Identity Enabled Networks
The Core Service Building Block for
Service Oriented Architectures

Dr. Ramaswamy Rangarajan "Dr. Ranga"
Principal Network Design Engineer
Sprint

Rakesh Radhakrishnan
Sr. Principal IT Architect
(Client Services -Telecommunications)

September, 2004

Table of Contents

I   Introduction and Overview

This paper explores the possibilities of leveraging Standards based Identity System for a Telecommunication environment and provides a vision for the future trends in converged communication services. This paper is also based on the investigative/evaluative work done by the authors recently, using Sun's Identity System as a Security Framework/Environment for Telecom Services –Data, Voice and Video (including Call Processing). Initially we saw the proliferation of Telecom Services to Cell Phones and Mobile Devices over 3G and 2.5 G Networks – where in a Cell Phone/Mobile Device evolved into a more complex device that handles TV, email, SMS, IM, Games, Pictures, Videos, Video mail and more. This in conjunction with the deployment of 802.11 (wifi), 802.16 (wimax) access networks and the evolution into 4G networks where seamless traversal between all types of wireless networks is made possible- makes Identity enabled Service Delivery even more appealing. All locations such as, Airport Lounges, Hotels and Conference facilities, retail locations such as Starbucks, Regional Malls, McDonalds, have rolled out these networks (see white paper on Wifi and Network Identity). Along the same lines, both Wire-line and Wire-less Communication Service Providers (CSPs) are seeking new ways to expand into delivering data services securely with offerings in broadband access networks ranging from DSL to Cable Modem, as well.

Telecom Services utilize voice, data and video (multi-media) to deliver more complex and advanced services such as Context sensitive delivery of Entertainment. The goal is to transcend all types of access networks and access devices and deliver User Sensitive (preference, profile and policy based), Location based, Context driven Services with true Service Mobility. Going beyond user and terminal mobility. Different dialects of XML are used here, including, SAML/SPML, MOML/MSML, CpML, XKMS, VXML and more. Lately many software vendors have addressed the need for an Integrated Security framework that addresses Security requirements with extension of their solutions to Network Identity Systems (such as Java Enterprise Identity System).

This paper also explores possibilities around Telecom Industry initiatives (3GPP's GUP, IETF's ENUM, TMF's ETOM, etc.), and how they are applied to IDEN[1] – such as GUP (generic user profile) – folding into WS-PP, Web Services Personal Profile (as part of the liberty alliance and liberty specifications), and more. This paper also takes an in-depth look at the approaches to integrating these technologies (GUP and ETOM with IDEN) and the value proposition of doing so. First an introduction to Network Identity Solutions is covered, followed by the four perspectives from which an IDEN needs to be looked at. It also examines ENUM as this new standard evolves.

Identity System - Data/Meta-Data

This includes the management of the information and identities of users, including the communications identity of a user, users profiles as an employee/person/partner, etc., the workflow and provisioning of users data, meta-data pertaining to services, and more.

Identity System - Services

Services from an Identity System perspective can be categorized as
Core Identity Services
Identity enabled Services (Services protected via Agents and extensions)
And Identity based Services (Identity enabled services that also share data/metadata)

Identity System - Networking

An identity system extends to all types of access networks (including wimax (802.16, 802.20), wifi (802.11), DSL, Cable, 3/3.5G and more) from the Services Network and the Core Network, all the way to different types of devices (both client devices and network devices). This makes service mobility possible at both the access networks and access devices making the delivery of service client device agnostic and access network agnostic – with session state maintained all through.

Identity System – User Centricity

Here Identity System plays a major role in capturing users profile, preferences and personalization elements – to deliver Services in a context sensitive manner (who, what, when, where, etc.). User centricity implies that a user is given an option to define how, when, where, etc., for his/her services that are consumed. The services are also user centric in nature, i.e., they also understand the user's context.
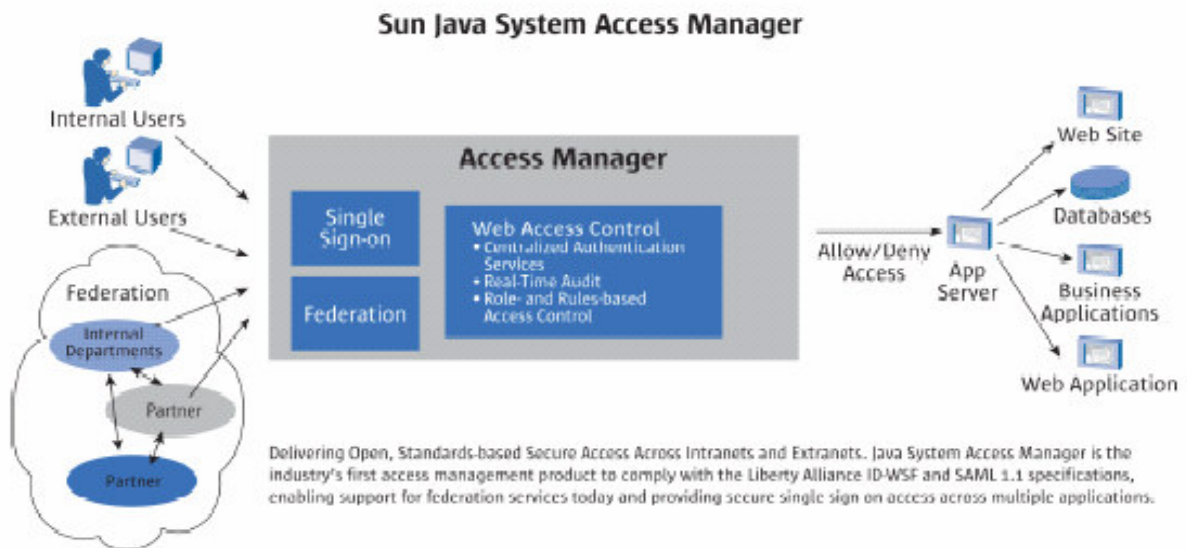
---

[1] Identity Enabled Networks

II   IDEN and Access Management

An Identity System software is a standards-based solutions designed to help organizations (Enterprises and Telecommunications Companies) manage secure access to Web and non Web-based applications both on the intranet and extranet acting as a Architectural Building Block (ABB). Within enterprises such as Coke, Home Depot and American Airlines this ABB is typically leveraged for Business Services (B2B, B2C or B2E[2]) and within Telecommunications environments it's a strategic ABB that is leveraged for all types of Voice, Data and Video services. From an enterprise perspective, an Identity System provides more financial, organizational, and competitive agility to compete in the marketplace, through scalable access management services that help secure the delivery of business information services, improve the user experience through Web single sign-on, and put a federated identity framework in place that helps create new revenue opportunities through enhanced affinity relationships with business partners and customers. It is important to note that an Identity System acts as the Foundation for True Boundary-less Information Flow. From a telecommunication perspective, an Identity system provides more agility through mobility with security that leads to true "service mobility" –meaning any data, voice, video service can be accessed in a device agnostic and network agnostic manner, yet user specific/location specific and preference/profile driven delivery of such services, based on user defined policies, is made possible any where in the globe.

Some of the key capabilities of Network Identity Solutions such as JES Identity Server are;

- **Federation services:** *Enables shared authentication with affiliate organization web sites, web applications and web users.*
- **Access Management services:** *Securely controls access to Web and non Web-based resources (such as Services delivered via a Service Delivery Platform, devices, roaming partners network equipments, etc.).*
- **Session Management Services:** *Ability to offer cohesive/integrated session management, i.e., full life cycle management of a users session.*
- **Policies:** *User defined policies for service delivery.*
- **Identity Administration services:** *Provides centralized administration of identities, policies, and services. Authentication controls including LDAP, RADIUS, X.509v3 certificates, Safe Word token cards, anonymous, and UNIX platform authentication services, Microsoft Windows NT and Windows 2000, resource-based authentication, Online Certificate Status Protocol (OCSP) validation for X.509 v3 digital certificate.*
- **Out-of-the-box modules:** *to help simplify integration into an existing security framework: Java Authentication and Authorization Service (JAAS) technology-based authentication framework. An open standard, flexible, and extensible authentication architecture that enables Organizations to customize authentication mechanisms, for J2EE/JAIN based services.*

Sun Java System Access Manager

Delivering Open, Standards-based Secure Access Across Intranets and Extranets. Java System Access Manager is the industry's first access management product to comply with the Liberty Alliance ID-WSF and SAML 1.1 specifications, enabling support for federation services today and providing secure single sign on access across multiple applications.

---

[2] Business to Business Services, Business to Consumer Services and Business to Employee Services

Figure 1: IDP Access Manager

The above AM Architecture depicted in Figure 1 shows the Central role-played by an Identity System as an Access Manager. ***"Managing the Access for Users, from Devices/Networks to different Services".*** Core Services provided by an Identity Infrastructure, such as Authentication, Authorization, SSO[3], Federation, Policy and Access Control act as a Service Building Block for all Business/Communication Services. This AM role ensures that mobility with security is addressed, by providing a Central mechanism to validate and verify Identity of Users, Services, Networks and Devices –end to end. From this perspective an IDEN acts as a distributed firewall, that enforces policies around users, devices, services and networks, where a typical policy contains (RULE, SUBJECT and CONDITION -see figure 2 below):

- Action that can be taken against a Service/Resource
- Who, where, where - who can access, time limitations, etc.
- Conditions - Level of authentication required, schema needed, IP address, etc.
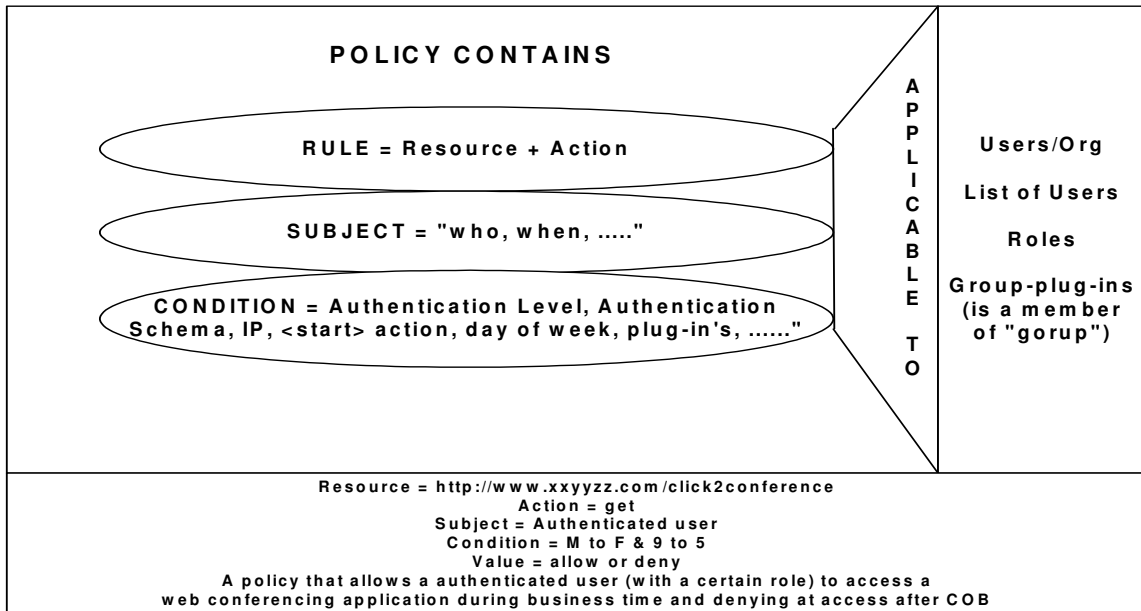

POLICY CONTAINS

RULE = Resource + Action

SUBJECT = "who, when, ..."

CONDITION = Authentication Level, Authentication Schema, IP, <start> action, day of week, plug-in's, ..."

APPLICABLE TO

Users/Org

List of Users

Roles

Group-plug-ins (is a member of "gorup")

Resource = http://www.xxyyzz.com/click2conference
Action = get
Subject = Authenticated user
Condition = M to F & 9 to 5
Value = allow or deny
A policy that allows a authenticated user (with a certain role) to access a web conferencing application during business time and denying at access after COB

Figure 2: IDP Policy Structure

---

[3] Single Sign On

III Identity System – Data Model and Meta-Data

To better understand these 4 perspectives, the following diagrams and illustrations can be used.

An Identity Systems primary role is to ensure that a user's identity/data that is typically distributed everywhere in a SILO nature is synchronized and centrally managed. This includes an identity of a user within an Enterprise's Business Systems (such as ERP, HRMS, CRM, etc.) and between Enterprises (such as a user's Identity at Amazon, Yahoo and Netflix).

A sample Logical Identity Architecture and its functionally decomposed into an ID Grid with ID Management Services, ID Transaction Services, ID Data Stores & Interfaces to Client/Portal/Applications is depicted in figure 4, below. Majority of these functionality addresses data elements in an Identity Grid.

- *Provisioning Users and there Profile data*
- *Password data Management*
- *Directory data Management*
- *User data Management*
- *Data Transformation*
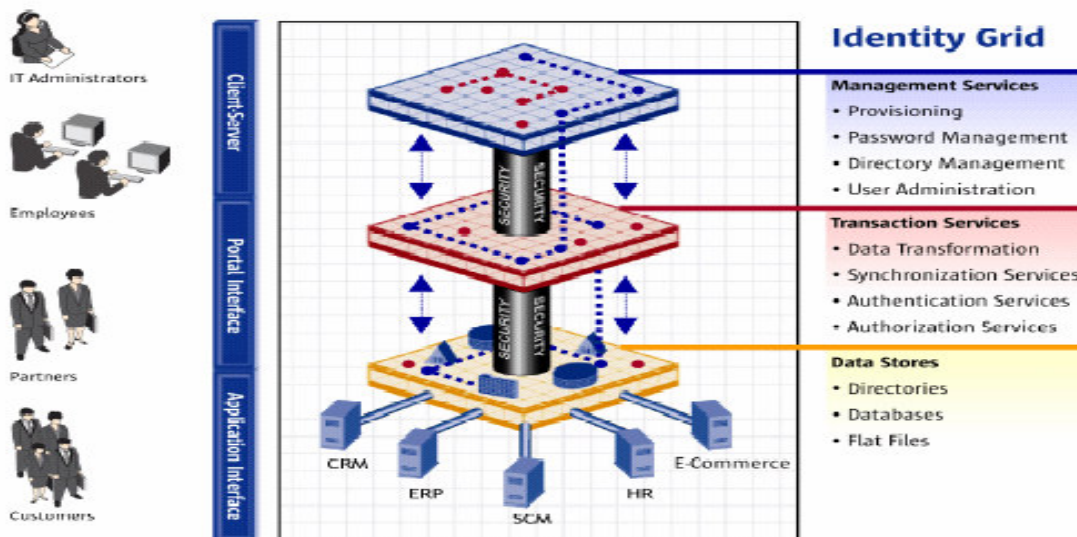- *Data Synchronization Services*
- *Data Storage Services*

Figure 3: Functional decomposition of an ID Grid (ID Management. Services, ID Transaction Services, ID Data Stores & Client/Portal/Application Interfaces to Identity)

Also from a data perspective a user has a bunch of profile data associated with the services he or she consumes. For e.g., a user's smart card's profile/pin, credit card profile, travel profile, airline profile, hotel profile, etc. These profiles that are typically fed into a system are shared through an ID server. Services such as Location, Presence and Payment are ID enabled Services; Mapping of profiles could take place with custom coding and policy enforcements as well.

Generic Industry Profiles (standards based user data models) that are powerful in terms of users Network Identity includes;
   a) *Liberty's WS-PP (personal profile for web services)*
   b) *Liberty's WS-EP (employee profile for web services)*
   c) *GUP – 3GPP's Generic User Profile (initiative is folded under Liberty WS-PP)*
   d) *Common Device Profiles*
   e) *Common Service Profiles*

ENUM could potentially be a an extension of the Personal Profile Services within Identity Services and all Services that require ENUM profile can lookup and re-use (through an ID System).
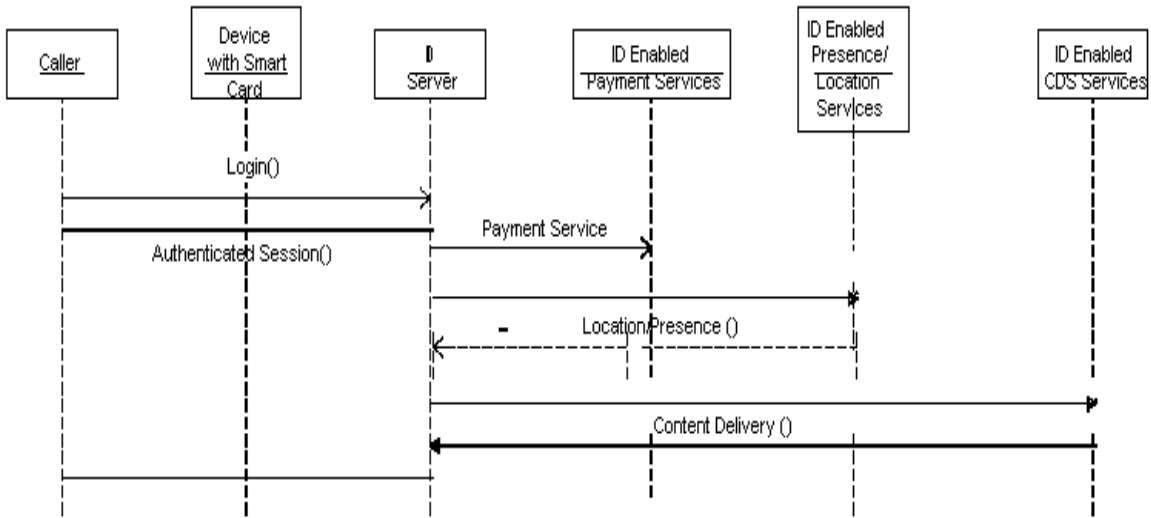
Figure 4: In each step a profile is shared – Caller Profile, Device/telephone Profile, Payment Service Profile, etc.

" These data models around a user, device and services and a user's profile/preferences are shared through a common profile management service". This acts as the foundation for not only seamless single-sign on across services and domains (see diagram below), but also ensures all related information/data models associated with a user is shared securely and seamlessly between services that are invoked (primarily through XML). In this case a caller/user using a Smart Card enabled device (such as a PDA/Cell phone) Logs into Identity Server (that seeks the Device profile) and establishes an authenticated Session. Based on the users profile, ID Server has a list of associated services that the user has access to. Majority of these services are ID enabled, i.e., they do not require re-authentication and the service sessions are invoked via ID Server.
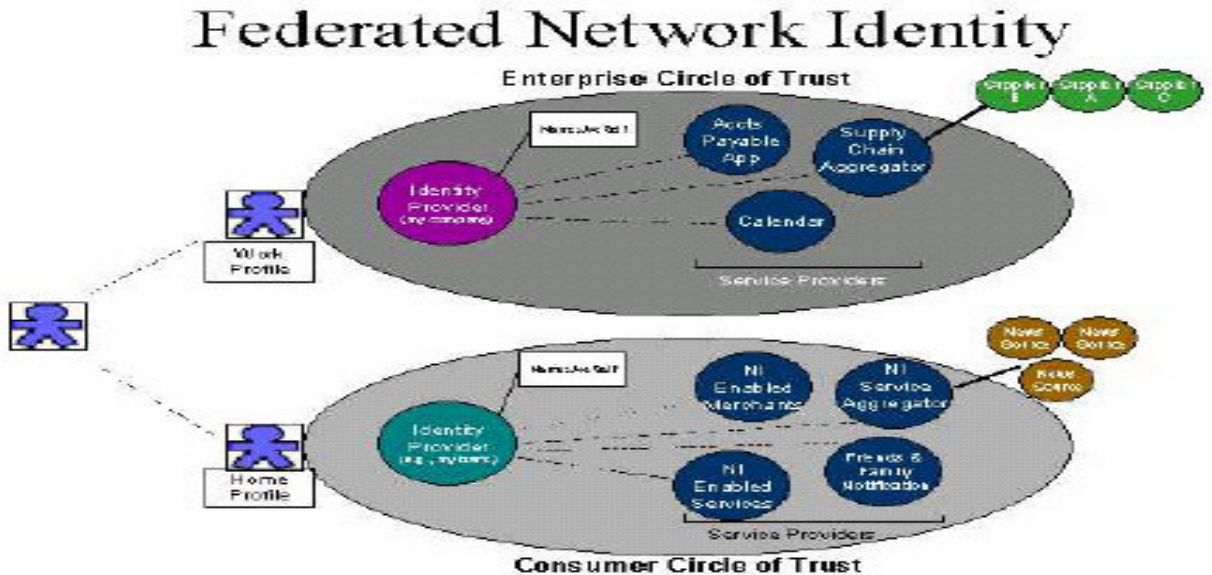

Figure 5: Profile Sharing between Services and Domains
More than half a decade of industry efforts has gone into the Liberty Alliance program, that has created standard protocols (liberty, saml, etc.), for sharing identities. These have been implemented by more than 12 ISV[4]s. The Liberty Alliance membership also ranges in the 200+ corporations (a large number of them are Fortune 500 firms).

---

[4] Independent Software Vendors

IV   Identity System - Services

Common Identity Services, (Core Identity services such as Authentication/Authorization/Auditing, Session Management and SSO Services), can be leveraged by both Communication Services and by Business Services as well as Web Services. *" This makes an Identity System a Core Service Building Block (similar to the potential offered by ENUM Services) for Converged Services".*
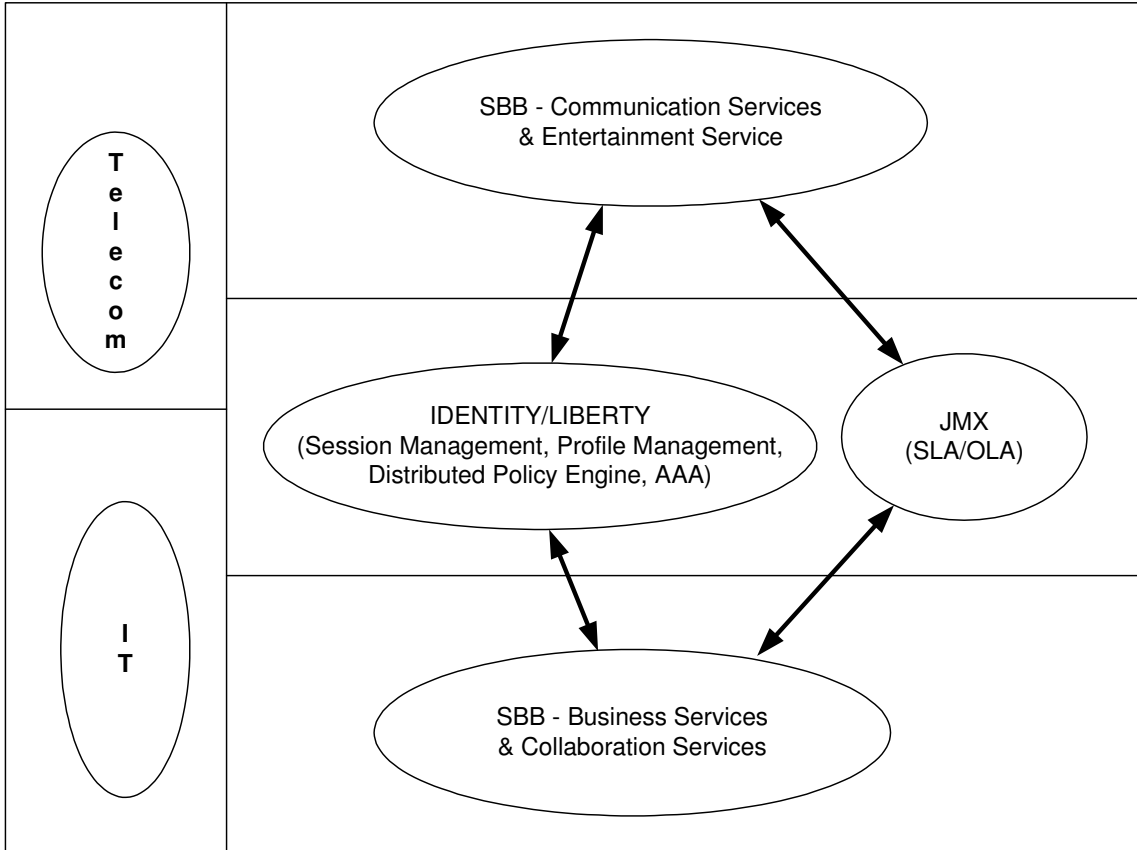

Figure 6: IDP acting as a Core SBB for both Telecom and IT Services

Here we see how *" Identity System acts as the central solution that ties devices and services together based on a users profile and preferences".* Services that are highly related to a users identity such as, location, presence, payment, digital rights management, etc., are treated as Service Building Blocks that get reused when building other Customer centric services.
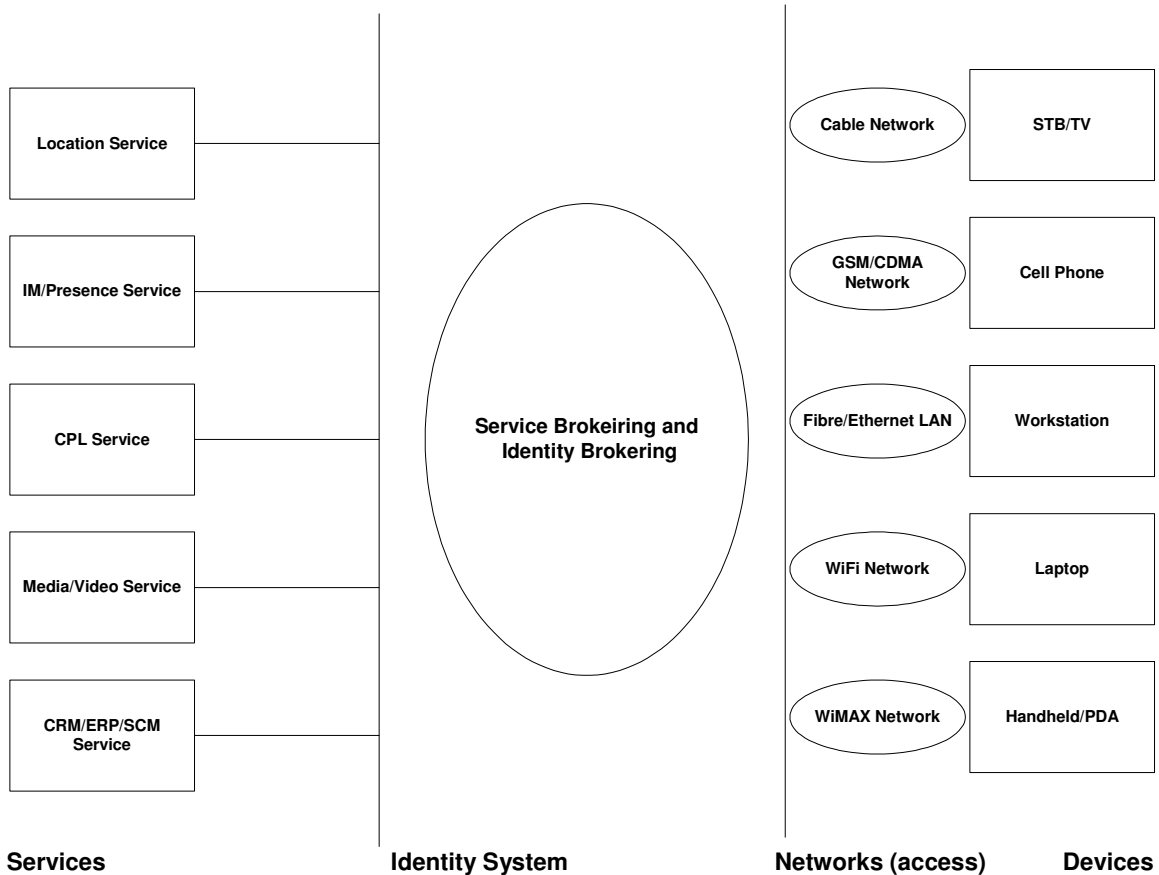
Figure 7: Core ID Services –playing a central role between services, access networks, devices and users.

The list of devices can include:
- *TV with a STB[5] (with a smart card)*
- *Cell Phone (with a SIM card)*
- *Laptop/Desktops*
- *Handheld/PDA's*

The list of Networks (access) can range from:
- *Cable Networks*
- *GSM/CDMA Networks*
- *Wifi Networks*
- *WiMAX/EVDO Networks*

The list of Identity enabled Services can be categorized into:

- *Enterprise Business Services (ERP, SCM and CRM)*
- *Communication Services (Voice, Data and Video)*
- *Contextual Services (such as Location and Presence)*
- *Entertainment Services (such as VOD, Digital Radio, etc.)*

Majority of the Enterprise Business Services and Entertainment Services are Identity enabled (i.e., service access is secured through ID agents), however over and above the Core Identity Services, Contextual and Communication Services are not only Identity enabled, but are also Identity based. As stated earlier Services from an Identity System perspective can be categorized as:

---

[5] Set Top Box

- *Core Identity Services (AAA, Session Management, Federation, etc).*
- *Identity enabled Services (Services protected via Agents and extensions)*
- *Identity based Services (Identity enabled services that also share data/metadata)*

It should be noted here as to how an IDEN and the core services of an Identity system compliment the notion of Service Oriented Architecture. Both by Identity enabling services i.e., protecting services as a resource via agents and extensions, and Identity based services that are provision-able, i.e., services that are not only identity enabled but also share data/meta-data between services via an Identity System.

A good example of an Identity based service that is also Contextual Service – that share user and service profiles and preferences extensively is one where a user – specifies that he or she want a message sent to there Cell phone – with a weather report/doppler image for the city they are in every morning at 8:00AM (regardless of the time zone). This will involve a user specific policy that works in conjunction with services such as messaging services, location services, and weather services and some sort of timing services. So if I'm in Sanfrancisco, California Monday morning I get a weather report at 8:00am PST for Sanfrancisco, CA and its vicinity. If I traveled to Chicago Tuesday night I get a similar report at 8:00am CST for Chicago and so on. This involves sharing a subset of my location profile to the weather service, and a subset of the weather profile shared with a Content Delivery service, etc. All these services are typically identity enabled (that is the user gets Single Sign On across all these service) first before they tend to become Identity based (i.e.,) profile sharing. Also Identity based Services are typically provision-able to users via the Identity System using Markup Languages such as SPML (service provisioning markup language).
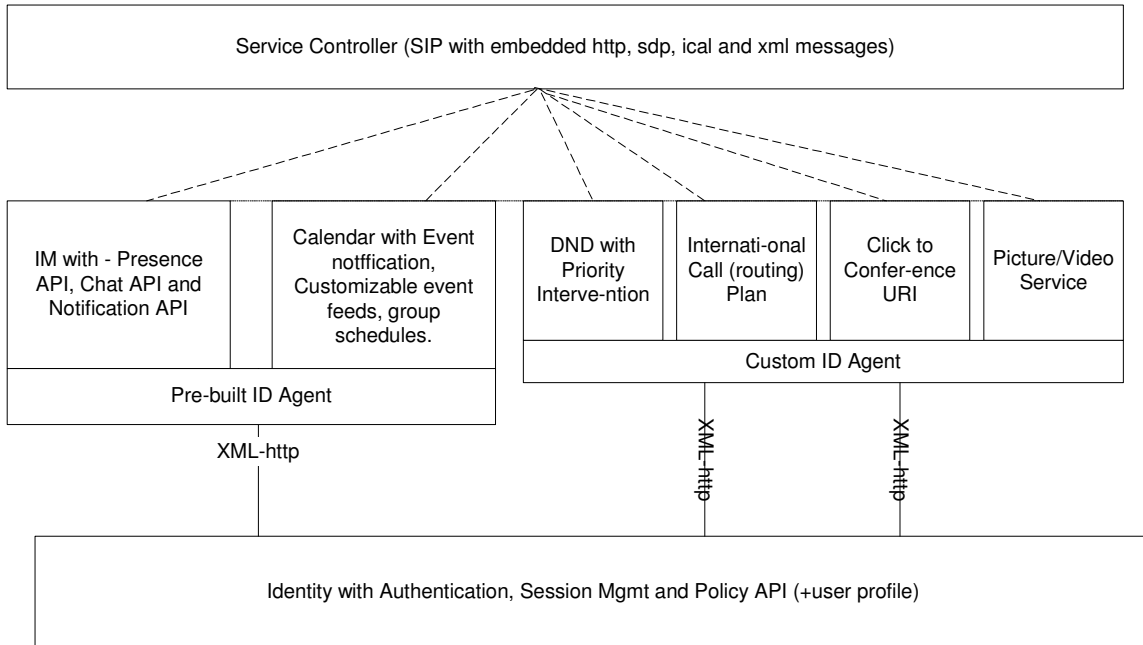

Figure 8: ID based Communication Services

V   Identity System - Networking

An identity system extends to all types of access networks (including DSL, Cable, 3/3.5G, wimax (802.16, 802.20), wifi (802.11), and more) from the Services Network and the Core Network, all the way to different types of devices (both client devices and network devices). This makes service mobility possible at both the access networks and access devices making the delivery of service client device agnostic and access network agnostic – with session state maintained all the way through. From figure 10, we see that Content and Services are Identity enabled (i.e., they use an Identity System as an Architectural Building Block for AAA, Session Mgmt, etc.), in the Service Network is where IDP and SP run their services (IDP-Identity Service Provider and SP – Service Provider's that offer identity enabled and identity based services), in the Core Network, networking devices and voice stack/services are identity enabled and identity based, Access Networks run Access Controllers (such as a Wifi Access Controller or a Cable/DSL controller) that extend to an IDP for establishing authenticated sessions when the user accesses the network, and Access Devices can have specialized client side authentication mechanisms that are mandated prior to authenticating with a IDP (such as SIM card or client side certificates).
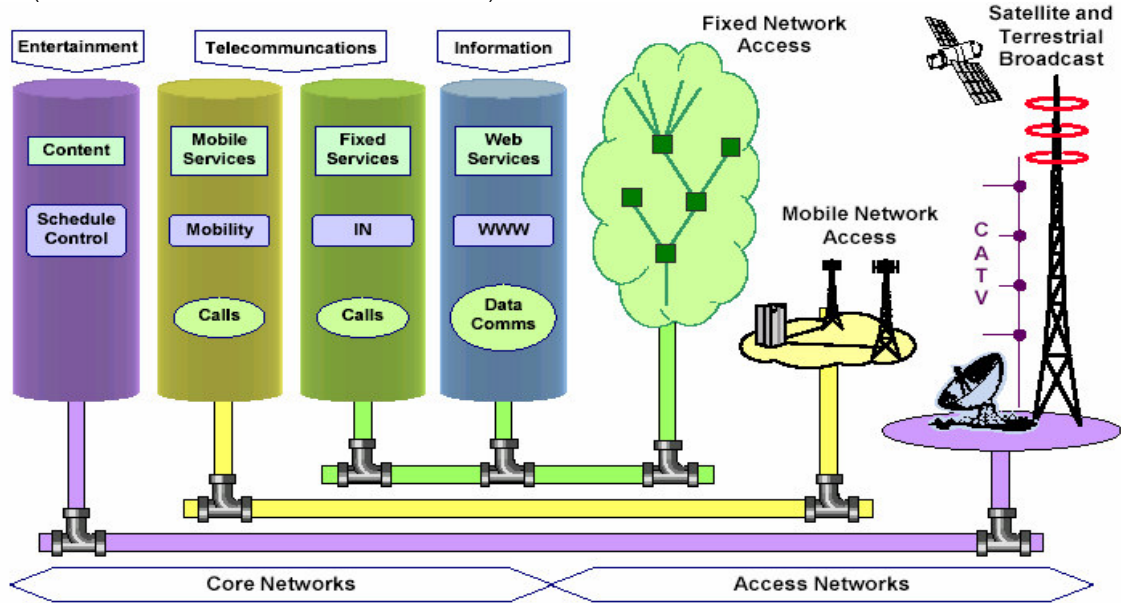

Figure 9: Silo Nature of today's Networks

This problem space depicted above ("silo nature of networks/devices/services) is beginning to be addressed with a standards based Core Service Building Block (ID System) that transcends all networks to offer user centric Services -"ME", as depicted below.
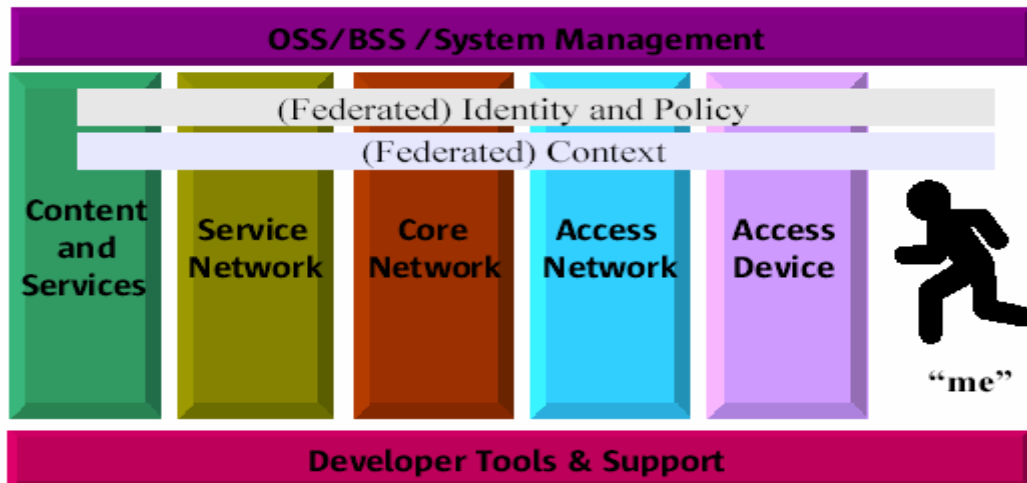

Figure 10: Identity in all Networks, Services and Devices

11

In the telecommunications world this is even more significant, since consumers are seeing a convergence in Devices, i.e., a Laptop is TV/DVD player, a TV can accepts Calls via a STB (set top box) and a Cell phone has enough resources to call it a computer, with mobile TV services. Essentially consumers expect all services to be accessible from all these devices, especially since these devices are evolving into pure IP devices and content (voice/data and video content) is digitized. Enterprises like Blockbuster and Netflix are looking into offering VOD, Cable Operators are offering not just TV, but high-speed Internet Access and SIP/VOIP applications. In all these advances the user is lost, i.e., his or her experiences is not shared between access networks and access devices. However, with an IDEN, what is delivered is a set of comprehensive, cohesive services that are user centric. A good example of Access Network and Device Agnostic delivery will be, one where a user accesses a VOD movie while flying from the east to the west coast – via a Wifi LAN after authenticating with an IDP via an Embedded device in a Plane, he or she, pauses the movie half way and works on something else. After reaching home in California he or she switches the TV On and LOGS IN – the TV prompts him if he wants to continue and finish watching the VOD movie that he/she paused in a plane. This implies that both the access networks wifi in a plane and the cable network from home are identity-enabled networks (IDEN) and the user's service session is tracked. This type of an Architectural Solution can be achieved only by augmenting traditional AAA services with Liberty based ID Services as described below.

Today, RADIUS protocol is a widely used protocol for performing network authentication, authorization, and accounting (AAA) functions. It is used to control remote and local user access - via dial-in, VPN, firewall, LAN, or any combination. It was a key component of any network security architecture in the past. RADIUS Architectures have depended on users connecting to a specific port on a device from a specific location on the network and is not user aware. Subnets, ACL[6] and COS[7], for example, are defined on ports of routers and switches and IT staff very often manage a users connection via the physical MAC address on the desktop device.

However, in a wireless environment (802.11, 802.16 and 3G/4G networks) devices and location can no longer be the control point since the user can be anywhere in the network (or any access network) and can attach to the network using any device. If we take into account the fact that NETWORKS exists to provide services to USERS, a user's identity is the best foundation. *" Identity enabled Networks (IDEN) revolutionizes the model for Network Service Delivery making it Access Network Agnostic, Device Agnostic – yet USER centric (profile/preference driven delivery of Services".*

While considering an Identity System some of the key value propositions of a RADIUS implementation have to be leveraged, such as,

Role-based Firewall/VPN Security
RADIUS plays a key role in enabling role-based network access security for firewall/VPN devices. True role-based network access security relies on tuning user access privileges with business policies and a device's vendor-specific attributes.

VPN User Authentication
In a VPN environment, RADIUS One can manage both user authentication and tunnel authorization, allowing you to reduce total cost of ownership by managing credentials from a central location.

Firewall Administration
RADIUS One can be used as a single, consolidated user database for firewall administrators. Centralizing authentication of firewall administrators reduces the chance that a failure to synchronize authentication data manually will cause a security problem. In fact, RADIUS One can simplify authentication for a wide variety of network access and policy-enforcement devices.

All these 3 key features can be extended and/or integrated to an Identity System. Taking this into account and Identity Platform's support for RADIUS as the data repository (along with LDAP/Directories, NIS, etc.) is also critical. An Identity Platform also supports PKI like features and Certificate/Signature based Security features – that force chained higher-level of authentication for users before more security sensitive services are accessed. For example, additional levels of restrictions can be applied to accessing certain services based on not only user's authentication level, but also the domain/network from which the device is attached

---

[6] Access Control Lists
[7] Class of Service

to, and more (through written policies). Fundamentally RADIUS was a solution created to meet the needs of more rigid non-mobile –non-service centric environments. However – the challenge of today is to address mobility with security in a highly Service centric environments. Mobility involves user mobility, device mobility and service mobility – which directly forces the requirements for a distributed firewall like network identity solution.

Key capabilities found in an Identity System that is not addressed in a RADIUS solution includes;

- *Single sign-on (SSO)*
- *Centralized authorization services*
- *Centralized Session Management services*
- *Federated Identity support*
- *Comprehensive APIs*
- *J2EE/Java Support*
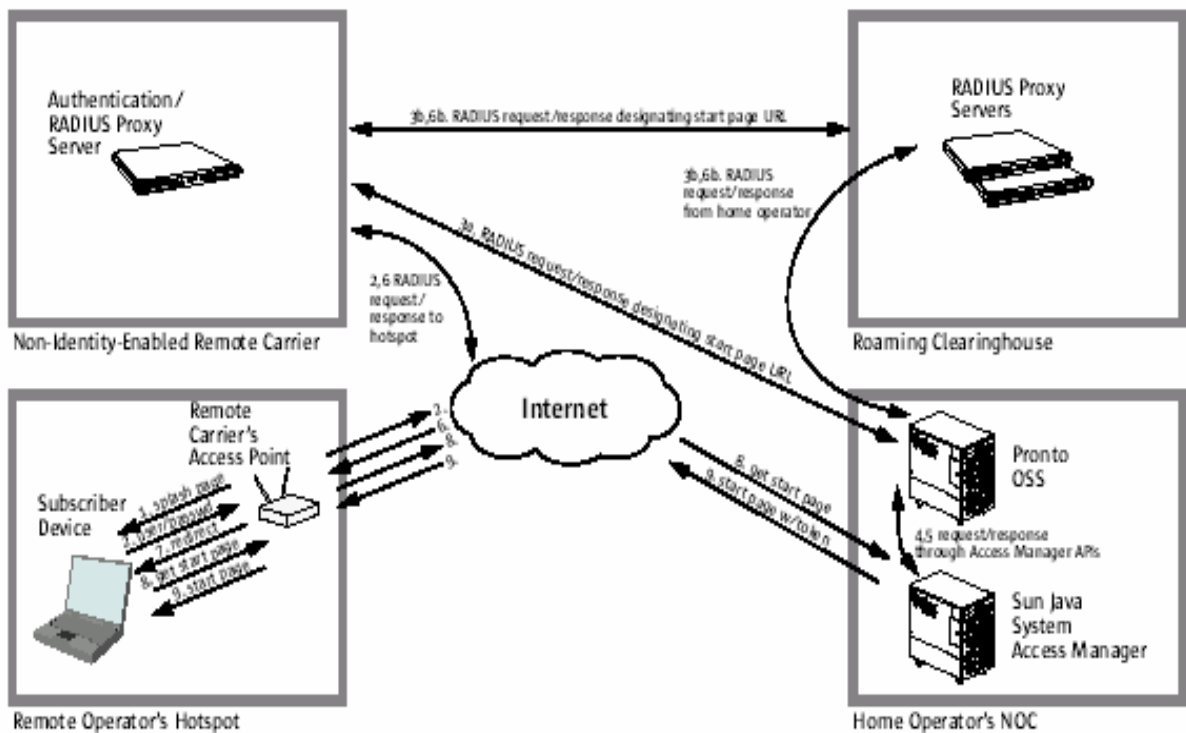- *Enterprise-class scalability and reliability*
- *Real-time audit*

Figure 11: Role of RADIUS and IDEN

Figure 19 depicts a scenario where a user roams from one wifi hotspot to another and accesses different services (such as a business tools and listing services).

Also from a Telecommunication Next Generation Network perspective, Identity Management Framework lays the foundation for a highly agile Services Architecture. For a highly Agile Service Architecture, which enables services to be built as a SBB (service building block) that are reusable, replaceable and accessible by users from any device and access (IP) network. The fundamental idea here is the fact that Service gets defined, built, integrated, tested and delivered in the network, once, and can be packaged and consumed in many different ways. This also highlights the significance of IDEN for NG OSS Solutions as proposed by TMF (telecommunication management framework) and their eTOM initiative.

VI   Identity System – User Centricity

Of all the perspectives from which one can view an Identity System the most important is the User perspective. The ID system provides the basis for a user centric "Service Mobility", i.e., services as accessible for users from any device and access networks, in a context sensitive manner. It is well know that consumers are seeking the following (regardless of the underlying technology):

Convenience –seeking access to services any time, anywhere
Consolidation –seeking a optimized cost structure resulting lower bills, and lower number of bills
Coherence – seeking customer centric coherence- profile, preference, policy driven services
Control – Having an option to define what they want, what gets shared, opting-in to trust circles, privacy protection, and.
Last but not the least; addressing **Complexity** –seeking simplicity and not being overwhelmed with complexities, no silos

Here Identity System plays a major role in capturing users profile, preferences and personalization elements – to deliver Services in a context sensitive manner (who, what, when, where, etc.).
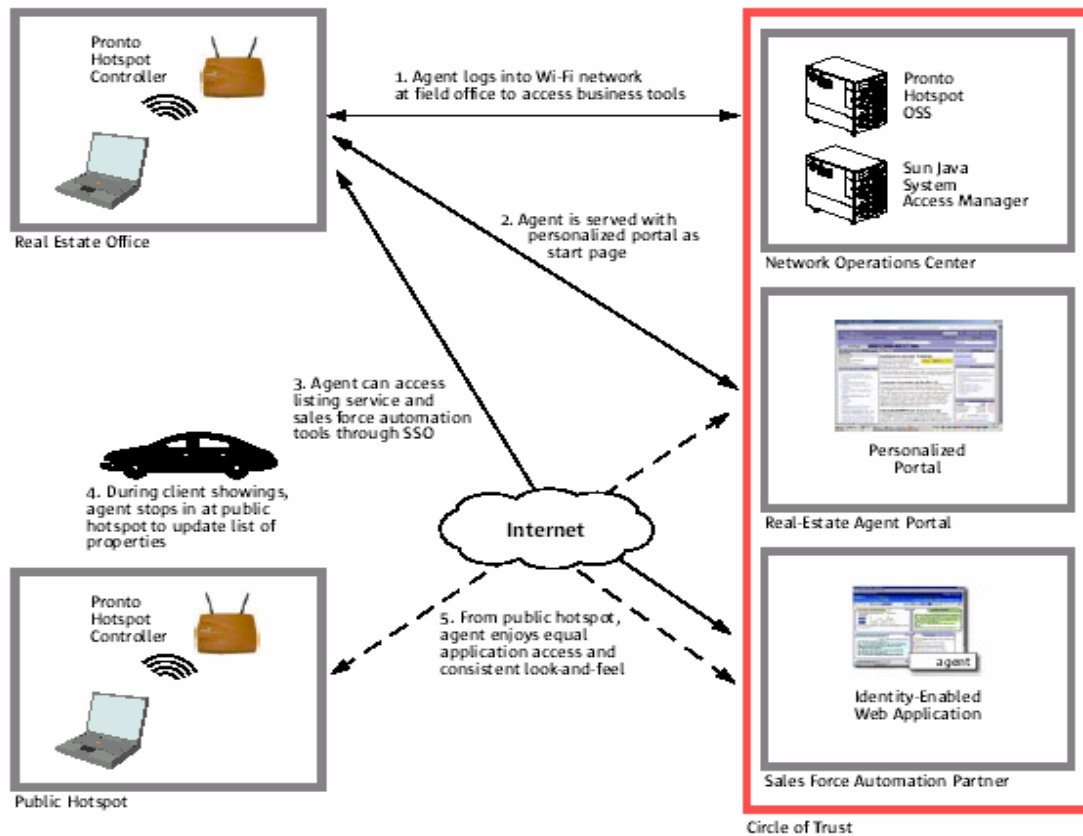

Figure 12: User Centric Service access (Roaming between hotspots and accessing location specific services)

The Identity System acts as a conduit that shares information and data between identity based services such as location, presence, payment, digital rights management, content delivery, etc.

There are restaurants in Boston (Harvard square area) that have an embedded flat panel in each table. The guest identifies the number of members in the group in the table and orders dinner via the digitized menu. This is 2004 – extrapolating the same a few years from now with an IDEN, the restaurant's network (wireless) identifies individuals (using retina scan, thumbprint or a simple id/credit card swipe) welcomes them by name, and generates custom menu based on preferences and time of day (such as vegetarian breakfast or seafood dinner, etc.). Preference and Profile driven services are further customized based on location, weather, etc.

Applying the same concept to the communication world, one scenario could involve the cancellation of a meeting a few hours before, due to unforeseen weather conditions. The notification of the cancellation could be via a beeper, email, sms, voicemail, instant message, etc., based on presence of the individual users and the service they are actively using, so that notification is sent via the appropriate service, that the user is actively using at a given point in time.

Customer Centricity also involves contextual affinity. Especially when customers have signed up with promotion programs such as earning frequent points at a Best Buy, earning Miles from United or free night stays from Marriott, etc. Through an Identity System, users can opt into combining their program points and consume benefits in a very cohesive manner. This is made possible by Liberty based Identity Systems and its federation capabilities across 2 or more service providers. This capability makes it easy for 2 or more companies collaborate with each other. A good example of this is a promotion like fly twice with united and get a free hertz one-week car rental for the third trip. By leveraging the identity system and data sharing between users united airlines frequent flyer program and hertz gold program, the consumer enrolls and is automatically provided that benefit by hertz when a car is rented the third trip (without coupons, membership ID, promotion code, etc.), without even the customer asking for it, ensuring true consumer convenience.

From a communication services perspective one relevant scenario is feeding in one's international calling card profile into the identity system provided by the local, long-distance carrier and every time a customer makes international call from a specific number, the calling card companies service is invoked. This implies that the consumer does not have to dial a specific 800 number, plug-in a 10-digit code, 4-digit pin and then the destination number. Similarly a user can define a few numbers as priority numbers in his/her profile and even when DND (do not disturb) is turned on incoming calls from the spouse or boss goes through.

" The idea here is that the user is offered an option to define how he/she wants the services to behave under varying conditions, is conceptually very powerful. Offering the user this capability will be a competitive edge, to begin with".

VII   Conclusion

The integration of Services, Network elements, Devices and Users data with Network Identity helps set the foundation for context driven/preference based content/service delivery to all Access networks and Access devices.

Also the proliferation of wireless networks cannot be stopped and is very strategic for Carrier's. The advances in Wireless Metropolitan and Wide Area Networks such as WiMAX, EVDO, etc., compliment the notion of an IDEN due to performance factors and the requirements around private/security. As traversal between LANs and Wireless WAN's are made seamless with varying throughput from devices, IDEN enhance the usefulness of related technologies such as Infrared and RFID. The end scenario eventually offers true ubiquity for end users accessing not just networks but also Services from all other types of networks. These developments along with standards such as SOAP, SAML, XKMS, RFID, also extend the capabilities of Identity Solutions to validate not just web users, but validate identity of web devices, web services, web sites and web applications.

Key Strategic points highlighted in this paper are;

> *" Identity Systems central role is managing the Access for Users, from Devices/Networks to different Services".*

> *" The data models around a user, device and services and a user's profile/preferences are shared through a common profile management service".*

> *" Identity System is a foundation Core Service Building Block (similar to the potential offered by ENUM Services) for Converged Services".*

> *" Identity enabled Networks (IDEN) revolutionizes the model for Network Service Delivery making it Access Network Agnostic, Device Agnostic – yet USER centric (profile/preference driven delivery of Services".*

> *" The idea that the user is offered an option to define how he/she wants the services to behave under varying conditions is conceptually very powerful. Offering the user this capability will be a competitive edge, to begin with".*

VIII   **References**

TSDE   *Sun White Paper on Telecom Service Delivery Environment*
Wifi and NI   *Sun/Pronto Joint Paper on wireless networks and identity*
CMA   *Sun White Paper on Common Mobility Architecture*
MDASOA   *Sun White Paper on Model Driven Architecture enabling Service Oriented Architecture*
RTN   *Restructuring Telecommunications Networks*