neisas

National & European Information Sharing & Alerting System

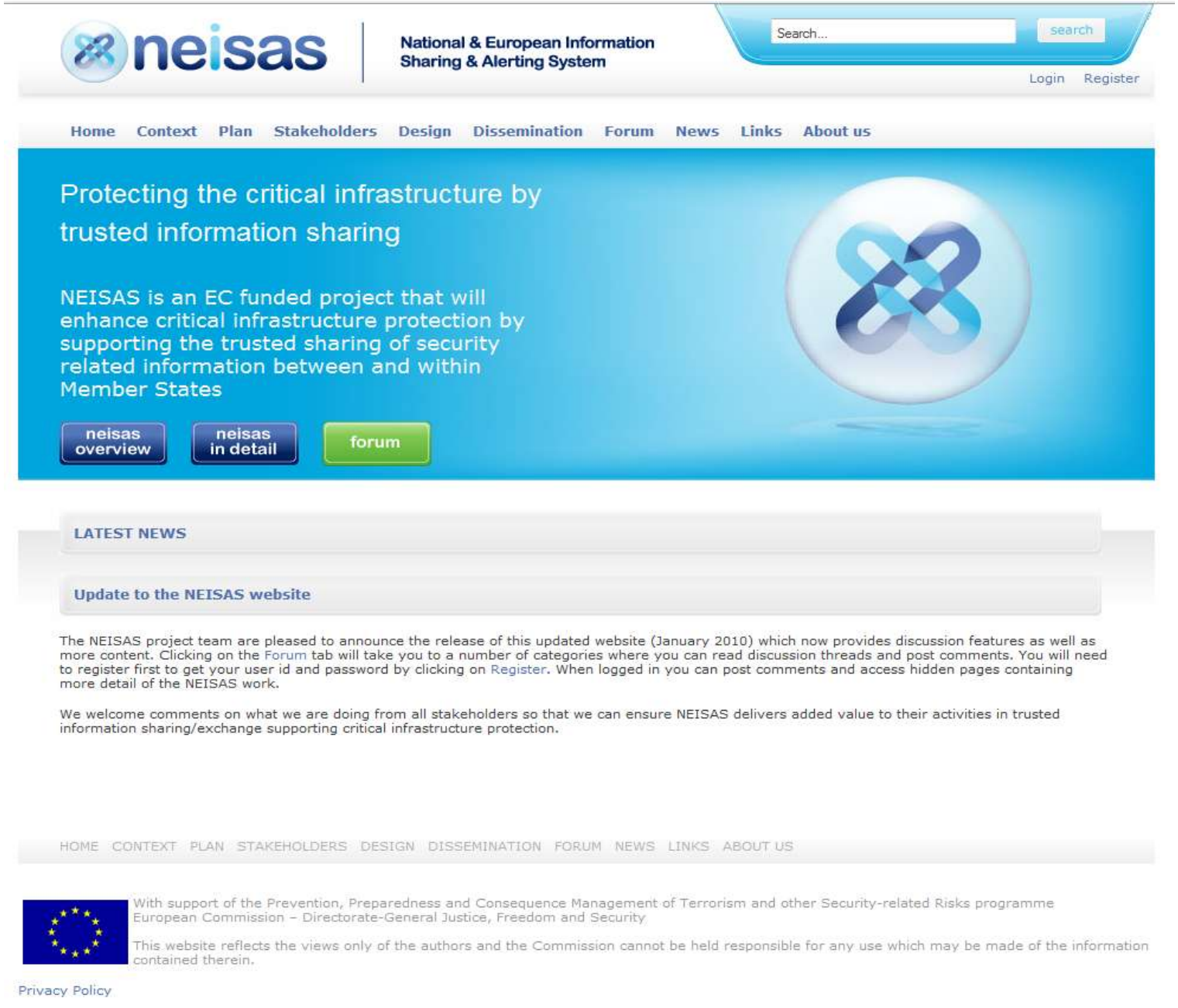
With the support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme"
European Commission - Directorate-General Justice, Freedom and Security"
"This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein."

Joint ENISA-NICC Workshop on: Network Security Information Sharing 16 – 17th March 2010

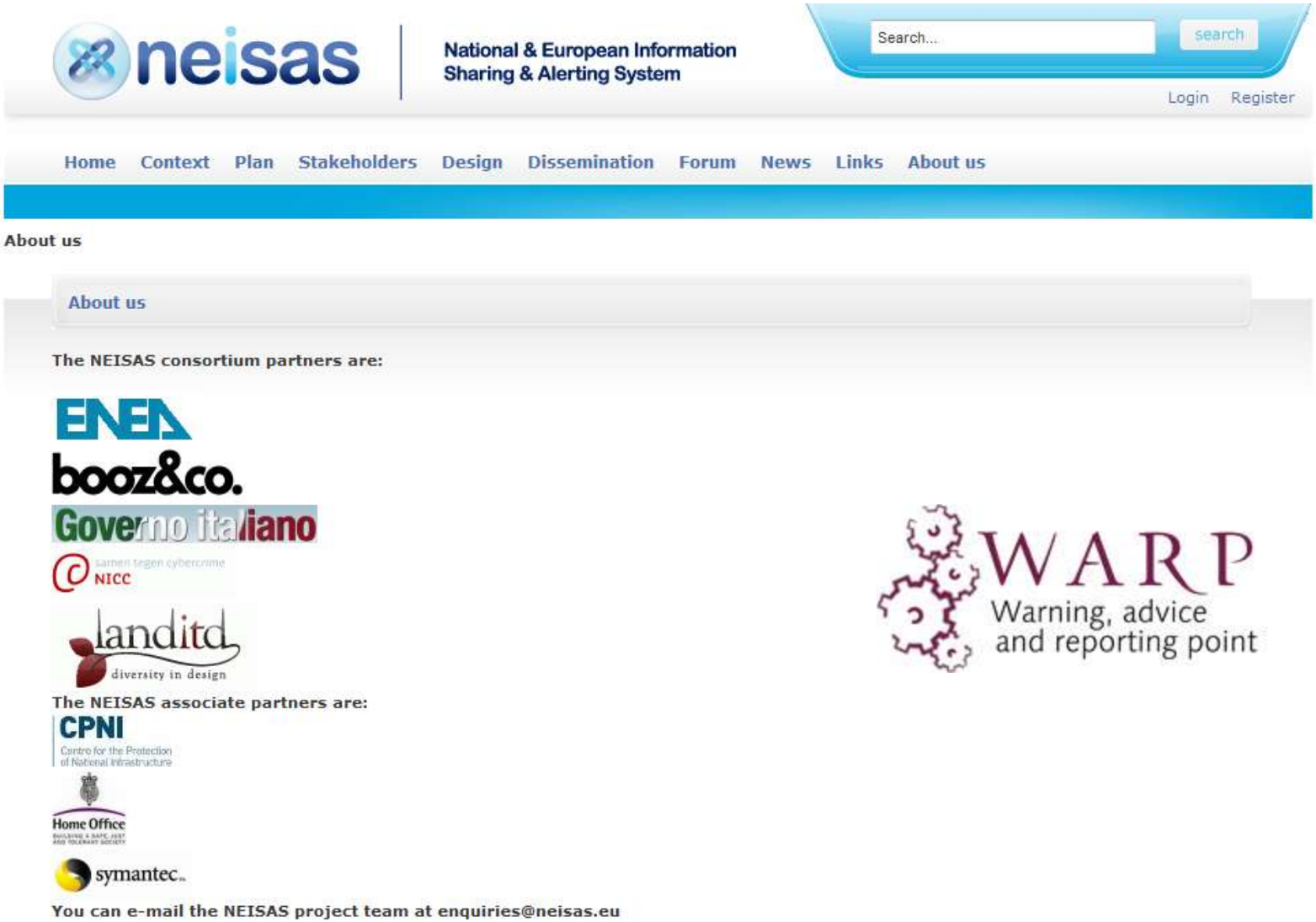
John Harrison - LanditD

Introduction and background to NEISAS

www.neisas.eu



About us


neisas
National & European Information Sharing & Alerting System
Search...
search
Login
Register
Home
Context
Plan
Stakeholders
Design
Dissemination
Forum
News
Links
About us
About us
About us
The NEISAS consortium partners are:
ENEA
booz&co.
Governo italiano
samen tegen cybercrime
NICC
landitd
diversity in design
WARP
Warning, advice and reporting point
The NEISAS associate partners are:
CPNI
Centre for the Protection of National Infrastructure
Home Office
symantec.
You can e-mail the NEISAS project team at enquiries@neisas.eu

Plan

The Plan is:

1.To study The Netherlands experience made by NICC with their ISACs

2.To study the UK experiences made by CPNI with their IEs

3.To agree on a common platform model for Public Private Partnership information sharing, taking note of emerging standards such as ISO/IEC 27010.

4.To study how the common model can be applied in Italy & possibly in other EU countries.

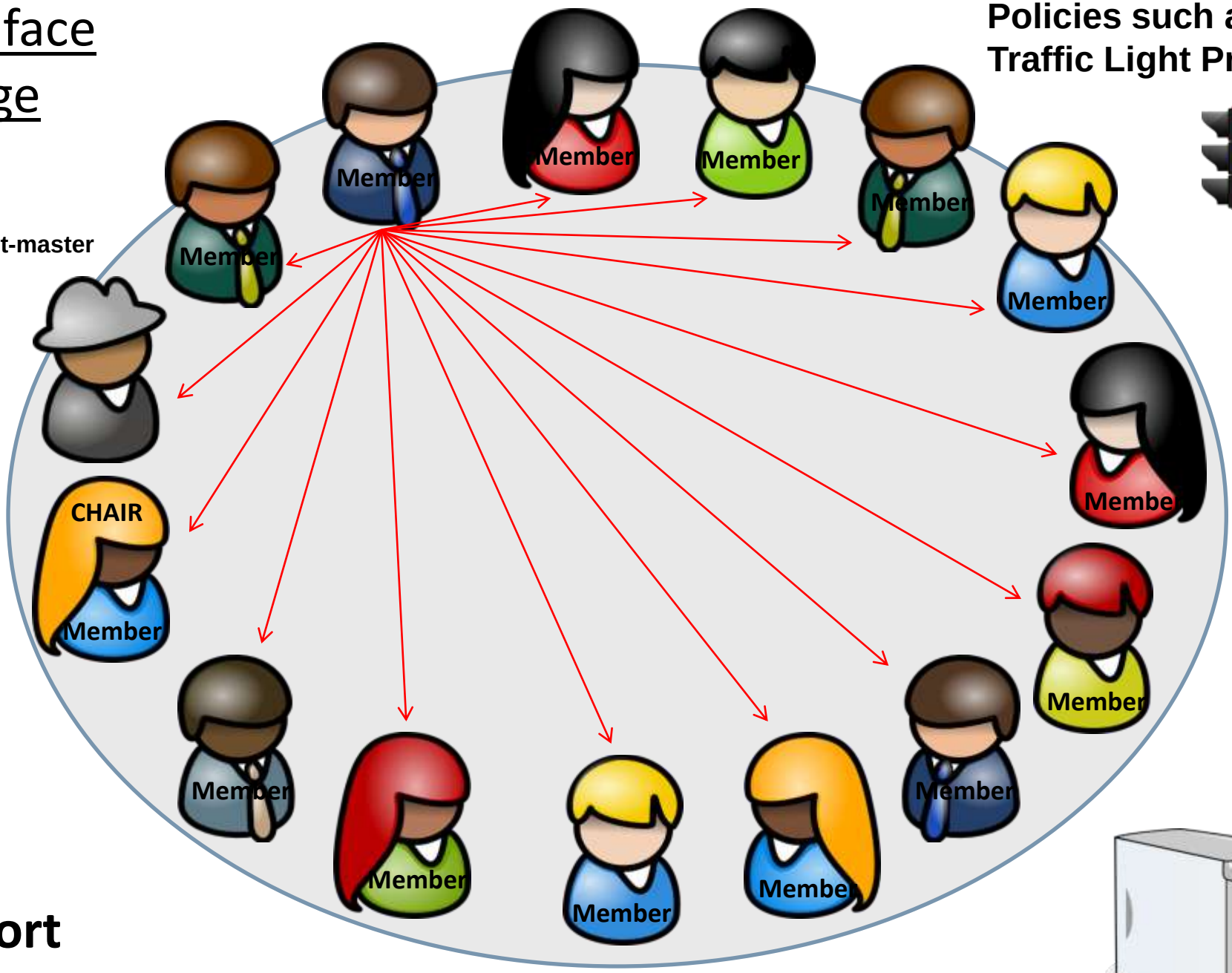
5.To produce a common prototype design for national platforms.

6.To implement pilot project trials in the Netherlands, the UK and Italy

7.To evaluate the value of the platform and degree of scalability/exportability of results.

8.To engage with stakeholders throughout the project and disseminate NEISAS findings.

Face to face Exchange

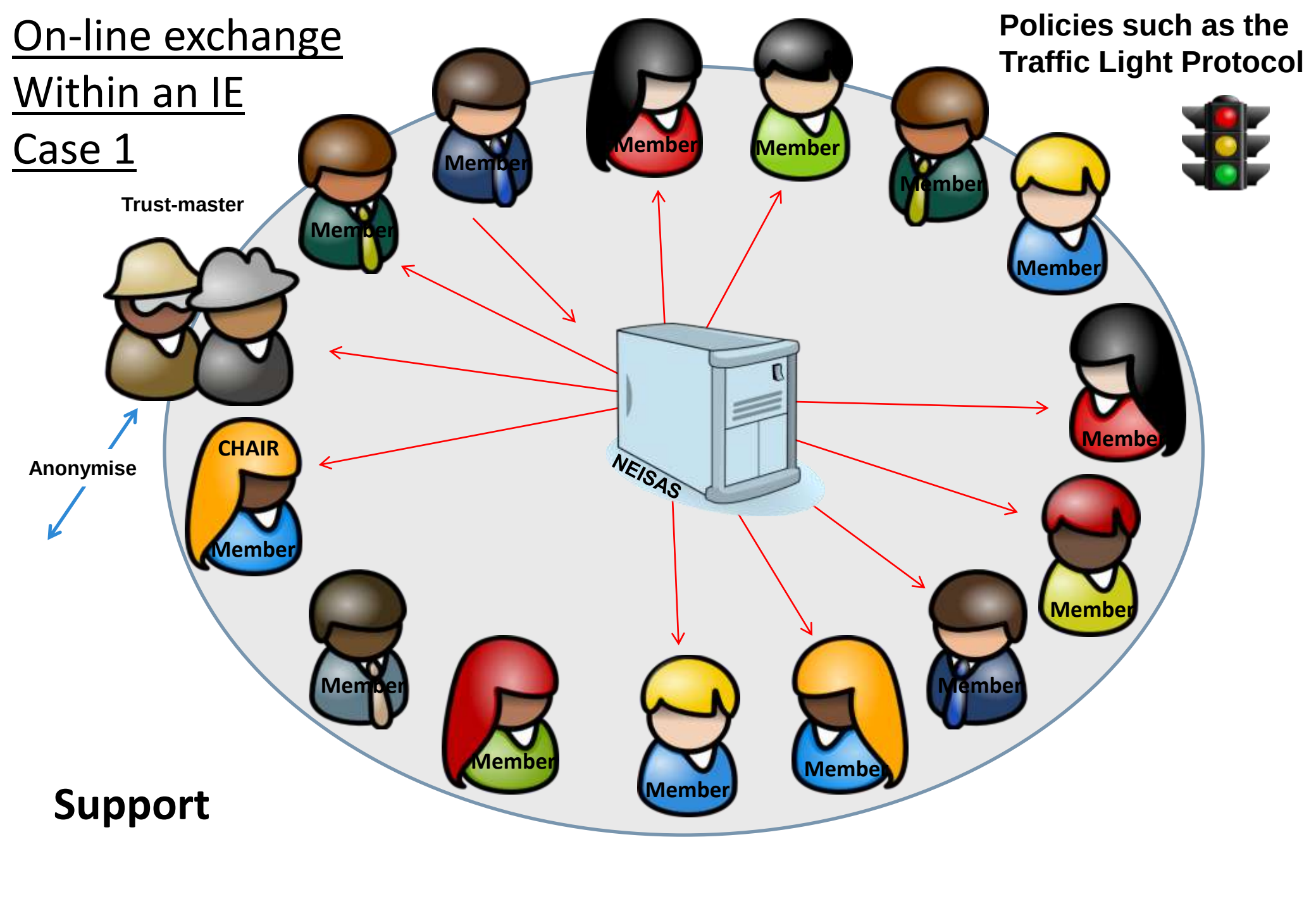


Policies such as the Traffic Light Protocol

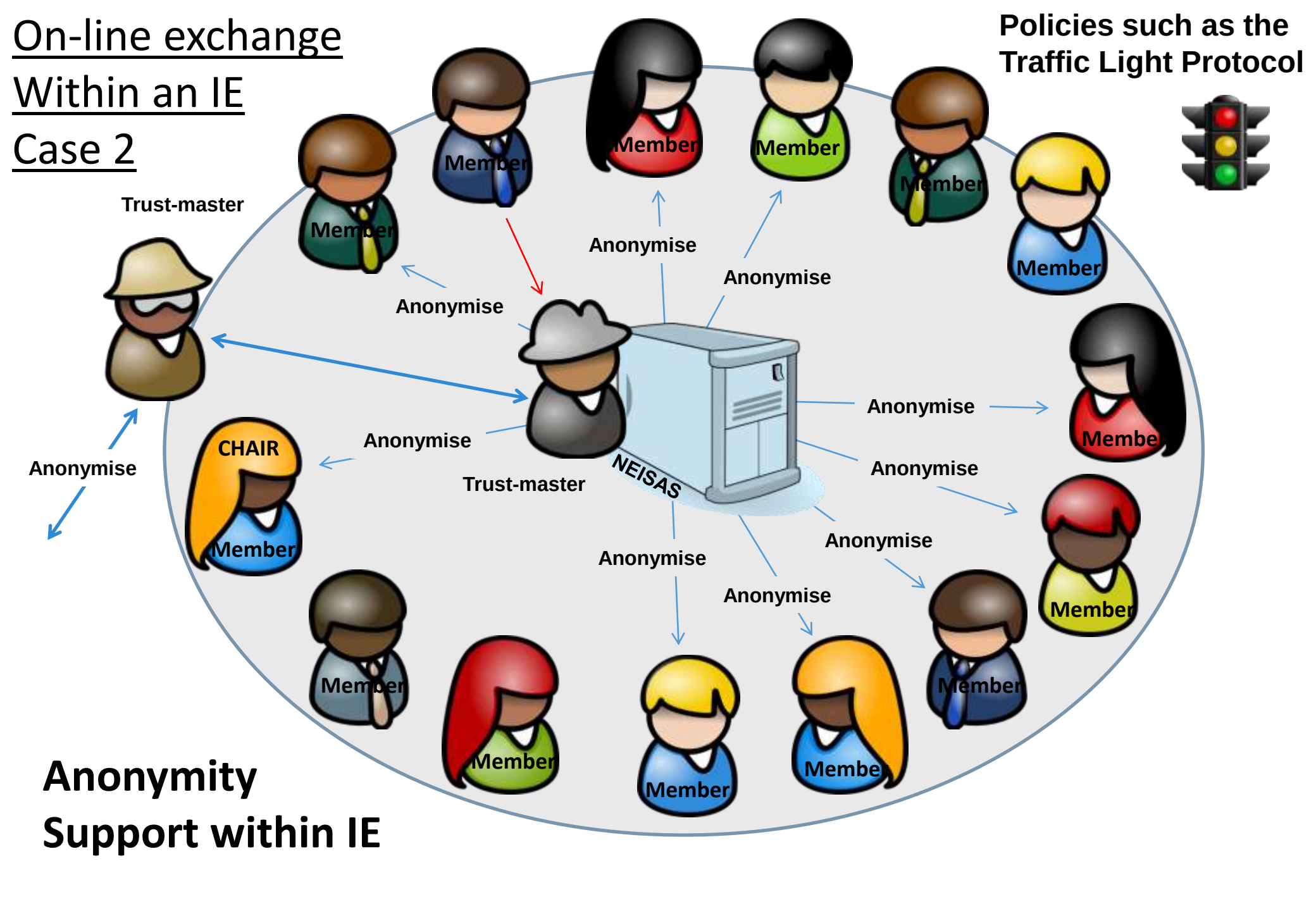
Support

Infrastructure

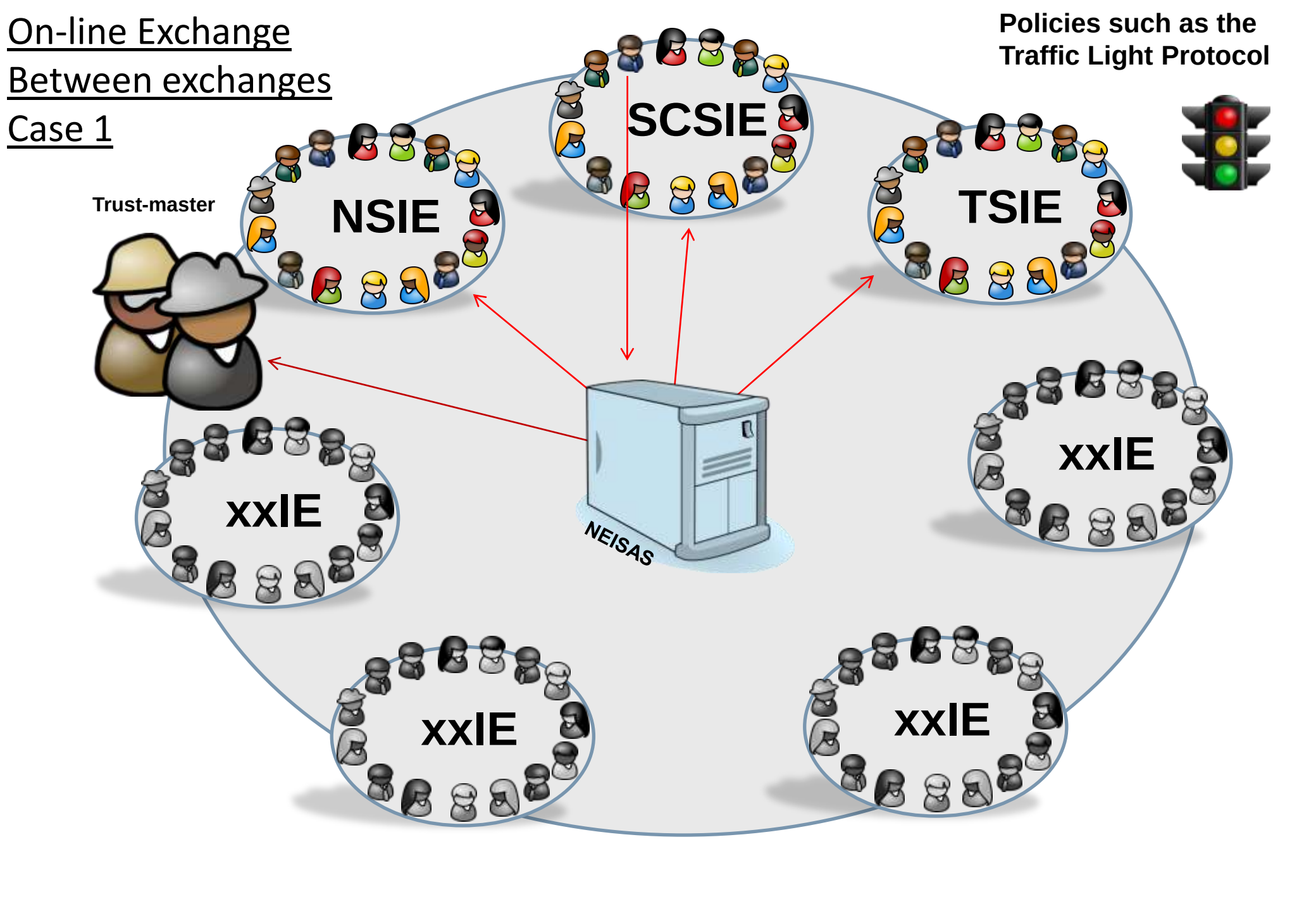
On-line exchange Within an IE Case 1

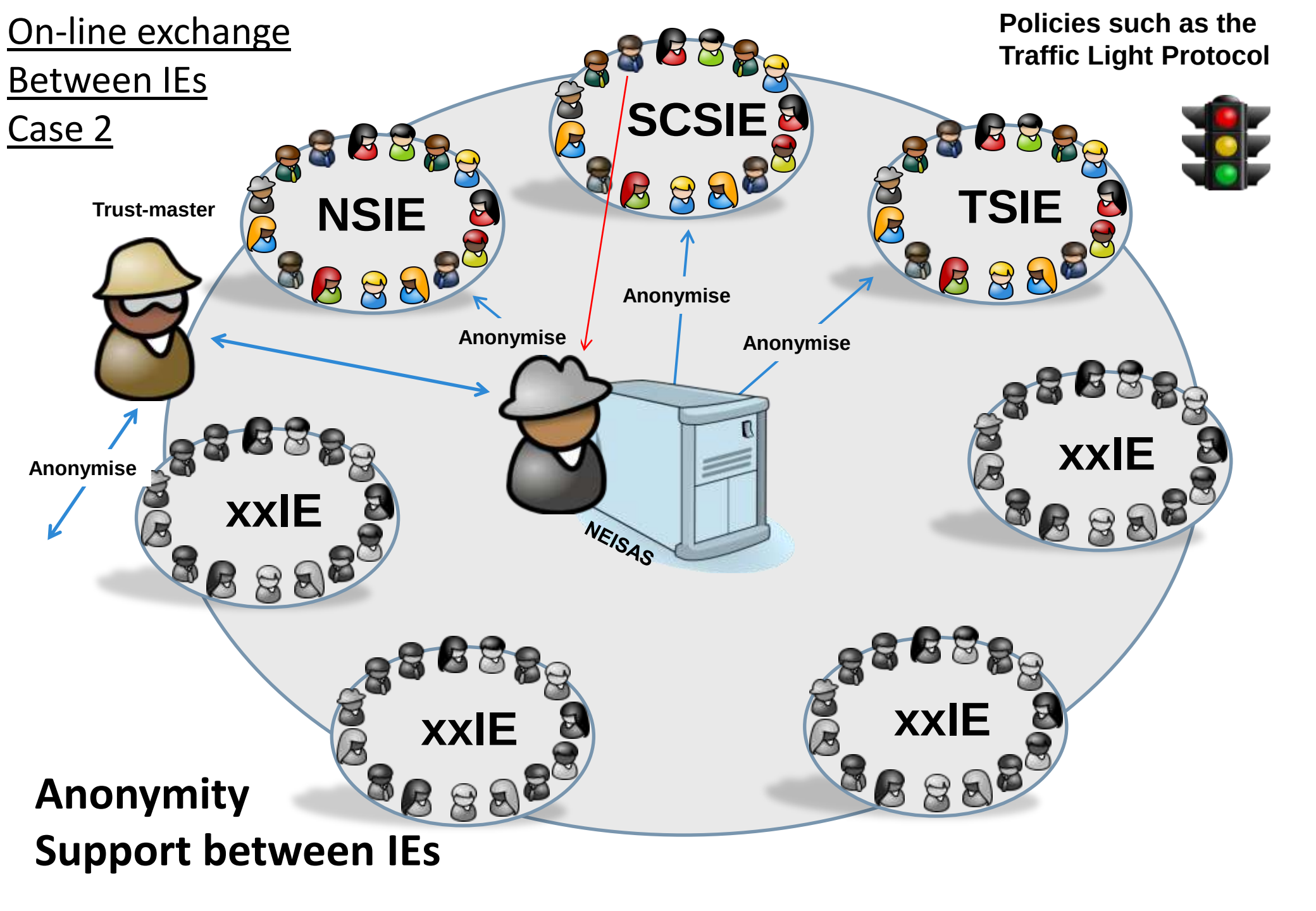


On-line exchange Within an IE Case 2

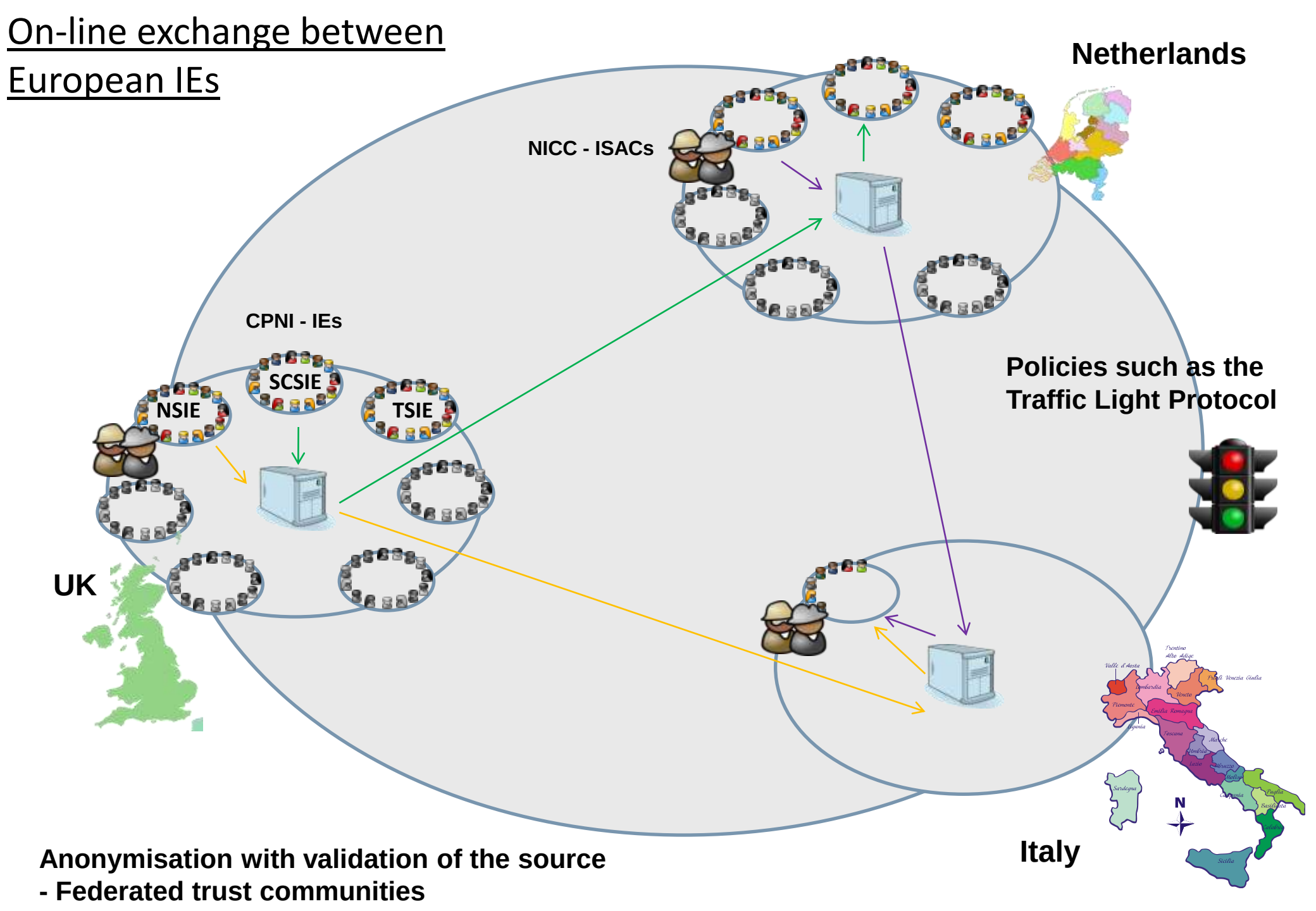



IE/ISAC


On-line Exchange
Between exchanges
Case 1
Policies such as the
Traffic Light Protocol
Trust-master
SCSIE
NSIE
TSIE
xxIE
xxIE
xxIE
xxIE
NEISAS

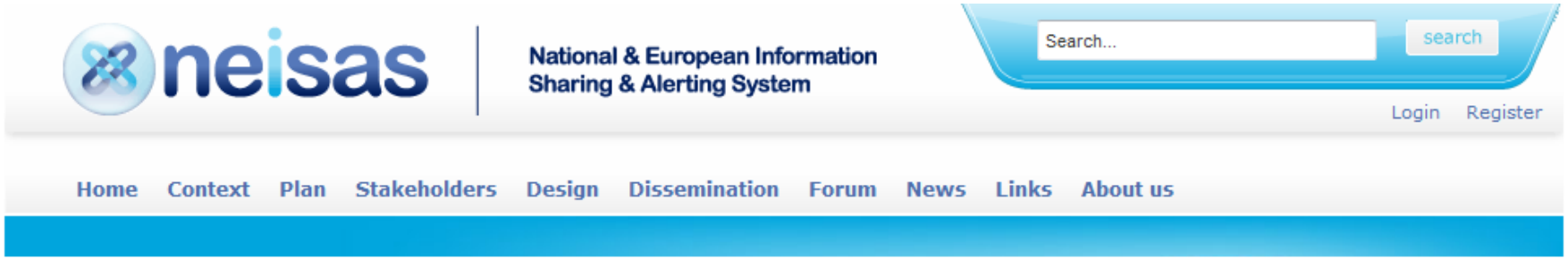

On-line exchange
Between IEs
Case 2
Policies such as the
Traffic Light Protocol
SCSIE
NSIE
TSIE
Trust-master
Anonymise
Anonymise
Anonymise
Anonymise
NEISAS
xxIE
xxIE
xxIE
xxIE
Anonymity
Support between IEs

On-line exchange between European IEs



Anonymisation with validation of the source
- Federated trust communities

Forum: > Requirements

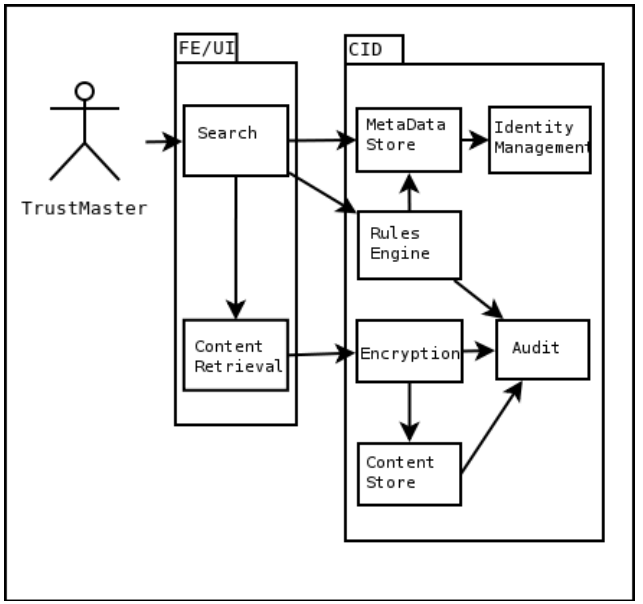


Requirements

TR1	The solution shall allow originators of information to assign a degree of trust in the data and information they input into NEISAS	Mandatory
TR2	The solution shall allow all data and information to be clearly identified with the source, including origin by country, company, organization and person, other than when this information is specifically anonymised	Mandatory
TR3	The solution shall allow for anonymous reporting and for information aggregation to allow masking of individual organizational or personal information contributions	Mandatory
TR4	The solution shall allow for both source and recipient to determine whether the information has been confirmed/validated independently by other users of the system	Mandatory
TR5	The solution shall allow recipients of the information to assign a subjective rating of the source of the information	Mandatory
TR6	The solution shall allow recipients of the information to assign a subjective rating of the relevance, pertinence, importance and urgency of the information	Mandatory
TR7	The solution shall allow providers of the information to control the classification, releasability and distribution of the information provided	

Analysis:

Use Case o+12: Anonymise published information
Primary Actor: TrustMaster
Scope: NEISAS
Level: Summary



Main success scenario:

1. **The TrustMaster is notified that content requires anonymisation via a persistent search.**
2. **The TrustMaster logs into NEISAS.**
3. **The TrustMaster is presented with a list of content for anonymisation via a special persistent search.**
4. **The TrustMaster selects a content item for anonymisation, and content retrieval retrieves and renders the content.**
5. **As the member is a TrustMaster, and the content requires anonymisation the anonymisation facility is available.**
6. **TrustMaster selects anonymise content, a new publish content session is started, owned by the TrustMaster, and pre-populated with the original content content.**
7. **The original content is deleted.**
8. **The TrustMaster modifies the content to implement anonymisation, this can include requesting a review by the originating member.**

Design:

Information Rights Management (IRM)

Information Rights Management (IRM) is a term that applies to a technology which protects sensitive information from unauthorised access. It is sometimes referred to as E-DRM, Enterprise Digital Rights Management. This can cause confusion because Digital Rights Management (DRM) technologies are typically associated with business to consumer systems designed to protect rich media such as music and video. Some existing IRM systems have been ongoing development of DRM style systems, however a true IRM system will have some important differences and is typically used to protect information in a business to business model, such as financial data, intellectual property and executive communications.

IRM currently applies mainly to documents and emails.

IRM technologies allow for several levels of security. Functionality offered by IRM usually comprises:

- Industry standard encryption of the information.
- Strong in use protection, such as controlling copy & paste, preventing screen shots and printing.
- A rights model/policy which allows for easy mapping of business classifications to information.
- Offline use allowing for users to create/access IRM sealed documents without needing network access for certain periods of time.
- Full auditing of both access to documents as well as changes to the rights/policy by business users

An example of IRM in use would be to secure a sensitive engineering document being distributed in an environment where the document's recipients could not necessarily be trusted. Alternatively, an e-mail could be secured with IRM, so if it accidentally is forwarded to an untrusted party, only authorised users would gain access.

Note that a well designed IRM system will not limit the ability for information to be shared, rather rules are only enforced when people attempt to gain access. This is important as often people share sensitive information with users who should legitimately have access but don't, and the technology needs to facilite the easy request of access back to the business owners.

IRM is far more secure than passwords, encryption is used to protect the information whilst it is at rest on a hard disk, network drive or other storage device. Crucially IRM continues to protect and control access to the document when it is in use.

Functionality such as preventing screen shots, disallowing the copying of data from the secure document to an insecure environment and guarding the information from programmatic attack, are key elements of an effective IRM solution.

http://en.wikipedia.org/wiki/Information_Rights_Management

Design:

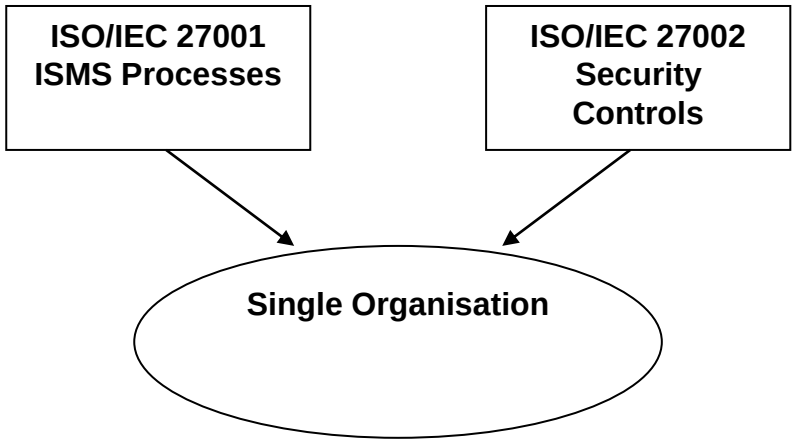
Information Rights Management (IRM)

Functionality offered by IRM usually comprises:

- Industry standard encryption of the information;
- Strong in use protection, such as controlling copy & paste,preventing screen shots and printing;
- A rights model/policy which allows for easy mapping of business classifications to information;
- Offline use allowing for users to create/access IRM sealed documents without needing network access for certain periods of time;
- Full auditing of both access to documents as well as changes to the rights/policy by business users.

http://en.wikipedia.org/wiki/Information_Rights_Management

ISO/IEC 27001/02

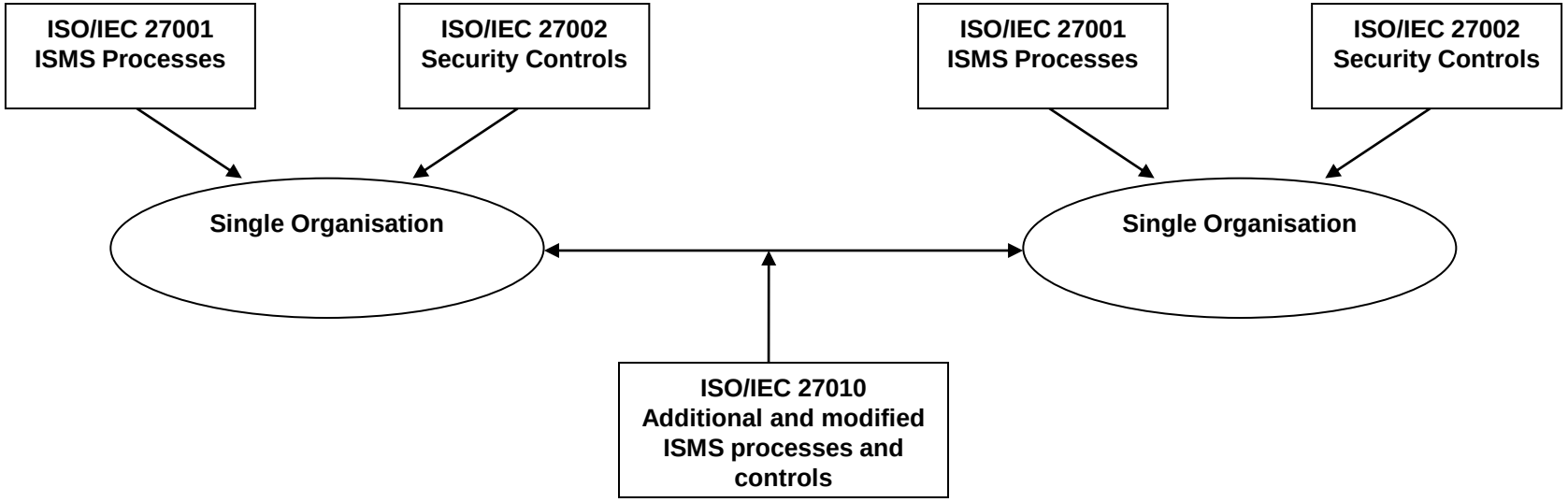


Examples:

Process requirement – “The organisation shall measure the effectiveness of controls to verify that the security requirements have been met” (ISO/IEC 27001, 4.2.3c)

Security control – “Information should be classified in terms of its value, legal requirements, sensitivity, and criticality to the organisation” (ISO/IEC 27002, 7.2.1)

ISO/IEC 27010 - Draft

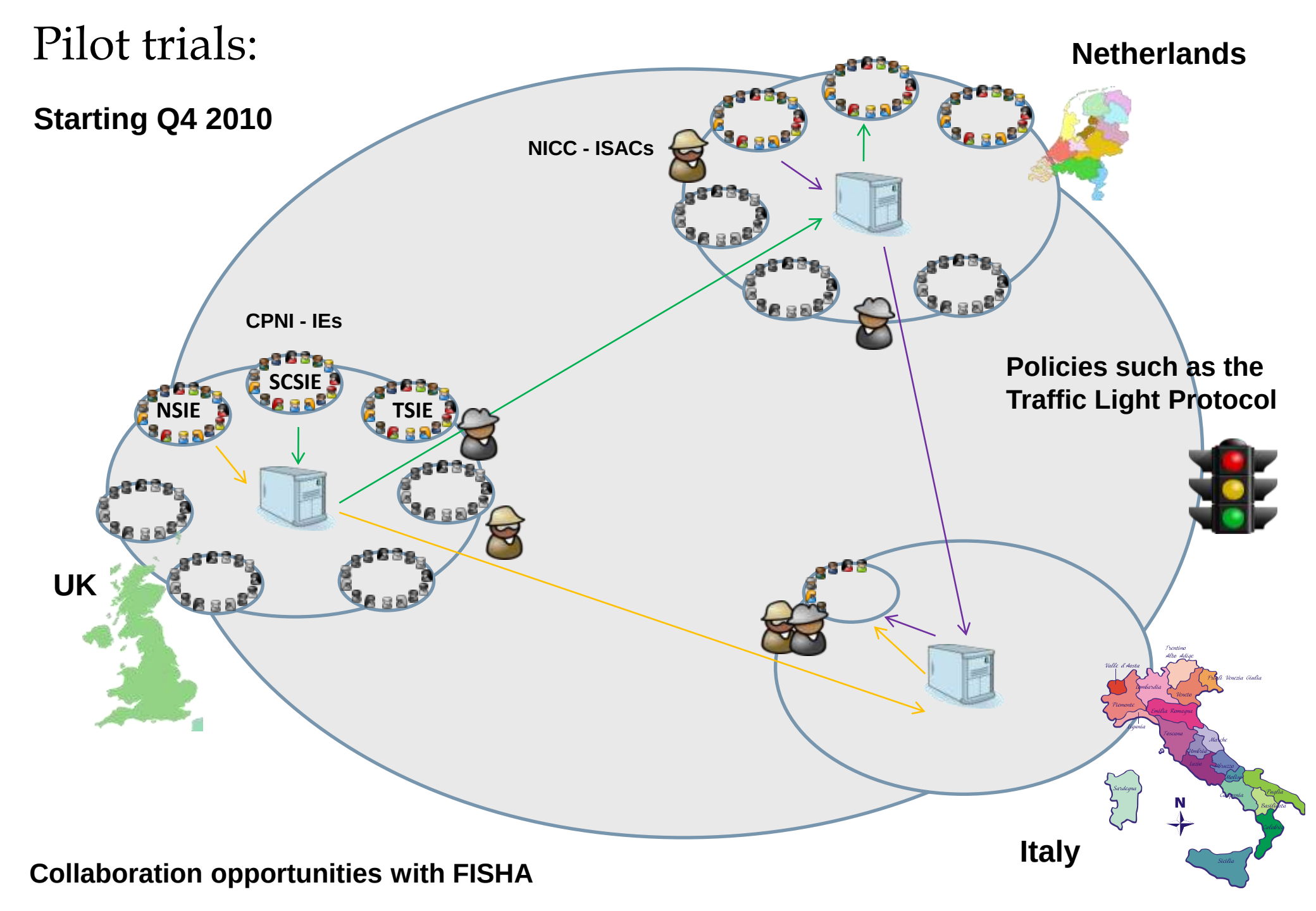


NEISAS feedback into ISO/IEC 27010 development:

"Anonymisation is an important tool for creating effective information sharing communities. However, the control as presented here is inadequate. It is important that the sanitisation process looks at message content as well as the message source, because analysis of the content may reveal the identity of the source. It is also good practice to ask the source where possible to review the anonymised information and the list of intended recipients before it is distributed."

Pilot trials:

Starting Q4 2010



Collaboration opportunities with FISHA

neisas

National & European Information Sharing & Alerting System

With the support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme"
European Commission - Directorate-General Justice, Freedom and Security"
"This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein."

Critical success factors for NEISAS prototype:

- **It must add value to NEISAS users**
- **It must reduce the risk of sharing on-line**
- **It must be seen to do both these**

www.neisas.eu

John Harrison – johnh@landitd.com