ICT-32-2014: Cybersecurity, Trustworthy ICT

WITDOM
"empoWering prIvacy and securiTy in non-trusteD envirOnMents"

Glossary

Last update 2015-08-25

Grant agreement number: 644371
Start date of project: 1 January 2015
Lead contractor: Atos Spain sae (Atos)
Duration: 36 months

Project co-funded by the European Commission within the EU Framework Programme for Research and Innovation HORIZON 2020, and the Swiss State Secretariat for Education, Research and Innovation (SERI)	
Dissemination Level	
PU = Public, fully open, e.g. web	✓
CO = Confidential, restricted under conditions set out in Model Grant Agreement	
CI = Classified, information as referred to in Commission Decision 2001/844/EC.	

Contents

1 Glossary

1.1 *Introduction*

This document comprises a list of acronyms and terms used in the project scope that aim to make the work of WITDOM more understandable by external readers.

The glossary is a live document to be updated with new terms over the project span: from January 2015 to December 2017.

1.2 *Acronyms*

1.2.1 Generic Terms

ACL	Access Control List
ADS	Authenticated Data Structure
ADV	Advertising (e.g., company)
API	Application Program Interface
AS	Authorization Server
BCR	Binding Corporate Rules
CA	Certification authority
CAP	Consistency, Availability, Partition tolerance
CSV	Comma-Separated Values
DHCP	Dynamic Host Configuration Protocol
DIS	Draft International Standard
DSS	Data Security Standard
ERP	Enterprise resource planning
FDIS	Final Draft International Standard
HCI	Human-Computer Interaction
HID	Human Interface Device
HPCA	High-Performance Computer Architecture
HTTP	Hypertext Transfer Protocol
ICT	Information and Communication Technologies
IdP	Identity Provider
IP	Internet Protocol
ISMS	Information Security Management System
IT	Information Technologies
JSON	JavaScript Object Notation
LINDDUN	Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, and Non-compliance
NMOC	Network Manager Operations Centre
OLAP	On-Line Analytical Processing
PKI	Public Key Infrastructure

SDLC	Software Development Life Cycle
SIPOC	Suppliers, Inputs, Process, Outputs, and Customers
SLA	Service-Level Agreement
SLO	Service-Level Objective
SME	Small and Medium Enterprise
SOAP	Simple Object Access Protocol
SOTA	State-Of-The-Art
SPACE	Security and PrivAcy CodEsign
SPbD	Security and Privacy by Design
STRIDE	Spoofing, Tampering, Repudiation, (Information) Disclosure, Denial of Service, and Elevation of Privilege
TRL	Technology Readiness Level
UIP	Untrusted Infrastructure Provider
URL	Uniform Resource Locator
UX	User Experience
XACML	eXtensible Access Control Markup Language
XML	Extensible Markup Language
WSS	Web Services Security

1.2.2 Scenario related terms

BAM	Binary Alignment/Map
CDO	Care Delivery Organization
CDW	Clinical Data Warehouse
DICOM	Digital Imaging and Communications in Medicine
DNA	Deoxyribonucleic acid
E2E	End-to-end
EGR	Electronic Genetic Record
EHR	Electronic Health Record
EMR	Electronic Medical Record
FS	Financial Services
FSWG	Financial Services Working Group
GbSP	Genetic-based Service Provider
GDPR	General Data Protection Regulation
GSVML	Genomic Sequence Variation Markup Language
HIPAA	Health Insurance Portability and Accountability Act
HL7	Health Level 7
HLR	High Level requirement
IFRS	International Financial Reporting Standards
IFX	Interactive Financial Exchange
LOINC	Logical Observation Identifiers Names and Codes
NGS	Next-Generation Sequencing

OFX	Open Financial Exchange
PHI	Personal Health Information
PA	Payment Application
SAM	Sequence Alignment/Map
SNP	Single Nucleotide Polymorphism
VCF	Variant Call Format

1.2.3 Privacy

DP	Data Protection
DPD	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
DPR	Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM(2012)0011 final – 25/01/2012
ECHR	European Convention for the Protection of Human Rights and Fundamental Freedoms
ECtHR	European Court of Human Rights
GDPR	General Data Protection Regulation
PbD	Privacy by Design
PDP	Provable Data Possession
PET	Privacy-enhancing Technology
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PLAO	Privacy Level Agreement Outline
PoR	Proof of Retrievability
PoW	Proof of Ownership
UDHR	Universal Declaration of Human Rights

1.2.4 Cryptography

FHE	Fully homomorphic encryption
HE	Homomorphic Encryption
KVS	Key-value store
PCP	Probabilistically checkable proof
PECKS	Public Key Encryption with Conjunctive Keyword Search
PEKS	Public Key Encryption with Keyword Search
PERKS	Public-key Encryption with Registered Keyword Search
TPM	Trusted Platform Module
SHE	Somewhat homomorphic encryption

VC	Verifiable computation
ZK	Zero-Knowledge
ZKP	Zero-knowledge proof

1.2.5 Cloud

CBS	Cloud Brokerage Service
CCM	Cloud Controls Matrix
CCSM	Cloud Certification Schemes Metaframework
COS	Cloud Object Store
CSP	Cloud Service Provider
DbaaS	Database as a service
IaaS	Infrastructure as a Service
IPOP	IP over P2P
JWE	JSON Web Encryption
JWT	JSON Web Token
P2P	Peer-to-peer
PaaS	Platform as a Service
SaaS	Software as a Service
SDN	Software Defined Network
SDS	Software Defined Storage
VEP	Virtual Execution Platform
XaaS	Anything as a Service

1.2.6 Organizations, projects and initiatives

ATOS	Atos Spain sae
BBVA	Banco Bilbao Vizcaya Argentaria
CEN	European Committee for Standardization
CIGTR	Center for the Technological Management of Risk
CIRRUS	Certification,InteRnationalisation and standaRdization in cloUd Security
CONTRAIL	pen Computing infrastructures for elastic services
CSA	Cloud Security Alliance
CSIG	Cloud Selected Industry Group
ENISA	European Union Agency for Network and Information Security
ETP	European Technology Platform
ETSI	European Telecommunications Standards Institute
FCSR	Fondazione Centro San Raffaele
HEAT	Homomorphic Encryption Applications and Technology
IBM	IBM Research Gmbh
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers

IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
JTC	Joint Technical Committee
KU Leuven	Katholieke Universiteit Leuven
mOSAIC	Open-Source API and Platform for Multiple Clouds
NESSI	Networked European Software and Services Initiative
NIS	Network Information Service
NIST	National Institute of Standards and Technology
OASIS	Organization for the Advancement of Structured Information Standards
OECD	Organisation for Economic Co-operation and Development
PRACTICE	Privacy-preserving computation in the Cloud
PRIPARE	PReparing Industry to Privacy-by-design by supporting its Application in REsearch
PRISMACLOUD	PRIvacy and Security MAintaining Services in the CLOUD
SC	Standardisation Subcommittee
SERI	State Secretariat for Education, Research and Innovation
SPECS	Secure Provisioning of Cloud Services based on SLA Management
SPEED	Signal Processing in the EncryptEd Domain
TC	Technical Committee
TCLOUDS	Trustworthy Clouds Privacy and Resilience for Internet-scale Critical Infrastructure
TREDISEC	Trust-aware, REliable and Distributed Information SEcurity in the Cloud
TRESCCA	TRustworthy Embedded Systems for Secure Cloud Computing Applications
UVIGO	Universidad de Vigo
W3C	World Wide Web Consortium
WITDOM	empoWering prIvacy and securiTy in non-trusteD envirOnMents
XLAB	XLAB razvoj programske opreme in svetovanje d.o.o

1.2.7 Generic terms of the project

DoA	Description of Actions
Dx.y	Deliverable number y corresponding to WP x
EB	Executive Board
EC	European Commission
IPR	Intellectual Property Right
KPI	Key Performance Indicator
MSx	Milestone number x
Mx	Month x
PAB	Project Advisory Board
R&D	Research and Development
Tx.y	Task number y related to WP x
QoS	Quality of Service

WD	Working Draft
WG	Working Group
WP	Working Package

1.3 *Terms*

1.3.1 Generic WITDOM Terms

- **Architecture** – in the context of WITDOM, architectures can be defined as "the fundamental organization of a system, embodied in its components, their relationships (including data flows) to each other and the environment, and the principles governing its design and evolution"
- **End-to-end security** – approach to security where data travelling between clients and servers' end-points are uninterruptedly protected, even where untrusted intermediaries entities or communication channels are required.
- **End-user environment** – environment in which the end user interactions with the system occur. It includes specific devices, software and user interfaces directly available to the people that will actually use the system.
- **Enforcement mechanism** – in the IT context, enforcement mechanisms are technical measures which guarantee that the execution and/or the outputs of a given system comply with some specific pre-established (security or privacy) policy.
- **Evaluation methodology** – technical activities performed to quantify de degree of compliance of a system (component or algorithm) with respect to a specific set of requirements.
- **Framework (privacy and security framework)** – system abstraction in which tools and algorithms can be instantiated in order to provide privacy and security guarantees.
- **ICT (Information and Communications Technology)** – according to ISO "ICT includes the specification, design and development, integration and interoperability of systems, tools and applications dealing with the capture, representation, accessibility, processing, security, transfer, interchange, presentation, management, organization, storage and retrieval of information, and their related cultural, linguistic adaptability and societal aspects".**Error! Reference source not found.**
- **Non-trusted/Uncontrolled environment** – as opposed to trusted or controlled ones, non-trusted environments are platforms on which the execution of some specific task cannot be relied. The platform cannot ensure neither the integrity nor the confidentiality during the execution of such task.
- **Outsourced environments** – within WIDOM's context, it refers to an arrangement by which the storage of some data and the execution of some computing tasks that would otherwise be performed in computing platforms internal to the organization, is transferred to an external entity specialized in the delivery of such tasks.
- **Platform** – A platform is a group of technologies that are used as a base upon which other software is run. It typically includes hardware architecture, an Operative System and runtime libraries.
- **Primitives or building blocks** – in the system engineering domain, primitives are the basic elements (entities, segments of code, classes…) that can be combined to build more sophisticated ones. In the cryptographic context, they are low-level cryptographic algorithms that can be combined to build more complex cryptographic protocols.
- **Prototype (vs Pilot)** – while both approaches are intended to test and verify a system, a pilot generally intends to test the full production system against a specific subset of the end users while the prototype may be focused on validating and learning from specific system aspects, implying that the prototype may not be part of the production-version of the system.

- **Quality requirements or non-functional requirements** – Complementary to functional requirements, which describes what a system is supposed to do, non-functional requirements describe "how a system is supposed to be". Non-functional requirements share with functional requirements the characteristics for good requirements (unitary, complete, consistent...).
- **Scenarios** – for WITDOM, these are pictures that illustrate and describe a future system, capturing its view from the outside. Scenarios are more abstract than use cases which are useful in discussing a proposed system with a customer.
- **Security requirements** – OWASP defines security requirements in its quick reference guide as "a set of design and functional requirements that help ensure the software is built and deployed in a secure manner". **Error! Reference source not found.**
- **Solution (vs Product)** – within the IT domain, the main difference of a solution and a product is that the solution usually must be tailored to address some customer' specific needs while the product can be used "as-is", with just minor parametrizations.
- **Technical requirements** – (WP3) are all of the requirements at the system level that describe the functions which the system as a whole should fulfill to satisfy the stakeholder needs and requirements, and are expressed in an appropriate combination of textual statements, views, and non-functional requirements; the latter expressing the levels of safety, security, reliability, etc., that will be necessary. **Error! Reference source not found.**
- **Toolkit** – in the context of software development, a toolkit is a set of software common development tools, including, sample code, technical notes and other documentation that allows the creation of applications for a certain platform.
- **Toolset** – in WITDOM's context, a toolset is a set of libraries which must be used in a specific way by the client code.
- **Usability** – "The extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use."
- **User empowerment** – providing users with the means to alter aspects of the services they are consuming, In the context of data protection it implies allowing data subjects to control their own data (delete, modify or access it) and who and with what purposes they can access it.
- **Validation framework and protocols** – following the platform definition, a validation framework is a conceptual structure, methods and tools intended to serve as a support or guide for checking the compliance of a system with respect to a set of requirements. A validation protocol is a predefined written procedural method that will ensure a successful replication of the validation process by other validation teams.

1.3.2 Scenario related terms

- **Anonymization:** The data subject is not identifiable by all the means likely reasonably to be used either by the controller or by any other person to identify the said person.[1]

[1] From the article 29 WP: The criterion of *"all the means likely reasonably to be used either by the controller or by any other person*" should in particular take into account all the factors at stake. The cost of conducting identification is one factor, but not the only one. The intended purpose, the way the processing is structured, the advantage expected by the controller, the interests at stake for the individuals, as well as the risk of organisational dysfunctions (e.g., breaches of confidentiality duties) and technical failures should all be taken into account. On the other hand, this test is a dynamic one and should consider the state of the art in technology at the time of the processing and the possibilities for development during the period for which the data will be processed. Identification may not be possible today with all the means likely reasonably to be used today. If the data are intended to be stored for one month, identification may not be anticipated to be possible during the "lifetime" of the information, and they should not be considered as personal data.

- **Business analytics:** skills, technologies and practices of iterative, methodical exploration and investigation of past business performance and of organization's data with emphasis on statistical analysis.
- **Data warehouse:** a collection of data within an organization primarily used for reporting and analysis to support management decision-making. A Data Warehouse often contains time-varying data integrated from different information sources. The data are usually structured, organized and accessible for business users by applying tools like online analytical processing (OLAP) or Data Mining.
- **Data mart:** a repository of data that is designed to serve a particular community of knowledge workers and usually oriented to a specific business line or team. Generally, an organization's data marts are subsets of the organization's data warehouse.
- **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 processing:** Any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.
- **Data processor:** Natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.
- **Data subject:** The person about whom data is collected.
- **Data subject's consent:** Any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to the processing of personal data relating to him/her.
- **Demographic information:** The term demographic refers to particular characteristics of a population. Examples of demographic characteristics include age, race, gender, level income, education, home ownership, etc.
- **Electronic Genomic Record (EGR):** All the information relative to the genetic analysis of an individual, including the raw data leading to the retrieval of such information.
- **Electronic Health Record (EHR):** a document maintained by each CDO the patient deals with (ANSI, 2003).
- **Electronic Medical Record (EMR):** legal record created, used, and maintained by the CDO with the aim of documenting, monitoring, and managing a health care delivery within the CDO.
- **Feared Event:** an event against which the system must be protected.
- **Financial portfolio:** grouping of financial assets such as stocks, bonds and cash equivalents, as well as their mutual, exchange-traded and closed-fund counterparts. Portfolios are held directly by investors and/or managed by financial professionals.
- **Fraud scoring: determination** of the level or risk associated to a transaction. It may provide either a pass/fail response or a quantitative score reflecting the transaction's risk.
- **Functional requirements:** a functionality or service that the system has to offer to a third party.

However, if they are intended to be kept for 10 years, the controller should consider the possibility of identification that may occur also in the ninth year of their lifetime, and which may make them personal data at that moment.

- **Health data**: Information relating to an identified or identifiable natural person and concerning this person's health. "Concerning health" means all personal data which have "a strong and clear link" with the description of the health status of a person, including genetic data. Data that only reveal a health status such as a holiday picture of a person with a broken leg is currently not included in this category.
- **Loan-to-value:** financial term used by banks and other institutions to represent the ration between the amount of money borrowed and the appraised value of real properties used as loan liens.
- **Metadata:** Data holding information about data.
- **Non-functional requirements:** a desired quality/feature of the system (e.g., accessibility, availability, maintainability, etc.).
- **Personal Data:** Any information relating to an identified or identifiable natural person, the 'data subject', an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity; this term covers both objective information, but also subjective information such as opinions or assessments.
- **Personally Identifiable Information (PII):** Used in US privacy law: it refers to any information about an individual maintained by an agency, including (1) both any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. It can be both sensitive or non-sensitive.
- **Personal Health Information (PHI):** Used in US HIPAA, it refers to any information in the medical record or designated record set that can be used to identify an individual and that was created, used, or disclosed in the course of providing a health care service such as diagnosis or treatment. PHI concerns only data associated with or derived from a healthcare service event (treatment, payment, operations, medical records).
- **Privacy:** the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. (Westin, 1967)
- **Privacy policy:** the declaration of an overall intention and direction, rules and commitment, as formally expressed by the data controller related to the processing of personal data in a particular setting.
- **Pseudonymization:** Pseudonymization is the process of disguising identities. The aim of such a process is to be able to collect additional data relating to the same individual without having to know his identity. This is particularly relevant in the context of research and statistics.

  Pseudonymization can be done in a retraceable way by using correspondence lists for identities and their pseudonyms or by using two-way cryptography algorithms for pseudonymization. Disguising identities can also be done in a way that no re-identification is possible, e.g. by one-way cryptography, which creates in general anonymized data.
- **Credit risk scoring:** determination of a derived numeric expression of the level or risk associated to a customer or a credit operation. It predicts whether or not a credit extended to an applicant will likely result in profit or losses for the lending institution. A credit score is based on, among other things, a person's past credit history
- **Scenario:** narrative description about the interaction activities between a user and a service in a specific environmental situation.
- **Security:** the degree of protection of an asset.

- **Sensitive data:** Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.
- **Service Level Agreements:** An agreement that sets the expectations between the service provider and the customer and describes the products or services to be delivered, the single point of contact for end-user problems and the metrics by which the effectiveness of the process is monitored and approved.
- **Service Level Objectives:** Within service-level agreements (SLAs), SLOs are the objectives that must be achieved — for each service activity, function and process — to provide the best opportunity for service recipient success.
- **Stakeholder (of a system):** an entity that can affect or is affected by the services offered by a system.
- **Third party:** Any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data.
- **Threat:** The possibility that an entity (called "attacker") exploits a vulnerability of the system.
- **Untrusted environment:** environments where a stakeholder cannot directly control or fully verify the underlying hardware, software or people accessing it, being vulnerable to malicious attacks. Examples of such environments are the Internet or public clouds.
- **Use-case:** list of steps that defines the interaction between the user and a service in order to achieve a goal.

1.3.3 Privacy-preserving technologies related terms

- **Adversarial capabilities** – collection of actions (e.g., observations, computations, storage) that represent the assumed power of the adversary at the time of deploying an attack.
- **Adversary** - entity that deploys attacks according to her adversarial capabilities with the goal of compromising a system and gain privileged access to sensitive information.
- **Anonymity** - Anonymity is the state of being not identifiable within a set of subjects, the anonymity set. The anonymity set is the set of all possible subjects who might cause an action.
- **Anonymous communication network** - network capable of hiding the relationships of communicating partner with respect to an adversary observing the communications.
- **Differential privacy** - Informally, the concept of differential privacy in a dataset states that any possible outcome of an analysis should be "almost" equally likely for two datasets that differ in just one element. Hence, the performed statistical analyses will not disclose significant information about one individual of the dataset
- **Inference attack** - attack that allows the adversary to deduce the value of an attribute from the value of other attributes.
- **PET (Privacy Enhancing Technologies)** - set of ICT measures protecting informational privacy by eliminating or minimising personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system.
- **Privacy metric** – means of quantification of the level of privacy achieved by one or more mechanisms with respect to a given privacy property.

- **Privacy model** – formalization, in technical terms, of the privacy protection that a system should provide
- **Privacy preference** – statement expressing users' expectation of the degree of a privacy offered by a system.
- **Privacy-and-security-by-design (PSbD) architecture** – system architecture that implicitly provides privacy and security protection.
- **Privacy-preserving and security toolset** – In WITDOM context, set of libraries comprising privacy-preserving building blocks, privacy and anonymity tools and cryptographic primitives designed for protecting data in distributed or outsourced environments.
- **Privacy-preserving building block/primitive** – Algorithms, protocols and techniques that can be applied to enhancing the privacy of the to-be-protected signals and data, by concealing them from adversaries.
- **Privacy-utility tradeoff** - balance between the level of privacy achievable on a system and its subsequent loss of utility.
- **Pseudoidentifier** – attribute which identifies an individual when it is combined with other attributes.
- **Pseudonymity** - Pseudonymity is the use of pseudonyms as Ids. A digital pseudonym is a bit string which is unique as ID and which can be used to authenticate the holder.
- **Trust model** –assumptions on the confidence a stakeholder in other stakeholders in the systems to preserve the privacy of sensitive data.
- **Unique identifier** - attribute which univocally identifies an individual within a dataset.
- **Unlinkability** - property that guarantees that two or more attributes regarding the same individual are no more no less related than they are given a priori knowledge.
- **Unobservability** - Unobservability is the state of items of interest being indistinguishable from any item of interest at all (e.g., sender unobservability means that it is not noticeable whether any sender within a set sends a message)

1.3.4 Cryptographic terms

- **Authenticated Data Structures (ADSs)** – is a model for verifying operations and their results over data outsourced to untrusted sources.
- **Availability** – is a distributed system property. It is the proportion of the total time during which a system is capable to respond to requests. Systems with high availability systems typically achieve values of 0.99999 (or "Five Nines").
- **Byzantine service** – is a service which normally follows the specification but may deviate arbitrary from the specification. In other words, a service which is potentially faulty or malicious.
- **Consistency, Availability, Partition tolerance (CAP) theorem** – dictates that it is impossible to achieve all three properties in a distributed system. That means, in order to achieve availability and partition tolerance, one has to give up consistency.
- **Certification authority (CA)** – is a trusted third-party entity in a public-key infrastructure (PKI) that issues digital certificates and certifies the identity of the public-key owner.
- **Consistency** – is a property that defines the order and visibility of events and resulting state in a distributed system, such as distributed data stores.
- **Cryptographic protocol** – is a protocol to achieve a specific security objective by defining operations of cryptographic primitives. Applications of cryptographic protocols are, for example, key exchange, secret sharing and authentication.

- **Data confidentiality** – comprises data privacy as well as exposing information to unprivileged entities and may established by using cryptographic encryption schemes. Preservation of confidentiality of outsourced data is one of the key aspects of cloud security.
- **Data integrity** – refers to the correctness of data outsourced to an untrusted environment. Enforcing data integrity means to preserve consistency and accuracy of data by preventing or indicating unauthorized altering or accidental data corruption. Preservation of data integrity is one of the key aspects of cloud security.
- **Digest** – is also called cryptographic hash value that is the output value of a cryptographic hash function for a given input data. It is used for data integrity verification.
- **Digital signature scheme** – consists of three algorithms. First, a key generation algorithm that generates a private key and the corresponding public key. Second, a signing algorithm that creates a signature for a message using a private key. And last, a signature verifying algorithm that verifies the signature for a message using a public key. Without knowledge of the private key, it is not possible to generate signatures that successfully pass the verification algorithm.
- **Fork-linearizability** – is a consistency model which guarantees that the events seen by every client of a remote service are linearizable and if the server causes the views of two clients to diverge, they may never again see common events without exposing the server as being faulty.
- **Hash chain** – is a successive invocation of a cryptographic hash function. That is, the hash function is multiple times invoked on the output hash value of the previous invocation.
- **(Cryptographic) hash functions** – map arbitrary input data to a short, unique hash value. Cryptographic hash functions are one-way functions, that is, it is infeasible to compute the input data from its hash value.
- **Homomorphic Encryption (HE, FHE, SHE)** – malleable encryption that allows for certain operations on encrypted data without decrypting them, thanks to a group (or ring) homomorphism between the plaintext and the ciphertext. Typically, additive homomorphic encryption (only encrypted additions) is used due to the current inefficiency of Fully Homomorphic Encryption (FHE), which allows for any encrypted operation. Somewhat Homomorphic Encryption (SHE) is an efficient relaxation of FHE that allows for the execution of limited depth circuits under encryption.
- **Key-value store (KVS)** – is a storage system providing the abstraction of an associative array that allows storage and retrieval of values associated with unique keys. The KVS model is often used to abstract real-world cloud storage services such as Amazon S3 or Openstack Swift.
- **Linearizability** – is a consistency model that guarantees that at every client all events appear in the same order and preserve the global real-time ordering.
- **Probabilistically checkable proofs (PCPs)** – are complexity-theoretic tools that allow a client to verify that the results of a computation, or the solution of a problem, is correct. Their key feature lies in efficiency, they use a randomized verification algorithm that accesses only a part of a (very long) proof.
- **(Cryptographic) protocol** – structured procedure which makes use of one or several cryptographic primitives to comply with a security-related function. It may involve several parties, specifying the interchanged messages (interactive protocol).
- **Public key Encryption with Keyword Search (PEKS)** – cryptographic mechanism that enables to test for the presence of a determined term (keyword) in an encrypted message.

- **Public key Encryption with Registered Keywork Search (PERKS)** – Variant of PEKS in which the sender must register the keyword with a receiver before using it, hence avoiding offline keyword guessing attacks.
- **Remote computation** – is the offloading of a computation task to another or multiple remote hosts. That is, a computationally client sends and invocation to the remote host and receives the computation result as a response.
- **Trusted Platform Module (TPM)** – is a secure co-processor found on modern computers that provides limited cryptographic operations and key storage. It permits to bootstrap a secure and verified computation infrastructure by informing a remote entity in cryptographically secure way about the actual hardware and software configuration of its host computer system.
- **Secure Processing** – Discipline that applies cryptographic protocols and primitives to protect and conceal data while it is processed. In the scope of processing of sensitive signals, it is usually denoted Secure Signal Processing or Signal Processing in the Encrypted Domain.
- **Secure Storage** – Set of strategies, hardware and software components and cryptographic primitives to protect data when it is neither in transit nor being processed.
- **Verifiable computation (VC)** – enables a client to verify the response of a remote computation with respect to a known program and known inputs.
- **Vector clock** – is a data structure that establishes a partial ordering of events in a distributed system and can serve to detect concurrent events.
- **Wait-free** – is a distributed algorithm property which guarantees that all entities in the system may progress independently of each other. That is, no entity needs to wait for another one to proceed.
- **Weak fork-linearizability** – is a consistency model that guarantees fork-linearizability but relaxes the guarantees for the last event at every client.
- **ZKPs - Zero-knowledge proofs** – Protocols that allow, through interaction, to prove the validity of a statement without disclosing any additional knowledge (zero-knowledge) besides that directly derived from the proven statement.

1.3.5 Cloud related terms

- **Access Control** – selective restrictions of access put in place in order to access (web) resources.
- **Authorization Server (AS)** – web service within a authorization framework which checks validity of authorization tokens. The server issuing access tokens to the client after successfully authenticating the resource owner and obtaining authorization.
- **Business flow** – a sequence of steps/flows between flow objects (events, activities, gateways) in a work flow.
- **Certificate Agency (CA) Service** – Certificate Authority, issues digital certificates. These certify ownerships of public keys of services or users and are used to identify these. Within a Public Key Infrastructure model of trust relationships, it is a trusted third party, trusted by both, the subject (owner) of the certificate and the party relying uppon the certificate.
- **Certificate Revocation** – a process of revoking (deleting) a certificate from the chain of trust (from the CA)
- **Cloud Adaptation Layer** – a layer between IaaS and services that enables existing non-cloud enabled services to utilize cloud services and resources.

- **Cloud API** – an Application Programming Interface towards cloud resources of IaaS or PaaS. Usually implemented as RESTful service utilizing HTTP methods to perform certain methods on the cloud infrastructure.
- **Cloud Brokerage Service (CBS)** – a model in which a company or other entity adds value to one or more (public or private) cloud services on behalf of one or more consumers of that service via three primary roles including aggregation, integration and customization brokerage.
- **Cloud deployment** – a process of deploying cloud service on physical or virtual infrastructure.
- **Cloud extensions** – a set of tools (libraries, services) enabling an existing cloud services to perform an extended action
- **Cloud Federation** – interconnected cloud environments (solutions) that are seen by the users as a single entity. Cloud mechanisms are abstracted from the user who seamlessly uses different cloud providers as these would be one entity.
- **Cloud infrastructures** – resources (physical or virtual) used to provide cloud services to the users.
- **Cloud Service Provider (CSP) –** an entity providing cloud services
- **ConPaaS** – Contrail PaaS, it is an open source Platform-as-a-service solution developed within Contrail project (http://contrail-project.eu/). Contrail was a Cloud Federation computing project that ran from 2010-10-01 until 2014-01-31.
- **ConSec –** Contrail Security framework is a framework developed within Contrail project. It comprises OAuth2 implementation with dynamic CA services. These can directly be used within elastic PaaS services. It also provides Identity Provider solution enabling different cloud platforms to use the same authentication mechanisms.
- **Cloud Object Store (COS)** – Cloud based storage that manages discrete units of storage. Abstracts some of the lower layers of storage away from administrators and applications.
- **Database as a service (DbaaS)** – database managed by cloud provider. Application owners do not have to install and maintain database on their own.
- **Federated Identity Management** – arrangement made between multiple enterprises that lets users use same identification data to obtain access to networks of all enterprises in the group.
- **Identity Provider (IdP) / External Identity Provider** – a system that creates, maintains and manages identity information for principals (users, services, or systems) and provides principal authentication to other service providers (applications) within a federation or distributed network.
- **Infrastructure as a Service (IaaS)** – service that provides physical or virtual machines and other resources.
- **IPOP (IP over P2P) Protocol** – software virtual network allowing end users to create their own virtual private networks (VPNs). Packets are transferred from source directly to destination over public network without intermediate server.
- **JSON Web Token (JWT)** – compact URL-safe means of representing claims to be transferred between two parties. Claims are encoded as JavaScript Object Notation (JSON) object that is used as the payload of a JSON Web Signature (JWS) structure or as the plaintext of a JSON Web Encryption (JWE) structure, enabling the claims to be digitally signed or MACed and/or encrypted.

- **NoSQL Database** – provides a mechanism for storage and retrieval of data that is modeled in means other than the tabular relations used in relational databases. Motivations for this approach include simplicity of design, horizontal scaling and finer control over availability.
- **OAuth2** – provides client applications a secure delegated access to server resources on behalf of a resource owner. It specifies a process for resource owners to authorize third-party access to their server resources without sharing their credentials.
- **OpenID** – decentralized protocol that allows users to be authenticated by certain cooperating websites using a third party service thus eliminating the need for users to register on every website.
- **Peer-to-peer (P2P)** – distributed application architecture in which peers communicate directly with each other.
- **Platform as a Service (PaaS)** – service that provides a platform allowing customers to develop, run and manage applications without complexity of building and maintaining the infrastructure.
- **POSIX File System** – part of POSIX specification that defines requirements for file systems. It mandates things like hierarchical file names, permissions and multi-user protection.
- **Runtime Environment** – contains state values that are accessible during program execution, as well as active entities (like environment variables) that can be interacted with during program execution.
- **Software Defined Network (SDN)** – an approach to networking in which control is decoupled from the physical infrastructure, allowing network administrators to support a network fabric across multi-vendor equipment.
- **Software Defined Storage (SDS)** – an approach to data storage in which the programming that controls storage-related tasks is decoupled from the physical storage hardware. Software that enables a software-defined storage environment can provide functionality such as deduplication, replication, thin provisioning, snapshots and backup.
- **Security Vulnerability Assessment (SVA)** – an inspection process that determines vulnerabilities of inspected entity. The aim of SVA is to assess the size of attack surface and try to minimize it.
- **Service Level Agreement (SLA)** – contract between service provider and customer that defines the guaranteed level of service performance.
- **Service-oriented Architecture (SoA)** – a design pattern in which application components provide services to other components via a communications protocol, typically over a network. The principles of service-orientation are independent of any vendor, product or technology. Service is a self-contained unit of functionality.
- **Software as a Service (SaaS)** – users are provided access to application software. Cloud providers manage infrastructure and platforms that run the applications.
- **Virtual Execution Platform (VEP)** – a cloud middleware software that interfaces multiple Infrastructure as a Service (IaaS) clouds and presents end-users with an interface facilitating ease of deployment and application life cycle management of distributed applications made up of several inter-networked virtual machines.
- **Virtual Private Networking** – extends private network across a public network. Computers send and receive data across public network as if it were directly connected to private network.
- **X509 Certificate** – uses X.509 public key infrastructure (PKI) standard to verify that a public key belongs to the user, computer or service identity contained within the certificate.

- **eXtensible Access Control Markup Language (XACML)** – a declarative access control policy language implemented in XML and a processing model describing how to evaluate access requests according to the rules defined in policies.
- **XtreemFS** – an object-based, distributed file system for wide area networks. It is fault tolerant and maintains POSIX file system semantics.