Trust Network as a Service (TNaaS)

April 2015

Resilient Network Systems
100 Pine St, Suite 700
San Francisco, CA 94111
Telephone: (415) 291-9600
www.resilient-networks.com

The Challenge

In today's competitive environment, industries are embracing the move toward SaaS to increase agility, improve customer experiences, work more effectively with suppliers, and provide more up-to-date information and responsiveness to sales and distribution channels. Whether an organization maintains its online presence via its own IT infrastructure or makes use of commercial cloud services, proper access control to shared applications and data is of critical importance. In this new model, an organization's capabilities must address adaptive access control for employees, as well as provide access for external users such as customers, suppliers, and distributors.

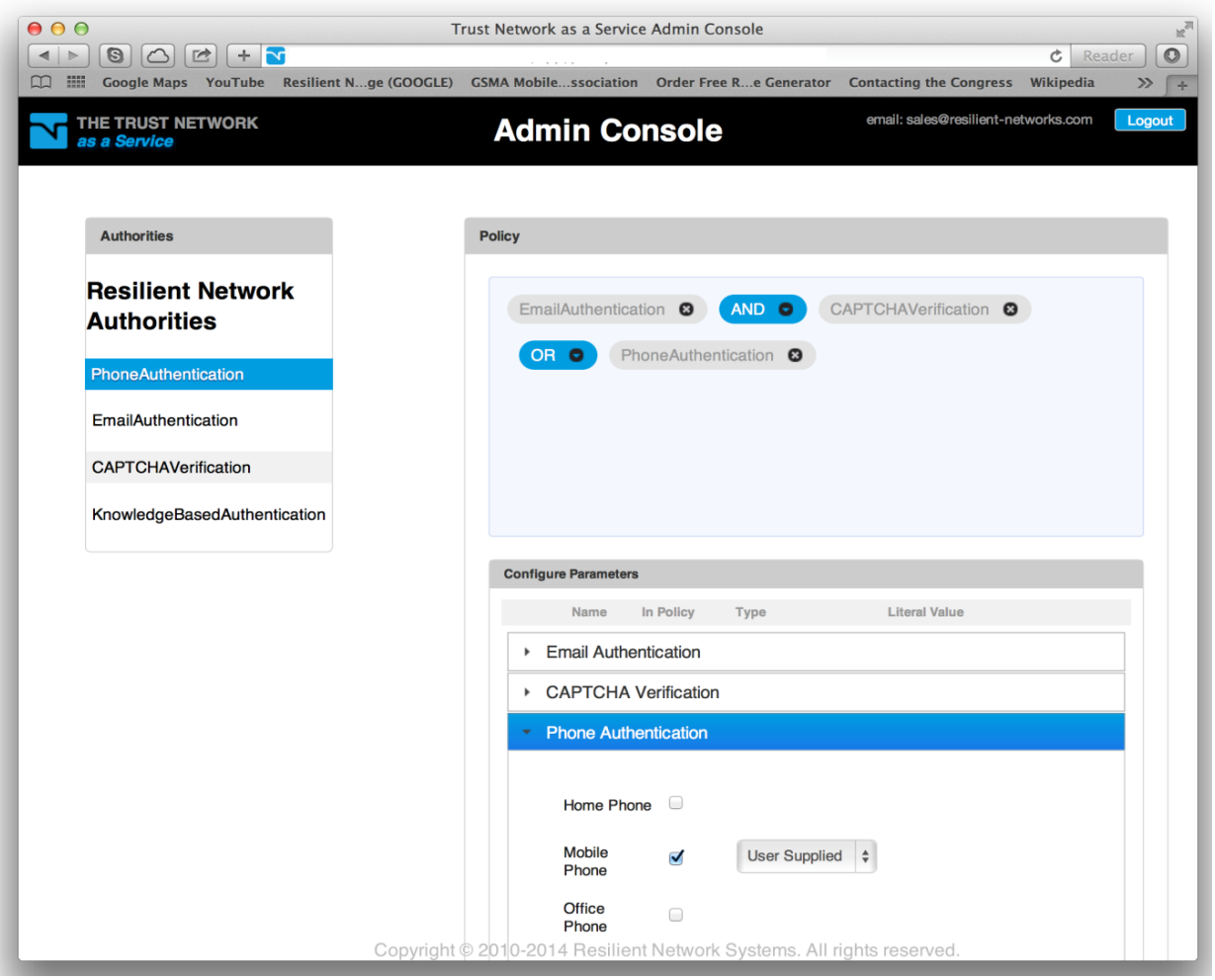
This drive for greater online access by external users presents significant challenges for organizations. Certainly there are greater security risks, as the attack surface grows with the requirement to provide access for users from other organizations. Further, to the degree an organization is holding and using personally identifiable information (PII), privacy issues become significant, and there can be tremendous liability to the organization in the event of a breach and exposure of stored PII. Lastly, legacy applications have typically embedded access control logic in the application, making it difficult to easily adapt access control to external identity stores, thus creating a set of stovepipes for users to deal with when accessing multiple applications.

In response to this set of challenges, Resilient Network Systems has developed Adaptive Access Management solution to enable "trust management", the next generation of identity and access management. Our network-based solution can enable the sharing of distributed data and applications, personalization of content for unknown users, and enforcement of granular privacy, security, and regulatory policies. RNS enables trusted interactions among people, organizations, and the multitude of online services and applications. Resilient offers TNaaS, an easy-to-configure cloud-based instance of the Resilient Adaptive Access Management in a multi-tenancy environment that enables organizations to rapidly leverage enhanced safeguards and privacy for conducting online interactions.

The Value Proposition

With TNaaS, an organization can easily configure multi-factor access control to its online resources, including applications, websites or webpages, and data. Through the use of an administrator's toolkit, organizations can establish access control for online resources in a matter of hours, in ways that match the organization's policy requirements for identity verification, authentication, authorization, and context. TNaaS ena-

bles an organization to rapidly and easily leverage existing authoritative identity and attribute sources, whether they are internal or commercial sources. With authentication and authorization functions carried out in the network, there is no need for the organization to hold the user's personally identifiable information (PII), both protecting the privacy of the user and the organization.



Authentication and authorization for an organization's online resources is just one facet of Resilient's capabilities. Organizations can also leverage the policy engine of the Trust Network to handle online interactions based on context, to include environmental attributes, regulatory or legal requirements, or factors related to specific events. As long as the decision data is accessible on the network, and policies can be expressed in Boolean logic, TNaaS can provide the mechanism to effectively handle the interaction, all while protecting the privacy of each organization and individual involved.

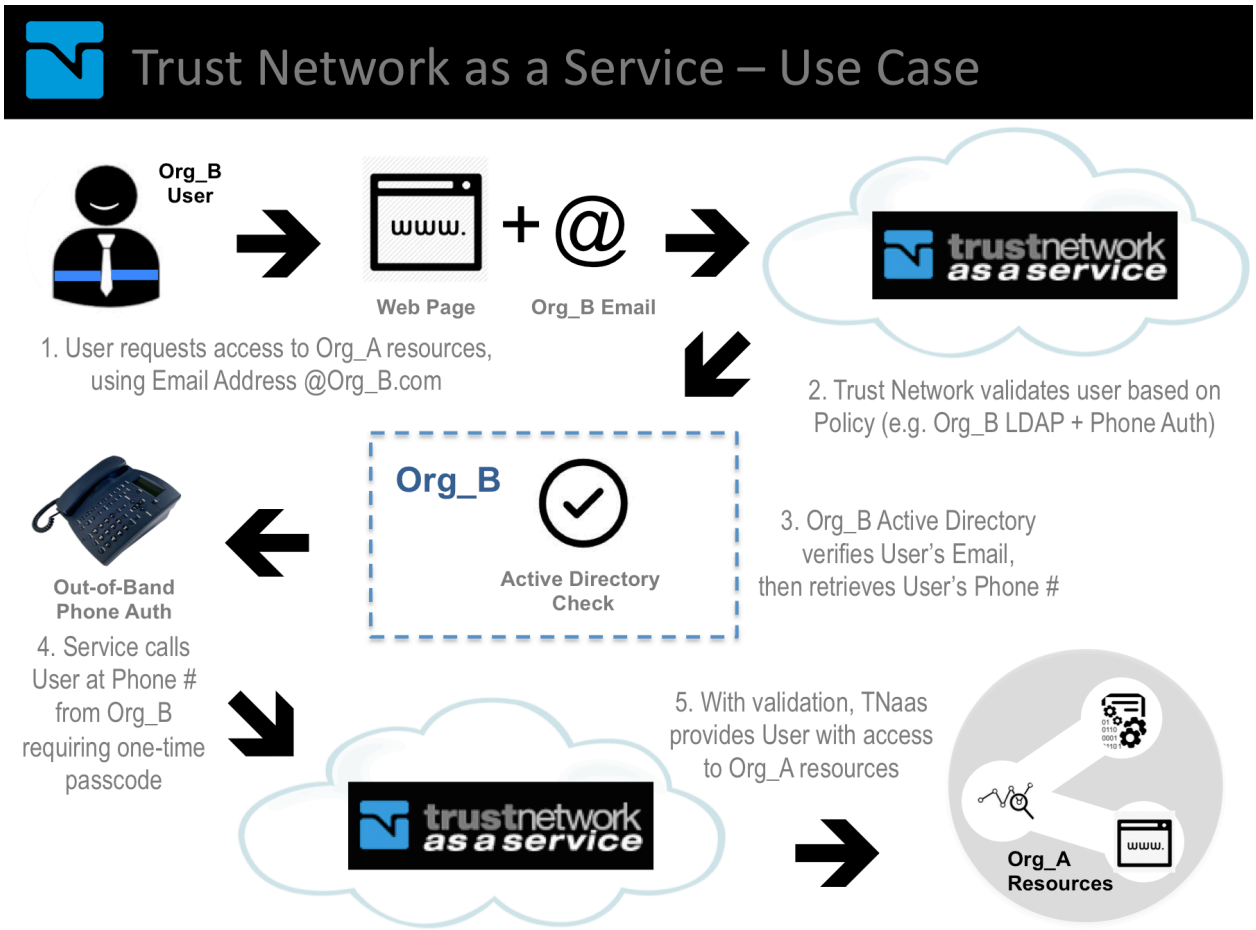
Example Use Cases

To ease the creation access control policies for an administrator or developer, TNaaS offers an easy-to-use, graphical user interface. The administrator can use the TNaaS Administrative Console to call upon standard, existing authorities or create new authorities for use in authenticating and authorizing users (e.g., an organization's Active Directory or user attribute store). These authorities can then be combined to create sophisticated access control policies, using Boolean operators (e.g., AND, OR) within the simple drag-and-drop interface provided as part of the TNaaS Administrative Console.

TNaaS can be used to provide access control directly for web applications, web pages or web-addressable data and documents. All of these capabilities are available and can be configured via the TNaaS Administrative Console. For instance, a simple cut and paste of the Trust Tag generated by the TNaaS Administrative Console into the top of a web page's source code instantly makes the access to the page protected by the policy configured in TNaaS. An example would be an administrator adding in a second factor of authentication to a web page by using TNaaS to configure a policy to invoke an out-of-band e-mail, phone call, or SMS text, or even to do a voice biometric check.

In addition to enhanced authentication, TNaaS can be used to securely retrieve attributes from any defined authoritative data source and use these attributes in the evaluation of a policy. As an example, a company may keep a supplier list in an internal application, and enable certain representatives of suppliers to have access to sensitive company data via a specific web application. TNaaS could be configured to first authenticate a supplier's representative via the supplier list and perform a second factor out-of-band phone authentication using the phone number contained in the supplier list. A further refinement of this example would be a case in which a supplier's representative, after the two-factor authentication, is only authorized in the application to access data specific to that supplier.

As a final example, the figure below shows how Organization A can use TNaaS to enable access to an online application for external users from Organization B. With approval, an administrator can add Organization's B Active Directory (via LDAP) as an authority available on the TNaaS. The administrator can then construct a policy such that when users from Organization B attempt access to Organization A's protected application, the access relies on authenticating the user via Organization B's LDAP. Further, an out-of-band phone authentication is used as a second factor for authentication, using the phone number that resides in Organization B's Active Directory. In this example, Organization A does not hold or manage the PII of users from Organization B, yet a strong multi-factor access control is used for access.



About Resilient Network Systems, Inc.

Resilient Network Systems makes adaptive access management software for identities you don't (or can't) manage. Our network-based, distributed architecture is highly flexible and scalable, allowing customers in government and enterprises to safeguard their data and applications, while enabling more collaboration and information sharing with their entire ecosystem. We make it simple to leverage existing identity and security products, or add external identity sources and services, with easy-to-implement, predefined and custom policies. Resilient Network Systems is a privately held, venture-backed company based in San Francisco.