Tailored IoT & BigData Sandboxes and Testbeds for Smart, Autonomous and Personalized Services in the European Finance and Insurance Services Ecosystem

D6.13 – Testbeds Support and Certification Services

Revision Number	3.0
Task Reference	T6.6
Lead Beneficiary	NOVA
Responsible	Pedro Malò
Partners	AGRO AKTIF ATOS BANKIA BOC BOS BPFI CP CXB ENG GFT JRC NBG NOVA UNP UPRC WEA
Deliverable Type	Report (R)
Dissemination Level	Public (PU)
Due Date	2021-03-31
Delivered Date	2020-05-11
Internal Reviewers	GFT, NUIG
Quality Assurance	INNOV
Acceptance	WP Leader Accepted and Coordinator Accepted
EC Project Officer	Pierre-Paul Sondag
Programme	HORIZON 2020 - ICT-11-2018
	This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement no 856632

Contributing Partners

Partner Acronym	**Role**[1]	**Author(s)**[2]
NOVA	Lead Beneficiary	
GFT, NUIG	Internal reviewers	
INNOV	QA reviewer	

Revision History

Version	Date	Partner(s)	Description
0.1	2019-12-31	NOVA	ToC Version
1.0	2021-04-25	NOVA	First Version for Internal Review
2.0	2021-05-01	NOVA	Version for Quality Assurance
2.1	2021-05-07	NOVA	Final Version
3.0	2021-05-11	GFT	Version ready for the submission

[1] Lead Beneficiary, Contributor, Internal Reviewer, Quality Assurance

[2] Can be left void

Executive Summary

This deliverable is the first delivery of task T6.6. This task will specify and implement processes for certifying and standardizing digital finance/insurance solutions in the project's tailored sandboxes and testbeds. Special emphasis will be paid in regulatory compliance and standards-compliance certification processes based on the specification and execution of appropriate tests. Moreover, the task will ensure that experimenters and innovators get appropriate support regarding their use of testbed facilities and sandboxes such as support on hardware/software deployment issues, as well as support on system and administration issues.

It is provided in this deliverable a definition and initial design of a certification model and related methodology/process for the fintech solutions. The certification and compliance services focus on regulatory and (security) standards compliance. The INFINITECH certification process has been defined to be served on a self-certification mode with a well-established stepwise process in-place.

Certification and compliance services focuses on regulatory and (security) standards compliance, particularly on the set of regulations with the most relevant impact on INFINITECH which are: ISO/IEC 27001 Information technology: Security techniques, Information security management systems Requirements; ISO/IEC 27701 Privacy Information Management System (PIMS); Payment Card Industry Data Security Standard (PCI DSS); National Institute of Standards and Technology (NIST) Cyber Security Framework – Financial Services Cyber Security Profile; GDPR - The General Data Protection Regulation; PSD 2 - Payment Service Directive 2; MiFID II - Markets in Financial Instruments Directive II; 4AMLD – 4th Anti-Money Laundering Directive.

Additionally, a set of support services have been defined for the NOVA testbed infrastructure for experimentation of digital finance solutions within the INFINITECH project. Support services include Software and Hardware Deployment Support Services, Helpdesk Service, and others. The provider of the support services is the NOVA Computing Division (NOVA DIV-I,). The NOVA Computing Division plans and maintain the entire computer and network infrastructure of the NOVA School of Science and Technology.

Deliverable D6.13 will be followed by two additional deliverables which the following foreseen content: Deliverable D6.13 'Testbeds Support and Certification Services - II' at M30: Report on the implemented Support and Certification Services for fintech solutions and testbeds; Deliverable D6.13 'Testbeds Support and Certification Services - III' at M36: Report on the testing & validation of Support and Certification Services for fintech solutions and testbeds, and on the optimisations performed.

Table of Contents

List of Figures

List of Tables

Abbreviations/Acronyms

Abbreviation	Definition
2FA	Two-factor Authentication
3AMLD	3rd Anti-Money Laundering Directive,
4AMLD	4th Anti-Money Laundering Directive
AML	Anti-money laundering
CTF	Counter-terrorist financing
FAQ	Frequently Asked Questions
GDPR	General Data Protection Regulation
IAM	Identity and Access Management
ISMS	Information Security Management System
KYC	Know Your Customer
MFA	Multi-Factor authentication
MiFID II	Markets in Financial Instruments Directive II
MiFIR	Markets in Financial Instruments Regulation
OTC	Over-the-Counter
PCI DSS	Payment Card Industry Data Security Standard
PIMS	Privacy Information Management System
PSD 2	Payment Service Directive 2
SIEM	Security Information and Event Management

1 Introduction

This deliverable is the first delivery of task T6.6. This task will specify and implement processes for certifying and standardizing digital finance/insurance solutions in the project's tailored sandboxes and testbeds. Special emphasis will be paid in regulatory compliance and standards-compliance certification processes based on the specification and execution of appropriate tests. Moreover, the task will ensure that experimenters and innovators get appropriate support regarding their use of testbed facilities and sandboxes such as support on hardware/software deployment issues, as well as support on system and administration issues.

It is provided in this deliverable a definition and initial design of a certification model and related methodology/process for the fintech solutions. The certification and compliance services focus on regulatory and (security) standards compliance. The INFINITECH certification process has been defined to be served on a self-certification mode with a well-established stepwise process in-place.

Certification and compliance services focuses on regulatory and (security) standards compliance, particularly on the set of regulations with the most relevant impact on INFINITECH which are: ISO/IEC 27001 Information technology: Security techniques, Information security management systems Requirements; ISO/IEC 27701 Privacy Information Management System (PIMS); Payment Card Industry Data Security Standard (PCI DSS); National Institute of Standards and Technology (NIST) Cyber Security Framework – Financial Services Cyber Security Profile; GDPR - The General Data Protection Regulation; PSD 2 - Payment Service Directive 2; MiFID II - Markets in Financial Instruments Directive II; 4AMLD – 4th Anti-Money Laundering Directive.

Additionally, a set of support services have been defined for the NOVA testbed infrastructure for experimentation of digital finance solutions within the INFINITECH project. Support services include Software and Hardware Deployment Support Services, Helpdesk Service, and others. The provider of the support services is the NOVA Computing Division (NOVA DIV-I,). The NOVA Computing Division plans and maintain the entire computer and network infrastructure of the NOVA School of Science and Technology.

1.1 Objective of the Deliverable

Deliverable D6.13 'Testbeds Support and Certification Services - I' provides the description and specification of the certification and support services to be established for fintech solutions and testbeds.

Deliverable D6.13 is the first output of task T6.6 'Testbeds Support, Certification and Standardisation Services' where two additional deliverables follow which the following foreseen content:

- Deliverable D6.13 'Testbeds Support and Certification Services - II' at M30: Report on the implemented Support and Certification Services for fintech solutions and testbeds; and
- Deliverable D6.13 'Testbeds Support and Certification Services - III' at M36: Report on the testing & validation of Support and Certification Services for fintech solutions and testbeds, and on the optimisations performed.

1.2 Insights from other Tasks and Deliverables

Certification and compliance services focuses on regulatory and (security) standards compliance, particularly on the set of regulations with the most relevant impact on INFINITECH as identified by the work performed already on task T2.4, duly reported in deliverables D2.7 'D2.8 – Security and Regulatory Compliance Specifications – Version I' and D2.8 'Security and Regulatory Compliance Specifications – Version II'.

1.3 Structure

Section 2 provides insights on the INFINITECH certification and compliance services focuses on regulatory and (security) standards compliance. The INFINITECH certification process will be served on a self-certification mode with a well-established process that's described in this section.

Section 3 provides a view on the set of support services have been defined for the NOVA testbed infrastructure for experimentation of digital finance solutions within the INFINITECH project.

2 Certification and Compliance Services

2.1 Certification Process

The INFINITECH certification and compliance services focuses on regulatory and (security) standards compliance. The certification process is to be used to by developers of fintech solutions to assure that their solutions comply with relevant and applicable standards and regulations.

The INFINITECH certification process will be served on a self-certification mode, meaning that applicants to the certification will perform themselves the certification process validation.

The applicants of the self-certification will follow a set of well-defined steps, as follows:

1) Step 1: Identification of applicable regulations and standards
2) Step 2: Analysis of compliance with the defined requirements
    a. Step 2.1: Execute automated tests of compliance for selected requirements
3) Step 3: Issue a declaration of conformity

2.1.1 Step 1: Identification of applicable regulations and standards

Certification and compliance services focuses on regulatory and (security) standards compliance, particularly on the set of regulations with the most relevant impact on INFINITECH as identified by the work on task T2.4, reported in deliverables D2.7 'D2.8 – Security and Regulatory Compliance Specifications – Version I' and D2.8 'Security and Regulatory Compliance Specifications – Version II' which are:

- ISO/IEC 27001 Information technology: Security techniques, Information security management systems Requirements
- ISO/IEC 27701 Privacy Information Management System (PIMS)
- Payment Card Industry Data Security Standard (PCI DSS)
- National Institute of Standards and Technology (NIST) Cyber Security Framework – Financial Services Cyber Security Profile
- GDPR - The General Data Protection Regulation
- PSD 2 - Payment Service Directive 2
- MiFID II - Markets in Financial Instruments Directive II
- 4AMLD – 4th Anti-Money Laundering Directive

2.1.1.1 ISO/IEC 27001 – Information technology: Security techniques, Information security management systems Requirements

ISO/IEC 27001 is the international standard focused on information security, from the International Organization for Standardization (ISO), in partnership with the International Electrotechnical Commission (IEC). It was developed to help organizations, of any size or any industry, to protect their information in a systematic and cost-effective way, through the adoption of an Information Security Management System (ISMS).

The ISMS is a system that helps to prevent and counteract interruptions to business activities. It facilitates management, monitoring and auditing of an organization's information security practice in a comprehensible way. Moreover, the ISMS based on ISO 27001 principles supports protection of company information, intellectual property, and personal data. It protects critical processes from the effects of information security incidents, disasters and major failures of information systems and ensures the timely continuation of normal operations.

2.1.1.2 ISO/IEC 27701 Privacy Information Management System (PIMS)

ISO/IEC 27701:2019 is the international standard for privacy information management. It is structured in the same way as ISO/IEC 27001 – hence from the establishment of the privacy information management system (PIMS) through to its review and adaptation. There are also sections on performance evaluation and improvement. The standard outlines a comprehensive set of operational controls that can be mapped to various regulations, including the GDPR. Once mapped, the PIMS operational controls are implemented by privacy professionals and audited by internal or third-party auditors resulting in a certification and comprehensive evidence of conformity.

ISO/IEC 27701:2019 is a privacy extension to the international information security management standard, ISO/IEC 27001 (ISO/IEC 27701 Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines). ISO 27701 specifies the requirements for – and provides guidance for establishing, implementing, maintaining, and continually improving – a PIMS (privacy information management system).

2.1.1.3 Payment Card Industry Data Security Standard (PCI DSS)

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards formed in 2004. The compliance scheme aims to secure credit and debit card transactions against data theft and fraud. The PCI SSC (Payment Card Industry Security Standards Council) has no legal authority to compel compliance, it is however a requirement for any business that processes credit or debit card transactions. It is also considered the best way to safeguard sensitive data and information.

2.1.1.4 NIST Cyber Security Framework

The framework from NIST provides best practices for voluntary use in all critical infrastructure sectors, including, for example, government, healthcare, financial services, and transportation. It is designed to help organizations develop information security protection programs.

The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes. The Framework consists of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. The Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across critical infrastructure sectors, providing the detailed guidance for developing individual organizational Profiles. Through use of the Profiles, the Framework will help the organization align its cybersecurity activities with its business requirements, risk tolerances, and resources. The Tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk.

2.1.1.5 GDPR - The General Data Protection Regulation

The General Data Protection Regulation is a European Union law that was implemented on May 25th of 2018, and requires organizations to safeguard personal data and uphold the privacy rights of anyone in EU territory. Personal data means any information which, directly or indirectly, could identify a living person. Name, phone number, and address are schoolbook examples of personal data. Interests, information about past purchases, health, and online behaviour is also considered personal data as it could identify a person.

The regulation includes seven principles of data protection that must be implemented and eight privacy rights that must be facilitated. It also empowers member state-level data protection authorities to enforce the GDPR with sanctions and fines. The GDPR replaced the 1995 Data Protection Directive, which created a country-by-country patchwork of data protection laws. The GDPR, passed in European Parliament by overwhelming majority, unifies the EU under a single data protection regime.

2.1.1.6 PSD 2 - Payment Service Directive 2

The directive establishes a clear and comprehensive set of rules that will apply to existing and new providers of innovative payment services. These rules seek to ensure that these players can compete on equal terms, leading to greater efficiency, choice, and transparency of payment services, while strengthening consumers' trust in a harmonized payments market. The directive is applied since 12 January 2016 with EU countries having to incorporate it into national law by 13 January 2018.

The Directive (EU) 2015/2366 (Payment Service Directive 2 — PSD 2) provides the legal foundation for the further development of a better integrated internal market for electronic payments within the EU. It puts in place comprehensive rules for payment services, with the goal of making international payments (within the EU) as easy, efficient, and secure as payments within a single country. It seeks to open up payment markets to new entrants leading to more competition, greater choice and better prices for consumers. It also provides the necessary legal platform for the Single Euro Payments Area (SEPA). It repealed Directive 2007/64/EC (PSD) from 13 January 2018. The directive also aims to open up the EU payment market to companies offering consumer- or business-oriented payment services based on access to information about the payment account.

2.1.1.7 MiFID II - Markets in Financial Instruments Directive II

MiFID II is a legislative framework instituted by the European Union (EU) to regulate financial markets in the bloc and improve protections for investors. Its aim is to standardize practices across the EU and restore confidence in the industry, especially after the 2008 financial crisis. A revised version of the original MiFID, it rolled out on January 3rd, 2018. Technically, MiFID II applies to the legislative framework, and the rules it outlines are the Markets in Financial Instruments Regulation (MiFIR); but colloquially, the term MiFID is used to mean both.

MiFID II harmonizes the application of oversight among member nations and broadens the scope of the regulations. In particular, it imposes more reporting requirements and tests in order to increase transparency and reduce the use of dark pools (private financial exchanges that allow investors to trade without revealing their identities) and over-the-counter (OTC) trading. Under the new rules, the trading volume of a stock in a dark pool is limited to 8% over 12 months. The new regulations also target high-frequency trading. Algorithms used for automated trading must be registered, tested, and have circuit breakers included.

MiFID II extends the scope of requirements under MiFID to more financial instruments. Equities, commodities, debt instruments, futures and options, exchange-traded funds, and currencies all fall under its purview. If a product is available in an EU nation, it is covered by MiFID II — even if, say, the trader wishing to buy it is located outside the EU. The original Markets in Financial Instruments Directive (MiFID) went into effect in November 2007.

2.1.1.8 4AMLD - 4th Anti-Money Laundering Directive

The 4th Anti-Money Laundering Directive (4AMLD) is part of a package of EU legislative measures aimed at preventing money laundering and terrorist financing that includes Regulation (EU) 2015/847 on the traceability of money transfers. The directive has applied since 25 June 2015 and was originally supposed to become law in the EU countries by 26 June 2017. This deadline was, however, further extended by, several amendments, in particular Directive (EU) 2018/843, which had to be fully incorporated into EU countries' national law by 10 January 2020.

Directive (EU) 2015/849 (4th Anti-Money Laundering Directive, 4AMLD) aims to combat money laundering and the financing of terrorism by preventing the financial market from being misused for these purposes. It seeks to extend and replaces the previous Directive (EC) 2005/60 (3rd Anti-Money Laundering Directive, 3AMLD) that entered into force in 2007. Its purpose is to remove any ambiguities in the previous directive and associated legislation, and to improve the consistency of anti-money laundering (AML) and counter-

terrorist financing (CTF) rules across all EU countries. The 4AMLD also considers recommendations of the Financial Action Task Force (FATF) from 2012.

2.1.2 Step 2: Analysis of compliance with defined requirements

2.1.2.1 Requirements from ISO/IEC 27001

GMS-0001 Security Information and Event Management (SIEM)	Logging capabilities on security events for enterprises used to analyse and/or report on the log entries received.
GMS-0002 Risk Management/Monitoring	Track risk and mitigations, rank hazards by their critical value, produce reports and manage compliance.
GMS-0003 Security Awareness & Training	Provide awareness training and set out key security requirements and practices within the context of the applications and/or services being provided.
GMS-0004 Password Policy Enforcement	Gives administrators the power to impose certain password policies on users when they choose a password such as: complexity, contained in a dictionary, keyboard pattern, repeating patterns or similarity.
GMS-0005 Information Asset Management	To identify and record the data subjects, volumes held, retention periods and who has access to the assets and their contents.
GMS-0006 Anonymization	The process of removing personal identifiers, both direct and indirect, that may lead to an individual being identified.
GMS-0007 Pseudonymization	A technique that is used to reduce the chance that personal data records and identifiers lead to the identification of the natural person (data subject) whom they belong too.
GMS-0008 Authentication and Authorization mechanisms	Strong and secure Access Management to prevent unauthorised access.
GMS-0009 Data Encryption	Method where information is encoded and can only be accessed or decrypted by a user with the correct encryption key.
GMS-0010 Data Discovery and Classification	Visibility of sensitive data held by the organisation with efficient data discovery, classification, and risk analysis across heterogeneous data stores - the cloud, big data, and traditional environments - in the enterprise.

2.1.2.2 Requirements from ISO/IEC 27701 PIMS

GMS-0006 Anonymization (see above)	The process of removing personal identifiers, both direct and indirect, that may lead to an individual being identified.
GMS-0011 Pseudonymization	A technique that is used to reduce the chance that personal data records and identifiers lead to the identification of the natural person (data subject) whom they belong too.
GMS-0012 Authentication and Authorization mechanisms	Method where information is encoded and can only be accessed or decrypted by a user with the correct encryption key.
GMS-0009 Data Encryption (see above)	Strong and secure Access Management to prevent unauthorised access.
GMS-0010 Data Discovery and Classification (see above)	Visibility of sensitive data held by the organisation with efficient data discovery, classification, and risk analysis across heterogeneous data

	stores - the cloud, big data, and traditional environments - in the enterprise.

2.1.2.3 Requirements from PCI DSS

GMS-0013 Secure network	A firewall configuration must be installed and maintained. System passwords must be original (not vendor-supplied).
GMS-0014 Secure cardholder data	Stored cardholder data must be protected. Transmissions of cardholder data across public networks must be encrypted.
GMS-0015 Vulnerability management	Anti-virus software must be used and regularly updated. Secure systems and applications must be developed and maintained.
GMS-0016 Access control	Cardholder data access must be restricted to a business need-to-know basis. Every person with computer access must be assigned a unique ID. Physical access to cardholder data must be restricted.
GMS-0017 Network monitoring and testing	Access to cardholder data and network resources must be tracked and monitored Security systems and processes must be regularly tested
GMS-0018 Information security	A policy dealing with information security must be maintained

2.1.2.4 Requirements from NIST Cyber Security Framework

GMS-0019 Supplier Management	Maintain quality, safety, and risk management processes throughout the supply chain. Monitor Supplier Compliance and Capability.
GMS-0001 Security Information and Event Management (SIEM) (see above)	Logging capabilities on security events for enterprises used to analyse and/or report on the log entries received.
GMS-0020 Risk Management/Monitoring	Track risk and mitigations, rank hazards by their critical value, produce reports and manage compliance.
GMS-0003 Security Awareness & Training (see above)	Provide awareness training and set out key security requirements and practices within the context of the applications and/or services being provided.
GMS-0004 Password Policy Enforcement (see above)	Gives administrators the power to impose certain password policies on users when they choose a password such as: complexity, contained in a dictionary, keyboard pattern, repeating patterns or similarity.
GMS-0005 Information Asset Management (see above)	To identify and record the data subjects, volumes held, retention periods and who has access to the assets and their contents.
GMS-0008 Authentication and Authorization mechanisms (see above)	Strong and secure Access Management to prevent unauthorised access.
GMS-0009 Data Encryption (see above)	Method where information is encoded and can only be accessed or decrypted by a user with the correct encryption key.

2.1.2.5 Requirements from GDPR

GMS-1001 Information Security Policies	Maintain an information security policy and develop appropriate procedures to support and implement that policy.
GMS-1002 Business Continuity	Protocols and measures should be in place to back-up personal data and ensure that it can be recovered and maintained in the event of an incident.
GMS-1003 Risk Assessment	Comprehensive assessments should be carried out for high-risk data and processing activities and mitigating solutions/procedures should be in place to prevent or reduce risks.
GMS-1004 Policies and Procedures	Implement robust policies and procedures so that the whole organisation and its employees know what their obligations are and what to do if certain situations occur.
GMS-1005 Management Information & Reporting	Regular reports and information are passed to upper management is essential for ensuring that the adequate resources and funding are made available and for accountability at all levels.
GMS-0005 Security Awareness & Training	A culture of security and data protection awareness will ensure that employees, contractors, and any third-party working for or with the organisation, know what is expected of them and how to maintain compliance.
GMS-1006 Reviews & Audits	This ensures that policies, controls and/or measures that are put in place can be monitored for effectiveness, accurate and fit for purpose.
GMS-1007 Due Diligence	Carrying out due diligence checks on suppliers and service providers (and in some sectors, customers); is an essential and often legal requirement (i.e., fraud checks, anti-money laundering measures).
GMS-1008 Building Security	You should have robust measures and protocols for securing access to any office or building and ensure that all employees are aware of such controls.
GMS-1009 Disposal	Specify the appropriate procedures compliant with GDPR for the disposal of paperwork and devices and appropriate controls for anything that is registered as lost.
GMS-0004 Password Policy Enforcement	Specify a password policy that enforces strong passwords that are changed on a regular basis.
GMS-1010 Supplier Relationships	Implement procedures to manage third-party risks coming into your organization and systems resulting from a failure to follow good security practice by suppliers, e.g. AWS.

2.1.2.6 Requirements from PSD 2

GRS-0001 Strong Multi-Factor authentication (MFA)	A requirement for the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN.
GRS-0002 SIEM (Security Information Event	Used to collect and aggregate log data generated throughout the organization's technology infrastructure, from host systems and

Management) systems (equals GMS-0001 above)	applications to network and security devices such as firewalls and antivirus filters.
GRS-0003 Patch Management	Distributing and applying updates to software. It will support the following objectives: Security, System uptime, Compliance and Feature improvements.

2.1.2.7 Requirements from MiFID II

GRS-0002 SIEM (Security Information Event Management) systems (equals GMS-0001 above)	Auditing logs for maintaining and monitoring the security and integrity of data.
GRS-0005 Phone Call Recording	Phone call recording to maintain a record of all interactions with customers providing an evidence trail of all advice and information provided.
GRS-0006 Email Logging	Email logs to maintain a record of all interactions with customers providing an evidence trail of all advice and information provided.
GRS-0001 Strong Multi-Factor authentication (MFA)	Strong authentication, preferably multi-factor, and authorization mechanisms.

2.1.2.8 Requirements from 4AMLD

GRS-0007 Examination & Investigation	AML compliance, AML/Suspicious transaction monitoring, trade surveillance, operational risk, and anti- fraud case management.
GRS-0008 Customer Due Diligence	Single data entry point and risk rating for all existing and new customer and account data in support of Know Your Customer (KYC) requirements incorporating third party data sources and registers.
GRS-0009 Name/Entity Matching	Matching and scoring tools and techniques that improve the searching of account and transaction information across systems, regions, and business lines to create one view of the customer or to improve the name/entity screening,

2.2 Step 2.1a: Execute compliance tests for selected requirements

Automated Compliance Services will be made avalaible for testing the compliance with selected requirements – these services are to be used by applicated for testing and evaluating conformity. An example is the service for testing Two-factor Authentication (2FA).

2.2.1 Strong Multi-factor authentication compliance testing

The testing of Strong Multi-factor authentication compliance aims to test the compliance with GRS-0001 Strong Multi-Factor authentication (MFA).

2.2.1.1 Testing Two-factor Authentication (2FA)

Two-factor authentication is a concept where a person requires a second form of authentication after an initial login with username and password, hence the term two-factor.

A testing method for 2FA has been proposed by Michelangelo van Dam, senior PHP architect, PHP community leader and international conference speaker with many contributions to PHP projects and community events, described here [1]. A short overview/specification of this is provided next.

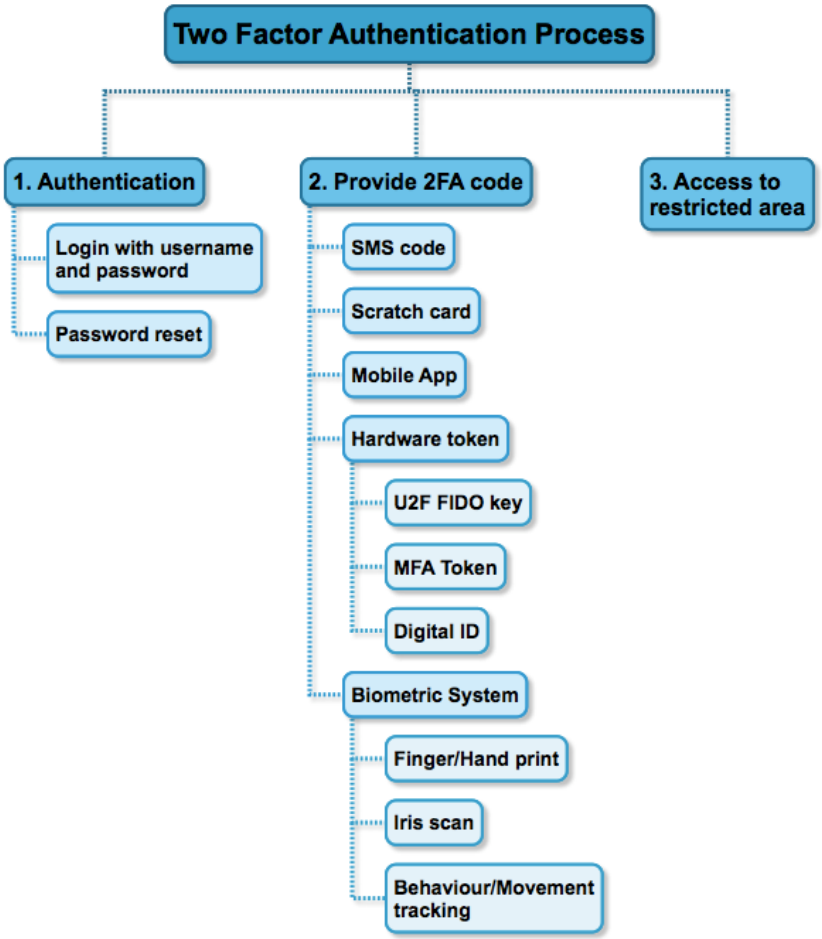

Figure 1 - Two Factor Authentication Process (from [1])

2.2.1.1.1 Functional Testing 2FA

Approaching 2FA for functional testing is a straight-forward process for human testers as they can use the device or service for secondary authentication. But how can you automate this? For SMS or call services you can make use of an external phone service that will receive the code for you and provides it as value for your 2FA input field. In the example below we make use of Twilio.

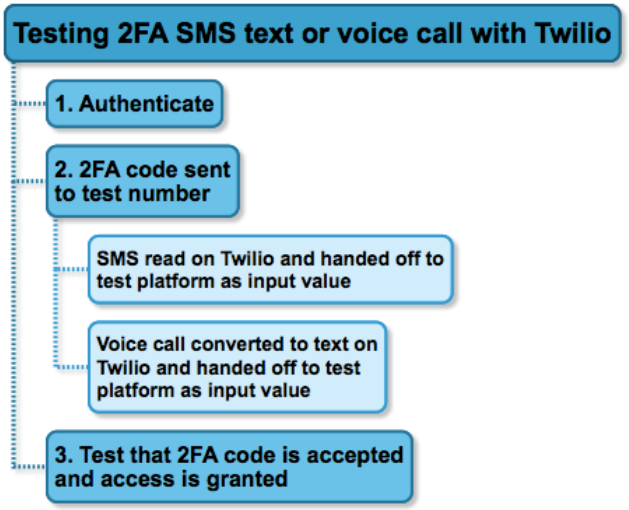

Figure 2 - Testing Process of 2FA (from [1])

2.2.1.1.2 Unit Testing 2FA

When writing unit tests for 2FA is simple as long we consider the 2FA service as an external system which we can stub. Consider the following PHP code for 2FA verification.

Table 1 - Validate 2FA code snippet

```
/**
 * Validates a provided 2FA code against the 2FA service and throws an
 * Exception when the given code is invalid or will return TRUE on
 * successful verification.
 *
 * @param string $twoFactorCode
 * @return bool
 * @throws \InvalidArgumentException
 */
public function validateTwoFactorCode(string $twoFactorCode): bool
{
    if (!$this->twoFactorService->validateCode($this->accountEntity, $twoFactorCode)) {
        throw new \InvalidArgumentException('Provided 2FA code is invalid');
    }
    return true;
}
```

We can test this both invalid as valid processing of a provided 2FA code with the following code snipit using PHPUnit where the 2FA service itself doesn't have to be defined, just following the interface blueprint.

Table 2 - Test Authentication code snippet

```
/**
 * Authentication throws exception for invalid two factor code
 *
 * @covers \LoginForm\Auth\Service\AuthenticationService::__construct
 * @covers \LoginForm\Auth\Service\AuthenticationService::validateTwoFactorCode
 * @expectedException \InvalidArgumentException
 */
public function testAuthenticationThrowsExceptionForInvalidTwoFactorCode()
{
    $twoFactorCode = '123456';

    $this->twoFactorServiceMock->expects($this->once())
        ->method('validateCode')
```

```
        ->willReturn(false);

    $authService = new AuthenticationService(
        $this->validator,
        $this->accountModel,
        $this->accountEntity,
        $this->twoFactorServiceMock
    );
    $authService->validateTwoFactorCode($twoFactorCode);
    $this->fail('Expected exception was not triggered for invalid 2FA code');
}

/**
 * Authentication accepts valid two factor code
 *
 * @covers \LoginForm\Auth\Service\AuthenticationService::__construct
 * @covers \LoginForm\Auth\Service\AuthenticationService::validateTwoFactorCode
 */
public function testAuthenticationAcceptsValidTwoFactorCode()
{
    $twoFactorCode = '123456';

    $this->twoFactorServiceMock->expects($this->once())
        ->method('validateCode')
        ->willReturn(true);

    $authService = new AuthenticationService(
        $this->validator,
        $this->accountModel,
        $this->accountEntity,
        $this->twoFactorServiceMock
    );
    $validTwoFactorCode = $authService->validateTwoFactorCode($twoFactorCode);
    $this->assertTrue($validTwoFactorCode,
        sprintf('Expected 2FA code "%s" to be valid', $twoFactorCode)
    );
}
```

This will result in successful processing of 2FA authentication without implementing the service.

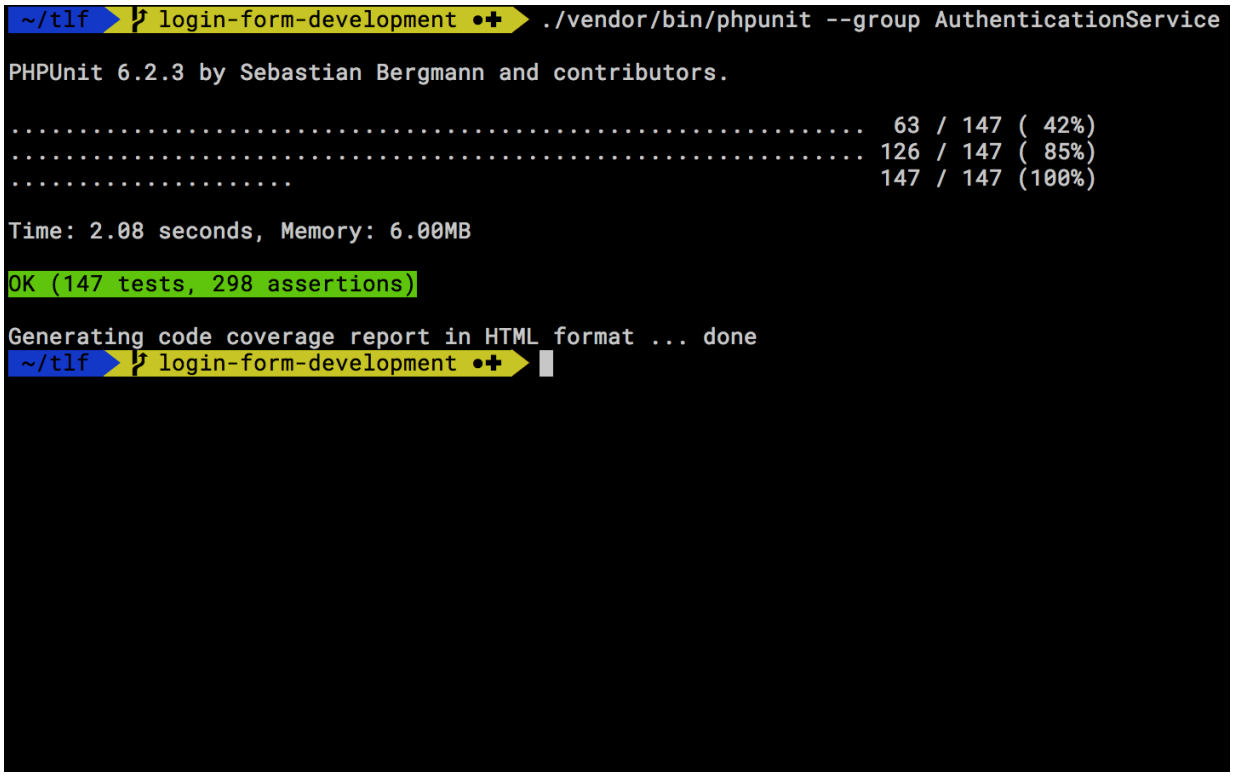

Figure 3 - Testing Execution of 2FA (from [1])

2.3 Step 3: Issue a declaration of conformity

The declaration of conformity should include at least:

- your name and address, or those of any authorised representatives
- a brief description of the solution
- a statement, stating you take full responsibility
- means of identification of the solution allowing traceability
- your name and signature
- the date the declaration was issued
- supplementary information (if applicable)
- the relevant legislation with which the product complies, as well as any harmonised standards or other means used to prove compliance:

	Not Applicable	Full Compliance	Partial Compliance	Observations / Comments
GMS-0001 Security Information and Event Management (SIEM)				
GMS-0002 Risk Management/Monitoring				
GMS-0003 Security Awareness & Training				
GMS-0004 Password Policy Enforcement				
GMS-0005 Information Asset Management				

GMS-0006 Anonymization				
GMS-0007 Pseudonymization				
GMS-0008 Authentication and Authorization mechanisms				
GMS-0009 Data Encryption				
GMS-0010 Data Discovery and Classification				
GMS-0011 Pseudonymization				
GMS-0012 Authentication and Authorization mechanisms				
GMS-0013 Secure network				
GMS-0014 Secure cardholder data				
GMS-0015 Vulnerability management				
GMS-0016 Access control				
GMS-0017 Network monitoring and testing				
GMS-0018 Information security				
GMS-0019 Supplier Management				
GMS-0020 Risk Management/Monitoring				
GRS-0001 Strong Multi-Factor authentication (MFA)				
GRS-0003 Patch Management				
GRS-0005 Phone Call Recording				
GRS-0006 Email Logging				
GRS-0007 Examination & Investigation				
GRS-0008 Customer Due Diligence				
GRS-0009 Name/Entity Matching				
GMS-1001 Information Security Policies				
GMS-1002 Business Continuity				
GMS-1003 Risk Assessment				
GMS-1004 Policies and Procedures				

GMS-1005 Management Information & Reporting				
GMS-1006 Reviews & Audits				
GMS-1007 Due Diligence				
GMS-1008 Building Security				
GMS-1009 Disposal				
GMS-1010 Supplier Relationships				

3 Support Services

A set of support services have been defined for the NOVA testbed infrastructure for experimentation of digital finance solutions within the INFINITECH project. Here follows the details on the provider of the support services and the definition of these services.

3.1 Provider of the Support Services: NOVA DIV-I

The provider of the support services is the NOVA Computing Division (NOVA DIV-I, www.fct.unl.pt/en/faculty/services/computing-division). The NOVA Computing Division plans and maintain the entire computer and network infrastructure of the NOVA School of Science and Technology.

Specific competences of the NOVA Computing Division relevant for INFINITECH:

- Contribute to the definition and procurement of the INFINITECH testbed infrastructure at NOVA:
  - a) Collect the computer network requirements
  - b) Design, plan and manage the computer network
  - e) Set the Data Processing Center requirements, including computer servers and services
  - f) Design and plan the Data Processing Center structure, including computer servers and services
  - q) Designing and planning the architecture of information systems
  - r) Ensure the integration of new applications with existing services, participating in the realization of acceptance testing and compliance

- Perform the installation, configuration, and management of the INFINITECH testbed infrastructure at NOVA:
  - c) Install, configure, and manage the active equipment of the computer network
  - g) Install, configure, and manage servers and IT services under its control
  - k) Define and monitor the implementation of the use of all information systems policies, communication infrastructure, systems, and services
  - r) Ensure the integration of new applications with existing services, participating in the realization of acceptance testing and compliance
  - s) Manage the maintenance, updating and implementation of new features in applications adopted in line with the needs the Faculty
  - r) Ensure the integration of new applications with existing services, participating in the realization of acceptance testing and compliance

- Support to Data Management in the INFINITECH testbed infrastructure at NOVA:
  - h) Ensure backup copies of critical information in computer systems and information systems
  - j) Set confidentiality criteria, safety, and longevity of data

- Monitor and service the INFINITECH testbed infrastructure at NOVA:
  - k) Define and monitor the implementation of the use of all information systems policies, communication infrastructure, systems, and services
  - l) Establish and implement the safety rules of IT infrastructure, applications, services, and procedures
  - m) Define metrics for assessing the quality of services rendered
  - n) Monitor, audit, and evaluate the quality of rendered services
  - o) Standardize and ensure the application of safety rules and technical procedures

- **Setup and provision of technical support for users of the INFINITECH testbed infrastructure at NOVA:**
  - **i) Ensure technical support in resolving the context of the communications infrastructure problems**
  - **i) Ensure the technical support for the resolution of problems under the System Administration of computer systems under their control**
  - **r) Ensure the integration of new applications with existing services, participating in the realization of acceptance testing and compliance**

3.2 Support Services

3.2.1 Software and Hardware Deployment Support Services

A set of documentation and tutorial videos will be made available on how to access and use the NOVA infrastructure, namely:

- VPN Access Configuration
- How to deploy an INFINITECH testbed
- Technical requirements for INFINITECH testbeds
- Etc.

NOVA team has background experience in preparing these materials hosting already a FAQ facility (https://www.div-i.fct.unl.pt/faq) and support videos for users presently available on the YouTube platform (https://youtube.com/playlist?list=PL64B66F46991849BB).

3.2.2 Helpdesk Service

A helpdesk service has been setup for users and managers for the INFINITECH infrastructure – the helpdesk service is accessible via e-mail infinitech.helpdesk@uninova.pt. The service hours are from 9h to 17h (Portuguese time).

The helpdesk follows a ticketing system to management, process, and catalogue support requests from users. The service is built-on Request Tracker (RT) which is a widely used and proven ticket-tracking system that is used to coordinate tasks and manage requests among a community of users.

A ticketing system is a management tool that processes and catalogues customer service requests. The ticketing system enables to register an event – create a ticket – on the request of a user, assign ticket to someone, define priorities, maintain change history, inform interested parties of changes, and start actions to address the need. The following figure depicts the flows of a ticketing systems.

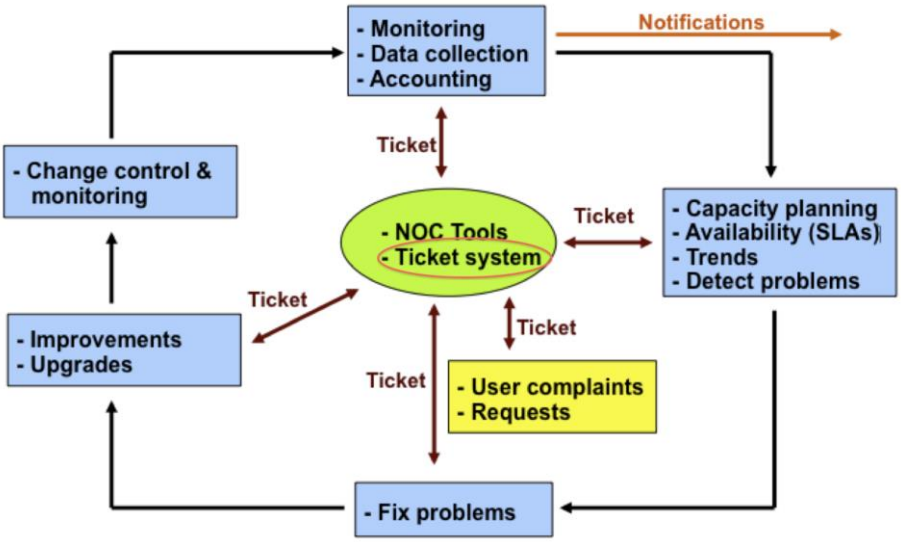

Figure 4 - Flows of Ticketing Systems

4 Conclusions

This deliverable is the first delivery of task T6.6. This task will specify and implement processes for certifying and standardizing digital finance/insurance solutions in the project's tailored sandboxes and testbeds. Special emphasis will be paid in regulatory compliance and standards-compliance certification processes based on the specification and execution of appropriate tests. Moreover, the task will ensure that experimenters and innovators get appropriate support regarding their use of testbed facilities and sandboxes such as support on hardware/software deployment issues, as well as support on system and administration issues.

It is provided in this deliverable a definition and initial design of a certification model and related methodology/process for the fintech solutions. The certification and compliance services focus on regulatory and (security) standards compliance. The INFINITECH certification process has been defined to be served on a self-certification mode with a well-established stepwise process in-place.

Certification and compliance services focuses on regulatory and (security) standards compliance, particularly on the set of regulations with the most relevant impact on INFINITECH which are: ISO/IEC 27001 Information technology: Security techniques, Information security management systems Requirements; ISO/IEC 27701 Privacy Information Management System (PIMS); Payment Card Industry Data Security Standard (PCI DSS); National Institute of Standards and Technology (NIST) Cyber Security Framework – Financial Services Cyber Security Profile; GDPR - The General Data Protection Regulation; PSD 2 - Payment Service Directive 2; MiFID II - Markets in Financial Instruments Directive II; 4AMLD - 4th Anti-Money Laundering Directive.

Additionally, a set of support services have been defined for the NOVA testbed infrastructure for experimentation of digital finance solutions within the INFINITECH project. Support services include Software and Hardware Deployment Support Services, Helpdesk Service, and others. The provider of the support services is the NOVA Computing Division (NOVA DIV-I,). The NOVA Computing Division plans and maintain the entire computer and network infrastructure of the NOVA School of Science and Technology.

Deliverable D6.13 will be followed by two additional deliverables which the following foreseen content: Deliverable D6.13 'Testbeds Support and Certification Services - II' at M30: Report on the implemented Support and Certification Services for fintech solutions and testbeds; Deliverable D6.13 'Testbeds Support and Certification Services - III' at M36: Report on the testing & validation of Support and Certification Services for fintech solutions and testbeds, and on the optimisations performed.

Appendix A: Literature

[1] Testing two-factor authentication, Michelangelo van Dam, 05/08/2017.
https://www.in2it.be/2017/08/testing-two-factor-authentication/