(19) Octrooicentrum Nederland

(11) **1032473**

(12) C **OCTROOI**[20]

(21) Aanvrage om octrooi: **1032473**

(22) Ingediend: **11.09.2006**

(51) Int.Cl.:
G07C9/00 (2006.01) ***H04L29/08*** (2006.01)

(41) Ingeschreven:
12.03.2008 I.E. 2008/05

(47) Dagtekening:
12.03.2008

(45) Uitgegeven:
01.05.2008 I.E. 2008/05

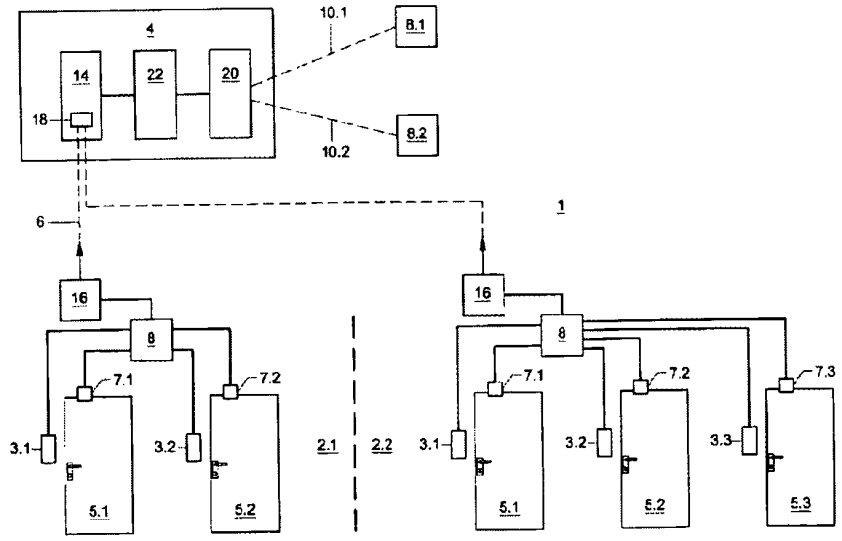
(73) Octrooihouder(s):
N.V. Nederlandsche Apparatenfabriek NEDAP te Groenlo.

(72) Uitvinder(s):
Patrus Wilhelmus Maria Paijens te Lochem.
Maurice Erick Rensink te Groenlo.

(74) Gemachtigde:
Drs. M.J. Hatzmann c.s. te 2508 DH Den Haag.

(54) **Stelsel voor toegangscontrole.**

(57) Stelsel voor toegangscontrole voorzien van tenminste een lokaal toegangscontrolesysteem dat is ingericht voor het detecteren, lezen en/of herkennen van bijvoorbeeld toegangscontrole pasjes, pincodes, biometrische kenmerken zoals irissen en dergelijke. Het stelsel is verder voorzien van een centraal besturingssysteem en tenminste een eerste communicatieve verbinding tussen het tenminste ene toegangscontrolesysteem en het besturingssysteem voor het uitwisselen van informatie tussen het besturingssysteem (4) en het tenminste ene toegangscontrolesysteem. Het besturingssysteem is voorzien van een FTP-type server en het tenminste ene toegangscontrolesysteem is voorzien van een FTP-type client voor het door het tenminste ene toegangscontrolesysteem versturen en ophalen van informatie.



NL C 1032473

Titel: Stelsel voor toegangscontrole

De uitvinding heeft betrekking op een stelsel voor toegangscontrole voorzien van tenminste een lokaal toegangscontrolesysteem dat is ingericht voor het detecteren, lezen en/of herkennen van bijvoorbeeld toegangscontrole pasjes, pincodes, biometrische kenmerken zoals irissen en dergelijke.

Een dergelijk stelsel is op zich bekend en wordt bijvoorbeeld toegepast in gebouwen van bedrijven en overheidsinstellingen. Personen kunnen hier toegang verkrijgen tot bepaalde ruimtes of delen van gebouwen door zich te melden bij een toegangscontrole-eenheid van het toegangscontrolesysteem dat bijvoorbeeld bij een deur is aangebracht. De toegangscontrole-eenheid, leest bijvoorbeeld een pinpas of scant een iris of er wordt een pincode bij de toegangscontrole-eenheid ingevoerd. Aan de hand van deze informatie controleert het toegangscontrolesysteem of de betreffende persoon toegang kan worden verschaft tot een bepaalde ruimte of een deel van een gebouw. Indien na controle blijkt dat de betreffende persoon toegang kan worden verschaft, kan het toegangscontrolesysteem bijvoorbeeld een deur ontgrendelen voor het verschaffen van de toegang.

Bij het bekende toegangscontrolesysteem wordt door een beheerder nieuwe informatie met betrekking tot bestaande of nieuwe pasjes, pincodes, biometrische kenmerken en dergelijke ingevoerd. Vanuit veiligheidsoverwegingen doet een beheerder dit rechtstreeks bij het toegangscontrolesysteem, welk systeem hiertoe bijvoorbeeld is voorzien van een invoerterminal zoals een computer.

Indien een beheerder een veelvoud van lokale toegangscontrolesystemen beheert die zich op van elkaar verschillende locaties bevinden, brengt dit het nadeel met zich dat de beheerder zich naar de betreffende locaties zal moeten begeven teneinde de nieuwe informatie

betreffende bestaand of nieuwe pasjes, pincodes, biometrische kenmerken en dergelijke in te voeren bij het locale toegangscontrolesysteem. Dit vergt reizen en daarmee kosten. Beheerders zijn vooralsnog niet bereid dergelijke nieuwe informatie op afstand van het betreffende lokale toegangscontrolesysteem in te voeren bijvoorbeeld via internet vanwege veiligheidsaspecten. Indien een toegangscontrolesysteem bijvoorbeeld via internet toegankelijk zou worden gemaakt voor het invoeren van informatie ontstaat het risico dat derden van buitenaf ook toegang nemen tot het toegangscontrolesysteem, hetgeen uiteraard als ongewenst wordt ervaren. Een verder nadeel van het bekende stelsel voor toegangscontrole is dat voor het lokaal kunnen invoeren van de betreffende nieuwe informatie het lokale toegangscontrolesysteem veelal is voorzien van een computer hetgeen kostenverhogend werkt.

Ook zal een beheerder log-files die door het lokale toegangscontrolesysteem worden aangemaakt en die bijvoorbeeld informatie omvatten over wanneer aan welke personen toegang tot welke ruimte is verschaft, rechtstreeks lokaal bij het toegangscontrolesysteem willen ophalen in verband met genoemde veiligheidsaspecten. Ook hier is een beheerder vooralsnog niet bereid op afstand via internet dergelijke informatie vanuit een toegangscontrolesysteem op te halen.

De uitvinding beoogt een stelsel te verschaffen dat aan genoemde nadelen tegemoet komt.

Volgens de uitvinding geldt dat het stelsel verder is voorzien van:

- een centraal besturingssysteem; en
- tenminste een eerste communicatieve verbinding tussen het tenminste ene toegangscontrolesysteem en het besturingssysteem voor het uitwisselen van informatie tussen het besturingssysteem en het tenminste ene toegangscontrolesysteem; waarbij het besturingssysteem is voorzien van een FTP-type server en het tenminste ene toegangscontrolesysteem is voorzien van een FTP-

type client voor het door het tenminste ene toegangscontrolesysteem versturen van informatie zoals een log-file naar het besturingssysteem en voor het door het tenminste ene toegangscontrolesysteem ophalen van informatie, zoals nieuwe informatie met betrekking tot bestaande of nieuwe pasjes, pincodes, biometrische kenmerken en dergelijke vanuit het besturingssysteem.

Doordat gebruik wordt gemaakt van een FTP-type server en een FTP-type cliënt doet het genoemde beveiligingsprobleem zich niet of in veel mindere mate voor. Het is immers het toegangscontrolesysteem zelf dat bepaalt wanneer informatie wordt opgehaald vanuit het centrale besturingssysteem en dus wanneer hiertoe een verbinding wordt gemaakt met de tenminste ene eerste communicatieve verbinding. Nadat deze informatie is opgehaald wordt de verbinding met de tenminste ene eerste communicatieve verbinding verbroken en is het toegangscontrolesysteem niet toegankelijk voor andere systemen die zouden zijn gekoppeld met de eerste communicatieve verbinding. Ook het initiatief voor het verzenden van log-files van het toegangscontrolesysteem naar het centraal besturingssysteem gaat uit van het toegangscontrolesysteem. Ook hiermee is wederom bereikt dat derden via de eerste communicatieve verbinding dergelijke log-files niet zouden kunnen ophalen uit het toegangscontrolesysteem.

Aldus is volgens de uitvinding geen VPN of private network nodig. Indien het toegangscontrolesysteem is voorzien van een firewall behoeven hierin ook geen holes of pipelines voor toegang vanaf buiten te worden aangebracht.

Bij voorkeur geldt dat het tenminste ene toegangscontrolesysteem is voorzien van een microcontroller waarop embedded client software draait. Doordat slechts gebruikt wordt gemaakt van een microcontroller behoeft het

toegangscontrolesysteem niet te zijn voorzien van een relatief dure computer zoals een pc.

In het tot nu toe besproken systeem kan een beheerder de nieuwe informatie klaarzetten in het besturingssysteem zodat het toegangscontrolesysteem dit op door het toegangscontrolesysteem bepaalde momenten kan ophalen. In het bijzonder kan een beheerder voor een veelvoud van toegangscontrolesystemen een veelvoud van nieuwe informatie klaarzetten dat door de betreffende toegangscontrolesystemen kan worden opgehaald. Elk toegangscontrolesysteem haalt dan zelf de informatie op die voor het betreffende toegangscontrolesysteem is bedoeld.

Volgens een nadere uitwerking van het stelsel volgens de uitvinding geldt dat het besturingssysteem bij voorkeur verder is voorzien van een Webserver, waarbij het stelsel voor toegangscontrole verder is voorzien van tenminste een computer, bij voorkeur voorzien van een Webclient, voor een beheerder van het tenminste ene toegangscontrolesysteem en tenminste een tweede communicatieve verbinding tussen het besturingssysteem en de tenminste ene computer waarbij het stelsel dusdanig is ingericht dat de beheerder informatie zoals nieuwe informatie met betrekking tot bestaande of nieuwe passen, pincodes, biometrische kenmerken en dergelijke met de tenminste ene computer via de tweede communicatieve verbinding naar het besturingssysteem kan sturen welke informatie na eventueel te zijn bewerkt door het besturingssysteem in het besturingssysteem wordt klaargezet zodat het tenminste ene toegangscontrolesysteem deze informatie kan ophalen via de tenminste ene eerste communicatieve verbinding middels het FTP-type protocol voor verdere verwerking door het tenminste ene toegangscontrolesysteem en/of waarbij het stelsel dusdanig is ingericht dat een beheerder informatie van het besturingssysteem kan ophalen die eerder door het tenminste ene toegangscontrolesysteem aan het besturingssysteem is verzonden. Op deze manier kan een beheerder vanaf een willekeurige positie, wereldwijd nieuwe informatie met betrekking tot bestaande of

nieuwe passen, pincodes, biometrische kenmerken en dergelijke naar het besturingssysteem verzenden en/of informatie ophalen. In het besturingssysteem wordt de te verzenden informatie dan klaargezet zodat deze informatie door het toegangscontrolesysteem waarvoor het bedoeld is kan worden opgehaald. Voorts kan wereldwijde informatie worden opgehaald die eerder door een toegangscontrolesysteem aan het besturingssysteem is verzonden. Ook voor deze nadere uitwerking geldt dat het toegangscontrolesysteem goed beveiligd is omdat deze slechts op eigen initiatief informatie ophaalt van het besturingssysteem en/of informatie toestuurt aan het besturingssysteem en alleen op deze momenten is verbonden met de tenminste ene eerste communicatieve verbinding. In het bijzonder kan een beheerder met de computer 8 ook informatie ophalen van het besturingssysteem die eerder door het toegangscontrolesysteem aan het besturingssysteem is toegezonden zoals de eerder genoemde log-files. In het bijzonder geldt hierbij dat het tenminste ene toegangscontrolesysteem tenminste een poort omvat die is gekoppeld met de tenminste ene eerste communicatieve verbinding en die niet permanent open staat. Meer in het bijzonder geldt hierbij dat de tenminste ene poort van het tenminste ene toegangscontrolesysteem alleen onder besturing van het tenminste ene toegangscontrolesysteem opengaat voor het versturen van de informatie naar het besturingssysteem of voor het ophalen van informatie van het besturingssysteem.

Praktisch gezien zal het stelsel zijn voorzien van een veelvoud van toegangscontrolesystemen en een veelvoud van computers die toebehoren aan verschillende beheerders. Iedere beheerder kan dan via zijn computer een verbinding aangaan met het besturingssysteem voor het toezenden van nieuwe informatie bestemd voor die toegangscontrolesystemen die onder zijn beheer staan. Evenzo kan een beheerder verbinding maken met het besturingssysteem voor het ophalen van informatie afkomstig van die toegangscontrolesystemen die onder zijn beheer staan. Het

besturingssysteem kan aldus worden benut door een veelvoud van beheerders die elk een veelvoud van toegangscontrolesystemen onder hun beheer hebben. Een voordeel hiervan is dat de individuele beheerders niet elk de kosten van een FTP-server behoeven te dragen. Deze wordt immers gemeenschappelijk voor verschillende beheerders benut.

Voor zowel de eerste als tweede communicatieve verbinding geldt dat deze het internet, UMTS, WAN, LAN, GPRS en/of dergelijke verbindingen omvatten. In het bijzonder geldt hier voorts nog dat het stelsel voor toegangscontrole is ingericht om de informatie die via de tenminste ene eerste communicatieve verbinding wordt verstuurd te versleutelen. Tevens geldt in het bijzonder dat het stelsel voor toegangscontrole is ingericht om de informatie die via de tenminste ene tweede communicatieve verbinding wordt verstuurd te versleutelen.

De uitvinding zal thans nader worden toegelicht aan de hand van de tekening.

Hierin toont:

Figuur 1 een mogelijk uitvoeringsvorm van een stelsel volgens de uitvinding.

- In Fig. 1 is met referentienummer 1 een stelsel voor toegangscontrole volgens de uitvinding aangeduid. Het stelsel voor toegangscontrole is voorzien van een eerste lokaal toegangscontrolesysteem 2.1 en een tweede lokaal toegangscontrolesysteem 2.2. Zowel voor het eerste als tweede lokaal toegangscontrolesysteem geldt dat deze zijn ingericht voor het detecteren, lezen en/of herkennen van bijvoorbeeld toegangscontrolepasjes, pincodes, biometrische kenmerken zoals irissen en dergelijke. Beide toegangscontrolesystemen kunnen autonoom werken. In het voorbeeld is het toegangscontrolesysteem 2.1 voorzien van een eerste toegangscontrole-eenheid 3.1 en een tweede toegangscontrole-eenheid 3.2. In het voorbeeld zijn de toegangscontrole-eenheid 3.1 en 3.2 elk ingericht voor het lezen van

toegangscontrolepassen die bijvoorbeeld zijn voorzien van RFID-chips met identificatiecodes die middels een elektromagnetisch ondervraagveld kunnen worden uitgelezen. De toegangscontrole-eenheden 3.1 en 3.2 zijn in dit voorbeeld verbonden met een microcontroller 8 die het toegangscontrolesysteem 2.1 bestuurt. Indien bijvoorbeeld door de toegangscontrole-eenheid 3.1 een pas wordt uitgelezen wordt informatie over deze pas naar de microcontroller 8 gestuurd. De microcontroller 8 analyseert op op zich bekende wijze of de uitgelezen informatie (identificatiecode) betrekking heeft op een pas van iemand die toegang heeft tot een bepaalde ruimte, welke ruimte in dit voorbeeld zich achter een deur 5.1 bevindt. Indien dit het geval is zal de microcontroller 8 bewerkstelligen dat een vergrendelingsmechanisme 7.1 van de deur 5.1 wordt vrijgegeven zodat de deur 5.1 kan worden geopend. Is dit niet het geval dan zal het vergrendelingsmechanisme gesloten blijven. De informatie over passen waarmee toegang kan worden verkregen tot bepaalde ruimtes is in dit voorbeeld in de microcontroller 8 opgeslagen. Geheel analoog kan een pas worden uitgelezen met behulp van de toegangscontrole-eenheid 3.2 met als doel het vergrendelingsmechanisme 7.2 van de deur 5.2 te openen teneinde toegang te verkrijgen tot een ruimte die zich achter de deur 5.2 bevindt.

Het toegangscontrolesysteem 2.2 is in dit voorbeeld voorzien van drie toegangscontrole-eenheden 3.1, 3.2 en 3.3 die respectievelijk bij drie deuren 5.1, 5.2 en 5.3 zijn aangebracht. De toegangscontrole-eenheden 3.1, 3.2 en 3.3 zijn gekoppeld met een microcontroller 8 van het toegangscontrolesysteem 2.2 en de deuren 5.1, 5.2 en 5.3 zijn respectievelijk voorzien van vergrendelingsmechanisme 7.1, 7.2 en 7.3. De werking van het toegangscontrolesysteem 2.2 is geheel analoog zoals hiervoor besproken voor het toegangscontrolesysteem 2.1. In het voorbeeld bevindt het toegangscontrolesysteem 2.1 zich in een eerste gebouw terwijl het toegangscontrolesysteem 2.2 zich in een ander gebouw bevindt.

Het stelsel volgens de uitvinding is verder voorzien van een besturingssysteem 4 dat zich in het voorbeeld op afstand bevindt van de toegangscontrolesystemen 2.1 en 2.2 en wel in een geheel ander gebouw. Het besturingssysteem 4 is voorzien van een computer 14 die is voorzien van software zodat de computer 14 de functie heeft van een FTP-type server; deze computer met software zal hierna ook wel worden aangeduid als FTP-type server (14). Voorts is het toegangscontrolesysteem 2.1 voorzien van een FTP-type client. In het voorbeeld is de microcontroller 8 hiertoe voorzien van FTP-type client software. De microcontroller 8 draait op embedded client software. Het toegangscontrolesysteem 2.1 is in dit voorbeeld voorts voorzien van een modem 16 die in het voorbeeld nog is voorzien van een firewall. De computer 14 is eveneens voorzien van een modem 18 die in het voorbeeld ook is voorzien van een firewall. Het stelsel (1) is voorts voorzien van een eerste communicatieve verbinding 6 tussen de modem 16 en de modem 18, dat wil zeggen tussen het tenminste ene toegangscontrolesysteem 2.1 en het besturingssysteem 4.

Voor het toegangscontrolesysteem 2.2 geldt geheel analoog als besproken voor het toegangscontrolesysteem 2.1 dat deze is voorzien van een modem 16 waarbij het toegangscontrolesysteem 2.2 is voorzien van een FTP-type client. In dit voorbeeld geldt dat het besturingssysteem 4 verder nog is voorzien van een computer 20 voorzien van webserver software zodat de computer 20 functioneert als een webserver 20. Verder is het besturingssysteem voorzien van een database server 22. De FTP-server 14, de database server 22 en webserver 20 zijn onderling met elkaar verbonden. In dit voorbeeld is het stelsel verder nog voorzien van een eerste computer 8.1 die toebehoort aan een eerste beheerder en een tweede computer 8.2 die toebehoort aan een tweede beheerder. In het voorbeeld beheert de eerste beheerder het toegangscontrolesysteem 2.1 terwijl de tweede beheerder het toegangscontrolesysteem 2.2 beheert. Voor de computer 8.1 en 8.2 geldt dat deze elk zijn voorzien van webclient software waarbij zich tussen de

computer 8.1 (webclient) en de webserver 20 tenminste een tweede communicatieve verbinding 10.1 uitstrekt en waarbij zich tussen de computer 8.2 en de webserver 20 eveneens een tweede communicatieve verbinding 10.2 uitstrekt.

De werking van het tot op dit punt omschreven stelsel is als volgt. Stel de eerste beheerder wil middels zijn computer 8.1 nieuwe informatie met betrekking tot bestaande en/of nieuwe passen bij het eerste toegangscontrolesysteem 2.1 invoeren. De beheerder maakt hiertoe met zijn computer 8.1 via de tweede communicatieve verbinding 10.1, die in dit voorbeeld het internet omvat, verbinding met de webserver 20. Het stelsel is in dit voorbeeld dusdanig ingericht dat een beheerder met de computer 8.1 alleen met de juiste toegangsrechten genoemde informatie naar de webserver 20 kan sturen. In dit voorbeeld moet de beheerder hiertoe een wachtwoord ingeven dat wordt gecontroleerd door de webserver 20. Aangenomen dat in dit voorbeeld het juiste wachtwoord wordt ingegeven kan de beheerder 8.1 vervolgens de nieuwe informatie via de webserver 20 aan de database server 22 toevoeren. Hierbij geeft de beheerder tevens aan dat de betreffende informatie bedoeld is voor het toegangscontrolesysteem 2.1. Het toegangscontrolesysteem is hiertoe op op zich bekende wijze identificeerbaar in het stelsel en kan hiertoe bijvoorbeeld zijn voorzien van een unieke aanduiding.

Het besturingssysteem 4 bewerkt de ontvangen informatie dusdanig dat deze op een later tijdstip kan worden opgehaald middels in dit voorbeeld het FTP-protocol. De bewerkte informatie inclusief de identiteit van een bestemming voor deze informatie wordt in dit voorbeeld klaargezet om te worden opgehaald in de database server 22.

In het voorbeeld geldt verder dat het toegangscontrolesysteem 2.1 is geprogrammeerd om op voorbepaalde tijdstippen een communicatieve verbinding aan te gaan via de tenminste ene eerste communicatieve verbinding 6 met het besturingssysteem 4 voor het ophalen van genoemde

informatie. In het voorbeeld bevindt dit programma zich in de microcontroller 8. Het gevolg is dat de microcontroller 8 via modem 16 op een vooraf bepaald tijdstip via de eerste communicatieve verbinding 6, die in het voorbeeld eveneens internet omvat, een verbinding legt via modem 18 met de FTP-server 14. De microcontroller 8 verzendt hierbij informatie aan de client server 14 over zijn identiteit. De FTP-server 14 controleert vervolgens of er in de database server 22 informatie klaarstaat voor de toegangscontrole-eenheid 2.1 met de betreffende identiteit. Indien dit het geval is bewerkstelligt de FTP-server 14 dat deze informatie middels het FTP-protocol aan de microcontroller 8 wordt toegevoerd. De microcontroller 8 kan deze informatie die in dit voorbeeld betrekking heeft op nieuwe informatie over bestaande en nieuwe passen opnemen en registreren waardoor het toegangscontrolesysteem 2.1 is ge-update. Hierna wordt de verbinding tussen het toegangscontrolesysteem en het besturingssysteem verbroken. Omdat het toegangscontrolesysteem niet remote accessable is maar alleen zelf een verbinding kan opbouwen met het besturingssysteem behoeven in de genoemde firewall derhalve geen pipelines te worden aangebracht voor het toegang verschaffen van buiten. Immers de firewall die in het modem 16 is aangebracht kan simpelweg alle toegang van buiten tegenhouden omdat toegang van buiten alleen wordt geïnitialiseerd door het toegangscontrolesysteem zelf dat immers fungeert als een FTP-type client.

Geheel analoog kan de tweede beheerder van het toegangscontrolesysteem 2.2 met zijn computer 8.2 nieuwe informatie toevoeren aan de webserver 20. Ook hiertoe moet de tweede beheerder via de computer 8.2 een wachtwoord ingeven alvorens hij de nieuwe informatie via de webserver 20 aan de database server 22 kan toevoeren. Ook hierbij dient de tweede beheerder aan te geven voor welk toegangscontrolesysteem de nieuwe informatie bestemd is. In dit voorbeeld gaat het om het toegangscontrolesysteem 2.2. Indien hij zou aangeven dat het gaat om het toegangscontrolesysteem 2.1 zal de databaseserver 22 de betreffende

informatie niet klaarzetten omdat volgens gegevens die opgeslagen zijn in de database server 22, de betreffende tweede beheerder slechts beheerder is van het toegangscontrolesysteem 2.2 en niet van het toegangscontrolesysteem 2.1. Ga we er echter vanuit dat de tweede beheerder nieuwe informatie toevoert met vermelding dat deze bestemd is voor het toegangscontrolesysteem 2.2 zal de database server de betreffende informatie bewerken en klaarzetten samen met een aanduiding dat deze bestemd is voor het toegangscontrolesysteem 2.2 zodat het toegangscontrolesysteem 2.2 de betreffende nieuwe informatie kan ophalen. Ook het toegangscontrolesysteem 2.2 is dusdanig geprogrammeerd dat deze op vooraf bepaalde tijdstippen contact maakt met de FTP-server 14. De FTP-server 14 zal in reactie op de verbinding die is aangegaan door het toegangscontrolesysteem 2.2 controleren of er nieuwe informatie klaarstaat die bestemd is voor het toegangscontrolesysteem 2.2. Indien dit het geval is zal deze informatie middels het FTP-protocol aan toegangscontrolesysteem 2.2 worden toegevoerd waarna het toegangscontrolesysteem 2.2 deze informatie kan verwerken analoog zoals is besproken voor het toegangscontrolesysteem 2.1. Hierna wordt de verbinding tussen het toegangscontrolesysteem en het besturingssysteem verbroken.

In het voorbeeld is het toegangscontrolesysteem 2.1 ook geprogrammeerd om op vooraf bepaalde tijdstippen een communicatieve verbinding aan te gaan via de tenminste ene eerste communicatieve verbinding 6 met het besturingssysteem 2 voor het versturen van informatie aan het besturingssysteem 2. Gedacht kan hierbij bijvoorbeeld worden aan log-files die informatie omvatten over wanneer aan wie bij welke deuren toegang is verschaft. Ook deze informatie wordt middels het FTP-protocol aan de FPT-server 14 toegevoerd. Deze zorgt ervoor dat de betreffende informatie in de database server 22 wordt opgeslagen. Hierna wordt de verbinding tussen het toegangscontrolesysteem en het besturingssysteem verbroken. Wanneer de beheerder met zijn computer 8.1 een verbinding

maakt met de webserver 20 kan deze aan de webserver 20 vragen of er informatie in de database server 22 klaarstaat die afkomstig is van het toegangscontrolesysteem 2.1. Indien dit het geval is, bewerkstelligt het besturingssysteem 4 dat in dit voorbeeld de log-file via de webserver 20 aan de webclient van de computer 8.1 wordt toegevoerd.

Geheel analoog kan informatie afkomstig van het toegangscontrolesysteem 2.2 op door het toegangscontrolesysteem 2.2 bepaalde vooraf bepaalde tijdstippen aan het besturingssysteem 4 worden toegevoerd. De tweede beheerder kan dan via de computer 8.2 contact leggen met de webserver 20 teneinde te verifiëren of er informatie afkomstig van toegangscontrolesystemen die onder zijn beheer staan klaarstaat om te worden opgehaald.

In dit voorbeeld geldt dat de toegangscontrolesystemen 2.1 en 2.2 elk zijn ingericht om autonoom te werken onafhankelijk van het besturingssysteem 4.

Wanneer het toegangscontrolesysteem 2.1 bijvoorbeeld voor het eerst in gebruik wordt gesteld is deze reeds geprogrammeerd om op vooraf bepaalde tijdstippen een communicatieve verbinding aan te gaan via de eerste communicatie verbinding met het besturingssysteem 4 voor het ophalen van informatie vanuit het besturingssysteem 4. Deze informatie kan ook informatie omvatten over nieuwe vooraf bepaalde tijdstippen waarop het toegangscontrolesysteem 2.1 een verbinding dient aan te gaan met het besturingssysteem voor het ophalen van nieuwe informatie. Deze informatie over nieuwe tijdstippen kan bijvoorbeeld door de eerste beheerder via zijn computer 8.1 bij het besturingssysteem 4 zijn ingevoerd, geheel analoog zoals besproken voor het invoeren van nieuwe informatie over nieuwe of bestaande passen. Eén en ander geldt mutatis mutandis geheel analoog voor het toegangscontrolesysteem 2.2.

In het bijzonder geldt dat elk toegangscontrolesysteem 2.1, 2.2 tenminste een poort omvat die is verbonden met de respectievelijke eerste

communicatie verbindingen 6.1 en 6.2, welke poorten niet permanent openstaan. Hierbij geldt in dit voorbeeld dat een dergelijke poort van het toegangscontrolesysteem 2.1 alleen onder besturing van het toegangscontrolesysteem 2.1 zelf, dat wil zeggen in dit voorbeeld onder besturing van de microcontroller 8 van het toegangscontrolesysteem 2.1 opengaat voor het versturen van de informatie naar besturingssysteem 4 of voor het ophalen van informatie van het besturingssysteem 4. Dit geldt analoog voor de tenminste ene poort van het toegangscontrolesysteem 2.2

In het voorbeeld geldt dat de eerste communicatieve verbindingen 6.1 en 6.2 internet omvatten. Het is ook mogelijk dat (eventueel tevens) andere verbindingen zoals UMTS, WAN, LAN en/of GPRS en dergelijke worden omvat. In dit voorbeeld geldt tevens dat de tweede communicatieve verbinding 10.1 en de tweede communicatieve verbinding 10.2 internet omvat. Andere verbinding zoals UMTS, WAN, LAN en/of GPRS en dergelijke zijn echter eveneens mogelijk.

In dit voorbeeld geldt voorts dat de eerste beheerder met de computer 8.1 informatie kan toezenden en ophalen van het toegangscontrolesysteem 2.1. Het is echter eveneens mogelijk dat de eerste beheerder meer dan één toegangscontrolesysteem onder zijn beheer heeft. Geheel analoog is het mogelijk dat de tweede beheerder behalve het toegangscontrolesysteem 2.2 ook nog andere toegangscontrolesystemen onder zijn beheer heeft. Opgemerkt wordt dat de computers 8.1 en 8.2 willekeurige computers zijn. Een beheerder kan dus waar ook ter wereld met een willekeurige computer contact maken met de webserver 20 (nadat deze zich op de juiste wijze heeft geïdentificeerd, wachtwoorden heeft ingegeven en dergelijke) om de genoemde informatie klaar te zetten in de database server 22 om later te worden opgehaald door de door hem aangewezen toegangscontrolesystemen. Ook kan hij dan informatie ophalen zoals log-files die voor hem door toegangscontrolesystemen die onder zijn beheer staan aan het toegangscontrolesysteem 2 zijn toegevoerd.

In het bijzonder geldt dat het stelsel van toegangscontrole is ingericht om de informatie die via de tenminste ene eerste communicatieve verbinding wordt verstuurd te versleutelen. Hierbij geldt in het bijzonder dat de betreffende informatie via het SFTP-protocol wordt verstuurd. Dit is een nadere uitwerking van het FTP-protocol dat versleuteling mogelijk maakt. Evenzo kan informatie die tussen de computer 8.1 en de webserver 20 via de tenminste ene tweede communicatieve verbinding wordt uitgewisseld zijn versleuteld op op zich bekende wijze. Hierbij geldt in het bijzonder dat de betreffende informatie via het SFTP-protocol wordt verstuurd. Dit geldt eveneens voor informatie die wordt uitgewisseld tussen de computer 8.2 en de webserver 20.

De uitvinding is geenszins beperkt tot de hiervoor geschetste uitvoeringsvormen. In dit voorbeeld zijn de toegangscontrolesystemen elk voorzien van lokale toegangscontrole-eenheden in de vorm van een paslezer. Andere toegangscontrole-eenheden zoals Iris-scanners dan wel eenheden waar een pincode kan worden ingevoerd behoren uiteraard ook tot de mogelijkheden. Ook kan het stelsel (veel) meer dan twee toegangscontrolesystemen omvatten. In dit voorbeeld omvat het systeem de computers 8.1 en 8.2 ten behoeve van twee beheerders. Uiteraard kan er ook sprake zijn van (veel) meer dan twee beheerders die gebruik maken van meer computers waarbij het echter niet is uitgesloten dat verschillende beheerders gebruik maken van één en dezelfde computer. Dergelijke varianten worden elk geacht binnen het kader van de uitvinding te vallen. Ook is het denkbaar dat het stelstel niet is voorzien van computers 8.1 en 8.2 die zich op afstand van besturingssysteem 4 bevinden. In plaats hiervan kan de beheerder bij het besturingssysteem 4 rechtstreeks de betreffende informatie ingeven of ophalen. Dergelijk varianten worden elk geacht binnen het kader van de uitvinding te vallen.

CONCLUSIES

1. Stelsel voor toegangscontrole (1) voorzien van tenminste een lokaal toegangscontrolesysteem (2) dat is ingericht voor het detecteren, lezen en/of herkennen van bijvoorbeeld toegangscontrole pasjes, pincodes, biometrische kenmerken zoals irissen en dergelijke, met het kenmerk, dat het stelsel (1) verder is voorzien van:

- een centraal besturingssysteem (4); en
- tenminste een eerste communicatieve verbinding (6) tussen het tenminste ene toegangscontrolesysteem (2) en het besturingssysteem (4) voor het uitwisselen van informatie tussen het besturingssysteem (4) en het tenminste ene toegangscontrolesysteem (2); waarbij het besturingssysteem (4) is voorzien van een FTP-type server en het tenminste ene toegangscontrolesysteem (2) is voorzien van een FTP-type client voor het door het tenminste ene toegangscontrolesysteem (2) versturen van informatie zoals een log-file naar het besturingssysteem (4) en voor het door het tenminste ene toegangscontrolesysteem (2) ophalen van informatie, zoals nieuwe informatie met betrekking tot bestaande of nieuwe pasjes, pincodes, biometrische kenmerken en dergelijke vanuit het besturingssysteem (4).

2. Stelsel volgens conclusie 1, met het kenmerk, dat het tenminste ene toegangscontrolesysteem (2) is voorzien van een microcontroller (8) waarop embedded client software draait.

3. Stelsel volgens conclusie 1 of 2, met het kenmerk, dat de microcontroller (8) geen deel uitmaakt van een PC.

4. Stelsel volgens een der voorgaande conclusies, met het kenmerk, dat het tenminste ene toegangscontrolesysteem (2) geen PC omvat.

5. Stelsel volgens een der voorgaande conclusies, met het kenmerk, dat het besturingssysteem (4) bij voorkeur verder is voorzien van een Webserver, waarbij het stelsel (1) verder is voorzien van tenminste een computer (8), bij voorkeur voorzien van een Webclient, voor een beheerder van het tenminste ene toegangscontrolesysteem (2) en tenminste een tweede communicatieve verbinding (10) tussen het besturingssysteem (4) en de tenminste ene computer (8) waarbij het stelsel (1) dusdanig is ingericht dat de beheerder informatie zoals nieuwe informatie met betrekking tot bestaande of nieuwe passen, pincodes, biometrische kenmerken en dergelijke met de tenminste ene computer (8) via de tweede communicatieve verbinding naar het besturingssysteem (4) kan sturen welke informatie na eventueel te zijn bewerkt door het besturingssysteem (4) in het besturingssysteem (4) wordt klaargezet zodat het tenminste ene toegangscontrolesysteem (2) deze informatie kan ophalen via de tenminste ene eerste communicatieve verbinding (6) middels het FTP-type protocol voor verdere verwerking door het tenminste ene toegangscontrolesysteem (2) en/of waarbij het stelsel dusdanig is ingericht dat een beheerder informatie van het besturingssysteem kan ophalen die eerder door het tenminste ene toegangscontrolesysteem aan het besturingssysteem is verzonden.

6. Stelsel volgens conclusie 5, met het kenmerk, dat het stelsel (1) dusdanig is ingericht dat een beheerder met de tenminste ene computer (8) alleen met juiste toegangsrechten genoemde informatie naar het besturingssysteem kan sturen en/of van het besturingssysteem kan ophalen.

7. Stelsel volgens een der voorgaande conclusies, met het kenmerk, dat het tenminste ene toegangscontrolesysteem (2) is ingericht om autonoom te werken, onafhankelijk van het besturingssysteem (4).

8. Stelsel volgens een der voorgaande conclusies, met het kenmerk, dat het tenminste ene toegangscontrolesysteem (2) is geprogrammeerd

om op vooraf bepaalde tijdstippen een communicatieve verbinding aan te gaan via de tenminste ene eerste communicatieve verbinding (6) met het besturingssysteem (4) voor het ophalen van genoemde informatie vanuit het besturingssysteem (4).

9. Stelsel volgens een der voorgaande conclusies, met het kenmerk, dat het tenminste ene toegangscontrolesysteem (2) is geprogrammeerd om op vooraf bepaalde tijdstippen een communicatieve verbinding aan te gaan via de tenminste ene eerste communicatieve verbinding (6) met het besturingssysteem (2) voor versturen van genoemde informatie naar het besturingssysteem (2).

10. Stelsel volgens conclusie 8 of 9, met het kenmerk, dat het stelsel (1) dusdanig is ingericht dat, in gebruik, de vooraf bepaalde tijdstippen door het tenminste ene toegangscontrolesysteem (2) via de tenminste ene eerste communicatieve verbinding (6) vanuit het besturingssysteem (4) kunnen worden opgehaald door het tenminste ene toegangscontrolesysteem.

11. Stelsel volgens een der voorgaande conclusies, met het kenmerk, dat de tenminste ene eerste communicatieve verbinding (6) het internet, UMTS, WAN, LAN en/of GPRS en/of dergelijke verbindingen omvat.

12. Stelsel volgens conclusie 5 of 6, met het kenmerk, dat de tenminste ene tweede communicatieve verbinding (10) het internet, UMTS, WAN, LAN en/of GPRS en/of dergelijke verbindingen omvat.

13. Stelsel volgens een der voorgaande conclusies, met het kenmerk, dat het stelsel (1) is ingericht om de informatie die via de tenminste ene eerste communicatieve verbinding (6) wordt verstuurd te versleutelen.

14. Stelsel volgens een der voorgaande conclusies 5, 6 of 12, met het kenmerk, dat het stelsel (1) is ingericht om de informatie die via de tenminste ene tweede communicatieve verbinding (10) wordt verstuurd te versleutelen.

15. Stelsel volgens een der voorgaande conclusies, met het kenmerk, dat het tenminste ene toegangscontrolesysteem (2) tenminste een poort omvat die is gekoppeld met de tenminste ene eerste communicatieve verbinding (6) en die niet permanent zijn geopend.

16. Stelsel volgens conclusie 15, met het kenmerk, dat de tenminste ene poort van het tenminste ene toegangscontrolesysteem (2) alleen onder besturing van het tenminste ene toegangscontrolesysteem (2) open gaat voor het versturen van de informatie naar het besturingssysteem (4) of voor het ophalen van informatie van het besturingssysteem (4).

17. Stelsel volgens een der voorgaande conclusies, met het kenmerk, dat het stelsel (1) is voorzien van een veelvoud van lokale toegangscontrolesystemen (2) die elk met tenminste een van de tenminste ene eerste communicatieve verbinding (6) met het besturingssysteem (4) zijn verbonden, waarbij de toegangscontrolesystemen (2) elk zijn ingericht voor het detecteren, lezen en/of herkennen van bijvoorbeeld toegangscontrole pasjes, pincodes, biometrische kenmerken zoals irissen e.d. waarbij elk toegangscontrolesysteem is voorzien van een FTP-type client voor het door de toegangscontrole-eenheden (2) versturen van informatie zoals log-files naar het besturingssysteem (4) en voor het door de toegangscontrolesystemen (2) ophalen van informatie, zoals nieuwe informatie met betrekking tot bestaande of nieuwe pasjes, pincodes, biometrische kenmerken en dergelijke vanuit het besturingssysteem (4).

18. Stelsel volgens conclusie 17, met het kenmerk, dat de toegangscontrolesystemen (2) identificeerbaar zijn binnen het systeem.

19. Stelsel volgens conclusies 5 en 18, met het kenmerk dat het stelsel voor toegangscontrole (1) dusdanig is ingericht dat een beheerder tenminste een van de toegangscontrolesystemen (2) kan selecteren teneinde via de tenminste ene tweede communicatieve verbinding (10) tussen het besturingssysteem (4) en de tenminste ene computer (8)

informatie ten behoeve van het geselecteerde toegangscontrolesysteem (2), zoals nieuwe informatie met betrekking tot bestaande of nieuwe passen, pincodes, biometrische kenmerken e.d. voor het geselecteerde toegangscontrolesysteem (2) met de tenminste ene computer (8) naar het besturingssysteem (4) te sturen welke de informatie, in gebruik, na eventueel te zijn bewerkt door het besturingssysteem (4) in het besturingssysteem wordt klaargezet zodat het geselecteerde toegangscontrolesysteem (2) deze informatie kan ophalen via de eerste communicatieve verbinding (6) middels het FTP-type protocol voor verdere verwerking door het geselecteerde toegangscontrolesysteem (2).

20. Stelsel volgens conclusie 19, met het kenmerk dat het stelsel (1) dusdanig is ingericht dat een veelvoud van verschillende toegangscontrolesystemen (2) respectievelijk worden beheerd door verschillende beheerders waarbij elke beheerder met een computer (8) tenminste één van de door hem beheerde toegangscontrolesystemen (2) kan selecteren teneinde informatie ten behoeve van het geselecteerde toegangscontrolesysteem, zoals nieuwe informatie met betrekking tot bestaande of nieuwe passen, pincodes, biometrische kenmerken en dergelijke voor het geselecteerde toegangscontrolesysteem (2) met de betreffende computer (8) naar het besturingssysteem (4) te sturen welke de informatie na eventueel te zijn bewerkt door het besturingssysteem (4) in het besturingssysteem klaarzet zodat het geselecteerde toegangscontrolesysteem (2) deze informatie kan ophalen via de eerste communicatieve verbinding (6) middels het FTP-type protocol voor verdere verwerking door het geselecteerde toegangscontrolesysteem (2).

21. Stelsel volgens conclusie 20, met het kenmerk, dat het stelsel (1) is voorzien van een veelvoud van computers (8), die bij voorkeur elk zijn voorzien van een Webclient, voor beheerders van de toegangscontrolesystemen (2).

22. Stelsel volgens een der voorgaande conclusies, met het kenmerk, dat het FTP-type server en het FTP-type client respectievelijk een FTP-server en een FTP-client of een SFTP-server en een SFTP-client zijn.

23. Stelsel volgens een der voorgaande conclusies, met het kenmerk, dat het tenminste ene lokale toegangscontrolesysteem is voorzien van tenminste een toegangscontrole-eenheid zoals een paslezer, een invoereenheid voor pincodes of irisscanner en dergelijke.

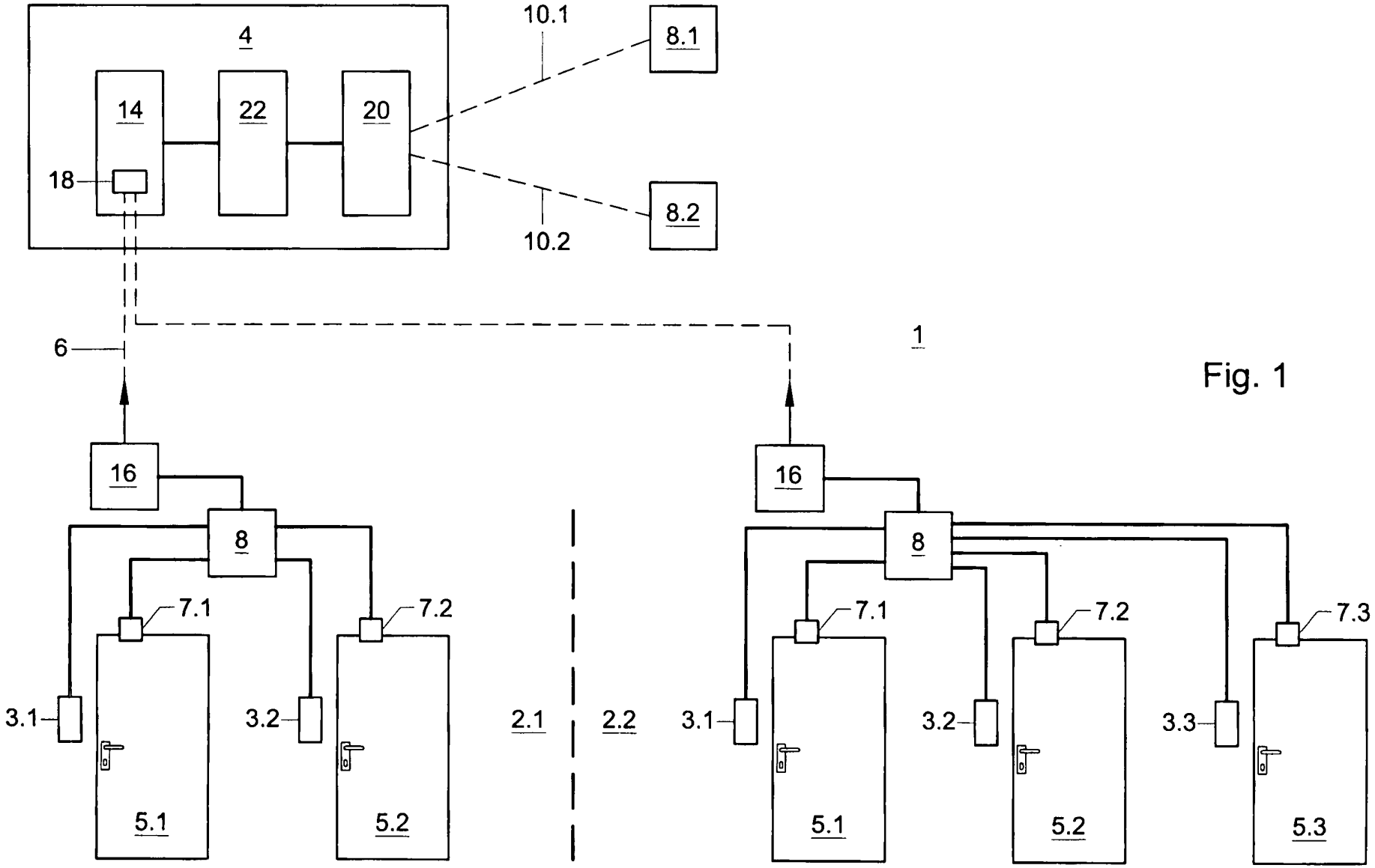

4
14
22
20
18
10.1
8.1
8.2
10.2
6
1
16
8
7.1
7.2
3.1
3.2
5.1
5.2
2.1
2.2
16
8
7.1
7.2
7.3
3.1
3.2
3.3
5.1
5.2
5.3

Fig. 1

SAMENWERKINGSVERDRAG (PCT)

RAPPORT BETREFFENDE NIEUWHEIDSONDERZOEK VAN INTERNATIONAAL TYPE

IDENTIFICATIE VAN DE NATIONALE AANVRAGE	KENMERK VAN DE AANVRAGER OF VAN DE GEMACHTIGDE
	P78482NL00
Nederlands aanvraag nr. **1032473**	Indieningsdatum **11-09-2006**
	Ingeroepen voorrangsdatum
Aanvrager (Naam) **NV Nederlandsche Apparatenfabriek**	
Datum van het verzoek voor een onderzoek van internationaal type	Door de Instantie voor Internationaal Onderzoek aan het verzoek voor een onderzoek van internationaal type toegekend nr. **SN 47821**

I. CLASSIFICATIE VAN HET ONDERWERP (bij toepassing van verschillende classificaties, alle classificatiesymbolen opgeven)

Volgens de internationale classificatie (IPC)

G07C9/00 H04L29/08

II. ONDERZOCHTE GEBIEDEN VAN DE TECHNIEK

Onderzochte minimumdocumentatie

Classificatiesysteem	Classificatiesymbolen
IPC8	**G06F G07C H04L**

Onderzochte andere documentatie dan de minimum documentatie, voor zover dergelijke documenten in de onderzochte gebieden zijn opgenomen

III. ☐ **GEEN ONDERZOEK MOGELIJK VOOR BEPAALDE CONCLUSIES** (opmerkingen op aanvullingsblad)

IV. ☐ **GEBREK AAN EENHEID VAN UITVINDING** (opmerkingen op aanvullingsblad)

VERSLAG VAN HET NIEUWHEIDSONDERZOEK VAN INTERNATIONAAL TYPE

Nummer van het verzoek om een nieuwheidsonderzoek
NL 1032473

A. CLASSIFICATIE VAN HET ONDERWERP
INV. G07C9/00 H04L29/08

Volgens de Internationale Classificatie van octrooien (IPC) of zowel volgens de nationale classificatie als volgens de IPC.

B. ONDERZOCHTE GEBIEDEN VAN DE TECHNIEK

Onderzochte miminum documentatie (classificatie gevolgd door classificatiesymbolen)
G06F G07C H04L

Onderzochte andere documentatie dan de mimimum documentatie, voor dergelijke documenten, voor zover dergelijke documenten in de onderzochte gebieden zijn opgenomen

Tijdens het internationaal nieuwheidsonderzoek geraadpleegde elektronische gegevensbestanden (naam van de gegevensbestanden en, waar uitvoerbaar, gebruikte trefwoorden)
EPO-Internal, WPI Data

C. VAN BELANG GEACHTE DOCUMENTEN

Categorie °	Geciteerde documenten, eventueel met aanduiding van speciaal van belang zijnde passages	Van belang voor conclusie nr.
X	WO 03/069566 A (PENCO PRODUCTS INC [US]; DIGITECH INTERNATIONAL INC [US]) 21 augustus 2003 (2003-08-21) het gehele document	1-23
A	US 2004/083128 A1 (BUCKINGHAM DUANE W [US] ET AL) 29 april 2004 (2004-04-29) bladzijde 2, alinea 18 - bladzijde 3, alinea 29 bladzijde 4, alinea 32 - alinea 33 bladzijde 4, alinea 36 - bladzijde 7, alinea 55	1-23

-/--

[X] Verdere documenten worden vermeld in het vervolg van vak C.

[X] Leden van dezelfde octrooifamilie zijn vermeld in een bijlage

° Speciale categorieën van aangehaalde documenten

"A" document dat de algemene stand van de techniek weergeeft, maar niet beschouwd wordt als zijnde van bijzonder belang

"E" eerder document, maar gepubliceerd op de datum van indiening of daarna

"L" document dat het beroep op een recht van voorrang aan twijfel onderhevig maakt of dat aangehaald wordt om de publikatiedatum van een andere aanhaling vast te stellen of om een andere reden zoals aangegeven

"O" document dat betrekking heeft op een mondelinge uiteenzetting, een gebruik, een tentoonstelling of een ander middel

"P" document gepubliceerd voor de datum van indiening maar na de ingeroepen datum van voorrang

"T" later document, gepubliceerd na de datum van indiening of datum van voorrang en niet in strijd met de aanvrage, maar aangehaald ter verduidelijking van het principe of de theorie die aan de uitvinding ten grondslag ligt

"X" document van bijzonder belang; de uitvinding waarvoor uitsluitende rechten worden aangevraagd kan niet als nieuw worden beschouwd of kan niet worden beschouwd op inventiviteit te berusten

"Y" document van bijzonder belang; de uitvinding waarvoor uitsluitende rechten worden aangevraagd kan niet worden beschouwd als inventief wanneer het document beschouwd wordt in combinatie met één of meerdere soortgelijke documenten, en deze combinatie voor een deskundige voor de hand ligt

"&" document dat deel uitmaakt van dezelfde octrooifamilie

Datum waarop het nieuwheidsonderzoek van internationaal type werd voltooid	Verzenddatum van het rapport van het nieuwheidsonderzoek van internationaal type
18 April 2007	

Naam en adres van de instantie	De bevoegde ambtenaar
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	VAN DER HAEGEN, D

1

VERSLAG VAN HET NIEUWHEIDSONDERZOEK VAN INTERNATIONAAL TYPE

Nummer van het verzoek om een nieuwheidsonderzoek
NL 1032473

C.(Vervolg). VAN BELANG GEACHTE DOCUMENTEN

Categorie *	Geciteerde documenten, eventueel met aanduiding van speciaal van belang zijnde passages	Van belang voor conclusie nr.
A	GB 2 367 973 A (COMPLEMENTARY TECH LTD [GB]) 17 april 2002 (2002-04-17) bladzijde 8, regel 25 - bladzijde 9, regel 3 bladzijde 10, regel 16 - regel 27 bladzijde 12, regel 8 - bladzijde 13, regel 27 -----	8-10,13

Formulier PCT/ISA/201 (vervolg tweede blad) (Januari 2004)

VERSLAG VAN HET NIEUWHEIDSONDERZOEK VAN INTERNATIONAAL TYPE

Informatie over leden van dezelfde octrooifamilie

Nummer van het verzoek om een nieuwheidsonderzoek: NL 1032473

In het rapport genoemd octrooigeschrift	Datum van publicatie	Overeenkomend(e) geschrift(en)	Datum van publicatie
WO 03069566 A	21-08-2003	AU 2003209050 A1	04-09-2003
		US 2005179349 A1	18-08-2005
		US 6879243 B1	12-04-2005
US 2004083128 A1	29-04-2004	GEEN	
GB 2367973 A	17-04-2002	AU 9397601 A	22-04-2002
		EP 1340357 A2	03-09-2003
		WO 0232069 A2	18-04-2002
		US 2005102402 A1	12-05-2005

OCTROOICENTRUM NEDERLAND

WRITTEN OPINION

File No.	Filing date *(day/month/year)*	Priority date *(day/month/year)*	Application No.
SN47821	11.09.2006		NL1032473

International Patent Classification (IPC)
INV. G07C9/00 H04L29/08

Applicant
N.V. Nederlandsche Apparatenfabriek NEDAP te Groen

This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the application
- ☐ Box No. VIII Certain observations on the application

	Examiner
	VAN DER HAEGEN, D

WRITTEN OPINION

Box No. I Basis of this opinion

1. This opinion has been established on the basis of the latest set of claims filed before the start of the search.

2. With regard to any **nucleotide and/or amino acid sequence** disclosed in the application and necessary to the claimed invention, this opinion has been established on the basis of:

   a. type of material:

   ☐ a sequence listing

   ☐ table(s) related to the sequence listing

   b. format of material:

   ☐ on paper

   ☐ in electronic form

   c. time of filing/furnishing:

   ☐ contained in the application as filed.

   ☐ filed together with the application in electronic form.

   ☐ furnished subsequently for the purposes of search.

3. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

4. Additional comments:

Box No. V Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty	Yes:	Claims	1-23
	No:	Claims	
Inventive step	Yes:	Claims	
	No:	Claims	1-23
Industrial applicability	Yes:	Claims	1-23
	No:	Claims	

2. Citations and explanations

see separate sheet

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Document WO 03/069566 (D1) is considered to represent the most relevant state of the art.

   D1 describes an electronically-controlled locker system (cf. D1: abstract). The disclosed system comprises:
   - a plurality of locker control units LCU adapted to use data from an input device and to control access to a number of lockers (cf. D1: Figs.1 and 2, ref.signs 26, 28 and 30 / Fig.11);
   - a system control unit SCU acting as a master control unit (cf. D1: Fig.1, ref.sign 24 / page 5, lines 23-25); and
   - a TCP communications link between the LCUs and the SCU for uploading data related to inputs, lock openings and closings, etc. ... from the LCU to the SCU, and for downloading authorised user and locker information from the SCU to the LCU (cf. D1: Fig.9, ref.sign S38 / Fig.11, ref.sign L49 / page 2, lines 8-9 / page 12, lines 9-12 / page 13, lines 10-14).

2. The system according claim 1 differs from the system of D1 in that the central control unit is arranged as a server - i.e. as a slave, and the local control unit as a client - i.e. as a master. Furthermore, data between the control units is transferred using FTP. Hence, the claimed central and local control units are set up as an FTP server and a FTP client, respectively.

   The use of FTP allows the transfer of data from one computing system to another over a network. Arranging the local control units as (FTP) clients and the central control unit as a (FTP) server allows to coordinate the uploading/downloading of data with the actual demands of the local control units - e.g. based on the actual availability of the computing and communication resources of the local units.

3. FTP is merely one of several commonly used protocols for exchanging information over any network that supports TCP. Selecting FTP as an application protocol to upload/download files over the TCP network of D1 is straightforward for the skilled person and does not require the exercise of inventive skill.

FTP clients by default initiate a connection to the FTP server. Once connected the FTP client can do a number of file manipulation operations such as uploading files to the server, download files from the server and so on. In other words, setting up the FTP control stream is demand driven by the FTP client, and inherent to FTP. Hence, a person skilled in FTP and confronted with the technical problem of coordinating the uploading/downloading of data with the actual demands of the local control units of D1, would readily adapt the system of D1 such that the SCU acts as a "slave control" - i.e. a (FTP) server, and the LCUs as a "master control" - i.e. a (FTP) client. Therefore, the claimed arrangement of central and local control units does not involve an inventive step.

4. Dependent claims 2-23 do not add any inventive matter to claim 1:

- D1 implies an embedded application and system in the sense of claims 2-4, cf. Fig.11;
- a system administrator computer linked to the central control unit and adapted to upload/download data from and to the central control unit (cp. claim 5) is known from D1, cf. Fig.1, ref.sign 22 / page 4, lines 11-12 / page 5, lines 8-20 / page 13, line 10 - page 27, line 2;
- the application of administrator access rights as recited in claim 6 is a general practice in the field of system administration, cf. D1, table 4;
- the LCUs of D1 operate autonomously (cp. claim 7), cf. Fig.8;
- communicating with the central control unit on predetermined periodic intervals to download/upload information as defined in claims 8 and 9 is a matter of normal design, cf. document GB-A-2 367 973 (D2), page 8, line 25 - page 9, line 3;
- acquiring this predetermined periodic intervals from the central control unit (cp. claim 10) is also known from D2, which shows the use of time and date stamps indicating when a downloaded file needs to be updated, cf. page 10, lines 16-27;
- the additional features of claims 11 and 12 are known from D1;
- encrypting FTP sessions in the sense of claim 13 is also shown in D2, cf. page 12, line 8 - page 13, line 27;
- encrypting the session between the administrator and the central control unit (cp. claim 14) falls within the scope of customary practice of the skilled person;
- controlling a communications port in the sense of claims 15 and 16 is common

when using FTP in its active transfer mode;

- a plurality of local control units as recited in claim 17 is rendered obvious in view of the teaching of D1 and the common knowledge the skilled person, cf. items 1-3 above;
- using ID's to identify (cp. claim 18) and to select (cp. claim 19) the local control units is implicit from what is explicitly shown in D1, cf. table 5, the record labelled "LCU" / table 16, the record labelled "LockerID";
- having a plurality of administrators and administrator computers in the sense of claims 20 and 21 is rendered obvious by D1, cf. tables 3 and 4;
- the additional features of claim 22 do not involve an inventive step, cf. items 1-3 above; and
- access control devices as recited in claim 23 are described in D1, cf. Fig.2, ref.signs 128-428.