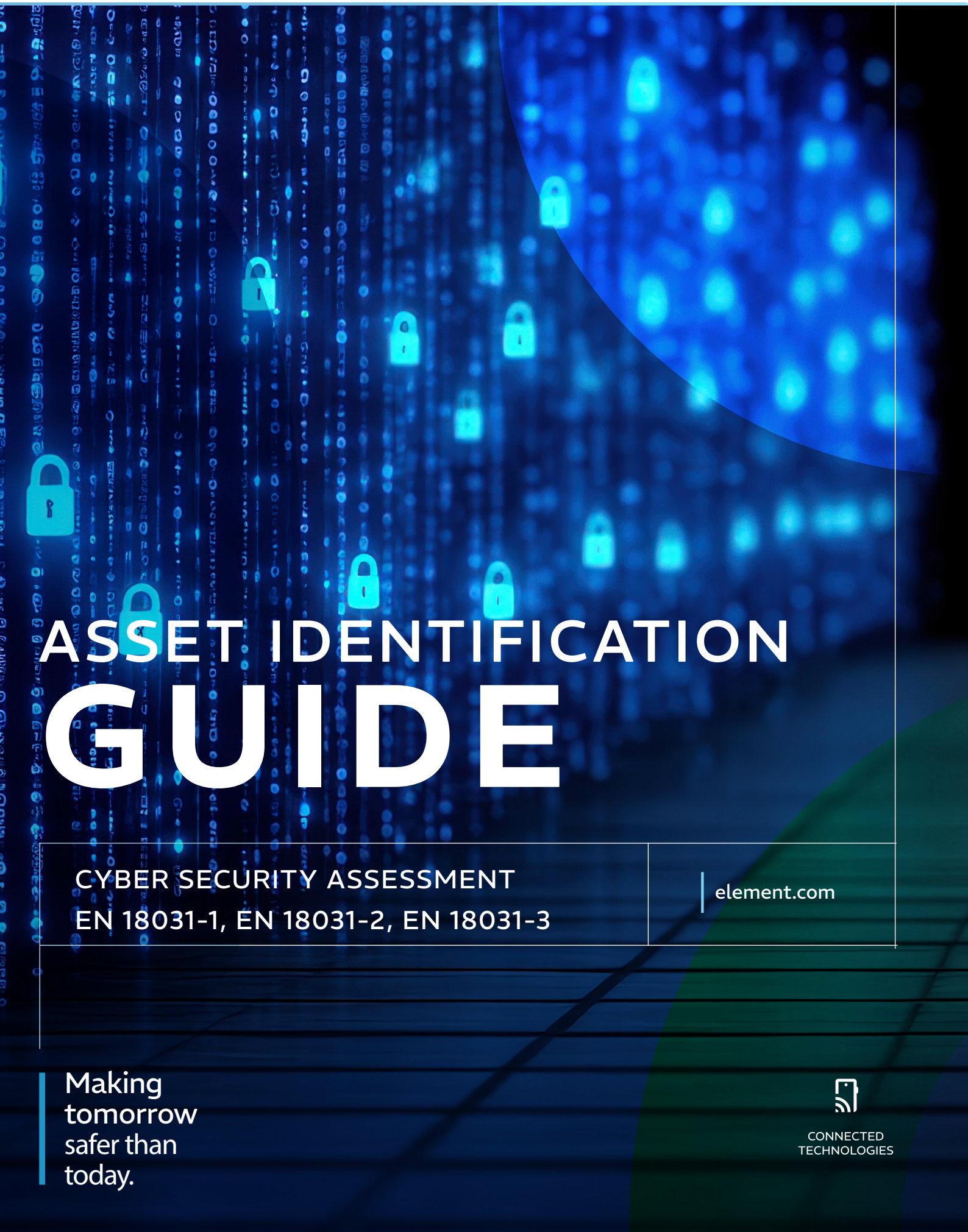
element

SECURITY PATTERN



ASSET IDENTIFICATION GUIDE

CYBER SECURITY ASSESSMENT
EN 18031-1, EN 18031-2, EN 18031-3

element.com

Making tomorrow safer than today.

CONNECTED TECHNOLOGIES

CONTENTS

2. Introduction
3. EN 18031-1
5. EN 18031-2
7. EN 18031-3
10. Worked Example One: IoT sensor
11. Worked Example Two: Attendance Tracker
13. Meet the Authors
14. The Element Advantage
14. Security Pattern: Your Benefits

INTRODUCTION

The EN 18031-X series of standards are written around a set of decision trees, which, in theory, should make the process for assessment very straightforward for test lab and manufacturers, regardless of their level of experience in cyber security product assessment. However, the majority of these decision trees start with a set of 'For each…' statements, and so the first step in the process is populating a list of entries for each of these statements, such that the decision trees can be worked through for each combination of entries in these lists.

In some instances, this is trivial. The statement **'For each external interface'** is easy to understand and it's therefore straightforward to populate this list. In some cases though, this is not the case. In particular, the **'For each network asset'** statement is particularly challenging for anyone not well-versed in product cyber security. "What even is a network asset?", you might ask.

Unfortunately for anyone attempting to assess a product to one or more of these standards, the answer to this question is complex, and is further complicated as the three standards ask for slightly different combinations of the following:

- Security assets
- Network assets
- Privacy assets
- Financial assets.

So, it should just be as simple as finding the definitions for each of the items above in each of the standards. In reality, of course, it is not so straightforward. The definitions of each item above refer to various other definitions (and are subtly different between standards). See the diagrams on page 4 for the definitions in the EN 18031-1 standard.

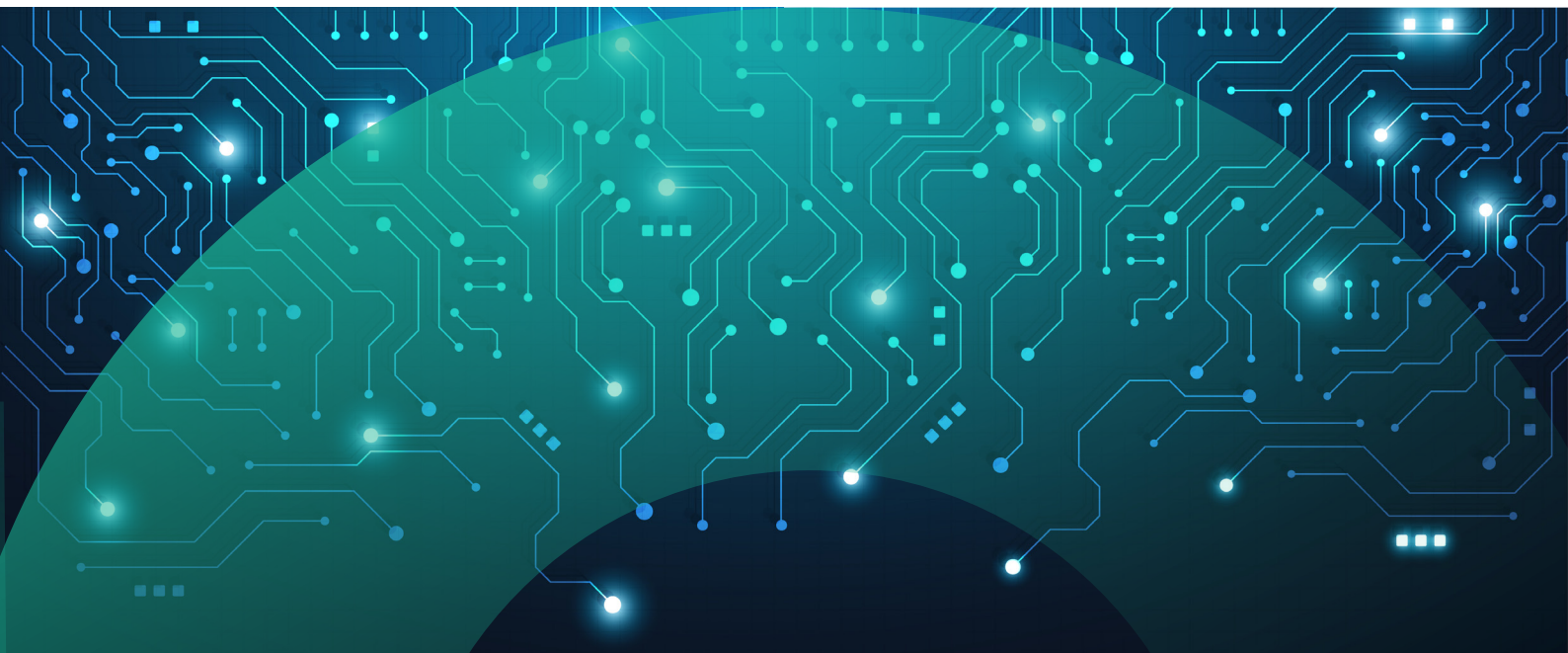
The definitions in the EN 18031-2 standard are more complex than those in EN 18031-1, and those in EN 18031-3 are more confusing still, even including a circular reference between a security asset and a security function. See the following pages for these diagrams.

To help cut through some of this confusion, this guide aims to provide a straightforward process that manufacturers can follow to ensure they identify all of the relevant assets their products possess.

Asset Identification

How should a manufacturer begin the process of dentifying all of the different assets that their equipment possesses? Rather than starting at the left-hand-side of the diagrams which follow, and asking "what assets does the product possess?", a potentially easier route is to start at the right-hand-side, asking the questions "what functionality does the product possess?" (and, for EN 18031-2 and EN 18031-3, "what personal information and what financial data does the product process?").

This is effectively a top-down approach, starting with everything the product does, and working backwards to determine which are relevant assets. Here is the process broken down into four simple steps for each standard.



EN 18031-1

The asset definitions in EN 18031-1 all ultimately point to **network functions** or **security functions**, and therefore the steps will be as below. It may be helpful to read these steps with the diagram of definitions open alongside, and follow the arrows from right to left at each step.

1. STEP ONE

Step one is to create a comprehensive list of all functionality on the product.

2. STEP TWO

Step two is then to determine which items from the list in step one are either providing or utilizing network[1] resources (thus making them a **network function** and therefore also a **network asset**), or are relevant to protect from harming the network or its functioning or misusing network resources (thus making them a **security function** and therefore also a **security asset**).

3. STEP THREE

Step three is then, for each of these identified **network functions** and **security functions**, to make a comprehensive list of all of the **security parameters** and **network function configurations** that these functions rely on.

4. STEP FOUR

Step four is then to determine which of these **security parameters** and **network function configurations** could lead to harming the network or its functioning or misusing network resources if they were either manipulated (thus making them either a **sensitive security parameter** or a **sensitive network function configuration** and therefore also either a **security asset** or a **network asset**) or disclosed (thus making them either a **confidential security parameter** or a **confidential network function configuration** and therefore also either a **security asset** or a **network asset**).

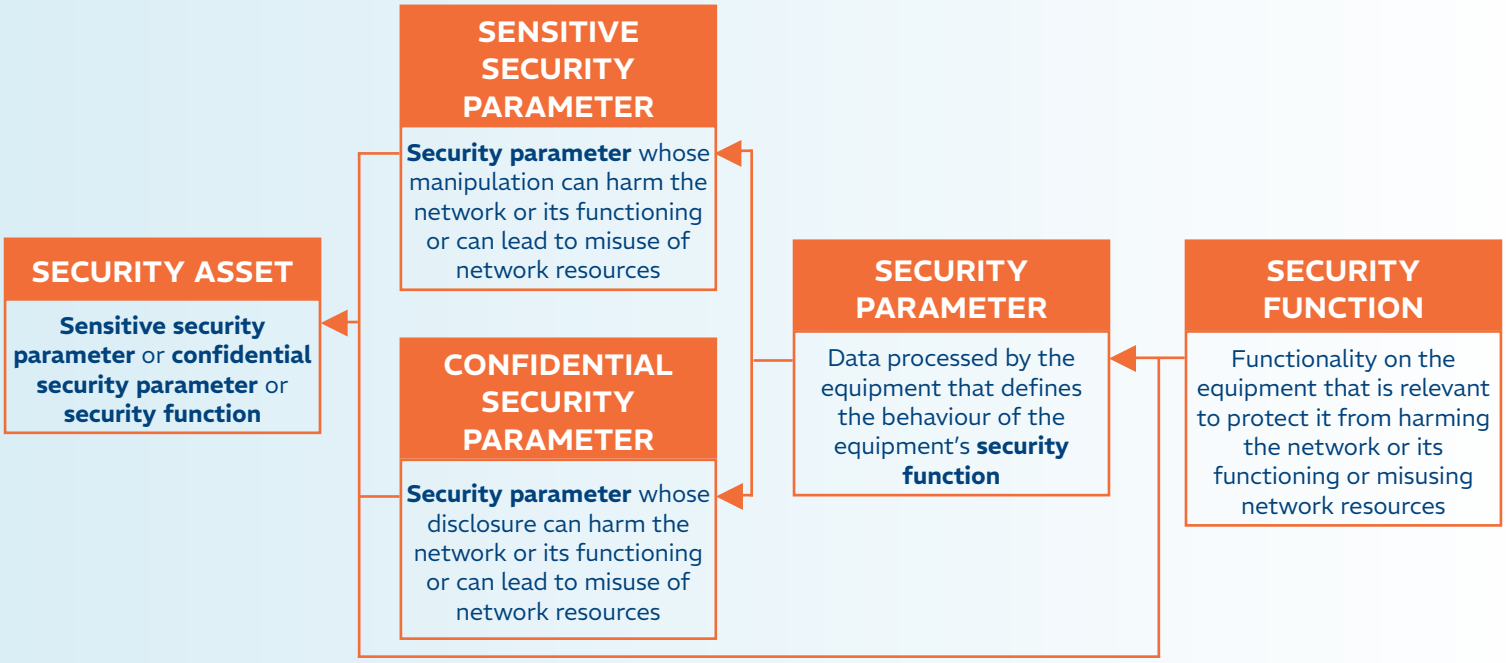
OUTPUT

The combined outputs from both step two and step four are then a complete list of all of the **network assets** and **security assets** the equipment possesses.

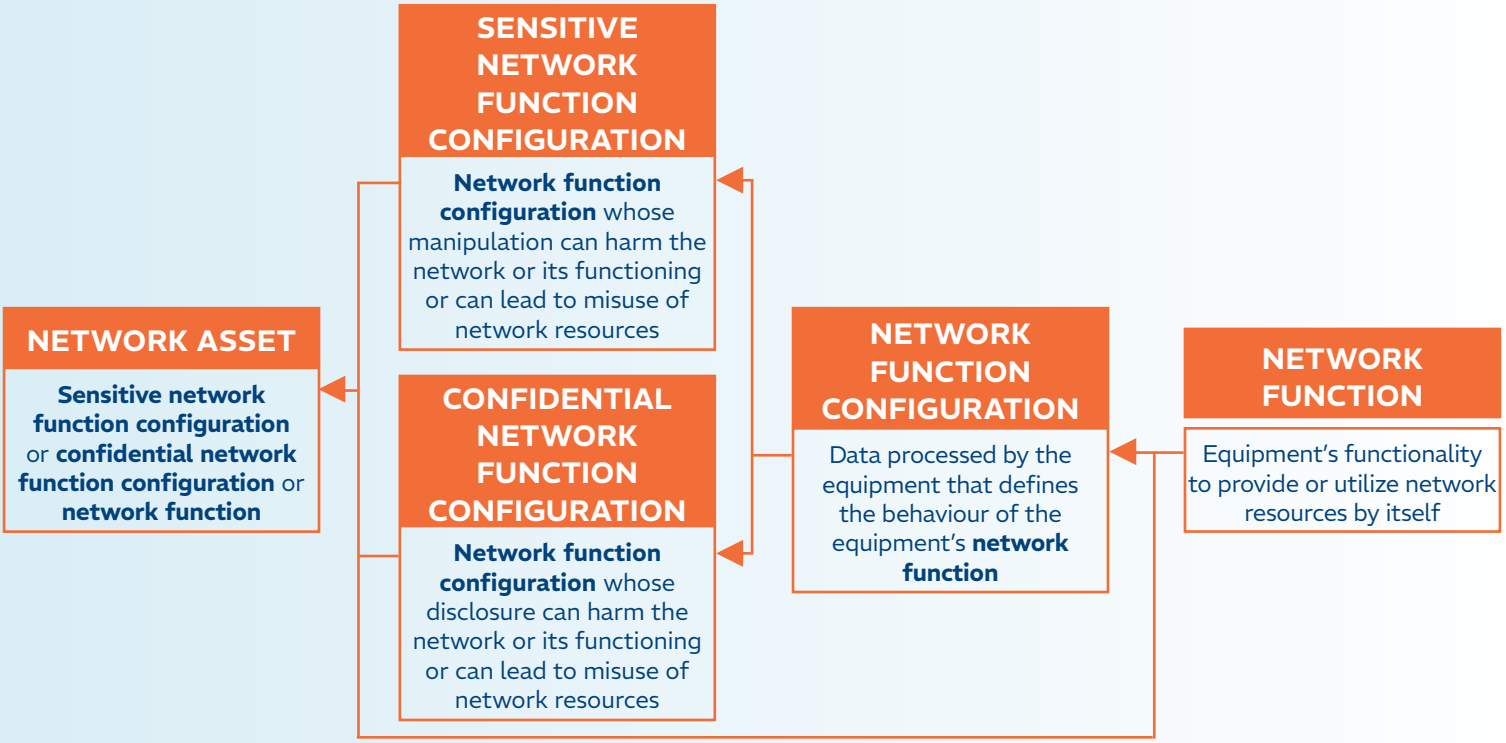
NOTES ON EN 18031-1 DEFINITIONS

[1]One point worth noting is that there is no concrete definition of what a network actually is. Some people argue that a network means potential for connecting more than two devices, and therefore interfaces like a serial port would not be a network interface (as they only ever connect two devices), but Ethernet would be, for example.

SECURITY ASSET



NETWORK ASSET



EN 18031-2

The asset definitions in EN 18031-2 all ultimately point to **personal information** or **security functions**, and therefore the steps will be slightly different to those above. Again, it may be helpful to read these steps with the diagram of definitions open alongside, and follow the arrows from right to left at each step.

0. STEP ZERO

Step zero (which we are calling step zero as it should probably have already been done long before attempting an assessment to any standard) is to create a comprehensive list of all personal information[2] (i.e. personal data, traffic data, and location data) processed by the product, and to identify which of these pieces of information could lead to a compromise of the user's or subscriber's privacy if they were either manipulated or disclosed (thus making them either **sensitive personal information** or **confidential personal information** and therefore also a **privacy asset**).

1. STEP ONE

Step one is, as above, to create a comprehensive list of all functionality on the product.

2. STEP TWO

Step two is then to determine which items from the list in step one are either processing personal information (thus making them a **privacy function** and therefore also a **privacy asset**, noting that this refers to any of the personal information listed above, not just those which are also privacy assets), or that ensure the personal data and the privacy of the user and of the subscriber are protected (thus making them a **security function** and therefore also a **security asset**).

3. STEP THREE

Step three is then, for each of these identified **privacy functions** and **security functions**, to make a comprehensive list of all of the **security parameters** and **privacy function configurations** that these functions rely on.

4. STEP FOUR

Step four is then to determine which of these **security parameters** and **privacy function configurations** could lead to a compromise of the user's or subscriber's privacy if they were either manipulated (thus making them either a **sensitive security parameter** or a **sensitive privacy function configuration** and therefore also either a **security asset** or a **privacy asset**) or disclosed (thus making them either a **confidential security parameter** or a **confidential privacy function configuration** and therefore also either a **security asset** or a **privacy asset**).

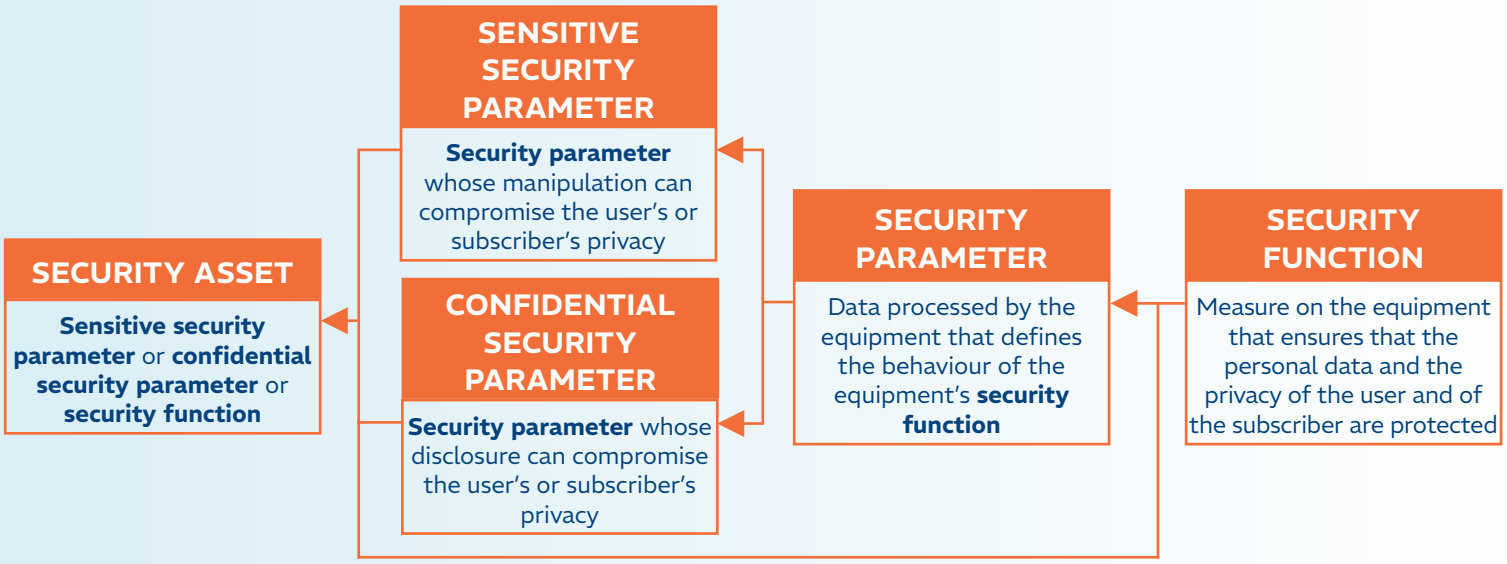
OUTPUT

The combined outputs from step zero, step two, and step four are then a complete list of all of the **security assets** and **privacy assets** the equipment possesses.

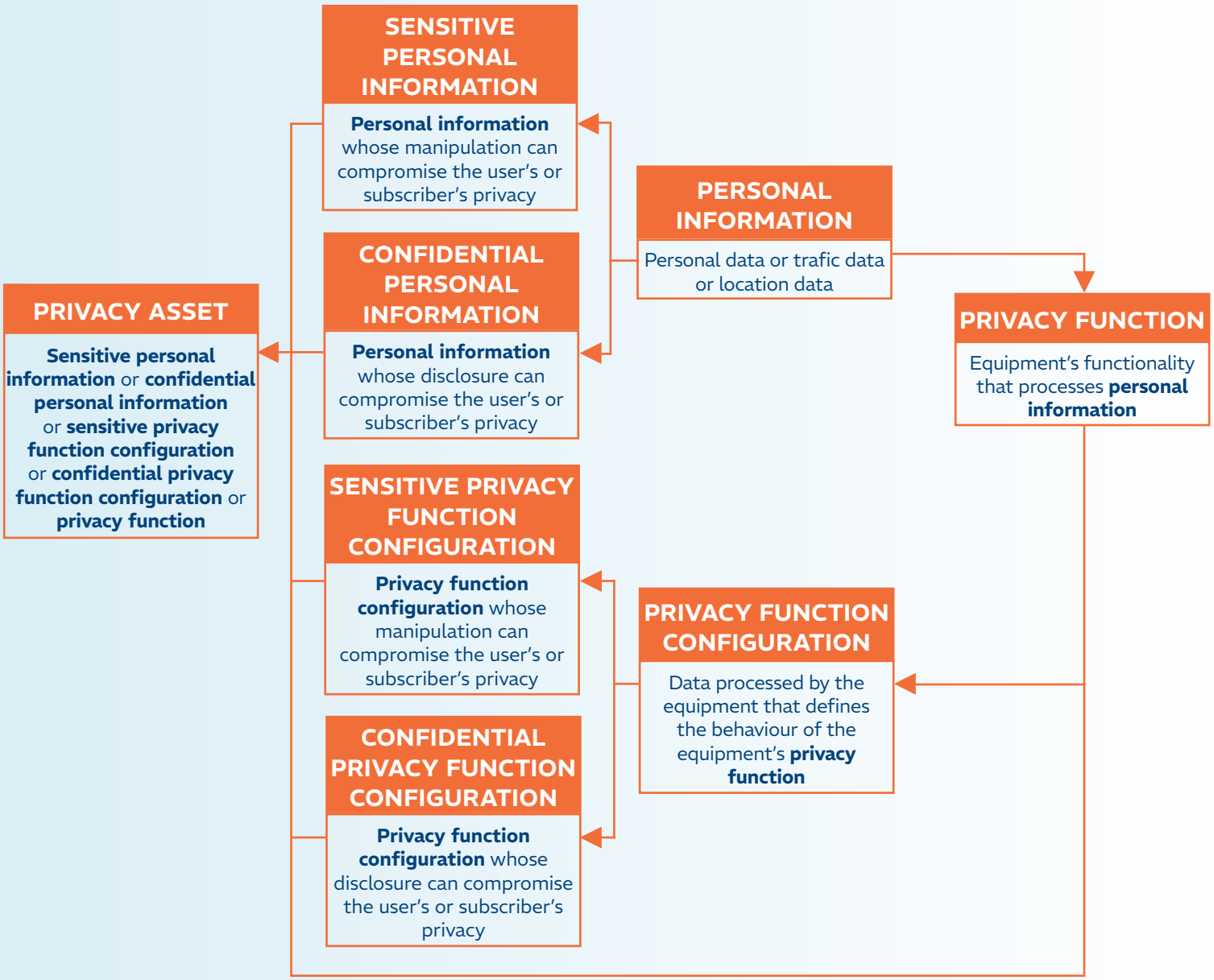
NOTES ON EN 18031-2 DEFINITIONS

[2] The terms personal data, traffic data, and location data are not defined in the standard, but are defined in Article 4(1) of Regulation (EU) 2016/679 (the General Data Protection Regulation), or in Article 2, points (b) and (c), of Directive 2002/58/EC (the Directive on privacy and electronic communications, or "ePrivacy Directive").

SECURITY ASSET



PRIVACY ASSET



EN 18031-3

The asset definitions in EN 18031-3 all ultimately point to **financial information** or **security functions**, and therefore the steps will be similar to those above. Again, it may be helpful to read these steps with the diagram of definitions open alongside, and follow the arrows from right to left at each step.

0. STEP ZERO

Step zero (which we are calling step zero as it should probably have already been done long before attempting an assessment to any standard) is to create a comprehensive list of all financial data processed by the product, and to identify which of these pieces of data could lead to a compromise fraud if they were either manipulated or disclosed (thus making them either **sensitive financial data** or **confidential financial data** and therefore also a **financial asset**).

1. STEP ONE

Step one is, as above, to create a comprehensive list of all functionality on the product.

2. STEP TWO

Step two is then to determine which items from the list in step one are either processing financial data (thus making them a **financial function** and therefore also a **financial asset**, noting that this refers to any of the financial data listed above, not just those which are also **financial assets**), or that protect[3] from fraud (thus making them a **security function** and therefore also a **security asset**).

3. STEP THREE

Step three is then, for each of these identified **financial functions** and **security functions**, to make a comprehensive list of all of the **security parameters** and **financial function configurations** that these functions rely on.

4. STEP FOUR

Step four is then to determine which of these **security parameters** and **financial function configurations** could lead to fraud if they were either manipulated or unauthorisedly modified (thus making them either a **sensitive security parameter** or a **sensitive financial function configuration** and therefore also either a **security asset** or a **financial asset**) or disclosed (thus making them either a **confidential security parameter** or a **confidential financial function configuration** and therefore also either a **security asset** or a **financial asset**).

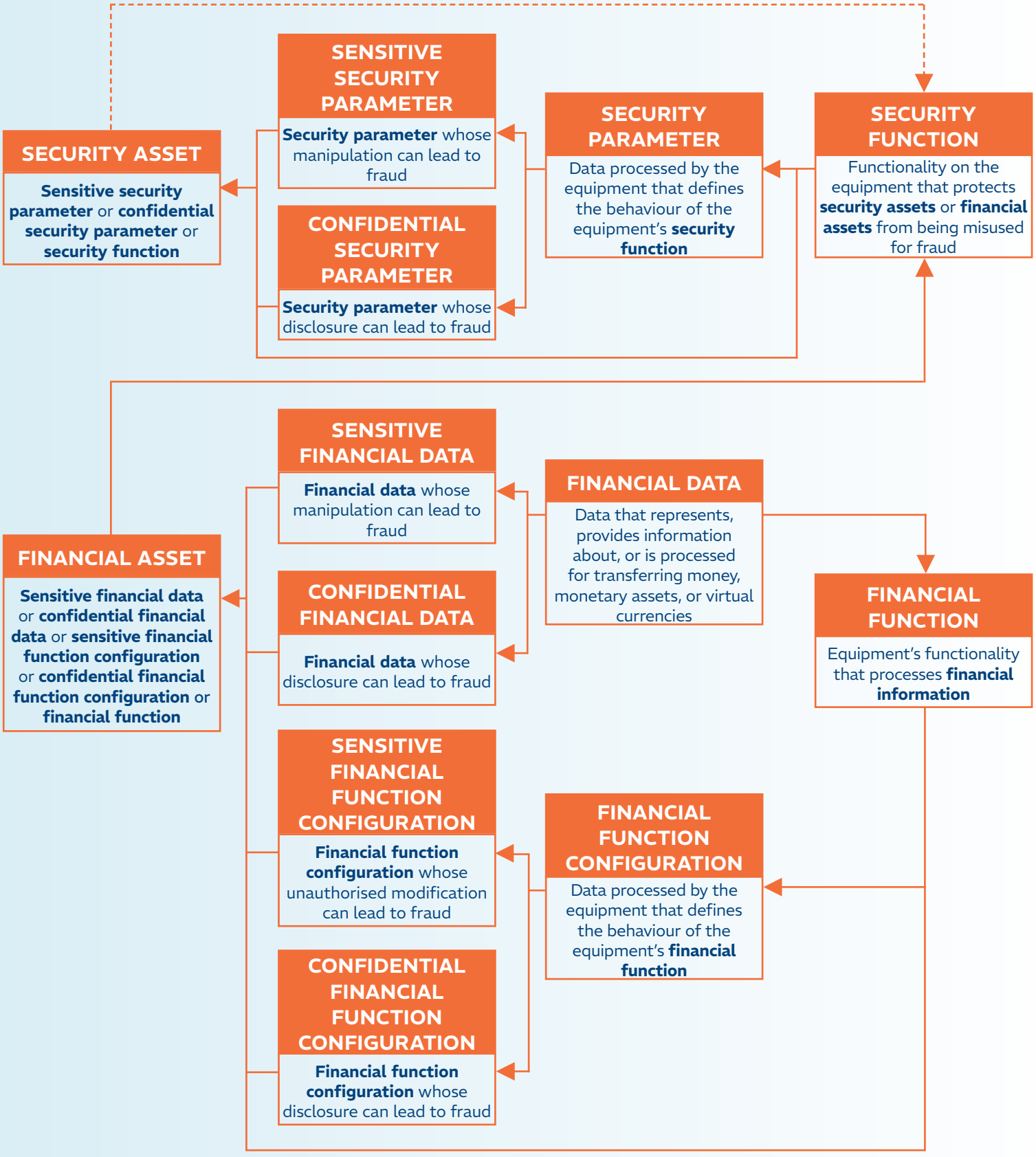
OUTPUT

The combined outputs from step zero, step two, and step four are then a complete list of all of the security assets and financial assets the equipment possesses.

NOTES ON EN 18031-3 DEFINITIONS

[3]There is a circular reference in the definition for security function in that it refers to a security asset, which includes any security function. A practical solution is to read this as simply being a function which protects financial assets (not other security assets) from being misused.

SECURITY AND FINANCIAL ASSET



WORKED EXAMPLE ONE - IOT SENSOR

Let's imagine a simple IoT environmental sensor, intended to be installed in a remote location to sense temperature and air quality, and to report this back over a cellular link to a back end server. In this example, only EN 18031-1 is applicable as the device does not process any personal or financial information.

Looking to our suggested method for EN 18031-1:

1. STEP ONE

Step one is to list all functionality.

2. STEP TWO

Step two is to determine which of these functions are either a network function or a security function.

STEP ONE	STEP TWO
List all functions	**Is this a network function or a security function?**
Temperature sensing	No
Air quality sensing	No
Cellular connectivity	Yes (network function)
Data processing	No

So we can see there is only one function that meets this criteria. This function (cellular connectivity) is our first asset. The other functions do not meet the definition of either a network function or a security function, and so we can discount them.

3. STEP THREE

Step three is to list all of the configurations this function depends on.

4. STEP FOUR

Step four is to determine which of those are confidential or sensitive (i.e. could their disclosure or manipulation harm the network or its functioning or lead to misuse of network resources).In this example, we only run through these steps once (as there is only one relevant function, the cellular connectivity). For more complex devices, these steps would be followed for each of the functions identified above.

In this example, the cellular connection depends on an IMSI, an IMEI, and the secret key stored in the SIM. Neither the IMSI or IMEI are confidential (their disclosure does not present a risk) or sensitive (their manipulation does not present a risk), but the SIM secret key is confidential (as its disclosure could lead to misuse of network resources).

STEP THREE	STEP FOUR
List all configurations or parameters	**Is this configuration or parameter either sensitive or confidential?**
Cellular IMSI	No
Cellular IMEI	No
SIM secret key	Yes (confidential)

OUTPUT

Combining the results from step two and step four gives us our complete list of network and security assets for this device:

1. Cellular connectivity (network function)
2. SIM secret key (confidential network function configuration).

WORKED EXAMPLE TWO - ATTENDANCE TRACKER

Let us now consider a slightly more complex device, a clocking-in-and-out system for use in a factory. The devices sit at the entrances and exits to a building and users can sign in and out by using an RFID fob or their fingerprint. The device has an Ethernet connection (using TLS) for backhaul, and a USB port for data export which relies on an admin user to log in. In this example, both EN 18031-1 and EN 18031-2 will be relevant, but EN 18031-3 will not be.

Following the process described above:

0. STEP ZERO

Step zero is to identify all of the personal information. This could include names, addresses, fingerprints etc., but for simplicity let's just lump these together and call them all "personal data".

In practice, this approach is acceptable provided each item of data is treated in the same way. If, for example, the names and addresses were stored or transmitted separately to the fingerprints, these should be considered as separate assets.

STEP ZERO	
List all personal information	**Is this information either sensitive or confidential?**
Personal data	Yes (confidential)

1. STEP ONE

Step one is then to make a list of all device functionality.

2. STEP TWO

Step two is to is to determine which of these functions are either a network function or a privacy function or a security function (noting the slight difference in definition of security function between the two standards).

STEP ONE	STEP TWO
List all functions	**Is this a network function or a privacy function or a security function?**
Fingerprint reading	Yes (privacy function)
RFID reading	No
Data processing	Yes (privacy function)
Ethernet connectivity	Yes (network function and security function)
USB connectivity	No
Admin login function	Yes (security function)

So we have four functions which meet the definitions of a network function or a privacy function or a security function, and which are therefore assets. In the above, data processing will be considered as an asset (whereas in the previous example it was not). Note that we are assuming no personal information is transferred over RFID, but this may not always be the case for all devices that use RFID. The Ethernet connectivity function is considered both a network function and security function, as it both uses network resources and is relevant to protecting the data.

3. STEP THREE

Step three is then to list all of the configurations or parameters these four functions depend on.

4. STEP FOUR

Step four is to determine which of those configurations or parameters are confidential or sensitive (i.e. could their disclosure or manipulation harm the network or its functioning or lead to misuse of network resources or compromise the user's or subscriber's privacy).

The table below is broken into sections to make this clearer.

STEP THREE	STEP FOUR
List all configurations or parameters	**Is this configuration or parameter either sensitive or confidential?**
Fingerprint reading	
None	N/A
Data processing	
None	N/A
Ethernet connectivity	
MAC address	No
TLS key	Yes (confidential)
Admin login function	
Admin usernames	No
Admin passwords	Yes (confidential)

OUTPUT

In this example, two of the functions (fingerprint reading and data processing) do not have any parameters or configurations (or at least none worth noting – the fingerprint scanner may well have settings for brightness or timing etc., but for simplicity let's assume not).

The Ethernet connectivity depends on a MAC address and TLS keys. The MAC is public and is not confidential or sensitive, but the TLS keys will be confidential as their disclosure could compromise the personal information.

Similarly, the admin login function will depend on a username, which may be public, and a password, which will be confidential. Note that this is just an example, and actually a real device may use a password hash, not a password, which may be sensitive but not confidential (i.e. it should be protected from manipulation but not necessarily from disclosure).

Combining the results from step zero, step two, and step four gives us our complete list of network, privacy, and security assets for this device:

1. Personal data (confidential personal information)
2. Fingerprint reading (privacy function)
3. Data processing (privacy function)
4. Ethernet connectivity (network function and security function)
5. Admin login function (security function)
6. TLS key (confidential security parameter)
7. Admin passwords (confidential security parameter).

MEET THE AUTHORS

Alex Toohie | Technical Solution Manager | Element

Alex has been working in regulatory compliance for more than a decade, both within Element's Connected Technology & Mobility group and in industry as Compliance Manager for a global leader in wireless intruder and fire alarm systems.

As Element's Technical Solution Manager, Alex draws on a wealth of experience in UKCA and CE marking (covering RED, EMCD, CPR, ATEXD, RoHSD, etc.), FCC and ISED, as well as the evolving global product cyber security requirements, to help manufacturers find the most effective and cost-efficient certification paths for complex and varied radio equipment.

Filippo Melzani | CTO & Co-Founder | Security Pattern

Filippo has developed a wide experience on building cryptographic components with different needs in terms of performance, footprint, and security. He continuously investigates how security elements can be mixed in a system guaranteeing they are used at their best.

Filippo is a promoter of innovative formal methodologies to support the development and the evaluation of secure devices and systems. He is co-author of 12 scientific publications, participates in several program committees of security-related workshops and conferences, and is the author of fourregistered patents in the field of secure cryptographic implementations.

Arianna Gringiani | Security Expert | Security Pattern

Arianna graduated in Mathematics with a specialisation in Cryptography and began her career at Security Pattern, where she works as a Security Expert. She has focused on regulatory compliance for cybersecurity legislation affecting connected products, including CRA and RED, and supports manufacturers in understanding and applying these requirements. Arianna's work includes systematic security assessments of IoT devices, training on cybersecurity regulations, and the development of methods to evaluate product security from both technical and compliance perspectives.

THE ELEMENT ADVANTAGE

Element's advanced wireless testing capabilities encompass radio spectrum usage, EMC, safety, interoperability, environmental, reliability, RF exposure, and cyber security.

As a leading authority in testing and certification, Element is one of very few labs to offer specialist services such as Dynamic Frequency Selection (DFS), Over-the-Air (OTA), and Specific Absorption Rate (SAR) tests.

As well as being UKAS accredited to ISO/IEC 17025:2017, Element is a Notified Body for RED, EMCD, and ATEX Directive, an Approved Body for UK Radio, EMC, and Explosive Atmospheres Regulations, and a certification body under the IECEE CB Scheme. Our expert team will support you through the certification process for key regulatory and voluntary radio certifications, meaning we can project manage your test and certification programs for multiple markets to reduce costs and deliver faster certification times.

For more information about Element and our testing and certification services, or to speak to our experts, contact us today.

| contact.us@element.com
| www.element.com

SECURITY PATTERN: YOUR BENEFITS

We have supported numerous organisations to comply with EN 18031, plus requirements from other standards such as IEC 62443 (Industrial), IEC 81001 (Medical), ISO/SAE 21434 (Automotive) and ETSI EN 303 645 (Consumer IoT).

We are active participants in the cryptographic research community and in two European funded projects. Personnel of Security Pattern has co-authored 50+ scientific papers and Guido Bertoni, our CEO, co-authors the NIST SHA-3 algorithm.

Each technical team member gained a pluriannual experience in the domains of security and crypto for microcontrollers, smartcards, automotive, wireless connectivity, ASIC and FPGA. We support device manufacturers in reaching their security and business targets by offering state-of-the-art consultancy, products and training.

We listen to the needs of technical people, managers, marketers, and customers, and offer pre-packed solutions as well as tailored services in order to fulfil all your security needs.

| hello@securitypattern.com
| www.securitypattern.com

element

Scan to find out more.

WHY CHOOSE ELEMENT?

Element Connected Technologies & Mobility, is a leading provider of testing, inspection, and certification services for connected devices and mobility solutions.

We provide comprehensive testing and certification services that ensure products meet international standards for connectivity, interoperability, and safety.

CONTACT

Our LinkedIn

Telephone: +44 (0) 808 234 1667 Web: element.com Email: contact.us@element.com

Making tomorrow safer than today.

CONNECTED TECHNOLOGIES