



Statens vegvesen
Norwegian Public Roads
Administration

Cybersecurity of NAP

Paal Aaserud
Masi Massiliano
Bard de Vries
Knut Evensen



Session agenda

- Cybersecurity of NAP

- Inventory questionnaire
- Introduction – Paal Aaserud
- Security building blocks – Massimiliano Masi
- Napcore-x – Bard de Vries
- METR – Knut Evensen
- Discussion – All

Introduction



Real threats

GPS Spoofing
Remote Hijacking of Vehicles



Data Breaches
Ransomware Cyber Attacks
Infrastructure Sabotage



Supply Chain Cyber Attacks
Malware cyber attacks
Derail city trams with injuries
Cause Power outages



Social engineering



European
Union

EU-wide legislation

NIS2
2022/2555

ITS
2023/2661
(2010/40/EU)

RTTI
2022/670
(2015/962)

CHAPTER I GENERAL PROVISIONS

Article 1

Subject matter

1. This Directive lays down measures that aim to achieve a high common level of cybersecurity across the Union, with a view to improving the functioning of the internal market.
2. To that end, this Directive lays down:
 - (a) obligations that require Member States to adopt national cybersecurity strategies and to designate or establish competent authorities, cyber crisis management authorities, single points of contact on cybersecurity (single points of contact) and computer security incident response teams (CSIRTs);
 - (b) cybersecurity risk-management measures and reporting obligations for entities of a type referred to in Annex I or II as well as for entities identified as critical entities under Directive (EU) 2022/2557;
 - (c) rules and obligations on cybersecurity information sharing;
 - (d) supervisory and enforcement obligations on Member States.

Article 2

Scope

1. This Directive applies to public or private entities of a type referred to in Annex I or II which qualify as medium-sized enterprises under Article 2 of the Annex to Recommendation 2003/361/EC, or exceed the ceilings for medium-sized enterprises provided for in paragraph 1 of that Article, and which provide their services or carry out their activities within the Union.
2. Regardless of their size, this Directive also applies to entities of a type referred to in Annex I or II, where:
 - (a) services are provided by:
 - (i) providers of public electronic communications networks or of publicly available electronic communications services;
 - (ii) trust service providers;
 - (iii) top-level domain name registries and domain name system service providers;
 - (b) the entity is the sole provider in a Member State of a service which is essential for the maintenance of critical societal or economic activities;
 - (c) disruption of the service provided by the entity could have a significant systemic risk, in particular for sectors where such disruption could have a cross-border impact;
 - (d) disruption of the service provided by the entity could induce a significant systemic risk, in particular for sectors where such disruption could have a cross-border impact;
 - (e) the entity is critical because of its specific importance at national or regional level for the particular sector or type of service, or for other independent sectors in the Member State;
 - (f) the entity is a public administration entity:
 - (i) of central government as defined by a Member State in accordance with national law; or
 - (ii) at regional level as defined by a Member State in accordance with national law that, following a risk-based assessment, provides services the disruption of which could have a significant impact on critical societal or economic activities.
3. Regardless of their size, this Directive applies to entities identified as critical entities under Directive (EU) 2022/2557.

DIRECTIVE (EU) 2010/40

amending

THE EUROPEAN

having regard to

or transmission of the draft legislation

ing regard to the proposal from the European Commission,

consulting the Committee of the Regions,

in accordance with the ordinary legislative procedure (7),

Commission's communication of 9 December 2020 entitled 'Sustainable and Smart Mobility Strategy – putting European

on track for the future' ('the Sustainable and Smart Mobility Strategy') identifies the deployment of intelligent transport

('ITS') as a key action for achieving connected and automated multimodal mobility, and therefore contributing to the

ation of the European transport system in order to achieve the objective of efficient, safe, sustainable, smart and resilient

logistics. The Sustainable and Smart Mobility Strategy also announced for 2022 a revision of Commission Delegated

(EU) 2017/1926 (7) to include mandatory accessibility of dynamic datasets, as well as an assessment of the need for

on rights and duties of multimodal digital service providers together with an initiative on ticketing, including rail

Directive should ensure that ITS applications in the field of road transport enable seamless integration with other

rt, such as rail or active mobility, thus facilitating a shift to those modes whenever possible, to improve efficiency

Smart Mobility Strategy confirms the objective of bringing the death toll for all modes of transport in the

by 2050. Several actions in the scope of Directive 2010/40/EU of the European Parliament and of the

to the safety of road users, such as eCall, road safety-related traffic information services and information

and secure parking places for trucks and commercial vehicles, as certified in accordance with

Regulation (EU) 2022/1012 (7).

Commission of 11 December 2019 entitled 'The European Green Deal' highlights the increasing role of

multimodal mobility, together with smart traffic management systems enabled by digitalisation, and the

in sustainable transport and mobility services that can improve mobility, reduce congestion and

in areas, and foster the transition to cleaner modes of transport by promoting modal shift and better

in this evolution, consideration of appropriate technical screening criteria within the framework of

the European Parliament and of the Council (7) (also known as the taxonomy regulation) to support

use of data in making transport chains more sustainable, secure, efficient and resilient, calls for

framework with other initiatives aimed at harmonising and facilitating data sharing in the

tors with a multimodal perspective such as the common European mobility data space and its (6)

056 of the European Parliament and of the Council (7), and the work pursued by the Digital

) while taking into consideration rules on data protection and privacy.

transport, increase road safety and reduce congestion, the deployment and use of intelligent

should be further developed on the trans-European transport network.

on in road transport create employment opportunities by developing new projects in the industry.

OF THE COUNCIL

port Systems in the field of road

COMMISS

IVE 2010/40/EU of the European Parliament and of the Council with regard to
real-time traffic information services
(Text with EEA relevance)

COMMISSION,

Treaty on the Functioning of the European Union,

Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the
elligent Transport Systems in the field of road transport and for interfaces with other modes of transport (7), and in
thereof,

Article 5 of Directive 2010/40/EU sets as a priority action the provision of EU-wide real-time traffic information services for
ment and use of specifications and standards.

(1) of Directive 2010/40/EU requires the Commission to adopt specifications necessary to ensure compatibility,
rability and continuity for the deployment and operational use of Intelligent Transport Systems (ITS) for the provision of
le real-time traffic information services. The Commission establishes these specifications in Commission Delegated

tion (EU) 2015/962 (7), with a view to improving the accessibility, exchange, re-use and update of data required for the
ion of high quality and continuous real-time traffic information services across the Union.

continues to provide the contextual basis for the generation of real-time traffic information. As the deployment of ITS
derates across the Union, it requires continued support in the form of increased and seamless access to existing and new data
es relevant to the provision of real-time traffic information services, with a higher geographical coverage. Therefore, an update
the requirements on data provision is necessary to continue ensuring effective re-use in information services to end users. These

updated requirements can potentially affect the entire data chain, from data sourcing, formatting and aggregation to distribution
nd inclusion in traffic information services.

Article 5 of Directive 2010/40/EU provides that specifications adopted in accordance with Article 6 of this Directive should apply
to the ITS applications and services when these are deployed without prejudice to the right of each Member State to decide on the
deployment of such applications and services on its territory.

These specifications should apply to the provision of all real-time traffic information services without prejudice to particular
specifications adopted in other acts under Directive 2010/40/EU, notably Commission Delegated Regulation (EU)
No 885/2013 (7) and Commission Delegated Regulation (EU) No 886/2013 (7).

A market for the provision of real-time traffic information services already exists in the Union and it is in the interest of both the
users and customers as well as the providers of those services that the right conditions are created for this market in order to be
preserved and further developed in innovative ways. As regards the provision of real-time traffic information services, Directive
(EU) 2019/1024 of the European Parliament and of the Council (7) sets out minimum rules for the re-use of public sector
information throughout the Union. With respect to the re-use of data held by road authorities and public road operators, the rules
established by this Regulation, in particular the ones concerning data updates, are applicable without prejudice to the rules
established by the Directive (EU) 2019/1024. With respect to the re-use of data held by private data holders, the rules established
by this Regulation do not impose sharing data free of charge. Data held by private data holders may be subject to licence
agreements to regulate their re-use.

(7) Directive 2007/2/EC of the European Parliament and of the Council (7) creates a European Union spatial data infrastructure in

EU-wide legislation

- NIS2 directive – effective October 2024
 - Measures for high common EU-wide cybersecurity
 - Defines critical entities for the transportations sector both public and private
 - Points to both the ITS directive and the RTTI delegated regulation in “Annex I Sectors of high criticality” for subsector road describing the Road authorities and operators of Intelligent Transport Systems
- ITS Directive amended – effective November 2023
 - Defines a C-ITS credentials management system (CCMS)
 - Defines secure exchange of messages from C-ITS stations
 - Defines crucial data categories
- RTTI Delegated regulation amended – effective January 2025
 - Mention interoperability and accessibility and these are parts of Cybersecurity
 - Defines secure truck parking
- And many more...

— Road authorities as defined in Article 2, point (12), of Commission Delegated Regulation (EU) 2015/962 responsible for traffic management control, excluding public entities for which traffic management or the operation of intelligent transport systems is a non-essential part of their general activity

— Operators of Intelligent Transport Systems as defined in Article 4, point (1), of Directive 2010/40/EU of the European Parliament and of the Council

NIS1 -> NIS2

- **Unified Criteria:** NIS2 mandates more stringent cybersecurity requirements and introduces uniform criteria across the EU to classify which entities are within its scope.
- **Enhanced Compliance:** Stronger regulatory measures and penalties promote consistent, effective cybersecurity measures, aligning the EU's cyber resilience approach. Refers to both member states, public or private companies regarding compliance. Push use of open standards to achieve interoperability.
- **Scope Expansion:** NIS2 expands coverage from 6 to 15 sectors, integrating both "essential" and "important" entities for consistent cybersecurity standards across critical industries.



Energy



Health



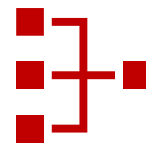
Transport



Banking/
Finance

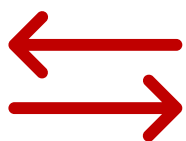


Water



Digital infrastructure

NIS1



ICT B2B



Public
administration



Space



Postal
Service



Waste
Management



Chemicals
supplychain



Food
supplychain



Manufacturing



Digital
providers



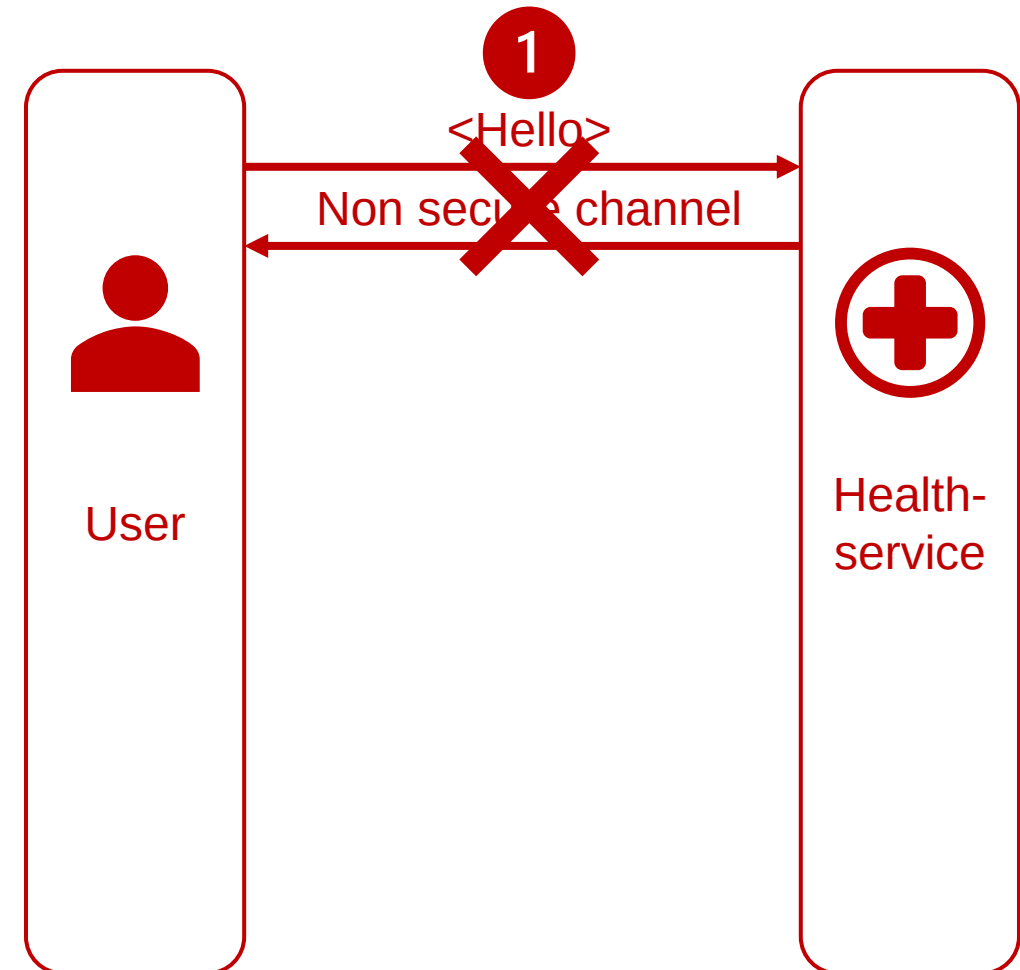
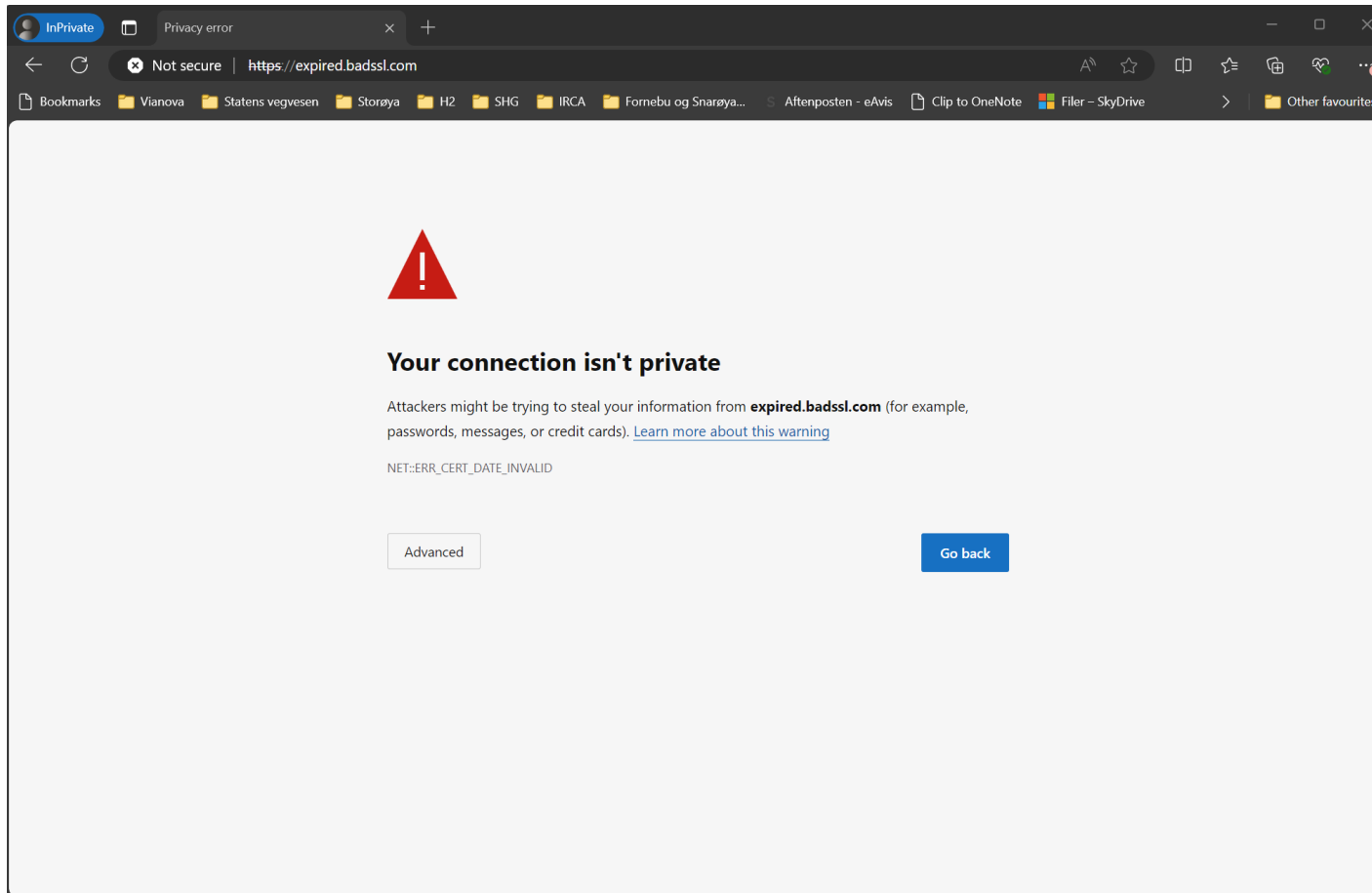
Research

NIS2

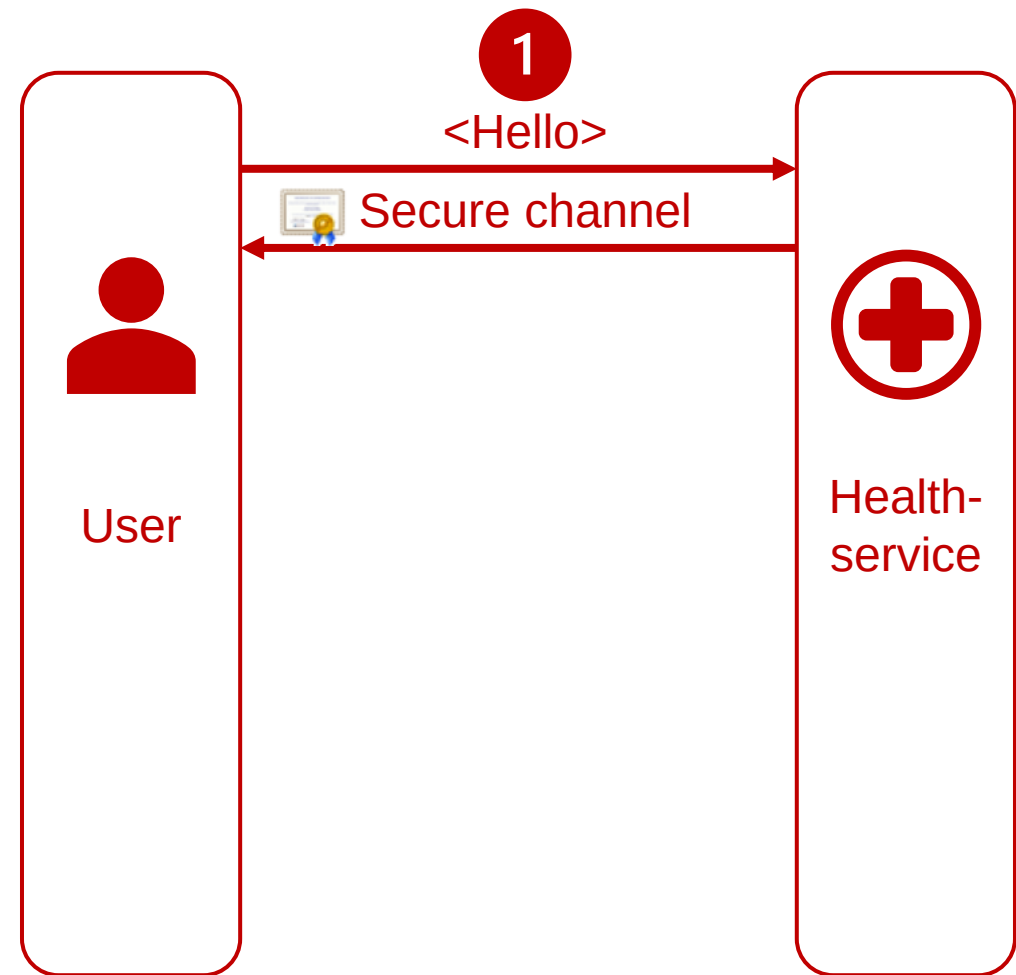
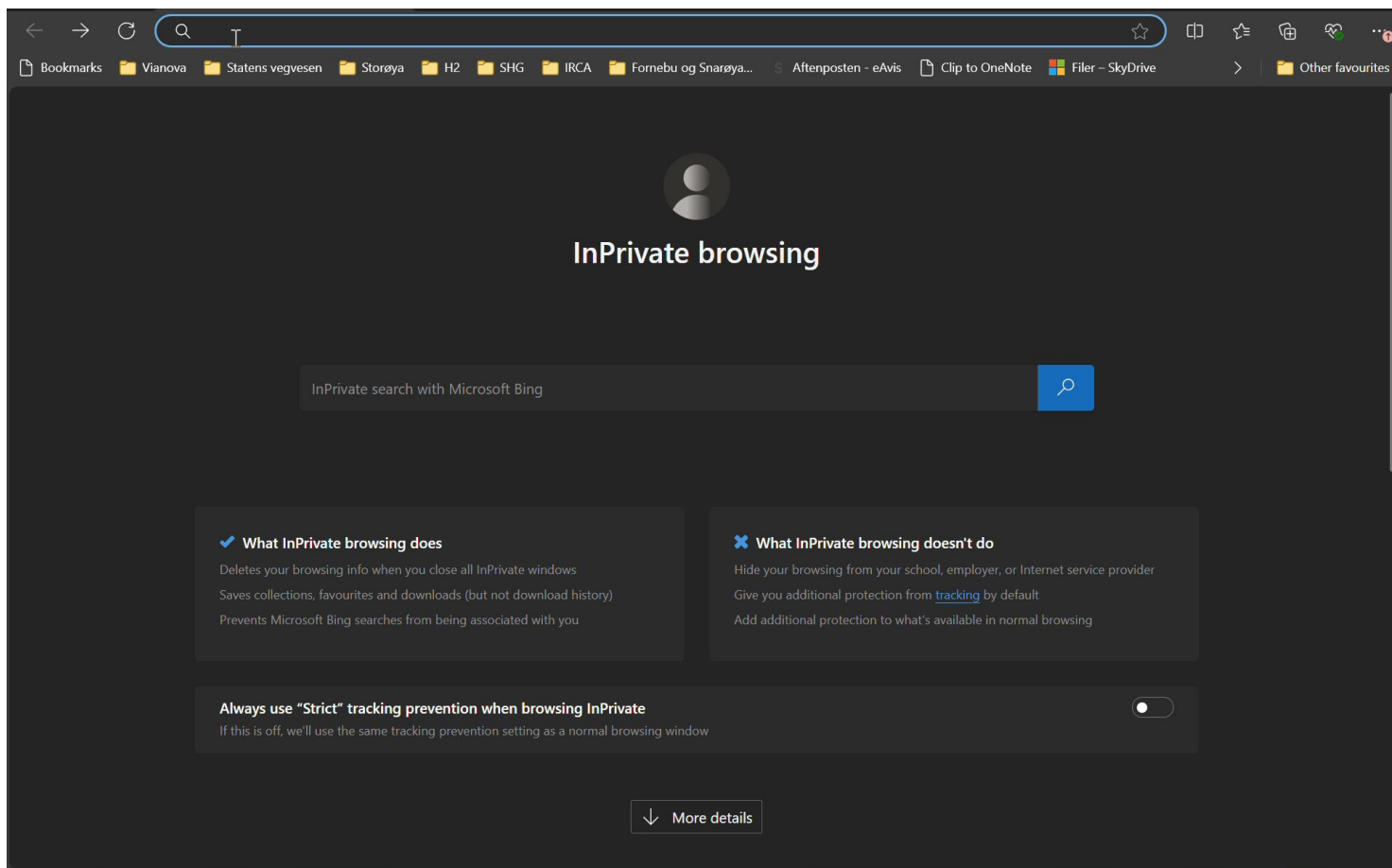
NIS2 Cybersecurity risk management measures

1. Policies on **risk analysis** and information system security
2. **Incident handling**
3. **Business continuity**, such as backup management and disaster recovery, and crisis management
4. **Supply chain security**, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers
5. **Security in network** and information systems acquisition, development and maintenance, including **vulnerability handling** and disclosure
6. Policies and procedures to assess the **effectiveness of cybersecurity risk-management measures**
7. Basic **cyber hygiene** practices and cybersecurity **training**
8. Policies and procedures regarding the use of cryptography and, where appropriate, **encryption**
9. **Human resources security**, access control policies and asset management
10. The use of **multi-factor authentication** or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

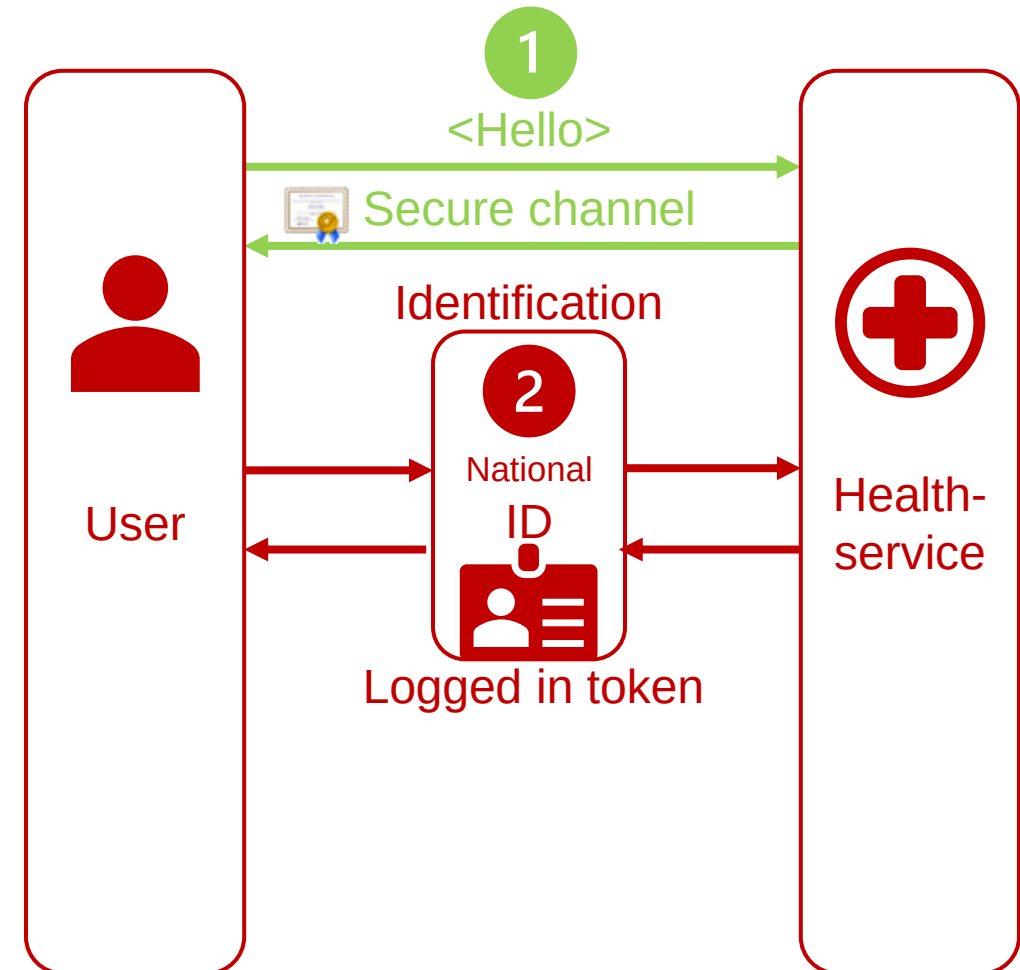
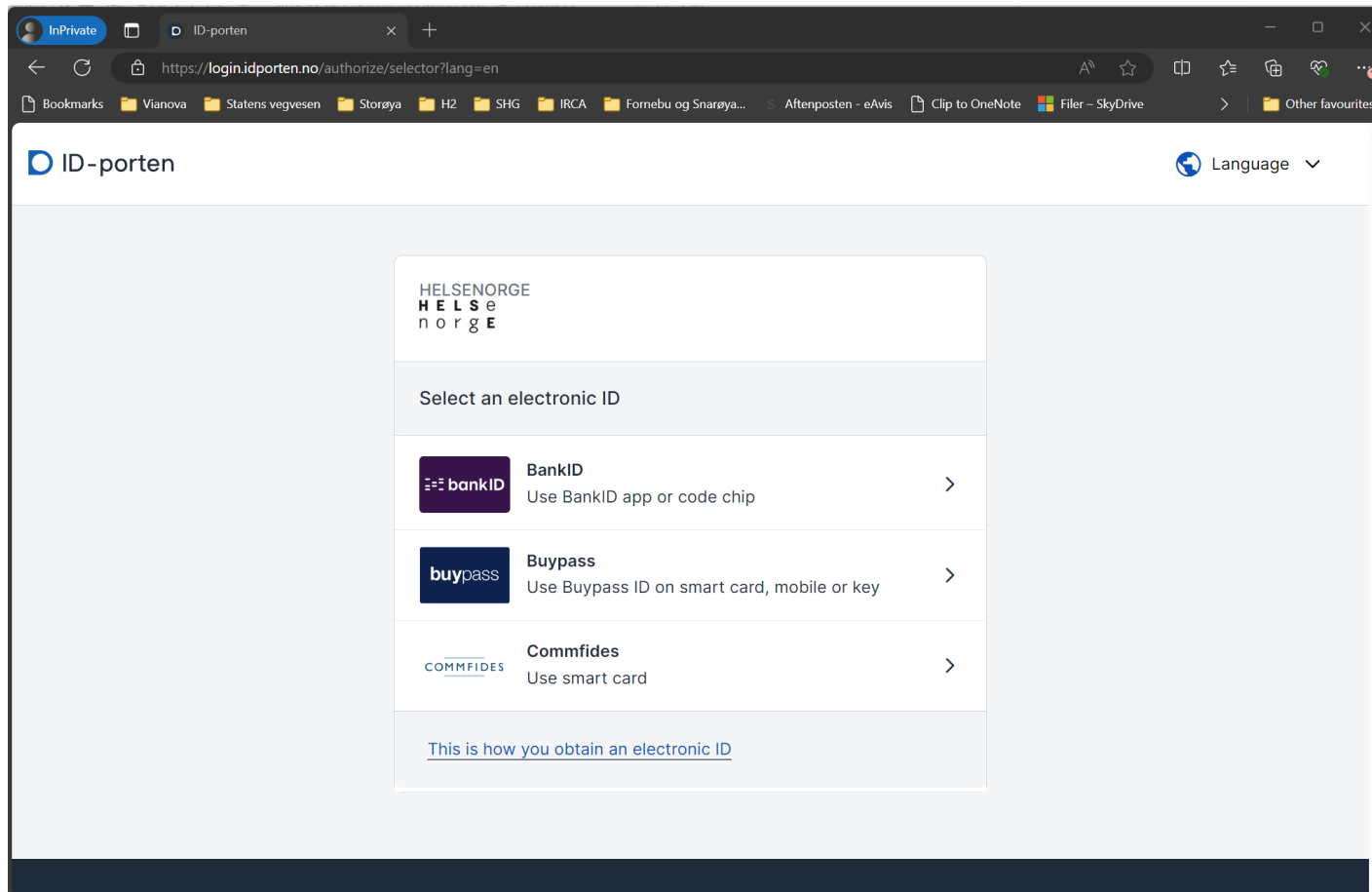
When and whom to trust – secure channel



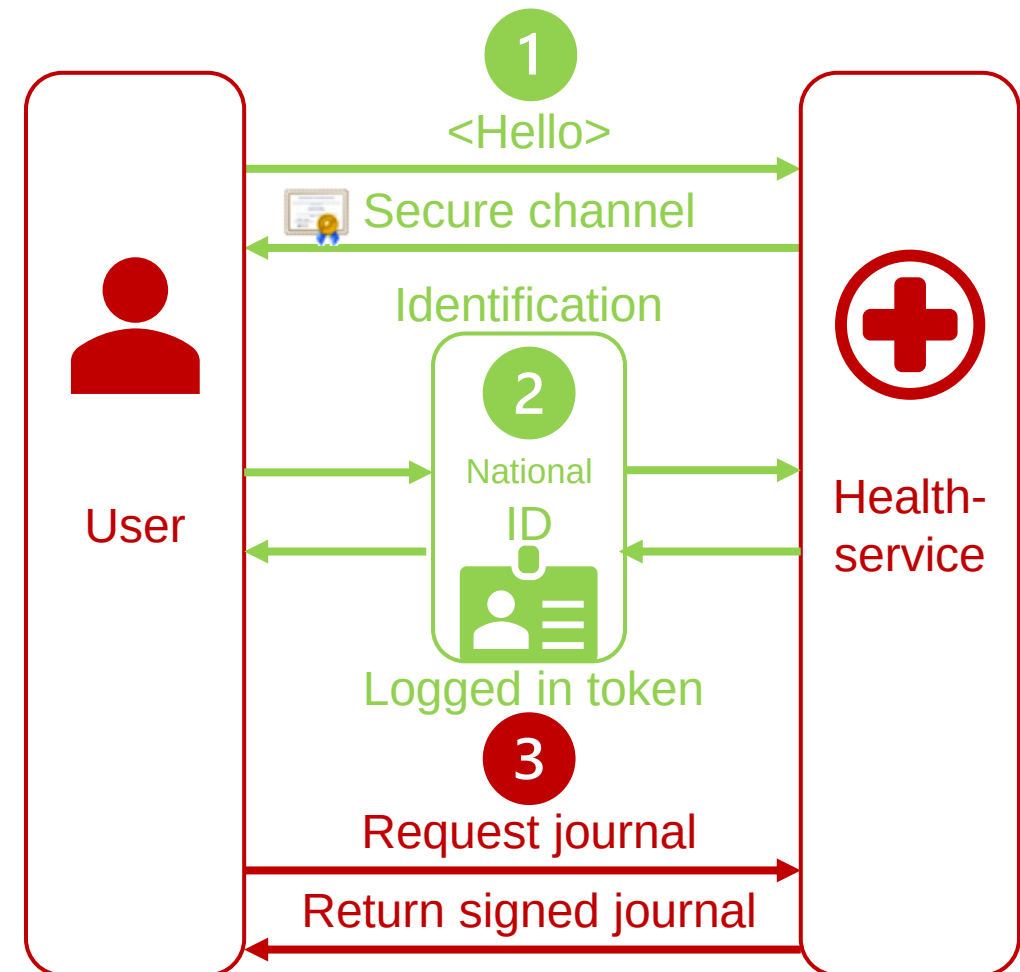
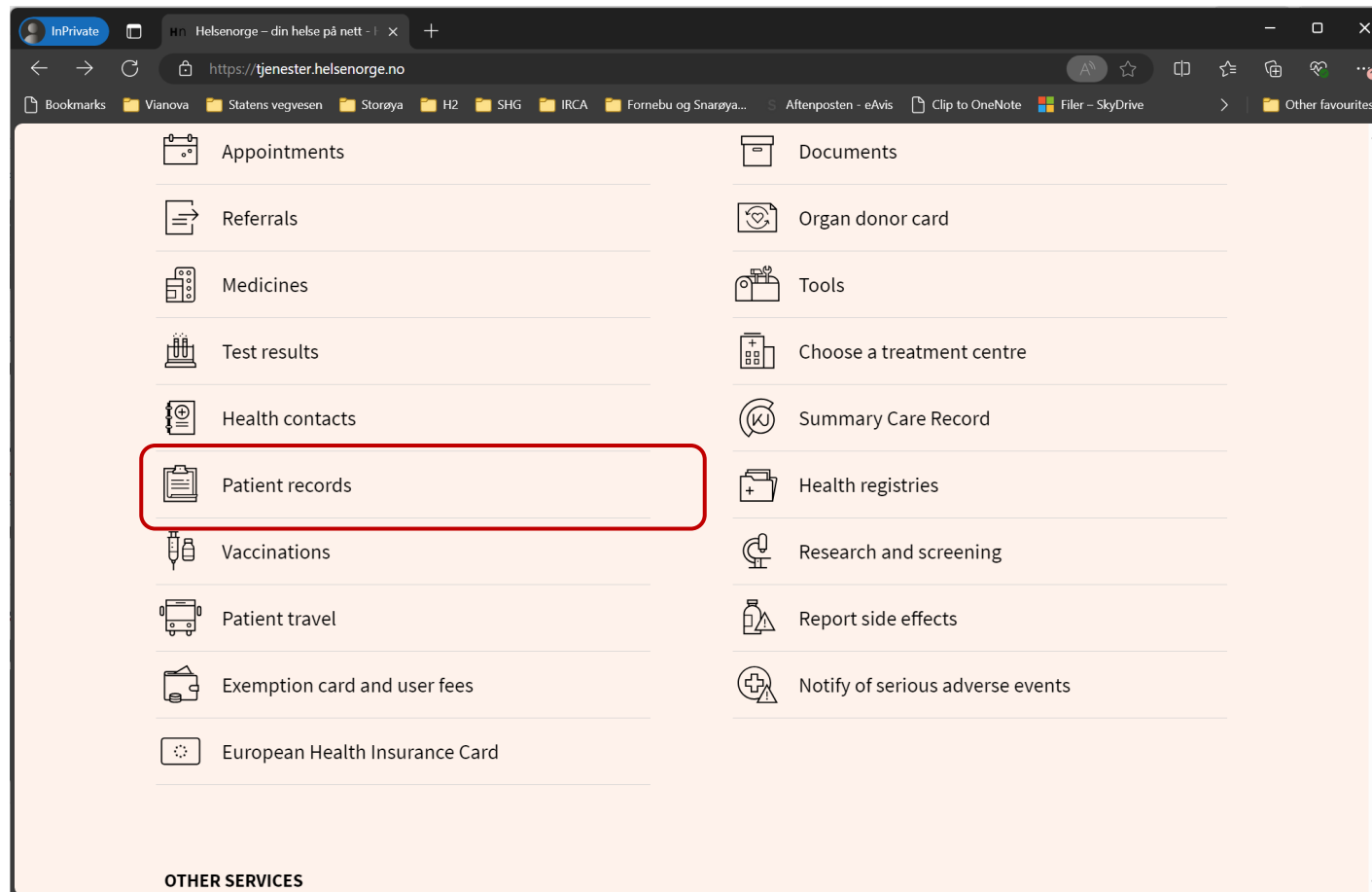
When and whom to trust – secure channel



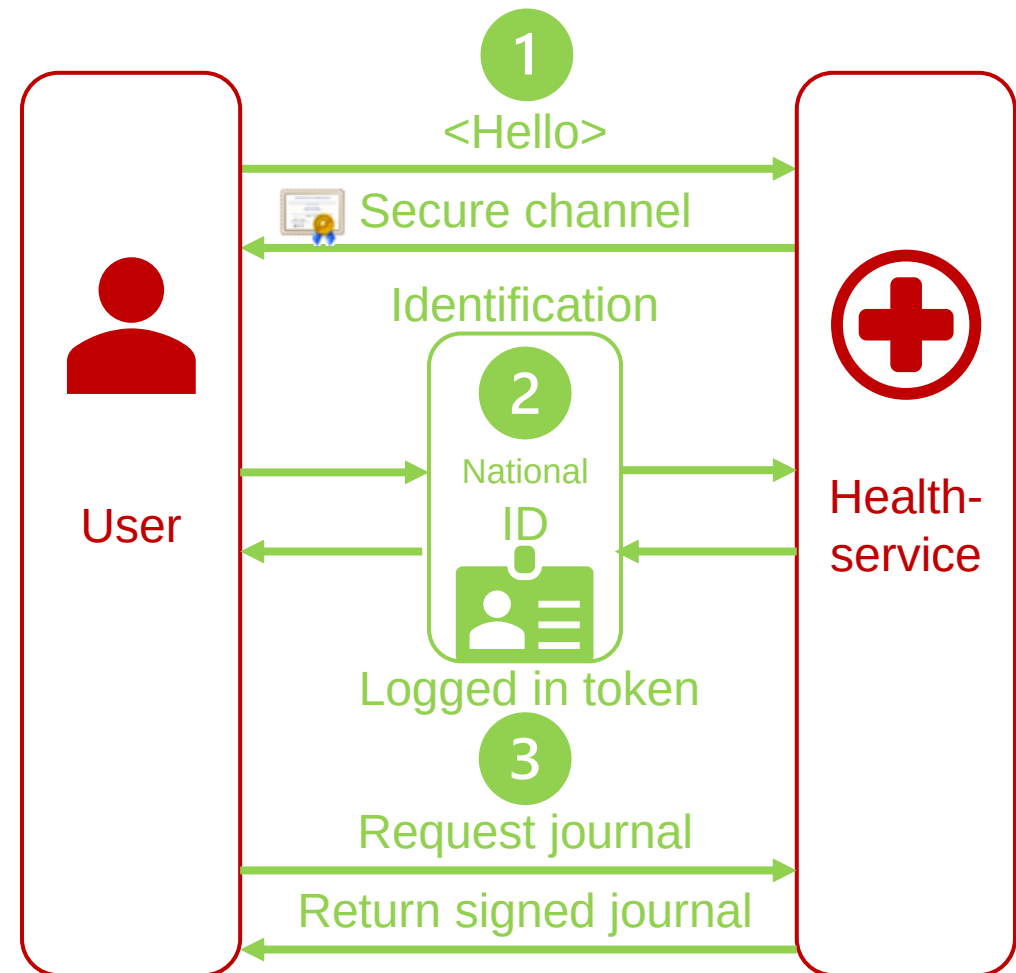
When and whom to trust – identification



When and whom to trust – signed information



When and whom to trust – signed information



Questions



Security building blocks



What is a National Access Point? (ITS Directive)

- A digital interface set up by a Member State that constitutes a single point of access to data (Art. 4)
- The commission shall first adopt the specifications necessary to ensure the interoperability and continuity for the deployment [...] (Art. 6)
- The NAP is therefore a Software System that shall enjoy interoperability to face different scenarios.
Example:
 - Deliver roadtraffic (DATEXII) and roadfeature (TN-ITS) data
 - Participate in the Mobility Data Space

Interoperability as Cybersecurity Dimension

- Cybersecurity is described by ISO 27001:2022 in terms of *Confidentiality, Integrity, and Availability* (CIA)
- Availability means to ensure information is accessible when needed
- If a NAP authenticates the data delivery through username/password, while the client expects to have a digital key, data is not accessible.
- Cybersecurity countermeasures shall be interoperable as well!

What is the status?

- 31 NAPs are deployed
- 8 Different authentication methods
 - Specific crafted URL
 - Basic Authentication (user and pass sent in the request)
 - Oauth 2.0 Client Credentials
 - X-DATEX-API-KEY
 - Client certificate
 - X-api-key
 - Signed soap message, certificate provided by email
 - No authentication at all
- The situation is against the provisions of the ITS directive.

NAPCORE Description of a NAP

- NAPCORE defines a Reference Architecture for two kinds of NAP
 - Metadata Directory: the NAP contains descriptions of the data and services important for their identification, assessment, and subscription by consumer
 - Data Platform: the NAP contains descriptions of the data and services important for their identification, assessment, and subscription by consumer, i.e., metadata, together with the data and/or services themselves
- NAPs are implementing several use cases:
 - Mobility Data Space connector
 - TN-ITS
 - Datex II

Cybersecurity of NAP

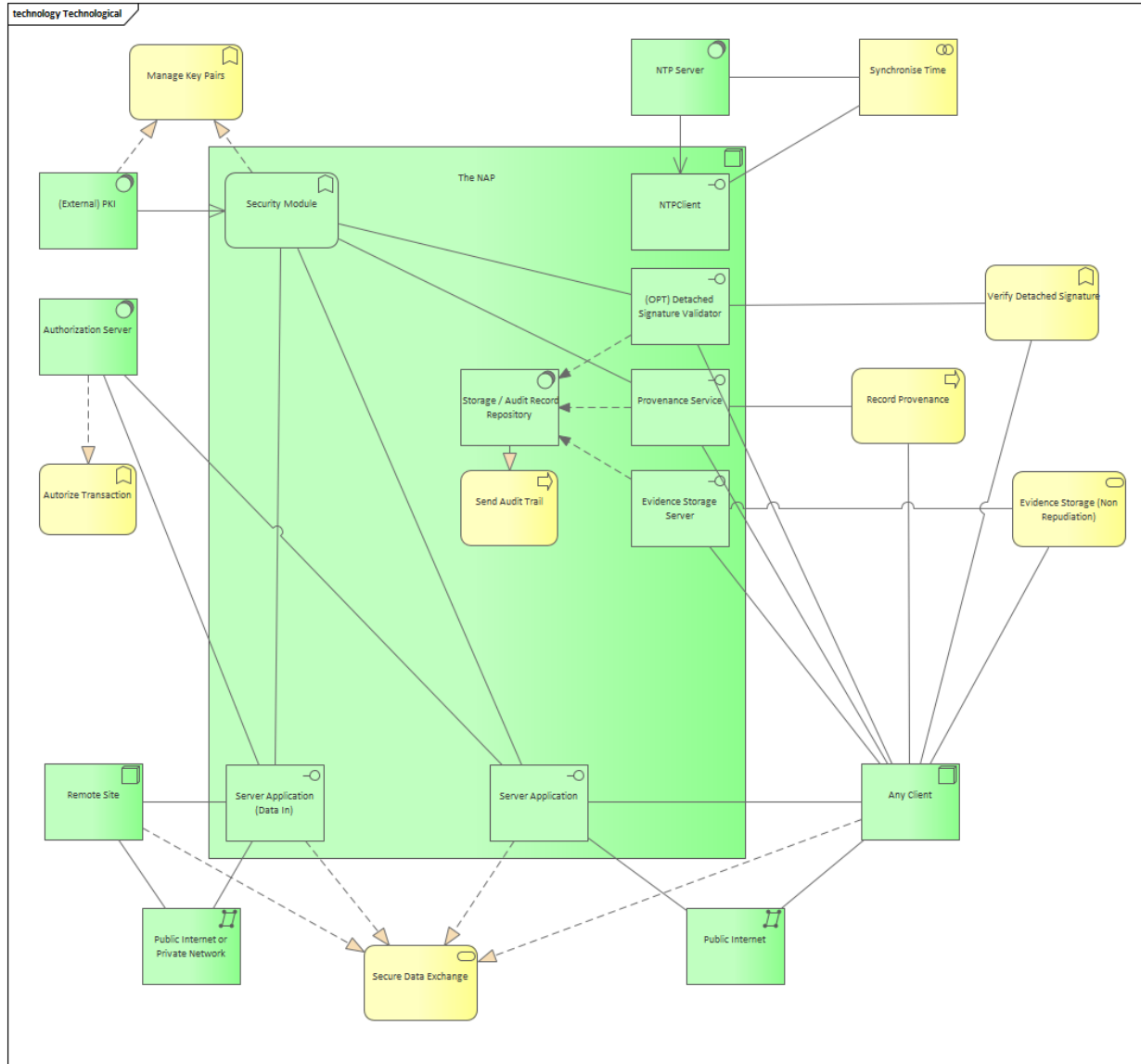
- Hard to define a set of specific technology to implement ...
- ... However, we need to attain Interoperability
- The NAP Cybersecurity measures are given in the form of *Reusable Building Blocks*, covering concepts such as
 - Confidentiality of data in transit, and at rest
 - Integrity of data
 - Non-Repudiation and Provenance
 - Audit Trails (for forensic analysis), and Data Classification

Cybersecurity of NAP

Each Building block has:

- A set of ISO 27001:2022 controls that are implemented (*NAPs are considered by the NIS 2 directive*)
- A set of Interoperability Building Blocks, IBBs, containing technological information to realize the Cybersecurity concept (e.g., Confidentiality in Transit is trivially implemented by using TLS 1.3)

The NAP Security Reference Architecture

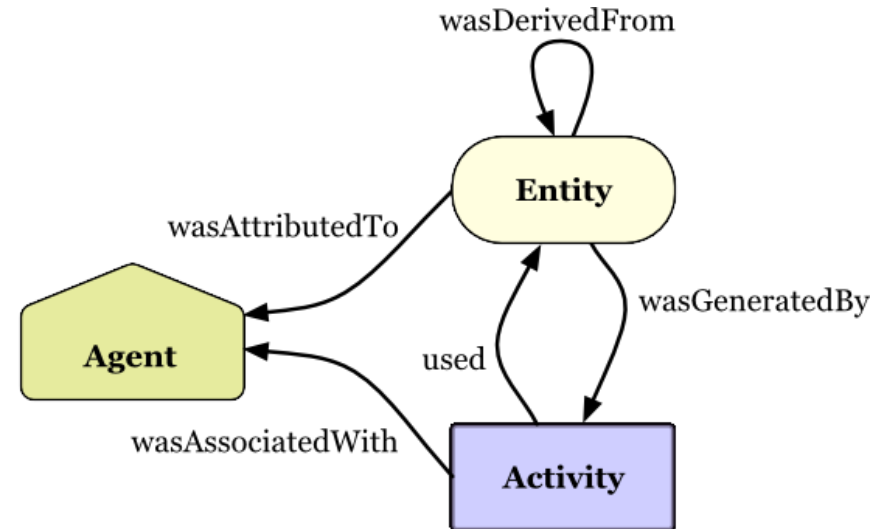


Additional interfaces for:

- Secure Communications (TLS 1.3)
- Authorization (OAuth 2.0)
- Audit Record Repository (Syslog)
- Provenance tracking (W3C Prov)
- Non-Repudiation tokens (ISO 13888)

Focus on Provenance

- Data provenance is the foundation of data quality
- From a data source, it answers the question “where the data goes”, while from the data destination, answers the question “where the data comes from”
- The Provenance ABB has been engineered to track all the data manipulation and creation



Focus on Non-Repudiation

- Non-repudiation services are mandated to **generate, collect, maintain, make available** and **validate evidence** concerning a claimed event or action **in order to resolve disputes** about the occurrence or non-occurrence of the event or action
- **Application logging**: unreliable data sent over unreliable message exchange
- **Audit Trail**: reliable data sent over unreliable message exchange
- **Non-Repudiation**: reliable data over reliable message exchange

Focus on Non-Repudiation (ISO 13888)

- ▶ Different aspects:

- ▶ Non-Repudiation of Origin, of Receipt, of Delivery, of Submission

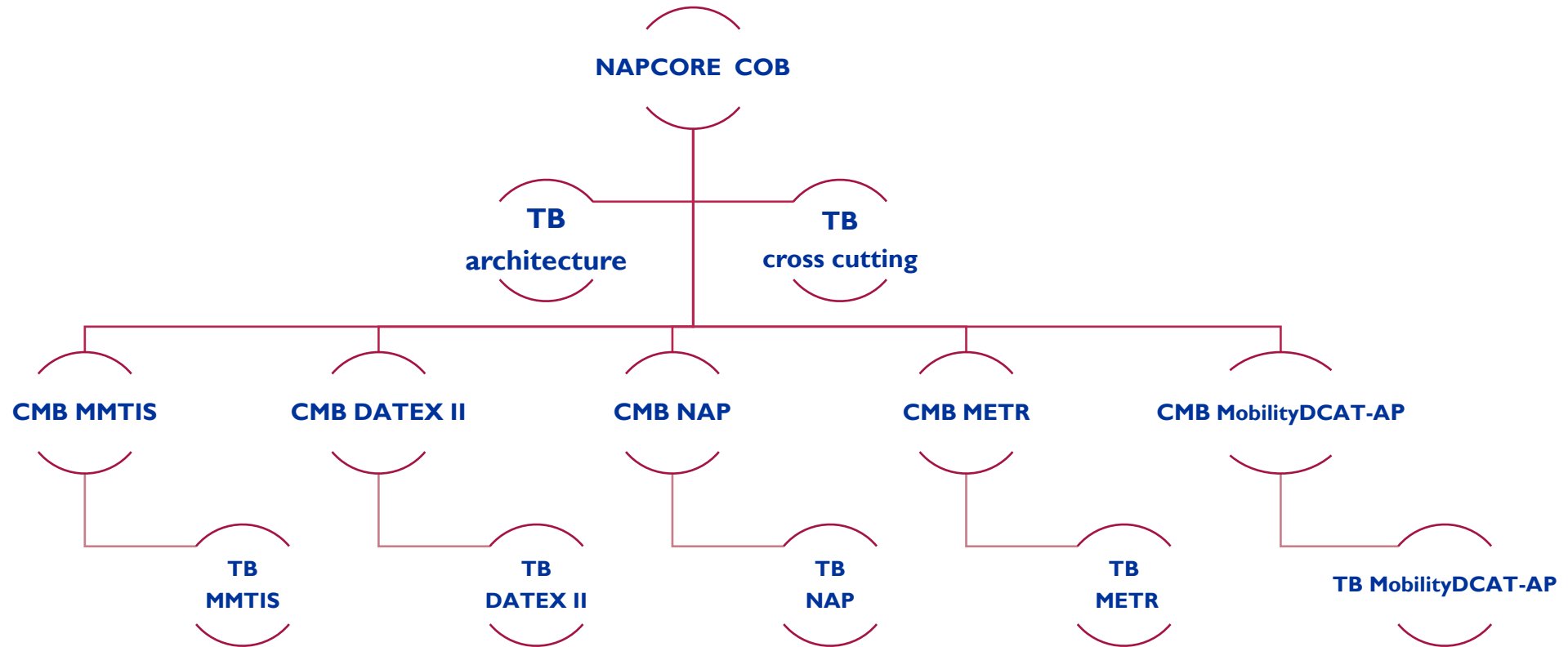
- ▶ The “Fairness” property

- ▶ **Strong fairness**, when the exchange is completed, sender A can prove to an arbitrator that recipient B has received (or still can receive) the item, *without any further need of cooperation from either B or any trusted third party*
 - ▶ **Weak fairness**, when exchange completed, A can prove that B has received (or still can receive) the item, or otherwise an affidavit can be presented to demonstrate that B misbehaved, or a network failure occurred. We need to have a trusted third party
 - ▶ **Eventually Strong**: fairness is ensured within the system but with the provision that additional assumptions about the participating parties are made.

NAPCORE-x



What is proposed for NAPCORE-x to address this topic



TASK 4.1 – MOBILITY DATA ECOSYSTEM ARCHITECTURE

and its cross cutting aspects

- *Monitor and assess requirements stemming from ITS – and related legislation*
- *Architectures of NAP-Centric mobility data ecosystems*
- *Cybersecurity, trust and data authenticity*

All actors need to take cybersecurity measures in order to make the data provision safe and secure. Especially to bring trustworthiness and confidence that data is really originating from a reliable source in an open data environment, there is a big interest in interoperable choices. Without further alignment on this subject the implemented solutions will by definition be not interoperable, causing a lot of additional costs and potential failure of the concept.

■ *Data publication/interchange/exchange alignment*

- Standardised deployment of the technical interfaces (API's) with regard to exchange technology and platforms, in combination with harmonised cybersecurity measures is a cross domain cutting effort to achieve interoperable access to the different data holder's data. At least standardised solutions for snapshot publications, delta publications and standardised push interfaces for low latency data services will be defined. (where possible cross domain, but at least within each domain)
- *Joint toolkit for schema creation and creation of deployable technical artefacts such as profiles*

Cybersecurity building blocks for NAP

-a simple intro



Building blocks

Highly simplified picture ...



Traffic Authority / Regulator



Central system



END USER

Building blocks – Signature



A digitally signed Electronic Traffic Regulation can be compared to a physical document that has a stamp from the authority and a signature from the person with authority rights.

The end user will have full trust in the origin of this regulation



Traffic Authority / Regulator

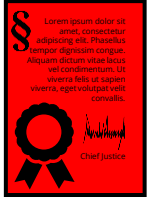


Central system



END USER

Building blocks – Secure Transfer



A digitally signed Electronic Traffic Regulation can be compared to a physical document that has a stamp from the authority and a signature from the person with authority rights.



The secure transfer of a TRO can be compared to a physical envelope that has a wax seal and is sent via registered mail. Content is protected and delivered only to correct recipient, source and destination reception is logged

End-to-end trust in complete chain



Traffic Authority / Regulator

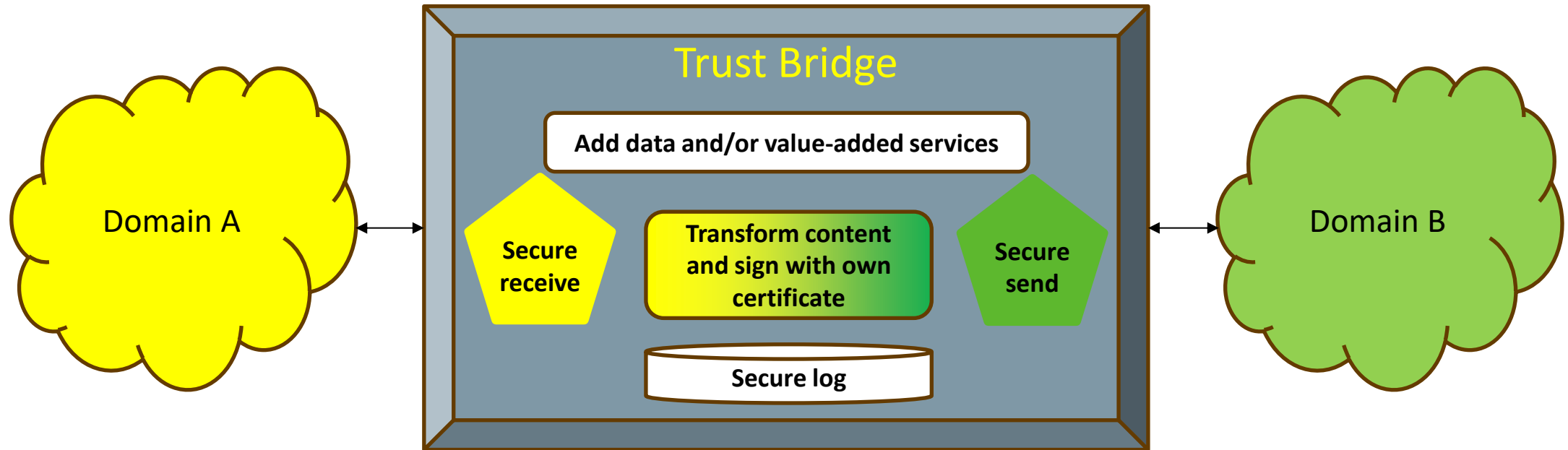


Central system



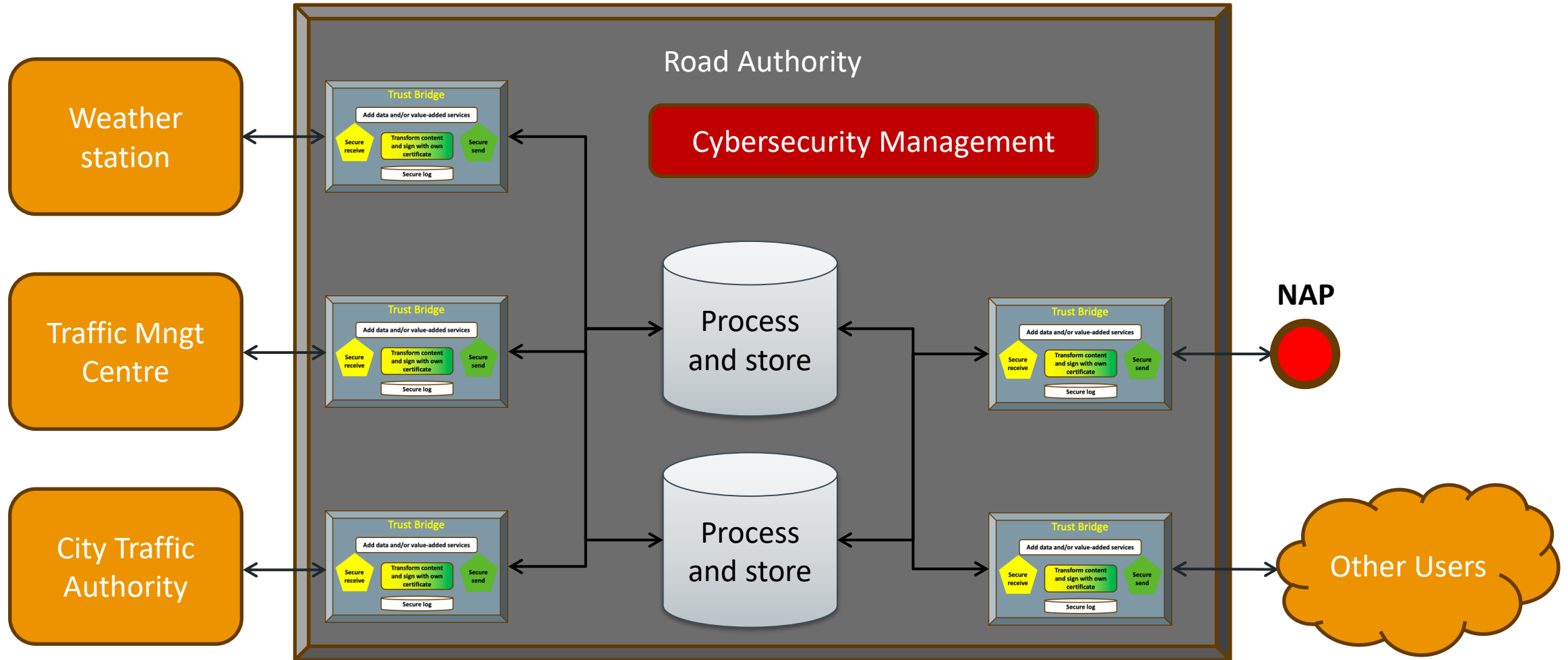
END USER

Building blocks – Transfer of trust between domains

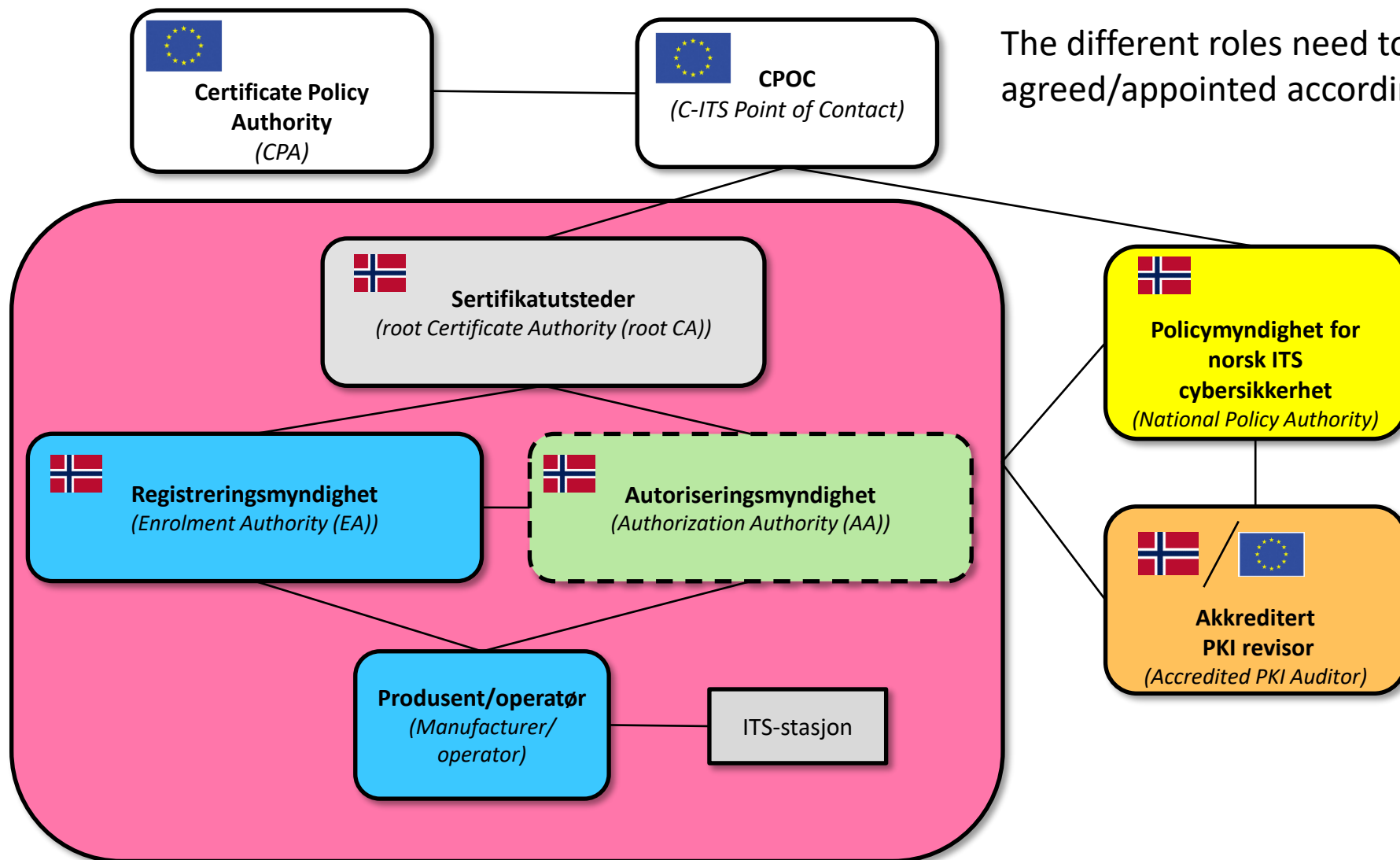


- The prerequisite for bridging trust is to follow a complete set of policies incl verification, certification, management, governance, etc.
- Examples of policy requirements:
 - The cloud system must be certified secure, i.e. all critical processes happen in a secure environment
 - The PKI must be trusted by all involved actors
 - All critical processes must be logged and signed, so that a critical data frame received by a user can be unraveled and traced back to its secure origin (forensics)
 - Non-repudiation for all access points, including proprietary interfaces
- Good news: Many security standards in this domain, and similar policies as starting point

Example: Road Authority configuration



Policy management hierarchy (PKI) - proposed Norwegian PKI model



The different roles need to be filled with actors agreed/appointed according to the Policy



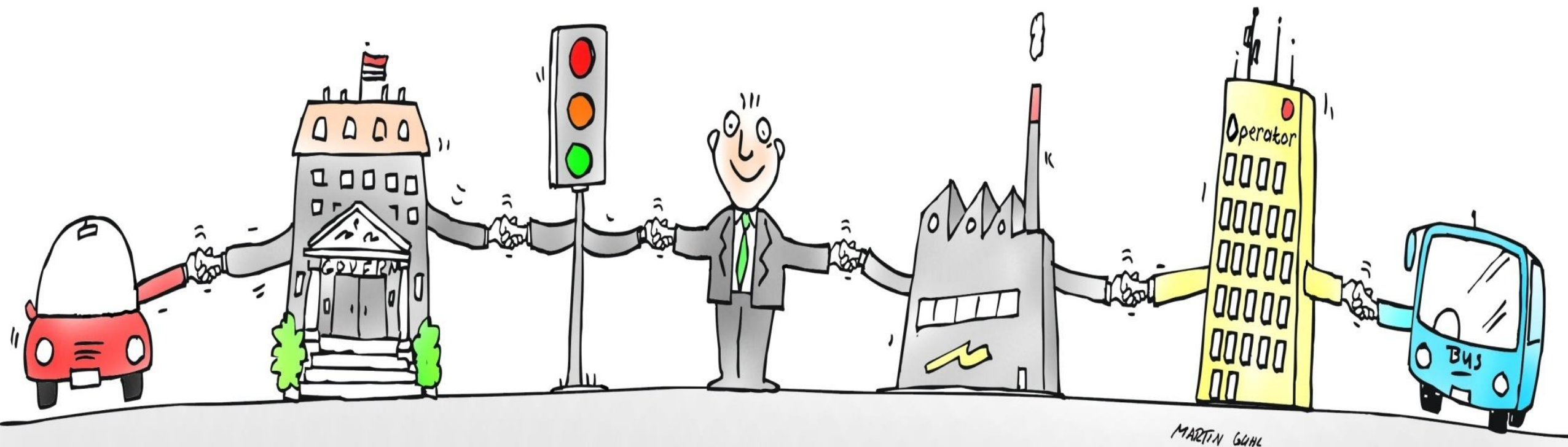
Discussion



Discussion topic: Secure the NAPs

- Metadata directory: The metadata directory contains descriptions of the data and services important for their identification, assessment, and subscription by consumer, i.e., metadata. It provides facilities to authenticate data provider and functionality to insert a metadata records.
- Data platform: The data platform contains descriptions of the data and services important for their identification, assessment, and subscription by consumer, i.e., metadata, together with the data and/or services themselves. It provides facilities to authenticate data provider, and optionally, data consumer and functionality to insert a data and metadata records to NAP internal database.
- How and to what extent should they be secured without breaking interoperability?

Thanks for your attention!



Responses Overview Active

Responses

31

Average Time

02:08

Duration

20 Days

1. Do you know CIA in cybersecurity



2. Are you familiar with NIS2 effective october 2024



3. What sector are you in

31

Responses

Latest Responses

"Road operator"

"Rail transport"

"Public sector, traffic management"

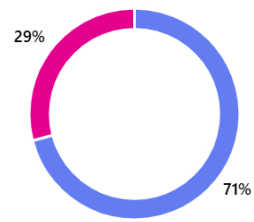
...

5 respondents (16%) answered Public for this question.



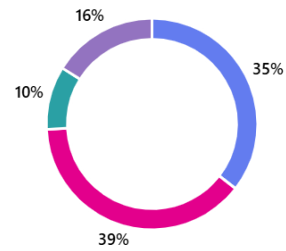
4. Is there a defined approach on security measures in your sector

Yes	22
No	9



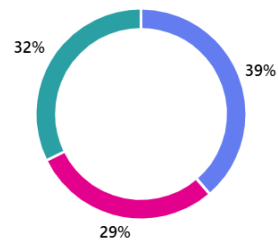
5. What type of NAP in your country

A central data repository (NAP data platform)	11
A distributed repository with central lookup (NAP registry)	12
Other solution	3
Don't know	5



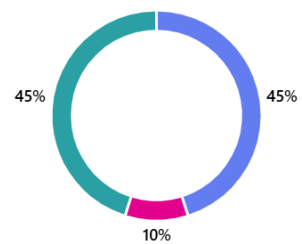
6. Is security applied to your NAP, such as authentication methods

Yes	12
No	9
Don't know	10



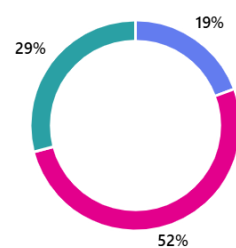
7. Do you know the relevance of PKI (Public Key Infrastructure) for NAP

Yes	14
No	3
Some, but would like to learn more	14



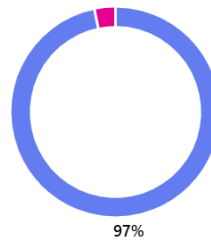
8. Have you heard any complains on different security concepts being applied

Yes	6
No	16
Some, but would like to learn more	9



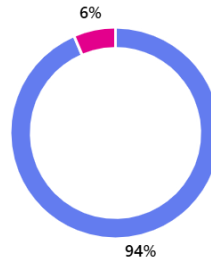
9. Do you use online banking services

● Yes 30
● No 1



10. Do you trust online banking service

● Yes 29
● No 2



11. Do you know the term "trust" in Cyber security

● Yes 25
● No 6

