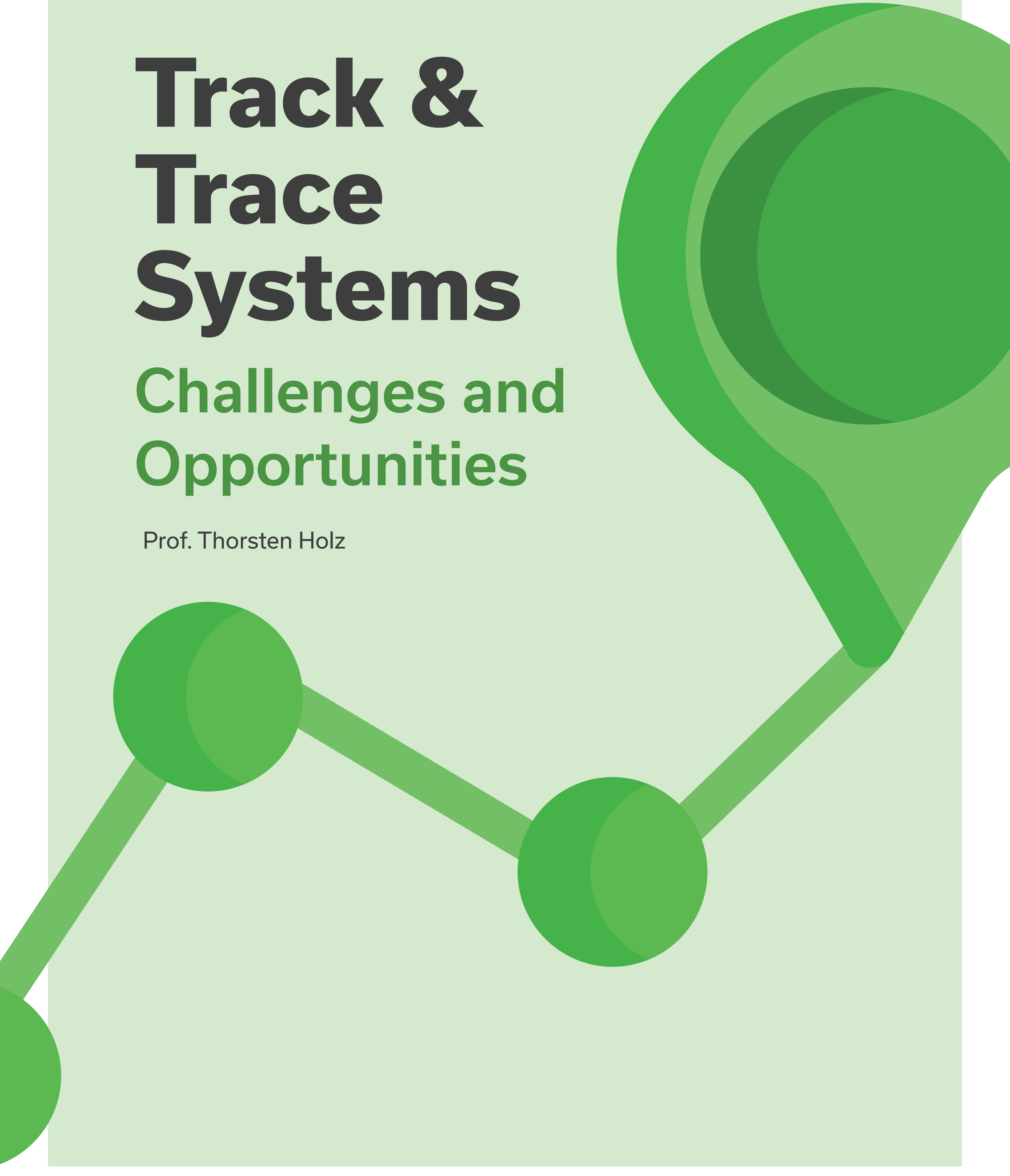
Track & Trace Systems

Challenges and Opportunities

Prof. Thorsten Holz

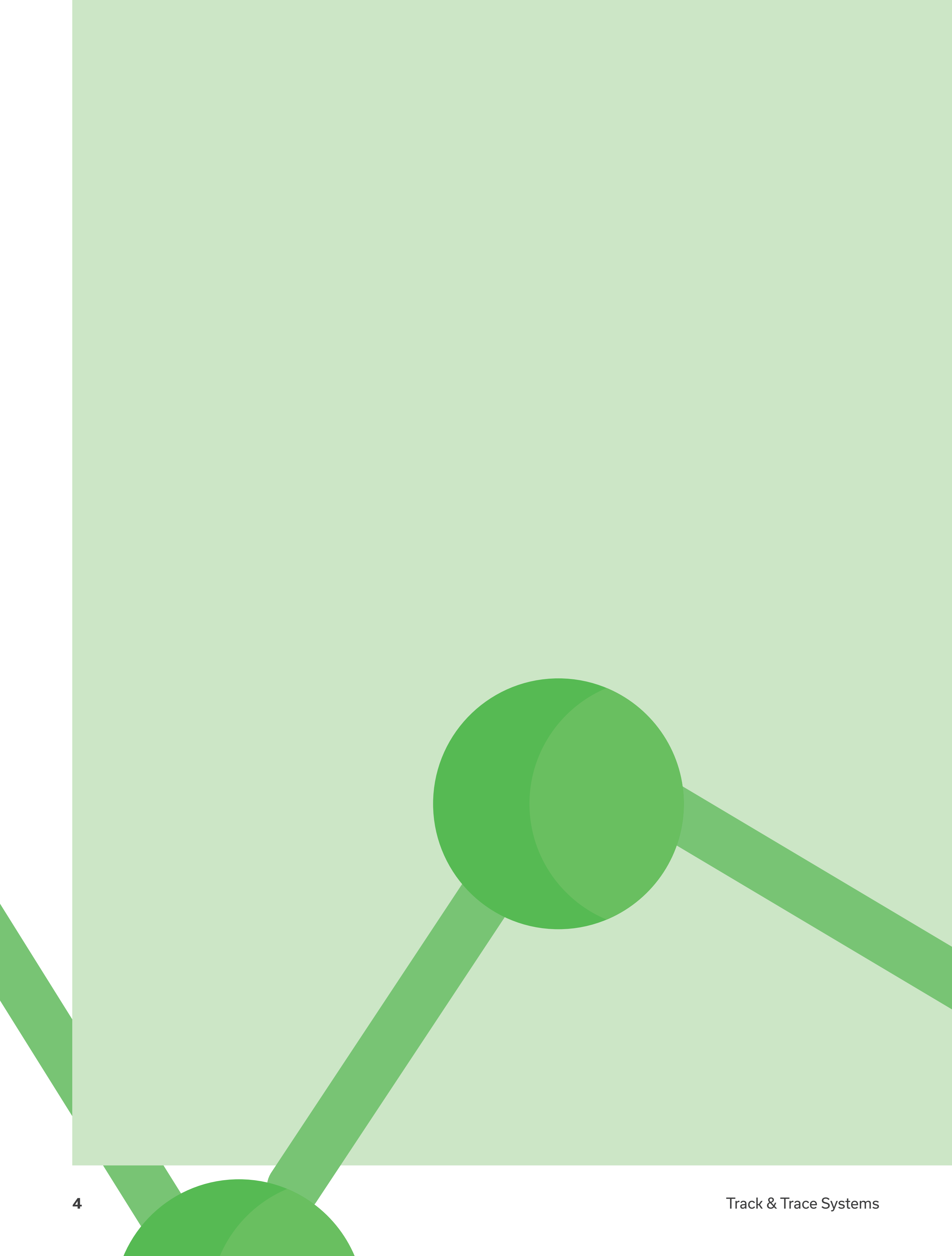


EXECUTIVE SUMMARY

Illicit tobacco trade is a major problem in practice, and this type of criminal activity is responsible for many millions of Euros in tax losses per year. In recent years, several regulatory frameworks have been created to address this problem, most notably the *Protocol to Eliminate Illicit Trade in Tobacco Products (also known as the Illicit Tobacco Trade Protocol (ITP) and FCTC Protocol)* adopted by the World Health Organization (WHO). To eliminate all forms of illicit trade in tobacco products, the FCTC Protocol mandates that a *global Track & Trace* (T&T) system for the legal supply chain of tobacco products must be in place by September 2023. The basic idea of a T&T system is to precisely *track* each produced product and meta-information during distribution and enable *traceability* through the entire supply chain. The FCTC Protocol envisions a global T&T ecosystem that connects national/regional T&T systems via a so-called *global information-sharing focal point* (GISFP). Still, the exact requirements and specifications of the GISFP are not clear yet. As a signatory to the FCTC Protocol, the European Union has incorporated the principles and measures of the Protocol into the *Tobacco Products Directive* (EU TPD). As a result, the EU has been operating a T&T system since May 2019. By March 2021, the system has already successfully tracked more than 53 billion products across 810,000 economic operators and 1,5 million facilities in the supply chain belonging to the 27 EU Member States.

Security and privacy are critical factors in the development and operation of a trusted global T&T environment, mainly because organized criminal groups, terrorists, and other large-scale adversaries have an incentive to disrupt the operation of such a system. Such adversaries could, for example, derive information about ongoing investigations by observing the communication channels of the system. Hacktivists and industrial espionage are other threats that need to be considered in the design of the T&T system. In this study, we analyze the data security and privacy requirements of a T&T system as required by the FCTC Protocol. We focus on critical properties that need to be fulfilled to obtain a trusted system and analyze the attack surface. Using various case studies, we show that both data security and data protection requirements must be taken into account in the early stages of the design phase, not just after the fact. Adding such requirements only in the implementation or deployment phase is almost impossible and only leads to band-aid solutions that are brittle and vulnerable. We conclude with several recommendations and potential next steps for the implementation of the FCTC Protocol.

CONTENTS



INTRODUCTION

Illicit tobacco trade and related activities are responsible for many millions of Euros in tax revenue losses every year in the European Union (EU) and the whole world. Although measuring the real size of the corresponding underground market is challenging, a recent study estimates that illicit trade cost the 27 EU Member State governments about 11 billion Euros annually [4]. On a global level, another study estimates that the annual revenue losses in tobacco taxation is around 40–50 billion US-Dollars [13]. Most worrisome, the illicit tobacco trade has been identified as a primary source of revenue for organized crime and terrorism. Moreover, such illicit products are often substantially cheaper than legal tobacco products, and these products are less likely to comply with official regulations (e.g., official health warnings), which poses additional health risks.

To address this challenging and pressing problem, several regulatory frameworks were created in the past years to fight the illicit trade of tobacco products and to secure the legitimate trade. *The World Health Organization Framework Convention on Tobacco Control* (WHO FCTC) was adopted in 2003 to govern the production, sale, distribution, advertisement, and taxation of tobacco products. As a supplementary international treaty, the *Protocol to Eliminate Illicit Trade in Tobacco Products* (also known as the *Illicit Tobacco Trade Protocol* (ITP) and *FCTC Protocol)* was adopted in 2012. The specific focus of this Protocol is to eliminate all forms of illicit trade in tobacco products. To this end, the FCTC Protocol mandates that a *Track & Trace* (T&T) system must be established to closely control/monitor the legal supply chain of tobacco products.

A simplified, high-level overview of the general procedure of a T&T system is shown in Figure 1.1. A unique identifier *(tracking code)* is requested from a (trusted) third party for each product produced, and the code is applied during production. Information regarding the tracking code is then sent to a repository. The figure shows the most basic setup with a single, centralized database.

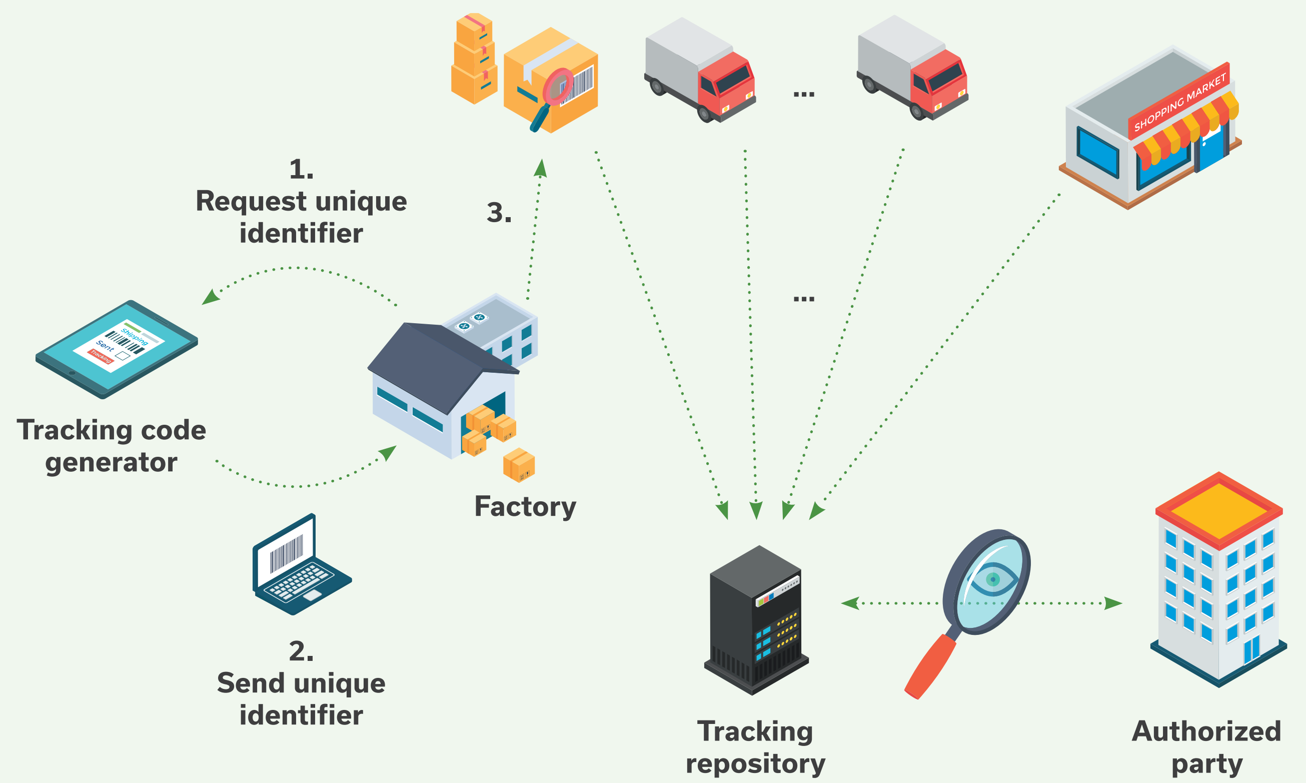


Figure 1.1: Basic setup of a Track & Trace (T&T) system

Depending on the requirements, the repository can also be deployed in other configurations (e.g., decentralized setup, federated setup, hierarchical setup, etc.). To trace the supply chain, an update is sent to the database during each step of the distribution process *(tracing)*. Authorized parties (e.g., the company or regulators) can access the database and check the content.

By September 2023, all parties to the ITP must deploy their own T&T system, and a global information exchange mechanism will need to be designed, developed, and deployed. This ecosystem will allow the individual T&T systems to connect to each other and exchange information. In the EU, the *Tobacco Products Directive* (EU TPD) governs the T&T system. Such a system is in use since May 2019: tracking and tracing information for both production and logistics of tobacco products has to be collected, and the resulting data is stored in a set of data repositories. As of March 2021, more than 53 billion products were already tracked and traced via this system [1].

In this study, we analyze the data security and privacy requirements of a T&T system as required by the FCTC Protocol. The Protocol envisions the establishment of a *world-wide* T&T ecosystem consisting of national and / or regional T&T systems combined with a so-called *global information-sharing focal point* (GISFP). The exact requirements and specifications of the GISFP are not clear yet.

We examine such a system's security and privacy requirements, and analyze the potential attack surface. Given that the illicit tobacco trade is mainly performed by organized crime groups and similar competent adversaries, we need to consider a powerful attacker model. We argue that both data security and privacy requirements must be taken into account already in the early stages of the design phase, and not as an after-thought: adding such requirements only in the implementation or deployment phase is impossible and only leads to band-aid solutions that are brittle and fragile.

Furthermore, this requirement analysis leads to several recommendations that should be followed when implementing the Protocol. We argue that the GISFP should be deployed as a query-based system / message broker that relays inquiries between the individual T&T systems because this approach leads to a solution with a more manageable risk. However, such a message broker approach is challenging to implement in practice, and we discuss potential caveats that should be taken into account. For example, the design must ensure that European data is handled in a secure and confidential way, and this data must be protected by European legislation such as the *General Data Protection Regulation* (EU GDPR). When different T&T systems are interconnected, security and privacy requirements need to be taken into account early on. These requirements also increase as the complexity and interoperability of the system architecture develop over time.

Another important concern that needs to be addressed is the question of who designs, implements, and maintains the GISFP. Many financial, legal, and political interests are involved, and we argue that the European implementation of a T&T system can serve as a role model: Europe has about two years of operational experience in running such a complex system, and the underlying system architecture is likely the most compelling approach to implement the Protocol.

OUTLINE

The rest of this study is outlined as follows: In Chapter 2, we explain the technical and regulatory background for T&T systems for tobacco products. Data security and privacy challenges of such a T&T system are examined in Chapter 3, with a specific focus on potential risks. In Chapter 4, we discuss several recommendations and potential next steps for an implementation of the FCTC Protocol, and we conclude this study in Chapter 5.

TECHNICAL AND REGULATORY BACKGROUND

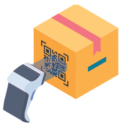
2

2.1 TRACK AND TRACE SYSTEMS

Securing and monitoring the supply (and value) chain is a crucial aspect in many domains, especially in logistics. Generally speaking, the main focus of *supply chain security* is to prevent illicit trade. Two specific aspects need to be taken care of: (i) preventing products from being diverted from the legal supply chain and (ii) preventing counterfeit products from entering the legal supply chain. This aim can be achieved by closely *tracking* each product: starting from production and during distribution, each product needs to be tracked until a consumer buys the product.

A closely related aspect is the requirement that it should be possible to *trace* the origin of a product upon receipt (i.e., tracing the supply chain in the backward direction). Rotunno et al. define such systems as follows: „Track and Trace (T&T) can be defined as the capability to chase products throughout the whole supply chain, by recording a given set or type of information that allows the verification of history, location or application."[10] T&T systems influence business factors like efficiency, synchronization of different entities, visibility of the supply chain, and security aspects.

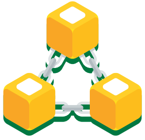
Beyond companies, T&T systems also offer great potential for state and international authorities when it comes to monitoring supply chains. For example, T&T systems can provide an effective and efficient tool against pressing problems like smuggling, illicit trade, theft, and counterfeit products. From the government's point of view, T&T systems play a major role especially in strongly regulated markets such as pharmaceuticals, food supply, chemicals, and tobacco. In the past years, several different technologies were developed to implement a T&T system. In practice, commonly used approaches include:



A barcode is a method for representing data in a visual, machine-readable form. There are different types of barcodes, the simplest variant being *linear* (also called *one-dimensional* (1D)) barcodes made up of lines and spaces of various widths. Linear barcodes can be read by special optical scanners and they are often used in retail (e.g., to implement the *European Article Number*). The generalized variant are *two-dimensional* (2D) variants (also called *matrix codes*) and more advanced approaches. A prominent example is *QR codes*, but many different variants exist.

Transmitter-receiver systems are based on a digital signal that is transmitted between a sender (typically called *tag*) placed on the product and a receiver. Communication protocols such as RFID, NFC, and Infrared are used to implement the communication channel between the tag and the receiver.

Real-Time Locating Systems (RTLS), also known as *real-time tracking systems*, allow to automatically identify and track the location of products in real time. There is a wide variety of systems concepts and designs to implement RTLS, ranging from RFID systems, Bluetooth, Zigbee, and WLAN for tracking in a limited area to Ultra-wideband (UWB), 4G/5G, or GPS for tracking over longer (potentially world-wide) locations.



Blockchains (also called *distributed ledgers*) are based on a list of data records that are chronologically linked to each other via cryptographic mechanisms. Such systems have received a lot of attention lately, but are still in an early development phase and crucial aspects such as scalability and interoperability still need to be solved.

CASE STUDY:

Track and trace in health sector

T&T systems are used in many highly regulated industries. One example is the envisaged global T&T system for the worldwide distribution of vaccines (supported primarily by the WHO and UNICEF). Local T&T networks for vaccine tracking currently exist in many countries, and the next step is now to expand to global structures. The development of such a T&T system is likely to lag well behind that of the tobacco system; as of December 31, 2021, the obligation to affix GS1 standard-capable barcodes will become mandatory. Overall, it is clear that the idea of a T&T system in the tobacco sector is already further advanced than in other industries and could thus take on a leading role concerning the establishment of technical standards.

The current generation of T&T systems is still limited to national or regional (EU) borders. In the near future, T&T systems will be expanded to a global scale, but many technical and regulatory challenges need to be solved along the way. For example, international standards must be established, interoperability needs to be ensured, and data security and data privacy challenges need to be addressed. In the following, we focus on T&T systems for tobacco products and present both the technical and regulatory background for such systems.

2.2 FCTC PROTOCOL

The *World Health Organization Framework Convention on Tobacco Control* (WHO FCTC) aims to govern the production, sale, distribution, advertisement, and taxation of tobacco, with a specific focus on better control of the demand and supply of tobacco products. It was adopted in May 2003 and came into force on February 27, 2005. As of March 2021, the treaty has been signed by 168 countries and is legally binding in 182 ratifying countries [11].

Based on the FCTC treaty, negotiations for the development of a supplementary international treaty began. These discussions were based on FCTC Article 15, which concerns the commitment of the involved parties to eliminate all forms of illicit trade in tobacco products [11]. After long negotiations, the *Protocol to Eliminate Illicit Trade in Tobacco Products* (also known as the *Illicit Tobacco Trade Protocol* (ITP) and *FCTC Protocol*) was adopted in November 2012 and entered into force on September 25, 2018.

The first Meeting of the Parties (MOP) to the Protocol took place in October 2018 and by March 2021, there were 62 parties to the Protocol [12]. Germany signed the document on October 1, 2013, and it was ratified on October 31, 2017.

The FCTC Protocol is the first legally binding treaty under the FCTC and explicitly aims to coordinate an international response to the problem of all forms of illicit tobacco trade. It consists of 47 articles that outline the expected provisions and the steps that all parties are expected to take in order to tackle illicit tobacco trade in an efficient and effective way. For the focus of this study, especially Article 8 on *Tracking and Tracing* (T&T) is relevant:

> **For the purposes of further securing the supply chain and to assist in the investigation of illicit trade in tobacco products, the Parties agree to establish within five years of entry into force of this Protocol a global tracking and tracing regime, comprising national and/or regional tracking and tracing systems and a global information-sharing focal point located at the Convention Secretariat of the WHO Framework Convention on Tobacco Control and accessible to all Parties, enabling Parties to make enquiries and receive relevant information.**

As stated in Article 8 (1), a T&T system has to be established with a deadline of five years from the entry date of the Protocol (i.e., by September 25, 2023) for cigarettes (and ten years for other kinds of tobacco products). This is a challenging goal, especially given that a *global* T&T ecosystem consisting of *national and/or regional* T&T systems and a *global* information-sharing focal point (GISFP) needs to be established such that a cross-border T&T mechanism can be enabled.

By September 2023, all FCTC Protocol signatories who had ratified the Protocol when it entered into force must have a fully functional T&T system on their territory. If a new Party ratifies the Protocol, it has five years to implement the system according to Article 8 (3) of the FCTC Protocol. Note that (at least a prototype implementation of) the GISFP needs to be ready by September 2023; the system can be extended in later stages. This is a very complex task, especially given that it requires multinational coordination with many different parties being involved. To further complicate the task, the Protocol does neither provide any technical guidelines for the implementation of a T&T system nor any official implementation guidelines. Article 8 (4) only specifies what kind of information needs to be available (e.g., date and location of manufacture, detailed information regarding the first customer who is not affiliated with the manufacturer, or any warehousing and shipping), but further operational details are missing.

To address these shortcomings and to minimize the space for interpretation, a working group of Parties was established during the first MOP to develop proposals for clear rules and guidelines for implementation. The task force was tasked to present its findings and recommendations at the second MOP meeting scheduled for November 2020. However, due to the ongoing COVID-19 pandemic, the meeting was postponed by one full year to November 2021, which implies further delays and certain danger to the schedule.

We estimate that it is a challenging task to implement a first version of the information exchange mechanism via the GISFP by September 2023. Given the complexity of such a system, sufficient time for testing (especially related to data security, data privacy, and interoperability) should be reserved when planning a reasonable timeline. In later stages, the system will be expanded step by step; also in these phases data security, data privacy, and related challenges need to be considered.

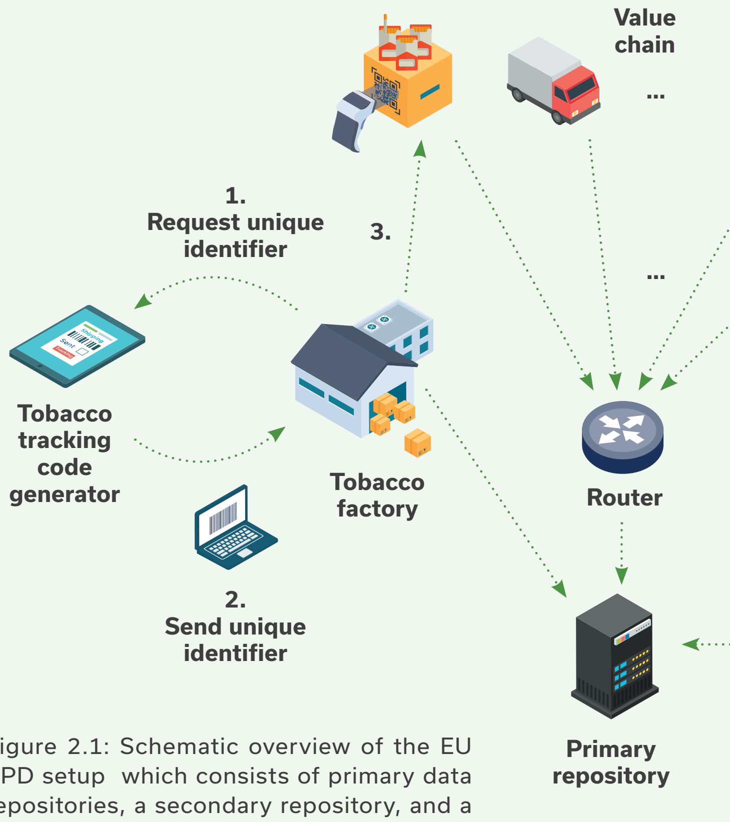
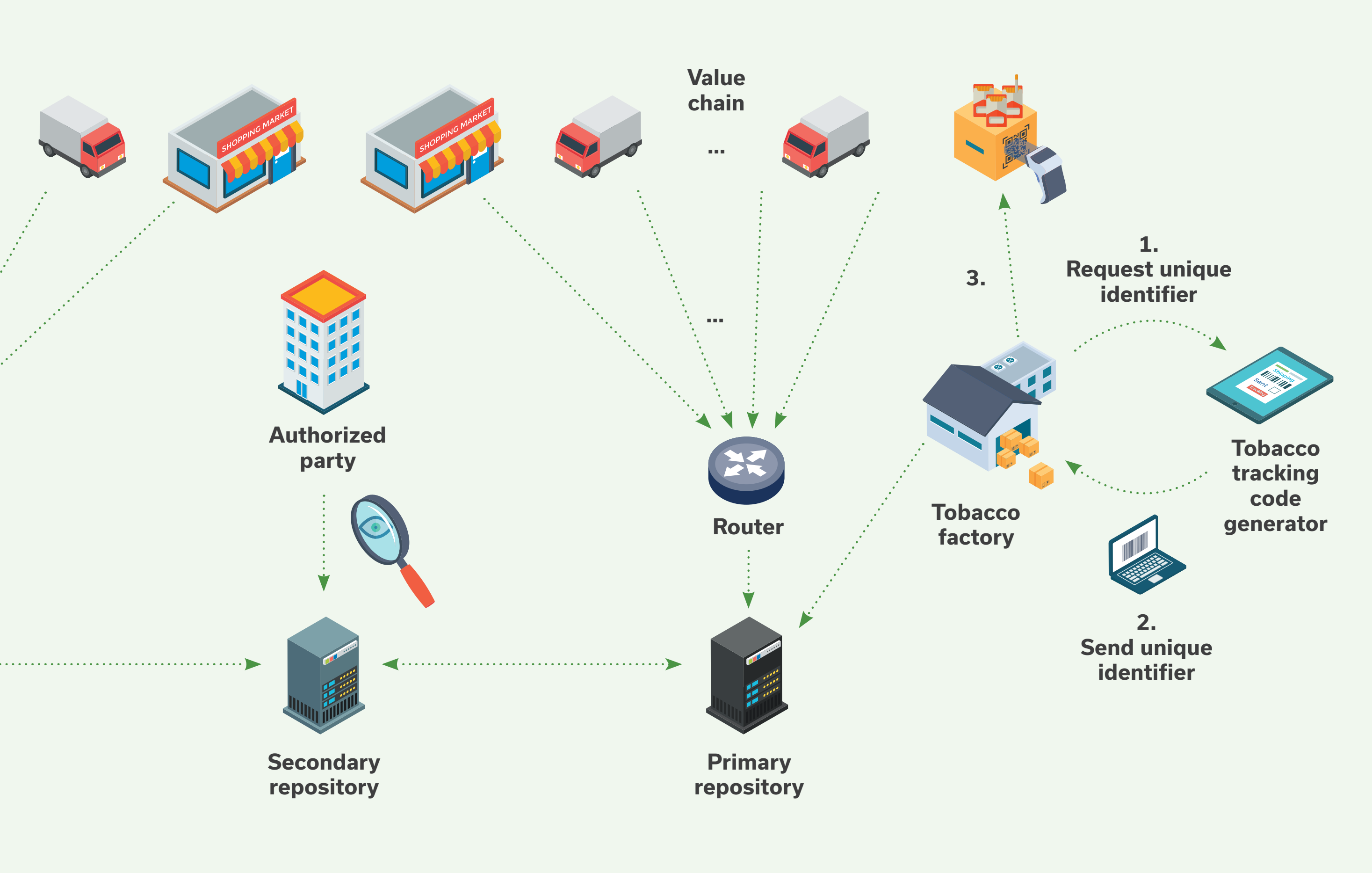

Value chain
...
1. Request unique identifier
3.
...
Tobacco tracking code generator
Tobacco factory
Router
2. Send unique identifier
Primary repository

Figure 2.1: Schematic overview of the EU TPD setup which consists of primary data repositories, a secondary repository, and a routing service.

Another important article of the FCTC Protocol is Article 9 ("Record-keeping"):

> **Each Party shall require, as appropriate, that all natural and legal persons engaged in the supply chain of tobacco, tobacco products and manufacturing equipment maintain complete and accurate records of all relevant transactions. Such records must allow for the full accountability of materials used in the production of their tobacco products.**

This article codifies that all natural and legal persons involved in the supply chain in any capacity must keep and submit records of all relevant transactions. This significantly enlarges the attack surface of a T&T system given that a potentially huge



number of entities need to interact with the system, which leads to a magnitude of security and privacy challenges that will be outlined in Chapter 3.

2.3. EU TPD AND REGULATIONS IN GERMANY

The European Union (EU), as a signatory to the FCTC Protocol, has incorporated the principles and measures of the Protocol into the *Tobacco Products Directive* (EU TPD, 2014/40/EU[8]). In line with the Protocol, the directive places limits on the sale and merchandising of tobacco and tobacco-related products in the EU and also introduces EU-wide tracking and tracing to prevent illicit trade of tobacco products. The directive entered into force in April 2014 and became applicable in the EU Member States in May 2016. Note that this was well ahead of the FCTC Protocol itself, which entered into force in September 2018. Figure 2.1 provides a high-level overview of the individual building blocks of the TPD system and the data flows. Similar to the FCTC Protocol, the TPD also regulated that a T&T system must be established within five years (i.e., until May 2019). Beyond the directive, the European Commission (EC) has adopted implementing legislation that lays down more detailed technical rules, an implementation plan, and an additional act to establish technical standards for the EU T&T system and security features [2]. The Commission Implementing Regulation (EU) 2018/574 [9] provides more technical details and guidelines on how such a system should be implemented. In the context of this study, especially Article 24 is relevant which regulates the different components of the repositories system:

Primary data repositories: This kind of repository is established to store any kind of information relating to tobacco products of individual manufacturers and importers. Each primary repository shall exclusively host information that relates to the tobacco products of the manufacturer or importer who contracted the repository. [9, Article 26]

Secondary data repository: A secondary repository is established which contains a copy of all data stored in the primary repositories system. Further requirements which need to be fulfilled by the secondary repository are specified in Article 27f of the Commission Implementing Regulation (EU) 2018/574 [9]. The EC directly appoints the provider of the secondary repository.

Router: A routing service is set up and managed by the provider of the secondary repository system to enable data exchange between the primary and secondary repositories.

Furthermore, Article 24 (2) states that "The sub-systems referred to in paragraph 1 shall be fully interoperable with one another, irrespective of the service provider used." [9] This is important to enable the interoperability of the various system components. The Commission Delegated Regulation (EU) 2018/573 specifies key elements of data storage contracts to be concluded as part of the T&T system for tobacco products. Finally, the Commission Implementing Decision (EU) 2018/576 provides technical standards for (physical) security features applied to tobacco products.

The EU was one of the first entities to introduce a T&T system for tobacco products. Since May 2019, tracking and tracing information for both production and logistics has to be collected and the data is stored in a data repository. Furthermore, an information exchange system between the 27 EU Member States has been established. The system guarantees comprehensive traceability of the entire supply chain, from production to the first retailer. For almost two years, the system is in use and valuable lessons can be learned from the experience in the EU – both as an overall T&T system but also on the level of individual states – that should be taken into account when discussing how the Protocol regulation should be implemented in practice. This will minimize potential risks and proven, successful characteristics can be adopted for a global T&T ecosystem.

The underlying design goal of the EU TPD system is to ensure that all kinds of tobacco products manufactured or circulating within the EU can be tracked and traced, even if individual Member States decide to implement their own method. This approach is based on the insight that the EU is an association of individual states and hence certain independence needs to be ensured. From a security and privacy point of view, the TPD approach has many advantages, as will be discussed in Chapter 3.

To implement the TPD T&T system, the European Commission and 27 EU Member States are collaborating with Dentsu Tracking to design and operate the technical solution for supply chain control across the European tobacco industry, in compliance with the WHO FCTC Protocol (see a press release by Dentsu Tracking for more details [1]). As of March 2021, the system has already tracked more than 53 billion pack level unique identifiers at more than 810,000 economic operators and 1,5 million facilities across 27 EU Member States [1].

Differences between EU TPD and FCTC Protocol

The most important difference between the EU TPD and the FCTC Protocol is that the FCTC Protocol foresees creating a framework for data exchange between existing national or regional T&T systems via the GISFP, whereas the EU TPD foresees setting up a regional T&T systems covering all EU member states. There is a lot of discussion on how FCTC § 8.12 and 8.13 should be interpreted. Some sources, mostly from Tobacco Control NGO's, interpret this as a blanket ban from any interaction between public authorities and economic operators from the tobacco sector. The EU Commission's implementation, validated by the FCTC Secretariat as FCTC compliant, has concentrated on keeping the essential functions strictly reserved to the public authorities (i.e., issuing of codes, appointment of the central database provider, access to the data), while ensuring that all necessary safeguards are put in place to ensure that Parties keep complete control over the rest of the implementation of the T&T system (i.e., independent audits, independent providers of key components, and other control mechanisms).

As noted above, the technical implementation of the FCTC Protocol, in particular the GISFP, has not yet been clarified and the COVID-19 pandemic induces further delays. It will be critical in implementation to plan realistically for deadlines and allow sufficient time for testing. Until we have a global T&T setup with easy, secure information sharing worldwide that effectively supports the fight against illicit tobacco trade, there is still a challenge for all stakeholders – those who already have a system in place and those who are about to roll it out.

Regulatory Background in Germany

In Germany, the TPD is codified via the *Tabakerzeugnisgesetz* (TabakerzG), which regulates – among other aspects – ingredients, emission values, and information requirements of tobacco and related products. Further details on the application of the law are available in the *Tabakerzeugnisverordnung* (TabErzV). For the context of this study, Subsection 4 (§§19 – 23) and especially Article 20 of TabakerzV are important given that they regulate the requirements for a T&T system in Germany. §20 (1) TabakerzV states:

> "*Manufacturers of tobacco products are required to provide economic operators with the equipment necessary to record the information referred to in Articles 32 and 33 of the Commission Implementing Regulation (EU) 2018/574. The equipment shall be capable of electronically reading and transmitting the captured information to the repository system referred to in Article 24 of the Commission Implementing Regulation (EU) 2018/574.*"

2.4 OTHER REGULATORY FRAMEWORKS

Besides the EU TPD, there are several national systems for T&T systems of tobacco products that will be briefly presented in the following. This description is meant to illustrate the wide variety of goals and technical approaches used in different parts of the world, which imply a lot of integration challenges.

United Arab Emirates (UAE) and Saudi Arabia

The T&T system of the UAE focuses on the fight against smuggling, especially in free trade zones, and on the monitoring of tax payments. As a result, the most important feature is the secure and unambiguous identification of tobacco products. Saudi Arabia uses a system with similar requirements.

Russia

Russia has not yet ratified the FCTC Protocol but has already established its own multi-product T&T system covering tobacco products, pharmaceutical products, and several other consumer goods. Given that this T&T system was developed not only for tobacco products but for a wide range of products, its scope of application goes beyond the obligations of the Protocol. Generally speaking, manufacturers are responsible for generating a unique tracking identifier, but they must integrate a unique code generated and approved by the state authorities into the identifier, so there is close control. The products are tracked and reported up to the last point in the supply chain: the last scan takes place at the time of purchase by the end-user, which implies a longer tracing chain compared to the TPD system.

Pakistan

In March 2021, Pakistan announced that it had signed a licensing agreement with an industry consortium to establish a T&T system for tobacco products, cement, sugar, and fertilizer. The system is expected to track and trace approximately 6.5 billion consumer products per year, which will significantly reduce and eliminate illicit trade.

The required implementation guidelines for the Protocol should ensure that the global T&T ecosystem does not exclude the multitude of systems already established or in planning (e.g., EU, Saudi Arabia, etc.). The compatibility of existing national systems (e.g., UAE or Russia) with forthcoming Protocol specifications will certainly influence whether these states will join the agreement, which is also a crucial aspect that needs to be considered.

CHALLENGES AND RISKS

3.1 OVERVIEW

3.2 DATA SECURITY CHALLENGES AND RISKS

3.3 DATA PRIVACY CHALLENGES AND RISKS

3.4 OTHER CHALLENGES AND RISKS

3

3.1. OVERVIEW

Security and privacy are critical factors for developing and operating a trustworthy T&T system, and both aspects need to be considered already during the design phase ("security and privacy by design"). In the following, we focus on the security and privacy challenges of T&T systems for tobacco products, with a specific focus on the risks associated with the deployment options for the Global Information-Sharing Focal Point (GISFP), which will be located at the Convention Secretariat of the WHO Framework Convention on Tobacco Control. Furthermore, we will also discuss general challenges and potential attacks against the full infrastructure, including the individual T&T systems.

We emphasize that a decentralized, message broker-based approach to design and implement the GISFP (as envisioned by the FCTC Protocol) is appealing given that it offers several advantages from a data security and privacy perspective. Nevertheless, we want to point out that the GISFP is an attractive target for attackers and a data breach cannot be excluded in practice, with all associated implications such as fines, settlements, and loss of reputation. Hence this system and all of its components need to be carefully designed, implemented, and tested to reduce risk.

Awarding the contract for development and operation of the information exchange mechanism (GISFP) opens the possibility that the system will be implemented *outside* the EU. This could lead to a situation where a future core capability and expertise in supply chain security is not available in Europe anymore, although the EU is already successfully operating a T&T system for almost two years within the TPD.

In addition, this has important implications for the strict EU data protection requirements: In the past years, Europe has played a leading role in improving privacy. Most importantly, the European Union's *General Data Protection Regulation* (Regulation EU 2016 /679; GDPR) has achieved prominent status. First, it establishes clear rules on personal data processing. Second, it expands the scope extraterritorially to all actors who are outside the EU but offer goods or services to persons in the EU or monitor their behavior (cf. Article 3(2) GDPR). Note that the GDPR does not directly apply to the GISFP, as Switzerland is not a member of the EU or the European Economic Area (EEA).

Attacker model

Before discussing the challenges and risks, we need to clarify the attacker model – against which kind of attacks do we need to protect the T&T system and what capabilities does a typical adversary have?

The 2019 Illicit Trade Report of the World Customs Organization (WCO) [14] provides some insights into this area; the report summarizes 26,285 cases comprised of 32,426 seizures of smuggled products, of which 83.8% involved tobacco products (22,045 cases). This number alone illustrates the sheer size of the illicit trade in this area. As an example, the report describes a case where one of the biggest illegal cigarette factories was dismantled in Hungary in 2019: six million cigarettes and enough tobacco for producing a further 21 million counterfeit, untaxed cigarettes were found by the Hungarian National Tax and Customs Administration. In 2018 and 2019, six illegal tobacco factories and related warehouses were dismantled in Spain, Greece, Belgium, Italy, the Czech Republic, and Slovakia. Altogether, 109 persons were arrested during these operations.

The report also indicates links between the illicit tobacco trade and organized crime groups, who are especially attracted by high potential profits. According to the WCO report, "Numerous studies from around the world link the counterfeiting industry to economic terrorism and the financing of terrorism as part of the attempts of terrorists and criminal organizations to fund their activities." [14, page 67]

As a result, we need to consider a potent adversary for a T&T system: organized crime groups, terrorist and other large-scale adversaries are a particular threat because they are exceptionally determined, very well resourced, and extraordinarily capable in terms of their technical expertise. Furthermore, they have the organizational structure to perform long-term, systematic attacks. An adversary can have several incentives to attack the GISFP directly or the individual T&T system, as illustrated via the following examples:

- Eavesdropping on all communication between the GISFP and individual repositories to learn about all requests (e.g., to deduce information about ongoing investigations).
- Unauthorized access to tracking codes in order to supply illegally manufactured products to the legal supply chain (e.g., by adding stolen tracking codes to counterfeit products).
- Concealment of routes through the supply chain when legal products are diverted from the legal distribution system (e.g., by deleting or modifying information in the repositories).

Beyond organized crime, another potential kind of adversaries are *hacktivists*, i.e., people who want to somehow harm the (tobacco) industry, for example by a reputation loss resulting from a successful compromise of one of the T&T system components or harassment campaigns. Finally, *industrial espionage* plays a major role in practice and should be considered as well. We will discuss different kinds of attacks throughout this chapter. In summary, we argue that security and privacy play a vital role and need to be considered with the highest priority.

3.2. DATA SECURITY CHALLENGES AND RISKS

In the following, we first present several key attributes to obtain security, and for each of them, we discuss how it influences the design of a T&T system for tobacco products.

- **Confidentiality** describes the absence of unauthorized disclosure of information, i.e., only authorized parties are allowed to access data records. All data processed and stored by a T&T system need to be treated confidentially, given that sensitive information about the production and distribution of tobacco products is handled (e.g., the information should neither be public nor in the hands of adversaries, competitors, or other parties). This is especially true for the GISFP, it must not be possible for an adversary to eavesdrop on the communication.

  Confidentiality can be enforced by rigorous control of who can access which information in what way (e.g., read or write data to a data repository). For example, if an attacker obtains access to tracking codes, this information could be misused to turn counterfeit products into seemingly legal products. In addition, confidentiality can be enforced via cryptographic protocols, e.g., by encrypting all information at rest. In case an adversary attains unauthorized access to a data repository, he only obtains encrypted data records and cannot derive meaningful information.

- **Integrity** requires the absence of unauthorized system alterations (e.g., changing, adding, or deleting records within a data repository). For smuggling or illicit trade, an attacker might want to delete records in the T&T system to destroy evidence of an organized crime, hence the integrity of all processed data is a crucial security goal.

  Integrity can be enforced by rigorous control of who can access which resources in what way; a strict access control policy is a key requirement and only authorized parties are allowed to communicate with the GISFP. Furthermore, cryptographic primitives such as digital signatures or message authentication codes can support integrity.

- **Availability** describes the readiness for correct service of the T&T system, i.e., the system needs to provide the expected service whenever an entity wants to interact with it. In other words, availability describes the prevention of unauthorized withholding of information or resources. In practice, enforcing availability is not trivial and is one of the most severe computer security problems. So-called Denial-of-Service

(DoS) attacks are still a significant problem in practice. Proper mechanisms such as load balancing, on-demand scaling, and similar mechanisms help improve availability.

In essence, security is the composite of **C**onfidentiality, **I**ntegrity, and **A**vailability – the so-called "CIA principle" of data security. Several closely related attributes characterize other security requirements:

- **Authenticity** describes the integrity of a message's content and origin, a repository should process only authentic information. Authenticity can imply other information, such as the time of sending a data record to a repository or other meta-information that is valuable for tracking and tracing.

- **Accountability** requires the availability and integrity of the identity of the entity who performed an operation. This information is essential to ensure the traceability of interaction within the T&T system; potential breaches can be detected and analyzed more efficiently. This requirement ensures that all changes to the repository can be checked, and an adversary cannot modify or delete entries.

- **Nonrepudiability** specifies the availability and integrity of the identity of the sender of a data record (nonrepudiation of the origin) or the receiver (nonrepudiation of reception). Nonrepudiability ensures proper handling of all data records processed by a system. An attacker could try to smuggle forged tracking codes into a repository, which would turn counterfeit products into seemingly legal ones.

A closely related concept is *dependability,* the ability of a system to avoid service failures that are more frequent or more severe than is acceptable. Dependability is based on the insight from practice that a system can (and usually does!) fail – we are not able to build complex systems that do not fail at all, an element of risk always remains. A prominent and often cited example in this context is the US space program: despite tremendous efforts and resources, the Challenger (1986) and Columbia (2003) disasters showed that the remaining risk cannot be fully resolved.

For software-based systems, the unavoidable presence and occurrence of faults can also be quantified with the concept of *defect density*, e.g., the number of defects per 10,000 lines of software code is a metric for software quality. A defect density below 1.0 is considered well-maintained code. However, complex systems typically consist of millions of lines of code (e.g., Mozilla Firefox consists of about 21 million lines of code, while the Microsoft Windows operating system has roughly 50 million lines of code), and hence there are likely many undetected vulnerabilities in such systems.

As a result, systems are never totally available, reliable, safe, or secure, and an element of risk remains. In practice, there are three concepts to reduce this risk:

- **Fault prevention** such that we can prevent the occurrence or introduction of faults.

- **Fault tolerance** which means to avoid service failures in the presence of faults.

- **Fault removal** which includes all mechanisms to reduce the number and severity of faults.

For a T&T system, the implication is that we need to anticipate that the system will sometimes fail and an adversary might be able to successfully compromise the system (e.g., observe the communication between individual repositories and the GISFP, modify or add records in a repository, etc.).

In the design and implementation phase, data security muste hence play an essential role such that the associated risk can be minimized. We want to emphasize that the decentralized and redundant approach followed by the TPD and envisioned by the FCTC Protocol has many appealing properties.

Having discussed all these challenges and risks, one of the main question we address in Chapter 4 is: *Which mechanisms can we use to design a T&T system that achieves the goals discussed above?* As we will see, this is a complex task given that a potentially powerful attacker wants to actively violate these attributes.

Data Breaches in the Past

To better understand what implications a successful attack can have in practice, we examine several case studies of data breaches observed in the past years. These case studies serve as an illustration to better understand the risks and challenges of a T&T system:

- **Marriot International, Inc.**: In November 2018, Marriot International, an international hospitality company, announced that attackers had stolen data records on up to 500 million customers from Starwood hotels reservation system. This incident resulted from a multi-year incident: the initial breach occurred in 2014 in computer systems belonging to Starwood hotels. When Marriot acquired Starwood in 2016, the incident was not detected, and the attackers could continue their attack. Only in September 2018, the compromise was discovered. Personal information such as contact information, passport number, birth dates, travel information, and similar data was stolen. It remains unclear if the attackers could access the (presumably encrypted) credit card numbers and expiration dates.

- **Mitsubishi Electric Corp:** In May 2020, Japan has launched an investigation into the potential exposure of confidential missile data as part of a successful attack on Mitsubishi in June 2019. As part of the attack, about 200 MB of files, mostly business documents, were stolen.

- **Equifax Inc.:** Equifax, one of the largest consumer credit reporting agencies in the US, announced in September 2017 that attackers were able to steal about 148 million data records. The attack began in May 2017 and was likely the result of an unpatched system the attackers could compromise. In addition, an inadequate network setup enabled the attackers' lateral movement such that they could compromise the actual database to steal personal information such as contact information, Social Security numbers, birth dates, and even credit card numbers.

- **German Bundestag and Federal Agencies:** There have been repeated attacks on the German Bundestag and federal agencies. The most serious attack to date probably took place from the beginning of 2015 and was discovered in May 2015. Threat actors compromised the network of the German parliament for the purpose of espionage. In late 2016, attackers penetrated the federal government's data network by first infecting one of the connected computers with malicious software and then compromising other computers within the network. From computers of the German Foreign Office, the attackers captured documents related to the Brexit negotiations and the diplomatic relationship to the Ukraine.

- **Yahoo!:** Yahoo, an American web services provider, announced several successful attacks against its network in the past years, and the company estimates that all of its about three billion user accounts were compromised. Again, the attackers could compromise personal information, including dates of birth, email addresses and passwords, and security questions and answers.

- **Intel:** In August 2020, the US chipmaker announced that it started to investigate a leak of intellectual property from its partner and customer resource center. About 20 GB of proprietary data and source code from the company was published in an online forum by an unknown third party, likely resulting from a successful data breach.

- **World Health Organization:** According to several media reports, top officials at the World Health Organization (WHO) were being targeted by attackers in March 2020 as they work on the global response to the COVID-19 pandemic. In April 2020, lists of email addresses and passwords allegedly from the WHO and

National Institute of Health (NIH) were published online. The motives of the attackers remained unclear, the incident might be related to an earlier data breach in these organizations.

- **Tu Ora Compass Health:** In October 2019, the NGO Tu Ora Compass Health, a primary health organization based in New Zealand that provides essential healthcare, has revealed a data breach resulting in the potential exposure of sensitive medical information belonging to one million individuals.

Implications and Settlements
Data security incidents can lead to many types of implications; the following examples illustrate a few cases of data breach fines, penalties, and settlements:

- **Equifax Inc.:** As noted above, the company had failed to patch a critical vulnerability for several months, did not correctly monitor for intruders, and failed to inform the victims of the breach for weeks after it was discovered. As a result, the credit reporting agency agreed to pay $575 million in a settlement with the Federal Trade Commission (FTC), the Consumer Financial Protection Bureau (CFPB), and 50 US states due to the "company's failure to take reasonable steps to secure its network led to a data breach in 2017 that affected approximately 147 million people".[3]

- **Yahoo!:** The data breaches had an immediate impact on the company, which was in the process of being acquired by Verizon in 2016. After the data breach was announced, Verizon lowered its offer by $350 million to $4.48 billion. Furthermore, in April 2018, the US Securities and Exchange Commission (SEC) fined the company $35 million for failing to disclose the breach adequately.

- **Morgan Stanley:** In October 2020, the US Office of the Comptroller of the Currency (OCC) fined the American bank $60 million for failing to properly decommission hardware containing wealth management business data from two data centers in 2016. [7] In 2019, Morgan Stanley experienced similar vendor management control deficiencies in connection with decommissioning other network devices that also stored customer data. This example illustrates that security needs to be considered along the whole life cycle of a system.

- **Premera Blue Cross and UCLA Health:** In May 2015, Premera Blue Cross, a not-for-profit health insurance company based in the United States, experienced a security breach, possibly leaking the private information of 11 million of its members. The attackers may have gotten access to the claims data of Premera's customers that includes clinical information, banking account numbers, social security numbers, birth dates and more private information. As part of the settlement, Premera has agreed to pay $74 million to resolve the litigation; $42 million to improve data security and $32 million to persons affected from the data breach.

  In a similar case, UCLA Health, an academic medical center which comprises a number of hospitals and an extensive primary care network in the Los Angeles region, announced in May 2015 a data breach that affected 4.5 million patients. In March 2019, a $7.5 million settlement was reached; the settlement provides $2 million for unreimbursed loss and preventative measures claims, while the remaining $5.5 million will provide a cybersecurity enhancement fund.

- **British Airways and 1&1 Telecom:** In October 2020, the British Information Commissioner's Office (ICO) fined British Airways £20m for failing to protect the personal and financial details of more than 400,000 of its customers [6]. An ICO investigation found that the airline was processing a significant amount of personal data without adequate security measures in place. This failure broke the General Data Protection Regulation (GDPR). Subsequently, British Airways was the subject of a successful attack during 2018, which the company did not detect for more than two months. In a similar case, a German court ruled in November 2020 that the German telecommunications provider 1&1 Telecom needs to pay a fine of 900,000 € in relation to a GDPR breach.

3.3 DATA PRIVACY CHALLENGES AND RISK

Another critical aspect that was not discussed in detail so far is privacy, i.e., confidentiality with respect to personal data. On the one hand, this can be "information" such as data records within a data repository. On the other hand, this can be "meta-information" about an interaction with the T&T system (e.g., the identity of a user who performed a particular operation, sent a specific data record, timestamp of the operation, etc.). Again, there are specific key attributes from a data privacy perspective:

- **Anonymity** describes the confidentiality of a person's identity (for instance, who invoked a specific operation). An alternative and broader definition is the state of being not identifiable within a set of subjects (the so-called *anonymity set*).

- **Unlinkability** requires that different transactions/ activities are not linkable to each other.

- **Unobservability** specifies that the state of items of interest (e.g., subjects, data records, or events) are indistinguishable from any item (of the same type) at all.

The fundamental and human right to privacy can be found in various international and national legal sources. The *Universal Declaration of Human Rights* states in Article 12 that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation."

In the face of progressive and expanding data processing by private and state actors, informational privacy has become the focus of national and international law. The *Charter of Fundamental Rights* of the European Union (2010/C 83/02) includes in Article 8 the right to the protection of personal data – more specific than any other legal framework in the world.

As mentioned earlier, Europe has been a global leader in improving data protection in recent years. The General Data Protection Regulation (GDPR) was adopted in April 2016 and became enforceable on May 25, 2018. The GDPR establishes – albeit not consistently precise and comprehensive – rules on personal data processing. Furthermore, it expands the scope extraterritorially to all actors who are outside the EU but offer goods or services to persons in the EU or monitor their behavior (cf. Article 3(2) GDPR).

Other privacy laws such as California's *Consumer Privacy Act* (CCPA) or Brazil's *Lei Geral de Proteção de Dados Pessoais* (LPDP) have several striking similarities to the GDPR. Purposeful data collection and compliant use contribute to transparency, legal certainty, and predictability. GDPR's principles aim to protect subjects by imposing restrictions on using their data by data controllers and reinforcing the processing's adequacy.

From the author's perspective, providers of primary repositories and the provider of the secondary repository are data processors within the definition of the GDPR, given that they will likely process personal data about the users interacting with the repositories. Hence the GDPR has many implications for a (global) T&T system, e.g., related to transfers of personal data into other jurisdictions or contracting structures. Note that according to Article 8 of the FCTC Protocol, "a global information-sharing focal point [will be] located at the Convention Secretariat of the WHO Framework Convention on Tobacco Control," which implies that the GISFP will be deployed in Geneva and Swiss regulations apply.

However, the GDPR is directly relevant to *any* type of data processing carried out by companies based in the EU and companies based in Switzerland when they conduct business activities within the European Union and have access to personal data of their EU customers and suppliers.

In the following, we discuss some of the implications, but this study does not represent a comprehensive treatment of this complex topic.

According to Article 44 of the GDPR, any transfer of personal data that is undergoing processing or is intended for processing after transfer to a third country or to an international organization needs to comply with the legislation's rules. Pursuant to Article 45 (1), personal data may only be transferred to a third country or an international organization if the European Commission has issued a so-called *adequacy decision*, which confirms that the respective entity has an adequate level of data protection. Each entity that wants to process data hence needs to guarantee sufficient protection of data.

Furthermore, GDPR introduces several new regulations such as the *Right of access by the data subject* (Article 15), the *Right to erasure* ("right to be forgotten", Article 17), and the *Right to data portability* (Article 20). In Article 32, the security of processing is regulated, such as

1. the pseudonymisation and encryption of personal data,
2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, and
3. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

The implications of GDPR on a global T&T ecosystem and especially the GISFP need to be examined in detail before a system can actually be deployed in practice. Given the complex nature of the system, many aspects need to be carefully analyzed by data privacy experts and additional expert opinions should be prepared. The operational experience of the TPD implementation operated by *Dentsu Tracking* can serve as valuable input for such a discussion.

A related framework that is worth mentioning in this context is the *EU–US Privacy Shield,* which was developed to govern the transatlantic exchanges of personal data for commercial purposes between the EU and the US. It is a replacement for the *International Safe Harbor Privacy Principles*, which were declared invalid by the European Court of Justice in October 2015. In July 2020, the European Court of Justice also declared the EU–US Privacy Shield invalid and at the time of writing it remains unclear how the new regulations for transatlantic exchanges of personal data will be designed.

The future legal framework for transatlantic data exchange must be taken into account in the design of the T&T system and corresponding legislative processes should be closely monitored.

In summary, we advise that the legal requirements of the GDPR need to be taken into account and the underlying principle of "Privacy by Design, Privacy by Default" must be respected when designing a global T&T system. *Privacy by design* means that both software and hardware are designed and developed from the ground up so that relevant data protection measures are taken into account from the outset. The system design is oriented to data protection requirements in all areas. *Privacy by default* is primarily intended to protect users who are less tech-savvy. This means that software, hardware and services must be preset to be privacy-friendly when deployed.

Europe plays a leading role in privacy in the world and we should not give up the critical privacy requirements and our core values when designing FCTC's global T&T system and the global information-sharing focal point (GISFP). This is a challenging situation given that many entities in different legal restrictions are involved, but the experience from operating the TPD system in Europe for almost two years is valuable and should guide the development of a global system.

3.4 OTHER CHALLENGES AND RISKS

Beyond the data security and data privacy challenges and risks of a T&T system discussed above, several other aspects are worth mentioning. The broader context is the whole topic of supply chain (cyber) security: how can we improve the security aspects of the software and networks involved in the data processing in the face of threats such as data theft, malicious software, advanced persistent threats (APTs), and similar opponents? Basic security best practices such as disconnecting critical machines from the Internet, proper network segmentation, patch management, incident response plans that includes both incident detection as well as incident response, disaster recovery plans, data breach management, and related aspects must be considered.

A sensitive topic is the question of who actually controls the T&T system. Within the framework of the TPD, the EU already has a T&T system in place that successfully processed billions of events across 27 EU member states. We argue that the EU TPD system should serve as a role model for implementing the FCTC Protocol, mostly since clear rules and guidelines for implementing the Protocol are still missing and the postponed second MOP meeting leads to further delays.

In general, an implementation of a global T&T system until September 2023 seems to be too early, and it might be better to move the starting date by at least one year to allow better testing of the whole system. Postponing the start date is especially important because the interoperability of different system components is a complex challenge that likely cannot be solved without proper testing; hence enough time must be reserved for this task.

4

KEY RECOMMENDATIONS

4.1 DISTRIBUTED APPROACH

4.2 QUERY-BASED APPROACH / MESSAGE BROKER

4.3 CLEAR SPECIFICATIONS

4.4 RAMP-UP PHASE

4.5 MARKET CONSIDERATIONS

4.6 BLOCKCHAIN AND SMART CONTRACTS

In the following, we outline several recommendations and potential next steps for the implementation of the FCTC Protocol. These recommendations are based on the challenges and risks related to computer security and privacy outlined in the previous chapter. Furthermore, we take a broader view of the topic of T&T systems and discuss feasible options to implement and deploy such a system in a secure and trustworthy way.

4.1 DISTRIBUTED APPROACH

The Protocol provides for a global T&T system consisting of national and/or regional T&T systems and a global information-sharing focal point (GISFP) located at the Convention Secretariat of the WHO Framework Convention on Tobacco Control (Article 8 (1) of the FCTC Protocol). From a security and privacy point of view, in particular, the GISFP is considered critical because it plays a central and important role in the system.

If the GISFP would hypothetically be implemented as a central database, it would constitute an attractive target for cyber-attacks and the availability of the system could not be guaranteed. Organized crime, terrorist, hacktivists and other powerful adversaries have the interest to sabotage such a system. Hence security and privacy need to be considered in detail and from the design phase onwards.

The case studies of successful data breaches discussed in the previous chapter illustrate that complex computer systems with (business-) critical, important information can potentially be compromised – the more sensitive the data, the more interesting it gets from an attacker's point of view. And the GISFP clearly falls into this category, given that it would allow a global view of all tobacco-related activities from all parties involved in this market.

Furthermore, setting up such a global information exchange mechanism is a very challenging task given that many different (financial and legal) interests are involved, and many other jurisdictions need to be considered. Finally, scaling a system for worldwide tracking of all tobacco-related activities would be a challenging engineering task in itself.

The European Union's implementation of the TPD has several appealing properties, especially related to several data repositories and clear interfaces for routing services. An analogy is the Internet: The Internet consists of interconnected computer networks – each of them being managed individually – that use specific protocols such as TCP/IP to communicate between networks and devices. A device can send a request to a server and receive relevant information as a response. The Internet was designed to withstand a nuclear attack and achieves high dependability in practice.

The TPD implementation used in the EU follows a similar philosophy. Different kinds of security and privacy attributes can be enforced, and access control can be implemented more rigorously. The Protocol implementation of a T&T system should follow a similar paradigm.

4.2 QUERY-BASED APPROACH / MESSAGE BROKER

A fundamental property for implementing the Protocol that should be followed is to keep the GISFP as simple as possible; only then the security of the system can be enforced. This argument follows the KISS principle (an acronym for keep it simple, stupid), which constitutes a design principle noted by the US Navy in 1960.

Simplicity can be achieved by implementing the GISFP as a query-based system that links the national and/or regional T&T systems together. For an inquiry, a party sends a request to the GISFP, which is then routed to the relevant T&T system where the query is processed. The answer is then sent back to the requesting party, either via the GISFP (which can potentially lead to a bottleneck/single point of failure) or directly to the requesting party without the involvement of the GISFP. The advantages and disadvantages of both approaches should be examined in detail.

Such a message broker design loosely follows the design principle of many kinds of distributed systems, and we have a good understanding of the resilience of such systems. We strongly recommend following such an approach because it minimizes risks from a security point of view.

4.3 CLEAR SPECIFICATIONS

A query-based approach also has some challenges that need to be addressed. First, clear interface and protocol definitions are necessary to ensure the operability of different implementations of existing national and/or regional T&T systems. Second, the maintainability of the overall system as well as the individual systems must be ensured (e.g., in case of a release change of the communication protocol between the individual repositories). Again, clear specifications must be defined to ensure interoperability.

In practice, a range of national or regional T&T systems are already deployed or are in the process of being set up in the near future. While these systems follow the same high-level goal, they nonetheless significantly differ in the design or technical implementation. Clear interfaces (especially related to the GISFP) will make sure that an information exchange platform will be created without prescribing one model or another.

Another essential requirement is a clear access control policy: only authorized users should be able to access the data given that potentially sensitive information passes through the GISFP. This policy needs to be strictly developed, implemented, and enforced to ensure that confidentiality requirements are followed. Note that access control entails the management of users and access rights, and clear rules need to be defined as well.

4.4 RAMP-UP PHASE

As noted earlier, a start date of September 25, 2023, is seen as very ambitious; the delay introduced due to the COVID-19 pandemic and the postponed second MOP meeting already lead to a postponement in the overall setup process. Enough time and resources must be allocated for proper testing of a global T&T system, as these requirements must not be underestimated.

Given the challenging timing, a viable option could be to implement a highly simplified but functional approach based on the absolute basic requirements of the Protocol and then scale this system in the future. In a pilot phase, a manual data processing might be a viable option before then gradually more automated methods will be added to the system.

As the complexity and the interoperability of the system steadily increase, so does the need for an effective data security and privacy architecture. We strongly recommend that security and privacy must be ensured from the very beginning (“security and privacy by design“), and both aspects need to be considered in step with the growing complexity of the system. A clear specification, which also evolves over time, is necessary to successfully build such a sophisticated system.

4.5 MARKET CONSIDERATIONS

From a practical point of view, it should be ensured that existing national and/or regional T&T can be interconnected to the FCTC Protocol without significant revision of their system architecture. The EU has already invested a lot of effort and resources to set up and operate the European T&T system along the TPD. And it should be possible to use the resulting system as part of the Protocol. Similarly, other countries have also started to implement their own T&T system, and these systems should also be interconnected to the overall system. Note that this has an important implication: in the future, potentially, a large number of T&T systems with data security properties of varying quality will be put into operation. We must ensure that European data is also secure in other countries such as South America or Africa; the high security and privacy requirements (such as GDPR) must be safeguarded.

A critical question that needs to be solved is the role of the GISFP administrator: who is responsible for the implementation, maintenance, further development, and control of the system? In our opinion, the recommended party is the FCTC Convention Secretariat given that the WHO governs the whole process. However, the Convention Secretariat is unlikely to undertake this task alone and would need support from an independent third party (or would have to delegate this task to a third party). This will become especially important when a critical number of requests need to be handled by the system. To protect the European interests, it is important that the third party be selected in an objective and transparent manner.

Furthermore, the EU already has almost two years of operational experience with the TPD that should be considered when deciding on the governance structure of the GISFP.

4.6 BLOCKCHAIN AND SMART CONTRACTS

Blockchain or distributed ledger technology (DLT) open up enormous potential for new and innovative applications. Trust and control (in the sense of forgery-proof documentation) are created by the technology itself, an ideal property for a T&T system. This enables applications that were previously only possible with the help of trusted intermediaries. By combining the blockchain with self-executing programs linked to precisely defined conditions – so-called *smart contracts* and second-layer applications based on them – a system is created that enables entire business processes to be handled fully automatically and autonomously directly machine-to-machine (M2M). This approach could be interesting for a T&T system to fully automate the communication and processing between the individual repositories.

The security of blockchain-based applications is of crucial importance. Previous experience with the technology has shown that small design mistakes can cause significant damage. The high complexity and the multitude of attack vectors (such as the hardware used, the underlying blockchain infrastructure, or wallet systems and second-layer applications built on top of it) pose particular challenges. The fully automated and autonomous execution of entire business processes using smart contracts also brings the security of these processes to the fore.

In order to exploit the full potential of blockchain technology, several hurdles hence need to be overcome. For many technological reservations, solutions are already available from research or are being intensively researched (for example, efficiency, scalability, secure integration of machines and sensors). The main technological challenges, and also the main criticisms that are regularly raised, are the poor scalability and the enormous energy consumption of blockchain technology. Current blockchain systems such as Bitcoin and Ethereum consume huge amounts of energy (e.g., the Bitcoin network has an energy consumption comparable to the Czech Republic), and their transaction throughput and processing speed are limited to a few transactions per second, which is orders of magnitude too low for a T&T system. However, the problems of scalability and sustainability can be addressed using off-chain technologies. This allows the large volume of transactions to be processed off the blockchain in a second-layer network, dramatically increasing the efficiency of transaction processing.

A complementary approach that is used in particular in the industrial environment is permissioned blockchains, which completely dispense with proof-of-work schemes and offer sustainable solutions for an industrial environment. Such an approach could be used within a T&T system as well.

The architecture of blockchains generally contradicts the basic data protection principle of changeability and deletion of data. There is a need to clarify how (or if) deletion must be performed to be compliant with the GDPR, in case a blockchain-based system architecture is considered.

One of the strengths of blockchain technologies is the transparency they offer. This transparency implies that all transactions carried out on a blockchain can be traced without any gaps, a key feature for T&T systems. However, this conflicts with the goal of data protection and confidentiality. In order to meet the respective data protection requirements, this contradiction must be resolved technologically (e.g., via a permissioned data exchange). For example, IBM has developed *Digital Health Pass*, a blockchain-based approach that allows individuals to store their health information and vaccine status, with full control over who can access the data. Moreover, the COVID-19 vaccine distribution can be controlled in an end-to-end fashion via a blockchain – an ideal use case for supply-chain tracking [5].

5

CONCLUSION

In this study, we have analyzed various data security and privacy requirements of a global T&T ecosystem as envisioned by the FCTC Protocol. The Protocol mandates in Article 8 (1) that an information exchange mechanisms via the GISFP has to be established by September 2023. Unfortunately, the specification of this system is not complete yet: due to the postponement of the second Meeting of the Parties, precise requirements and implementation guidelines are still missing. This is a significant concern: Only exact and comprehensive requirements that take both security and privacy into account can lead to a trustworthy system. Also, extensive testing of such a complex system is an essential requirement, and sufficient time must be allocated to this task. We encourage all parties involved to discuss in detail the planned timeline for the implementation of the system and to prepare the development and deployment steps carefully. A sensible approach could be to roll out a simple but functional system first and expand it gradually.

We explored various security and privacy challenges of a global T&T system. We argue that a powerful adversary model should be considered: organized crime groups, terrorists, and similar large-scale adversaries have an incentive to target (components of) this system, such as the national/regional T&T systems or the GISFP. These attackers are highly motivated, have excellent resources, and may have a long-term plan to gain unauthorized access to the system or manipulate the data. Besides, hacktivists and industrial espionage must also be considered; various groups may have an incentive to target the system. Data security, therefore, plays a crucial role, and the system's attack surface must be carefully examined to minimize the risk of possible attacks. To better understand these risks and challenges, we have illustrated the impact of successful data breaches through several case studies from different sectors.

Various data privacy requirements must also be taken into account. In particular, the General Data Protection Regulation (GDPR) has established clear rules on how personal data must be protected. These requirements must be considered when implementing the global T&T ecosystem: Europe plays a leading role in data protection in the world – we should not abandon critical data protection requirements and our core values when designing a global T&T system.

Orthogonal to these data security and privacy requirements is another dimension. With the Tobacco Products Directive (EU TPD), Europe is a global pioneer in this area: since May 2019, the EU has been operating a T&T system in the 27 Member States that has already successfully recorded billions of transactions. To safeguard Europe's interests, the question of which entity develops, deploys, and operates the global T&T system and especially the GISFP needs to be carefully discussed.

We provide several recommendations and next steps for implementing the Protocol:

- The envisioned approach of using a query-based approach with the GISFP as the message broker is reasonable, but data security and privacy requirements must be carefully considered.
- Clear interface and protocol definitions are necessary to ensure the interoperability of different implementations of existing T&T systems. A precise specification, which also evolves over time, is necessary to build such a sophisticated system successfully.
- The specification must ensure the maintainability of the overall system and the individual components. For example, a release change of the communication protocol must not interrupt the connectivity of individual repositories.
- Consideration should be given to a ramp-up phase where security and privacy are considered as an integral part from the beginning.
- It should be ensured that existing T&T systems can be connected to the global T&T system without significant revision of their system architecture.
- The question of who is responsible for the implementation, maintenance, further development, and control of the overall system should be clarified on time; we must ensure that European interests are taken into account.

ABOUT THIS STUDY

DISCLAIMER

This study was written by Prof. Thorsten Holz and financially supported by Philip Morris GmbH (PMG). The author is exclusively responsible for the text and the interpretations presented in this document.

CURRICULUM VITAE

Prof. Thorsten Holz is a full professor in the Faculty of Electrical Engineering and Information Technology at Ruhr-University Bochum, Germany. His research interests include technical aspects of secure systems, with a specific focus on systems security. Currently, his work concentrates on automated vulnerability detection, software security, and studying the latest attack vectors.

Prof. Holz has published more than 160 peer-reviewed articles in computer security and regularly serves on the technical program committee of the leading academic security conferences. He received the Dipl.-Inform. degree in Computer Science from RWTH Aachen, Germany (2005) and the Ph.D. degree from University of Mannheim (2009). Prior to joining Ruhr-University Bochum in 2010, he was a postdoctoral researcher in the Automation Systems Group at the Technical University of Vienna, Austria.

In 2011, Prof. Holz received the Heinz Maier-Leibnitz Prize from the German Research Foundation (DFG) and in 2014 an ERC Starting Grant. Furthermore, he is Co-Spokesperson of the Cluster of Excellence “CASA — Cyber Security in the Age of Large-Scale Adversaries” (with C. Paar and E. Kiltz).

graphical concept and layout | c.robrahn | c74 gestaltung & design | www.c74.org

BIBLIOGRAPHY

[1] Dentsu Tracking. Dentsu Tracking celebrates one year working with the EU on supply chain control solutions for tobacco (EU TPD). https://dentsutracking.com/dentsu-tracking-celebrates-one-year-working-with-the-eu-on-supply-chain-control-solutions-for-2020.

[2] European Commission. Implementing the Tobacco Products Directive (Directive 2014/40/EU). https://ec.europa.eu/health/tobacco/products/revision/implementation_en.

[3] Federal Trade Commission. Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach. https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related.

[4] Marina Foltea. Brexit and the Control of Tobacco Illicit Trade. Springer, 2020.

[5] IBM. A Groundbreaking VaccineWill Need a Groundbreaking Supply Chain. https://newsroom.ibm.com/A-Groundbreaking-Vaccine-Will-Need-a-Groundbreaking-Supply-Chain, 2020.

[6] Information Commissioner's Office. ICO fines British Airways £20m for data breach affecting more than 400,000 customers. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/,2020.

[7] Office of the Comptroller of the Currency. OCC Assesses $60Million CivilMoney Penalty AgainstMorgan Stanley. https://www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-134.html, 2020.

[8] Official Journal of the European Union. Directive 2014/40/EU of the European Parliament and of the Council. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOL_2014_127_R_0001, April 2014.

[9] Official Journal of the European Union. Commission Implementing Regulation (EU) 2018/574. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0574&from=ES, December 2017.

[10] Raffaele Rotunno, Vittorio Cesarotti, Attilio Bellman, Vito Introna, and Miriam Benedetti. Impact of Track and Trace Integration on Pharmaceutical Production Systems. International Journal of Engineering BusinessManagement, 6, 2014. doi:10.5772/58934.

[11] WHO. WHO Framework Convention on Tobacco Control. https://treaties.un.org/pages ViewDetails.aspx?src=TREATY&mtdsg_no=IX-4&chapter=9&clang=_en,May 2003.

[12] WHO. Protocol to Eliminate Illicit Trade in Tobacco Products. https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IX-4-a&chapter=9&lang=en, November 2012.

[13] World Bank Group. Confronting illicit tobacco trade—a global review of country experiences. http://pubdocs.worldbank.org/en/248361548435105081/WBG-Tobacco-IllicitTrade-UnitedKingdom.pdf, 2019.

[14] World Customs Organization (WCO). Illicit Trade Report. http://www.wcoomd.org/-/media/wco/public/global/pdf/topics/enforcement-and-compliance/activities-and-programmes/illicit-trade-report/itr_2019_en.pdf, 2019. 20