

How to negotiate a proper SLA?



CSA Cloud Bytes



Dr. Jesus Luna

Research Director, EMEA,
Cloud Security Alliance



Frédéric Engel

CEO of Market Engel SAS
SAS



Daniele Catteddu

Managing Director, EMEA,
Cloud Security Alliance





Arthur van der Wees

Managing Director of
international law firm
Arthur's Legal



Dr. Said Tabet

Senior Technologist and
Industry Standards Strategist,
Strategist, Corporate Office of
Office of the CTO, EMC
Corporation



AGENDA

Introduction - Jesus Luna 5'

The SME perspective - Frédéric 10'

Cloud security challenges - Daniele 10'

The legal aspects - Arthur 10'

Standardization landscape - Said 10'

Open discussion





Dr. Jesus Luna

Research Director, EMEA,
Cloud Security Alliance



Introduction

- A cloud SLA is a **documented agreement** between the cloud service provider (CSP) and cloud service customer that **identifies services and associated quality levels** (i.e., cloud service level objectives or SLOs).
- **Security specification** in Cloud SLAs (**secSLAs**) aims to provide useful/measurable (security) information to Customers, beyond what we can find on applicable certifications.
- Despite their advocated advantages, most Cloud SLAs/secSLAs are offered on a **“take it, or leave it”** manner.



Negotiating a “good enough” SLA/secSLA

- Why is this important for SMEs?
- Which are the legal implications?
- Why SMEs would like to negotiate security levels?
- The standardization perspective





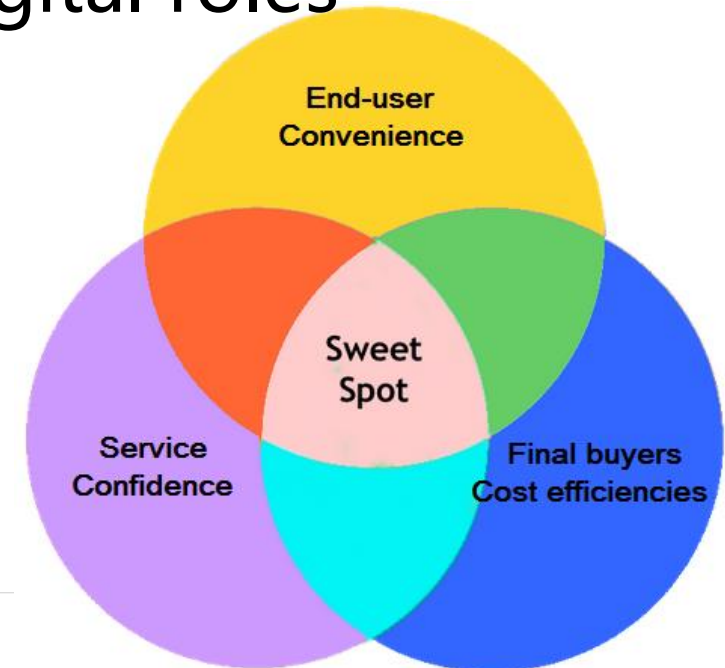
Frédéric Engel

CEO of Market Engel SAS

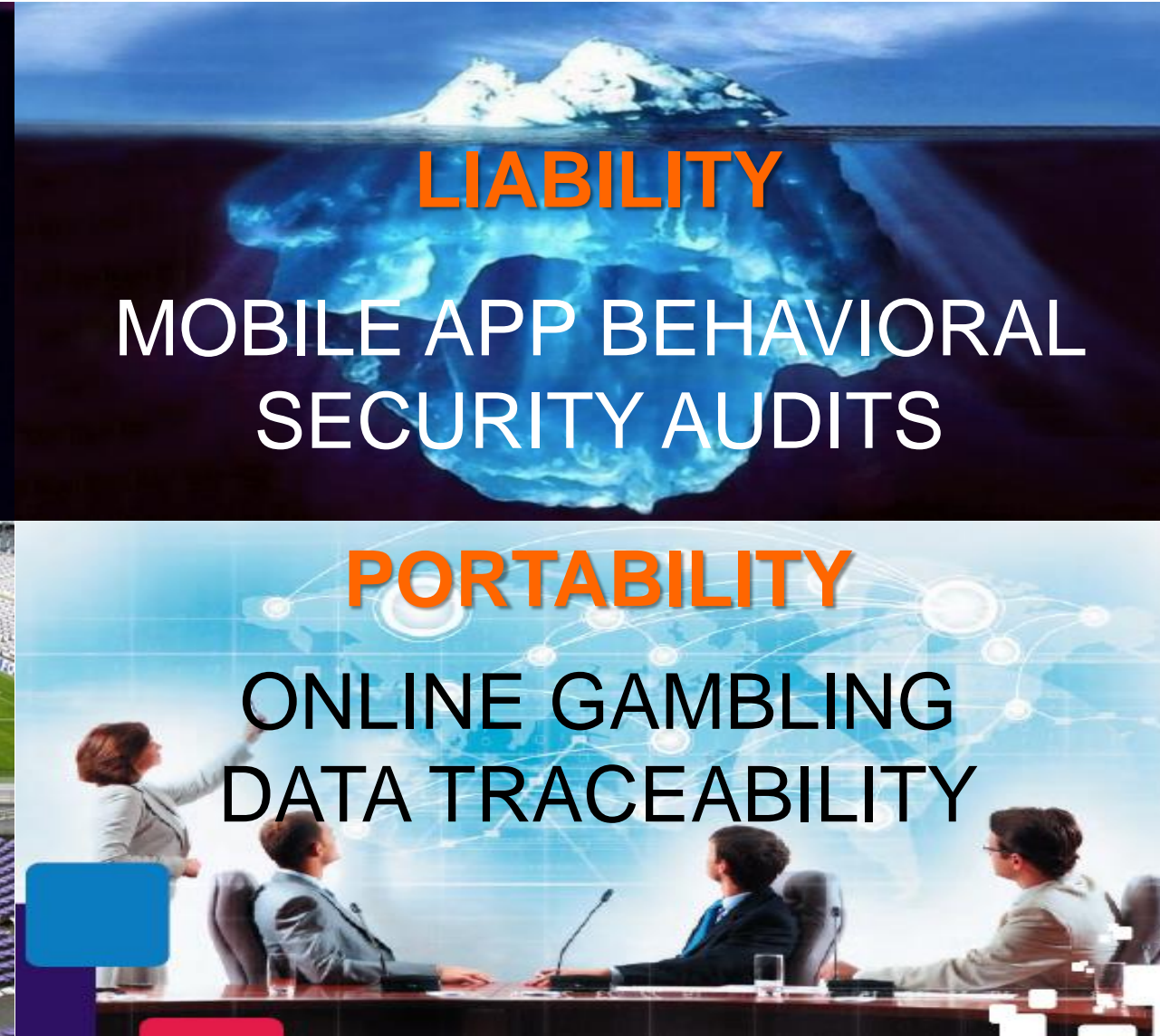


Who & What ... are we talking about?

- Who: SME are here SaaS providers, relying on CSPs
- What: SLA in terms of... availability, liability, usability, portability...
- How: compliance with customers' SLA requirements
- Why: SLA compliance translates leading SME digital roles
- Where: everywhere, online or ... offline!
- When: at anytime, real time...
- 4 examples:



The SME perspective – 4 SME use cases that illustrate some SLA requirements

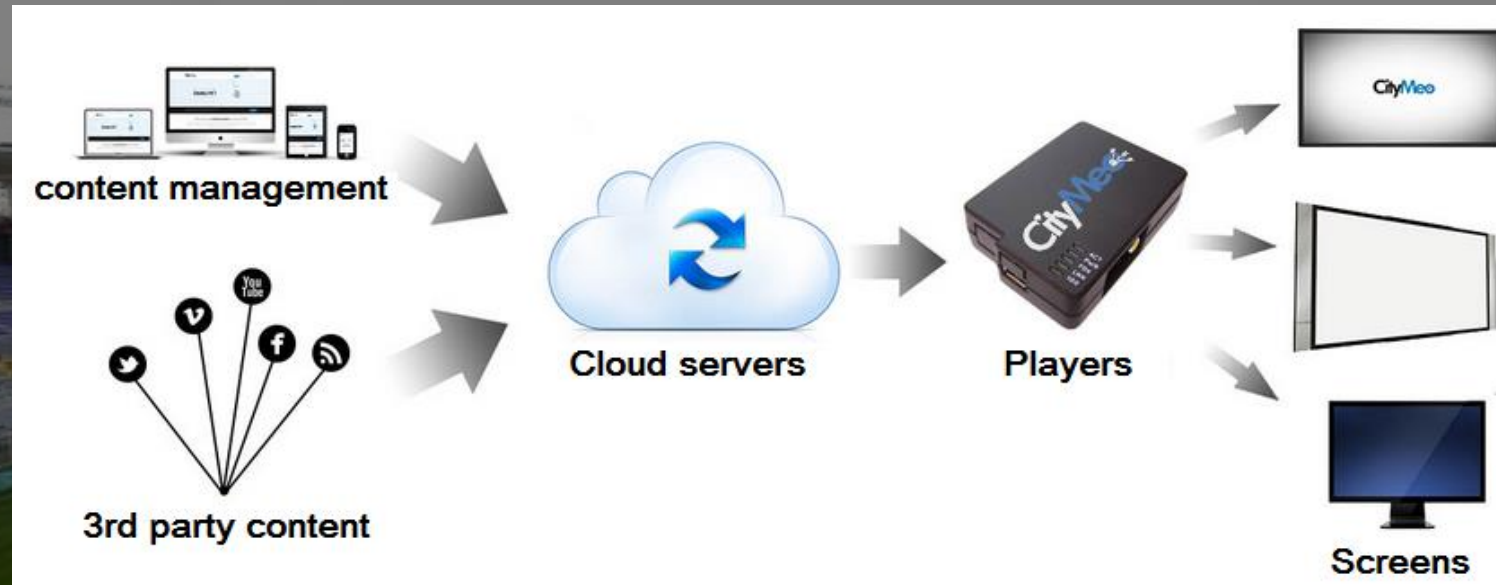




**CLIENT EXPECTS SYSTEM TO RUN REAL TIME ONLINE
PROBLEM IS THAT SYSTEM IS MOBILE & RELIES ON WIFI
CHALLENGE IS TO ASSURE WIFI AVAILABILITY
SLA OFFERING DESIGNED TO BE 100% AVAILABLE**

The « Appsberg » syndrom

**CLIENTS RELY ON BYOD SYSTEMS & APPLICATIONS
PROBLEM IS THAT 25% APPs HAPPEN TO MISBEHAVE
CHALLENGE IS THAT 250K APPS DOWLOADED PER MINUTE
SLA OFFERING DESIGNED TO ENFORCE APP LIABILITY**



**BRANDS WANT DIGITAL CAMPAIGN ON ALL SCREENS
PROBLEM IS THAT SCREENS ARE HETEROGENEOUS
CHALLENGE IS TO MAKE LEGACY SYSTEMS USABLE
SLA OFFERING DESIGNED TO ASSURE 100% USABILITY**



**GAMBLING OPs EXTERNALIZE DATA TRACEABILITY
PROBLEM IS THAT OPERATORS NEED PORTABILITY
CHALLENGE IS TO MIGRATE DATA TO 3rd PARTIES
SLA OFFERING DESIGNED TO COMPLY WITH MIGRATION**

Lessons learned

- #1 SMEs' SLA designed with Medium & Large Enterprises' SLA in mind.
- #2 SLA may include more services requirements than above listed
- #3 SLA "sweet spot" based on convenience, cost and confidence focus
- ...

SLA "by design" can demonstrate how much SME leads digital

SaaS SMEs agree to design Service Levels in order
to turn technology into transformation...



Daniele Catteddu

Managing Director, EMEA,
Cloud Security Alliance



- The lack of transparency of some Cloud Service Providers or brokers
- Lack of clarity in Service Level Agreements
- Cloud security not easy to understand for SME's



- More transparency = **Customer trust!**
- Create a **standardized** way to specify/manage security and privacy among CSPs and Customers.
- Enable **realistic levels of automation** for the whole security life cycle: Plan (negotiation), Do (enforcement), Check (monitoring), Act (remediation)

secSLA + PLA: Advantages

- More transparency = **Customer trust!**
- Create a **standardized** way to specify/manage security and privacy among CSPs and Customers.
- Enable **realistic levels of automation** for the whole security life cycle: Plan (negotiation), Do (enforcement), Check (monitoring), Act (remediation)

secSLA: Scope/Components

- Security Policy
- Asset Management
- Access Control
- Cryptography
- Operations Security
- Communication Security
- Supplier Relationship
- Incident Management
- BCM
- Audits

Privacy: Scope/Components

- Contact information
- Ways in which data will be processed
- Data transfer
- Data security measures
- Monitoring
- Personal Data Breach Notification
- Data portability, Migration and Transfer back assistance
- Data retention, restitution and deletion
- Accountability
- Cooperation
- Law Enforcement Access

Example: secSLA content

- Describe the services covered by the SLA: VM instances, Storage services, etc.
- Describe the CSP's security commitments (Service Level Objectives) and associated metrics:
 - Metrics: % of Critical Vulnerabilities, Frequency of 3rd party audits, Cryptographic Strength, etc.
 - SLO: Availability > 99,999% , Full Backup Frequency < 24hrs, etc.
- Describe (economic) penalties associated to secSLA violation

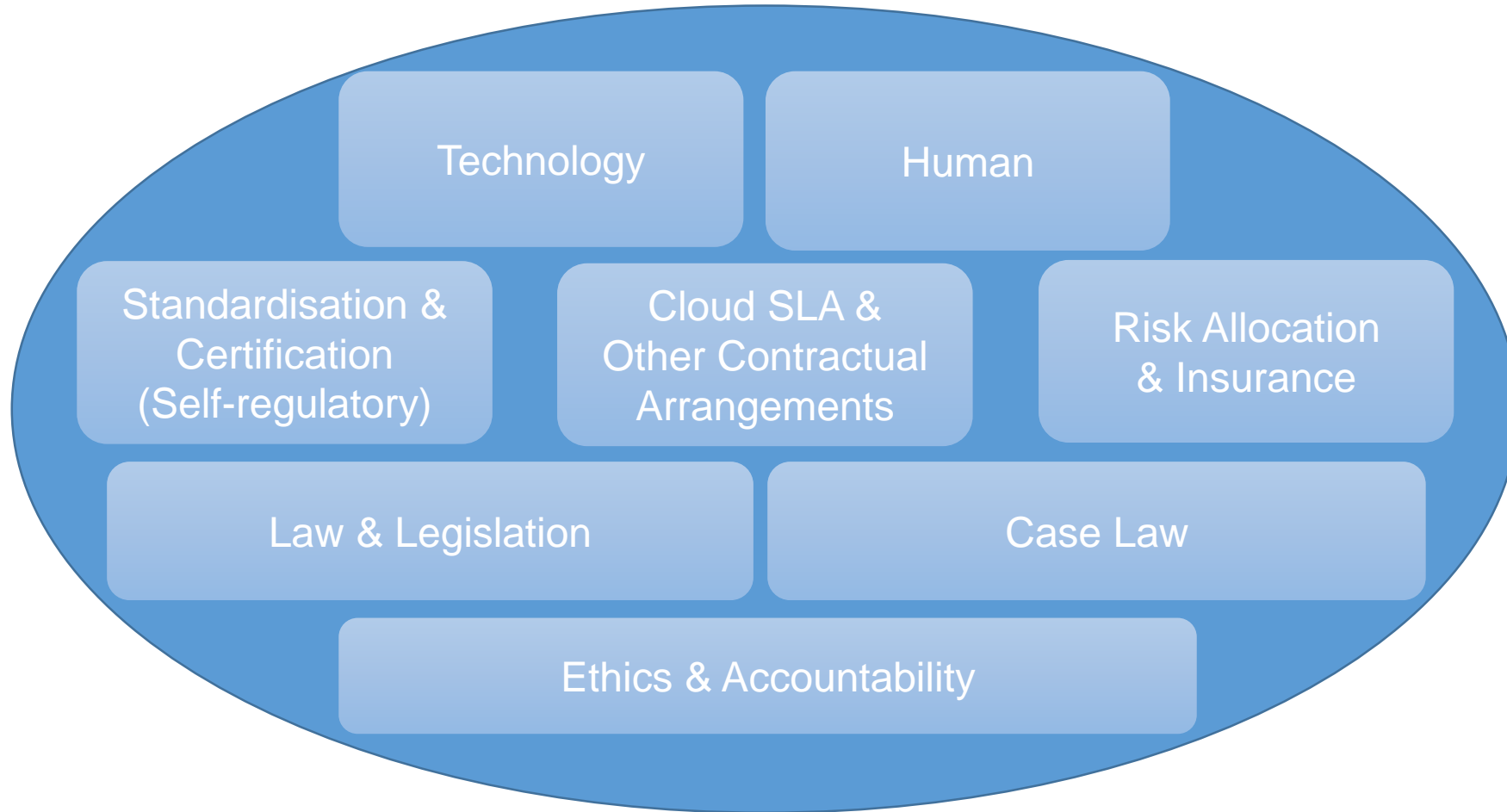


Arthur van der Wees

Managing Director of
international law firm
Arthur's Legal



Cloud Service Level Legal Ecosystem



Cloud SLA Legal Life Cycle

When zooming in at one (1) SLA from a legal, negotiation and contract management perspective, the life cycle of a SLA can be split in seven (7) headline legal life cycle phases:

- 1. Assessment**
- 2. Preparation**
- 3. Negotiation & Contracting**
- 4. Execution & Operation**
- 5. Updates & Amendments**
- 6. Escalation, and;**
- 7. Termination & Consequences of Termination**

A.	PRE-ASSESSMENT RELATION	Preparation	Market Intelligence	Check Specific Cloud Service Provider	Competitors				
B.	PRE-SALES	Non-Disclosure	Inbound Communication	Outbound Communication	Business Case	First Headline Proposal			
C.	FEASIBILITY	Further Assessment	First Pre-Evaluation	Third Party Offers	Fine-tune Goals				
D.	INTENTIONS	Preparation	Business Goals & Strategy	Letter of Intent /Heads of Agreement	Planning & Process Arrangements	Assumptions	Due Diligence		
E.	NEGOTIATIONS	Preparation	Goals	Strategy	Deal Making	Common Ground	BATNA	Boldness vs. Recklessness	
F.	AGREEMENT	Parties	Scope / Out- of-Scope	Diligence	Multi- Disciplinary Involvement	Wording	Double-Check	Authorisation / Sign-Off	
G.	SIGNING	Proceedings	Representation	Double check	Communication	Filing	Press		
H.	EXECUTION	Contract Holder	Project / Plan	Task Management	Communication	Documentation	Filing		
I.	COMMUNICATION	Visit	Contact Channels	e-Tools	Documentation	Filing			
J.	AMENDMENT	Change Objectives	Change Scope	Update	Extension	Filing			
K.	ESCALATION	Preparation / Goal & Strategy	Multi-Disciplinary Involvement	Communication / Documentation	BATNA	Negotiate	Document	Filing	
L.	DISPUTES	Preparation / Goal & Strategy	Dispute Resolution / BATNA	Litigation: Last Resort?	Media	Settlement Agreements	Filing		
M.	END RELATION	Goal & Strategy	Alternatives & Preparation	Termination Agreements	Termination Arrangements	Customer Care	Bankruptcy		



Said Tabet

Senior Technologist and
Industry Standards Strategist,
Corporate Office of the CTO,
EMC Corporation

EMC²



SDOs and Industry Role

- Cloud Standards
- Data Protection, Privacy, Security
- Vocabulary, Interoperability, Architecture
- Liaison Activities between SDOs

Cloud standards

ISO/IEC 17788

(Cloud computing – Vocabulary and overview)

- Collaborative Team (CT) with ITU-T/SG13 to develop common text
- Defines key cloud terminology and provides an overview of cloud computing
- Intended to be a foundation document for cloud computing

ISO/IEC 17789

(Reference architecture)

- Collaborative Team (CT) with ITU-T/SG13 to develop common text
- Covers general concepts and characteristics of cloud computing, the
- components/functions and roles and their capabilities and inter-relationships

Cloud standards (Cont'd)

ISO/IEC 27017: Code of practice for information security controls for cloud computing services based on ISO/IEC 27002

- Common text standard with ITU-T/SG17
- Additional implementation guidance for relevant information security controls specified in ISO/IEC 27002;
- Additional controls and implementation guidance that specifically relate to cloud computing services.

Cloud standards (Cont'd)

ISO/IEC 27036-4

(Information security for supplier relationships – Part 4: Guidelines for security of cloud services)

- Provides cloud service providers and customers
 - Managing the information security risks caused by using cloud services
 - Integrating information security processes and practices into the cloud-based product and service lifecycle service lifecycle processes
 - Responding to risks specific to the acquisition or provision of cloud-based services
- Defines guidelines supporting the implementation of information security security management for the use of cloud services

Cloud Service Level Agreement (Cloud SLA)

ISO/IEC 19086-x

- **19086-1:** Information technology — Cloud computing — Service Level Agreement (SLA) framework — Part 1: Overview and concepts
- **19086-2:** Information Technology - Cloud Computing – Service Level Agreement (SLA) Framework — Part 2: Metrics
- **19086-3:** Information Technology - Cloud Computing – Service Level Agreement (SLA) Framework — Part 3: Core Requirements
- **19086-4:** Information Technology - Cloud Computing – Service Level Agreement (SLA) Framework — Part 4: Security and privacy

Cloud Service Level Agreement (Cloud SLA)

ISO/IEC 19086-x

- Provides an overview of SLAs for cloud services
- Identifies the relationship between the master service agreement and the SLA
- Addresses SLA concepts and requirements that can be used to build SLAs
- Specifies terms and conditions as well as metrics commonly used in SLAs for cloud services
- Establish a set of common SLA building blocks
- Facilitate common understanding between the Cloud Service Providers and the Cloud Service Customers

Discussion

Send your questions using chat



Summary: are we there yet?

- **Standards** (vocabularies, metrics, ...), and best practices (making Cloud SLAs usable for SMEs).
 - ISO/IEC 19086
- Cloud SLAs in **supply chains/multi-cloud** systems.
- **Certifications or SLA's** or both?



Thank you!

www.cloudwatchhub.eu



See other CloudWATCH webinars:
www.cloudwatchhub.eu/webinars