Cloud Standards for Trusted Public Clouds for Government

Cloud computing is an attractive business model for public bodies which are under pressure to drastically reduce their budgets. Cloud services enable public administrations not only to reduce costs, but also to implement more efficient services. This includes new citizen services as part of the digital transformation. Benefits include: improved accessibility to applications and data from remote locations and multiple devices, extra scalability, elasticity to deal with peak workloads, and resilience and security.

Characteristics of a Trusted Public Clouds for Government

Most important characteristics
» Advanced Security
» Measured Service
» Resource Pooling

Least important characteristics
» On demand self-service
» Virtualisation
» Massive scale

Which standards?

Standards are crucial for enabling interoperability and secure, trusted clouds. This can increase confidence and uptake of cloud services. Standards are also one of the most important means to bring new technologies to market.

Standards for Advanced Security.

» **ISO/IEC 27000 family**. Often called ISO 27k, this family of specifications defines general-purpose security related vocabulary and controls for information security management systems (ISMS). Of particular interest is ISO/IEC 27018 "Code of practice for data protection controls for public cloud computing services" (e.g. for STORM CLOUD in particular).

» **NIST Special Publication 800-53**. SP 800-53 is a collection of "Security and Privacy Controls for Federal Information Systems and Organizations". While the title clearly indicates its scope towards US federal government, it also applies to other public administration and governmental IT systems since it provides a comprehensive list of controls and procedures of which a subset may be selected for implementation by Texel, GEMMA, and STORM CLOUD in particular.

» **CSA CCM 3.01**. Similarly, the Cloud Security Alliance (CSA) Cloud Control Matrix (CCM) provides a comprehensive list of more than 130 controls for advanced security measures. The CCM maps controls to cloud architecture subsystems, cloud service models, and most importantly, already existing other international security controls such as the two referenced above.

CloudWatch

Smart cloud services for innovation,
savings & sustainability

Standards for a measured service.

» **Usage Record 2**. The Usage Record specification from the Open Grid Forum defines a comprehensive list of resources and their metrication means. It is extensively used in large worldwide scientific collaborations such as the European Grid Infrastructure (EGI), the Worldwide LHC Computing Grid (WLCG) which also uses resources of EGI, the Open Science Grid (OSG), and XSEDE in the US.

» **NIST Special Publication 500-307**. SP 500-307 defines a model for the development and definition of Cloud service metrics for a number of well-defined use cases. SP 500-307 classifies metrics following three typical service lifecycle phases: Service Selection, Service Agreement, and Service Measurement. Many more measurement scenarios exist, but are out of scope of NIST SP 500-703, or do not follow its metric modelling framework.

» **DMTF Cloud infrastructure Management Interface (CIMI) Model and RESTful HTTP-based Protocol**. The CIMI specification defines a number of metrics for cloud services implementing the IaaS model using the CIMI management interface. It is bound to the underpinning DMTF Common Information Model (CIM) specification.

» **AMQP (Advanced Message Queuing Protocol)**. AMQP 1.0 is an OASIS standard since 2012, and approved by the International Standards Organisation (ISO) as ISO/IEC 19464. It provides reliable messaging (from fire-and-forget, to exactly once delivery), cross-platform portable data representation, flexible deployments (peer-to-peer, client-broker, broker-broker networks) and is entirely broker-independent (i.e. allowing heterogeneous and inter-provider deployments). It has a strong industry backing including two major Cloud service providers (Microsoft, VMWare). Even though AMQP does not define any metrics by itself and therefore can be argued as not applicable in this section, it is described nonetheless in this context, since at least two of the three fundamental metric scopes defined in NIST SP 500-307 require a metric measurement delivery model (i.e. Service Agreement and Service Measurement) – we consider measurement infrastructures as enabling technology to deliver cloud services regardless the service delivery model (IaaS, PaaS, SaaS).

Resource Pooling

This is considered a non-functional cloud characteristic, and as such an internal function of a cloud service not requiring interoperability across providers or in a consumer/provider relationship.

Connect with CloudWATCH

www.cloudwatchhub.eu | info@cloudwatchhub.eu
Follow us on twitter @CloudWatchHub

CloudWatch

A European Cloud observatory supporting cloud policies, standards profiles & services