# ETSI GR CIM 007 V1.1.1 (2022-03)




# Context Information Management (CIM); Security and Privacy



***Disclaimer***

The present document has been produced and approved by the cross-cutting Context Information Management (CIM) 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/CIM-007-SEC

Keywords
API, architecture, GAP, information model, privacy, security, smart city

***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

# 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) cross-cutting Context Information Management (CIM).



# 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.

# Introduction

The present document identifies the security and privacy aspects that are relevant when building systems based on the NGSI-LD API and the NGSI-LD information model. It defines high-level objectives that have to be taken into account when specifying the mechanisms that enable addressing the security and privacy aspects.

Contributions to the present document have been supported by the following European Union Horizon 2020 research projects: Fed4IoT (Grant number 814918) and IoTCrawler (Grant number 779852).

# 1 Scope

The present document provides a security and privacy review of the ISG CIM specifications, in particular the NGSI-LD API [i.1] and the Data Model [i.2]. The review identifies the risks from attack and means to mitigate the risk in the form of core security objectives and privacy protection objectives to be met by NGSI-LD Systems.

NOTE: The scope of the security and privacy protection objectives include those related to data provenance, and the role of data aggregation as impacting the attack surface of NGSI-LD System deployments.

# 2 References

## 2.1 Normative references

Not applicable to 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 GS CIM 009: "Context Information Management (CIM); NGSI-LD API".

[i.2] ETSI GS CIM 006: "Context Information Management (CIM); Information Model (MOD0)".



NOTE: Available at https://www.etsi.org/deliver/etsi_gs/CIM/001_099/006/01.01.01_60/gs_cim006v010101p.pdf.

[i.3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (GDPR).

[i.4] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive).

[i.5] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC (Radio Equipment Directive (RED)).

[i.6] European Treaty Series No. 185: "Convention on Cybercrime".

NOTE: Available at https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185.

[i.7] ETSI EN 303 645: "CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements".

NOTE: Available at https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf.

[i.8] ETSI TS 102 165-1: "CYBER; Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)".

NOTE: Available at https://www.etsi.org/deliver/etsi_ts/102100_102199/10216501/05.02.03_60/ts_10216501v050203p.pdf.

[i.9] ETSI TS 102 165-2: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 2: Protocol Framework Definition; Security Counter Measures".

NOTE: Available at https://www.etsi.org/deliver/etsi_ts/102100_102199/10216502/04.02.01_60/ts_10216502v040201p.pdf.

[i.10] IETF RFC 3986: "Uniform Resource Identifier (URI): Generic Syntax".

NOTE: Available at https://tools.ietf.org/html/rfc3986.

[i.11] Jean Louis Raisaro, Juan Ramon Troncoso-Pastoriza, Mickael Misbach, Joao Sa Sousa, Sylvain Pradervand, Edoardo Missiaglia, Olivier Michielin, Bryan Ford, and Jean-Pierre Hubaux. 2019. MedCo: Enabling Secure and Privacy-Preserving Exploration of Distributed Clinical and Genomic Data. IEEE/ACM Trans. Comput. Biol. Bioinformatics 16, 4 (July 2019), 1328-1341.

NOTE: DOI: https://doi.org/10.1109/TCBB.2018.2854776.

[i.12] i2b2, Informatics for Integrating Biology & the Bedside, National Center for Biomedical Computing, USA.

NOTE: Available: https://www.i2b2.org/index.html.

[i.13] L. Cinquini et al., "The Earth System Grid Federation: An open infrastructure for access to distributed geospatial data," 2012 IEEE 8th International Conference on E-Science, 2012, pp. 1-10.

NOTE: DOI: https://doi.org/10.1016/j.future.2013.07.002.

[i.14] ETSI TS 103 485: "CYBER; Mechanisms for privacy assurance and verification".

[i.15] ETSI TS 103 486: "CYBER; Identity Management and Discovery for IoT".

[i.16] ETSI TS 187 020: "Radio Frequency Identification (RFID); Coordinated ESO response to Phase 1 of EU Mandate M436".

[i.17] ETSI TS 102 894-2: "Intelligent Transport Systems (ITS); Users and applications requirements; Part 2: Applications and facilities layer common data dictionary".

[i.18] OASIS: "eXtensible Access Control Markup Language (XACML) Version 3.0".

[i.19] ETSI TR 103 719: "CYBER; Guide to Identity Based Cryptography".

[i.20] ETSI TS 103 352: "CYBER; Attribute Based Encryption for Attribute Based Access Control".



# 3 Definition of terms, symbols and abbreviations

## 3.1 Terms

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

**Access Control:** means of prevention of unauthorized use of an Object or Service by a User or the public

**Action:** operation involving modifying or reading an Object or its Attribute. e.g. create, read, update, delete

**Actor:** individual person, group of persons, organization, or company

**Administrator Policy:** Policy defined by an administrator and applicable to any of the current data and services in the NGSI-LD System

**Agent:** software program that represents Actors to produce, consume or manipulate data

**Attribute:** characteristic of an Object or User

NOTE: An Attribute is the minimal piece of data that the system grants access to or bases access control decisions upon.

**Consumer:** User consuming data

**Context:** measured and inferred knowledge that describes the environment of an Entity

**Context-based Access Control:** Access Control decision process based on Context

**Contract:** formal agreement governing part of the collective behaviour of the involved Actors

**Credentials:** data that is transferred to establish or confirm the claimed Identity of a User

**Data Controller:** natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of Personal Data

**Data Processor:** natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller

**Data Provenance:** metadata that is associated with data that details the origin, changes to, and details supporting the confidence or validity of data



**Data Subject:** identified or identifiable natural person, who can be identified directly or indirectly in particular by reference to an identification number or to one or a combination of factors specific to physical, physiological, mental, economic, cultural or social identity

**Entity:** Object that is an informational representation of something that is considered to exist in the real world, physically or conceptually



**Group:** named set of Users, Objects or Attributes

**Identity:** set of Attributes by which an Entity or User is uniquely described, recognized or known

**Integrity:** surety that the data or service has not been altered or destroyed in an unauthorized manner

**NGSI-LD Actor:** human or legal entity, operating the NGSI-LD Agents and legally responsible for their actions.

**NGSI-LD Agent:** software components that interact with each other using NGSI-LD

**NGSI-LD Attribute:** NGSI-LD Property or an NGSI-LD Relationship

**NGSI-LD Context Information:** measured and inferred knowledge that describe the environment represented by means of NGSI-LD Entities and/or NGSI-LD Attributes

**NGSI-LD Consuming Actor:** NGSI-LD Actor consuming data from an NGSI-LD Providing Actor including the NGSI-LD Broker

**NGSI-LD Entity:** Entity in an NGSI-LD System

**NGSI-LD Property:** description which associates a main characteristic, i.e. an NGSI-LD Value, to either an NGSI-LD Entity, an NGSI-LD Relationship or another NGSI-LD Property

**NGSI-LD Providing Actor:** NGSI-LD Actor providing data to an NGSI-LD System

**NGSI-LD Relationship:** description of a directed link between a subject which is either an NGSI-LD Entity, an NGSI-LD Property or another NGSI-LD Relationship on one hand, and an object, which is an NGSI-LD Entity, on the other hand

**NGSI-LD System:** set of all interconnected software components that use the NGSI-LD API for communicating among each other

**NGSI-LD User:** User that is registered in an NGSI-LD System

**NGSI-LD Value:** JSON value (i.e. a string, a number, true or false, an object, an array), or a JSON-LD typed value (i.e. a string as the lexical form of the value together with a type, defined by an XSD base type or more generally an IRI), or a JSON-LD structured value (i.e. a set, a list, a language-tagged string)

**Object:** data unit created or requested by an application

**Personal Data:** any information relating to an identified or identifiable natural person (Data Subject)

**Policy:** set of Access Control rules defining allowed Users for certain operations within specified contexts that each User has to comply with to be granted access to an Object

**Provider:** User providing data

**Service:** software functionality that different Users can reuse, together with the Policies that should control its usage

**Subject:** User acting as Consumer or Provider of a Service

**Trust:** level of confidence in the capabilities and Integrity of a User or Service

**User:** Virtual representation of an Actor or Agent

NOTE: If users have to be registered in a registration process then this requires issuing Credentials

**User Policy:** Policy defined by a User and restricted to the set of data inserted by that User

## 3.2 Symbols

Void.



## 3.3 Abbreviations

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



| | |
|---|---|
| API | Application Programming Interface |
| CIA | Confidentiality, Integrity and Availability |
| CoE | Council of Europe |
| DTE | Deterministic Encryption |
| EAV | Entity Attribute Value |
| EN | European Norm |
| ESGF | Earth System Grid Federation |
| EU | European Union |
| GDPR | General Data Protection Regulation |
| HIV | Human Immunodeficiency Virus |
| HTTP | Hypertext Transfer Protocol |
| HVAC | Heating Ventilation and Air Conditioning |
| IBC | Identity Based Cryptography |
| ICT | Information and Communication Technology |
| IdM | Identity Management |
| IP | Internet Protocol |
| IRI | Internationalized Resource Identifier |
| ISG | Industry Specification Group |
| JSON | JavaScript Object Notation |
| JSON-LD | JSON Linked Data |
| LD | Linked Data |
| MQTT | Message Queuing Telemetry Transport |
| NGSI | Next Generation Service Interfaces |
| PDP | Policy Decision Point |
| PEP | Policy Enforcement Point |
| SA | Security Association |
| SPU | Storage and Processing Unit |

| | |
|---|---|
| SSL | Secure Sockets Layer |
| TCP | Transport Control Protocol |
| UDP | User Datagram Protocol |
| UML | Unified Modelling Language |
| URI | Uniform Resource Identifier |
| VPN | Virtual Private Network |
| XACML | eXtensible Access Control Markup Language |
| XML | eXtensible Markup Language |
| XSD | XML Schema Definition |

# 4 Security and Privacy in the context of NGSI-LD Systems

ETSI ISG Context Information Management (CIM) has defined NGSI-LD as a means of managing and exchanging context information (in a broad sense) between a variety of systems. The present document addresses security and privacy with respect to NGSI-LD and the NGSI-LD API.

In examining the role to be played by Security and Privacy provisions for NGSI-LD, several characteristics regarding the NGSI-LD architecture are considered as below:

- NGSI-LD systems use the NGSI-LD API through which they can query other systems, provide notifications, and receive responses to queries.

EXAMPLE: A Parking Management System could query a Traffic Management System about road occupancy at a particular egress gate.

- Means are available for NGSI-LD systems to discover, register, and report existence of entities and relationships within and across several instances of platforms.
- Distributed NGSI-LD system instances need to be able to reconcile the identity of entities referenced in different systems.



# 5 System Architecture

## 5.1 The security model

In most ICT security systems, the provisions for security are made with respect to Confidentiality, Integrity and Availability (CIA) characteristics of data, processes, protocols or systems. In addition, many security analysis approaches consider Security Associations (SA) between peers, conventionally referred to as Alice and Bob, with Eve playing the role of universal adversary. Thus, the CIA model is presented as follows:

- Confidentiality, wherein data shared by Alice with Bob cannot be accessed by Eve.
- Integrity, offering assurance that data shared by Alice with Bob cannot have been manipulated by Eve.
- Availability, offers assurance that data is available to Alice when it is required and not available to any Eve masquerading as Alice.

NOTE 1: The CIA triad, or CIA paradigm, has no straightforward defining reference as its source but, rather, has evolved in a number of environments over time, with references found in increasing numbers from the early 1970s and leading to almost universal acceptance over the intervening period. Offering a single authoritative source as a reference to the term "CIA" is likely to be misleading, or to be contested.

NOTE 2: The convention of naming actors Alice, Bob and Eve has been widely adopted in the security domain as a more reader friendly approach than referring to Peer-A, Peer-B, Peer-C and so on. A Wikipedia article (https://en.wikipedia.org/wiki/Alice_and_Bob) offers some additional insight although there is some dispute regarding the origin of the Alice and Bob names and the origins may be related to any story like adaption used to describe a complex process.

In other words, the wider impact of applying the CIA paradigm is that data originating from Alice is assured to have come from Alice (Availability), that is has not been modified since Alice released the data for transmission (Integrity), and that no unauthorised party has been able to access the content of the data (Confidentiality). A number of consequences follow from this including the need to be able to reliably identify Alice and Bob, to have assurance that Eve cannot masquerade as Alice, thus promoting the requirement for identity management, and authentication. If the CIA paradigm is underpinned by cryptographic mechanisms the nature of the key management has an impact on the core architecture of the system as well as on the problem of key binding to any established SA.

## 5.2 CIA and Trust frameworks

In consideration of NGSI-LD API trust is established between the calling entity and the called entity such that end-to-end trust is established. The simplified architecture shown in figure 5.2-1 places a broker entity between the context consumer and each of the context source and context producer although the description in ETSI GS CIM 009 [i.1] allows for a direct relationship between the consumer and source/producer (thus bypassing the role of the broker as trusted intermediary).

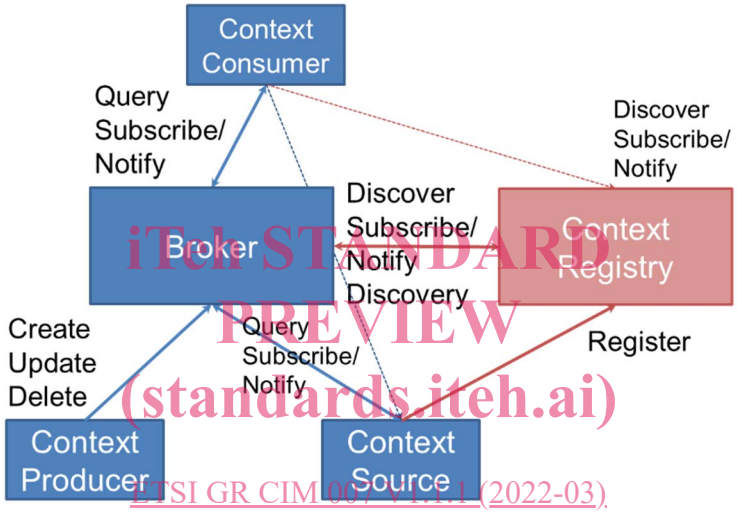




**Figure 5.2-1 NGSI-LD architectural roles**



In the context of figure 5.2-1 the Context Producer and Context Source have to be trusted by the broker but have no direct trust relationship to the Context Consumer. The NGSI-LD API specification does allow for direct connection between the Context Consumer and each of the Context Producer and Context Source. If the same data is retrieved with both the broker involved, and not involved, in the transaction the trust calculation may be different for each path.

## 5.3 Security and privacy constraints for NGSI-LD Systems

It is important to recognize that the constraints listed below apply to the user or provider of data, such as used in an NGSI-LD system. The consequences from a technology perspective are that provisions to allow an implementation to comply to regulation (e.g. data protection) are expected to be made available to users and providers. One purpose of the present document is therefore to assist in the identification of those technical provisions. Of itself a secure variant of NGSI-LD would be insufficient to confer regulatory compliance to mechanisms such as GDPR but may, when deployed, give greater likelihood of an operator being able to claim compliance.

It is also noted that regulation applies to legal entities and not to the technical entities (i.e. if a regulatory breach is discovered it is the legal entity that is held liable and not the technology).

There are a number of constraints placed on the use of data, including those implied by a number of regulatory frameworks, that are likely to apply to any deployment of NGSI-LD into network based systems and this includes the following (this list is indicative and no claim is made for its completeness):

- General Data Protection Regulation (GDPR) defined in [i.3] and equivalent regulations in non-EU markets.
- Network Information Systems directive (NIS) defined in [i.4] and equivalent regulations in non-EU markets.

NOTE: There is, at the time of writing, a development to update and strengthen the NIS Directive [i.14] in order to further improve the resilience and incident response capacities of public and private entities, competent authorities and the EU as a whole in both the field of cybersecurity and critical infrastructure protection.

- The Radio Equipment Directive (RED) defined in [i.5] and equivalent regulations in non-EU markets where radio equipment is used.
- Right to repair legislation may apply to ensure that when equipment is repaired and maintained independently of the original manufacturer and supply chain that data in the equipment maintains protection (this may add new entities into the trust model for NGSI-LD).
- Regional and national regulation concerning the safety of equipment and any consequences relating to data safety.
- Regional and national regulation concerning the disposal of equipment at end of life (see also GDPR) wherein data has to be disposed of.

In addition, in many markets there is a broad requirement to enable lawful access to data and content of networks and specific obligations fall onto operators to ensure that their networks and services are appropriately enabled.

EXAMPLE: The European Treaty 185, "Convention on Cybercrime" [i.6] applies for members of Council of Europe and places obligations on CoE members that are in turn placed on data and service providers to ensure reasonable access to data and other digital domain services to prevent crime conducted in the digital domain.

Where NGSI-LD is implemented in devices the security considerations given in ETSI EN 303 645 [i.7] should be taken into consideration.

In summary NGSI-LD deployments are impacted, but NGSI-LD itself is not requested to ensure and enforce compliance, but just to support it.



## 5.4 Contextualising Security in the scope of an NGSI-LD system



NGSI-LD operates within a wider protocol stack, e.g. in order to allow connectivity of consumer to broker to source NGSI-LD is bound to protocols such as HTTP and MQTT (see ETSI GS CIM 009 [i.1], clauses 6 and 7). Each of HTTP and MQTT have their own security properties. In addition HTTP/MQTT are bound to lower layer connectivity protocols including TCP and UDP over IP, which again have their own security properties. There is a contribution to system security and to system trust, of the entire protocol stack across the networks that connect consumer to broker to source, that should be taken into account in the overall risk management of systems that deploy NGSI-LD.

A conceptual overview of an NGSI-LD system is shown in figure 5.4-1, illustrating the different sources of information that are managed, as well as the security and privacy functionality, which protects it.

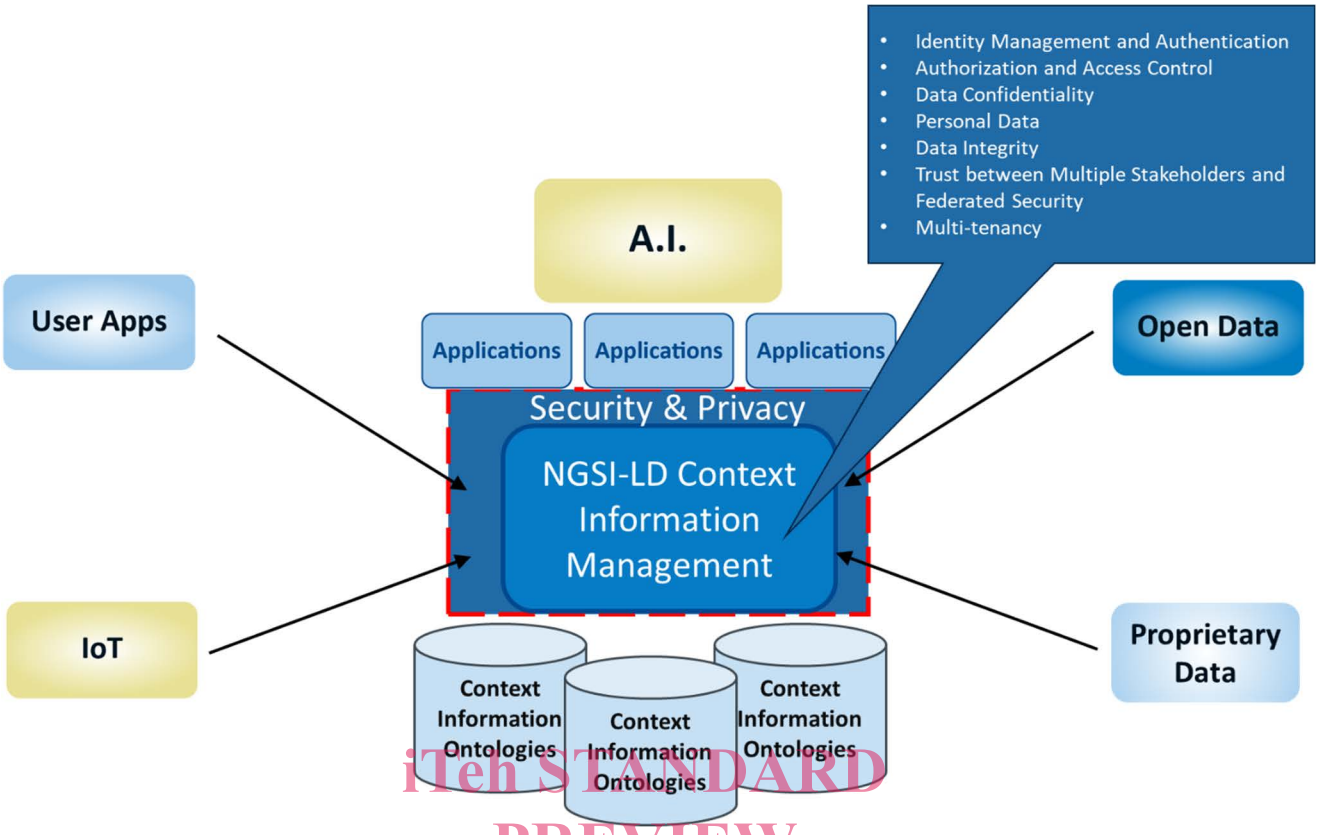


**Figure 5.4-1: Conceptual view of an NGSI-LD System where Security & Privacy functionality is represented**



In the following, security and privacy features, listed below, are investigated with respect to objectives for NGSI-LD Systems:



- Identity Management and Authentication
- Authorization and Access Control
- Data Confidentiality
- Personal Data
- Data Integrity
- Trust between Multiple Stakeholders and Federated Security
- Multi-tenancy

## 5.5 Possible system configurations

The NGSI-LD API [i.1] builds on the NGSI-LD Information Model [i.2]. It does not prescribe all possible architectural configurations that can be built on top of it, but instead introduces architectural roles and three prototypical architectures. The NGSI-LD API is designed in such a way that these prototypical architectures can be supported efficiently, but additional architectures can be envisioned as well.

For the purposes of the present document, the default design decision for a deployment of NGSI-LD is that all the components are fully decentralised and may also be federated. From a security analysis perspective, designing security measures for the most complex of scenarios is appropriate, even if deployment decisions are later made for simpler approaches. The underlying protocol stacks that support connectivity of NGSI-LD, in particular HTTP and MQTT, assume a network interconnection, and the identity structure of NGSI-LD using URIs for identification makes this analysis decision appropriate (i.e. global access and naming is assumed).