



**Identity and access management for
Networks and Services (INS);
Security and privacy requirements for
collaborative cross domain network monitoring**

[ETSI GS INS 009 V1.1.1 \(2012-09\)](https://standards.iteh.ai/catalog/standards/etsi/20cb5c14-d30e-458d-9a3f-4425c094584a/etsi-gs-ins-009-v1-1-1-2012-09)

<https://standards.iteh.ai/catalog/standards/etsi/20cb5c14-d30e-458d-9a3f-4425c094584a/etsi-gs-ins-009-v1-1-1-2012-09>

Disclaimer

This document has been produced and approved by the Identity and access management for Networks and Services 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

DGS/INS-009

Keywords

access control, data sharing, multi-party
computation, network monitoring, policies, policy
management, privacy, security

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 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

<https://standards.iteh.ai>
Document Preview

Important notice

Individual copies of the present document can be downloaded from:

<https://standards.iteh.ai/catalog/standards/etsi/20cb11-9a3f-4425c094584a/etsi-gs-ins-009-v1-1-1-2012-09>
<http://www.etsi.org>

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

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

<http://portal.etsi.org/tb/status/status.asp>

If you find errors in the present document, please send your comment to one of the following services:

http://portal.etsi.org/chaicor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2012.
All rights reserved.

DECT™, PLUGTESTS™, UMTS™ and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPP™ and LTE™ are Trade Marks of ETSI registered for the benefit of its Members and
of the 3GPP Organizational Partners.
GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

Intellectual Property Rights	5
Foreword.....	5
Introduction	5
1 Scope	6
2 References	6
2.1 Normative references	6
2.2 Informative references.....	6
3 Abbreviations	9
4 Scenario description and basic concepts	9
4.1 Cooperative incident handling by network operators	10
4.2 Cooperative incident handling among enterprises.....	11
4.3 Cooperative anomaly and misuse detection	11
5 Sharing schemes used in cooperative incident handling	11
5.1 Annotated Sharing Schemes.....	12
5.2 Trusted-Third-Party Sharing Schemes	13
5.3 Secure Sharing Schemes	13
6 Requirements.....	14
6.1 Business requirements	14
6.1.1 Confidentiality of business-sensitive data.....	14
6.1.2 Impact on network operations.....	14
6.1.2.1 Roles	14
6.1.2.2 Same domain operations	14
6.1.2.3 Cross-domain operations.....	14
6.1.2.4 Legacy systems	15
6.2 Regulatory requirements	15
6.2.1 Lawfulness of data processing.....	15
6.2.2 Purposes for which data are processed	15
6.2.3 Necessity, adequacy and proportionality of the data processed.....	15
6.2.4 Quality of the data processed.....	15
6.2.5 Minimal use of personal identification data.....	15
6.2.6 Storage of personal data.....	15
6.2.7 Data retention.....	15
6.2.8 Access limitation	16
6.2.9 Information to and rights of the data subject	16
6.2.10 Consent of the data subject	16
6.2.11 Data security measures	16
6.2.12 Special categories of data	16
6.2.13 Coordination with competent Data Protection Authority	16
6.2.14 Supervision and sanctions.....	16
6.2.15 Communications confidentiality.....	17
6.2.16 Dissemination of data to third parties	17
6.2.17 Transfer of data to third countries.....	17
6.2.18 Flexibility and adaptability of legal compliance provisions	17
6.3 Technical requirements	17
6.3.1 Privacy requirements	17
6.3.1.1 Purpose specification and binding.....	17
6.3.1.2 Necessity, adequacy and proportionality.....	18
6.3.1.3 Cooperation with third parties.....	18
6.3.1.4 Complementary actions.....	18
6.3.1.5 Data storage and retention.....	18
6.3.1.6 Data protection mechanisms	18
6.3.1.7 Access control	19

6.3.1.8	Semantics	19
6.3.2	Security requirements	19
6.3.2.1	Confidentiality	19
6.3.2.2	Integrity	19
6.3.2.3	Availability.....	19
6.3.2.4	Backup	19
6.3.2.5	Access audit logs.....	19
6.3.2.6	Network Segmentation.....	20
7	Available solutions and gaps.....	20
7.1	Incident information sharing (IETF INCH and MILE)	20
7.1.1	The Incident Object Description Exchange Format - IODEF.....	20
7.1.2	Real-time Inter-network Defense – RID	21
7.1.3	Applicability to collaborative cross-domain network monitoring	21
7.2	Access Control	21
7.3	Secure multiparty computation and other cryptographic approaches.....	23
8	Conclusion.....	23
Annex A (informative): Authors & contributors.....		24
History		25

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[ETSI GS INS 009 V1.1.1 \(2012-09\)](https://standards.iteh.ai/catalog/standards/etsi/20cb5c14-d30e-458d-9a3f-4425c094584a/etsi-gs-ins-009-v1-1-1-2012-09)

<https://standards.iteh.ai/catalog/standards/etsi/20cb5c14-d30e-458d-9a3f-4425c094584a/etsi-gs-ins-009-v1-1-1-2012-09>