(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 July 2008 (24.07.2008)

PCT

(10) International Publication Number
WO 2008/088945 A1

(51) International Patent Classification:
G06F 15/00 (2006.01) *G06F 21/00* (2006.01)

(21) International Application Number:
PCT/US2008/050205

(22) International Filing Date: 4 January 2008 (04.01.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/885,598 18 January 2007 (18.01.2007) US
11/856,636 17 September 2007 (17.09.2007) US

(71) Applicant *(for all designated States except US)*: **MICROSOFT CORPORATION** [US/US]; One Microsoft Way, Redmond, Washington 98052-6399 (US).

(72) Inventors: **GAJJALA, Vijay K.**; One Microsoft Way, Redmond, Washington 98052-6399 (US). **BRACE, Colin H.**; One Microsoft Way, Redmond, Washington 98052-6399 (US). **DEL CONTE, Derek T.**; One Microsoft Way, Redmond, Washington 98052-6399 (US). **NANDA, Arun K.**; One Microsoft Way, Redmond, Washington 98052-6399 (US). **KWAN, Stuart L.S.**; One Microsoft Way, Redmond, Washington 98052-6399 (US). **RAJ, Rashmi**; One Microsoft Way, Redmond, Washington 98052-6399 (US). **NORI, Vijayavani**; One Microsoft Way, Redmond, Washington 98052-6399 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

[Continued on next page]

(54) Title: PROVISIONING OF DIGITAL IDENTITY REPRESENTATIONS

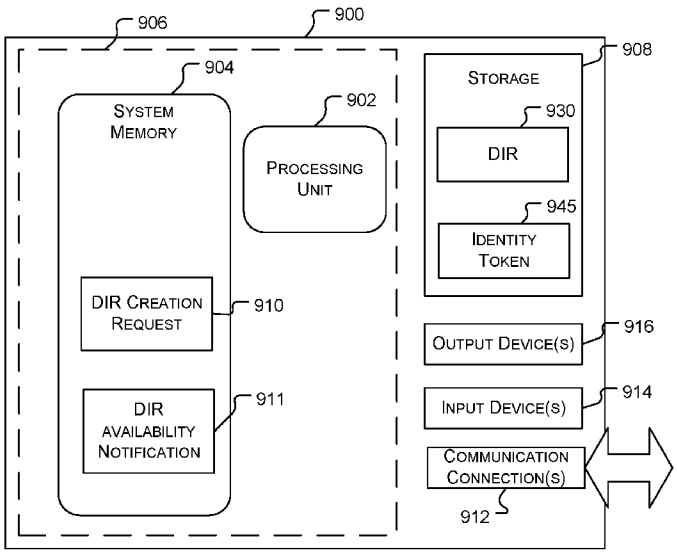

FIG. 9

(57) Abstract: A system and method for provisioning digital identity representations ("DIRs") uses various techniques and structures to ease administration, increase accuracy, and decrease inconsistencies of a digital-identity provisioning system. Various methods are provided for creating new DIRs, requesting DIRs, notifying principals of available DIRs, and approving issuance of new DIRs.

WO 2008/088945 A1

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

PROVISIONING OF DIGITAL IDENTITY REPRESENTATIONS

BACKGROUND

Tremendous innovation has occurred recently in developing systems to give individuals more control over how their personal identity information is distributed and used, particularly in a digital context. For example, Microsoft Corporation of Redmond, Washington, among others, has propagated a system sometimes referred to as the Information Card Selector – Microsoft's instantiation being referred to as Windows CardSpace. In a Windows CardSpace system, a principal obtains one or more digital identity representations, sometimes referred to as information cards. When the principal attempts to access a resource (a "relying party") that requires a set of claims made about the principal, the principal employs a digital identity representation (hereafter called a "DIR") to initiate communication with an identity provider that can assert those claims. In some cases, the identity provider may be controlled by a principal and run on the principal's own machine. In others it may be controlled by a third party. The identity provider returns an "identity token" that includes the required claims information.

Little attention has been directed, however, towards the creation and provisioning of DIRs. Currently, administrators of digital identity systems are forced to craft DIRs manually. For example, an administrator may manually use a software utility, such as an XML generator, to craft a DIR and save it to a particular location. The administrator might then send the principal a pointer to the DIR, and the principal would then go retrieve the DIR. This system is ad hoc, subject to errors and security vulnerabilities, and labor intensive for an administrator.

SUMMARY

This Summary is provided to introduce a selection of concepts in a simplified form that are further described below in the Detailed Description. This Summary is not intended to identify key features or essential features of the claimed subject matter, nor is it intended to be used as an aid in determining the scope of the claimed subject matter.

One aspect relates to a method for provisioning a DIR for a principal. A request is received through a first channel, such as an HTTP request, to create the

DIR for the principal. A notification is then sent through a second channel, e.g., email, that the DIR has been requested. Approval for the DIR to be created is then received before the DIR is created.

Another aspect relates to still another method for provisioning a DIR for a principal. A notification that the DIR is available for the principal is issued. A request to create the DIR is then received before the DIR is created.

Another aspect relates to still another method for provisioning a DIR for a principal. A DIR generation system is polled (e.g., by an application running on the principal's machine) to determine whether any new DIRs are available to the principal. It is then determined whether a new DIR is available to the principal. If so, a request is sent for the new DIR to be created. Finally, the new DIR is received.

Another aspect relates to method for provisioning a DIR for a group of principals. A policy is set that the group of principals is permitted access to the DIR. The group of principals is then notified that the DIR is available. A request is then received from at least a first principal in the group of principals to create the DIR. Finally, the DIR is created for at least the first principal.

BRIEF DESCRIPTION OF THE DRAWINGS

Reference will now be made to the accompanying drawings, which are not necessarily drawn to scale, and wherein:

Figure 1 illustrates an example DIR system including a principal, a principal machine, a relying party, an identity provider, a DIR generation system, an identity data store, an administrator system, and a data capture system;

Figure 2 illustrates an example method for DIR provisioning and use;

Figure 3 illustrates another example method for DIR provisioning and use;

Figure 4 illustrates another example method for DIR provisioning;

Figure 5 illustrates another example method for DIR provisioning;

Figure 6 illustrates another example method for DIR provisioning;

Figure 7 illustrates another example method for DIR provisioning;

Figure 8 illustrates another example method for DIR provisioning; and

Figure 9 illustrates an example of a computing device.

DETAILED DESCRIPTION:

Example embodiments will now be described more fully hereinafter with reference to the accompanying drawings. Like numbers refer to like elements throughout.

Example embodiments disclosed herein relate generally to identity systems including DIRs used in initiating communication for production of identity tokens that can be exchanged between a principal, an identity provider, and a relying party to authenticate an identity and/or information related to the principal. In example embodiments herein, the principal may be a natural person or persons, a computer, a network, or any other entity. The relying party has goods, services, or other information that the principal desires to access and/or obtain. In example embodiments, the relying party can be any resource, privilege, or service that requires a security policy to enter, access, or use. For example, a relying party may comprise one or more of: computers, computer networks, data, databases, buildings, personnel, services, companies, organizations, physical locations, electronic devices, or any other type of resource.

Referring now to Figure 1, an example DIR system 100 is shown including a principal 110 and a relying party 120. Principal 110 is in possession or control over principal machine 111. Principal machine 111 includes a computer system at least temporarily controlled by the principal 110. Relying party 120 may also include a computer system. System 100 may also include an administrator system 160, a data capture system 162, a DIR generation system 164, and identity data store 168, and an identity provider 115, each of which are discussed further below and may include, or be part of, a computer system.

Principal 110 and relying party 120 can communicate with each other over one or more networks, such as the Internet, or through telephonic or other forms of wired or wireless communication. In example embodiments, principal 110 can request goods, services, information, privileges, or other access from relying party 120. Relying party 120 can require authentication of the identity of, or information about, principal 110 before or in conjunction with providing the requested access to principal 110.

Also shown in Figure 1 is an example identity provider 115. Identity provider 115 includes a computer system. In example embodiments, identity provider 115 includes a claims transformer 130 and a claims authority 140. The claims transformer 130 is sometimes referred to as a "security token service." In the example shown, identity provider 115 can provide one or more claims about principal 110. A claim is a statement or assertion made about the principal, possibly including information about the principal such as, for example, name, address, social security number, age, credit history, transactional requirements, etc. As described further below, identity provider 115 can provide claims to principal 110 and/or relying party 120 in the form of a digitally signed identity token. In example embodiments, identity provider 115 is in a trusted relationship with relying party 120, so that relying party 120 trusts the claims in the signed identity token from identity provider 115.

Although claims transformer 130 and claims authority 140 of identity provider 115 are shown as separate entities in Figure 1, in alternative embodiments claims transformer 130 and claims authority 140 can be the same entity or different entities. Identity provider 115 may take the form of a security token service in some example embodiments. Similarly, identity provider 115 and DIR generation system 164 may be the same or different entities.

Computer systems described herein include, without limitation, a personal computer, server computer, hand-held or laptop device, microprocessor system, microprocessor-based system, programmable consumer electronics, network PCs, minicomputers, mainframe computer, smart card, telephone, mobile or cellular communication device, personal data assistant, distributed computing environment that includes any of the above systems or devices, and the like. Some computer systems described herein may comprise portable computing devices. A portable computing device is any computer system that is designed to be physically carried by a user. Each computer system may also include one or more peripherals, including without limitation: keyboard, mouse, a camera, a web camera, a video camera, a fingerprint scanner, an iris scanner, a display device such as a monitor, a microphone, or speakers.

Each computer system includes an operating system, such as (without limitation) the WINDOWS operating system from Microsoft Corporation, and one or more programs stored on the computer readable media. Each computer system may also include one or more input and output communications devices that allow the user to communicate with the computer system, as well as allow the computer system to communicate with other devices. Communications between the computer systems used by principal 110 (e.g., principal machine 111), relying party 120, DIR generation system 164, administrator system 160, data capture system 162, and identity provider 115 can be implemented using any type of communications link, including, without limitation, the Internet, wide area networks, intranets, Ethernets, direct-wired paths, satellites, infrared scans, cellular communications, or any other type of wired or wireless communications.

In some example embodiments disclosed herein, system 100 is implemented at least in part as an Information Card system provided in the .NET 3.0 framework developed by Microsoft Corporation of Redmond, Washington. The Information Card system allows principals to manage multiple DIRs from various identity providers.

The Information Card system utilizes a web services platform such as the Windows Communication Framework in the .NET 3.0 framework. In addition, the Information Card system is built using the Web Services Security Specifications propagated at least in part by Microsoft Corporation of Redmond, Washington. These specifications include a message security model WS-Security, an endpoint policy WS-SecurityPolicy, a metadata exchange WS-MetadataExchange, and a trust model WS-Trust. Generally, the WS-Security model describes how to attach identity tokens to messages. The WS-SecurityPolicy model describes end point policy requirements, such as required identity tokens and supported encryption algorithms. Such policy requirements can be conveyed and negotiated using a metadata protocol defined by WS-MetadataExchange. The WS-Trust model describes a framework for trust models that enables different web services to interoperate. Some example embodiments described herein refer to the Web Services Security Specifications described above. In alternative embodiments, one

or more other specifications can be used to facilitate communications between the various subsystems in system 100.

Referring again to Figure 1, principal 110 can send a request via principal machine 111 to relying party 120 for access to goods, services, or other information. For example, in one embodiment, principal machine 111 sends a request to relying party 120 for access to information from relying party 120 that principal 110 desires. The request sent by principal machine 111 can include a request for the authentication requirements of relying party 120 using, for example, the mechanisms provided in WS-MetadataExchange.

In response to the request, relying party 120 may send principal machine 111 requirements for relying party 120 to authenticate principal's identity or other information about principal 110. The requirements of relying party 120 for authentication are referred to herein as a security policy. A security policy minimally defines the set of claims from a trusted identity provider 115 that the principal 110 must provide to relying party 120 for relying party 120 to authenticate principal 110. A security policy can include a requirement of proof regarding a personal characteristic (such as age), identity, financial status, etc. It can also include rules regarding the level of verification and authentication required to authenticate any offers of proof (e.g., digital signature from a particular identity provider).

In one example, relying party 120 specifies its security policy using WS-SecurityPolicy, including both the claim requirements and type of identity token required by relying party 120. Examples of types of claims include, without limitation, the following: first name, last name, email address, street address, locality name or city, state or province, postal code, country, telephone number, social security number, date of birth, gender, personal identifier number, credit score, financial status, legal status, etc.

The security policy can also be used to specify the type of identity token required by relying party 120, or a default type can be used as determined by the identity provider. In addition to specifying the required claims and token type, the security policy can specify a particular identity provider required by the relying

party. Alternatively, the policy can omit this element, leaving the determination of the appropriate identity provider up to principal 110. Other elements can be specified in the security policy as well such as, for example, the freshness of the required security token.

In some embodiments, principal 110 can require that relying party 120 identify itself to principal machine 111 so that principal 110 can decide whether or not to satisfy the security policy of relying party 120, as described below. In one example, relying party 120 identifies itself using an X509 certificate. In other embodiments, relying party 120 can identify itself using other mechanisms such as, for example, a Secure Sockets Layer ("SSL") server certificate.

Principal machine 111 may include one or more DIRs for principal 110. These DIRs (sometimes referred to as "Information Cards" in the Windows Cardspace system provided in the .NET 3.0 framework developed by Microsoft Corporation of Redmond, Washington) are artifacts that represent the token issuance relationship between principal 110 and a particular identity provider, such as identity provider 115. Each DIR may correspond to a particular identity provider, and principal 110 can have multiple DIRs from the same or different identity providers. The use of DIRs in an identity system is described in detail in United States Patent Application No. 11/361,281, which is incorporated herein by reference as if fully set forth herein.

DIRs can include, among other information, the identity provider's issuance policy for identity tokens, including the type of tokens that can be issued, the claim types for which it has authority, and/or the credentials to use for authentication when requesting identity tokens. DIRs may be represented as XML documents that are issued by identity providers 115 or DIR generation systems 164 and stored by principals 110 on a storage device such as principal machine 111.

Principal machine 111 may also include an identity selector. Generally, an identity selector is a computer program and user interface that permits principal 110 to select between one or more DIRs of principal 110 on principal machine 111 to request and obtain identity tokens from one or more identity providers, such as identity provider 115. For example, when a security policy from relying party 120

is received by principal machine 111, the identity selector may be programmed to identify one or more DIRs that satisfy one or more of the claims required by the security policy using the information in DIRs. Once principal 110 receives the security policy from relying party 120, principal 110 can communicate with (using, for example, principal machine 111) one or more identity providers to gather the claims required by the policy.

In example embodiments, principal 110 requests one or more identity tokens from identity provider 115 using the issuance mechanism described in WS-Trust. In example embodiments, principal 110 forwards the claim requirements in the policy of relying party 120 to identity provider 115. The identity of relying party 120 can, but need not, be specified in the request sent by principal 110 to identity provider 115. The request can include other requirements as well, such as a request for a display token.

Generally, claims authority 140 of identity provider 115 can provide one or more of the claims required by the security policy from relying party 120. Claims transformer 130 of identity provider 115 is programmed to transform the claims and to generate one or more signed identity tokens 150 that include the claim(s) relating to principal 110.

As noted above, principal 110 can request an identity token in a certain format in its request to identity provider 115, based on requirements from relying party 120. Claims transformer 130 can be programmed to generate identity tokens in one of a plurality of formats including, without limitation, X509, Kerberos, SAML (versions 1.0 and 2.0), Simple eXtensible Identity Protocol ("SXIP"), etc.

For example, in one embodiment, claims authority 140 is programmed to generate claims in a first format A, and the security policy of relying party 120 requires an identity token in a second format B. Claims transformer 130 can transform the claims from claims authority 140 from format A into format B before sending an identity token to principal 110. In addition, claims transformer 130 can be programmed to refine the semantics of a particular claim. In example embodiments, the semantics of a particular claim are transformed to minimize the amount of information provided in a particular claim and/or identity token to

reduce or minimize the amount of personal information that is conveyed by a given claim.

In example embodiments, claims transformer 130 forwards the identity token 150 to principal 110 using the response mechanisms described in WS-Trust. In one embodiment, claims transformer 130 includes a security token service (sometimes referred to as an "STS"). In an example embodiment, principal 110 forwards identity token 150 to relying party 120 by binding identity token 150 to an to application message using the security binding mechanisms described in WS-Security. In other embodiments, identity token 150 may be sent directly from the identity provider 115 to relying party 120.

Once relying party 120 receives identity token 150, relying party 120 can verify (e.g., by decoding or decrypting the identity token 150) the origin of signed identity token 150. Relying party 120 can also utilize the claim(s) in identity token 150 to satisfy the security policy of relying party 120 to authenticate principal 110.

Provisioning of DIRs will now be discussed in greater detail. Principal 110 may obtain a DIR in a variety of ways. In the example embodiment illustrated in Figure 1, DIR generation system 164 is generally used to communicate with principal 110, create new DIRs, and notify principal 110 of available DIRs. DIR generation system 164 may in some embodiments comprise an internet web site. In other embodiments, DIR generation system 164 may comprise a web service. DIR generation system 164 may also include or work in conjunction with an internet information server (IIS) 166 in certain embodiments.

Identity data store 168 is a digital information storage system that can be accessed in certain embodiments by identity provider 115, DIR generation system 164, and administrator system 160. Identity data store 168 may comprise a database server, computer memory, or any other data storage device(s). Identity data store 168 may be comprised of a plurality of devices or systems in a distributed data model. Identity data store 168 may also include or comprise a directory service such as Active Directory 169 propagated by Microsoft Corporation of Redmond, Washington.

Administrator system 160 may include a computer system, including a user interface that will allow an administrator to communicate with identity data store 168 and DIR generation system 164. Administrator system 160 permits an administrator to organize and administer the data within identity data store 168. It also permits an administrator to determine the types of DIRs that DIR generation system 164 creates, and allows an administrator to control whether a particular principal is eligible to receive particular DIRs. Use of administrator system 160 is discussed further below.

Certain embodiments may include a separate data capture system 162. Data capture system 162 may comprise a computer system adapted to capture information relating to principals. For example, data capture system 162 may comprise a human-resources computer system that captures personal information about a principal, such as name, phone number, social security number, address, etc. Data capture system 162 may include separate storage or may utilize the identity data store 168.

Figure 2 illustrates a method 200 that may be implemented via system 100. At step 210, an administrator configures an identity data store. For example, an administrator may use administrator system 160 to configure identity data store 168. The administrator may, in some embodiments, use administrator system 160 to set up tables in identity data store 168 that will be used to administer, generate, and manage DIRs. In an exemplary embodiment, the administrator may determine the types of claims that will be supported in DIRs created by DIR generation system 164 and identity tokens generated by identity provider 115. The administrator may also use administrator system 160 to configure identity data store 168 to store policy information, such as the types of tokens identity provider 115 supports, entitlement information, and federation metadata. Other information in identity data store 168 that may be embedded in a DIR include a photograph of the principal 110 and connectivity information relating to identity providers such as identity provider 115.

The method 200 then proceeds to step 220, when principal 110 requests a DIR. A request for a DIR can be made in a variety of ways. For example,

principal 110 can use principal machine 111 to access DIR generation system 164. In some embodiments, DIR generation system 164 is a web site, and principal machine 111 accesses the DIR generation system 164 through an Internet browser to request a DIR. In some embodiments, principal 110 requests a particular DIR. In other embodiments, discussed further below, principal 110 requests a list of DIRs available to principal 110 and chooses from that list.

The method 200 then proceeds to step 230, when DIR generation system 164 checks with the identity data store 168, generates the DIR, and provides the DIR to principal 110. In one embodiment, DIR generation system 164 first checks with identity data store 168 to determine whether the principal 110 is entitled to the requested DIR. This can be accomplished in a variety of ways, including by checking an entitlements DLL within identity data store 168, performing an Active Directory access check, etc. DIR generation system 164 may also access identity system metadata stored within identity data store 168 to determine what types of identity claims are available to be included within the new DIR.

When DIR generation system 164 creates the new DIR, the DIR may take the form of an XML document and may include, among other information: an image for display on the principal machine; a list of claims included in the DIR; a list of available token types for the DIR; a unique DIR identifier; a credential hint (discussed further below); identification of the identity provider; and an end-point reference for the identity provider 115. The new DIR may be provided to the principal in a variety of ways as well, including an email of the new DIR, an HTTP message, or other methods. As used herein, "email" includes text messaging, instant messaging, and similar forms of electronic communication.

Upon receipt of the new DIR, the principal 110 stores 240 the DIR, for example in memory associated with principal machine 111. Principal 250 then requests access to a relying party, such as relying party 120. The relying party denies access (e.g., via a redirect to an authentication page) and provides 260 its security policy back to the principal 110. The principal 110 then selects 270 a DIR to meet the security policy of the relying party 120. This can be accomplished, for example, through a user interface on the principal machine 111 that displays all

available DIRs to principal 110. In some embodiments, DIRs that meet the requirements of the relying party's security policy may be highlighted for the principal 110, and other cards may be dimmed to make the selection process easier for the principal 110.

Principal 110 then sends 280 the request for an identity token to an identity provider, such as identity provider 115. This request for an identity token can be generated automatically by principal machine 111 upon selection by principal 110 of a DIR stored on principal machine 111. Identity provider 115 checks 285 the identity data store 168 to obtain the required information to populate the requested identity token. This information could include, for example, claims data. For example, if the selected DIR includes a claim of age, the identity provider 115 may check the identity data store 168 to determine the age of principal 110. Identity provider 115 is then able to create 285 the requested identity token and send 290 it to the principal. The principal then sends 295 the identity token to the relying party and is granted access as previously discussed.

In providing access by identity provider 115 to the same identity data store 168 used by DIR generation system 164, an administrator can ensure that the generation of DIRs remains in synch with the actual data available to fulfill claims in a requested identity token. For example, if an administrator configures identity data store 168 such that data for an age claim is not stored there, then DIR generation system 164 will not create a DIR that includes an option for an age claim. Otherwise, synchronization problems can arise. For example, assume an administrator creates a new DIR ad hoc (without reference to available identity data), and an age claim is included and sent as part of a DIR back to a principal. When the principal attempts to obtain an identity token with an age claim, that information is not available, and the token will be rejected by the relying party as insufficient. System 100, by contrast, permits automatic synchronization of the DIRs generated and the availability of underlying data to populate corresponding identity tokens. An administrator is provided the ability through administrator system 160 to make changes in the identity data store that will automatically affect both provisioning of DIRs and issuance of corresponding identity tokens.

In some embodiments, when the administrator makes particular changes to identity data store 168 that affect the validity of already-issued DIRs, any principals who have received affected DIRs are notified and permitted to obtain new DIRs. For example, assume privacy regulations require that the administrator eliminate the home addresses of any principals stored in identity data store 168. Any principal 110 that received a DIR that included a claim as to his/her home address now has an invalid DIR (because there is no longer any data in identity data store 168 to satisfy that claim). In one embodiment, all such principals are notified, for example via an email from DIR generation system 164, that the DIR(s) are now invalid and inviting the principals to obtain a new DIR that does not include the no-longer-supported home address claim. In this manner, the single change by the administrator to the identity data store 168 (a) prevents new DIRs from being issued with a home address claim, and (b) alerts principals that existing DIRs that include that claim are invalid and may be replaced.

Referring now to Figure 3, an exemplary method 300 is described in relation to the system 100 shown in Figure 1. In this example, the principal 110 authenticates to the principal machine 111. Principal machine 111, for example, may be connected to an intranet that includes a directory service, such as Active Directory server 169. Authentication of principal 110 to principal machine 111 may include using sign-on information from any known method, including username/password, smart card, etc. Principal 110 then initiates 320 a DIR request by, for example, pointing a browser on the principal machine 111 to a web site that comprises the DIR generation system 164. Principal 110 then authenticates 330 at the DIR generation system 164. In some embodiments, principal machine 111, DIR generation system 164, identity data store 168, identity provider 115, and administrator system 160 could be part of the same intranet. In that embodiment, it is possible that single-sign-on capability may be available. For example, if the principal machine is running a WINDOWS operating system available from Microsoft Corporation of Redmond, Washington, and Windows Integrated Authentication is turned on, then authentication at the DIR generation system 164 may be automatic and seamless to the principal 110 – information used to log on to

principal machine 111 is passed to DIR generation system 164 along with the request for access. In other embodiments, the administrator may configure DIR generation system 164 to require a separate authentication of principal 110. The administrator may configure the DIR generation system 164 to require any of a variety of authentication mechanisms, including username/password, smart card, etc. In some embodiments, the principal 110 may be authenticated by IIS 166, which can be easily configured by an administrator to accept any of a variety of authentication methods.

Once the principal 110 is authenticated, DIR generation system 164 accesses 350 identity data store 168. In this example, the DIR generation system 164 takes the form of a web service to allow negotiation between the DIR generation system and the principal 110. In this example, the negotiation determines the type of DIR that will be returned to the principal 110. In this instance, the DIR generation system 164 obtains 350 available DIR descriptors. In exemplary embodiments, an administrator uses administrator system 160 to create DIR descriptors. For example, a corporate IT administrator may create descriptors that represent different DIRs for different levels of employees. A part-time employee, for example, may have a different set of claims than a full-time employee. A CEO may have a different set of claims than a staff employee. Even the images that are associated with each DIR descriptor may vary – e.g., the sales group DIR image could be orange while the accounting group DIR image is green. Further, it is possible to personalize the card image to contain the image of the principal 110 (obtained from the identity data store 168). This enhances the association that the principal 110 makes between his/her DIRs and the identity provider 115. It provides better "fingerprinting" capabilities as well.

In some embodiments, the administrator system 160 includes a user interface that parses through all of the available types of information available in the identity data store 168 and presents the administrator with an easy way to create descriptors. For example, the administrator may be presented with a list of: (a) principal classes (e.g., part-time employee, full-time employee, executive team member, sales group member, etc.); (b) claim types (name, address, phone number,

age, etc.); (c) security clearances; (d) employment status (current, terminated); etc. The administrator could then decide to create distinct descriptors available to some or all of the classes of principals. For example, all principals may be eligible to receive a basic DIR that includes the principal's name, phone number, and employment status. However, only the executive team may be eligible to receive a DIR that also includes a high-level security clearance. These descriptors can be created by the administrator and saved in the identity data store along with a policy delineating which principals are permitted to receive DIRs corresponding to particular descriptors. Possible commands that may be useful to an administrator in managing descriptors include: "GET DESCRIPTORS, GET ALL DESCRIPTORS, ADD DESCRIPTORS, CHANGE DESCRIPTORS, DELETE DESCRIPTORS, COPY DESCRIPTOR, etc."

The request by the principal 110 for available descriptors may be accomplished by the principal machine 111 through a web service method such as "GET DESCRIPTORS." This would cause the DIR generation system to check the principal 110 against the policy set by the administrator to determine which, if any, descriptors are available to that principal 110. This can be accomplished, e.g., via an Active-Directory access check. Descriptors may be stored in any or all of, e.g.: an identity data store 168, memory associated with DIR generation system 164, or a separate store.

The DIR generation system 164 then sends 360 the available descriptors to the principal machine 111. Principal 110 then selects 370 from the available descriptors and requests particular DIR(s) corresponding to the descriptor(s). Again, this can be accomplished, for example, by a web service method such as "GET CARD(s)" (referring in this example to Information Cards available in the Windows CardSpace system propagated at least in part by the Microsoft Corporation of Redmond, Washington). A principal 110 may request one or several available DIRs.

The DIR generation system 164 then creates 380 the requested DIR(s). In exemplary embodiments, the DIR generation system includes in the DIR a credential hint to "back" the DIR. For example, the DIR may include a

username/password credential hint, and the principal 110 may be required to authenticate using that username/password in order to use the DIR to obtain an identity token. In some embodiments, the authentication type can be taken from the authentication used by principal 110 to gain access to the DIR generation system 164. For example, if the principal 110 used a username/password combination to authenticate to IIS 166, the DIR generation system 164 may use the same username and password to back the DIR when it is sent back to the principal 110.

In other embodiments, the digital generation system may have access to a directory service, such as Active Directory 169, that may include other available authentication methods for a particular principal 110. For example, if principal 110 uses a username/password to authenticate to DIR generation system 164, but Active Directory also includes a certificate associated with a smart card registered to the principal 110, the DIR generation system 164 could include either or both authentication types as part of the DIR returned to the principal 110. In addition, if single-sign-on capability is enabled between the principal machine 111 and the DIR generation system 164, the authentication type that is included in the DIR may be the authentication type used by the principal 110 to authenticate to the principal machine 111.

Once the DIR(s) is/are generated by the DIR generation system 164, they are sent 390 to the principal 110 via any of a variety of methods, including email, HTTP, etc. In some embodiments, the file that includes the DIR(s) may be pin protected. This is because, particularly in the case where multiple DIRs are sent to the principal 110, the file containing the DIRs may include cryptographic key material that should be protected against unauthorized access. The pin allows the establishment of a shared secret between principal machine 111 and DIR generation system 164. A file containing DIR(s) then could be decrypted by the principal when installing the DIRs onto principal machine 111. Exemplary methods for initiating, approving, and sending DIRs are discussed further below.

Referring now to Figure 4, a method 400 is illustrated. At step 410 a request to create a DIR is received through a first channel. For example, principal 110 may

use an internet browser on principal machine 111 to request a new DIR from DIR generation system 164. At step 420, a notification is issued 420 through a second channel that the DIR has been requested. For example, in response to a request for a new DIR from principal 110, the DIR generation system 164 or an application running on principal machine 111 may send an email notification that the request has been made. This may act as a "check" to ensure that the principal 110 is the one who is requesting the DIR and not an imposter. In some embodiments, the email may be directed to a known email address for the principal. In other embodiments, the notification may be directed to a third-party whom the administrator's policy requires to approve the issuance of a new DIR for the particular principal 110. For example, some DIRs may be available to certain employees in an organization only if their managers approve the issuance. This type of DIR may be used, for example, to gain access to a confidential work group.

As used herein, a "channel" refers to the manner in which information at issue is communicated. The distinction between different channels in method 400 is a logical one. Two distinct channels could employ some or all of the same physical or electronic communication link or different paths altogether. For example, a notification at step 420 could be sent over the same communication link (e.g., the Internet) as the approval at step 430, but the channels may be logically different (e.g., one could be an email and the other could be an HTTP message).

At step 430, an approval for the DIR to be created is received. For example, the recipient of the notification in step 420 from the DIR generation system 364 may respond and approve the issuance of the requested DIR. This can be accomplished in a variety of ways. For example, the notification in step 420 could comprise an email with a link to an approval site hosted by the DIR generation system 364.

At step 440, the requested DIR is created. If approval were denied by the recipient of the notification at step 420, other events may occur. For example, the administrator may be notified that an unauthorized request was made for a DIR.

Referring now to Figure 5, another exemplary method 500 is shown. At step 510, a notification is issued that a DIR is available to a principal. For example,

DIR generation system 364 could send principal 110 an email alerting the principal 110 that a new DIR is available. Alternatively, the notification could go to a third party, such as the principal's manager. This type of notification could be useful in a situation where the administrator has, for example, changed the identity data store 168 to include an additional descriptor. DIR generation system 364 could then be used to notify all principals in a class that qualifies for the descriptor that the new DIR is available. For instance, a manager in a particular business unit may ask an administrator to create a new descriptor for a DIR to be used in conjunction with a particular project. Once the administrator creates the descriptor, the notification of all the principals the manager desires to have the new DIR could be automatic.

Notification 510 could also be included as part of a general business workflow. For example, when a new principal starts work an organization, the human resources department could capture information about the principal through data capture system 162. That data capture could kick off a series of automated steps, including storing the relevant identity data regarding the principal in the identity data store 168 and notifying the principal 110 that a DIR is now available to him/her. Notification can take many forms, including an email to the principal that includes a link to a web site that comprises the DIR generation system 164. Alternatively, an application could be running on the principal machine 111 that is adapted to receive a message from the DIR generation system 164 that a new DIR is available to the principal 110 (e.g., the application could spawn a pop-up message, an icon could appear in a toolbar on the principal machine 111, etc.).

At step 520, a request to create the DIR is received. This step can be accomplished again in a variety of manners. For example, the principal 110 could respond to a notification email by clicking on a link that takes him/her to a web page that gives the principal the option to request the DIR. Alternatively, where an application on the principal machine 111 alerts the principal 110 that the DIR is available, the principal could request the DIR within such application and the application could send a message back to the DIR generation system 364 to make the request.

At step 530, the DIR is created as requested. The creation of the DIR may be accomplished as described elsewhere herein. The DIR is then sent 540 to the principal, also as described elsewhere herein.

Referring now to Figure 6, another exemplary method 600 is shown. At step 610, a DIR generation system is polled for new DIRs that are available to the principal. For example, principal machine 111 may be programmed to periodically poll the DIR generation system 164 at predetermined intervals. At step 620, it is determined whether any new DIRs are available to the principal. The DIR generation system 164, for example, could check in identity data store 168 whether any new descriptors have become available to principal 110 since the time it was last polled by principal machine 111. At step 630, a request is made that the new DIR be created. Continuing the example, upon receipt of notification that a new DIR is available, the principal 110 could request that the DIR generation system 164 create the new DIR. At step 640, the new DIR is received (e.g., a new DIR could be received by the principal machine 111 from the DIR generation system 164). This method 600 is another example of how an administrator's job could be simplified. If all principal machines were programmed to poll for new DIRs, for example, when an administrator creates a new DIR descriptor in identity data store 168, the issuance and delivery of the new DIRs is automatic and requires no further work on behalf of the administrator.

It may also be beneficial to be able to create DIRs dynamically in response to a relying party's security policy. Referring now to Figure 7, an example method 700 is illustrated. At step 710, access is requested to a relying party. For example, if relying party 120 is a restricted web site, principal machine 111 attempts to access the web site through a browser. At step 720, access to the relying party is denied and a security policy from the relying party is received. Continuing the example, the relying party 120 sends principal machine 111 its security policy and an HTTP message that redirects the principal machine 111 browser to an authentication web page. A DIR that satisfies the security policy is then requested 730 from a DIR generation system. In the example above, the principal machine 111 may first check whether it has a sufficient DIR and, if not, principal machine

111 may be programmed to query a local cache for identity providers that offer DIRs meeting the security policy of relying party 120. Principal machine may also query a public list of DIR providers hosted by a third party. Principal 110 can then choose an appropriate DIR provider and DIR generation system, such as DIR generation system 164. At step 740, the DIR is received. In the example above, the principal machine 111 receives the new DIR, which it can then forward to identity provider 115 to obtain the necessary identity token to gain access to relying party 120.

In some embodiments, the principal machine 111 may forward the security policy of relying party 120 to the DIR generation system 164. The DIR generation system 164 may then check the identity data store 168 to determine whether the claims and other requirements set forth in the security policy can be satisfied. If so, a DIR meeting the security policy would be created. In this manner, a principal is able to obtain a DIR on an as-needed basis, regardless of whether the administrator has preconfigured an identity descriptor that meets the needs of that particular relying party's security policy.

Referring now to Figure 8, another exemplary method 800 is shown. At step 810 a policy is set for a group of principals, authorizing the group of principals that a DIR is available. With reference to the exemplary system 100 of Figure 1, an administrator could use administrator system to set a policy in identity data store 168 authorizing all principals that are part of a particular group to receive a particular DIR. In some embodiments, this can be accomplished by an administrator using the "Group Policy" feature available in Active Directory 169 or other means to launch a client-side application resident on principal machine 111. At step 820, the group of principals to whom the DIR is available is notified. In the example above, the client-side application resident on principal machine 111 is activated. This can result in the principal 110 being prompted that a DIR is now available (e.g., through a pop-up, a tool-bar icon, etc.). The client-side application can have its own set of rules (e.g., ability for the principal 110 to choose to be reminded later, to provide the principal 110 only a certain amount of time to retrieve the new DIR, etc.). At step 830, a request from at least a first principal in

the group of principals is received to create the DIR. In some embodiments this may involve the user authorizing the creation of the DIR through the client-side application resident on principal machine 111. In other embodiments, the client-side application may request the DIR without further involvement of the principal 110. At step 840, the DIR is created for the first principal.

FIG. 9 illustrates a general computing device 900 (also referred to herein as a computer or computer system), which can be used to implement the embodiments described herein. The computing device 900 is only one example of a computing environment and is not intended to suggest any limitation as to the scope of use or functionality of the computer and network architectures. Neither should the computing device 900 be interpreted as having any dependency or requirement relating to any one or combination of components illustrated in the example computing device 900. In embodiments, computing device 900 may be used, for example, as a principal machine 111, DIR generation system 164, data capture system 162, IIS 166, identity data store 168, active directory 169, administrator system 160, identity provider 115, or relying party 120 as described above with respect to FIG. 1.

In its most basic configuration, computing device 900 typically includes at least one processing unit 902 and memory 904. Depending on the exact configuration and type of computing device, memory 904 may be volatile (such as RAM), non-volatile (such as ROM, flash memory, etc.) or some combination of the two. This most basic configuration is illustrated in FIG. 9 by dashed line 906. System memory 904 stores applications that are executing on computing device 900. In addition to applications, memory 904 may also store information being used in operations being performed by computing device 900, such as a DIR creation request 910 and/or a DIR availability notification 911, as described below with respect to FIGS. 1-8.

Additionally, computing device 900 may also have additional features/functionality. For example, computing device 900 may also include additional storage 908 (removable and/or non-removable) including, but not limited to, magnetic or optical disks or tape. Such additional storage is illustrated in FIG. 9

by storage 908. Computer storage media includes volatile and nonvolatile, removable and non-removable media implemented in any method or technology for storage of information such as computer readable instructions, data structures, program modules or other data. Memory 904 and storage 908 are examples of computer storage media. Computer storage media includes, but is not limited to, RAM, ROM, EEPROM, flash memory or other memory technology, CD-ROM, digital versatile disks (DVD) or other optical storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other medium which can be used to store the desired information and which can accessed by computing device 900. Any such computer storage media may be part of computing device 900.

As those with skill in the art will appreciate, storage 908 may store a variety of information. Among other types of information, storage 908 may store a digital identity representation 930 (e.g., in the case of a principal machine) or an identity token 945 (e.g., in the case of an identity provider).

Computing device 900 may also contain communications connection(s) 912 that allow the system to communicate with other devices. Communications connection(s) 912 is an example of communication media. Communication media typically embodies computer readable instructions, data structures, program modules or other data in a modulated data signal such as a carrier wave or other transport mechanism and includes any information delivery media. The term "modulated data signal" means a signal that has one or more of its characteristics set or changed in such a manner as to encode information in the signal. By way of example, and not limitation, communication media includes wired media such as a wired network or direct-wired connection, and wireless media such as acoustic, RF, infrared and other wireless media. The term computer readable media as used herein includes both storage media and communication media.

Computing device 900 may also have input device(s) 914 such as keyboard, mouse, pen, voice input device, touch input device, etc. Output device(s) 916 such as a display, speakers, printer, etc. may also be included. All these devices are well know in the art and need not be discussed at length here.

The various embodiments described above are provided by way of illustration only and should not be construed to limiting. Those skilled in the art will readily recognize various modifications and changes that may be made to the embodiments described above without departing from the true spirit and scope of the disclosure or the following claims.

We claim:

1. A method (400) for provisioning a digital identity representation (930) for a principal (110), comprising the steps of:

receiving (410) a request through a first channel to create the digital identity representation (930) for the principal (110);

issuing (420) a notification through a second channel that the digital identity representation (930) has been requested;

receiving (430) approval for the digital identity representation (930) to be created;

creating (440) the digital identity representation (930).

2. The method of claim 1, wherein the notification is an electronic message sent to a known address for the principal.

3. The method of claim 1, wherein the notification is an electronic message sent to a third party.

4. The method of claim 1, wherein the notification includes an electronic link to facilitate the approval.

5. The method of claim 1, wherein the first channel is an HTTP request and the second channel is an email.

6. The method of claim 1, further comprising the steps of:

receiving a second request through the first channel to create a second digital identity representation for the principal;

issuing a second notification through the second channel that the second digital identity representation has been requested;

receiving a denial of approval for the digital identity representation to be created;

sending an electronic message to a third party that the denial of approval has been received.

7. A method (500) for provisioning one or more digital identity representations (930) for a principal (110), comprising the steps of:

issuing (510) a notification that the one or more digital identity representations (930) are available for the principal (110);

receiving (520) a request to create the one or more digital identity representations (930);

creating (530) the one or more digital identity representations (930).

8. The method of claim 7, wherein the notification includes a link to an electronic site to enable creation of the request.

9. The method of claim 7, further comprising the step of:

capturing data regarding the principal;

wherein the step of issuing is automatically performed following the step of capturing.

10. The method of claim 7, wherein the notification is issued to a third party.

11. The method of claim 7, further comprising the step of:

creating a digital identity representation descriptor;

wherein the step of issuing a notification is automatically performed following the step of creating.

12. The method of claim 7, wherein the principal is a member of a group of principals, further comprising the step of:

setting a policy that the group of principals are permitted access to the digital identity representation;

wherein the step of issuing the notification comprises issuing the notification to the group of principals.

13. The method of claim 1, wherein the step of issuing the notification comprises sending a message to at least one application running on a principal machine that is associated with at least one of the principals in the group of principals.

14. The method of claim 13, wherein the request is created by the at least one application automatically, without prompting by the at least one principal.

15. The method of claim 7, further comprising the steps of:

cryptographically protecting the one or more digital identity representations;

sending the one or more cryptographically protected digital identity representations to a principal machine.

16. A method (600) for provisioning a digital identity representation (930) for a principal (110), comprising the steps of:

polling (610) a digital identity representation generation system (164) to determine whether any new digital identity representations (930) are available to the principal (110);

receiving (620) a notification that a first new digital identity representation (930) is available to the principal (110);

requesting (630) that the first new digital identity representation (930) be created;

receiving (640) the first new digital identity representation (930).

17. The method of claim 16, wherein the step of polling is performed automatically and periodically by a principal machine.

18. The method of claim 16, further comprising the step of:

after receiving the notification, alerting the principal that the digital identity representation is available.

19. The method of claim 18, wherein the step of issuing a notification comprises causing a pop-up notice to appear on a user interface of a principal machine.

20. The method of claim 18, wherein the step of alerting includes providing the principal an option to be reminded later to cause the requesting step to be performed.

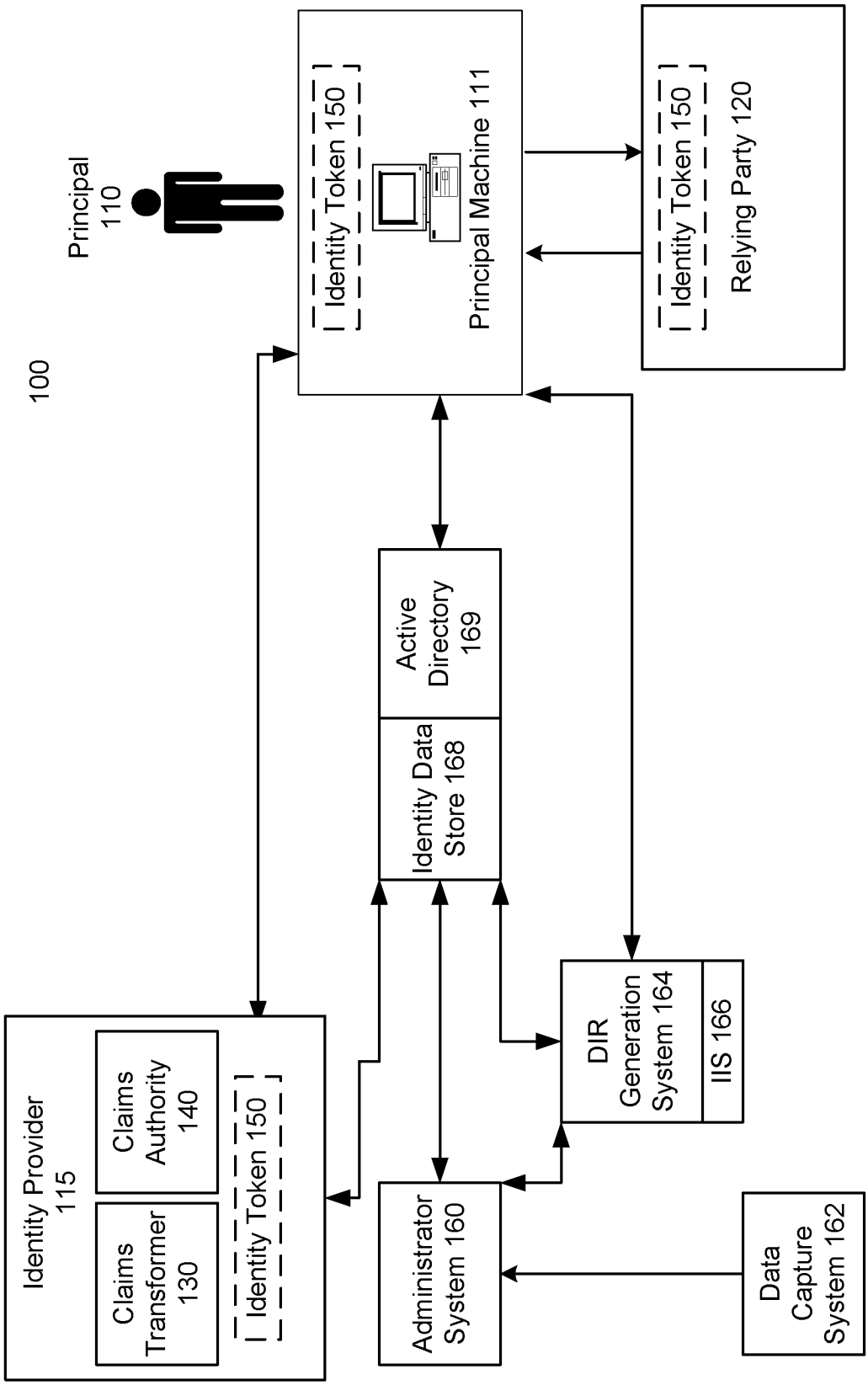
100
Principal
110
Identity Token 150
Principal Machine 111
Identity Token 150
Relying Party 120
Active Directory 169
Identity Data Store 168
Identity Provider 115
Claims Authority 140
Claims Transformer 130
Identity Token 150
DIR Generation System 164
IIS 166
Administrator System 160
Data Capture System 162

Fig. 1

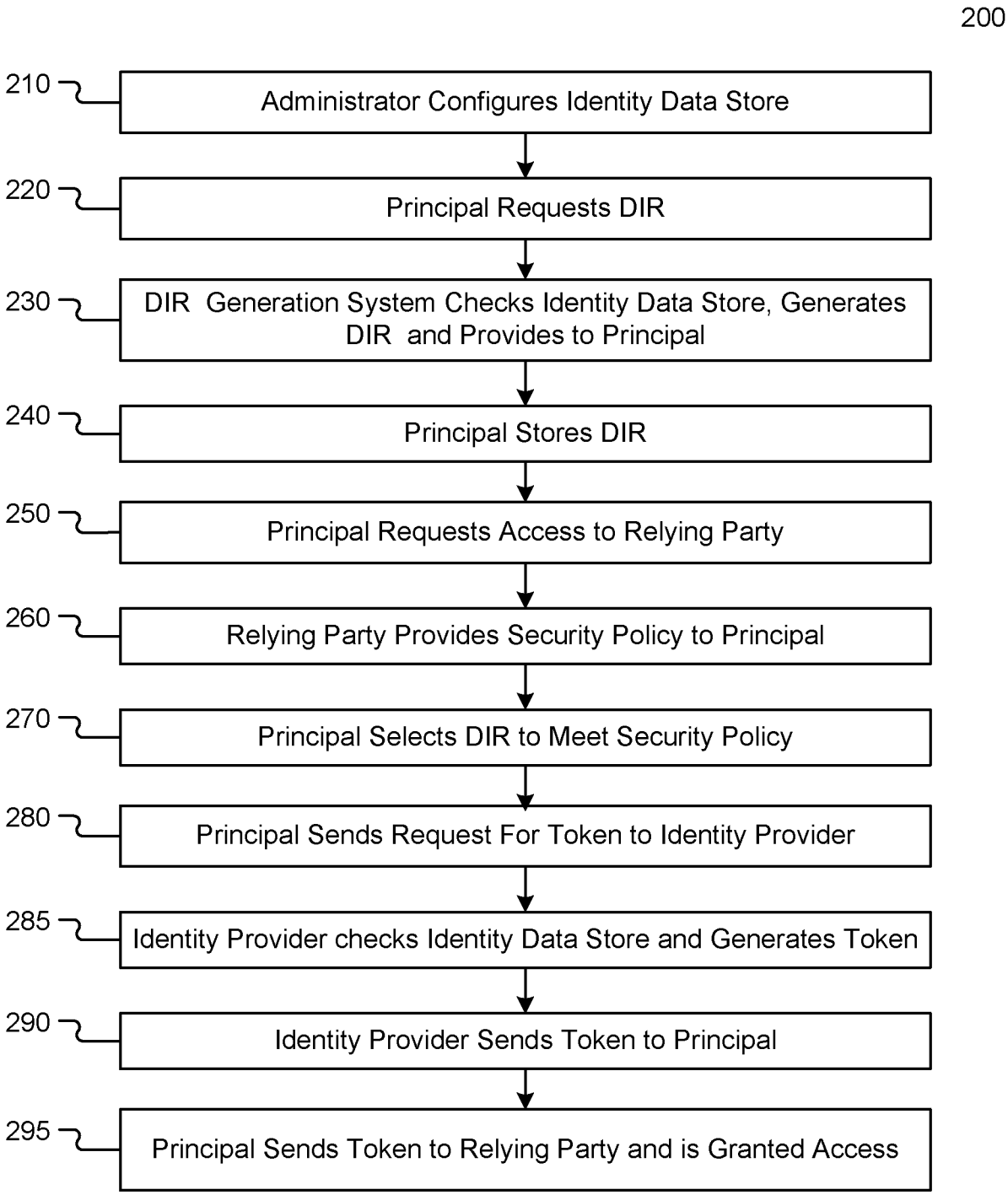
200
210
Administrator Configures Identity Data Store
220
Principal Requests DIR
230
DIR Generation System Checks Identity Data Store, Generates DIR and Provides to Principal
240
Principal Stores DIR
250
Principal Requests Access to Relying Party
260
Relying Party Provides Security Policy to Principal
270
Principal Selects DIR to Meet Security Policy
280
Principal Sends Request For Token to Identity Provider
285
Identity Provider checks Identity Data Store and Generates Token
290
Identity Provider Sends Token to Principal
295
Principal Sends Token to Relying Party and is Granted Access

Fig. 2

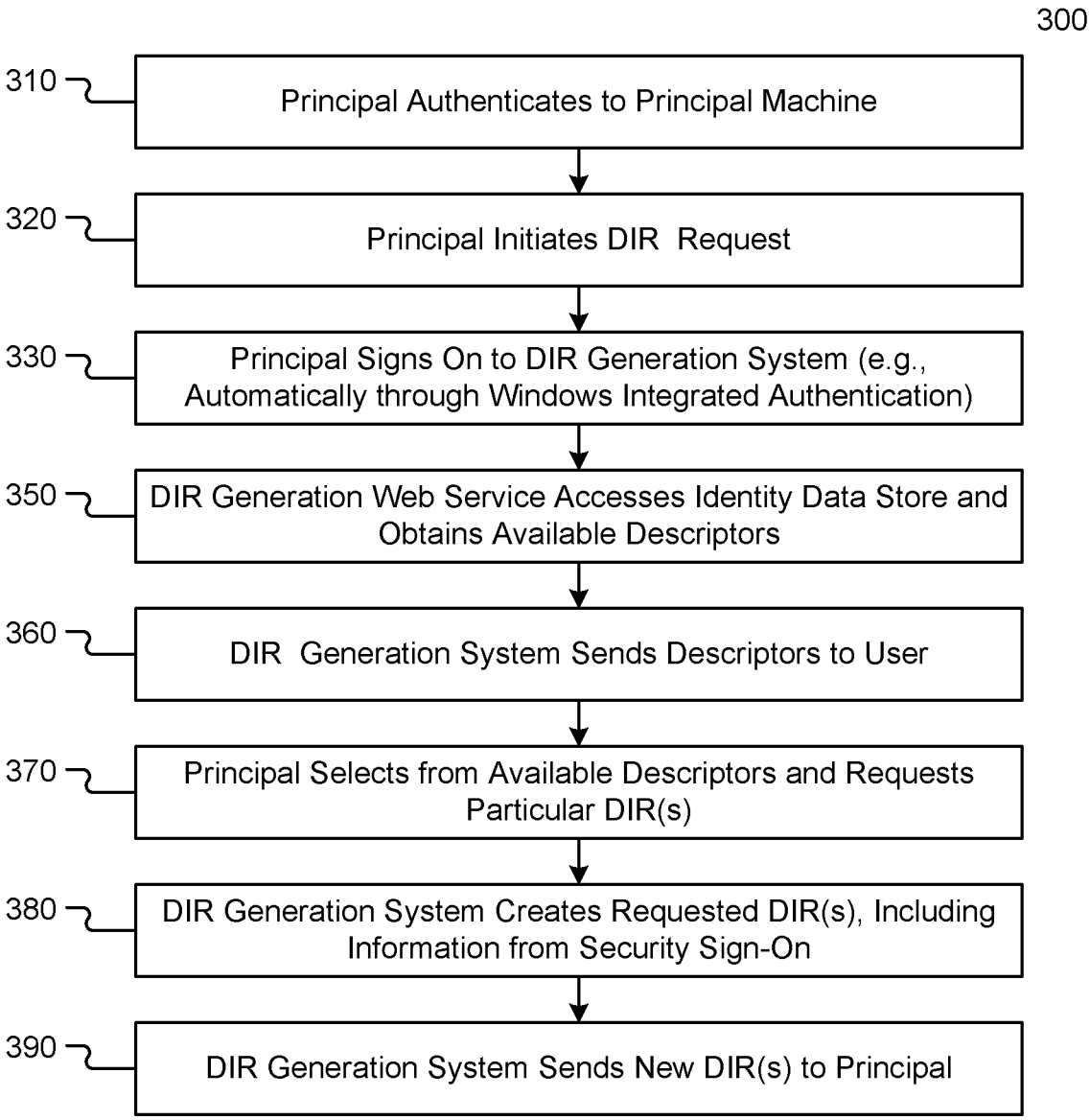
300
310
Principal Authenticates to Principal Machine
320
Principal Initiates DIR Request
330
Principal Signs On to DIR Generation System (e.g., Automatically through Windows Integrated Authentication)
350
DIR Generation Web Service Accesses Identity Data Store and Obtains Available Descriptors
360
DIR Generation System Sends Descriptors to User
370
Principal Selects from Available Descriptors and Requests Particular DIR(s)
380
DIR Generation System Creates Requested DIR(s), Including Information from Security Sign-On
390
DIR Generation System Sends New DIR(s) to Principal

Fig. 3

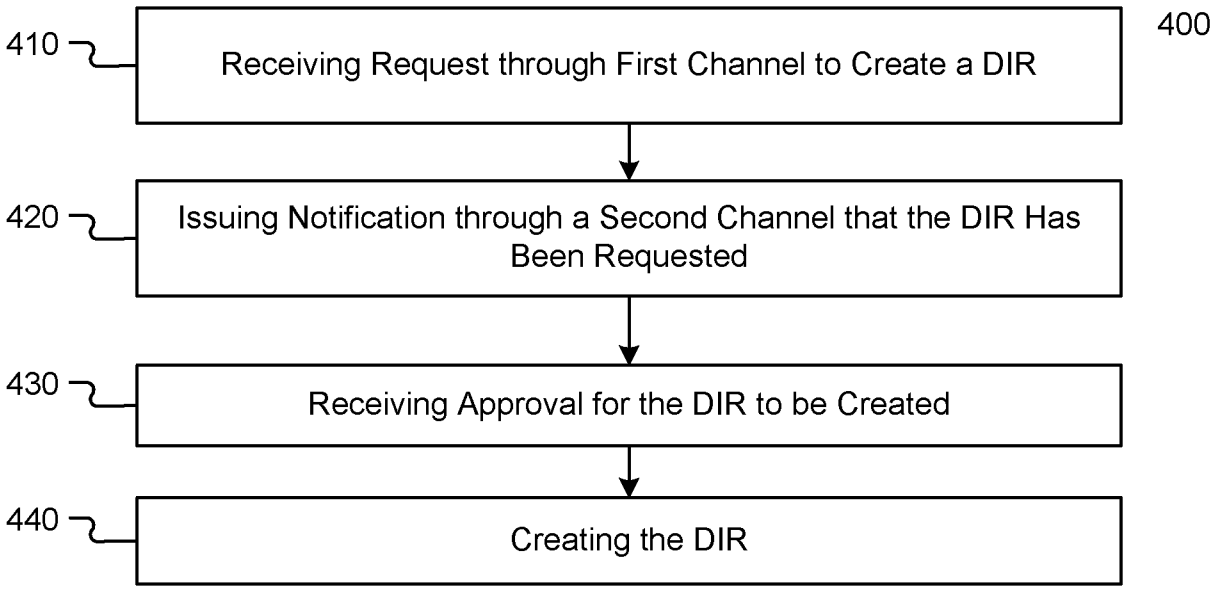
400
410
Receiving Request through First Channel to Create a DIR
420
Issuing Notification through a Second Channel that the DIR Has Been Requested
430
Receiving Approval for the DIR to be Created
440
Creating the DIR

Fig. 4

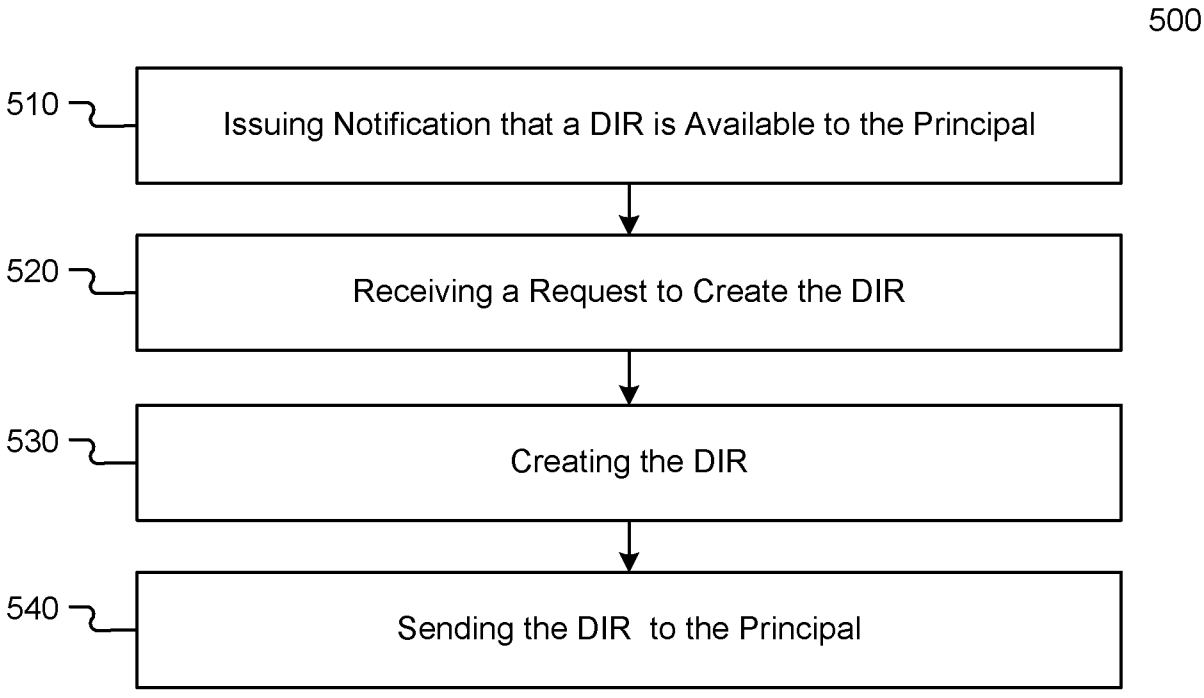
500
510
Issuing Notification that a DIR is Available to the Principal
520
Receiving a Request to Create the DIR
530
Creating the DIR
540
Sending the DIR to the Principal

Fig. 5

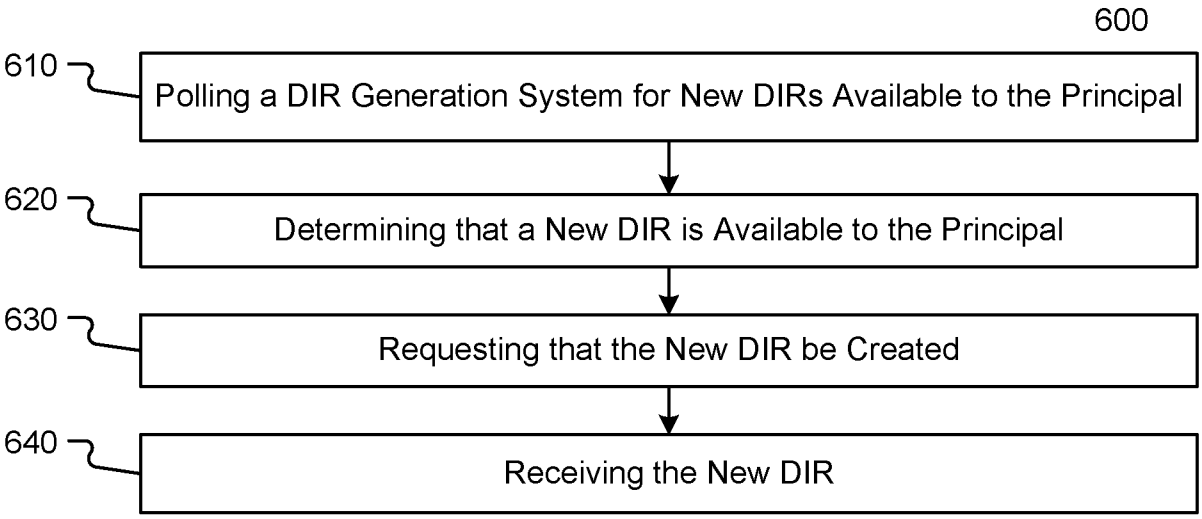
600
610
Polling a DIR Generation System for New DIRs Available to the Principal
620
Determining that a New DIR is Available to the Principal
630
Requesting that the New DIR be Created
640
Receiving the New DIR

Fig. 6

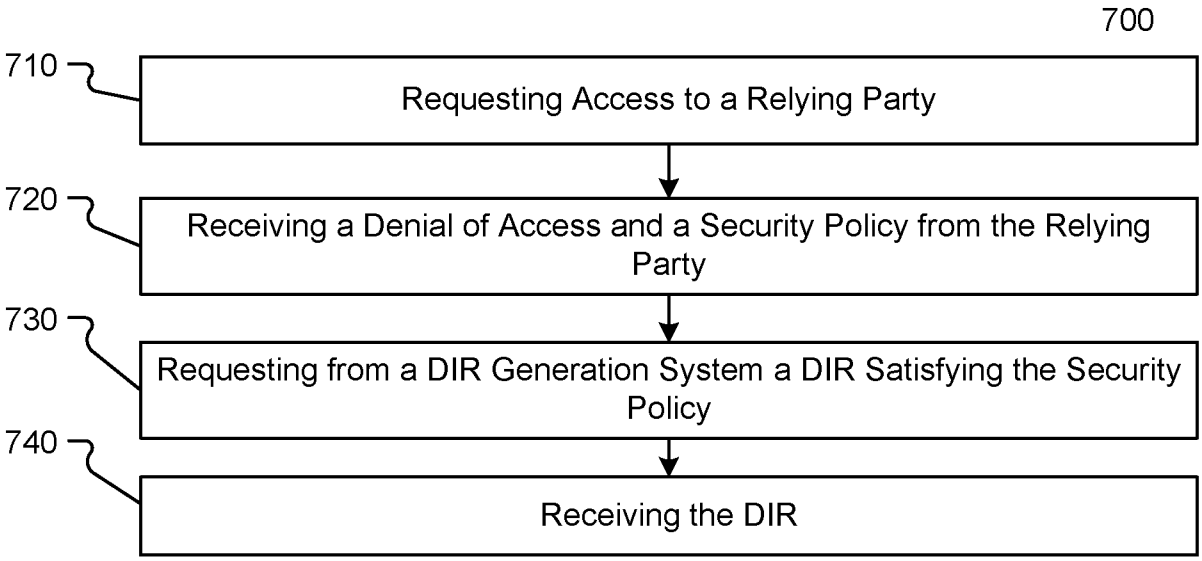
700
710
Requesting Access to a Relying Party
720
Receiving a Denial of Access and a Security Policy from the Relying Party
730
Requesting from a DIR Generation System a DIR Satisfying the Security Policy
740
Receiving the DIR

Fig. 7

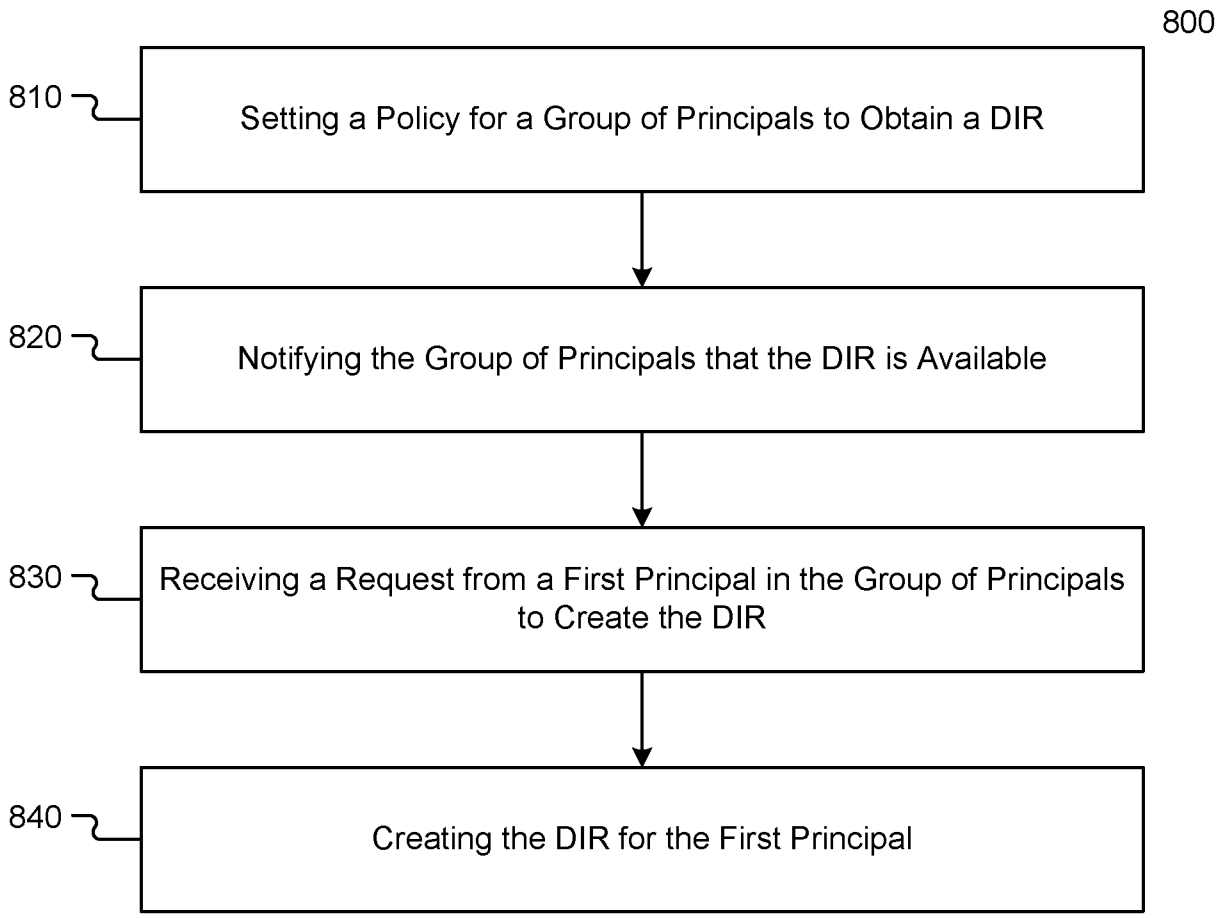
800
810
Setting a Policy for a Group of Principals to Obtain a DIR
820
Notifying the Group of Principals that the DIR is Available
830
Receiving a Request from a First Principal in the Group of Principals to Create the DIR
840
Creating the DIR for the First Principal

Fig. 8

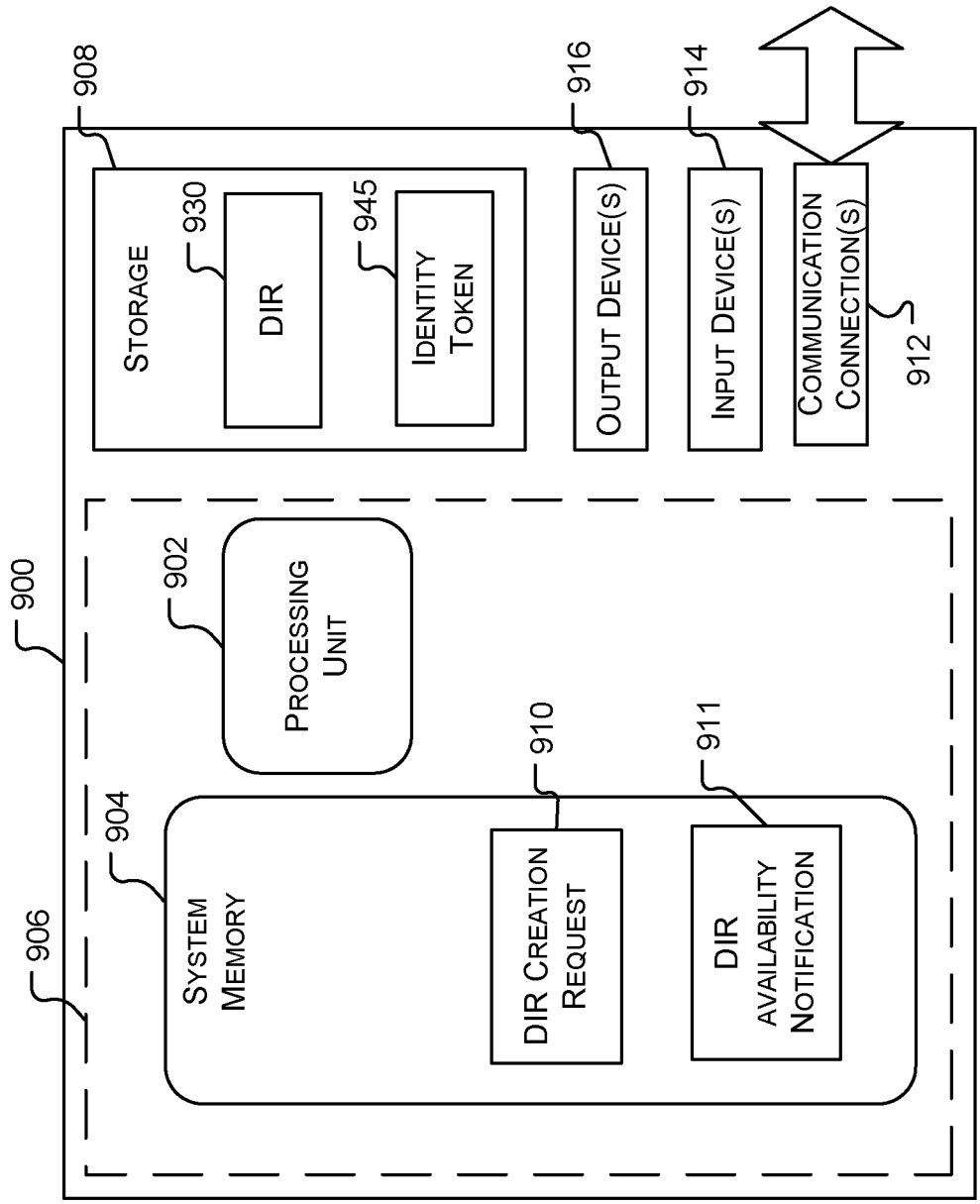
900
902
PROCESSING UNIT
904
SYSTEM MEMORY
906
908
STORAGE
930
DIR
945
IDENTITY TOKEN
910
DIR CREATION REQUEST
911
DIR AVAILABILITY NOTIFICATION
916
OUTPUT DEVICE(S)
914
INPUT DEVICE(S)
COMMUNICATION CONNECTION(S)
912

FIG. 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2008/050205

A. CLASSIFICATION OF SUBJECT MATTER

G06F 15/00(2006.01)i, G06F 21/00(2006.01)i, H04L 9/32(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 8 : G06F 11/30, 13/00, 15/16

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean Utility Model and applications for Utility Model since 1975
Japanese Utility Model and applications for Utility Model since 1975

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKIPASS(KIPO internal), IEEE xpl, Google, "principal", "registration", "business"

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2004/036348 A2 (E2OPEN LLC) 29 April 2004 See abstract, pp. 3-24, claims	1-3, 7, 10
A	US 2004/0205243 A1 (HURVIG HANS, et al.) 14 October 2004 See abstract, claims	1-20
A	US 6981043 B2 (BOTZ PATRICK S., et al.) 27 December 2005 See abstract, claims	1-20
A	US 6754829 B1 (BUTT ALAN B., et al.) 22 June 2004 See abstract, claims	1-20

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 MAY 2008 (14.05.2008)	**14 MAY 2008 (14.05.2008)**

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
Government Complex-Daejeon, 139 Seonsa-ro, Seo-gu, Daejeon 302-701, Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

LEE, Jong Ick

Telephone No. 82-42-481-8373

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2008/050205

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2004/036348 A2	29.04.2004	AU 2003272809 A1 US 20040078316 A1	04.05.2004 22.04.2004
US 2004/0205243 A1	14.10.2004	WO 2002073926 A1	19.09.2002
US 6981043 B2	27.12.2005	US 20020143909 A1	03.10.2002
US 6754829 B1	22.06.2004	NONE	