VERGIC SYSTEM INTEGRATION
Single sign on using SAML2

Technical documentation (Supplement)

1 Document history

Version	Date	Author	Note
0.5	2015-02-06	Roger Månsson	Created
0.6	2016-02-09	Esben Carlsen	Complemented
1.0	2018-06-27	Anders Hellström	Updated

2 Table of content

3 Introduction

3.1 Intention

This document aims at describing the and single sign on interface (SSO) provided by Vergic for associated partners and customers who wish to integrate their systems with VEP (Vergic Engage Platform). The intended audience is technical staff external to Vergic. It describes the system-level communication workflows and technical contracts.

3.2 Terms and Abbreviations

The primary users of the overall system functionality are the contact centre agents, referred to as *agent* here. The other party to the agent is seeking contact and is referred to as *visitor* here. The dialogue of chat messages between agents and visitors is referred to as *conversation*. A competence group is a logical set of agents, usually sharing the same business competences. Such a competence group is referred to as *group*. A *queue* is an ordered list of visitors assigned to a group, often depending on the visitor's entry point. A CRM system is a Customer Relations Management system, keeping track of information known about a customer, including what interactions have occurred with a particular customer.

Abbreviation	Explanation
VEP	The Vergic Engage Platform
Partner System	The system connecting to VEP through this API
SSL/TLS	Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), both of which are frequently referred to as 'SSL', are cryptographic protocols that provide communications security over a computer network.
GUID	A globally unique identifier (GUID) is a unique reference number used as an identifier in computer software.
Agent	Contact center agents; the primary users of the overall system functionality
Visitor	The other party to the agent seeking contact from the web site
Group	A logical set of agents, usually sharing the same business competences
Queue	An ordered list of visitors assigned to one or more groups, often depending on the visitor's entry point or visitor attributes
Conversation	The dialogue of chat messages between agents and visitors

Case	An overall grouping of events, participants, time stamps and other meta data related to conversations
SSO	Single sign-on is a property of access control of multiple related, yet independent, software systems

4 Business Use Cases

The purpose of this integration is to accomplish the business use cases described in this chapter.

4.1 A Partner System needs to enable SSO with VEP using SAML2

Partner system needs a seamless way for agents to log-in into VEP if they are already logged-in to Partner System, essentially SSO solution and using a SAML2 token as base. Vergic implementation of SAML2 is based on a template from Microsoft as used in ActiveDirectory Federated Services (ADFS).

5 Technical Requirements

Partner System shall provide Vergic with information to be able to trust the external SAML token provider.

6 Integration Model

6.1 SAML 2.0 Metadata

SAML 2.0 Metadata is an XML document describing SPs and IdPs.

The metadata for Microsoft's SP can be retrieved from the following URL: https://nexus.microsoftonline-p.com/federationmetadata/2007-06/federationmetadata.xml

6.2 Information needed from customer or partner

Setting up SAML2 based SSO requires users to be created and assigned roles in VEP. When this is done, user will be matched on email, a parameter in the SSO token.

To be able to access tokens Vergic needs information from the customer/partner system. This information can be extracted from the SAML metadata file.

When setting up the SAML trust, the customer will normally send a URL to the metadata XML file, or the actual file, to Vergic. The SAML issues system will also need some information from VEP. This is described in the chapter below.

The partner system does not need to trust VEP.

6.2.1 Application Endpoint URL (SAML)

This is an example of the information/settings that Vergic typically will provide the customer/partner with.

Relying Party Identifiers
URL:

Application Endpoint URL (SAML)
URL:
Endpoint Type: SAML
Assertion Consumer Binding: POST

Secure Hash Algorithm: SHA256

Requested Claims: We recommend UPN

Token Encryption Certificate: No

Multi-Factor Authentication: No