SiLA 2 Part (C) - Standard Features Index

Release v1.0 - 30 September 2019

© 2008-2019 Association Consortium Standardization in Lab Automation (SiLA)

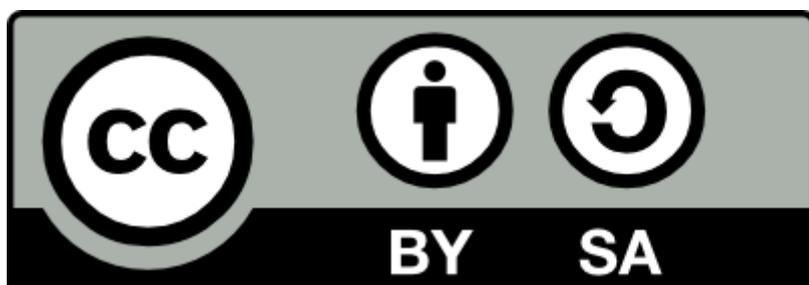http://www.sila-standard.org/

Notices

License

SiLA 2 Version History

For the version history, please refer to Part (A) (Current Version).

Refer to the Structure of the SiLA 2 Specification for details about how the different documents are related.

SiLA 2 Working Group Members

Please refer to [Part (A) (Current Version)](#).

SiLA 2 Working Group Organization

Please refer to [Part (A) (Current Version)](#).

SiLA 2 Roadmap

Please refer to [Part (A) (Current Version)](#).

SiLA 2 Adoptions

Please refer to [Part (A) (Current Version)](#).

Status of The SiLA 2 Specification

Please refer to [Part (A) (Current Version)](#).

Table of Contents

Abstract

Please Note: This document is an index to all SiLA Features. It does not contain specifications, but just serves as an index, linking to specific Feature specifications.

This document will eventually be replaced by a Feature registration, commenting and voting platform on the SiLA website.

The technical specification of core Features can be found on https://gitlab.com/SiLA2/sila_base.

= = = START OF NORMATIVE PART = = =

Structure of the SiLA 2 Specification

[COMPLETE; as of 0.1]

The SiLA 2 specification is a multi part specification:

- Part (A) - Overview, Concepts and Core Specification (current version): contains the user requirements specification of SiLA 2. It describes **what** SiLA would like to achieve.
  It describes the core of SiLA 2 including the Features Framework in details, but does not map to a specific implementation. This document deals with:
    - Overview of the design goals
    - SiLA 2 ·Features· specification
    - SiLA 2 ·Features· design rules
    - SiLA 2 ·Features· development and balloting process
    - Error handling and ·SiLA Data Types·
    - Security and Authentication
    - ·SiLA Server Discovery· and ·SiLA Feature Discovery·
- Part (B) - Mapping Specification (current version): describes **how** the user requirements shall be implemented. The mapping specification document describes the specific mapping to a technology and an actual implementation
- Part (C) - Standard Features Index (current version of **this document**): The Standard Features Index document is an index to ·Features· that are either standardized or currently being descussed to become standardized.

Terminology and Conformance Language

[COMPLETE; as of 0.1]

Unless otherwise noted, the entire text of this specification is normative. Exceptions include:

- Notes
- Sections explicitly marked non-normative
- Examples and their commentary
- Informal descriptions of details formally and normatively stated elsewhere (such informal descriptions are typically introduced by phrases like "Informally, ..." or "It is a consequence of ... that ...")

Explicit statements that some material is normative are not implying that other material is non-normative, other than items mentioned in the list just described.

Special terms are defined at their point of introduction in the text.

For example:

[Definition: Term] a **Term** is something used with a special meaning. The definition is labeled as such and the **Term** it defines is displayed in boldface. The end of the definition is not specially marked in the displayed or printed text. Uses of defined **Terms** are links to their definitions, set off with middle dots, for instance ·Term·.

Normative text describes one or both of the following kinds of elements:

- Vital elements of the specification
- Elements that contain the conformance language keywords as defined by [RFC2119](#) "Key words for use in RFCs to Indicate Requirement Levels"

Informative text is potentially helpful to the user, but dispensable. Informative text can be changed, added, or deleted editorially without negatively affecting the implementation of the specification. Informative text does not contain conformance keywords.

All text in this document between "START OF NORMATIVE PART" and "END OF NORMATIVE PART" is, by default, normative.

The key words words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119](#) "Key words for use in RFCs to Indicate Requirement Levels".

SiLA Standard Features Index

SiLA Service

[COMPLETE; as of 0.1]

The Feature each SiLA Server MUST implement. It is the entry point to a SiLA Server and helps to discover the Features it implements.

Definition: [SiLAService](#)

Authentication and Authorization

Authentication Service

[COMPLETE; as of 0.2]

In SiLA 2, authentication is the process of actually confirming the identity of a SiLA Client, executed by a SiLA Server.

This Feature provides SiLA Clients with access tokens based on an identification and password or other means of [authentication](#). Access tokens are issued in a context. That is, when authenticating, the SiLA Client MUST specify the server for which an access is to be granted and which features need to be accessed. If the list of requested features is empty, this is treated as a wildcard request. That is, it is equivalent to requesting access to all features the server offers.

The SiLA server MUST respond either with an error message that the authentication failed or with an access token that the SiLA Client can use to authorize further requests.

It is RECOMMENDED that a SiLA Server always authenticates the identity of a SiLA Client by implementing the Feature "AuthenticationService" if using username/password authentication.

Definition: [AuthenticationService](#)

Authorization Service

[COMPLETE; as of 0.2]

In SiLA 2, authorization is the function of access control, executed by a SiLA Server in order to grant or deny access to the SiLA Server by a SiLA Client.

This Feature specifies the SiLA Client Meta Data for the access token, that has been granted e.g. by the AuthenticationService.

It is RECOMMENDED that a SiLA Server always authorizes the access of a SiLA Client by implementing the Feature "AuthorizationService".

Definition: AuthorizationService

Authorization Provider Service

This Feature provides SiLA Clients with a function to check whether a given access token is valid for a given server and feature. SiLA Servers that do not have their own user management or need to integrate into an existing user management can use this feature in order to check whether a provided access token is valid.

Definition:

Authorization Configuration Service

This Feature provides SiLA Clients with a function to check which authorization provider is used by a given SiLA server in case the SiLA Server uses a user management integrated into an existing user management system. In addition, the feature allows to change the authorization provider used by a SiLA Server. This functionality can be used from a SiLA Client to integrate a new SiLA Server into an existing user management infrastructure.

Definition:

Example Authentication and Authorization Scenarios

The Authentication Service / Authorization Sercvice Features are intended to allow a variety of authentication / authorization scenarios that are described in the remainder of this section.

Local Authentication and Authorization

The simplest scenario of authentication / authorization is where the SiLA Client authenticates against the SiLA Server directly. For this, the SiLA Server must implement the AuthenticationService feature. The client then uses the Login command to obtain an access token. This is depicted in the sequence diagram below.
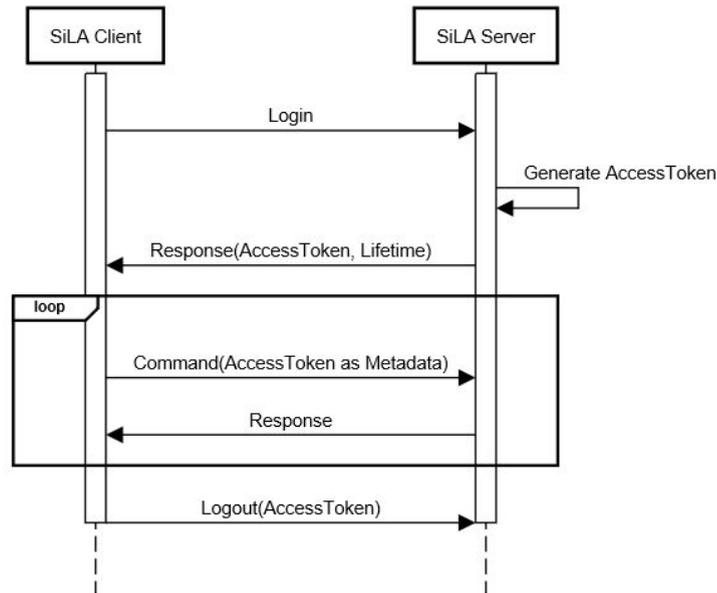
The SiLA Client logs into the SiLA Server. The Server then generates an access token with a given lifetime and returns both access token and lifetime to the client. Then, the client may issue requests. Because the server issued the access token itself, it is able to validate the access token and perform the command. Afterwards, the client logs out from the server.
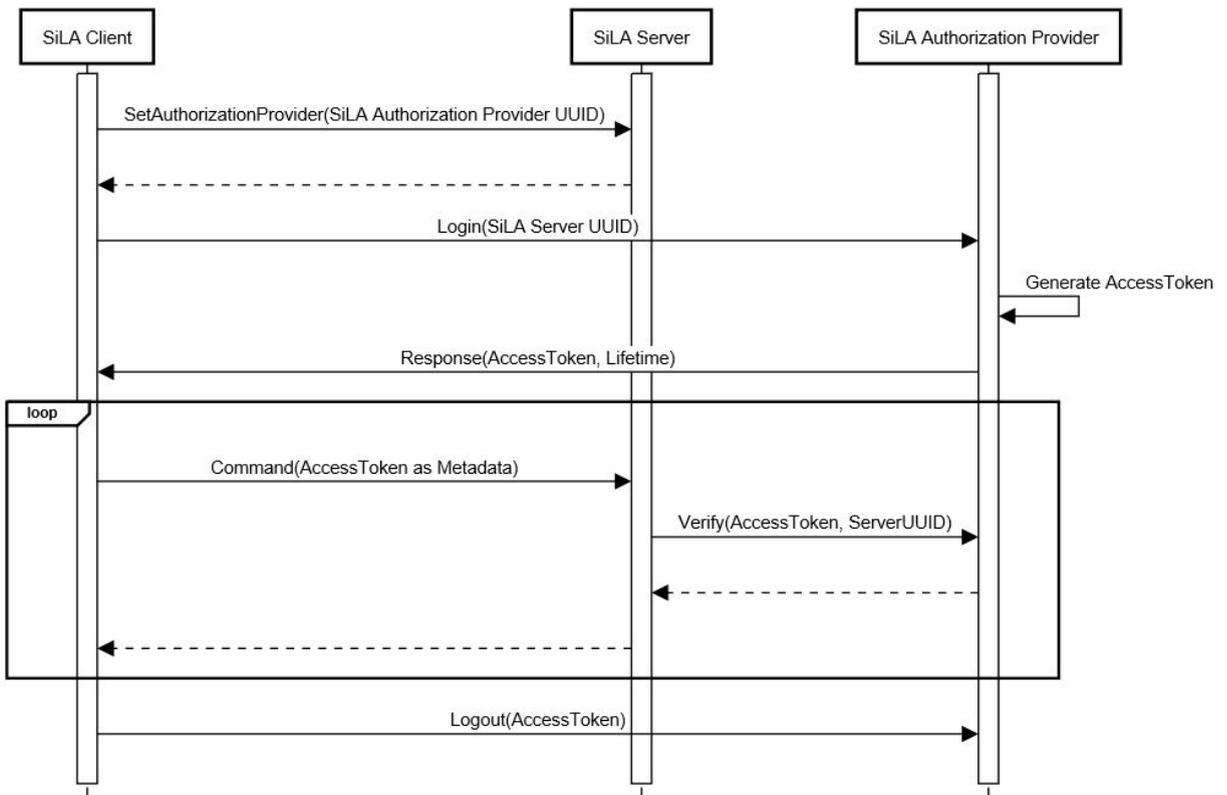
Authorization Provider

In many cases, it is desirable to integrate a SiLA Server into an existing authentication/authorization infrastructure. For this to work, there has to be another server referred to as SiLA Authorization Provider that has to implement the AuthenticationService and the AuthorizationProvider feature. In this case, the sequence of calls is as depicted in the figure below.
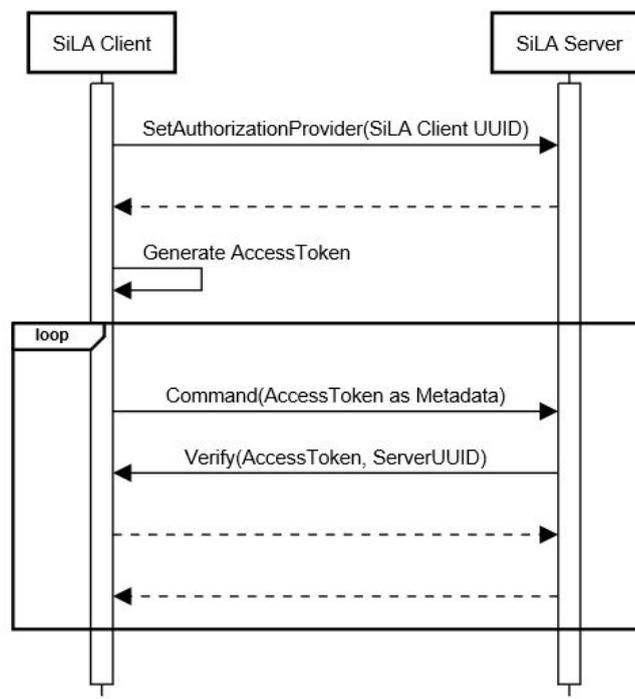
In this case, the SiLA Client first has to configure the SiLA Server which Authorization Provider to use. For this to work, the SiLA Server must implement the AuthorizationConfiguration feature. This only has to be done once. It is strongly recommended that the call to set the authorization provider is protected.

Afterwards, the SiLA Client logs into the authorization provider, passing the information for which server an access token should be created. The Authorization Provider generates an access token and responds to the client with this access token and a token lifetime. With this access token, the client may issue requests to the SiLA Server. However, because the SiLA Server cannot validate the access token itself, it forwards the request to the Authorization Provider.

SiLA Client as Authorization Provider

The SiLA Client and the SiLA Authorization Provider in the above scenario may be the same application. In this case, any calls between those two participants may collapse. This scenario is depicted below.

Similarly, the SiLA Client first configures the authorization provider for the SiLA Server to use, in this case the SiLA Client itself. Afterwards, the SiLA Client may generate an access token itself which it then passes to the SiLA Server in order to authorize requests.

Combination of Local Authentication and Authorization Providers

It is recommended that SiLA Servers implement both the AuthenticationService feature and the AuthorizationConfiguration feature. The SiLA Server may be shipped with a default admin username and password combination. Any SiLA Client wanting to access the server could either continue to use the local authentication using the username/password provided by the SiLA Server or choose to integrate the SiLA Server into an existing authentication/authorization infrastructure. To do so, the client would have to authenticate with the SiLA Server locally and then change the Authorization Provider to the standard Authorization Provioder server used in this network.

Parameter Constraints Provider

[COMPLETE; as of 0.2]

A Feature that allows to find out constraints (min value, max value, min length, max length for strings, etc.) that given parameters of a given command have; also depending on other parameter or state. It is RECOMMENDED that a SiLA Server implements this feature.

Definition: ParameterConstraintsProvider

Lock Controller

[COMPLETE; as of 0.2]

This Feature allows a SiLA Client to lock a SiLA Server for exclusive use, preventing other SiLA Clients from using the server while it is locked. To lock a SiLA Server a lock identifier has to be set, using the 'LockServer' command. This identifier has to be sent along with every (lock protected) request to the SiLA Server in order to use its functionality. To send the lock identifier the SiLA Client Meta Data 'LockIdentifier' has to be used. When locking a SiLA Server a timeout can be specified that defines the time after which the SiLA Server will be automatically unlocked if no request with a valid lock identifier has been received meanwhile. After the timeout has expired or after explicit unlock no lock identifier has to be sent any more.

Definition: LockController

Simulation Controller

[COMPLETE; as of 0.2]

A Feature that allows to implement a simulation mode (as in SiLA 1.x).

Definition: SimulationController

Observable Command Controller

[COMPLETE; as of 0.2]

Allows to pause, resume or stop a currently running observable command.

Definition: ObservableCommandController

Internationalization Service

Please refer to Part (C) (Current Version).

Audit Trail Service

Please refer to Part (C) (Current Version).

Parameter Defaults Provider

Please refer to [Part (C) (Current Version)](#).

Server Detail Provider

Please refer to [Part (C) (Current Version)](#).

Initialization Controller

Please refer to [Part (C) (Current Version)](#).

Duration Provider

Please refer to [Part (C) (Current Version)](#).

Server Monitoring Service / Alarm Provider / Logging Service

Please refer to [Part (C) (Current Version)](#).

Error Recovery Service

Please refer to [Part (C) (Current Version)](#).

Time Normal Provider / Time Sync Provider

Please refer to [Part (C) (Current Version)](#).

Heart Beat Provider / Keep Alive Service

Please refer to [Part (C) (Current Version)](#).

Discovery Service / Server Registry

Please refer to [Part (C) (Current Version)](#).

Broker Service / Late Binding Service

Please refer to [Part (C) (Current Version)](#).

License Service

Please refer to [Part (C) (Current Version)](#).

Architectural Concepts Based on Feature Definitions

Please refer to [Part (C) (Current Version)](#).

Chromatography Data System Services (CDS Services)

Please refer to [Part (C) (Current Version)](#).

Orchestration Services

Please refer to [Part (C) (Current Version)](#).

= = = END OF NORMATIVE PART = = =