CREDENTIAL

Secure Cloud Identity Wallet

You are what you keep!

Deliverable D1.3
PROJECT HOME PAGE AND COLLABORATION PLATFORM

Deliverable due date: 01.01.2016
Deliverable submission date: 22.12.2015

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 653454

Project Information	
Project Title	Secure Cloud Identity Wallet
Project Acronym	CREDENTIAL
Grant Agreement No	653454
Type of Action	Innovation Action
Call	H2020-DS-2014-1 Digital Security: Cybersecurity, Privacy and Trust
Partners	12
Estimated Project Cost	6.645.185,00 €
Requested EU Contribution	5.978.082,50 €
Start Date	01.10.2015
Duration	36 months

Web Presence	
CREDENTIAL Website	https://credential.eu
CREDENTIAL Twitter	@CredentialH2020
CREDENTIAL LinkedIn	https://www.linkedin.com/in/credential

This document is issued within the CREDENTIAL project. This project has received funding from the European Union's Horizon 2020 Programme under grant agreement no. 653454.

This document and its content are the property of the CREDENTIAL Consortium. All rights relevant to this document are determined by the applicable laws. Access to this document does not grant any right or license on the document or its contents. This document or its contents are not to be used or treated in any manner inconsistent with the rights or interests of the CREDENTIAL Consortium and are not to be disclosed externally without prior written consent from the CREDENTIAL Partners. Each CREDENTIAL Partner may use this document in conformity with the CREDENTIAL Consortium Grant Agreement provisions. The information in this document is provided as is, and no warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

Document Information	
Title	Project home page and collaboration platform
Editor	Agi Karyda (AIT)
Deliverable no.	D1.3
Work Package No.	WP1
Type	Websites, patents filling etc.
Dissemination Level	PU
Release Date	22.12.2015
Document description	This deliverable describes the technical implementation of the project's public homepage and internal collaboration platform.

Authors List

Authors	**Name**	**E-mail**	**Organisation**
Editors	Agi Karyda	agi.karyda@ait.ac.at	AIT
Contributors	Stephan Krenn	stephan.krenn@ait.ac.at	AIT
Reviewers	Tobias Pulls	tobias.pulls@kau.se	KAU
	Welderufael Tesfay	welderufael.tesfay@m-chair.de	GUF
	Bernd Zwattendorfer	bernd.zwattendorfer@iaik.tugraz.at	SIC
	Florian Thiemer	florian.thiemer@fokus.fraunhofer.de	FOKUS

Versioning

Version	**Date**	**Reason/Change**	**Editor**
0.1	12.11.2015	Initial content	Agi Karyda
0.2	01.12.2015	Incorporated comments by Tobias Pulls	Agi Karyda, Stephan Krenn
0.3	16.12.2015	Incorporated comments from SIC, GUF, FOKUS	Stephan Krenn
1.0	22.12.2015	Final polishing	Agi Karyda, Stephan Krenn

Project Description

With increasing mobility and Internet usage, the demand for digital services increases and has reached critical and high assurance domains like e-Government, e-Health and e-Business. Those domains have high security and privacy requirements and hence will be harnessed with various novel mechanisms for secure access. Approaches for handling the resulting variety of authentication and authorisation mechanisms include the use of digital identity and access management systems (IAM). Like other technologies IAMs follow the trend of using cloud services. This allows abstracting over used resources and enables ubiquitous access to identity data which is stored and processed in the cloud, but also results in an additional degree of complexity for securely operating IAMs. The goal of CREDENTIAL is to develop, test, and showcase innovative cloud based services for storing, managing, and sharing digital identity information and other critical personal data. The security of these services relies on the combination of strong hardware-based multi-factor authentication with end-to-end encryption representing a significant advantage over current password-based authentication schemes. The use of sophisticated proxy cryptography schemes will enable a secure and privacy preserving information sharing network for cloud-based identity information in which even the identity provider cannot access the data in plain-text and hence protect access to identity data. CREDENTIAL does not focus on evaluating and applying novel crypto-approaches for IAMs only but also on implementing them in an easy-to-use way to motivate secure handling of identity data, even in other areas than the cloud. To empirically evaluate CREDENTIAL's work and to produce outputs of a high technical readiness CREDENTIAL considers the demonstration of its project results in different use cases within the domains e-Government, e-Health and e-Business.

1 Contents

2 Executive Summary

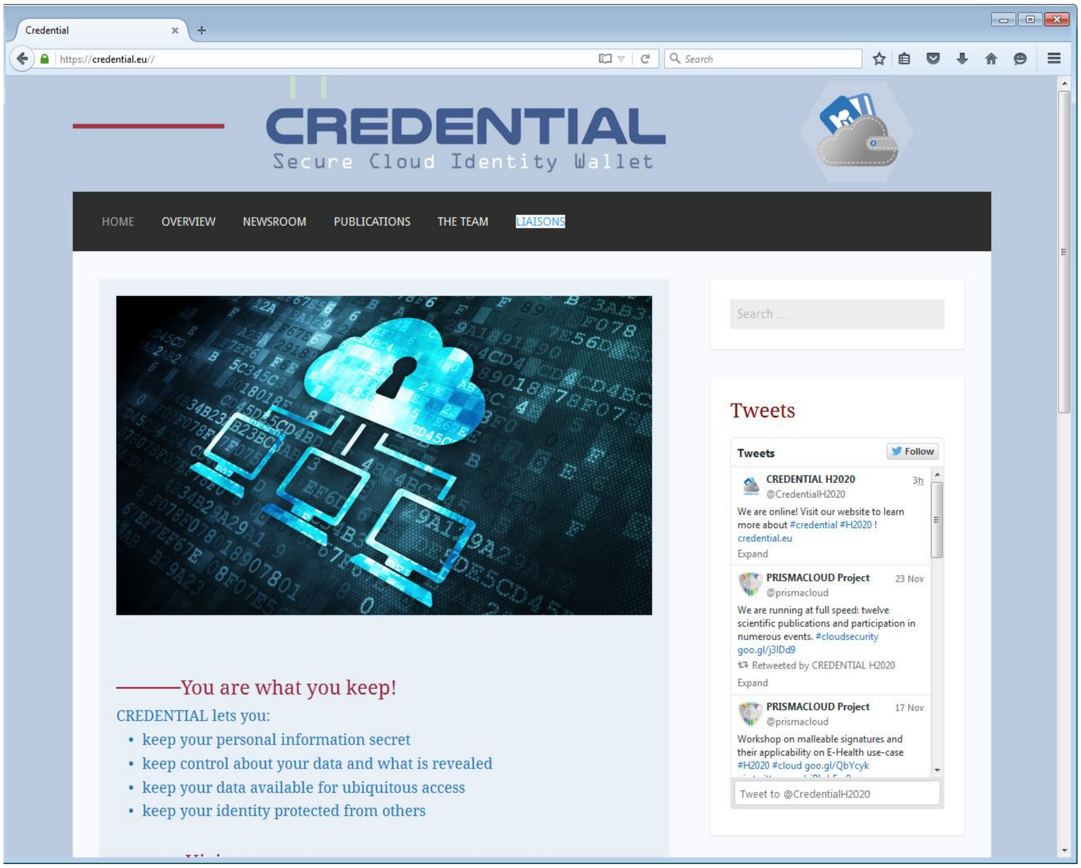
In this document we present the technical platform for the CREDENTIAL homepage, the internal collaboration platform and the whole set of tools that support partners' cooperation within the project, and the coordination with and dissemination to the public. The CREDENTIAL homepage has been set up from the beginning of the project and constitutes the main communication channel between the project consortium and the broad public audience, especially the research, industry and the end-users communities. For internal collaboration the CREDENTIAL consortium has decided to use the SharePoint platform for sharing files and communicating actions, Redmine for coordinating the use-case and requirement development, as well as GitLab as a central repository for developed implementations and documents. During the project's lifetime, the homepage and the internal collaboration platform will be evaluated and updated according to the project's needs.

3 Abbreviations

DIFF	Difference
OS	Operating System
PU	Public
SSL	Secure Sockets Layer
VM	Virtual Machine

4 Technical Implementation of the Homepage

The CREDENTIAL homepage is hosted and maintained by the project coordinator AIT Austrian Institute of Technology GmbH. It is designed in a way to meet the needs of the consortium and to communicate the project and its results to the public. It has a clean design and it is optimized for viewing in any device. Moreover, it is compatible with most popular browsers. A screenshot can be found in Figure 1, and a detailed description can be found in "D7.1 – Public Project Web Presence".



You are what you keep!

CREDENTIAL lets you:

- keep your personal information secret
- keep control about your data and what is revealed
- keep your data available for ubiquitous access
- keep your identity protected from others

Tweets

Tweets

CREDENTIAL H2020 @CredentialH2020 3h
We are online! Visit our website to learn more about #credential #H2020 ! credential.eu

PRISMACLOUD Project @prismacloud 23 Nov
We are running at full speed: twelve scientific publications and participation in numerous events. #cloudsecurity goo.gl/j3lDd9
Retweeted by CREDENTIAL H2020

PRISMACLOUD Project @prismacloud 17 Nov
Workshop on malleable signatures and their applicability on E-Health use-case #H2020 #cloud goo.gl/QbYcyk

Figure 1: Screenshot of the main page of the CREDENTIAL homepage

4.1 Domain

The domain used for the CREDENTIAL Public Homepage is https://credential.eu. This domain has been registered by the AIT Webadmin via the registration company InterNetworX Ltd. & Co. KG (www.inwx.com) and is valid from February 9, 2015 until February 9, 2016. It will be renewed on a yearly basis until at least one year after the official end of the project.

4.2 Server

The Public Website is hosted on a virtual machine (VM) located at the Digital Safety & Security Department of AIT VM Cluster with the configuration: 4GB RAM, 80 GB HDD, and a dual core CPU. This basic configuraiton can be upgraded easily if necessary.

The VM is running Ubuntu[1] as an operating system, as well as MySQL[2]-, PHP[3]-, and Apache Web servers[4]. The concrete versions will change during the project duration due to updates and are therefore omitted here.

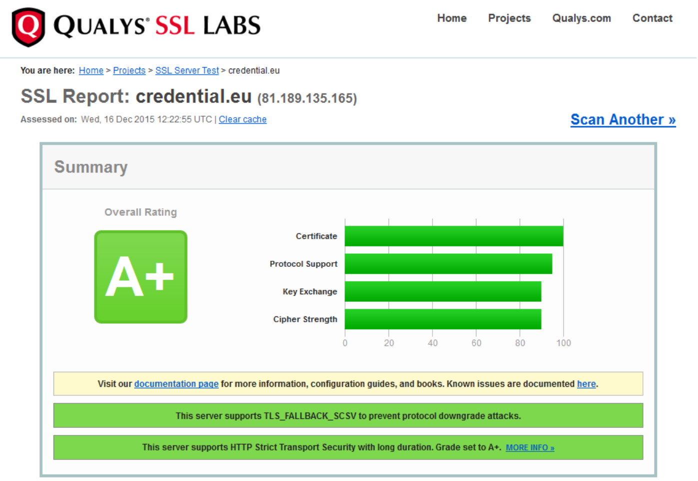
4.3 Software

The software used for the public homepage is WordPress[5] 4.3.1. Updates will be done by the IT Department of AIT accordingly.

4.4 Security Guidelines

The CREDENTIAL homepage complies with best practices regarding security for web pages.

In particular, SSL/TLS (HTTPS) protection with a valid certificate (bought from and signed by an official ceritificate authority) has been implemented for all Project portal pages and important parts of the Public part of the website, e.g. Members login page.



You are here: Home > Projects > SSL Server Test > credential.eu

SSL Report: credential.eu (81.189.135.165)

Assessed on: Wed, 16 Dec 2015 12:22:55 UTC | Clear cache

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports TLS_FALLBACK_SCSV to prevent protocol downgrade attacks.

This server supports HTTP Strict Transport Security with long duration. Grade set to A+. MORE INFO »

Figure 2: SSL Report for the project website

[1] http://www.ubuntu.com/

[2] http://www.mysql.com/

[3] http://php.net/

[4] https://httpd.apache.org/

[5] https://wordpress.com/

Figure 2 shows an SSL report obtained from the Qualys SSL Labs free SSL/TLS testing webpage[6] validating the configuration in use.

The admin area of the homepage is protected using the "WP Password Policy Manager"[7] for WordPress. The password policy enforces passwords consisting of at least 10 characters, containing lowercase and uppercase characters, as well as at least one numeric digit, and at least one special character. For usability reasons, passwords are only required to be changed at least once per year.

4.5 Databases

The Project Portal has a dedicated MySQL database. The information contain in this database is only required by the WordPress framework.

4.6 Back up

Automated Backups of the Public Homepage including databases are performed daily by the IT department of AIT.

4.7 Disk Usage and Bandwidth

The Public Homepage is updated regularly and potentially large files might be uploaded to and downloaded from it. The Public Homepage contents types include news, publications, personal partner pages, photos, and documents. Based on experience from numerous previous projects, the web server and its implementation have the disk space and Internet bandwidth to handle these types of content and to afford the level of concurrency expected in the project. A monitoring tool sends low disk space alerts and daily reports about all servers running to the Service Desk of the Digital Safety & Security Department of AIT.

4.8 Statistics - Traffic

Detailed monitoring of the traffic to the homepage will be done using Piwik[8], which is an open source web analytics software. The used Piwik instance is hosted locally at AIT to avoid the usage of cloud based trackers and analysis tools such as Google Analytics.

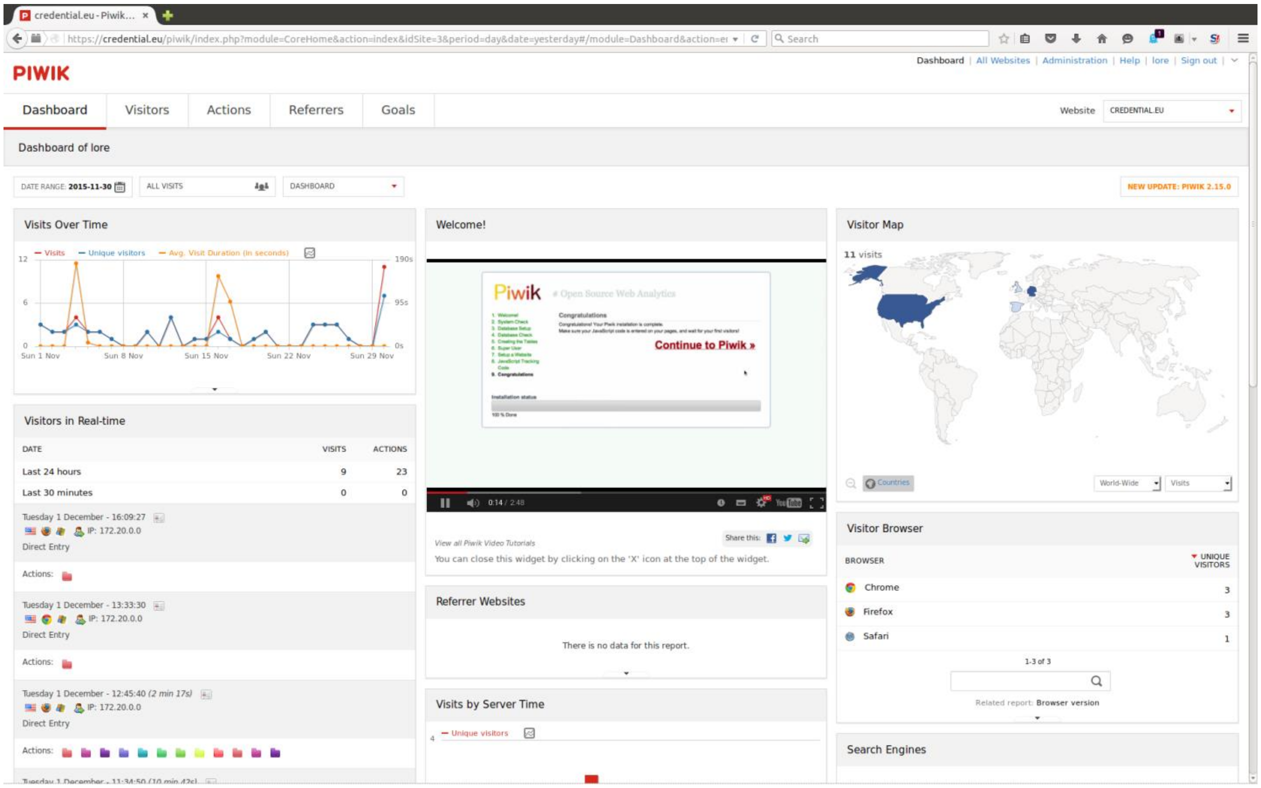
Piwik offers a big amount of features such as real time flow of visits to the homepage, geolocation, pages transition, site speed and pages speed reports, and track traffic from different search engines, which will allows us to analyse and maximise the dissemination impact of the webpage.

[6] https://www.ssllabs.com/
[7] https://wordpress.org/support/view/plugin-reviews/wp-password-policy-manager?filter=5
[8] http://piwik.org/

A screenshot of the Piwik output is provided in **Figure 3**.

Piwik can be accessed under:

https://credential.eu/piwik/index.php



DATE	VISITS	ACTIONS
Last 24 hours	9	23
Last 30 minutes	0	0

Tuesday 1 December - 16:09:27
IP: 172.20.0.0
Direct Entry
Actions:

Tuesday 1 December - 13:33:30
IP: 172.20.0.0
Direct Entry
Actions:

Tuesday 1 December - 12:45:40 *(2 min 17s)*
IP: 172.20.0.0
Direct Entry
Actions:

Tuesday 1 December - 11:34:50 (10 min 42s)

View all Piwik Video Tutorials

Share this:

You can close this widget by clicking on the 'X' icon at the top of the widget.

There is no data for this report.

BROWSER	UNIQUE VISITORS
Chrome	3
Firefox	3
Safari	1

1-3 of 3

Related report: Browser version

Figure 3: Screenshot of Piwik statistics for the CREDENTIAL homepage

5 Project Electronic Communication Platform

5.1 CREDENTIAL SharePoint

The CREDENTIAL consortium decided to use as the main team collaboration tool the SharePoint 2013[9] software, which is provided and maintained by the project coordinator (AIT). SharePoint 2013 is a web-application platform, which offers an online archive of project documents and information, continuously accessible by the participants and provides version tracking and collaborative editing.

5.1.1 Compatibility

SharePoint 2013 is compatible with Windows 10, Windows 8.1, and Windows 7 and with the most popular browsers, in particular Internet Explorer, Chrome, and Firefox.

5.1.2 Domain

The domain to access the CREDENTIAL SharePoint platform is:
https://portal.ait.ac.at/sites/SQT/credential/

5.1.3 Security guidelines

Sensitive information is protected through strong security and access control mechanisms. The SharePoint Portal Site is protected via SSL (HTTPS) and an F5 Firewall Access Policy Manager[10]. Authentication of users is done using usernames and passwords.

5.1.4 Databases

- SharePoint portal Site Collection Content DB is MS SQL.
- every Site Collection has an own Content Database.

5.1.5 Back up

This Content Databases are backed up daily (DIFF), and every Saturday (FULL).

5.2 CREDENTIAL Redmine

The CREDENTIAL consortium decided to use a Project Management software, which is provided and maintained by the project coordinator (AIT). Redmine[11] is a flexible web application platform, which

[9] https://products.office.com/en-us/sharepoint/sharepoint-2013-overview-collaboration-software-features
[10] https://f5.com/products/modules/access-policy-manager
[11] http://www.redmine.org/

includes a Gantt chart, calendar, wiki, forums, multiple roles, and email notification. The CREDENTIAL Redmine can be reached under:

https://credential.eu/requirements

The Redmine instance is hosted by the Service Desk of the Safety & Security Department of AIT, and will be updated on a regular basis.

5.2.1 Security Guidelines

Similar to Section 4.4, the Redmine instance is protected with an SSL/TLS certificate. The authentication of users is done based on usernames and passwords, where the passwords need be at least 8 characters.

5.2.2 Database

The Project Portal has a separate MySQL database.

5.2.3 Backup

Automated Backups of the Redmine instance including databases, are performed once daily by the Service Desk of the Digital Safety & Security Department of the AIT.

5.3 CREDENTIAL GitLab

The CREDENTIAL consortium decided to use a Source Code Management system, which is provided and maintained by the project coordinator (AIT). Gitlab provides issue tracking, source code and pull-request management, wiki, forums, multiple roles, and email notification. The CREDENTIAL Gitlab setup can be reached under:

https://git.credential.eu

5.3.1 Server

The GitLab server is hosted on a VM (Virtual Machine) located at the Digital Safety & Security Department of AIT VM Cluster with the configuration: 1GB RAM, 20 GB HDD, single-core and can be upgraded easily if necessary.

The VM is running Ubuntu as an operating system, as well as a Nginx web server, a PostgreSQL database, and a GitLab installation. All software installations will be upgraded on a regular basis, and therefore concrete version numbers are omitted in this document.

5.3.2 Security Guidelines

This is as in § 4.4.