TLP:CLEAR

ICT, Strategy & Policy
www.tno.nl
+31 88 866 00 00
info@tno.nl

TNO 2025 P11921 – 23 march 2025

Cryptographic Asset Discovery and Inventory

A market survey and fit-gap analysis

Authors: Thom Sijpesteijn
Maaike van Leuken
Frederik Kerling

Report classification: TNO Public

Number of pages: 64
Number of attachments: 2
Funded by: CIO Rijk,
the Chief Information Officer of the Central Government,
National Cybersecurity Centre,
Ministry of Economic Affairs

Board summary

This document is the result of study into commercially available tooling for cryptographic asset discovery & inventory (CADI). CADI is aimed at creating an overview of all cryptography used within an organisation. Such an overview is important from a security perspective and, in particular, with an eye to the upcoming migration to post-quantum cryptography (PQC). Input has been collected via a workshop involving technical and policy stakeholders within the government, as well as via desk research and structured interviews with product providers. Based on the results, requirements have been drafted for a *minimum viable product* (MVP) and the *ideal CADI tool*. This study was funded by the Ministry of the Interior and Kingdom Relations, the National Cybersecurity Centre, and the Ministry of Economic Affairs. As such, the results of this study are relevant to government bodies, but may also provide insights for a broader scope of public and private organisations.

During the study, it was found that there are many differences between the various CADI tools, both on a technical level and in terms of product maturity. The ideal for IT environments is not fully reached at this time, but some tools do approximate it. We conclude that the deployment of CADI tooling is a trade-off, with higher precision scaling with greater efforts. Existing *full-stack* solutions for CADI are generally expensive and not European-made. IT asset management in a broad sense is already seen as complex in many organisations; as such, it is important that CADI is properly aligned with existing solutions. CADI tooling providers are aware of this fact and integration with existing, more generic cybersecurity and asset management products is an ongoing focus.

In addition, we find that CADI tooling is less mature in the field of *operational technology* (OT) than in the field of *information technology* (IT). For example, there is few existing OT tooling to tie into, and some providers indicate having no interest in expanding their product range with OT support. OT does play an increasingly important role within the government, e.g. for vital infrastructures, and is increasingly often linked to the internet. As a result, we do see CADI as highly relevant for OT. Accordingly, we recommend increasing cooperation with other stakeholders in terms of OT in CADI and to push forward with legislation and regulations surrounding cryptographic inventory within the government. Also refer to ‘Strategische Kennisagenda BZK en VRO 2025-2030’ (Strategic Knowledge Agenda for the Ministry of the Interior Affairs and Kingdom Relations and the Ministry of Housing and Spatial Planning 2025-2030).

In order to concretely compare the performance of various CADI tools, the tools must be tested in a controlled environment. In this respect, we see opportunities for the government bodies involved: they may be able to expand on their knowledge and understanding of this topic by facilitating the establishment of a *ground truth*, which can serve as a baseline for measuring the quality of different CADI products. In addition, they can strengthen their knowledge and leadership position around CADI through smart government tendering around CADI tooling, PQC migration and related services.

Finally, we recommend not to wait for the ideal tool or external best practices around CADI. It is important to start accruing knowledge and expertise around cryptographic assets as soon as possible. To this end, information can be gathered via existing, running tools. In

addition, the government bodies can incentivise (market) parties – through influence and tenders – to bridge the present *gaps*, i.e. the present shortcomings.

Contents

1 Introduction

1.1 Background information

It is important for organisations to have a good overview of all the cryptography in use: which algorithms (and corresponding parameters) are being used, where, and for what purpose? This information can be presented by means of a so-called *cryptographic inventory*. Attentively maintaining a cryptographic inventory can provide multiple benefits to an organisation, including:

- *Preventing data leaks and unauthorised access:* using outdated, obsolete or otherwise unsuitable cryptography may lead to data leaks and/or unauthorised access. By having a good overview of the cryptography used, an organisation can ensure that these risks are minimised. In addition, a good cryptographic inventory can be used to more quickly respond should something go wrong with the cryptography. This results in quicker incident response times, which in turn limits the potential impact of a cryptographic asset issue.
- *Compliance:* organisations use and/or implement policy around the use of cryptography. This often goes hand in hand with a crypto-strategy or policy, partly based on existing legislation and regulations. A cryptographic inventory can be used to demonstrate whether an organisation meets the requirements under policy, legislation and regulations.
- *Planning the migration to PQC:* at present, the first standards for post-quantum cryptography (PQC) have been published: cryptography that can withstand a quantum computer. The migration to this new cryptography is a complex process, requiring an organisation to know which organisational systems and processes are vulnerable to quantum attacks, and to what degree. A cryptographic inventory with the right overview is necessary for this purpose.

Preparing a cryptographic inventory is a measure that can bring the general security level of an organisation to the next level. We also refer to this activity as *'cryptographic asset discovery and inventarisation'*, or 'CADI'.

CADI is a challenging task. Cryptography is incredibly widespread in modern IT infrastructures, across all sorts of systems, libraries and applications. Many organisations have no idea which cryptography is in use and where, nor which cryptography is deployed by external service providers or dependencies. In addition, cryptography is used at several layers: on both hardware and software level, but also in the network layer. Moreover, modern organisations often have legacy systems and mutual dependencies between the various IT and OT assets, further complicating CADI.

1.2 Objective

In this report, we present the insights and findings from the research into the CADI tooling already available. By doing so, we contribute to the decision-making processes organisations have around the use of such tooling. The primary target audience for this report is (stakeholders within) government bodies. The reason for this is the spearheading role the

government has in the field of PQC, as well as the fact that government bodies have a complex and comprehensive, in-house IT infrastructure. Nevertheless, the insights provided will also be relevant to organisations other than in the public sector, especially to large enterprises with applications developed in-house.
The research question is threefold:

1. What do a *minimum viable product* (MVP) and an ideal tool for CADI look like, and what requirements should they meet?
2. What is the current status of the CADI tools already commercially available, and how do they relate to the ideal and the MVP?
3. How can the gap between the MVP and an ideal CADI tool be bridged?

We delve into these questions in the subsequent chapters. In addition, we define concrete follow-up steps and new research questions that arise from this study.

1.3 Creation of this report

This study was financed by CIO Rijk (the Dutch National Chief Information Officer) the National Cybersecurity Centre, and the Ministry of Economic Affairs. The research was conducted by TNO. These parties work using different methods, together and individually, on the preparations and implementation of migrations to quantum-secure cryptography. They also work together in Quantumveilige Cryptografie (QvC) Rijk, the quantum-safe (post-quantum) cryptography programme of the central government.

In collaboration with the parties, a workshop was organised with other Dutch (private) organisations on the use of and need for CADI tooling. These organisations all had a large-scale presence, ranging from IT and/or OT systems, at this workshop.

1.4 Confidentiality and integrity of providers

This report contains confidential information (Appendices 2, 3 and 4) on supplies, only accessible to the government bodies aforementioned. You may have received a version without these appendixes. For questions regarding which specific parties have been consulted, we refer you to the government bodies involved.
We recognise that not all potential providers have been interviewed. This is due to various reasons. In some cases, contact was difficult to establish or could not be established, as a result of which an interview was no longer possible. In other cases, providers indicated that they did not want to be interviewed. In specific cases, we chose not to interview a party because several parties of the same type had already been interviewed.
If we did not interview a party, this is not reflective of the quality of their products or services. The mere fact that a party is not named in this report should not be interpreted as an argument not to purchase products or services from this party.

1.5 Terminology

In general, terminology that is common to the IT industry is used in this report. For the sake of completeness, we name a number of technical terms below.

Cryptographic assets – An umbrella term for all components or elements of a system related to cryptography. This includes items like algorithms or keys, as well as protocols or encrypted data using cryptography.

Cryptographic asset discovery and inventory (CADI) – The identification of cryptographic assets within a pre-determined scope. This encompasses both searching (scanning) for cryptographic assets and the orderly saving/mapping thereof. Due to a lack of standardised terminology, CADI has been introduced as a term by TNO as, in our opinion, it best describes the process. There are a plethora of terms in the market used to describe this phenomenon or with a slightly different nuance, e.g. *cryptographic scanning, crypto-graphic discovery, cryptographic inventory, and cryptographic asset discovery*.

Endpoint – An endpoint is a physical or virtual device that connects to a network, including: (virtual) desktop and laptop computers and other workstations, mobile devices, smartphones, tablets, (virtual) servers, and IoT devices (*Internet of Things*).

Agent – Specifically dedicated software running on an endpoint as a function of other software (of users). In the current context, agents are used to collect information on cryptographic assets (and send this to a central entity).

2 Methodology

Input was collected in different ways for the research into CADI tooling. First, *desk research* was used to explore and first identify the existing literature in this domain. Small-scale brainstorm activities took place with experts on CADI and what the tool could look like. In addition, a workshop was organised with experts and stakeholders from both the private and public sectors, to collect insights on an ideal CADI tool. Finally, interviews were conducted with commercial parties aimed at or interested in CADI. We explain these three methodologies in more detail below.

2.1 Literature review

As a first step in this project, the existing literature on CADI was reviewed by means of *desk research*. In this process, the lack of academic literature on this topic immediately stood out, presumably because CADI has been in focus only relatively recently. In addition, presumably also as a consequence of the fact that this is a new field of interest, there is little consistency in the terminology used: various parties use different terms, sometimes interchangeably. Accordingly, a plethora of terms were used in our desk research (refer to Appendix 5 – Search terms).

Nonetheless, various blog articles can be found on this topic. These articles are often written by CADI tooling providers. These articles do provide insights, but it should be taken into account that the aim and contents may be guided by commercial interests. Most of the information available online on the CADI products is non-technical; it does not address, or rarely addresses, the technical operation or properties of the products. This is also characteristic of low maturity in the CADI solutions domain and their adoption.

Some documents of the U.S. National Institute for Standards and Technology (NIST) are more objective in nature. NIST is already working on the drafting of documents and recommendations around CADI solutions, but this project is still at a relatively early stage[1].

Based on this literature review, we prepared a number of insights, requirements and questions. We also drafted a shortlist of CADI providers with whom interviews may be productive. A similar shortlist was drafted for providers of IT products with a broader scope, for whom the development of or integration with CADI solutions may prove interesting.

2.2 Brainstorming with experts

On 18 September 2024, we organised a brainstorm session with Oscar Koeroo (Ministry of Health, Welfare and Sport), Dion Koeze (National Cybersecurity Centre) and Maaike van Leuken (TNO) on the topic of what an ideal CADI tool would consist of and the questions to put to the CADI providers for the required information.

In order to outline the ideal tool and MVP, it was important to identify what our approach to creating a CADI solution would be. We arrived at a general desirable structure, where the

[1] Migration to Post-Quantum Cryptography | NCCoE and NIST SP 1800-38B in particular

network infrastructure first has to be mapped, after which network detection can be used to identify endpoints of interest in the network. Subsequently, these endpoints can be scanned using agents to map which (crypto)library they call. This would be a good basis for an MVP. In order to then map which cryptographic protocols and primitives are actually called in runtime, dynamic tracing has to be executed via an agent. These layers, with small steps being taken to increase accuracy, form the foundation of the model set out in Section 4.3.2. From his background in operations, Oscar indicated that it would be of much help to him if 80% of the cryptographic assets could be found.

In addition, a short discussion was held on how to best put precise and targeted questions to the CADI providers. To this end, Oscar put forward a basic use case description, based on which we structured the interviews. Oscar also looked over the survey and added two questions to it.

2.3 Workshop

This study contributes to the knowledge of CADI within the Netherlands. The aim in particular is for Dutch government bodies (and, where applicable, private parties) to be able to base their decision-making on the concrete outcomes of this study. A workshop was organised to ensure this connection with the government and industry, which was held on the 23rd of September 2024.

This workshop was aimed at, in association with the relevant stakeholders, identifying the requirements that a CADI tool must meet if it is to be successfully deployed in the various IT infrastructures. The workshop, which took approximately two hours, consisted of two parts. In the first part, a series of questions on the practical requirements for CADI tooling was put forward. These questions/requirements were prepared based on the literature review. The answers of the participants were collected by question, and any noteworthy similarities or differences were discussed. The second part of the workshop consisted of dividing the participants into groups, allowing for a less structured discussion of CADI and the related bottlenecks.

A more extensive report of the workshop is included as an appendix. The outcomes of this workshop have also been used within the project to further fine-tune targeted questions during the interviews with providers.

2.4 Interviews

In the context of this study, a number of companies were interviewed. Two types of companies were interviewed, this to get a picture of the broader ecosystem. Firstly, three companies were contacted that offer tooling aimed specifically at CADI. In addition, five providers of alternative, related cybersecurity tooling were interviewed, to identify whether or not CADI is part of their operations and their views on CADI.

2.4.1 Interviews with CADI providers

Many different CADI tools, developed by commercial entities, are already being marketed. In this study, a number of such providers of CADI tools were approached for an interview, this with the aim of assessing the quality of the tool. Ultimately, three interviews were conducted. These interviews were designed to discuss critical questions derived from the desk research, workshop and brainstorm sessions described previously.

In Chapter 5, we describe the key findings of these interviews. The specific interview questions and the interview summaries can be found in Appendix 3 – CADI provider interview summaries.

2.4.2 Interviews with generic security providers

In addition to providers of standalone CADI products, five interviews were also conducted with market parties that supply alternative cybersecurity tooling. The idea is that such parties may also be interested in expanding their existing product range with CADI tooling. Use could be made of the existing tooling and/or infrastructure in particular. Moreover, many workshop participants (refer to the above) indicated that integration with existing tooling is highly desirable for CADI tooling, this to keep management streamlined.

Accordingly, the aim of these interviews was to assess the degree to which the relevant providers are interested in the integration with CADI tooling or, as the case may be, have the ambition to develop a tool in this domain themselves. Because these parties currently do not have a CADI tool, the interviews were more explorative, searching and constructive in nature.

In Chapter 6, we describe the key findings of these interviews. The interview questions and the interview summaries can be found in Appendix 4 – Generic security provider interview summaries.

3 Technical background information

3.1 Scanner types

The IT infrastructure within an organisation has to be scanned in order to prepare a cryptographic inventory. There are several tools available for this purpose, as listed in this report. However, cryptography is used in various different places in modern IT infrastructures, and not all cryptography use can be detected in the same manner.

This is why CADI tools use several sub-tools in practice, under the hood, that all address a different layer or use a different scanning method. These sub-tools are also referred to as *point solutions*. The output of these point solutions can be aggregated, analysed and, if applicable, presented in a dashboard (refer to Figure 1). In practice, commercial CADI tools may combine one or multiple open-source solutions with their own solutions to achieve a tool with broad coverage.

We list the point solution types in this chapter. It is important to note that several levels of depth are possible: some scans are more accurate than others, but in general such scans require more effort or are more invasive. Also refer to the model in Section 4.3 for this purpose.

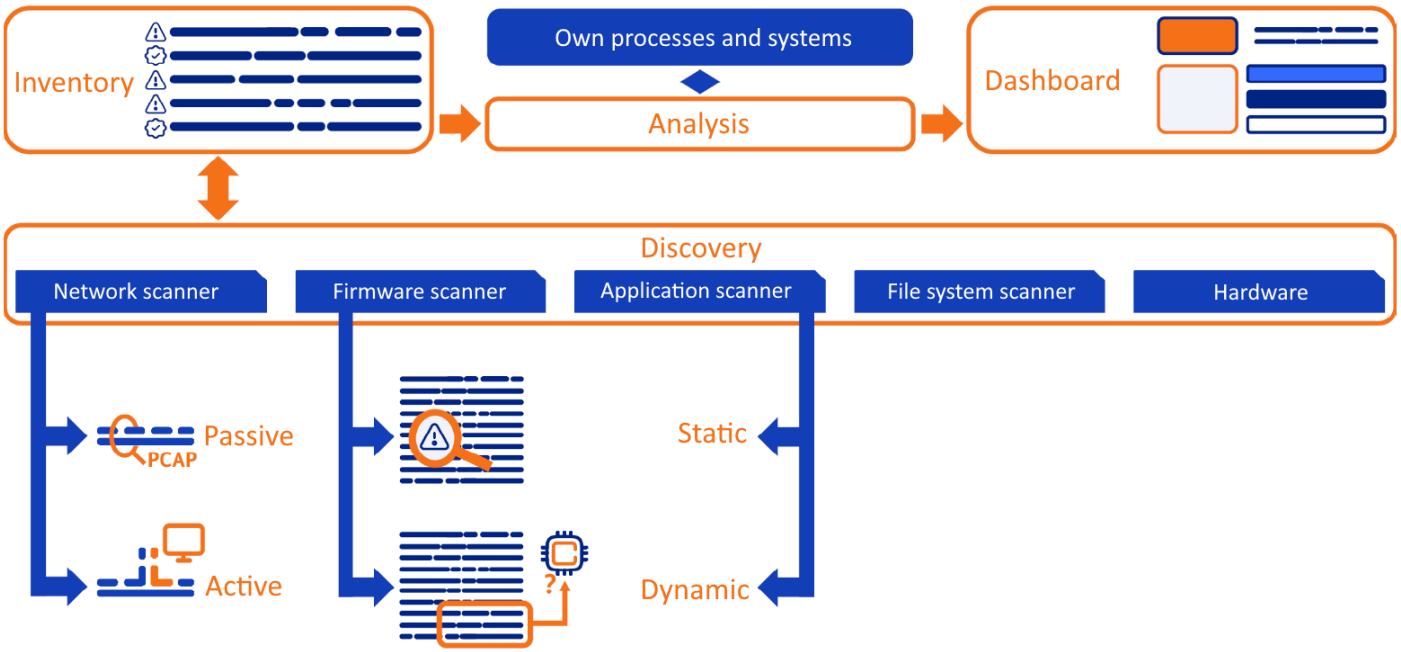

Figure 1. Schematic overview of a CADI tool and its sub-tools in the various layers. The CADI tooling retrieves information from other systems (e.g. cybersecurity management tooling) and can also output information to existing systems (e.g. an incident to an SIEM tool).

3.1.1 Different layers

Based on the desk research, we identified a number of layers, which were subsequently validated during the interviews with CADI providers. These are:

Network

Network scanners target *data in transit*: data shared via a connection between different computers or endpoints. These network connections have to be analysed to identify which cryptography is used and supported. This includes, for instance, TLS and SSH traffic, both within an organisation and outgoing. As most traffic is encrypted, the data contents cannot be analysed for the presence of cryptographic assets.

Applications and libraries

Applications running on an endpoint also use cryptography, e.g. by calling specific cryptographic libraries. In order to identify the cryptography, all applications and libraries in a system also have to be analysed.

Firmware

Cryptography is not just used by applications and libraries running on a system, but also by the firmware of the system itself. For example, cryptography is used for secure updates. This means that firmware also needs to be scanned.

File systems

Whereas network scanners target *data in transit*, file system scanners target *data at rest*. This refers to (sensitive) data saved by the organisation in encrypted form. A cryptographic inventory must identify how these files are encrypted. This requires the scanning of the file types of the organisation, including any databases.

Hardware

For a comprehensive overview of all cryptography, hardware also has to be considered. There are several options for identifying the cryptography in use by the hardware, depending on the hardware type and context.
The relevant data for smart cards (e.g. access cards for premises) can be identified by performing a network endpoint detection first. Subsequently, network analysis can be used to examine the cryptography in use. Strictly speaking, scanning then falls under the network layer, but also touches on the hardware layer.
In addition, hardware may exist in the form of hardware security modules (HSMs) and related technologies that can be deemed a cryptographic co-processor. In that case, an analysis can be performed by scanning the firmware, again putting this under a different branch of scanning.
Ideally, hardware providers should enclose a *cryptographic bill of materials* (CBOM) with their products (refer to Section 4.2.4): this is the most accurate and least invasive process.

3.1.2 Types of scans

Scanners do not only differ in terms of the layer they scan, but also in terms of the way they scan.

Active or passive

Of the scanners aimed at network connections, two broad types can be distinguished.
Passive scanners 'listen in' on the data traffic and analyse the packages in order to identify

the types of cryptography used. The main disadvantage here is that a passive scan identifies the cryptography in use for a particular connection, but not the (possibly insecure) cryptography supported. An active scan can identify this, because it actively attempts to connect to endpoints in order to identify the cryptography types supported. This means that an active scan is more precise but requires more effort: the endpoints are blasted with connection requests.

Static or dynamic

We can see a distinction between passive scans (static) and active scans (dynamic) in the application and library layer as well. The difference between static and dynamic is primarily reflected in the application and library layer. A static scan analyses the existing source code of an application or library and examines the cryptography mentioned or called in it. A static scan does not execute the code: the code itself is analysed only. This is where a dynamic scan differs: by calling (part of) the code, the presence of any vulnerabilities is checked in run-time. This means that a dynamic scan also provides insight into which libraries are actually called, and configuration files are also taken into account. This distinction is also relevant when it comes to firmware, but not relevant when it comes to e.g. file systems, as these are non-executable.

Online or offline

Some layers can be scanned while the device is non-operational, allowing the test to take place independently, without impacting operations. This includes the static analysis of applications, firmware and images (e.g. for *operating systems*). The dynamic analysis of code can also take place offline, provided there is a testing environment (*staging*) with the right configuration files and the right *dependencies*. For the network layer, offline scans are not possible, as it is precisely about the connection.

3.1.3 Use of agents

The use (or non-use) of agents is another dimension in which tools differ from each other. An 'agent' is a bit of software installed on and executed at an endpoint, analysing data from that point; in our case, these data being cryptographic assets. Agents are highly flexible and, by virtue of this, can provide greater depth and accuracy than is possible through non-agent scanning. However, the downside is that agents are somewhat invasive. After all, software is installed on endpoints, which requires more access and effort than a more passive approach. Moreover, the agent requires computation power and memory, potentially impeding operational process continuity.
In practice, the deployment of agents is more of a spectrum than a binary choice. For example, agents may be given different access levels, and temporary agents are also available. In the context of CADI, it is also an option to piggyback on agents already deployed by other cybersecurity products.

3.2 CADI tools

As explained in the previous section, there are various point solutions available, which mutually differ in terms of approach and domain. CADI providers generally offer a product that combines different point solutions. The output of these point solutions is then combined to arrive at an inventory that covers several layers. Some of the point solutions can be procured individually, as open-source solution, whereas others have been developed by the CADI providers themselves.

Moreover, some CADI providers present the combined findings of the point solutions in the form of a schematic overview. If a CADI provider combines a large number of point solutions to obtain an overarching inventory and presents this schematically, we refer to this as a *'full-stack solution'*.

3.3 Generic security tools

Generic security products, such as those of Generic Security Provider D and Generic Security Provider B, see widespread use to ensure organisational security. This includes aspects like scanning the business network to detect and block connections with malicious IP addresses, as well as keeping track of all IT products, services and other assets purchased. Such tools support the keeping of records of licences required, in turn preventing fines and unexpected costs during audits. Many of these products have grown into multifunctional platforms over the years, embedding multiple tasks within a single product.
All large organisations use one or multiple cybersecurity products. Accordingly, being able to integrate CADI tooling with such products is a logical step, especially if there is overlap in technical features with the existing product. Section 5.1 provides a case example. We have spoken to several generic security providers to this end in this study, this in addition to some CADI providers.
Below, we provide an outline of the different types of common security tools and their mutual connections. The overlap with CADI functionalities is described in Section 6.2.

Endpoint detection and response (EDR/XDR) monitors for threats using agents on the endpoints, e.g. mobile devices and IoT devices. *Extended detection and response* (XDR) expands on this by monitoring network behaviour on endpoints and user behaviour.

IT asset management (ITAM) is used for IT asset lifecycle management. It covers information about the types of devices in use, the MAC and IP addresses, the version numbers, serial numbers, licences allocated, and access.

Certificate lifecycle management (CLM) is used to keep a record of the digital certificates used within an organisation and to manage these.

A **configuration management database (CMDB)** records information on the different hardware and software components of an IT system and how these are connected. This helps in the effective management and maintenance of such components. A CMDB is ordinarily linked to different security tools, e.g. ITAM tooling.

Vulnerability scanning tools scan IT systems for security issues, e.g. missing updates and incorrect configurations, to identify all potential threats. These then generate an alert, allowing for these to be solved.

Security operations centres (SOCs) monitor the IT environment for attacks and incidents, and respond to them. SOC analysts receive alerts via the platform, generated via other security tooling such as **intrusion detection systems (IDS), vulnerability scanners** and **security information & event management (SIEM)** systems.

IT service management refers to a process and the corresponding tooling for handling service tickets. This also covers other disciplines, e.g. application management, technical management, and other management tasks with the associated tooling. This has some overlap with ITAM.

The range of such tools available is highly varied and open-source. Resultingly, the shortlist of Section 6.1. is based on the tools already in use at various ministries or which were known to TNO and, as such, showed an overlap with the intended purpose.

3.4 IT and OT

This study has a broad scope in the sense that both *operational technology* (OT) and *information technology* (IT) are covered. Contrary to IT, OT is primarily aimed at physical processes within the organisation and their management.

OT systems are generally extraordinarily limited in terms of their computational power and memory. The management of physical processes generally does not require as much computational power as some computations within the domain of IT. Endpoints in an OT environment have a specific purpose, with corresponding (low) computational power, and the completion of that purpose may not be influenced. Combined with the intellectual property rights of the developer to the software and hardware, this makes the use of agents difficult if not impossible.

In addition, OT environments consist of a mix of modern and, predominantly, *legacy* systems, each with their own communication protocols, APIs and underlying cryptography. This means that if it is possible to use agents at all, each product type would require new code to be able to communicate with it and retrieve the correct information. For these reasons, the active detection of cryptographic assets in OT environments is (nigh) unfeasible. Another difference between OT and IT environments is their security. OT security significantly lags behind IT security, precisely because of the aforementioned differences (legacy systems and limited modifiability of systems). In addition, the availability of OT environments is more important than that of IT environments, as a result of which availability has the highest priority, with integrity and confidentiality only being next in line. This means that there are fewer security tools in use, e.g. network scanners and vulnerability scanners, compared to IT environments. The network architecture also differs. In IT environments, the architecture is often segmented (*air-gapped*), whereas OT networks are often not segmented.
The new NIS2 directive[2] attempts to bridge this gap in OT security by requiring that network and information systems are proactively scanned for vulnerabilities and assets inventoried.

[2] Refer to the NIS2 directive, L_2022333NL.01008001.xml.

4 Ideal tool and MVP

In this chapter, we describe the functional and practical requirements for a so-called *minimum viable product* (MVP) and for an ideal CADI tool. In particular, we provide a list with potential features of CADI tooling identified by means of desk research, the workshop, and the interviews with CADI providers. We explain by feature what the required details of that feature would be for an MVP and what the requirement would look like for an ideal solution.

In Section 4.3, the features and their required details for an MVP and an ideal tool are organised and summarised in a table. In this section, we also introduce a model showing the individual levels of CADI tooling, set off against increasing accuracy and effort (Figure 2).

In Chapter 5, we look at CADI tools on the market and how they compare to the MVP and the ideal tool.

4.1 Defining the MVP and ideal tool

In Section 4.2, we describe the existing features of CADI tools and which requirements an MVP and an ideal CADI tool must meet. First, we specify what we mean by 'MVP' and 'ideal tool'.

4.1.1 Minimum viable product (MVP)

A *minimum viable product* (MVP) is part of the strategy for launching a new product. The idea behind an MVP is that the product itself is not yet perfect, but 'viable' as a standalone product. For users, an MVP is useful enough to warrant its purchase. For providers, an MVP is an opportunity to release an (alpha or beta) version without the definitive product with all its features and options being ready.

In the context of CADI, we see the MVP as a product that can be deployed by an organisation to get a first impression of (part of) the cryptography in use within the organisation, without the insights obtained having to be re-obtained at a later time. The idea is to enable the organisation to take the first actions on the basis of the MVP scan outcomes, thus strengthening management support for large-scale implementation of CADI tooling. As such, a good MVP is not specific in terms of which 'layer' (refer to Figure 1), but does align well with the later stages of PQC migration and is simple to migrate/embed in a later *full-stack* solution.

In the workshop (refer to 2.3 and Appendix 1), various stakeholders indicated that it would be good if they could start with the inventory, even if this would not yet result in a comprehensive overview. The MVP is useful to this end; it removes the chicken and egg problem for CADI tooling integration.

4.1.2 Ideal tool

We define the 'ideal CADI tool' as a tool that performs a cryptographic inventory *as well as realistically possible*. The ideal tool is not a Platonic ideal that can only exist in a perfect world; we consciously choose to define the ideal tool as the best tool given the spectrum of what is technically feasible. The reason for this is that we will be comparing a number of existing CADI tools to this ideal (and the MVP) in Chapter 5. Such a comparison is less useful if the ideal is not realistic.

Please note: the details of an MVP and of an ideal tool strongly depend on the use case. The concrete specifics may depend on the operational setting, the business processes running, availability requirements, and the risk profile (which dictates the desired result accuracy). This is why we have chosen to differentiate between IT and OT environments, where possible, with the knowledge that further distinctions have to be made during the specification of a concrete use case.

4.2 Features and requirements

Each of the following sections describes a different feature of CADI tooling. The required specifics of a feature, MVP and ideal tool are also explained for each feature.

4.2.1 Scanning frequency

The scanning frequency of a tool refers to the number of times a scan is performed. The larger the scanning frequency, the more accurate the cryptographic inventory, i.e. the earlier any abnormalities or vulnerabilities are identified.

Please note: the findings set out below are only a guideline, deviation is possible in some cases. For example, the frequency can be temporarily scaled up if major changes are implemented in the system. In addition, a full system scan may not be needed in every single case: as described elsewhere, CADI tooling consists of several sub-scans, of which some are necessary more often than others. Refer to Section 3.1 and Figure 1 in particular for more information on the scan types.

An ideal solution in an IT environment scans continuously, both actively and passively, so that the cryptographic inventory is always up to date. Any vulnerabilities are then immediately identified and can be remedied at short notice. Things are different for OT: active scans are currently not feasible in this regard (and often not desired with an eye to security) and are therefore not required. During the workshop, stakeholders also indicated that continuous scanning using passive scans is similarly not realistic. After all, a scan uses computational power and access, both of which are limited in OT. A scan could potentially interfere with the correct functioning of the environment. In addition, OT environments are in general more difficult to access, which complicates performing scans. On the other hand, OT is less frequently updated than IT, which means a cryptographic inventory has to be updated less frequently. Ideally, we suggest a passive daily scan for OT environments. Where a daily scan is not feasible due to physical or operational restrictions, 'daily' should be read as 'as often as feasible'. This can be done at a time that the normal system processes experience low loads, e.g. at night for a *building management system*.

For an MVP in IT, continuous passive scanning is still a requirement. For active scanning, we request a minimum scan frequency of once per week. Although a higher frequency is better, scans take up computational power and bandwidth, which may interfere with other

(business) processes. At frequencies less than once per week, vulnerabilities can remain undetected for a number of weeks, which is too great of a risk. In OT, we suggest an MVP with a minimum passive scanning frequency of once per month and, again, active scanning remains outside the scope.

4.2.2 Location (on-premise/remote)

In this section, we refer to the location where the tool is deployed or running. In a broad sense, there are two types. Tooling can be installed directly on the systems of an organisation and run there. We call this *on-premise* tooling. The other option is running the tool *remotely*, e.g. via a SaaS-like (*Software as a Service*) structure.

For both the MVP and an ideal solution, we require the **option** of on-premise deployment of the tool. This is because remote execution requires a network connection with the provider of the tool, which results in security risks. Even though some CADI providers do offer cloud-based versions of their tool, or intend to do so in the future, this is not relevant to the target audience of this study. The authors of this report find that CADI is too sensitive and intrusive for cloud deployment. Moreover, stakeholders in the workshop indicated that they want to retain a great degree of control over the deployment of tooling; not a single party present indicated to accept data sharing with providers.

This means that there has to be the option of **not providing** the CADI provider with **insight** into the scan results. Otherwise, the provider becomes aware of the use of any vulnerable cryptography in an organisation. In that case, the absence of communication from on-premise systems to systems outside the network also has to be ensured.

4.2.3 Agent use

The deployment of agents results in a high degree of flexibility and accuracy, as the agents run autonomously within the system and can actively gather data. Without agents, certain types of data cannot be retrieved, e.g. the cryptographic modules called within a specific software. A downside to this is that the deployment of agents requires a great degree of access and some computational power. The use of agents is common for general, broad cybersecurity tooling.

An ideal tool will require agent deployment in order to reach a degree of accuracy and flexibility that is as high as possible. The need for agents to ensure sufficient depth was recognised by experts (outside the direct project team) of TNO, during the brainstorm session with experts (refer to 2.2), and by various CADI providers that offer agents. Ideally, agents are installed and run in a smart manner, so that the impact on other processes is minimised. This can be done by having the agents piggyback on existing agents within the cybersecurity tooling already in use.

For the same reason, an MVP will generally also make use of agents. Conversely, in the case of an MVP for OT, the deployment of agents is not feasible for OT from the perspective of computational power and even not desirable from the perspective of safety, as agents may disrupt the availability of vital processes.

Finally, we note that we refer to the *option of* deploying agents. With the final implementation of the tool, choices can be made on restricting agent deployment to a specific sub-system or a specific scope.

4.2.4 Importing CBOMs

In addition to scanning for cryptographic assets, a CADI tool could also provide insights derived from existing knowledge on a system. For example, CADI tools have been marketed that can import existing overviews on cryptography, such as cryptographic bills of materials (CBOMs).

For both an ideal solution and an MVP, we argue that importing third-party CBOMs has to be supported. This argument is primarily based on the current researchers. Importing external CBOMs can increase the accuracy of a cryptographic inventory with relatively minimal effort. Some products, e.g. Liboqs by Open Quantum Safe[3], provide a CBOM with their code. Being able to import such a CBOM is an accessible and highly useful feature that we consequently require for both an MVP and the ideal tool.

4.2.5 Logs

The most important outcomes of a scan will be presented clearly and in an organised manner by most tools. In addition to these important outcomes, most scans will still gather much more data, e.g. interim results, errors and other seemingly less prominent information. By '*logging*', we mean writing (i.e. not deleting) this information to a separate file (a log).

For both the ideal solution and an MVO, saving or writing *all* data collected to logs is a non-negotiable requirement. During the workshop, all stakeholders indicated to find logging highly important. In addition, carefully writing to logs is the standard at present for nearly all existing cybersecurity tooling; as such, it makes sense to place the same requirement on CADI tooling.

4.2.6 Assets within the scope

There are different types of cryptographic assets that may be present in a system. These include cryptographic keys, which may be symmetrical or asymmetrical. In addition, you can scan for different types of cryptographic primitives, such as key exchange algorithms, digital signature, symmetric primitives, and hash functions. There are several algorithms available for each primitive. Finally, it is worth noting the protocols (TLS, SSH, etc.) and cryptography used.

For both an ideal tool and an MVP, we require that all cryptographic assets listed above can be detected, for both modern and legacy cryptography. After all, this is a necessary element to provide a correct and usable cryptographic inventory. For the ideal tool, we furthermore require that these assets can also be identified for newer, quantum-secure cryptography. as After all, it is interesting for organisations mature in preparing inventories (and for whom an MVP is not relevant) to know where PCQ is already being used.

In addition, the ideal CADI tool provides context for the cryptographic assets discovered: wherever possible, the department that owns the asset and the business process to which it relates is indicated, by asset. We do note that this requires integration in a context broader than simple CADI tooling, e.g. broader asset management, organisational structure and/or architecture.

[3] liboqs/docs/cbom.json at main · open-quantum-safe/liboqs

During the workshop, this requirement was not prominent across the board for all stakeholders. Nevertheless, we believe this to be a very important aspect of a healthy inventory. In addition, CADI Provider B and CADI Provider C indicated that precisely this contextual information is highly important, both to them and to their clients.

4.2.7 Accuracy

By 'accuracy', we mean the degree of completeness of the overview resulting from a scan. In other words: how much of the cryptography present in an organisation/system can be found using the tool? We do note that the precision of a tool cannot be verified in practice: after all, the actual calculation thereof requires knowledge of the total cryptography present. This is why accuracy is generally assessed based on estimates and test environment results.

For an ideal tool, we require 85% accuracy within IT. In the interview with CADI Provider B, our contact referred to a major Wall Street bank, one of their clients. This bank indicated to strive for 85% accuracy. In our workshop as well, participants indicated that 80-90% tool accuracy is sufficient. Work can be done manually to further increase accuracy. Scanning is more complex for OT; we lower the threshold accordingly to a minimum of 60%. This gives a good overview of the things at play, without the overview being exhaustive.
In terms of accuracy, an MVP does not have to perform as well. The reasoning behind this is that an MVP is less accurate but also requires less effort. An MVP can be used to make a first estimate of the scope of cryptography use within an organisation, which is highly useful as standalone feature. Accordingly, we require a level of accuracy of 60% within IT and 30% within OT.

As with scanning frequency, the numbers above have to be taken as guidelines. The need and feasibility of a specific level of accuracy may differ by application. Moreover, CADI tools generally consist of a number of sub-tools, and the (expected) level of accuracy may differ per sub-tool.

4.2.8 Integration

Many organisations already use all sorts of tooling to manage their IT environment and keep it secure. It would be highly valuable for CADI tooling use if it is able to be integrated with such pre-existing tooling. This may enable CADI tooling to import information on the system or even on cryptographic assets. Moreover, CADI agents may be able to piggyback on existing infrastructure, which significantly simplifies their deployment. Conversely, existing tooling may capitalise on the output of the CADI tool. CADI tool output may be exported to a different tool.

For the ideal CADI tool, we expect it to integrate with the major or well-known other security tooling: there are ready-made modules (API calls) that enable easy linking. Moreover, the ideal provider of CADI tooling provides custom services to enable the integration with other, lesser-known tooling. We base this requirement on two insights. Firstly, many workshop participants indicated that the deployment of new tooling is not an issue, provided it exports to existing tooling already in use. Secondly, on the basis of our meetings with the CADI providers, we concluded that integration is also important on their end: not just for exporting results, but also for piggybacking on existing infrastructure, e.g. in less intrusive agent deployment.

An MVP does not have to provide ready-made integrations. Nevertheless, integration with existing tooling is important enough for the tool to take this into account to a certain degree. The provider advises on how the integration with existing tooling could be implemented. In addition, the link to several systems can be made, because the results of the CADI tool **have** to be easily exportable.

4.3 Overview & effort-accuracy

The various features and requirements around CADI tooling were described above. This section summarises the findings in a table. We also introduce a model in which we plot the potential (sub-)functionalities of a CADI tool against an increasing degree of effort and accuracy.

4.3.1 Overview of features and requirements

The table below shows the above in an orderly manner: the requirements identified and their specifics for an MVP or, as the case may be, an ideal solution.

Requirement	Brief description	MVP	Ideal solution
Scanning frequency	How often does the scan take place?	Monthly passive (OT); continuously passive and weekly active (IT).	Daily passive (OT); continuously passive and active (IT).
Location	Where does the scan run (on-premise or remote)?	Option of on-premise.	Option of on-premise.
Agents	Can agents be deployed and used?	No (OT), yes (IT).	Yes.*
Importing CBOMs	Can provider CBOMs be imported?	Yes.	Yes.
Logs	What data is logged?	All data surrounding performing the scan, errors and results.	All data surrounding performing the scan, errors and results.
Scope	Which cryptographic assets can be found?	Key (materials), crypto-primitives and protocol.	Same as for MVP, but also for PQC. Provides context on the assets (owner, process).
Accuracy	How many cryptographic assets can be found?	30% (OT), 60% (IT).	60% (OT), 85% (IT).
Integration	What is the degree of integration with pre-existing/present tooling?	Not ready-made. With advice.	Ready-made for use with major, well-known products. Customisation for other products.

Table 1. Overview of requirements for an MVP and ideal solution.

** Agents are a relatively new concept when it comes to use at OT endpoints. In general, agents are not placed on OT systems out of fear of a negative impact on system uptime and operational performance. Nevertheless, due to mounting cybersecurity risks for OT endpoints (infected maintenance hardware, controller errors, malicious employees, stolen authentication data, etc.) and this is a particularly interesting target for advanced persistent threats (APTs), the need for endpoint solutions has been increasing similarly to IT. Although this change is partly present in new OT, making agents an option, this is not an option in the larger share of existing OT.*

4.3.2 The effort-accuracy model

A general principle applies for the commissioning of CADI tooling: the more accurate the results have to be, the greater the effort required. Here, 'accuracy' is defined as in Section 4.2.7: the percentage of cryptographic assets found. 'Effort' refers to the combination of the time, funds and manpower needed, as well as the impact of the scan on the system being examined.

We concretised the low effort/low accuracy to high effort/high accuracy spectrum in Figure 2. The upper steps refer to measures or sub-tools of a CADI tool that are very feasible or easily deployable, but have limited accuracy. The lower steps of the ladder can be deployed for greater accuracy; these do require more effort.

The MVP for OT consists of (1), (2) and (3). The first two steps are simple to execute and do not require any new tooling nor computational power at endpoints. However, there is a likelihood that this results in extremely little information. As such, we included passive scanning (3) network traffic and part of the MVP. This requires the deployment of a new tool, but the impact of operational process continuity is low, if any. Passive scanning should result in information on which endpoints are sending messages and which protocols are used.
In addition to (1), (2) and (3), **the ideal tool for OT** also includes (6) and (9). We are of the opinion that actively scanning online systems in OT environments – using agents – is not feasible. Offline scanning binaries and firmware does not impact operations processes but does require specialised tools, where legacy products may cause bottlenecks. Multiple products of the same type only need to be analysed once (provided their configurations are identical). Statically analysing binaries outputs the crypto-systems that can potentially be called, whereas dynamically scanning firmware provides insight in the crypto-systems actually being called.

The MVP for IT consists of (1), (2), (3), (4), (5) and (7). As for OT, (1) and (2) are simple to implement and already provide a lot of insight. Step (3) will similarly not require much effort, as (major) IT companies already deploy network scanners. Placing the sensors at the right locations remains a challenge, this due to the network segmentation present in major IT companies for the sake of security. Contrary to OT, we require the option of deploying agents for an MVP in IT. This can be done by introducing new agents (4) (possibly by repurposing existing probes or agents in edited form) but a better option would be by reusing agents and integrating these with existing EDR tooling (5) (also refer to Section 3.3). In terms of application and library scanning, we require an MVP in IT to not have active scans but passive scans (7), as these are more easily feasible.

The ideal tool for IT also includes (6) and (8) in addition to the foregoing. As noted for OT, offline scanning of binaries and firmware does not impact operational processes but does require specialised tools (6). Specialised tools are also required for the dynamic tracing of applications and libraries; such tools require a great amount of random access memory. This may impact operational processes and doing this continuously is likely not feasible. Statically scanning firmware (9) requires a great deal of effort. How big the information gap to be bridged by this form of scanning actually is, will have to be assessed after performing the first eight steps of the model. As such, this is currently not described as part of the ideal tool for IT.

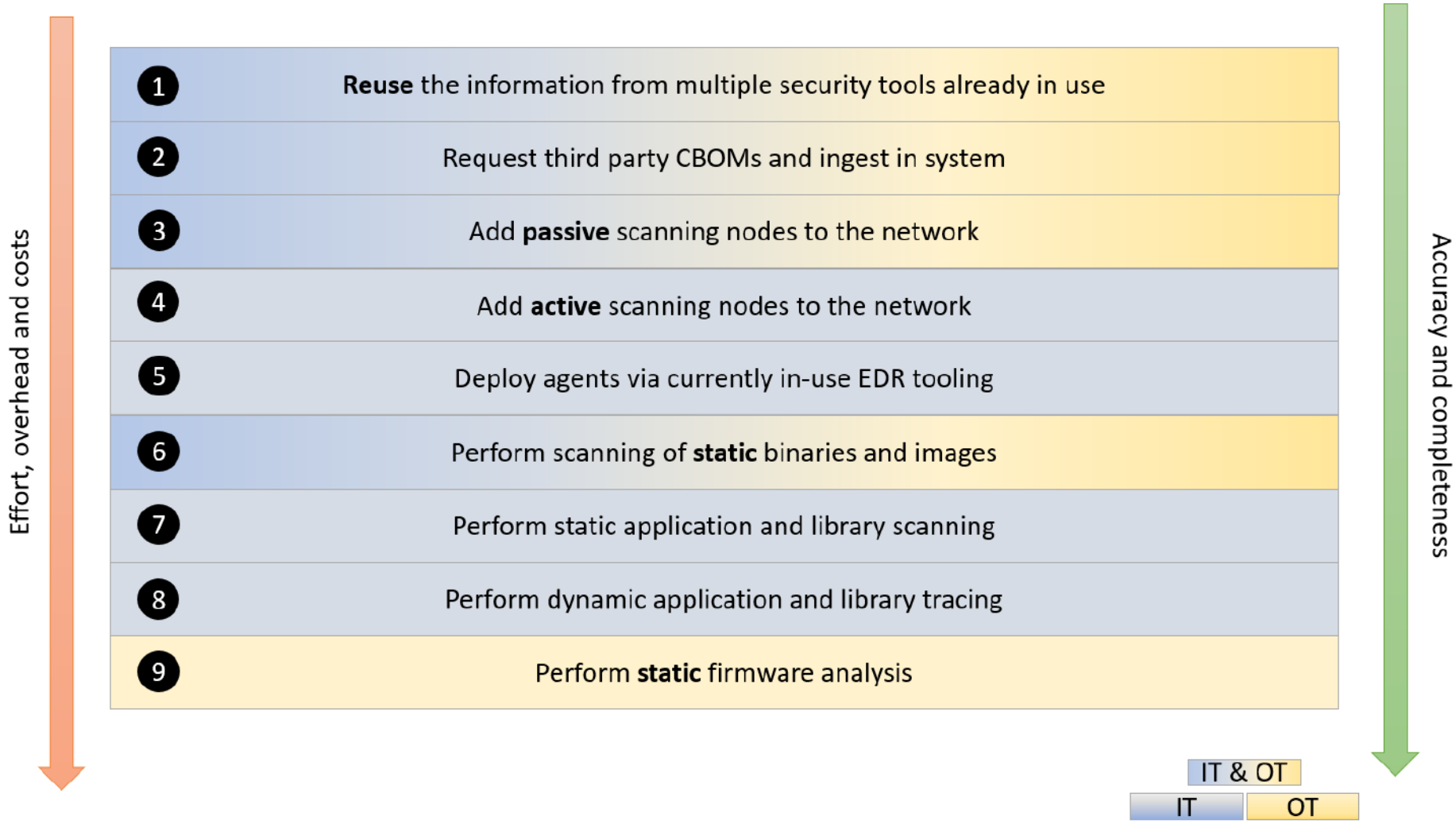

Figure 2. The different levels of CADI functionalities. The higher the functionality number, the higher the resulting accuracy as well as the effort required to achieve it.

5 Commercial CADI tool

Even though cryptography use is extensive and highly widespread, the domain of commercial CADI tooling is relatively new: only in 2013 and 2014 were the first companies specialised in this area founded. In this chapter, we name a number of commercial CADI tools and their features.

The chapter is structured as follows: Section 5.1 provides a brief overview of the current landscape of CADI tooling providers and service providers. This is followed by a shortlist of the CADI tools examined, in Section 5.2. Then, we discuss the mapping of the solutions for the MVP and ideal CADI tool in Section 5.3. We conclude with the key findings that follow from our study and the interviews, in Section 5.4. We link the MVP, the ideal, the CADI providers and the other providers interviewed at the end of this chapter, in table format.

5.1 Market landscape

The description of the market landscape is built based on existing knowledge of TNO, unless otherwise indicated.

The market landscape consists of the known CADI providers and generic security providers, as mentioned here. In addition, it consists of the organisations that adopt, integrate and maintain these solutions.

5.1.1 Adoption by service providers

The interest for the PQC migration manual[4] and the presentations on this topic have shown that the adoption of services around CADI tooling is on the rise. The interested parties include end users as well as consultancies and other service providers already familiar with IT asset management tooling integrations at end clients.

Most of the CADI providers interviewed indicate that the consultancy services around setting up and maintaining their CADI tool at the end user is part of their profit model. Only CADI Provider A indicates that it solely wants to be a *software-as-a-service* company. Providers who do not offer consultancy services will have to either make the set-up and maintenance process highly simple or ensure that the documentation is so comprehensive that end-users can do this themselves; alternatively, a service provider can pick up this slack. Service providers have the knowledge and experience needed for large-scale implementations in IT landscapes, as well as the implementation in risk management strategies present for the client. The latter because software and hardware asset management is a pre-existing market for such service providers. In general, some organisations are able and willing to perform PQC migrations themselves, while others would rather outsource this to a service provider. Consultancies and the generic security providers referred to are seemingly preparing for this, or intend to do so. This is evidenced by the interviews (refer to Appendix 4 – Generic security provider interview summaries) and their continuing interest to exchange ideas with TNO on this matter.

[4] Vernieuwd handboek voor quantumveilige cryptografie (the New Manual of Post-quantum Cryptography).

5.1.2 Mergers, acquisitions, or new developments

We expect that many of the start-ups working on CADI tooling will be acquired by larger companies[5]. CADI Provider B indicated that this has already happened for them. We expect that, in a broad sense, there are two types of organisations procuring CADI tools to strengthen their product range. Firstly, the generic security providers in the IT domain see CADI as a natural extension to their product range as soon as the market continues developing. Secondly, there are organisations with an existing client base to whom (a specific form of) CADI is highly relevant, e.g. within the OT domain.

It is also likely that existing providers of generic security tooling will develop CADI functionalities themselves, as soon as the market for CADI tooling grows. Two of the generic security providers (A and D) are already moving in this direction. Because the larger generic security providers already have a large existing client base, they can grow their market share via *upselling* relatively quickly and easily. The downside is that they do not have the knowledge and experience in this field that, for instance, CADI Provider B and CADI Provider C already have at this time.

5.1.3 Expected developments

We expect that the distinction between existing CADI solutions and the expansion of existing solutions will primarily be made by the service providers.

If the service providers are not assessed on accuracy, or if they are not held accountable as a service provider for the actual migration of an asset to a PQC variant, they will choose a solution that is easy to integrate and cost-effective. This may be a pre-existing solution enhanced with CADI features. The latter because this is the most profitable option for them. However, if a service provider is assessed on accuracy, or if they will be performing the migration themselves, they will be incentivised to invest more in their CADI tool to achieve higher levels of maturity and accuracy. This ensures that they can continue developing more easily in the future, increasing their profitability. As such, an end customer with an end issue directly influences the CADI tooling selection by the service providers.

We expect that this will influence the course of – existing or new – CADI tooling development over the coming five years.

5.2 Shortlist drafting

As a first step, we searched the internet and our network for companies active in this field. The fact that CADI tooling is known by different terms (e.g. *crypto(graphy) scanning, cryptographic inventory, cryptographic discovery, cryptographic asset discovery*) was taken into account in this regard, as well as variations and combinations of such terms (refer to Appendix 5 – Search terms). A list of companies was prepared in this manner, containing mostly start-ups. Information was very limited on a large number of these companies: some had no website (the tool only being referred to in another document), others had a fairly basic website, and it was often not clear what the provider offered exactly: is there a working product, or is it an advertisement for a tool still under development?

[5] In the period between first publication and English translation, this has already occurred.

This is why compiling a 'shortlist' was the method of choice: commercial CADI tools that we deem sufficiently mature to warrant further investigation via an interview. In addition, we also included CADI Provider A, <>.

These parties were approached in different ways. We approached an employee at CADI Provider B via a TNO colleague, who referred us internally to the right point of contact for the CADI product. We approached CADI Provider C via LinkedIn, as the contact form did not result in a (timely) response. CADI Provider A was approached via email, with the email addresses being listed on the website. CADI Provider F was also approached via email, but contact failed after a first (positive) introduction via email at the start of June.

5.3 Mapping of existing solutions for the MVP and ideal tool

Chapter 4 describes the requirements a CADI tool must meet to become a minimum viable product (MVP) and the requirements we impose on an ideal CADI tool. The table below compares the CADI products of CADI Supplier A, CADI Supplier B and CADI Supplier C with these requirements.

For each requirement, the extent to which each of the products meet the requirements of the MVP or the ideal tool is indicated:

- a green highlight means that the product meets the ideal for this requirement;
- a yellow marking means that the product meets the MVP for this requirement, but not the ideal;
- a red highlight means that the product does not meet the MVP for this requirement (and also not the ideal);
- a blue highlight means that it is not clear or unknown to what extent the product meets the requirement.

Please note: because all three parties indicated during the interviews to have no experience in OT, we chose to compare the CADI tools with the MVP and ideal tool for an IT setting in the table below.

5.4 Key findings

The key findings around CADI tooling are summarised below. These findings include insights from the mapping of the various tools compared to the ideal tool and the MVP, as well as from the interviews with these CADI providers.

The findings in the remainder of this chapter are based on a number of different sources:

- Interviews with providers, which at times have been several meetings with the same party, on the basis of a previously agreed survey.
- Follow-up questions (in follow-up interviews and via email) based on functional tooling capacities of other providers (without naming the provider).
- Consultation with own TNO experts on similar tooling and its challenges, including in order to interpret some claims in interviews in terms of their feasibility.
- (Online) desk research

Requirement	MVP (IT)	Ideal solution (IT)	CADI Provider A	CADI Provider B	CADI Provider C
Scanning frequency	Weekly	Continuously	Not discussed	Can be full-spectrum. Weekly updates are common for clients.	They suggest quarterly. Can be monthly or even daily.
Location	On-premise	On-premise	On-premise	On-premise (or via cloud)	On-premise
Agents	Yes	Yes	No	Multiple options available	Multiple options available
Importing CBOMs	Yes	Yes	No	Yes	Not discussed
Logs	All information surrounding scan performance, errors and results	All information surrounding scan performance, errors and results	All information surrounding scan performance, errors and results	All information surrounding scan performance, errors and results	All information surrounding scan performance, errors and results
Scope	Key (materials), crypto-primitives and protocols	Same as for MVP, but including PQC. Provides context for the assets (owner, process)	Key (materials), crypto-primitives and protocols.	Key (materials), crypto-primitives and protocols. Also attention to providing context for assets (e.g. cross-references). Finding PQC was not discussed.	Key (materials), crypto-primitives and protocols. Also PQC.
Accuracy	60%	85%	CADI Provider A only analyses network traffic, but claims to be very accurate in this.	No clear data, as there is no ground truth.	No clear data, as there is no ground truth.
Integration	Not ready-made but with advice.	Ready-made for major, well-known products. Customised work for other products.	No integrations at this time, but with a plan for an API to a CMDB.	Broad integration with existing tools.	Broad integration with existing tools. This is one of their strong suits, according to them.

Table 2. Relationship between tools of the parties interviewed, MVP and ideal. Refer to 5.3.

5.4.1 OT environments

OT environments show a high discrepancy between the ideal and the existing solutions. This is due to the challenges described in Section 3.4. As previously mentioned, all three CADI providers reported to have no experience deploying the tool in the OT domain. CADI Provider B also indicated that OT is not part of their objectives: according to the contact, such applications are too niche to warrant the investment. CADI Provider C and CADI Provider A were open to the idea of exploring OT domain applications, but had no concrete plans for doing so at the time of the interview.
This requires a specifically dedicated party to tackle this issue. These interviews led us to conclude that firmware analysis would be the most suitable option. At this point, we identified only one tool that could analyse the firmware in OT systems, i.e. that of Generic Security Provider E. This does require thorough mapping of endpoints.

5.4.2 Availability of third-party CBOMs

Scanning third-party libraries or software is highly complex and requires insight into the code (*white box*). It would be a great boon if software providers were to enclose a CBOM with each of their products, listing the cryptography used in the product. In this way, organisations can include the CBOM in their cryptographic inventory, removing the need to scan each product (insofar that is at all possible).
We recommend contributing to legislation and recommendations, to steer the market in this direction, perhaps at a European-wide level. Many products from the U.S. may do so faster, as the U.S. is a pioneer in PQC legislation.

5.4.3 Absence of a *ground truth* for accuracy

Multiple parties, and CADI Provider B and CADI Provider C in particular, indicated that estimating the accuracy of their solution is a difficult feat. This is due to the absence of a *ground truth*: you do not know which cryptography is used in a system in advance, meaning you are unable to compare the cryptography identified by your tool percentage-wise.
Both parties indicate to be interested in a test. A test environment could be set up in which the cryptography used is tracked manually during set-up and labelled. This creates a ground truth. Subsequently, the tools can be executed on the system. The findings can be analysed by level and scan type and, resultingly, the accuracy of the CADI tool can be determined. This could be an objective measure for CADI tooling evaluation.

5.4.4 Costs

Generally speaking, commercial CADI tools are highly expensive. In response, several companies make use of various pricing models, with the price depending on factors such as the number of endpoints, the number of applications, the number and type of scanners, the number of integrations with other tools, and so on and so forth. For larger businesses, the costs range up to hundreds of thousands or even millions of euros annually. This is a difficult or even unrealistic investment for many organisations.

5.4.5 Identifying PQC

To our knowledge, only the tool of CADI Provider C is able to detect the (new) PQC algorithms. This is arguably not the top priority at this time, but will become increasingly important over the coming years, in order to be able to estimate the degree of quantum safety of the company at this time and the PQC algorithms in use and their location. Even if algorithms such as SIKE have already been implemented but turn out to be vulnerable, detection and migration can take place.

5.4.6 Agents and their potential use

Not all solutions deploy agents. This is because the use of agents is often seen as undesirable. This sentiment was echoed during the workshop. Moreover, this was common feedback from clients to CADI Provider B and CADI Provider C. Accordingly, they chose to make three formats available:

1. **No agents**, but it is worth noting that this goes hand in hand with a decrease in quality of the substantive information retrieved, as some data cannot be retrieved without the use of agents.
2. ***Dissolving* or *piggy-backing* agents**, that a client can place in agents of e.g. a security product already in use. This method does not require a new strategy or implementation for additional agent deployment. This lowers the risk of issues involving agents and computational power, while also allowing for the minimisation of memory use.
3. **Own, new agents**, which a client can install at their own discretion.

Option 2 seems the best choice to TNO, as obtaining a comprehensive cryptographic inventory without the use of agents is not realistic. On the other hand, agents with full access privileges are highly invasive, which is generally undesirable to organisations. The costs and benefits will have to be estimated for each use case and organisation.

Table 3. Overview of the layers and types of scans for MVPs, ideal tools, CADI solutions and the options for cyber security solutions to scan at this level.

		MVP (IT)	Ideal (IT)	MVP (OT)	Ideal (OT)	CADI Provider A	CADI Provider B	CADI Provider C	Generic Security Provider B	Generic Security Provider C	Generic Security Provider D	Generic Security Provider E
Network	Passive	X	X	X		X	X	X	X			
	Active	X	X			X	X	X	X		X	
Applications & libraries	Static	X	X				X	X	X	X	X	
	Dynamic		X				X					
Firmware	Static		?		X			X			X	X
	Dynamic		?									
File system	Static	X	X		X		X	X				

6 Cyber security solutions

As set out in Section 3.2.2, generic cyber security solutions can be expanded with CADI features. Section 6.1 describes the process of arriving at the interview shortlist, and Section 6.2 explains how the cyber security solutions could meet the requirements (as set out in Section 4.1). Finally, the most important findings of these interviews are listed in Section 6.3.

6.1 Shortlist creation

In addition to the CADI providers previously selected, we also included the established asset management solution providers resulting from the survey by QvC Rijk, the quantum-safe (post-quantum) cryptography department of the central government. This showed that Generic Security Provider D, Generic Security Provider G and Generic Security Provider B are most often engaged among the government bodies surveyed. We searched for a variety of cyber security solutions, as described in Section 3.2.2.

- Generic Security Provider B (SOC, SIEM, EDR, ITAM)
- Generic Security Provider D (SOC, SIEM, EDR, ITAM)
- Generic Security Provider G (ITAM, CMDB)
- Generic Security Provider F (SOC, SIEM, EDR, CMDB, ITSM)
- Generic Security Provider H (CMDB, ITSM, ITIM)

No timely contact with the right persons was made for Generic Security Provider G and Generic Security Provider F.
Generic Security Provider C was approached via contacts within the team and previous interest in CADI.
Generic Security Provider A was contacted as part of the explorative phase, by contacts within the team.

It would have been best had we been able to interview Generic Security Provider D, whose products are in use by most ministries. Unfortunately, we have not been able to do so.

6.2 Expansion with CADI features

A number of generic security products described in Section 3.3 have a technological basis similar to that of CADI tooling. Among other things, they make use of an identical backend as is required for network scanning, application and library scanning, firmware (code) scanning, and file system scanning.

- **EDR/XDR** solutions originate from endpoint protection against viruses and malware. As automation increases and threats become more specialised, EDR solutions have started basing themselves on agents with extensive access rights to inspect the status of endpoints, scanning these, and intervening if needed.
  These agents are also required for CADI tooling. Nevertheless, due to their high degree of access and high continued development and challenges as set out in Section 5.4.6, expanding on agents is not always desired. EDR/XDR tools can relatively easily be expanded to include active scanning of cryptography use. Many

of the agents or agent-options of the CADI suppliers also work on this basis. The question remains: how efficient can this be? There is always a balancing act between agent comprehensiveness (for EDR/XDR or CADI) and the user experience.

- **ITAM**: these tools generally scan the entire IT environment. This is a precondition for CADI tooling: you can only arrive at a comprehensive CBOM if you include the full scope of IT assets. In addition, ITAM tooling can also link systems to operational processes. ITAM tools generally use agents themselves.
- **CLM**: these tools provide substantive certificate management. Although a CLM solution is not necessary for an organisation, it does benefit them, especially when it comes to large-scale changes such as cryptographic migration. In general, CADI tooling seems perfectly capable of finding certificates, but is not able to manage them. Moreover, CLM is often not a standalone activity, and is often subdivided across different services and IT landscape components. This is sufficient for current automated processes, as it is often set up and only requires active management for incidents. Nevertheless, this is not the case for system migrations, nor for the management of, for instance, hybrid certificates[6].
- **CMDB**: this tooling depends on solid ITAM *and* EDR/XDR solutions for input. In turn, CMDB acts as a source for systems that manage specific IT assets, e.g. software asset management (SAM) systems. These solutions show some overlap: ITAM, SAM and CMDB solutions together generally cover the full asset management. The CMDB or the ITAM solution often acts as the *single source of truth*, on the basis of which management takes place. Some CADI tooling uses such a single source of truth, or even depends on it. This single source of truth is also a potential point where we can expect to find a resulting CBOM, and where crypto assets are linked to hardware and software components for management purposes. But this can also be done separately, as long as the link is solid.
- **Vulnerability scanning**: these tools scan for potential vulnerabilities. Some vulnerability scanners already provide incident reports when outdated cryptography is used, such as that of Generic Security Provider E. We suspect that many CADI tools have expanded on existing vulnerability scanners for cryptography scanning in applications and firmware. Such tools do depend on access to the source code and are often poorly suited or not suited to software developed or provided by third parties.

The development of the tooling above has been user-driven for decades, completely following market demand. This means that it is likely that such existing solutions will broaden their scope with CADI features if or as soon as demand for this increases.

[6] https://hapkido.tno.nl/news/proof-concept-live/

6.3 Key findings

The generic security providers were, in general, interested in CADI as a potential addition to their current range. The maturity level varied by provider: some companies had been working in this area for a while, whereas it was new albeit interesting to others.

The most important finding was the following: different organisations indicated to be interested in CADI as a topic, but to not take any concrete steps towards it at this time, the latter due to a lack of direct drivers. Some providers had incidental questions from clients on the topic of PQC or CADI, but these were very limited in general. From a commercial perspective, CADI research, development and products were not attractive for these providers at this time.

7 Summary and conclusion

This chapter summarises the insights of the study in a number of conclusions. Refer to Chapter 8 for concrete recommendations (related to these conclusions).

For the sake of clarity, we repeat the threefold research question from the introduction:

1. What do a *minimum viable product* (MVP) and an ideal tool for CADI look like, and what requirements should they meet?
2. What is the current status of the CADI tools already commercially available, and how do they relate to the ideal and the MVP?
3. How can the gap between the MVP and an ideal CADI tool be bridged?
4.

We refer to Table 1 for Research Question 1, and to Table 2 for Research Question 2. We propose a number of recommendations in Chapter 8 to answer the third research question.

Cryptographic inventory moves on a spectrum of accuracy and effort. Under the hood, a CADI tool consists of multiple point solutions. Cryptographic inventory accuracy, comprehensiveness and costs increase as the number of point solutions deployed and their depth (i.e. higher numbering) increases (refer to Figure 2).

Existing full-stack solutions for CADI are expensive. CADI Provider B and CADI Provider C reported a rough estimate of the procurement costs for their tool during the interviews, in the range of hundreds of thousands or millions of euros per year. This creates a chicken and eggtype problem: during the workshop, several stakeholders mentioned that obtaining funding for PQC-related activities proves difficult, and that they would like to use a cryptographic inventory to prove the severity of the problem to their management. This means that the budget is often very limited for the inventory itself, making expensive tooling a problem.

Existing full-stack solutions for CADI are not European. CADI Provider B and CADI Provider C are not located in Europe. Although work can take place on-premise and structures with *non-disclosure agreements* (NDAs) are an option, this may be an issue for high-assurance environments.
It is worth noting than many of the technological experts in these companies are, in fact, European. This shows that there is not a lack of knowledge in Europe, but a lack of opportunity to establish a business in Europe in this field or to grow a business in this field. This may change if demand for CADI solutions in Europe exceeds that of the U.S.

The market for CADI providers is compliance-driven. Both CADI Provider B and CADI Provider C indicated that compliance with laws and regulations is the most important driver for their clients at this time. Although the impending migration to PQC and general cryptographic hygiene are mentioned, compliance is the first argument used. Regulations around PQC migration and in particular cryptographic asset discovery in the United States are ahead[7] of the European Union.

[7] Text - H.R.7535 - 117th Congress (2021-2022): Quantum Computing Cybersecurity Preparedness Act | Congress.gov | Library of Congress

Integration with generic cyber security tooling is a high priority. This applies to stakeholders we spoke to during the workshop as well as the CADI providers. This second fact is a great development, as it simplifies the adoption and integration of such systems. The other way around, all generic security providers indicated to be interested in CADI. Some parties even reported wanting to develop CADI tooling themselves. Alternatively, taking over an existing CADI provider was mentioned as an option.

Operational technology (OT) lags behind in terms of security and CADI. Although some providers indicated an interest here, none of the CADI providers interviewed had any experience at all with clients in the OT domain. As OT has a smaller market share than IT and poses extra challenges, there is no business incentive for the CADI providers. Expert opinions from TNO colleagues and the workshop also indicated many challenges in the field of OT.
This gives rise to major challenges in the field of OT, for which there is little knowledge available from TNO as well. This means that not much is known about the extent of the PQC migration challenge for the OT domain, the specific operational bottlenecks involved, and the specific features CADI tooling should have to locate sufficient cryptographic assets. For example, discussions and knowledge of these researchers as well as TNO colleagues point towards the property protection of most OT technology. Because there is no precise insight into source code or into precisely how the OT protocols are executed, deploying a CADI tool is impossible. This means that the OT provider market has to be motivated to tackle this issue. This impedes the development of similar independent CADI tooling.

There are general challenges surrounding asset management. It is good to know where the 'crown jewels' – their most important, key assets – are located for the deployment of an MVP in an organisation. This enables prioritisation within the CADI tool. During the workshop, it became apparent that various organisations are not aware of the location of their own key assets. Organisations are dependent on good asset management in order to map the location of their key assets, in turn obtaining a prioritisation for the deployment of CADI tooling.
This may also be a bottleneck for the rollout of an MVP, for which at least a part of the key assets have to be thoroughly mapped. Without this overview as a minimum, no launch can take place, which impedes the general adoption of such tooling. Such dependency on good asset management has a negative effect on CADI tooling adoption and, in turn, the market stimulation.

8 Recommendations

Collaborate intensively with the existing OT stakeholder landscape. The workshop and interviews in this report made it clear that OT is truly a key bottleneck. A large share of the vital Dutch infrastructure depends on secure OT. OT environments are increasingly connected to the internet[8]. Vulnerabilities within OT are very attractive for *advanced persistent threats* (APTs) and will increasingly be exploited.
This study has shown that OT is a blind spot when it comes to most CADI tooling. There is no market incentive for CADI providers to expand their tool to cover OT. However, the challenges CADI providers face in this respect are not specific to cryptography; generic security providers notice this more broadly. There is much to be learnt in the field of OT security. Cryptography can be a strong security mechanism for many of these OT applications. Several parties are involved in OT security research. This has to be stimulated further, and the CADI research needs to tie into this.
Concrete forward-facing steps can be defined through collaboration with the existing stakeholder landscape of QvC Rijk, the quantum-safe (post-quantum) cryptography department of the central government. This is an opportunity to close the gap present in CADI tooling for OT.
Relevant to:

- *NCSC: in collaboration with their relationships with critical infrastructure managers;*
- *CIO-Rijk: in driving, for instance, the Directorate General for Public Works and Water Management to take a leading role in this.*

Facilitate the establishment of a ground truth for accuracy. QvC Rijk is in a unique position and stakeholder landscape to collaboratively arrive at a CADI competition. This CADI competition will require a ground truth, i.e. all cryptography implemented in the test environment, for parties to measure their tools against.

Although this involves costs, this is the best way for the central government to influence and direct commercial solutions and their accuracy. Stimulating the market in this way will eventually cause large-scale migrations to be more affordable. This amply offsets the costs of such a competition. Because QvC Rijk is highly regarded internationally, it can set up a well-founded competition in collaboration with other associations or organisations. During the interviews, CADI providers already indicated to want to take action in this respect because they do not have an objective environment like this at this time, meaning the is no measurement basis for their results. Good tests results can serve as sales pitch for them as well.
Relevant to QvC Rijk, NCSC, BZK (the Ministry of the Interior and Kingdom Relations) and EZ (the Ministry of Economic Affairs): in capitalising on their current international position as pioneering government initiative in this field.

Improving insight into 'crown jewels', i.e. key assets. Insight into crown jewels strengthens the deployment of CADI tools within organisations as well as security in general. This is not a pre-condition but a preference.

[8] Het Cybersecuritybeeld Nederland 2023 (The Dutch Cyber Security Overview 2023), refer to Cybersecuritybeeld Nederland 2023 | Rapport | Rijksoverheid.nl.

Start with an (MVP) solution. Not every CADI solution is equally suited to large-scale implementation, but every CADI solution should be able to provide a first risk inventory. Large-scale CADI tooling implementations will not be cheap and management support is required to facilitate this. This support will only be given if there is a clear organisational risk. This risk can only be quantified through a first inventory, preferably on a select high-impact organisational scope. This can be done using every solution that was part of the interviews, and is at times offered as a service. Do not wait for an ideal solution and be one step ahead in terms of organisational challenges. Even if there is no comprehensive overview of the 'crown jewels', i.e. the key assets, starting work on the known part thereof is advisable.
Relevant to all organisations, whether public or private.
Dependent on 'Improving insight into "crown jewels", i.e. key assets'.

Importance of tendering scope. As described in Section 5.1.3, the demands of the end user influence the quality and scope of the CADI tool. As there is no reliable indicator for CADI tool accuracy at this time, this demand is difficult to define. It is similarly difficult to retrospectively validate that the demand has been met. For the tendering for large-scale implementation of CADI tooling, we recommend also including a service component for interpretation or migration activity definition, placing the responsibility for low accuracy with the service provider. Again, we emphasise the recommendation to establish a ground truth, as referred to above.
Relevant to all major end users, government bodies in particular, as there is a high focus on PQC within initiatives like QvC Rijk.

Incentivise tendering processes. (CADI) providers need market incentives to continue development and improve. It is not a matter of *whether* this market will grow, but *when*. The geographical growth location of this market is decisive in terms of how future developments will unfold. There is an opportunity for QvC Rijk in this respect, as this relationship already has a high maturity and strong focus on PQC. Also refer to the recommendation above.
Relevant to QvC Rijk.
Dependent on 'Importance of tendering scope'.

Work on compliance. The U.S. is a pioneer in CADI tooling precisely because regulations required federal authorities to start on CADI. This is a known challenge in Europe. Starting on this in a timely manner helps, as the market is compliance-driven.
Relevant to QvC Rijk.

Connect follow-up research to other BOM studies. The challenges surrounding the cryptographic bill of materials (CBOM) are not unique to these CBOMs. Similar techniques are studied to locate other asset types. TNO finds that this technological basis should be capitalised on by broadening the scope of (existing) BOM research. Not doing so would have us reinvent the wheel. This is especially relevant to OT.
Relevant to all parties involved.

Show restraint in terms of the focus on closing the gap with an ideal CADI tool for IT and the focus on OT. Some of the CADI solutions are close to the ideal. Where this is not the case, they are well underway and will reach this point via market incentive. This incentive – i.e. compliance and ground truth – is among the advice previously mentioned, after which the existing gaps are expected to become bridged without further intervention. According to TNO and as discussed during the workshop, this is not the case for OT, where bridging the gaps is a major challenge and which should be an area of enhanced focus, as

the market does not provide this incentive at this time. Tapping into research into broader OT security and BOM solves the OT challenges (property rights, legacy and computational power limitations, refer to Section 3.4) that CADI providers currently face. This increases the willingness of CADI providers to enter this market and develop solid CADI tooling as a result.
Relevant to QvC Rijk, NCSC, BZK (the Ministry of the Interior and Kingdom Relations) and EZ (the Ministry of Economic Affairs).
***Dependent on**: 'Facilitate the establishment of a ground truth for accuracy' and 'Work on compliance'.*

Conduct research into evaluation criteria**.** Ideally, CADI tooling should be evaluated on the basis of a standardised set of requirements. A standard framework or series of requirements can be drawn up, based on which CADI tools can be assessed. This does require a pre-existing ground truth, as recommended previously. This means that this recommendation is further down the line. It could also go hand in hand with compliance, e.g. because organisations are only permitted to use certified CADI tools.
Relevant to EZ (the Ministry of Economic Affairs) and BZK (the Ministry of the Interior and Kingdom Relations).
Dependent on 'Facilitate the establishment of a ground truth for accuracy'.

Appendix 1 – Workshop summary

Workshop organisation

The workshop took place on 23rd of September in the ZZIIN Conference Centre in The Hague. The attendees present were highly diverse. Among them were stakeholders from the Central Government as well as corporate representatives. A number of technical experts and policymakers were present as well.

The first part consisted of a series of questions focusing on the practical requirements for CADI tooling. These questions/requirements were based on the literature review. The participants' answers were collected by question and any noteworthy similarities or agreements were discussed. In the second part of the workshop, the participants were split into groups and CADI and the corresponding challenges were discussed more informally.

An overview of the questions asked and answers received follows below. Subsequently, a number of observations based on the discussion during the questions and the notes of the groups from the second part of the session are listed.

Functional requirements survey

The questions as put forward during the workshop are listed below. Each question was projected on a screen, during which participants could choose from a range of options (multiple-choice also being an option). The answers were gathered via Mentimeter[9].

The most common answer is given in blue for each question (or which answers, if results were close). Any other items raised for discussion are listed under the question and explained.

Integrability. Should a tool with CADI features be easy to integrate with other generic cyber security tooling?

A. The CADI feature has to be provided within the existing tooling already in use, and I do not mind waiting a few years for that.
B. I would rather see the CADI feature as part of my existing tooling, but I would have to assess the risk first. I can also accept a (temporary) tool for that purpose, as long as it exports to my existing tooling.
C. **I am comfortable handling new tooling, as long as it exports to my most important management tools.**
D. I am comfortable handling new tooling, even if it does not export data.
E. I would need a one-off scan using a tool before I know my risk and, accordingly, how to answer this question.
F. I would like to fully separate CADI and generic cyber security solutions.

[9] https://www.mentimeter.com/

G. Other, which I would like to explain further verbally.

Comprehensive information. How important is it to map *all* cryptographic assets? At what important locations should cryptographic assets be found? What locations are less important to scan?

A. All cryptographic assets should be able to be found. I want my entire system mapped, including the cryptographic assets in my external products.
B. Only operational devices, applications and networks need to be scanned. Test systems or unused systems fall outside the scope.
C. Only the cryptographic assets for communication to the outside world need to be identified.
D. Other, which I would like to explain further verbally.

Information capabilities. What depth should a tool have? For instance, how much insight into the result, visualisations and cross-references are needed?

A. The tool should have a simple search function.
B. If I can easily link it to systems via an export, I can use my existing tooling to view mutual systems dependency.
C. I would like a visual overview of the cryptography present and its dependencies.
D. I need sufficient insight into a (cryptographic) asset, so I can easily verify the correctness of the result manually.
E. If needed, I am happy to dig through an Excel export myself, as long as I know what is located in which system/application.
F. I want to be able to easily view which cryptographic assets have changed compared to the previous scan.
G. Other, which I would like to explain further verbally.

Support. How much support do you need to use a new tool or new functionality in existing tooling?

A. My current service level is perfectly adequate.
B. We want to be able to fully manage it in-house, possibly with a technical consultation if we run into an issue we cannot solve ourselves. We do expect to receive (security) updates, but not any feature updates.
C. We do most management in-house, but we do want to receive (security) updates, feature updates, and we would like the provider to step in should things go wrong.
D. Other, which I would like to explain further verbally.

Access. What type of access do you want a tool to have in your environment?

A. The tool can have system access at all locations in the production environment, but I decide where and when the tool functions. I do not want the tool to 'run rampant' in my environment.
B. The tool can have kernel-level access to my systems.
C. The tool can have system access to everything, but not in the production environment.
D. I want to determine which network domains are monitored and when. In addition, I want to have control over the deployment of any scanning agents on (virtual) systems.
E. The tool can have access to all aspects set by the tooling provider.
F. The tool can also output results to the supplier in a cloud solution or an SaaS model.
G. The tool can only output results locally; I do not want results to be output elsewhere than my own environment.
H. The tool should be able to work offline.
I. Other, which I would like to explain further verbally.
Note: this also differs by (sub-)tool. Offline is particularly important to OT.

Logging. What should be logged?

A. The scan results.
B. Where, when and which scan has been performed.
C. Errors if a scan could not be performed, and why.
D. Unexpected changes if a system is re-scanned.
E. Other, which I would like to explain further verbally.

Provider trustworthiness. Can we trust the provider?

A. A clear agreement has to be drafted with the provider, including the option to specify my situation; I do not want a standard agreement.
B. If the standard agreement of the provider meets my security requirements and legal obligations, that is fine.
C. The provider has to be located in the Netherlands.
D. The provider has to at least be located within the EU.
E. The provider has to be one of our current generic security tool providers.
F. Other, which I would like to explain further verbally.
Note: this can be complex for multinational organisations if requirements differ.

Continuity & back-ups. What requirements are there for tool continuity?

A. None. I manage it myself and save the results and settings myself. This means that it is my own responsibility.
B. I do not expect to use the tool often. If it is unavailable for a week, that is not a problem. A month would prove difficult.
C. I expect to use the tool extensively, so downtime should not be more than a day to a week.
D. I expect to use this tool (bi)annually. It has to be available then.
E. I do not want to lose results and a daily or better back-up feature has to be available.
F. I do not want to have to re-do more than one week of work, and the back-ups have to reflect that.
G. I export data immediately and do not leave it on the platform, so a back-up feature seems redundant.
H. Other, which I would like to explain further verbally.

System capacity requirements. What impact does running the tool have on other systems and applications?

A. I do not want overly heavy system requirements, but I intend to not run it in a production environment; the impact on my employees is low.
B. I want a clear picture, so I run the tool in the production environment. I do not want to need more than 10% additional capacity in any area.
C. I want a clear picture, so I run the tool in the production environment. I do not want to need more than 30% additional capacity in any area.
D. As long as it does not disrupt my core operational processes. I will investigate this myself once the tool has been provided to me and find my own solutions to this.
E. Other, which I would like to explain further verbally.
Note: capacity is generally not a big issue, except for OT.

Exports. Should you be able to export the raw data? If so, what should the file type be?

A. The file type should be JSON.
B. The file type matters little, as long as it is common and recognised (e.g. JSON, CSV, TSV, XML, HTML, etc.).
C. Other, which I would like to explain further verbally.

Observations and findings

The key observations and findings from the workshop are listed below, covering both the plenary survey session and the group-based discussions.

- Many organisations show low awareness: why is CADI needed? This applies to developers as well as management.
- A chicken and egg problem seems to exist when it comes to cryptographic inventory (and cryptographic migrations). Tooling costs money, a risk analysis is needed for that, for which in turn tooling is needed.
    - The risk analysis does not need to be comprehensive/perfect to create management buy-in; an incomplete result is a good start.
- There is a larger problem when it comes to *asset management*. Some organisations have high maturity in terms of visibility of running assets, but that does not apply across the board. It is also reported that there is no solid data format that encompasses cryptographic, hardware and software asset management. This results in there being no overview.
- Sub-solutions exist that can be deployed in practice, e.g. for CI/CD pipelines, but their outcomes are not aggregated and, accordingly, there is no overview.
- Tools should be able to be managed in-house, and a tool has to be able to run on-premise/locally with solid (automated) export capabilities.

Appendix 5 – Search terms

During the first phase of this study, available material was explored via desk research. The following terms were used to do so for the first round. Subsequently, more information was sought based on the sources acquired in this manner.

‘cryptographic assets discovery’
‘cryptographic assets in organisations’
‘crypto(graphy) identification method (scanner)’
‘crypto(graphy) scanner’
‘cryptography tracer’
‘cryptographic discovery’
‘cryptographic risk management’
‘quantum risk management’
‘cryptographic asset management’
‘(automated) identify cryptographic vulnerabilities’
‘automated cryptographic discovery and inventory’/’ACDI tooling’
‘cryptography management (platform)’
‘network analyzer cryptography’
‘application analyzer cryptography’
‘filesystem analyzer cryptography’
‘cryptography discovery scanner’
‘public key application discovery tools’
‘cryptography scanning’