ETSI GR ETI 002 V1.1.1 (2023-03)

GROUP REPORT

Encrypted Traffic Integration (ETI); Requirements definition and analysis

Disclaimer

The present document has been produced and approved by the Encrypted Traffic Integration (ETI) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference

DGR/ETI-002

Keywords

confidentiality, network measurement, network monitoring, network performance

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Group Report (GR) has been produced by ETSI Industry Specification Group (ISG) Encrypted Traffic Integration (ETI).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document identifies the requirements for allowing Encrypted Traffic Integration (ETI) across an abstracted network architecture. The present document is informed by the ETI Problem Statement [i.1] and the Zero Trust Architecture (ZTA) security model [i.6] and its application, to provide an explicitly trusted commutations environment across all enabled layers of the Open Systems Interconnection (OSI) model. In addition the present document describes a security model, by way of ZTA, that enforces transparency and explicability of the role of security functions, particularly encryption.

NOTE 1: The OSI model [i.3], and the OSI based security model [i.4], [i.5] when implemented may not explicitly enable some layers, in particular layers 5 (Session) and 6 (Presentation) are often implied.

In addition, the present document defines use cases where ETI might not be sufficient to enable a ZTA environment and identifies mitigations to maintain ETI, while adhering to ZTA.

NOTE 2: The ZTA model begins by not trusting anything and builds and reinforces trust continuously during operation.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI GR ETI 001: "Encrypted Traffic Integration (ETI); Problem Statement".

[i.2] ETSI TS 103 486: "CYBER; Identity Management and Discovery for IoT".

[i.3] ISO/IEC 7498-1: "Information technology -- Open Systems Interconnection -- Basic Reference Model: The Basic Model".

[i.4] Recommendation ITU-T X.800: "Security Architecture for Open Systems Interconnection for CCITT Applications".

[i.5] ISO 7498-2: "Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture".

NOTE: ISO 7498-2 and Recommendation ITU-T X.800 contain the same text.

[i.6] NIST Special Publication 800-207: "Zero Trust Architecture".

[i.7] ETSI TR 103 309: "CYBER; Secure by Default - platform security technology".

[i.8] IETF RFC 6749: "The OAuth 2.0 Authorization Framework".

[i.9] ETSI GR SAI 007: "Securing Artificial Intelligence (SAI); Explicability and transparency of AI processing".

[i.10] ETSI TS 102 165-2: "CYBER; Methods and protocols; Part 2: Protocol Framework Definition; Security Counter Measures".

[i.11] ETSI TS 103 523-1: "CYBER; Middlebox Security Protocol; Part 1: MSP Framework and Template Requirements".

[i.12] Mbanaso and Cooper: "Conceptual Design of Obligation of Trust Protocol".

[i.13] Proposal for a regulation of the European parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

Zero Trust Architecture (ZTA): cybersecurity model that seeks to eliminate implicit trust

NOTE: In addition, NIST SP 800-207 [i.6] extends this term to address the evolving set of cybersecurity paradigms that move defences from static, network-based perimeters to focus on users, assets, and resources.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

A2ApoA	Application to Application point of Attachment
A2SpoA	Application to Service point of Attachment
AC	Access Control
ACL	Access Control List
ApoA	Application point of Attachment
CIA	Confidentiality Integrity Availability
CRA	Cyber Resilience Act
DDoS	Distributed Denial of Service
DP	Data Protection
E2E	End to End
ETI	Encrypted Traffic Integration
FTP	File Transfer Protocol
GC	Good Citizen
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
ICT	Information Communications Technology
MAC	Message Authentication Code
MSP	Middlebox Security Protocols
NoO	Notice of Obligations
OoT	Obligation of Trust
OSI	Open Systems Interconnection
PDU	Protocol Data Unit
PII	Personal Identifying Information
S2SpoA	Service to Service point of Attachment
S2TpoA	Service to Transport point of Attachment
SA	Security Association

SAI	Securing Artificial Intelligence
SAO	Signed Acceptance of Obligations
SDU	Service Data Unit
SNMP	Simple Network Management Protocol
SpoA	Service point of Attachment
T2TpoA	Transport to Transport point of Attachment
TCP	Transport Control Protocol
TLS	Transport Layer Security
TpoA	Transport point of Attachment
UDP	Unacknowledged Datagram Protocol
VPN	Virtual Private Network
ZTA	Zero Trust Architecture

4 Review of ETI problem and a solution

As identified in ETSI GR ETI 001 [i.1] one of the consequences of pervasive encryption is that some of the obligations placed on operators and suppliers with respect to regulation, law or convention, or operator security policy, may be difficult to meet.

It is also noted in ETSI GR ETI 001 [i.1] that whilst the use of encryption as the default approach to enhance the confidentiality (and often privacy) of communications often offers benefits, it may at the same time expose users and networks to threats from malicious traffic which, by not being recognized as a result of being hidden behind encryption, can no longer be filtered out by the network operator to protect the end user or the operator's network. This masking of function by the use of end-to-end encryption leads to a restriction of the ability of network management, anti-fraud, cyber security, and regulatory monitoring systems to manage data and communications flowing into, through, and out of networks which is detrimental to the user and network operators. Therefore it is stated in ETSI GR ETI 001 [i.1] that whilst encryption protects traffic flowing through a network from unauthorized inspection, encryption in itself does not protect the communicating end points or networks from attacks. Further, it reduces the ability of the operator to remove malicious traffic by appropriate use of the cybersecurity tools.

NOTE: Confidentiality as a synonym for privacy is not always accurate and using encryption to enhance confidentiality of data in transit, or in storage, does not offer any guarantee of privacy once the encryption is stripped off at the end point.

In a broad interpretation of the ETI problem statement it is surmised that making the operator and other stakeholders explicitly aware of the use and role of encryption, and other security techniques, in the system will allow mitigation of the negative effects of encryption whilst promoting their positive effects. The consequence for the present document is to make all security functions in a network explicit, with the further requirement to ensure that every transaction is made within a bounded set of Security Associations (SAs), while validating legitimacy of the transmitted data, that build to provide an explicit per transaction security model. The security model by being explicit should then also be considered as making an explicit trust model for each transaction. The initial point should be that the entire transaction and all the elements and data involved in the transaction are untrusted and insecure. The end point at which the transaction should take place is that all elements and data in the connection are secured and trusted.

An ETI conformant network should be able to demonstrate that for each connection there is an established trust contract, and an associated security contract. The remainder of the present document identifies the role of Zero Trust Architecture (ZTA) [i.6] and its close association to an active (rather than static) implementation of the secure by default paradigm [i.7] in providing the transparency and explicability of the use of encryption, while adhering to ZTA principles within related technologies to mitigate the ETI problem.

5 Requirements for supporting ETI in ICT systems

5.1 Overview

As stated in clause 4 above to support ETI the operator and other stakeholders should be explicitly aware of the use and role of encryption, and other security techniques, in the system. Thus all security functions in the ICT system or network should be explicit. In practical terms this requires that each security function is transparent and the rationale for each function is explicable, while conforming with ZTA.

NOTE: Whilst the primary focus of ISG ETI is on the integration of encryption into ICT systems it is recognized that for many laymen the term encryption is often used as a catch-all term to address other cryptographic functions. This then extends the scope of ETI to address those cryptographic operations that support encryption, including hashing, authentication and forms of access control.

5.2 Transparency

It should be possible for an authorized entity to request the encryption state of any connection or data at any involved, identifiable, and addressable object (hereinafter referred to as an entity), in the ICT system by direct interrogation of the entities participating in the connection. The requesting entity should be within the same trusted environment of the target entity (the one whose state is being interrogated) and therefore has to be identified and authenticated before being allowed to operate on the entity. The encryption state of any connection should be reported as one of: encryption applied; encryption not applied; or unknown.

NOTE 1: The identification of who is an authorized party is described in clause 5.4 of the present document.

NOTE 2: The entities refer to link, content, access, timing, destination and source information, resulting in conformance with ZTA.

In order to enable the transparency requirement, all entities in the communication chain should have a well defined (i.e. standardized) point of inspection, and a standardized query interface should be used.

As part of the goal of achieving transparency the sub-goals of accountability and explicability are considered. For this to be achieved the base requirement above should apply to the connection as a whole and the context in which encryption is applied.

NOTE 3: A number of means exist that attempt to verify and provide proof of the path any packet has taken across a network by addition of data to the packet header for 3rd party verification. The approach in the present document is to develop a trust and security contract for the connection that provides an alternative approach to achieve such proofs.

The model for explicability and transparency identified below extends from that found in ETSI GR SAI 007 [i.9] and summarized in Figure 1.

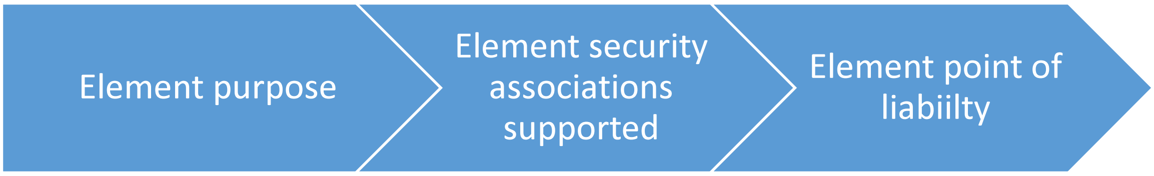
Element purpose
Element security associations supported
Element point of liabiilty

Figure 1: Components required in element documentation for transparency

Every element should be able to be identified and able to explain its purpose in the system. Every element should identify the forms of security association it supports, and for each security association the root of trust (as the point of liability) should be identifiable.

5.3 Management of cryptographic keys

The trend in cryptographic protection is towards perfect forward secrecy in which session keys cannot be compromised even if the root key from which the session keys are derived is itself made known. Ephemeral keys are a consequence or attribute closely associated to trying to achieve forward secrecy. A key is described as ephemeral when it is created uniquely for each key establishment process. The assurance of forward secrecy requires that the ephemeral session key is discarded after use.

For the purposes of ETI the legitimate use of forward secrecy should be maintained for each Security Association (SA) in a transaction. However the form of key agreement should be visible to authorized parties.

5.4 Identification of authorized parties

In clause 5.2 it is stated that the encryption state of any connection should only be disclosed to authorized parties. An authorized party should be unambiguously identified and that identity should be authenticated. The identity of the authorized party may take a number of forms including those defined in ETSI TS 103 486 [i.2] and using forms of attribute rich identity coupled to attribute based authentication modes as described in ETSI TS 103 486 [i.2].

Implementation of authorization should be explored in more detail in future work and may include examination of OAuth as defined in IETF RFC 6749 [i.8].

6 Trust architecture for ETI

A layered communications architecture, as defined for OSI in ISO/IEC 7498-1 [i.3], has implicit trust relationships at each layer determined by the functional model of each layer. The present document extends the OSI model to a wider concept of ZTA as in NIST SP 800-207 [i.6] beyond the enterprise network to a full public telecommunications network addressing the particular model described in clause 3.1.3 of [i.6] (ZTA Using Network Infrastructure and Software Defined Perimeters) to the entirety of the OSI stack.

The rationale of the ZTA is that there should be no assumptions as to what happens before or after each hop in and across the infrastructure, starting with the source and ending with the destination of a particular data flow at all layers of OSI. Every device, application and microservice is responsible for its own security. With each step a user (or the proxy for the user) makes through the infrastructure, the following two aspects provide adherence to ZTA:

- The system should provide means to validate, authenticate, and apply threat prevention capabilities across all locations consistently.
- The system should be able to validate the "who", the "what", the "where", the "when", the "why", and the "how" across all traffic flows throughout the lifecycle of those flows.

Whilst the abstracted model from ETSI TS 102 165-2 [i.10] is recommended for addressing the ETI problem it is recognized that the managed security of networks is broadly addressed by the following services as defined by the OSI 7-layer security model (see table 2 of Recommendation ITU-T X.800 [i.4] and its mirror ISO 7498-2 [i.5]) and the aspects of ZTA [i.6]:

- At layer 7:
    - Identity Assertion ("who").
    - Application Validation ("what").
    - To-be-accessed Targeted Resources Destination ("where").
    - Data Flow Time-stamping ("when").
    - Data Classification ("why").
    - Identity Assertion of the Targeted Resources Access ("how").
    - Peer Entity Authentication.
    - Data Origin Authentication.

  - etc.

- At layer 6:
  - Facilities provided by the presentation layer offer support to the provision of security services by the application layer to the application process.
  - The facilities provided by the presentation layer rely on mechanisms which can only operate on a transfer syntax encoding of data.
  - Security mechanisms in the presentation layer operate as the final stage of transformation to the transfer syntax on transmission, and as the initial stage of the transformation process on receipt.
- At layer 5: No security services are provided in the session layer.
- At layer 4:
  - Peer Entity Authentication;
  - Data Origin Authentication;
  - Access Control service;
  - Connection Confidentiality;
  - Connectionless Confidentiality;
  - Connection Integrity with Recovery;
  - Connection Integrity without Recovery; and
  - Connectionless Integrity.
- At layer 3:
  - Peer entity authentication.
  - Data origin authentication.
  - Access Control List (ACL).
  - Connection confidentiality.
  - Connectionless confidentiality.
  - Packet flow confidentiality.
  - Connection integrity without recovery.
  - Connectionless integrity.
- At layer 2:
  - Connection confidentiality.
  - Connectionless confidentiality.
- At layer 1:
  - Connection confidentiality.
  - Traffic flow confidentiality.

Each security service in the OSI model exists as a peer to peer service, i.e. network layer to network layer, application layer to application layer. Each layer has an implicit security association determined by the key used to protect the services at that layer. The model in the present document extends the OSI peer-to-peer model with the ZTA defined in [i.6] and addresses the identity management requirements as an instance of the model for ZTA Using Enhanced Identity Governance ([i.6], clause 3.1.1).

Layers should be developed as independent trust zones with clear visibility (see clause 5.1 Transparency) of the services offered. By the term independent trust zone it is intended that each layer should have autonomy from any other layer.

As Figure 2 illustrates, ZTA adds the following attributes to each of the OSI layers:

- Layer 7: Data Validation and Integrity check, Threat Intelligence, Microsegmentation of Services; Identity Assertion.
- Layer 6: This is folded into Layer 7.
- Layer 5: This is folded into Layer 7.
- Layer 4: Pure Access Control Lists do not guarantee ZTA, hence this is folded into Layer 7.
- Layer 3: Microsegmentation, Data Source validation, Data Destination validation, Data Destination Authentication.
- Layer 2: This is folded into Layer 3.
- Layer 1: Authenticity and validation checks of all hardware and software components.

In summary, ZTA follows the principle of "never trust, always verify".

The model of trust, on the other hand, is that whilst content of user communication may view the network as untrusted and the user may choose to apply application layer services to ensure confidentiality of user content, the lower layers are themselves contained in layer specific trust relationships. In this way all data required to enable layer operations should be visible to that layer.

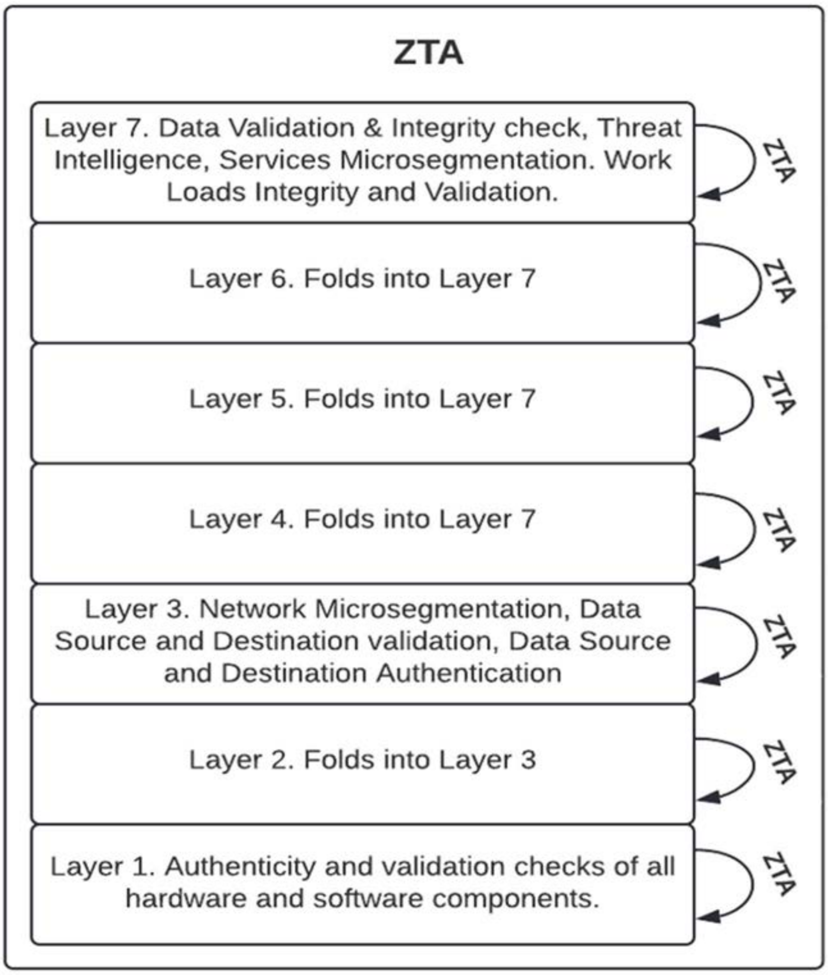
ZTA
Layer 7. Data Validation & Integrity check, Threat Intelligence, Services Microsegmentation. Work Loads Integrity and Validation.
ZTA
Layer 6. Folds into Layer 7
ZTA
Layer 5. Folds into Layer 7
ZTA
Layer 4. Folds into Layer 7
ZTA
Layer 3. Network Microsegmentation, Data Source and Destination validation, Data Source and Destination Authentication
ZTA
Layer 2. Folds into Layer 3
ZTA
Layer 1. Authenticity and validation checks of all hardware and software components.
ZTA

Figure 2: Representation of ZTA mapping to OSI layers

In general, whereas trust can be defined in spoken and written English as "*firm belief in the reliability, truth, or ability of someone or something*" this has to be translated into something more tangible and exact for ICT systems and has often been simplified into the assertion of integrity of an object where that assertion is made, or attested to, by a known entity. A number of forms of integrity assertion exist, summarized in ETSI TS 102 165-2 [i.10], including the use of Message Authentication Codes (MACs), Hash functions, and digital signatures. The present document does suggest that security association is used as a synonym for trust association.

An end-to-end connection is composed of at least one and more likely an indeterminate, but finite, number of security associations. E2E security is thus not just an end-point issue but a composition of SAs issue. Each security association is also a representation of a trust association and for the purposes of the present document trust is a weighting that applies to a security association.

$$\sum Trust.SA$$

Each security association should be protected by a unique key. For compositions of security associations, where one security association is dependent on another security association within the overall composition, they should be protected by different (*and also unique*) keys. The nature of an SA, one-to-one, one-to-many (including broadcast), many-to-one and many-to-many, has a significant influence on the selection of keying strategy to protect to the SA, details of keying strategies are addressed in ETSI TS 102 165-2 [i.10].

NOTE 1: An SA does not imply encryption but rather explicitly identifies the nature of the security association, e.g. an SA and key for each of integrity/confidentiality/availability. Therefore SA should not be read as shorthand for encrypted link.

In the ETI model each link should represent trust for each attribute of the CIA paradigm:

- How is data encrypted and decrypted? Who establishes the keys?
- Source authentication → as a prerequisite for the other attributes.
- How is data integrity preserved?
- How is the identity of the asset and link assured?
- How is access control to data and services related to the link assured?

When the ZTA model is completed the result is a trust contract between end points that details the form of security association on each link and at each layer.

NOTE 2: Not all links will be explicit as some links will essentially be passive (layer 1 and 2 links often have no complex security associations).

The role of trust contracts is addressed in part by obligation of trust protocols (see ETSI TS 103 486 [i.2] and also [i.12]).

7 Reference model of an ICT network for ETI

7.1 Layered abstract model

In the OSI model [i.3] a layer, N, offers services to the higher layer, N+1, using a model whereby services of layer N can be "requested" by layer N+1, and that requested service is "indicated" to the peer layer N+1. This is illustrated in Figures 3, 4 and 5. The same degree of abstraction applies in ETSI TS 102 165-2 [i.10] in the model adopted in the present document as Figure 6 in clause 7.2.

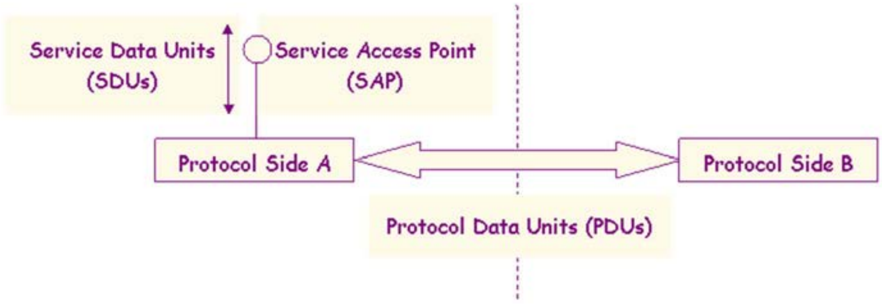

Figure 3: OSI model of Service Access Points to access a protocol layer

With respect to the layering model the service offered by layer N may include an encryption service, i.e. to encrypt the SDU as the payload of the resulting PDU. As a PDU at Layer N becomes an SDU of Layer (N-1) (see Figure 3) any encryption applied at Layer N is not visible to Layer N-1 as the data content of the Layer N SDU is not intended to be visible to Layer N-1. Where the content of the Layer N SDU is required to be visible to Layer N-1 it is a layering violation.

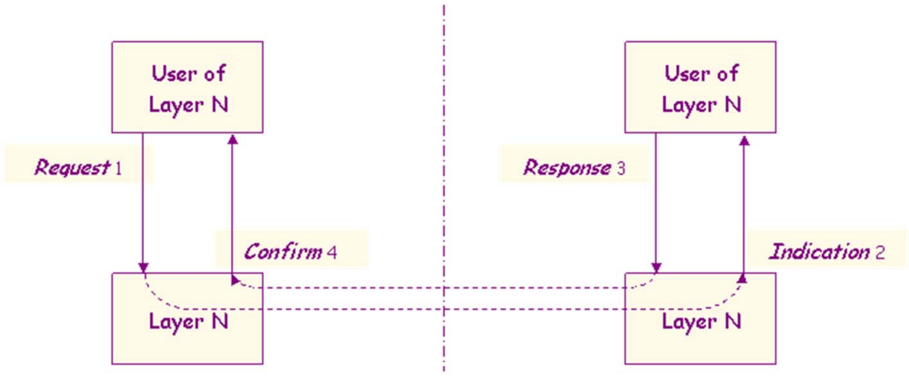

Figure 4: OSI model showing the role of req/ind and resp/conf information flows

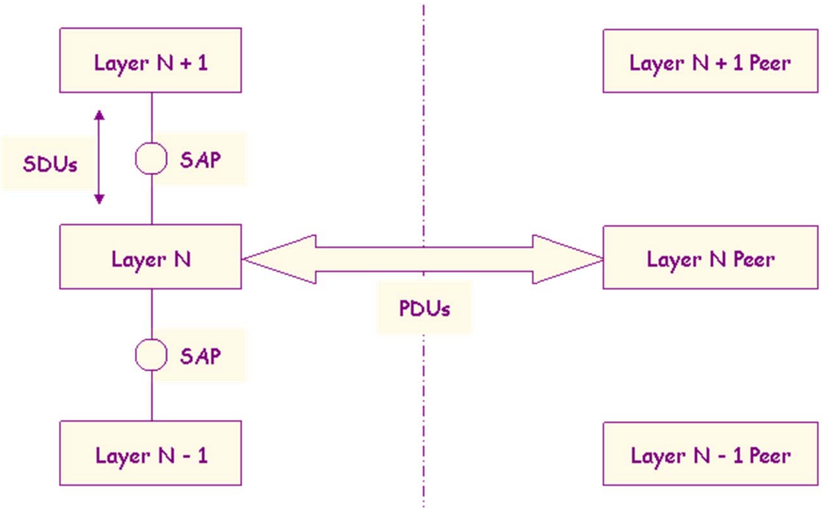

Figure 5: The OSI model across multiple layers

7.2 Planar abstract model

An alternative security model for ETI, and the one recommended in the present document, is that found in ETSI TS 102 165-2 [i.10] and copied below for convenience. In this latter model the OSI model [i.3], [i.5] is simplified to 3 planes: Transport; Service and Application. Between planes both horizontally and vertically are "points of attachment" and it is at these points of attachment that the security services lie. The transport service approximates to the lower layers of the OSI model, the service layer approximates to the higher layers of the OSI model, with the application layer addressing the user level application.

NOTE 1: The specific terminology from ETSI TS 102 165-2 [i.10] is drawn from a traditional telecoms consideration but with a relaxed interpretation can be mapped to non-telecoms environments, including those of conventional programming, to business practices and similar.

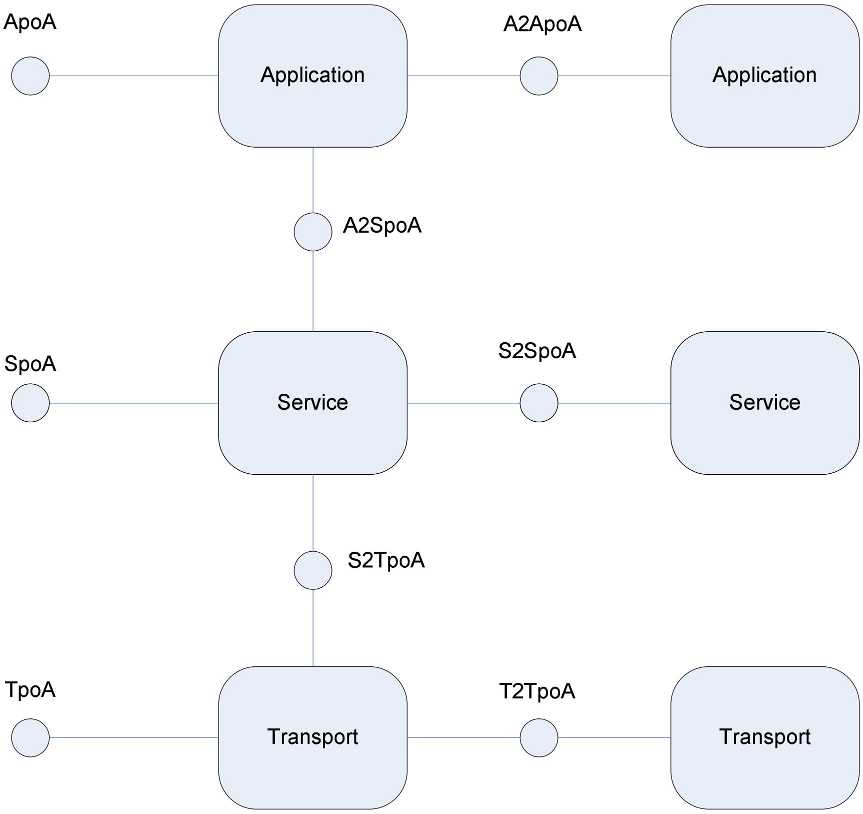

Figure 6: Abstract architecture for security countermeasure application from ETSI TS 102 165-2 [i.10]

The user connects to each layer using a layer specific point of Attachment (poA):

- TpoA Transport point of Attachment (TpoA reference point).
- SpoA Service point of Attachment (SpoA reference point).
- ApoA Application point of Attachment (ApoA reference point).

The countermeasures are described with respect to the user interaction with each layer:

- Inbound authentication at TpoA/SpoA/ApoA.
- Outbound authentication at TpoA/SpoA/ApoA.

NOTE 2: If an authentication exchange nests inbound and outbound authentication, it is termed mutual authentication. However if the exchanges are discrete and with different lifetimes the term mutual authentication is inappropriate.

- Integrity of communication at TpoA/SpoA/ApoA.
- Confidentiality of communication at TpoA/SpoA/ApoA.

Within the system the countermeasures are extended to cover interactions between layers both vertically and horizontally. The set of countermeasures thus include:

- Service to Service authentication.
- Integrity of communication from Service to Service.
- Confidentiality of communication from Service to Service.

NOTE 3: The term Service is used as a synonym for any of the three abstract layers of the ICT architecture.

The services apply to the following points on Figure 4:

- A2SpoA Application to Service reference point.
- S2TpoA Service to Transport reference point.
- A2ApoA Application to Application reference point.
- S2SpoA Service to Service reference point.
- T2TpoA Transport to Transport reference point.

NOTE 4: The model does not show a specific reference point between Application and Transport on the assumption that a Service layer always exists.

In addition to the countermeasures provided at the identified reference points a secure system may have to deploy other countermeasures to protect their assets. Such countermeasures may include billing controls, system auditing and event logging.

7.3 Example protocols mapping to ETI model

7.3.1 Obligation of trust protocol models

In a generalization of the Obligation of Trust (OoT) protocol each party exchanges difficult-to-repudiate digitally signed obligating constraints (termed Notification of Obligations (NoO)) which detail their requirements for sending data or information to the other party, and proof of acceptances (or Signed Acceptance of Obligations (SAO)), which acknowledge the conditions they have accepted for receiving the other party's sensitive information.

The intent of the OoT exchange is that parties to data negotiate the conditions (constraints) that apply to data that they share. Obligations that are exchanged may take 2 distinct forms:

- security obligations (cryptographic mechanisms required for protection); and
- privacy obligations (usage and onward sharing requirements).

The aim of these kind of protocols is to develop support for "non-repudiation of consent" in which the system and users build a strong proof of having given consent to specific processing of precisely defined data. The relationship to ETI is that the OoT, NoO and SAO together form a trusted contract for a particular security association between the parties.

The describing of obligations in the context of OoT protocols is closely related to the explicit identification of the security offered in an SA but has its roots in protection of Personal Identifying Information (PII) hence the more detailed framework of non-repudiation schemes at its root.

Obligation of trust for protection of PII to be extended to the wider and more extensive network model that supports ETI is not trivial but may have particular application at the ApoA (see Figure 6). The application of OoT protocols in the ETI environment is not trivial but the core model is which the SAO and the NoO structures set up a flexible framework for device communications, capable of underpinning discovery and trust establishment, whether in simple environments or complex, multi-authority environments in which devices have complete flexibility as to their policies for:

- establishment and evaluation of trust relationships;
- information sharing during discovery;

- protection mechanisms for authentication, integrity and confidentiality.

Further development of OoT in the context of ETI is encouraged for further study.

7.3.2 Middlebox security models

The role of proxies or middleboxes in networks and the means to allow them to intervene in traffic management is introduced in ETSI TS 103 523-1 [i.11] and summarized in the present document. In particular the role of middlebox control using Middlebox Security Protocols (MSP) is driven by the following objectives:

E: Endpoints are able to access middlebox services securely.

M: Middleboxes are able to provide services to endpoints securely.

The MSP identifies four principles in building the MSP Framework:

1) Given that there is a risk of data not being protected from network attackers the Data Protection (DP) principle explicitly protects data from network attackers and malicious actors.

2) Given the risk of not fully knowing which parties have what access to the data the Transparency (T) principle explicitly makes available to authorized parties knowledge of which parties have what access to the data.

3) Given the difficulty for endpoints meaningfully being able to grant access to parties without this knowledge gives rise to the Access Control (AC) principle in which endpoints can meaningfully grant access to relevant.

4) Given the complexity of networks that that adds DDoS attack vectors to the network has identified a Good Citizen (GC) principle that addresses the complexity to limit the likelihood of DDoS attack vectors entering the network by data sharing and collective responsibility.

With respect to ETI the overall framework of transparency arising from the above principles appears to be a close match. In particular it is recognized that the MSP Framework is hierarchical; each of the four principles is subdivided and forms a 'tree'. The level of detail increases through the 'branches' and 'sub-branches', until reaching detail where it is reasonably easy to judge whether each property is met ('leaves'). Labels are applied to every level of the tree in the MSP Framework. These labels relate to the parent branches from where the requirement is derived, to show the hierarchical nature of the requirement derivation. This is illustrated in Figure 7.

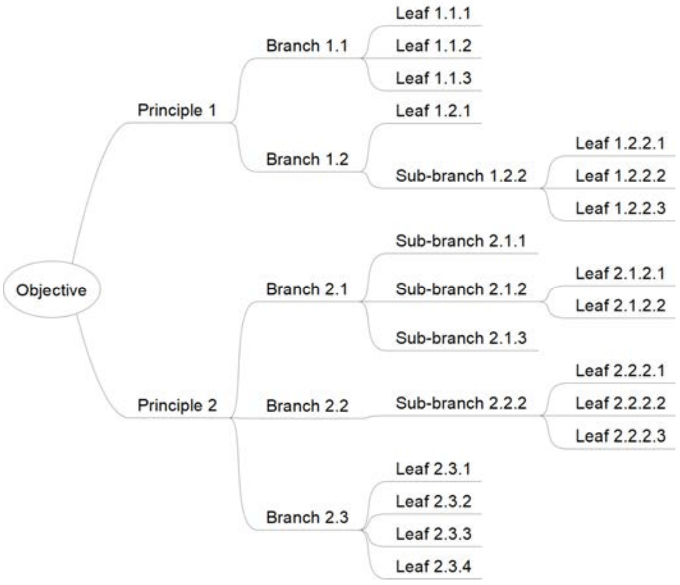

Figure 7: Example tree

The MSP Framework is designed to be flexible. Within the MSP framework, profiles, such as for ETI, can be defined that ensure that the four principles outlined above hold true.

7.3.3 Internet protocol models

There are many ways of modelling the "internet". It is possible to model the connectionless and connection-oriented concepts of telecoms connections to, for example, UDP and TCP, and to suggest content protocols in many forms, e.g. FTP, HTTP, map to application layers, with additional content definitions, e.g. HTML, SNMP also mapping at the upper layers of an OSI model view.

Table 1

	Peer#1	Local hub	Core network	Core network	Core network	Local hub	Peer#2
Application	end-to-end encryption						
Presentation							
Session	Session or Transport layer encryption (e.g. TLS)						
Transport							
Network	Network encryption (e.g. Ipsec)						
Link	Link encryption						
Physical							

NOTE: Common (layperson) interpretation is that TLS is an end-to-end security provision, similarly many VPN implementations are commonly understood to be end-to-end security provisions. The conventions used in the present document adhere to the OSI model and therefore distinguish virtual network security (layering violations) from strict interpretation of peer relationships.

The importance of ETI is that it has to be inclusive of all protocols.

Annex A: Illustration of how ETI/ZTA enables regulatory compliance

A significant number of global regulations apply to the placement of goods and services in the market. As ETI cannot be retroactively applied the following illustration is only applicable to an understanding of the future direction and expectations of regulation.

The EU Cyber Resilience Act (CRA) [i.13] applies to entities containing digital elements. The role of ETI/ZTA in allowing a system to address the requirements of the CRA is given in Table A.1 against statements found in Annex I of the CRA.

NOTE: The term shall in Table A.1 is quoted from the CRA [i.13] and is not to be interpreted as per the ETSI rules for modal verbs.

Table A.1: Illustrative application of ETI to the Cyber Resilience Act

Products with digital elements shall …	ETI role
be delivered with a secure by default configuration, including the possibility to reset the product to its original state;	ETI and its use of ZTA enhances the use of secure by default by active enforcement, and reinforcement, of a trusted security association throughout the active life of the association.
ensure protection from unauthorized access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems;	ETI makes the application of security controls visible within a ZTA model and thus implements the model of least privilege that restricts access by default.
protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms;	ETI is a reaction to encryption everywhere by allowing oversight and control
protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorized by the user, as well as report on corruptions;	n/a
process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended use of the product ('minimization of data');	n/a
protect the availability of essential functions, including the resilience against and mitigation of denial of service attacks;	One purpose of ETI is to ensure that essential functions for maintenance of the network are available in the presence of encryption
minimize their own negative impact on the availability of services provided by other devices or networks;	As above
be designed, developed and produced to limit attack surfaces, including external interfaces;	n/a

History

Document history		
V1.1.1	March 2023	Publication