TR 82 : 2020
(ICS 35.020; 35.040; 35.240.01)

TECHNICAL REFERENCE

Guidelines for Cloud Native security

Singapore Standards Council

TR 82 : 2020
(ICS 35.020; 35.040; 35.240.01)

TECHNICAL REFERENCE

Guidelines for Cloud Native security

Published by Enterprise Singapore

ISBN 978-981-49-2536-5

The content of this Technical Reference was approved on 27 November 2020 by the Information Technology Standards Committee (ITSC) under the purview of the Singapore Standards Council.

First published, 2021

ITSC consists of the following members:

		Name	Representation
Chairman	:	Mr Chak Kong Soon	*Individual Capacity*
Deputy Chairman	:	Mr Harish Pillay	*Individual Capacity*
Advisor	:	Mr Yap Chee Yuen	*Individual Capacity*
Secretary	:	Mr Tao Yao Sing	*Infocomm Media Development Authority of Singapore*
Members	:	Assoc Prof Benjamin Gan	*Singapore Management University*
		Mr Hong Tse Min	*Infocomm Media Development Authority of Singapore*
		Assoc Prof Huang Zhiyong	*National University of Singapore*
		Prof Li Xiaoli	*Institute for Infocomm Research*
		Mr Sam Liew	*Singapore Computer Society*
		Ms Lim Bee Kwan	*Government Technology Agency*
		Mr Lim Soon Chia	*Cyber Security Agency*
		Mr Kelvin Ng	*Nanyang Polytechnic*
		Mr Ong Hian Leong	*Individual Capacity*
		Mr Andy Sim	*SGTech*

ITSC set up the Technical Committee on Cloud Computing Standards to oversee the preparation of this standard. The Technical Committee consists of the following members:

		Name	Representation
Chairman	:	Mr Robert Chew	*Individual Capacity*
Secretary	:	Mr Steven Tan	*Infocomm Media Development Authority of Singapore*
Members	:	Dr Anton Ravindran	*Singapore Computer Society*
		Mr Chan Kin Chong	*Individual Capacity*
		Dr Calvin Chan Meng Lai	*Singapore University of Social Sciences*
		Mr Chew Weiqiang	*Pactera Singapore Pte Ltd*
		Mr Hammad Rajjoub	*Individual Capacity*
		Dr Kang Meng Chow	*SGTech*
		Dr Ryan Ko	*Individual Capacity*
		Mr Kwa Kim Chiong	*Information Technology Management Association*
		Mr James Loo	*Information Technology Management Association*

Members	:	Mr Kelvin Ng	*Nanyang Polytechnic*
		Ms Ng Lay Ngan	*Institute of Systems Science*
		Mr Harish Pillay	*Individual Capacity*
		Mr Raju Chellam	*SGTech*
		Dr Suria P Asai	*Institute of Systems Science*
		Mr Tao Yao Sing	*Infocomm Media Development Authority of Singapore*
		Mr Wong Onn Chee	*Resolvo Systems*
		Mr Martin Yates	*Singapore Computer Society*

The Technical Committee set up the Working Group on Multi-Tiered Cloud Security to prepare this standard. The Working Group consists of the following experts who contribute in their *individual capacity*:

		Name
Convenor	:	Dr Kang Meng Chow
Deputy Convenor	:	Mr Lim Soon Chia
Members	:	Dr Anton Ravindran
		Mr Mandar Bale
		Dr Ken Baylor
		Mr Chai Chin Loon
		Mr Chan Meng Fai
		Mr Dave Cheng
		Mr Chetan Sansare
		Mr Chong Jian Yi
		Mr Patrick Choong Wee Meng
		Ms Dhana Lakshmi
		Mr Gajun Ganendran
		Mr Hong Jian Hui
		Mr Lucas Kauffman
		Mr Richard Koh
		Prof Lam Kwok Yan
		Dr Lee Hing Yan
		Ms Lim May Ann
		Mr Loh Chee Keong
		Mr Manoj Wadhwa
		Mr Mok Boon Poh
		Mr Chris Ng Khee Soon
		Mr Raju Chellam
		Mr Sanjeev Gupta
		Mr Andrew Seit
		Mr Sim Bak Chor
		Mr Suresh Agarwal

Members	:	Mr Tao Yao Sing
		Ms Irene Wang
		Mr Wong Onn Chee
		Mr Xiang Bin
		Mr Zhuang Haojie

The organisations in which the experts of the Working Group are involved are:

AliCloud
Amazon Web Services
Asia Cloud Computing Association
Association of Information Security Professionals
BSI Group Singapore Pte. Ltd.
Certification Partner Global
Cloud Security Alliance APAC
Cyber Security Agency
Ernst & Young CertifyPoint B.V.
Google Cloud
Government Technology Agency
IBM Softlayer Cloud
Infocomm Media Development Authority of Singapore
Microsoft Cloud Services
Salesforce.com
SCS Cloud Chapter
SGTech, Cloud and Data Chapter
Singapore Chinese Chamber of Commerce and Industry
SOCOTEC Certification Singapore
TÜV SÜD PSB Pte Ltd

Contents

Page

Foreword

This Technical Reference (TR) was prepared by the Working Group on Multi-Tiered Cloud Security Working Group set up by the Technical Committee on Cloud Computing Standards under the purview of ITSC.

Cloud Computing shifts away from conventional hosting and delivery of services, to utility-based consumption in both the enterprise and personal space. In the midst of building Cloud Native applications, traditional IT security models are no longer adequate.

In operating cloud user virtual environments, shared responsibility model emerged as Cloud Service Providers (CSPs) focus on protecting the underlying global infrastructure that supports the virtual cloud environments that cloud users build and configure to safeguard their applications. In offering Cloud Native services, there is a need to lay out a set of security best practices to guide CSPs to mitigate security risks and vulnerabilities that may be present in Cloud Native architectures.

This TR provides guidance on Cloud Native security for relevant controls specified in SS 584, to mitigate vulnerabilities that are applicable for CSP.

This TR is a provisional standard made available for application over a period of three years. The aim is to use the experience gained to update the TR so that it can be adopted as a Singapore Standard. Users of the TR are invited to provide feedback on its technical content, clarity and ease of use. Feedback can be submitted using the form provided in the TR. At the end of the three years, the TR will be reviewed, taking into account any feedback or other considerations, to further its development into a Singapore Standard if found suitable.

In preparing this TR, reference was made to SS 584 : 2020, “Specification for multi-tiered cloud computing security”.

Attention is drawn to the possibility that some of the elements of this TR may be the subject of patent rights. Enterprise Singapore shall not be held responsible for identifying any or all of such patent rights.

NOTE

1. *Singapore Standards (SSs) and Technical References (TRs) are reviewed periodically to keep abreast of technical changes, technological developments and industry practices. The changes are documented through the issue of either amendments or revisions. Where SSs are deemed to be stable, i.e. no foreseeable changes in them, they will be classified as “Mature Standards”. Mature Standards will not be subject to further review, unless there are requests to review such standards.*

2. *An SS or TR is voluntary in nature except when it is made mandatory by a regulatory authority. It can also be cited in contracts making its application a business necessity. Users are advised to assess and determine whether the SS or TR is suitable for their intended use or purpose. If required, they should refer to the relevant professionals or experts for advice on the use of the document. Enterprise Singapore and the Singapore Standards Council shall not be liable for any damages whether directly or indirectly suffered by anyone or any organisation as a result of the use of any SS or TR. Although care has been taken to draft this standard, users are also advised to ensure that they apply the information after due diligence.*

3. *Compliance with a SS or TR does not exempt users from any legal obligations.*

Guidelines for Cloud Native security

1 Scope

This Technical Reference (TR) provides additional guidance for relevant controls specified in SS 584 : 2020, to mitigate vulnerabilities specific to Cloud Native architecture that are applicable for the Cloud Service Provider (CSP). This TR should be used together with SS 584, as it excludes the guidance for common implementation contained in SS 584.

This TR defines three common characteristics of Cloud Native architecture, as follows:

1. Use of Container technologies;
2. Use of Microservices-based technologies; and
3. Use of DevOps pipeline.

Currently, the use of Container technologies and Microservices-based technologies is growing amongst CSPs. It will be the primary focus of this TR.

Container and Microservices-based technologies are provided as software services to help users run, scale and secure containerised applications. The CSP should incorporate security best practices as part of their software development lifecycle process.

The recommendations in this TR are relevant for the CSP's implementation of Cloud Native technologies and service offerings.

2 Normative references

There are no normative references in this standard.