(19) Octrooicentrum Nederland

(11) **2010733**

(12)C **OCTROOI**

(21) Aanvraagnummer: **2010733**

(22) Aanvraag ingediend: **29.04.2013**

(51) Int.Cl.:
G06F 21/35 (2013.01) ***G06F 21/43*** (2013.01)
H04L 29/06 (2006.01)

(43) Aanvraag gepubliceerd:
-

(47) Octrooi verleend:
30.10.2014

(45) Octrooischrift uitgegeven:
05.11.2014

(73) Octrooihouder(s):
Baseline Automatisering B.V. te Amsterdam.

(72) Uitvinder(s):
Johannes Jacobus Marie Dorresteijn te Amsterdam.

(74) Gemachtigde:
ir. F.E. Hoeben te Hilversum.

(54) **Werkwijzen voor authenticatie, server, inrichting en datadrager.**

(57) De onderhavige uitvinding betreft een werkwijze voor authenticatie tussen een serverproces en een cliëntproces middels meervoudige communicatie omvattende tenminste een primaire authenticatiecommunicatie en een secundaire authenticatiecommunicatie, waarbij de werkwijze stappen omvat voor:
- het door het serverproces ontvangen van een initiatiecommunicatie van de primaire authenticatiecommunicatie vanaf het cliëntproces,
- het door het serverproces initiëren van de secundaire authenticatiecommunicatie tussen het serverproces en een cliëntauthenticatieproces,
- het door het serverproces ontvangen van primaire authenticatieinformatie omvattende een authenticatiecode of een authenticatieresultaat middels de primaire authenticatiecommunicatie,
- het door het serverproces ontvangen van secundaire authenticatieinformatie omvattende een authenticatiecode of een authenticatieresultaat van de secundaire authenticatiecommunicatie,
- het door het serverproces vaststellen van de authenticatie op basis van de primaire en secundaire authenticatieinformatie,
waarbij de primaire authenticatiecommunicatie en de secundaire authenticatiecommunicatie gescheiden communicaties zijn en/of waarbij het serverproces op basis van de secundaire authenticatiecommunicatie op zichzelf een secundaire authenticatie kan vaststellen.

NL C 2010733

Werkwijzen voor authenticatie, server, inrichting en datadrager.

De onderhavige uitvinding betreft een werkwijze voor authenticatie tussen een serverproces en een cliëntproces middels meervoudige communicatie omvattende ten minste een primaire authenticatiecommunicatie en een secundaire authenticatiecommunicatie. Voorts betreft de onderhavige uitvinding een werkwijze voor een cliëntauthenticatieproces. Voorts betreft de onderhavige uitvinding een machineuitleesbaar medium omvattende instructies voor het uitvoeren van een serverproces of een cliëntauthenticatieproces volgens de onderhavige uitvinding. Voorts betreft de onderhavige uitvinding een server voor het uitvoeren van een serverproces volgens de onderhavige uitvinding. Voorts betreft de onderhavige uitvinding een inrichting voor het uitvoeren van een cliëntauthenticatieproces volgens de onderhavige uitvinding.

Authenticatie van gebruikers van gedistribueerde computersystemen is een heet hangijzer, in die zin dat ongeautoriseerde toegang tot gegevens, applicaties en systemen dient te worden voorkomen terwijl tevens het gebruikersgemak van de gedistribueerde systemen van belang is.

Er zijn derhalve verschillende soorten van authenticatie ontwikkeld, waarbij de authenticatie op basis van gebruikersnaam en wachtwoord de meest voorkomende is. Wanneer een dergelijke authenticatie op basis van gebruikersnaam en wachtwoord niet volstaat wordt bijvoorbeeld gebruik gemaakt van een verdere authenticatie waarbij de gebruiker op een mobiele telefoon een kort tekstbericht ontvangt waarvan de gebruiker de inhoud kan invoeren nadat hij zijn reguliere wachtwoord heeft ingevoerd. Met een dergelijke authenticatie zou een valse authenticatie

slechts mogelijk kunnen zijn op basis van gebruikersnaam, wachtwoord en de inhoud van het korte tekstbericht dat slechts kan worden ontvangen wanneer iemand in het bezit is van de mobiele telefoon van de gebruiker.

Het is een inzicht van de onderhavige uitvinder der het voor de gebruiker een frustrerende ervaring is deze code handmatig te moeten ontnemen vanaf een beeldscherm van de mobiele telefoon, en deze foutloos te moeten invoeren in bijvoorbeeld zijn computer.

Op basis van dit inzicht heeft het onderhavige uitvinder een alternatieve wijze van authenticatie op basis van een alternatieve communicatie als doel gehad. Derhalve verschaft de onderhavige uitvinding een werkwijze voor authenticatie tussen een serverproces en een cliëntproces middels meervoudige communicatie omvattende ten minste een primaire authenticatiecommunicatie en een secundaire authenticatiecommunicatie, waarbij de werkwijze stappen omvat voor:

- het door het serverproces ontvangen van een initiatiecommunicatie van de primaire authenticatiecommunicatie vanaf het cliëntproces,
- het door het serverproces initiëren van de secundaire authenticatiecommunicatie tussen het serverproces en een cliëntauthenticatieproces,
- het door het serverproces ontvangen van primaire authenticatieinformatie omvattende een authenticatiecode of een authenticatieresultaat middels de primaire authenticatiecommunicatie,
- het door het serverproces ontvangen van secundaire authenticatieinformatie omvattende een authenticatiecode of een authenticatieresultaat van de secundaire authenticatiecommunicatie,

- het door het serverproces vaststellen van de authenticatie op basis van de primaire en secundaire authenticatieinformatie,

waarbij de primaire authenticatiecommunicatie en de secundaire authenticatiecommunicatie gescheiden communicaties zijn en/of waarbij het serverproces op basis van de secundaire authenticatiecommunicatie op zichzelf een secundaire authenticatie kan vaststellen.

Een voordeel van een werkwijze volgens de onderhavige uitvinding is dat er evenals bij het voorbeeld met de sms van de stand van de techniek een separate authenticatie mogelijk is terwijl de gebruiker als deel van de primaire authenticatieinformatie en/of de primaire authenticatiecommunicatie geen gegevens die afkomstig zijn van het cliëntauthenticatieproces of de secundaire authenticatiecommunicatie behoeft in te voeren. Hierdoor is de werkwijze volgens de onderhavige uitvinding voor de gebruiker in belangrijke mate vereenvoudigd en gebruiksvriendelijker gerealiseerd.

De werkwijze volgens de onderhavige uitvinding is bijvoorbeeld toepasbaar in een situatie waarbij een gebruiker gebruik maakt van een PC voor het verkrijgen van toegang tot een serverproces, zoals een bedrijfsapplicatie, sociaal media account, elektronische dienstenaccount, e-mailaccount, et cetera. Hierbij identificeert de gebruiker zich op een op zichzelf bekende wijze middels een gebruikersnaam en wachtwoord. Vervolgens, of simultaan maakt het serverproces contact met het cliëntauthenticatieproces en/of een inrichting van de gebruiker dat middels een terugmelding aan het serverproces de authenticatie bevestigd.

In een eerste voorkeursuitvoeringsvorm volgens de onderhavige uitvinding omvat de secundaire authenticatie-

communicatie stappen voor het door het cliëntauthenticatieproces ontvangen van een gebruikeracceptatieinvoer. Bij voorkeur omvat een dergelijke gebruikeracceptatieinvoer het actueren van een terugkoppelingactuator, zoals een toets of een aanraakschermgedeelte dat is ingericht als een toets. Hiermee kan bijvoorbeeld worden geverifieerd dat in een vooraf bepaalde tijd de actuatie is uitgevoerd waarmee kan worden geaccepteerd dat de authenticatie in orde is.

In een verdere voorkeursuitvoeringsvorm zijn het cliëntproces en het cliëntauthenticatieproces uitvoerbaar op dezelfde inrichting. Hierdoor is het gebruikersgemak voor de gebruiker op bijzondere wijze hoog aangezien de gebruiker slechts een inrichting behoeft te hanteren of daar de beschikking over behoeft te hebben. Op alternatieve wijze is echter op doelmatige wijze door de uitvinder voorzien dat het cliëntproces en het cliëntauthenticatieproces functioneren op twee verschillende inrichtingen. Hierdoor is het bijvoorbeeld mogelijk middels een mobiele telefoon gebruik te maken van twee verschillende computersystemen die gefixeerd zijn gerangschikt op respectieve verschillende gebruikslocaties.

Bij verdere voorkeur is het cliëntauthenticatieproces gebaseerd op een unieke inrichtingidentificatie van een inrichting waarop deze wordt uitgevoerd zoals bijvoorbeeld een IMEI-nummer. Een voordeel hiervan is dat een hoge mate van zekerheid van de identiteit van de inrichting kan worden verkregen. Een verder voordeel is dat inrichting middels dit getal kan worden geadresseerd voor het afleveren van het bericht.

In een verdere voorkeursuitvoeringsvorm wordt het cliëntauthenticatieproces uitgevoerd op een eerder bij de server aangemelde inrichting, waarbij een eerdere aanmel-

ding bij voorkeur is gebaseerd op een unieke identificatie van de inrichting voor het daarop uitvoeren van het cliëntauthenticatieproces en/of een gebruikersidentificatie, welke bij voorkeur is gebaseerd op een primaire authenticatie van de gebruiker, zoals middels een gebruikersnaam wachtwoord, en welke bij verdere voorkeur is geverifieerd middels een eerdere verificatie met de gebruiker. Het is hierdoor bijvoorbeeld mogelijk een registratie bij te houden van een op een relaties tussen gebruikers van gebruikersaccounts en inrichtingen voor de authenticatie waardoor het mogelijk wordt binnen dergelijke registraties die authenticatie te beperken. Een verder voordeel is dat registraties die kunnen worden toegekend ook kunnen worden verwijderd waardoor een additionele beveiliging van het systeem wordt verschaft. Verder wordt het hierdoor bijvoorbeeld mogelijk om gebruikersaccounts in stand te houden terwijl toch op effectieve wijze de mogelijkheid tot inloggen kan worden gestopt.

Bij verdere voorkeur omvat het cliëntauthenticatieproces stappen voor het ontvangen van een invoer van een beveiligingscode, zoals een pincode of een wachtwoord, van een gebruiker. Hierdoor wordt een additionele beveiliging verschaft voor het geval de inrichting in het bezit zou komen van andere personen dan de gebruiker die behoort bij een gebruikersaccount.

In een verdere voorkeursuitvoeringsvorm omvattende stappen voor het initiëren van de secundaire authenticatiecommunicatie stappen voor het door de server naar het cliëntauthenticatieproces verzenden van een bericht, zoals een pushbericht, bij voorkeur omvattende een door het serverproces samengesteld token. Hiermee wordt een wijze voor het uitvoeren van de secundaire authenticatiecommunicatie op efficiënte wijze ingevuld met als specifiek voor-

deel dat door het toepassen van een pushbericht het bericht direct kan worden verwerkt door de applicatie die het cliëntauthenticatieproces uitvoert. Hierdoor wordt een vertraging die een gebruiker vervelend zou vinden voorkomen en daarmee het systeem gebruikersvriendelijk.

Bij verdere voorkeur worden hiertoe stappen toegepast voor het gebruiken van een gateway ingericht voor het naar het cliëntauthenticatieproces overbrengen van pushnotificaties. Het toepassen van een dergelijke gateway verschaft als voordeel dat gebruik kan worden gemaakt van standaardprocessen in een mobiele inrichting.

Bij verdere voorkeur vormen in de werkwijze de primaire en secundaire authenticatiecommunicatie afzonderlijke communicatielussen. Dit heeft als voordeel dat de gebruiker niet zoals bijvoorbeeld bij een bestaande sms verificatie ingewikkelde codes moet inlezen en overtypen in het cliëntproces voor verwerking door de server. Hiermee wordt het gebruikersgemak van een systeem en werkwijze volgens de onderhavige uitvinding in belangrijke mate verhoogd. Ditzelfde geldt bij de voorkeursuitvoeringsvorm waarbij geen informatieoverdracht wordt uitgevoerd tussen de primaire authenticatie en de secundaire authenticatie en/of tussen de secundaire authenticatie en de primaire authenticatie. Wanneer een dergelijke informatieoverdracht niet nodig is, middels bijvoorbeeld een eerdere registratie van de inrichting wordt het gebruikersgemak verhoogd.

Dergelijke voordelen ontstaan eveneens wanneer het serverproces toegang heeft tot een gegevensbron omvattende eerder ingevoerde authenticatiegegevens met betrekking tot inrichtingen waarop het cliëntauthenticatieproces wordt uitgevoerd. Door de toepassing van de eerdere authenticaties van de inrichtingen en/of the cliëntauthenticatieprocessen kan het verhoogde gebruikersgemak, doordat de ge-

bruiker geen gegevens hoeft in te voeren, en daarmee de automatische dubbele factor authenticatie worden verschaft. Op soortgelijke wijze is het daarbij van voordeel wanneer het serverproces toegang heeft tot een gegevensbron omvattende eerder ingevoerde authenticatiegegevens met betrekking tot vooraf geconfigureerde cliëntauthenticatieprocessen, zoals een app voor een cliëntauthenticatieproces omvattende een opslag voor authenticatiegegevens.

Bij verdere voorkeur omvat de primaire authenticatie een controle van het serverproces op een gebruikersnaam en wachtwoord welke is ontvangen door de server middels de primaire authenticatiecommunicatie tussen het clientproces en het serverproces. Hiermee wordt op voor de gebruiker op zichzelf bekende en daarmee voordelige wijze de primaire authenticatie verschaft.

In een verdere voorkeursuitvoeringsvorm omvat de werkwijze een verdere authenticatie middels een tertiaire authenticatiecommunicatie, bij voorkeur omvattende een controlecode, verzonden door de server middels een bericht en het door de server terugontvangen van de controlecode door een gebruikerinvoer middels het cliëntproces. Hiermee kan in onveilig geachte omstandigheden een additionele bescherming worden verschaft, welke weliswaar het gebruikersgemak van het systeem verlaagt maar de veiligheid verhoogt.

Een verder aspect volgens de onderhavige uitvinding betreft een werkwijze voor een cliëntauthenticatieproces voor toepassing in een werkwijze volgens de onderhavige uitvinding omvattende stappen voor:

- het vanaf een serverproces ontvangen van een bericht, zoals een pushbericht, bij voorkeur omvattende een door het serverproces samengesteld token,

- het door middel van een gebruikerinvoer ontvangen van een bevestiging of een authenticatie, bij voorkeur een lokale authenticatie,

- het naar het serverproces verzenden van een bericht inhoudende een bevestiging van de authenticatie, bij voorkeur omvattende een bevestigingen of een authenticatiecode. Middels een dergelijk aspect worden voordelen verschaft zoals in de het voorgaande beschreven aan de hand van het eerdere aspect.

In een verdere voorkeursuitvoeringsvorm omvat de werkwijze stappen voor het door het cliëntauthenticatieproces op basis van het ontvangen bericht bepalen dat het bericht bedoeld is voor het specifieke cliëntauthenticatieproces en of de inrichting waarop deze functioneert. Een verder aspect volgens de onderhavige uitvinding betreft een machineuitleesbaar medium omvattende instructies voor het uitvoeren van een serverproces of een cliëntauthenticatieproces volgens de onderhavige uitvinding voor het implementeren van een werkwijze volgens de onderhavige uitvinding. Middels een dergelijk aspect worden voordelen verschaft zoals in de het voorgaande beschreven aan de hand van eerdere aspecten van werkwijzen.

Een verder aspect volgens de onderhavige uitvinding betreft een server ingericht voor of omvattende code voor het uitvoeren van een werkwijze en/of een serverproces volgens de onderhavige uitvinding.

Een verder aspect volgens onderhavige uitvinding betreft een inrichting ingericht voor of omvattende code voor het uitvoeren van een werkwijze en/of een cliëntauthenticatieproces volgens de onderhavige uitvinding.

De termen server en serverproces worden afwisselend met dezelfde betekenis gebruikt.

Verdere voordelen, kenmerken en details van de onderhavige uitvinding zullen in het navolgende in groter detail worden beschreven aan de hand van een of meerdere voorkeursuitvoeringsvormen onder verwijzing naar de aangehechte figuren. Soortgelijke doch niet noodzakelijkerwijs identieke onderdelen van verschillende voorkeursuitvoeringsvormen zijn aangeduid met dezelfde verwijzingscijfers.

Fig. 1 betreft een schematische weergave van een systeem voor het daarop laten functioneren van een voorkeursuitvoeringsvorm volgens de onderhavige uitvinding.

Fig. 2 betreft een schematische weergave van een werkwijze volgens een voorkeursuitvoeringsvorm volgens de onderhavige uitvinding.

Fig. 3 betreft een schematische weergave van een werkwijze volgens een verdere voorkeursuitvoeringsvorm volgens de onderhavige uitvinding.

Fig. 4 betreft een schematische weergave van een werkwijze volgens een verdere voorkeursuitvoeringsvorm volgens de onderhavige uitvinding.

Fig. 5 betreft een schematische weergave van een werkwijze volgens een verdere voorkeursuitvoeringsvorm volgens de onderhavige uitvinding.

Een eerste voorkeursuitvoeringsvorm (Fig. 1) volgens de onderhavige uitvinding betreft een werkwijze voor het uitvoeren van een authenticatie middels twee afzonderlijke communicatielussen. Als voorbeeld is een systeem weergegeven waarbinnen een dergelijke werkwijze kan worden uitgevoerd. Een centrale server 3 functioneert voor het verschaffen van een bedrijfsapplicatie met accounts voor verschillende medewerkers, e-mailaccount, gebruikeraccount bij een of enkele, al dan niet gecombineerde, webdiensten, en/of bijvoorbeeld een sociaal media account. Wanneer een

gebruiker wil inloggen in zijn account start deze op een cliëntinrichting 1 een cliëntproces op welke contact maakt met de server 3 middels een tweewegcommunicatie 19 voor het over en weer communiceren van applicatie gegevens, zoals bijvoorbeeld een webinterface. De communicatie geschiedt volgens het onderhavige voorbeeld op op zichzelf bekende wijze via een computernetwerk 4 zoals het internet. De server communiceert terug via een communicatie 19, bij voorkeur omvattende een challenge voor het opvragen van een gebruikersnaam en een wachtwoord, welke een authenticatiecode voor de eerste authenticatie vormen. Na het invoeren door de gebruiker van de gebruikersnaam en het wachtwoord worden deze via de communicatie 11 verzonden naar het serverproces in afwachting van een later te ontvangen bericht 12 inhoudende een afronding van een secundaire authenticatie.

De genoemde communicatie 11 en 12 vormen tezamen binnen het begrip van de onderhavige uitvinding de primaire authenticatiecommunicatie. Nadat de gebruiker de gebruikersnaam en het wachtwoord heeft opgegeven is de primaire authenticatiecommunicatie afgerond maar kan de gebruiker het cliëntproces en toegang daarmee tot het serverproces nog niet gebruiken omdat er nog geen secundaire authenticatie heeft plaatsgevonden.

Nadat de primaire authenticatie middels de primaire authenticatiecommunicatie is afgerond begint de server met de secundaire authenticatiecommunicatie. Hiertoe verzendt het serverproces, eveneens via het internet en/of via een mobiel telefoonnetwerk, een challenge 14 naar de mobiele telefoon 2 van de gebruiker. Deze challenge 14 omvat bijvoorbeeld pushbericht voor het bereiken van een applicatie die functioneert op de mobiele telefoon, welke applicatie toegang heeft tot een unieke identificatie van

de mobiele telefoon, en welke is toegerust voor het uitvoeren van het cliëntauthenticatieproces middels informatie opgenomen in de challenge 14, het terugzenden 16 van het resultaat van de bewerking naar het serverproces voor het completeren van een authenticatie door het serverproces.

Teneinde deze authenticatie te kunnen uitvoeren heeft het serverproces toegang tot gegevens met betrekking tot de inrichting 2, welke gegevens zijn samengesteld op basis van eerdere authenticaties, zoals beschreven aan de hand van Fig. 5, van de inrichtingen 2.

Na het completeren van de authenticatie door het serverproces verzendt het serverproces een bevestiging van de authenticaties naar de computer een middels het bericht 12 waarna de gebruiker toegang heeft tot zijn account. Het is middels een dergelijke werkwijze niet nodig dat een gebruiker gegevens overneemt van de mobiele telefoon voor invoering daarvan in de computer 1. Met andere woorden verschaft de onderhavige werkwijze een dubbele factor authenticatie op volledig automatische wijze. Dit is mogelijk omdat de 2 factor authenticatie gebruik maakt van zich een eerdere authenticatie van de mobiele inrichting of een daarop functionerende applicatie.

Ten behoeve van het pushbericht wordt gebruik gemaakt van een gateway voor pushnotificaties, zoals een Apple™ pushnotificatiedienst. Op alternatieve wijze kan er gebruik gemaakt worden van een e-mail, pushnotificaties of een applicatie die contact onderhoudt met een andersoortige push dienst. Op nog verdere alternatieve wijze kan er gebruik gemaakt worden van een activatie door de gebruiker van een applicatie die na activatie door de gebruiker contact zoekt met de server of een verdere met de server contact onderhouden de dienst.

De werkwijze van het serverproces is in een voorkeursvoorbeeld getoond in fig. 2. Werkwijze start in stap 21. In stap 22 wordt de invoer van de gebruiker van de gebruikersnaam en wachtwoord ontvangen door de server (vergelijk 11 volgens Fig. 1). In stap 23 controleert de server het gebruikersnaam en wachtwoord waarbij wordt teruggekeerd naar stap 22 indien de gegevens incorrect worden bevonden. In stap 24 verzendt het serverproces het pushbericht naar de mobiele telefoon van de gebruiker en ontvangt het serverproces een beantwoordende communicatie van de mobiele telefoon (vergelijk 14, 16 volgens Fig. 1).

In stap 25 wordt bepaald of de gebruiker bijvoorbeeld binnen de geldende tijdsduur een acceptatie heeft gegeven middels het activeren van een knop. Indien dit niet het geval is vervolgt de werkwijze in stap 22. In stap 26 wordt door het serverproces het terug ontvangen bericht ontleed en de informatie met betrekking tot de authenticatie (token) geverifieerd en de status geregistreerd. Indien de authenticatie niet is geslaagd wordt vervolgd in stap 22. Indien de authenticatie is geslaagd vervolgt de werkwijze in stap 27 met het naar de computer van de gebruiker verzenden van een bevestiging (vergelijk 12 volgens figuur 1) van het op correcte wijze inloggen waarna de werkwijze eindigt in stap 28.

Het proces volgens communicatie 19 is weergegeven in Fig. 3. Werkwijze begint in stap 31. In stap 32 is de server bereid tot het ontvangen van een initialisatie van een cliëntproces. Tussen stap 32 en 33 wordt de primaire authenticatiecommunicatie uitgevoerd alsmede verstuurt de server het pushbericht naar de telefoon. In stap 33 wacht de server op een bevestiging vanaf de mobiele telefoon met betrekking tot het pushbericht. Wanneer een gestelde tijd verloopt deactiveert de server het token en zet de server

terug in een toestand bereid tot het ontvangen van een initialisatie van een cliëntproces. Tussen stap 33 en 34 wordt de secundaire authenticatiecommunicatie uitgevoerd. In stap 34 verzendt de server de vestiging met betrekking tot een geslaagde inlogactie naar de computer 1 van de gebruiker

In Fig. 4 is de werkwijze op de authenticatie inrichting 2 als voorbeeld beschreven. De werkwijze start in stap 41. In stap 42 ontvangt de unieke geregistreerde inrichting het pushbericht met een token. In stap 43 wordt de gebruiker een prompt getoond voor het accepteren van de token. Indien de token niet wordt geaccepteerd eindigt de werkwijze in stap 43'. Indien een stap 43 de token wordt geaccepteerd verzendt in stap 44 het cliëntauthenticatieproces een bericht terug naar de server, het bericht inhoudende de acceptatie van het token op de unieke geregistreerde inrichting. Doordat de acceptatie op de unieke geregistreerde inrichting wordt uitgevoerd is de authenticatie veilig.

In Fig. 5 is de werkwijze voor het bij de server of het serverproces aanmelden van de unieke inrichting als voorbeeld getoond. De werkwijze start in stap 51 waarna in stap 52 de gebruiker middels de applicatie inhoudende het cliëntauthenticatieproces het serverproces dat wordt uitgevoerd op de server benaderd en middels zijn bij de server bekende inloginformatie inlogt. Het kan hierbij gaan om het de gebruikersnaam en het wachtwoord waarmee hij normaal inlogt op zijn account. Het kan echter evenzeer om een separate combinatie van gebruikersnaam en wachtwoord zijn. Na een controle door de server van de inloggegevens in stap 53 wordt deze inlogauthenticatie ofwel afgewezen waarna wordt teruggekeerd in stap 52, ofwel in stap 54 wordt de inrichting geregistreerd op de server en

gekoppeld aan een gebruiker. Deze werkwijze eindigt in stap 54.

Op alternatieve wijze wordt de koppeling aan een gebruiker niet uitgevoerd in stap 54 maar separaat na een additionele controle door een beheerder van de server middels een handmatige koppeling. Het is hierbij ofwel mogelijk dat de gebruiker de inloggegevens volgens Fig. 5 slechts kan invoeren/aanleveren aan de server in aanwezigheid van de beheerder, ofwel dat de stappen voor deze registratie authenticatie alleen mag worden uitgevoerd door de beheerder onder toepassing van speciale authenticatiecodes.

In het voorgaande is de onderhavige uitvinding beschreven aan de hand van enkele voorkeursuitvoeringsvormen. De computer een van de gebruiker van een veelheid van inrichtingen betreffen, zoals een persoonlijke computer, een tablet, een mobiele telefoon, een thin client, et cetera. De inrichting voor de secundaire authenticatiecommunicatie kan elke inrichting of proces dat daarop wordt uitgevoerd betreffen waarmee een initiële registratie dan wel authenticatie kan worden uitgevoerd op basis waarvan een latere authenticatie als vertrouwd kan worden beschouwd. Deze authenticatie kan worden uitgevoerd op basis van een unieke identificator van de inrichting, zoals een IMEI nummer van een mobiele telefoon of een processornummer van een persoonlijke computer of een identificatie van een speciale identificatiechip op een elektronische inrichting. Het is echter evenzeer mogelijk dat een applicatie op zichzelf authenticatiemiddelen omvat of geschikt is door middel van speciale bewerkingen authenticatiecodes te ontvangen, te berekenen en te verzenden, waarmee een applicatie op zichzelf als basis kan dienen voor een betrouwbaar te achten authenticatie. Op alternatieve wijze

is het bijvoorbeeld mogelijk om een inhoud of een deel van een inhoud van een SMS bericht als input voor cliëntauthenticatieproces te laten functioneren, met andere woorden dat het clientauthenticatieproces deze inhoud als inhoud van het pushbericht beschouwd en op basis van deze inhoud de autenticatieterugkoppeling naar de server wordt verzonden.

Verschillende aspecten van verschillende uitvoeringen worden beschreven geacht in combinatie met elkaar waarbij alle combinaties die bij lezing door een vakman van het vakgebied op basis van dit document door een vakman binnen het begrip van de uitvinding vallen beschouwd worden te zijn meegelezen. De volgorde van werkwijze stappen volgens de onderhavige uitvinding is niet op vastleggen de wijze bepaald, noch in de conclusies noch in de specificatie. Vakman voorzienbare alternatieven op basis van de uitvinding of de specificatie van eveneens onder dit document. Deze voorkeursuitvoeringsvormen zijn derhalve niet beperkend voor de beschermingsomvang van dit document. De gevraagde rechten worden bepaald in de aangehechte conclusies.

*****

CONCLUSIES

1. Werkwijze voor authenticatie tussen een serverproces en een cliëntproces middels meervoudige communicatie omvattende ten minste een primaire authenticatiecommunicatie en een secundaire authenticatiecommunicatie, waarbij de werkwijze stappen omvat voor:

- het door het serverproces ontvangen van een initiatiecommunicatie van de primaire authenticatiecommunicatie vanaf het cliëntproces,
- het door het serverproces initiëren van de secundaire authenticatiecommunicatie tussen het serverproces en een cliëntauthenticatieproces,
- het door het serverproces ontvangen van primaire authenticatieinformatie omvattende een authenticatiecode of een authenticatieresultaat middels de primaire authenticatiecommunicatie,
- het door het serverproces ontvangen van secundaire authenticatieinformatie omvattende een authenticatiecode of een authenticatieresultaat van de secundaire authenticatiecommunicatie,
- het door het serverproces vaststellen van de authenticatie op basis van de primaire en secundaire authenticatieinformatie,

waarbij de primaire authenticatiecommunicatie en de secundaire authenticatiecommunicatie gescheiden communicaties zijn en/of waarbij het serverproces op basis van de secundaire authenticatiecommunicatie op zichzelf een secundaire authenticatie kan vaststellen.

2. Een werkwijze volgens conclusie 1 waarbij de secundaire authenticatiecommunicatie stappen omvat voor

het door het cliëntauthenticatieproces ontvangen van een gebruikeracceptatieinvoer.

3. Werkwijze volgens een of meer van de voorgaande conclusies waarbij het cliëntproces en het cliëntauthenticatieproces uitvoerbaar zijn op dezelfde inrichting.

4. Werkwijze volgens een of meer van de voorgaande conclusies waarbij het cliëntproces en het cliëntauthenticatieproces functioneren op twee verschillende inrichtingen.

5. Werkwijze volgens een of meer van de voorgaande conclusies waarbij het cliëntauthenticatieproces is gebaseerd op een unieke inrichtingidentificatie van een inrichting waarop deze wordt uitgevoerd.

6. Werkwijze volgens een of meer van de voorgaande conclusies waarbij het cliëntauthenticatieproces wordt uitgevoerd op een eerder bij de server aangemelde inrichting, waarbij een eerdere aanmelding bij voorkeur is gebaseerd op een unieke identificatie van de inrichting voor het daarop uitvoeren van het cliëntauthenticatieproces en/of een gebruikersidentificatie, welke bij voorkeur is gebaseerd op een primaire authenticatie van de gebruiker, zoals middels een gebruikersnaam wachtwoord, en welke bij verdere voorkeur is geverifieerd middels een eerdere verificatie met de gebruiker.

7. Werkwijze volgens een of meer van de voorgaande conclusies waarbij het cliëntauthenticatieproces stappen omvat voor het ontvangen van een invoer van een beveili-

gingscode, zoals een pincode of een wachtwoord, van een gebruiker.

8. Werkwijze volgens een of meer van de voorgaande conclusies waarbij de stappen voor het initiëren van de secundaire authenticatiecommunicatie stappen omvatten voor het door de server naar het cliëntauthenticatieproces verzenden van een bericht, zoals een pushbericht, bij voorkeur omvattende een door het serverproces samengesteld token.

9. Werkwijze volgens conclusie 8 omvattende stappen voor het gebruiken van een gateway ingericht voor het naar het cliëntauthenticatieproces overbrengen van pushnotificaties.

10. Werkwijze volgens een of meer van de voorgaande conclusies waarbij de primaire en secundaire authenticatiecommunicatie afzonderlijke communicatielussen vormen.

11. Werkwijze volgens een of meer van de voorgaande conclusies waarbij geen informatieoverdracht wordt uitgevoerd tussen de primaire authenticatie en de secundaire authenticatie en/of tussen de secundaire authenticatie en de primaire authenticatie.

12. Werkwijze volgens een of meer van de voorgaande conclusies waarbij het serverproces toegang heeft tot een gegevensbron omvattende eerder ingevoerde authenticatiegegevens met betrekking tot inrichtingen waarop het cliëntauthenticatieproces wordt uitgevoerd.

13. Werkwijze volgens een of meer van de voorgaande conclusies waarbij het serverproces toegang heeft tot een gegevensbron omvattende eerder ingevoerde authenticatiegegevens met betrekking tot vooraf geconfigureerde cliëntauthenticatieprocessen, zoals apps voor een cliëntauthenticatieproces omvattende een opslag voor authenticatiegegevens.

14. Werkwijze volgens een of meer van de voorgaande conclusies waarbij de primaire authenticatie een controle van het serverproces omvat op een gebruikersnaam en wachtwoord ontvangen door de server middels de primaire authenticatiecommunicatie tussen het cliëntproces en het serverproces.

15. Werkwijze volgens eens meer van de voorgaande conclusies omvattende een verdere authenticatie middels een tertiaire authenticatiecommunicatie, bij voorkeur omvattende een controlecode, verzonden door de server middels een bericht en het door de server terugontvangen van de controlecode door een gebruikerinvoer middels het cliëntproces.

16. Werkwijze voor een cliëntauthenticatieproces voor toepassing in een werkwijze volgens een of meer van de conclusies 1 – 15 omvattende stappen voor:

– het vanaf een serverproces ontvangen van een bericht, zoals een pushbericht, bij voorkeur omvattende een door het serverproces samengesteld token,

– het door een gebruikerinvoer ontvangen van een bevestiging of een authenticatie, bij voorkeur een lokale authenticatie,

- het naar het serverproces verzenden van een bericht inhoudende een bevestiging van de authenticatie, bij voorkeur omvattende een bevestigingen of een authenticatiecode.

17. Werkwijze volgens conclusie 16 omvattende stappen voor het door het cliëntauthenticatieproces op basis van het ontvangen bericht bepalen dat het bericht bedoeld is voor het specifieke cliëntauthenticatieproces en of de inrichting waarop deze functioneert.

18. Machineuitleesbaar medium omvattende instructies voor het uitvoeren van een serverproces of een cliëntauthenticatieproces volgens een of meer van de voorgaande conclusies voor het implementeren van een werkwijze volgens een of meer van de voorgaande conclusies.

19. Server ingericht voor of omvattende code voor het uitvoeren van een werkwijze en/of een serverproces volgens een of meer van de voorgaande conclusies 1 - 17.

20. Inrichting ingericht voor of omvattende code voor het uitvoeren van een werkwijze en/of een cliëntauthenticatieproces volgens een of meer van de voorgaande conclusies 1 - 17.

*****

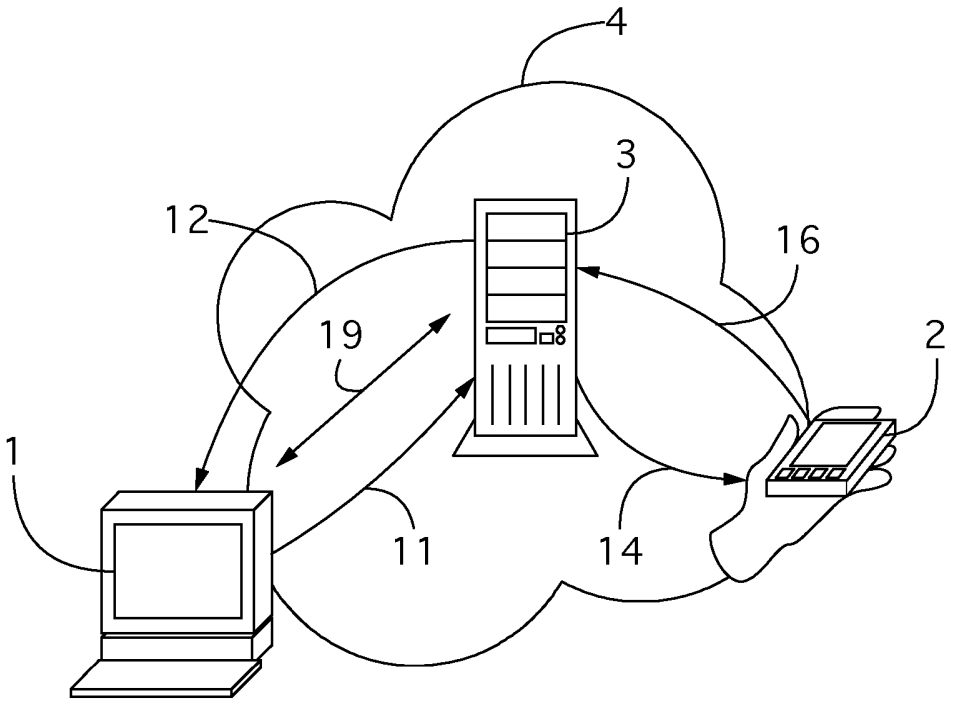

Fig.1

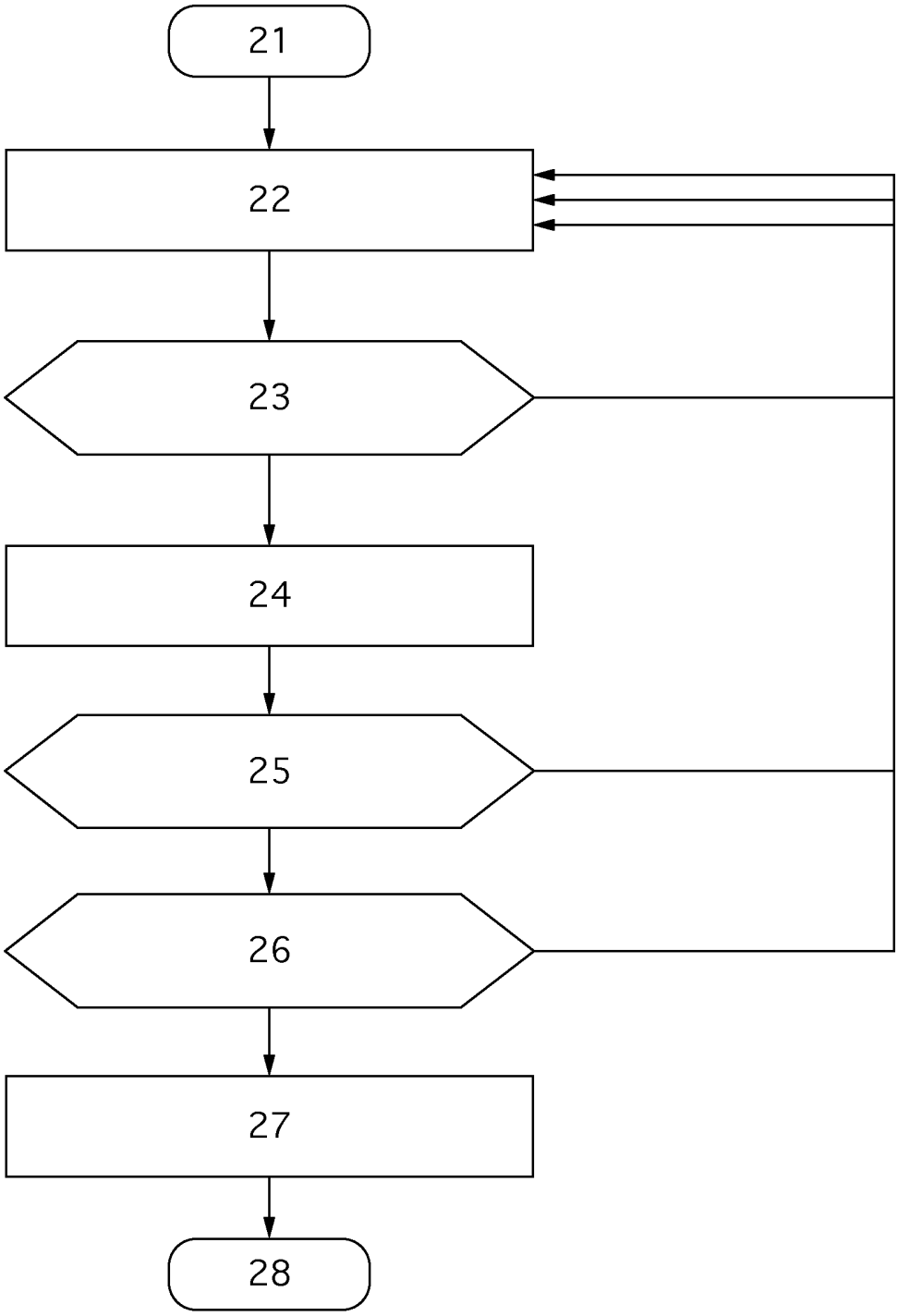

Fig.2

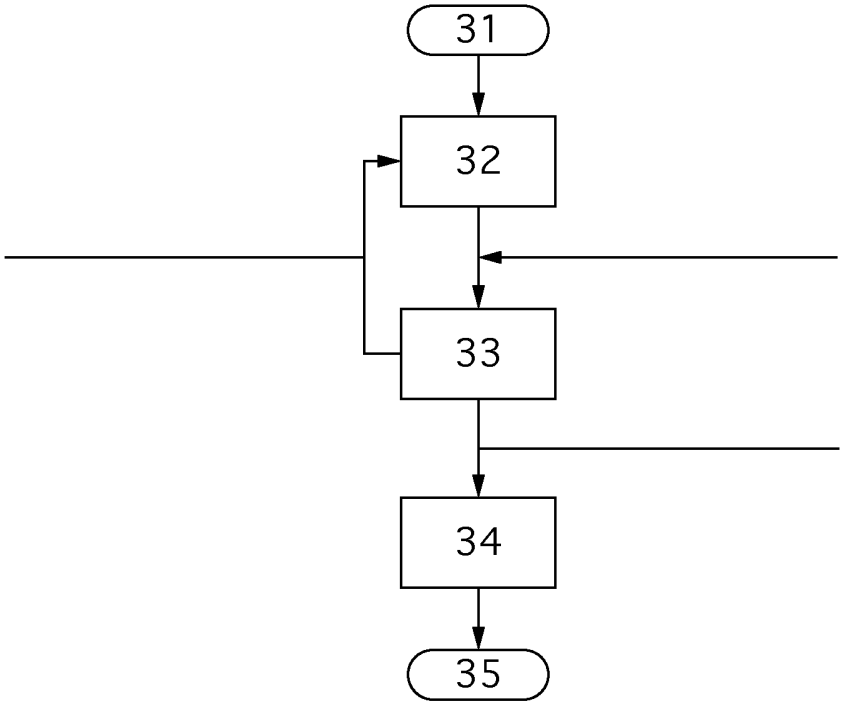

Fig.3

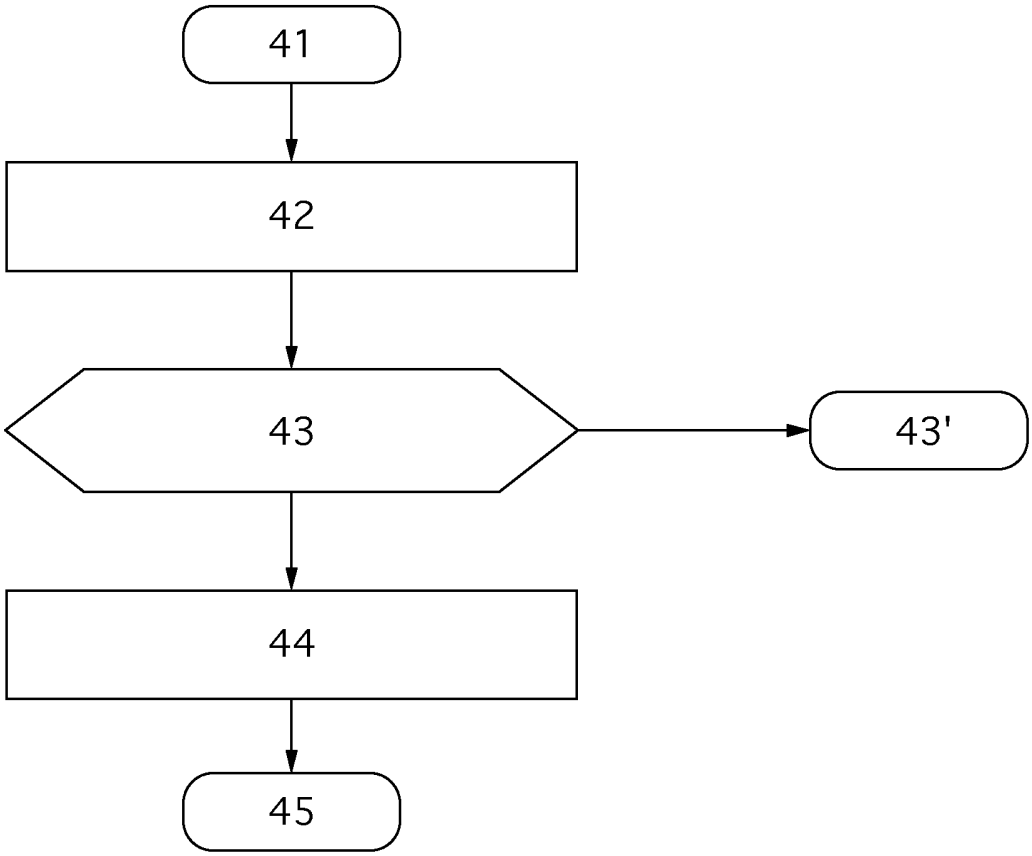

Fig.4

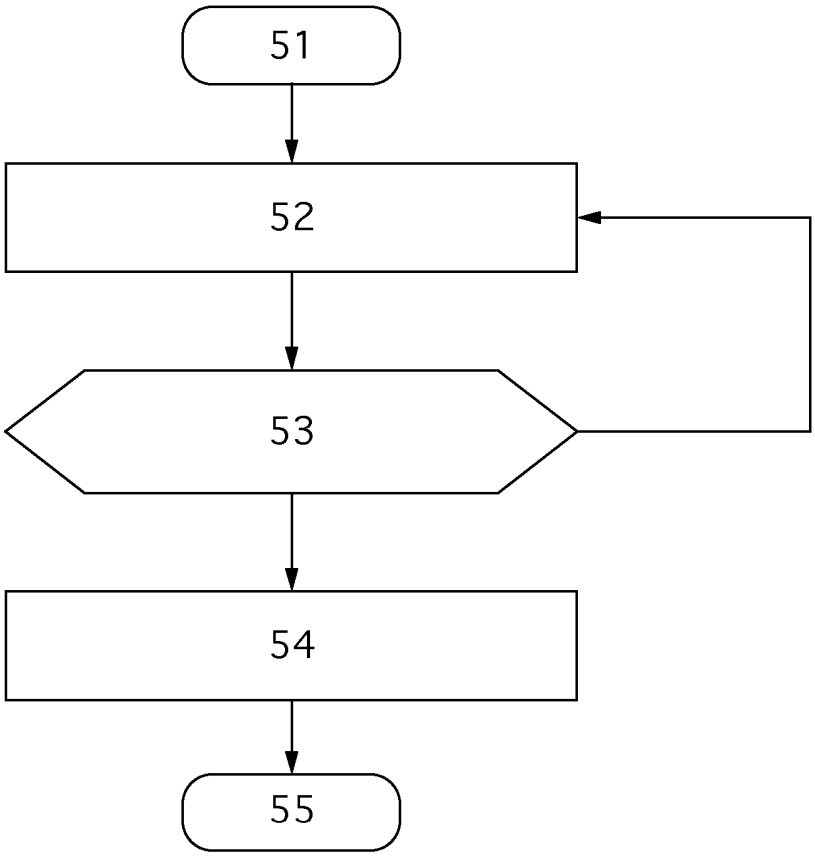

Fig.5

Agentschap NL
Ministerie van Economische Zaken

OCTROOIAANVRAAG NR.:
NO 138778
NL 2010733

ONDERZOEKSRAPPORT

BETREFFENDE HET RESULTAAT VAN HET ONDERZOEK NAAR DE STAND VAN DE TECHNIEK

RELEVANTE LITERATUUR

Categorie[1]	Literatuur met, voor zover nodig, aanduiding van speciaal van belang zijnde tekstgedeelten of figuren.	Van belang voor conclusie(s) nr:	Classificatie (IPC)
X	US 8 365 258 B2 (DISPENSA STEVEN [US] DISPENSA STEPHEN T [US]) 29 januari 2013 (2013-01-29) * kolom 12, regel 6 - regel 67; figuur 9 * * kolom 13, regel 1 - kolom 15, regel 10; figuur 10 * * kolom 15, regel 11 - regel 24; figuur 11 * * kolom 15, regel 66 - kolom 16, regel 6 *	1-20	INV. G06F21/35 G06F21/43 H04L29/06
X	US 2011/213711 A1 (SKINNER ERIC R [CA] ET AL) 1 september 2011 (2011-09-01) * alinea [0015] - alinea [0018]; figuur 1 * * alinea [0021] - alinea [0027]; figuur 2 *	1	
A	WO 2012/004640 A1 (ENTERSECT TECHNOLOGIES PTY LTD [ZA]; BRAND CHRISTIAAN JOHANNES PETRUS) 12 januari 2012 (2012-01-12) * het gehele document *	1-20	

Onderzochte gebieden van de techniek

G06F
H04L

Indien gewijzigde conclusies zijn ingediend, heeft dit rapport betrekking op de conclusies ingediend op:

Plaats van onderzoek:	Datum waarop het onderzoek werd voltooid:	Bevoegd ambtenaar:
's-Gravenhage	11 maart 2014	Vinck, Bart

[1] CATEGORIE VAN DE VERMELDE LITERATUUR

X: de conclusie wordt als niet nieuw of niet inventief beschouwd ten opzichte van deze literatuur
Y: de conclusie wordt als niet inventief beschouwd ten opzichte van de combinatie van deze literatuur met andere geciteerde literatuur van dezelfde categorie, waarbij de combinatie voor de vakman voor de hand liggend wordt geacht
A: niet tot de categorie X of Y behorende literatuur die de stand van de techniek beschrijft
O: niet-schriftelijke stand van de techniek
P: tussen de voorrangsdatum en de indieningsdatum gepubliceerde literatuur
T: na de indieningsdatum of de voorrangsdatum gepubliceerde literatuur die niet bezwarend is voor de octrooiaanvrage, maar wordt vermeld ter verheldering van de theorie of het principe dat ten grondslag ligt aan de uitvinding
E: eerdere octrooi(aanvrage), gepubliceerd op of na de indieningsdatum, waarin dezelfde uitvinding wordt beschreven
D: in de octrooiaanvrage vermeld
L: om andere redenen vermelde literatuur
&: lid van dezelfde octrooifamilie of overeenkomstige octrooipublicatie

EOB FORM 02.83 (P04146)

AANHANGSEL BEHORENDE BIJ HET RAPPORT BETREFFENDE HET ONDERZOEK NAAR DE STAND VAN DE TECHNIEK, UITGEVOERD IN DE OCTROOIAANVRAGE NR.

NO 138778
NL 2010733

Het aanhangsel bevat een opgave van elders gepubliceerde octrooiaanvragen of octrooien (zogenaamde leden van dezelfde octrooifamilie), die overeenkomen met octrooischriften genoemd in het rapport.
De opgave is samengesteld aan de hand van gegevens uit het computerbestand van het Europees Octrooibureau per
De juistheid en volledigheid van deze opgave wordt noch door het Europees Octrooibureau, noch door het Bureau voor de Industriële eigendom gegarandeerd; de gegevens worden verstrekt voor informatiedoeleinden.

11-03-2014

In het rapport genoemd octrooigeschrift	Datum van publicatie	Overeenkomend(e) geschrift(en)	Datum van publicatie
US 8365258 B2	29-01-2013	US 2008120711 A1	22-05-2008
		US 2013185775 A1	18-07-2013
US 2011213711 A1	01-09-2011	GEEN	
WO 2012004640 A1	12-01-2012	GEEN	

EPO FORM P0466

Algemene informatie over dit aanhangsel is gepubliceerd in de 'Official Journal' van het Europees Octrooibureau nr 12/82 blz 448 ev

OCTROOICENTRUM NEDERLAND

SCHRIFTELIJKE OPINIE

DOSSIER NUMMER	INDIENINGSDATUM	VOORRANGSDATUM	AANVRAAGNUMMER
NO138778	29.04.2013		NL2010733

CLASSIFICATIE
INV. G06F21/35 G06F21/43 H04L29/06

AANVRAGER
Baseline Automatisering B.V.

Deze schriftelijke opinie bevat een toelichting op de volgende onderdelen:

- ☒ Onderdeel I Basis van de schriftelijke opinie
- ☐ Onderdeel II Voorrang
- ☐ Onderdeel III Vaststelling nieuwheid, inventiviteit en industriële toepasbaarheid niet mogelijk
- ☐ Onderdeel IV De aanvraag heeft betrekking op meer dan één uitvinding
- ☒ Onderdeel V Gemotiveerde verklaring ten aanzien van nieuwheid, inventiviteit en industriële toepasbaarheid
- ☐ Onderdeel VI Andere geciteerde documenten
- ☐ Onderdeel VII Overige gebreken
- ☐ Onderdeel VIII Overige opmerkingen

DE BEVOEGDE AMBTENAAR
Vinck, Bart

Aanvraag nr.:

SCHRIFTELIJKE OPINIE

NL2010733

Onderdeel I Basis van de Schriftelijke Opinie

1. Deze schriftelijke opinie is opgesteld op basis van de meest recente conclusies ingediend voor aanvang van het onderzoek.

2. Met betrekking tot **nucleotide en/of aminozuur sequenties** die genoemd worden in de aanvraag en relevant zijn voor de uitvinding zoals beschreven in de conclusies, is dit onderzoek gedaan op basis van:

   a. type materiaal:

   ☐ sequentie opsomming

   ☐ tabel met betrekking tot de sequentie lijst

   b. vorm van het materiaal:

   ☐ op papier

   ☐ in elektronische vorm

   c. moment van indiening/aanlevering:

   ☐ opgenomen in de aanvraag zoals ingediend

   ☐ samen met de aanvraag elektronisch ingediend

   ☐ later aangeleverd voor het onderzoek

3. ☐ In geval er meer dan één versie of kopie van een sequentie opsomming of tabel met betrekking op een sequentie is ingediend of aangeleverd, zijn de benodigde verklaringen ingediend dat de informatie in de latere of additionele kopieën identiek is aan de aanvraag zoals ingediend of niet meer informatie bevatten dan de aanvraag zoals oorspronkelijk werd ingediend.

4. Overige opmerkingen:

Aanvraag nr.:

SCHRIFTELIJKE OPINIE

NL2010733

Onderdeel V Gemotiveerde verklaring ten aanzien van nieuwheid, inventiviteit en industriële toepasbaarheid

1. Verklaring

Nieuwheid	Ja:	Conclusies 9, 15, 17
	Nee:	Conclusies 1-8, 10-14, 16, 18-20
Inventiviteit	Ja:	Conclusies
	Nee:	Conclusies 1-20
Industriële toepasbaarheid	Ja:	Conclusies 1-20
	Nee:	Conclusies

2. Citaties en toelichting:

Zie aparte bladzijde

Re Item V

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

Reference is made to the following documents:

D1: US 8 365 258 B2 (DISPENSA STEVEN [US] DISPENSA STEPHEN T [US]) 29 januari 2013 (2013-01-29)

D2: US 2011/213711 A1 (SKINNER ERIC R [CA] ET AL) 1 september 2011 (2011-09-01)

1 The present application does not meet the criteria of patentability, because the subject-matter of **claim 1** is not new.

1.1 D1 (US8365258 B2) discloses:

Werkwijze voor authenticatie tussen een serverproces (Figure 9: the combination of 930, 940, 942 and 944) en een cliëntproces (Figure 1: one or more of 910a, 910b, 910c, 910d and 910e) middels meervoudige communicatie omvattende ten minste een primaire authenticatiecommunicatie (Figure 10: 1010-1025) en een secundaire authenticatiecommunicatie (Figure 10: 1035-1060), waarbij de werkwijze stappen omvat voor:

- het door het serverproces ontvangen van een initiatiecommunicatie van de primaire authenticatiecommunicatie vanaf het cliëntproces (Figure 10: 1015; column 13, lines 12-13),
- het door het serverproces initiëren van de secundaire authenticatiecommunicatie tussen het serverproces en een cliëntauthenticatieproces (Figure 10: 1035; column 13, lines 48-49),
- het door het serverproces ontvangen van primaire authenticatieinformatie omvattende een authenticatiecode of een authenticatieresultaat middels de primaire authenticatiecommunicatie (Figure 10: 1015; column 13, lines 6-9: a username and password combination),
- het door het serverproces ontvangen van secundaire authenticatie-informatie omvattende een authenticatiecode of een authenticatie-resultaat van de secundaire authenticatiecommunicatie (Figure 10: 1050; column 14, lines 19-50),
- het door het serverproces vaststellen van de authenticatie op basis van de primaire (Figure 10: 1020-1030; column 13, lines 13-47) en secundaire authenticatieinformatie (Figure 10: 1055-1065; column 14, lines 50-56),

waarbij de primaire authenticatiecommunicatie en de secundaire authenticatiecommunicatie gescheiden communicaties zijn (column 13, lines 49-52: a second communication channel different from the first communication channel) en/of

waarbij het serverproces op basis van de secundaire authenticatiecommunicatie op zichzelf een secundaire authenticatie kan vaststellen (insofar this feature is clear: the secondary authentication procedure is independent of the first authentication procedure).

1.2 Although D1 describes a method that includes all the method steps of claim 1, the wording may suggest some differences:

- claim 1 suggests a method wherein the sever first receives a initial request, and subsequently, separately, an authentication result, and this for the primary authentication, whereas in D1, the initial request includes the authentication result;
- claim 1 suggests that the user is authenticated using the primary authentication method after user authentication using the secondary authentication method is started, whereas in D1, the secondary authentication method is started is started after the user is authenticated using the first authentication method.

1.3 If claim 1 is read with this interpretation, then it may be considered new with respect to D1.

1.4 However, also in that interpretation, the present application does not meet the criteria of patentability, because in that case, the subject-matter of claim 1 does not involve an inventive step, and this for the following reasons:

1.4.1 Indeed, both the cited prior art and claim 1 disclose few technical details about the primary authentication. When connections are set-up, typically a plurality of messages are exchange between server and client. This is also the case in D1, even when the document does not mention any messages preceding the authentication request. Any of these unmentioned messages may be considered the message initiating the primary authentication method that is specified in claim 1.

1.4.2 The order in which the different method steps are performed is a trivial design choice. It is generally known to the person skilled in the art that the order of the method steps may be changed without this affecting the end result, especially because the primary and the secondary authentication methods are independent of one another.

1.5 Furthermore, the subject-matter of claim 1 does not appear new and inventive with respect to D2 (US2011/0213711 A1). D2 discloses:

Werkwijze voor authenticatie tussen een serverproces (104-Figure 1; [0015]: server) en een cliëntproces (102-Figure 1; [0015]: first unit and 106-Figure 1; [0018]: second unit) middels meervoudige communicatie omvattende ten minste een primaire authenticatiecommunicatie ([0016]: the first unit allows a user to provide authentication information such as a password) en een secundaire authenticatie-communicatie (see below), waarbij de werkwijze stappen omvat voor:

- *het door het serverproces ontvangen van een initiatiecommunicatie van de primaire authenticatiecommunicatie vanaf het cliëntproces (200-Figure 2; [0021]: initiating a transaction, such as a web transaction, by user 108 of the first unit 102 to authenticate the user to the desired website),*
- *het door het serverproces initiëren van de secundaire authenticatiecom-municatie tussen het serverproces en een cliëntauthenticatieproces (204-Figure 2: [0023]: the server sends and transaction confirmation request **136** b to the second unit),*
- *het door het serverproces ontvangen van primaire authenticatieinformatie omvattende een authenticatiecode of een authenticatieresultaat middels de primaire authenticatiecommunicatie (200-Figure 2; [0021]: requiring a user to submit a password and PIN prior to gaining access to a secure web page associated with a service provider),*
- *het door het serverproces ontvangen van secundaire authenticatie-informatie omvattende een authenticatiecode of een authenticatie-resultaat van de secundaire authenticatiecommunicatie (210-Figure 2: [0026]: sending the transaction verification code back to the server by the second unit removes the user from having to enter and potentially mistype information. These operations are shown, for example, in block **210**),*
- *het door het serverproces vaststellen van de authenticatie op basis van de primaire (202-Figure 2; [0021]: the transaction is initiated if the user authenticates properly with the server **104** using known techniques) en secundaire (212-Figure 2; [0027]: The server having generated its own expected transaction code using, for example, the authentication unit **110**, compares the expected transaction code to the received transaction confirmation code from the second unit (also referred to as destination unit) authenticatieinformatie,*

*waarbij de primaire authenticatiecommunicatie en de secundaire authentica-tiecommunicatie gescheiden communicaties zijn ([0015]: a second unit **106** that is different from the first unit **102** but may be in communication with the server **104** via any*

suitable network or networks via a different channel (...) such as a mobile carrier's data network communication channel or any other suitable channel) en/of waarbij het server-proces op basis van de secundaire authenticatiecommunicatie op zichzelf een secundaire authenticatie kan vaststellen (insofar this is clear, it appears to follow from [0027]).

2 For essentially the same reasons, also the corresponding method of **claim 16**, comprising the steps executed by the client process, the machine-readable medium of **claim 18**, the server of **claim 19** and the system of **claim 20** are not new.

3 **Dependent claims 2-15 and 17** do not contain any features which, in combination with the features of any claim to which they refer, meet the requirements of novelty and/or inventive step.

3.1 Per **claim 2**: D1 discloses "een gebruikersacceptatieinvoer" (column 14, lines 21-28).

3.2 Per **claims 3 and 4**: D1 discloses "twee verschillende inrichtingen" (column 15, lines 13-16: a computing device and a telefphone) and discloses "dezelfde inrichting" (column 15, lines 16-24: a single network device).

3.3 Per **claim 5**: D1 discloses the use of a "unieke inrichtingsidentificatie" (Figure 11: column 13, lines 60-63: a contact number).

3.4 Per **claim 6, 12 and 13**: D1 discloses the use of a server comprising a database with data on user accounts, including gebruikersnaam, wachtwoord and unieke identificatiecode (Figure 11: username, password, contact; column 15, line 66 - column 16, line 6).

3.5 Per **claim 7**: D1 disclose "het ontvangen van een beveiligingscode" (column 14, lines 19-24: pressing a predetermined sequence of keystrokes; Figure 11: authentication code).

3.6 Per **claims 8**: D1 discloses "een pushbericht" (column 14, lines 29-31: a text message).

3.7 Per **claims 9**: The use of a "gateway" is a straightforward option that the skilled person would consider if the circumstances favour it.

3.8 Per **claims 10 and 11**: D1 discloses primary and secondary authentication methods that are independent of one another.

3.9 Per **claim 14**: D1 discloses the verification of gebruikersnaam en wachtwoord (column 13, lines 18-21: username and password combination).

3.10 Per **claim 15**: D1 teaches a primary and a secondary authentication method. It would be obvious to the skilled person to combine this with a tertiary authentication method to further secure the authentication.

3.11 Per **claim 17**: The additional feature is understood as follows: the push message sent by the server to the second client contains a reference to the session or resource that the user is trying to access. In this interpretation, this is a straightforward option that the skilled person would consider.

Betreffende Item V

Beargumenteerde verklaring met betrekking tot nieuwheid, inventiviteit of industriële toepasbaarheid; referenties en toelichting ter ondersteuning van deze verklaring

Er wordt verwezen naar de volgende documenten:

D1: US 8 365 258 B2 (DISPENSA STEVEN [US] DISPENSA STEPHEN T [US]) 29 januari 2013 (2013-01-29)

D2: US 2011/213711 A1 (SKINNER ERIC R [CA] ET AL) 1 september 2011 (2011-09-01)

1 De onderhavige aanvrage voldoet niet aan de criteria van octrooieerbaarheid, omdat de materie volgens **conclusie 1** niet nieuw is.

1.1 In D1 (US8365258 B2) wordt geopenbaard:

Werkwijze voor authenticatie tussen een serverproces (figuur 9: de combinatie van 930, 940, 942 en 944) en een cliëntproces (figuur 1: een of meer van 910a, 910b, 910c, 910d en 910e) middels meervoudige communicatie omvattende ten minste een primaire authenticatiecommunicatie (figuur 10:1010-1025) en een secundaire authenticatiecommunicatie (figuur 10:1035-1060), waarbij de werkwijze stappen omvat voor:

- het door het serverproces ontvangen van een initiatiecommunicatie van de primaire authenticatiecommunicatie vanaf het cliëntproces (figuur 10: 1015; kolom 13, regels 12-13),
- het door het serverproces initiëren van de secundaire authenticatiecommunicatie tussen het serverproces en een cliëntauthenticatieproces (figuur 10:1035; kolom 13, regels 48-49),
- het door het serverproces ontvangen van primaire authenticatie-informatie omvattende een authenticatiecode of een authenticatieresultaat middels de primaire authenticatiecommunicatie (figuur 10:1015; kolom 13, regels 6-9: combinatie van een gebruikersnaam en wachtwoord),
- het door het serverproces ontvangen van secundaire authenticatie-informatie omvattende een authenticatiecode of een authenticatieresultaat van de secundaire authenticatiecommunicatie (figuur 10:1050; kolom 14, regels 19-50),
- het door het serverproces vaststellen van de authenticatie op basis van de

primaire (figuur 10:1020-1030; kolom 13, regels 13-47) en secundaire authenticatie-informatie (figuur 10:1055-1065; kolom 14, regels 50-56), waarbij de primaire authenticatiecommunicatie en de secundaire authentica-tiecommunicatie gescheiden communicaties zijn (kolom 13, regels 49-52: een tweede communicatiekanaal dat anders is dan het eerste communicatiekanaal) en/of

waarbij het serverproces op basis van de secundaire authenticatiecommunicatie op zichzelf een secundaire authenticatie kan vaststellen (voor zover deze maatregel duidelijk is: de secundaire authenticatieprocedure is afhankelijk van de eerste authenticatieprocedure).

1.2 Ofschoon in D1 een werkwijze wordt beschreven die alle werkwijzestappen volgens conclusie 1 omvat, kan de formulering enkele verschillen suggereren:

- in conclusie 1 wordt een werkwijze gesuggereerd waarin de server eerst een eerste verzoek ontvangt en vervolgens afzonderlijk een authenticatieresultaat - voor de primaire authenticatie -, terwijl in D1 het eerste verzoek het authenticatieresultaat bevat;
- in conclusie 1 wordt gesuggereerd dat de gebruiker wordt geauthenticeerd met behulp van de primaire authenticatiewerkwijze nadat de gebruikersauthenticatie met behulp van de secundaire authenticatiewerkwijze is gestart, terwijl in D1 de secondaire authenticatiewerkwijze wordt gestart nadat de gebruiker met behulp van de eerste authenticatiewerkwijze is geauthenticeerd.

1.3 Indien conclusie 1 met deze interpretatie wordt gelezen, dan kan deze worden geacht nieuw te zijn ten opzichte van D1.

1.4 Echter, in die interpretatie voldoet de onderhavige aanvrage eveneens niet aan de criteria van octrooieerbaarheid, omdat in dat geval de materie volgens conclusie 1 geen inventiviteit omvat, en wel vanwege de volgende redenen:

1.4.1 Inderdaad worden zowel in de geciteerde stand van de techniek als in conclusie 1 weinig technische gegevens over de primaire authenticatie geopenbaard. Wanneer verbindingen tot stand gebracht worden, worden gewoonlijk een aantal berichten uitgewisseld tussen server en cliënt. In D1 is dit eveneens het geval, zelfs wanneer in het document geen berichten voorafgaand aan het authenticatieverzoek worden genoemd. Deze niet genoemde berichten kunnen worden geacht het bericht te zijn dat de primaire authenticatiewerkwijze initieert die in conclusie 1 wordt gespecificeerd.

1.4.2 De volgorde waarin de verschillende werkwijzestappen worden uitgevoerd is

een triviale ontwerpkeuze. Voor een deskundige in het vakgebied is het algemeen bekend dat de volgorde van de werkwijzestappen kan worden veranderd zonder dat dit van invloed is op het eindresultaat, in het bijzonder omdat de primaire en de secondaire authenticatiewerkwijzen onafhankelijk van elkaar zijn.

1.5 Voorts lijkt de materie volgens conclusie 1 niet nieuw en inventief te zijn ten opzichte van D2 (US2011/0213711 A1). In D2 wordt geopenbaard:

Werkwijze voor authenticatie tussen een serverproces (104-figuur 1;[0015]: server) en een cliëntproces (102-figuur 1; [0015]: eerste eenheid en 106-figuur 1; [0018]: tweede eenheid) middels meervoudige communicatie omvattende ten minste een primaire authenticatiecommunicatie ([0016]: de eerste eenheid maakt het mogelijk een gebruiker authenticatie-informatie, zoals een wachtwoord, te verschaffen) en een secundaire authenticatiecommunicatie (zie hierna), waarbij de werkwijze stappen omvat voor:

- *het door het serverproces ontvangen van een initiatiecommunicatie van de primaire authenticatiecommunicatie vanaf het cliëntproces (200-figuur 2; [0021]: het initiëren van een transactie, zoals een internettransactie, door gebruiker 108 van de eerste eenheid 102 voor het authenticeren van de gebruiker voor de gewenste website),*
- *het door het serverproces initiëren van de secundaire authenticatiecommunicatie tussen het serverproces en een cliëntauthenticatieproces (204-figuur 2: [0023]: de server verzendt een transactiebevestigingsverzoek **136** b naar de tweede eenheid),*
- *het door het serverproces ontvangen van primaire authenticatie-informatie omvattende een authenticatiecode of een authenticatieresultaat middels de primaire authenticatiecommunicatie (200-figuur 2; [0021]: waarvoor een gebruiker een wachtwoord en PIN moet opgeven alvorens toegang tot een beveiligde internetpagina van een dienstverlener te krijgen),*
- *het door het serverproces ontvangen van secundaire authenticatie-informatie omvattende een authenticatiecode of een authenticatieresultaat van de secundaire authenticatiecommunicatie (210-figuur 2: [0026] door het terugsturen van de transactieverificatiecode naar de server door de tweede eenheid hoeft de gebruiker geen informatie meer in te voeren, waarbij mogelijk typefouten kunnen optreden. Deze bewerkingen worden bijvoorbeeld getoond in blok **210**),*
- *het door het serverproces vaststellen van de authenticatie op basis van de primaire (202-figuur 2; [0021]: de transactie wordt geïnitieerd indien de gebruiker op de juiste wijze authenticeert met de server **104** met behulp van bekende technieken) en*

*secundaire (212-figuur 2; [0027]: Nadat de server zijn eigen verwachte transactiecode heeft gegenereerd, vergelijkt bijvoorbeeld de authenticatie-eenheid **110** de verwachte transactiecode met de ontvangen transactiebevestigingscode uit de tweede eenheid (eveneens bestemmingseenheid genoemd) authenticatie-informatie,*

*waarbij de primaire authenticatiecommunicatie en de secundaire authenticatiecommunicatie gescheiden communicaties zijn ([0015]: een tweede eenheid **106** die verschillend is van de eerste eenheid **102**, maar die kan communiceren met de server **104** via (een) geschikt netwerk(en) via een ander kanaal (...) zoals datanetwerkcommunicatiekanaal van een mobiele drager of een ander geschikt kanaal) en/of waarbij het serverproces op basis van de secundaire authenticatiecommunicatie op zichzelf een secundaire authenticatie kan vaststellen (voor zover dit duidelijk is, lijkt dit te volgen uit [0027]).*

2 Om in essentie dezelfde redenen zijn eveneens de overeenkomstige werkwijzeconclusie volgens **conclusie 16,** omvattende de stappen die worden uitgevoerd door het cliëntproces, het machineleesbare medium volgens **conclusie 18,** de server volgens **conclusie 19** en het systeem volgens **conclusie 20,** niet nieuw.

3 De **afhankelijke conclusies 2-15 en 17** bevatten geen maatregelen die in combinatie met de maatregelen volgens een der conclusies waarnaar zij verwijzen voldoen aan de eisen van nieuwheid en/of inventiviteit.

3.1 Met betrekking tot **conclusie 2:** In D1 wordt "een gebruikersacceptatie-invoer" geopenbaard (kolom 14, regels 21-28).

3.2 Met betrekking tot de **conclusies 3 en 4:** In D1 worden "twee verschillende inrichtingen" (kolom 15, regels 13-16: een rekeninrichting en telefoon) en "dezelfde "inrichting" geopenbaard (kolom 15, regels 16-24: één netwerkinrichting).

3.3 Met betrekking tot **conclusie 5:** In D1 wordt het gebruik van een "unieke inrichtingsidentificatie" (figuur 11: kolom 13, regels 60-63): een contactnummer) geopenbaard.

3.4 Met betrekking tot de **conclusies 6, 12 en 13:** In D1 wordt het gebruik van een server omvattend een database met data op gebruikersaccounts geopenbaard, bevattende gebruikersnaam, wachtwoord en unieke identificatiecode (figuur 11: gebruikersnaam, wachtwoord, contact; kolom 15, regel 66 - kolom 16, regel 6).

3.5 Met betrekking tot **conclusie 7**: In D1 wordt geopenbaard: "het ontvangen van een beveiligingscode" (kolom 14, regels 19-24: het indrukken van toetsen in een vooraf bepaalde volgorde; figuur 11: authenticatiecode).

3.6 Met betrekking tot **conclusie 8**: In D1 wordt "een pushbericht" geopenbaard

(kolom 14, regels 29-31): een tekstbericht).

3.7 Met betrekking tot **conclusie 9**: Het gebruik van een "gateway" is een voor de hand liggende optie die een deskundige in het vakgebied zou overwegen indien de omstandigheden dit verlangen.

3.8 Met betrekking tot de **conclusies 10 en 11**: In D1 worden primaire en secundaire authenticatiewerkwijzen geopenbaard die onafhankelijk van elkaar zijn.

3.9 Met betrekking tot **conclusie 14**: In D1 wordt de verificatie van gebruikersnaam en wachtwoord geopenbaard (kolom 13, regels 18-21: combinatie van gebruikersnaam en wachtwoord).

3.10 Met betrekking tot **conclusie 15**: In D1 wordt een primaire en een secundaire authenticatiewerkwijze vermeld. Voor een deskundige in het vakgebied zou het voor de hand liggend zijn deze te combineren met een tertiaire authenticatiewerkwijze voor het verder verzekeren van de authenticatie.

3.11 Met betrekking tot **conclusie 17**: De aanvullende maatregel wordt als volgt begrepen: het pushbericht dat door de server naar de tweede cliënt wordt verzonden bevat een verwijzingsteken naar de sessie of het middel waartoe de gebruiker toegang probeert te krijgen. In deze interpretatie is dit een voor de hand liggende optie die een deskundige in het vakgebied in overweging zou nemen.