The Liberty Alliance
GLOBAL ADOPTION
N E W S L E T T E R

Volume III
Fall 2006
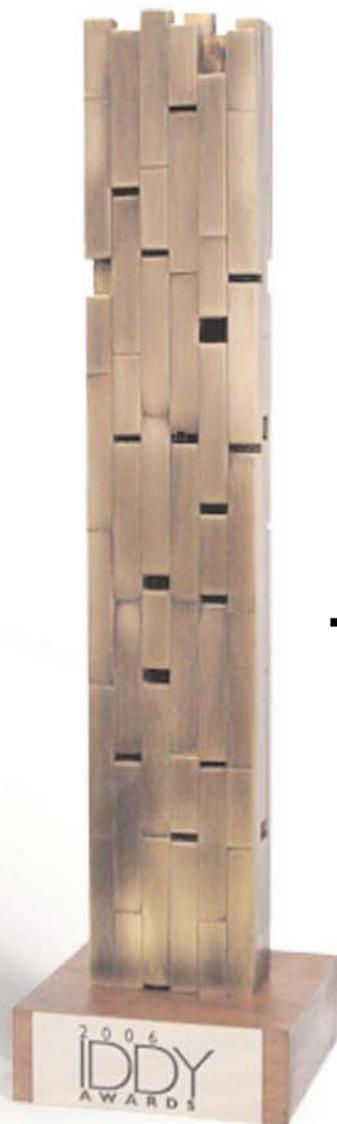
All About
the IDDY

2006
IDDY
AWARDS

CONTENTS

Liberty Alliance Presents
First Annual IDDY Awards
for Excellence in Identity Management

The DIDW Conference in September kicked off in a new way with the presentation of the first annual Liberty Alliance IDDY Awards for excellence in identity management. IDDY stands for Identity Deployment of the Year.

Close to 300 individuals were there for the early morning presentation at the Santa Clara Marriott, where George Goodman announced the three winners: Deutsche Telekom AG (T-Com, Business Unit T-Online), EduTech and the UK Government. Goodman formally presented the winners with the actual IDDY Award, a foot-high brass sculpture that was designed by Kristian Iglesias, a sculptor and metal designer living and working in Greenport, New York.

"We were delighted to partner with DIDW for the presentation of the IDDY Awards," said Britta Glade, the director of marketing for the Liberty Alliance. "DIDW is the industry's leading event for all things related to identity so it was an ideal forum to highlight excellence and recognize some of the most exciting deployments in the marketplace."

George Goodman, Liberty Alliance President, introduces the IDDY at Digital ID World

The IDDY Embraces Identity Diversity

Liberty Alliance standards are having an enormous impact across the world and in multiple vertical markets. According to Glade, the timing was right for Liberty Alliance to step back and formally recognize the rich diversity of applications and deployments in the market. "We learned last year that by the end of 2006 there will be more than one billion Liberty-enabled identities and devices. Some reflect a traditional employee-focused federated approach, others a user-driven, consumer-centric focus," she said. "The IDDY recognizes the very different business use cases that are out there truly pioneering identity. This deployment diversity is a testament to the elegance and strength of the Liberty specifications as foundational to a wide variety of identity deployments."

IDDY Award nominations were evaluated based on criteria that include the benefits deployments are delivering to organizations and users; the ROI the application is demonstrating; and how the solution may successfully address key identity issues such as reducing identity theft, meeting regulatory requirements or providing consumers with increased privacy protection. This year's IDDY Award recipients have successfully deployed Circles of Trust (the legal, business and policy agreements governing federation) and Liberty-enabled technologies in the education, government and service provider sectors.
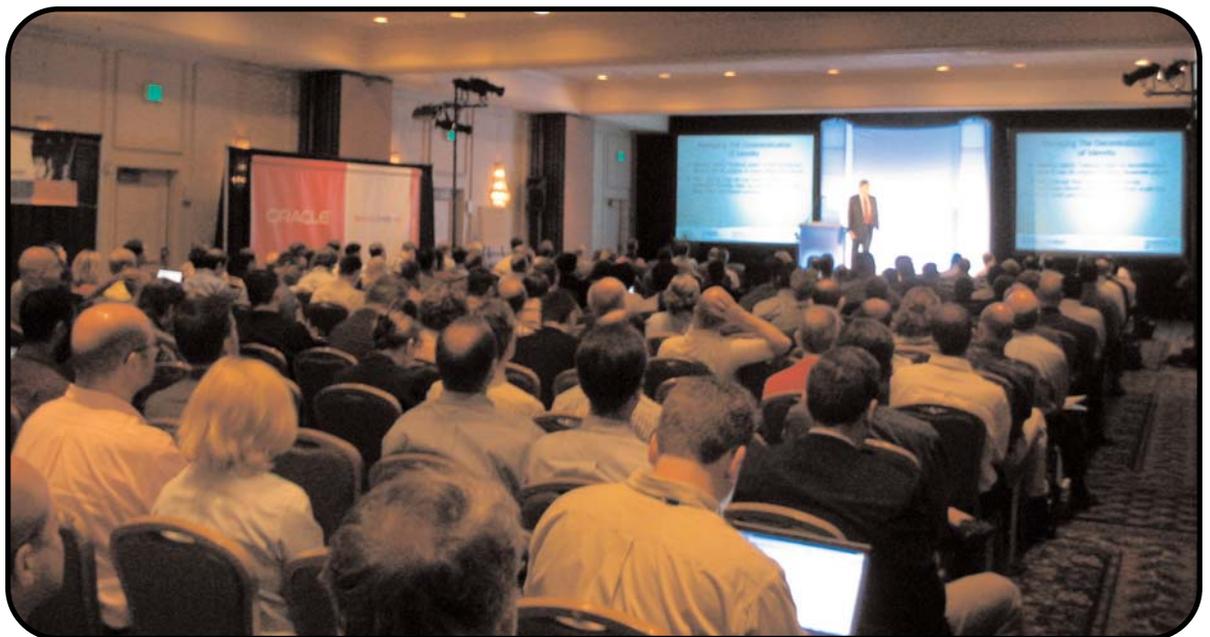
The crowd at the IDDY Awards presentation

"We're thrilled by the submissions we received and also by the additional up-and-coming deployments we heard about," said Glade. "One of the most exciting parts of organizing this award was hearing about projects in progress—and what's in store for next year. It's so clear that the range of ways that the Liberty specifications can be deployed in the digital ecosystem is only beginning to be explored."

THE IDDY JUDGES:

- Michael Barrett, CISO, PayPal, Inc.
- John Fontana, senior editor, infrastructure, Network World;
- Gerry Gebel, service director-IdPS, Burton Group
- George Goodman, president of the Liberty Alliance management board and director of the platform capabilities lab at Intel
- Paul Madsen, co-chair of the Liberty Alliance technology expert group and identity standards researcher at NTT
- Robin Wilton, co-chair of the Liberty Alliance public policy expert group and corporate architect at Sun Microsystems
- Christine Varney, partner, Hogan & Hartson

APPLYING FOR THE 2007 IDDY

In the Spring of 2007, Liberty will make available the 2007 IDDY Award submission form. If you'd like to be on the mailing list for IDDY related announcements, send an email to: IDDYUPDATES@projectliberty.org

2006 IDDY Award Winner: EduTech

EduTech, the organization that provides technology to 697 New York State school districts, was honored for their deployment of a set of federated identity applications that dramatically improve how educators and staff share, access and deploy information and resources across an entire technology ecosystem.

Background on EduTech:

Educational Technology Services (EduTech) is one of 12 Regional Information Centers (RICs) in New York state that provides technology services to the 697 school districts in the state. EduTech is directly responsible for supporting the technology needs of 47 school districts in the Genesee Valley and Wayne Finger Lakes BOCES regions of NY state.

In addition to traditional hardware and software, EduTech supports a number of administrative (server-based) applications for student and financial applications. EduTech also provides Web–based courses for students and staff development, traditional

IDDY winners, Jenine Welch and Brian Hegeman from EduTech

technology workshops, Web-based tools for data analysis of student assessment results, and assistance in instructional–technology integration.

EduTech's Identity Management Objectives: EduTech deploys a number of applications, one of which is called DataMentor. This application displays district-wide performance test results used by teachers and administrators to assess progress and delivers additional tools that educators use to advance their teaching. DataMentor needed a way for teachers and administrators to build their own assessments for evaluating progress and for exposing what topics they need to focus on.

EduTech wanted educators to be able to use single sign-on to seamlessly access all of the tools available to them across the ecosystem. The EduTech team recognized the value of delivering wider access to the siloed arsenal of valuable applications existing within the trusted network of Regional Information Centers. Once the RICs were federated and communicating, EduTech helped reduce hard costs by allowing the RIC's assets, including applications, to be securely shared.

To deploy federated identity across districts, EduTech knew a consortium or a trusted network had to be built amongst the Regional Information Centers to support all of the districts, including Buffalo and Syracuse, the two largest districts in the state. Furthermore, in NY state, all school districts must report testing results to a central data warehouse run by the State, posing a challenge for administrators looking to accurately assess data in real time to uncover areas where improvements are needed.

The Results: In New York state, many of the school districts use DataMentor as their IDM provider through a WebSphere portal. Others use a homegrown application built with open-source tools to create a place within the RIC for people to login, because a portal is simply too expensive for them. To support existing installs, EduTech also had to offer the option to use Cognos as a centralized authentication to DataMentor across the ecosystem.

Because federation uniquely identifies every user across the entire State system, a teacher or administrator who transfers to another district

would continue to have access to authorized information, saving districts time and money. The educator's identity does not have to be recreated because he/she is already authenticated can access everything authorized when they need it, rather than having to contact numerous IT administrators to be productive.

Today, DataMentor is currently deployed to 80% of NY State's Education System and the decision to embrace and deploy federated identity management touched almost every teacher and administrator without them even knowing it.

QuizMaker is a home-grown application designed by one of EduTech's companion RICs, known as SCT, to help teachers target and build strengths in weak areas. SCT services nine districts in NY state, and QuizMaker was only available to the teachers in these districts. Once identity federation was deployed with PingFederate, everyone in the ecosystem had seamless access to QuizMaker.

Looking at ROI: The objective of the deployment of Federated Identity across the school ecosystem was to increase teacher and administrator access to tools and information, enhance teaching efforts, increase test scores and lower operational costs.

Once federation was deployed by EduTech, the State Department of Education had a big shift in their thinking on how identity is handled. Originally the State started creating one big portal, intending to own and offer all available applications district-wide. This approach dictated that the RICs would have to give up control or simply stop coordinating with the State, which would prevent easy access to State-owned testing results and limit success. The State recognized the value of federation, the partnerships it creates, and the financial and performance benefits of sharing information and applications.

The State Department of Education is now using identity federation to offer state-level services and applications to their RIC partners. Because of this, educators can be more successful and leverage tools that others have created and own. For the RICs, federated identity lowered their costs without forcing them to give up control. Everyone is able to tap into a much larger market and a much larger tool kit. The end result has been that test scores are moving higher and teachers are more successful in building student skills.

The Technology: Eductech deployed PingFederate from PingIdentity. PingFederate is a stand-alone federation server for enabling single sign-on to online services for employees, customers and business partners. It is designed to integrate and coexist with home-grown and commercial Identity Management deployments. As a result, enterprise-wide identity federation is achievable without requiring extensive upgrades to an entrenched Identity Management system.

According to Welch, its tightly integrated support for WS-Federation, SAML 1.0, SAML 1.1 and SAML 2.0 single sign-on functionality reduced redundant account maintenance, improved administrative efficiency, increased security and even brought about new revenue-generating opportunities for the RICs and the State. "We looked at other products, but our partners refused to support them. For this deployment to be successful, a solution had to support all federated identity standards. Once this was installed, people began to understand that they could still use all of the applications they were used to using including WebSpere and Windows. PingFederate was critically important to the success of this project. PingFederate's ease of use removed the fear some people had and got the collaboration to happen," she said.

What's Next: The deployment of PingFederate and federated identity initiated serious and productive conversations about collaboration across the entire NY education system. According to Welch, people recognized and experienced that data synchronization using the School Interoperability Framework (SIF) currently deployed is not all that is needed. They quickly recognized that with federation, people can now work together, share applications that enhance their work, and cross-pollinate ideas and skills . "Identity federation has built community and enabled conversations to happen that have never happened among groups and people who should be collaborating," said Welch. "New possibilities and opportunities continue to open up."

T-Online Netzausweis: 2006 IDDY Award Winner

Deutsche Telekom AG, T-Com, dramatically improves the way services are accessed, simplifies Internet usage and reaches nearly 12 million customers with a new federated system.

Project Background:
T-Com launched "Netzausweis" (Net ID-Card) in 2005 to bring the benefits of federated identity management to its customers and partners. This Liberty-enabled federated system provides consumers with easy, secure and privacy-respecting access to applications, services, and partners with new opportunities for reducing costs and increasing revenues. The deployment supports nearly 12 million customers and over 200 products in the telecom and Internet service provider sector in areas such as gaming, Web-hosting, IP-TV and IP-Telephony. The

IDDY winner, Michael Gaertner from Deutsche Telecom AG, T-Com, Business Unit T-Online with Liberty's George Goodman

"Netzausweis" requires a Circle of Trust across all its partners: established in the context of the exchange of a user's personal data between the parties. Features include single log-in/sign-on, auto identification, overview, data vault, age verification and single log-out.

Objectives: To provide consumers with easy, secure and privacy-respecting access to applications and services. To provide partners with new opportunities for reducing costs and increasing revenues.

Bringing Identity Management to the Mass Market:
With "Netzausweis" T-Com brings the concepts and ideas of identity management to its partners and customers.

From the user's point of view this means:

- Easy-to-use
- Transparent
- Highly secure

From the content and service provider's point of view this means:

- Easy implementation
- Retention of customer ownership
- Reach is extended

From the identity provider's point of view this includes:

- Enabling T-Com to be an Identity Provider in Germany by means of introducing the "Netzausweis" as a service and authentication product for the end customer
- Introducing innovative identity management functionalities, such as service- and division-wide single log-in and single log-out, federation of accounts, and age verification for third parties
- The "Netzausweis" shall be based upon the "Liberty Alliance Project" standard, and embed business partners of T-Com as well as third parties

The Technology: The technologies used in the deployment are based on a well-defined architecture and standards:

- The "Netzausweis" functionalities have been implemented within the existing system architecture. Within that existing architecture a separate layer encapsulates the identity management functionalities called "AAA-platform."

- Opening the IDM functionalities to different partners and their systems in distributed system environments becomes a reality through defined interfaces called "reference points."

- The implementations of the "reference points" are based on open standards—Web-services based on SOAP/XML.

- In 2005 existing authentication interfaces were extended according to the Liberty Alliance standard ID-FF 1.2 (Identity Federation Framework).

Product interoperability is important, as it is fundamental to broaden the "Netzausweis" partner community:

- Without product interoperability the reach of the "Netzausweis" partner community would be limited by technical implementation needs.

- The extension of existing authentication interfaces according to the Liberty Alliance standard ID-FF 1.2 facilitates the connection to existing IDM-environments which are also ID-FF 1.2 conformant. For instance, connecting a partner who uses Sun Access/Identity Manager ID-FF 1.2 implementation to the SourceID-based ID-FF 1.2 implementation is NOT about complete integration, rather just configure-and-play.

- Liberty Alliance is a standard that helps T-Com's partners and itself to manage identities in distributed environments.

Benefits to Consumers: As an IDM solution designed for consumers, the "Netzausweis" delivers various benefits to the consumers—with one primary goal: "Simplify daily Internet usage."

From the consumer's point of view the benefits include:

- Single Log-in, Single Sign-on and Auto Identification: A user can then easily browse a large range of Internet sites
- Overview: Meaning having the capability to view all interesting information in one place—and navigate through a "personal Internet" with fewer clicks
- Data Vault: Type in personal information only once—and distribute it as liked and needed
- Age Verification: Access age sensitive content or services registering only once and using a known system—without special software/hardware
- Login Status: View actual login status—anytime
- Secure Single Log-out: Spanning all Netzausweis sites

The benefits could be summarized by the following statement: "With Netzausweis everything will be just a mouseclick away."

The ROI: The "Netzausweis" is a key business enabler:

- It allows quick and cost-efficient link-up with partners by usage of Liberty Alliance Project standards.
- It reduces the complexity of the IT-architecture, last but not least by use of modular software components.
- It allows the use of seamless services within the group Deutsche Telekom AG, the parent company of its business unit T-Online, as well as centralization of AAA-services on one single platform rather than implementing them separately within each business unit of Deutsche Telekom.

Addressing Privacy Concerns: This project improves privacy in a number of key ways:

- The Liberty Alliance specifications enable the storage of personal data transparent to the user. In the past, a user often was not aware of all the data he submitted to his numerous accounts.

- The user is assured that his credentials are stored only with the ID-provider he trusts and only provided to other providers by specified and consistent processes he can manage himself.

- Using one-off services a user does not need to reveal all his personal data as trust providers don't necessarily give away personal details in the Liberty Alliance context.

Exceeding Deployment Objectives: By establishing an IDM-solution package (not just single sign-on/log-in) the key objectives were exceeded — bringing additional value to T-Com and its partners:

- The "Netzausweis" enables partners to lower the hurdle of utilization for their end-customer's offers.

- At the same time, traffic can be raised and costs can be reduced. Through the "Netzausweis Überblick" (Overview) the partner gets the possibility to make available specific information to its users, without the user having to directly access the services of the partner.

- Based on a completed authentication solution, services can be used even better seamlessly and be connected with each other.

Protection Against Identity Theft: Protection against identity theft also improves with the new capabilities:

- The IDM based on Liberty Alliance makes it easier for the user to manage and use his credentials, most of which are either insecure and easy to hack, or cryptic and easy to forget. The problem of remembering different passwords has been addressed by only needing one set of credentials per customer. Therefore fewer identities and passwords will be written down. The danger of the passwords being compromised is therefore reduced.

- A consistent level of security, especially with the transmission of credentials, is implemented as the interfaces to the Liberty Alliance components are specified in detail and have to be considered by each and every application. In the past, many customers used the same password for different applications, so if one of them was compromised in a certain way due to weak security implementation of one application, the others were in danger as well.

2006 IDDY Award Winner:
UK Government's Gateway Project

The Government Gateway Service is the authentication server for all e-government services in the UK. The Gateway leverages open federation and interoperability of federation products to secure the electronic delivery of government services to citizens.

Project Background: The UK government is in the midst of a large scale e-government initiative. The Government Gateway is the authentication server for all e-government service access, on a national scale and some eight million registrations have been recorded. To date, adoption of e-government has been somewhat constrained by the difficulty service-user organizations were experiencing in writing to the existing authentication interfaces. The UK government sought to improve interaction through the application of the Liberty standards.

The IDDY and the E-government Squishy, a popular souvenir from the 2005 UK Local Government Conference

Objectives: This project greatly extends the potential for uptake of the Gateway's authentication service and has set out to meet three specific goals:

- Secure the electronic delivery of government services
- Enable single sign-on in support of "joined up government"
- Break down technical silos that were hindering "transformational government"

The project also extends the accessibility of Liberty standards, potentially into the whole UK local government market.

Core Deliverables: The core deliverables for this project were software modules which implemented the Liberty ID-FF and Web Services WS-Federation specifications. These modules were then added to the UK "Government Gateway" application—a centralised authentication server for UK e-government services. Release 1.6.8 went live in June 2006.
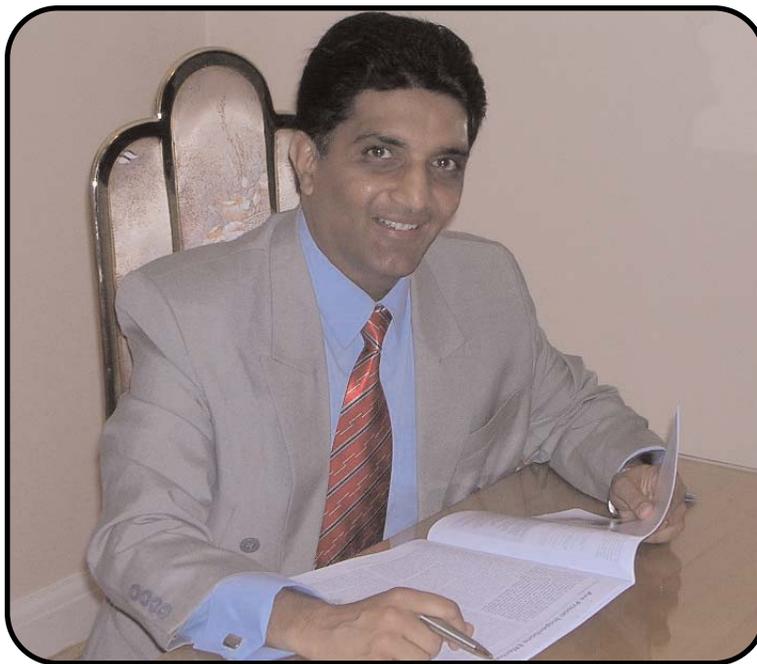
Citizen Empowerment: The Gateway authentication service is explicitly aimed at citizens (for example, authenticating in order to submit online tax returns). However, before this project, the citizen still had to sign on separately with each service provider. This project opens the way to single sign-on across participating central and local government organizations, whether these use ID-FF or WS-Federation as their authentication protocol. Now that Release 1.6.8 has been launched, the Cabinet Office have begun to advertise its availability to UK citizens via the Radio and Television media.

Technology: The Gateway server application is written in Microsoft BizTalk and implements a proprietary authentication protocol to a back-end database. This was perceived by the target user communities as overly hard to write to, and was not supported by mainstream off-the-shelf products. As a result of this project, the Gateway now exposes Liberty and WS-Federation interfaces.

Looking at ROI: The key strategic ROI for this project was that it supplemented the existing (proprietary) Government Gateway authentication protocol with two industry-standard protocols, Liberty

and WS-Federation. This has two effects: first, it demonstrates the Gateway's ability to support interoperability of the two protocols; second, it gives the 'customers' of the Gateway (including all UK local government authorities) the option to use off-the-shelf products that support the Liberty ID-FF protocol.

Helping to Prevent Identity Theft: Today, the local authorities can more easily use the Government Gateway as a centralized authentication service and there is less need for each authority to develop or implement its own secure authentication mechanism. In the UK, local authorities are under constant budgetary pressure, and frequently cut or out source IT services based on cost—which in turn often reduces the effectiveness particularly of IT security measures. This project provides local authorities with a single, consistent and robust security mechanism at minimal cost and effort on their part.

Sun Microsystems Bipin Dattani, a key figure in the UK Government Project

Addressing Privacy Concerns: This project is primarily aimed at the G2C segment rather than consumers. However, in the local government market the line between citizen and consumer is often far more blurred (for example, in the provision of contracted-out leisure services). Potentially, easier access to the Government Gateway for authentication could be used to improve the online security of these public/private sector partnerships.

The IDDY's Impact: The UK government is now beginning to inform the UK citizens of the availability of this gateway through radio and TV advertisement. "Winning the IDDY Award will act as a serious 'shot in the arm' for this campaign and help the on-going adoption of this much needed service," said Sun's Bipin Dattani.

Meet the IDDY Artist:
Kristian Iglesias at Work

Finding the right artist to create the actual IDDY Award was a critical step in the overall development of the IDDY program.

Kristian Iglesias constructing the IDDY

"We wanted an award that would convey the magnitude of identity," explained Britta Glade, director of marketing, Liberty Alliance. "How do you capture and convey 'identity' and everything it is for individuals and organizations working with those individuals to maintain privacy and security? It's a tall order, and we needed some artistic creative genius."

Enter Kristian Iglesias, an artist and designer based out of Greenport, New York, on Long Island's North Shore. Kristian specializes in custom furniture, sculpture and prototype objects. He works with bamboo, wood, metals and found objects. And his work is strongly influenced by Asian culture.

"Kristian was extremely good at listening to what we wanted to convey," explained Glade. "From his work with other clients, we knew that Kristian had a lot of breadth and depth to his approach—all of it illustrative of the message he was trying to communicate. So we gave him 'artistic liberty' to create a plan for illustrating the IDDYs."

Kristian immediately "got" what Liberty was all about and the Liberty marketing team was captivated by his initial set of ideas. "I was inspired by what federation accomplishes and how it connects different individuals and companies," Kristian said.

"My original idea was to use a group of varying sized metal pieces, representing differing sized companies, wrapped together by rings to symbolize trust. The concept then progressed to be a more organized and structurally solid composition, composed of varying sized brass pieces. I felt that trust was better symbolized by something that was more solid, but totally connected together."

The final design featured brass and bronze rectangular pieces stacked to 12 inches. "I favored using brass/bronze because it is visually stimulating as it is able to hold a great variety of patinas which I thought was essential to compliment the wide variety of industries that Liberty has an impact on," Kristian said.

The artist at his boatyard studio

Once a final design was agreed upon, Kristian got to work fabricating the IDDYs in his shipyard studio located on quiet harbor on the Peconic Bay. "To me, it was interesting to be working on this particular project in an old boatyard," he said. "In my studio, I'm surrounded by structures and tools used to build boats back to the 1800s. Boats were the vehicles for commerce back then, sort of like how federation and identity standards are the vehicles and promoters of commerce now."

Within a few weeks, he had the final product ready to ship to the IDDY Awards ceremony. "I finished and sealed the sculpture with the old and natural method of using wax," he explained. "It brings a warmer feel to the sculpture, than spraying it with some sort of polyurethane. It was of also honoring the past."

The marketing team was thrilled with the final product, as were the recipients. "The awards are definitely solid," said Britta. "When we presented them at DIDW, we had many admiring compliments about the 'solidity of trust' that was conveyed through them visually. If I could capture in a word the driving principle of Liberty it would be that— 'trust'— and trust must be built upon a solid foundation with privacy and security. Kristian did a beautiful job of capturing what we are, what we offer to the marketplace, and the phenomenal deployments that our winners have achieved in meeting the individual needs of their various constituents."

For more information on Kristian's work, email kaidesign1@yahoo.com

About the Liberty Alliance Project

The Liberty Alliance Project (www.projectliberty.org) is a global alliance of companies, non-profit and government organizations developing open standards and business, policy and privacy guidelines for federated network identity. Federated identity offers businesses, governments, employees and consumers a more convenient and secure way to control identity information and is a key component in driving the use of e-commerce, personalized data services and identity-based Web services. Liberty specifications are deployed worldwide by organizations that include American Express, AOL, BIPAC, Ericsson, General Motors, France Telecom, Nokia, NTT and Sun Microsystems. Membership is open to all commercial and non-commercial organizations. A full list of Liberty Alliance members, as well as information about how to become a member, is available at **www.projectliberty.org**