A Trust Network to Support Children

*Enabling children, educators, parents and caregivers to collaborate and share sensitive information across the Web.*

produced by National Laboratory for Education Transformation & Resilient Network Systems
A Trust Network to Support Children

Enabling children, educators, parents and caregivers to collaborate and share sensitive information across the Web.

To foster the well being and education of children, NLET and Resilient Network Systems are proposing to create a Trust Network that will enable children, educators, parents, and caregivers across public and private organizations to collaborate and share sensitive information with confidence across the Web. This Trust Network to Support Children will enable responsible and appropriate sharing of information amongst those working to help a child: their parents or guardians; school officials; social and health-service government agencies; and if required, juvenile justice officials. This network will also advance the availability and effectiveness of online learning by providing personalized yet privacy-protecting rights management, so children can conveniently, and anonymously, access online content or services from multiple sources via any of their devices.
Problem Statement

At-risk children often require combined support from educational, social, health and even criminal justice organizations. Unfortunately, there are both technology and privacy barriers to sharing the appropriate data about these children with the adults who are providing these services. These supporters and the children themselves are forced to wait for information requests to be processed manually, to ask and answer the same questions again and again, and to operate with incomplete understanding about what is happening in these children’s lives.

These same barriers limit children’s access to online learning tools; reduce existing services’ effectiveness by preventing optimal personalization based upon each child’s personal and historic information; and practically outlaw services that could analyze children’s data across systems to identify and solve education challenges ranging from individuals to populations. Traditional approaches to access control and privacy cause these other online services to widen educational systems’ exposure to hackers and increase the probability of breaches, both in those systems and in other systems the children access.

Background

The National Laboratory for Education Transformation (NLET), www.NLET.org, and Resilient Network Systems, www.Resilient-Networks.com have partnered to provide a best of breed solution for the trusted identity, access, privacy and security issues faced by children and their caregivers from educational, social, health and criminal justice agencies.

NLET is a Silicon Valley based non-profit, devoted to transformative solutions to persistent education problems. Founder Gordon Freedman has a background in education technology. NLET runs a joint center with University of California Santa Cruz, which is committed to better social outcomes through data analysis. Resilient Network Systems is a San Francisco and Washington, DC based for-profit corporation, delivering Trust Network platform with software and delivery services to federal and state law enforcement, as well as healthcare and education organizations. Resilient’s CEO, Richard Spires served as the Chief Information Office for Homeland Security and Deputy Commissioner for the IRS.

A Past Pilot Demonstrated Trust Network Capabilities in Education

Resilient Network Systems and NLET were awarded a grant for 2012-2014 from the National Institute of Standards and Technology (NIST) to support the National Strategy for Trusted Identities in Cyberspace (NSTIC). The pilot leveraged a Trust Network to coordinate interactions among parents, students, educational institutions, and media providers to address the online safety and security of children. During the pilot, participating parents, children and educators were able to use online services connected by Resilient’s Trust Network platform to communicate and access online learning content, while in compliance with the Family Education Rights and Privacy Act (FERPA) and the Children’s Online Privacy Protection Act (COPPA), based on their affiliation with school districts or their family relationships. Pilot participants included: the Pajaro Valley Unified School District in Watsonville, CA; the Riverside Unified School District in Riverside, CA; along
with technology and data service providers, such as the Kantara Initiative (nonprofit organization working to support more natively trustworthy on-line experiences), Sungard (school information system and parent portal provider), Clever (attribute provider recognized as a nation wide player in education), Authentify (out-of-band phone authentication service), and Knowledge Factor (relying party for online learning programs).

Access, Privacy and Security in Education and Social Services Delivery

As more of the functions of daily life rely on the Internet and mobile networks to move data, transactions and interactions, the needs for privacy, security, access control, and authentication of users multiply.

While commercial and consumer activity and personal information on the Internet are continually susceptible to sophisticated hacking and theft, the solutions for control and safe-keeping of identity and information in the healthcare, education and social agency environments, and between these social and personal segments, ought to be held to higher standards to comply with multiple existing regulatory frameworks (e.g. FERPA, COPPA, HIPAA) governing their data. However, to date, such solutions have relied on two factors: (1) low-security information access and privacy protection; and (2) numerous, uncoordinated authentication and access systems from multiple product vendors.

In general, the incentives to break into social, education and healthcare systems have been much less than to steal commercial and consumer information that leads to financial gain by perpetrators. However, breaches are not uncommon in education, healthcare systems, and in some social systems. These are generally less reported, because their scale and the consequent damage are less clearly understood than with commercial accounts and consumer information. Particularly in education, students with technical expertise, but not necessarily with criminal intent, routinely breach student information systems (SIS).

The threat exists that sophisticated hacking could lead not just to isolated breaches, but to larger-scale use of information to aggregate profiles across education, healthcare and social agencies that may be combined with consumer and commercial data. In other words, routes into personal information typically find entry points via less monitored systems. This threat is weighed against the need to use education, social and criminal justice information, across multiple agencies, to serve families and children in need of multiple services, which, in today's practice, are generally not coordinated.

Coordinated service delivery from multiple agencies and institutions is hampered by inefficient, heterogeneous, and largely low-security access control and privacy protection. At the same time, access to such data is subject to multiple compliance regulations and laws. The lack of technical coordination conflicts with agencies' stringent compliance requirements, making it difficult to both safeguard a child or family's privacy and, at the same time, create an environment that provides support and coordinated assistance.

Security vs. Service

Thus, the trade off between security versus service is present in education and social services on a daily basis, with the general result that security is given a higher
Ironically, the level of security of education systems is actually low compared to the legal requirements for their safekeeping.

When analyzed, it is clear that while there are compliance mandates and laws, system compliance and product safeguards are actually quite low and, for the most part, not monitored. Healthcare, by contrast, is heavily monitored and has a great deal of investment focused on the problem.

It is a common frustration in education and other social services that there are multiple logins and authentications necessary for processing routine data and information, which results in poor security practices and low barriers to breach. The problem is that education and social services generally require access to multiple heterogeneous data sources that are inconvenient to access singularly, but these data are necessary in order to succeed in coordinated service delivery to children and their families.

A Trust Network to Support Children

A Trust Network to Support Children will address a key national concern: to ensure all children have access to personalized educational, social and health services that are coordinated to meet their needs and prepare them for success, while also protecting their privacy by only sharing relevant information with authorized educators, parents, public services and online learning organizations. Providing personalized services and secure, blended and online learning opportunities requires an innovative technology approach that accounts for varying users and systems with uncoordinated methods for sharing information. A Trust Network to Support Children will provide a common infrastructure for identifying users or exchanging data across multiple applications and organizations (e.g. student information systems, public data systems, online learning services), as well as enabling all of these services to comply with their regulatory requirements for security and privacy.

As shown in the figure above, NLET and Resilient Network Systems will work with government
agencies and online education providers to establish a trust framework of required policies and a network of identity services for on-demand, multi-factor authentication and identity verification of children, parents, teachers and staff, along with other caregivers and government personnel. Data shared among these services will rely upon network-based “privacy services” for accessing school enrollment, student information, and/or insurance or healthcare databases.

The Trust Network Platform

The Trust Network to Support Children will extend FERPA and COPPA compliant communications and data access to parents, children and other authorized caregivers via email and web-portals. It will support privacy by aligning with Fair Information Practice Principles, while enabling FERPA-compliant record matching and linking across multiple data sources, suitable for enabling child-centric analytics in support of personalized online education and performance assessments. Also, a Trust Network to Support Children will provide services that support online rights management enforcement to authorize access by parents and children to online content, based on their family relationships and schools attended.

To enable people and organizations to share better, faster and more cost-effectively, Resilient Network Systems, Inc. has created the Trust Network platform to address the urgent need for ubiquitous trust management at Internet-scale. The Trust Network platform serves as middleware to coordinate interactions among users, the online resources (e.g. applications, databases) that users are trying to access, and the existing authorities (e.g. user identity directories, multi-factor authentication services) that can verify users’ identities and their rights to access those resources.

By enforcing the resource owners’ policies for authorized access, while also protecting the privacy of users’ identities, the Trust Network platform supports collaboration and connection without giving up control or compliance. The Trust Network platform is designed based on the following five principles:

■ **Common Language** - Policies and credentials are expressed in common, simple, interoperable and human-readable form.

■ **Neutrality** - The network neutrally enforces whatever policies each party has published to protect the
resources it is making available, whether they are applications, websites, or data contained in databases or individual records.

- **Flexibility** - A flexible set of Trust Network extensions enables use of existing identity management systems, attribute authorities, and resources capable of providing context.

- **Local Control** - Each participant in the Trust Network determines the policies and decisions upon which it shares resources and services.

- **Interoperability** - Enables many different applications, with widely varying policy requirements, to share a common infrastructure for trust management, and to generate complex, multi-party user experiences without requiring consensus by all parties.

Resilient Network Systems has invented a new type of Internet infrastructure that is the core component of the Trust Network platform. This forms an open and secure network with a technology and vendor-neutral architecture, allowing disparate standards and systems to be linked together and leveraged, while maintaining privacy and security. To support network adoption and scalability, there is no central point of control of the network. Each Trust Network component can be replicated to the degree necessary to support all Trust Network participants. All network nodes are peer-to-peer software components that can be easily installed in a participant’s environment or hosted by cloud infrastructure providers.

**USE CASE 1: Multi-Caregiver Online Access for the Benefit of an At-Risk Child**

This child-centric case demonstrates capabilities for teachers, social workers, healthcare professionals, etc. to have limited access to an at-risk child’s records, which are necessary for each of caregivers’ support. Using services on a Trust Network to Support Children, these caregivers will be empowered to conveniently and transparently access the child’s records contained in multiple systems from multiple organizations (e.g. SIS, social work, juvenile justice) where these records already exist. Caregivers’ access will be authorized by verifying their professional credentials, organizational affiliations and the context of their responsibilities to support that child during a specific time, case, etc. The child’s records will remain in their existing systems, and caregivers’ identities will be verified in their existing systems, rather than aggregating all of the data into a new system with new identities.
USE CASE 2: Authorized Access to Online Education Content and Applications

This use case demonstrates convenient on-demand, single-sign-on access to online educational content by children, parents and teachers based upon their affiliation with a school or district. A child’s school ID can be verified by this Trust Network, while providing minimal data about the child to the content providers’ websites and applications. These capabilities ensure schools, districts and children can reduce their challenges to access new educational sources, while also supporting all parties’ compliance with the latest privacy requirements and regulations.
About the National Laboratory of Education Transformation (NLET)

On the cutting edge of knowledge technology and education, the National Laboratory of Educational Transformation (NLET) serves as the liaison between technology and education communities. NLET is a non-profit organization founded to apply scientific expertise, new methods, and better tools to improve the structure of education and the culture of learning in the United States. NLET was created in response to an education system that now appears designed and developed for an earlier era, an era in which a more structured manufacturing economy required a highly organized, predictable and stratified workforce. Now, in the 21st century economy, we perceive that societal and information transactions have evolved well beyond what the old education model was structured for. We therefore believe it is time for education to reorganize and leverage the vast amounts of knowledge available through technology. NLET’s goal, as stated throughout www.NLET.org, are (a) to foster individual learning, (b) to promote greater education system efficiency and (c) to improve access to knowledge for both learners and educators. Identity security for learners is therefore critical to NLET’s mission.

About Resilient Network Systems, Inc.

Resilient Network Systems has built and launched the Trust Network platform, to address the pressing need for secure and privacy-protecting access across the Internet. The Trust Network virtualizes real-world relationships and conditions of trust by confirming identities within the network, and enforcing each participant’s resource access policies while divulging the minimum required personal information. Both sides of any type of access, data sharing, or transaction event develop higher levels of trust due to improved authentication of each party and adherence to each other’s policy requirements.

Resilient is based in San Francisco, California and maintains a second office in Washington, DC. The initial funding has allowed the core technology to be designed and built, initial revenues to be generated, and for three initial pilot implementations with large potential customers to be completed. The first production instance of the Trust Network supports more than 300 law enforcement organizations in Northern California. Learn more at www.resilient-networks.com.