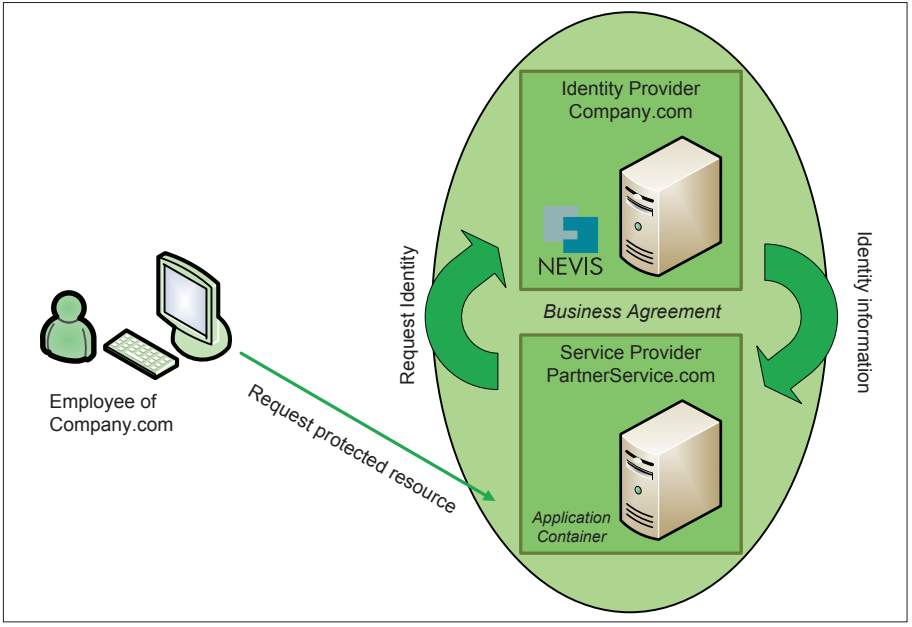
Josua Trösch

Identity Federation with SAML 2.0

Graduate candidate	Josua Trösch
Examiner	Prof. Dr. Andreas Steffen
Co-examiner	Prof. Dr. Ralf Hauser, PrivaSphere AG, Zürich
Subject area	Internet Technologies and Applications
Project partner	AdNovum Informatik AG, Zürich

Nowadays IT systems are no longer isolated entities, but rely heavily on information exchanged with other systems. Usually, authorization verification needs to be completed before access is provided to another system's data. Nevis is a security infrastructure for the protection of sensitive data, services and applications. It is developed and maintained by AdNovum Informatik AG. Like many other vendors of security software, AdNovum has implemented a proprietary protocol and format to provide security information over network connections. As more and more Internet services have started to collaborate, the need for an open standard to describe and exchange security information has emerged. The SAML 2.0 standard serves this need by providing a suite of protocols and message formats to describe and exchange security information.

In a first phase of this thesis, an overview of current support of the SAML 2.0 standard by various software products was compiled. The two application containers BEA WebLogic and IBM WebSphere include broad support for the SAML 2.0 standard. JBoss currently provides support for the SAML 1.0 standard. The open Java and C++



Identity Federation Use Case

library OpenSAML 2.0 provides Software developers with functionality for validating and handling SAML 2.0 XML documents and supports various profiles and bindings.

In a second phase, selected features of the OASIS SAML 2.0 standard were implemented into AdNovum's Nevis framework. The Nevis framework was enabled to handle SAML 2.0 Authentication Requests. Based on the specific Request, a SAML 2.0 conforming Response is composed and sent back to the requesting service. If access is granted, this Response contains a SAML 2.0 Assertion with the requested security information to log a user into the remote system. Performance and profile conformance were tested against a BEA WebLogic Server instance. The implementation has been merged into the Nevis Framework and can be used in future projects.