



A YOUnite® White Paper

Understanding the YOUnite Interchange

Abstract

This white paper provides an overview of the YOUnite Interchange and how the technology addresses the fundamental problems related to personal attribute and identity data management that proliferate the digital world today. The white paper describes how the YOUnite Interchange solves the problem of personal attribute and identity data inaccuracy and lack of granular control. There is a detailed discussion on how the YOUnite Interchange works, including the relevant technical details, examples of how the technology can be deployed, and the standard protocols utilized by the technology. The white paper concludes with details on how further information about YOUnite® and its technology can be obtained.

The information contained in this document represents the current view of YOUnite Inc., on the issues discussed as of the date of publication. Because YOUnite must respond to changing market conditions, it should not be interpreted to be a commitment on the part of YOUnite Inc., and YOUnite Inc. cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. YOUnite Inc. MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of YOUnite Inc.

YOUnite may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from YOUnite, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© YOUnite Inc... All rights reserved. YOUnite, YOUnite Enterprise, YOUnite Mobile, YOUnite Community and YOUnite Webtop are registered trademarks of YOUnite Inc. in the United States and/or other countries.

Other product and company names mentioned herein may be the trademarks of their respective owners.

YOUnite Inc. • 650 Castro Street – #120-377 • Mountain View, CA 94043 • USA • 866.794.4968

03/2011

Contents

Introduction	4
The Problem	5
The Opportunity	7
The Solution	9
How the YOUnite Interchange Works	10
<i>YOUnite Interchange - The Essentials</i>	11
<i>YOUnite Interchange - An Overview</i>	13
<i>YOUnite Interchange - Reference Implementation</i>	15
<i>YOUnite Interchange - YOUnite® Domains</i>	16
<i>YOUnite Interchange - Authentication Scheme</i>	16
<i>YOUnite Interchange - Master Data Management</i>	17
<i>YOUnite Interchange - Permissions, Connections and Endpoint Control</i>	19
<i>YOUnite Interchange - Resources</i>	21
<i>YOUnite Interchange - Populating the Interchange - Putting it all Together</i>	22
<i>YOUnite Interchange - Transactions and Fine Grained Transaction Reporting</i>	26
<i>YOUnite Interchange - Scaling for Larger Deployments</i>	27
Standards Based Protocols Used by YOUnite®	28
YOUnite Interchange API	29
Summary	30
Acronyms & Definitions	31

Introduction

The YOUnite Interchange is a flexible platform independent, scalable, and cost-effective solution that allows companies to create a secure personal information data exchange to enable an entity (business or individual) to securely distribute and control access to personal attributes (i.e. personal information) with complete customizable permissions without having to store that information on a centralized server.

The intent of this white paper is to explain how the YOUnite Interchange and underlying technology works as well as to highlight the unique patented capabilities of the YOUnite Interchange. In so doing, the white paper explains the importance of distributed infrastructure technology. By deploying the YOUnite Interchange, our partners will be at the center of a revolutionary global information interchange through a system enabling distributed sharing of personal information.

Patent No. US 7,461,071 B2 - Distributed Management Framework For Personal Attributes (Filed: 3 April 2006; Approved: 2 December 2008)

Inventors: Mark Fitzpatrick and Anthony Siress

Patent Attorney: William Ahmann - Sheppard Mullin Richter & Hampton LLP

Related Patent: US 7,698,445 - Obtaining Data From Unavailable Clients

Inventors: Mark Fitzpatrick and Anthony Siress

Patent Attorney: William Ahmann - Sheppard Mullin Richter & Hampton LLP

The Problem

Personal Attributes and Identity Inaccuracy

Personal attributes and identity information drive the digital world and there is a massive problem to be solved with respect to keeping it accurate. Inaccurate data can lead to losses in productivity, increases in operating expenses and the potential for fraudulent activity.

As the world becomes increasingly interconnected, the need for the information owner to manage accuracy and maintain control of their personal attributes and identity information across multiple platforms, devices, enterprise systems and social networks is becoming more and more critical. Today, it is impossible for individuals and organizations to ensure that their personal attributes and identity information is accurately updated and propagated to all institutions, business entities and individuals.

For Businesses

In an increasingly competitive global economy, information is critical to doing business and maintaining relationships. An enormous amount of personal data is transacted on a daily basis. Businesses are using information about individuals to help provide a better customer experience, customize web pages and send catalogs or offers tailored to individuals' specific interests or purchasing history. Businesses also use your information on a for-profit basis to facilitate unsolicited phone calls and mail, both physical and electronic. Every day physical addresses and e-mail addresses are bought, sold, traded and even stolen.

Businesses lose enormous amounts of time and wasted productivity trying to manage and accurately update information. The cost of customer support, updating and correcting inaccurate data, lost business opportunities, and lost personal and professional contacts is enormous. While business applications providers, such as Salesforce.com or Intuit, provide a repository for data, they do not solve the fundamental problem of its accuracy. Nor do they necessarily keep the data up-to-date or control distribution seamlessly to multiple systems and devices in a distributed and networked world. These applications help manage certain information and relationships on a micro/local level, but do not solve the problem on a macro/global level. The YOUNite Interchange provides the mechanism to enable businesses and individuals to connect islands of personal information as well as to manage and customize access to that personal information seamlessly.

In Our Personal Life

Personal Information is not limited to text (e.g. names, addresses, phone numbers, email addresses, IDs, account numbers, reports, documents, preferences), but can take any form (e.g. photo albums, videos, music, graphics, blogs and/or conversation strings). In the event that any of the information changes or the permissions to access the information changes, an individual is required to manage these changes across numerous devices, systems, networks and business relationships. This is not only time consuming, it can create opportunities for data to become lost or even corrupted.

Social networks have enabled sharing of personal content, but the ability to control access is limited to broadly defined categories of basic relationships, such as "Friends" or "Not Friends". These environments simply don't allow for individualized privacy (i.e. access control). By too broadly defining relationship access to personal content, there is an increased potential for identity theft and a limited ability to maintain privacy. The notion of selective sharing of personal content solves this problem.

The Opportunity

Future of Personal Information Management, Access and Control

YOUnite makes it possible to seamlessly exchange, share, and update distributed data in a controlled and secure way. It creates a distributed data sharing mechanism upon which a Global Information Exchange can be built.

Businesses and Organizations MUST Maintain Control

For an information exchange to work for organizations it is imperative that the exchange be distributed (the information be kept on their own servers and client devices). A centralized approach (where all users, businesses and organizations keep their data on a single set of central servers) cannot work by definition since businesses and organizations have fiduciary responsibilities surrounding the privacy of their own data.

Large corporations have over 5 billion employees worldwide, with growing competitive pressures to be more efficient and productive in the global economy. They are geographically dispersed, have mobile workforces, customer relationship and vendor management needs as well as human resource issues to manage on a daily basis. These corporations must control access to their data, while ensuring its accuracy, security and privacy. In addition, large corporations need to manage multiple devices provided to employees and enable data access and support between home and work computers, laptops, mobile phones and PDAs. All of this can be facilitated by the deployment of the YOUnite Interchange. Some specific examples include:

- Database vendors organize, store, sort, and retrieve data, but they do not solve the fundamental problem of its accuracy. These inaccuracies highlight an enormous problem and cost in data healing, add significantly to customer service costs, and lead to identity theft and business fraud. The YOUnite Interchange is a solution which can be applied to any pre-existing relationship between individuals, individuals and businesses or business and business that require both accurate and specific data provided in both directions without becoming one or the others store of the data. A decentralized approach allows data to be kept locally under the control of the owner and seamlessly updated to users of that data reducing costs, and eliminating inaccuracies.
- Enterprise software vendors have applications that in some manner require accurate connection information from individual employees such as HR, Payroll or smaller Customer Relationship Management (CRM). The YOUnite Interchange can facilitate this connection. Other applications include

notifications for software updates, special promotions, sales notifications and confirmations, recall notices and safety notifications.

- Call centers will no longer need to process Change of Address (COA) requests via the phone, which are often prone to inaccuracies due to human error. Databases and web-interfaces can now be designed without a COA feature.
- Customer relationship management will improve, because businesses will always have the most current information about their customer base facilitating accurate contact and relevant market offers.

Individuals MUST Maintain Control

The Facebook phenomenon has made social networks virtually ubiquitous. Facebook alone has over 600 million users, but the fundamental problem with social networks is in the inability to control access to one's personal attributes; it is simply not granular and in many cases, when "friending", one allows access to either all or nothing.

According to a recent survey conducted by Harris Interactive, it was found that the key to stealing a person's identity is built around a small number of personal attributes that are commonly found in an individual's public social network profile. Moreover, Harris Interactive said that the basic personal attributes available in open or public social profiles can easily enable criminals to answer identity verification questions and other security measures necessary to access financial accounts. By deploying the YOUnite Interchange, users could decide exactly what personal attributes to share and with whom, with complete granularity and control.

The Solution

YOUnite® is an exciting technology that can help reshape the face of personal information management. YOUnite® has created a platform that enables solution and service providers to create an information interchange with which virtually any device, client or system can interact. Solutions and services can connect to the interchange, make connections to other users and set permissions to information and files they own. Past attempts to create an interchange have forced all parties to store their information on a single set of centralized servers, but with YOUnite®, the customer controls where their information is stored. YOUnite's transactions in-flight are encrypted data and only reside on the YOUnite Interchange servers until such time as delivery is confirmed. Once delivery of data is confirmed, the data is expunged.

The YOUnite Interchange enables solution providers to create solutions that allow their customers to maintain complete accuracy of their information. They decide who can have access to their information as they choose by the use of a peer-to-peer distribution model and proven public-key encryption to enable secure data transmission to only those contacts authorized by the user.

Given the increasing amounts of fraud and other security threats, YOUnite® was architected with security as a paramount concern. YOUnite® is not a security vendor, but we fully understand the importance of securing information and personal data. The YOUnite Interchange is not a security product, but it is a secure product.

How the YOUnite Interchange Works

YOUnite® has developed a patented and flexible platform that allows developers to create secure, personal attribute and personal preference data exchanges to enable an organization or individual to securely distribute these details on a user-controlled and customizable basis without having to store that data on a centralized server.

This distributed permission based attribute sharing system is a server infrastructure called the YOUnite Interchange. YOUnite® can host an interchange or the interchange technology can be licensed and deployed by Partners within their own data centers. The system allows an organization to establish a multitude of users to connect and share attributes based on the permission settings set by the organization and/or the owner of the information.

Servers, services, devices and clients connect to the YOUnite Interchange by consuming YOUnite's RESTful API, with virtually any device or service that supports HTTP being able to connect to the interchange.

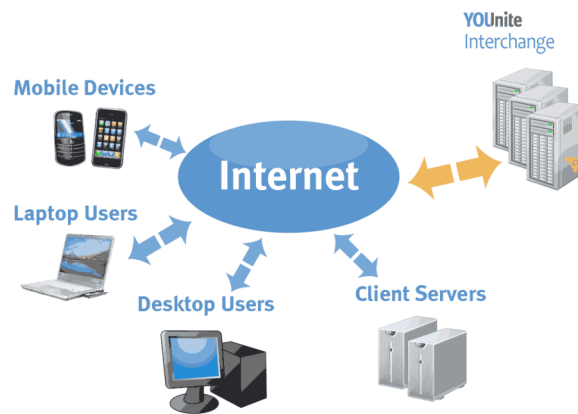


Figure 1 High Level View of the Interchange

The flow of data between users is not limited to C2C, but can include B2C as well as B2B. For example, a user can share their home addresses with their mobile provider and the mobile provider can share the phone numbers associated with the products the consumer is using as well as the location of the closest branch office.

YOUnite Interchange - The Essentials

The basic elements of the YOUnite Interchange are the `user`, `attributes` and `connections`. Attributes describe the user. Types of attributes that can be exchanged between users and organizations (connections) in the interchange include primitive or enumerated types attributes (e.g. phone numbers, email addresses, shirt sizes, and job preference) and binary large objects, blobs (e.g. images, documents, and MP4 files).

The set of attributes that describe users is called the Master Data Record (MDR). YOUnite provides master Data Management (MDM) features that allow developers to normalize data that may be exchanged between varying data silos by building rules that facilitate the exchange of the data between disjointed data sets. Other features of the Master Data Record include attribute dependencies and various data filters. Additionally, the MDR can be extended by adding new attributes and associated attribute rules.

A user has endpoints, each of a endpoint-type; examples of endpoint-types include smart phones, social sites, and data silos. Endpoint-types are plug-able Java code that are MDR aware and written by partners#.

Some endpoint-types just receive attributes (e.g. data silo), while others can be developed to send and receive attributes (e.g. a smart phone). These applications typically have a partner's front-facing web application that manages the endpoint-types. In both cases, attribute sharing are handled by the YOUnite Interchange.

Users can connect with each other and set permissions on the attributes they want to share.

Users, endpoints, endpoint-types, connections, permissions and other resources are grouped together into manageable entities called YOUnite `domains`. Each domain has an `authuser` that makes requests on behalf of all users in that domain.

It is often easiest to understand how YOUNite enabled users and the interchange work together by describing a simple scenario.

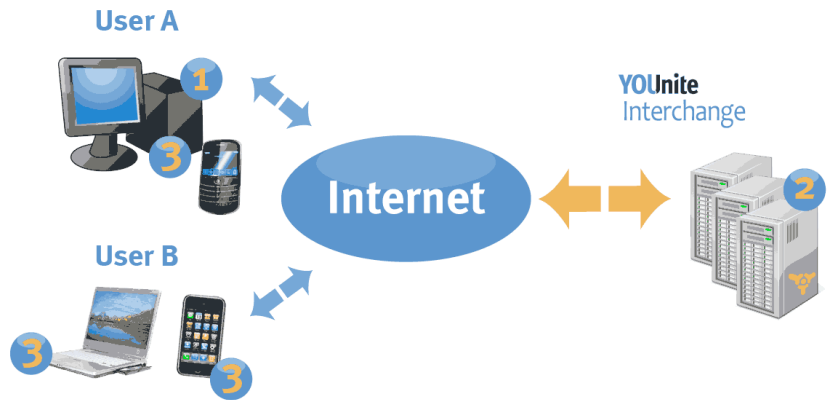


Figure 2 Simple Scenario of users and the interchange

Assume there are two users with multiple devices that are YOUNite[®] enabled. User A has shared his mobile phone number with User B. When (1) User A changes his mobile phone number on one of his devices, YOUNite[®] checks the permissions associated with that change and then forwards it to the (2) interchange. The interchange generates the (3) appropriate transactions, not only for User B's devices, but also for User A's other devices as well.

As more users and organizations are added, the interchange becomes a large permissions engine.

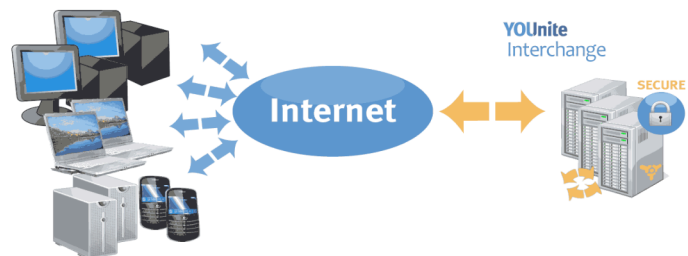


Figure 3 The Interchange becomes a permissions engine

YOUnite Interchange - An Overview

The YOUnite Interchange is scalable web application servers that can either be hosted by YOUnite or deployed into a Partner's data center.

At the core of the YOUnite Interchange are the Interchange Engine and the Pluggable Endpoint Engine:

- The Interchange Engine handles incoming HTTP requests and manages the resources such as users, endpoints, attributes, permissions and connections.
- The Pluggable Endpoint Engine performs the basic read/write operations to various endpoint-types on behalf of the users. Endpoint types can be dropped into the engine dynamically.

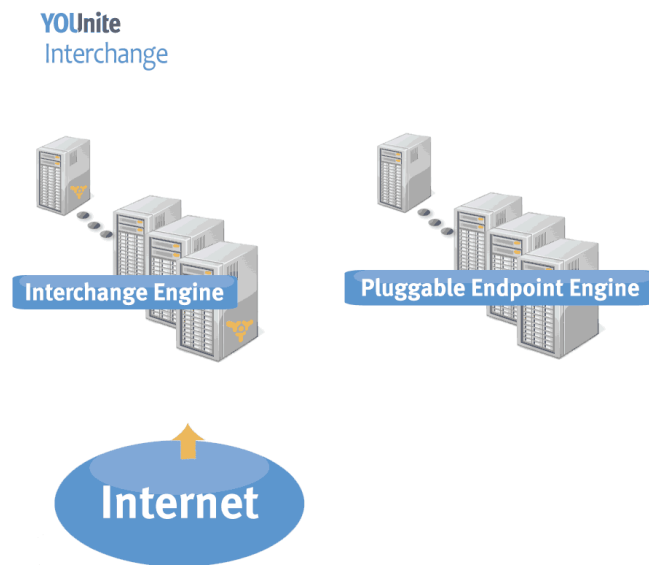


Figure 4 YOUnite Interchange

The figure below represents a typical deployment into a Partner's data center. The Partner's front-facing web application makes requests to the YOUnite interchange on behalf of the Partner's endpoints.

Attribute changes are made in the form of requests that are made on behalf of the Partner's endpoints (e.g. social sites, smart phone apps, data silos) using a RESTful interface. These attribute changes are processed by the interchange and sent out to the appropriate endpoints, as shown in the figure below.

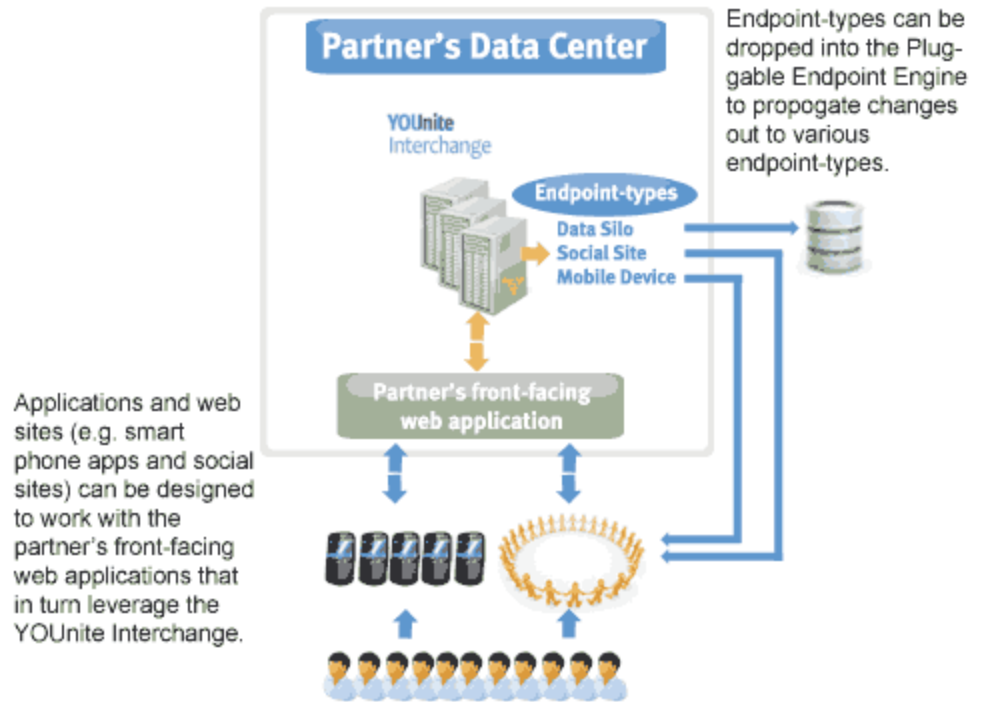


Figure 5 YOUnit Interchange Deployment

At the core of the YOUnit Interchange are the Interchange Engine and the Pluggable Endpoint Engine:

- The Interchange Engine handles incoming HTTP requests and manages the resources such as users, endpoints, attributes, permissions and connections.
- The Pluggable Endpoint Engine performs the basic read/write operations to various endpoint-types on behalf of the users. Endpoint types can be dropped into the engine dynamically.

YOUnite Interchange - Reference Implementation

For partners who wish to license the interchange, the reference interchange runs using (but is not limited to) the following technology:

- CentOS Linux
- Glassfish Application Server
- HornetQ JMS
- MySQL



Figure 6 YOUnite interchange reference implementation

YOUnite Interchange - YOUnite® Domains

YOUnite® supports the notion of domains, which enable the grouping of end-users and other resources into manageable entities. YOUnite® domains can reside in data centers separate from the YOUnite Interchange and users from multiple domains can share information.

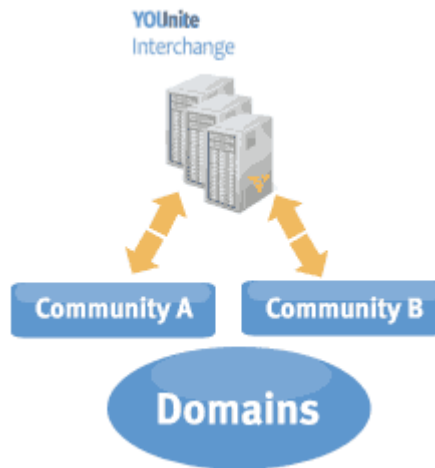


Figure 7 YOUnite interchange domains

YOUnite Interchange - Authentication Scheme

Each domain has an authuser that consumes the API on behalf of the users and resources in the domain. The authuser communicates to the Interchange using SSL and basic authentication. An authuser has a password -- the authuser's name and password are sent in the Basic Auth header of all requests sent to YOUnite®.

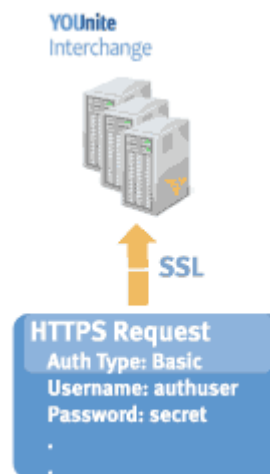


Figure 8 YOUnite Authentication Scheme

YOUnite Interchange - Master Data Management

The interchange has Master Data Management (MDM) features that allows for the normalization of data. Issues can arise when exchanging data between varying data silos. One silo may refer to a user's last name as "Last Name", while another silo may refer to it as "Surname". The YOUnite® Master Data Record allows the developer to build rules that facilitate the exchange of the data between the disjointed data sets. Other MDM features within the Master Data Record include attribute dependencies and a variety of data filters and the ability to add new attributes to the Master Data Record for a given domain.

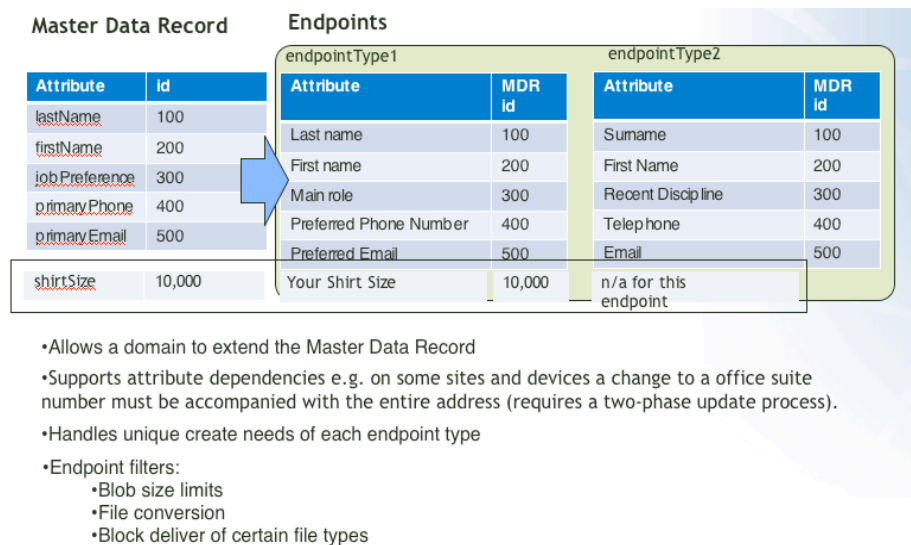


Figure 9 YOUnite interchange - Master Data Management

The endpoint types must be aware of the Master Data Record and be coded to normalize the data for that particular endpoint type. This Master Data Record normalization coding can be extended to various endpoint types.

Once a Partner has created their required domains and endpoints, and these endpoint types are plugged-in so that they can communicate with the interchange, the YOUnite Interchange becomes a large permissions and data normalization engine for sharing data between disparate and disjointed data sets in a distributed fashion.

Attribute Dependencies and Self-Healing Transactions

Intelligence is built into YOUnite attribute-change (or delta) transactions. The following simple example illustrates one scenario where this feature can be leveraged:

- A user moves to a different suite in their office building and updates their addressLine attribute.

-
- When the request is submitted to the interchange, the interchange checks the endpoint-rules for all endpoints that will receive the new suite number.
 - The interchange detects that a few of the endpoint-types that will receive this change don't allow a single address line change -- they require that the entire address be sent (all address lines, region, state, postal code and country).
 - The appropriate HTTP response code is sent back to the API consumer with entity body information calling for the complete address.
 - The request can be resubmitted with the appropriate data so that the transaction can be fulfilled -- or it can be resubmitted with only the suite number with the knowledge that not all endpoints will receive the update.

YOUnite Interchange - Permissions, Connections and Endpoint Control

A user can set permissions for any or all of the user's attributes. Say that UserA has attributes associated with:

- First Name
- Last Name
- Home Phone Number
- Mobile Phone Number
- Email Address
- Mailing Address
- Profile Image

In addition, say that UserA has connected with UserB. Through the notion of permissions, UserA can share any attribute with UserB; for example, User A has decided to share:

- First Name
- Last Name
- Mobile Phone Number
- Email Address
- (but not) Home Phone, Mailing Address or Profile Image

The user also has endpoint control of the shared attributes, called endpoint rules. Through endpoint rules, UserB can control what endpoints receive what attributes from other users for example, UserB has two endpoints: An Android device and a social website account. UserB can set controls for these endpoints such that the Android device receives all of the attributes shared by UserA, but the Android device only receives the First Name, Last Name and Email Address (no images).

In addition, the Master Data Record attributes can be enabled or disabled for a given endpoint type; for example, if an endpoint type cannot support a data field for an image, the interchange will never send the image to that particular endpoint.

Users can then select or define permissions for the attributes that they wish to share with specific users to which they are connected. Users also have an auto-connect security token that can be shared with users with whom they would

like to connect. Typically, UserA invites UserB to connect with them. UserA then waits until UserB either accepts or declines the invitation to connect.

There is also an auto-connect feature where UserB gives UserA the security token (e.g. "bump" smart phones) and UserA then submits a connect request using User B's security token. The interchange will automatically connect the two users and apply the Master Data Record attribute endpoint rules, user defined permissions and endpoint controls.

YOUnite Interchange - Resources

The YOUnite Interchange provides a RESTful API and as such operates using the features of the HTTP “request and response” protocol. Requests are made of the interchange in the form of `PUT`, `POST`, `DELETE`, and `GET` verbs, with the corresponding return responses being nouns in the form of resources.

There are some particularly prominent or significant resources within the YOUnite[®] API. These resources, in hierarchical order, are as follows:

<code>/domains</code>
<code>/authusers</code>
<code>/endpoints-types</code>
<code>/endpoints</code>
<code>/attribute-definitions</code>
<code>/attribute-enumerations</code>
<code>/users</code>
<code>/connections</code>
<code>/permissions</code>
<code>/transactions</code>

Both the requests (i.e. HTTP verbs) and responses (i.e. resources) have headers that define the content type and bodies that consist of XML or JSON documents.

YOUnite Interchange - Populating the Interchange - Putting it all Together

The following describes a generic deployment of the YOUnite Interchange and how the deployment would be populated.

Imagine a new partner, whose name is NewCo, has just deployed the YOUnite Interchange. When NewCo deploys the interchange, it is initialized with the domain NewCo and for this example, the authuser will be called: NewCoAuthUser. Going forward, all calls that are made to the interchange on behalf of the resources in this domain will use NewCoAuthUser's credentials.



Figure 10A Populating the YOUnite Interchange

NewCo's developers create a Gmail endpoint-type and drop it into the Pluggable Endpoint Engine.

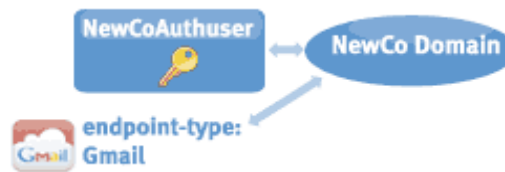


Figure 10B Populating the YOUnite Interchange

Continuing with this example deployment, NewCo adds a domain for their Telco business partner and the corresponding authuser: they are called Telco1 and Telco1Authuser. POST calls are made to create the new domain and authuser.

POST /domain

POST /authuser

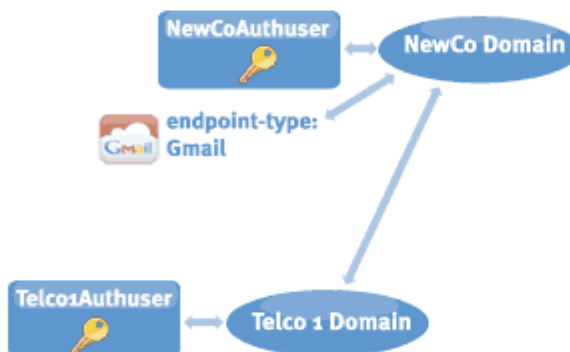


Figure 10C Populating the YOUnite Interchange

Telco1 creates an iPhone endpoint-type for the domain and drops it into the Pluggable Endpoint Engine.

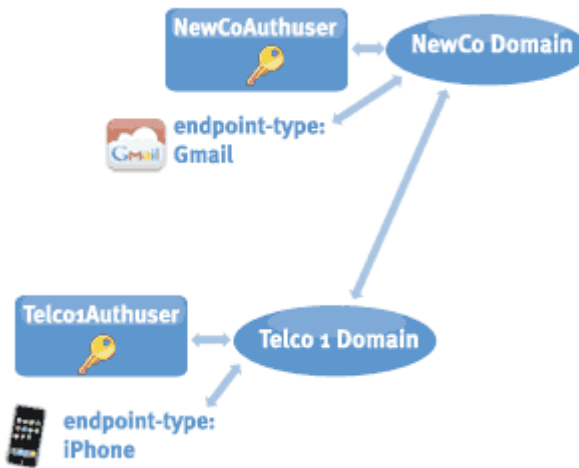


Figure 10D Populating the YOUNite Interchange

The Telco1 webapp makes the appropriate POST calls and creates two users for the domain; for this example: user1 and user2. The POST call also specifies to which domain the users belong.

POST /user

POST /user

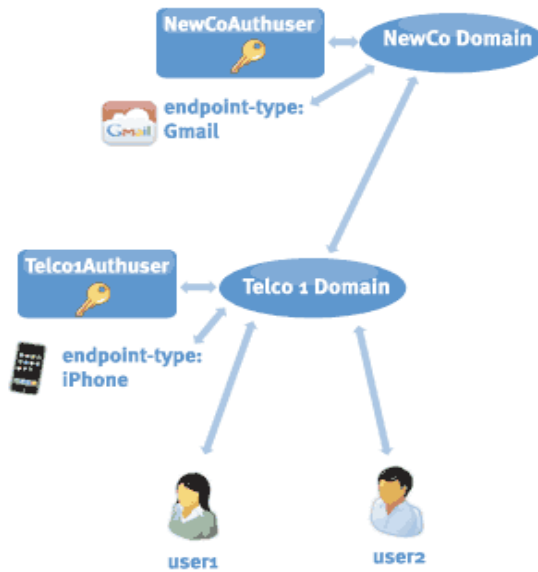


Figure 10E Populating the YOUNite Interchange

For User1, two endpoints are created with individual post calls: Google and iPhone. Similarly, an iPhone endpoint for User2 is created.

POST /endpoint

POST /endpoint

POST /endpoint

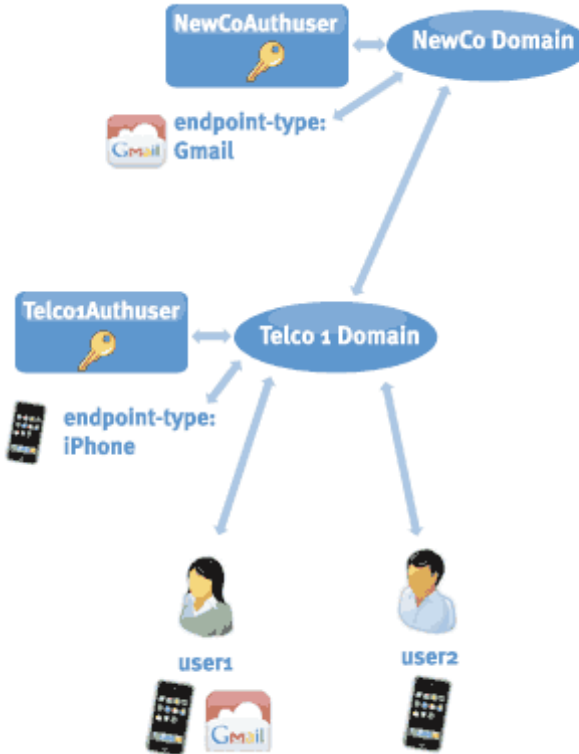


Figure 10F Populating the YOUnit Interchange

This process is repeated for a third domain named: Telco2, which adds an authuser, Facebook endpoint-type and a telco data silo endpoint-type.
 POST /domain

POST /authuser

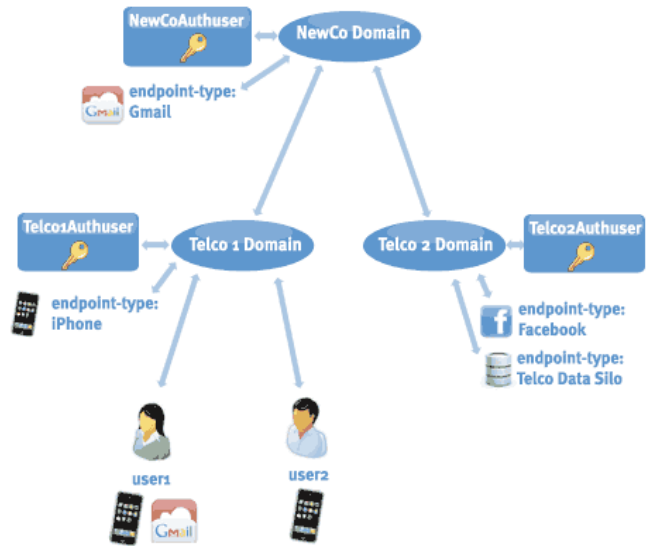


Figure 10G Populating the YOUnite Interchange

The Telco2 domain has a user called User3 with two endpoints: Facebook and the data silo.

POST /user

POST /endpoint

POST /endpoint

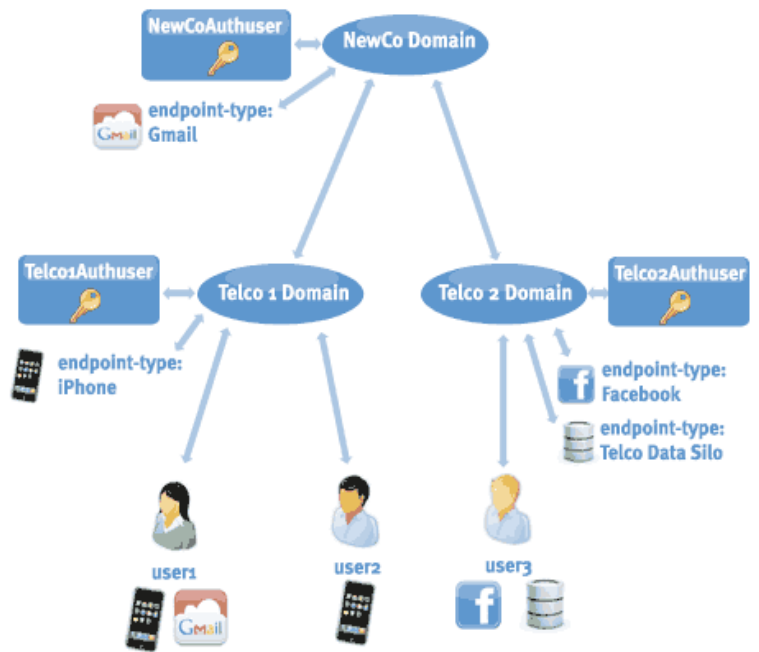


Figure 10H Populating the YOUnite Interchange

At this point, the users can make connections to other users and assign permissions to their attributes. The users can also apply endpoint rules to their individual endpoints; this enables endpoint control. Moreover, the NewCo Authuser can facilitate connections between subordinate domains, thereby allowing users from the Telco1 domain to connect with users from the Telco2 domain and/or vice versa. Finally, attributes of the Master Data Record can be enabled or disabled for any of the available endpoint-types based on the ability of the endpoint-type to support the type of data being shared.

In addition, the Master Data Record is predefined at the NewCo domain level, which then facilitates the master data management features that are available.

YOUnite Interchange - Transactions and Fine Grained Transaction Reporting

Overview

The YOUnite Interchange executes requests by the user to add, delete or modify attributes. These requests are called transactions and are made via POST calls to the interchange. In addition, the interchange provides details (via GET requests) of every transaction which enables fine grained transaction reporting.

Continuing with the deployment example, Telco1 User1 posts a connection with associated permissions to Telco1 User2. If Telco1 User1 changes an attribute (e.g. email address or mobile phone number), then that change is propagated to all associated endpoints. There is a three-step transaction protocol, where:

- Transaction is accepted and the request is pushed out to the endpoints
- Upon transaction completion, a callback is sent to notify the requester
- Details of the transaction can be inspected by the requester

Every transaction is given a Transaction ID Number and every transaction is comprised of transaction items, which are given Transaction Item ID Numbers, Master Data Record ID Numbers, Endpoint ID Numbers, and are assigned status Code Numbers that are generated by the interchange. All of these details are logged in the history table, so that every transaction item of a transaction can be monitored in great detail.

The number of transaction items generated for a given transaction is derived by the number of attributes changed and the total number of endpoints that will receive the attributes. As users typically have several endpoints and a single user can have hundreds of connections, a single transaction could generate hundreds or thousands of transaction items.

The partner's front-facing web application, by way of its authentication token, can GET the details of each transaction by either polling the status of the ongoing transaction items or a callback can be registered so that the API consumer can get the full status of the transaction once it is completed.

YOUnite Interchange - Scaling for Larger Deployments

Requests made to the interchange are stateless and it is built to scale vertically with load. As mentioned earlier, there are two components: the YOUnite Interchange engine; and the Pluggable Endpoint Engine. The Interchange Engine handles incoming HTTPS requests and the Pluggable Endpoint Engine sends data to the endpoints.

Internally HornetQ JMS, MySQL and NFS are used, but other JMS, SQL and filesystem technologies should plug in.

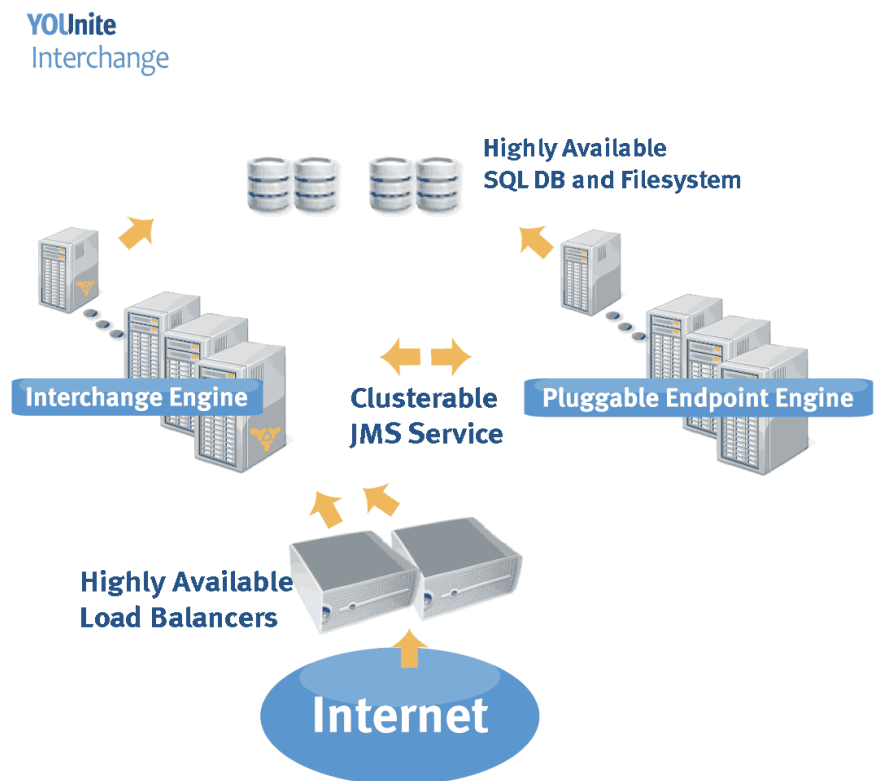


Figure 11 Scaling for larger Deployments

Standards Based Protocols Used by YOUnite®

YOUnite® leverages many existing, standard protocols. Using these standardized protocols aids in ensuring interoperability between vendor implementations. The protocols used to implement YOUnite® are found in use on the Internet and on local area networks everywhere. This prevalence ensures that there is a large pool of people knowledgeable in implementing and deploying solutions based on these protocols. The following is a list of the major protocols; please reference the Acronyms and Definitions table below:

- GlassFish (Apache Tomcat Derivative)
- HTTP / HTTPS
- JMS
- JSON
- REST
- SSL
- XML

YOUnite Interchange API

Where to go to Further Your Knowledge

If applications are to be built on the services provided by the YOUnite Interchange, the user should get all facets of YOUnite[®], namely:

- Information control
- Accurate information from others
- Consistent information across all devices and services

YOUnite provides a rich RESTful API that can be used to facilitate the secure, accurate transfer of data between users and their endpoints, as described in the previous scenarios. For more information, please refer to the YOUnite RESTful API documentation.

Summary

Now, more than ever before, computing power is being added to smaller, more common devices. Inexpensive and ubiquitous networking media technology is here, or is close to realization. The cost reduction in networking and computing power of recent years is considerable.

Data drives the digital world and there is a massive problem to be solved with keeping personal attributes accurate and controlling access to it. YOUnite[®] was founded to not only address, but also to surpass, the increased expectations of personal attribute privacy, management and control. YOUnite[®] fully addresses and solves these problems with the introduction of the YOUnite Interchange, a platform independent, flexible, highly secure, scalable, and cost-effective solution. YOUnite[®] technology ensures data is available, accurate and consistent across all environments. In addition, the YOUnite Interchange provides privacy of personal attributes through the notion of selective sharing. YOUnite[®] technology presents a revolutionary, patented means to securely distribute data as soon as it has been updated.

YOUnite's vision is to create a new Global Data Management and Exchange market that will allow businesses and organizations to create global, distributed information exchanges. Using the YOUnite[®] SDK, developers can create applications that will propagate information between multiple devices/clients, users and organizations without requiring data to be stored in a central repository. Users, businesses and organizations can choose where they want their data stored, with which they want to share it and what they want to share down to the attribute level.

Acronyms & Definitions

API	Application Programming Interface
Base64	Base64 is a group of similar encoding schemes that represent binary data in an ASCII string format.
BLOB	Binary Large Object. YOUNite attribute update transactions are generally strings, enumerated types or BLOBs.
EJB3	The EJB specification is one of several Java APIs in the Java EE specification. EJB is a server-side model that encapsulates the business logic of an application.
GLASSFISH	GlassFish is an open source application server project led by Sun Microsystems for the Java EE platform. It is a derivative of Tomcat's reference application server implementation.
HTML	HyperText Markup Language, is the predominant markup language for web pages . HTML is the basic building-blocks of webpages.
HTTP/HTTPS	HyperText Transfer Protocol - TCP/IP provides the base protocol stack to provide network connectivity between YOUNite clients and the YOUNite Interchange. HTTP (Hypertext Transfer Protocol), which is hugely responsible for the success of the Internet, is also a core part of YOUNite. All aspects of YOUNite build on top of HTTP or its variants. Some of the explanations of higher-level protocols and the workings of YOUNite assume a basic knowledge of the HTTP protocol.
JAVA EE	Java Platform, Enterprise Edition or Java EE is a widely used platform for server programming in the Java programming language. YOUNite uses JEE 6.
JMS	The Java Message Service (JMS) API is a Java Message Oriented Middleware (MOM) API for sending messages between two or more clients . YOUNite implements HornetQ JMS.
JPA	The Java Persistence API, sometimes referred to as JPA, is a Java programming language framework managing relational data in applications using Java Platform, Standard Edition and Java Platform, Enterprise Edition .
JSON	Java Script Object Notation is a lightweight text-based open standard designed for human-readable data interchange. XML and JSON are a core part of YOUNite used in server requests and responses.
MySQL	A relational database management system (RDBMS)[1] that runs as a server providing multi-user access to a number of databases.
REST	Representational State Transfer - A style of software architecture for distributed hypermedia systems such as the

	World Wide Web. The term is often used in a looser sense to describe any simple interface which transmits domain-specific data over HTTP without an additional messaging layer such as SOAP or session tracking via HTTP cookies. REST (Representational State Transfer) is a core part of the YOUNite API and is used in all requests and responses between a YOUNite enabled client and the YOUNite Interchange.
SSL	Secure Sockets Layer (SSL), are cryptographic protocols that provide communications security over the Internet .
TCP/IP	The Transmission Control Protocol (TCP) and the Internet Protocol (IP) - networking protocol stack serves as the base for YOUNite. By using the standard, prevalent TCP/IP protocol suite, YOUNite leverages the protocol's ability to span different physical media and ensures multiple vendor interoperability.
XML	Extensible Markup Language (XML), to use the W3C definition, is the universal format for structured data on the Web. Put another way, XML is a way to place nearly any kind of structured data into a text file. XML looks a lot like HTML in that it uses tags and attributes. Actually, it is quite different in that these tags and attributes are not globally defined as to their meaning, but are interpreted within the context of their use. These features of XML make it a good fit for developing schemas for various document types. The use of XML as a schema language is defined by the W3C. XML and JSON are a core part of YOUNite used in server responses to client requests.

YOUservice LLC, a California Limited Liability Corporation, was founded in 2004 by Mr. Anthony Siress and his business partner, Mr. Mark Fitzpatrick. In late 2004, they incorporated, and funded YOUservice LLC. YOUNite, Inc. was then formed in November 2006 for the purposes of developing the patented YOUNite Interchange technology. YOUNite, Inc. is located in Mountain View, CA. YOUNite, Inc. is a Delaware "C" corporation and is a wholly owned by YOUservice LLC. To learn more about YOUNite, Inc. or the YOUNite Interchange, visit www.youniteinc.com.