EU-SEC Workshop & Tutorial:
Continuous Auditing-based Certification

Berlin

8th Oct 2019

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

Agenda

Time	Session	Speaker(s)
9:30 – 10:00	**Presentation and EU-SEC Introduction**	Jürgen Großmann
10:00 – 10:40	**Introduction to the Continuous Auditing Based Certification (CABC) scheme for Cloud Services**	Alain Pannetrat
10:40 – 11:10	***Coffee Break***	
11:10 – 11:30	**The EU-SEC Continuous Auditing Based Certification pilot**	Ramon Martín de Pozuelo
11:30 – 12:00	**CABC for Cloud Users (CaixaBank)**	Ramon Martín de Pozuelo
12:00 – 13:00	***Lunch Break***	
13:00 – 13:30	**CABC for Certification Authorities**	Alain Pannetrat
13:30 – 14:00	**CABC for CSPs**	Björn Fanta
14:00 – 14:30	**CABC for Technology Providers**	Christian Banse
14:30 – 15:00	***Coffee Break***	
15:00 – 15:30	**CABC for Auditors**	Tatu Suhonen
15:30 – 16:00	**Round Table discussion (Questions and Answers)**	Questions and Answers
16:00 – 16:30	***Networking coffee***	

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

Introduction to EU-SEC

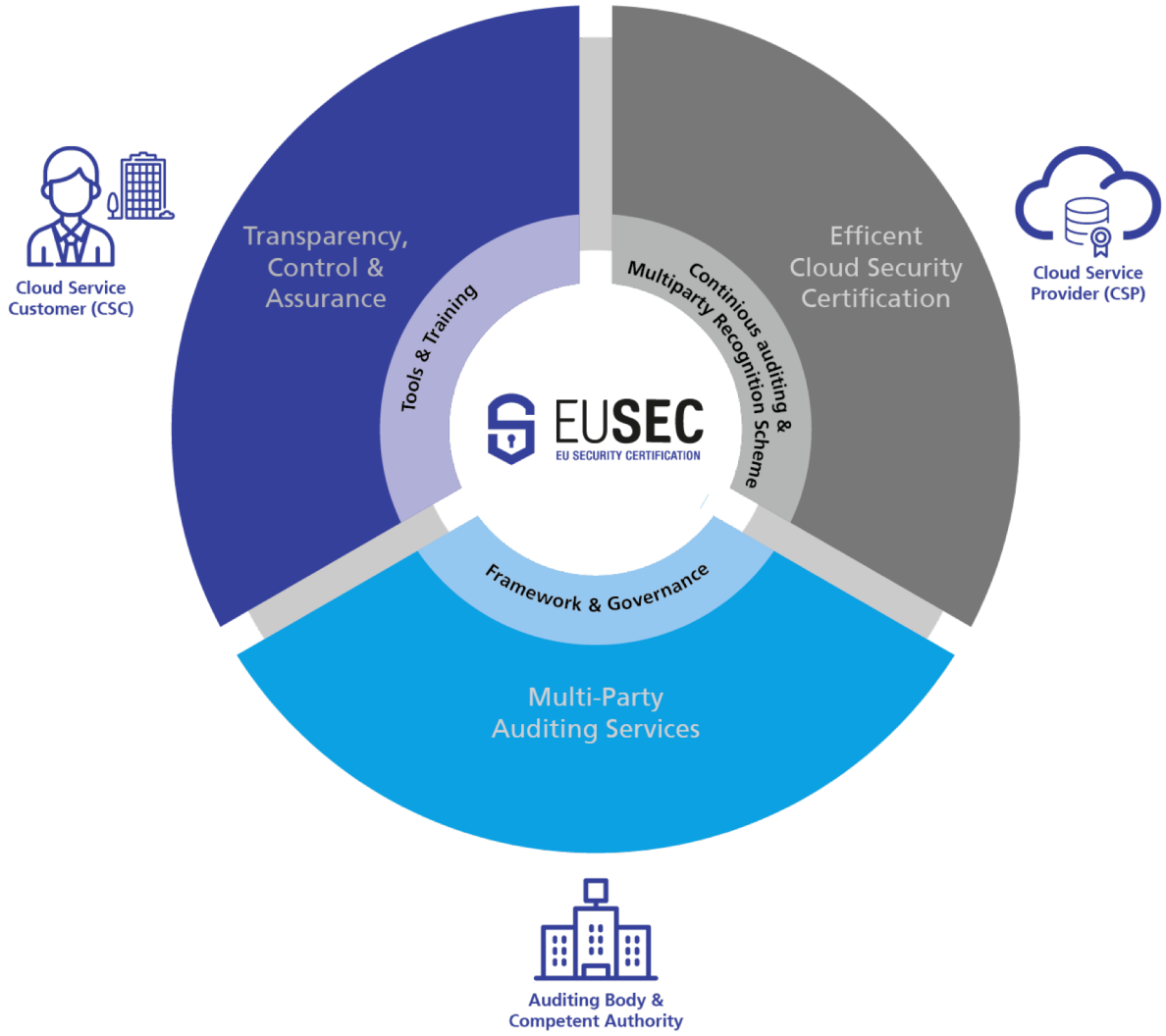
Jürgen Großmann (FRAUNHOFER)

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

Trust in Cloud by Certification
The European Security Certification Framework (EU-SEC)

EU-SEC aims to create a framework under which existing certification and assurance approaches can co-exist. It has a goal to improve the business value, effectiveness and efficiency of existing **cloud security certification schemes**.

- **Multiparty Recognition Framework (MPRF)** for cloud security certifications,
- **Continuous Auditing-based Certification (CAC)**
- **Privacy Code of Conduct (PLA CoC)** , and



This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

Project Set Up and Partners
A successful cooperation under the hood of a common project

EUSEC
EU SECURITY CERTIFICATION

Funded by **EU Horizon 2020**, a funding programme created by the European Union to support and foster research in the European Research Area

9 Partners (including CSPs, Cloud Users, Auditors, Scheme Owners and Researchers)

Duration: January 2017 - December 2019

Web: https://www.sec-cert.eu/
Contact: *contact@sec-cert.eu*
Twitter: @EU_SEC

CaixaBank
cloud security alliance® CSA
Fabasoft
Fraunhofer FOKUS
Fraunhofer AISEC
MINISTERSTVO FINANCIÍ SLOVENSKEJ REPUBLIKY
REPUBLIKA SLOVENIJA MINISTRSTVO ZA JAVNO UPRAVO
NIXU cybersecurity.
pwc | Deutschland
sixsq

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

EU-SEC Objectives
Increasing trust, efficiency and sustainability

- Increase user trust in Cloud Service Providers by
  - **defining principles, rules and processes for mutual recognition** between different certification schemes indicating security and privacy level.
  - **defining an approach for higher frequency security audits** for high security applications
- Support EU-SEC's long term sustainability by initiating the process **for the trans-European adoption of the EU-SEC framework and of the format used to express security requirements, controls and audit results.**


Photo by Noah Busher on Unsplash

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

EU-SEC Achievements
Applicability, flexibility and tool support

- **Cross-industry applicability** of the EU-SEC framework.
- **High level of security and privacy assurance and control** while the CSP enhances the Cloud Service, continuously.
- Consolidated framework which can be **adapted to new technical, compliance and market requirements**, easily and promptly.
- **Flexible and functional architecture and tools** for cloud security governance, risks management and compliance.


The U.S. National Archives

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

EU-SEC Activities
Define, evaluate, improve and maintain the framework

- Collect and maintain security and privacy requirements relevant to the public and private sector.
- Define the continuous auditing and certification framework and enable it for mutual recognition of existing certification and assurance approaches.
- Develop a governance structure to support trans-European EU-SEC framework adoption. Provide architecture and adapt existing tools to facilitate continuous auditing and control of security and privacy level service.
- Validate the framework with pilot use cases executed by public and private sector partners to ensure its effectiveness, efficiency and market readiness in large-scale demonstrators.
- Strengthen the value proposition, market uptake and long-term sustainability of EU-SEC framework through commercial exploitation, influencing other standardization initiatives and performing strategic awareness and training activities.

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

EU-SEC Business Drivers
Value Proposition for Cloud Service Providers, Auditors and Users

- **Saving money:** MPRF reduces compliance costs
- **Increased efficiency:** MPRF streamlines the compliance approach
- **Improved security**: CACs reduces security risks (higher audit frequency, less auditors approaching your data)
- **Transparency and clarity**: One standard of reference to enable comparison and integration between many different ones
- **Up to date with most recent legislation:** EU-SEC addresses the needs of the EU-Cyber Security Act

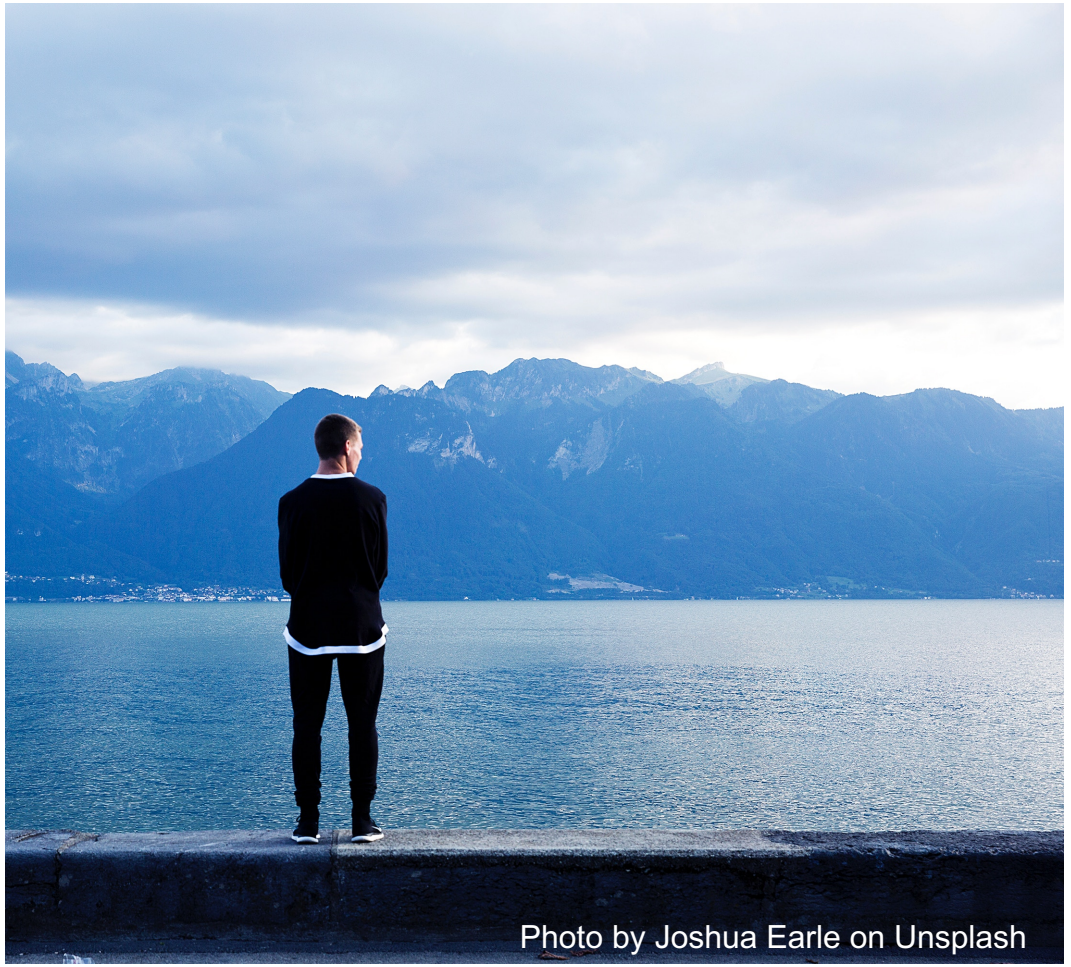


Photo by Joshua Earle on Unsplash

8th October 2019

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

EU-SEC Public Materials
Information portal at www.wec-cert.eu

- **Deliverables**
- **Slide Decks**
- **Whitepapers**
- **Articles**
- **News**
- **Workshops**

Workshop & Tutorial on Multi-Party Recognition in Berlin on 9th October 2019!
Date: Wed., Oct. 09, 2019
Location: Berlin, Germnay

Workshop & Tutorial on Continuous Auditing Based Certification on 8th October!
Date: Tue., Oct. 08, 2019
Location: Berlin, Germany

Workshop on Multi-Party Recognition on 13 May 2019!
Date: Mon., May 13, 2019
Location: Amsterdam, Netherlands

Workshop on Continuous Auditing Based Certification
Date: Tue., Apr. 09, 2019
Location: Barcelona

European Security Certification
Date: Mon., Sep. 10, 2018 to Mon., Sep. 10, 2018
Location: Brussels
The HORIZON 2020 European Security Certification (EU-SEC) project will provide first results for a multi-party recognition framework for cloud services.

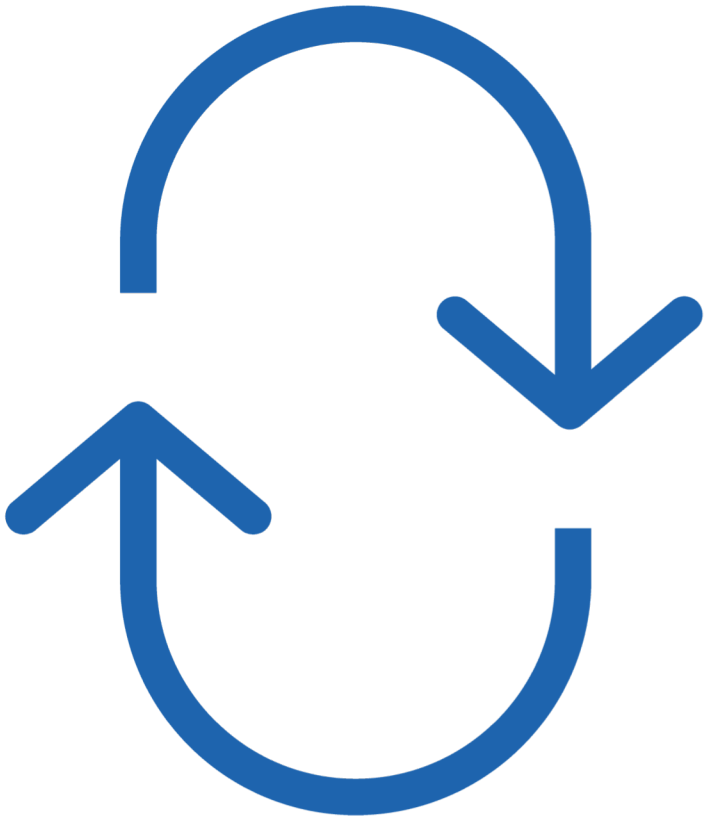
This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

Introduction to the Continuous Auditing Based Certification scheme for Cloud Services

Alain Pannetrat (CSA)

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.


Certification!



But...

For some cloud customers in heavily regulated industries such as banking or healthcare, (bi-)annual certificates are not good enough.

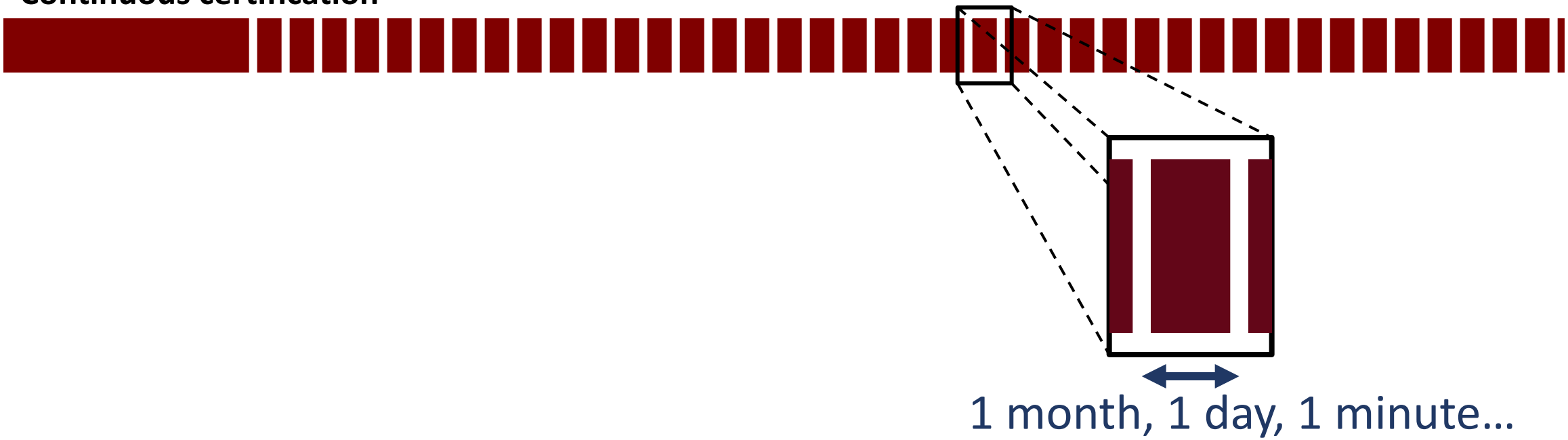
They need **CONTINUOUS** assurance.

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

EU-SEC introduces: continuous audit-based certification

“Traditional certification”

“Continuous certification”



“Traditional” vs. “Continuous”

EUSEC
EU SECURITY CERTIFICATION

“Traditional” certification	“continuous” audit-based certification		
Control objectives	Security Attributes	Metrics	Service Level Objective & Service Qualitative Objective
Manual evaluation	Automated evaluation		

A requirement: automate as much as possible

Traditional certification evaluates “control objectives”, continuous certification targets “service level objectives” or “service qualitative objective”, which can be assessed automatically more easily.

CONTROL OBJECTIVES

“Business continuity plans shall be documented and tested regularly”

SECURITY ATTRIBUTES

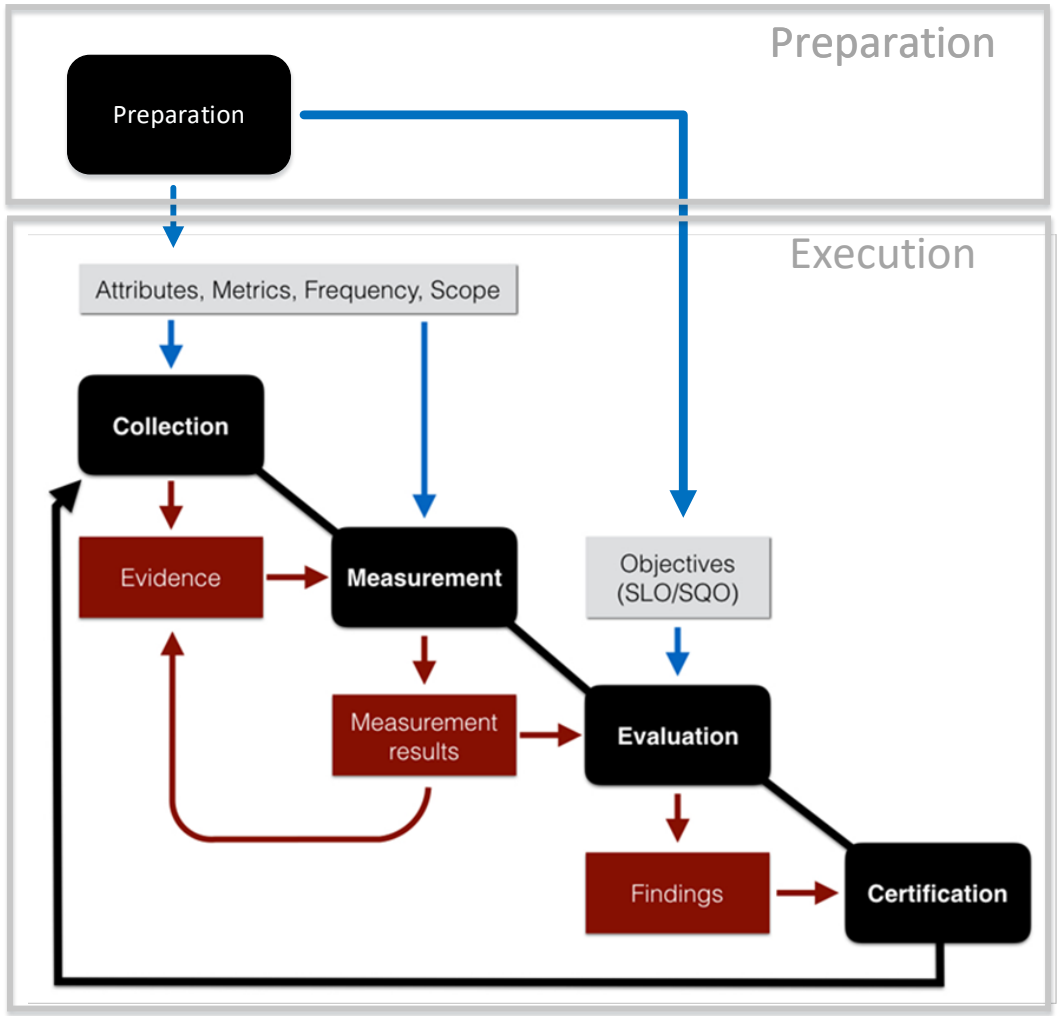
- Percentage of backup restoration tests per month
- Percentage of backup restoration failures per month
- Maximum recovery time
- Recovery point actual (RPA)

Check: Monthly, daily, hourly…

for research, technological development and demonstration under grant agreement no 731845.

Continuous Auditing-based Certification
Methodology – phases

1. **Preparation**: mainly devoted to the operationalisation of the controls
   - This initial setup is performed once
   - SLO's and SQO's are defined to describe controls
   - The output are: scope, SLO/SQO and frequency of assessment.
2. **Collection**: devoted to the collection of evidence
3. **Measurement**: the metrics are applied to the collected evidence.
4. **Evaluation**: it checks if an objective is fulfilled.
5. **Certification**: according to the result of the evaluation, a certificate is granted or not.

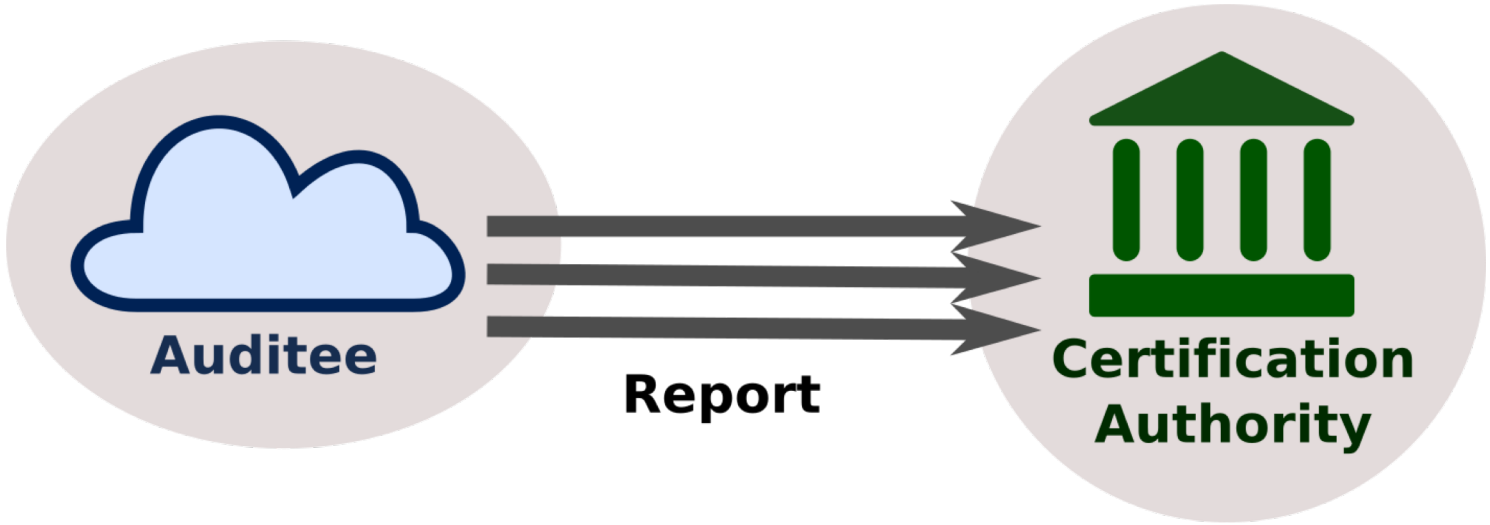


This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

3 assurance levels

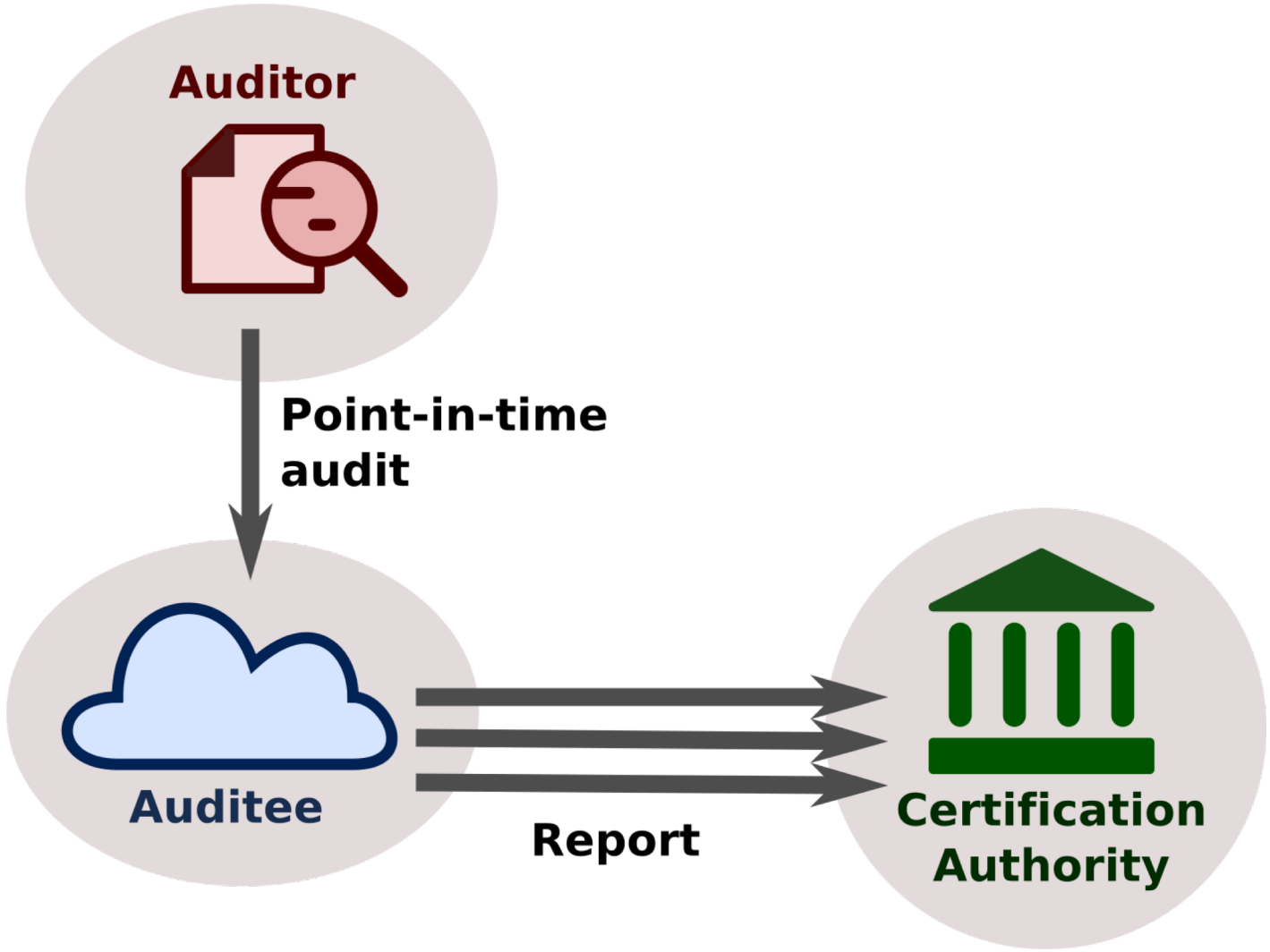
This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

Level 1: Continuous self-assessment



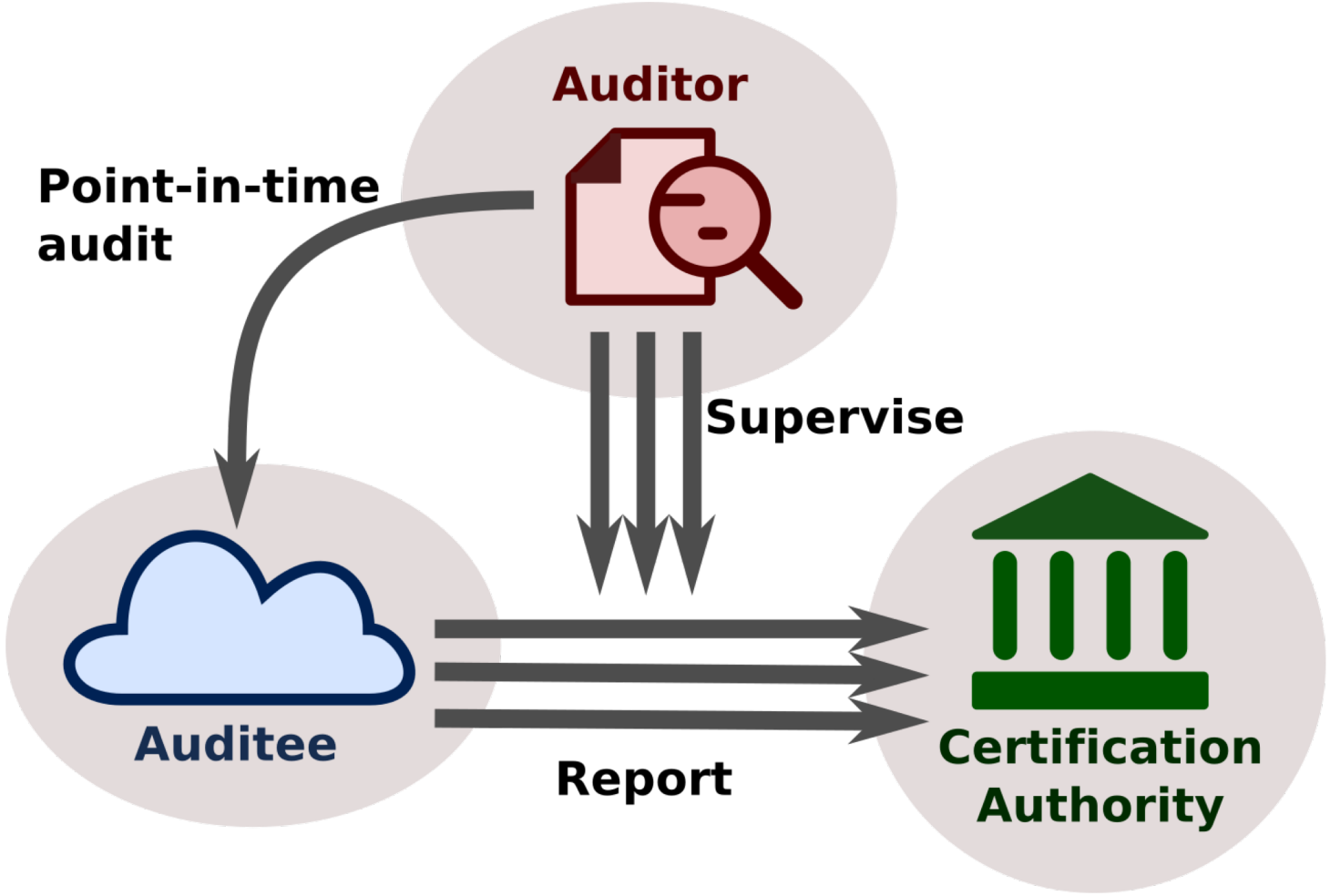
This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

Level 2: Extended certification with continuous self-assessment



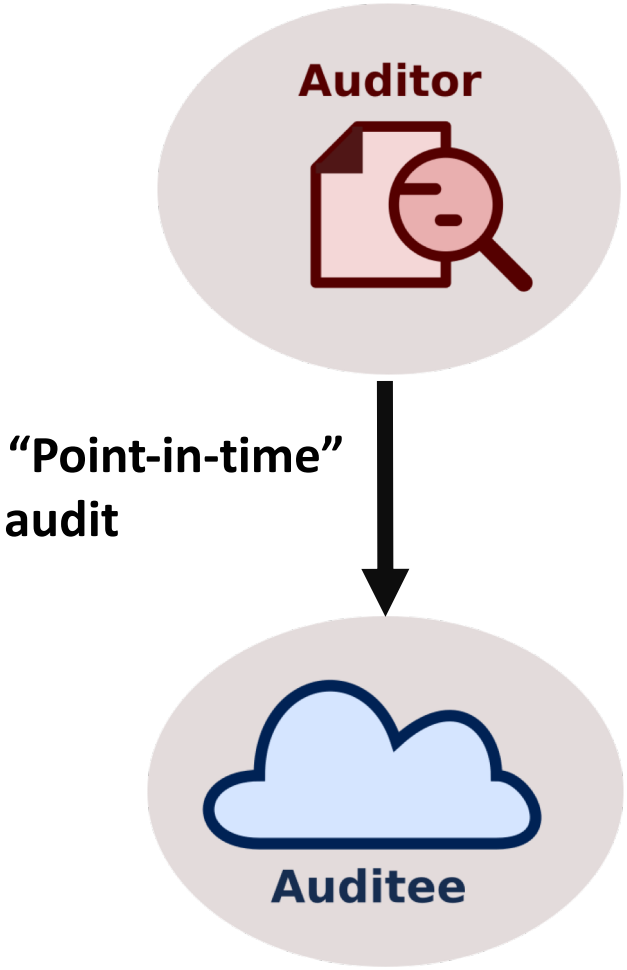
This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

Level 3: Continuous certification



This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

Continuous certification: preparation

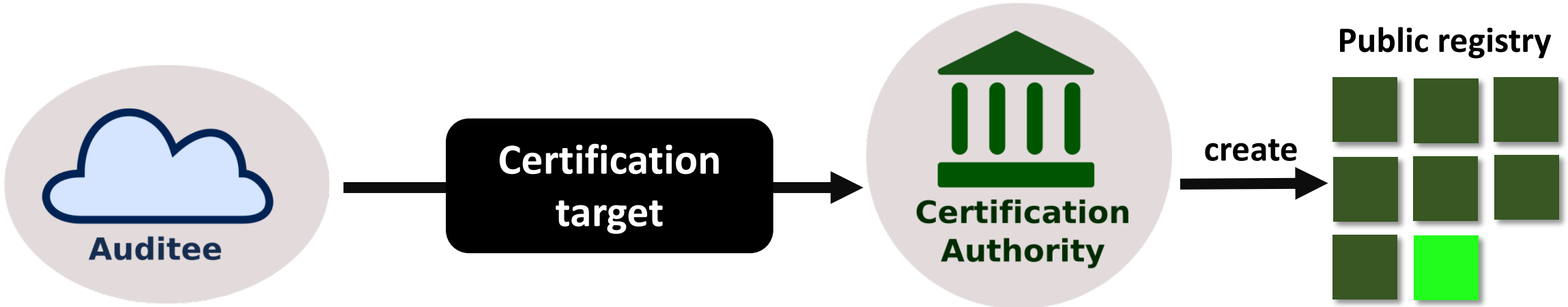


Output:

- A traditional certificate
- A continuous certification target
  - Scope
  - SLO & SQO
  - Frequencies of assessment
- Audit tool validation

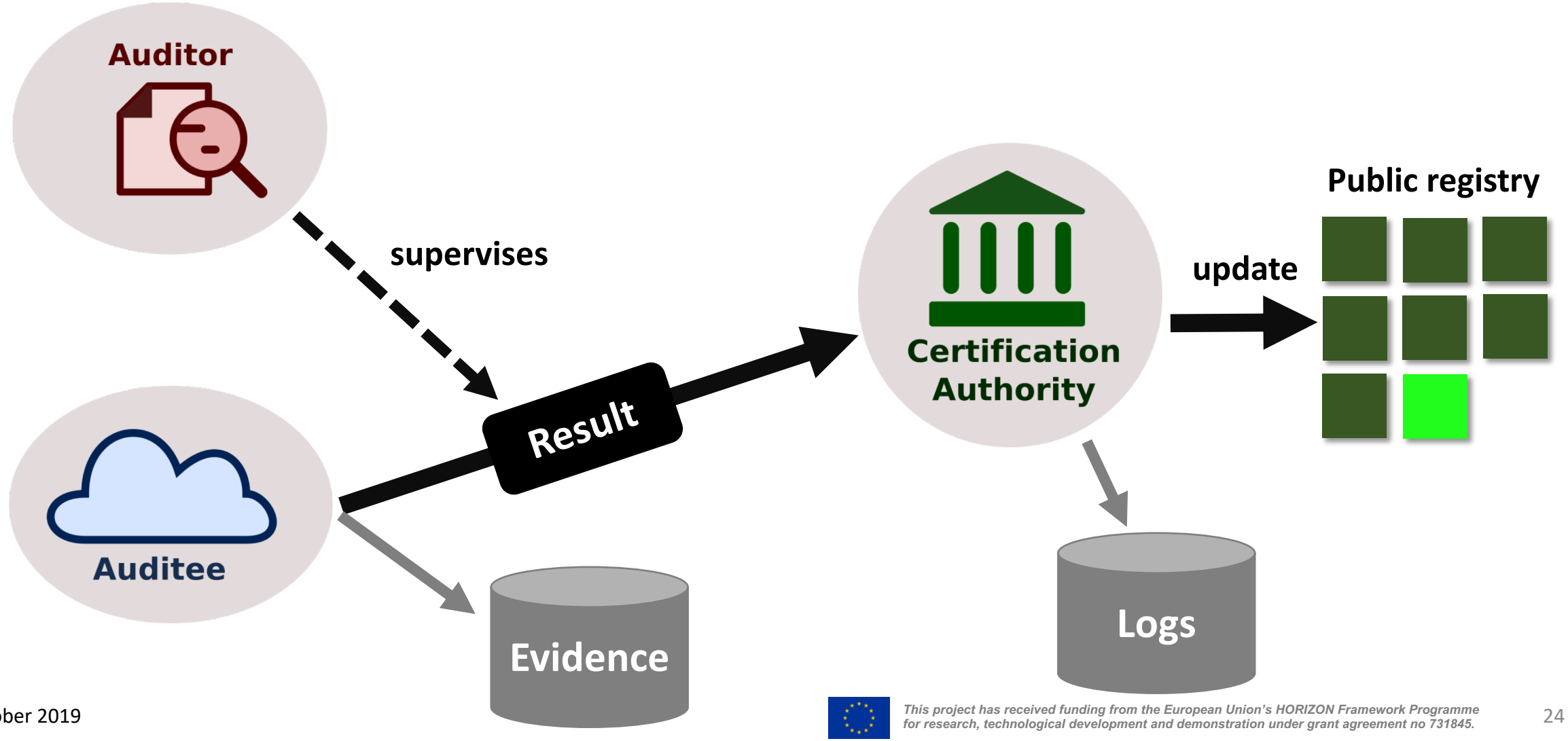
This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

Continuous certification: initialization



This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

Continuous certification: continuous assessment



This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

The EU-SEC Continuous Auditing Based Certification pilot

Ramon Martín de Pozuelo (CAIXABANK)

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

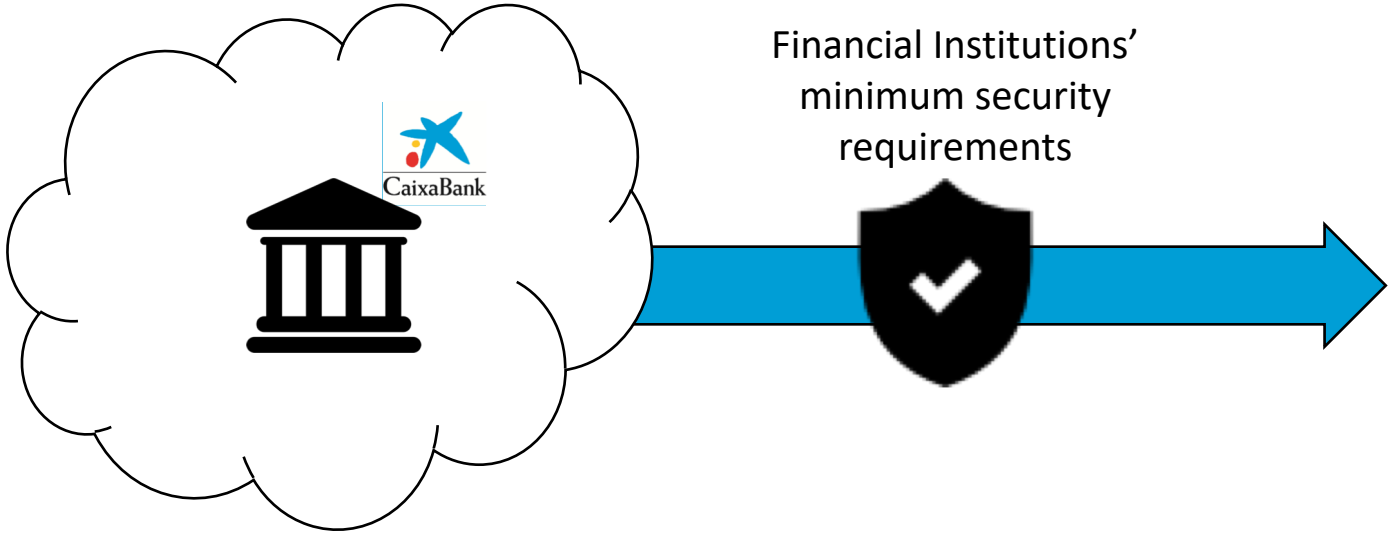
Description of the Pilot
Introduction

EUSEC
EU SECURITY CERTIFICATION

Trusted information sharing — Financial institutions need to report sensible information to the regulators in a reliable and trusted way.

Collaboration — In some cases, this exchange of information can involve multiple entities and organisations.

Industrial gap motivation: Lack of a continuous auditing service that verifies that the cloud provider running the information sharing service actually complies with Financial Institutions' requirements.



Goal: Continuous auditing of security requirements in a **Financial Information SHaring (FISH)** application with EU-SEC platform.

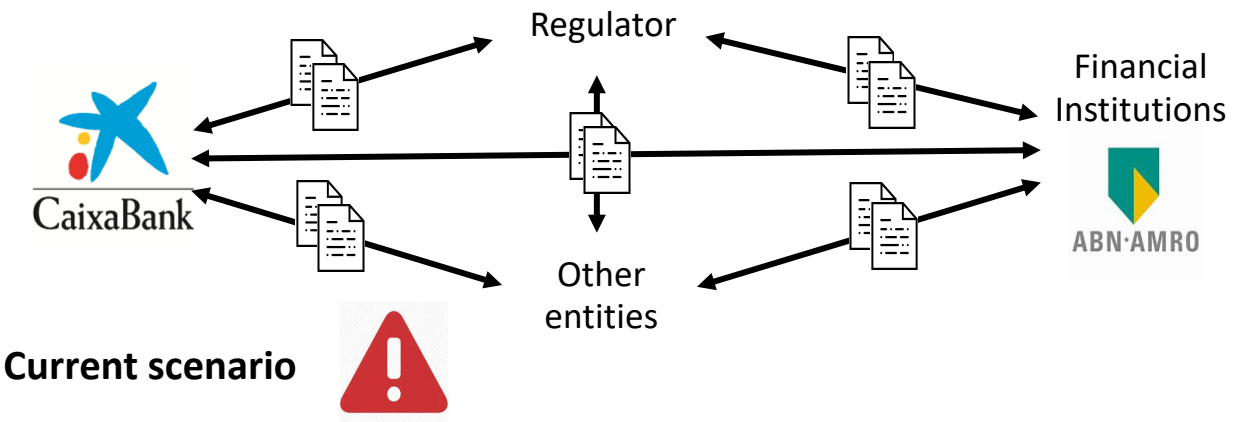
This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

Description of the Pilot
Introduction

Current scenario and problem statement:

- Regulatory entities **require banks to share information.**
- **Regulators may ask CaixaBank for confidential information** of accounts:
  - **Incident reporting** with information of mule accounts for fraud and money laundering, terrorism, etc.
  - **Periodic reports** about security and privacy projects and procedures.

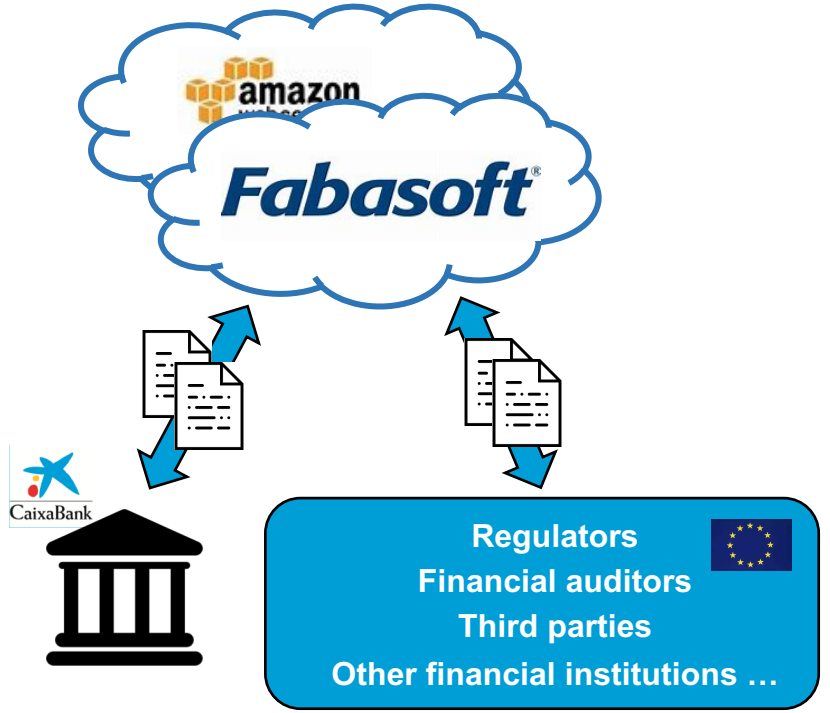
- Information is **shared across groups of regulators/banks**:
  - A simple repository hosted by a bank cannot be trusted by others.
- This may lead to **bad practices and/or onerous document management**:
  - Report sensitive information via mail, physical sharing of information,…



FISH: Neutral European service used by both financial entities and regulators.

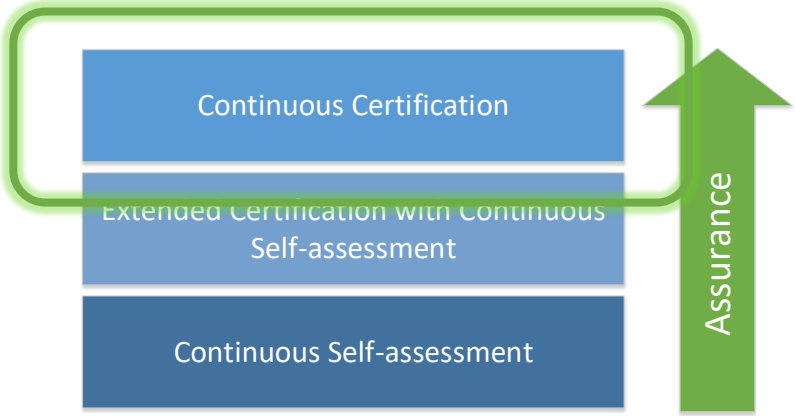
Pilot 2 different approaches:

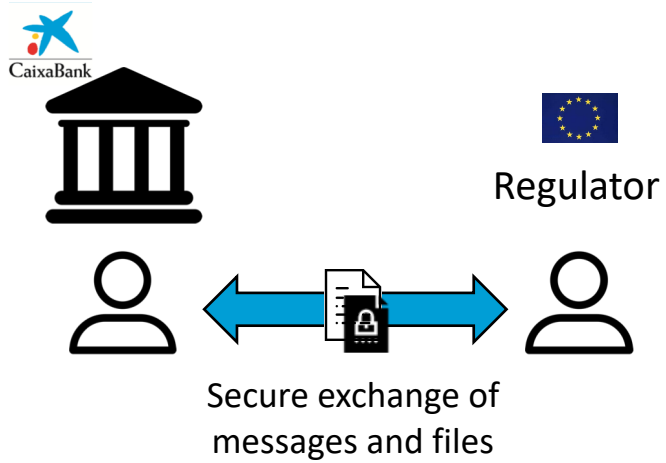
- Custom-tailored FISH over commercial cloud provider (IaaS).
- Fabasoft as a cloud platform for information sharing (SaaS).



This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

Description of the Pilot
Definition

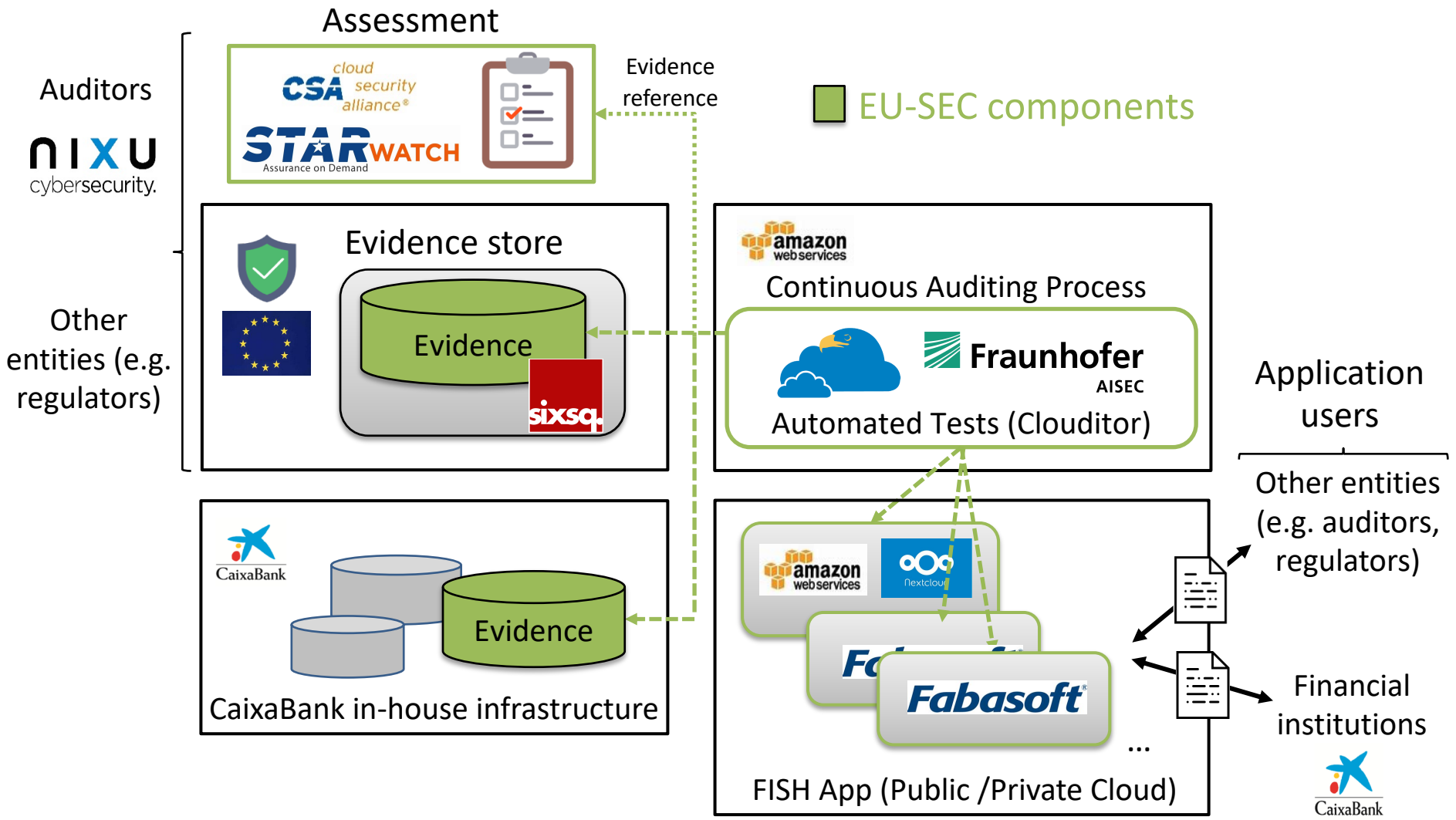




Requirements	Control	CCM code
Data location	The location of all sensitive data and its usage by applications and databases should be known. Moreover, all data should be located within European Economic Space.	CCM-GRM-02, CCM-STA-05
Encryption	All data should be encrypted both at rest and in transit. Cryptographic key management policies and procedures should be defined.	CCM-EKM-04, CCM-EKM-02
Identity Federation	Strong authentication of admin users. Access control and admin profiles should be defined.	CCM-IAM-12
Critical logs in SIEM	All monitoring and evidences logs should be stored in CaixaBank infrastructure.	CCM-IVS-01

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

Description of the Pilot
Architecture

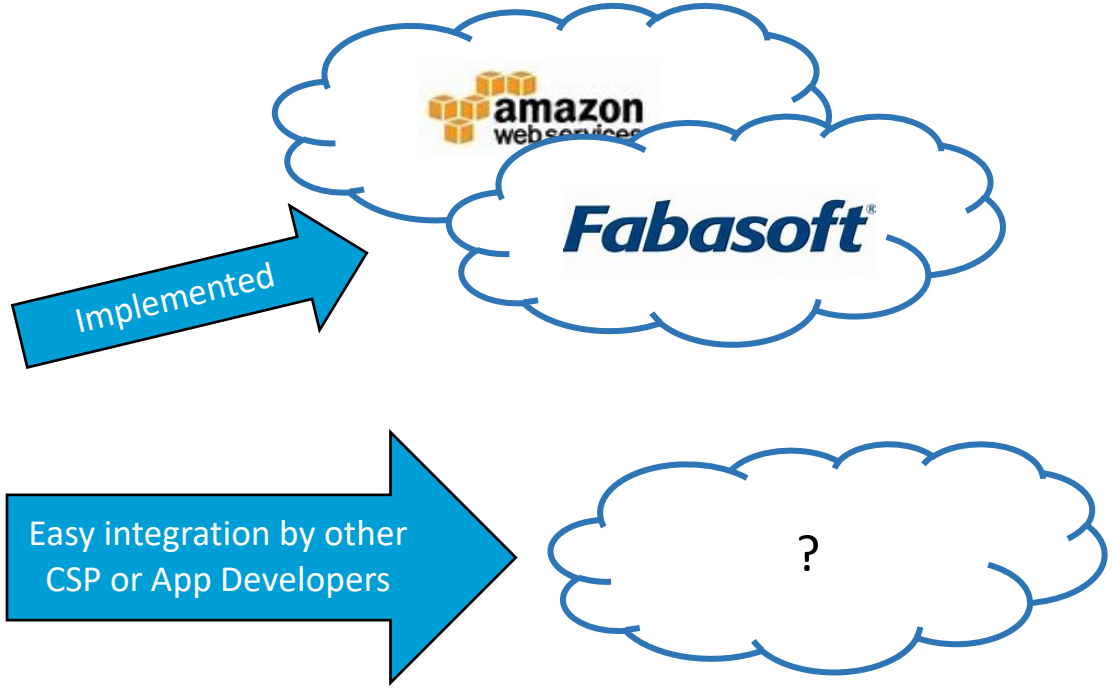


This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

Description of the Pilot
Continuous Auditing API and pilot approaches

- **Continuous Audit API**
  - **CaApiDataLocation**
    GET /{scope}/datalocation/{objectId}/storage/
  - **CaApiEncryption**
    GET /{scope}/encryption/{objectId}/
  - **CaApiIam**
    GET /{scope}/identityfederation/admins/
    POST /{scope}/identityfederation/data/access
    GET /{scope}/identityfederation/{userId}/logins
    GET /{scope}/identityfederation/{userId}/auth
    GET /{scope}/identityfederation/{userId}/groups
  - **CaApiScope**
    GET /scope/

  …

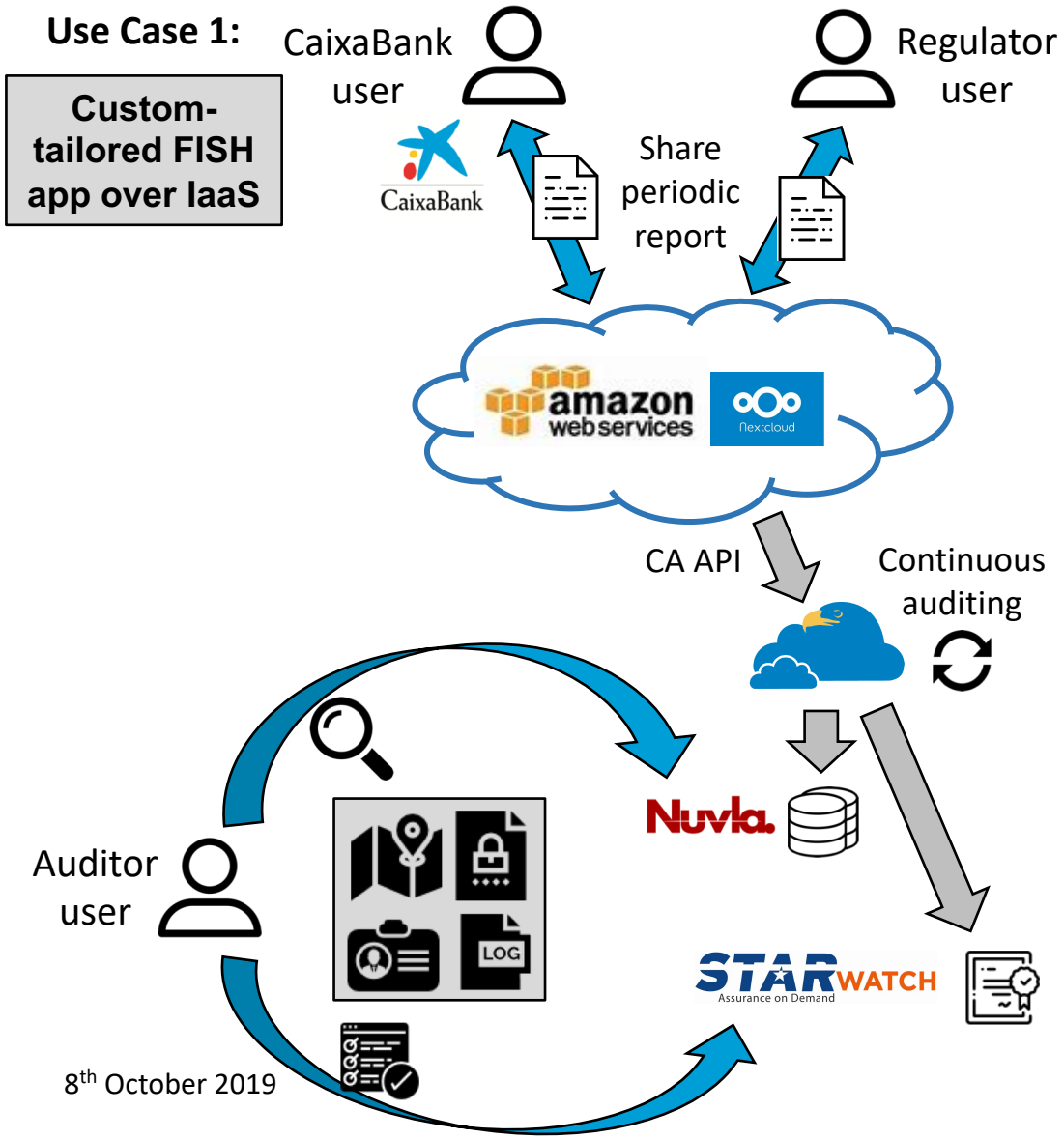


This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

Continuous Auditing Technical Architecture
Use case specification

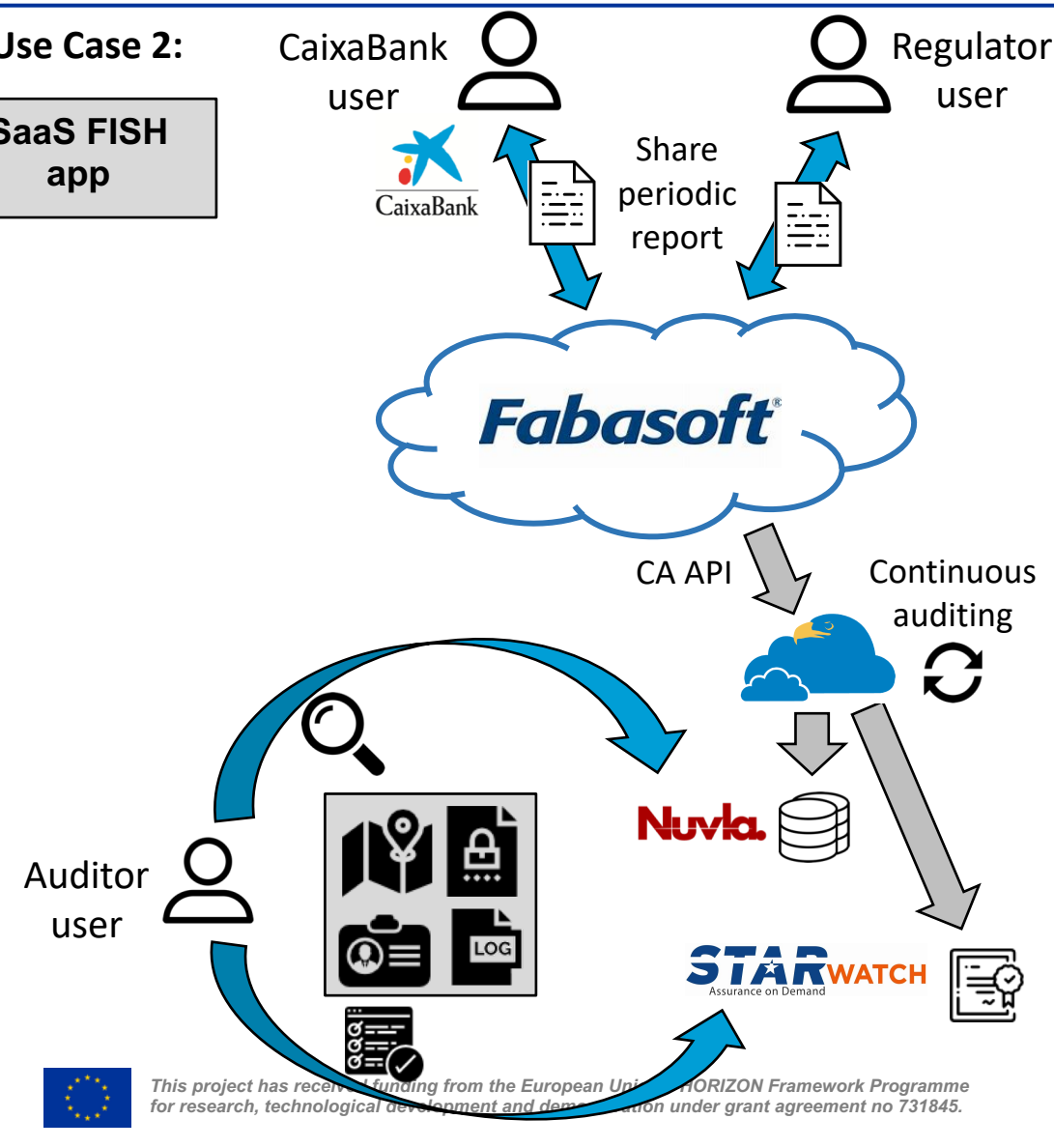
Use Case 1:

Custom-tailored FISH app over IaaS



Use Case 2:

SaaS FISH app



This project has received funding from the European Union HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

Continuous Auditing-based Certification Pilot
Conclusions

- **All tools are correctly integrated and work as expected.**
- **Enabled a continuous audit of 15 SLO/SQOs.**
- **The pilot was demoed multiple times to various stakeholder, testing both success and failures for each SLO/SQO.**

- **The pilot shows that the tools adequate for the task.**
  - **The tools were reviewed and concluded that they are adequate for the purpose of the pilot.**
  - **External stakeholders were also able to use the tools and see how they reported compliance in real-time.**

- **Internal and external stakeholders were able to witness the practicality of continuous audit-based certification.**
  - **The feedback provided by internal stakeholders and the External Advisory Board is generally positive.**

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

Continuous Auditing-based Certification Pilot
Conclusions

- **First step towards the Continuous Auditing based Certification.**
  - Framework & governance model defined.
  - Reference architecture and modules implemented and deployed.
  - FISH use case tested within EU-SEC partners and external stakeholders.

- **Flexibility to define the audit controls and the way to store evidence records.**

- **It does not completely substitute point-in-time auditing.**
- **Still needs some trust on the CSP and the contract with the customer.**

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

Continuous Auditing-based Certification Pilot
Conclusions

EUSEC
EU SECURITY CERTIFICATION

Value proposition & benefits:

Different actors and perspectives

Certification Authority

Assurance and transparency

Continuous certification framework

Methodology

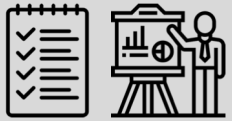
Implementation guidance

- Free material

- Paid training

Public registry of excellence

Auditor



Computer-assisted, automated auditing

Increase productivity

Extend the auditing services

Guidance

Support

Training

Cloud Service Provider

Real-time & automated security control checking

Save money (on the long run)

Competitive advantage from "big players"

Proof of Trustworthiness

Quality / Professionalism label

Easier cooperation / partnerships

Cloud Customer

Certification

Compliance to regulators

Easier Cloud Service adoption

Cost reduction

Demonstrate trustworthiness to own customers

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

Continuous Auditing-based Certification Pilot
Strong partners allow for commercial kick off

- **CSA**: Long term provision and maintenance of the Continuous Auditing-based Certification scheme
- **NIXU, PWC:** Provision of consultancy and audit services dedicated to Continuous Auditing-based Certification
- **Fraunhofer, SIXSQ and CSA**: Provision of tool to drive the operationalization
  - StarRegistry: Mean to publish and maintain Certificates from Continuous Auditing-based Certifications.
  - Clouditor: Cloud Compliance Tool to automatically check the compliance status of a cloud service.
  - Nuvla: Portal for the management and analysis of evidence records, both for supporting the continuous auditing process and for rapid visual assessment of compliance.
  - Continuous Auditing API: Standardized access to Cloud Service Provider security controls information
- **Fabasoft, CAIXA:** Initial adopters of the Continuous Auditing-based Certification

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

Continuous Auditing-based Certification Pilot
References

- Deliverables
  - EU-SEC D2.2 – Continuous Auditing Certification Scheme
  - EU-SEC D5.1 – Pilot Definition
  - EU-SEC D5.2 – Pilot Implementation and Testing of Continuous Auditing
  - EU-SEC D5.3 – Analysis of Pilot Results

- White Paper
  - Continuous Auditing based Certification white paper

- Scientific Papers
  - Continuous Location Validation of Cloud Service Components
  - A Process Model to Support Continuous Certification of Cloud Services
  - Towards Continuous Security Certification of SaaS Applications Using Web Application Testing Techniques
  - Evaluating the Performance of Continuous Test-based Cloud Service Certification

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

CABC for Cloud Users

Ramon Martín de Pozuelo (CAIXABANK)

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

CABC for Cloud Users

- **Cloud users should be the main promoters of CABC**
  - **Do all cloud users need CABC?**
  - **Customers of sectors that deal with sensitive critical information (Financial, Health, Public Adm., etc.)**

- **Certification and compliance**
  - **Demonstrating cloud security control enhancement to regulators.**
  - **Aligned with CSP CERT WG recommendations for the implementation of the CSP certification scheme.**

- **Security as a business value**
  - **Demonstrate trustworthiness to own customers**

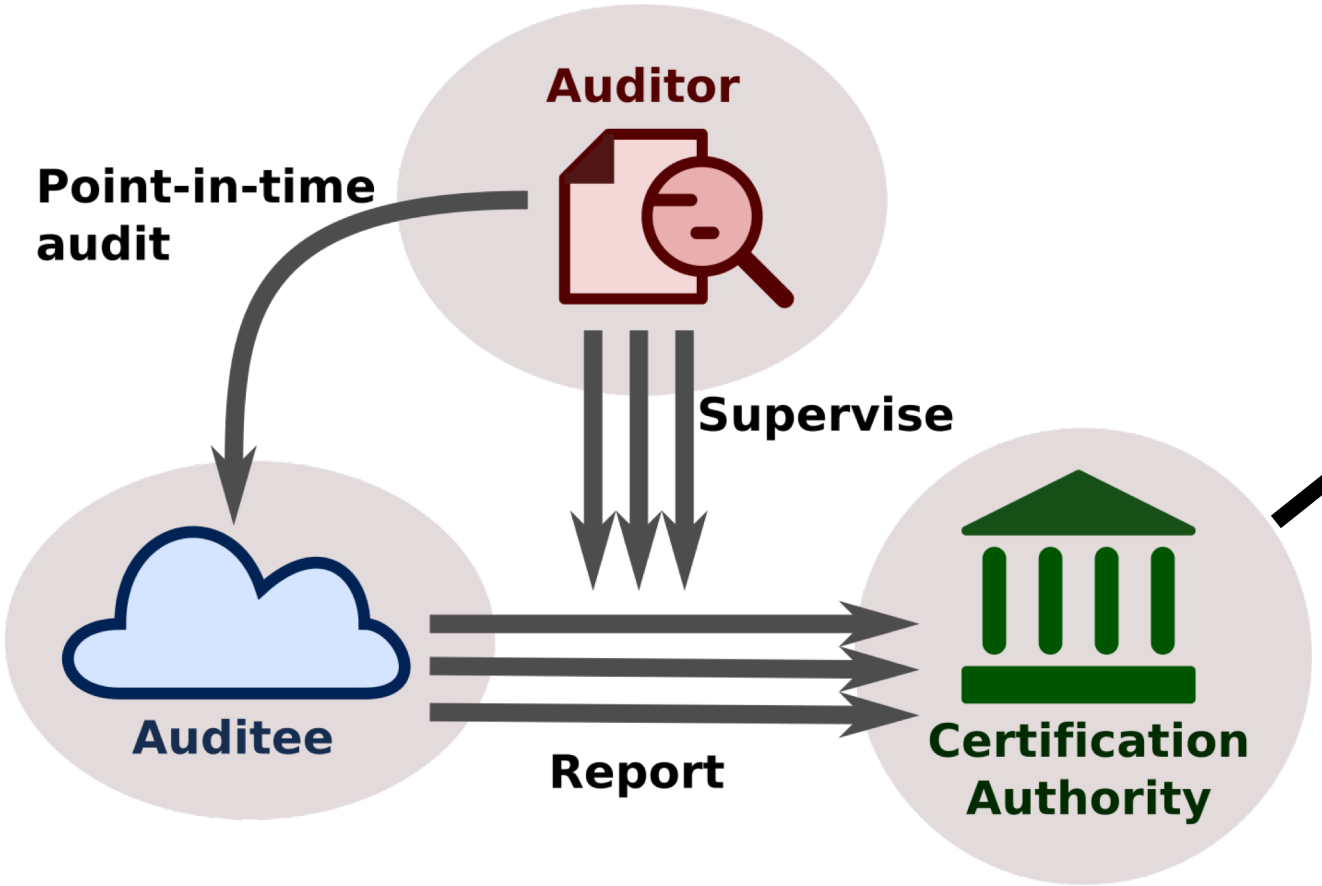
- **Easier Cloud Service adoption**
  - **Access to real-time assurance of CSPs**
  - **Streamline the CSP validation**
  - **Cost reduction**

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

CABC for Certification Authorities

Alain Pannetrat (CSA)

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.



- Accreditation of CBs
- Certification registry
- Complaints
- Standardisation

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

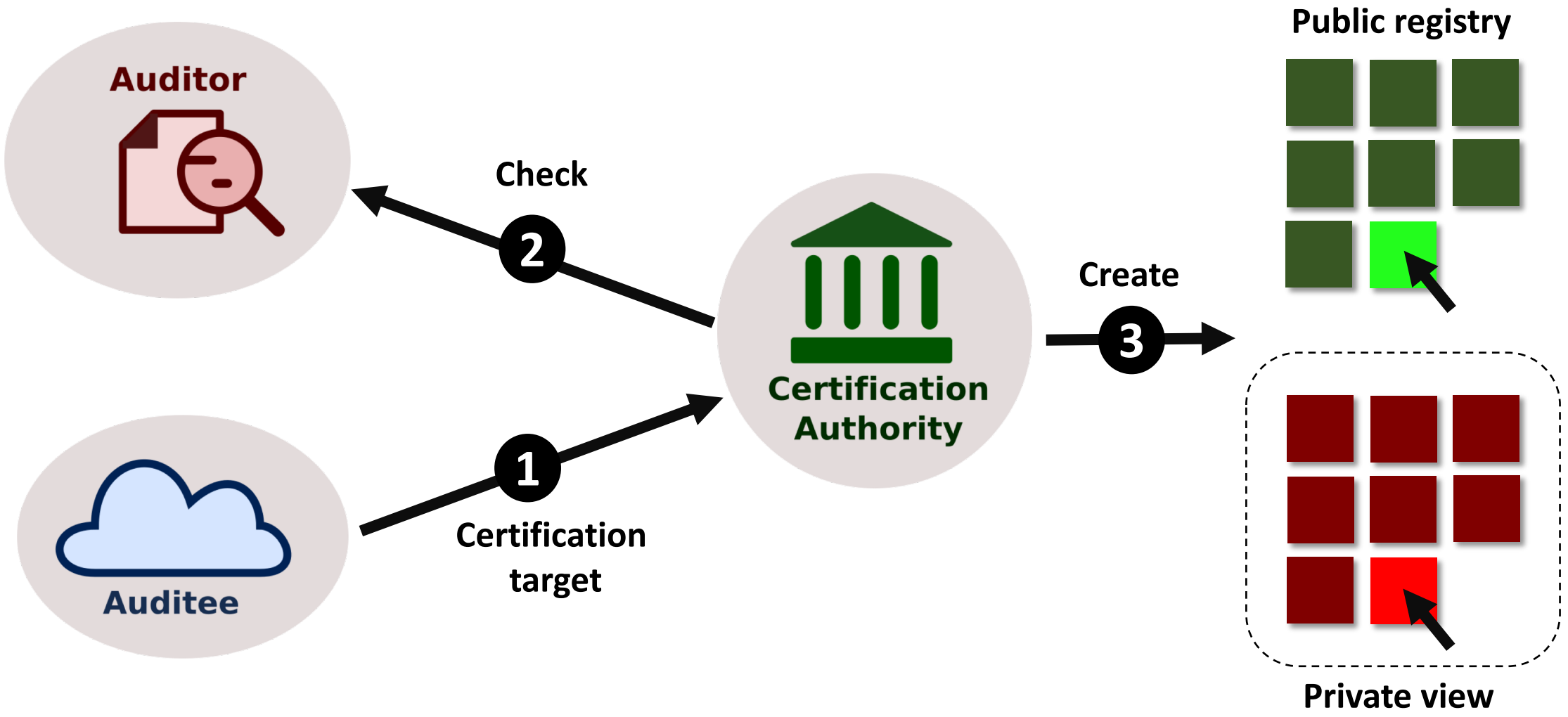
Accreditation of certification bodies

- Auditors will need extended skills
  - Tool validation
  - Monitoring

- CA to maintain a public registry will list accredited certification bodies.

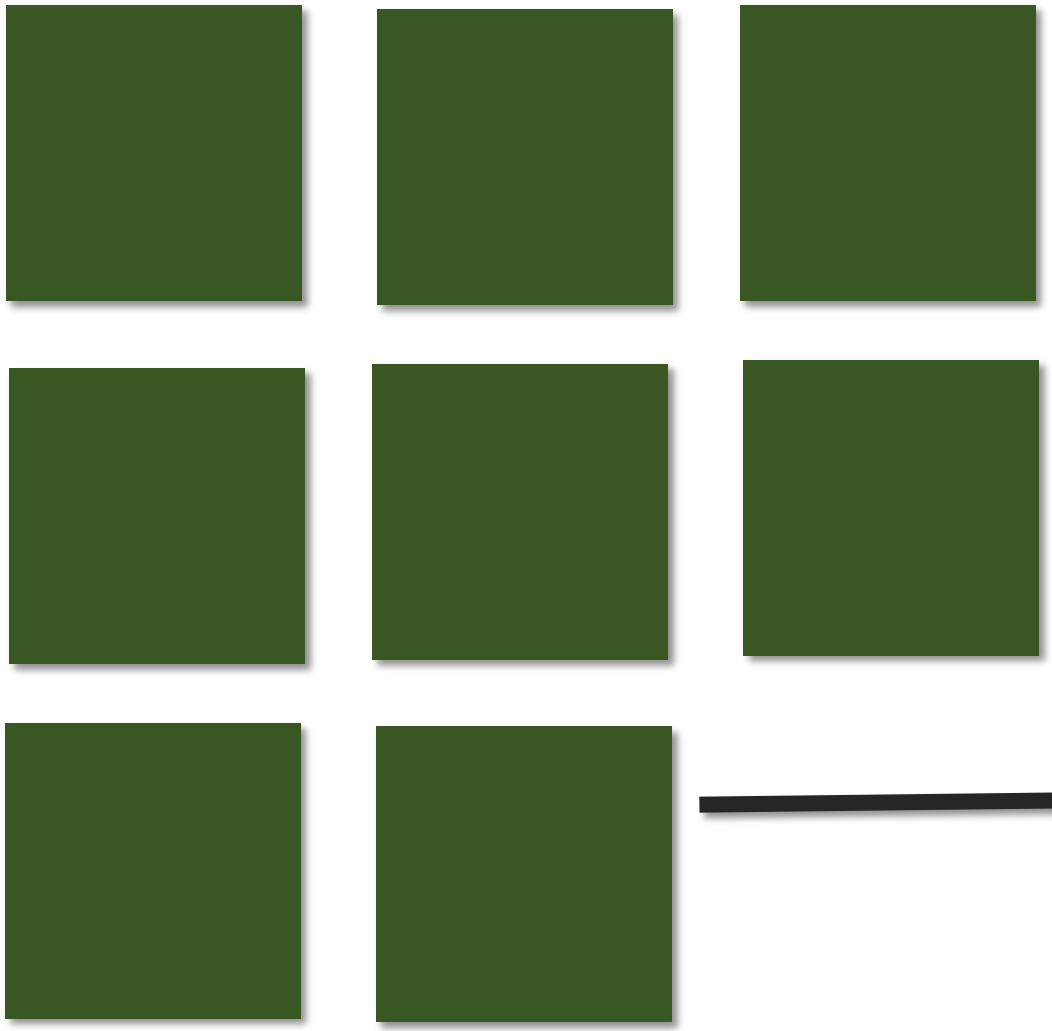
This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

Certification registry: initialization



This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

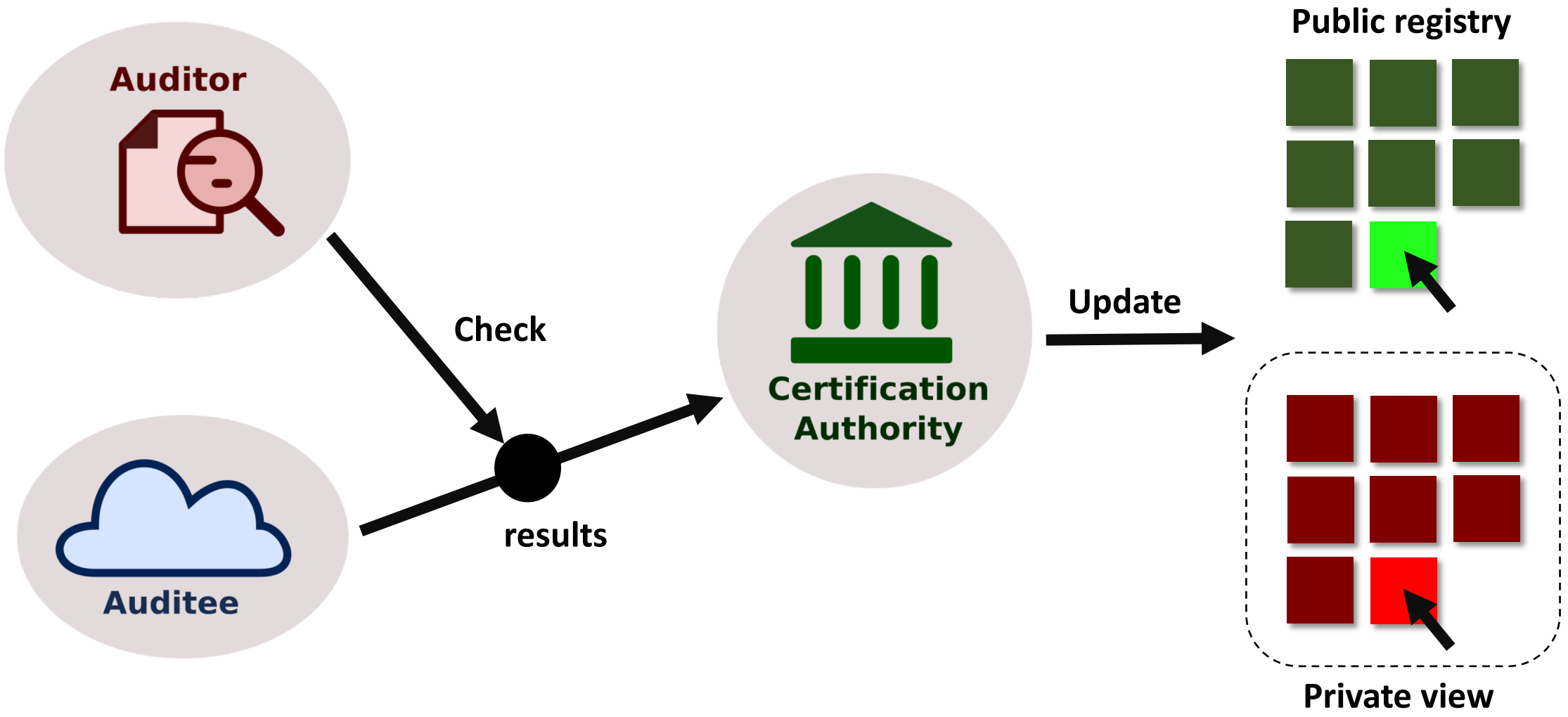
Public registry



- Identity of CSP and scope
- The start and end date
- The last verification date
- The state of the assessment:
  - Pending
  - Ended
  - Running/Valid

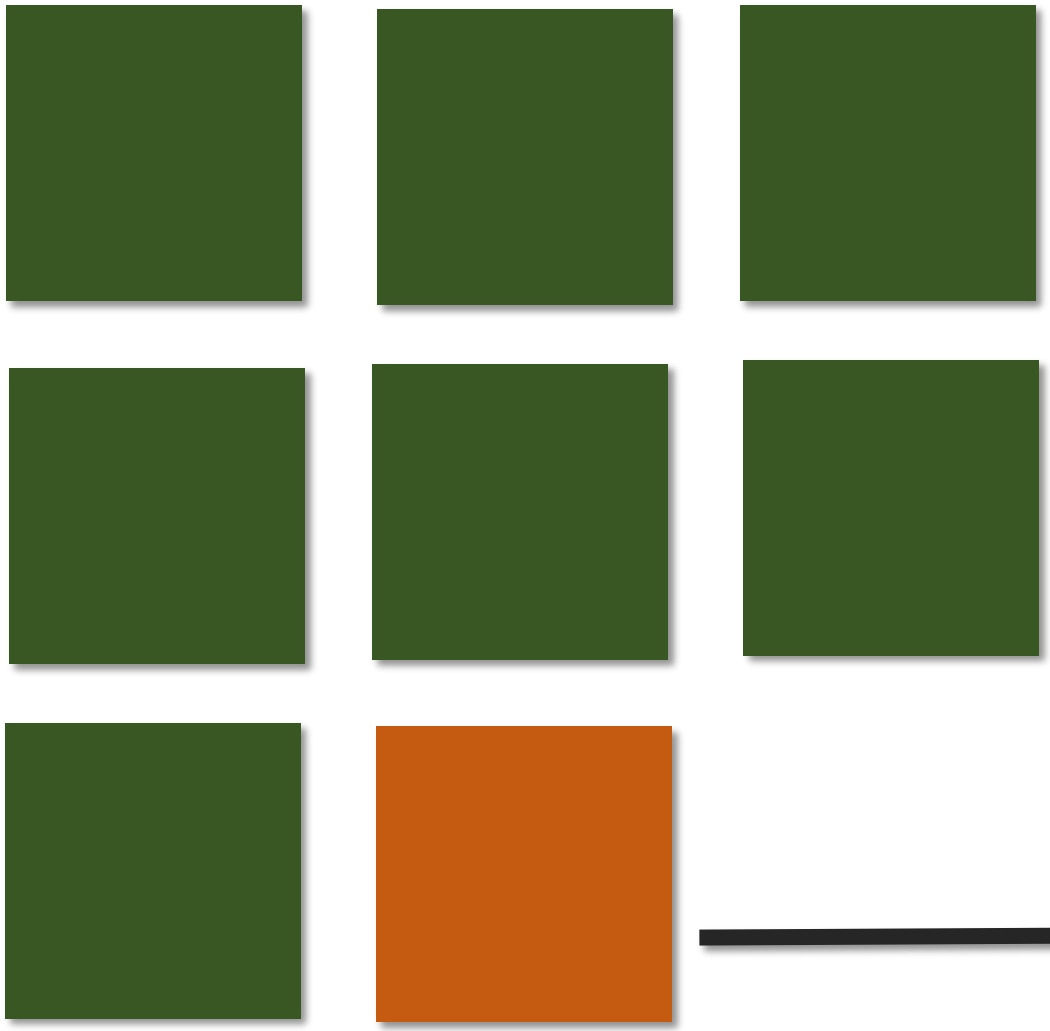
This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

Certification registry: updates



This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

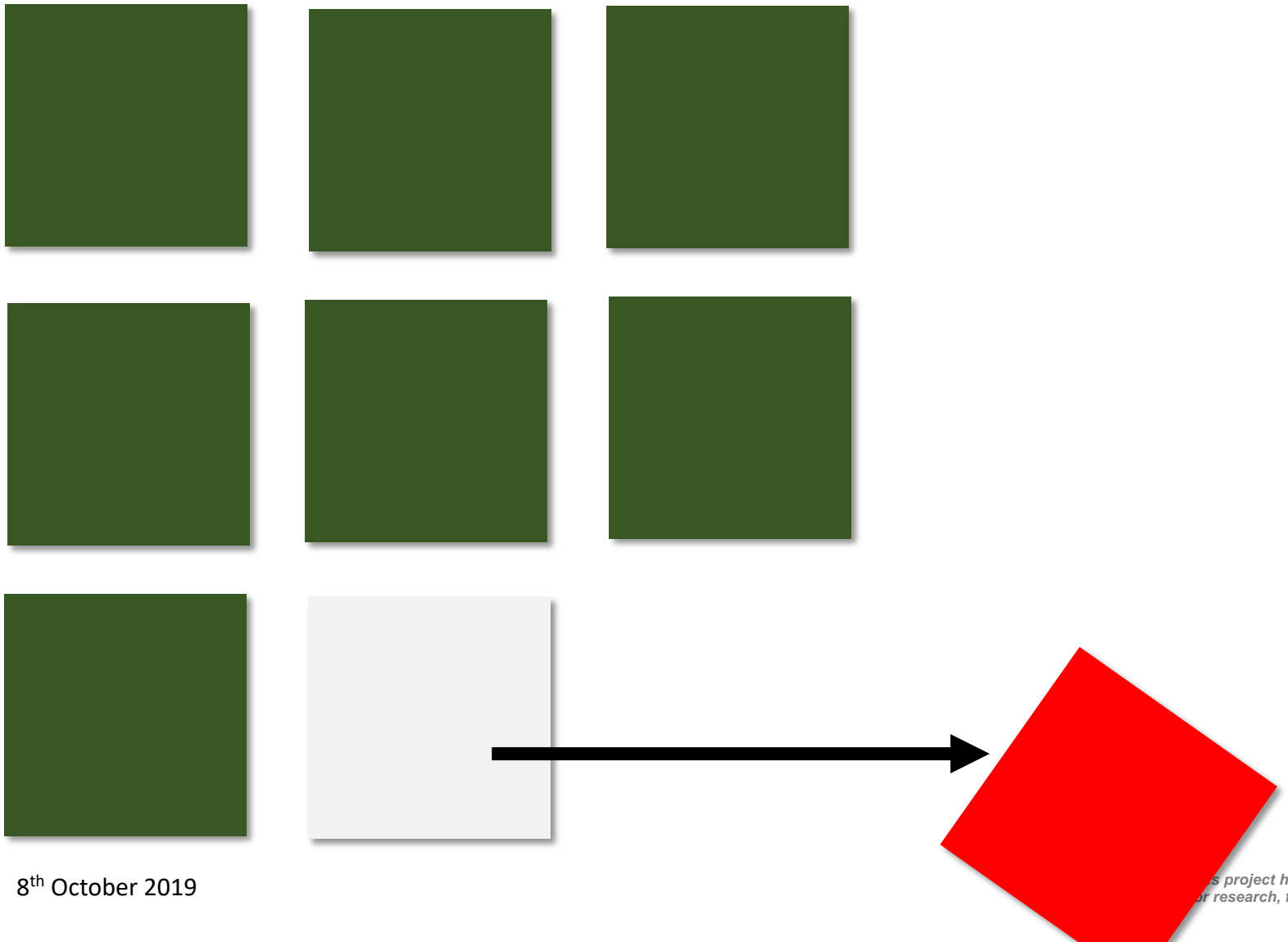
Public registry: temporary non-compliance



- Verification date < now
- The state of the assessment:
  - Running/Valid

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

Public registry: revoked certificates are removed



s project has received funding from the European Union's HORIZON Framework Programme
or research, technological development and demonstration under grant agreement no 731845.

Complaints & Standardization

- Possible complaints
  - Non-compliance detected by end-users
  - Unfair revocation

- Standardization and best practices
  - Measuring security
  - A catalogue of industry-agreed security and privacy attributes/metrics.

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

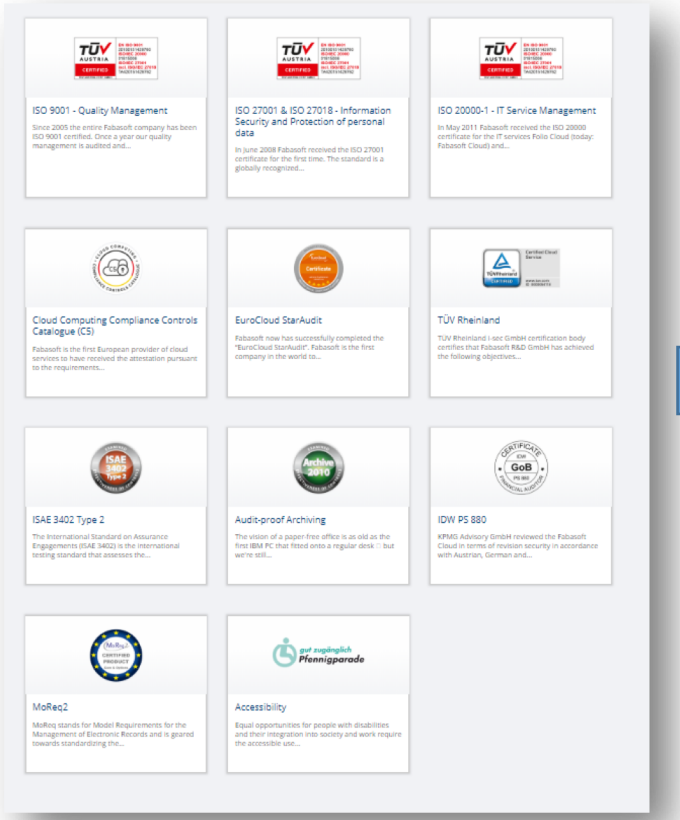
CABC for CSPs

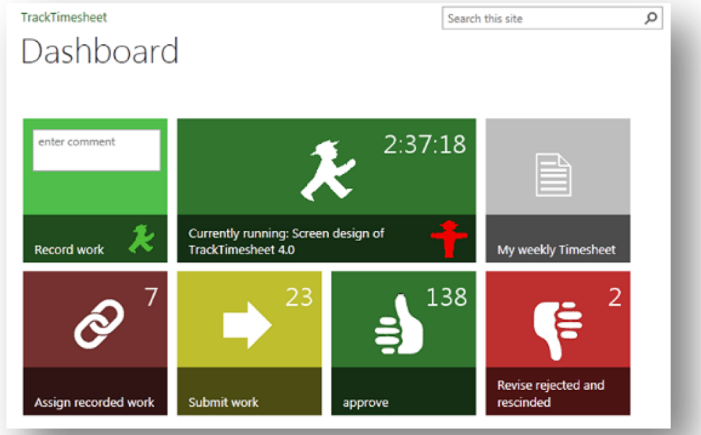
Björn Fanta (FABASOFT)

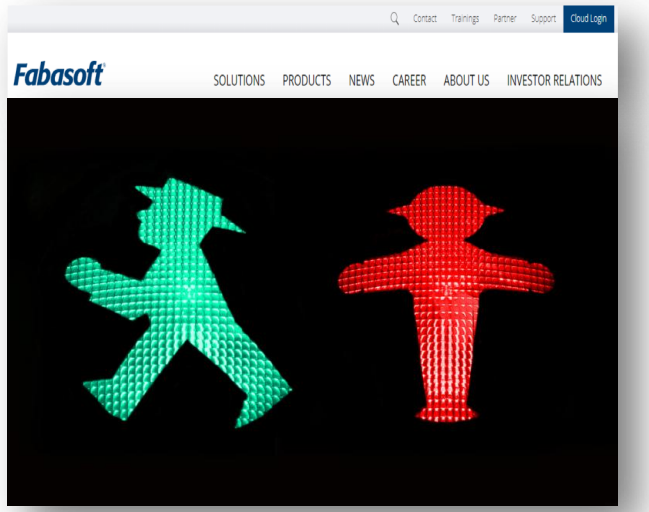
This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

The „Why?“

- Our goal of approaching CABC is to enhance the overall visibility of the organization and its security measurements / precautions as well as the effective use of technology



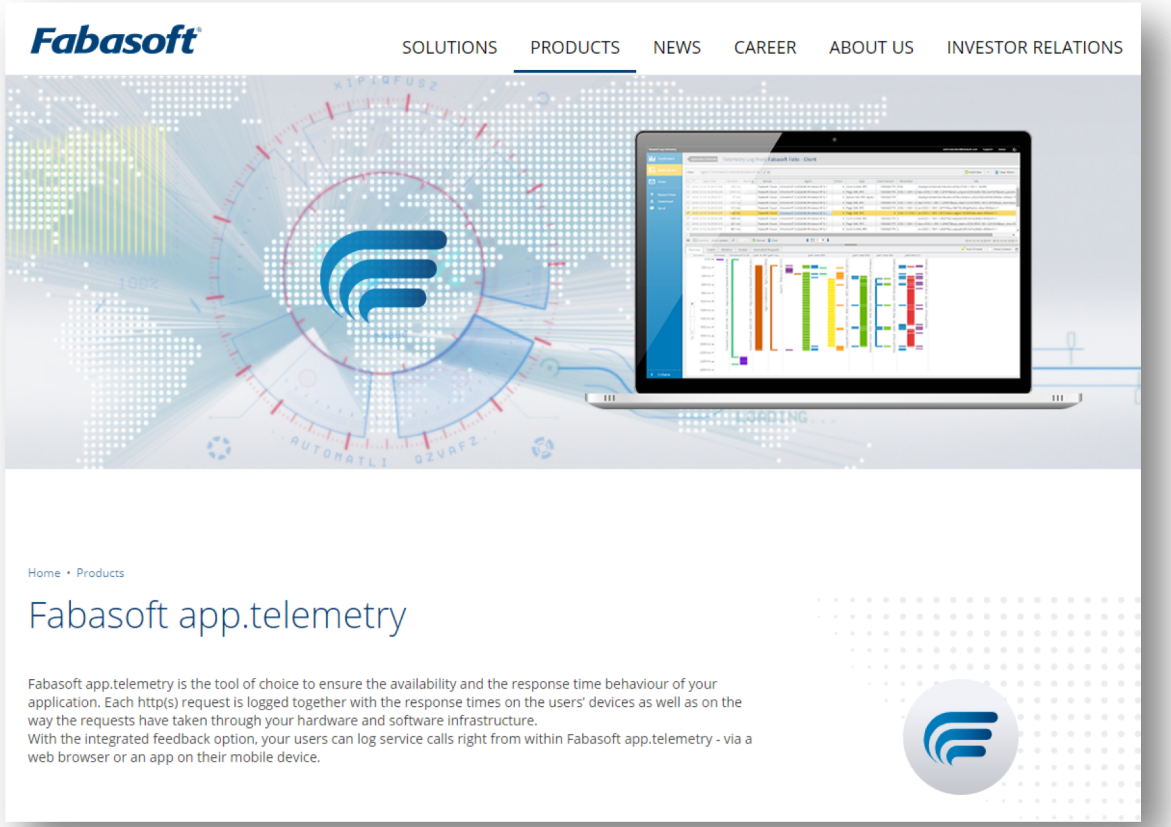


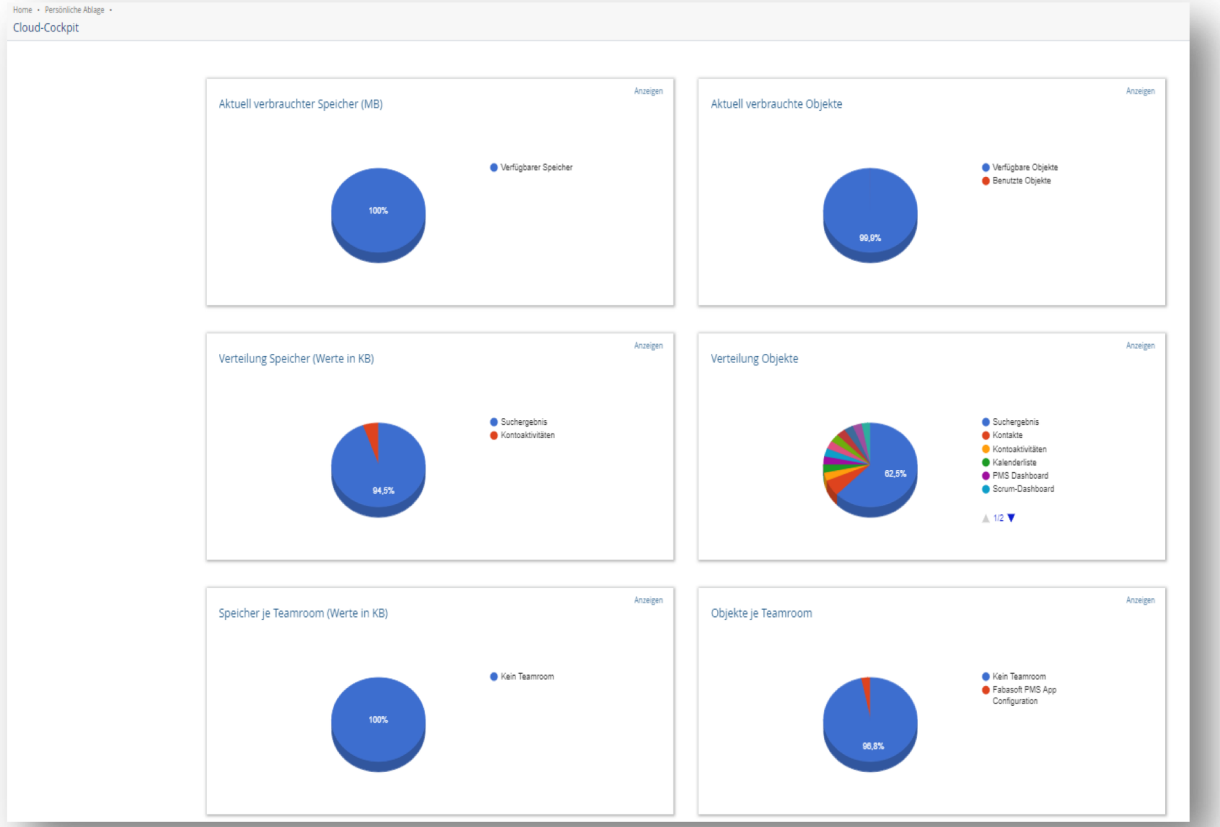


This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

„Under the Hood“

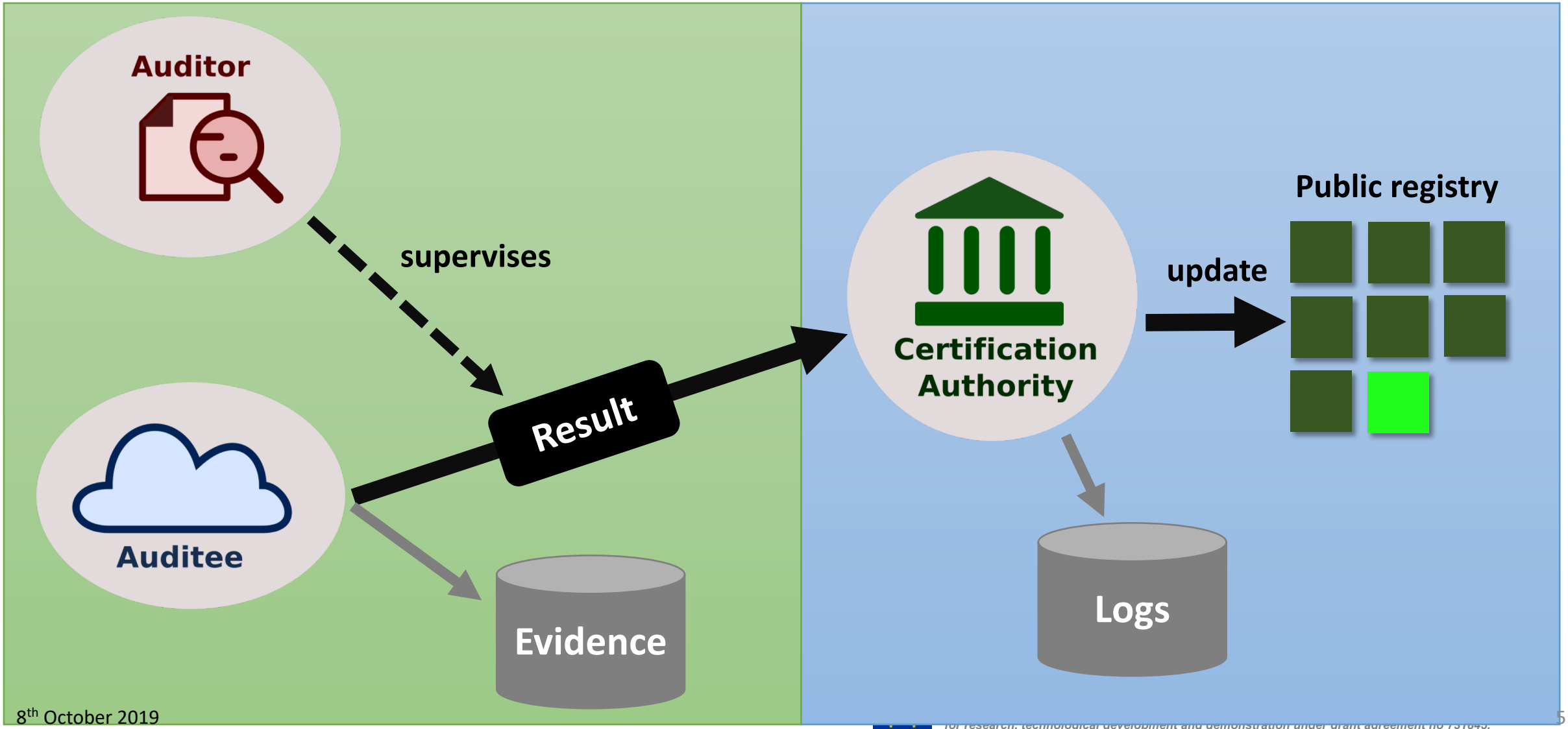
- A key element is to understand the technical implementation for a set of requirements





This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

„Technology Gap“



for research, technological development and demonstration under grant agreement no 731845.

The „How?“

- With our own controls, **we can derive a formalization for certain sets of requirements**
  - in line with the proof of concept, provided by the EU-SEC Framework

- We can then decide on continuously monitored evidence collection and connect to tools like “Clouditor”

- Resulting in:

#benefits

  - Greater audit efficiency and effectiveness
  - A long-term reduction of complexity
  - Enhanced internal controls and improved performance
  - More timely information to expedite response and reduce cost
  - Greater transparency for us and our customers

This project has received funding from the European Union’s HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

CABC for Technology Providers

Christian Banse (FRAUNHOFER AISEC)

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

Continuous Auditing Based Certification for Technology Providers

- Tools that support Continuous Auditing are the glue between Service Providers and Auditors
- Tools need to potentially address different stake holders
  - Auditors
  - Security Officers
  - Internal Compliance Officers
- Tools need to interface with different components in the certification scenario
  - Service Providers (*to audit*)
  - Storage / Databases / Evidence systems (*to store and possibly retrieve digital evidences*)
  - Certification Bodies / Scheme holders (*to update the compliance status*)

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

Continuous Auditing Based Certification for Technology Providers

- The world of service providers is constantly evolving and growing
  - EU-SEC efforts to harmonize and standardize interfaces to retrieve auditing information from Cloud services (https://github.com/eu-sec/continuous-auditing-api-spec)
  - Deliverable 3.5 offers a standardized format for the transmission of compliance status to certification bodies (currently implemented in CSA StarWatch)
- *Clouditor* as reference implementation for a continuous auditing tool
  - Community edition Available as Open Source implementation from Fraunhofer AISEC on GitHub
  - https://github.com/clouditor/clouditor

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

CABC for Auditors

Tatu Suhonen (NIXU)

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

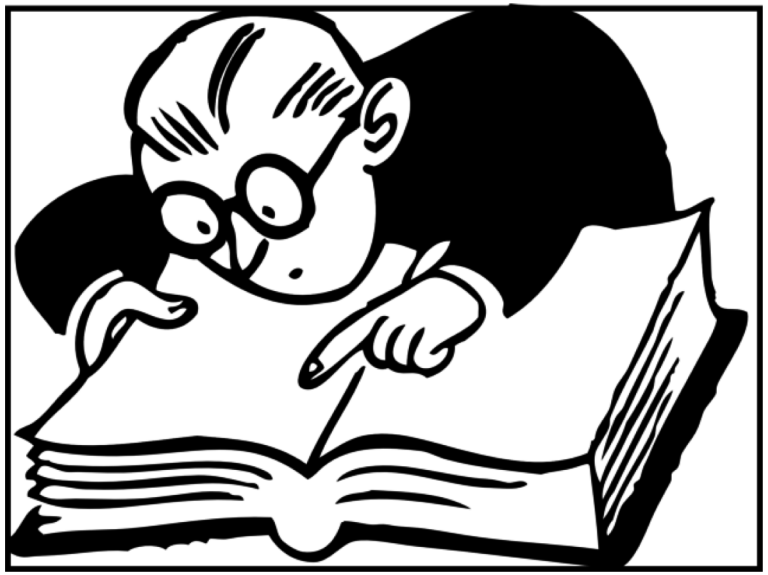
CABC - What's the interest for auditors?

- Traditional approach has its limitations
  - Audits are project-like point-in-time audits
  - Passive monitoring
    - Auditee's notification of significant change
    - Complaints
    - Special audits
  - Period of uncertainty between audits
- Continuous auditing as a solution for better assurance
  - From passive to active monitoring
    - Ability to actively conduct surveillance activities
    - Auditor is less dependent of information from external sources
  - Frequency of checks is shorter for automated controls
    - Control is in place with higher probability in next audits as well

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

CABC – Point-in-time audits

- Traditional audits still play a key role
  - Possibility to have a more in-depth analysis of the environment
    - Automated controls follow a predefined ruleset to collect and analyze evidence
    - Point-in-time audits allow to have a closer look into security controls if needed
  - Some controls require human intervention
    - Written security policies, physical security etc.
  - Multiple channels of verification
    - Automated controls can use multiple channels of verification
    - Humans can be more creative (observation, document review, interview, technical tests etc.)
  - Certification life-cycle needs to be followed
    - Yearly surveillance/recertification audits are necessary to maintain certification



This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

Continuous audit monitoring

Auditor has the responsibility for continuous monitoring and status of certification

- The auditor is provided with access to the monitoring tools
  - ability to verify the monitoring tools' evaluation results as well as the configuration of the monitoring tools

- Trust towards the monitoring tools is required
  - Quality definition of SLO's and SQO's is essential to ensure that right things are monitored
    - Link between security controls and the evidence collection results must be trustworthy
  - Evaluation of tool configuration
  - Evaluation of measurement processes to ensure evidence suitability
    - Right things are measured
    - Correct evidence is used

- Use of validated products is highly recommended as auditor's trust is required
  - If measurement results can't be trusted, a certificate can't be granted.

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

CABC - What's the interest for auditors?

New business opportunities

- CABC as a service is new
- Possibility to extend service portfolio from project assignments towards continuous services
- Competitive advantage

Conduct yearly surveillance/recertification audits with less effort

- Auditee preparation: continuous security instead of last-minute preparation
- Continuous auditing ensures less time spent on remediation activities
- Time & effort saved, audits finish on time

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

Round Table Discussion – Questions & Answers

Ramon Martín de Pozuelo (CAIXABANK)

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

Continuous Auditing-based Certification
Round Table Discussion - Questions and Answers

- How is your entity dealing with sensitive information sharing (e.g FI reporting to regulator)? How are you performing it? Are you following and standardized way? Which platforms/tools are you using?
- What security requirements do you consider when moving services to the cloud? Which security controls would you define in the auditing process? Which certification scheme would you be interested to integrate?
- What would you demand of the EU-SEC Continuous Auditing architecture in order to completely trust and rely on it?
- As a customer, which Continuous Auditing client application approach would be more appealing for your entity? Would you rely on a SaaS app provided by a Cloud Service Provider or develop your own app over IaaS?
- What would you expect from EU-SEC pilot? What would you like to test?
- What do you consider the most critical points for wide adoption of the proposed solution? Are there any missing features, or ones you would change, in order to use this solution in your entities? Which drivers or obstacles do you foresee?

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

EUSEC
EU SECURITY CERTIFICATION

Online Questionnaires:

Cloud Service Providers

https://www.surveymonkey.com/r/5K58TV8

Cloud Customers

https://www.surveymonkey.com/r/58B8T5X

Auditors

https://www.surveymonkey.com/r/5L7MG8T

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

Thank you for your attention!

Web: https://www.sec-cert.eu/

Contact: *contact@sec-cert.eu*

Twitter: @EU_SEC

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.