal startes av en eier og administreres av en hypervisor (230), hvori metadataene (240) er utilgjengelige for den sikre gjesten (210) og for hypervisoren (230), der hver kontroll av den ene eller flere kontroller som er inkludert i metadataene (240) er en granulær kontroll av funksjonalitet som indikerer til den sikre grensesnittkontrollen (250) om den sikre gjesten (210) generert fra datafilen med oppstartprogram har tillatelse til å få et svar på en spesiell forespørsel, hvori den ene eller flere prosessorene (16) er kommunikativt koblet til hypervisoren (230), hvor

hypervisoren (230) administrerer én eller flere gjester inkludert én eller flere sikre gjester (210);
oppfange, ved hjelp av den sikre grensesnittkontrollen (250), via hypervisoren (230), fra den sikre gjesten (210) generert fra datafilen med oppstartprogram, under kjøretiden til den sikre gjesten (210), en forespørsel;
å gi tilgang, ved hjelp av den sikre grensesnittkontrollen (250), den ene eller flere kontroller (260) i metadataene (240) ved å bruke en privat vertsnøkkel;
å bestemme, ved hjelp av den sikre grensesnittkontrollen (250), basert på den ene eller flere kontroller (260), om den sikre gjesten (210) har tillatelse til å motta et svar på forespørselen;
basert på å bestemme at den sikre gjesten (210) har tillatelse til å oppnå svaret, ved å starte, ved den sikre grensesnittkontrollen (250), oppfyllelse av forespørselen, innenfor databehandlingssystemet; og
basert på å bestemme at den sikre gjesten (210) ikke har tillatelse til å oppnå svaret, og ignorerer, av den sikre grensesnittkontrollen (250), forespørselen.

13. Dataprogramproduktet ifølge krav 12, hvori innledningen omfatter:

å oppnå, ved hjelp av den sikre grensesnittkontrollen (250), svaret på forespørselen; og
å overføre, ved hjelp av den sikre grensesnittkontrollen (250), svaret til den sikre gjesten (210).

14. Dataprogramproduktet ifølge krav 12 eller 13, hvori tilgangen til én eller flere kontroller (260) i metadataene (240) videre omfatter
dekryptering, ved hjelp av den sikre grensesnittkontrollen (250), en del av metadataene (240) knyttet til datafilen med oppstartprogram til den sikre gjesten (210), hvori metadataene (240) er integritetsbeskyttet og delen ble kryptert med en nøkkel utledet bruk ved av den private vertsnøkkelen som omfatter et kryptografisk mål på datafilen med oppstartprogram til den sikre gjesten (210).

15. Dataprogramproduktet ifølge ett av kravene 12 til 14, hvori forespørselen er valgt fra gruppen bestående av: en forespørsel til en eller flere prosessorer (16) om å sende ut en innkapslet nøkkel brukt til å eksportere en side, en forespørsel til den ene eller flere prosessorer (16) for å generere metadata (240) for en oppdatert versjon av datafilen med oppstartprogram til den sikre gjesten (210), en forespørsel om å tillate en eller flere prosessorer (16) å kryptere data ved å bruke nøkler gitt i metadataene (240) og returner de krypterte dataene til den sikre gjesten (210).

16. Dataprogramproduktet ifølge ett av kravene 12 til 15, hvori svaret på forespørselen er valgt fra gruppen som består av: den innkapslede nøkkelen som brukes til å eksportere siden, metadataene (240) for den oppdaterte versjonen av datafilen med oppstartprogram til den sikre gjesten (210), og krypterte data, hvori de krypterte dataene ble kryptert av en eller flere prosessorer (16) ved å bruke nøklene tilveiebrakt i metadataene (240).

17. Dataprogramproduktet ifølge ett av kravene 12 til 16, hvori den private vertsnøkkelen eies av den sikre grensesnittkontrollen (250) og beregnes utelukkende av den sikre grensesnittkontrollen (250).

18. Et system som omfatter:

et minne (28);
én eller flere prosessorer (16) i kommunikasjon med minnet (28);

programinstruksjoner som kan utføres av én eller flere prosessorer (16) via minnet (28) for å utføre en fremgangsmåte, fremgangsmåten omfatter:

å oppnå, ved hjelp av en sikker grensesnittkontroll (250) i et datasystem utført av den ene eller flere prosessorer (16) i datasystemet, krypterte metadata (240) som omfatter én eller flere kontroller (260), metadataene (240) er kryptografisk koblet til et oppstartsbilde av en sikker gjest (210) som skal startes av en eier og administreres av en hypervisor (230), hvori metadataene (240) er utilgjengelige for den sikre gjesten (210) og for hypervisoren (230), der hver kontroll av den ene eller flere kontroller som inngår i metadataene (240) er en granulær kontroll av funksjonalitet som indikerer til den sikre grensesnittkontrollen (250) om den sikre gjesten (210) generert fra datafilen med oppstartprogram har tillatelse til å få svar på en spesiell forespørsel, hvor den ene eller flere prosessorer (16) er kommunikativt koblet til hypervisoren (230), hvor hypervisoren (230) administrerer én eller flere gjester; oppfange, ved hjelp av den sikre grensesnittkontrollen (250), via hypervisoren (230), fra den sikre gjesten (210) generert fra datafilen med oppstartprogram, under kjøretiden til den sikre gjesten (210), en forespørsel;
å gi tilgang, ved hjelp av den sikre grensesnittkontrollen (250), den ene eller flere kontroller (260) i metadataene (240) ved å bruke en privat vertsnøkkel;
å bestemme, ved hjelp av den sikre grensesnittkontrollen (250), basert på den ene eller flere kontroller (260), om den sikre gjesten (210) har tillatelse til å motta et svar på forespørselen;
basert på å bestemme at den sikre gjesten (210) har tillatelse til å oppnå svaret, ved å starte, ved den sikre grensesnittkontrollen (250), oppfyllelse av forespørselen, innenfor databehandlingssystemet; og
basert på å bestemme at den sikre gjesten (210) ikke har tillatelse til å oppnå svaret, og ignorerer, av den sikre grensesnittkontrollen (250), forespørselen.