





# Larry Ellison, CEO, Oracle

*“The interesting thing about cloud computing is that we’ve redefined cloud computing to include everything that we already do.... The computer industry is the only industry that is more fashion-driven than women’s fashion.”*

*“I don’t understand what we would do differently in the light of cloud computing other than change the wording of some of our ads.”*

*“Maybe I’m an idiot, but I have no idea what anyone is talking about. What is it? It’s complete gibberish. It’s insane. When is this idiocy going to stop?”*









# Overview

- ★ What is it?
- ★ What is ENISA doing with it?
  - ★ SME migration
  - ★ eGovernment/eHealth
  - ★ Resilience
- ★ What are the implications for eIdentity?
- ★ Where can I go for dinner?

# Is it all hype?



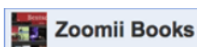
## Net Applications

Net Applications gains a competitive edge over other Web analytics solutions by using Alexa Web Information Service to deliver in-depth Web traffic information.



## The Talk Market

The Talk Market uses Amazon Flexible Payments Service to power their credit card processing pipeline.



## Zoomii

Zoomii pulls book data from Amazon's Product Advertising API to create a highly visual, interactive online bookstore powered by Amazon S3 and EC2.

↑ T

## High Performance Computing



## Harvard Medical School

Harvard's Laboratory for Personalized Medicine (LPM) uses customized Oracle AMIs on Amazon EC2 to run genetic testing models and simulations.



## Pathwork Diagnostics

Pathwork Diagnostics, a molecular diagnostics company, uses Amazon EC2 and UniCloud to run complex algorithms to aid in the identification and diagnosis of cancer tumors.



## Washington Post

The Washington Post uses Amazon EC2 to turn Hillary Clinton's White House schedule



## LiveLeader

LiveLeader estimates that they've saved nearly \$200,000 by deploying their live chat tool for business on Amazon Web Services.



## Morph

Built from the ground up using Amazon Web Services, Morph Labs markets a "full service" deployment, delivery and management system for web applications.



## Napera

Napera built their network security management layer on top of Amazon EC2, allowing them to go to market in under nine months.



## PostRank

As a young, bootstrapped company, the founders of PostRank architected their new service to take advantage of the AWS cloud computing platform. "Without EC2, the project would have been impossible."



## Rackspace

Rackspace Email & Apps, formerly Mailtrust, uses Amazon S3 for a fully scalable, high performance backup system.



## rPath

rPath saves \$80,000 by migrating 7,000 software appliance images from rBuilder Online to Amazon S3.



## Smartsheet

To accommodate their growing business, Smartsheet—a web-based solution for managing tasks, projects and processes—turns to Amazon S3 for document storage.



## StarPound (New)

StarPound Technologies, an enterprise software company, deployed their business process management and telephony platforms on the Amazon Elastic Compute Cloud.



## Risk Assessment of Cloud Computing Technologies Aimed At:

- ★ European Policymakers: research policy.
- ★ European Policymakers: economic incentives, legislation, awareness-raising.
- ★ Business leaders to evaluate the risks and mitigation strategies.
- ★ Individuals/citizens to evaluate the cost/benefit of using consumer cloud apps.

# Process

- ★ Scenario description - selected scenarios:
  - ★ **SME Migration**
  - ★ **Resilience**
  - ★ **Government eHealth**
- ★ Analysis of risks (Assets, Vulnerabilities, Threats)
- ★ Recommendations
- ★ Using ENISA Emerging and Future Risk Framework

# Our Expert Group

- ★ Amazon
- ★ Avenade
- ★ BT
- ★ Bologna University
- ★ Cisco Systems
- ★ Cloudsecurity.org (Craig Balding)
- ★ Fujitsu Labs Europe
- ★ Spire Security
- ★ Google
- ★ HP
- ★ IBM
- ★ Microsoft
- ★ Reservoir Project
- ★ Symantec
- ★ Cloudsecurity.org (Craig Balding)
- ★ The Israeli Association of GRID Technologies (IGT)
- ★ UCL
- ★ Virtualisation.info


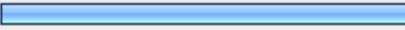

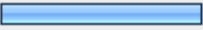

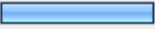
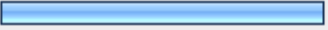
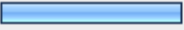
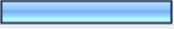

**+ Liason with CSA (Cloud Security Alliance)**

# SME Scenario

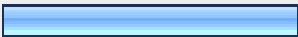
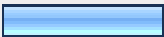
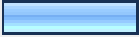



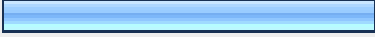

- ★ Security risks for an SME migrating to the cloud.
- ★ Important concern for many SME's.
- ★ Scenario based on a rough survey of the concerns and cloud usage pattern of SME's.



# SME's - Reasons for adoption

Remove economic/expertise barriers impeding to modernize business processes by the introduction of Information Technology		29.5%	18
Avoiding capital expenditure in hardware, software, IT support, Information Security by outsourcing infrastructure/platforms/services		70.5%	43
Flexibility and scalability of IT resources		67.2%	41
Increasing computing capacity and business performance		34.4%	21
Diversification of IT systems		8.2%	5
Local and global optimisation of IT infrastructure through automated management of virtual machines		26.2%	16
Business Continuity and Disaster recovery capabilities		55.7%	34
Assessing the feasibility and profitability of new services (i.e. by developing business cases into the Cloud)		31.1%	19
Adding redundancy to increase availability and resilience		29.5%	18
Controlling marginal profit and marginal costs		14.8%	9

# SME's - Business Processes Considered

Payroll		35.5%	22
Human Resources		19.4%	12
Procurements		16.1%	10
CRM/Sales Management		56.5%	35
Accounting and Finance		32.3%	20
Project management		46.8%	29
Application development on the cloud		45.2%	28
Anonymised data analysis		32.3%	20

# SME's: Main Concerns

	Not Important	Medium Importance	Very Important	Showstopper	Rating Average	Response Count
Privacy	0.0% (0)	12.3% (7)	43.9% (25)	43.9% (25)	3.32	57
Availability of services and/or data	1.8% (1)	10.9% (8)	47.3% (26)	40.0% (22)	3.25	55
Integrity of services and/or data	0.0% (0)	13.0% (7)	42.6% (23)	44.4% (24)	3.31	54
Confidentiality of corporate data	1.8% (1)	3.6% (2)	30.9% (17)	63.6% (35)	3.56	55
Repudiation	2.1% (1)	41.7% (20)	47.9% (23)	8.3% (4)	2.63	48
Loss of control of services and/or data	3.8% (2)	20.8% (11)	47.2% (25)	28.3% (15)	3.00	53
Lack of liability of providers in case of security incidents	2.0% (1)	25.5% (13)	43.1% (22)	29.4% (15)	3.00	51
Inconsistency between trans national laws and regulations	11.8% (6)	43.1% (22)	23.5% (12)	21.6% (11)	2.55	51
Unclear scheme in the pay per use approach	14.0% (7)	46.0% (23)	24.0% (12)	16.0% (8)	2.42	50
Uncontrolled variable cost	4.1% (2)	36.7% (18)	46.9% (23)	12.2% (8)	2.67	49
Cost and difficulty of migration to the cloud (legacy software etc...)	14.3% (7)	53.1% (26)	22.4% (11)	10.2% (5)	2.29	49
Intra-clouds (vendor lock-in) migration	8.3% (4)	37.5% (18)	35.4% (17)	18.8% (9)	2.65	48

# Clean Future: Company Profile

**Name:** Clean Future

**Business Sector:** photovoltaic business. The company produces and supplies complete solar and photovoltaic systems and key components for solar systems and heating

Base in **Germany** with 3 branch offices in **Europe**

Clean Future employs 93 people and a variable number (between 10 and 30) of contractors (interim agents, sales representatives, consultants, trainees, etc.).



# IT and Security requirements

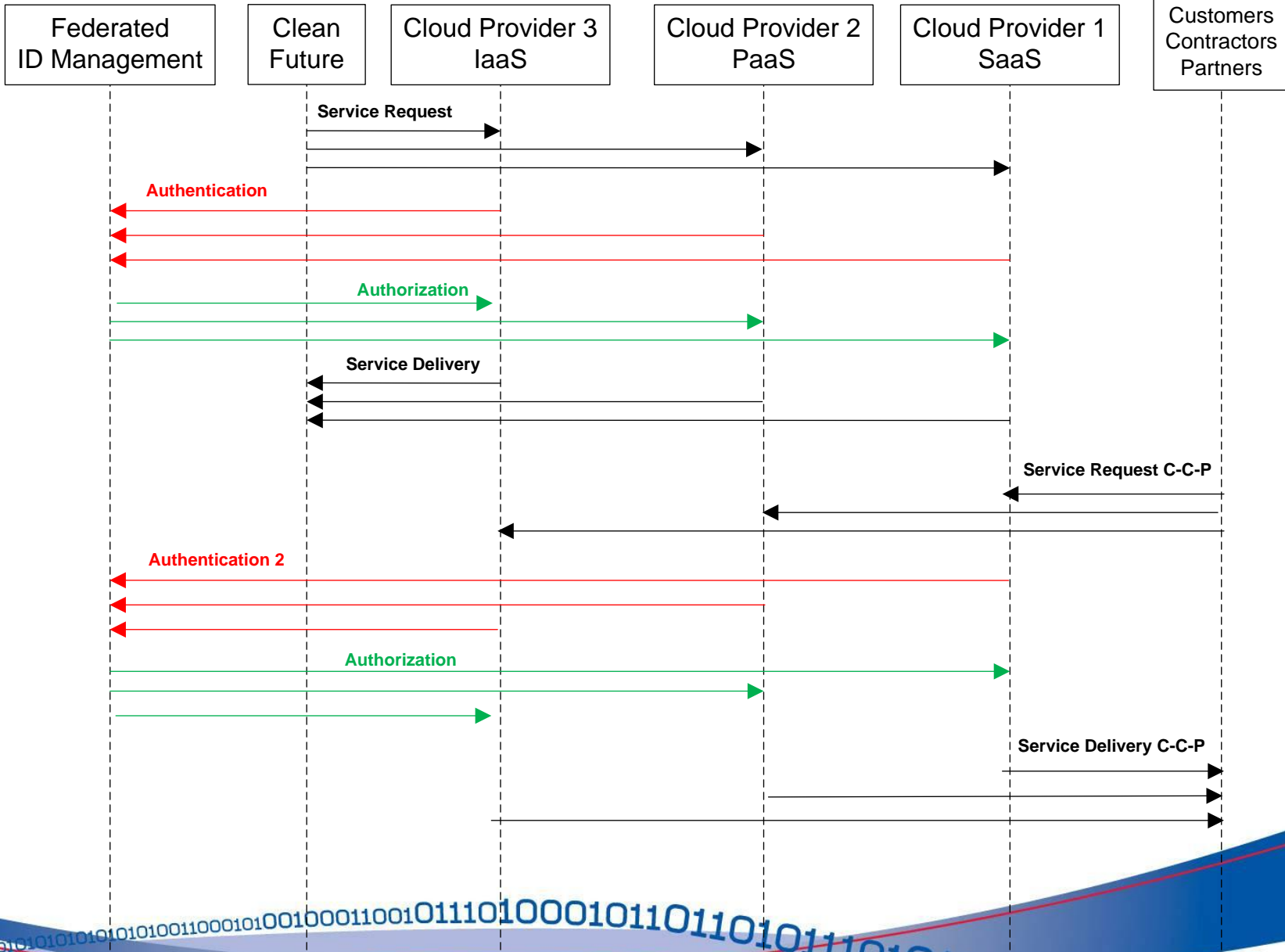
## ★ More flexibility and scalability:

- ★ Variable needs for IT services, employees, partners/suppliers
- ★ Sudden changes in the market
- ★ Possible cooperation with Research Centre, enlargement.

## ★ Business Continuity and Disaster Recovery

## ★ A test-bed for assessing new applications

- ★ Business efficiency and innovation capacity



# Progress so far: Resilience Scenario

## Resilience:



*“The ability of a system to provide & maintain an acceptable level of service in the face of faults (unintentional, intentional, or naturally caused) affecting normal operation.”*

# Resilience Scenario

- ★ Effects of using a cloud computing infrastructure on resilience of a service where high availability, reliability, integrity and confidentiality are crucial to the business model.
  
- ★ Focus on resilience against
  - ★ DDoS
  - ★ Natural Disaster
  - ★ Misuse of platform



# XK-Ord

- ★ Real-time price data and charts for goods in purchasing portals
- ★ Historical data for use in price-prediction and analysis
- ★ Order histories and stock control reports for companies.
- ★ Real-time currency conversion and FX histories
- ★ Provides up to date SOX & EU anti-monopoly trading reports
- ★ Financial data for more complex applications.

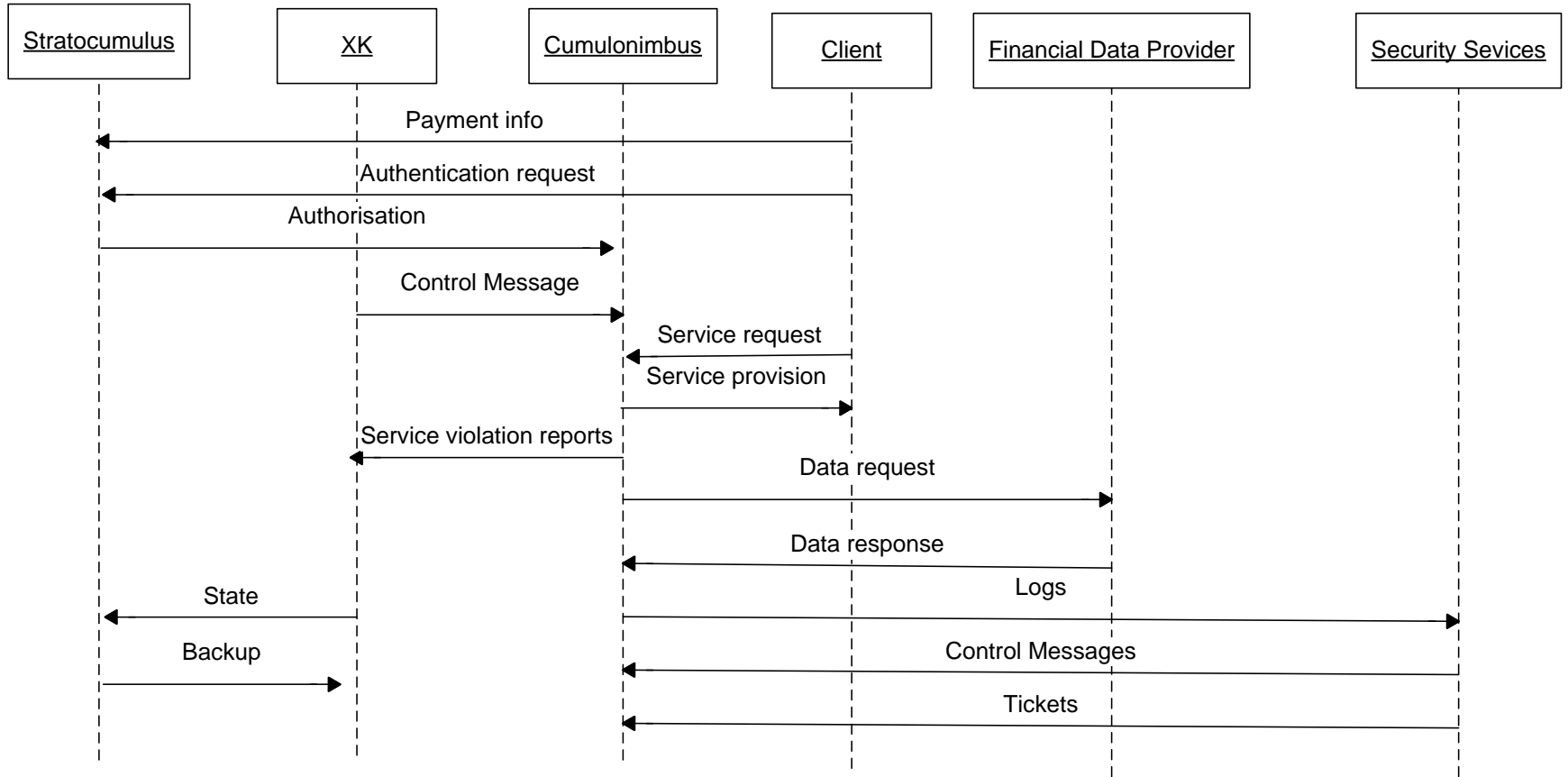
# Requires High reliability of:

- ★ Latency
- ★ Request fulfilment
  - ★ Database queries and result presentation
  - ★ Web server fulfilment of http requests.
  - ★ TCP/IP infrastructure.
- ★ Data integrity
- ★ Confidentiality

# Scenario characteristics

- ★ 2007 – traditional infrastructure
  - ★ Typical data centre managed by XK
  - ★ Multi-homed
  - ★ SAN off-site backup
  - ★ No SLA

- 2012 –cloud infrastructure
  - Shared resources (including network, filtering etc...) with smart management algorithms.
  - Faster and cheaper scaling of resources
  - SLA of XK and cloud provider
  - Cloud disaster recovery



# eHealth Scenario

- ★ In partnership with UK National Health Service (Connecting for Health)
- ★ Special requirements for eGovernment/Sensitive data.
  - ★ E.g. Data must not leave the UK.
- ★ Initial scenario – remote monitoring:
  - ★ Home devices are running on the cloud using IaaS.
  - ★ The services running at the monitoring center are running on the cloud using IaaS.
  - ★ Monitored data is also stored in the cloud using Database as a Service (DaaS).
  - ★ The various eHealth service providers are using cloud computing infrastructures.





# Cloud Identity – Food for Thought



Who Am I?



# A driver for Federated Identity

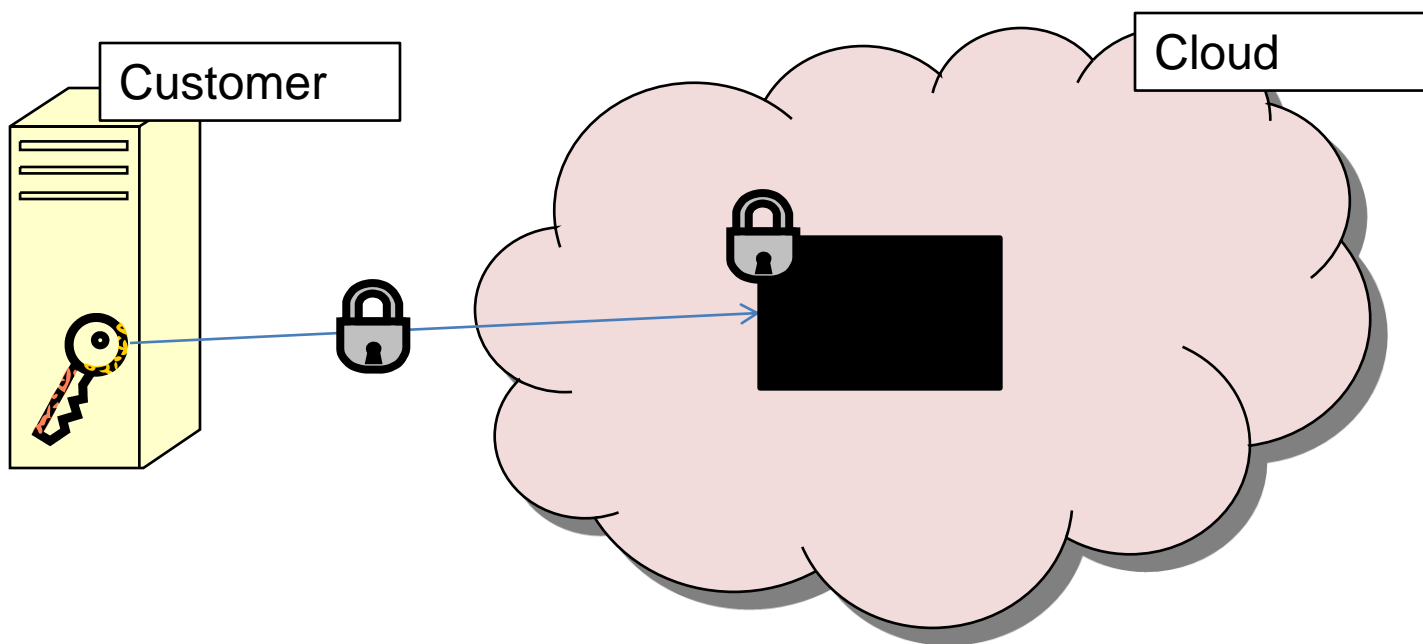
- ★ FIM is the only solution which scales to the cloud.
- ★ FIM providers can also manage key distribution.
- ★ FIM applications themselves (except key storage) can be run using cloud infrastructure.
- ★ Cloud-based IdP gives more resilience of overall system.





# Data storage and processing without security guarantees?

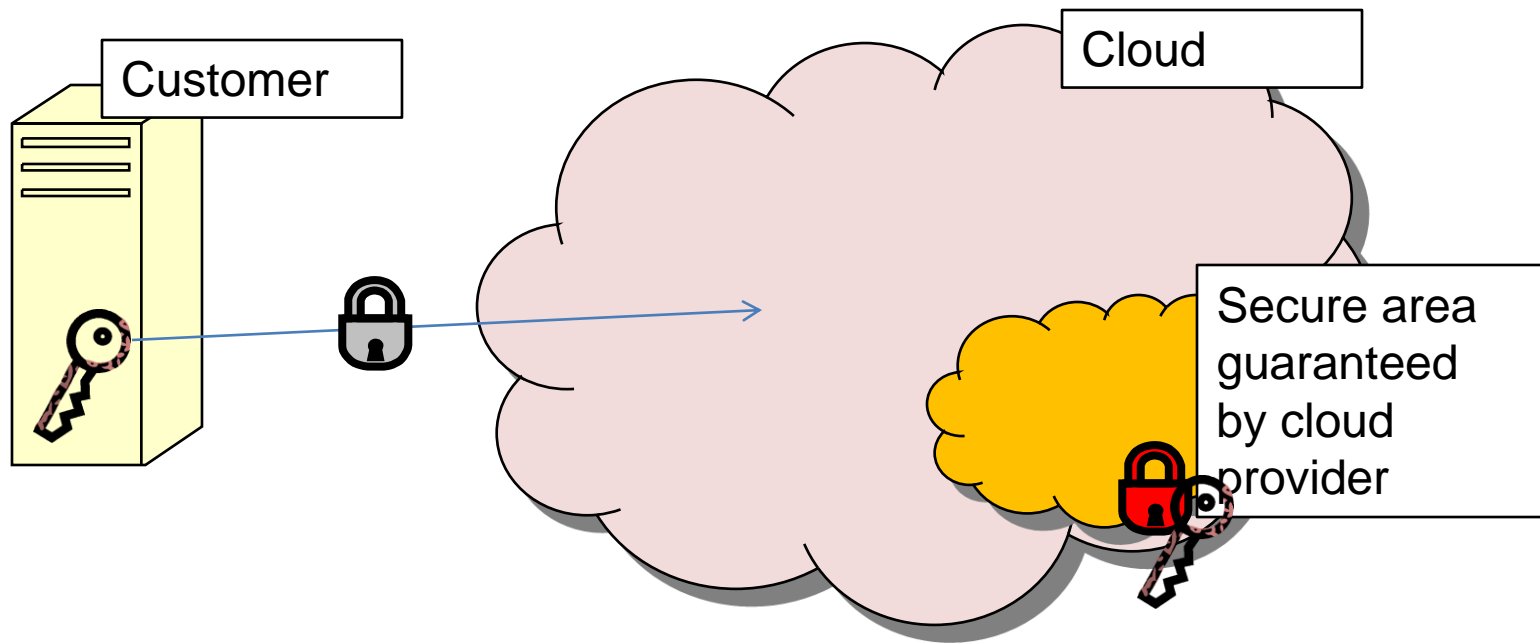
## ★ Alternative 1. – HARD TO IMPLEMENT!



Try to encrypt all operations to hide them from the untrusted hardware

# Data storage and processing without security guarantees?

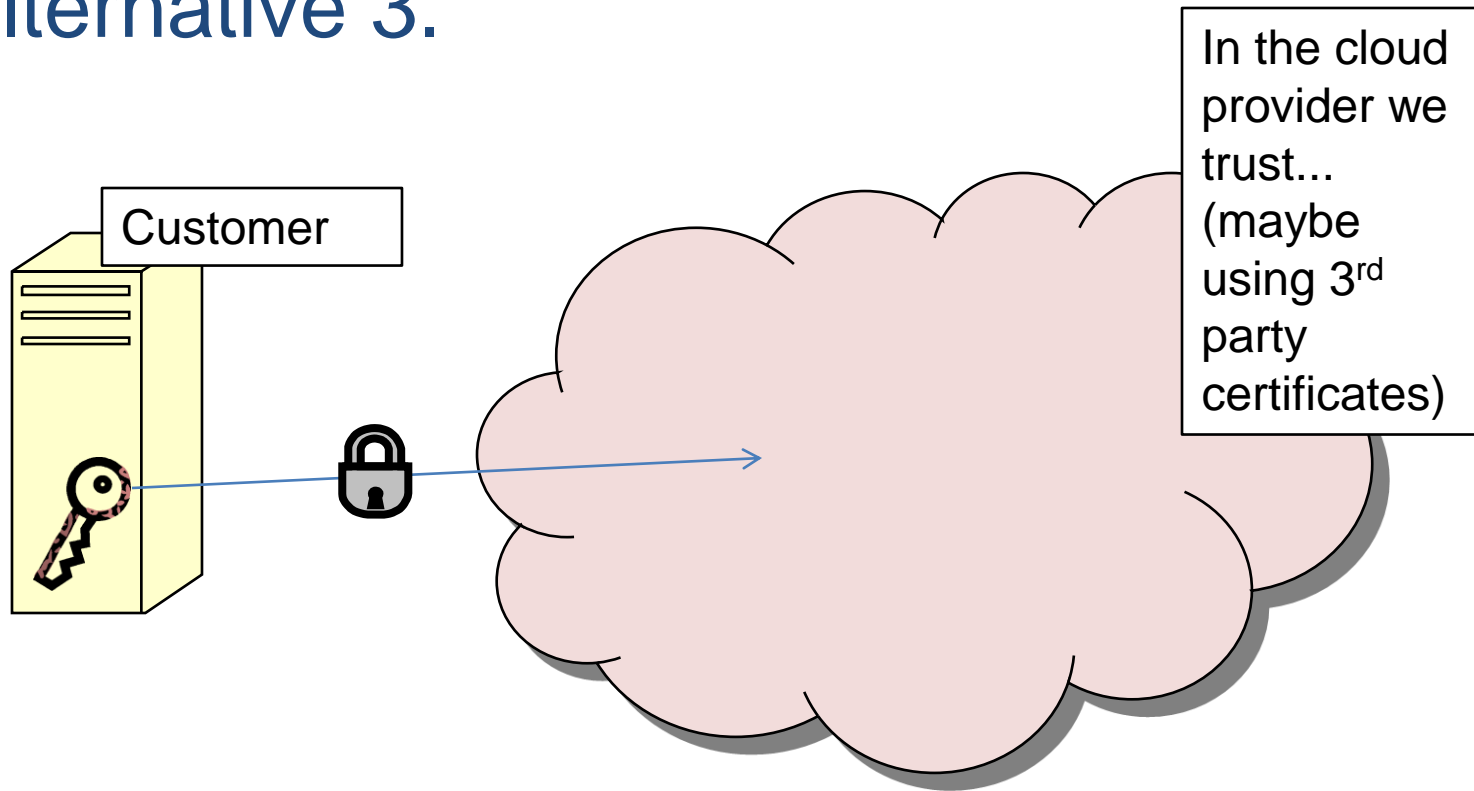
## ★ Alternative 2.



**Use a secure area with security guarantees provided by cloud provider**

# Data storage and processing without security guarantees?

## ★ Alternative 3.



Trust the cloud provider

# Key management 2

- ★ Key storage and provisioning almost impossible to do on-cloud with current technologies
  - ★ HSM's don't scale to the cloud
  - ★ PKCS#10,11 don't talk cloud
  - ★ Revocation is even more complicated...
- ★ Need new crypto and key management standards and solutions adapted to cloud paradigm.

# Drawbacks of current implementations

- ★ Amazon – One Key per account – doesn't scale to multiple accounts/account holders.
- ★ Data security - no alternative but trusting the brand.
  - ★ External pen testing not permitted.
  - ★ External audit not permitted.
  - ★ Very limited logs available.
  - ★ Usually no forensics offered (ghosting a ghost – Craig Balding).
  - ★ No idea of actual location/jurisdiction of data.



# The cloud as an anonymous attack platform

- ★ Poor identity verification makes cloud platforms vulnerable to use as attack platforms. This affects all users.
  - ★ Password cracking
  - ★ DDoS
  - ★ Captcha breaking.
  - ★ IP ranges blocked for other users.

# Other Data protection issues

- ★ Jurisdiction hell (E.g. UK NHS has a requirement that data does not LEAVE the UK)
- ★ Hunt the Data Controller 😊
- ★ Vulnerable to hypervisor layer attacks on virtual machines.
  - ★ No known compromise without access to the hypervisor at this time.
  - ★ BUT – any attacks on hypervisor (even internally) are extremely high impact.
  - ★ (See <http://invisiblethingslab.com/bh08/part3.pdf>)

# Somebody else's problem (SEP)

*“Appirio Cloud Storage fully encrypts each piece of data as it passes from your computer to the Amazon S3 store. Once there, it is protected by the same strong security mechanisms that protect thousands of customers using Amazon’s services” (Thanks to Craig Balding for spotting this)*

# Amazon AWS ToS

- ★ “YOU ARE SOLELY RESPONSIBLE FOR APPLYING APPROPRIATE SECURITY MEASURES TO YOUR DATA, INCLUDING ENCRYPTING SENSITIVE DATA.”
- ★ *“You are personally responsible for all Applications running on and traffic originating from the instances you initiate within Amazon EC2. As such, you should protect your authentication keys and security credentials. Actions taken using your credentials shall be deemed to be actions taken by you.”*

# Key take-aways



- ★ Watch out for the results of ENISA's cloud security study – out in Oct/Nov (<http://www.enisa.europa.eu>)
- ★ The cloud cannot work without federated identity providers.
- ★ Data protection in the cloud – be careful and read our recommendations!
- ★ Key management in the cloud needs a new approach.



