How to negotiate a proper SLA?
SPEAKERS

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
SPEAKERS

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

The SME perspective
The SME perspective

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

AVAILABILITY
COLLABORATIVE REMOTE PRESENCE SYSTEMS

USABILITY
DIGITAL BRAND CAMPAIGN MANAGEMENT

LIABILITY
MOBILE APP BEHAVIORAL SECURITY AUDITS

PORTABILITY
ONLINE GAMBLING DATA TRACEABILITY
The SME perspective – REAL TIME ONLINE AVAILABILITY OF REMOTE PRESENCE

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

The « Appsberg » syndrom
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
Cloud security challenges

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
The legal aspects

Arthur van der Wees
Managing Director of international law firm Arthur's Legal
Cloud Service Level Legal Ecosystem

- Technology
  - Standardisation & Certification (Self-regulatory)
- Human
  - Cloud SLA & Other Contractual Arrangements
  - Risk Allocation & Insurance
- Law & Legislation
- Case Law
- Ethics & Accountability
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
<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A.</td>
<td>PRE-ASSESSMENT RELATION</td>
<td>Preparation</td>
<td>Market Intelligence</td>
<td>Check Specific Cloud Service Provider</td>
</tr>
<tr>
<td>B.</td>
<td>PRE-SALES</td>
<td>Non-Disclosure</td>
<td>Inbound Communication</td>
<td>Outbound Communication</td>
</tr>
<tr>
<td>C.</td>
<td>FEASIBILITY</td>
<td>Further Assessment</td>
<td>First Pre-Evaluation</td>
<td>Third Party Offers</td>
</tr>
<tr>
<td>E.</td>
<td>NEGOTIATIONS</td>
<td>Preparation</td>
<td>Goals</td>
<td>Strategy</td>
</tr>
<tr>
<td>F.</td>
<td>AGREEMENT</td>
<td>Parties</td>
<td>Scope / Out-of-Scope</td>
<td>Diligence</td>
</tr>
<tr>
<td>G.</td>
<td>SIGNING</td>
<td>Proceedings</td>
<td>Representation</td>
<td>Double check</td>
</tr>
<tr>
<td>H.</td>
<td>EXECUTION</td>
<td>Contract Holder</td>
<td>Project / Plan</td>
<td>Task Management</td>
</tr>
<tr>
<td>I.</td>
<td>COMMUNICATION</td>
<td>Visit</td>
<td>Contact Channels</td>
<td>e-Tools</td>
</tr>
<tr>
<td>J.</td>
<td>AMENDMENT</td>
<td>Change Objectives</td>
<td>Change Scope</td>
<td>Update</td>
</tr>
<tr>
<td>K.</td>
<td>ESCALATION</td>
<td>Preparation / Goal &amp; Strategy</td>
<td>Multi-Disciplinary Involvement</td>
<td>Communication / Documentation</td>
</tr>
<tr>
<td>L.</td>
<td>DISPUTES</td>
<td>Preparation / Goal &amp; Strategy</td>
<td>Dispute Resolution / BATNA</td>
<td>Litigation: Last Resort?</td>
</tr>
<tr>
<td>M.</td>
<td>END RELATION</td>
<td>Goal &amp; Strategy</td>
<td>Alternatives &amp; Preparation</td>
<td>Termination Agreements</td>
</tr>
</tbody>
</table>
Said Tabet
Senior Technologist and Industry Standards Strategist, Corporate Office of the CTO, EMC Corporation
SDOs and Industry Role

• Cloud Standards

• Data Protection, Privacy, Security

• Vocabulary, Interoperability, Architecture

• Liaison Activities between SDOs
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 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 processes
  - Responding to risks specific to the acquisition or provision of cloud-based services

- Defines guidelines supporting the implementation of information 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


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