SECURE AND AGILE CONNECTED THNGS

**SCRATCh**

****

Copyright © 2018-2022, SCRATCh

Deliverable <XX>



Deliverable <XX>: <Deliverable Title>

**Work package:** WP2

**Affected milestone:** M<XY>

**Partners involved:** **ANYWI**

<Organization2>

<…>

<OrganizationN>

**Date:** **12/02/2020**

**Deliverable version: v 0.1**

**Editor:** **Franklin Selgert, AnyWi**

**Author(s):** **Fanklin Selgert, AnyWi**

<Author2>, <Organization2>

<…>

<AuthorN>, <OrganizationN>

**Responsible Contact:** <Name>

<Organization>

<Address>

<Mail>

<Business phone>

# Version history

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Author** | **Comment** |
| 12/01/2020 | 0.1 | Franklin Selgert | First draft steps design code build devops |
| … | … | … | … |
| … | … | … | … |

|  |  |  |  |
| --- | --- | --- | --- |
| Role Approver | Name Approver | Approval date | Signature |
| Process Owner |  |  |  |
| Quality Assurance |  |  |  |

Inhoudsopgave

[Version history 2](#_Toc33006583)

[Introduction 4](#_Toc33006584)

[Purpose 4](#_Toc33006585)

[Scope 4](#_Toc33006586)

[Stakeholders 4](#_Toc33006587)

[Overview 4](#_Toc33006588)

[System Overview 6](#_Toc33006589)

[SDG Context and Conceptual View 6](#_Toc33006590)

[System Requirements 6](#_Toc33006591)

[Functional Requirements 6](#_Toc33006592)

[SGD Management 6](#_Toc33006593)

[SGD device update mechanisms 9](#_Toc33006594)

[SGD Communication 10](#_Toc33006595)

Introduction

Purpose

This document contains the system requirements for the Scratch Generic demonstrator.

Scope

This document describes the technical implementation of the commercial requirements specified in the [SGD UR] and [SGD BR] The system is described in the System Design Specification [SGD SDS].

Stakeholders

The main stakeholders and their interests for this document are:

* Product Manager, validate the constructed system implements the commercial requirements
* System Architect, deployment and HSDP interactions
* Software Architect, software design and development
* Software Engineers, derive what must be developed
* Test Manager, Testers, verify the constructed system
* Service Manager, validate the constructed system implements the service requirements

Overview

Chapter 1 gives an overview of the document. Chapter 2 describes the product perspective of the SGD, the context, as well as the principles of operation. Subsequent chapters list the functional and non-functional requirements for the SGD.

 The sections of this document contain informative and/or normative texts. All informative text is tagged with an identifier consisting of a tag (Folder) and an ID number like in:

**<Heading>**

<Informative text describing the subject.>

All normative requirement texts are tagged with a requirement identifier consisting of a tag (SR) and an ID number like in:

**<Heading>**

|  |
| --- |
| **SR-<Supported release>-<ID number>** |

<Normative text describing the requirement.>

*[Acceptance Criteria:*

*<text describing the acceptance criteria>]*

*[Information:*

*<text giving additional information>]*

The <Heading> is formulated in a tagged and structured manner, such that tracing can easily recognize the origin of the requirement:

<ReqType>.<(Sub)System>.<High level Feature/Requirements>

E.g.:  *SR.SGD.firmware.update* or *SR.SGD.monitoring.endnode*

Within a tagged requirement description optional parts may give Rationale and/or Information. These parts are shown in italic type and are considered informative only.

System Overview

SDG Context and Conceptual View

The Scratch Generic Demonstrator is a development and testing environment meant for the SCRATCh participant to develop, test and deploy the software and tools developed in the project. Each member may make adjustments to the environment and document it in a copy of this document

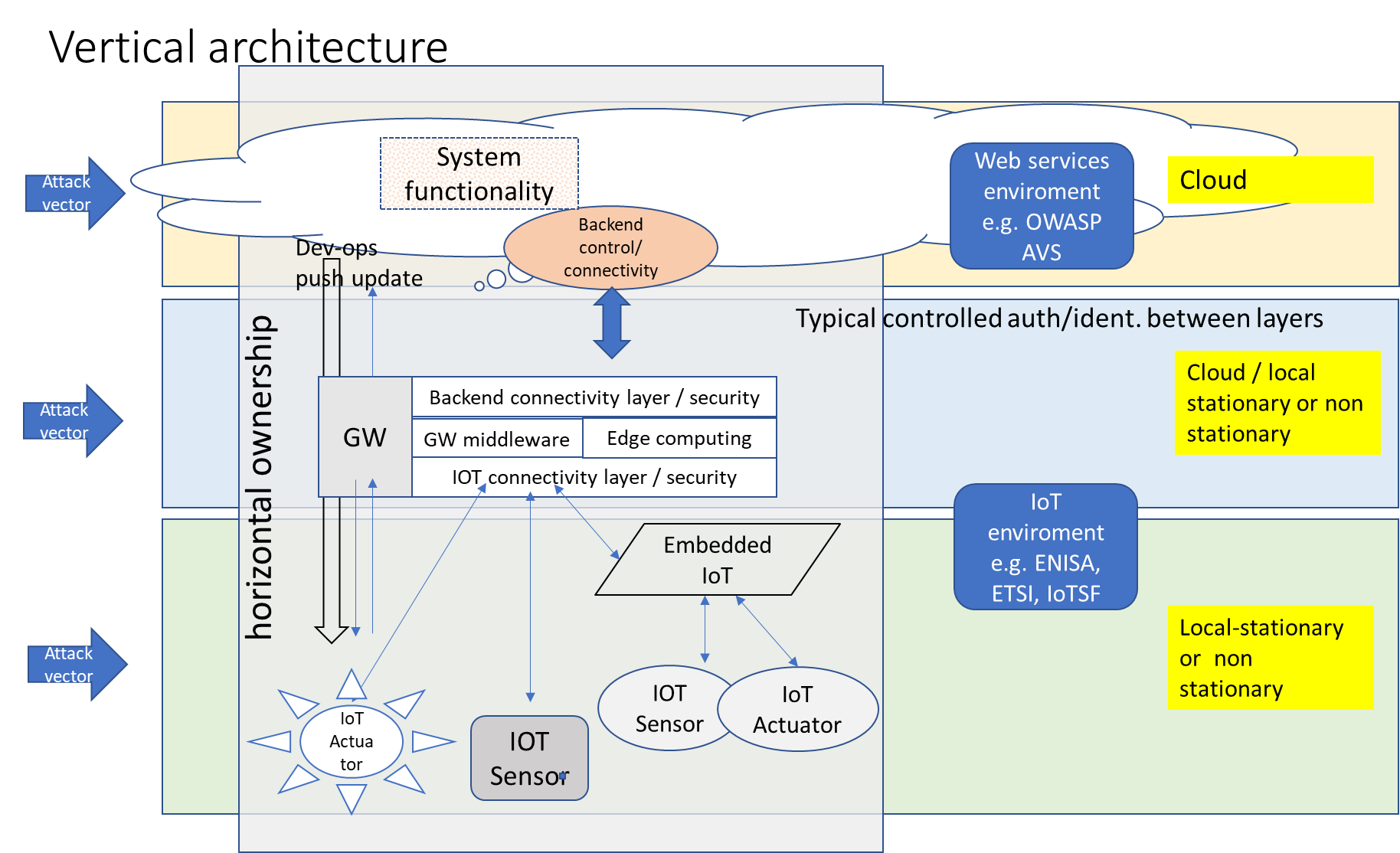


Figure SGD Architecture

System Requirements

Functional Requirements

SGD Management

The management of SGD is decentralized and out of scope of this document

SR.SGD.Management.documentation

|  |
| --- |
| SGD-1.0-SR001 |

There shall be a description how the management of firmware updates is regulated, roles and responsibilities mentioned in this description should be implemented in the software

Table example of rights structure for a certain demonstrator

|  |  |
| --- | --- |
| **Clusters** | **Clarification** |
| **SGD rights** |  |
| Firmware update push | Device manufacturer when specified in policy |
| Firmware update pull | IoT device owner, based on manufacturer message |
| Provisioning new device | IoT device owner. |
| Blocking IoT device | System based on detection of certain event |

Acceptance Criteria:

* An instance of the SGD shall have a management policy with associated rights structure.

SR.SGD.Management.asset

|  |
| --- |
| SGD-1.0-SR002 |

The Gateway shall have a method and policy to control which device can be connected and by which protocols it is allowed to communicate.

 Acceptance Criteria:

* Whether a device has a connection with a gateway is determined by a white list and the communication policy associated with the device.
* The device/whitelist can be queried and adjusted by a secure management function.
* Non registered devices should be rejected and the attempt logged if so, indicated by the policy

SR.SGD.Management.asset.sandbox

|  |
| --- |
| SGD-1.0-SR003 |

If non secure or unencrypted sensors are allowed to connect to the gateway, this connection should be handled as non-safe and sandboxed

Acceptance Criteria:

* It shall be possible to set a connect all policy, only when the gateway can sandbox the connection of non-whitelisted devices.
* The data handling of non-whitelisted devices should be isolated and have no access to critical functionality of the gateway.
* By default, all non-registered devices shall be blocked unless.

SR.SGD.Management.asset.provisioning

|  |
| --- |
| SGD-1.0-SR004 |

It shall be possible to whitelist a device remotely. The registration should be possible also during installation of the new device. (related to SGD-1.0-SR001)

Acceptance Criteria:

* It shall be possible to create a whitelisted device entry remotely
* If a device tries to register and is not whitelisted, a secure mechanism should be in place to register the device immediately.

SR.SGD.Management.asset.disabeling

|  |
| --- |
| SGD-1.0-SR005 |

It shall be possible to block a connected device based on a policy or set of behavioral criteria. (related to SGD-1.0-SR001)

Acceptance Criteria:

* It shall be possible to monitor a set of predefined behavioral characteristics of a device
* It shall be possible to disable a device
  + When its behavior is outside the policy set for it
  + When a device is blocked an alert will be generated
  + Upgrading software or firmware of a device without this being checked by the gateway is in all circumstances malicious behavior and will lead to blocking/ decommissioning the device.

SR.SGD.User.Management

|  |
| --- |
| SGD-1.0-SR006 |

There shall be a user management function for adding, editing, disabling of users that have access to the configuration parts of the gateway. (related to SGD-1.0-SR001)

Acceptance Criteria:

* Each user shall have a unique ID
* Each user shall have an associated profile limiting its control over the gateway.
* A mechanism shall exist to detect malicious attempt to add users.

SR.SGD.User.Management.cloud

|  |
| --- |
| SGD-1.0-SR007 |

It shall be possible to add a new receiving site to the allowed upstream connection of the gateway, (related to SGD-1.0-SR001)

Acceptance Criteria:

* It shall be possible to add a new receiving site based on a unique site ID end a encrypted authorization key.
* When a new upstream site is added, the registered users and their policy determine the access to the gateway
* The option to add a new site connection is only enabled when a site has the related permissions

SGD device update mechanisms

SR.SGD.firmware.update.gateway

|  |
| --- |
| SGD-1.0-SR008 |

It shall be possible to update the firmware of the gateway.

Acceptance Criteria:

* Firmware updates are sent and received encrypted.
* Encryption is based on unique identifiers of the receiving gateway
* Received firmware updates are checked by the gateway
* In case of noncompliance to set criteria, the firmware update is canceled and a message is sent.
* During firmware updates the gateway shall not loose connectivity with the backend.
* During and after upgrade a rollback mechanism shall be possible

SR.SGD.firmware.update.end.node

|  |
| --- |
| SGD-1.0-SR008 |

It shall be possible to update the firmware of an end node

Acceptance Criteria:

* Firmware updates are sent and received encrypted by the gateway.
* Encryption is based on unique identifiers of the receiving end nodes
* Received firmware updates are checked by the gateway
* In case of noncompliance to set criteria, the firmware update is canceled and a message is sent.
* During firmware updates the gateway shall not loose connectivity to the end.node
* During and after upgrade a rollback mechanism shall be possible.

SGD Communication

SR.SGD.communication.gateway

|  |
| --- |
| SGD-1.0-SR009 |

All communication between gateway and backend shall be encrypted.

 Acceptance Criteria:

* It shall not be possible to setup an unencrypted connection with the gateway
* The gateway shall monitor traffic and alert in situations that there is no encryption.

SR.SGD.communication.end.node

|  |
| --- |
| SGD-1.0-SR010 |

All communication between gateway and end-node should be encrypted

 Acceptance Criteria:

* An unencrypted connection of an end device with the gateway is isolated?
* The gateway shall monitor traffic and alert in situations that there is no encryption from a device with encryption enabled in its registered profile.