# **Appendices**

## Appendix A: Project-to-Policy Contribution

**The Critical-Chains Consortium Project-to-Policy Responses to EC Policy Unit Questionnaire relating to Regulatory, Standardisation, Compliance and Certification issues.**

 **Date: 21-09-20**

**Q1 What *do you consider as the main shortcomings of the cybersecurity legislation and policy that your project has encountered? -Could you propose any workable solutions how these could be tackled?***

Regulatory mechanisms need to support threat-driven, risk-based and operational-context-aware security and privacy-by-design as well as compliance assurance audit including of IT products and cloud services.

The rapid pace of innovations relating to cryptocurrencies and mobile money has opened up new business models some of which have operated in a regulatory void whilst new spaces have emerged in the financial transaction’s domain exposed to various types of irregularity and fraudulent conduct. In particular there is no regulatory regime for cryptocurrencies at European level. Some countries of the EU (e.g. Germany) have already put in place legislation relating to the new currencies; thus, there is a vacuum to be addressed by European level directives that will inevitably have to pass through a phase of harmonisation and homogenisation of the regulations already present. A lack of legal certainty is often cited as the main barrier to developing a sound crypto-asset market in the EU -the goal proclaimed by the recent declarations of Valdis Dombrovskis (European Union’s Executive Vice President of the European Commission for An Economy that Works for People). (<https://www.coindesk.com/eu-bloc-wide-regulatory-regime-crypto-economic-chief>).

Personal data and card holder data need to be protected in compliance with the General Data Protection Regulation (GDPR) and the Payment Card Industry Security Standards (PCI – DSS). The application of these regulations should be certified by a Qualified Security Assessor (QSA) to verify correct implementation and adherence to security measures and processes required by each regulation and cover all minimum issues related to applicable directives and standards. Additional applicable local laws also need to be reviewed.

In the wider private sector who are the source of much of the financial transactions and as such constitute one side of the stakeholders involved, security policies range from non-existent to not-so-easily align-able to support business-to-business collaboration - lacking a common security requirements baseline.

This is not helped by the universally shared observation that some cyber privacy-security legislation is not easily translatable to operational implementation actions. This is due to:

* lack of a commonly accepted cost-effective solution requirement (which anyhow would have to be prioritised in each case based on the criticality of any risks to core business operations)
* lack of specific technology standard or prescribed solution for specific sectoral business context
* Lack of clear definitions e.g. the PSD2 provides a guideline as to how to create secure authentication methods, but it lacks a clear definition of what “independent” authentication factors means.

Some companies are well prepared for GDPR compliance and others are more focused on protecting confidentiality and integrity during the exchange of financial data.

Without specific schemas (or guidelines, at least) it is difficult to set-up a properly balanced security audit plan (when needed). The audit level of detail and the extent of evidence must be applicable to business operational context.

Cybersecurity attitudes are not homogeneous across different personnel roles. Usually people are not fully aware of security risks, threats and incidents and may be inadequately trained to identify and respond to them.

A security strategy should integrate all the security requirements, identify relevant context-specific security objectives, and orchestrate all the activities that operate the established security measures responsive to the regulations, and standards.

It is possible to imagine that the advent of transformative technologies may open up new security protection capabilities that may obviate the need for some regulatory mechanisms whilst, as a side-effect, also creating new security loopholes requiring new regulatory mechanisms. In this sense, and particularly given the rapid pace of innovation of systems and business models in the financial sector, the regulatory innovation has to remain closely responsive to the emerging patterns of new security needs and new malicious use-cases to ensure a rapidly learning regulatory eco-system keeping up with the disruptive innovation and resulting business models and putting in place the required regulatory mechanisms to ensure the trustful integration of new technology whilst preventing the new evolving patterns of fraud.

For example, the advantages of DLT and blockchain include greater user control, reduced transaction time and cost, immutability, enhanced efficiency and automation, transparent financial audits, tamper-proof logging, and overall fewer chances of errors or fraud. The general security measures in the financial domain have significant problems because of the trade-off between security and efficiency, privacy and efficiency and trustworthiness. The online transactions, especially at worldwide level are cumbersome which may cause serious latencies in transactions and lack of trust between transactors. Blockchain infrastructure can provide effectively support some of the requirements but as highlighted in the Kaspersky report on DLT cybersecurity[[1]](#footnote-1), the risks associated with DLT and blockchain still remain. As new attack surfaces emerge so do new attacks, finding new vulnerabilities to exploit. However, traditional blockchain implementations do not prioritise time-critical transactions or data while they are waiting to be added to the blockchain. Cumbersome blockchain infrastructures can fail to achieve coherence within an acceptable latency. This may cause serious problems in various sectors such as Industry 4.0, smart health, or transportation where the integrity of processes may be directly or indirect affected by related financial flows. For instance, a typical smart transportation application requires toll collection or the use of city cards where millions of people pay for mobility cards and use them in mobility systems. Hence, there is a strong need to define and elaborate sector-specific security, privacy and even safety measures that should be linked to financial operations covering payment systems, insurance, online banking, and promotional systems.

This points to a dual strategy of parallel innovation in new security paradigms and technological solutions on the one hand, and, a fast-learning regulatory innovation framework on the other hand. For example, supporting digital signing solutions that are scalable and make digital infrastructure more transparent.

 The major security shortcomings in the Financial Industry may be listed as personal data hijacking, for example theft, usage and/or sale (e.g. on the dark net) of victims’ credit cards detail via bank or merchant fraud, and illicit money trafficking. The fully decentralised nature of blockchain may cause vulnerabilities and weaknesses that can be exploited by fraudsters and criminals. This is not only applicable to financial crimes but also other crimes, such as human trafficking, communication and illegal online material sharing over private chains. For instance, some crime organisations share videos and photos of children for sexual exploitation. The triangular model that is proposed in the Critical-Chains project adds authorities (e.g. banks, governmental organisations) in the loop as an approver, and regulatory needs learning and feedback node, for any transaction between two (or more) transactors (e.g. sender and receiver). This model consisting of transactor 1, transactor 2 and the authority can be standardised for any transactions over any smart application to offer both immutability and accountability. In doing so the distributed ledgers and smart contracts may include the trusted parties (authorities) in the chain which makes for semi-decentralised approval available 24/7 at a global scale

**Q2- *To what extent do you think the general security measures baselines (based for example on ISO27001) are effective at sectoral level and would more sector-specific measures be needed for the financial sector?***

General security measures baselines, for example, ISO27001, are in general able to answer security challenges in traditional financial institutions, with a constraint that all updates to a standard, such as ISO/IEC 27701:2019 (Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines), should be implemented.

The ISO 27001/27002 security measures can identify high level objectives that need to be achieved by specific security measures. PCI and GDPR identify the processes required to determine what specific security measures and processes are most suitable for a specific architecture based on the specific risks and vulnerabilities related to the systems, communications and applications deployed as part of a specific solution.

These standards and other frameworks e.g. COBIT, NIST CSF etc. are multi-purpose schemes applicable in different contexts, but they do not pose specific security requirements that define common security measures for a specific sector (e.g. they do not define that an IT system used in the Financial Sector shall be designed, developed, tested, installed, configured, etc. in a particular way and the system shall meet specific security requirements, the same for the policies, procedures etc. that are part of a management system). Thus, more specific/sectorial security requirements should be identified for network segregation, access control, accounting, logging, integrity checking and so on.

The general security measures baselines such as ISO27001 are thus not very effective when applied to modern applications in the Financial Sector that have specific security requirements and often involve the usage of mobile applications. In these cases, the generic security measure baselines must be integrated and expanded with security controls for other frameworks. In this way significant progress has been made in terms of responding to cyber threats and protecting personal data through specific tools such as the NIS regulation and the PSD2 regulation.

* These regulations have increased the level of cyber security but will require, continuous technological refinement to remain constantly updated responsive to the continuing mutation of cyber threats.
* Sector-specific measures are needed, but it is difficult to publish them as business interests prevail. The financial sector must prove that they can be transparent and have earned the trust needed. Internal auditing and compliance systems have shown monitoring failures, for example, in money laundering cases.
* Specific requirements should be identified also for the risk management process, periodic vulnerability assessment, personnel drills (both for IT and non-IT personnel). Standardised security certification of IT products should be more widely implemented.
* Special attention, and a potential standard review, should be considered for cloud based FinTech services, because they bring in new challenges and threats.
* General signing requirements enable analysis afterwards at a detailed level, of any digital event.

***Q3- How do you assess the role of digital service providers and in particular cloud service providers within the financial sector as compared to other critical sectors?***

The financial sector is one of the most active sectors investing in digital services and cloud infrastructure. With the recent developments in online systems, for example over the cloud, banking and the insurance sectors have evolved into the digital age. Recent trends such as mobile banking, e‑banking, online stores and purchasing over the Internet, e-insurance, e-government, e-payment, e‑tax, etc. have shown that the level of technology acceptance in the Financial Sector is high. The service or cloud providers can support the Fintech processes by undertaking some of the most common issues of infrastructure with the highest level of technology at accessible prices.

Accordingly, the rising trend for financial service providers is to move their services to the cloud. Compared to other critical sectors, the Financial Sector is even more exposed to cyber-attacks as its business is totally exposed to the cloud network. In this sense, the sector is moving in the direction of a shared information security model. This move from physical to cloud could make companies increasingly dependent on service providers.

Cloud service providers are crucial for the Financial Sector to establish and maintain worldwide and 24/7 availability of financial services as well as for providing capabilities for crypto services. As the global economy depends highly on a steady money flow, cloud service providers must ensure a safe and easy access to their services for individuals as well as for companies.

However, digital service providers must earn the trust of other Financial Sector partners and customers. Different measures have been used. Payment system providers have been successful in this so far.

One approach to assessing the role of digital service providers and in particular cloud service providers is to add the security measures and processes required as part of the SLA requirements and perform audits to assess the correct management of the information related to the service provided by the third party.

Since the Financial Sector is more sensitive to privacy issues compared to other sectors, digital service providers, and especially cloud service providers, need to focus more on compliance with privacy protection related regulation. Critical infrastructure sectors (energy, water distribution,), for example, should be more focused on safety and availability issues, to protect users and service delivery.

**Q4**-***Do you observe a specific need for additional or revised policy or regulation in the Financial Sector, which renders it different from other critical sectors?***

One has to wonder whether indeed it was a lack of regulations or poor monitoring that have led to the various reported failures in timely detection and the tracking of money transactions in cases such as the apparent disappearance of over 2 billion Euro from the Wirecard balance sheet.

It may be that there indeed exist sufficient policies and regulatory mechanisms but that monitoring, and enforcement would need to be strengthened. The authorities would need to maintain the focus on existing policies through constant monitoring of the evolution of cyber security scenarios with a view to periodically updating existing policies in order to achieve the goal of continuous improvement that enables an effective and efficient response to the continuous mutations of the cyber threat scenario (e.g. increasing the use of artificial intelligence for cybercrime).

However given that E-banking is a reality and will be the main banking channel in the near future it can be argued that there is a need for regulation that supports litigation against the bank, using legally admissible evidence based on forensic data intelligence that proves the nature of the digital activities.

Even although the financial sector data exchange does not involve the safety or the health of individuals, it is still the case that specific security and privacy protection requirements and controls should be defined prior, during and after a transaction or data exchange, focusing on security measures which involve data confidentiality, authenticity and integrity both for data in transit and data at rest.

There is a specific need to revise the policies about using blockchain not only in the Financial Sector but also in other sectors as the financial sector provides a cross-sectoral underpinning that influences all other domains. This is not only related to the use of cryptocurrencies in financial transactions, but also regulations related to smart contracting and distributed ledgers, and the participation of a centralised authority or authorities in such financial operations. Such a regulatory revision should also tackle the coordination and collaboration of many centralised authorities; for instance, two different banks or a bank-insurance company.

An instance of this is the type of solution stack that support a critical sector infrastructure (e.g. transportation) that manages cardholder data which needs to be verified and secured in transit and at rest to protect the confidentiality of the information managed without compromising the availability of the service. Such pipelines should be assessed to determine the level of maturity/complexity required over the security measures that should be implemented to protect the critical, sensitive, or personal data managed by the solutions through the pipeline.

## Appendix B: Links to Critical-Chains Presentation PowerPoints

For the Project-to-Policy Workshop held at the REA, Brussels 31-01-2021

<https://research.reading.ac.uk/critical-chains/wp-content/uploads/sites/130/Unorganized/Critical-Chains-833326-Policy-Workshop-15PPset-Atta-Badii-22-01-2020.pdf>

## Appendix C: Abstracts of Scientific & Technical Papers and Links to full text

Paper#1 by IMEC-NL

Relay attacks pose a serious security threat to wireless systems, such as contactless payment systems, keyless entry systems, or smart access control systems. Distance bounding protocols, which allow an entity to not only authenticate another entity but also determine whether it is physically close by, effectively mitigate relay attacks. However, secure implementation of distance bounding protocols, especially of the time critical challenge-response phase, has been a challenging task.

In this paper, we design and implement a secure and accurate distance bounding protocol based on Narrow-Band signals, such as Bluetooth Low Energy (BLE), to particularly mitigate relay attacks. Narrow-Band ranging, specifically, phase-based ranging, enables accurate distance measurement, but it is vulnerable to phase rollover attacks. In our solution, we mitigate phase rollover attacks by also measuring Time-of-Flight (ToF) to detect the delay introduced by such attacks. Therefore, our protocol effectively combines the best of both worlds: phase-based ranging for accuracy and Time-of-Flight (ToF) measurement for security. To demonstrate the feasibility and practicality of our solution, we prototype it on NXP KW36 BLE chips and evaluate its performance and relay attack resistance. The obtained precision and accuracy of the presented ranging solution are 2.5cm and 30cm, respectively, in wireless measurements.

Link to full text: Not published yet.

Paper #2 by ERARGE

This brief presents a reconfigurable Random Number Generator (RNG) based on transient effect of ring oscillators. Users can select a method based on the irregular sampling of a regular waveform or on the regular sampling of an irregular waveform to obtain a random bit sequence to be used in different applications, such as lightweight cryptography or high-security communication. The entropy is acquired by exploiting Transient Effect Ring Oscillators (TEROs). The proposed fully-digital RNG structure is firstly implemented on a Zynq-7000 FPGA (Field Programmable Gate Array) without any post-processing method such as the Von Neumann. In addition to the RNG structure, an on-the-line test module based on FIPS 140-2 is also implemented to check the randomness of the produced data statistically in real time. Users can change the statistical test parameters according to their desired security levels. Finally, an ASIC (Application Specific Integrated Circuits) implementation of the proposed RNG is done following the Cadence digital design flow for the TSMC 180 nm CMOS process. The implemented ASIC design occupies an area of 0.85 mm x 0.85 mm and the estimated power required is 11.827 mW.

Link to full text: <https://ieeexplore.ieee.org/document/9153808>

Paper #3 by ERARGE

Blockchain has the capacity to transform the industries disruptively as it presents new features like smart contracts, tokenization of content, eliminating counterfeit products, supply chain improvement, digital twins, and end-to-end security. This letter presents a Diamond Accountability Model (DAM) where a public or private authority is included in the blockchain transactions providing non-repudiation of digital transactions, holistic security and effective governance. The proposed technique aims to present a decentralized solution for multi-agent applications where many partnering organizations have to collaborate without suffering from the security, accountability, maintenance, scalability, and integrity problems over distributed cyber-physical systems (CPS). The proposed scheme positions authorities also in the chain that enables additional accountability and trust. The scheme proposes a verification mechanism where the authorized organizations are also included in the verification of transactions over the blockchain. In order to elucidate, a conceptual use case is presented where at least two partnering organizations collaborate with each other within a decentralized but also authorized blockchain-enabled scheme.

Link to full text: <https://ieeexplore.ieee.org/document/9209518>

Paper #4 by ERARGE

A novel cross-coupled bipolar transistor-based non-autonomous chaotic oscillator is proposed. The derivation methodology of this novel chaotic oscillator is based on integrating two of existing chaotic oscillators symmetrically and employing a differential-pair stage. Simulation and experimental results, verifying the feasibility and the correct operation of the circuit are also given.

Link to full text: <https://ieeexplore.ieee.org/document/8884899>

Paper #5 by ERARGE

This brief presents a random number generator (RNG) based on irregular sampling of regular waveform method where the irregular signal is obtained by combining Fibonacci-Galois ring oscillators with an XOR gate. The RNG is implemented on a FPGA (field-programmable gate array). The regular waveform generated by the digital clock manager of the FPGA, is sampled at times corresponding to certain number of rising edges of the irregular signal, and the resulting bit stream is subjected to statistical tests of randomness. It is demonstrated that the resulting bit sequence from the proposed RNG satisfies NIST 800-22 test suit and Rabbit and SmallCrush batteries from TestU01 library without any need for post-processing such as Von Neumann or XOR. A comparison between the methods regular sampling of irregular waveform and irregular sampling of regular waveform is given in terms of robustness against external interference. The impact of selection of Fibonacci-Galois polynomials is discussed. Using digital design flow for TSMC 65nm process, a basic implementation of the proposed RNG is given having 1115 gates and 4.811 mW estimated power.

Link to full text: <https://ieeexplore.ieee.org/document/8789641>

Paper #6 by ERARGE

This paper presents a comparative study on continuous-time chaos-based random number generation methods regarding their robustness against changes in chaos controlling parameters and external interference. Chaotic systems suggest enabling high throughput random data without need for post processing and with less complex hardware. However, due to effects of aging or fabrication process variations, the chaos controlling parameters of the random number generator may change. Furthermore, external interference can be applied on the chaotic oscillator to manipulate its output. Therefore, in a chaotic RNG, the bit generation method should be immune to parameter variation and external interference. In this study, two widely used methods for random number generation have been compared: 1) Regular sampling of chaotic waveform (RSCW), and 2) Chaotic sampling of regular waveform (CSRW). A double-scroll chaotic system is chosen as the chaotic oscillator and it is numerically simulated in normalized time domain to generate random bit sequences using both methods. Applying the concepts of autocorrelation and approximate entropy to the output bitstreams, the robustness of the two-bit generation methods against parameter variation and external interference have been compared. It is demonstrated that chaotic sampling of regular waveform method provides more robustness against parameter changes and external interference compared to regular sampling of chaotic waveform method.

Link to full text: <https://ieeexplore.ieee.org/document/8953106>

Paper #7 by ERARGE

A novel attack system is proposed to reveal the security weaknesses of a microcomputer-based random number generator (RNG). Convergence of the attack system is proved using auto-synchronization. Secret parameters of the microcomputer-based RNG are revealed where the available information are the structure of the RNG and a scalar time series observed from the chaotic system used as the seed of the RNG. Simulation results verifying the feasibility of the attack system are given such that, next bit can be predicted while the same output sequence of the RNG can be generated.

Link to full text: <https://ieeexplore.ieee.org/document/9006666>

Paper #8 by ERARGE

With the recent advancements in blockchain technology, it has become obvious that this technology is not just for crypto-currencies but instead can be used as a decentralized tool for better accountability. Blockchain has the capacity to transform the industries disruptively as it presents new features like smart contracts, tokenization of content, eliminating counterfeit products, supply chain improvement, digital twins, and end-to-end security. This paper presents a blockchain-based model for distributed and collaborative digital twin environments which is becoming indispensable in new “Any 4.0” era. The proposed model includes a public or private authority in the digital twin ecosystem providing non-repudiation of blockchain transactions, holistic security and privacy preservation. The proposed technique is based on the “X-by-design” and “X-as-a-service” principles which can be discussed as a novel model for better security, accountability and integrity in decentralized mechanisms. In order to elucidate, two case studies are described where the digital twin operations, stakeholders' activities and regarding transactions are stored on a blockchain.

Link to full text: <https://ieeexplore.ieee.org/document/8914304>

**Paper #9 by JR**

Automated detection methods for targeted cyber-attacks are getting more and more prominent. In order to test these methods properly, it is crucial to have a suitable dataset. This paper provides a review on datasets and their creation for use in APT detection in literature. A special focus is placed on feature engineering, including construction, selection and dimensionality reduction. Two use cases based on the underlying infrastructure are distinguished, large enterprise networks and Cyber Physical System, additionally including cloud computing systems, financial technology networks and Internet of Things networks. These datasets are usually based on an attack model. A description of different stages including approaches and goals of such attacks are given. The major achievement is the description and analysis of existing feature extraction methodologies and detailed overview of datasets used in APT detection related literature. This shows that the large enterprise network use case, has incorporated a much more frequent use of datasets with quite short periods of time. In the case of Cyber Physical System, a realistic dataset is publicly available.

Link to full text: <https://doi.org/10.1016/j.cose.2020.101734>

**Paper #10 by JR, UREAD**

Nowadays, virtually all products and services offered by financial institutions are backed by technology. While the frontend banking services seem to be simple, the core-banking backend systems and architecture are complex and often based on legacy technologies. Customer-facing applications and services are evolving rapidly, yet they have data dependencies on core banking systems running on ancient technology standards. While those legacy systems are preferred for their stability, reliability, availability, and security properties, in adapting the frontends and services many security and privacy issues can occur. Clearly, these issues are arising as those systems have been designed decades ago, without considering the enormous amounts of data that they are required to handle and also considering different threat scenarios. Moreover, the trend towards using new technologies such as Distributed Ledger Technologies (DLT) has also emerged in the financial sector. As the nodes in DLT systems are decentralized, additional security threats come to light. The focus of this work is the security of financial technologies in the FinTech domain. We provide relevant categorization and taxonomies for a better understanding of the main cyber-attack types, and suitable countermeasures. Our findings are supported by using security-by-design principles for some selected critical financial use-cases, and include a detailed discussion of the resulting threats, attack vectors and security recommendations.

Link to full text: <https://eprint.iacr.org/2020/1440>

**Paper #11 by JR, FHG, UREAD**

Financial technology, or Fintech, represents an emerging industry on the global market. With online transactions on the rise, the use of IT for automation of financial services is of increasing importance. Fintech enables institutions to deliver services to customers worldwide on a 24/7 basis. Its services are often easy to access and enable customers to perform transactions in real-time. In fact, advantages like these make Fintech increasingly popular among clients. However, since Fintech transactions are made up of information, ensuring security becomes a critical issue. Vulnerabilities in such systems leave them exposed to fraudulent acts, which cause severe damage to clients and providers alike. For this reason, techniques from the area of Machine Learning (ML) are applied to identify anomalies in Fintech applications. They target suspicious activity in financial datasets and generate models in order to anticipate future frauds. We contribute to this important issue and provide an evaluation on anomaly detection methods for this matter. The experiments are conducted on several fraudulent datasets from real-world and synthetic databases, respectively. The obtained results confirm that ML methods contribute to fraud detection with varying success. Therefore, we discuss the effectiveness of the individual methods with regard to the detection rate. In addition, we provide an analysis on the influence of selected features on their performance. Finally, we discuss the impact of the observed results for the security of Fintech applications in the future.

Link to full text: NA

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. <https://www.kaspersky.com/enterprise-security/dlt-cybersecurity> [↑](#footnote-ref-1)