# NETHERLANDS CRYPTOLANDS

## STARTING POINT OF THE CRYPTO-COMMUNICATIONS ROADMAP: AN OVERVIEW OF 4 IMPORTANT DEVELOPMENTS IN CRYPTOGRAPHY


**Authors**

Yoram Meijaard (TNO)
Maran van Heesch (TNO)
Ronald Cramer (CWI and University of Leiden)
Jelger Groenland (Innovation broker cryptocommunications)



May 2021


CWI dcypher Ministerie van Economische Zaken en Klimaat TNO

# MANAGEMENT SUMMARY

Cryptography is *fundamental* to Dutch society. Our highly digitalised society is dependent on the availability, integrity and confidentiality that cryptography can offer. Moreover, cryptography plays a key role in the strategic autonomy of the Netherlands.

There are three aspects that are important to the practical implementation of cryptography resulting in a *cryptographic end-product*: (1) the underlying mathematics; (2) implementation of the software and hardware; and (3) embedding the end-product in the organisation. In practice, a cryptographic end-product is an all-in package of mathematics, software and hardware. All these specialist disciplines are links in the *cryptography value chain*.

Mathematics makes a distinction between two types of cryptography: *unilateral*, where two parties exchange information while keeping it secret from a third party, and *multilateral*, where multiple parties carry out calculations while keeping information secret from each other. Furthermore, without good implementation of the cryptographic protocol in both software and hardware, secure use of cryptography is impossible. Good implementation involves meeting many requirements—the problem is that they are sometimes contradictory. Ultimately, what matters is the correct embedding in the organisation and therefore the correct use of the cryptographic end-product. Certification can offer aids for the deployment of the right product at the right security level, but this means the cryptographic end-product has to be controllable.

There are many different cryptographic end-products, each with its own functionality. We categorise them in terms of *data at rest*, *data in use* and *data in transit*. The Netherlands mainly uses two well-known cryptographic end-product taxonomies: that of the *Nationaal Bureau voor Verbindingsbeveiliging* (Netherlands National Communications Security Agency – NBV) and that of the Common Criteria. This survey compares these two lists by linking them with the three identified data categories. It becomes apparent that not all product categories under the Common Criteria are covered by NBV-assessed products. The important point is that existing cryptographic end-products do not always keep pace with the development and acceptance of new digital technology. The product categories that are not served represent gaps where there is insufficient coverage.

The cryptography landscape in the Netherlands is constantly evolving. The Netherlands holds a strong lead and has many pioneering scientists of international renown. A number of Dutch medium-sized enterprises supply cryptographic end-products. In the Common Criteria taxonomy it can be noticed that products approved for use in the Netherlands are predominantly supplied by foreign companies.

New developments are constantly changing the backdrop in cryptography. At present, we discern four developments in the field of cryptography that we think are going to pose the greatest threat and offer the greatest opportunities over the next few years (see Figure).

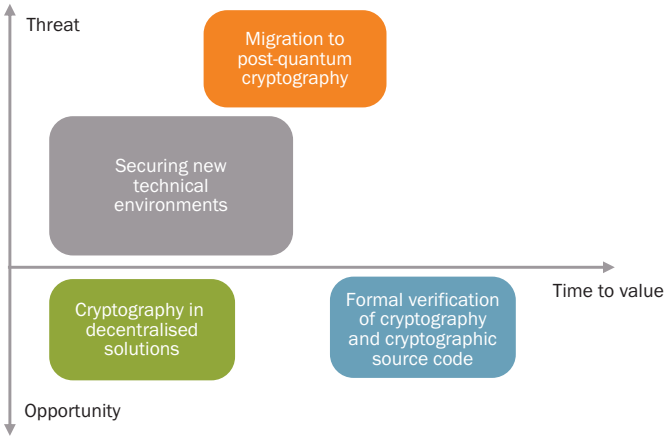



*Figure: Chart of the 4 high-impact developments in cryptography, divided into opportunities and threats against time. 1. securing new technical environments (grey) 2. migration to post-quantum cryptography (orange); 3. cryptography in decentralised solutions (green); 4. formal verification (blue).*

1. *Making new technical environments secure:* ongoing development and the adoption of new technical environments make adequate security a necessity. New environments must be fit for use in situations where security is very important. In principle, this product development can be done with forward using generally available, unilateral cryptography and is achievable in the short term.

2. *Migration to post-quantum cryptography:* the development of the quantum computer represents a danger to widely used cryptographic systems. Work is in progress on post-quantum cryptography that is resistant to the quantum computer. The migration to post-quantum cryptography is a challenge to the whole value chain, in both the short and long term. A spin-off benefit is that structural migration can improve the systems' crypto-agility.

3. *Deployment of cryptography for new decentralised applications:* the development of multilateral cryptography is forging ahead and leading to new, decentralised solutions such as secure multi-party computation. Exploiting these solutions opens opportunities for the Dutch economy. Various market applications are expected in the Netherlands in the near future.

4. *Formal verification of cryptography and cryptographic source code:* formal verification is a method of carrying out automated checks by computer on software implementations. Using the techniques of formal verification on cryptographic protocols offers guarantees of the security of cryptographic products. Expectations are very high, but practical application will presumably come in the long term.

The Netherlands will have to take steps to make full use of these opportunities and rise to the challenges. In the Cryptocommunications Roadmap of the Ministry of Economic Affairs and Climate Policy, we are working out which steps to take. As the authors of this survey, we invite you, our readers, to work with us on the Crypto-Communications Road Map and make the Netherlands a Crypto Country, starting with an economically active and sound ecosystem, strategic autonomy and digital security.

# CONTENTS

# 1. INTRODUCTION AND BACKGROUND

Cyber security is important. It enables consumers, industry and governments to make secure and reliable use of computers, the internet and all kinds of digital systems. Cyber security embraces many aspects, such as information flow monitoring and access management.
One thing is clear: cryptography is a critical building block for cyber security. Cryptography is *fundamental* to Dutch society, which depends on the confidentiality, availability and integrity that cryptography can offer.

Cryptography is a very broad subject. Its roots lie in mathematics, in open and published science. Secure communications are an application of cryptography. These communication systems are implemented in software and hardware, developed behind closed doors. The transition from mathematical perfection to the real world has aspects of its own. The hardware used must be secure, including all components delivered along the supply chain. Applying cryptography correctly means handling all these aspects well. In practice, a cryptographic end-product is an all-in package of mathematics, software and hardware. These independent, specialist disciplines are links in the *cryptography value chain*.

In the Netherlands, one application of cryptography is to keep highly classified information secure. Thus, cryptography plays a key role in the strategic autonomy of the Netherlands. “Strategic autonomy” means that the Netherlands is able to make the choice between self-sufficiency, cooperation or dependency on other countries for sectors of strategic importance. This freedom of choice is essential. Examples of factors that impede this strategic autonomy are lack of knowledge and absence of economic activity in a given sector. Cryptography is a field in which the Netherlands seeks strategic autonomy. This does not mean the Netherlands has to be self-sufficient, but it must be able to make informed choices on what cryptographic technology to develop in the Netherlands and which technology, developed outside the Netherlands, it can import and use.

Constant new developments are features of the cryptographic landscape. Some of these threaten the current security level, while others actually offer new opportunities to Dutch corporate life and the academic sector. The Ministry of Economic Affairs and Climate Policy wants to stimulate cooperation in the Dutch cryptography landscape, to profit from all developments by aligning supply and demand and, where necessary, actively stimulating innovation along the supply chain.

This explains the decision to develop a shared innovation roadmap on the subject of Cryptocommunications in this sense means cryptography in its applied form, in all types of digital communication. The term indicates that the road map is wider than mathematics alone, and it gains added value from cryptography’s applications in information technology and other fields. “Crypto communications” also indicates that this is not about cryptocurrencies and digital assets, but about application in the secure exchange of information between parties via digital channels.

The cryptocommunications roadmap focuses on “how” the Netherlands must act to deal with all these developments. This survey gives an initial impression of ‘what’ the developments are in cryptography and what the topics are for the road map. We survey the concepts of cryptography, crypto communications and other relevant aspects. This survey is the starting point for the cryptocommunications roadmap.

## 1.1 CONTENT AND STRUCTURE

In Chapter 2, we describe what is necessary to deploy cryptography in practice in the form of a *cryptographic end-product*, while Chapter 3 looks at the various types of cryptographic end-products. In Chapter, 4 we outline the Dutch crypto landscape. In Chapter 5, we describe the four high-impact developments (opportunities and threats) in cryptography that call for action by the Netherlands. Finally, in Chapter 6, we conclude the document, and in Chapter 7, we invite our readers to contribute actively to the cryptocommunications roadmap.

**"CRYPTOGRAPHY IS THE BEDROCK OF DIGITAL SECURITY AND IS IMPORTANT TO THE NETHERLANDS' STRATEGIC AUTONOMY.** THE CRYPTOGRAPHY LANDSCAPE IS CONSTANTLY EVOLVING, SO NEW THREATS AND OPPORTUNITIES MAY EMERGE AT ANY TIME."

# 2. CRYPTOGRAPHY: FROM PROTOCOL TO END-PRODUCT

This section describes the different facets of a usable cryptographic end-product: see Figure 1. It offers a summary of the maths behind the cryptography and the associated nomenclature. The features and risks of IT applications of cryptography are reviewed as well. Finally, the section deals with the embedding of cryptographic end-products in an organisation's processes.

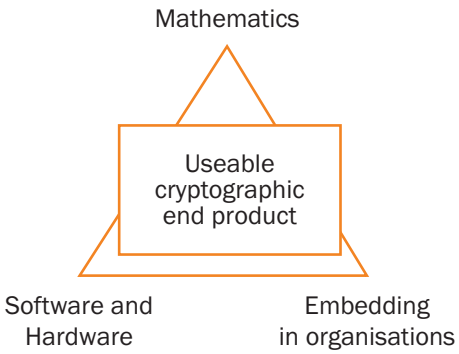



*Figure 1. The three aspects of cryptography.*

## 2.1 WHAT IS CRYPTOGRAPHY?

Cryptography is the science that supplies the building blocks for "secure" information handling. The meaning of "secure" depends on the context, but often comprises one or more of the following characteristics.

- Availability: the data are available to those who need them;
- Integrity: third parties have not tampered with the data;
- Confidentiality: third parties cannot access the data;
- Non-repudiation: it is clear from whom the data originates.

In theory, cryptography is divisible into at least two sub-fields which differ radically from each other. Each sub-field has its own methods. In *unilateral cryptography*, two parties exchange information that is kept secret from a third party. This contrasts with *multilateral cryptography*, where multiple parties carry out calculations together, while keeping information secret from each other.

Unilateral cryptography is the oldest and most developed sub-field. It can be divided into three techniques: *symmetric cryptography*, where both/all parties encrypt and decrypt information with the same secret key; *asymmetric cryptography*, where each party uses a public and an associated private key; and *cryptographic hash functions*, which can prepare a near-unique digital fingerprint of the data.

The paradox of symmetric cryptography is that a key must first be agreed, but the medium by which that key is communicated is only secure once the key is agreed. This catch-22 situation is known as the "key exchange problem." Asymmetric cryptography has been introduced to solve this problem. A message can be encrypted using a receiver's public key, so that the message can only be decrypted with the receiver's private key. Asymmetric cryptography offers the further option of creating digital signatures.

An advantage of symmetric cryptography is that it is much faster than asymmetric cryptography. That is why modern crypto systems first use asymmetric cryptography to authenticate the parties and exchange a key and then encrypt data using symmetric cryptography. These combined cryptosystems occur universally in our digital society, from the encryption of banking transactions to website visits, instant messaging and logging in to a web shop.

Cryptographic hash functions play an important role in making digital fingerprints of data. These fingerprints are unique,[1] and minor changes to the data create a totally different fingerprint. This allows control, for example, of the integrity of a downloaded program. The role of cryptographic hash functions is also important as a heuristic approximation to randomness, strengthening different cryptographic systems.

Multilateral cryptography has other applications. There are situations in which multiple parties share a common goal but do not trust each other: hence, they do not share information. To achieve a result despite this, a *trusted third party* is used to obtain all the information from all parties and reach a conclusion independently. Take the example of an auction, in which all participants submit secret bids to the auctioneer, who then decides who has placed the highest bid. It is not possible for individual bidders to retrospectively trace who placed which bid. Only the auctioneer knows all the bids. The bidders trust the auctioneer to have genuinely accepted the highest bid and not to have abused that knowledge of the bids.

The confidentiality of the *trusted third party* presents a problem, since confidentiality is very hard to verify, and individual participants have no control over it. Unilateral cryptography offers no solution to this trust paradox. However, techniques from multilateral cryptography can emulate the trusted third party, so that the cryptography takes over the confidentiality role. Multilateral cryptography enables multiple parties to carry out a random calculation together without a trusted third party, while preserving the confidentiality of individual input, and with a result verifiable as correct.

## 2.2 TECHNICAL ASPECTS OF A CRYPTOGRAPHIC END PRODUCT

The roots of cryptography lie in mathematics, but it depends for its application on the software and hardware used. As a rule, cryptography is implemented in software and hardware, and this entails dangers of its own, such as:

– *Side-channels*, which leak information about the cryptography used and the associated keys, for example through tiny differences in execution time; and
– *Glitches*, short-lived faults in the hardware that may bypass crucial cryptographic stages.

Consequently, a cryptographic method is secure from a mathematical viewpoint, but may be vulnerable in its implementation.

1. *The literature refers to "collision resistance" when it is very difficult to find two inputs for a hash function with the same fingerprint. In practice, these fingerprints are almost unique.*

In practice, cryptographic end-products are all-in packages of mathematics, software and hardware. The independent, specialist disciplines each form links in the cryptography value chain. The value chain as a whole ultimately leads to a cryptographic end-product with various features, some of which work against each other. We identify the following features below:
– The *functionality* provided by the product; Chapter 3 examines this in greater depth;
– The *security level*, the degree of protection provided by the product;
– *Complexity*, the degree of sophistication of a product;
– *Modularity*, the extent to which a product can be divided into separate components;
– The product's *performance*, for example measured in terms of achievable speed and throughput;
– The product's *crypto-agility*, the degree of changeability of the underlying cryptography;
– *Verifiability*, the extent to which a user or external verifier can check an end-product's properties;
– *User-friendliness*, the ease of use of the cryptographic end-product.

An example of crypto-agility is the ability to change cryptographic primitive, for example from 3DES to AES. This can be useful when new insights lead to different requirements for the cryptography used. This feature represents what might be described as a "plug 'n' play" option, preserving the product's functionality while altering its security properties.

The different features may reinforce or conflict with each other. Complexity and verifiability work against each other, as a highly complex product is difficult to verify. Modularity may to some extent reduce the product's complexity, by breaking the end-product down into readily usable modules. A software product is typically more complex and more crypto-agile than a hardware product. However, there are reasons for opting for a hardware product, which typically performs better and achieves a higher security level. The context of use of a cryptographic end-product dictates what balance to strike between conflicting properties.

## 2.3 CRYPTOGRAPHY IN THE OPERATIONAL PROCESS

Cryptography is used wherever information is handled digitally. This includes communication, data storage, signatures and software updates. The use of end-products in an organisation requires correct embedding in operational processes and technical infrastructure. For this purpose, it is very important both to choose the product that offers the right functionality and to use it in the right way.

The crucial factor when selecting the appropriate cryptographic end-product is the *certainty* that it meets the organisation's security requirements. Cryptographic end-products are the core of the organisation's security, so that a degree of distrust and caution is present. To obtain certainty that a product meets the requirements, that product must to some extent be *verifiable*.

Organisations have to make their own choice of a given product. *Certification* offers guidance to organisations in selecting a cryptographic end-product that fits the desired security level. Known examples of certification are the tests by the *Nationaal Bureau voor Verbindingsbeveiliging* (NBV)[2] and the Common Criteria[3]. The NBV is a branch of the General Intelligence and Security Service (AIVD) of the Netherlands and acts as a gatekeeper for the deployment of products in the domain of state secrecy. The Common Criteria are an international standard against which various parties can offer certification. This survey deals with the NBV in Section 3.

2. *https://www.aivd.nl/onderwerpen/informatiebeveiliging/beveiligingsproducts/geevalueerde-products*
3. *https://www.commoncriteriaportal.org/*

Conditions of the use of cryptographic end-products in an organisation are identity, key and access management. Identity management is the process that establishes a user's identity. Key management is the process that generates the cryptographic keys and links them to the established identities. Access management is the process governing access to information for certain identities. Achieving the correct mesh of these systems in major organisations is non-trivial task.

**"IN PRACTICE, A CRYPTOGRAPHIC END-PRODUCT IS AN ALL-IN PACKAGE OF MATHEMATICS, SOFTWARE AND HARDWARE.** THE INDEPENDENT SPECIALIST DISCIPLINES ARE LINKS IN THE *CRYPTOGRAPHY VALUE CHAIN*."

# 3. CRYPTOGRAPHIC END-PRODUCTS IN PRACTICE

This section takes a closer look at the functionalities of cryptographic end-products. For this purpose, we introduce a reference model for the application of cryptography. This model can be used to place the desired functionality of the cryptographic end-product in context. Using the reference model, we will examine the taxonomies of cryptographic product categories as used by the *Nationaal Bureau Verbindingsveiligheid* (NBV) and the Common Criteria. Finally, we will use the NBV taxonomy to give an initial indication of which functionalities the Dutch government needs.

## 3.1 A REFERENCE MODEL FOR CRYPTOGRAPHY

In practice, a cryptographic end-product has many applications. Figure 2 shows a reference model to which the various functionalities of cryptographic end-products can be attached. It is an adaptation of the reference model used in a past TNO report[4] and highlights the stages in which data may be present.

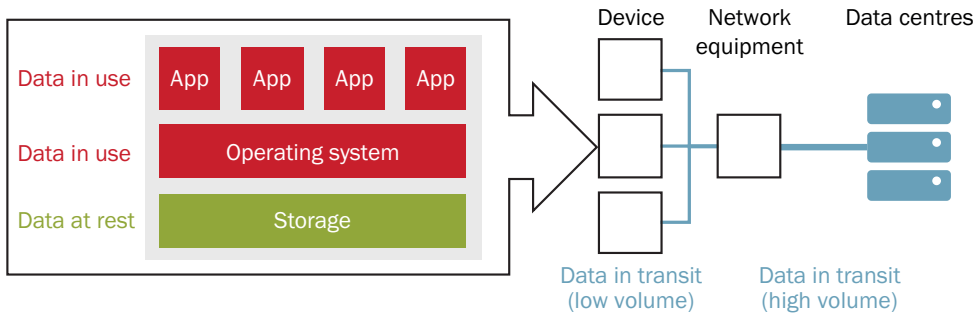



*Figure 2: Reference model of cryptographic end-products.*

Within a *device* such as a laptop or mobile phone, there is a tiered architecture: see Figure 2. Data are stored on the *disk* for use by the *operating system* and related *apps*. Different devices exchange data at both slower and faster speeds, as happens between *data centres*.

The reference model defines three different stages in which data may be present: *data are at rest, in transit or in use*. There are also three derivative areas in which cryptography is used: in an end user's device, in network equipment and in data centres. The different places on the network entail different security requirements, so there is a need for a very diverse product portfolio.

4. *TNO report "Verdieping Valorisatieketens: Basis voor de routekaart 'Veilig werken in een onveilige cloud'" ["Deepening value chains: Basis of the roadmap 'secure working in an insecure cloud'"]*

## 3.2 TAXONOMIES FOR FUNCTIONALITY IN CRYPTOGRAPHY

Various taxonomies are used to distinguish between an end-product's functionalities. In this section, we examine two existing taxonomies of cryptographic end-products: the NBV taxonomy and the Common Criteria. The reason for this choice is applicability within the Netherlands: the NBV assessment guides the government, while the Common Criteria play a big role in the Dutch business sector. The taxonomies are taken from the list of NBV-assessed products[5] (see Table 1) and from the list of products certified according to the Common Criteria (see Table 2). Both tables show where the products are used within the reference model: see Figure 2.

The NBV taxonomy involves a subdivision between products for media and file encryption, products for network security and products for *mobile communications*. The other category includes *keyboard*, *video* and *mouse (KVM) switches*, products used to simultaneously connect keyboard, mouse and video to several computers. A typical application of a KVM switch is in a data centre, to ensure efficient access to the many servers on a single server rack.

*Table 1: Taxonomy of NBV-assessed security products.*

| NBV taxonomy of product categories | Reference model |
|---|---|
| Media and file encryption | Data at rest |
| Offline security | Data at rest |
| Laptop security | Data at rest |
| Security of external media | Data at rest |
| Network security products | Data in transit |
| Secure mobile communication products | Data in transit |
| Other securtiyproducts | Not applicable |

This taxonomy's emphasis lies on the *high-assurance* domain in which information has to be handled under state secrecy. Work on departmentally confidential information takes place in the *low-assurance* domain.

The Common Criteria have more categories than the NBV taxonomy: see Table 2. Interestingly, all the NBV categories recur in the Common Criteria taxonomy, with the proviso that the Common Criteria subdivide *network security* into further categories such as *boundary protection* and *network devices*. On the other hand, the Common Criteria also list product categories that do not occur in the NBV taxonomy.

*Table 2: The Common Criteria taxonomy of cryptographic product categories.*

| The Common Criteria taxonomy of product categories | Reference model |
|---|---|
| Access Control Devices and Systems | Data in transit |
| Boundary Protection Devices and Systems | Data in transit |
| Data Protection | Data at rest |
| Databases | Data at rest |
| Detection Devices and Systems | Data in transit |
| ICs, Smart Cards and Smart Card-Related Devices and Systems | Data at rest |
| Key Management Systems | Data in transit, rest and use |
| Multi-Function Devices | Data in use |
| Network and Network-Related Devices and Systems | Data in transit |
| Operating Systems | Data in use |
| Products for Digital Signatures | Data in transit, rest and use |
| Secure mobile devices | Data in transit |
| Trusted Computing | Data in use |
| Other Devices and Systems | Not applicable |

5. *https://www.aivd.nl/onderwerpen/informatiebeveiliging/beveiligingsproducts/geevalueerde-products*

The tables highlight differences between the two taxonomies. First, the NBV taxonomy in Table 1 does not include data-in-use products such as trusted computing, operating systems and multi-function devices. These products do occur in the taxonomy of the Common Criteria, Table 2. Furthermore, the Common Criteria list supports products such as access control, key management and digital signatures. Please note that, to some extent, the existing cryptographic end-products will incorporate these applications. Neither taxonomy lists cloud computing solutions as a category.

All the above solutions can be implemented with currently available unilateral cryptography. Chapter 5.1 will pay further attention to expanding the existing product portfolio.

"THE CRUCIAL FACTOR WHEN SELECTING THE RIGHT CRYPTOGRAPHIC END-PRODUCT IS THE **CERTAINTY** THAT THE PRODUCT MEETS THE ORGANISATION'S SECURITY REQUIREMENTS."

# 4. THE CRYPTOGRAPHIC LANDSCAPE IN THE NETHERLANDS

Given the Netherlands' strategic autonomy, it is important to have a clear picture of the entire Dutch cryptographic ecosystem. This section gives a preliminary outline of the position of the Dutch universities in terms of knowledge and an initial indication of the companies engaged in the cryptographic field in the Netherlands. The emphasis is on companies that offer solutions for data at rest, in transit and in use. Companies that offer other types of solutions or play a different role in the cryptographic ecosystem in the Netherlands are not considered.

This position of the universities as repositories of knowledge is the foundation of the crypto-communications value chain. The knowledge they develop opens opportunities for businesses to make rapid use of the new developments and produce a cryptographic end-product. The coordination between research and exploitation can be examined in detail and mapped out on the cryptocommunications roadmap of the Ministry of Economic Affairs and Climate Policy.

## 4.1 THE NETHERLANDS' KNOWLEDGE POSITION

The Netherlands holds a good position in terms of knowledge. There is a strong academic ecosystem of internationally renowned universities and knowledge institutions researching cryptography to the full extent. The academic working groups, institutes and knowledge institutions hold an international lead in all relevant sub-fields of cryptography. In other words, academics at Dutch institutions are doing pioneering research in their respective fields. Especially in the fields of post-quantum cryptography and multilateral cryptography, the Netherlands holds an international lead and an outstanding knowledge position.

Table 3 gives a first impression of which sub-areas of cryptography are researched at which university. This overview is based on the public websites of the universities and the research groups associated with them. The researched sub-fields of cryptography correspond to the subdivision of cryptography described in Section 2.1, supplemented by quantum cryptography (which will be dealt with in Section 5.2) and hardware cryptography as described in Section 2.2.

*Table 3: Preliminary summary of cryptography at Dutch knowledge institutions. Green indicates that this sub-field is being researched by a permanent staff of the knowledge institution and yellow that research related to the sub-field is under way.*

| Knowledge institution | Sub-fields of cryptography | | | |
|---|---|---|---|---|
| | Unilateral | Multilateral | QKD | Hardware |
| CWI | | | | |
| Radboud University | | | | |
| University of Groningen | | | | |
| Delft University of Technology | | | | |
| Eindhoven University of Technology | | | | |
| Leiden University | | | | |
| University of Twente | | | | |
| University of Amsterdam | | | | |
| Vrije Universiteit Amsterdam (VU Amsterdam) | | | | |
| TNO | | | | |

## 4.2 FIRST IMPRESSION OF PRODUCT SUPPLIERS

It is difficult to compile a complete picture of all national and international companies trading as suppliers of cryptographic end-products on the Dutch market. An initial estimate can be made by looking at the manufacturers that supply NBV-assessed products or products that have a Common Criteria certification for the Dutch system. This information is given in Tables 4 and 5.

*Table 4: Summary of international companies that supply NBV-assessed products to the Netherlands. Companies highlighted in bold are Dutch.*

| Suppliers of NBV-assessed products | | |
|---|---|---|
| APITech | **Fox Crypto** | Microsoft |
| Black Box | Hiddn | Sectra |
| Blancco | Ironkey | Secunet |
| **Compumatica** | iStorage | Sophos |
| | | **Technolution** |

*Table 5: Summary of national and international companies that supply products according to the Common Criteria for the Dutch system.*

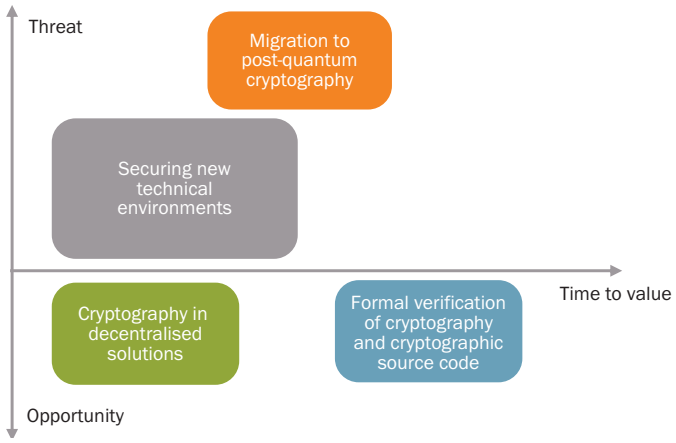
| Suppliers of products according to the Common Criteria | | | |
|---|---|---|---|
| A.E.T. Europe | DocuSign | Infineon Technologies | Sony |
| AllWipe | Eurowitcel | JR EAST MECHATRONICS | STMicroelectronics |
| Arm | Fox-IT | nCipher Security | Symantec |
| Blue Coat Systems | G+D Mobile Security | NetIQ | Thales |
| CEC Huada Electronic Design | HID Global | Nexor | Toshiba |
| Check Point Software Technologies | HiSilicon | NXP Semiconductors | Utimaco |
| Cisco Systems | Huawei Technologies | SafeNet | Waterfall Security Solutions |
| Cryptomathic A/S | Idemia | Samsung Electronics | ZTE Corporation |

Remarkably, there is little overlap between companies supplying approved products to the Dutch government and to the Dutch commercial market. This is probably attributable to the limited scale of the Dutch market and the strong international competition. The Netherlands cannot easily compete at international level in R&D. Clearly, if the Netherlands wants strategic autonomy, it must invest more in cryptography.

# 5. PENDING DEVELOPMENTS IN CRYPTOGRAPHY

This section outlines the four developments that are going to have a big impact on Dutch society in both the short and the long term. Figure 3 presents an overview of all four, identifying whether a development poses a threat or offers an opportunity to the Netherlands. An estimate is also offered of how soon these developments will take place. The following sections deal extensively with these developments.

*Figure 3: Explanation of the four main developments in cryptography, divided into opportunities and threats and spread over time to value: 1. securing new technical environments (grey); 2. migration to post-quantum cryptography (orange); 3. cryptography in decentralised solutions (green); 4. formal verification (blue).*




The formulation of these developments is the fruit of cooperation between representatives of industry, government and knowledge institutions in the Netherlands. No further developments emerged during the conversations held.

The developments are similar in terms of scope, with the exception of *securing new technical environments*. There are so many new technical environments to secure before they can be used in high-security situations, that this development is broader in scope compared to the others.

## 5.1 SECURING NEW TECHNICAL ENVIRONMENTS

There is a growing supply of new digital products that do not guarantee unilateral security. The use of these techniques does not present any problem outside the high-assurance domain. However, this gives rise to a mismatch between the technology normally used at work and technology that meets strict security requirements. This represents a very real problem in practice, both for government and in the corporate sector.

This development begins with a number of specific examples of developments in digital technology that have become normal, but whose unilateral security development still has some way to go. The examples are subdivided according to the reference model in Section 3.1.

### DATA IN TRANSIT

- **Connectors** keep networks of different security levels separate, but possibly allow data exchange, e.g. via (advanced) data diodes.
- **High-performance encryption** can be used to exchange data at high-assurance level with high bandwidth (specifically, this means further development of existing line encryption).
- **Industrial applications** to secure SCADA/ICS systems. Traditionally, these are standalone systems without internet access, though they are now increasingly connected to the corporate network. Examples of how cryptography can help to mitigate the risks of linked SCADA/ICS systems are restricting access via data diodes and authentication of the different systems and of the integrity of exchanged data. We would explicitly point out that the usefulness of encrypting information in a SCADA/ICS system has been questioned;[6]
- **Internet of Things (IoT) applications** allow secure handling of IoT equipment and networks. This equipment is often not capable of handling powerful cryptographic protocols. "Lightweight" cryptography will need to be developed for this specific purpose.

### DATA AT REST

- **Data carriers** that allow secure movement of data sound like a problem solved. However, for the time being, it is not possible to use data carriers such as USB sticks to move data at high-assurance level. This is not a minor problem, because an intercepted USB stick is prone to attack in many ways. A secure data carrier must, by contrast, be proof against such attack.
- **Cloud storage** means data can be stored securely in the cloud. In everyday life, storing data in the cloud poses no problem. This changes when the stored data are classified, because the main cloud providers are foreign companies. TNO has published a report offering guidance on this, such as local encryption of the file or using a new, trusted cloud service.[7]

### DATA IN USE

- **Workstations** that are secure for homeworking or work at different sites are rare. At low-assurance level, a home workstation is possible with limitation of the functionality of the installed software. However, this is certainly not possible at high-assurance level. To be specific, this means developing workstations with less connectivity in the installed software, secure internal storage media and a secure outward connection.
- **Video calls** are the logical successor to secure telecommunications. The coronavirus pandemic has revealed how important video calls are. The security of video call applications depends on the underlying service provided. Solutions are available for the low-assurance domain, but at high-assurance level, this development has yet to be realised.

### OTHER

- **Hardware acceleration** can ensure more intensive cryptography. Custom-developed processors accelerate encryption, facilitating processes that are complex in cryptographic terms. These processors are already available on a large scale, but for now, it is unclear to what extent the knowledge relating to hardware acceleration for cryptography exists in the Netherlands.
- **Identity, authentication and key management systems** form the basis of cryptographic solutions. These solutions serve specifically to make room for granular access control to digital services. Especially in the case of connectors between networks of different classification levels, sound administration of user identity, role and related keys is definitely of critical importance.

Most examples can in principle be solved with currently available, unilateral cryptographic techniques. Little additional fundamental knowledge is required to realize these solutions. However, investment is still necessary in the implementation stage of the development. After all, these solutions require more than pure cryptography. To make these applications usable in the high-assurance domain, the development will have to comply with strict requirements and, in addition, be controllable.

6. *https://ieeexplore.ieee.org/document/8340732*
7. *TNO report: Deepening value chains: basis of the road map 'secure working in an insecure cloud'*

The examples cover a very wide range of product categories, making this a somewhat more extensive development. However, precisely because of its breadth, this development has a major impact on society. A generally enhanced security level is of great value to Dutch strategic autonomy and is also feasible in the relatively short term.

## 5.2 MIGRATION TO POST-QUANTUM CRYPTOGRAPHY

The greatest threat to much of the asymmetric cryptography currently in use is the development of the quantum computer. Sufficiently powerful quantum computers can break the underlying mathematics of commonly used asymmetric cryptography. By about 2035, quantum computers are very likely to be sufficiently powerful to endanger cryptography[8].

As a result, the confidentiality of all asymmetrically encrypted information will be compromised, including all asymmetrically exchanged keys. This will also put the confidentiality of all information exchanged with these keys at risk. For state players, it is feasible, and relatively cheap, to intercept and store all today's encrypted information and wait until it can be decrypted by a quantum computer. This *"store now, decrypt later"* approach makes secrecy almost impossible for 15+ years.

There are several options for replacing quantum-insecure with quantum-safe cryptography. The possibility of a quantum-based communications network is being investigated, focusing specifically on *quantum key distribution*. This method uses quantum effects to agree a key between two parties. This key can then be used for symmetric encryption of data. Although the technology is promising, its development will not come in time to protect against the *store now, decrypt later* scenario. Moreover, this technology needs a whole new infrastructure and cannot cover all aspects of asymmetric cryptography. Another approach to a solution is to use only symmetric cryptography, as was the norm before the introduction of asymmetric cryptography.

A possible solution with a shorter payback time is migration to post-quantum cryptography. This is cryptography that is resistant to quantum computer attacks and is not based on quantum mechanics, but on mathematical protocols—like the cryptography we are accustomed to using. These involve mathematical problems that are hard to solve, even for a quantum computer. Decades of research have already been spent on this. The Netherlands is playing a leading role internationally and has a great deal of experience in post-quantum cryptography.

Currently, a worldwide process is under way to standardise post-quantum cryptography[9]. There are proposals with key involvement of Dutch knowledge institutions in this. The standardisation process is going to indicate a number of methods that can presumably guarantee the functionality of asymmetric cryptography. These presumptions are based on decades of academic work on the security of post-quantum cryptography.

The ideas deriving from the standardisation process will somehow have to find their way into end-products. Hybrid cryptosystems can be expected, which will combine post-quantum with existing, asymmetric cryptography. This leaves room for further cryptanalysis[10] and side-channel analysis of the post-quantum methods in practice. These analyses may, for example, lead to key-length adjustments.

The transition to post-quantum cryptography will not happen by itself. The entire Dutch value chain will have to work on it. To some extent, this work can proceed in parallel. While the science dedicates itself to developing post-quantum cryptography, industry can already concentrate on end-product crypto-agility, so that the migration can take place more easily in the future.

8. *TNO position paper "Migration to quantum-safe cryptography: about making decisions on when, what and how to migrate to a quantum-safe situation"*
9. *https://csrc.nist.gov/projects/post-quantum-cryptography*
10. *Cryptanalysis entails a mathematical/algorithmic study of how much security a cryptographic system offers (per bit of key length).*

## 5.3 CRYPTOGRAPHY IN DECENTRALISED SOLUTIONS

The development of multilateral cryptography offers new possibilities outside the commonly used unilateral cryptography: carrying out secure computation in the absence of mutual trust, while keeping individual input secret. Effectively, decentralisation takes place: control of the data rests with the user rather than in a centralised cloud environment. This decentralisation is technology driven. The opportunities that this development will offer to businesses and government are not yet known.

In practice, the applications of multilateral cryptography will soon be available. The next few years will reveal what possibilities and applications multilateral cryptography can offer in practice. The business sector is experimenting widely with these techniques at the international level.[11] In the Netherlands, too, applications of *secure multi-party computation*, *secure sovereign identity* and *zero-knowledge proofs* are subjects of research. Our expectation is that applications of decentralised techniques will come to the market in the Netherlands in various domains in the near future.

A specific example of decentralisation is data exchange in health care[12]. All medical data are highly confidential and personal. But these data are also valuable and can contribute to research into all kinds of diseases. Decentralisation gives patients control over their own data, and they can decide what to share or not to share with researchers. Moreover, because patients dispose of their decentralised data themselves, the data can be shared regardless of which health care institution would normally store them. Thus, data gathered from multiple care facilities can be analysed with due respect for privacy, and databases do not require interlinking.
Thus, decentralisation brings new opportunities and possibilities in a responsible manner.

Decentralisation is a technological development that will also have an impact in the longer term. Therefore, it is crucially important to keep it secure against known future threats such as quantum computers. Major development work is in progress to make this decentralisation feasible with post-quantum cryptography.

## 5.4 FORMAL VERIFICATION OF CRYPTOGRAPHY AND CRYPTOGRAPHIC SOURCE CODE

In practice, cryptographic end-products are trusted with incredibly sensitive information. This trust relies on the cumulative work of cryptographers. All aspects of a cryptographic method are investigated through years of testing via cryptanalysis. With the passage of time, this critical research generates trust in the cryptographic method. It is a very costly and labour-intensive process, part of which can be automated by formal verification.

A similar problem occurs in the software: programmers' trust that their code does what it is supposed to do derives from extensive software testing. Another route is formal verification of the software. This is an a computer science technique used to determine whether software has the features it is supposed to have, e.g. no dead ends. This is a non-trivial task, because software is nowadays highly complex. Nevertheless, scientists have been successful in the formal verification of highly complex software packages.[13]

The expectation is that developments in formal verification will increasingly become applicable to cryptographic implementations and secure software in general. In the longer term, it is expected that formal verification will increasingly be able to bolster human trust at all levels of a cryptographic end-product. Examples of formally verified security software are available at various levels, such as the operating system[14], widely used cryptographic protocols[15] and compilers[16].
Although formal verification has undergone much development, its application to cryptography

11. *Examples: https://polkadot.network/; https://web3.foundation/; https://dfinity.org/*
12. *https://www.tno.nl/en/tno-insights/articles/privacy-friendly-data-technology-expands-oncology-research-opportunities/*
13. *MIT 6.822, Spring 2021.*
14. *Such as seL4, a formally verified operating system.*
15. *Such as miTLS, a formally verified TLS implementation from Microsoft Research's Project Everest.*
16. *CS 6120: CompCert: Formally Verified C Compiler (cornell.edu).*

still requires fundamental research. Specifically, the science is now focusing on:
- Verification of the cryptographic protocol, examining whether the protocol really meets certain security claims;
- Verification of the software implementation, examining whether the implementation does in fact conform to the protocol, that it contains no errors and that the implementation contains no possible side-channels.

The use of formal verification should make it possible to provide open-source cryptography with extra certainty. This facilitates greater use of different open-source implementations and thus offers additional high-quality alternatives to software developed by national and international companies. Furthermore, formal verification plays an important role in controlling software developed by companies, which is often so complex that human verification is only possible to a limited extent.

The potential of formal verification of cryptography is immense and offers great opportunities for the Netherlands. Because much fundamental research is still necessary, the real value of formal verification of cryptography will only emerge in the longer term.

# 6. CONCLUSION

Cryptography is the bedrock of digital security and is important to the strategic autonomy of the Netherlands. The landscape of cryptography is constantly evolving, and new threats and opportunities are continuously emerging. The Netherlands has a strong ecosystem in the field of cryptography and is therefore well placed to anticipate these threats and opportunities.

New ground covered by this survey are the four major developments in cryptography, with associated threats and opportunities for the Netherlands. First, in the short term, making new technical environments secure creates space for new product development. Secondly, the migration to post-quantum cryptography already requires great flexibility along the entire value chain. Thirdly, the deployment of cryptography for new, decentralised applications offers new economic opportunities. Fourthly, in the future, formal verification of cryptography will open new possibilities for the development of cryptography, because this technique will consolidate trust in the cryptography used.

The described developments present both challenges and opportunities. In the short term, decentralisation offers new economic opportunities, just as formal verification does in the longer term. However, it is important to continue investing in knowledge and development, so that these economic opportunities are actually exploited.

There will be major challenges in mitigating the threat from quantum computers and new digital environments. It is dangerous to underestimate how great these threats are, and no single party can independently realise all solutions. Close cooperation throughout the value chain is therefore required.

The Netherlands is well placed from the outset to exploit the future opportunities and mitigate the threats. However, expertise in cryptography and its implementation in particular is very scarce. Further investment is therefore necessary to build up enough knowledge and capacity. The following are specific recommendations for the direction of these investments:

1. Map out:
    a. Which players are active in Dutch business, both as suppliers and as consumers (Chapter 4 gives an initial indication);
    b. What obstacles business encounters in bringing a new cryptographic end-product to market. In doing so, consider the time it takes to have a cryptographic end-product assessed, the associated risk and the shortage of personnel;
    c. What barriers new businesses face in their market entry. In doing so, consider the strict security requirements a new business must meet.
2. What role can the government play in removing the obstacles.

The Ministry of Economic Affairs and Climate Policy's cryptocommunications roadmap will tackle these points.

# 7. THE CRYPTO-COMMUNICATIONS ROADMAP

In view of the complexity of the developments and the challenges that lie ahead for the value chain, it is time as an ecosystem to work out a route to implementation. As the authors of this survey, we invite you, our readers, to cooperate in the Ministry of Economic Affairs and Climate Policy's cryptocommunications roadmap, which will map out the needs, challenges and possibilities for the ecosystem. The plans set out in the roadmap will lend initial impetus to strategic investments in cryptography.

The process leading to a shared road map begins in May 2021 and would benefit from your participation. The road map will be realised through interviews and co-creation sessions. The developments discussed in this survey form a preliminary approach to the subjects that will be reflected in the road map. Your input to the road map, and your help in configuring it, will be very welcome as we work towards making the Netherlands a Crypto Country.

**Road Map contact:**
dcypher cooperation platform:
info@dcypher.nl