



# **Initial release of the SafeCloud platform**

## **D4.2**

**Project reference no. 653884**

**August 2017**



**European  
Commission**

Horizon 2020  
European Union funding  
for Research & Innovation

## Document information

Scheduled delivery	31.08.2017
Actual delivery	31.08.2017
Version	1.1
Responsible Partner	CYBER

## Dissemination level

Public

## Revision history

Date	Editor	Status	Version	Changes
15.08.2017	K. Tarbe	Draft	0.1	Initial version
20.08.2017	F.Maia	Draft	0.2	INESC TEC review
27.08.2017	H. Mercier	Draft	0.3	UniNE Revision
29.08.2017	K. Tarbe	Draft	0.4	Incorporated the reviews
30.08.2017	K. Tarbe	Final	1.0	Finalise the document
31.08.2017	K. Tarbe	Final	1.1	Updated Figure 3

## Contributors

K. Tarbe (CYBER)  
V. Sokk (CYBER)

## Internal reviewers

F. Maia (INESC TEC)  
H. Mercier (UniNE)

## Acknowledgements

This project is partially funded by the European Commission Horizon 2020 work programme under grant agreement no. 653884.

## More information

Additional information and public deliverables of SafeCloud can be found at <http://www.safecloud-project.eu>

**Table of contents**

**Document information..... 2**

**Dissemination level..... 2**

**Revision history..... 2**

**Contributors ..... 2**

**Internal reviewers..... 2**

**Acknowledgements..... 2**

**More information..... 2**

**Table of contents..... 3**

**Executive summary ..... 4**

**Introduction..... 5**

**Content..... 7**

## **Executive summary**

This deliverable summarizes the initial release of the SafeCloud platform on the SafeCloud website.

## Introduction

The framework proposed by SafeCloud consists of three layers: secure communication, secure storage, and secure queries. Secure communication provides schemes for the establishment of channels amongst protocol participants employing technologies for tamper-resistant channels, ensuring confidentiality and availability. Secure storage provides techniques for reliable storage, such as long-term confidentiality, protection against file corruption or data deletion. Finally, secure queries provide cryptographic constructions from the database storage layer to the end-user processing requests. The overarching idea is to allow system developers to use the techniques provided by these three layers in order to achieve application-specific deployments. These deployments should surpass the state-of-the-art of existing tools with respect to functionality, performance and security. We recall Figure 1, from the general SafeCloud framework description.

<b>Secure communication</b>	State of the art: TLS secure channels	<b>Solution:</b>	<b>SC1 - Vulnerability-tolerant channels</b>	<b>SC2 - Protected channels</b>	<b>SC3 - Route-aware channels</b>
		<i>Gives:</i>	Tolerance to vulnerabilities in components	Decreased risk of fake certificates; resistance to port scans and enumeration of network infrastructure	Improved confidentiality with warnings about route hijacking and making harder access to communication
		<i>API:</i>	Extended secure socket API	Extended secure socket API	Extended secure socket API
		<i>Provided by:</i>	INESC-ID, TUM	INESC-ID, TUM	INESC-ID, TUM
<b>Secure storage</b>	State of the art: Encrypted storage	<b>Solution:</b>	<b>SS1 - Secure block storage</b>	<b>SS2 - Secure data archive</b>	<b>SS3 - Secure file system</b>
		<i>Gives:</i>	Block storage on individual data centers with fine control over data placement	Entangled immutable data storage for protection against tampering and censorship	Distributed secure file storage leveraging the secure block storage
		<i>API:</i>	Key/value	REST (S3 or similar)	POSIX-like
		<i>Provided by:</i>	UniNE, INESC TEC	UniNE, INESC TEC	UniNE, INESC-ID
<b>Secure queries</b>	State of the art: CryptDB	<b>Solution:</b>	<b>SQ1 - Secure database server</b>	<b>SQ2 - Secure multi-cloud database server</b>	<b>SQ3 - Secure multi-cloud application server</b>
		<i>Gives:</i>	Privacy of data against the server	Privacy of data against non-colluding servers	Privacy of data against non-colluding servers and clients
		<i>API:</i>	SQL	SQL	SQL
		<i>Provided by:</i>	INESC TEC	INESC TEC, Cyber	Cyber

**Figure 1: Components of the SafeCloud architecture.**

The SafeCloud platform is a set of solutions that are being developed in the SafeCloud project. The initial release contains the following solutions:

- Secure communications 1 – Vulnerability-tolerant channels – vtTLS
- Secure communications 2 – Protected channels – sKnock
- Secure communications 3 – Route-aware channels
- Secure storage 3 – Secure file system – SafeCloud FS
- Secure queries 1 – Secure database server
- Secure queries 3 – Secure multi-cloud application server – sharemind-SQL

The solutions are listed on the SafeCloud public website and are directly accessible at <http://www.safecloud-project.eu/platform/>. The landing page for SafeCloud platform mimics the SafeCloud architecture as can be seen on Figure 2.

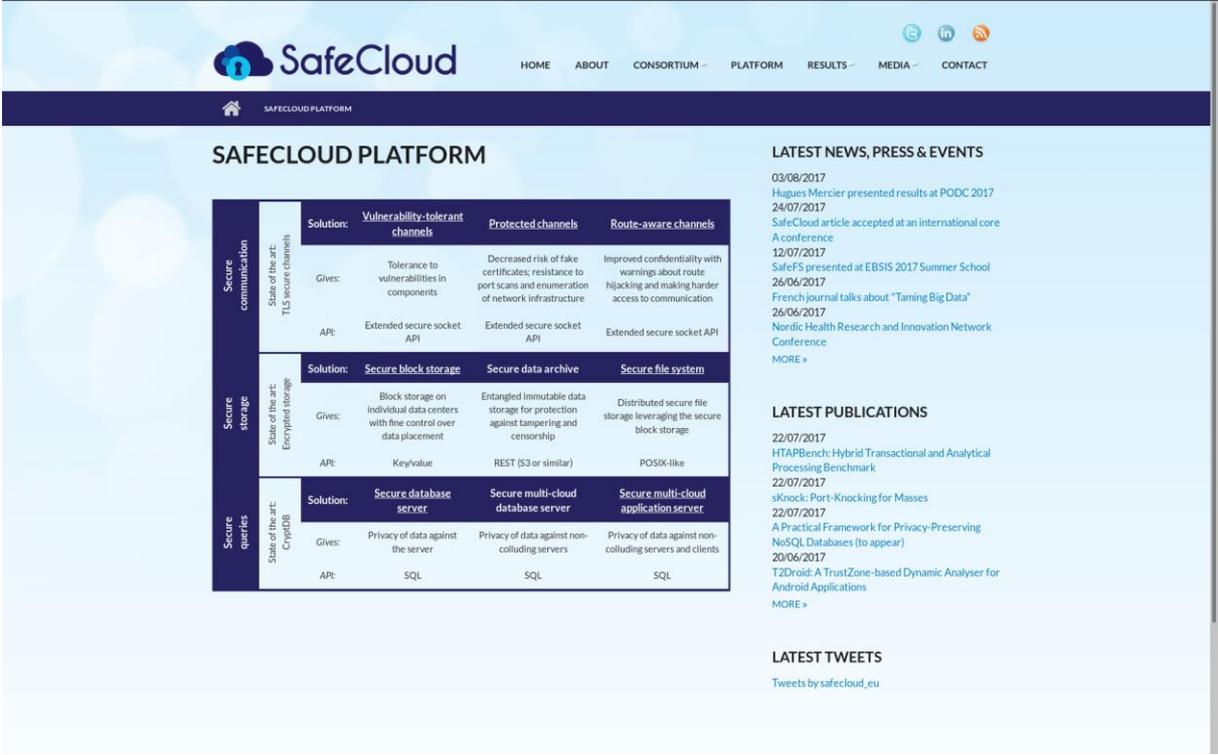


Figure 2: The landing page of SafeCloud platform on the SafeCloud website.

## Content

The subpage for each solution contains information about where to obtain said solution, and instructions on how to deploy it. Additional information like scientific publications and relevant public SafeCloud deliverables are also linked.

Detailed user guides are not available as part of the initial release, but the solution subpages will be updated and improved when such material is ready. For an example, the subpage for SafeCloud Secure queries layer solution 1 can be seen on Figure 3.

We favour Docker containers for distributing our software. Docker containers are easy to set up, test and deploy. These properties are paramount for the adoption of the SafeCloud technologies.

**SafeCloud** HOME ABOUT CONSORTIUM PLATFORM RESULTS MEDIA CONTACT

### SECURE DATABASE SERVER

Any application that wants to integrate SafeCloud secure queries solutions has two distinct APIs available. It can use either a SQL interface or a NoSQL one. For this solution in particular (Secure Database Server), SafeCloud provides full SQL compatibility and a full HBase-like NoSQL interface.

On-premises Infrastructure

Third-party Cloud Infrastructure

APP

SQL NoSQL

SafeCloud

SafeCloud

To offer a SQL and NoSQL integration for the client application, SafeCloud solutions are deployed across two main sites (one trusted site and one untrusted). The figure depicts a high-level overview of such deployment scheme.

Concretely, the client application has access to the trusted deployment site where it can issue requests to the desired API - SQL or NoSQL. Each request is handled in such a way that ensures that data remains private even while being in transit, stored and processed at the untrusted deployment (third-party cloud infrastructures).

**GET IT HERE**  
Contact [Francisco Almeida Maia](#).

**RELATED PUBLICATIONS**  
[D3.3 - Non-elastic secure Key Value Store.](#)

#### LATEST NEWS, PRESS & EVENTS

- 03/08/2017 [Hugues Mercier presented results at PODC 2017](#)
- 24/07/2017 [SafeCloud article accepted at an international core A conference](#)
- 12/07/2017 [SafeF5 presented at EBSIS 2017 Summer School](#)
- 26/06/2017 [French journal talks about "Taming Big Data"](#)
- 26/06/2017 [Nordic Health Research and Innovation Network Conference](#)

[MORE >](#)

#### LATEST PUBLICATIONS

- 22/07/2017 [HTAPBench: Hybrid Transactional and Analytical Processing Benchmark](#)
- 22/07/2017 [sKnock: Port-Knocking for Masses](#)
- 22/07/2017 [A Practical Framework for Privacy-Preserving NoSQL Databases \(to appear\)](#)
- 20/06/2017 [T2Droid: A TrustZone-based Dynamic Analyser for Android Applications](#)

[MORE >](#)

#### LATEST TWEETS

[Tweets by safecloud\\_eu](#)

**Figure 3: An example of a subpage describing one SafeCloud Platform component.**