TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Anton Kolisnetsenko 242797IVCM

Analysis of E-ITS Control Coverage for MITRE ATT&CK PKI and Cryptography-Related Techniques

Master's thesis

Supervisor: Toomas Lepik

MSc

Tallinn 2025

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Anton Kolisnetsenko 242797IVCM

E-ITS turvameetmete katvuse analüüs MITRE ATT&CK PKI ja krüptograafiaga seotud tehnikate suhtes

Magistritöö

Juhendaja: Toomas Lepik

MSc

Tallinn 2025

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Anton Kolisnetšenko

20.05.2026

Tallinn 2025

Abstract

Public Key Infrastructure (PKI) and cryptographic mechanisms form a core part of modern digital security. They support secure communication, identity assurance, and software integrity across a wide range of systems. At the same time, organisations rely on security standards such as the Estonian Information Security Standard (E-ITS) to guide the implementation and management of these mechanisms.

This thesis evaluates the effectiveness of E-ITS controls from a threat-informed perspective by mapping them to relevant techniques and sub-techniques from the MITRE ATT&CK. The study focuses specifically on PKI and cryptography-related techniques and develops a structured methodology to support the mapping process.

The results show that E-ITS provides broad coverage of many cryptography-related attack techniques, particularly through controls related to access management, monitoring, and system configuration. At the same time, the findings indicate that PKI and cryptographic controls alone are not sufficient to mitigate most threats in this domain. Effective defence depends on a combination of control types, where cryptographic mechanisms are supported by identity management, detection capabilities, and operational practices.

In addition to the empirical findings, the thesis contributes a reusable methodology for mapping security standards to adversary behaviour frameworks. This approach helps bridge the gap between compliance requirements and real-world attack scenarios and can be applied to other standards beyond E-ITS.

This thesis is written in English and is 39 pages long, including 6 chapters, 0 figures and 1 table.

Lühikokkuvõte

E-ITS turvameetmete katvuse analüüs MITRE ATT&CK PKI ja krüptograafiaga seotud tehnikate suhtes

Avaliku võtme infrastruktuur (PKI) ja krüptograafilised mehhanismid moodustavad tänapäevase digitaalse turvalisuse tuuma. Need toetavad turvalist suhtlust, identiteedi tagamist ja tarkvara tervikluse säilitamist paljudes erinevates süsteemides. Samal ajal tuginevad organisatsioonid nende mehhanismide rakendamisel ja haldamisel turvastandarditele, nagu Eesti infoturbestandard (E-ITS).

Käesolev lõputöö hindab E-ITS turvameetmete tõhusust ohupõhisest vaatenurgast, kaardistades need asjakohastele MITRE ATT&CK tehnikatele ja alatehnikatele. Uuring keskendub konkreetselt PKI ja krüptograafiaga seotud tehnikatele ning arendab struktureeritud metoodika kaardistamisprotsessi toetamiseks.

Tulemused näitavad, et E-ITS katab laialdaselt paljusid krüptograafiaga seotud ründetehnikaid, eelkõige juurdepääsuhalduse, monitooringu ja süsteemikonfiguratsiooni kontrollidega. Samas viitavad leiud sellele, et üksnes PKI ja krüptograafilised meetmed ei ole piisavad enamiku selles valdkonnas esinevate ohtude leevendamiseks. Tõhus kaitse sõltub erinevate turvameetmete kombinatsioonist, kus krüptograafilisi mehhanisme toetavad identiteedihaldus, tuvastamisvõimekus ja operatiivsed praktikad.

Lisaks empiirilistele tulemustele panustab töö taaskasutatava metoodikaga, mis võimaldab kaardistada turvastandardeid ründekäitumise raamistikuga. See lähenemine aitab ületada lõhe vastavusnõuete ja tegelike ründestsenaariumide vahel ning seda saab rakendada ka teistele standarditele peale E-ITS. Kokkuvõttes näitab uuring, et ohupõhine vaatenurk võimaldab realistlikumalt hinnata turvameetmete tõhusust ning toetab vastupidavamate turbearhitektuuride kujundamist.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 39 leheküljel, 6 peatükki, 0 joonist, 1 tabelit.

List of abbreviations and terms

ACME	Automatic Certificate Management Environment
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
CA	Certificate Authority
CIS	Center for Internet Security
CISA	Cybersecurity and Infrastructure Security Agency
E-ITS	Estonian Information Security Standard
HTTPS	Hypertext Transfer Protocol Secure
MFA	Multi Factor Authentication
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastucture
SAML	Security Assertion Markup Language

Table of contents

List of tables

1 Introduction

1.1 Research Background and Motivation

Public Key Infrastructure is one of the foundations of digital trust. It supports secure communication, software integrity, and identity assurance across almost every modern service. A single compromised certificate can enable impersonation, traffic interception, or supply chain attacks. A compromised CA (Certificate Authority) can undermine trust for millions of users. Past breaches show that PKI is not an abstract security layer. It is a critical dependency with real operational risks.

At the same time, national and sector-specific security standards continue to guide how organizations should build and protect PKI. These standards define what must be done to secure keys, manage certificates, operate trust stores, and detect misuse. In Estonia, the E-ITS serves this role. It aims to align organizations around a consistent baseline of security requirements. Yet these requirements do not always reflect the way adversaries actually compromise PKI systems today.

Security teams increasingly rely on adversary-behavior frameworks such as MITRE ATT&CK to understand how attackers behave. These frameworks describe what attackers do, how they move, and which techniques they apply. They are widely used to guide detection engineering and incident response. They are less often used to evaluate control standards. This creates a growing gap between formal compliance requirements and the techniques real attackers use in the field. Organizations may comply with a standard and still remain exposed to common PKI attack paths.

There is no systematic study that examines how E-ITS controls cover adversary behavior against PKI systems. This thesis aims to address this gap. A structured mapping between E-ITS and MITRE ATT&CK can also support operational teams. It can help them interpret compliance requirements in the context of real attacks, help them prioritize detection and monitoring and highlight areas where E-ITS controls are strong and where they need reinforcement. The mapping framework developed in this

thesis can also be reused for other standards. It provides a blueprint for transforming compliance-driven security into threat-informed security.

For these reasons, the topic has both academic and practical value. It contributes to the study of threat-informed defense. It extends existing research on control-to-ATT&CK mappings. It also supports Estonia's national cybersecurity posture. The work bridges a gap that affects defenders, auditors, policy makers, and system architects by providing a clear understanding of how E-ITS addresses PKI-related adversary behavior.

1.2 Research Questions

Without a mapping between E-ITS control requirements and MITRE ATT&CK techniques, there is no reliable way to know whether compliance with a standard such as E-ITS provides meaningful protection against threats that target Public Key Infrastructure. This thesis addresses this gap by evaluating the cryptographic and PKI-related controls of E-ITS through the lens of the MITRE ATT&CK framework.

To achieve the main goal of this thesis the following research goals were formulated:

[RQ 1] How can the controls within the Eesti Infoturbestandard (E-ITS) be systematically mapped to the Public Key Infrastructure (PKI) and cryptographic techniques and sub-techniques of the MITRE ATT&CK framework to create a threat-informed compliance model?

[RQ 2] What methodological approach can be developed to systematically map national or domain-specific security standards, such as E-ITS, to adversary behavior frameworks like MITRE ATT&CK?

Together, these questions define both the practical and methodological goals of the thesis. The first question evaluates the extent of E-ITS coverage from a threat-informed perspective. The second asks how to design a mapping process that can be used again in other contexts. Both questions support a broader goal. This is the creation of a clearer link between compliance requirements and real attacker techniques, which can help organizations understand the effectiveness of their security controls and strengthen their PKI defenses.

1.3 Scope and Goal

The goal of this study is to evaluate how well the controls of the Estonian Information Security Standard (E-ITS) mitigate real-world adversarial behaviour in cryptographic and Public Key Infrastructure (PKI) domain. The study aims to produce a threat-informed view of these controls by mapping them to the techniques and sub-techniques of the MITRE ATT&CK framework. The main outcome is an assessment of defensive coverage and the identification of gaps, overlaps, or insufficiently addressed threats. A secondary outcome is a structured mapping approach that can support future evaluations of national or domain-specific security standards.

The scope of this thesis is limited to cryptographic and PKI-related techniques and sub-techniques in MITRE ATT&CK. Other domains, such as physical security, personnel security, or business continuity, remain out of scope. The study focuses on the latest available versions of E-ITS in English and MITRE ATT&CK at the time of writing. The evaluation considers the control descriptions as written. It does not assess the quality of implementation in specific organisations.

Several assumptions guide the study. First, it is assumed that the descriptions of adversarial behaviour in MITRE ATT&CK are representative of techniques relevant to Estonian organisations. Second, it is assumed that E-ITS controls are sufficiently detailed to support meaningful interpretation and mapping.

The study has limitations. Mapping between a security standard and ATT&CK requires subjective judgement, even when using a structured method. The evaluation does not quantify risk or perform technical testing. It provides a conceptual link between controls and known adversary behaviour rather than a measurement of residual risk. The results reflect the scope and assumptions of the mapping and should be interpreted with these constraints in mind.

1.4 Novelty

The novelty of this study lies in applying a threat-informed perspective to a national security standard that has not previously been analysed through the lens of adversary behaviour. While MITRE ATT&CK has been widely used to support risk assessments

and strengthen operational security programs, its use for evaluating the coverage and resilience of formal regulatory controls remains limited. No published work has mapped requirements of the Eesti Infoturbestandard (E-ITS) to the cryptographic and PKI ATT&CK techniques, nor has anyone examined how well a national standard reflects modern attacker behaviours against PKI ecosystems. The proposed mapping methodology and resulting coverage analysis therefore represent original contributions that can support the improvement of E-ITS and offer a transferable approach for assessing other national or sector-specific security frameworks.

2 Literature Review

The objective of this literature review is to find relevant literature and research across three domains: Public Key Infrastructure (PKI) security and threat landscape, existing methods of mapping security controls from control frameworks and security standards to adversarial techniques and MITRE ATT&CK use in cyber defense evaluation.

The literature review draws on academic publications from IEEE Xplore, ACM Digital Library, and ScienceDirect, complemented by authoritative grey literature from MITRE, CISA, and the Estonian Information System Authority.

2.1 PKI Security and Threat Landscape

Public Key Infrastructure (PKI) remains a foundational component of modern digital trust. It supports secure communication, certificate-based authentication, software integrity, and identity assurance across a wide range of systems. However, the reviewed literature shows that PKI security depends not only on cryptographic strength, but also on the correct operation of certificate authorities, certificate lifecycle management, private key protection, revocation mechanisms, and trust validation processes. This makes PKI a socio-technical security domain, where weaknesses often arise from implementation, governance, and operational practice rather than from the failure of cryptographic algorithms themselves.

Several studies highlight the systemic impact of Certificate Authority (CA) compromise and certificate misuse. Serrano, Hadan, and Camp analyse known PKI incidents and show that failures in the PKI ecosystem can have broad consequences because trust is delegated through certificate authorities and intermediate trust relationships [1]. Kim et al. further demonstrate that CA practices affect the security of the HTTPS ecosystem, especially when certificates are issued or managed in ways that can be abused by attackers [2]. This is particularly relevant for threat modelling, since a compromised or misused certificate can enable impersonation, traffic interception, phishing, or the

bypassing of trust-based security controls. In this sense, CAs and certificate services represent high-value targets because they do not protect only one system. They support trust across many systems.

The literature also shows that PKI-related abuse extends beyond traditional TLS certificates. Kozák et al. examine the underground trade in code-signing certificates and show that attackers may obtain certificates not only through theft, but also through purchase from legitimate certificate authorities or intermediaries [3]. This finding is important because code-signing certificates allow malicious software to appear more trustworthy to operating systems, users, and security products. Such abuse demonstrates that PKI can be exploited as part of defense evasion and software supply chain compromise, even when the cryptographic mechanisms themselves remain technically valid.

Modern automation has further changed the PKI threat landscape. Kim et al. note that automated certificate issuance, including ACME-based processes, has lowered the barrier for deploying HTTPS at scale, but has also created opportunities for large-scale abuse, such as phishing sites using valid certificates and short-lived domains [2]. This does not mean that automation is inherently harmful. Rather, it shows that improved accessibility and speed can introduce new operational risks when validation, monitoring, and revocation practices do not keep pace with attacker behaviour. PKI security therefore requires not only secure issuance, but also continuous oversight of how certificates are requested, deployed, renewed, and revoked.

Revocation infrastructure is another recurring weakness. Ivanov identifies design flaws in the Online Certificate Status Protocol (OCSP) that can be exploited to generate forged certificate status responses [4]. This illustrates a broader issue in PKI security: mechanisms intended to preserve trust after compromise may themselves become fragile points in the trust chain. If revocation checking is unreliable, delayed, or vulnerable to manipulation, compromised or improperly issued certificates may remain useful to attackers for longer than intended. Overall, the reviewed studies indicate that PKI-related threats involve certificate issuance, certificate misuse, private key compromise, code-signing abuse, and weaknesses in revocation and validation processes. These threat patterns provide the basis for analysing PKI and cryptography-related MITRE ATT&CK techniques [5] against E-ITS controls.

2.2 Control Framework Mapping

Control framework mapping refers to the structured alignment of security controls with external reference models, such as threat taxonomies, risk models, attack techniques, or security objectives. In cybersecurity governance, this process is used to translate abstract control requirements into a more operational understanding of what those controls are expected to prevent, detect, or mitigate. A growing body of work explores the value of mapping formal security controls to the MITRE ATT&CK framework [6, 7].

Control catalogues such as E-ITS, NIST SP 800-53, and CIS Controls describe desired security measures, but they do not always express them in terms of adversary behaviour. Threat-informed frameworks such as MITRE ATT&CK address this gap by describing techniques used by adversaries across different stages of an attack. Mapping controls to such techniques therefore supports coverage assessment, gap identification, and defensive prioritisation. Rahman and Williams demonstrate this logic by analysing the relationship between security controls and MITRE ATT&CK techniques, showing that control-to-technique mapping can be used to identify both areas of strong coverage and techniques with limited mitigation support [6].

The value of such mappings lies in their ability to connect compliance-oriented control catalogues with operational security concerns. A control may require access management, logging, secure configuration, or cryptographic key protection, but the defensive significance of that control becomes clearer when it is linked to concrete adversary techniques. For example, ATT&CK-based risk and defence models have been applied in information system risk assessment, industrial control system security, power system defence, SOC activities, and threat modelling [10-14]. These studies show that ATT&CK is not limited to attack description. It can also support structured reasoning about defensive measures and control priorities. Practical mapping guidance from CISA further emphasises that ATT&CK mappings should be based on observed behaviour and mitigation intent, rather than superficial keyword similarity [8]. Similarly, the CIS Controls mapping to MITRE ATT&CK illustrates how a control framework can be interpreted through adversary techniques to make defensive coverage more explicit [9].

However, control framework mapping also involves important methodological challenges. Security controls and attack techniques are usually written at different levels of abstraction [10]. ATT&CK techniques describe adversary actions, while control catalogues often describe organisational requirements, governance practices, or broad technical safeguards. As a result, mappings are rarely one-to-one. A single ATT&CK technique may require several controls for effective mitigation, such as access restriction, monitoring, configuration management, and incident response. At the same time, one control may mitigate or support mitigation for several techniques. This many-to-many structure creates interpretation challenges, especially when control wording is general and technique descriptions are detailed [12-13]. Terminology also differs between frameworks. A control may address the same security objective as an ATT&CK mitigation without using the same vocabulary. For this reason, mapping requires analysis of control intent, mitigation objective, and operational context.

These challenges mean that intermediate mappings and external references cannot be treated as automatic proof of coverage. However, ATT&CK mitigation guidance and studies linking ATT&CK to other control frameworks can still support validation by showing whether a proposed mapping is conceptually consistent with established sources. [6, 8, 9]

2.3 Threat Informed Defense

Threat-informed defense represents a shift from purely compliance-driven security toward a more adversary-oriented security posture. Traditional control frameworks define what safeguards should be implemented, but they do not always explain how those safeguards relate to specific attack behaviours. Threat-informed defense addresses this limitation by using knowledge about adversary tactics, techniques, and procedures to guide risk assessment, control prioritisation, detection engineering, and incident response. In this context, defensive measures are not evaluated only by their formal presence, but also by their relevance to realistic attack paths and attacker objectives.

MITRE ATT&CK is widely used as a structured taxonomy for applying this approach. It provides a common language for describing adversary behaviour across different stages of an attack lifecycle, including initial access, persistence, credential access, defense evasion, exfiltration, and impact. Several studies apply ATT&CK in this way

across different domains, including power systems, industrial control systems, SOC operations, threat modelling, and threat path construction [12-16]. These applications show that ATT&CK can support more systematic analysis of how attackers operate and how defenders can align controls, monitoring, and response capabilities to those behaviours.

The value of threat-informed defense is that it helps organisations move beyond generic security requirements. Instead of asking whether a control exists, organisations can ask which adversary techniques the control helps prevent, detect, or limit. This makes it possible to identify defensive gaps, prioritise controls with wider mitigation value, and improve the alignment between technical security operations and governance requirements. In SOC environments, for example, ATT&CK can help structure detection logic and incident analysis around known attacker behaviours [13]. In threat modelling, it can be combined with other frameworks such as STRIDE or the Cyber Kill Chain to describe both attack structure and defensive response [14, 15].

2.4 Analysis of Research Gaps

A research gap represents an unanswered question or unexplored area in a field of study. This review has identified a research gap that this thesis will address.

While mappings exist for more widespread security standards, such as NIST SP 800-53 [21], there is no available mapping for the E-ITS. This thesis will provide the first dedicated mapping of E-ITS security controls [17-20] to MITRE ATT&CK adversary techniques [5] related to PKI and cryptography. This mapping will offer a great direct value to organisations that decide to implement this standard.

The conducted literature review confirms the viability and value of mapping security controls to MITRE ATT&CK and shows a clear need for a focused mapping of E-ITS standard. This thesis will directly address this gap by creating a detailed PKI-centric map of E-ITS security controls to ATT&CK adversary techniques.

3 Methodology

This study follows a qualitative research design that combines document analysis, systematic mapping, validation by cross-referencing. The goal is to evaluate how controls of the E-ITS correspond to adversarial cryptographic and PKI-related techniques described in the MITRE ATT&CK framework.

3.1 Data Sources

Data collection is based on two sources. The first source is the latest publicly available English version of E-ITS. The second source is the MITRE ATT&CK knowledge base, including techniques, sub-techniques, and their associated mitigations. Both sources are treated as authoritative documents and are analysed in their written form.

To support the mapping process, additional literature is reviewed. This includes academic work on control mapping, threat-informed defence, PKI security, and framework alignment.

3.2 Technique Identification

The identification of relevant techniques was carried out using a rule-based selection approach. The aim was to isolate those techniques and sub-techniques from the MITRE ATT&CK that have a meaningful relationship with PKI or cryptographic mechanisms. This step is important because the ATT&CK framework is broad, and many techniques only involve cryptography in a superficial or incidental way. Without clear criteria, the selection process would be inconsistent and difficult to reproduce.

To address this, explicit inclusion and exclusion criteria were defined before the analysis began. These criteria were applied systematically across all tactics in the ATT&CK Enterprise matrix.

3.2.1 Technique Inclusion Criteria

A technique was included in the dataset if it satisfied at least one of the following conditions.

First, techniques were included if they directly involve the use of cryptographic primitives. This includes encryption, decryption, hashing, digital signatures, or message authentication mechanisms. The focus here is not simply on the presence of cryptography, but on whether the technique relies on it as a core component of execution, evasion, or persistence. For example, techniques that use encryption to conceal payloads or communications fall into this category.

Second, techniques were included if they involve the abuse or manipulation of PKI-related artifacts. This includes certificates, certificate chains, trust stores, and authentication tokens that rely on cryptographic trust. The key consideration is whether the attacker leverages trust relationships established through PKI. This may include actions such as forging, stealing, misusing, or bypassing certificate-based trust. Techniques involving token-based authentication mechanisms, such as SAML tokens, were also considered under this criterion when their security properties depend on cryptographic validation.

Third, techniques were included if they target key management processes. This covers the generation, storage, distribution, rotation, or revocation of cryptographic keys. Attacks that aim to extract private keys, weaken key generation, or interfere with key lifecycle management are relevant here. These scenarios are particularly important because weaknesses in key management often undermine otherwise strong cryptographic systems.

3.2.2 Technique Exclusion Criteria

A technique was excluded if cryptography was present but not relevant to the attack logic. In many cases, modern systems use encryption by default, for example through HTTPS or encrypted storage. However, if the attacker does not interact with, exploit, or rely on the cryptographic component, the technique was not considered relevant for this study.

Techniques were also excluded when cryptographic elements were purely environmental. For instance, if encryption is part of the system configuration but does not influence the success, detection, or mitigation of the attack, it was treated as incidental. The goal was to avoid overestimating the role of cryptography in attack scenarios where it does not materially affect the outcome.

In cases where classification was not immediately clear, a conservative approach was taken. Techniques were only included if a clear and defensible link to PKI or cryptographic mechanisms could be established. This helped reduce ambiguity and ensured that the final dataset reflects meaningful relationships rather than loose associations.

The application of these criteria resulted in a focused subset of ATT&CK techniques that are either dependent on, or significantly influenced by, cryptographic and PKI-related mechanisms. This subset forms the basis for the subsequent mapping to E-ITS security controls.

3.3 Mapping Procedure

Once the relevant techniques had been identified, each technique was analysed using a structured and repeatable procedure. The purpose of this step was to translate descriptive attack information from the MITRE ATT&CK into a form that can be consistently mapped to E-ITS security controls. The process was applied individually to each technique and sub-technique included in the dataset.

The first step involved a detailed analysis of the technique itself. This included reviewing the official ATT&CK description, associated examples, and documented adversary behaviour. The goal was to understand how the technique is executed in practice, what system components it interacts with, and what conditions are required for it to succeed. Particular attention was paid to whether the technique relies on, interacts with, or attempts to bypass cryptographic mechanisms.

The next step was to classify the role of PKI or cryptography within the technique. Some techniques rely directly on cryptographic mechanisms for execution, for example through encryption or digital signatures. Others involve the misuse of trust established

by PKI, such as abusing certificates or token-based authentication. In some cases, cryptography is present but only plays a supporting role. This classification helped maintain consistency in later analysis and provided additional context for interpreting the results.

After this, the mitigation intent was normalized. The descriptions provided in ATT&CK often vary in level of detail and wording, even when they refer to similar defensive concepts. To address this, mitigation strategies were abstracted into generalized security objectives. This step ensured that similar defensive measures could be compared and mapped in a uniform way, regardless of how they were originally described.

The final step consisted of mapping the normalized mitigation intents to specific controls in E-ITS. Each technique was mapped to one or more controls, depending on the nature of the mitigation required. The mapping was based on alignment between the security objective derived from the technique and the intent of the control as defined in the E-ITS reference security catalogue. Both direct and supporting controls were considered. Direct controls are those that prevent or significantly hinder the execution of the technique. Supporting controls contribute indirectly, for example by improving detection, increasing visibility, or strengthening the overall security posture.

To maintain consistency, the same mapping logic was applied across all techniques. In cases where multiple controls were applicable, all relevant mappings were retained rather than forcing a one-to-one relationship. When ambiguity arose, mappings were only accepted if a clear and defensible connection between the technique and the control could be established. This approach ensured that the resulting mapping reflects meaningful relationships rather than speculative associations.

The outcome of this procedure is a structured mapping between ATT&CK techniques and E-ITS controls, supported by a consistent analytical framework. This mapping forms the basis for the results and analysis presented in the following chapter.

3.4 Validation

To improve the reliability of the mapping and reduce the risk of omissions or subjective bias, a multi-step validation process was applied. This process focused on three aspects:

completeness of technique identification, consistency of mappings, and identification of coverage gaps.

The first step was a second-pass completeness check. After the initial identification and mapping of techniques, the entire MITRE ATT&CK was reviewed again using the same inclusion criteria defined in Section 3.2. The purpose of this step was to capture any techniques or sub-techniques that may have been overlooked during the first pass. This is particularly relevant given the breadth of the ATT&CK framework and the interpretive nature of identifying cryptography-related relevance. Any newly identified techniques were subjected to the same mapping procedure described in Section 3.3 to ensure consistency.

The second step involved cross-validation of the mappings against established references. For each mapped technique, the identified E-ITS controls were compared with mitigation guidance provided within ATT&CK, as well as with mappings between ATT&CK techniques and controls from NIST SP 800-53. The objective was not to achieve exact one-to-one correspondence, but to assess whether the underlying mitigation intent aligns across frameworks.

The final step focused on the identification of coverage gaps. A gap was defined as a situation where a technique's normalized mitigation objectives, derived in Section 3.3, are not adequately addressed by any corresponding E-ITS control. This includes cases where:

- no relevant control exists within E-ITS;
- existing controls only address the objective indirectly or at a very high level;
- the control lacks sufficient specificity to be considered an effective mitigation in practice.

Gap identification was performed systematically across all mapped techniques. These gaps form an important input to the synthesis section, where their implications for the completeness and effectiveness of E-ITS are discussed.

Together, these validation steps provide a level of assurance that the mapping is both comprehensive and grounded in established security frameworks, while also highlighting areas where E-ITS may require further development.

3.5 Rationale for the Selected Methodological Approach

Several alternative approaches were considered. A keyword-based mapping was rejected because the terminology used in E-ITS does not always correspond directly to the terminology used in MITRE ATT&CK. A quantitative scoring model was also not selected, because the available data does not support reliable measurement of actual control effectiveness or residual risk. A fully automated approach was not selected, because it would risk producing superficial mappings based on terminology overlap rather than substantive mitigation relevance. A purely expert-based approach was also avoided, because it would be less reproducible and more dependent on individual judgement. Finally, a direct reuse of existing NIST SP 800-53 mappings was not sufficient, because E-ITS has its own structure, terminology, and control granularity. Existing mappings were therefore used for cross-validation rather than as the primary mapping source.

The selected methodological approach this study uses is a qualitative document analysis approach supported by systematic mapping. This approach allows each ATT&CK technique to be analysed in terms of its underlying security objective, after which the corresponding mitigation intent can be compared with E-ITS controls. The selected method therefore combines structured inclusion criteria, rule-based technique selection, mitigation intent normalisation, and cross-validation against ATT&CK mitigation guidance and NIST SP 800-53 mappings. This provides a balance between interpretive depth and methodological transparency. It also supports the secondary aim of the thesis, which is to develop a mapping process that can be reused for other national or domain-specific security standards.

3.6 Scope Limitation

A deliberate decision was made to exclude controls that are specific to Estonia's X-Road data exchange layer and its national electronic identity (eID) infrastructure. These controls, located primarily in the SYS.EE module of E-ITS, address highly specialized requirements such as qualified electronic stamps, X-tee trust anchors, and OCSP validation for ID-cards. While these controls are undoubtedly cryptographic in nature, they are not generally applicable to most organizations. Their implementation is

mandatory only for public sector bodies or private entities that choose to connect to X-Road or issue eID certificates. Including them would have distorted the analysis by introducing context-dependent controls that do not represent baseline cryptographic hygiene. Therefore, to keep the mapping relevant for a broad audience – including private sector organizations without X-Road or eID obligations – all SYS.EE controls were excluded from further consideration. The remaining controls from other modules (CON, ORP, OPS, NET, INF, SYS non-EE, APP, IND) reflect requirements that are universally applicable regardless of national infrastructure choices.

4 Results and Analysis

4.1 Overview of Identified Techniques

This section provides a high-level overview of the techniques and sub-techniques selected for analysis. The aim is to establish the scope of the dataset and to highlight general patterns before moving into detailed mapping results.

In total, 25 techniques and sub-techniques were identified as relevant to PKI and cryptographic mechanisms based on the inclusion criteria defined in Section 3.2. These techniques were drawn from across the MITRE ATT&CK and span multiple stages of the attack lifecycle.

A subset of the identified techniques illustrates the different ways cryptographic mechanisms and PKI-related components are leveraged across adversary behaviour. For example, T1486 Data Encrypted for Impact involves an adversary encrypting data on target systems or across a network to disrupt availability, typically for extortion (ransomware) or sabotage. The adversary uses cryptographic algorithms to render files, databases, or entire systems inaccessible, withholding the decryption key, and is primarily associated with the Impact (TA0040) tactic. In a different context, T1553.002 Code Signing reflects an attack where adversaries create, acquire, or steal valid code-signing certificates to sign their malware or tools. A valid signature then allows the binary to bypass operating system trust controls (e.g., Windows Defender Application Control, SmartScreen, macOS Gatekeeper) and appear legitimate to users and security tools, typically within the Defense Evasion (TA0005) tactic. T1558.003 Kerberoasting involves an adversary requesting service tickets (TGS) for service principal names (SPNs) from a domain controller. The encrypted portion of these tickets contains a hash derived from the service account's password (typically using RC4 encryption). The adversary extracts this hash and performs an offline brute-force attack to recover the plaintext password of the service account, targeting weak service account credentials derived from Kerberos ticket encryption mechanisms. [5]

Other techniques highlight the abuse of cryptographic trust rather than direct cryptographic operations. T1606.002 SAML Tokens involves adversaries forging SAML tokens with arbitrary permissions claims and lifetimes if they possess a valid SAML token-signing certificate, potentially bypassing MFA and gaining administrative privileges in Entra ID / Active Directory Federation Services (AD FS), generally falling under the Credential Access (TA0006) tactic. T1552.004 Private Keys focuses on adversaries searching compromised systems for private key files, where they attempt to extract sensitive cryptographic material directly from systems, often enabling broader compromise of encrypted communications or authentication systems. In a similar vein, T1649 Steal or Forge Authentication Certificates involves adversaries obtaining (stealing) or creating (forging) digital certificates used for authentication. By acquiring a valid certificate the adversary can authenticate as the target identity (user or machine) without needing the account password. Thus, the compromise of certificate-based trust relationships allows impersonation or unauthorized access. [5]

When grouped by tactic, the distribution shows that cryptography-related techniques are not confined to a single phase of an attack. Instead, they appear across several tactics, with higher concentrations observed in Credential Access (TA0006): 6 techniques, Defense Evasion (TA0005): 6 techniques, and Resource Development (TA0042): 5 techniques. Lower representation was observed in Command and Control (TA0011): 3 techniques, Exfiltration (TA0010): 2 techniques and Impact (TA0040), Persistence (TA0003) and Reconnaissance (TA0043): 1 technique each. This distribution indicates that cryptographic mechanisms are leveraged by adversaries in a variety of contexts. [5]

Together, these examples demonstrate that cryptographic elements in the ATT&CK framework are not limited to encryption or data protection functions. They also appear in authentication mechanisms, trust infrastructure, and key management processes, each contributing differently depending on the adversary objective and the stage of the attack lifecycle.

To better understand the role of cryptography within these techniques, each entry was classified based on its level of dependence on PKI or cryptographic components.

A total of approximately 32% of the identified techniques involve direct use of cryptographic mechanisms. These include cases where encryption, digital signatures,

hashing, or certificate-based authentication form a core part of the attack. In such techniques, cryptography is essential for execution, concealment, or achieving the intended impact.

The remaining 68% of techniques were classified as having indirect cryptographic relevance. In these cases, cryptography is present but not central to the attack logic. This includes scenarios where attackers exploit trust relationships, misuse authentication tokens, or operate within environments where cryptographic protections exist but are not directly targeted.

This distinction highlights an important pattern. While cryptography and PKI are widely present across modern systems, only a subset of techniques depend on them as a primary mechanism. A larger portion interacts with cryptographic systems in a secondary or supporting role. This observation provides context for the mapping results presented in the following sections, particularly in understanding the extent to which PKI and cryptographic controls contribute to mitigating these techniques.

4.2 Mapping Results

The mapping of identified techniques to E-ITS controls reveals several recurring structural patterns. Rather than a one-to-one correspondence between techniques and controls, the results show a highly interconnected relationship where multiple techniques often map to the same control set, while individual techniques frequently map to several different control domains. This reflects the layered nature of modern security architectures, where a single defensive control may mitigate multiple types of threats, and a single technique may require multiple controls to be effectively addressed.

A prominent pattern observed in the results is the many-to-one relationship, where multiple techniques map to the same E-ITS control. This is especially evident in controls related to access restriction, identity management, and operational security. For example, techniques such as T1553.006 Code Signing Policy Modification, T1606.002 SAML Tokens, and T1098.004 SSH Authorized Keys all converge on similar control objectives related to credential protection, access enforcement and environment monitoring. This indicates that E-ITS relies on a shared set of foundational controls to

mitigate a wide range of cryptography-related threats, rather than providing highly specialised controls for individual attack techniques. [17, 5]

In contrast, one-to-many relationships are also common. A single technique often requires multiple control types to be effectively mitigated. For instance, T1486 Data Encrypted for Impact maps not only to preventive controls outlining resilience mechanisms like backup and recovery, but also to detection-oriented controls such as logging and monitoring. This demonstrates that certain techniques, particularly those with high impact potential, cannot be mitigated through a single defensive layer and instead require a combination of preventive, detective, and corrective controls. [17, 5]

4.3 E-ITS Control Coverage Analysis

When the results are analysed by control domain, a more structured pattern emerges.

Cryptography concepts module (CON.1) form the foundational layer of the mapping. These controls define how cryptographic mechanisms are planned, managed, and enforced within the environment. They appear consistently across techniques involving encryption, certificate usage, and key management. However, their role is primarily enabling rather than directly preventive in many cases. [17]

Management of identity and rights module (ORP.4) controls appear across a wide range of techniques, particularly those involving authentication abuse, certificate misuse, and privileged access scenarios. These controls enforce organisational rules around authentication strength, access rights, and administrative separation of duties. Their recurring presence highlights that many cryptography-related attack paths ultimately depend on weaknesses in identity and privilege management rather than cryptographic primitives themselves. [17]

Detection of security incidents module (DER.1) represents another frequently mapped domain. Controls such as centralised logging and additional detection systems are repeatedly associated with techniques that involve stealth, encryption, or credential misuse. These controls are particularly important in scenarios where encryption limits direct inspection, making behavioural and metadata-based detection essential. [17]

Main IT Operations module (OPS.1.1) also plays a significant role. These controls include malware protection, compliance monitoring, and configuration management mechanisms. They are frequently mapped to techniques involving system modification, credential abuse, and persistence mechanisms. Their primary function is to ensure system integrity and detect deviations from secure baselines. [17]

Networks and communication controls (NET) are mostly associated with encrypted communication and data exfiltration techniques. Controls such as firewall guidelines and network zoning consistently appear in relation to outbound encrypted traffic and command-and-control channels. In addition, proxy-based inspection controls provide an important enforcement mechanism by terminating and analysing encrypted traffic at network boundaries. However, these controls are generally most effective when combined with endpoint and detection mechanisms rather than operating in isolation. [17]

Overall, the mapping results demonstrate that mitigation of PKI and cryptography-related techniques in E-ITS is not concentrated within a single control domain. Instead, effective mitigation is achieved through a combination of cryptographic governance, detection and monitoring, network enforcement, and identity management controls. This reinforces the observation that cryptographic mechanisms alone are not sufficient as a defensive layer, and must be supported by broader security architecture components to address the full range of adversary techniques.

4.4 Validation Results

The validation phase provided additional assurance regarding the completeness and consistency of the mapping between MITRE ATT&CK techniques and E-ITS controls. This section summarises the results of the second-pass review, cross-framework agreement analysis, and the identification of coverage gaps.

4.4.1 Second-pass completeness check

The second-pass completeness check resulted in the identification of 5 additional techniques and sub-techniques that were not captured during the initial analysis. These additions were primarily found in areas where cryptographic relevance is indirect or

embedded within authentication and trust mechanisms. The updated total represents a 20% increase in the number of techniques included in the final dataset. This indicates that the initial pass captured the majority of relevant cases, but also highlights the value of iterative review in reducing selection bias.

4.4.2 Cross-validation

Cross-validation against external references showed a generally high level of consistency between the developed E-ITS mapping and established frameworks.

When compared with mitigation guidance from MITRE ATT&CK, the majority of mappings were classified as aligned or partially aligned, indicating that the E-ITS control interpretations are broadly consistent with ATT&CK-defined mitigation strategies. In most cases, differences were related to granularity rather than conceptual disagreement, where E-ITS controls tend to be more generalised compared to the technique-specific mitigations defined in ATT&CK.

A similar pattern was observed in the comparison with mappings derived from NIST SP 800-53. The majority of control mappings demonstrated conceptual alignment, particularly in areas related to access control, system monitoring, and cryptographic key management. Partial alignment cases typically arose where E-ITS controls aggregate multiple NIST control concepts into broader organisational-level requirements.

4.4.3 Identified Gaps

Finally, the validation process identified a small number of techniques with limited or no corresponding E-ITS control coverage. A total of 5 techniques were classified as unmappable to the E-ITS framework:

- T1587.002 Code Signing Certificates
- T1587.003 Digital Certificates
- T1608.003 Install Digital Certificate
- T1588.003 Code Signing Certificates
- T1588.004 Digital Certificates

All these techniques are from the Resource Development (TA0042) tactic and cover adversaries actions outside the enterprise environment. According to MITRE, these

techniques cannot be easily mitigated with preventive controls. This is also supported by NIST SP 800-53 where these techniques are marked unmappable.

These gaps are particularly relevant for understanding structural limitations in E-ITS coverage of cryptography-related threat scenarios. They are further discussed in the synthesis section, where their implications for control completeness and potential framework enhancement are analysed.

5 Synthesis

The results of this study point to a clear conclusion. PKI and cryptographic mechanisms, while essential, do not operate as standalone security controls in practice. Across the mapped techniques, cryptography rarely appears as the primary line of defence. Instead, it functions as part of a broader system of controls, where its effectiveness depends on how well it is supported by surrounding mechanisms such as access control, monitoring, and system configuration management.

This is most visible in techniques that explicitly rely on cryptography, such as encrypted command and control or data encryption for impact. Even in these cases, mitigation is not achieved through cryptographic controls alone. Preventing abuse of encrypted channels requires network controls, traffic inspection, and endpoint detection. Limiting the impact of ransomware depends on backup strategies, access restrictions, and operational resilience. Similarly, attacks involving certificates or authentication tokens are rarely mitigated by strengthening cryptographic primitives themselves. Instead, they are addressed through identity management, privilege control, and secure handling of key material. This indicates that the security problem is not rooted in cryptography as a technology, but in how it is implemented, managed, and integrated into the wider system.

From this perspective, security should be understood as a control ecosystem rather than a set of isolated domains. Controls do not operate independently. They reinforce each other, compensate for each other's limitations, and together provide defence in depth. Cryptographic mechanisms establish trust and protect data, but they rely on access control to prevent misuse, on monitoring to detect abuse, and on operational controls to maintain their integrity over time. When these supporting controls are weak, even strong cryptography can be bypassed or misused. The mapping results consistently reflect this interdependence, showing that most techniques require a combination of control types rather than a single specialised solution.

The analysis also highlights both strengths and limitations within the E-ITS framework. One of its key strengths lies in its emphasis on foundational and cross-cutting controls. Areas such as identity and access management, centralised logging, configuration management, and organisational procedures are well represented and widely applicable across the mapped techniques. These controls provide broad coverage and are effective against a wide range of attack scenarios, including those involving cryptographic components. The framework's structured approach to governance and operational processes also supports consistency in implementation, which is critical for maintaining security over time.

At the same time, certain gaps and limitations become visible when focusing specifically on PKI and cryptography-related threats. Some techniques identified in this study could not be directly mapped to existing E-ITS controls, suggesting that specific attack scenarios are not fully addressed. In addition, several important mitigation strategies appear only indirectly or at a high level within the framework. While these areas may be partially covered through general controls, their lack of explicit representation reduces clarity and may lead to inconsistent implementation in practice.

In addition to the empirical findings, this study also contributes a structured methodology for mapping security standards to adversary behaviour frameworks. The approach developed in this thesis follows a clear sequence of steps. It begins with defining inclusion criteria to identify relevant techniques, followed by systematic analysis of each technique to extract underlying security objectives. These objectives are then normalised into consistent mitigation intents, which are mapped to corresponding controls within the target framework. The process is supported by iterative validation, including a second-pass review and cross-referencing with established sources.

The strength of this approach lies in its generalisability. Although it was applied to E-ITS in this study, the same methodology can be used to evaluate other national or sector-specific standards. It provides a repeatable way to translate compliance-oriented control frameworks into a threat-informed context. This helps bridge the gap between what organisations are required to implement and how attackers actually operate. As a result, the methodology supports not only analysis, but also practical decision-making in

areas such as control prioritisation, detection engineering, and security architecture design.

5.1 Future Directions

This study focused specifically on PKI and cryptography-related techniques within the MITRE ATT&CK. While this provided a clear and manageable scope, it also leaves open the question of how well E-ITS addresses adversary behaviour in other domains. Many techniques outside the PKI and cryptographic space, such as those related to initial access, lateral movement, or persistence, were not included in the analysis. These areas may reveal different patterns of control coverage and different types of gaps.

A natural next step would be to apply the same mapping methodology to the full ATT&CK framework. This would allow for a more comprehensive evaluation of E-ITS as a whole, rather than within a single domain. It would also make it possible to compare coverage across different categories of techniques and identify whether the patterns observed in this study are consistent or domain-specific.

From a practical perspective, extending the mapping could support organisations in building a fully threat-informed view of their compliance posture. It would enable security teams to understand not only how PKI-related threats are mitigated, but how well their overall control environment aligns with real-world attacker behaviour. This could inform prioritisation of controls, guide detection engineering efforts, and support more targeted improvements to both E-ITS and its implementation in practice.

6 Conclusion

The main objective of this thesis was to evaluate how well the controls of the Estonian Information Security Standard (E-ITS) address adversarial behaviour targeting Public Key Infrastructure and cryptographic systems. This was achieved by mapping selected techniques and sub-techniques from the MITRE ATT&CK to corresponding E-ITS controls and analysing the resulting coverage. In parallel, the study aimed to develop a structured methodology that can be used to perform similar mappings between security standards and adversary behaviour frameworks.

The first research question asked how E-ITS controls can be systematically mapped to PKI and cryptography-related ATT&CK techniques in order to create a threat-informed view of compliance. This thesis demonstrates that such mapping is both feasible and informative when supported by a structured process. By identifying relevant techniques, extracting their underlying security objectives, and aligning these with E-ITS control intent, it is possible to establish a clear link between formal requirements and real-world attack scenarios. The resulting mapping provides a practical way to interpret E-ITS controls in the context of adversary behaviour and highlights where coverage is strong and where it is limited.

The second research question focused on the development of a methodological approach. The study proposes a repeatable mapping process that combines rule-based technique selection, structured analysis, mitigation intent normalisation, and cross-validation against established references such as NIST SP 800-53 and ATT&CK mitigation guidance. This approach reduces subjectivity and provides a consistent basis for comparing controls across different frameworks. It also offers a foundation for future research and practical applications beyond the scope of this thesis.

The findings of the analysis lead to several important conclusions. First, PKI and cryptographic controls alone are not sufficient to mitigate the majority of relevant attack techniques. While cryptography plays a critical role in establishing trust and protecting data, most techniques are mitigated primarily through access control, monitoring,

configuration management, and network security mechanisms. This shows that many attacks targeting cryptographic systems do not break cryptography itself, but instead exploit weaknesses in how it is implemented and managed.

Second, the effectiveness of E-ITS lies in its emphasis on foundational and cross-cutting controls. Areas such as identity and access management, centralised logging, and operational procedures provide broad and consistent coverage across many techniques. These controls form the backbone of defence against a wide range of threats, including those involving PKI and cryptography.

At the same time, the analysis identified several limitations. A small number of techniques could not be directly mapped to existing E-ITS controls, and some mitigation areas are only addressed indirectly or at a high level. This suggests that while E-ITS provides a solid baseline, certain modern attack scenarios, particularly those involving abuse of trust mechanisms or cloud-based environments, may require more explicit treatment.

In conclusion, this thesis demonstrates that mapping security standards to adversary behaviour frameworks provides valuable insight into the real-world effectiveness of those standards. It shows that compliance alone does not guarantee protection against relevant threats, but that a threat-informed perspective can help bridge this gap. By combining structured methodology with practical analysis, this work contributes both a reusable approach and a clearer understanding of how E-ITS supports the defence of PKI and cryptographic systems.

References

[1] Serrano, N., Hadan, H., & Camp, L. J. (2019). A complete study of P.K.I. (PKI's Known Incidents). SSRN Electronic Journal, vol. TPRC, no. 47. https://par.nsf.gov/biblio/10204025-complete-study-pkis-known-incidents

[2] D. Kim et al., "Security Analysis on Practices of Certificate Authorities in the HTTPS Phishing Ecosystem," Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security, May 2021, doi: https://doi.org/10.1145/3433210.3453100

[3] K. Kozák, B. J. Kwon, D. Kim, and T. Dumitraş, "Issued for Abuse: Measuring the Underground Trade in Code Signing Certificate," arXiv (Cornell University), Jan. 2018, doi: https://doi.org/10.48550/arxiv.1803.02931

[4] K. Ivanov, "Autonomous collision attack on OCSP services," arXiv (Cornell University), Jan. 2016, doi: https://doi.org/10.48550/arxiv.1609.03047.

[5] MITRE, "MITRE ATT&CK for Enterprise Version 18.1" (Oct. 2025). https://attack.mitre.org/

[6] M. R. Rahman and L. Williams, "An investigation of security controls and MITRE ATT&CK techniques," arXiv (Cornell University), Nov 2022. doi: https://doi.org/10.48550/arXiv.2211.06500

[7] P. Bhosale, W. Kastner, and T. Sauter, "Mapping ICS Vulnerabilities: Prioritization and Risk Propagation Analysis with MITRE ATT&CK Framework and Bayesian Belief Networks," 2024 IEEE 29th International Conference on Emerging Technologies and Factory Automation (ETFA), pp. 1–8, Sep. 2024, doi: https://doi.org/10.1109/etfa61755.2024.10710893

[8] CISA. "Best Practices for MITRE ATT&CK Mapping." (2023). https://www.cisa.gov/sites/default/files/2023-01/Best%20Practices%20for%20MITRE%20ATTCK%20Mapping.pdf

[9] CIS. "CIS Controls v8 Master Mapping to MITRE Enterprise ATT&CK v82". (2024). https://www.cisecurity.org/insights/white-papers/cis-controls-v8-master-mapping-to-mitre-enterprise-attck-v82

[10] T. He and Z. Li, "A Model and Method of Information System Security Risk Assessment based on MITRE ATT&CK," 2021 2nd International Conference on Electronics, Communications and Information Technology (CECIT), Dec. 2021, doi: https://doi.org/10.1109/cecit53797.2021.00022

[11] W. Wang, X. Bai, B. Hu, G. Ge, and L. Han, "A Network Security Risk Management Model Based on ATT&CK for ICS," Dec. 2022, doi: https://doi.org/10.1109/icftic57696.2022.10075132

[12] T. Wang, Y. Ma, Z. Shao, and Z. Xu, "Research on Power System Cyber Security Defense based on ATT&CK Framework," Jul. 2023, doi: https://doi.org/10.1109/eeps58791.2023.10256874

[13] J. Uralov, S. Abdullaeva, I. Risolat, M. Yusupova, S. Kutliev, and M. Qazaqov, “Using the MITRE ATT&CK Framework in SOC Activities and Analyzing Cyber Attack,” 2025 IEEE 26th International Conference of Young Professionals in Electron Devices and Materials (EDM), pp. 2160–2164, Jun. 2025, doi: https://doi.org/10.1109/edm65517.2025.11096745

[14] J. Straub, “Modeling Attack, Defense and Threat Trees and the Cyber Kill Chain, ATT&CK and STRIDE Frameworks as Blackboard Architecture Networks,” IEEE Xplore, Nov. 2020. doi: https://doi.org/10.1109/SmartCloud49737.2020.00035

[15] Muhamad Akdzan Angganegara, Iqbal Yulizar Mukti, and Muhammad Fathinnuddin, “Integration of STRIDE and MITRE ATT&CK Frameworks for Enhanced Cyber Threat Modeling: A Case Study of Digital Merchant Banking Application,” pp. 1–6, Feb. 2025, doi: https://doi.org/10.1109/icadeis65852.2025.10933223

[16] Z. Jing, Zhang Guangzhou, J. Xueqi, You Jiachuan, and L. Ye, “Research on Threat Path Construction Technology of Power Monitoring System Based on ATT&CK Framework,” pp. 93–100, Nov. 2024, doi: https://doi.org/10.1109/icn64251.2024.10865972

[17] RIA. “Meetmete kataloog 2024”. (n.d.). https://eits.ria.ee/api/2/home/asset/E-ITS%202024_meetmete_tabel_CC.xlsx

[18] RIA. “E-ITS auditeerimiseeskiri_2024”. (n.d.). https://eits.ria.ee/api/2/home/asset/Lisa%203.pdf

[19] RIA. “E-ITS nõuded infoturbe halduse süsteemile 2024”. (n.d.). https://eits.ria.ee/api/2/home/asset/Lisa%201.pdf

[20] RIA. “E-ITS meetmete kataloog_2024”. (n.d.). https://eits.ria.ee/api/2/home/asset/Lisa%202.pdf

[21] MITRE Center for Threat-Informed Defense, “NIST 800-53 Controls to ATT&CK Mappings,” January 13, 2022. https://ctid.mitre.org/projects/nist-800-53-control-mappings/

Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis[1]

I, Anton Kolisnetšenko

1 grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis “Analysis of E-ITS Control Coverage for MITRE ATT&CK PKI and Cryptography-Related Techniques“, supervised by Toomas Lepik

1.1 to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;

1.2 to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.

2 I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.

3 I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

[1] The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.

Appendix 2 – Mapping Results Table

Tabel 1. Mapping of MITRE ATT&CK PKI and Cryptography-Related Techniques to E-ITS Controls

Technique ID	*Technique Name*	*E-ITS Control*	*E-ITS Control Name*	*Comments*	*NIST 800-53*	*MITRE*
T1573	Encrypted Channel	CON.1.M10	Cryptography concept	Establishes authorized encryption boundaries and key stores.	SC-12	-
T1573	Encrypted Channel	DER.1.M11	Centralised logging infrastructure for security event analysis	Correlates encrypted traffic logs with endpoint activity.	SI-04	-
T1573	Encrypted Channel	OPS.1.1.4.M1	Protection Against Malware	Detects the local process initiating the encrypted channel.	SI-03	-
T1573	Encrypted Channel	DER.1.M9	Additional detection systems	Uses IDS to detect C2 patterns in encrypted flow metadata.	-	M1031
T1573	Encrypted Channel	DER.1.M10	TLS and SSH proxies	Terminates and inspects encrypted C2 traffic at the boundary.	-	M1020
T1573	Encrypted Channel	NET.3.2.M2	Security guidelines for firewalls	Restricting internal hosts that can initiate outbound encrypted connections prevents direct malware C2 channels.	AC-04	-
T1573	Encrypted Channel	ORP.4.M12	Authentication procedure for IT systems and applications	Establishes organizational policy requiring strong, authenticated protocols (SSH, TLS) and prohibiting weak, hijackable sessions that could hide T1573 traffic.	SC-23	-
T1573.001	Symmetric Cryptography	CON.1.M10	Cryptography concept	Establishes authorized encryption boundaries and	SC-12	-

Technique ID	*Technique Name*	*E-ITS Control*	*E-ITS Control Name*	*Comments*	*NIST 800-53*	*MITRE*
				key stores.		
T1573.001	Symmetric Cryptography	DER.1.M11	Centralised logging infrastructure for security event analysis	Correlates encrypted traffic logs with endpoint activity.	SI-04	-
T1573.001	Symmetric Cryptography	OPS.1.1.4.M1	Protection Against Malware	Detects the local process initiating the encrypted channel.	SI-03	-
T1573.001	Symmetric Cryptography	DER.1.M9	Additional detection systems	Uses IDS to detect C2 patterns in encrypted flow metadata.	-	M1031
T1573.001	Symmetric Cryptography	DER.1.M10	TLS and SSH proxies	Terminates and inspects encrypted C2 traffic at the boundary.	-	M1020
T1573.001	Symmetric Cryptography	NET.3.2.M2	Security guidelines for firewalls	Restricting internal hosts that can initiate outbound encrypted connections prevents direct malware C2 channels.	AC-04	-
T1573.001	Symmetric Cryptography	ORP.4.M12	Authentication procedure for IT systems and applications	Establishes organizational policy requiring strong, authenticated protocols (SSH, TLS) and prohibiting weak, hijackable sessions that could hide T1573 traffic.	SC-23	-
T1573.002	Asymmetric Cryptography	CON.1.M10	Cryptography concept	Establishes authorized encryption boundaries and key stores.	SC-12	-
T1573.002	Asymmetric Cryptography	DER.1.M11	Centralised logging infrastructure for security event analysis	Correlates encrypted traffic logs with endpoint activity.	SI-04	-
T1573.002	Asymmetric Cryptography	OPS.1.1.4.M1	Protection Against Malware	Detects the local process initiating the encrypted channel.	SI-03	-

Technique ID	*Technique Name*	*E-ITS Control*	*E-ITS Control Name*	*Comments*	*NIST 800-53*	*MITRE*
T1573.002	Asymmetric Cryptography	DER.1.M9	Additional detection systems	Uses IDS to detect C2 patterns in encrypted flow metadata.	-	M1031
T1573.002	Asymmetric Cryptography	DER.1.M10	TLS and SSH proxies	Terminates and inspects encrypted C2 traffic at the boundary.	-	M1020
T1573.002	Asymmetric Cryptography	NET.3.2.M2	Security guidelines for firewalls	Restricting internal hosts that can initiate outbound encrypted connections prevents direct malware C2 channels.	AC-04	-
T1573.002	Asymmetric Cryptography	ORP.4.M12	Authentication procedure for IT systems and applications	Establishes organizational policy requiring strong, authenticated protocols (SSH, TLS) and prohibiting weak, hijackable sessions that could hide T1573 traffic.	SC-23	-
T1606.002	SAML Tokens	CON.1.M4	Cryptography concept	Directly mitigates theft or misuse of the token-signing private key required for T1606.002.	SC-12	M1015
T1606.002	SAML Tokens	OPS.2.2.M18	Regular use of federation services	Prevents over-privileged forged tokens from going unnoticed.	IA-13	-
T1606.002	SAML Tokens	ORP.4.M2	Granting, modifying, and revoking rights	Restricts access to the AD FS server to only privileged accounts.	AC-06	M1026
T1606.002	SAML Tokens	ORP.4.M24	Implementation of the four eyes principle in IT management	This mitigates the risk of a single compromised admin account being used to establish a rogue federation trust or export the token-signing certificate.	AC-02	M1026
T1606.002	SAML Tokens	DER.1.M11	Centralised logging infrastructure for security	Enables detection of suspicious changes to federation configurations, certificate exports, or	SI-04	M1047

Technique ID	*Technique Name*	*E-ITS Control*	*E-ITS Control Name*	*Comments*	*NIST 800-53*	*MITRE*
			event analysis	anomalous token issuance patterns.		
T1553.002	Code Signing	CON.1.M4	Secure key management	Protects the private key of the code-signing certificate, preventing theft by adversaries.	-	-
T1553.003	SIP and Trust Provider Hijacking	DER.1.M18	Regular integrity checks	Monitoring system DLLs and registry hive files for unauthorized changes directly detects SIP hijacking attempts.	SI-07	-
T1553.003	SIP and Trust Provider Hijacking	OPS.1.1.5.M3	Configuring the logging of events	Enables detection of registry modifications (e.g., SACL on SIP registry keys) and DLL load events.	SI-04	M1047
T1553.003	SIP and Trust Provider Hijacking	ORP.4.M2	Granting, modifying, and revoking rights	Enforces least privilege for user accounts. Prevents non-administrative users from modifying protected registry keys or replacing DLLs in System32.	AC-06	M1024
T1553.003	SIP and Trust Provider Hijacking	OPS.1.1.7.M11	Regular compliance analysis of systems management	Detects unauthorized changes to registry settings or file placements that deviate from the secure configuration baseline.	CM-06	-
T1553.003	SIP and Trust Provider Hijacking	OPS.1.1.4.M1	Protection Against Malware	Detects a malicious SIP DLL dropped to disk and blocks it.	SI-03	-
T1553.004	Install Root Certificate	ORP.4.M2	Granting, modifying, and revoking rights	Prevents non-administrative users from installing root certificates.	AC-06	M1028
T1553.004	Install Root Certificate	OPS.1.1.7.M11	Regular compliance analysis of systems	Detects unauthorized additions to the system's certificate store (e.g., new root certificates) and alerts	CM-06	-

Technique ID	*Technique Name*	*E-ITS Control*	*E-ITS Control Name*	*Comments*	*NIST 800-53*	*MITRE*
			management	on deviation.		
T1553.004	Install Root Certificate	OPS.1.1.5.M3	Configuring the logging of events	Enables logging of security-relevant events, including modifications to the certificate store.	SI-04	-
T1553.004	Install Root Certificate	CON.1.M10	Cryptography concept	Defines the organization's cryptographic strategy, including which root CAs are trusted and how trust anchors are managed.	CM-06	-
T1553.004	Install Root Certificate	OPS.1.1.3.M1	Procedure for patch and change management	Ensures changes to system configuration (including certificate store) are documented, approved, and audited. Reduces the likelihood of unauthorized changes slipping through unnoticed.	-	-
T1553.006	Code Signing Policy Modification	ORP.4.M2	Granting, modifying, and revoking rights	Prevents non-administrative users from modifying code signing policy.	AC-06	M1026
T1553.006	Code Signing Policy Modification	OPS.1.1.7.M11	Regular compliance analysis of systems management	Detects changes to boot configuration by comparing current configuration against a secure baseline.	CM-02	-
T1553.006	Code Signing Policy Modification	OPS.1.1.3.M1	Procedure for patch and change management	Controls changes to system configuration, including boot parameters, reducing the risk of unauthorized tampering.	CM-03	-
T1553.006	Code Signing Policy Modification	ORP.4.M2	Granting, modifying, and revoking rights	Prevents non-administrative users from modifying code signing policy.	AC-06	M1026
T1553.006	Code Signing Policy Modification	DER.1.M18	Regular integrity checks	Monitoring code signing policy files for unauthorized changes	SI-07	-

Technique ID	*Technique Name*	*E-ITS Control*	*E-ITS Control Name*	*Comments*	*NIST 800-53*	*MITRE*
				detects code signing policy modification attempts.		
T1600	Weakening Encryption	CON.1.M1	Planning the implementation of cryptographic mechanisms	Establishes the cryptographic baseline that adversaries attempt to weaken. Any deviation is a violation of this planning control.	-	-
T1600	Weakening Encryption	CON.1.M10	Cryptography concept	Provides the policy foundation to identify and reject weakened crypto configurations during change management.	-	-
T1600	Weakening Encryption	CON.1.M15	Reacting to the impairment of cryptographic mechanisms	Directly addresses scenario where weak encryption is discovered.	-	-
T1600.001	Reduce Key Space	CON.1.M1	Planning the implementation of cryptographic mechanisms	Requires use of approved algorithms without known weaknesses and current recommended key lengths, which prevents the configuration of a reduced key space if enforced technically.	-	-
T1600.001	Reduce Key Space	CON.1.M15	Reacting to the impairment of cryptographic mechanisms	Requires annual review of cryptographic methods/parameters against trusted sources and a procedure for restoring the required security level when a mechanism weakens, which addresses the scenario where a weak cipher is enabled.	-	-
T1600.001	Reduce Key Space	OPS.1.1.7.M11	Regular compliance analysis of systems	Detects the reduced key space anomaly on the network device.	-	-

Technique ID	*Technique Name*	*E-ITS Control*	*E-ITS Control Name*	*Comments*	*NIST 800-53*	*MITRE*
			management			
T1600.002	Disable Crypto Hardware	CON.1.M20	Identifying manipulations of hardware and software with cryptographic functions	Directly addresses the technique's goal of disabling hardware crypto covertly by requiring that cryptographic hardware cannot be bypassed or deactivated unnoticed and that manipulation attempts are detected.	-	-
T1600.002	Disable Crypto Hardware	OPS.1.1.7.M11	Regular compliance analysis of systems management	Detects the mismatch where hardware encryption is disabled.	-	-
T1600.002	Disable Crypto Hardware	OPS.1.1.7.M14	Central management of the configurations of the IT systems managed	Mandates central configuration management where device configurations are stored, versioned, and monitored. If disabling hardware crypto deviates from the secure baseline, this control enables detection and rollback.	-	-
T1048.001	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	NET.1.1.M12	Security of outgoing data traffic	Provides a choke point where exfiltration attempts over alternative protocols can be blocked or inspected.	SC-07	M1037
T1048.001	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	DER.1.M10	TLS and SSH proxies	Terminates and inspects encrypted C2 traffic at the boundary.	AC-04	M1037
T1048.001	Exfiltration Over Symmetric Encrypted	NET.1.1.M4	Network zoning	Requires network segmentation, isolates critical systems from direct internet access	SC-07	M1030

Technique ID	*Technique Name*	*E-ITS Control*	*E-ITS Control Name*	*Comments*	*NIST 800-53*	*MITRE*
	Non-C2 Protocol			forcing an adversary with a foothold in the internal network to cross a firewall boundary to exfiltrate data, increasing the chance of detection or blocking.		
T1048.001	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	DER.1.M9	Additional detection systems	Uses IDS to detect C2 patterns in encrypted flow metadata.	-	M1031
T1048.002	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	NET.1.1.M12	Security of outgoing data traffic	Provides a choke point where exfiltration attempts over alternative protocols can be blocked or inspected.	SC-07	M1037
T1048.002	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	DER.1.M10	TLS and SSH proxies	Terminates and inspects encrypted C2 traffic at the boundary.	AC-04	M1037
T1048.002	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	NET.1.1.M4	Network zoning	Requires network segmentation, isolates critical systems from direct internet access forcing an adversary with a foothold in the internal network to cross a firewall boundary to exfiltrate data, increasing the chance of detection or blocking.	SC-07	M1030
T1048.002	Exfiltration Over Asymmetric Encrypted Non-C2	DER.1.M9	Additional detection systems	Uses IDS to detect C2 patterns in encrypted flow metadata.	-	M1031

Technique ID	*Technique Name*	*E-ITS Control*	*E-ITS Control Name*	*Comments*	*NIST 800-53*	*MITRE*
	Protocol					
T1098.004	SSH Authorized Keys	OPS.1.1.7.M11	Regular compliance analysis of systems management	Detects unauthorized changes to the authorized SSH keys file that deviate from the secure configuration baseline.	CM-06	-
T1098.004	SSH Authorized Keys	OPS.1.1.7.M14	Central management of the configurations of the IT systems managed	Mandates central configuration management where device configurations are stored, versioned, and monitored. If an unauthorized addition of a public key, this control enables detection and rollback.	CM-02	-
T1098.004	SSH Authorized Keys	ORP.4.M10	Protection of privileged accounts	Requires MFA for privileged accounts. If an adversary adds a key to a privileged account, MFA still blocks access.	IA-02	-
T1098.004	SSH Authorized Keys	ORP.4.M2	Granting, modifying, and revoking rights	Prevents non-administrative users from adding SSH keys.	AC-06	M1022
T1596.003	Digital Certificates	CON.1.M19	List of cryptographic tools in use	Requires maintaining an inventory of cryptographic tools (including digital certificates), which can help identify which certificates are deployed and where, enabling review of the information they expose.	-	-
T1649	Steal or Forge Authentication Certificates	CON.1.M4	Secure key management	Mandates a secure key management system covering the entire key lifecycle, including protection of private/secret keys against unauthorized access,which mitigates theft of private keys associated with	IA-05	M1041

Technique ID	*Technique Name*	*E-ITS Control*	*E-ITS Control Name*	*Comments*	*NIST 800-53*	*MITRE*
				authentication certificates.		
T1649	Steal or Forge Authentication Certificates	CON.1.M16	Physical security of cryptographic hardware modules	Requires physical security measures for hardware cryptographic modules such as HSMs. Storing CA private keys or high-value user certificates in HSMs/TPMs prevents software-based extraction by adversaries.	IA-05	M1041
T1649	Steal or Forge Authentication Certificates	ORP.4.M10	Protection of privileged accounts	MFA reduces the risk of an adversary authenticating using a stolen certificate.	IA-02	-
T1649	Steal or Forge Authentication Certificates	OPS.1.1.7.M11	Regular compliance analysis of systems management	Detects unauthorized changes to CA server settings or certificate template permissions.	-	M1047
T1552.004	Private Keys	CON.1.M4	Secure key management	Addresses the root cause of private key theft by mandates a secure key management system covering the entire lifecycle of cryptographic keys, including protection of private/secret keys against unauthorized access.	SC-12	M1041
T1552.004	Private Keys	CON.1.M2	Ensuring data security when using cryptographic mechanisms	Mandates storing long-term keys offline, ensuring that private key material is not exposed in easily accessible backups or system storage.	SC-28	M1041
T1552.004	Private Keys	ORP.4.M8	Procedure for the use of passwords	For private keys protected by a passphrase, this control requires complex passphrases, making offline brute-force attacks	IA-05	M1027

Technique ID	*Technique Name*	*E-ITS Control*	*E-ITS Control Name*	*Comments*	*NIST 800-53*	*MITRE*
				against stolen key files significantly harder.		
T1552.004	Private Keys	ORP.4.M7	Management of data access	Manages access rights to data, including restricting file system permissions to ensure that only authorized users (and processes) can access certificate stores.	AC-03	M1022
T1552.004	Private Keys	OPS.1.1.7.M11	Regular compliance analysis of systems management	Detects unauthorized changes to file permissions on sensitive directories (e.g., ~/.ssh), which would indicate preparation for private key theft.	CM-06	M1047
T1558.003	Kerberoasting	ORP.4.M22	Establishment of password quality requirements	Mandates password quality requirements, including minimum length and complexity. Applying this to service accounts ensures passwords are sufficiently complex to withstand offline brute-force attacks against Kerberoasted hashes.	IA-05	M1027
T1558.003	Kerberoasting	ORP.4.M8	Procedure for the use of passwords	Establishes password usage rules including regular password changes and prohibiting easily guessable passwords, aligning with the principle of limiting the exposure window of a compromised service account password.	IA-05	M1027
T1558.003	Kerberoasting	CON.1.M1	Planning the implementation of cryptographic mechanisms	This supports configuring Active Directory to use AES encryption for Kerberos tickets instead of the weak, crackable RC4 algorithm.	IA-05	M1041

Technique ID	*Technique Name*	*E-ITS Control*	*E-ITS Control Name*	*Comments*	*NIST 800-53*	*MITRE*
T1558.003	Kerberoasting	ORP.4.M2	Granting, modifying, and revoking rights	Service accounts should be granted only the specific rights required for the service to function and should never be added to highly privileged groups like Domain Admins. This limits the impact of a cracked service account password.	AC-06	M1026
T1558.003	Kerberoasting	DER.1.M15	Centralised real-time management of event notifications	Enables correlation of Windows Event Logs (e.g., Event ID 4769 - TGS request) to detect anomalous patterns indicative of Kerberoasting, such as a single account requesting a high volume of service tickets.	SI-04	-
T1558.004	AS-REP Roasting	CON.1.M1	Planning the implementation of cryptographic mechanisms	This supports configuring Active Directory to use AES encryption for Kerberos tickets instead of the weak, crackable RC4 algorithm.	IA-05	M1041
T1558.004	AS-REP Roasting	ORP.4.M22	Establishment of password quality requirements	Mandates password quality requirements, including minimum length and complexity. Applying this to service accounts ensures passwords are sufficiently complex to withstand offline brute-force attacks against Kerberoasted hashes.	IA-05	M1027

Technique ID	*Technique Name*	*E-ITS Control*	*E-ITS Control Name*	*Comments*	*NIST 800-53*	*MITRE*
T1558.004	AS-REP Roasting	OPS.1.1.7.M14	Central management of the configurations of the IT systems managed	User account attributes (including DONT_REQ_PREAUTH) can be managed centrally, ensuring that preauthentication is enabled by default.	CM-02	M1047
T1558.004	AS-REP Roasting	OPS.1.1.7.M11	Regular compliance analysis of systems management	Detects deviations such as user accounts with Kerberos preauthentication disabled, alerting administrators to this misconfiguration.	CM-06	M1047
T1558.004	AS-REP Roasting	ORP.4.M2	Granting, modifying, and revoking rights	Limits the number of highly privileged user accounts reducing the potential impact of a cracked password from an AS-REP roasting attack.	AC-06	-
T1558.005	Ccache Files	ORP.4.M2	Granting, modifying, and revoking rights	If an adversary steals a ticket, the damage is limited to the privileges of that specific account.	AC-06	-
T1558.005	Ccache Files	ORP.4.M7	Management of data access	Prevents unauthorized users from reading credential cache files.	AC-03	-
T1486	Data Encrypted for Impact	CON.3.M5	Regular data backup	Mandates regular data backups, which is the primary recovery mechanism against ransomware.	CP-09	M1053
T1486	Data Encrypted for Impact	CON.3.M12	Secure storage of backup data media	Requires secure storage of backup media in a location separate from the source system, preventing the ransomware from encrypting or deleting the backups.	CP-06	M1053
T1486	Data	CON.3.M14	Protection of	Ensures that an adversary	CP-09	M1053

Technique ID	*Technique Name*	*E-ITS Control*	*E-ITS Control Name*	*Comments*	*NIST 800-53*	*MITRE*
	Encrypted for Impact		backup copies	cannot tamper with or encrypt the backup data.		
T1486	Data Encrypted for Impact	CON.3.M15	Regular testing of backup	Testing ensures that backups are not corrupted and can be successfully restored within the required recovery time objective	CP-10	M1053
T1486	Data Encrypted for Impact	OPS.1.1.4.M1	Protection Against Malware	Mandates malware protection including signature-based and behavioral detection.	SI-03	M1040
T1587.002	Code Signing Certificates	N/A	-	Covers adversaries actions outside the enterprise environment, cannot be mitigated by preventive controls.	-	M1056
T1587.003	Digital Certificates	N/A	-	Covers adversaries actions outside the enterprise environment, cannot be mitigated by preventive controls.	-	M1056
T1608.003	Install Digital Certificates	N/A	-	Covers adversaries actions outside the enterprise environment, cannot be mitigated by preventive controls.	-	M1056
T1588.003	Code Signing Certificates	N/A	-	Covers adversaries actions outside the enterprise environment, cannot be mitigated by preventive controls.	-	M1056
T1588.004	Digital Certificates	N/A	-	Covers adversaries actions outside the enterprise environment, cannot be mitigated by preventive controls.	-	M1056