Federated Trusted Network Connect (TNC)
FAQ
May 2009

Q1. What is the purpose of Federated TNC?
A. The goal of Federated TNC is standardize the expression of endpoint posture information, and the methods of its communication between security domains, using the OASIS Security Assertion Mark-up Language (SAML). This allows information about device identity and/or health to be conveyed from one organization or server to another.

Q2. What does Federated TNC define?
A. Federated TNC defines three new profiles of SAML:

- The Roaming Assessment Profile
- The Web Assessment Profile
- An FTNC Attribute Profile

Q3. How can Federated TNC be used?
A. The Roaming Assessment Profile is intended for use in scenarios where endpoints roam between networks that are operated by different organizations. The Roaming Assessment Profile enables a 'host' network operator to make richer authorization decisions, using posture information collected by the roaming endpoint's 'home' operator, about roaming endpoints. An unhealthy endpoint may be quarantined, for example.

The Web Assessment Profile is intended for use in scenarios where a web application requires information (such as posture information) about the endpoint that a browser is operating on. The Web Assessment Profile enables the web application to make richer authorization decisions about endpoints, using posture information collected by the visiting endpoint's security domain (for example, the corporate customer of a Software-as-a-Service provider), about connecting endpoints.

Q4. Can Federated TNC express other information in addition to endpoint posture?
A. Federated TNC is not constrained to the expression of endpoint posture. Federated TNC can be used to express arbitrary attributes about an endpoint and arbitrary attributes about the user associated with the endpoint or browser.

This facility can be used, for example, to allow a roaming network operator to make an authorization decision on the basis of user attribute information. For example, in the case of the Roaming Assessment Profile, this could be used to indicate that a roaming user subscribes to a 'premium' or 'standard' network service, or that the user is under the age of eighteen.

Q5. How does Federated TNC complement the TNC architecture?
A. Prior to Federated TNC, the TNC architecture did not address scenarios in which an endpoint associated with a security domain could be assessed by one or more other security domains (for example, two or more distinct organizations).

Federated TNC is most useful in scenarios where there exist two or more distinct organizations that engage in RADIUS-based roaming or SAML-based Web Single Sign-On (SSO) federation.

Q6. Does Federated TNC require changes to the client?
A. No, Federated TNC was designed to avoid any software changes to the client. The Roaming Assessment Profile will work with any standard 802.1X supplicant. The Web Assessment Profile will work with any HTTP/1.1 browser.

Q7. What relationship does Federated TNC have with other standards?
A. The Roaming Assessment Profile leverages RADIUS (or the emerging RadSec standard, if a high level of security is necessary) to federate, using conventional proxy functionality, EAP-based authentication and TNC-based posture assessment of roaming endpoints. The SAML 2.0 Assertion Query/Request Profile, or alternatively the Shibboleth Attribute Exchange Profile in SAML 1.1 deployments, is used to transmit endpoint posture and user attributes.

The Web Assessment Profile builds on the SAML 1.1 and 2.0 Web SSO Profiles. The SAML 2.0 Assertion Query/Request Profile, or alternatively the Shibboleth Attribute Exchange Profile, is used to transmit endpoint posture.

Q8. Who benefits from Federated TNC?
A. Users benefit from improved assessment capabilities for their endpoints, increasing the security of their information and systems. Users may also benefit through additional or richer services, if the host organization is able to achieve a higher level of trust in the user and/or endpoint on the basis of the attributes provided by the user's home organization (for example, a network operator may open more network ports to an endpoint that satisfies a local network security policy). Users may also benefit from 'simplified' or 'single' sign-on.

Host organizations benefit from the ability to request and obtain (subject to the home organization's privacy policy) information about endpoints and users affiliated with other organizations. This information could be used to determine the security posture of an endpoint, or other technical properties (such as its operating system), or other information about the user.

Home organizations benefit from improved security of its endpoints (for example, by the ability to assess an endpoint while it is roaming) and the potential to offer its users additional or richer services that leverage the information made available by the home organization.

Home and host organizations both benefit from the ability to re-use, and extract further value from their existing investments in TNC and SAML related technologies.

Users, home organizations and host organizations all benefit from the privacy benefits realized using federation technology (see below).

Q9. How does Federated TNC protect privacy?
A. Federated TNC helps protect privacy by avoiding the need for Relying Parties (such as roaming network operators) to establish a direct relationship with the endpoint or user affiliated with its federated organization(s). Endpoints and users are always authenticated and/or assessed by their 'home' organization.

The home organization can then choose to release (or not) the information required to satisfy the authorization policies of the federated organization(s). The host organization receives only the information that it requires, and no other personal information that might subsequently become a legal or reputational liability if its own systems are compromised.

Q10. How widespread is implementation and adoption of Federated TNC?
A. Federated TNC is still a new specification so implementation and adoption are just beginning. However, SAML is widely implemented and deployed. Organizations that have implemented or deployed SAML can add support for Federated TNC fairly easily. Since device health is a considerable worry in today's network security environment, we expect adoption of Federated TNC to move swiftly.

Contact: Anne Price, TCG market communications
anne@prworksonline.com
1-602-840-6495